# NetScaler Gateway 13.1

Copyright © 1997–2026. Citrix Systems, Inc. All Rights Reserved.

# Contents

Notas de la versión de NetScaler Gateway 42
Acerca de NetScaler Gateway 43
- Arquitectura de NetScaler Gateway 44
- Cómo funcionan las conexiones de usuario 46
- Conectarse con el cliente de Citrix Secure Access 47
- Conectarse con Citrix Workspace app 48
- Conectarse con dispositivos iOS y Android 48

Despliegues comunes de NetScaler Gateway 50
- Implementar NetScaler Gateway en una DMZ 50
- Conectividad de NetScaler Gateway en una DMZ 51
- Implementar NetScaler Gateway en una red segura 52

Requisitos de software del cliente 53
- Requisitos del sistema del cliente Citrix Secure Access™ 53
- Requisitos de Endpoint Analysis 55

Compatibilidad de NetScaler Gateway con los productos Citrix® 58
- Productos Citrix y versiones compatibles 58
- Aplicaciones Citrix Workspace, aplicaciones de productividad móvil de Citrix y complementos 58

Licencias de NetScaler Gateway 61
- Tipos de licencia de NetScaler Gateway 61
  - La licencia de plataforma 62
  - La licencia universal 62
    - Obtención de la licencia Universal 63
    - Instalación de la licencia universal 64
    - Verificación de la instalación de la licencia universal 64
- Recursos relacionados 65
- Instalar una licencia en NetScaler Gateway 65

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Establecer el número máximo de usuarios 66
verificar la instalación de la licencia Universal 66
Para verificar la instalación de la licencia Universal mediante la GUI 66
Para verificar la instalación de la licencia Universal mediante la CLI 66
Preguntas frecuentes sobre las licencias de NetScaler Gateway 67
¿Cómo puedo obtener ayuda con las licencias de prueba o de demostración? 67
¿Cómo instalar licencias? 67
¿Cuáles son los diferentes tipos de licencias de Gateway? 67
¿Cuántas sesiones de usuario simultáneas se admiten? 67
¿Cómo comprobar las sesiones de usuario simultáneas con licencia actuales? 68
¿Cómo comprobar si se ha alcanzado el límite de rendimiento con licencia? 68
¿Cómo comprobar si se descartan paquetes al alcanzar el rendimiento de la licencia? 68
¿Cómo puedo averiguar cuál es el rendimiento con licencia de un dispositivo NetScaler? 69
¿Cómo agregar más usuarios a las licencias de Gateway existentes? 70
Antes de empezar 71
Requisitos previos para instalar NetScaler Gateway 72
Planificación de la seguridad 73
Configurar la gestión segura de certificados 73
Compatibilidad con la autenticación 73
Proteja su implementación de NetScaler Gateway 74
Lista de comprobación previa a la instalación de Gateway 75
Dispositivos de usuario 75
Conectividad de red básica de NetScaler Gateway 75
Redes internas accesibles a través de NetScaler Gateway 76
Alta disponibilidad 76
Autenticación y autorización 77
Autenticación LDAP 77
Autenticación y autorización RADIUS 78

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Autenticación SAML 78
Apertura de puertos a través de los firewalls (DMZ de un solo salto) 78
En el firewall entre la red no segura y la DMZ 79
En el firewall entre la red segura 79
Citrix Virtual Desktops™, Citrix Virtual Apps o StoreFront 79
Citrix Endpoint Management™ 79
Implementación de DMZ de doble salto con Citrix Virtual Apps™ 80
NetScaler Gateway en la primera DMZ 80
NetScaler Gateway en la segunda DMZ 81
Instalar y configurar el dispositivo NetScaler Gateway 82
Configurar el dispositivo NetScaler Gateway mediante asistentes 82
Asistente de configuración inicial 83
Configurar NetScaler Gateway con el asistente de configuración inicial 83
Asistente de configuración rápida 84
Configurar ajustes con el asistente de configuración rápida 85
Asistente de NetScaler Gateway 89
Configurar ajustes mediante el asistente de NetScaler Gateway 89
Asistente de configuración 90
Asistente de aplicaciones publicadas 90
Configuración integrada de Citrix Endpoint Management 91
Configurar NetScaler Gateway 91
Uso de la utilidad de configuración 92
Iniciar sesión en la utilidad de configuración 92
Crear servidores virtuales 93
Para crear servidores virtuales 94
Puntos a tener en cuenta al vincular un perfil de red al servidor virtual VPN 95
Usuarios actuales y usuarios conectados totales en el servidor virtual 95
Configurar tipos de conexión en el servidor virtual 96

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configurar una política de escucha para servidores virtuales comodín 97
Configurar direcciones IP en NetScaler Gateway 98
Cómo NetScaler Gateway utiliza las direcciones IP 99
Direcciones IP de subred 100
Configurar IPv6 para conexiones de usuario 100
Resolver servidores DNS ubicados en la red segura 101
Para configurar un servicio DNS y un monitor DNS 102
Para vincular un servicio DNS a un servidor virtual DNS 102
Configurar servidores virtuales DNS 102
Para configurar un servidor virtual DNS 103
Configurar proveedores de servicios de nombres 103
Para agregar un servidor DNS a NetScaler Gateway 103
Para agregar un servidor WINS a NetScaler Gateway 104
Para especificar la prioridad de búsqueda de nombres 104
Configurar conexiones iniciadas por el servidor 104
Configurar el rango de puertos privados para conexiones iniciadas por el servidor 106
Configurar el enrutamiento en NetScaler Gateway 107
Configurar una ruta estática 107
Configurar la negociación automática 108
Para habilitar o deshabilitar la negociación automática 108
Configurar el nombre de host y el FQDN en NetScaler Gateway 109
Para ver el FQDN de un certificado 109
Políticas y perfiles en NetScaler Gateway 109
Cómo funcionan las políticas 110
Políticas condicionales 110
Prioridades de las políticas 111
Crear directivas en NetScaler Gateway 112
Configuración de expresiones del sistema 112

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configuración de expresiones de seguridad del cliente 113
Administración de certificados en NetScaler Gateway 113
Crear una solicitud de firma de certificado 114
Crear una CSR mediante el asistente de NetScaler Gateway 115
Crear una CSRÂ mediante la GUI de NetScaler 115
Instalar el certificado firmado en NetScaler Gateway 115
Configurar certificados intermedios 117
Instalar un certificado intermedio 119
Vincular un certificado intermedio a un certificado de servidor 119
Usar certificados de dispositivo para la autenticación 120
Pasos para configurar certificados de dispositivo 121
Habilitar la comprobación del certificado de dispositivo en un servidor virtual para la política EPA clásica 122
Verificación del certificado de dispositivo en una máquina Windows 122
Importar e instalar un certificado existente 123
Para instalar el certificado y la clave privada en NetScaler Gateway 124
Convertir un certificado del formato PFX al formato PEM 125
`OpenSSL utility` 126
Listas de revocación de certificados 128
Parámetros de actualización de CRL 129
Supervisar el estado del certificado con OCSP 132
Configurar el estado del certificado OCSP 133
Administración de certificados en NetScaler Gateway 135
Crear una solicitud de firma de certificado 136
Crear una CSR mediante el asistente de NetScaler Gateway 136
Crear una CSRÂ mediante la GUI de NetScaler 137
Instalar el certificado firmado en NetScaler Gateway 137
Configurar certificados intermedios 139

© 1997–2026 Citrix Systems, Inc. All rights reserved. 

Instalar un certificado intermedio 141
Vincular un certificado intermedio a un certificado de servidor 141
Usar certificados de dispositivo para la autenticación 142
Pasos para configurar certificados de dispositivo 143
Habilitar la comprobación del certificado de dispositivo en un servidor virtual para la política EPA clásica 144
Verificación del certificado de dispositivo en una máquina Windows 144
Importar e instalar un certificado existente 145
Para instalar el certificado y la clave privada en NetScaler Gateway 146
Listas de revocación de certificados 147
Parámetros de actualización de CRL 148
Supervisar el estado del certificado con OCSP 151
Configurar el estado del certificado OCSP 153
Gestionar la configuración de NetScaler Gateway 154
Guardar la configuración de NetScaler Gateway 154
Para guardar la configuración en NetScaler Gateway 154
Para ver y guardar el archivo de configuración en NetScaler Gateway 155
Para ver la configuración en ejecución actual 155
Para comparar la configuración guardada y la configuración en ejecución 155
Borrar la configuración de NetScaler Gateway 156
Para borrar la configuración de NetScaler Gateway 157
Pruebe la configuración de NetScaler Gateway 157
Crear una cuenta de usuario mediante la GUI 157
Actualizar el software de NetScaler Gateway 159
Buscar actualizaciones de software 159
Actualizar NetScaler Gateway mediante el Asistente de actualización 160
Actualizar NetScaler Gateway mediante un símbolo del sistema 160
Implementar NetScaler Gateway en una DMZ de doble salto 161

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Cómo funciona una implementación de doble salto 162
Prepararse para una implementación de DMZ de doble salto 163
Componentes necesarios para iniciar la implementación 163
Flujo de comunicación en una implementación de DMZ de doble salto 164
Proceso de conexión 165
Instalación y configuración de NetScaler Gateway en una DMZ de doble salto 168
Instalar NetScaler Gateway en la primera DMZ 168
Configurar NetScaler Gateway en la primera DMZ 168
Instalar NetScaler Gateway en la segunda DMZ 168
Configurar ajustes en los servidores virtuales del proxy de NetScaler Gateway 169
Para habilitar el doble salto en el servidor virtual del proxy de NetScaler Gateway mediante la GUI 169
Para deshabilitar la autenticación en el servidor virtual del proxy de NetScaler Gateway mediante la GUI 170
Configurar el dispositivo para que se comunique con el proxy del dispositivo 171
Para configurar NetScaler Gateway para que se comunique con el proxy de NetScaler Gateway 171
Para vincular globalmente el servidor de salto siguiente de NetScaler Gateway 171
Para enlazar el servidor de siguiente salto de NetScaler Gateway a un servidor virtual 172
Configurar NetScaler Gateway para gestionar el tráfico STA e ICA 172
Abrir los puertos adecuados en los firewalls 173
Mantenimiento y monitorización del sistema 176
Configuración de administradores delegados 176
Configuración de directivas de comandos para administradores delegados 177
Para crear un usuario administrativo en NetScaler Gateway 178
Creación de grupos administrativos 178
Configuración de directivas de comandos personalizadas para administradores delegados 179
Para crear una directiva de comandos personalizada simple 179

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Para crear una directiva de comandos personalizada avanzada 180
Para vincular una política de comandos personalizada a un usuario o grupo 180
Configuración de auditoría en NetScaler Gateway 181
Configuración de registros en NetScaler Gateway 182
Para crear una directiva de auditoría 182
Para vincular una directiva de auditoría globalmente 183
Para modificar una directiva de auditoría 183
Para eliminar una directiva de auditoría 184
Configuración del registro de ACL 184
Para configurar el registro de ACL mediante la utilidad de configuración 185
Para habilitar el registro de ACL o TCP en NetScaler Gateway 185
Habilitación del registro de Citrix Secure Access™ 186
Para supervisar las conexiones ICA® 187
Registros de sesión ICA 187
Autenticación y autorización 189
Configuración de tipos de autenticación global predeterminados 190
Para configurar la autenticación globalmente 191
Configuración de la autenticación sin autorización 191
Configuración de la autorización 192
Configuración de directivas de autorización 192
Ejemplos de expresiones de políticas de autorización 193
Para configurar una política de autorización mediante la GUI 193
Para vincular una política de autorización a un usuario mediante la GUI 194
Para vincular una política de autorización a un grupo mediante la GUI 194
Configuración de la autorización global predeterminada 194
Deshabilitar la autenticación 195
Para deshabilitar la autenticación 195
Configuración de la autenticación para horas específicas 196

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Para configurar la autenticación por hora, fecha o día de la semana 196
Cómo funcionan las políticas de autenticación 196
Configuración de perfiles de autenticación 197
Para crear una directiva de autenticación mediante la utilidad de configuración 198
Para modificar una directiva de autenticación mediante la utilidad de configuración 198
Para eliminar una directiva de autenticación 198
Enlazar directivas de autenticación 199
Para enlazar una directiva de autenticación globalmente mediante la GUI 199
Para desenlazar una directiva de autenticación global mediante la GUI 199
Establecer prioridades para las directivas de autenticación 199
Para establecer o cambiar la prioridad de las directivas de autenticación globales 200
Para cambiar la prioridad de una directiva de autenticación vinculada a un servidor virtual 200
Configuración de usuarios locales 200
Para crear usuarios locales 200
Para cambiar la contraseña de un usuario 201
Para cambiar el método de autenticación de un usuario 201
Para eliminar un usuario 201
Configuración de grupos 202
Para crear un grupo 202
Para eliminar un grupo 202
Adición de usuarios a grupos 203
Configuración de directivas con grupos 203
Configuración de la autenticación LDAP 204
Para configurar la autenticación LDAP mediante la utilidad de configuración 207
Determinar atributos en su directorio LDAP 209
Configuración de la extracción de grupos LDAP 209
Cómo funciona la extracción de grupos LDAP directamente desde el objeto de usuario 210
Cómo funciona la extracción de grupos LDAP del objeto de grupo indirectamente 210

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Campos de atributo de grupo de autorización LDAP 211
Para configurar la autorización LDAP 211
Configuración de la extracción de grupos anidados de LDAP 211
Configuración de la extracción de grupos LDAP para varios dominios 213
Creación de directivas de sesión para la extracción de grupos 213
Creación de directivas de autenticación LDAP para varios dominios 214
Creación de grupos y vinculación de directivas para la extracción de grupos LDAP para varios dominios 215
Notificación de caducidad de contraseña de 14 días para autenticación LDAP 216
Configuración de la autenticación de certificados de cliente 217
Para configurar el certificado de cliente como tipo de autenticación predeterminado mediante la GUI 217
Extracción del nombre de usuario del certificado de cliente 218
Configuración y vinculación de una política de autenticación de certificado de cliente 218
Configuración de la autenticación de certificado de cliente de doble factor 220
Configuración de la autenticación con tarjeta inteligente 220
Configuración de la autenticación con tarjeta inteligente con conexiones Secure ICA® 222
Configuración de la autenticación RADIUS 223
Configuración de Gemalto Protiva 224
Configuración de SafeWord 224
Para configurar la autenticación RADIUS 224
Elección de protocolos de autenticación RADIUS 225
Configuración de la extracción de direcciones IP 226
Configuración de la extracción de grupos RADIUS 227
Configuración de RADIUS en Windows Server 2003 227
Configuración de RADIUS para la autenticación en Windows Server 2008 228
Para configurar la autorización RADIUS 230
Configuración de la contabilidad de usuarios RADIUS 230

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Para crear una directiva RADIUS 232
Para crear una directiva de sesión 232
Para enlazar la directiva de sesión globalmente 233
Para enlazar la directiva de sesión a un servidor virtual de NetScaler Gateway 233
Configuración de la autenticación SAML 234
Configuración de Active Directory Federation Services 2.0 235
Configuración de la autenticación SAML de dos factores 237
Para configurar la autenticación SAML 238
Referencias 242
Mejoras en la autenticación SAML 242
Solución 242
Plataforma 243
Configuración 243
Uso de la autenticación SAML para iniciar sesión en NetScaler Gateway 244
Plataformas y aplicaciones compatibles 244
Configurar la autenticación SAML mediante directivas SAML avanzadas 244
Configuración de la autenticación TACACS+ 245
Borrar Configuración Básica No Debe Borrar la Configuración TACACS 246
Nuevo Comando 246
Configuración de CLI 247
Configuración de la autenticación multifactor 247
Configuración de la autenticación en cascada 248
Para establecer la prioridad de las políticas de autenticación globales 248
Para cambiar la prioridad de una política de autenticación vinculada a un servidor virtual 249
Configuración de la autenticación de dos factores 249
Para configurar la autenticación de dos factores 250
Seleccionar el tipo de autenticación para el inicio de sesión único 250
Configuración de certificados de cliente y autenticación de dos factores LDAP 251

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configuración del inicio de sesión único 254
Configuración del inicio de sesión único con Windows 254
Para configurar el inicio de sesión único con Windows globalmente 255
Para configurar el inicio de sesión único con Windows mediante una directiva de sesión 255
Configuración del inicio de sesión único para aplicaciones web 255
Para configurar el inicio de sesión único para aplicaciones web globalmente 256
Para configurar el inicio de sesión único para aplicaciones web mediante una directiva de sesión 256
Para definir el puerto HTTP para el inicio de sesión único en aplicaciones web 256
Configuración del inicio de sesión único en aplicaciones web mediante LDAP 257
Configuración de inicio de sesión único en un dominio 258
Para configurar el inicio de sesión único en un dominio 258
Configuración del inicio de sesión único para Microsoft Exchange 2010 259
Realice lo siguiente mediante la CLI 259
Configuración de reescritura mediante la CLI 260
Configuración del uso de contraseñas de un solo uso 260
Configuración de la autenticación RSA SecurID 261
Configuración de la devolución de contraseñas con RADIUS 262
Configuración de la autenticación SafeWord 264
Configuración de la autenticación Gemalto Protiva 265
nFactor para la autenticación de Gateway 265
Requisitos de licencia de las funciones de autenticación, autorización y auditoría 266
Casos de uso 268
Gestión de respuestas de autenticación 269
Soporte al cliente 269
Compatibilidad del tipo de credencial de WebView con los mecanismos de autenticación 270
Configuración de línea de comandos 270
Desafíos de interoperabilidad 271

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Análisis de puntos finales (EPA) 271
Consideraciones sobre la configuración incorrecta 271
Definición de clientes 271
Restricción de nFactor para Gateway 272
LoginSchema 272
Descripción del parámetro 273
Conocimientos necesarios sobre LoginSchema y nFactor 274
Configuración de la autenticación de doble factor sin usar LoginSchema 274
Expresiones de nombre de usuario y contraseña 274
Pasos de alto nivel en la configuración de nFactor 275
Configuración de la GUI 276
Crear un servidor virtual 276
Crear un servidor virtual de autenticación 280
Crear un perfil CERT de autenticación 282
Crear una directiva de autenticación 283
Agregar un servidor de autenticación LDAP 284
Agregar una política de autenticación LDAP 284
Agregar un servidor de autenticación RADIUS 285
Agregar una directiva de autenticación RADIUS 285
Crear un esquema de inicio de sesión de autenticación 286
Crear una etiqueta de directiva 287
Configuración de re-Captcha para la autenticación nFactor 289
Configuración de Captcha 289
Crear un servidor virtual de Gateway para la autenticación nFactor en la licencia estándar de NetScaler 295
Referencias 297
Visualizador de Unified Gateway 297
Configurar Unified Gateway 298

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configuración de la GUI 301

Detalles de los servidores virtuales VPN 303

`The Pre Auth Block` 306

`The Auth Block` 307

Adición de StoreFront™ 309

Adición de SaaS 310

Adición de aplicaciones web 311

Configurar NetScaler Gateway para usar autenticación RADIUS y LDAP con dispositivos móviles/tabletas 313

Restringir el acceso a NetScaler Gateway para miembros de un grupo de Active Directory 323

Método de filtro de búsqueda LDAP 324

Información general 324

Requisitos previos 324

Pasos para configurar un filtro de búsqueda LDAP para miembros de un grupo de Active Directory 324

Método de directiva de sesión de NetScaler Gateway 327

Soporte OTP nativo para autenticación 329

Ventajas del soporte OTP nativo 330

Flujo de trabajo de OTP nativo 330

Requisitos previos 331

Configurar OTP nativo mediante la GUI 332

Crear esquema de inicio de sesión para el primer factor 332

Configurar el servidor virtual de autenticación, autorización y auditoría 332

Crear esquema de inicio de sesión para OTP de segundo factor 334

Configurar la política de conmutación de contenido para gestionar OTP 334

Configurar OTP nativo mediante la CLI 335

Para configurar la página de registro y administración de dispositivos OTP 335

Para crear una acción de inicio de sesión LDAP 335

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Para agregar una directiva de autenticación para el inicio de sesión LDAP 336
Para presentar la interfaz de usuario a través de LoginSchema 336
Mostrar la página de registro y administración de dispositivos 336
Para configurar la página de inicio de sesión de usuario mediante la CLI 337
Registre su dispositivo con NetScaler 339
Iniciar sesión en NetScaler mediante la OTP 341
Uso de alta disponibilidad 342
Cómo funciona la alta disponibilidad 344
Directrices para configurar la alta disponibilidad 344
Configuración de ajustes para alta disponibilidad 345
Para añadir un nodo de alta disponibilidad 346
Para habilitar o deshabilitar el nodo secundario 347
Para configurar los ajustes de alta disponibilidad 347
Cambiar la contraseña de un nodo RPC 347
Para cambiar la contraseña de un nodo RPC y habilitar una conexión segura 348
Para cambiar la contraseña de un nodo RPC mediante la CLI 348
Configuración de los dispositivos principal y secundario para alta disponibilidad 349
Configuración de los intervalos de comunicación 350
Para configurar los intervalos de comunicación para el NetScaler Gateway secundario 350
Sincronización de dispositivos NetScaler Gateway 351
Para habilitar o inhabilitar la sincronización de alta disponibilidad 351
Para forzar la sincronización entre dispositivos 351
Sincronización de archivos de configuración en una configuración de alta disponibilidad 352
Parámetros para sincronizar archivos en una configuración de alta disponibilidad 352
Para sincronizar archivos en una configuración de alta disponibilidad mediante la utilidad de configuración 353
Configuración de la propagación de comandos 353
Para habilitar o deshabilitar la propagación en el nodo principal 354

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Solución de problemas de propagación de comandos 354
Configurar el modo a prueba de fallos 355
Para configurar el modo a prueba de fallos 357
Configuración de la dirección MAC virtual 357
Configuración de direcciones MAC virtuales IPv4 358
Creación o modificación de una dirección MAC virtual IPv4 358
Configuración de direcciones MAC virtuales IPv6 360
Crear o modificar una dirección MAC virtual para IPv6 360
Configuración de pares de alta disponibilidad en subredes diferentes 361
Cómo funciona la configuración de red independiente 361
Adición de un nodo remoto 363
Para agregar un nodo remoto para el modo de computación de red independiente 363
Para eliminar un nodo remoto 363
Configuración de monitores de ruta 364
Agregar o eliminar monitores de ruta 366
Para agregar un monitor de ruta 366
Para eliminar un monitor de ruta 366
Configuración de la redundancia de enlaces 366
Para configurar la redundancia de enlaces 367
Para quitar interfaces del conjunto de interfaces de conmutación por error 367
Para quitar un conjunto de interfaces de conmutación por error 367
Comprensión de las causas de la conmutación por error 368
Forzar la conmutación por error desde un nodo 369
Forzar la conmutación por error en el nodo principal o secundario 369
Para forzar la conmutación por error en el nodo principal o en un nodo secundario 370
Forzar al nodo principal a permanecer como principal 370
Para forzar al nodo principal a permanecer como principal 370
Forzar que el nodo secundario permanezca secundario 370

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Para forzar que el nodo secundario permanezca secundario 371

Para devolver NetScaler Gateway al servicio como un dispositivo de alta disponibilidad activo 371

Uso de la agrupación en clúster 372

Configuración de clúster 372

Para crear una instancia de clúster de NetScaler Gateway mediante la utilidad de configuración 373

Adición de nodos a un clúster de NetScaler Gateway 374

Creación de un grupo de nodos de clúster 375

Vincular el nodo de clúster local al grupo de nodos del clúster 375

Vinculación de un servidor virtual de NetScaler Gateway al grupo de nodos del clúster 376

Unified Gateway 378

NetScaler con Unified Gateway: una única URL 378

El asistente de configuración de Unified Gateway 379

Administración de configuración adicional 380

Servidor virtual de conmutación de contenido 381

Servidor virtual VPN 381

Preguntas frecuentes sobre Unified Gateway 382

¿Qué es Unified Gateway? 382

¿Por qué usar Unified Gateway? 382

¿Puede haber más de un servidor virtual Unified Gateway? 382

¿Por qué se necesita la conmutación de contenido para Unified Gateway? 383

En versiones anteriores a la 11.0, la conmutación de contenido se puede utilizar para recibir tráfico para varios servidores virtuales. ¿Ese uso también se denomina Unified Gateway? 383

¿Qué ha cambiado con las directivas de conmutación de contenido en Unified Gateway? 383

¿Qué funciones de NetScaler Gateway no son compatibles actualmente con Unified Gateway? 383

Con Unified Gateway, ¿cuál es el comportamiento de los escaneos de EPA? 384

¿Cuáles son los requisitos de licencia para Unified Gateway? 384

© 1997–2026 Citrix Systems, Inc. All rights reserved. 

¿El servidor virtual de NetScaler Gateway utilizado con Unified Gateway necesita una configuración de IP/Puerto/SSL? 384

¿Necesito reaprovisionar los certificados SSL/TLS que están en el servidor virtual de NetScaler Gateway para usarlos con un servidor virtual de Unified Gateway? 384

¿Cuál es la diferencia entre una URL única y una implementación de varios hosts? ¿Cuál necesito? 384

¿Qué mecanismos de autenticación se pueden usar con Unified Gateway? 385

¿Qué es la autenticación “SelfAuth”? 385

¿Qué es la autenticación «StepUp»? 386

Is StepUp authentication supported for NetScaler AAA TM virtual servers? 386

¿Qué es `login once/logout once`? 386

¿Se pueden especificar políticas de autenticación comunes a nivel de Unified Gateway con un servidor virtual de equilibrio de carga NetScaler AAA TM específicamente autenticado y vinculado a nivel de servidor virtual de equilibrio de carga? ¿Cuáles son los pasos de configuración para admitir este caso de uso? 386

¿Cómo se configura Unified Gateway para que los servidores virtuales de NetScaler AAA TM vinculados tengan sus propias políticas de autenticación? 387

¿Se requiere un servidor virtual de autenticación NetScaler AAA TM para autenticar a los usuarios que acceden a través de un servidor virtual de Unified Gateway? 387

¿Dónde se especifican las directivas de autenticación de NetScaler Gateway: en el servidor virtual de Unified Gateway o en el servidor virtual de NetScaler Gateway? 387

¿Cómo se habilita la autenticación en los servidores virtuales de NetScaler AAA TM detrás de un servidor virtual de conmutación de contenido de Unified Gateway? 387

¿Cómo agrego servidores virtuales TM detrás de la conmutación de contenido (URL única frente a varios hosts)? 387

¿Qué sucede con las directivas de autenticación vinculadas a un servidor virtual de equilibrio de carga de NetScaler AAA TM si ese servidor virtual se mueve detrás de un servidor virtual de Unified Gateway? 388

¿Cómo se configuran las directivas de sesión para las sesiones de NetScaler AAA TM? 388

¿Cuáles son los cambios en el portal de NetScaler Gateway en NetScaler 11.0? 388

¿NetScaler 11.0 admite la personalización del portal de NetScaler Gateway? 388

© 1997–2026 Citrix Systems, Inc. All rights reserved. 

¿Se admiten los temas del portal en implementaciones de alta disponibilidad o clúster de NetScaler? 389

¿Se migrarán mis personalizaciones como parte del proceso de actualización de NetScaler 11.0? 389

¿Hay algún paso previo a la actualización que seguir para preparar los temas del portal en NetScaler 11.0? 389

Tengo personalizaciones almacenadas en la instancia de NetScaler, invocadas por rc.conf o rc.netscaler. ¿Cómo me muevo a los temas del portal? 390

¿Cómo puedo exportar mis personalizaciones actuales y guardarlas antes de actualizar a NetScaler 11.0? ¿Puedo mover los archivos exportados a otro dispositivo NetScaler? 390

¿Se admiten los temas del portal para los servidores virtuales NetScaler AAA TM? 390

¿Qué cambió en la función de proxy RDP para NetScaler Gateway 11.0? 390

Cambios en las licencias 391

Comando de habilitación 391

Otros cambios en el proxy RDP 391

¿Cómo se migra una configuración de proxy de Protocolo de escritorio remoto (RDP) basada en NetScaler 10.5.e a NetScaler 11.0? 391

¿Cómo se configura NetScaler Gateway para la configuración de proxy RDP mediante la versión NetScaler 11.0? 392

¿Es HDX™ Insight compatible con Unified Gateway? 392

¿Cómo migro mi configuración existente de HDX Insight? 392

Configuración de VPN en un dispositivo NetScaler Gateway 393

Cómo se conectan los usuarios con el cliente Citrix Secure Access™ 394

Establecer el túnel seguro 395

Tunelizar el tráfico de red privada a través de conexiones seguras 395

Conectarse a través de firewalls y proxies 396

Controlar la actualización de los clientes de Citrix Secure Access 396

Requisitos 397

Comportamientos del complemento 397

© 1997–2026 Citrix Systems, Inc. All rights reserved. 

Parámetros de CLI para controlar la actualización del complemento VPN 401
Parámetros de CLI para controlar la actualización del complemento EPA 401
Configuración de VPN 402
Configuración de EPA 402
Configuración completa de VPN en NetScaler Gateway 403
Requisitos previos 403
Configurar una configuración VPN completa en un dispositivo NetScaler Gateway 404
Configurar la tunelización dividida 410
Opciones de tunelización dividida 411
Tunelización dividida DESACTIVADA 412
Tunelización dividida ACTIVADA 412
Tunelización dividida inversa 413
Configurar la resolución de servicio de nombres 414
Referencias 415
Seleccionar el método de acceso de usuario 415
Implementar el cliente Citrix Secure Access™ para el acceso de los usuarios 417
Implementar el cliente Citrix Secure Access mediante el paquete de instalación MSI 417
Ventajas de usar una herramienta de implementación centralizada 417
Determinar qué plug-in de software implementar 418
Seleccionar el **Citrix Secure Access™ client** para los usuarios 418
Configurar el plug-in globalmente 418
Configurar el tipo de plug-in para Windows o macOS en un perfil de sesión 419
Cliente Citrix Secure Access para Windows 419
Instalar el cliente Citrix Secure Access para Windows 420
Configurar el cuadro de diálogo de inicio de sesión para el cliente Citrix Secure Access para Windows 421
Establecer el modo de intercepción para el cliente Citrix Secure Access para Windows 421
Compatibilidad con Microsoft Edge WebView para Citrix Secure Access de Windows 422

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Cliente de Citrix Secure Access para Windows que utiliza la Plataforma de filtrado de Windows 422
Cliente de Citrix Secure Access para macOS 428
Aplicar el acceso a la LAN local a los usuarios finales según la configuración de ADC 429
Implementar el cliente Citrix Secure Access™ desde Active Directory 431
Para descargar el paquete MSI del cliente Citrix Secure Access desde la utilidad de configuración 431
Para crear un punto de distribución 432
Administrar el cliente Citrix Secure Access™ mediante Active Directory 433
Eliminar el cliente Citrix Secure Access de los dispositivos de usuario 433
Solucionar problemas de instalación del cliente Citrix Secure Access mediante Active Directory 434
Integrar el cliente Citrix Secure Access con la aplicación Citrix Workspace 434
Cómo se conectan los usuarios con la aplicación Citrix Workspace 435
Desacoplar el icono de la aplicación Citrix Workspace 436
Configurar la integración del icono mediante la CLI 436
Configurar la integración del icono mediante la GUI 436
Configurar IPv6 para conexiones ICA® 437
Para configurar IPv6 para ICA Proxy mediante la CLI 437
Configurar la página de inicio de la aplicación Citrix Workspace en NetScaler Gateway 438
Para configurar la página de inicio de la aplicación Citrix Workspace globalmente 439
Para configurar la página de inicio de la aplicación Citrix Workspace en un perfil de sesión 439
Aplicar el tema de la aplicación Citrix Workspace a la página de inicio de sesión de NetScaler Gateway 439
Crear un tema personalizado para la página de inicio de sesión de NetScaler Gateway 440
Crear e implementar el tema personalizado mediante la CLI 440
Claves del registro del cliente VPN de NetScaler Gateway para Windows 441
Aplicar la marca HttpOnly en las cookies de autenticación 474

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Escenario compatible 474
Configurar la función HttpOnly mediante la CLI 475
Limitaciones 475
Personalizar el portal de usuario para usuarios VPN 476
Aplicar un tema de portal 476
Tema Caxton 477
Tema Green bubble 478
Tema X1 478
Vincular un tema de portal a un servidor virtual VPN 478
Vincular un tema de portal a un servidor virtual VPN mediante la CLI 479
Vincular un tema de portal a un servidor virtual VPN mediante la GUI 479
Vincular un tema de portal a VPN global 479
Vincular un tema de portal a VPN global mediante la CLI 479
Vincular un tema de portal a VPN global mediante la GUI 479
Crear un tema de portal 480
Usar un tema de portal estándar como plantilla para un tema de portal personalizado 480
Crear un tema de portal mediante la CLI 480
Crear un tema de portal mediante la GUI 481
Personalización del tema del portal 481
Acerca de la interfaz de temas del portal 481
Tipos de atributos de página personalizables 482
Crear un EULA 484
Crear una entidad EULA mediante la CLI 485
Crear una entidad EULA mediante la GUI 485
Vincular un EULA a la VPN global mediante la CLI 486
Vincular un EULA a la VPN global mediante la GUI 486
Vincular un EULA a un servidor virtual de VPN mediante la CLI 486
Vincular un EULA a un servidor virtual de VPN mediante la GUI 486

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Pedir a los usuarios que actualicen los navegadores antiguos o no compatibles mediante la creación de una página personalizada 487

Cómo crear una página personalizada para pedir a los usuarios que actualicen los navegadores antiguos no compatibles basados en SSL 487

Configurar el acceso VPN sin cliente con NetScaler Gateway 488

Cómo funcionan las directivas de acceso VPN sin cliente 488

Habilitar el acceso VPN sin cliente 490

Para habilitar el acceso sin cliente globalmente 490

Para habilitar el acceso sin cliente mediante una directiva de sesión 491

Codificar la dirección web 491

Configurar la codificación de direcciones web globalmente 492

Configurar la codificación de direcciones web mediante la creación de una directiva de sesión 492

Crear directivas de acceso sin cliente 492

Crear una directiva de acceso sin cliente utilizando la configuración predeterminada 493

Vincular una directiva de acceso sin cliente a un servidor virtual 493

Crear y evaluar expresiones de directivas de acceso sin cliente 493

Acceso VPN sin cliente avanzado con NetScaler Gateway 494

Requisitos previos 494

Configurar el acceso VPN sin cliente avanzado 495

Advertencias 496

Configurar el acceso a dominios para los usuarios 496

Para configurar el acceso a dominios mediante el asistente de NetScaler Gateway 497

Para configurar los ajustes de dominio mediante la utilidad de configuración 497

Acceso VPN sin cliente para SharePoint 2003, SharePoint 2007 y SharePoint 2013 498

Configurar el acceso sin cliente para SharePoint mediante la GUI de NetScaler 498

Establecer un sitio de SharePoint como página de inicio 498

Habilitar la resolución de nombres para los servidores de SharePoint 2007 499

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configurar un sufijo DNS 500
Habilitar cookies persistentes de acceso VPN sin cliente 500
Configurar cookies persistentes para el acceso VPN sin cliente para SharePoint 501
Cliente VPN Citrix® SSO para dispositivos móviles 502
Referencias 502
Configurar la página de opciones de cliente 502
Mostrar la página de opciones de cliente al iniciar sesión 503
Habilitar las opciones de cliente globalmente 504
Habilitar las opciones de cliente como parte de una directiva de sesión 504
Configurar las opciones de Opciones de cliente 504
Crear un grupo de autorización 505
Crear un perfil de sesión para las opciones de cliente 505
Configurar el servidor STA globalmente 506
Vincular la STA a un servidor virtual 507
Configurar la reserva de escenario de acceso 507
Crear políticas para la reserva de escenario de acceso 508
Crear un grupo de cuarentena 509
Configurar ajustes para poner en cuarentena las conexiones de usuario 509
Crear una directiva de sesión para la reserva de escenarios de acceso 510
Vincular la política de sesión al grupo de cuarentena 510
Crear una política de seguridad de cliente global 511
Configurar conexiones para el cliente Citrix Secure Access™ 511
Configurar el número de sesiones de usuario 512
Para establecer el límite global de usuarios 512
Para establecer el límite de usuarios por servidor virtual 512
Configurar ajustes de tiempo de espera 513
Configurar tiempos de espera forzados 514
Configurar tiempos de espera de sesión o de inactividad 515

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Para configurar un tiempo de espera de sesión o de inactividad del cliente globalmente mediante la GUI 516

Para configurar los ajustes de tiempo de espera de sesión o de inactividad del cliente mediante una directiva de sesión con la GUI 516

Conectar a recursos de red internos 517

Configurar el acceso a la red para recursos de red internos 517

Configurar la tunelización dividida 517

Para configurar la tunelización dividida 518

Configuración de la tunelización dividida y la autorización 519

Configurar la intercepción de cliente 519

Configurar aplicaciones de intranet para el cliente Citrix Secure Access™ 520

Para crear una aplicación de intranet para una dirección IP 521

Para configurar un rango de direcciones IP 521

Para crear una aplicación de intranet para un nombre de host 522

Configurar la resolución de servicio de nombres 522

Agregar un servidor DNS o WINS dentro de un perfil de sesión 523

Habilitar la compatibilidad con proxy para conexiones de usuario 523

Configuración del proxy 523

Para configurar la compatibilidad con proxy para conexiones de usuario 524

Para configurar un servidor proxy para usar todos los protocolos para NetScaler Gateway 525

Para configurar NetScaler Gateway como servidor proxy 526

Configurar grupos de direcciones 526

Registro DNS de IP de intranet 528

Configurar grupos de direcciones para un usuario, grupo o servidor virtual mediante la GUI 530

Configurar grupos de direcciones globalmente mediante la GUI 530

Configurar grupos de direcciones mediante la CLI 530

Definir opciones de grupo de direcciones 531

© 1997–2026 Citrix Systems, Inc. All rights reserved. 

Para definir grupos de direcciones 532
Configurar la página de inicio de sesión de transferencia 532
Configurar un sufijo DNS 533
Compatibilidad con teléfonos VoIP 534
Configurar la interfaz de acceso 535
Cambiar la Interfaz de acceso 536
Reemplace la interfaz de acceso con una página de inicio personalizada 536
Crear y aplicar enlaces web 537
Creación de marcadores empresariales 537
Creación de marcadores personales 541
Configurar tokens de nombre de usuario en marcadores 543
Configurar SmartAccess 544
Directivas de tráfico 544
Crear una directiva de tráfico 545
Ejemplos de expresiones de políticas de tráfico 545
Configurar una política de tráfico mediante la GUI 546
Configurar el inicio de sesión único basado en formularios 546
Configurar el inicio de sesión único basado en formularios 547
Configurar el inicio de sesión único de SAML 548
Configurar el inicio de sesión único de SAML 548
Enlazar una directiva de tráfico 548
Enlazar una directiva de tráfico globalmente mediante la GUI 548
Eliminar directivas de tráfico 549
Desenlazar una directiva de tráfico mediante la GUI 549
Eliminar una directiva de tráfico mediante la GUI 549
Directivas de sesión 550
Crear una directiva de sesión 551
Ejemplos de expresiones de directivas de sesión 551

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Vincular directivas de sesión 551
Vincular una directiva de sesión a un servidor virtual mediante la GUI 551
Enlazar una directiva de sesión a un grupo de autenticación, autorización y auditoría mediante la GUI 552
Enlazar una directiva de sesión a un usuario de autenticación, autorización y auditoría mediante la GUI 552
Crear un perfil de sesión 553
Configurar la configuración de red para las conexiones de usuario en un perfil de sesión 553
Configurar los ajustes de conexión en un perfil de sesión 553
Configurar la configuración de seguridad en un perfil de sesión 554
Configurar los ajustes de Citrix Virtual Apps and Desktops en un perfil de sesión 554
Soporte de políticas avanzadas para marcadores empresariales 556
Configurar la URL VPN como una política avanzada 556
En la GUI 556
En la CLI 559
Políticas de puntos finales 563
Cómo funcionan las políticas de puntos finales 563
Ejemplos de expresiones EPA 565
Evaluar las opciones de inicio de sesión de usuario 565
Omitir el análisis de EPA 566
Análisis de Endpoint Analysis compatibles con Ubuntu 567
Directivas y perfiles de preautenticación 568
Configurar perfil de preautenticación 569
Configurar expresiones personalizadas 572
Configurar expresiones compuestas 573
Enlazar directivas de autenticación previa 573
Desvincular y eliminar directivas de autenticación previa 574
Establecer la prioridad de las políticas de preautenticación 575

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Directivas de postautenticación 576
Configurar una directiva de postautenticación 577
Configurar la frecuencia de los análisis posteriores a la autenticación 577
Grupos de cuarentena y autorización 578
Expresiones de comprobación de dispositivos de preautenticación para dispositivos de usuario 581
Configurar expresiones de antivirus, firewall, seguridad de Internet o antispam 582
Configurar directivas de servicio 583
Configurar políticas de proceso 585
Configurar directivas del sistema operativo 586
Configurar directivas de registro 587
Configurar expresiones compuestas de comprobación de dispositivos cliente 590
Configurar directivas mediante el operador NOT (\!) 591
Certificado de dispositivo en nFactor como componente EPA 592
Configurar el certificado de dispositivo en nFactor como componente EPA 593
Referencias 595
Análisis EPA como factor en la autenticación nFactor 596
Exclusividad mutua del factor EPA 598
Ejecución de EPA 598
Configurar el análisis EPA para que se ejecute después de la autenticación 599
Referencias 607
Tipos de clasificación de análisis EPA en el cliente de Windows 607
Configurar los tipos de clasificación de análisis de EPA mediante la GUI 608
Referencias 609
Análisis avanzados de Endpoint Analysis 609
En la GUI 610
En la CLI 614
Actualizar bibliotecas EPA 615

© 1997–2026 Citrix Systems, Inc. All rights reserved. 

Solución de problemas de análisis avanzados de Endpoint Analysis 616
Análisis EPA para direcciones MAC 616
Configurar el análisis EPA para direcciones MAC mediante la GUI 617
Configurar el análisis EPA para direcciones MAC mediante la CLI 618
Puntos a tener en cuenta 619
Limitaciones 620
Referencias 620
Referencia de expresiones de directiva de análisis avanzado de puntos finales 620
Formato de expresión 620
Cadenas de expresión 621
Métodos de análisis de aplicaciones 622
Administrar sesiones de usuario 629
Administrar sesiones de usuario mediante la GUI 630
Para ver las sesiones de usuario 630
Para actualizar la lista de sesiones 630
Para finalizar sesiones de usuario o de grupo o una sesión que tenga una dirección IP de intranet específica 630
Administrar sesiones de usuario mediante la CLI 630
Inicio de sesión automático de Windows 631
Configurar el inicio de sesión automático de Windows mediante la CLI 631
Inicio de sesión automático con autenticación Kerberos 631
Requisitos previos 631
Configurar la autenticación Kerberos con el cliente Citrix Secure Access™ 632
Referencias 632
Always On 632
Cuándo usar Always On 632
Descripción del marco de Always On 633
Restablecimiento automático de un túnel 634

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Métodos de autenticación de usuario admitidos para el establecimiento de túneles sin interrupciones 634
Requisitos de configuración para Always On 634
Consideraciones al habilitar la función Always On 635
Configuración de Always On 635
Nota sobre las IIP 637
Resumen del comportamiento de diferentes configuraciones para usuarios administradores y no administradores 637
Permitir URL seleccionadas cuando Always On está inactivo 638
Para configurar el registro AlwaysOnAllowlist 638
Always On VPN antes del inicio de sesión de Windows (formalmente servicio Always On) 639
Capacidades de Always On VPN antes del inicio de sesión de Windows 639
Comprensión de Always On VPN antes del inicio de sesión de Windows 640
Pantalla del administrador de credenciales de Windows después de la configuración de Always On VPN antes del inicio de sesión de Windows 641
Configurar Always On VPN antes del inicio de sesión de Windows 642
Requisitos previos 642
Pasos de configuración de alto nivel 643
Túnel a nivel de máquina 643
Túnel a nivel de usuario 650
Configuración del lado del cliente 655
Uso de la política avanzada para crear políticas VPN 658
¿Por qué migrar de la política clásica a la política avanzada? 658
EPA de preautenticación mediante EPA avanzada 659
EPA de postautenticación mediante EPA avanzada 659
EPA de preautenticación y postautenticación mediante políticas avanzadas 660
Análisis EPA periódico como factor en la autenticación nFactor 660
Configurar el servidor virtual VPN DTLS mediante el servidor virtual VPN SSL 662

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Puntos a tener en cuenta 662
Configurar un servidor virtual VPN DTLS mediante la GUI 663
Configurar un servidor virtual VPN DTLS mediante la CLI 664
Parámetros de servidor virtual VPN DTLS admitidos 665
Parámetros de servidor virtual VPN DTLS no admitidos 665
Configurar un servidor virtual DTLS mediante el asistente de XenApp y XenDesktop® 666
Limitaciones 667
Integración con productos Citrix® 669
Cómo se conectan los usuarios a las aplicaciones, escritorios y ShareFile 670
Integrar NetScaler Gateway con StoreFront 671
Configurar NetScaler Gateway para usar con StoreFront 672
1. Crear una directiva de sesión para el acceso basado en navegador web 672
2. Crear una directiva de sesión para el acceso basado en la aplicación Citrix Workspace™ 677
3. Crear un perfil de autenticación 678
4. Crear un servidor virtual de NetScaler® Gateway 678
5. Agregar una instancia de NetScaler Gateway en StoreFront 680
Referencias 680
Integrar NetScaler Gateway con Citrix Virtual Apps and Desktops 681
Implementación con Citrix Endpoint Management™, Citrix Virtual Apps and Desktop 682
Configuración de los ajustes para su entorno de Citrix Endpoint Management™ 684
Requisitos de licencia para las funciones de NetScaler 685
Asistente de NetScaler para Citrix Endpoint Management 686
Configurar servidores de equilibrio de carga para Citrix Endpoint Management o Citrix XenMobile Server 691
Para usar el modo puente SSL para VIP de NetScaler 692
Para usar el modo de descarga SSL para VIP de NetScaler 693

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configurar servidores de equilibrio de carga para Microsoft Exchange con filtrado de seguridad de correo electrónico 695

Configurar el filtrado de ActiveSync del Conector de NetScaler de Citrix Endpoint Management (XNC) 696

Permitir el acceso desde dispositivos móviles con las aplicaciones de productividad móvil de Citrix 697

Configurar Secure Browse en NetScaler Gateway 697

Configurar los tiempos de espera de los tokens de aplicación y MDX 701

Inhabilitar el análisis de puntos finales para dispositivos móviles 701

Admitir consultas DNS mediante sufijos DNS para dispositivos Android 702

Configurar la autenticación de dominio y de token de seguridad para Citrix Endpoint Management 704

Requisitos previos 704

Para configurar la autenticación de dominio y de token de seguridad 704

Configurar el certificado de cliente o el certificado de cliente y la autenticación de dominio 706

Configurar NetScaler Gateway para la autenticación con certificado de cliente mediante la GUI 706

Configurar NetScaler Gateway para la autenticación de certificado de cliente y dominio mediante la GUI 707

Lista de revocación de certificados (CRL) de NetScaler 708

Configuración de SmartControl 708

Directivas 710

Agregar 710

Editar 712

Eliminar 713

Mostrar enlace 714

Administrador de directivas 714

Agregar enlace 714

Enlace de política 715

© 1997–2026 Citrix Systems, Inc. All rights reserved. 

**Desvincular política** 716

**Vincular NOPOLICY** 716

**Editar** 717

Editar enlace 718

Editar política 718

Editar acción 720

Acción 720

Acción 721

Agregar 721

Editar 723

Configurar acción 724

Eliminar 725

Acción 725

Perfiles de acceso 726

Crear un perfil de acceso con la GUI 727

Agregar un perfil de acceso a una directiva mediante la GUI 727

Agregar 727

Editar 729

Configurar perfil de acceso 730

Eliminar 730

Procesos comunes 731

Crear una acción 731

Seleccionar una acción 732

Crear un perfil de acceso 732

Seleccionar un perfil de acceso existente 733

Expresiones 733

Identificación de grupo 735

Preautenticación 735

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Sesión 738
Crear una acción de registro 740
Crear acción de mensaje de auditoría 740
Revisar una acción de registro 741
Configurar acción de mensaje de auditoría 742
Seleccionar una directiva existente 743
Crear una política 743
Configuración del análisis de puntos finales de preautenticación y postautenticación 743
Configuración de postautenticación 744
Crear perfil de sesión de NetScaler Gateway 746
Configuración de la autenticación previa 748
Crear perfil de preautenticación 751
Integración de Microsoft Intune 753
Integración de micro VPN de Citrix® con Microsoft Endpoint Manager 753
Cuándo usar la solución MDM de Intune integrada 754
Descripción de la integración de MDM de NetScaler Gateway con Intune 755
Compatibilidad con la API Intune NAC v2 756
Configurar la comprobación de dispositivos de Control de Acceso a la Red para el servidor virtual de NetScaler Gateway para el inicio de sesión de factor único 756
Licencias 757
Requisitos del sistema 757
Requisitos previos 758
Referencias 758
Para agregar un servidor virtual NetScaler Gateway con nFactor para la implementación de la puerta de enlace 758
Para vincular el esquema de inicio de sesión de autenticación al servidor virtual de autenticación para indicar a los complementos VPN que envíen el ID del dispositivo como parte de la solicitud /cgi/login 771
Compatibilidad con la API v2 de Intune NAC 773

© 1997–2026 Citrix Systems, Inc. All rights reserved. 

Solución de problemas 776
Problemas generales 776
Problemas de NetScaler Gateway 776
Estado de OAuth de NetScaler Gateway y condición de error 777
Comprobación de la configuración de Intune 777
Configuración de una aplicación NetScaler Gateway en el portal de Azure 777
Requisitos previos 777
Para crear una aplicación NetScaler Gateway en Azure 778
Descripción de la autenticación de tokens MSAL 785
Configuración del servidor virtual de NetScaler Gateway para la autenticación de tokens MSAL 785
Configurar NetScaler Gateway para usar micro VPN con Microsoft Endpoint Manager 789
Requisitos del sistema 789
Requisitos previos 789
Conceder permisos de aplicación de Microsoft Entra ID 790
Configurar NetScaler Gateway para micro VPN 790
Validar la comunicación de NetScaler Gateway con los servicios de Microsoft 791
Configuración del navegador Microsoft Edge 792
Solución de problemas 795
Problemas generales 795
Problemas de NetScaler Gateway 795
Estado de OAuth de NetScaler Gateway y condición de error 796
Último punto final del servicio de control de acceso a la red (NAC) de OAuth 796
Soporte extendido para Azure AD Graph 797
Soporte de transporte de datos optimizado HDX™ 799
Cuándo utilizar el soporte de transporte de datos iluminado 799
Configurar NetScaler Gateway para admitir Enlightened Data Transport 800
Configurar NetScaler Gateway para admitir Enlightened Data Transport 801
Para configurar NetScaler Gateway para admitir EDT mediante la GUI 801

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Para configurar NetScaler Gateway para la compatibilidad con EDT mediante la CLI 803
Configurar NetScaler Gateway para admitir HDX Insight 803
Para configurar NetScaler Gateway para admitir HDX Insight mediante la GUI 804
Para configurar NetScaler Gateway para admitir HDX Insight mediante la CLI 809
Deshabilitar HDX Insight para sesiones HDX de AppFlow (NSAP) que no son de NetScaler 810
Detección de PMTUD y propagación de bits DF para EDT a través de NetScaler Gateway 810
Habilitar la compatibilidad con PMTUD mediante la CLI 810
Habilitar la compatibilidad con PMTUD mediante la GUI 811
Umbral de latencia L7 812
Diferencia entre la latencia L7 y la latencia L4 813
Diferencia entre los cálculos de ICA RTT y latencia L7 813
Configurar el umbral de latencia L7 mediante la CLI 814
Argumentos 814
Configurar el umbral de latencia L7 mediante la GUI 815
Ver parámetros de latencia L7 en NetScaler ADM 817
El modelo de medición de latencia L7 frente al modelo de informes de umbral de latencia L7 817
El modelo de medición de latencia L7 817
Modelo de informes de umbral de latencia L7 818
Proxy RDP 820
Implementación a través de VPN sin cliente 821
Implementación a través de proxy ICA 821
Detalles de la aplicación 822
Parámetros RDP admitidos para la aplicación 822
Flujo de conexión 822
Compatibilidad con puerta de enlace sin estado (dual) 823
Compatibilidad con una única puerta de enlace 824
Compatibilidad con un único agente de escucha 825
Requisitos de licencia para RDP Proxy 826

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Marcador 826
Crear marcadores 827
Funciones y modos que deben habilitarse para el proxy RDP 827
Pasos de configuración de alto nivel del proxy RDP 827
Configurar un perfil de cliente 828
Configurar un perfil de servidor 829
Configuración del proxy RDP mediante la CLI 829
Configuración del proxy RDP mediante la GUI 830
Opción para deshabilitar SSO 845
Proxy RDP sin estado 846
Flujo de conexión 846
Requisitos previos 848
Configurar el proxy RDP sin estado mediante la CLI 848
Configurar el proxy RDP sin estado mediante la GUI 850
Contador de conexiones 851
Notas de actualización 851
Redirección de conexión RDP 851
Requisitos previos 852
Implementar proxy RDP en presencia de un agente de conexión 852
Configurar el proxy RDP en presencia de un agente de conexión mediante la CLI 852
Configurar la redirección de conexión RDP mediante la GUI de NetScaler 853
Rellenar URL de RDP basadas en el atributo LDAP 853
Para rellenar URL de RDP basadas en el atributo LDAP mediante la CLI 853
Configuración del servidor LDAP 854
Para rellenar URL de RDP basadas en el atributo LDAP mediante la GUI 854
Aleatorizar el nombre de archivo RDP con proxy RDP 855
Configurar la compatibilidad con la aleatorización del nombre de archivo RDP con proxy RDP 855

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configurar el nombre de los archivos RDP 855

Configurar un nombre para los archivos RDP 856

Soporte de proxy ICA® saliente 857

Descripción del soporte de proxy ICA saliente 857

Soporte SSL en el proxy LAN de NetScaler 858

Configuración del proxy ICA® saliente 858

Configurar el proxy LAN de NetScaler para el proxy ICA saliente 858

Soporte de proxy PCoIP habilitado en NetScaler Gateway para VMware Horizon View 860

Configurar el proxy PCoIP habilitado para NetScaler Gateway para VMware Horizon View 860

Requisitos previos 860

Pasos para habilitar la redirección USB 864

Actualizar la expresión de conmutación de contenido para Unified Gateway 864

Usar la puerta de enlace PCoIP 865

Configuración del servidor de conexión de VMware Horizon View 865

Configuración automática de proxy para la compatibilidad con proxy de salida para NetScaler Gateway 866

Configurar los parámetros globales de NetScaler Gateway para admitir PAC para proxy de salida mediante la CLI 866

Configurar NetScaler Gateway para admitir PAC en un perfil de sesión mediante la CLI 866

Configurar los parámetros globales de NetScaler Gateway para admitir PAC para proxy de salida mediante la GUI 867

Configurar NetScaler Gateway para admitir PAC en el perfil de sesión mediante la GUI 867

Soporte de configuración para el atributo de cookie SameSite 868

Configurar el atributo de cookie `SameSite` 868

Configuración del atributo `SameSite` mediante la CLI 869

Vinculación de cookies a `patset` mediante la CLI 869

Configuración del atributo SameSite mediante la GUI 869

Optimizar el tráfico de red con Citrix SD-WAN™ WANOP 872

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Para crear una directiva de tráfico 873
Configuración de la experiencia de usuario de RfWebUI Persona en Gateway 874
Cuándo usar RfWebUI Persona 874
Funcionalidades proporcionadas por RfWebUI Persona 874
GO 875
Agregación de aplicaciones 875
Enlaces de proxy RDP configurados por el usuario 875
Aplicaciones favoritas 875
Consideraciones al habilitar la persona RfWebUI 876
Configuración de la persona RfWebUI 876
Parámetros de configuración de RfWebUI 876
Personalización del portal de Gateway mediante plug-ins personalizados 883
Ejemplo de configuración 885
Personalización del portal de Gateway mediante plug-ins personalizados 887
Ejemplo de configuración 888
Crear y personalizar el esquema de inicio de sesión 890
Crear un perfil de esquema de inicio de sesión 891
Vincular un perfil de esquema de inicio de sesión a un servidor virtual de autenticación, autorización y auditoría 893
Personalizaciones del portal desde la interfaz de usuario de administración 894
Atributos comunes 895
Personalizaciones de cadenas 898
Optimización del túnel dividido VPN de NetScaler Gateway para Office365 901
Configuración mediante la GUI 902
Para configurar el túnel dividido mediante la GUI 902
Para crear una aplicación de intranet VPN mediante la GUI 902
Configuración mediante la CLI 904
Lista de direcciones IP de los servicios de Office 365 (EXO, SPO y Microsoft Teams) 905

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Rango de direcciones IPv4 905

Rango de direcciones IPv6 906

Soporte de tipo de servicio para tráfico UDP 907

Configuración de la extensión de indicación de nombre de servidor 908

Validación del certificado del servidor durante un protocolo de enlace SSL 909

Configuración simplificada de aplicaciones SaaS mediante una plantilla 911

Configuración y publicación de aplicaciones mediante plantilla - Configuración específica de NetScaler Gateway 911

Configuración y publicación de aplicaciones mediante plantilla - Configuración específica del servidor de aplicaciones 915

© 1997–2026 Citrix Systems, Inc. All rights reserved.

# Notas de la versión de NetScaler Gateway

Las notas de la versión describen cómo ha cambiado el software en una compilación particular y los problemas conocidos que existen en esa compilación.

El documento de notas de la versión incluye todas o algunas de las siguientes secciones:

- **Novedades**: Las mejoras y otros cambios lanzados en la compilación.
- **Problemas resueltos**: Los problemas que se han resuelto en la compilación.
- **Problemas conocidos**: Los problemas que existen en la compilación.
- **Puntos a tener en cuenta**: Los aspectos importantes a tener en cuenta al usar la compilación.
- **Limitaciones**: Las limitaciones que existen en la compilación.

**IMPORTANTE:**

Las notas de la versión de NetScaler Gateway se incluyen como parte de las notas de la versión de ADC. Para obtener información detallada sobre las mejoras, los problemas conocidos y las correcciones de errores de NetScaler Gateway 13.1, consulte la página notas de la versión.

**Nota:**

- Las etiquetas bajo las descripciones de los problemas son ID de seguimiento internos utilizados por el equipo de NetScaler.
- Estas notas de la versión no documentan las correcciones relacionadas con la seguridad. Para obtener una lista de las correcciones y avisos relacionados con la seguridad, consulte el boletín de seguridad.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

# Acerca de NetScaler Gateway

NetScaler Gateway es fácil de implementar y sencillo de administrar. La configuración de implementación más típica es ubicar el dispositivo NetScaler Gateway en la DMZ. Puede instalar varios dispositivos NetScaler Gateway en la red para implementaciones más complejas.

La primera vez que inicie NetScaler Gateway, puede realizar la configuración inicial mediante una consola serie, el Asistente de configuración en la utilidad de configuración o el Protocolo de configuración dinámica de host (DHCP). En el dispositivo MPX, puede usar el teclado LCD del panel frontal del dispositivo para realizar la configuración inicial. Puede configurar ajustes básicos específicos de su red interna, como la dirección IP, la máscara de subred, la dirección IP de la puerta de enlace predeterminada y la dirección del Sistema de nombres de dominio (DNS). Después de configurar los ajustes básicos de red, configure los ajustes específicos para el funcionamiento de NetScaler Gateway, como las opciones de autenticación, autorización, recursos de red, servidores virtuales, directivas de sesión y directivas de punto final.

Antes de instalar y configurar NetScaler Gateway, revise los temas de esta sección para obtener información sobre la planificación de su implementación. La planificación de la implementación puede incluir la determinación de dónde instalar el dispositivo, la comprensión de cómo instalar varios dispositivos en la DMZ y los requisitos de licencias. Puede instalar NetScaler Gateway en cualquier infraestructura de red sin necesidad de realizar cambios en el hardware o software existente que se ejecuta en la red segura. NetScaler Gateway admite otros productos de red, como equilibradores de carga de servidores, motores de caché, firewalls, enrutadores y dispositivos inalámbricos IEEE 802.11.

Puede anotar sus ajustes en la Lista de comprobación previa a la instalación para tenerlos a mano antes de configurar NetScaler Gateway.

| | |
|---|---|
| Dispositivos NetScaler Gateway | Proporciona información sobre los dispositivos NetScaler Gateway y las instrucciones de instalación del dispositivo. |
| Lista de comprobación previa a la instalación | Proporciona información de planificación para revisar y una lista de tareas que completar antes de instalar NetScaler Gateway en su red. |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| | |
|---|---|
| Implementaciones comunes | Proporciona información sobre la implementación de NetScaler Gateway en la DMZ de la red, en una red segura sin DMZ y con otros dispositivos para admitir el equilibrio de carga y la conmutación por error. También proporciona información sobre la implementación de NetScaler Gateway con Citrix Virtual Apps and Desktops. |
| Licencias | Proporciona información sobre la instalación de licencias en el dispositivo. También proporciona información sobre la instalación de licencias en varios dispositivos NetScaler Gateway. |

# Arquitectura de NetScaler Gateway

Los componentes principales de NetScaler Gateway son:

- **Servidores virtuales**. El servidor virtual de NetScaler Gateway es una entidad interna que representa todos los servicios configurados disponibles para los usuarios. El servidor virtual es también el punto de acceso a través del cual los usuarios acceden a estos servicios. Puede configurar varios servidores virtuales en un único dispositivo, lo que permite que un dispositivo NetScaler Gateway preste servicio a varias comunidades de usuarios con diferentes requisitos de autenticación y acceso a recursos.
- **Autenticación, autorización y auditoría**. Puede configurar la autenticación, la autorización y la contabilidad para permitir a los usuarios iniciar sesión en NetScaler Gateway con credenciales que NetScaler Gateway o los servidores de autenticación ubicados en la red segura, como LDAP o RADIUS, reconozcan. Las directivas de autorización definen los permisos de usuario, determinando a qué recursos está autorizado a acceder un usuario determinado. Para obtener más información sobre la autenticación y la autorización, consulte (/es-es/netscaler-gateway/13-1/authentication-authorization.html). Los servidores de auditoría mantienen datos sobre la actividad de NetScaler Gateway, incluidos los eventos de inicio de sesión de los usuarios, las instancias de acceso a los recursos y los errores operativos. Esta información se almacena en NetScaler Gateway o en un servidor externo. Para obtener más información sobre la auditoría, consulte (/es-es/netscaler-gateway/13-1/maintain-monitor/ns-maintain-auditing-configure-overview-con.html)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Conexiones de usuario**. Los usuarios pueden iniciar sesión en NetScaler Gateway mediante los siguientes métodos de acceso:
  - El cliente Citrix Secure Access para Windows es un software que se instala en un equipo basado en Windows. Los usuarios inician sesión haciendo clic con el botón derecho en un icono del área de notificación de un equipo basado en Windows. Si los usuarios utilizan un equipo en el que no está instalado el cliente Citrix Secure Access, pueden iniciar sesión utilizando un explorador web para descargar e instalar el complemento. Si los usuarios tienen instalada la aplicación Citrix Workspace, inician sesión con el cliente Citrix Secure Access desde la aplicación Citrix Workspace. Cuando la aplicación Citrix Workspace y el cliente Citrix Secure Access están instalados en el dispositivo del usuario, la aplicación Citrix Workspace añade automáticamente el cliente Citrix Secure Access.
  - El cliente Citrix Secure Access para macOS X que permite a los usuarios que ejecutan macOS X iniciar sesión. Tiene las mismas características y funciones que el cliente Citrix Secure Access para Windows. Puede proporcionar soporte de análisis de puntos finales para esta versión del complemento instalando NetScaler Gateway 10.1, Build 120.1316.e.
  - La aplicación Citrix Workspace que permite las conexiones de usuario a aplicaciones publicadas y escritorios virtuales en una granja de servidores mediante Citrix StoreFront.
  - La aplicación Citrix Workspace, Secure Hub, WorxMail y WorxWeb que permite a los usuarios acceder a aplicaciones web y SaaS, aplicaciones móviles iOS y Android, y datos de ShareFile alojados en Citrix Endpoint Management.
  - Los usuarios pueden conectarse desde un dispositivo Android que utiliza la dirección web de NetScaler Gateway. Cuando los usuarios inician una aplicación, la conexión utiliza Micro VPN para enrutar el tráfico de red a la red interna. Si los usuarios se conectan desde un dispositivo Android, debe configurar los ajustes de DNS en NetScaler Gateway. Para obtener más información, consulte (/es-es/netscaler-gateway/13-1/integrate-citrix-gateway-with-citrix-products/configure-citrix-endpoint-management-settings-to-integrate-with-citrix-gateway/allow-access-from-mobile-devices-with-citrix-mobile-productivity-apps.html).
  - Los usuarios pueden conectarse desde un dispositivo iOS que utiliza la dirección web de NetScaler Gateway. Puede configurar Secure Browse globalmente o en un perfil de sesión. Cuando los usuarios inician una aplicación en su dispositivo iOS, se inicia una conexión VPN y la conexión se enruta a través de NetScaler Gateway.
  - Acceso sin cliente que proporciona a los usuarios el acceso que necesitan sin instalar software en el dispositivo del usuario.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Al configurar NetScaler Gateway, puede crear directivas para configurar cómo inician sesión los usuarios. También puede restringir el inicio de sesión de los usuarios creando directivas de sesión y de análisis de puntos finales.

- **Recursos de red**. Incluyen todos los servicios de red a los que los usuarios acceden a través de NetScaler Gateway, como servidores de archivos, aplicaciones y sitios web.
- **Adaptador virtual**. El adaptador virtual de NetScaler Gateway admite aplicaciones que requieren suplantación de IP. El adaptador virtual se instala en el dispositivo del usuario cuando se instala el cliente Citrix Secure Access. Cuando los usuarios se conectan a la red interna, la conexión saliente entre NetScaler Gateway y los servidores internos utiliza la dirección IP de la intranet como dirección IP de origen. El cliente Citrix Secure Access recibe esta dirección IP del servidor como parte de la configuración.

  Si habilita la tunelización dividida en NetScaler Gateway, todo el tráfico de la intranet se enruta a través del adaptador virtual. Al interceptar el tráfico destinado a la intranet, el adaptador virtual interceptará las consultas DNS de tipo A y AAAA, dejando intactas todas las demás consultas DNS. El tráfico de red que no está destinado a la red interna se enruta a través del adaptador de red instalado en el dispositivo del usuario. Las conexiones a Internet y a la LAN privada (LAN) permanecen abiertas y conectadas. Si deshabilita la tunelización dividida, todas las conexiones se enrutan a través del adaptador virtual. Cualquier conexión existente se desconecta y el usuario debe restablecer la sesión.

  Si configura una dirección IP de intranet, el tráfico a la red interna se suplanta con la dirección IP de la intranet a través del adaptador virtual.

## Cómo funcionan las conexiones de usuario

Los usuarios pueden conectarse a sus correos electrónicos, recursos compartidos de archivos y otros recursos de red desde una ubicación remota. Los usuarios pueden conectarse a los recursos de red internos con el siguiente software:

- Cliente de Citrix Secure Access™
- Aplicación Citrix Workspace
- WorxMail y WorxWeb
- Dispositivos móviles Android e iOS

© 1997–2026 Citrix Systems, Inc. All rights reserved.

# Conectarse con el cliente de Citrix Secure Access

El cliente de Citrix Secure Access permite el acceso de los usuarios a los recursos de la red interna mediante los siguientes pasos:

1. Un usuario se conecta a NetScaler Gateway por primera vez escribiendo la dirección web en un explorador web. Aparece la página de inicio de sesión y se le pide al usuario que introduzca un nombre de usuario y una contraseña. Si hay servidores de autenticación externos configurados, NetScaler Gateway se pone en contacto con el servidor y los servidores de autenticación verificar las credenciales del usuario. Si la autenticación local está configurada, NetScaler Gateway realiza la autenticación del usuario.
2. Si configura una directiva de preautenticación, cuando el usuario escribe la dirección web de NetScaler Gateway en un explorador web en un equipo basado en Windows o un equipo macOS X, NetScaler Gateway comprueba si hay alguna directiva de seguridad basada en el cliente antes de que aparezca la página de inicio de sesión. Las comprobaciones de seguridad verificar que el dispositivo del usuario cumple las condiciones relacionadas con la seguridad, como las actualizaciones del sistema operativo, la protección antivirus y un firewall correctamente configurado. Si el dispositivo del usuario no supera la comprobación de seguridad, NetScaler Gateway impide que el usuario inicie sesión. Un usuario que no puede iniciar sesión debe descargar las actualizaciones o paquetes necesarios e instalarlos en el dispositivo del usuario. Cuando el dispositivo del usuario supera la directiva de preautenticación, aparece la página de inicio de sesión y el usuario puede introducir las credenciales de inicio de sesión. Puede utilizar Advanced Endpoint Analysis en un equipo macOS X si instala NetScaler Gateway 10.1, Build 120.1316.e.
3. Cuando NetScaler Gateway autentica correctamente al usuario, NetScaler Gateway inicia el túnel VPN. NetScaler Gateway solicita al usuario que descargue e instale el cliente de Citrix Secure Access para Windows o el cliente de Citrix Secure Access para macOS X.
4. Si configura un análisis posterior a la autenticación, después de que un usuario inicie sesión correctamente, NetScaler Gateway analiza el dispositivo del usuario en busca de las directivas de seguridad de cliente requeridas. Puede exigir las mismas condiciones relacionadas con la seguridad que para una directiva de preautenticación. Si el dispositivo del usuario no supera el análisis, la directiva no se aplica o el usuario se coloca en un grupo de cuarentena y el acceso del usuario a los recursos de red es limitado.
5. Cuando se establece la sesión, el usuario es dirigido a una página de inicio de NetScaler Gateway donde puede seleccionar los recursos a los que acceder. La página de inicio que se incluye con NetScaler Gateway se denomina Interfaz de acceso. Si el usuario inicia sesión utilizando el cliente de Citrix Secure Access para Windows, un icono en el área de notificación

© 1997–2026 Citrix Systems, Inc. All rights reserved.

del escritorio de Windows muestra que el dispositivo del usuario está conectado y el usuario recibe un mensaje de que la conexión se ha establecido. El usuario también puede acceder a los recursos de la red sin utilizar la Interfaz de acceso, como abrir Microsoft Outlook y recuperar el correo electrónico.

6. Si la solicitud del usuario supera las comprobaciones de seguridad de preautenticación y postautenticación, NetScaler Gateway se pone en contacto con el recurso solicitado e inicia una conexión segura entre el dispositivo del usuario y ese recurso.
7. El usuario puede cerrar una sesión activa haciendo clic con el botón derecho en el icono de NetScaler Gateway en el área de notificación de un equipo basado en Windows y, a continuación, haciendo clic en Cerrar sesión. La sesión también puede caducar debido a la inactividad. Cuando la sesión se cierra, el túnel se apaga y el usuario ya no tiene acceso a los recursos internos. El usuario también puede escribir la dirección web de NetScaler Gateway en un explorador. Cuando el usuario pulsa Intro, aparece la Interfaz de acceso desde la que los usuarios pueden cerrar sesión.

**Nota:** Si implementa Citrix Endpoint Management en su red interna, un usuario que se conecte desde fuera de la red interna debe conectarse primero a NetScaler Gateway. Cuando el usuario establece la conexión, puede acceder a aplicaciones web y SaaS, aplicaciones móviles de Android e iOS, y datos de ShareFile alojados en Citrix Endpoint Management. Un usuario puede conectarse con el cliente Citrix Secure Access a través de acceso sin cliente, o utilizando Citrix Workspace app o Secure Hub.

## Conectarse con Citrix Workspace app

Los usuarios pueden conectarse con Citrix Workspace app para acceder a sus aplicaciones basadas en Windows y escritorios virtuales. Los usuarios también pueden acceder a aplicaciones desde Endpoint Management. Para conectarse desde una ubicación remota, los usuarios también instalan el cliente Citrix Secure Access en su dispositivo. Citrix Workspace app agrega automáticamente el cliente Citrix Secure Access a su lista de complementos. Cuando los usuarios inician sesión en Citrix Workspace app, también pueden iniciar sesión en el cliente Citrix Secure Access. También puede configurar NetScaler Gateway para realizar el inicio de sesión único en el cliente Citrix Secure Access cuando los usuarios inician sesión en Citrix Workspace app.

## Conectarse con dispositivos iOS y Android

Los usuarios pueden conectarse desde un dispositivo iOS o Android utilizando Secure Hub. Los usuarios pueden acceder a su correo electrónico utilizando Secure Mail y conectarse a sitios web con WorxWeb.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Cuando los usuarios se conectan desde el dispositivo móvil, las conexiones se enrutan a través de NetScaler Gateway para acceder a los recursos internos. Si los usuarios se conectan con iOS, se habilita Secure Browse como parte del perfil de sesión. Si los usuarios se conectan con Android, la conexión utiliza automáticamente la Micro VPN. Además, Secure Mail y WorxWeb utilizan Micro VPN para establecer conexiones a través de NetScaler Gateway. No es necesario configurar Micro VPN en NetScaler Gateway.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

# Despliegues comunes de NetScaler Gateway

Puede implementar NetScaler Gateway en el perímetro de la red interna de su organización (o intranet) para proporcionar un único punto de acceso seguro a los servidores, aplicaciones y otros recursos de red que residen en la red interna. Todos los usuarios remotos deben conectarse a NetScaler Gateway antes de poder acceder a cualquier recurso de la red interna.

NetScaler Gateway se instala con mayor frecuencia en las siguientes ubicaciones de una red:

- En la DMZ de la red
- En una red segura que no tiene una DMZ

También puede implementar NetScaler Gateway con Citrix Virtual Apps, Citrix Virtual Desktops, StoreFront y Citrix Endpoint Management para permitir a los usuarios acceder a sus aplicaciones de Windows, web, móviles y SaaS. Si su implementación incluye Citrix Virtual Apps, StoreFront y Desktops 7, puede implementar NetScaler Gateway en una configuración DMZ de salto único o de doble salto. Una implementación de doble salto no es compatible con versiones anteriores de Citrix Virtual Desktops o Citrix Endpoint Management.

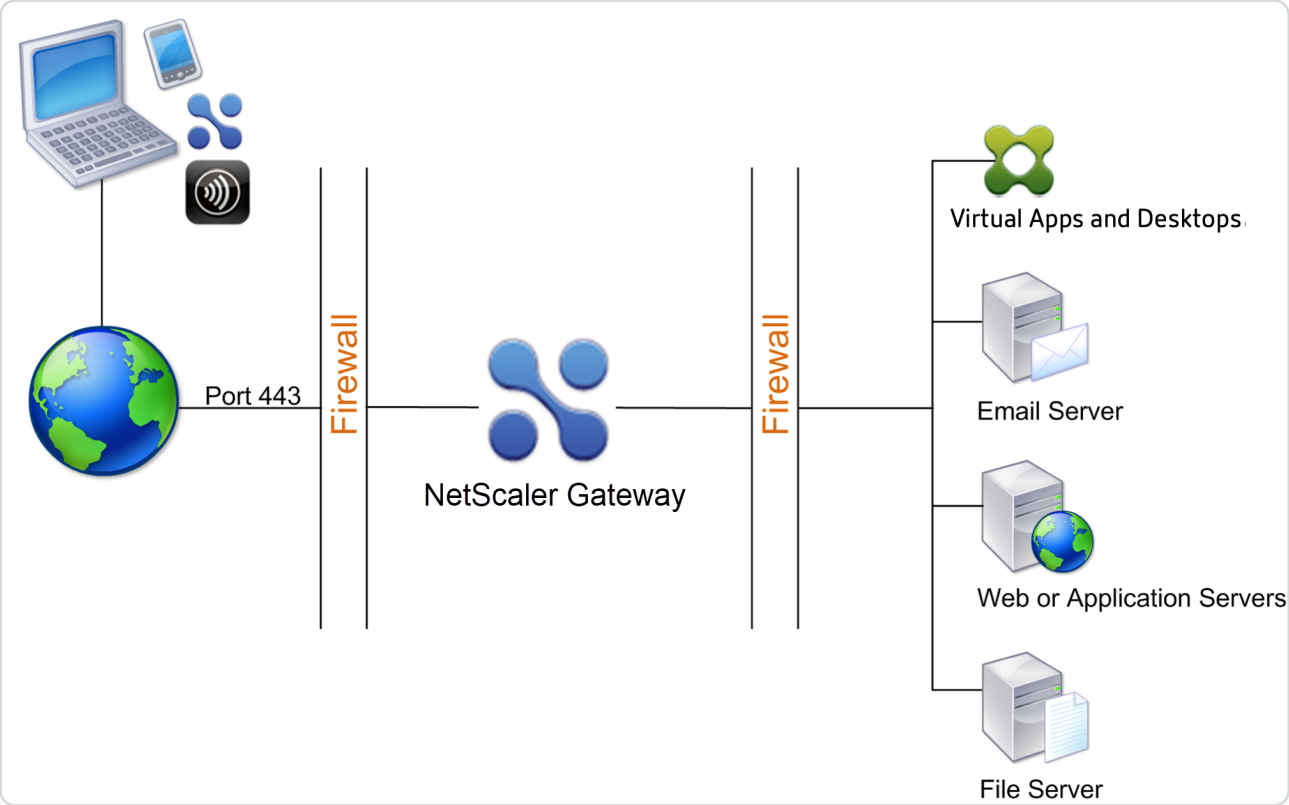
Para obtener más información sobre cómo ampliar su instalación de NetScaler Gateway con estas y otras soluciones de NetScaler compatibles, consulte el tema Integración con productos NetScaler.

## Implementar NetScaler Gateway en una DMZ

Muchas organizaciones protegen su red interna con una DMZ. Una DMZ es una subred que se encuentra entre la red interna segura de una organización e Internet (o cualquier red externa). Cuando implementa NetScaler Gateway en la DMZ, los usuarios se conectan con Citrix Secure Access para Windows o la aplicación Citrix Workspace.

Figura 1. NetScaler Gateway implementado en la DMZ

© 1997–2026 Citrix Systems, Inc. All rights reserved.




En la configuración que se muestra en la figura anterior, instala NetScaler Gateway en la DMZ y lo configura para que se conecte tanto a Internet como a la red interna.

## Conectividad de NetScaler Gateway en una DMZ

Cuando implementa NetScaler Gateway en la DMZ, las conexiones de usuario deben atravesar el primer firewall para conectarse a NetScaler Gateway. De forma predeterminada, las conexiones de usuario utilizan SSL en el puerto 443 para establecer esta conexión. Para permitir que las conexiones de usuario lleguen a la red interna, debe permitir SSL en el puerto 443 a través del primer firewall.

NetScaler Gateway descifra las conexiones SSL del dispositivo de usuario y establece una conexión en nombre del usuario a los recursos de red detrás del segundo firewall. Los puertos que deben estar abiertos a través del segundo firewall dependen de los recursos de red a los que autorice el acceso a los usuarios externos.

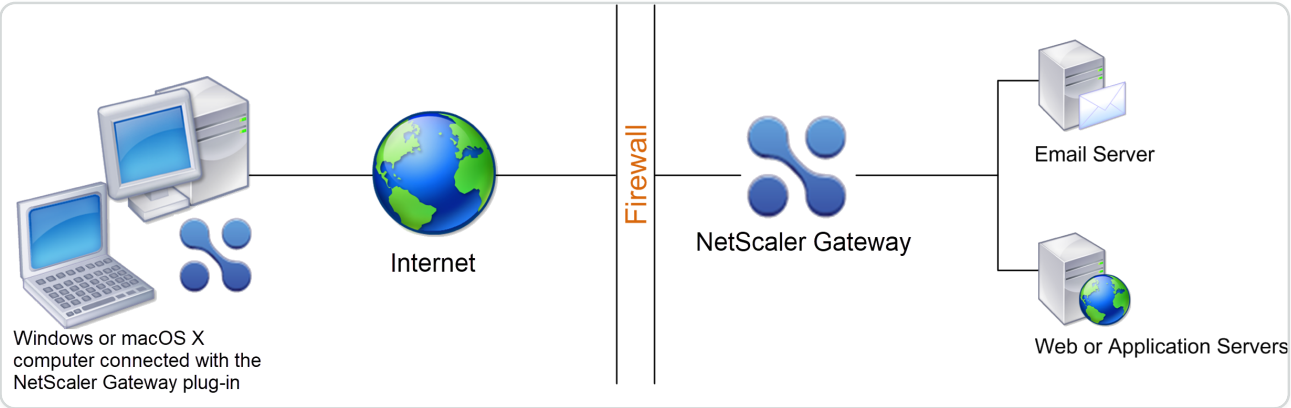
Por ejemplo, si autoriza a usuarios externos a acceder a un servidor web en la red interna, y este servidor escucha las conexiones HTTP en el puerto 80, debe permitir HTTP en el puerto 80 a través del segundo firewall. NetScaler Gateway establece la conexión a través del segundo firewall con el servidor HTTP en la red interna en nombre de los dispositivos de usuario externos.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

# Implementar NetScaler Gateway en una red segura

Puede instalar NetScaler Gateway en la red segura. En este escenario, un firewall se interpone entre Internet y la red segura. NetScaler Gateway reside dentro del firewall para controlar el acceso a los recursos de red.

Figura 1. NetScaler Gateway implementado en la red segura




Cuando implementa NetScaler Gateway en la red segura, conecte una interfaz de NetScaler Gateway a Internet y la otra interfaz a los servidores que se ejecutan en la red segura. Colocar NetScaler Gateway en la red segura proporciona acceso a usuarios locales y remotos. Dado que esta configuración solo tiene un firewall, hace que la implementación sea menos segura para los usuarios que se conectan desde una ubicación remota. Aunque NetScaler Gateway intercepta el tráfico de Internet, el tráfico entra en la red segura antes de que los usuarios se autentiquen. Cuando NetScaler Gateway se implementa en una DMZ, los usuarios se autentican antes de que el tráfico de red llegue a la red segura.

Cuando NetScaler Gateway se implementa en la red segura, las conexiones de Citrix Secure Access para Windows deben atravesar el firewall para conectarse a NetScaler Gateway. De forma predeterminada, las conexiones de usuario utilizan el protocolo SSL en el puerto 443 para establecer esta conexión. Para admitir esta conectividad, debe abrir el puerto 443 en el firewall.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

# Requisitos de software del cliente

NetScaler Gateway admite conexiones de usuario mediante el cliente Citrix Secure Access. Cuando los usuarios inician sesión con el complemento, este establece un túnel VPN completo. Con el cliente Citrix Secure Access, los usuarios pueden conectarse a los recursos de red a los que usted permite el acceso.

Si las directivas de punto final están configuradas en NetScaler Gateway, NetScaler Gateway descarga e instala automáticamente el cliente Citrix EPA en el dispositivo del usuario cuando los usuarios inician sesión.

## Requisitos del sistema del cliente Citrix Secure Access™

El cliente Citrix Secure Access establece una conexión segura desde la máquina cliente al dispositivo NetScaler Gateway.

El complemento se distribuye como una aplicación de escritorio para los sistemas operativos Microsoft Windows, macOS X y Linux. Después de autenticarse en la URL segura del dispositivo NetScaler Gateway con su navegador web, el complemento se descarga e instala automáticamente en su máquina.

El complemento se aprovisiona como una aplicación móvil para dispositivos Android e iOS.

**NOTA:**

- Para instalar el complemento, se requieren privilegios de administrador/root en el sistema operativo.
- Los navegadores que admiten el cliente Citrix Secure Access también admiten VPN sin cliente.

El cliente Citrix Secure Access como aplicación de escritorio es compatible con los siguientes sistemas operativos y navegadores web.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| SISTEMA OPERATIVO | NAVEGADORES COMPATIBLES |
|---|---|
| macOS X (10.9 y posterior) | Safari 7.1 o posterior; Google Chrome versión 30 o posterior; Mozilla Firefox versión 30 o posterior |
| Windows 11 | Google Chrome versión 30 o posterior; Mozilla Firefox versión 24 o posterior; Edge Chromium |
| Windows 10 (x86 y x64) | Google Chrome versión 30 o posterior; Mozilla Firefox versión 24 o posterior; Edge Chromium |
| Linux; Ubuntu 18.04 LTS, 20.04 LTS, 22.04 LTS, 24.04 LTS | Mozilla Firefox versión 44 y superior; Google Chrome 50 y superior |

**NOTA:**

Actualmente, el cliente Citrix Secure Access y el cliente Citrix® EPA para Ubuntu solo admiten el administrador de pantalla GNOME predeterminado.

Si faltan los paquetes de dependencia necesarios, el comando los enumera y la instalación del complemento falla. Estos paquetes de dependencia deben instalarse manualmente. Los administradores pueden instalar un paquete que falta escribiendo el siguiente comando mediante la interfaz de línea de comandos.

```
apt-get install <dependency package>
```

El cliente Citrix Secure Access como aplicación móvil es compatible con los siguientes sistemas operativos.

| APLICACIÓN VPN | SISTEMAS OPERATIVOS COMPATIBLES |
|---|---|
| Android | Android 7.0 y posterior |
| iOS | iOS 12.0 y posteriores |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**NOTA:**

Si utiliza las últimas versiones de SO de Apple, como macOS 14/iOS 17 y posteriores, le recomendamos que actualice a Citrix Secure Access client/Citrix SSO versión 23.09.1 o posterior.

## Requisitos de Endpoint Analysis

NetScaler Gateway instala el cliente Citrix EPA en el dispositivo del usuario. El cliente Citrix EPA escanea el dispositivo del usuario en busca de los requisitos de seguridad de punto final que haya configurado en NetScaler Gateway. Los requisitos incluyen información como el sistema operativo, el antivirus o las versiones del navegador web.

Cuando los usuarios se conectan a NetScaler Gateway por primera vez mediante el navegador, el portal solicita la instalación del cliente Citrix EPA. En los intentos de inicio de sesión posteriores, el cliente Citrix EPA verifica la configuración de control de actualización para confirmar si es necesaria su actualización. Si es necesario, el usuario recibe una solicitud para descargar e instalar la última versión del cliente Citrix EPA. El cliente Citrix EPA para Windows se instala como una aplicación de 32 bits de Windows. El cliente Citrix EPA para macOS se instala como una aplicación de 64 bits. No se requieren privilegios especiales para instalar o usar el cliente Citrix EPA, excepto cuando se usa EPA para acceder a certificados de dispositivo. Para obtener más información sobre cómo usar EPA para la autenticación de certificados de dispositivo, consulte Usar certificados de dispositivo para la autenticación.

Las descripciones emergentes de la consola de la interfaz de usuario de administración explican los análisis en detalle. Para obtener más información sobre las bibliotecas de EPA, consulte `<https://www.citrix.com/downloads/citrix-secure-access/epa-libraries/epa-libraries-for-netscaler-gateway.html>`.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**IMPORTANTE:**

- Los navegadores que admiten EPA también admiten VPN sin cliente.
- En el análisis de punto final previo a la autenticación, el usuario no puede iniciar sesión con el cliente Citrix Secure Access si no instala el complemento de Endpoint Analysis o si omite el análisis.
- En el análisis de punto final posterior a la autenticación, el usuario puede acceder a los recursos para los que no se requiere un análisis mediante el acceso sin cliente o mediante la aplicación Citrix Workspace.
- Para los análisis relacionados con OPSWAT, debe instalar el paquete binario `epaPackage.exe` en la máquina cliente.

El siguiente software es necesario en los dispositivos de usuario para utilizar el complemento de Endpoint Analysis:

| SISTEMA OPERATIVO | NAVEGADORES COMPATIBLES |
|---|---|
| macOS (10.9 y posteriores) | Safari 7.1 o posterior; Google Chrome versión 30 o posterior; Mozilla Firefox versión 30 o posterior |
| Windows 11 | Google Chrome versión 30 o posterior; Mozilla Firefox versión 24 o posterior; Edge Chromium |
| Windows 10 | Google Chrome versión 30 o posterior; Mozilla Firefox versión 24 o posterior; Edge Chromium |
| Linux; Ubuntu 18.04 LTS, 20.04 LTS, 22.04 LTS. | Mozilla Firefox versión 44 y posteriores; Google Chrome 50 y posteriores |

**Nota:**

- Todas las ediciones de las variantes de sistemas operativos mencionadas anteriormente son compatibles.
- Windows 10 y Windows 11 en modos S no son compatibles.
- Para las ediciones de Windows, todos los Service Packs y las actualizaciones críticas deben estar instalados.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Para las versiones de Mozilla Firefox, el Análisis de puntos finales debe tener los complementos habilitados. La versión mínima requerida es la 3.0.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

# Compatibilidad de NetScaler Gateway con los productos Citrix®

La siguiente tabla proporciona los productos y las versiones con los que NetScaler Gateway es compatible.

**NOTA:**

Las funciones de NetScaler Gateway están disponibles en NetScaler VPX.

## Productos Citrix y versiones compatibles

| PRODUCTO CITRIX | VERSIÓN DE LANZAMIENTO |
|---|---|
| Citrix SD-WAN | 10.2, 11.0, 11.1, 11.2, 11.3, 11.4 |
| Plataformas NetScaler | Todos los modelos MPX y VPX actuales, incluidos los dispositivos compatibles con FIPS. |
| StoreFront | Todas las versiones de StoreFront actualmente compatibles. |
| Citrix Aplicaciones y escritorios virtuales | Todas las versiones de Citrix Virtual Apps and Desktops actualmente compatibles. |
| Citrix Endpoint Management | Todas las versiones de Citrix Endpoint Management actualmente compatibles. |

## Aplicaciones Citrix Workspace, aplicaciones de productividad móvil de Citrix y complementos

*La primera compilación compatible para cada versión de software se enumera en la siguiente tabla. Todas las compilaciones posteriores son compatibles a menos que se especifique lo

© 1997–2026 Citrix Systems, Inc. All rights reserved.

contrario. Para obtener más información sobre el ciclo de vida de las versiones, consulte la Matriz de productos.

| APLICACIÓN O COMPLEMENTO CITRIX WORKSPACE | VERSIÓN MÍNIMA COMPATIBLE* |
|---|---|
| Cliente Citrix Secure Access para macOS X | 3.1.8 |
| Cliente Citrix Secure Access para Windows | 12.0 |
| Cliente Citrix Secure Access para iOS | 3.1.4 |
| Cliente Citrix Secure Access para Android | 2.0.14 |
| Aplicación Citrix Workspace para Android | 3.11 |
| Citrix Workspace app para iOS | 7.1.3 |
| Citrix Workspace app para Mac | 12.4 |
| Citrix Workspace app para Windows | 4.4 |
| Citrix Workspace app para Linux | 13.4 |
| Citrix Workspace app para HTML5 | 2.3 |
| Citrix Workspace app para Chrome | 2.3 |
| Secure Hub para iOS | 10.5 |
| Secure Hub para Android | 10.5 |
| Secure Mail para iOS | 10.5 |
| SecureWeb para iOS | 10.5 |
| Secure Mail para Android | 10.5 |
| SecureWeb para Android | 10.5 |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**NOTA:**

- Para obtener más información sobre algunas de las funciones de uso común admitidas para cada cliente VPN, consulte Clientes VPN de NetScaler Gateway y funciones admitidas.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

# Licencias de NetScaler Gateway

Después de instalar NetScaler Gateway, puede obtener sus archivos de licencia de plataforma o universal de Citrix. Inicie sesión en el sitio web de Citrix para acceder a sus licencias disponibles y generar un archivo de licencia. Una vez generado el archivo de licencia, descárguelo en un equipo. Cuando el archivo de licencia esté en el equipo, cárguelo en NetScaler Gateway. Para obtener más información sobre las licencias de Citrix, consulte Sistema de licencias de Citrix.

Antes de obtener los archivos de licencia, asegúrese de configurar el nombre de host del dispositivo mediante el Asistente de configuración y, a continuación, reinicie el dispositivo.

Para obtener sus licencias, vaya a la página web Activar, actualizar y administrar licencias de NetScaler. En esta página, puede obtener su nueva licencia y activar, actualizar y administrar licencias de NetScaler.

**Importante:**

- Debe instalar las licencias en NetScaler Gateway. El dispositivo no obtiene licencias del servidor de licencias de NetScaler.
- Citrix recomienda que conserve una copia local de todos los archivos de licencia que reciba. Cuando guarda una copia de seguridad del archivo de configuración, todos los archivos de licencia cargados se incluyen en la copia de seguridad. Si debe reinstalar el software del dispositivo NetScaler Gateway y no tiene una copia de seguridad de la configuración, necesitará los archivos de licencia originales.

Antes de instalar las licencias en NetScaler Gateway, establezca el nombre de host del dispositivo y, a continuación, reinicie NetScaler Gateway. Utilice el Asistente de configuración para configurar el nombre de host. Cuando genera la licencia universal para NetScaler Gateway, el nombre de host se utiliza en la licencia.

## Tipos de licencia de NetScaler Gateway

NetScaler Gateway requiere una licencia de plataforma. La licencia de plataforma permite un número ilimitado de conexiones a Citrix Virtual Apps, Citrix Virtual Desktops o StoreFront mediante ICA Proxy. Para permitir conexiones VPN a la red desde el cliente Citrix Secure Access, un punto

© 1997–2026 Citrix Systems, Inc. All rights reserved.

de inicio de sesión de SmartAccess, o Secure Hub, WorxWeb o Secure Mail, también debe agregar una licencia universal. NetScaler Gateway VPX incluye la licencia de plataforma.

La licencia de plataforma es compatible con las siguientes versiones de NetScaler Gateway:

- NetScaler Gateway 12.1
- NetScaler Gateway 12.0
- NetScaler Gateway 11.1
- NetScaler Gateway 11.0
- NetScaler Gateway 10.5
- NetScaler Gateway 10.1
- Access Gateway 10
- NetScaler VPX

**IMPORTANTE:**

Citrix recomienda que conserve una copia local de todos los archivos de licencia que reciba. Al guardar una copia de seguridad del archivo de configuración, todos los archivos de licencia cargados se incluyen en la copia de seguridad. Si necesita reinstalar el software del dispositivo NetScaler Gateway y no tiene una copia de seguridad de la configuración, necesitará los archivos de licencia originales.

## La licencia de plataforma

La licencia de plataforma permite conexiones de usuario ilimitadas a aplicaciones publicadas en Citrix Virtual Apps o escritorios virtuales de Citrix Virtual Desktops. Las conexiones que utilizan Citrix Receiver no usan una licencia universal de NetScaler Gateway. Estas conexiones solo necesitan la licencia de plataforma. La licencia de plataforma se entrega electrónicamente con todos los nuevos pedidos de NetScaler Gateway, ya sean físicos o virtuales. Si ya posee un dispositivo cubierto por una garantía o un contrato de mantenimiento, puede obtener la licencia de plataforma en el sitio web de Citrix.

## La licencia universal

La licencia universal de NetScaler Gateway limita el número de sesiones de usuario simultáneas al número de licencias adquiridas. Si adquiere 100 licencias, puede tener 100 sesiones simultáneas en cualquier momento. Si adquiere una licencia de edición Standard, puede tener 500 sesiones simultáneas en cualquier momento. Cuando un usuario finaliza una sesión, esa licencia

© 1997–2026 Citrix Systems, Inc. All rights reserved.

se libera para el siguiente usuario. Un usuario que inicia sesión en NetScaler Gateway desde más de un equipo ocupa una licencia por cada sesión.

Si todas las licencias están ocupadas, no se pueden abrir conexiones adicionales hasta que un usuario finalice una sesión o el administrador la termine mediante la utilidad de configuración. Cuando se cierra una conexión, la licencia se libera y se puede usar para un nuevo usuario.

Cuando reciba su dispositivo NetScaler Gateway, la concesión de licencias se realiza en el siguiente orden:

- Recibirá el código de acceso a la licencia (clave de licencia) en un correo electrónico.
- Utilice el Asistente de configuración para configurar NetScaler Gateway con el nombre de host.
- Asigne las licencias de NetScaler Gateway desde el sitio web de Citrix. Utilice el nombre de host para vincular las licencias al dispositivo durante el proceso de asignación.
- Instale el archivo de licencia en NetScaler Gateway.

La licencia Universal admite las siguientes funciones:

- Túnel VPN completo
- Micro VPN
- Análisis de puntos finales
- SmartAccess basado en directivas
- Acceso sin cliente a sitios web y recursos compartidos de archivos

### Obtención de la licencia Universal

Necesita la siguiente información antes de ir al sitio web de Citrix® para obtener la licencia universal.

Su ID de usuario y contraseña de la cuenta de Citrix.

```
Regístrese en el sitio web de Citrix (<https://www.citrix.com/welcome/
create-account/>) para recibir su ID de usuario y contraseña.

Nota: Si no puede localizar el código de licencia o su ID de usuario y
contraseña, póngase en contacto con el Servicio de atención al cliente de
Citrix.
```

El nombre de host de NetScaler Gateway

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> El campo de entrada para este nombre en el sitio web de Citrix distingue entre mayúsculas y minúsculas, así que asegúrese de copiar el nombre de host exactamente como está configurado en el dispositivo NetScaler.

- El número de licencias que desea incluir en el archivo de licencia

> No tiene que descargar todas las licencias a las que tiene derecho a la vez. Por ejemplo, si su empresa compró 100 licencias, puede optar por descargar 50. Puede asignar el resto en otro archivo de licencia más tarde. Se pueden instalar varios archivos de licencia en el
>
> NetScaler Gateway.
>
> **Nota:** Antes de obtener sus licencias, asegúrese de configurar el nombre de host del dispositivo NetScaler mediante el Asistente de configuración y, a continuación, reinicie el dispositivo.

#### Para obtener su licencia universal

1. Inicie sesión en el sitio web de Citrix (https://www.citrix.com/en-in/account/) con sus credenciales de Citrix.
2. En **Citrix Manage Licenses is here**, siga las instrucciones para obtener su archivo de licencia.

### Instalación de la licencia universal

Para instalar la licencia, consulte «Instalación de la licencia». Después de la instalación, verificar que la licencia se haya instalado correctamente.

### Verificación de la instalación de la licencia universal

Antes de continuar, verificar que su licencia universal esté instalada correctamente.

#### Para verificar la instalación de la licencia universal mediante la CLI

1. Abra una conexión SSH al dispositivo NetScaler mediante un cliente SSH, como PuTTY.
2. Inicie sesión en el dispositivo NetScaler con las credenciales de administrador.
3. Utilice el comando show license para verificar que «SSL VPN = YES» y que el número máximo de usuarios haya aumentado de 5 al número esperado de usuarios simultáneos.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**Para verificar la instalación de la licencia universal mediante la GUI**

1. En un explorador web, escriba la dirección IP del dispositivo NetScaler, como `http://192.168.100.1`.
2. En Nombre de usuario y Contraseña, escriba las credenciales de administrador.
3. En el panel de navegación, expanda Sistema y, a continuación, haga clic en Licencias.
4. En el panel Licencias, verá una marca de verificación verde junto a **Citrix Gateway**. El campo Usuarios máximos permitidos de NetScaler Gateway muestra el número de sesiones de usuario simultáneas con licencia en el dispositivo NetScaler.

## Recursos relacionados

- Sistema de licencias de Citrix
- Hoja de datos de NetScaler
- Tipos de licencias de NetScaler y NetScaler Gateway

## Instalar una licencia en NetScaler Gateway

Después de descargar correctamente el archivo de licencia en su equipo, puede instalar la licencia en NetScaler Gateway. La licencia se instala en el directorio /nsconfig/license.

Si utilizó el Asistente de configuración para configurar los ajustes iniciales en NetScaler Gateway, el archivo de licencia se instala al ejecutar el asistente. Si asigna parte de sus licencias y, más tarde, asigna un número adicional, puede instalar las licencias sin utilizar el Asistente de configuración.

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda **Sistema** y, a continuación, haga clic en **Licencias**.
2. En el panel de detalles, haga clic en **Administrar licencias**.
3. Haga clic en **Agregar nueva licencia**, luego haga clic en **Examinar**, vaya al archivo de licencia y, a continuación, haga clic en **Aceptar**.

   Aparece un mensaje en la utilidad de configuración que indica que debe reiniciar NetScaler Gateway. Haga clic en Reiniciar.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

## Establecer el número máximo de usuarios

Después de instalar la licencia en el dispositivo, debe establecer el número máximo de usuarios que pueden conectarse al dispositivo. El número máximo de usuarios se establece en la directiva de autenticación global.

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda **NetScaler Gateway** y, a continuación, haga clic en **Configuración global**.
2. En el panel de detalles, en Configuración, haga clic en **Cambiar configuración de autenticación AAA**.
3. En Número máximo de usuarios, escriba el número total de usuarios y, a continuación, haga clic en **Aceptar**.

   El número de este campo corresponde al número de licencias contenidas en el archivo de licencia. Este número debe ser menor o igual que el número total de licencias instaladas en el dispositivo. Por ejemplo, si instala una licencia que contiene 100 licencias de usuario y una segunda licencia que contiene 400 licencias de usuario, el número total de licencias es 500. El número máximo de usuarios que pueden iniciar sesión es igual o inferior a 500. Si 500 usuarios han iniciado sesión, a cualquier usuario que intente iniciar sesión más allá de ese número se le denegará el acceso hasta que un usuario cierre la sesión o usted finalice una sesión.

## verificar la instalación de la licencia Universal

Antes de continuar, verificar que su licencia Universal esté instalada correctamente.

### Para verificar la instalación de la licencia Universal mediante la GUI

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda Sistema y, a continuación, haga clic en Licencias.

   En el panel Licencias, verá una marca de verificación verde junto a NetScaler Gateway. El campo Usuarios máximos permitidos de NetScaler Gateway muestra el número de sesiones de usuario simultáneas con licencia en el dispositivo.

### Para verificar la instalación de la licencia Universal mediante la CLI

1. Abra una conexión Secure Shell (SSH) al dispositivo mediante un cliente SSH, como PuTTY.
2. Inicie sesión en el dispositivo con las credenciales de administrador.
3. En un símbolo del sistema, escriba;

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
show license
```

La licencia se instala correctamente si el parámetro SSL VPN es igual a Sí y el parámetro de usuarios máximos es igual al número de licencias.

# Preguntas frecuentes sobre las licencias de NetScaler Gateway

## ¿Cómo puedo obtener ayuda con las licencias de prueba o de demostración?

Muchos de los productos de NetScaler se ofrecen ahora como experiencias de demostración completas, privadas, uno a uno y dirigidas por expertos. Nuestros expertos de Citrix personalizan la demostración para adaptarla a sus necesidades, casos de uso y proyectos activos. No se requieren descargas, licencias ni instalaciones. Necesita una configuración mínima para ver una demostración instantánea. Después de la demostración, para continuar con una prueba de concepto o una prueba de una solución de Citrix que se aplique a sus servicios, póngase en contacto con los expertos de Citrix. Para demostraciones, haga clic `<https://demo.citrix.com/>`.

## ¿Cómo instalar licencias?

Para obtener más información sobre la instalación de licencias, consulte Para instalar una licencia en NetScaler Gateway.

## ¿Cuáles son los diferentes tipos de licencias de Gateway?

La licencia de plataforma permite un número ilimitado de conexiones a Citrix Virtual Apps, Citrix Virtual Desktops™ o StoreFront mediante ICA Proxy. La licencia universal es una licencia adicional a las licencias de plataforma de NetScaler. Esto permite conexiones VPN a la red desde el cliente Citrix Secure Access, un punto de inicio de sesión de SmartAccess, o Secure Hub, Secure Web o Secure Mail. Para obtener más detalles, consulte Tipos de licencias de NetScaler Gateway.

## ¿Cuántas sesiones de usuario simultáneas se admiten?

Las sesiones admitidas dependen del tipo de licencia de Gateway. Para obtener más información, consulte Tipos de licencias de NetScaler Gateway.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Otro factor a considerar es la capacidad del hardware subyacente. Consulte la hoja de datos de NetScaler MPX/SDX o la hoja de datos de NetScaler VPX para conocer las consideraciones de rendimiento.

## ¿Cómo comprobar las sesiones de usuario simultáneas con licencia actuales?

En la utilidad de configuración, en la ficha Configuración, expanda **Sistema** y, a continuación, haga clic en **Licencias**. En el panel **Licencias**, verá una marca de verificación verde junto a NetScaler Gateway. El campo **Usuarios máximos de NetScaler Gateway permitidos** muestra el número de sesiones de usuario simultáneas con licencia en el dispositivo.

## ¿Cómo comprobar si se ha alcanzado el límite de rendimiento con licencia?

Puede extraer el rendimiento en tiempo real mediante `newnslog`. Por ejemplo, si el rendimiento de la licencia es de 500 Mbps, puede extraer el rendimiento en tiempo real superior a 500 mediante el siguiente comando.

```
nsconmsg -K newnslog -g mbits -d past -s disptime=1 -s ratecount=500 |
more
```

```
reltime:mili second between two records Mon Feb  5 13:47:13 2018
 Index   rtime totalcount-val      delta rate/sec symbol-name&device-no&time
    12    7000      801130681       3701      528 allnic_tot_rx_mbits  Mon Feb  5 13:47:55 2018
    13       0      460776045       3682      526 nic_tot_rx_mbits interface(0/2) Mon Feb  5 13:47:55 2018
    14    7000      801134437       3756      536 allnic_tot_rx_mbits  Mon Feb  5 13:48:02 2018
    15       0      460779784       3739      534 nic_tot_rx_mbits interface(0/2) Mon Feb  5 13:48:02 2018
    16    7000      801138166       3729      532 allnic_tot_rx_mbits  Mon Feb  5 13:48:09 2018
    17       0      460783497       3713      530 nic_tot_rx_mbits interface(0/2) Mon Feb  5 13:48:09 2018
    18    7000      801141896       3730      532 allnic_tot_rx_mbits  Mon Feb  5 13:48:16 2018
    19       0      460787213       3716      530 nic_tot_rx_mbits interface(0/2) Mon Feb  5 13:48:16 2018
    20    7000      801145623       3727      532 allnic_tot_rx_mbits  Mon Feb  5 13:48:23 2018
    21       0      460790929       3716      530 nic_tot_rx_mbits interface(0/2) Mon Feb  5 13:48:23 2018
    22    7000      801149353       3730      532 allnic_tot_rx_mbits  Mon Feb  5 13:48:30 2018
    23       0      460794646       3717      531 nic_tot_rx_mbits interface(0/2) Mon Feb  5 13:48:30 2018
    24    7000      801153067       3714      530 allnic_tot_rx_mbits  Mon Feb  5 13:48:37 2018
    25       0      460798342       3696      528 nic_tot_rx_mbits interface(0/2) Mon Feb  5 13:48:37 2018
```

## ¿Cómo comprobar si se descartan paquetes al alcanzar el rendimiento de la licencia?

Puede usar el siguiente comando para comprobar si se descartan paquetes.

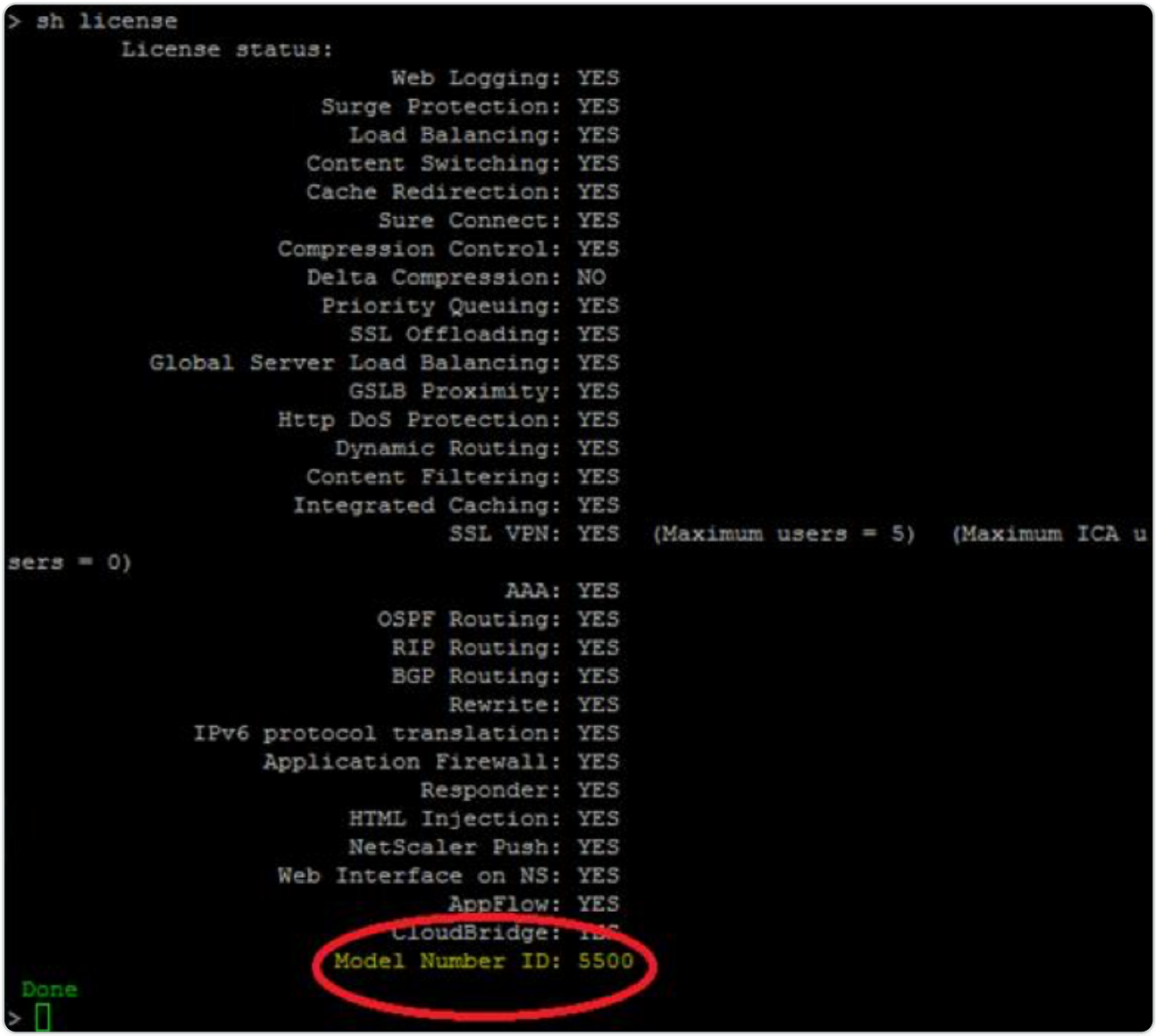
```
nsconmsg -K newnslog -d current -g nic_err_rl_pkt_drops -s disptime=1 |
more
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

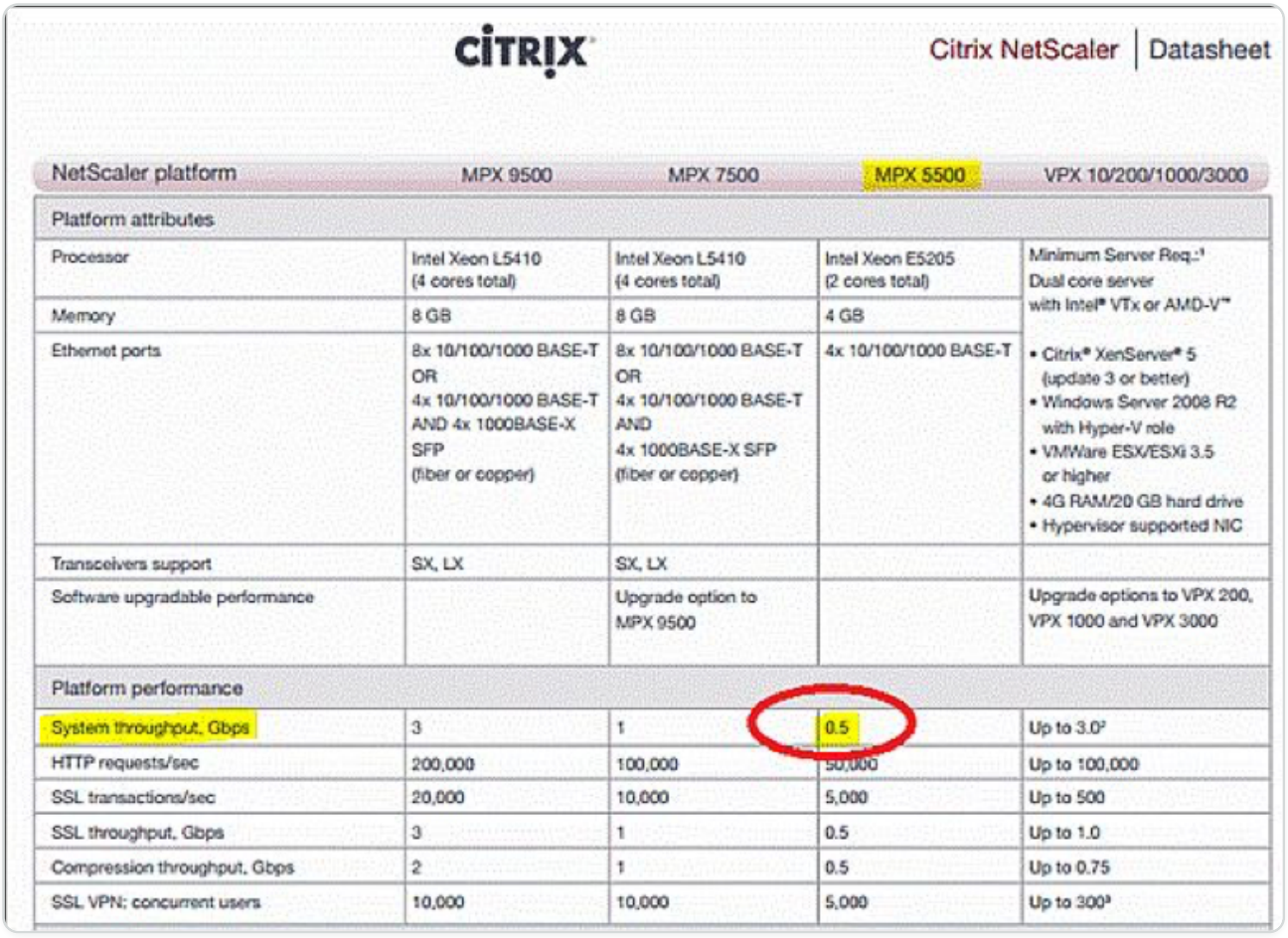
```
reltime:mili second between two records Fri Feb  2 00:12:38 2018
 Index    rtime    totalcount-val      delta rate/sec symbol-name&device-no&time
     0 1966993          23723602        478       68 nic_err_rl_pkt_drops interface(1/2) Fri Feb  2 00:12:38 2018
     1        0          48048402        465       66 nic_err_rl_pkt_drops interface(1/1) Fri Feb  2 00:12:38 2018
     2        0        8307679782     145475    20782 nic_err_rl_pkt_drops interface(0/2) Fri Feb  2 00:12:38 2018
     3     7000          23723933        331       47 nic_err_rl_pkt_drops interface(1/2) Fri Feb  2 00:12:45 2018
     4        0          48048712        310       44 nic_err_rl_pkt_drops interface(1/1) Fri Feb  2 00:12:45 2018
     5        0        8307787105     107323    15331 nic_err_rl_pkt_drops interface(0/2) Fri Feb  2 00:12:45 2018
     6     7000          23723941          8        1 nic_err_rl_pkt_drops interface(1/2) Fri Feb  2 00:12:52 2018
     7        0          48048735         23        3 nic_err_rl_pkt_drops interface(1/1) Fri Feb  2 00:12:52 2018
     8        0        8307811163      24058     3436 nic_err_rl_pkt_drops interface(0/2) Fri Feb  2 00:12:52 2018
```

## ¿Cómo puedo averiguar cuál es el rendimiento con licencia de un dispositivo NetScaler?

Ejecute el comando `show license` desde la CLI y, a continuación, use el número de modelo para obtener el rendimiento de la hoja de datos de ADC o Gateway MPX, SDX y VPX.




© 1997–2026 Citrix Systems, Inc. All rights reserved.



CITRIX

Citrix NetScaler | Datasheet

| NetScaler platform | MPX 9500 | MPX 7500 | MPX 5500 | VPX 10/200/1000/3000 |
|---|---|---|---|---|
| **Platform attributes** | | | | |
| Processor | Intel Xeon L5410 (4 cores total) | Intel Xeon L5410 (4 cores total) | Intel Xeon E5205 (2 cores total) | Minimum Server Req.:[1] Dual core server with Intel® VTx or AMD-V™ • Citrix® XenServer® 5 (update 3 or better) • Windows Server 2008 R2 with Hyper-V role • VMWare ESX/ESXi 3.5 or higher • 4G RAM/20 GB hard drive • Hypervisor supported NIC |
| Memory | 8 GB | 8 GB | 4 GB | |
| Ethernet ports | 8x 10/100/1000 BASE-T OR 4x 10/100/1000 BASE-T AND 4x 1000BASE-X SFP (fiber or copper) | 8x 10/100/1000 BASE-T OR 4x 10/100/1000 BASE-T AND 4x 1000BASE-X SFP (fiber or copper) | 4x 10/100/1000 BASE-T | |
| Transceivers support | SX, LX | SX, LX | | |
| Software upgradable performance | | Upgrade option to MPX 9500 | | Upgrade options to VPX 200, VPX 1000 and VPX 3000 |
| **Platform performance** | | | | |
| System throughput, Gbps | 3 | 1 | 0.5 | Up to 3.0[2] |
| HTTP requests/sec | 200,000 | 100,000 | 50,000 | Up to 100,000 |
| SSL transactions/sec | 20,000 | 10,000 | 5,000 | Up to 500 |
| SSL throughput, Gbps | 3 | 1 | 0.5 | Up to 1.0 |
| Compression throughput, Gbps | 2 | 1 | 0.5 | Up to 0.75 |
| SSL VPN: concurrent users | 10,000 | 10,000 | 5,000 | Up to 300[3] |

## ¿Cómo agregar más usuarios a las licencias de Gateway existentes?

Puede instalar una licencia universal adicional. Por ejemplo, suponga que ha instalado una licencia universal que contiene 100 licencias de usuario. Si instala la segunda licencia universal que contiene 400 licencias de usuario, el número total de licencias de usuario es igual a 500.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

# Antes de empezar

Antes de instalar NetScaler Gateway, debe evaluar su infraestructura y recopilar información para planificar una estrategia de acceso que satisfaga las necesidades específicas de su organización. Al definir su estrategia de acceso, debe considerar las implicaciones de seguridad y completar un análisis de riesgos. También debe determinar las redes a las que los usuarios pueden conectarse y decidir las directivas que permiten las conexiones de los usuarios.

Además de planificar los recursos disponibles para los usuarios, también debe planificar su escenario de implementación. NetScaler Gateway es compatible con los siguientes productos de NetScaler:

- Citrix Endpoint Management™
- Citrix Virtual Apps™
- Citrix Virtual Desktops™
- StoreFront™
- Citrix SD-WAN™

Para obtener más información sobre la implementación de NetScaler Gateway, consulte Implementaciones comunes e Integración con productos de NetScaler

Mientras prepara su estrategia de acceso, siga los siguientes pasos preliminares:

- Identifique los recursos. Enumere los recursos de red a los que desea proporcionar acceso, como aplicaciones web, SaaS, móviles o publicadas, escritorios virtuales, servicios y datos que definió en su análisis de riesgos.
- Desarrolle escenarios de acceso. Cree escenarios de acceso que describan cómo los usuarios acceden a los recursos de red. Un escenario de acceso se define por el servidor virtual utilizado para acceder a la red, los resultados del análisis de puntos finales, el tipo de autenticación o una combinación de estos. También puede definir cómo los usuarios inician sesión en la red.
- Identifique el software cliente. Puede proporcionar acceso VPN completo con el cliente Citrix Secure Access, lo que requiere que los usuarios inicien sesión con la aplicación Citrix Workspace, Secure Hub o mediante acceso sin cliente. También puede restringir el acceso al correo electrónico a Outlook Web App o WorxMail. Estos escenarios de acceso también

© 1997–2026 Citrix Systems, Inc. All rights reserved.

determinan las acciones que los usuarios pueden realizar cuando obtienen acceso. Por ejemplo, puede especificar si los usuarios pueden modificar documentos mediante una aplicación publicada o conectándose a un recurso compartido de archivos.

- Asocie directivas con usuarios, grupos o servidores virtuales. Las directivas que cree en NetScaler Gateway se aplican cuando el individuo o el conjunto de usuarios cumplen las condiciones especificadas. Usted determina las condiciones basándose en los escenarios de acceso que cree. Luego, crea directivas que extienden la seguridad de su red al controlar los recursos a los que los usuarios pueden acceder y las acciones que pueden realizar en esos recursos. Asocia las directivas con los usuarios, grupos, servidores virtuales apropiados o globalmente.

Esta sección incluye los siguientes temas para ayudarle a planificar su estrategia de acceso:

- La planificación de la seguridad incluye información sobre autenticación y certificados.
- Requisitos previos que definen el hardware y software de red que podría necesitar.
- La lista de comprobación previa a la instalación que puede utilizar para anotar su configuración antes de configurar NetScaler Gateway.

## Requisitos previos para instalar NetScaler Gateway

Antes de configurar los ajustes en NetScaler Gateway, revise los siguientes requisitos previos:

- NetScaler Gateway está instalado físicamente en su red y tiene acceso a la red. NetScaler Gateway se implementa en la DMZ o en la red interna detrás de un firewall. También puede configurar NetScaler Gateway en una DMZ de doble salto y configurar conexiones a una granja de servidores. Citrix recomienda implementar el dispositivo en la DMZ.
- Configure NetScaler Gateway con una puerta de enlace predeterminada o con rutas estáticas a la red interna para que los usuarios puedan acceder a los recursos de la red. NetScaler Gateway está configurado para usar rutas estáticas de forma predeterminada.
- Los servidores externos utilizados para la autenticación y autorización están configurados y en funcionamiento. Para obtener más información, consulte Autenticación y autorización.
- La red tiene un servidor de nombres de dominio (DNS) o un servidor de servicio de nombres de Internet de Windows (WINS) para la resolución de nombres para proporcionar la funcionalidad correcta del usuario de NetScaler Gateway.
- Ha descargado las licencias universales para conexiones de usuario con el cliente Citrix Secure Access desde el sitio web de Citrix y las licencias están listas para ser instaladas en NetScaler Gateway.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- NetScaler Gateway tiene un certificado firmado por una autoridad de certificación (CA) de confianza. Para obtener más información, consulte Instalación y administración de certificados.

Antes de instalar NetScaler Gateway, utilice la lista de comprobación previa a la instalación para anotar su configuración.

# Planificación de la seguridad

Al planificar su implementación de NetScaler Gateway, debe comprender los problemas de seguridad básicos asociados con los certificados, y con la autenticación y autorización.

## Configurar la gestión segura de certificados

De forma predeterminada, NetScaler Gateway incluye un certificado de servidor SSL (Secure Sockets Layer) autofirmado que permite al dispositivo completar los handshakes SSL. Los certificados autofirmados son adecuados para pruebas o para implementaciones de ejemplo, pero NetScaler no recomienda utilizarlos para entornos de producción. Antes de implementar NetScaler Gateway en un entorno de producción, Citrix recomienda solicitar y recibir un certificado de servidor SSL firmado de una entidad de certificación (CA) conocida y cargarlo en NetScaler Gateway.

Si implementa NetScaler Gateway en cualquier entorno donde NetScaler Gateway deba funcionar como cliente en un handshake SSL (iniciar conexiones cifradas con otro servidor), también debe instalar un certificado raíz de confianza en NetScaler Gateway. Por ejemplo, si implementa NetScaler Gateway con Citrix Virtual Apps y StoreFront, puede cifrar las conexiones de NetScaler Gateway a StoreFront con SSL. En esta configuración, debe instalar un certificado raíz de confianza en NetScaler Gateway.

## Compatibilidad con la autenticación

Puede configurar NetScaler Gateway para autenticar usuarios y controlar el nivel de acceso (o autorización) que los usuarios tienen a los recursos de red en la red interna.

Antes de implementar NetScaler Gateway, su entorno de red debe tener los directorios y servidores de autenticación configurados para admitir uno de los siguientes tipos de autenticación:

- LDAP
- RADIUS
- TACACS+
- Certificado de cliente con auditoría y compatibilidad con tarjetas inteligentes

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- RSA con configuración RADIUS
- Autenticación SAML

Si su entorno no admite ninguno de estos tipos de autenticación, o si tiene una pequeña población de usuarios remotos, puede crear una lista de usuarios locales en NetScaler Gateway. A continuación, puede configurar NetScaler Gateway para autenticar a los usuarios con esta lista local. Con esta configuración, no necesita mantener las cuentas de usuario en un directorio externo independiente.

## Proteja su implementación de NetScaler Gateway

Las diferentes implementaciones pueden requerir diferentes consideraciones de seguridad. Las directrices de implementación segura de NetScaler proporcionan orientación general de seguridad para ayudarle a decidir una implementación segura adecuada en función de sus requisitos de seguridad específicos.

Para obtener más información, consulte Directrices de implementación segura de NetScaler.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

# Lista de comprobación previa a la instalación de Gateway

La lista de comprobación consta de una lista de tareas e información de planificación que debe completar antes de instalar NetScaler Gateway.

Se proporciona espacio para que pueda marcar cada tarea a medida que la completa y tomar notas. Citrix recomienda que anote los valores de configuración que debe introducir durante el proceso de instalación y al configurar NetScaler Gateway.

Para conocer los pasos para instalar y configurar NetScaler Gateway, consulte Instalación de NetScaler Gateway.

## Dispositivos de usuario

- Asegúrese de que los dispositivos de usuario cumplen los requisitos previos de instalación descritos en Requisitos del sistema de Citrix Secure Access
- Identifique los dispositivos móviles con los que se conectan los usuarios. **Nota**: Si los usuarios se conectan con un dispositivo iOS, debe habilitar Secure Browse en un perfil de sesión.

## Conectividad de red básica de NetScaler Gateway

Citrix® recomienda obtener licencias y certificados de servidor firmados antes de empezar a configurar el dispositivo.

- Identifique y anote el nombre de host de NetScaler Gateway. **Nota**: Este no es el nombre de dominio completo (FQDN). El FQDN está contenido en el certificado de servidor firmado que está vinculado al servidor virtual.
- Obtenga licencias universales del sitio web de Citrix
- Genere una solicitud de firma de certificado (CSR) y envíela a una autoridad de certificación (CA). Introduzca la fecha en que envía la CSR a la autoridad de certificación.
- Anote la dirección IP del sistema y la máscara de subred.
- Anote la dirección IP de subred y la máscara de subred.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Anote la contraseña de administrador. La contraseña predeterminada que viene con NetScaler Gateway es `nsroot`.
- Anote el número de puerto en el que NetScaler Gateway escucha las conexiones seguras de los usuarios. El valor predeterminado es el puerto TCP 443. Este puerto debe estar abierto en el firewall entre la red no segura (Internet) y la DMZ.
- Anote la dirección IP de la puerta de enlace predeterminada.
- Anote la dirección IP del servidor DNS y el número de puerto. El número de puerto predeterminado es 53. Además, si va a agregar el servidor DNS directamente, también debe configurar ICMP (ping) en el dispositivo.
- Anote la dirección IP y el nombre de host del primer servidor virtual.
- Anote la dirección IP y el nombre de host del segundo servidor virtual (si corresponde).
- Anote la dirección IP del servidor WINS (si corresponde).

## Redes internas accesibles a través de NetScaler Gateway

- Anote las redes internas a las que los usuarios pueden acceder a través de NetScaler Gateway. Ejemplo: 10.10.0.0/24
- Introduzca todas las redes internas y segmentos de red a los que los usuarios necesitan acceso cuando se conectan a través de NetScaler Gateway mediante el cliente Citrix Secure Access.

## Alta disponibilidad

Si tiene dos dispositivos NetScaler Gateway, puede implementarlos en una configuración de alta disponibilidad en la que un NetScaler Gateway acepta y administra las conexiones, mientras que un segundo NetScaler Gateway supervisa el primer dispositivo. Si el primer NetScaler Gateway deja de aceptar conexiones por cualquier motivo, el segundo NetScaler Gateway toma el control y comienza a aceptar conexiones activamente.

- Anote el número de versión del software de NetScaler Gateway.
- El número de versión debe ser el mismo en ambos dispositivos NetScaler Gateway.
- Anote la contraseña de administrador (`nsroot`). La contraseña debe ser la misma en ambos dispositivos.
- Anote la dirección IP y el ID del NetScaler Gateway principal. El número de ID máximo es 64.
- Anote la dirección IP y el ID de NetScaler Gateway secundario.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Obtenga e instale la licencia Universal en ambos dispositivos.
- Instale la misma licencia Universal en ambos dispositivos.
- Anote la contraseña del nodo RPC.

# Autenticación y autorización

NetScaler Gateway admite varios tipos diferentes de autenticación y autorización que se pueden utilizar en varias combinaciones. Para obtener información detallada sobre la autenticación y la autorización, consulte Autenticación y autorización.

## Autenticación LDAP

Si su entorno incluye un servidor LDAP, puede utilizar LDAP para la autenticación.

- Anote la dirección IP y el puerto del servidor LDAP.

  Si permite conexiones no seguras al servidor LDAP, el puerto predeterminado es 389. Si cifra las conexiones al servidor LDAP con SSL, el puerto predeterminado es 636.
- Anote el tipo de seguridad.

  Puede configurar la seguridad con o sin cifrado.
- Anote el DN de enlace del administrador.

  Si su servidor LDAP requiere autenticación, introduzca el DN de administrador que NetScaler Gateway debe usar para autenticarse al realizar consultas al directorio LDAP. Un ejemplo es cn=administrator,cn=Users,dc=ace, dc=com.
- Anote la contraseña del administrador.

  La contraseña está asociada con el DN de enlace del administrador.
- Anote el DN base.

  DN (o nivel de directorio) bajo el cual se encuentran los usuarios; por ejemplo, ou=users,dc=ace,dc=com.
- Anote el atributo de nombre de inicio de sesión del servidor.

  Introduzca el atributo de objeto de persona del directorio LDAP que especifica el nombre de inicio de sesión de un usuario. El valor predeterminado es sAMAccountName. Si no utiliza Active Directory, los valores comunes para esta configuración son cn o uid. Para obtener más información sobre la configuración del directorio LDAP, consulte Configuración de la autenticación LDAP

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Anote el atributo de grupo. Introduzca el atributo de objeto de persona del directorio LDAP que especifica los grupos a los que pertenece un usuario. El valor predeterminado es memberOf. Este atributo permite a NetScaler Gateway identificar los grupos de directorio a los que pertenece un usuario.
- Anote el nombre del subatributo.

### Autenticación y autorización RADIUS

Si su entorno incluye un servidor RADIUS, puede usar RADIUS para la autenticación. La autenticación RADIUS incluye los productos RSA SecurID, SafeWord y Gemalto Protiva.

- Anote la dirección IP y el puerto del servidor RADIUS principal. El puerto predeterminado es 1812.
- Anote el secreto del servidor RADIUS principal (secreto compartido).
- Anote la dirección IP y el puerto del servidor RADIUS secundario. El puerto predeterminado es 1812.
- Anote el secreto del servidor RADIUS secundario (secreto compartido).
- Anote el tipo de codificación de contraseña (PAP, CHAP, MS-CHAP v1, MSCHAP v2).

## Autenticación SAML

El Security Assertion Markup Language (SAML) es un estándar basado en XML para intercambiar autenticación y autorización entre proveedores de identidad (IdP) y proveedores de servicios.

- Obtenga e instale en NetScaler Gateway un certificado IdP seguro.
- Anote la URL de redirección.
- Anote el campo de usuario.
- Anote el nombre del certificado de firma.
- Anote el nombre del emisor de SAML.
- Anote el grupo de autenticación predeterminado.

## Apertura de puertos a través de los firewalls (DMZ de un solo salto)

Si su organización protege la red interna con una única DMZ y usted implementa NetScaler Gateway en la DMZ, abra los siguientes puertos a través de los firewalls. Si está instalando dos

© 1997–2026 Citrix Systems, Inc. All rights reserved.

dispositivos NetScaler Gateway en una implementación de DMZ de doble salto, consulte Apertura de los puertos adecuados en los firewalls.

### En el firewall entre la red no segura y la DMZ

- Abra un puerto TCP/SSL (predeterminado 443) en el firewall entre Internet y NetScaler Gateway. Los dispositivos de usuario se conectan a NetScaler Gateway en este puerto.

### En el firewall entre la red segura

- Abra uno o más puertos apropiados en el firewall entre la DMZ y la red segura. NetScaler Gateway se conecta a uno o más servidores de autenticación o a equipos que ejecutan Citrix Virtual Apps and Desktops en la red segura a través de estos puertos.
- Anote los puertos de autenticación.

  Abra solo el puerto apropiado para su configuración de NetScaler Gateway.

  - Para las conexiones LDAP, el valor predeterminado es el puerto TCP 389.
  - Para una conexión RADIUS, el valor predeterminado es el puerto UDP 1812. Anote los puertos de Citrix Virtual Apps and Desktops.
- Si utiliza NetScaler Gateway con Citrix Virtual Apps and Desktops, abra el puerto TCP 1494. Si habilita la fiabilidad de la sesión, abra el puerto TCP 2598 en lugar del 1494. Citrix recomienda mantener ambos puertos abiertos.

## Citrix Virtual Desktops™, Citrix Virtual Apps o StoreFront

Complete las siguientes tareas si va a implementar NetScaler Gateway para proporcionar acceso a Citrix Virtual Apps and Desktops a través de StoreFront. El cliente de Citrix Secure Access no es necesario para esta implementación. Los usuarios acceden a las aplicaciones y escritorios publicados a través de NetScaler Gateway utilizando únicamente navegadores web y Citrix Receiver.

- Anote el FQDN o la dirección IP del servidor que ejecuta StoreFront.

## Citrix Endpoint Management™

Complete las siguientes tareas si implementa Citrix Endpoint Management en su red interna. Si los usuarios se conectan a Endpoint Management desde una red externa, como Internet, deben conectarse a NetScaler Gateway antes de acceder a las aplicaciones móviles, web y SaaS.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Anote el FQDN o la dirección IP de Endpoint Management.
- Identifique las aplicaciones web, SaaS y móviles iOS o Android a las que los usuarios pueden acceder.

# Implementación de DMZ de doble salto con Citrix Virtual Apps™

Complete las siguientes tareas si va a implementar dos dispositivos NetScaler Gateway en una configuración de DMZ de doble salto para admitir el acceso a servidores que ejecutan Citrix Virtual Apps.

## NetScaler Gateway en la primera DMZ

La primera DMZ es la DMZ en el borde más externo de su red interna (más cercana a Internet o a una red no segura). Los clientes se conectan a NetScaler Gateway en la primera DMZ a través del firewall que separa Internet de la DMZ. Recopile esta información antes de instalar NetScaler Gateway en la primera DMZ.

- Complete los elementos de la sección Conectividad de red básica de NetScaler Gateway de esta lista de comprobación para este NetScaler Gateway.

  Al completar esos elementos, la Interfaz 0 conecta este NetScaler Gateway a Internet y la Interfaz 1 conecta este NetScaler Gateway a NetScaler Gateway en la segunda DMZ.
- Configure la información del dispositivo de la segunda DMZ en el dispositivo principal.

  Para configurar NetScaler Gateway como el primer salto en la DMZ de doble salto, debe especificar el nombre de host o la dirección IP de NetScaler Gateway en la segunda DMZ en el dispositivo de la primera DMZ. Después de especificar cuándo se configura el proxy de NetScaler Gateway en el dispositivo del primer salto, vincúlelo a NetScaler Gateway globalmente o a un servidor virtual.
- Anote el protocolo de conexión y el puerto entre los dispositivos.

  Para configurar NetScaler Gateway como el primer salto en la DMZ doble, debe especificar el protocolo de conexión y el puerto en el que NetScaler Gateway de la segunda DMZ escucha las conexiones. El protocolo de conexión y el puerto son SOCKS con SSL (puerto predeterminado 443). El protocolo y el puerto deben estar abiertos a través del firewall que separa la primera DMZ y la segunda DMZ.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

## NetScaler Gateway en la segunda DMZ

La segunda DMZ es la DMZ más cercana a su red interna y segura. NetScaler Gateway implementado en la segunda DMZ actúa como proxy para el tráfico ICA, atravesando la segunda DMZ entre los dispositivos de usuario externos y los servidores de la red interna.

- Complete las tareas de la sección Conectividad de red básica de NetScaler Gateway de esta lista de comprobación para este NetScaler Gateway.

  Al completar esos elementos, la Interfaz 0 conecta este NetScaler Gateway a NetScaler Gateway en la primera DMZ. La Interfaz 1 conecta este NetScaler Gateway a la red segura.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

# Instalar y configurar el dispositivo NetScaler Gateway

Cuando reciba su dispositivo NetScaler Gateway, desempaquete el dispositivo y prepare el sitio y el rack. Después de determinar que la ubicación donde instala su dispositivo cumple con los estándares ambientales y que el rack del servidor está en su lugar según las instrucciones, instale el hardware. Después de montar el dispositivo, conéctelo a la red, a una fuente de alimentación y al terminal de consola que utiliza para la configuración inicial. Después de encender el dispositivo, realice la configuración inicial y asigne direcciones IP de administración y de red. Asegúrese de observar las precauciones y advertencias enumeradas en las instrucciones de instalación.

Al instalar un dispositivo virtual NetScaler VPX, primero debe adquirir la imagen del dispositivo virtual e instalarla en un hipervisor u otro monitor de máquina virtual.

Citrix recomienda utilizar el tema Lista de comprobación previa a la instalación de NetScaler Gateway para que pueda tomar nota de su configuración antes de intentar configurar un dispositivo NetScaler Gateway. La lista de comprobación incluye información sobre la instalación de NetScaler Gateway y un dispositivo.

## Configurar el dispositivo NetScaler Gateway mediante asistentes

NetScaler Gateway tiene los siguientes seis asistentes que puede usar para configurar los ajustes en el dispositivo:

- El asistente de configuración inicial aparece cuando inicia sesión en el dispositivo NetScaler Gateway por primera vez.
- El asistente de configuración rápida le ayuda a configurar las directivas, expresiones y ajustes correctos para las conexiones a Citrix Endpoint Management™ y StoreFront.
- El asistente de NetScaler Gateway le ayuda a configurar los ajustes específicos de NetScaler Gateway.
- El asistente de configuración le ayuda a configurar los ajustes básicos de NetScaler Gateway por primera vez.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- La configuración integrada de Citrix Endpoint Management le ayuda a configurar su entorno de NetScaler Gateway y Citrix Endpoint Management.
- El asistente de aplicaciones publicadas le ayuda a configurar los ajustes para las conexiones de usuario mediante la aplicación Citrix Workspace.

## Asistente de configuración inicial

Cuando termine de instalar y configurar los ajustes iniciales en el dispositivo NetScaler Gateway, al iniciar sesión en la utilidad de configuración por primera vez, aparece el asistente de configuración inicial si no se cumplen las siguientes condiciones:

- No ha instalado una licencia en el dispositivo.
- No ha configurado una subred o una dirección IP asignada.
- Si la dirección IP predeterminada de los dispositivos es 192.168.100.1.

### Configurar NetScaler Gateway con el asistente de configuración inicial

Para configurar NetScaler Gateway (el dispositivo físico o el dispositivo virtual VPX) por primera vez, necesita un equipo administrativo configurado en la misma red que el dispositivo.

Asigne una dirección IP de NetScaler Gateway (NSIP) como dirección IP de administración de su dispositivo y una dirección IP de subred (SNIP) a la que puedan conectarse sus servidores. Asigne una máscara de subred que se aplique tanto a las direcciones NetScaler Gateway como a las SNIP. Configure también una zona horaria. Si asigna un nombre de host, puede acceder al dispositivo especificando su nombre en lugar de la dirección NSIP.

Hay dos secciones en el Asistente de configuración por primera vez. En la primera sección, configure la configuración básica del sistema para el dispositivo NetScaler Gateway, incluyendo:

Dirección NSIP, dirección SNIP y máscara de subred Nombre de host del dispositivo Servidores DNS Zona horaria Contraseña de administrador En la segunda sección, instale las licencias. Si especifica la dirección de un servidor DNS, puede usar el número de serie del hardware (HSN) o la clave de licencia para asignar sus licencias, en lugar de cargarlas desde un equipo local al dispositivo.

Nota: Citrix® recomienda guardar sus licencias en su equipo local.

Cuando termine de configurar estos ajustes, NetScaler Gateway le pedirá que reinicie el dispositivo. Cuando vuelva a iniciar sesión en el dispositivo, podrá usar otros asistentes y la utilidad de configuración para configurar otros ajustes.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

## Asistente de configuración rápida

El asistente de configuración rápida le permite configurar varios servidores virtuales en NetScaler Gateway. Puede agregar, editar y eliminar servidores virtuales.

El asistente de configuración rápida permite una configuración perfecta para las siguientes implementaciones:

- Conexiones de StoreFront a Citrix Virtual Apps and Desktops, con la capacidad de configurar varias instancias de Secure Ticket Authority (STA)
- Solo Citrix Endpoint Management
- Solo StoreFront™
- Citrix Endpoint Management y StoreFront juntos

El asistente de configuración rápida le permite configurar los siguientes ajustes en el dispositivo:

- Nombre del servidor virtual, dirección IP y puerto
- Redirección de un puerto no seguro a uno seguro
- Servidor LDAP
- Servidor RADIUS
- Certificados
- Servidor DNS
- Citrix Endpoint Management y Citrix Virtual Apps and Desktops

  **Nota**: Para habilitar el SSO, debe habilitar manualmente la opción **Inicio de sesión único en aplicaciones web** en la ficha **Crear perfil de sesión de NetScaler Gateway > Experiencia del cliente** para la acción de sesión.

NetScaler Gateway admite conexiones de usuario directamente a Citrix Endpoint Management, lo que proporciona a los usuarios acceso a sus aplicaciones web, SaaS y móviles, junto con acceso a ShareFile. También puede configurar ajustes en StoreFront, lo que proporciona a los usuarios acceso a sus aplicaciones basadas en Windows y escritorios virtuales.

Al ejecutar el asistente de configuración rápida, se crean las siguientes directivas en función de la configuración de Citrix Endpoint Management y StoreFront:

- Directivas de sesión, incluidas directivas y perfiles para Receiver, Receiver para Web, el cliente Citrix Secure Access™ y Program Neighborhood Agent
- Acceso sin cliente

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Autenticación LDAP y RADIUS

### Configurar ajustes con el asistente de configuración rápida

Puede configurar los ajustes en NetScaler Gateway para habilitar la comunicación con Citrix Endpoint Management o StoreFront mediante el asistente de configuración rápida. Al completar la configuración, el asistente crea las directivas correctas para la comunicación entre NetScaler Gateway, Endpoint Management y StoreFront. Estas directivas incluyen directivas de autenticación, sesión y acceso sin cliente. Cuando el asistente finaliza, las directivas se vinculan al servidor virtual.

Al completar el asistente de configuración rápida, NetScaler Gateway puede comunicarse con Endpoint Management o StoreFront, y los usuarios pueden acceder a sus aplicaciones basadas en Windows y escritorios virtuales, así como a aplicaciones web, SaaS y móviles. Los usuarios pueden entonces conectarse directamente a Endpoint Management.

Durante el asistente, se configuran los siguientes ajustes:

- Nombre del servidor virtual, dirección IP y puerto
- Redirección de un puerto no seguro a uno seguro
- Certificados
- Servidor LDAP
- Servidor RADIUS
- Certificado de cliente para autenticación (solo para autenticación de dos factores)
- Endpoint Management o StoreFront

El asistente de configuración rápida admite la autenticación LDAP, RADIUS y de certificado de cliente. Puede configurar la autenticación de dos factores en el asistente siguiendo estas directrices:

- Si selecciona LDAP como tipo de autenticación principal, puede configurar RADIUS como tipo de autenticación secundaria.
- Si selecciona RADIUS como tipo de autenticación principal, puede configurar LDAP como tipo de autenticación secundaria.
- Si selecciona certificados de cliente como tipo de autenticación principal, puede configurar LDAP o RADIUS como tipo de autenticación secundaria.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

No puede crear varias directivas de autenticación LDAP mediante el asistente de configuración rápida. Por ejemplo, desea configurar una directiva que utilice sAMAccountName en el campo **Atributo de nombre de inicio de sesión del servidor** y una segunda directiva LDAP que utilice el nombre principal de usuario (UPN) en el campo **Atributo de nombre de inicio de sesión del servidor**. Para configurar estas directivas separadas, utilice la utilidad de configuración de NetScaler Gateway para crear las directivas de autenticación. Para obtener más información, consulte Configuración de la autenticación LDAP.

Puede configurar certificados para NetScaler Gateway en el asistente de configuración rápida mediante los siguientes métodos:

- Seleccione un certificado que esté instalado en el dispositivo.
- Instale un certificado y una clave privada.
- Seleccione un certificado de prueba. **Nota**: Si utiliza un certificado de prueba, debe agregar el nombre de dominio completo (FQDN) que se encuentra en el certificado.

Puede abrir el **asistente de configuración rápida** de una de las dos maneras siguientes:

- Cuando esté en la página de inicio de sesión de NetScaler Gateway y seleccione **NetScaler Gateway** en **Tipo de implementación**, aparecerá la ficha **Inicio**. Si selecciona cualquier otra opción en **Tipo de implementación**, la ficha **Inicio** no aparecerá.
- Desde el enlace **Crear/Supervisar NetScaler Gateway** en el panel de detalles de NetScaler Gateway. El enlace aparece si instala una licencia que habilita las funciones de NetScaler. Si solo licencia el dispositivo para NetScaler Gateway, el enlace no aparecerá.

Después de ejecutar el asistente inicialmente, puede volver a ejecutarlo para crear más servidores virtuales y configuraciones.

**IMPORTANTE:**

Si utiliza el asistente de configuración rápida para configurar un servidor virtual NetScaler Gateway adicional, debe utilizar una dirección IP única. No puede utilizar la misma dirección IP que se utiliza en un servidor virtual existente. Por ejemplo, tiene un servidor virtual con la dirección IP 192.168.10.5 con un número de puerto de 80. Ejecuta el asistente de configuración rápida para crear un segundo servidor virtual con la dirección IP 192.168.10.5 con el número de puerto 443. Cuando intenta guardar la configuración, se produce un error.

**Para configurar los ajustes con el asistente de configuración rápida**

1. En la utilidad de configuración, realice una de las siguientes acciones:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

a. Si el dispositivo tiene licencia solo para NetScaler Gateway, haga clic en la ficha **Inicio**.

b. Si el dispositivo tiene licencia para incluir funciones de NetScaler, en la ficha Configuración, en el panel de navegación, haga clic en **NetScaler Gateway** y, a continuación, en el panel de detalles, en **Introducción**, haga clic en **Configurar NetScaler Gateway para Enterprise Store**.

2. En el panel, haga clic en **Crear nuevo NetScaler Gateway**.
3. En **Configuración de NetScaler Gateway**, configure lo siguiente:

   a. En **Nombre**, escriba un nombre para el servidor virtual.

   b. En **Dirección IP**, escriba la dirección IP del servidor virtual.

   c. En **Puerto**, escriba el número de puerto. El número de puerto predeterminado es 443.

   d. Seleccione Redirigir solicitudes del puerto 80 al puerto seguro para permitir que las conexiones de usuario del puerto 80 vayan al puerto 443.

4. Haga clic en **Continuar**.
5. En la página Certificado, realice una de las siguientes acciones:

   a. Haga clic en **Elegir certificado** y, a continuación, en Certificado, seleccione el certificado.

   b. Haga clic en **Instalar certificado** y, a continuación, en **Elegir certificado** y en **Elegir clave**, haga clic en **Examinar** para buscar el certificado y la clave privada.

   c. Haga clic en **Usar certificado de prueba** y, a continuación, en FQDN de certificado, introduzca el nombre de dominio completo (FQDN) contenido en el certificado de prueba.

6. Haga clic en **Continuar**.
7. En Configuración de autenticación, haga lo siguiente:

   a. En **Autenticación principal**, seleccione LDAP, RADIUS o Cert.

   b. Seleccione un servidor de autenticación o configure los ajustes para el tipo de autenticación que seleccionó en el paso anterior. Si selecciona Cert, seleccione el certificado de cliente o instale un nuevo certificado de cliente.

   c. En **Autenticación secundaria**, seleccione el tipo de autenticación y, a continuación, configure los ajustes del servidor de autenticación.

8. Haga clic en **Continuar**.

Cuando termine de configurar la red y los ajustes de autenticación, podrá configurar los ajustes de Citrix Endpoint Management o Citrix Virtual Apps and Desktops (StoreFront).

© 1997–2026 Citrix Systems, Inc. All rights reserved.

### Configurar los ajustes del almacén empresarial

NetScaler Gateway admite el acceso de los usuarios a aplicaciones web, SaaS y móviles y a ShareFile solo a través de Endpoint Management. Si también implementa StoreFront, los usuarios tienen acceso a aplicaciones basadas en Windows y a escritorios virtuales. Puede configurar los ajustes para las siguientes opciones:

- Solo Endpoint Management
- Solo StoreFront
- Endpoint Management y StoreFront juntos

Cuando haga clic en **Continuar** en el procedimiento anterior, podrá configurar los ajustes para su escenario de implementación. Los siguientes procedimientos comienzan en la página Configuración de integración de Citrix.

Después de crear el servidor virtual, la edición del servidor virtual en el asistente de Configuración rápida no le permite cambiar la configuración de Citrix Endpoint Management o Citrix Virtual Apps and Desktops.

Por ejemplo, si cancela la configuración de un servidor virtual en cualquier etapa antes de configurar los ajustes de **Citrix Enterprise Store**, el asistente selecciona automáticamente StoreFront sin configurar ningún ajuste. Cuando esto ocurre, puede editar los detalles del servidor virtual para configurar StoreFront, pero no puede cambiar a Citrix Endpoint Management. Para cambiar, debe crear un nuevo servidor virtual y no debe cancelar el asistente en ningún momento durante la configuración. Si no necesita el servidor virtual de StoreFront, puede eliminarlo mediante el asistente de Configuración rápida.

#### Para configurar los ajustes solo para StoreFront

1. Haga clic en **Citrix Virtual Apps and Desktops**.
2. En **Tipo de implementación**, seleccione **StoreFront**.
3. En **FQDN de StoreFront**, introduzca el nombre de dominio completo (FQDN) del servidor StoreFront.
4. En **Ruta de Receiver para Web**, deje la ruta predeterminada o introduzca su propia ruta.
5. Seleccione **HTTPS** para conexiones de usuario seguras.
6. En **Dominio de inicio de sesión único**, introduzca el dominio para StoreFront.
7. En **URL de STA**, introduzca la dirección IP completa o el FQDN del servidor que ejecuta la Autoridad de tickets seguros (STA) si implementa StoreFront y proporciona acceso a

© 1997–2026 Citrix Systems, Inc. All rights reserved.

aplicaciones publicadas desde Citrix Virtual Apps o escritorios virtuales desde Citrix Virtual Desktops.

8. Haga clic en **Listo**.

Cuando los usuarios se conectan a StoreFront a través de NetScaler Gateway, pueden iniciar sus aplicaciones y escritorios desde Receiver para Web o Receiver.

**Para configurar los ajustes solo para Endpoint Management**

1. Haga clic en **Citrix Endpoint Management**.
2. En **FQDN del controlador de aplicaciones**, introduzca el FQDN para Endpoint Management.
3. Haga clic en **Listo**.

## Asistente de NetScaler Gateway

Utilice el asistente de NetScaler Gateway para configurar los siguientes ajustes en el dispositivo:

- Servidores virtuales
- Certificados
- Proveedores de servicios de nombres
- Autenticación
- Autorización
- Redirección de puertos
- Acceso sin cliente
- Acceso sin cliente para SharePoint

### Configurar ajustes mediante el asistente de NetScaler Gateway

Después de ejecutar el Asistente de configuración, puede ejecutar el asistente de NetScaler Gateway para configurar otros ajustes en NetScaler Gateway. El asistente de NetScaler Gateway se ejecuta desde la utilidad de configuración.

NetScaler Gateway incluye un certificado de prueba. Si no tiene un certificado firmado de una Autoridad de Certificación (CA), puede usar el certificado de prueba al utilizar el asistente de NetScaler Gateway. Cuando reciba el certificado firmado, puede eliminar el certificado de prueba e instalar el certificado firmado. Citrix recomienda obtener el certificado firmado antes de que NetScaler Gateway esté disponible públicamente para los usuarios.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Nota: Puede crear una Solicitud de Firma de Certificado (CSR) desde el asistente de NetScaler Gateway. Si utiliza el asistente de NetScaler Gateway para crear la CSR, debe salir del asistente y volver a iniciarlo cuando reciba el certificado firmado de la Autoridad de Certificación. Para obtener más información sobre los certificados, consulte Instalación y administración de certificados.

Puede configurar las conexiones de usuario para el Protocolo de Internet versión 6 (IPv6) en el asistente de NetScaler Gateway al configurar un servidor virtual. Para obtener más información sobre el uso de IPv6 para las conexiones de usuario, consulte Configuración de IPv6 para conexiones de usuario.

**Para iniciar el asistente de NetScaler Gateway**

1. En la utilidad de configuración, haga clic en la ficha Configuración y, a continuación, en el panel de navegación, haga clic en NetScaler Gateway.
2. En el panel de detalles, en Primeros pasos, haga clic en el asistente de NetScaler Gateway.
3. Haga clic en Siguiente y, a continuación, siga las instrucciones del asistente.

## Asistente de configuración

Utilice el Asistente de configuración para configurar los siguientes ajustes iniciales en el dispositivo:

- Dirección IP del sistema y máscara de subred
- Dirección IP asignada y máscara de subred
- Nombre de host
- Puerta de enlace predeterminada
- Licencias

Nota: Antes de ejecutar el Asistente de configuración, descargue sus licencias del sitio web de Citrix. Para obtener más información, consulte Licencias de NetScaler Gateway

## Asistente de aplicaciones publicadas

Utilice el asistente de aplicaciones publicadas para configurar NetScaler Gateway para conectarse a servidores que ejecutan Citrix Virtual Apps and Desktops en la red interna. Con el asistente de aplicaciones publicadas, puede:

- Seleccione un servidor virtual para las conexiones a la granja de servidores.
- Configure los ajustes para las conexiones de usuario para StoreFront, el inicio de sesión único y la Secure Ticket Authority.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Cree o seleccione directivas de sesión para SmartAccess.

Dentro del asistente, también puede crear expresiones de directivas de sesión para las conexiones de usuario. Para obtener más información sobre cómo configurar NetScaler Gateway para conectarse a una granja de servidores, consulte Integrar NetScaler Gateway con StoreFront.

### Configuración integrada de Citrix Endpoint Management

Puede implementar NetScaler Gateway con Citrix Endpoint Management MDM, que proporciona la capacidad de escalar, garantizar la alta disponibilidad de las aplicaciones y mantener la seguridad. Para utilizar la configuración de Citrix Endpoint Management, debe instalar la versión 10.1, compilación 120.1316.e.

La configuración integrada de Citrix Endpoint Management crea lo siguiente:

- Servidores de equilibrio de carga para Device Manager.
- Servidores de equilibrio de carga para Microsoft Exchange con filtrado de correo electrónico.
- Servidores de equilibrio de carga para ShareFile.

Para obtener más información sobre cómo crear configuraciones con la configuración integrada de Citrix Endpoint Management, consulte Configuración de los ajustes para su entorno de Citrix Endpoint Management

## Configurar NetScaler Gateway

Después de configurar los ajustes de red base en NetScaler Gateway, debe configurar los ajustes detallados para que los usuarios puedan conectarse a los recursos de red en la red segura. Estos ajustes incluyen:

- Servidores virtuales. Puede configurar varios servidores virtuales en NetScaler Gateway, lo que le permite crear diferentes directivas según el escenario de usuario que deba implementar. Cada servidor virtual tiene su propia dirección IP, certificado y conjunto de directivas. Por ejemplo, puede configurar un servidor virtual y restringir a los usuarios a los recursos de red en la red interna en función de su pertenencia a grupos y las directivas que vincule a los servidores virtuales. Puede crear servidores virtuales mediante los siguientes métodos:
  - Asistente de configuración rápida
  - Asistente de NetScaler Gateway
  - Utilidad de configuración

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Alta disponibilidad. Puede configurar la alta disponibilidad cuando implementa dos dispositivos NetScaler Gateway en su red. Si los dispositivos principales fallan, el dispositivo secundario puede tomar el control sin afectar las sesiones de usuario.
- Certificados. Puede usar certificados para proteger las conexiones de usuario a NetScaler Gateway. Cuando crea una solicitud de firma de certificado (CSR), agrega el nombre de dominio completo al certificado. Puede vincular certificados a servidores virtuales.
- Autenticación. NetScaler Gateway admite varios tipos de autenticación, incluidos LDAP local, RADIUS, SAML, certificados de cliente y TACACS+. Además, puede configurar la autenticación en cascada y de dos factores. Nota: Si utiliza RSA, Safeword o Gemalto Protiva para la autenticación, configure estos tipos mediante RADIUS.
- Conexiones de usuario. Puede configurar las conexiones de usuario mediante perfiles de sesión. Dentro del perfil, puede determinar los complementos con los que los usuarios pueden iniciar sesión, junto con cualquier restricción que los usuarios puedan requerir. Luego, puede crear una directiva con un perfil. Puede vincular directivas de sesión a usuarios, grupos y servidores virtuales.
- Página de inicio. Puede usar la interfaz de acceso predeterminada como página de inicio, o puede crear una página de inicio personalizada. La página de inicio aparece después de que los usuarios inician sesión correctamente en NetScaler Gateway.
- Análisis de puntos finales. Puede configurar directivas en NetScaler Gateway que comprueben el dispositivo del usuario en busca de software, archivos, entradas de registro, procesos y sistemas operativos cuando los usuarios inician sesión. El análisis de puntos finales le permite aumentar la seguridad de su red al requerir que el dispositivo del usuario tenga el software necesario.

## Uso de la utilidad de configuración

La utilidad de configuración le permite configurar la mayoría de los ajustes de NetScaler Gateway. Utiliza un navegador web para acceder a la utilidad de configuración.

### Iniciar sesión en la utilidad de configuración

1. En un navegador web, escriba la dirección IP del sistema de NetScaler Gateway, como `http://192.168.100.1`. Nota: NetScaler Gateway está preconfigurado con una dirección IP predeterminada de 192.168.100.1 y una máscara de subred de 255.255.0.0.
2. En Nombre de usuario y Contraseña, escriba `nsroot.`.
3. En Tipo de implementación, seleccione NetScaler Gateway y, a continuación, haga clic en Iniciar sesión.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Cuando inicie sesión en la utilidad de configuración por primera vez, el Panel de control se abrirá de forma predeterminada en la ficha **Inicio**. En la ficha **Inicio**, puede utilizar el asistente de Configuración rápida para configurar los ajustes de un servidor virtual, la autenticación, los certificados y Citrix Endpoint Management. También puede configurar los ajustes de StoreFront en el asistente de Configuración rápida.

Para obtener más información sobre la configuración de NetScaler Gateway, consulte:

- Configuración de los ajustes iniciales mediante el asistente de configuración.
- Configuración de los ajustes con el asistente de configuración rápida
- Configuración de los ajustes mediante el asistente de NetScaler Gateway.

## Crear servidores virtuales

Un servidor virtual es un punto de acceso al que los usuarios inician sesión. Cada servidor virtual tiene su propia dirección IP, certificado y conjunto de directivas. Un servidor virtual consta de una combinación de dirección IP, puerto y protocolo que acepta el tráfico entrante. Los servidores virtuales contienen la configuración de conexión para cuando los usuarios inician sesión en el dispositivo. Puede configurar los siguientes ajustes en los servidores virtuales:

- Certificados
- Autenticación
- Directivas
- Marcadores
- Grupos de direcciones (también conocidos como grupos de IP o IP de intranet)
- Implementación de DMZ de doble salto con NetScaler Gateway
- Autoridad de tickets seguros
- Transferencia de sesión de proxy ICA® de SmartAccess

Si ejecuta el asistente de NetScaler Gateway, puede crear un servidor virtual durante el asistente. Puede configurar más servidores virtuales de las siguientes maneras:

- **Desde el nodo de servidores virtuales**. Este nodo se encuentra en el panel de navegación de la utilidad de configuración. Puede agregar, modificar y eliminar servidores virtuales mediante la utilidad de configuración.
- **Con el asistente de configuración rápida**. Si implementa Citrix Endpoint Management™ o StoreFront en su entorno, puede usar el asistente de configuración rápida para crear el servidor virtual y todas las directivas necesarias para su implementación.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Si desea que los usuarios inicien sesión y utilicen un tipo de autenticación específico, como RADIUS, puede configurar un servidor virtual y asignarle una dirección IP única. Cuando los usuarios inician sesión, se les dirige al servidor virtual y se les solicitan sus credenciales RADIUS.

También puede configurar las formas en que los usuarios inician sesión en NetScaler Gateway. Puede usar una directiva de sesión para configurar el tipo de software de usuario, el método de acceso y la página de inicio que ven los usuarios después de iniciar sesión.

### Para crear servidores virtuales

Puede agregar, modificar, habilitar o deshabilitar, y eliminar servidores virtuales mediante la GUI de NetScaler Gateway o el asistente de configuración rápida. Para obtener más información sobre cómo configurar un servidor virtual con el asistente de configuración rápida, consulte Configuring Settings with the Quick Configuration Wizard.

**NOTA:**

El servidor virtual VPN admite DTLS versión 1.0, de forma predeterminada. Para habilitar DTLS versión 1.2, consulte Configure DTLS VPN virtual server using SSL VPN virtual server.

#### Para crear un servidor virtual mediante la GUI

1. Vaya a **NetScaler Gateway > Virtual Servers**.
2. En el panel de detalles, haga clic en **Agregar**.
3. Configure los ajustes según sus requisitos.
4. Haga clic en **Crear** y, a continuación, en **Cerrar**.

#### Para crear un servidor virtual mediante la CLI

En el símbolo del sistema, escriba;

```
add vpn vserver <name> <serviceType> [<IPAddress> [<port>]
```

**Ejemplo:**

```
add vpn vserver gatewayserver SSL 1.1.1.1 443
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

### Puntos a tener en cuenta al vincular un perfil de red al servidor virtual VPN

Puede crear perfiles de red (perfiles de red) para configurar el dispositivo para que utilice una dirección IP de origen especificada y vincular el perfil de red al servidor virtual VPN. Sin embargo, tenga en cuenta lo siguiente al vincular un perfil de red al servidor virtual VPN.

- Cuando se vincula un perfil de red a un servidor virtual de NetScaler Gateway, este selecciona una SNIP específica para que el servidor virtual la utilice al enviar tráfico a los servidores back-end.
- En ausencia de la vinculación del perfil de red, si hay varias SNIP, NetScaler Gateway utiliza el método round robin para seleccionar la SNIP que se utilizará.
- El perfil de red no funciona para servicios generados dinámicamente (STA, monitor SF). Para STA y otros servicios generados dinámicamente, puede vincular el perfil de red directamente a esos monitores y esos monitores se utilizan en ese momento. Sin embargo, si tiene varias puertas de enlace en el mismo dispositivo, todas las puertas de enlace utilizan el mismo perfil de red para los monitores configurados.

Para obtener más detalles sobre el perfil de red, consulte Utilizar una IP de origen especificada para la comunicación de back-end.

### Usuarios actuales y usuarios conectados totales en el servidor virtual

**Usuarios actuales:** Número de usuarios conectados a un servidor virtual específico. Se recomienda supervisar los usuarios actuales para el seguimiento de las CCU.

**Usuarios conectados totales:** Número de usuarios que tienen una o más conexiones activas a través del servidor virtual específico. El número total de usuarios conectados se utiliza principalmente en ICA Proxy.

Puede utilizar el contador de usuarios conectados totales en los siguientes escenarios:

- Considere que se establece una conexión ICA, pero no se establece ninguna sesión de autenticación, autorización y auditoría correspondiente. En este escenario, un usuario inicia una aplicación o un escritorio y cierra el navegador, y continúa trabajando en la aplicación o el escritorio iniciados. La sesión de autenticación, autorización y auditoría caduca, pero la conexión sigue activa. El número total de usuarios conectados se puede utilizar para identificar a los usuarios que aún están conectados.
- En el enrutamiento óptimo de HDX™, la puerta de enlace de autenticación y la puerta de enlace ICA pueden estar en diferentes dispositivos. Los usuarios conectados totales en este

© 1997–2026 Citrix Systems, Inc. All rights reserved.

caso se pueden utilizar para identificar el número de usuarios conectados en la puerta de enlace ICA.

**Puntos a tener en cuenta:**

- Los usuarios actuales superan a los usuarios conectados totales cuando hay sesiones activas (aún no caducadas) pero no hay conexiones activas en estas sesiones. Por ejemplo, un usuario inició una aplicación o un escritorio y lo cerró inmediatamente, pero no cerró la sesión de autenticación, autorización y auditoría.
- Los usuarios conectados totales superan a los usuarios actuales si las sesiones de autenticación, autorización y auditoría caducan, pero las conexiones ICA siguen activas.
- En una configuración VPN pura (sin ICA involucrado), el número de usuarios actuales y usuarios conectados totales es igual.

## Configurar tipos de conexión en el servidor virtual

Al crear y configurar un servidor virtual, puede configurar las siguientes opciones de conexión:

- Conexiones con la aplicación Citrix Workspace solo a Citrix Virtual Apps and Desktops sin SmartAccess, análisis de puntos finales o funciones de tunelización de capa de red.
- Conexiones con el cliente Citrix Secure Access™ y SmartAccess, que permiten el uso de SmartAccess, análisis de puntos finales y funciones de tunelización de capa de red.
- Conexiones con Secure Hub que establece una conexión Micro VPN desde dispositivos móviles a NetScaler Gateway.
- Conexiones paralelas realizadas a través del protocolo de sesión ICA por un usuario desde varios dispositivos. Las conexiones se migran a una única sesión para evitar el uso de varias licencias universales.

Si desea que los usuarios inicien sesión sin software de usuario, puede configurar una política de acceso sin cliente y vincularla al servidor virtual.

**Para configurar conexiones Basic o SmartAccess en un servidor virtual**

1. Vaya a **NetScaler Gateway** y, a continuación, haga clic en **Servidores virtuales**.
2. En el panel de detalles, haga clic en **Agregar**.
3. En **Nombre**, escriba un nombre para el servidor virtual.
4. En **Dirección IP** y **Puerto**, escriba la dirección IP y el número de puerto del servidor virtual.
5. Realice una de las siguientes acciones:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Para permitir solo conexiones ICA, haga clic en **Modo básico**.
- Para permitir el inicio de sesión de usuario con Secure Hub, el cliente Citrix Secure Access y SmartAccess, haga clic en **Modo SmartAccess**.
- Para permitir que SmartAccess administre las sesiones de proxy ICA para varias conexiones de usuario, haga clic en **Migración de sesión de proxy ICA**.

6. Configure los demás ajustes del servidor virtual, haga clic en **Crear** y, a continuación, haga clic en **Cerrar**.

### Configurar una política de escucha para servidores virtuales comodín

Puede configurar servidores virtuales de NetScaler Gateway para restringir la capacidad de un servidor virtual de escuchar en una VLAN específica. Puede crear un servidor virtual comodín con una política de escucha que lo restrinja al procesamiento de tráfico en la VLAN especificada.

Los parámetros de configuración son:

| PARÁMETRO | DESCRIPCIÓN |
|---|---|
| Nombre | El nombre del servidor virtual. El nombre es obligatorio y no se puede cambiar después de crear el servidor virtual. El nombre no puede exceder los 127 caracteres y el primer carácter debe ser un número o una letra. También puede usar los siguientes caracteres: arroba (@), guion bajo (_), guion (-), punto (.), dos puntos (:), signo de almohadilla (#) y un espacio. |
| IP | La dirección IP del servidor virtual. Para un servidor virtual comodín vinculado a la VLAN, el valor es siempre *. |
| Tipo | El comportamiento del servicio. Sus opciones son HTTP, SSL, FTP, TCP, SSL_TCP, UDP, SSL_BRIDGE, NNTP, DNS, ANY, SIP-UDP, DNS-TCP y RTSP. |
| Puerto | El puerto en el que el servidor virtual escucha las conexiones de usuario. El número de puerto debe estar entre 0 y 65535. Para el |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| PARÁMETRO | DESCRIPCIÓN |
| --- | --- |
| | servidor virtual comodín vinculado a una VLAN, el valor suele ser *. |
| Prioridad de escucha | La prioridad asignada a la política de escucha. La prioridad se evalúa en orden inverso; cuanto menor sea el número, mayor será la prioridad asignada a la política de escucha. |
| Regla de directiva de escucha | La regla de directiva se utiliza para identificar la VLAN a la que debe escuchar el servidor virtual. La regla es: CLIENT.VLAN.ID.EQ (`<ipaddressat>`) Para `<ipaddressat>`, sustituya el número de ID asignado a la VLAN. |

**Para crear un servidor virtual comodín con una directiva de escucha**

1. En el panel de navegación, expanda **NetScaler Gateway** y, a continuación, haga clic en **Servidores virtuales**.
2. En el panel de detalles, haga clic en **Agregar**.
3. En **Nombre**, escriba un nombre para el servidor virtual.
4. En **Protocolo**, seleccione el protocolo.
5. En **Dirección IP**, escriba la dirección IP del servidor virtual.
6. En **Puerto**, escriba el puerto del servidor virtual.
7. En la ficha **Avanzado**, en Directiva de escucha, en **Prioridad de escucha**, escriba la prioridad de la directiva de escucha.
8. Junto a Regla de directiva de escucha, haga clic en **Configurar**.
9. En el cuadro de diálogo **Crear expresión**, haga clic en **Agregar**, configure la expresión y, a continuación, haga clic en **Aceptar**.
10. Haga clic en **Crear** y, a continuación, en **Cerrar**.

## Configurar direcciones IP en NetScaler Gateway

Puede configurar direcciones IP para iniciar sesión en la utilidad de configuración y para las conexiones de usuario. NetScaler Gateway está configurado con una dirección IP predeterminada de 192.168.100.1 y una máscara de subred de 255.255.0.0 para el acceso de administración. La

© 1997–2026 Citrix Systems, Inc. All rights reserved.

dirección IP predeterminada se utiliza siempre que no hay un valor configurado por el usuario para la dirección IP del sistema (NSIP).

- Dirección NSIP. La dirección IP de administración de NetScaler Gateway que se utiliza para todo el acceso relacionado con la administración al dispositivo. NetScaler Gateway también utiliza la dirección NSIP para la autenticación.
- **Puerta de enlace predeterminada**. El enrutador que reenvía el tráfico desde fuera de la red segura a NetScaler Gateway.
- **Dirección IP de subred (SNIP)**. La dirección IP que representa el dispositivo de usuario al comunicarse con un servidor en una red secundaria.

La dirección SNIP utiliza los puertos 1024 hasta 64000.

### Cómo NetScaler Gateway utiliza las direcciones IP

NetScaler Gateway origina tráfico desde direcciones IP según la función que se esté realizando. La siguiente lista describe varias funciones y la forma en que NetScaler Gateway utiliza las direcciones IP para cada una, como pauta general:

- **Autenticación.** La dirección IP que utiliza NetScaler Gateway depende del tipo de servidor de autenticación.
  - Servidores LDAP/RADIUS/TACACS. Si AAAD se comunica directamente con el servidor virtual de autenticación, entonces se utiliza la dirección NSIP.
  - Si se utiliza un equilibrador de carga como proxy, entonces el equilibrador de carga utiliza la dirección SNIP para la autenticación. AAAD utiliza la dirección NSIP para comunicarse con el equilibrador de carga. La dirección IP que utiliza NetScaler depende de la entidad que se comunica con el servidor virtual de autenticación.
  - Servidores SAML/OAUTH/WEBAUTH: Estos servidores se comunican utilizando la dirección SNIP.
- **Transferencias de archivos desde la página de inicio.** NetScaler Gateway utiliza la dirección SNIP.
- **Consultas DNS y WINS.** NetScaler Gateway utiliza la dirección SNIP.
- **Tráfico de red a recursos en la red segura.** NetScaler Gateway utiliza la dirección SNIP o la agrupación de IP, según la configuración en NetScaler Gateway.
- **Configuración de proxy ICA.** NetScaler Gateway utiliza la dirección SNIP.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

### Direcciones IP de subred

La dirección IP de subred permite al usuario conectarse a NetScaler Gateway desde un host externo que reside en otra subred. Al agregar una dirección IP de subred, se crea una entrada de ruta correspondiente en la tabla de rutas. Solo se realiza una entrada por subred. La entrada de ruta corresponde a la primera dirección IP agregada en la subred.

A diferencia de la dirección IP del sistema y la dirección IP asignada, no es obligatorio especificar la dirección IP de subred durante la configuración inicial de NetScaler Gateway.

La dirección IP asignada y las direcciones IP de subred utilizan los puertos 1024 a 64000.

#### Para agregar una dirección IP de subred

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda **Sistema \ > Red** y, a continuación, haga clic en **IPs**.
2. En el panel de detalles, haga clic en **Agregar**.
3. En el cuadro de diálogo Crear IP, en Dirección IP, escriba la dirección IP.
4. En Máscara de red, escriba la máscara de subred.
5. En Tipo de IP, seleccione IP de subred, haga clic en **Cerrar** y, a continuación, haga clic en **Crear**.

### Configurar IPv6 para conexiones de usuario

Puede configurar NetScaler Gateway para que escuche las conexiones de usuario mediante el Protocolo de Internet versión 6 (IPv6). Al configurar una de las siguientes opciones, puede seleccionar la casilla de verificación IPv6 y, a continuación, introducir la dirección IPv6 en el cuadro de diálogo:

- Configuración global - Aplicaciones publicadas - Proxy ICA®
- Autenticación global - RADIUS
- Autenticación global - LDAP
- Autenticación global - TACACS
- Perfil de sesión - Aplicaciones publicadas - Proxy ICA
- Servidores virtuales de NetScaler Gateway
- Crear servidor de autenticación - RADIUS
- Crear servidor de autenticación - LDAP
- Crear servidor de autenticación - TACACS

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Crear servidor de auditoría
- Configuración de alta disponibilidad
- Enlazar/Desenlazar monitores de ruta para alta disponibilidad
- Servidor virtual (Equilibrio de carga)

Cuando se configura el servidor virtual de NetScaler Gateway para escuchar en una dirección IPv6, los usuarios solo pueden conectarse con la aplicación Citrix Workspace. Las conexiones de usuario con el cliente Citrix Secure Access no son compatibles con IPv6.

Puede utilizar las siguientes directrices para configurar IPv6 en NetScaler Gateway:

- Citrix Virtual Apps y StoreFront. Cuando se configura IPv6 para las conexiones de usuario y si hay una dirección IP asignada que utiliza IPv6, los servidores de Citrix Virtual Apps y StoreFront también pueden utilizar IPv6. StoreFront debe instalarse detrás de NetScaler Gateway. Cuando los usuarios se conectan a través de NetScaler Gateway, la dirección IPv6 se traduce a IPv4. Cuando la conexión regresa, la dirección IPv4 se traduce a IPv6.
- Servidores virtuales. Puede configurar IPv6 para un servidor virtual al ejecutar el asistente de NetScaler Gateway. En el asistente de NetScaler Gateway, en la página Servidores virtuales, haga clic en IPv6 e introduzca la dirección IP. Solo puede configurar una dirección IPv6 para un servidor virtual mediante el asistente de NetScaler Gateway.
- Otro. Para configurar IPv6 para ICA Proxy, autenticación, auditoría y alta disponibilidad, seleccione la casilla de verificación IPv6 en el cuadro de diálogo y, a continuación, escriba la dirección IP.

## Resolver servidores DNS ubicados en la red segura

Si su servidor DNS está ubicado en la red segura detrás de un firewall y el firewall está bloqueando el tráfico ICMP, no podrá probar las conexiones al servidor porque el firewall está bloqueando la solicitud. Puede resolver este problema siguiendo estos pasos:

- Crear un servicio DNS con un monitor DNS personalizado que se resuelva en un nombre de dominio completo (FQDN) conocido.
- Crear un servidor virtual DNS no direccionable directamente en NetScaler Gateway.
- Vincular el servicio al servidor virtual.

Nota:

- Configure un servidor virtual DNS y un servicio DNS solo si su servidor DNS está ubicado detrás de un firewall.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Si instala una licencia de equilibrio de carga de NetScaler en el dispositivo, el nodo Servidores virtuales y servicios no aparece en el panel de navegación. Puede realizar este procedimiento expandiendo Equilibrio de carga y, a continuación, haciendo clic en Servidores virtuales.

### Para configurar un servicio DNS y un monitor DNS

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda Servidores virtuales y servicios y, a continuación, haga clic en Servidores virtuales.
2. En el panel de detalles, haga clic en Agregar.
3. En Nombre, escriba un nombre para el servicio.
4. En Protocolo, seleccione DNS.
5. En Dirección IP, escriba la dirección IP del servidor DNS.
6. En Puerto, escriba el número de puerto.
7. En la pestaña Servicios, haga clic en Agregar.
8. En la pestaña Monitores, en Disponible, seleccione DNS, haga clic en Agregar, haga clic en Crear y, a continuación, haga clic en Cerrar.
9. En el cuadro de diálogo Crear servidor virtual (equilibrio de carga), haga clic en Crear y, a continuación, haga clic en Cerrar.

A continuación, cree el servidor virtual DNS mediante el procedimiento Para configurar un servidor virtual DNS y, a continuación, vincule el servicio DNS al servidor virtual.

### Para vincular un servicio DNS a un servidor virtual DNS

1. En el cuadro de diálogo Configurar servicio virtual (equilibrio de carga), en la pestaña Servicios, haga clic en Agregar, seleccione el servicio DNS, haga clic en Crear y, a continuación, haga clic en Cerrar.

## Configurar servidores virtuales DNS

Para configurar un servidor virtual DNS, debe especificar un nombre y una dirección IP. Al igual que el servidor virtual de NetScaler Gateway, debe asignar una dirección IP al servidor virtual DNS. Sin embargo, esta dirección IP debe estar en el lado interno de la red de destino para que los dispositivos de usuario resuelvan todas las direcciones internas. Además, especifique el puerto DNS.

**Nota**: Si instala una licencia de equilibrio de carga de NetScaler en el dispositivo, el nodo Servidores y servicios virtuales no aparece en el panel de navegación. Puede configurar esta

© 1997–2026 Citrix Systems, Inc. All rights reserved.

función mediante el servidor virtual de equilibrio de carga. Para obtener más información, consulte la documentación de NetScaler en la documentación del producto NetScaler.

### Para configurar un servidor virtual DNS

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda Servidores y servicios virtuales y, a continuación, haga clic en Servidores virtuales.
2. En el panel de detalles, haga clic en Agregar.
3. En Nombre, escriba un nombre para el servidor virtual.
4. En Dirección IP, escriba la dirección IP del servidor DNS.
5. En Puerto, escriba el puerto en el que escucha el servidor DNS.
6. En Protocolo, seleccione DNS y, a continuación, haga clic en Crear.

Finalmente, asocie el servidor virtual DNS con NetScaler Gateway mediante uno de los dos métodos siguientes, según las necesidades de su implementación:

- Enlace el servidor globalmente a NetScaler Gateway.
- Enlace el servidor virtual DNS por cada servidor virtual.

Si implementa el servidor virtual DNS globalmente, todos los usuarios tienen acceso a él. Luego, puede restringir a los usuarios vinculando el servidor virtual DNS al servidor virtual.

## Configurar proveedores de servicios de nombres

NetScaler Gateway utiliza proveedores de servicios de nombres para convertir direcciones web en direcciones IP.

Al ejecutar el asistente de NetScaler Gateway, puede configurar un servidor DNS o un servidor WINS. También puede usar la utilidad de configuración para configurar otros servidores DNS o WINS.

### Para agregar un servidor DNS a NetScaler Gateway

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda NetScaler Gateway y, a continuación, haga clic en Configuración global.
2. En el panel de detalles, en Configuración, haga clic en Cambiar configuración global.
3. En la ficha Configuración de red, haga clic en Agregar.
4. En el cuadro de diálogo Insertar servidor de nombres, en Dirección IP, escriba la dirección IP del servidor DNS, haga clic en Crear y, a continuación, haga clic en Cerrar.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. Haga clic en Aceptar en la utilidad de configuración.

### Para agregar un servidor WINS a NetScaler Gateway

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda NetScaler Gateway y, a continuación, haga clic en Configuración global.
2. En el panel de detalles, en Configuración, haga clic en Cambiar configuración global.
3. En la ficha Configuración de red, en IP del servidor WINS, escriba la dirección IP del servidor WINS y, a continuación, haga clic en Aceptar.

A continuación, especifique el nombre y la dirección IP del servidor virtual DNS. Al igual que el servidor virtual de NetScaler Gateway, se debe asignar una dirección IP al servidor virtual. Sin embargo, esta dirección IP debe estar en el lado interno de la red de destino para que los dispositivos de usuario resuelvan todas las direcciones internas correctamente. También debe especificar el puerto DNS.

Si configura un servidor DNS y un servidor WINS para la resolución de nombres, puede usar el asistente de NetScaler Gateway para seleccionar qué servidor realiza la búsqueda de nombres primero.

### Para especificar la prioridad de búsqueda de nombres

1. En la utilidad de configuración, haga clic en la ficha Configuración y, a continuación, en el panel de navegación, haga clic en NetScaler Gateway.
2. En el panel de detalles, en Introducción, haga clic en el asistente de NetScaler Gateway.
3. Haga clic en Siguiente para aceptar la configuración actual hasta que llegue a la página Proveedores de servicios de nombres.
4. En Prioridad de búsqueda de nombres, seleccione WINS o DNS y, a continuación, continúe hasta el final del asistente.

## Configurar conexiones iniciadas por el servidor

Para cada usuario que inicia sesión en NetScaler Gateway con las direcciones IP habilitadas, el sufijo DNS se añade al nombre de usuario y se agrega un registro de dirección DNS a la caché DNS del dispositivo. Esta técnica ayuda a proporcionar a los usuarios un nombre DNS en lugar de las direcciones IP de los usuarios.

Cuando se asigna una dirección IP a la sesión de un usuario, es posible conectarse al dispositivo del usuario desde la red interna. Por ejemplo, los usuarios que se conectan con Escritorio remoto o un cliente de computación de red virtual (VNC) pueden acceder al dispositivo del usuario para

© 1997–2026 Citrix Systems, Inc. All rights reserved.

diagnosticar una aplicación problemática. También es posible que dos usuarios de NetScaler Gateway con direcciones IP de red interna que han iniciado sesión de forma remota se comuniquen entre sí a través de NetScaler Gateway. Permitir el descubrimiento de las direcciones IP de red interna de los usuarios conectados en el dispositivo ayuda a esta comunicación.

Un usuario remoto puede usar el siguiente comando ping para descubrir la dirección IP de red interna de un usuario que puede haber iniciado sesión en NetScaler Gateway:

```
ping \<username.domainname\>
```

Un servidor puede iniciar una conexión a un dispositivo de usuario de las siguientes maneras:

- Conexiones TCP o UDP. Las conexiones pueden originarse desde un sistema externo en la red interna o desde otro equipo conectado a NetScaler Gateway. La dirección IP de red interna que se asigna a cada dispositivo de usuario conectado a NetScaler Gateway se utiliza para estas conexiones. Se describen los diferentes tipos de conexiones iniciadas por el servidor que admite NetScaler Gateway. Para las conexiones iniciadas por el servidor TCP o UDP, el servidor tiene conocimiento previo de la dirección IP y el puerto del dispositivo de usuario y establece una conexión con él. NetScaler Gateway intercepta esta conexión.

  Luego, el dispositivo de usuario establece una conexión inicial con el servidor y el servidor se conecta al dispositivo de usuario en un puerto conocido o derivado del primer puerto configurado.

  En este escenario, el dispositivo de usuario establece una conexión inicial con el servidor y luego intercambia puertos y direcciones IP con el servidor mediante un protocolo específico de la aplicación donde esta información está incrustada. Esto permite que NetScaler Gateway admita aplicaciones, como las conexiones FTP activas.
- Comando de puerto. Esto se utiliza en un FTP activo y en ciertos protocolos de Voz sobre IP.
- Conexiones entre plug-ins. NetScaler Gateway admite conexiones entre plug-ins mediante el uso de las direcciones IP de la red interna.

  Con este tipo de conexión, dos dispositivos de usuario de NetScaler Gateway que utilizan el mismo NetScaler Gateway pueden iniciar conexiones entre sí. Un ejemplo de este tipo es el uso de aplicaciones de mensajería instantánea, como Office Communicator o Yahoo\! Messenger.

Si un usuario cierra sesión en NetScaler Gateway y la solicitud de cierre de sesión no llegó al dispositivo, el usuario puede iniciar sesión de nuevo utilizando cualquier dispositivo y reemplazar

© 1997–2026 Citrix Systems, Inc. All rights reserved.

la sesión anterior por una nueva sesión. Esta característica puede ser beneficiosa en implementaciones donde se asigna una dirección IP por usuario.

Cuando un usuario inicia sesión en NetScaler Gateway por primera vez, se crea una sesión y se le asigna una dirección IP. Si el usuario cierra sesión pero la solicitud de cierre de sesión se pierde o el dispositivo del usuario no realiza un cierre de sesión limpio, la sesión se mantiene en el sistema. Si el usuario intenta iniciar sesión de nuevo desde el mismo dispositivo u otro dispositivo, después de una autenticación correcta, aparece un cuadro de diálogo de transferencia de inicio de sesión. Si el usuario elige transferir el inicio de sesión, la sesión anterior en NetScaler Gateway se cierra y se crea una nueva sesión. La transferencia de inicio de sesión está activa solo durante dos minutos después del cierre de sesión, y si se intenta iniciar sesión desde varios dispositivos simultáneamente, el último intento de inicio de sesión reemplaza la sesión original.

### Configurar el rango de puertos privados para conexiones iniciadas por el servidor

A partir de la versión 23.10.1.7 del cliente de Citrix Secure Access, puede configurar un puerto privado en el rango de 49152 a 64535 para conexiones iniciadas por el servidor (SIC). La configuración de puertos privados evita conflictos que podrían surgir al usar puertos para crear sockets entre el cliente de Citrix Secure Access y aplicaciones de terceros en las máquinas cliente. Esto solo es aplicable si el controlador WFP está en uso.

Puede configurar los puertos privados mediante el registro VPN de Windows `SicBeginPort`. Alternativamente, puede configurar el rango de puertos privados mediante un archivo JSON de personalización del complemento VPN en NetScaler.

Si un servidor inicia una conexión, el cliente de Citrix Secure Access utiliza los primeros 1000 puertos, a partir del registro VPN de Windows `SicBeginPort`, para crear los sockets. Si el registro está configurado en una máquina cliente, la configuración del registro tiene prioridad sobre la configuración JSON de NetScaler.

A continuación, se muestra un ejemplo de la configuración JSON del complemento VPN en NetScaler:

```
root@ADC# cat /var/netscaler/gui/vpn/pluginCustomization.json



{"SicBeginPort" : 51000}
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Para obtener detalles sobre la configuración del registro, consulte Claves del registro del cliente VPN de Windows de NetScaler Gateway.

**NOTA:**

El rango de puertos predeterminado que se utiliza para crear sockets es 62500–63500.

## Configurar el enrutamiento en NetScaler Gateway

Para proporcionar acceso a los recursos de red internos, NetScaler Gateway enruta los datos a sus redes internas y seguras. De forma predeterminada, NetScaler Gateway utiliza una ruta estática.

Las redes a las que NetScaler Gateway puede enrutar datos se determinan por la forma en que configure la tabla de enrutamiento de NetScaler Gateway y la puerta de enlace predeterminada que especifique para NetScaler Gateway.

La tabla de enrutamiento de NetScaler Gateway debe contener las rutas necesarias para enrutar datos a cualquier recurso de red interno al que un usuario pueda necesitar acceder.

NetScaler Gateway admite los siguientes protocolos de enrutamiento:

- Protocolo de información de enrutamiento (RIP v1 y v2)
- Abrir la ruta más corta primero (OSPF)
- Protocolo de puerta de enlace de borde (BGF)

### Configurar una ruta estática

Al configurar la comunicación con otro host o red, debe configurar una ruta estática desde NetScaler Gateway al nuevo destino si no utiliza el enrutamiento dinámico.

#### Para configurar una ruta estática

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda **Sistema \> Red \> Avanzado** y, a continuación, haga clic en **Rutas**.
2. En el panel de detalles, en la ficha Básico, haga clic en **Agregar**.
3. Configure los ajustes de la ruta y, a continuación, haga clic en **Crear**.

#### Para probar una ruta estática

1. En la utilidad de configuración, en el panel de navegación, expanda **Sistema** y, a continuación, haga clic en **Diagnósticos**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. En el panel de detalles, en Utilidades, haga clic en **Ping**.
3. En Parámetros, en Nombre de host, escriba el nombre del dispositivo.
4. En Avanzado, en Dirección IP de origen, escriba la dirección IP del dispositivo y, a continuación, haga clic en **Ejecutar**.

   Si se comunica correctamente con el otro dispositivo, los mensajes indican que se transmitió y recibió el mismo número de paquetes y se perdieron cero paquetes.

   Si no se comunica con el otro dispositivo, los mensajes de estado indican que se recibieron cero paquetes y se perdieron todos los paquetes. Para corregir esta falta de comunicación, repita el procedimiento para agregar una ruta estática.

Para detener la prueba, en el cuadro de diálogo **Ping**, haga clic en **Detener** y, a continuación, haga clic en **Cerrar**.

## Configurar la negociación automática

De forma predeterminada, el dispositivo está configurado para usar la negociación automática, en la que NetScaler Gateway transmite el tráfico de red en ambas direcciones simultáneamente y determina la velocidad adecuada del adaptador. Si deja la configuración predeterminada en Negociación automática, NetScaler Gateway utiliza el funcionamiento dúplex completo, en el que el adaptador de red es capaz de enviar datos en ambas direcciones simultáneamente.

Si deshabilita la negociación automática, NetScaler Gateway utiliza el funcionamiento semidúplex, en el que el adaptador puede enviar datos en ambas direcciones entre dos nodos, pero el adaptador solo puede usar una dirección u otra a la vez.

Para la primera instalación, Citrix recomienda configurar NetScaler Gateway para que utilice la negociación automática para los puertos conectados al dispositivo. Después de iniciar sesión inicialmente y configurar NetScaler Gateway, puede deshabilitar la negociación automática. No puede configurar la negociación automática globalmente. Debe habilitar o deshabilitar la configuración para cada interfaz.

### Para habilitar o deshabilitar la negociación automática

1. En la utilidad de configuración, en la pestaña Configuración, en el panel de navegación, expanda **System \ > Network,** y, a continuación, haga clic en **Interfaces**.
2. En el panel de detalles, seleccione la interfaz y, a continuación, haga clic en **Abrir**.
3. Realice una de las siguientes acciones en el cuadro de diálogo **Configurar interfaz**:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Para habilitar la negociación automática, haga clic en **Sí** junto a Negociación automática y, a continuación, haga clic en **Aceptar**.
- Para deshabilitar la negociación automática, haga clic en **No** junto a Negociación automática y, a continuación, haga clic en **Aceptar**.

# Configurar el nombre de host y el FQDN en NetScaler Gateway

El nombre de host es el nombre del dispositivo NetScaler Gateway que está asociado con el archivo de licencia. El nombre de host es único para el dispositivo y se utiliza al descargar la licencia Universal. Se define el nombre de host al ejecutar el Asistente de configuración para configurar NetScaler Gateway por primera vez.

El nombre de dominio completo (FQDN) se incluye en el certificado firmado que está vinculado a un servidor virtual. No se configura el FQDN en NetScaler Gateway. Un dispositivo puede tener un FQDN único asignado a cada servidor virtual configurado en NetScaler Gateway mediante certificados.

Puede encontrar el FQDN de un certificado viendo los detalles del certificado. El FQDN se encuentra en el campo de asunto del certificado.

## Para ver el FQDN de un certificado

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda **SSL** y, a continuación, haga clic en **Certificados**.
2. En el panel de detalles, seleccione un certificado, haga clic en **Acción** y, a continuación, haga clic en **Detalles**.
3. En el cuadro de diálogo Detalles del certificado, haga clic en **Asunto**. El FQDN del certificado aparece en la lista.

# Políticas y perfiles en NetScaler Gateway

Las políticas y los perfiles en NetScaler Gateway le permiten administrar e implementar la configuración en escenarios o condiciones específicos. Una política individual establece o define la configuración que entra en vigor cuando se cumple un conjunto de condiciones especificado. Cada política tiene un nombre único y puede tener un perfil vinculado a ella.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

## Cómo funcionan las políticas

Una política consta de una condición booleana y una colección de configuraciones llamada perfil. La condición se evalúa en tiempo de ejecución para determinar si la política debe aplicarse.

Un perfil es una colección de configuraciones que utilizan parámetros específicos. El perfil puede tener cualquier nombre y puede reutilizarlo en más de una política. Puede configurar varias opciones dentro del perfil, pero solo puede incluir un perfil por política.

Puede vincular políticas, con las condiciones y perfiles configurados, a servidores virtuales, grupos, usuarios o globalmente. Las políticas se denominan según el tipo de configuración que controlan. Por ejemplo, en una política de sesión, puede controlar cómo inician sesión los usuarios y el tiempo que pueden permanecer conectados.

Si utiliza NetScaler Gateway con Citrix Virtual Apps, los nombres de las políticas de NetScaler Gateway se envían a Citrix Virtual Apps como filtros. Al configurar NetScaler Gateway para que sea compatible con Citrix Virtual Apps y SmartAccess, configure los siguientes ajustes en Citrix Virtual Apps:

- El nombre del servidor virtual configurado en el dispositivo. El nombre se envía a Citrix Virtual Apps como el nombre de la granja de NetScaler Gateway.
- Los nombres de las políticas de preautenticación o de sesión se envían como nombres de filtro.

Para obtener más información sobre cómo configurar NetScaler Gateway para que sea compatible con Citrix Endpoint Management, consulte Configuración de los ajustes para su entorno de Citrix Endpoint Management.

Para obtener más información sobre cómo configurar NetScaler Gateway para que sea compatible con Citrix Virtual Apps and Desktops, consulte Integrar NetScaler Gateway con Citrix Virtual Apps and Desktops y Integración con Citrix Endpoint Management o StoreFront.

Para obtener más información sobre las políticas de preautenticación, consulte Configuración de políticas de punto final.

### Políticas condicionales

Al configurar políticas, puede utilizar cualquier expresión booleana para expresar la condición de cuándo se aplica la política. Al configurar políticas condicionales, puede utilizar cualquiera de las expresiones de sistema disponibles, como las siguientes:

- Cadenas de seguridad del cliente

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Información de red
- Encabezados y cookies HTTP
- Hora del día
- Valores del certificado de cliente

También puede crear políticas para aplicar solo cuando el dispositivo del usuario cumpla criterios específicos, como una política de sesión para SmartAccess.

Otro ejemplo de configuración de una política condicional es variar la política de autenticación para los usuarios. Por ejemplo, puede exigir que los usuarios que se conectan con el cliente Citrix Secure Access™ desde fuera de la red interna, como desde su equipo doméstico o mediante Micro VPN desde un dispositivo móvil, se autentiquen mediante LDAP y que los usuarios que se conectan a través de la WAN se autentiquen mediante RADIUS.

Nota: No puede usar condiciones de política basadas en los resultados del análisis de puntos finales si la regla de política está configurada como parte de la configuración de seguridad en un perfil de sesión.

### Prioridades de las políticas

Las políticas se priorizan y evalúan en el orden en que se vincula la política.

Los dos métodos siguientes determinan la prioridad de la política:

- El nivel al que está vinculada la política: globalmente, servidor virtual, grupo o usuario. Los niveles de política se clasifican de mayor a menor de la siguiente manera:
  - Usuario (prioridad más alta)
  - Grupo
  - Servidor virtual
  - Global (prioridad más baja)
- La prioridad numérica tiene precedencia independientemente del nivel al que esté vinculada la directiva. Si una directiva vinculada globalmente tiene un número de prioridad de uno y otra directiva vinculada a un usuario tiene un número de prioridad de dos, la directiva global tiene precedencia. Un número de prioridad más bajo otorga a la directiva una precedencia mayor.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

### Crear directivas en NetScaler Gateway

Puede usar la utilidad de configuración para crear directivas. Después de crear una directiva, la vincula al nivel adecuado: usuario, grupo, servidor virtual o global. Cuando vincula una directiva a uno de estos niveles, los usuarios reciben la configuración dentro del perfil si se cumplen las condiciones de la directiva. Cada directiva y perfil tiene un nombre único.

Si tiene Citrix Endpoint Management o StoreFront como parte de su implementación, puede usar el asistente de configuración rápida para configurar los ajustes de esta implementación. Para obtener más información sobre el asistente, consulte Configurar el dispositivo NetScaler Gateway mediante asistentes.

## Configuración de expresiones del sistema

Una expresión del sistema especifica las condiciones bajo las cuales se aplica la directiva. Por ejemplo, las expresiones en una directiva de preautenticación se aplican mientras un usuario inicia sesión. Las expresiones en una directiva de sesión se evalúan y aplican después de que el usuario se autentica e inicia sesión en NetScaler Gateway.

Las expresiones en NetScaler Gateway incluyen:

- Expresiones generales que limitan los objetos que los usuarios pueden usar al establecer una conexión con NetScaler Gateway. Por ejemplo, consulte:
  - Directivas de sesión
- Expresiones de seguridad del cliente que definen el software, los archivos, los procesos o los valores del registro que deben instalarse y ejecutarse en el dispositivo del usuario. Por ejemplo, consulte:
  - Directivas de punto final
- Expresiones basadas en la red que restringen el acceso en función de la configuración de red. Por ejemplo, consulte:
  - Directivas de tráfico
  - Directivas de autorización

NetScaler Gateway también se puede utilizar como un dispositivo NetScaler. Algunas expresiones en el dispositivo son más aplicables a NetScaler. Las expresiones generales y basadas en la red se usan comúnmente con NetScaler y no se usan generalmente con NetScaler Gateway. Las

© 1997–2026 Citrix Systems, Inc. All rights reserved.

expresiones de seguridad del cliente se utilizan en NetScaler Gateway para determinar que los elementos correctos están instalados en el dispositivo del usuario.

### Configuración de expresiones de seguridad del cliente

Las expresiones son un componente de una directiva. Una expresión representa una única condición que se evalúa frente a una solicitud o una respuesta. Puede crear una cadena de seguridad de expresión simple para comprobar condiciones como:

- Sistema operativo del dispositivo de usuario, incluidos los Service Packs
- Versión del software antivirus y definiciones de virus
- Archivos
- Procesos
- Valores del Registro
- Certificados de usuario

## Administración de certificados en NetScaler Gateway

En NetScaler Gateway, se utilizan certificados para crear conexiones seguras y autenticar usuarios.

Para establecer una conexión segura, se requiere un certificado de servidor en un extremo de la conexión. En el otro extremo de la conexión, se requiere un certificado raíz de la entidad de certificación (CA) que emitió el certificado del servidor.

- Certificado de servidor. Un certificado de servidor certifica la identidad del servidor. NetScaler Gateway requiere este tipo de certificado digital.
- Certificado raíz. Un certificado raíz identifica la CA que firmó el certificado del servidor. El certificado raíz pertenece a la entidad de certificación. Un dispositivo de usuario requiere este tipo de certificado digital para verificar el certificado del servidor.

Al establecer una conexión segura con un explorador web en el dispositivo del usuario, el servidor envía su certificado al dispositivo.

Cuando el dispositivo de usuario recibe un certificado de servidor, el explorador web, como Internet Explorer, comprueba qué CA emitió el certificado y si el dispositivo de usuario confía en la CA. Si la CA no es de confianza o si es un certificado de prueba, el explorador web solicita al

© 1997–2026 Citrix Systems, Inc. All rights reserved.

usuario que acepte o rechace el certificado (aceptando o rechazando, de hecho, la capacidad de acceder al sitio).

NetScaler Gateway admite los tres tipos de certificados siguientes:

- Un certificado de prueba que está vinculado a un servidor virtual y también se puede utilizar para conexiones a una granja de servidores. NetScaler Gateway viene con un certificado de prueba preinstalado.
- Un certificado en formato PEM o DER firmado por una CA y emparejado con una clave privada.
- Un certificado en formato PKCS#12 que se utiliza para almacenar o transportar el certificado y la clave privada. El certificado PKCS#12 se exporta normalmente desde un certificado de Windows existente como un archivo PFX y, a continuación, se instala en NetScaler Gateway.

Citrix® recomienda utilizar un certificado firmado por una CA de confianza, como Thawte o Verisign.

## Crear una solicitud de firma de certificado

Para proporcionar comunicaciones seguras mediante SSL o TLS, se requiere un certificado de servidor en NetScaler Gateway. Antes de poder cargar un certificado en NetScaler Gateway, debe generar una solicitud de firma de certificado (CSR) y una clave privada. Utilice la opción Crear solicitud de certificado incluida en el asistente de NetScaler Gateway o la utilidad de configuración para crear la CSR. La opción Crear solicitud de certificado crea un archivo .csr que se envía por correo electrónico a la Autoridad de certificación (CA) para su firma y una clave privada que permanece en el dispositivo. La CA firma el certificado y se lo devuelve a la dirección de correo electrónico que proporcionó. Cuando reciba el certificado firmado, puede instalarlo en NetScaler Gateway. Cuando reciba el certificado de la CA, empareje el certificado con la clave privada.

**IMPORTANTE:**

Cuando utilice el asistente de NetScaler Gateway para crear la CSR, debe salir del asistente y esperar a que la CA le envíe el certificado firmado. Cuando reciba el certificado, puede ejecutar el asistente de NetScaler Gateway de nuevo para crear la configuración e instalar el certificado. Para obtener más información sobre el asistente de NetScaler Gateway, consulte Configuración de ajustes mediante el asistente de NetScaler Gateway.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

### Crear una CSR mediante el asistente de NetScaler Gateway

1. En la utilidad de configuración, haga clic en la ficha Configuración y, a continuación, en el panel de navegación, haga clic en **NetScaler Gateway**.
2. En el panel de detalles, en Introducción, haga clic en el asistente de **NetScaler Gateway**.
3. Siga las instrucciones del asistente hasta llegar a la página Especificar un certificado de servidor.
4. Haga clic en **Crear una solicitud de firma de certificado** y complete los campos. Nota: El nombre de dominio completo (FQDN) no tiene por qué ser el mismo que el nombre de host de NetScaler Gateway. El FQDN se utiliza para el inicio de sesión del usuario.
5. Haga clic en **Crear** para guardar el certificado en su equipo y, a continuación, haga clic en **Cerrar**.
6. Salga del asistente de NetScaler Gateway sin guardar la configuración.

### Crear una CSRÂ mediante la GUI de NetScaler

También puede usar la GUI de NetScaler para crear una CSR, sin ejecutar el asistente de NetScaler Gateway.

1. Vaya a **Administración de tráfico** > **SSL > Archivos SSL** y seleccioneÂ **Crear solicitud de firma de certificado (CSR)**.
2. Complete la configuración del certificado y, a continuación, haga clic en **Crear**.

Después de crear el certificado y la clave privada, envíe el certificado por correo electrónico a la CA, como Thawte o Verisign.

Para obtener un procedimiento detallado, consulte Crear una solicitud de firma de certificado.

### Instalar el certificado firmado en NetScaler Gateway

Cuando reciba el certificado firmado de la Autoridad de certificación (CA), emparéjelo con la clave privada del dispositivo y, a continuación, instale el certificado en NetScaler Gateway.

#### Emparejar el certificado firmado con una clave privada mediante la GUI

1. Copie el certificado en NetScaler Gateway en la carpeta nsconfig/ssl mediante un programa Secure Shell (SSH) como WinSCP.
2. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda **SSL > Certificados**.
3. En la página **Certificado SSL**, haga clic en **Introducción**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. En el panel de detalles, haga clic en **Instalar**.
5. En **Nombre del par de claves de certificado**, escriba el nombre del certificado.
6. En **Nombre de archivo de certificado**, haga clic en **Dispositivo**.
7. Vaya al certificado, haga clic en **Seleccionar** y, a continuación, haga clic en **Abrir**.
8. En **Nombre de archivo de clave**, haga clic en **Dispositivo**. El nombre de la clave privada es el mismo que el de la solicitud de firma de certificado (CSR). La clave privada se encuentra en NetScaler Gateway en el directorio \\nsconfig\\ssl.
9. Elija la clave privada y, a continuación, haga clic en **Abrir**.
10. Si el certificado tiene formato PEM, en **Contraseña**, escriba la contraseña de la clave privada.
11. Si desea configurar una notificación para cuando el certificado caduque, seleccione **Notificar al caducar**.
12. En **Período de notificación**, escriba el número de días, haga clic en **Crear** y, a continuación, haga clic en **Cerrar**.

#### Vincular el certificado y la clave privada a un servidor virtual mediante la GUI

Después de crear y vincular un par de certificado y clave privada, vincúlelo a un servidor virtual.

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda **NetScaler Gateway > Servidores virtuales**.
2. En el panel de detalles, haga clic en un servidor virtual y, a continuación, haga clic en **Abrir**.
3. En la ficha Certificados, en **Disponible**, seleccione un certificado, haga clic en **Agregar** y, a continuación, haga clic en **Aceptar**.

#### Vincular el certificado y la clave privada a un servidor virtual mediante la CLI

En el símbolo del sistema, escriba;

```
bind ssl vserver <vServerName> -certkeyName <string> -ocspCheck
( Mandatory | Optional )
```

**Ejemplo:**

```
bind ssl vserver TestClient -CertkeyName ag51.xm.nsi.test.com -CA
-ocspCheck Mandatory
```

**Nota:** oscpCheck es opcional si no se requiere la comprobación OCSP para el certificado del dispositivo.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

### Desvincular certificados de prueba del servidor virtual mediante la GUI

Después de instalar el certificado firmado, desvincule los certificados de prueba que estén vinculados al servidor virtual. Puede desvincular los certificados de prueba mediante la utilidad de configuración.

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda **NetScaler Gateway > Servidores virtuales**.
2. En el panel de detalles, haga clic en un servidor virtual y, a continuación, haga clic en **Abrir**.
3. En la pestaña Certificados, en **Configurado**, seleccione el certificado de prueba y, a continuación, haga clic en **Quitar**.

## Configurar certificados intermedios

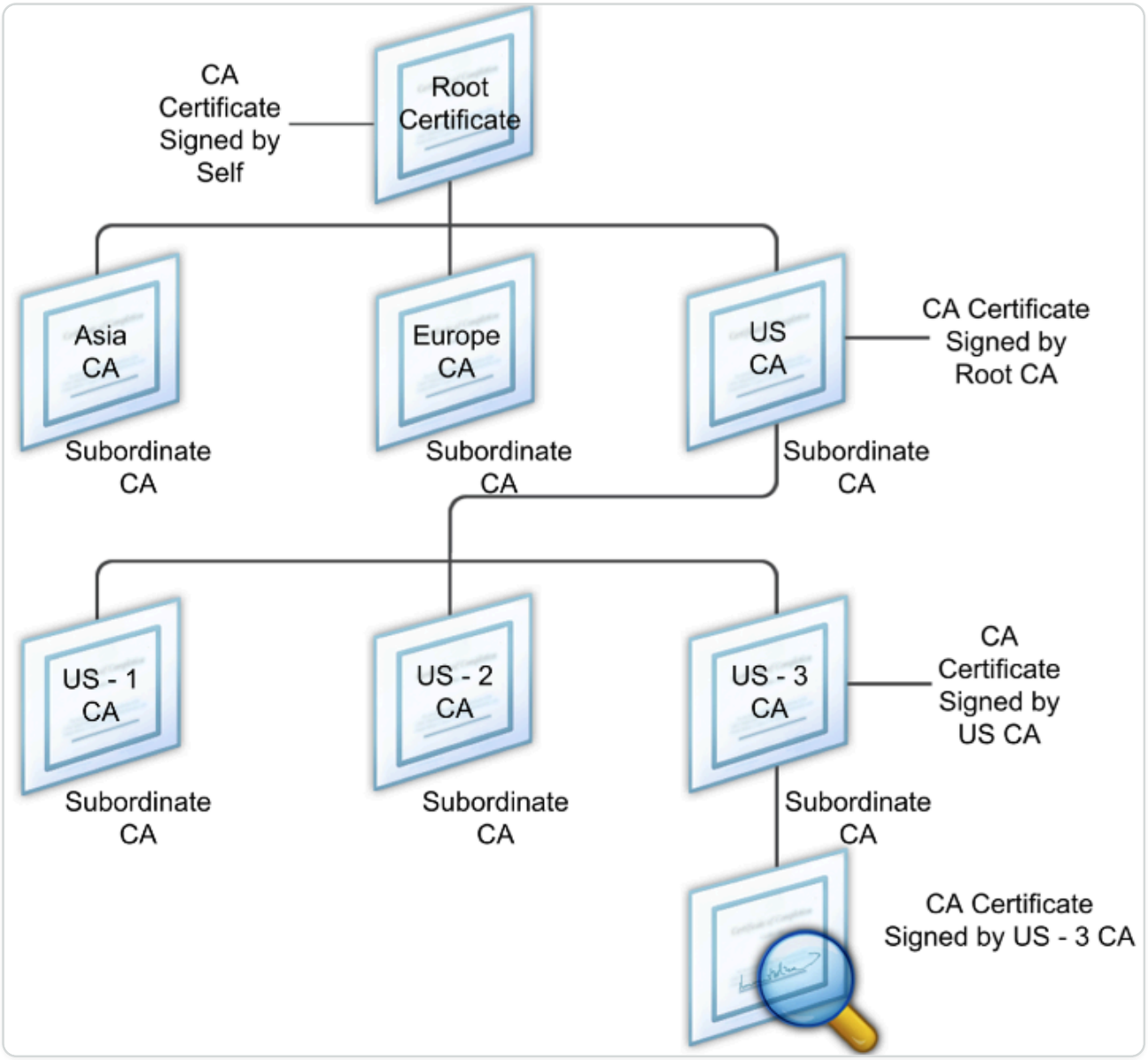
Un certificado intermedio es un certificado que se encuentra entre NetScaler Gateway (el certificado del servidor) y un certificado raíz (instalado en el dispositivo del usuario). Un certificado intermedio forma parte de una cadena.

Algunas organizaciones delegan la responsabilidad de emitir certificados para resolver el problema de la separación geográfica entre las unidades de la organización, o para aplicar diferentes políticas de emisión a diferentes secciones de la organización.

La responsabilidad de emitir certificados se puede delegar mediante la configuración de autoridades de certificación (CA) subordinadas. Las CA pueden firmar sus propios certificados (es decir, son autofirmados) o pueden ser firmados por otra autoridad de certificación. El estándar X.509 incluye un modelo para establecer una jerarquía de CA. En este modelo, como se muestra en la siguiente figura, la CA raíz se encuentra en la parte superior de la jerarquía y es un certificado autofirmado por la autoridad de certificación. Las CA que están directamente subordinadas a la CA raíz tienen certificados de CA firmados por la autoridad de certificación raíz. Las CA que se encuentran bajo las CA subordinadas en la jerarquía tienen sus certificados de CA firmados por las CA subordinadas.

Figura 1. El modelo X.509 que muestra la estructura jerárquica de una cadena de certificados digitales típica

© 1997–2026 Citrix Systems, Inc. All rights reserved.




Si un certificado de servidor está firmado por una CA con un certificado autofirmado, la cadena de certificados se compone de exactamente dos certificados: el certificado de entidad final y la autoridad de certificación raíz. Si un certificado de usuario o de servidor está firmado por una autoridad de certificación intermedia, la cadena de certificados es más larga.

La siguiente figura muestra que los dos primeros elementos son el certificado de entidad final (en este caso, gwy01.company.com) y el certificado de la autoridad de certificación intermedia, en ese orden. El certificado de la autoridad de certificación intermedia va seguido del certificado de su autoridad de certificación. Esta lista continúa hasta que el último certificado de la lista es para una autoridad de certificación raíz. Cada certificado de la cadena da fe de la identidad del certificado anterior.

Figura 2. Una cadena de certificados digitales típica

© 1997–2026 Citrix Systems, Inc. All rights reserved.




### Instalar un certificado intermedio

1. En la utilidad de configuración, en la ficha Configuration, en el panel de navegación, expanda SSL y, a continuación, haga clic en Certificates.
2. En el panel de detalles, haga clic en Install.
3. En Certificate-Key Pair Name, escriba el nombre del certificado.
4. En Details, en Certificate File Name, haga clic en Browse (Appliance) y, en la lista, seleccione Local o Appliance.
5. Vaya al certificado en su equipo (Local) o en NetScaler Gateway (Dispositivo).
6. En Formato de certificado, seleccione PEM.
7. Haga clic en Instalar y, a continuación, en Cerrar.

Al instalar un certificado intermedio en NetScaler Gateway, no es necesario especificar la clave privada ni una contraseña.

Una vez instalado el certificado en el dispositivo, debe vincularse al certificado de servidor.

### Vincular un certificado intermedio a un certificado de servidor

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda SSL y, a continuación, haga clic en Certificados.
2. En el panel de detalles, seleccione el certificado de servidor y, a continuación, en Acción, haga clic en Vincular.
3. Junto a Nombre del certificado de CA, seleccione el certificado intermedio de la lista y, a continuación, haga clic en Aceptar.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

## Usar certificados de dispositivo para la autenticación

NetScaler Gateway admite la comprobación de certificados de dispositivo que le permite vincular la identidad del dispositivo a la clave privada de un certificado. La comprobación de certificados de dispositivo se puede configurar como parte de las directivas de análisis de puntos finales (EPA) clásicas o avanzadas. En las directivas EPA clásicas, el certificado de dispositivo solo se puede configurar para EPA de preautenticación.

NetScaler Gateway verifica el certificado del dispositivo antes de que se ejecute el análisis de puntos finales o antes de que aparezca la página de inicio de sesión. Si configura el análisis de puntos finales, el análisis de puntos finales se ejecuta para verificar el dispositivo del usuario. Cuando el dispositivo supera el análisis y después de que NetScaler Gateway verifica el certificado del dispositivo, los usuarios pueden iniciar sesión en NetScaler Gateway.

**IMPORTANTE:**

- De forma predeterminada, Windows exige privilegios de administrador para acceder a los certificados de dispositivo.
- Para agregar una comprobación de certificado de dispositivo para usuarios que no son administradores, debe instalar el complemento VPN. La versión del complemento VPN debe ser la misma que la del complemento EPA en el dispositivo.
- Puede agregar varios certificados de CA a la puerta de enlace y validar el certificado del dispositivo.
- Si instala dos o más certificados de dispositivo en NetScaler Gateway, los usuarios deben seleccionar el certificado correcto cuando inicien sesión en NetScaler Gateway o antes de que se ejecute el análisis de puntos finales.
- Cuando cree el certificado de dispositivo, debe ser un certificado X.509.
- Si tiene un certificado de dispositivo emitido por una CA intermedia, entonces deben vincularse los certificados de CA intermedios y raíz.
- El cliente EPA necesita que el usuario tenga derechos de administrador local para poder acceder al almacén de certificados de la máquina. Esto rara vez ocurre, por lo que una solución alternativa es instalar el complemento completo de NetScaler® Gateway, que puede acceder al almacén local.

Para obtener más información sobre cómo crear certificados de dispositivo, consulte lo siguiente:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- "¿Qué es el Servicio de inscripción de dispositivos de red para los Servicios de certificados de Active Directory?" en la página de Microsoft Learn Challenge.
- Cómo solicitar un certificado a una entidad de certificación de Microsoft mediante DCE/RPC y la carga útil del perfil de certificado de Active Directory en el sitio web de soporte de Apple.
- Emisión de certificados para iPad/iPhone en el blog de soporte de Microsoft Ask the Directory Services Team.
- Configuración del servicio de inscripción de dispositivos de red en el sitio web de Windows IT Pro.
- Implementación de ejemplo paso a paso de los certificados PKI para Configuration Manager: Autoridad de certificación de Windows Server 2008 en el sitio web de Microsoft System Center.

### Pasos para configurar certificados de dispositivo

Para configurar un certificado de dispositivo, debe completar los siguientes pasos:

- Instale el certificado de la autoridad de certificación del emisor del certificado de dispositivo en NetScaler Gateway. Para obtener más información, consulte Instalación del certificado firmado en NetScaler Gateway.
- Enlace el certificado de la autoridad de certificación del emisor del certificado de dispositivo al servidor virtual de NetScaler Gateway y habilite la comprobación OCSP. Para obtener más información, consulte Instalación del certificado firmado en NetScaler Gateway.
- Cree y enlace OCSP (respondedor) en el certificado de la autoridad de certificación del emisor del certificado de dispositivo. Para obtener más información, consulte Supervisar el estado del certificado con OCSP.

Habilite la comprobación del certificado de dispositivo en el servidor virtual y agregue el certificado de la autoridad de certificación del emisor del certificado de dispositivo a la lista de comprobación de certificados de dispositivo. Para obtener más información, consulte Habilitar la comprobación del certificado de dispositivo en un servidor virtual para la política EPA clásica.

Complete la configuración y verificación del certificado de dispositivo del lado del cliente en la máquina Windows. Para obtener más información, consulte Verificación del certificado de dispositivo en una máquina Windows.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**NOTA:**

Todos los clientes que deseen utilizar la comprobación EPA del certificado de dispositivo deben tener el certificado de dispositivo instalado en el almacén de certificados del sistema de la máquina.

### Habilitar la comprobación del certificado de dispositivo en un servidor virtual para la política EPA clásica

Después de crear el certificado de dispositivo, instale el certificado en NetScaler Gateway mediante el procedimiento para Importar e instalar un certificado existente en NetScaler Gateway.

1. En la ficha Configuración, vaya a **NetScaler Gateway > Servidores virtuales**.
2. En la página **Servidores virtuales de NetScaler Gateway**, seleccione un servidor virtual existente y haga clic en **Editar**.
3. En la página **Servidores virtuales VPN**, en la sección **Configuración básica**, haga clic en **Editar**.
4. Desactive la casilla **Habilitar autenticación** para deshabilitar la autenticación.
5. Seleccione la casilla **Habilitar certificado de dispositivo** para habilitar el certificado de dispositivo
6. Haga clic en **Agregar** para añadir el nombre del certificado de CA de un emisor de certificado de dispositivo disponible a la lista.
7. Para vincular un certificado de CA al servidor virtual, haga clic en **Certificado de CA** en la sección **CA para certificado de dispositivo**, haga clic en **Agregar**, seleccione el certificado y, a continuación, haga clic en **+**.

**NOTA:**

Para obtener información sobre cómo habilitar y vincular certificados de dispositivo en un servidor virtual para una política EPA avanzada, consulte Certificado de dispositivo en nFactor como componente EPA.

### Verificación del certificado de dispositivo en una máquina Windows

1. Abra un explorador y acceda al FQDN de NetScaler Gateway.
2. Permita que se ejecute el cliente de Citrix® End Point Analysis (EPA). Si aún no está instalado, instale EPA.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix EPA se ejecuta y valida el certificado de dispositivo y redirige a la página de autenticación si la comprobación EPA del certificado de dispositivo se supera; de lo contrario, le redirige a la página de error de EPA. En caso de que tenga otras comprobaciones EPA, los resultados del análisis EPA dependerán de las comprobaciones EPA configuradas.

Para depurar más a fondo en el cliente, examine los siguientes registros EPA en el cliente: C:\Users\<User name>\AppData\Local\Citrix\AGEE\nsepa.txt

**Nota:**

No se admite la verificación del certificado de dispositivo con CRL.

## Importar e instalar un certificado existente

Puede importar un certificado existente desde un equipo basado en Windows que ejecute Internet Information Services (IIS) o desde un equipo que ejecute Secure Gateway.

Al exportar el certificado, asegúrese de exportar también la clave privada. A veces, no se puede exportar la clave privada, lo que significa que no se puede instalar el certificado en NetScaler Gateway. Si esto ocurre, utilice la Solicitud de firma de certificado (CSR) para crear un certificado. Para obtener más información, consulte Creación de una solicitud de firma de certificado.

Al exportar un certificado y una clave privada desde Windows, el equipo crea un archivo de intercambio de información personal (.pfx). Este archivo se instala después en NetScaler Gateway como un certificado PKCS#12.

Si va a reemplazar Secure Gateway por NetScaler Gateway, puede exportar el certificado y la clave privada de Secure Gateway. Si está realizando una migración in situ de Secure Gateway a NetScaler Gateway, el nombre de dominio completo (FQDN) de la aplicación y del dispositivo debe ser el mismo. Al exportar el certificado de Secure Gateway, retira inmediatamente Secure Gateway, instala el certificado en NetScaler Gateway y, a continuación, prueba la configuración. Secure Gateway y NetScaler Gateway no pueden ejecutarse en su red al mismo tiempo si tienen el mismo FQDN.

Si utiliza Windows Server 2003 o Windows Server 2008, puede usar la Consola de administración de Microsoft para exportar el certificado. Para obtener más información, consulte la Ayuda en línea de Windows.

Deje los valores predeterminados para todas las demás opciones, defina una contraseña y guarde el archivo .pfx en su equipo. Cuando se exporta el certificado, lo instala en NetScaler Gateway.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

### Para instalar el certificado y la clave privada en NetScaler Gateway

1. En la utilidad de configuración, haga clic en la ficha Configuración y, a continuación, en el panel de navegación, haga clic en **NetScaler Gateway**.
2. En el panel de detalles, en Introducción, haga clic en **Asistente de NetScaler Gateway**.
3. Haga clic en **Siguiente**, seleccione un servidor virtual existente y, a continuación, haga clic en **Siguiente**.
4. En **Opciones de certificado**, seleccione **Instalar un archivo PKCS#12 (.pfx)**.
5. En **Nombre de archivo PKCS#12**, haga clic en **Examinar**, navegue hasta el certificado y, a continuación, haga clic en **Seleccionar**.
6. En ((Contraseña)), escriba la contraseña de la clave privada.

   Esta es la contraseña que utilizó al convertir el certificado a formato PEM.
7. Haga clic en **Siguiente** para finalizar el asistente de NetScaler Gateway sin cambiar ninguna otra configuración.

Cuando el certificado se instala en NetScaler Gateway, el certificado aparece en la utilidad de configuración en el nodo **SSL \ > Certificados**.

#### Para crear una clave privada

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, haga clic en **SSL**.
2. En el panel de detalles, en **Claves SSL**, haga clic en **Crear clave RSA**.
3. En **Nombre de archivo de clave**, escriba el nombre de la clave privada o haga clic en Examinar para buscar un archivo existente.
4. En **Tamaño de clave (bits)**, escriba el tamaño de la clave privada.
5. En **Valor de exponente público**, seleccione F4 o 3.

   El valor del exponente público para la clave RSA. Esto forma parte del algoritmo de cifrado y es necesario para crear la clave RSA. Los valores son F4 (Hex: 0x10001) o 3 (Hex: 0x3). El valor predeterminado es F4.
6. En **Formato de clave**, seleccione PEM o DER. Citrix® recomienda el formato PEM para el certificado.
7. En **Algoritmo de codificación PEM**, seleccione DES o DES3.
8. En **Frase de contraseña PEM** y **verificar Passphrase**, escriba la contraseña, haga clic en **Crear** y, a continuación, haga clic en **Cerrar**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**Nota**: Para asignar una frase de contraseña, el formato de clave debe ser PEM y debe seleccionar el algoritmo de codificación.

Para crear una clave privada DSA en la utilidad de configuración, haga clic en **Crear clave DSA** y siga los pasos realizados para crear la clave privada RSA.

## Convertir un certificado del formato PFX al formato PEM

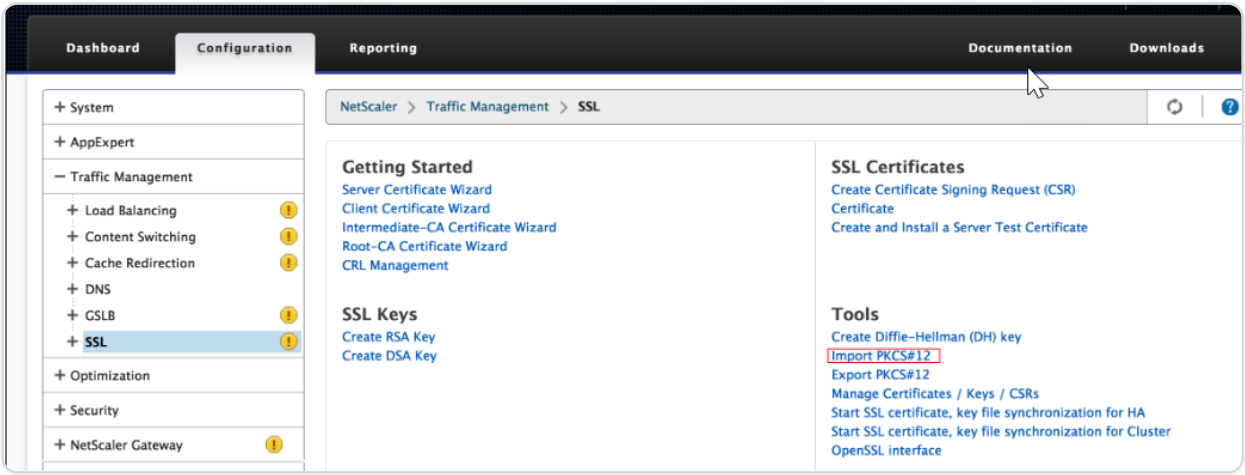
Los certificados SSL se utilizan para servidores virtuales de equilibrio de carga SSL y servidores virtuales de NetScaler Gateway. Los certificados PEM son archivos ASCII codificados en Base64. Los certificados PEM se pueden abrir en el Editor de texto/Bloc de notas y verá que contienen las declaraciones "-----BEGIN CERTIFICATE-----" y "-----END CERTIFICATE-----".

Para un acceso seguro y de confianza, debe instalar un certificado de servidor SSL en el servidor de NetScaler Gateway. El archivo de certificado cargado debe tener las siguientes características:

- Una Autoridad de Certificación (CA) en la que confíen los usuarios finales debe emitir el certificado del servidor. Para obtener los mejores resultados, utilice una CA comercial como Verisign, Thawte o GeoTrust.
- El certificado debe estar en formato Privacy Enhanced Mail (PEM), un formato basado en texto que es una codificación Base64 del formato binario Distinguished Encoding Rules (DER).
- El archivo de certificado debe incluir una clave privada y la clave privada no debe estar cifrada. No debe ser necesaria ninguna contraseña para usar el archivo PEM.
- Cualquier certificado intermedio necesario debe adjuntarse al final del archivo PEM.

Complete el siguiente procedimiento para convertir un certificado PFX a formato PEM mediante el Asistente de NetScaler Gateway:

1. Vaya a **Administración del tráfico**, seleccione el nodo **SSL**.
2. Haga clic en el enlace **Importar PKCS#12**.




© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. Especifique el nombre de archivo que desee para el certificado PEM en el campo **Nombre de archivo de salida**.
4. Haga clic en **Examinar** y seleccione el certificado PFX que desea convertir a formato PEM. Algunos usuarios prefieren cargar el certificado en el directorio /ncsonfig/SSL y usarlo desde allí. Si el certificado PFX está almacenado en NetScaler Gateway, elija la opción **Dispositivo**, y si está almacenado en su estación de trabajo, use Local.

   ](/en-us/netscaler-gateway/media/2-convert-pfx-certificate-to-pem-format-citrix.png)
5. Especifique la contraseña de importación.
6. Si el archivo está codificado, seleccione DES o 3DES como formato de codificación:
7. Haga clic en **Aceptar**.
8. Especifique la frase de contraseña PEM y la frase de contraseña PEM de verificar.
9. Haga clic en el vínculo **Administrar certificados/claves/CSR** para ver los archivos de certificado PEM convertidos.
10. Puede ver el archivo PFX cargado con el archivo PEM convertido.

    Archivos PFX disponibles(/en-us/netscaler-gateway/media/6-convert-pfx-certificate-to-pem-format-citrix.png)
11. Expanda el nodo **SSL**.
12. Seleccione el nodo Certificados.
13. Haga clic en **Instalar**.
14. Especifique un nombre de par de claves de certificado en el asistente **Instalar certificado**.
15. Busque el archivo PEM para el nombre del archivo de certificado y el nombre del archivo de clave privada.
16. Especifique la contraseña.
17. Haga clic en **Instalar**.

### `OpenSSL utility`

Si ha solicitado e instalado un certificado en un servidor Windows mediante el asistente de certificados de Internet Information Service (IIS), puede exportar ese certificado con su clave privada a un archivo Personal Information Exchange (PFX). Para importar este certificado en NetScaler Gateway, debe convertir el archivo PFX a formato PEM sin cifrar.

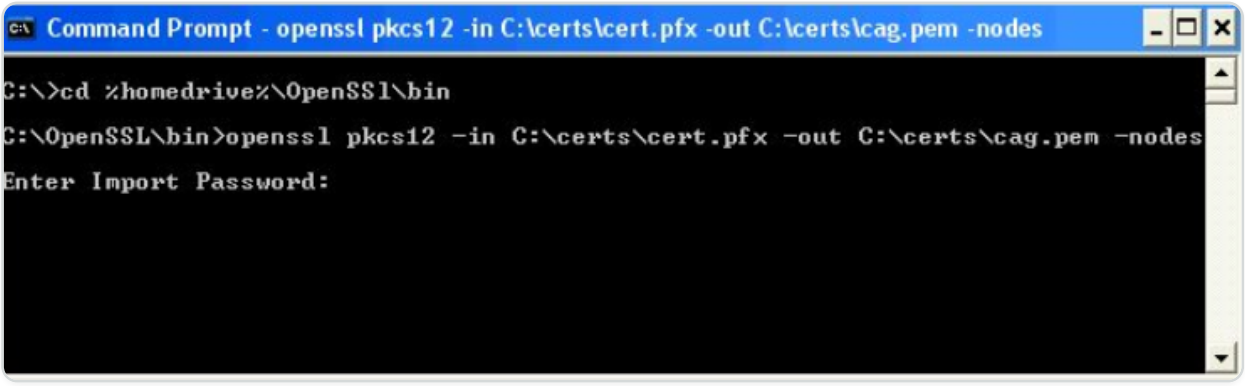
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Puede usar la utilidad de código abierto `OpenSSL` para realizar la conversión de PFX a PEM. Descargue una distribución Win32 de `OpenSSL` desde Win32 `OpenSSL`.

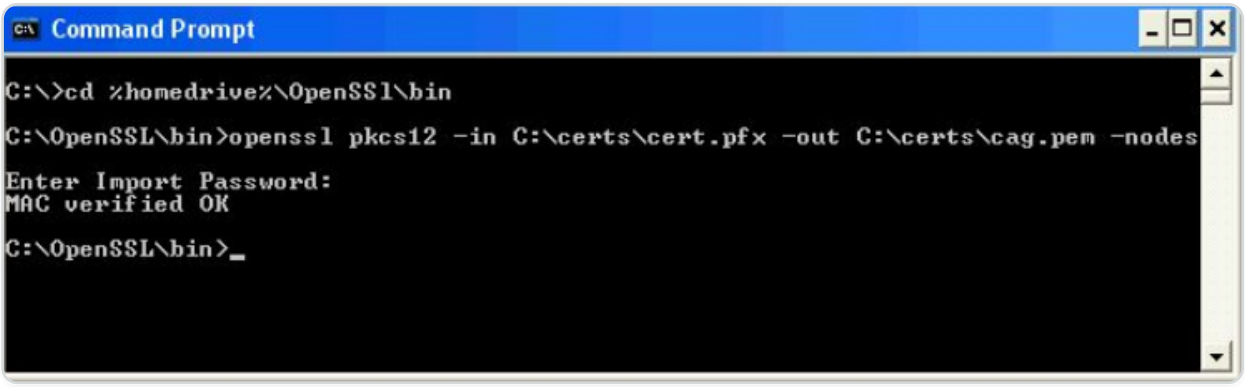
También podría necesitar archivos redistribuibles de C++ si desea usar `OpenSSL`. Descárguelos del Paquete redistribuible de Microsoft Visual C++ 2008 (x86).

Para convertir un archivo PFX a un archivo PEM, complete los siguientes pasos en una máquina Windows:

1. Descargue e instale el paquete Win32 `OpenSSL` desde Win32 `OpenSSL`.
2. Cree una carpeta c:\certs y copie el archivo yourcert.pfx en la carpeta c:\certs.
3. Abra el símbolo del sistema y cambie al directorio `OpenSSL`\bin: `cd %homedrive%\OpenSSL\bin`
4. Ejecute el siguiente comando para convertir el archivo PFX en un archivo PEM sin cifrar (todo en una línea): `OpenSSL` pkcs12 -in c:\certs\yourcert.pfx -out c:\certs\cag.pem –nodes




5. Cuando se le solicite la contraseña de importación, introduzca la contraseña que utilizó al exportar el certificado a un archivo PFX. Debe recibir un mensaje que diga MAC verified OK.




6. Dirija un navegador al portal de administración de NetScaler Gateway o al puerto HTTPS 9001: `https://netscaler-gateway-server:9001`.
7. Inicie sesión como root. La contraseña predeterminada es `rootadmin`.
8. Haga clic en el enlace **Maintenance** en la parte superior de la página.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

9. Haga clic en el botón **Browse** junto al campo **Upload Private Key+Certificate (.pem)**. Busque el archivo c:\certs\cag.pem y haga clic en **Upload**.
10. Reinicie NetScaler Gateway para que se aplique el nuevo certificado SSL.

## Listas de revocación de certificados

De vez en cuando, las Autoridades de Certificación (CA) emiten listas de revocación de certificados (CRL). Las CRL contienen información sobre certificados en los que ya no se puede confiar. Por ejemplo, supongamos que Ann deja XYZ Corporation. La empresa puede colocar el certificado de Ann en una CRL para evitar que firme mensajes con esa clave.

Del mismo modo, puede revocar un certificado si una clave privada se ve comprometida o si ese certificado ha caducado y se está utilizando uno nuevo. Antes de confiar en una clave pública, asegúrese de que el certificado no aparece en una CRL.

NetScaler Gateway admite los dos tipos de CRL siguientes:

- CRL que enumeran los certificados revocados o que ya no son válidos
- Protocolo de estado de certificados en línea (OSCP), un protocolo de Internet utilizado para obtener el estado de revocación de los certificados X.509

**Para añadir una CRL:**

Antes de configurar la CRL en el dispositivo NetScaler Gateway, asegúrese de que el archivo CRL esté almacenado localmente en el dispositivo. En el caso de una configuración de alta disponibilidad, el archivo CRL debe estar presente en ambos dispositivos NetScaler Gateway, y la ruta del directorio al archivo debe ser la misma en ambos dispositivos.

Si necesita actualizar la CRL, puede utilizar los siguientes parámetros:

- Nombre de CRL: El nombre de la CRL que se añade en NetScaler. Máximo 31 caracteres.
- Archivo CRL: El nombre del archivo CRL que se añade en NetScaler. NetScaler busca el archivo CRL en el directorio /var/netscaler/ssl de forma predeterminada. Máximo 63 caracteres.
- URL: Máximo 127 caracteres
- DN base: Máximo 127 caracteres
- DN de enlace: Máximo 127 caracteres
- Contraseña: Máximo 31 caracteres
- Días: Máximo 31

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. En la utilidad de configuración, en la ficha Configuración, expanda SSL y, a continuación, haga clic en CRL.
2. En el panel de detalles, haga clic en Agregar.
3. En el cuadro de diálogo Agregar CRL, especifique los valores para lo siguiente:
    - Nombre de CRL
    - Archivo CRL
    - Formato (opcional)
    - Certificado de CA (opcional)
4. Haga clic en **Crear** y, a continuación, haga clic en **Cerrar**. En el panel de detalles de CRL, seleccione la CRL que configuró y verificar que la configuración que aparece en la parte inferior de la pantalla es correcta.

**Para configurar la actualización automática de CRL mediante LDAP o HTTP en la GUI:**

Una CRL es generada y publicada por una CA periódicamente o, a veces, inmediatamente después de que se revoque un certificado en particular. Citrix recomienda que actualice las CRL en el dispositivo NetScaler Gateway regularmente para protegerse contra clientes que intentan conectarse con certificados no válidos.

El dispositivo NetScaler Gateway puede actualizar las CRL desde una ubicación web o un directorio LDAP. Cuando se especifican los parámetros de actualización y una ubicación web o un servidor LDAP, la CRL no tiene que estar presente en la unidad de disco duro local en el momento de ejecutar el comando. La primera actualización almacena una copia en la unidad de disco duro local, en la ruta especificada por el parámetro Archivo CRL. La ruta predeterminada para almacenar la CRL es /var/netscaler/ssl.

### Parámetros de actualización de CRL

#### Nombre de CRL

> El nombre de la CRL que se está actualizando en NetScaler Gateway.

#### Habilitar actualización automática de CRL

> Habilite o deshabilite la actualización automática de CRL.

#### Certificado de CA

© 1997–2026 Citrix Systems, Inc. All rights reserved.

El certificado de la CA que ha emitido la CRL. Este certificado de CA debe estar instalado en el dispositivo. El NetScaler solo puede actualizar las CRL de las CA cuyos certificados estén instalados en él.

### Método

Protocolo en el que se obtiene la actualización de la CRL de un servidor web (HTTP) o un servidor LDAP. Valores posibles: HTTP, LDAP. Predeterminado: HTTP.

### Ámbito

El alcance de la operación de búsqueda en el servidor LDAP. Si el ámbito especificado es

Base, la búsqueda se realiza al mismo nivel que el DN base. Si el ámbito especificado es

Uno, la búsqueda se extiende a un nivel por debajo del DN base.

### IP del servidor

La dirección IP del servidor LDAP desde el que se recupera la CRL. Seleccione IPv6 para usar una dirección IP IPv6.

### Puerto

El número de puerto en el que se comunica el servidor LDAP o HTTP.

### URL

La URL de la ubicación web desde la que se recupera la CRL.

### DN base

El DN base utilizado por el servidor LDAP para buscar el atributo CRL.

Nota: Citrix® recomienda utilizar el atributo DN base en lugar del Nombre

© 1997–2026 Citrix Systems, Inc. All rights reserved.

del emisor (Issuer-Name) del certificado de CA para buscar la CRL en el servidor LDAP. Es posible que el campo Nombre del emisor (Issuer-Name) no coincida exactamente con el DN de la estructura del directorio LDAP.

### DN de enlace

El atributo DN de enlace se utiliza para acceder al objeto CRL en el repositorio LDAP. Los atributos DN de enlace son las credenciales de administrador para el servidor LDAP. Configure este parámetro para restringir el acceso no autorizado a los servidores LDAP.

### Contraseña

La contraseña de administrador utilizada para acceder al objeto CRL en el repositorio LDAP. La contraseña es necesaria si el acceso al repositorio LDAP está restringido, es decir, si no se permite el acceso anónimo.

### Intervalo

El intervalo en el que se debe realizar la actualización de la CRL. Para una actualización instantánea de la CRL, especifique el intervalo como AHORA (NOW). Valores posibles: MENSUAL (MONTHLY), DIARIO (DAILY), SEMANAL (WEEKLY), AHORA (NOW), NINGUNO (NONE).

### Días

El día en que se debe realizar la actualización de la CRL. La opción no está disponible si el intervalo se establece en DIARIO (DAILY).

### Hora

La hora exacta en formato de 24 horas en que se debe realizar la actualización de la CRL.

### Binario

Establezca el modo de recuperación de CRL basado en LDAP en binario. Valores posibles: SÍ (YES), NO (NO). Predeterminado: NO (NO).

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. En el panel de navegación, expanda SSL y, a continuación, haga clic en CRL.
2. Seleccione la CRL configurada para la que desea actualizar los parámetros de actualización y, a continuación, haga clic en Abrir.
3. Seleccione la opción Habilitar actualización automática de CRL.
4. En el grupo Parámetros de actualización automática de CRL, especifique los valores para los siguientes parámetros: Nota: Un asterisco (*) indica un parámetro obligatorio.
    - Método
    - Binario
    - Ámbito
    - IP del servidor
    - Puerto*
    - URL
    - DN base*
    - DN de enlace
    - Contraseña
    - Intervalo
    - Días
    - Hora
5. Haga clic en Crear. En el panel CRL, seleccione la CRL que configuró y verificar que la configuración que aparece en la parte inferior de la pantalla es correcta.

### Supervisar el estado del certificado con OCSP

El Protocolo de estado de certificado en línea (OCSP) es un protocolo de Internet que se utiliza para determinar el estado de un certificado SSL de cliente. NetScaler Gateway admite OCSP tal como se define en RFC 2560. OCSP ofrece ventajas significativas sobre las listas de revocación de certificados (CRL) en términos de información oportuna. El estado de revocación actualizado de un certificado de cliente es especialmente útil en transacciones que implican grandes sumas de dinero y operaciones bursátiles de alto valor. También utiliza menos recursos del sistema y de la red. La implementación de OCSP en NetScaler Gateway incluye el procesamiento por lotes de solicitudes y el almacenamiento en caché de respuestas.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

### Implementación de OCSP en NetScaler Gateway

La validación OCSP en un dispositivo NetScaler Gateway comienza cuando NetScaler Gateway recibe un certificado de cliente durante un protocolo de enlace SSL. Para validar el certificado, NetScaler Gateway crea una solicitud OCSP y la reenvía al respondedor OCSP. Para ello, NetScaler Gateway extrae la URL del respondedor OCSP del certificado de cliente o utiliza una URL configurada localmente. La transacción permanece en estado suspendido hasta que NetScaler Gateway evalúa la respuesta del servidor y determina si permite la transacción o la rechaza. Si la respuesta del servidor se retrasa más allá del tiempo configurado y no hay otros respondedores configurados, NetScaler Gateway permite la transacción o muestra un error, dependiendo de si se configura la comprobación OCSP como opcional u obligatoria. NetScaler Gateway admite el procesamiento por lotes de solicitudes OCSP y el almacenamiento en caché de respuestas OCSP para reducir la carga en el respondedor OCSP y proporcionar respuestas más rápidas.

### Procesamiento por lotes de solicitudes OCSP

Cada vez que NetScaler Gateway recibe un certificado de cliente, envía una solicitud al respondedor OCSP. Para ayudar a evitar la sobrecarga del respondedor OCSP, NetScaler Gateway puede consultar el estado de más de un certificado de cliente en la misma solicitud. Para que el procesamiento por lotes de solicitudes funcione de manera eficiente, debe definir un tiempo de espera para que el procesamiento de un solo certificado no se retrase mientras se espera para formar un lote.

### Almacenamiento en caché de respuestas OCSP

El almacenamiento en caché de las respuestas recibidas del respondedor OCSP permite respuestas más rápidas al usuario y reduce la carga en el respondedor OCSP. Al recibir el estado de revocación de un certificado de cliente del respondedor OCSP, NetScaler Gateway almacena la respuesta localmente durante un período de tiempo predefinido. Cuando se recibe un certificado de cliente durante un protocolo de enlace SSL, NetScaler Gateway primero comprueba su caché local en busca de una entrada para este certificado. Si se encuentra una entrada que sigue siendo válida (dentro del límite de tiempo de espera de la caché), la entrada se evalúa y el certificado de cliente se acepta o se rechaza. Si no se encuentra un certificado, NetScaler Gateway envía una solicitud al respondedor OCSP y almacena la respuesta en su caché local durante un período de tiempo configurado.

## Configurar el estado del certificado OCSP

La configuración de un Protocolo de estado de certificado en línea (OCSP) implica agregar un respondedor OCSP, vincular el respondedor OCSP a un certificado firmado de una Autoridad de certificación (CA) y vincular el certificado y la clave privada a un servidor virtual Secure Sockets

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Layer (SSL). Si necesita vincular un certificado y una clave privada diferentes a un respondedor OCSP que ya configuró, primero debe desvincular el respondedor y luego vincularlo a un certificado diferente.

**Para configurar OCSP**

1. En la ficha Configuración, en el panel de navegación, expanda SSL y, a continuación, haga clic en Respondedor OCSP.
2. En el panel de detalles, haga clic en Agregar.
3. En Nombre, escriba un nombre para el perfil.
4. En URL, escriba la dirección web del respondedor OCSP.

   Este campo es obligatorio. La dirección web no puede exceder los 32 caracteres.
5. Para almacenar en caché las respuestas OCSP, haga clic en Caché y en Tiempo de espera, escriba el número de minutos que NetScaler Gateway retiene la respuesta.
6. En Agrupación de solicitudes, haga clic en Habilitar.
7. En Retraso de agrupación, especifique el tiempo, en milisegundos, permitido para agrupar un conjunto de solicitudes OCSP.

   Los valores pueden ser de 0 a 10000. El valor predeterminado es 1.
8. En Desviación de tiempo de producción, escriba la cantidad de tiempo que NetScaler Gateway puede usar cuando el dispositivo debe comprobar o aceptar la respuesta.
9. En Verificación de respuesta, seleccione Confiar en respuestas si desea deshabilitar las comprobaciones de firma por parte del respondedor OCSP.

   Si habilita Confiar en respuestas, omita el Paso 8 y el Paso 9.
10. En Certificado, seleccione el certificado que se utiliza para firmar las respuestas OCSP.

    Si no se selecciona un certificado, la CA a la que está vinculado el respondedor OCSP se utiliza para verificar las respuestas.
11. En Tiempo de espera de solicitud, escriba el número de milisegundos que se deben esperar para una respuesta OCSP.

    Este tiempo incluye el tiempo de Retraso de agrupación. Los valores pueden ser de 0 a 120000. El valor predeterminado es 2000.
12. En Certificado de firma, seleccione el certificado y la clave privada utilizados para firmar las solicitudes OCSP. Si no especifica un certificado y una clave privada, las solicitudes no se firman.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

13. Para habilitar el número utilizado una vez `(nonce) extension`, seleccione Nonce.
14. Para usar un certificado de cliente, haga clic en Inserción de certificado de cliente.
15. Haga clic en Crear y, a continuación, haga clic en Cerrar.

# Administración de certificados en NetScaler Gateway

En NetScaler Gateway, se utilizan certificados para crear conexiones seguras y autenticar usuarios.

Para establecer una conexión segura, se requiere un certificado de servidor en un extremo de la conexión. En el otro extremo de la conexión, se requiere un certificado raíz de la entidad de certificación (CA) que emitió el certificado del servidor.

- Certificado de servidor. Un certificado de servidor certifica la identidad del servidor. NetScaler Gateway requiere este tipo de certificado digital.
- Certificado raíz. Un certificado raíz identifica la CA que firmó el certificado del servidor. El certificado raíz pertenece a la entidad de certificación. Un dispositivo de usuario requiere este tipo de certificado digital para verificar el certificado del servidor.

Al establecer una conexión segura con un explorador web en el dispositivo del usuario, el servidor envía su certificado al dispositivo.

Cuando el dispositivo de usuario recibe un certificado de servidor, el explorador web, como Internet Explorer, comprueba qué CA emitió el certificado y si el dispositivo de usuario confía en la CA. Si la CA no es de confianza o si es un certificado de prueba, el explorador web solicita al usuario que acepte o rechace el certificado (aceptando o rechazando, de hecho, la capacidad de acceder al sitio).

NetScaler Gateway admite los tres tipos de certificados siguientes:

- Un certificado de prueba que está vinculado a un servidor virtual y también se puede utilizar para conexiones a una granja de servidores. NetScaler Gateway viene con un certificado de prueba preinstalado.
- Un certificado en formato PEM o DER firmado por una CA y emparejado con una clave privada.
- Un certificado en formato PKCS#12 que se utiliza para almacenar o transportar el certificado y la clave privada. El certificado PKCS#12 se exporta normalmente desde un certificado de Windows existente como un archivo PFX y, a continuación, se instala en NetScaler Gateway.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix® recomienda utilizar un certificado firmado por una CA de confianza, como Thawte o Verisign.

## Crear una solicitud de firma de certificado

Para proporcionar comunicaciones seguras mediante SSL o TLS, se requiere un certificado de servidor en NetScaler Gateway. Antes de poder cargar un certificado en NetScaler Gateway, debe generar una solicitud de firma de certificado (CSR) y una clave privada. Utilice la opción Crear solicitud de certificado incluida en el asistente de NetScaler Gateway o la utilidad de configuración para crear la CSR. La opción Crear solicitud de certificado crea un archivo .csr que se envía por correo electrónico a la Autoridad de certificación (CA) para su firma y una clave privada que permanece en el dispositivo. La CA firma el certificado y se lo devuelve a la dirección de correo electrónico que proporcionó. Cuando reciba el certificado firmado, puede instalarlo en NetScaler Gateway. Cuando reciba el certificado de la CA, empareje el certificado con la clave privada.

**IMPORTANTE:**

Cuando utilice el asistente de NetScaler Gateway para crear la CSR, debe salir del asistente y esperar a que la CA le envíe el certificado firmado. Cuando reciba el certificado, puede ejecutar el asistente de NetScaler Gateway de nuevo para crear la configuración e instalar el certificado. Para obtener más información sobre el asistente de NetScaler Gateway, consulte Configuración de ajustes mediante el asistente de NetScaler Gateway.

### Crear una CSR mediante el asistente de NetScaler Gateway

1. En la utilidad de configuración, haga clic en la ficha Configuración y, a continuación, en el panel de navegación, haga clic en **NetScaler Gateway**.
2. En el panel de detalles, en Introducción, haga clic en el asistente de **NetScaler Gateway**.
3. Siga las instrucciones del asistente hasta llegar a la página Especificar un certificado de servidor.
4. Haga clic en **Crear una solicitud de firma de certificado** y complete los campos. Nota: El nombre de dominio completo (FQDN) no tiene por qué ser el mismo que el nombre de host de NetScaler Gateway. El FQDN se utiliza para el inicio de sesión del usuario.
5. Haga clic en **Crear** para guardar el certificado en su equipo y, a continuación, haga clic en **Cerrar**.
6. Salga del asistente de NetScaler Gateway sin guardar la configuración.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

### Crear una CSRÂ mediante la GUI de NetScaler

También puede usar la GUI de NetScaler para crear una CSR, sin ejecutar el asistente de NetScaler Gateway.

1. Vaya a **Administración de tráfico** > **SSL > Archivos SSL** y seleccioneÂ **Crear solicitud de firma de certificado (CSR)**.
2. Complete la configuración del certificado y, a continuación, haga clic en **Crear**.

Después de crear el certificado y la clave privada, envíe el certificado por correo electrónico a la CA, como Thawte o Verisign.

Para obtener un procedimiento detallado, consulte Crear una solicitud de firma de certificado.

### Instalar el certificado firmado en NetScaler Gateway

Cuando reciba el certificado firmado de la Autoridad de certificación (CA), emparéjelo con la clave privada del dispositivo y, a continuación, instale el certificado en NetScaler Gateway.

#### Emparejar el certificado firmado con una clave privada mediante la GUI

1. Copie el certificado en NetScaler Gateway en la carpeta nsconfig/ssl mediante un programa Secure Shell (SSH) como WinSCP.
2. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda **SSL > Certificados**.
3. En la página **Certificado SSL**, haga clic en **Introducción**.
4. En el panel de detalles, haga clic en **Instalar**.
5. En **Nombre del par de claves de certificado**, escriba el nombre del certificado.
6. En **Nombre de archivo de certificado**, haga clic en **Dispositivo**.
7. Vaya al certificado, haga clic en **Seleccionar** y, a continuación, haga clic en **Abrir**.
8. En **Nombre de archivo de clave**, haga clic en **Dispositivo**. El nombre de la clave privada es el mismo que el de la solicitud de firma de certificado (CSR). La clave privada se encuentra en NetScaler Gateway en el directorio \\nsconfig\\ssl.
9. Elija la clave privada y, a continuación, haga clic en **Abrir**.
10. Si el certificado tiene formato PEM, en **Contraseña**, escriba la contraseña de la clave privada.
11. Si desea configurar una notificación para cuando el certificado caduque, seleccione **Notificar al caducar**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

12. En **Período de notificación**, escriba el número de días, haga clic en **Crear** y, a continuación, haga clic en **Cerrar**.

### Vincular el certificado y la clave privada a un servidor virtual mediante la GUI

Después de crear y vincular un par de certificado y clave privada, vincúlelo a un servidor virtual.

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda **NetScaler Gateway > Servidores virtuales**.
2. En el panel de detalles, haga clic en un servidor virtual y, a continuación, haga clic en **Abrir**.
3. En la ficha Certificados, en **Disponible**, seleccione un certificado, haga clic en **Agregar** y, a continuación, haga clic en **Aceptar**.

### Vincular el certificado y la clave privada a un servidor virtual mediante la CLI

En el símbolo del sistema, escriba;

```
bind ssl vserver <vServerName> -certkeyName <string> -ocspCheck
( Mandatory | Optional )
```

**Ejemplo:**

```
bind ssl vserver TestClient -CertkeyName ag51.xm.nsi.test.com -CA
-ocspCheck Mandatory
```

**Nota:** oscpCheck es opcional si no se requiere la comprobación OCSP para el certificado del dispositivo.

### Desvincular certificados de prueba del servidor virtual mediante la GUI

Después de instalar el certificado firmado, desvincule los certificados de prueba que estén vinculados al servidor virtual. Puede desvincular los certificados de prueba mediante la utilidad de configuración.

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda **NetScaler Gateway > Servidores virtuales**.
2. En el panel de detalles, haga clic en un servidor virtual y, a continuación, haga clic en **Abrir**.
3. En la pestaña Certificados, en **Configurado**, seleccione el certificado de prueba y, a continuación, haga clic en **Quitar**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

## Configurar certificados intermedios

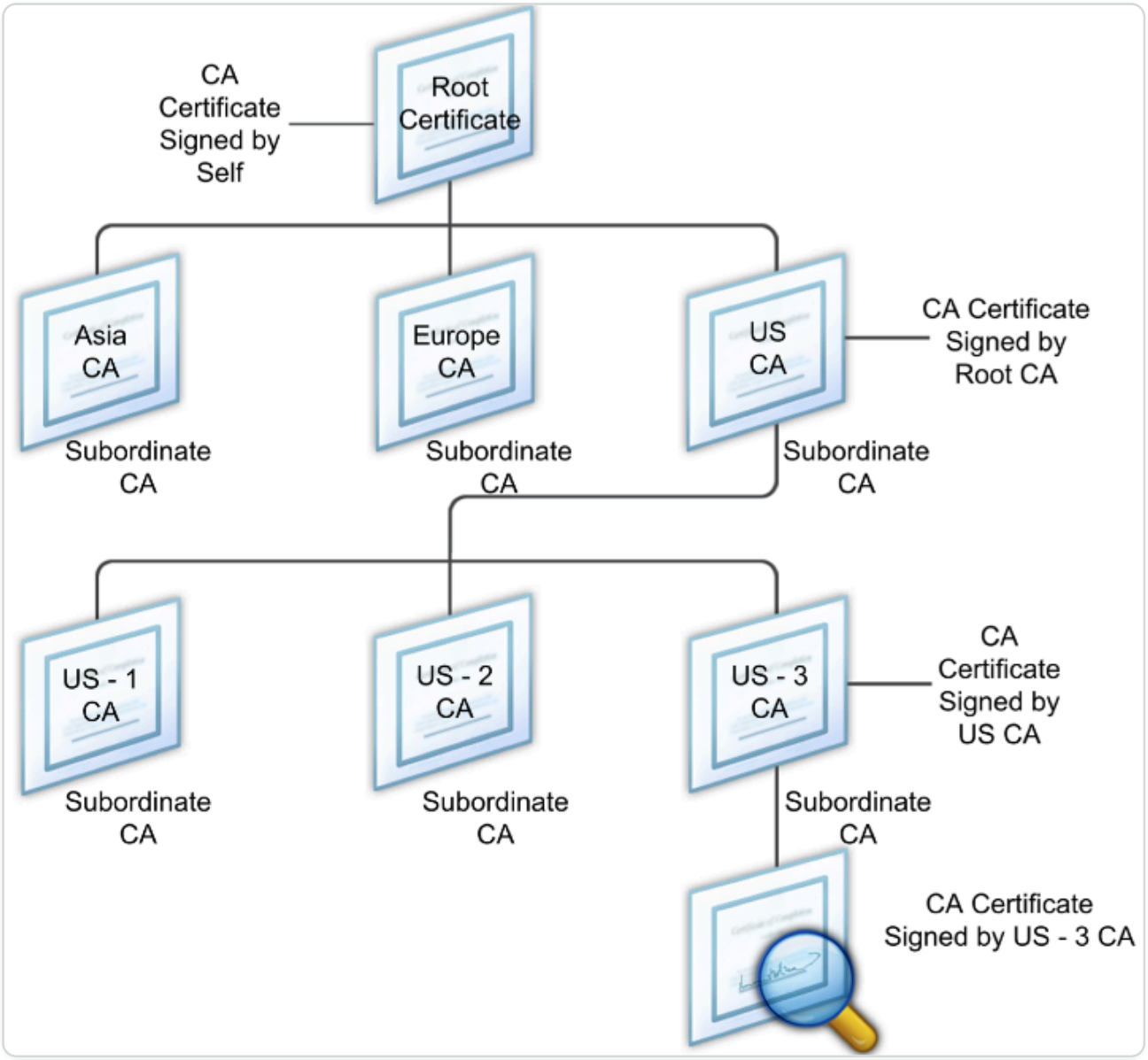
Un certificado intermedio es un certificado que se encuentra entre NetScaler Gateway (el certificado del servidor) y un certificado raíz (instalado en el dispositivo del usuario). Un certificado intermedio forma parte de una cadena.

Algunas organizaciones delegan la responsabilidad de emitir certificados para resolver el problema de la separación geográfica entre las unidades de la organización, o para aplicar diferentes políticas de emisión a diferentes secciones de la organización.

La responsabilidad de emitir certificados se puede delegar mediante la configuración de autoridades de certificación (CA) subordinadas. Las CA pueden firmar sus propios certificados (es decir, son autofirmados) o pueden ser firmados por otra autoridad de certificación. El estándar X.509 incluye un modelo para establecer una jerarquía de CA. En este modelo, como se muestra en la siguiente figura, la CA raíz se encuentra en la parte superior de la jerarquía y es un certificado autofirmado por la autoridad de certificación. Las CA que están directamente subordinadas a la CA raíz tienen certificados de CA firmados por la autoridad de certificación raíz. Las CA que se encuentran bajo las CA subordinadas en la jerarquía tienen sus certificados de CA firmados por las CA subordinadas.

Figura 1. El modelo X.509 que muestra la estructura jerárquica de una cadena de certificados digitales típica

© 1997–2026 Citrix Systems, Inc. All rights reserved.




Si un certificado de servidor está firmado por una CA con un certificado autofirmado, la cadena de certificados se compone de exactamente dos certificados: el certificado de entidad final y la autoridad de certificación raíz. Si un certificado de usuario o de servidor está firmado por una autoridad de certificación intermedia, la cadena de certificados es más larga.

La siguiente figura muestra que los dos primeros elementos son el certificado de entidad final (en este caso, gwy01.company.com) y el certificado de la autoridad de certificación intermedia, en ese orden. El certificado de la autoridad de certificación intermedia va seguido del certificado de su autoridad de certificación. Esta lista continúa hasta que el último certificado de la lista es para una autoridad de certificación raíz. Cada certificado de la cadena da fe de la identidad del certificado anterior.

Figura 2. Una cadena de certificados digitales típica

© 1997–2026 Citrix Systems, Inc. All rights reserved.




### Instalar un certificado intermedio

1. En la utilidad de configuración, en la ficha Configuration, en el panel de navegación, expanda SSL y, a continuación, haga clic en Certificates.
2. En el panel de detalles, haga clic en Install.
3. En Certificate-Key Pair Name, escriba el nombre del certificado.
4. En Details, en Certificate File Name, haga clic en Browse (Appliance) y, en la lista, seleccione Local o Appliance.
5. Vaya al certificado en su equipo (Local) o en NetScaler Gateway (Dispositivo).
6. En Formato de certificado, seleccione PEM.
7. Haga clic en Instalar y, a continuación, en Cerrar.

Al instalar un certificado intermedio en NetScaler Gateway, no es necesario especificar la clave privada ni una contraseña.

Una vez instalado el certificado en el dispositivo, debe vincularse al certificado de servidor.

### Vincular un certificado intermedio a un certificado de servidor

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda SSL y, a continuación, haga clic en Certificados.
2. En el panel de detalles, seleccione el certificado de servidor y, a continuación, en Acción, haga clic en Vincular.
3. Junto a Nombre del certificado de CA, seleccione el certificado intermedio de la lista y, a continuación, haga clic en Aceptar.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

## Usar certificados de dispositivo para la autenticación

NetScaler Gateway admite la comprobación de certificados de dispositivo que le permite vincular la identidad del dispositivo a la clave privada de un certificado. La comprobación de certificados de dispositivo se puede configurar como parte de las directivas de análisis de puntos finales (EPA) clásicas o avanzadas. En las directivas EPA clásicas, el certificado de dispositivo solo se puede configurar para EPA de preautenticación.

NetScaler Gateway verifica el certificado del dispositivo antes de que se ejecute el análisis de puntos finales o antes de que aparezca la página de inicio de sesión. Si configura el análisis de puntos finales, el análisis de puntos finales se ejecuta para verificar el dispositivo del usuario. Cuando el dispositivo supera el análisis y después de que NetScaler Gateway verifica el certificado del dispositivo, los usuarios pueden iniciar sesión en NetScaler Gateway.

**IMPORTANTE:**

- De forma predeterminada, Windows exige privilegios de administrador para acceder a los certificados de dispositivo.
- Para agregar una comprobación de certificado de dispositivo para usuarios que no son administradores, debe instalar el complemento VPN. La versión del complemento VPN debe ser la misma que la del complemento EPA en el dispositivo.
- Puede agregar varios certificados de CA a la puerta de enlace y validar el certificado del dispositivo.
- Si instala dos o más certificados de dispositivo en NetScaler Gateway, los usuarios deben seleccionar el certificado correcto cuando inicien sesión en NetScaler Gateway o antes de que se ejecute el análisis de puntos finales.
- Cuando cree el certificado de dispositivo, debe ser un certificado X.509.
- Si tiene un certificado de dispositivo emitido por una CA intermedia, entonces deben vincularse los certificados de CA intermedios y raíz.
- El cliente EPA necesita que el usuario tenga derechos de administrador local para poder acceder al almacén de certificados de la máquina. Esto rara vez ocurre, por lo que una solución alternativa es instalar el complemento completo de NetScaler® Gateway, que puede acceder al almacén local.

Para obtener más información sobre cómo crear certificados de dispositivo, consulte lo siguiente:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- "¿Qué es el Servicio de inscripción de dispositivos de red para los Servicios de certificados de Active Directory?" en la página de Microsoft Learn Challenge.
- Cómo solicitar un certificado a una entidad de certificación de Microsoft mediante DCE/RPC y la carga útil del perfil de certificado de Active Directory en el sitio web de soporte de Apple.
- Emisión de certificados para iPad/iPhone en el blog de soporte de Microsoft Ask the Directory Services Team.
- Configuración del servicio de inscripción de dispositivos de red en el sitio web de Windows IT Pro.
- Implementación de ejemplo paso a paso de los certificados PKI para Configuration Manager: Autoridad de certificación de Windows Server 2008 en el sitio web de Microsoft System Center.

### Pasos para configurar certificados de dispositivo

Para configurar un certificado de dispositivo, debe completar los siguientes pasos:

- Instale el certificado de la autoridad de certificación del emisor del certificado de dispositivo en NetScaler Gateway. Para obtener más información, consulte Instalación del certificado firmado en NetScaler Gateway.
- Enlace el certificado de la autoridad de certificación del emisor del certificado de dispositivo al servidor virtual de NetScaler Gateway y habilite la comprobación OCSP. Para obtener más información, consulte Instalación del certificado firmado en NetScaler Gateway.
- Cree y enlace OCSP (respondedor) en el certificado de la autoridad de certificación del emisor del certificado de dispositivo. Para obtener más información, consulte Supervisar el estado del certificado con OCSP.

Habilite la comprobación del certificado de dispositivo en el servidor virtual y agregue el certificado de la autoridad de certificación del emisor del certificado de dispositivo a la lista de comprobación de certificados de dispositivo. Para obtener más información, consulte Habilitar la comprobación del certificado de dispositivo en un servidor virtual para la política EPA clásica.

Complete la configuración y verificación del certificado de dispositivo del lado del cliente en la máquina Windows. Para obtener más información, consulte Verificación del certificado de dispositivo en una máquina Windows.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**NOTA:**

Todos los clientes que deseen utilizar la comprobación EPA del certificado de dispositivo deben tener el certificado de dispositivo instalado en el almacén de certificados del sistema de la máquina.

### Habilitar la comprobación del certificado de dispositivo en un servidor virtual para la política EPA clásica

Después de crear el certificado de dispositivo, instale el certificado en NetScaler Gateway mediante el procedimiento para Importar e instalar un certificado existente en NetScaler Gateway.

1. En la ficha Configuración, vaya a **NetScaler Gateway > Servidores virtuales**.
2. En la página **Servidores virtuales de NetScaler Gateway**, seleccione un servidor virtual existente y haga clic en **Editar**.
3. En la página **Servidores virtuales VPN**, en la sección **Configuración básica**, haga clic en **Editar**.
4. Desactive la casilla **Habilitar autenticación** para deshabilitar la autenticación.
5. Seleccione la casilla **Habilitar certificado de dispositivo** para habilitar el certificado de dispositivo
6. Haga clic en **Agregar** para añadir el nombre del certificado de CA de un emisor de certificado de dispositivo disponible a la lista.
7. Para vincular un certificado de CA al servidor virtual, haga clic en **Certificado de CA** en la sección **CA para certificado de dispositivo**, haga clic en **Agregar**, seleccione el certificado y, a continuación, haga clic en **+**.

**NOTA:**

Para obtener información sobre cómo habilitar y vincular certificados de dispositivo en un servidor virtual para una política EPA avanzada, consulte Certificado de dispositivo en nFactor como componente EPA.

### Verificación del certificado de dispositivo en una máquina Windows

1. Abra un explorador y acceda al FQDN de NetScaler Gateway.
2. Permita que se ejecute el cliente de Citrix® End Point Analysis (EPA). Si aún no está instalado, instale EPA.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix EPA se ejecuta y valida el certificado de dispositivo y redirige a la página de autenticación si la comprobación EPA del certificado de dispositivo se supera; de lo contrario, le redirige a la página de error de EPA. En caso de que tenga otras comprobaciones EPA, los resultados del análisis EPA dependerán de las comprobaciones EPA configuradas.

Para depurar más a fondo en el cliente, examine los siguientes registros EPA en el cliente: C:\Users\<User name>\AppData\Local\Citrix\AGEE\nsepa.txt

**Nota:**

No se admite la verificación del certificado de dispositivo con CRL.

## Importar e instalar un certificado existente

Puede importar un certificado existente desde un equipo basado en Windows que ejecute Internet Information Services (IIS) o desde un equipo que ejecute Secure Gateway.

Al exportar el certificado, asegúrese de exportar también la clave privada. A veces, no se puede exportar la clave privada, lo que significa que no se puede instalar el certificado en NetScaler Gateway. Si esto ocurre, utilice la Solicitud de firma de certificado (CSR) para crear un certificado. Para obtener más información, consulte Creación de una solicitud de firma de certificado.

Al exportar un certificado y una clave privada desde Windows, el equipo crea un archivo de intercambio de información personal (.pfx). Este archivo se instala después en NetScaler Gateway como un certificado PKCS#12.

Si va a reemplazar Secure Gateway por NetScaler Gateway, puede exportar el certificado y la clave privada de Secure Gateway. Si está realizando una migración in situ de Secure Gateway a NetScaler Gateway, el nombre de dominio completo (FQDN) de la aplicación y del dispositivo debe ser el mismo. Al exportar el certificado de Secure Gateway, retira inmediatamente Secure Gateway, instala el certificado en NetScaler Gateway y, a continuación, prueba la configuración. Secure Gateway y NetScaler Gateway no pueden ejecutarse en su red al mismo tiempo si tienen el mismo FQDN.

Si utiliza Windows Server 2003 o Windows Server 2008, puede usar la Consola de administración de Microsoft para exportar el certificado. Para obtener más información, consulte la Ayuda en línea de Windows.

Deje los valores predeterminados para todas las demás opciones, defina una contraseña y guarde el archivo .pfx en su equipo. Cuando se exporta el certificado, lo instala en NetScaler Gateway.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

### Para instalar el certificado y la clave privada en NetScaler Gateway

1. En la utilidad de configuración, haga clic en la ficha Configuración y, a continuación, en el panel de navegación, haga clic en **NetScaler Gateway**.
2. En el panel de detalles, en Introducción, haga clic en **Asistente de NetScaler Gateway**.
3. Haga clic en **Siguiente**, seleccione un servidor virtual existente y, a continuación, haga clic en **Siguiente**.
4. En **Opciones de certificado**, seleccione **Instalar un archivo PKCS#12 (.pfx)**.
5. En **Nombre de archivo PKCS#12**, haga clic en **Examinar**, navegue hasta el certificado y, a continuación, haga clic en **Seleccionar**.
6. En ((Contraseña)), escriba la contraseña de la clave privada.

   Esta es la contraseña que utilizó al convertir el certificado a formato PEM.
7. Haga clic en **Siguiente** para finalizar el asistente de NetScaler Gateway sin cambiar ninguna otra configuración.

Cuando el certificado se instala en NetScaler Gateway, el certificado aparece en la utilidad de configuración en el nodo **SSL \ > Certificados**.

#### Para crear una clave privada

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, haga clic en **SSL**.
2. En el panel de detalles, en **Claves SSL**, haga clic en **Crear clave RSA**.
3. En **Nombre de archivo de clave**, escriba el nombre de la clave privada o haga clic en Examinar para buscar un archivo existente.
4. En **Tamaño de clave (bits)**, escriba el tamaño de la clave privada.
5. En **Valor de exponente público**, seleccione F4 o 3.

   El valor del exponente público para la clave RSA. Esto forma parte del algoritmo de cifrado y es necesario para crear la clave RSA. Los valores son F4 (Hex: 0x10001) o 3 (Hex: 0x3). El valor predeterminado es F4.
6. En **Formato de clave**, seleccione PEM o DER. Citrix® recomienda el formato PEM para el certificado.
7. En **Algoritmo de codificación PEM**, seleccione DES o DES3.
8. En **Frase de contraseña PEM** y **verificar Passphrase**, escriba la contraseña, haga clic en **Crear** y, a continuación, haga clic en **Cerrar**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**Nota**: Para asignar una frase de contraseña, el formato de clave debe ser PEM y debe seleccionar el algoritmo de codificación.

Para crear una clave privada DSA en la utilidad de configuración, haga clic en **Crear clave DSA** y siga los pasos realizados para crear la clave privada RSA.

## Listas de revocación de certificados

De vez en cuando, las Autoridades de Certificación (CA) emiten listas de revocación de certificados (CRL). Las CRL contienen información sobre certificados en los que ya no se puede confiar. Por ejemplo, supongamos que Ann deja XYZ Corporation. La empresa puede colocar el certificado de Ann en una CRL para evitar que firme mensajes con esa clave.

Del mismo modo, puede revocar un certificado si una clave privada se ve comprometida o si ese certificado ha caducado y se está utilizando uno nuevo. Antes de confiar en una clave pública, asegúrese de que el certificado no aparece en una CRL.

NetScaler Gateway admite los dos tipos de CRL siguientes:

- CRL que enumeran los certificados revocados o que ya no son válidos
- Protocolo de estado de certificados en línea (OSCP), un protocolo de Internet utilizado para obtener el estado de revocación de los certificados X.509

**Para añadir una CRL:**

Antes de configurar la CRL en el dispositivo NetScaler Gateway, asegúrese de que el archivo CRL esté almacenado localmente en el dispositivo. En el caso de una configuración de alta disponibilidad, el archivo CRL debe estar presente en ambos dispositivos NetScaler Gateway, y la ruta del directorio al archivo debe ser la misma en ambos dispositivos.

Si necesita actualizar la CRL, puede utilizar los siguientes parámetros:

- Nombre de CRL: El nombre de la CRL que se añade en NetScaler. Máximo 31 caracteres.
- Archivo CRL: El nombre del archivo CRL que se añade en NetScaler. NetScaler busca el archivo CRL en el directorio /var/netscaler/ssl de forma predeterminada. Máximo 63 caracteres.
- URL: Máximo 127 caracteres
- DN base: Máximo 127 caracteres
- DN de enlace: Máximo 127 caracteres
- Contraseña: Máximo 31 caracteres

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Días: Máximo 31

1. En la utilidad de configuración, en la ficha Configuración, expanda SSL y, a continuación, haga clic en CRL.
2. En el panel de detalles, haga clic en Agregar.
3. En el cuadro de diálogo Agregar CRL, especifique los valores para lo siguiente:
    - Nombre de CRL
    - Archivo CRL
    - Formato (opcional)
    - Certificado de CA (opcional)
4. Haga clic en **Crear** y, a continuación, haga clic en **Cerrar**. En el panel de detalles de CRL, seleccione la CRL que configuró y verificar que la configuración que aparece en la parte inferior de la pantalla es correcta.

**Para configurar la actualización automática de CRL mediante LDAP o HTTP en la GUI:**

Una CRL es generada y publicada por una CA periódicamente o, a veces, inmediatamente después de que se revoque un certificado en particular. Citrix recomienda que actualice las CRL en el dispositivo NetScaler Gateway regularmente para protegerse contra clientes que intentan conectarse con certificados no válidos.

El dispositivo NetScaler Gateway puede actualizar las CRL desde una ubicación web o un directorio LDAP. Cuando se especifican los parámetros de actualización y una ubicación web o un servidor LDAP, la CRL no tiene que estar presente en la unidad de disco duro local en el momento de ejecutar el comando. La primera actualización almacena una copia en la unidad de disco duro local, en la ruta especificada por el parámetro Archivo CRL. La ruta predeterminada para almacenar la CRL es /var/netscaler/ssl.

### Parámetros de actualización de CRL

#### Nombre de CRL

```
El nombre de la CRL que se está actualizando en NetScaler Gateway.
```

#### Habilitar actualización automática de CRL

```
Habilite o deshabilite la actualización automática de CRL.
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

### Certificado de CA

El certificado de la CA que ha emitido la CRL. Este certificado de CA debe estar instalado en el dispositivo. El NetScaler solo puede actualizar las CRL de las CA cuyos certificados estén instalados en él.

### Método

Protocolo en el que se obtiene la actualización de la CRL de un servidor web (HTTP) o un servidor LDAP. Valores posibles: HTTP, LDAP. Predeterminado: HTTP.

### Ámbito

El alcance de la operación de búsqueda en el servidor LDAP. Si el ámbito especificado es

Base, la búsqueda se realiza al mismo nivel que el DN base. Si el ámbito especificado es

Uno, la búsqueda se extiende a un nivel por debajo del DN base.

### IP del servidor

La dirección IP del servidor LDAP desde el que se recupera la CRL. Seleccione IPv6 para usar una dirección IP IPv6.

### Puerto

El número de puerto en el que se comunica el servidor LDAP o HTTP.

### URL

La URL de la ubicación web desde la que se recupera la CRL.

### DN base

© 1997–2026 Citrix Systems, Inc. All rights reserved.

El DN base utilizado por el servidor LDAP para buscar el atributo CRL.

Nota: Citrix® recomienda utilizar el atributo DN base en lugar del Nombre del emisor (Issuer-Name) del certificado de CA para buscar la CRL en el servidor LDAP. Es posible que el campo Nombre del emisor (Issuer-Name) no coincida exactamente con el DN de la estructura del directorio LDAP.

### DN de enlace

El atributo DN de enlace se utiliza para acceder al objeto CRL en el repositorio LDAP. Los atributos DN de enlace son las credenciales de administrador para el servidor LDAP. Configure este parámetro para restringir el acceso no autorizado a los servidores LDAP.

### Contraseña

La contraseña de administrador utilizada para acceder al objeto CRL en el repositorio LDAP. La contraseña es necesaria si el acceso al repositorio LDAP está restringido, es decir, si no se permite el acceso anónimo.

### Intervalo

El intervalo en el que se debe realizar la actualización de la CRL. Para una actualización instantánea de la CRL, especifique el intervalo como AHORA (NOW). Valores posibles: MENSUAL (MONTHLY), DIARIO (DAILY), SEMANAL (WEEKLY), AHORA (NOW), NINGUNO (NONE).

### Días

El día en que se debe realizar la actualización de la CRL. La opción no está disponible si el intervalo se establece en DIARIO (DAILY).

### Hora

La hora exacta en formato de 24 horas en que se debe realizar la actualización de la CRL.

### Binario

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
Establezca el modo de recuperación de CRL basado en LDAP en binario.
Valores posibles: SÍ (YES), NO (NO). Predeterminado: NO (NO).
```

1. En el panel de navegación, expanda SSL y, a continuación, haga clic en CRL.
2. Seleccione la CRL configurada para la que desea actualizar los parámetros de actualización y, a continuación, haga clic en Abrir.
3. Seleccione la opción Habilitar actualización automática de CRL.
4. En el grupo Parámetros de actualización automática de CRL, especifique los valores para los siguientes parámetros: Nota: Un asterisco (*) indica un parámetro obligatorio.
    - Método
    - Binario
    - Ámbito
    - IP del servidor
    - Puerto*
    - URL
    - DN base*
    - DN de enlace
    - Contraseña
    - Intervalo
    - Días
    - Hora
5. Haga clic en Crear. En el panel CRL, seleccione la CRL que configuró y verificar que la configuración que aparece en la parte inferior de la pantalla es correcta.

### Supervisar el estado del certificado con OCSP

El Protocolo de estado de certificado en línea (OCSP) es un protocolo de Internet que se utiliza para determinar el estado de un certificado SSL de cliente. NetScaler Gateway admite OCSP tal como se define en RFC 2560. OCSP ofrece ventajas significativas sobre las listas de revocación de certificados (CRL) en términos de información oportuna. El estado de revocación actualizado de un certificado de cliente es especialmente útil en transacciones que implican grandes sumas de dinero y operaciones bursátiles de alto valor. También utiliza menos recursos del sistema y de la

© 1997–2026 Citrix Systems, Inc. All rights reserved.

red. La implementación de OCSP en NetScaler Gateway incluye el procesamiento por lotes de solicitudes y el almacenamiento en caché de respuestas.

### Implementación de OCSP en NetScaler Gateway

La validación OCSP en un dispositivo NetScaler Gateway comienza cuando NetScaler Gateway recibe un certificado de cliente durante un protocolo de enlace SSL. Para validar el certificado, NetScaler Gateway crea una solicitud OCSP y la reenvía al respondedor OCSP. Para ello, NetScaler Gateway extrae la URL del respondedor OCSP del certificado de cliente o utiliza una URL configurada localmente. La transacción permanece en estado suspendido hasta que NetScaler Gateway evalúa la respuesta del servidor y determina si permite la transacción o la rechaza. Si la respuesta del servidor se retrasa más allá del tiempo configurado y no hay otros respondedores configurados, NetScaler Gateway permite la transacción o muestra un error, dependiendo de si se configura la comprobación OCSP como opcional u obligatoria. NetScaler Gateway admite el procesamiento por lotes de solicitudes OCSP y el almacenamiento en caché de respuestas OCSP para reducir la carga en el respondedor OCSP y proporcionar respuestas más rápidas.

### Procesamiento por lotes de solicitudes OCSP

Cada vez que NetScaler Gateway recibe un certificado de cliente, envía una solicitud al respondedor OCSP. Para ayudar a evitar la sobrecarga del respondedor OCSP, NetScaler Gateway puede consultar el estado de más de un certificado de cliente en la misma solicitud. Para que el procesamiento por lotes de solicitudes funcione de manera eficiente, debe definir un tiempo de espera para que el procesamiento de un solo certificado no se retrase mientras se espera para formar un lote.

### Almacenamiento en caché de respuestas OCSP

El almacenamiento en caché de las respuestas recibidas del respondedor OCSP permite respuestas más rápidas al usuario y reduce la carga en el respondedor OCSP. Al recibir el estado de revocación de un certificado de cliente del respondedor OCSP, NetScaler Gateway almacena la respuesta localmente durante un período de tiempo predefinido. Cuando se recibe un certificado de cliente durante un protocolo de enlace SSL, NetScaler Gateway primero comprueba su caché local en busca de una entrada para este certificado. Si se encuentra una entrada que sigue siendo válida (dentro del límite de tiempo de espera de la caché), la entrada se evalúa y el certificado de cliente se acepta o se rechaza. Si no se encuentra un certificado, NetScaler Gateway envía una solicitud al respondedor OCSP y almacena la respuesta en su caché local durante un período de tiempo configurado.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

## Configurar el estado del certificado OCSP

La configuración de un Protocolo de estado de certificado en línea (OCSP) implica agregar un respondedor OCSP, vincular el respondedor OCSP a un certificado firmado de una Autoridad de certificación (CA) y vincular el certificado y la clave privada a un servidor virtual Secure Sockets Layer (SSL). Si necesita vincular un certificado y una clave privada diferentes a un respondedor OCSP que ya configuró, primero debe desvincular el respondedor y luego vincularlo a un certificado diferente.

### Para configurar OCSP

1. En la ficha Configuración, en el panel de navegación, expanda SSL y, a continuación, haga clic en Respondedor OCSP.
2. En el panel de detalles, haga clic en Agregar.
3. En Nombre, escriba un nombre para el perfil.
4. En URL, escriba la dirección web del respondedor OCSP.

   Este campo es obligatorio. La dirección web no puede exceder los 32 caracteres.
5. Para almacenar en caché las respuestas OCSP, haga clic en Caché y en Tiempo de espera, escriba el número de minutos que NetScaler Gateway retiene la respuesta.
6. En Agrupación de solicitudes, haga clic en Habilitar.
7. En Retraso de agrupación, especifique el tiempo, en milisegundos, permitido para agrupar un conjunto de solicitudes OCSP.

   Los valores pueden ser de 0 a 10000. El valor predeterminado es 1.
8. En Desviación de tiempo de producción, escriba la cantidad de tiempo que NetScaler Gateway puede usar cuando el dispositivo debe comprobar o aceptar la respuesta.
9. En Verificación de respuesta, seleccione Confiar en respuestas si desea deshabilitar las comprobaciones de firma por parte del respondedor OCSP.

   Si habilita Confiar en respuestas, omita el Paso 8 y el Paso 9.
10. En Certificado, seleccione el certificado que se utiliza para firmar las respuestas OCSP.

    Si no se selecciona un certificado, la CA a la que está vinculado el respondedor OCSP se utiliza para verificar las respuestas.
11. En Tiempo de espera de solicitud, escriba el número de milisegundos que se deben esperar para una respuesta OCSP.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Este tiempo incluye el tiempo de Retraso de agrupación. Los valores pueden ser de 0 a 120000. El valor predeterminado es 2000.

12. En Certificado de firma, seleccione el certificado y la clave privada utilizados para firmar las solicitudes OCSP. Si no especifica un certificado y una clave privada, las solicitudes no se firman.
13. Para habilitar el número utilizado una vez `(nonce) extension`, seleccione Nonce.
14. Para usar un certificado de cliente, haga clic en Inserción de certificado de cliente.
15. Haga clic en Crear y, a continuación, haga clic en Cerrar.

# Gestionar la configuración de NetScaler Gateway

Cuando realiza cambios de configuración en NetScaler Gateway, los cambios se guardan en archivos de registro. Puede ver varios tipos de configuraciones:

- Configuración guardada. Puede ver la configuración que ha guardado en NetScaler Gateway.
- Configuración en ejecución. Puede ver la configuración activa, como un servidor virtual o una política de autenticación, que ha configurado pero no ha guardado como configuración guardada en NetScaler Gateway.
- Configuración en ejecución frente a configuración guardada. Puede comparar lado a lado la configuración en ejecución y la guardada en NetScaler Gateway.

También puede borrar la configuración en NetScaler Gateway.

**IMPORTANTE:**

Si decide borrar la configuración en NetScaler Gateway, se eliminarán los certificados, los servidores virtuales y las políticas. Citrix recomienda no borrar la configuración.

## Guardar la configuración de NetScaler Gateway

Puede guardar su configuración actual de NetScaler Gateway en un equipo de su red, ver la configuración en ejecución actual y comparar las configuraciones guardadas y en ejecución.

### Para guardar la configuración en NetScaler Gateway

1. En la utilidad de configuración, encima del panel de detalles, haga clic en el icono Guardar y, a continuación, haga clic en Sí.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

### Para ver y guardar el archivo de configuración en NetScaler Gateway

La configuración guardada son los ajustes que se guardan en un archivo de registro en NetScaler Gateway, como los ajustes para servidores virtuales, políticas, direcciones IP, usuarios, grupos y certificados.

Cuando configura ajustes en NetScaler Gateway, puede guardar los ajustes en un archivo en su equipo. Si necesita reinstalar el software de NetScaler Gateway o elimina accidentalmente algunos ajustes, puede usar este archivo para restaurar su configuración. Si necesita restaurar los ajustes, puede copiar el archivo a NetScaler Gateway y reiniciar el dispositivo usando la interfaz de línea de comandos o un programa, como WinSCP, para copiar el archivo a NetScaler Gateway.

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda Sistema y, a continuación, haga clic en Diagnóstico.
2. En el panel de detalles, en Ver configuración, haga clic en Configuración guardada.
3. En el cuadro de diálogo Configuración guardada, haga clic en Guardar texto de salida en un archivo, asigne un nombre al archivo y, a continuación, haga clic en Guardar. Nota: Citrix recomienda guardar el archivo con el nombre de archivo ns.conf.

### Para ver la configuración en ejecución actual

Cualquier cambio en NetScaler Gateway que se produzca sin un esfuerzo por guardarlos se denomina configuración en ejecución. Esta configuración está activa en NetScaler Gateway, pero no se guarda en el dispositivo. Si configuró ajustes adicionales, como una directiva, un servidor virtual, usuarios o grupos, puede ver estos ajustes en la configuración en ejecución.

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda Sistema y, a continuación, haga clic en Diagnóstico.
2. En el panel de detalles, en Ver configuración, haga clic en Configuración en ejecución.

### Para comparar la configuración guardada y la configuración en ejecución

Puede ver qué configuraciones se guardan en el dispositivo y compararlas con la configuración en ejecución. Puede optar por guardar la configuración en ejecución o realizar cambios en la configuración.

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda Sistema y, a continuación, haga clic en Diagnóstico.
2. En el panel de detalles, en Ver configuración, haga clic en Guardada frente a en ejecución.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

## Borrar la configuración de NetScaler Gateway

Puede borrar la configuración de NetScaler Gateway. Puede elegir entre los tres niveles de configuración siguientes para borrar:

**IMPORTANTE:**

Citrix recomienda guardar la configuración antes de borrar la configuración de NetScaler Gateway.

- Básico. Borra todos los ajustes del dispositivo, excepto la dirección IP del sistema, la puerta de enlace predeterminada, las direcciones IP asignadas, las direcciones IP de subred, los ajustes de DNS, los ajustes de red, los ajustes de alta disponibilidad, la contraseña administrativa y los ajustes de funciones y modos.
- Extendido. Borra todos los ajustes, excepto la dirección IP del sistema, las direcciones IP asignadas, las direcciones IP de subred, los ajustes de DNS y las definiciones de alta disponibilidad.
- Completo. Restaura la configuración a los ajustes de fábrica originales, excluyendo la dirección IP del sistema (NSIP) y la ruta predeterminada, que son necesarios para mantener la conectividad de red con el dispositivo.

Cuando borra toda o parte de la configuración, los ajustes de las funciones se restablecen a los valores predeterminados de fábrica.

Cuando borra la configuración, los archivos almacenados en NetScaler Gateway, como certificados y licencias, no se eliminan. El archivo ns.conf no se modifica. Si desea guardar la configuración antes de borrarla, guárdela primero en su equipo. Si guarda la configuración, puede restaurar el archivo ns.conf en NetScaler Gateway. Después de restaurar el archivo en el dispositivo y reiniciar NetScaler Gateway, se restaurarán todos los ajustes de configuración de ns.conf.

Las modificaciones a los archivos de configuración, como rc.conf, no se revierten.

Si tiene un par de alta disponibilidad, ambos dispositivos NetScaler Gateway se modifican de forma idéntica. Por ejemplo, si borra la configuración básica en un dispositivo, los cambios se propagan al segundo dispositivo.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

### Para borrar la configuración de NetScaler Gateway

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda Sistema y, a continuación, haga clic en Diagnósticos.
2. En el panel de detalles, en Mantenimiento, haga clic en Borrar configuración.
3. En Nivel de configuración, seleccione el nivel que desea borrar y, a continuación, haga clic en Ejecutar.

# Pruebe la configuración de NetScaler Gateway

Después de configurar los ajustes iniciales en NetScaler Gateway, puede probar la configuración conectándose al dispositivo.

Para probar la configuración de NetScaler Gateway, cree una cuenta de usuario local. Luego, utilizando la dirección IP del servidor virtual o el nombre de dominio completo (FQDN) del dispositivo, abra un navegador web y escriba la dirección web. Por ejemplo, en la barra de direcciones, escriba `https://my.company.com` o `https://192.168.96.183`.

En la pantalla de inicio de sesión, introduzca el nombre de usuario y la contraseña de la cuenta de usuario que creó anteriormente. Después de iniciar sesión, se le pedirá que descargue e instale el cliente Citrix Secure Access™.

Después de instalar y conectarse correctamente con el cliente Citrix Secure Access, aparece la Interfaz de acceso. La Interfaz de acceso es la página de inicio predeterminada para NetScaler Gateway.

## Crear una cuenta de usuario mediante la GUI

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda **NetScaler Gateway \ > Administración de usuarios** y, a continuación, haga clic en **Usuarios AAA**.
2. En el panel de detalles, haga clic en Agregar.
3. En Nombre de usuario, escriba el nombre de usuario.
4. Si utiliza la autenticación local, desactive la casilla de verificación Autenticación externa. La autenticación de usuarios con tipos de autenticación externa, como LDAP o RADIUS, es la predeterminada. Si desactiva esta casilla, NetScaler Gateway autentica a los usuarios.
5. En Contraseña y Confirmar contraseña, escriba la contraseña del usuario, haga clic en Crear y, a continuación, haga clic en Cerrar.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Al agregar usuarios mediante la utilidad de configuración, puede vincular las siguientes directivas al usuario:

- Autorización
- Tráfico, sesión y auditoría
- Marcadores
- Aplicaciones de intranet
- Direcciones IP de intranet

Si tiene problemas para iniciar sesión con la cuenta de usuario de prueba, compruebe lo siguiente:

- Si recibe una advertencia de certificado, significa que hay un certificado de prueba o un certificado no válido instalado en NetScaler Gateway. Si hay un certificado firmado por una entidad de certificación (CA) instalado en el dispositivo, asegúrese de que haya un certificado raíz correspondiente en el dispositivo del usuario.
- Si utilizó un certificado firmado por CA, verificar que generó el certificado del sitio correctamente mediante la Solicitud de firma de certificado (CSR) firmada y que los datos del Nombre distinguido (DN) introducidos en la CSR son precisos. El problema también podría ser que el nombre de host no coincide con la dirección IP que figura en el certificado firmado. Compruebe que el nombre común del certificado configurado se corresponde con la información de la dirección IP del servidor virtual configurado.
- Si la pantalla de inicio de sesión no aparece o si aparece cualquier otro mensaje de error, revise el proceso de configuración y confirme que realizó todos los pasos correctamente e introdujo todos los parámetros con precisión.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

# Actualizar el software de NetScaler Gateway

Puede actualizar el software que reside en NetScaler Gateway cuando haya nuevas versiones disponibles. Puede buscar actualizaciones en el sitio web de Citrix. Solo puede actualizar a una nueva versión si sus licencias de NetScaler Gateway están bajo el programa Subscription Advantage cuando se publica la actualización. Puede renovar Subscription Advantage en cualquier momento. Para obtener más información, consulte el sitio web de soporte de NetScaler.

La ruta de actualización y la información de productos compatibles también están disponibles en la Guía de actualización de Citrix.

Para obtener información sobre la última versión de mantenimiento de NetScaler Gateway, consulte las notas de la versión de NetScaler.

## Buscar actualizaciones de software

1. Vaya al sitio web de Citrix.
2. Haga clic en **Mi cuenta** e inicie sesión.
3. Haga clic en **Descargas**.
4. En Buscar descargas, seleccione **NetScaler Gateway**.
5. En **Seleccionar tipo de descarga**, seleccione **Software de producto** y, a continuación, haga clic en **Buscar**. También puede seleccionar **Dispositivos virtuales** para descargar NetScaler VPX. Al seleccionar esta opción, recibirá una lista de software para la máquina virtual de cada hipervisor.
6. En la página de NetScaler Gateway, expanda **NetScaler Gateway o Access Gateway**.
7. Haga clic en la versión del software del dispositivo que desea descargar.
8. En la página del software del dispositivo para la versión que desea descargar, seleccione el dispositivo virtual y, a continuación, haga clic en **Descargar**.
9. Siga las instrucciones en pantalla para descargar el software.

Cuando el software se descargue en su equipo, puede usar el Asistente de actualización o el símbolo del sistema para instalar el software.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

# Actualizar NetScaler Gateway mediante el Asistente de actualización

1. En la utilidad de configuración, en la ficha **Configuración**, en el panel de navegación, haga clic en Sistema.
2. En el panel de detalles, haga clic en **Asistente de actualización**.
3. Haga clic en **Siguiente** y, a continuación, siga las instrucciones del asistente.

# Actualizar NetScaler Gateway mediante un símbolo del sistema

1. Para cargar el software en NetScaler Gateway, utilice un cliente FTP seguro, como WinSCP, para conectarse al dispositivo.
2. Copie el software de su equipo al directorio /var/`nsinstall` del dispositivo.
3. Utilice un cliente Secure Shell (SSH), como PuTTY, para abrir una conexión SSH al dispositivo.
4. Inicie sesión en NetScaler Gateway.
5. En un símbolo del sistema, escriba: `shell`
6. Para cambiar al directorio `nsinstall`, en un símbolo del sistema, escriba: `cd /var/nsinstall`
7. Para ver el contenido del directorio, escriba: `ls`
8. Para desempaquetar el software, escriba: tar –xvzf build_X_XX.tgz, donde build_X_XX.tgz es el nombre de la compilación a la que desea actualizar.
9. Para iniciar la instalación, en un símbolo del sistema, escriba: `./installns`
10. Cuando la instalación se complete, reinicie NetScaler Gateway.

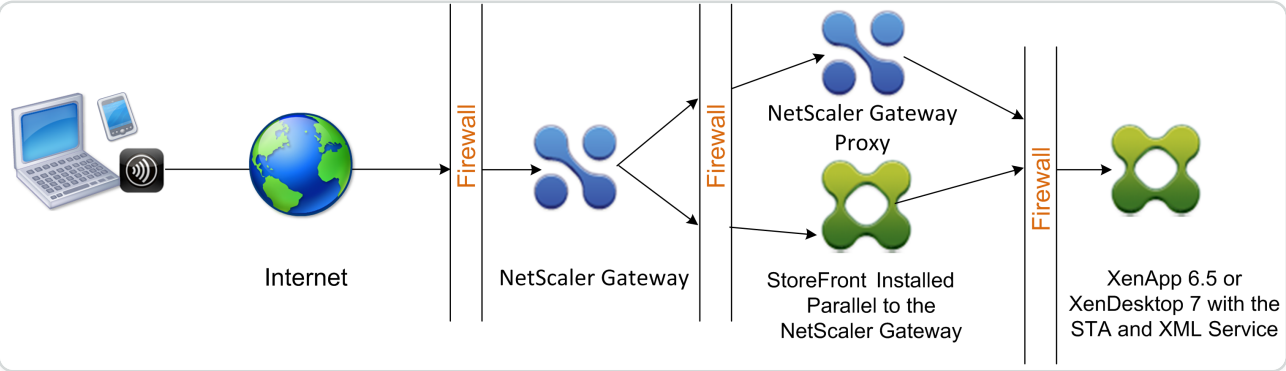
Después de que NetScaler Gateway se reinicie, para verificar la instalación correcta, inicie la utilidad de configuración. La versión de NetScaler Gateway que está en el dispositivo aparece en la esquina superior derecha.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

# Implementar NetScaler Gateway en una DMZ de doble salto

Algunas organizaciones utilizan tres firewalls para proteger sus redes internas. Los tres firewalls dividen la DMZ en dos etapas para proporcionar una capa adicional de seguridad a la red interna. Esta configuración de red se denomina DMZ de doble salto.

Figura 1. Dispositivos NetScaler Gateway implementados en una DMZ de doble salto




**NOTA:**

A efectos ilustrativos, el ejemplo anterior describe una configuración de doble salto que utiliza tres firewalls con StoreFront, NetScaler Gateway y Citrix Virtual Apps. Sin embargo, también puede tener una DMZ de doble salto con un dispositivo en la DMZ y otro dispositivo en la red segura. Si configura una configuración de doble salto con un dispositivo en la DMZ y otro en la red segura, puede ignorar las instrucciones para abrir puertos en el tercer firewall.

Puede configurar una DMZ de doble salto para admitir Citrix StoreFront instalado en paralelo al proxy de NetScaler Gateway. Los usuarios se conectan mediante la aplicación Citrix Workspace.

**NOTA:**

Si implementa NetScaler Gateway en una DMZ de doble salto con StoreFront, la detección automática basada en correo electrónico para la aplicación Citrix Workspace no funciona.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

# Cómo funciona una implementación de doble salto

Puede implementar dispositivos NetScaler Gateway en una DMZ de doble salto para controlar el acceso a los servidores que ejecutan Citrix Virtual Apps. Las conexiones en una implementación de doble salto se producen de la siguiente manera:

- Los usuarios se conectan a NetScaler Gateway en la primera DMZ mediante un explorador web y mediante la aplicación Citrix Workspace para seleccionar una aplicación publicada.
- La aplicación Citrix Workspace se inicia en el dispositivo del usuario. El usuario se conecta a NetScaler Gateway para acceder a la aplicación publicada que se ejecuta en la granja de servidores de la red segura.

  **Nota:** Secure Hub y el cliente Citrix Secure Access para Windows no son compatibles con una implementación de DMZ de doble salto. Solo la aplicación Citrix Workspace se utiliza para las conexiones de usuario.
- NetScaler Gateway en la primera DMZ gestiona las conexiones de usuario y realiza las funciones de seguridad de una VPN SSL. Este NetScaler Gateway cifra las conexiones de usuario, determina cómo se autentican los usuarios y controla el acceso a los servidores de la red interna.
- NetScaler Gateway en la segunda DMZ actúa como un dispositivo proxy de NetScaler Gateway. Este NetScaler Gateway permite que el tráfico ICA atraviese la segunda DMZ para completar las conexiones de usuario a la granja de servidores. Las comunicaciones entre NetScaler Gateway en la primera DMZ y la Secure Ticket Authority (STA) en la red interna también se gestionan mediante proxy a través de NetScaler Gateway en la segunda DMZ.

NetScaler Gateway admite conexiones IPv4 e IPv6. Puede usar la utilidad de configuración para configurar la dirección IPv6.

La siguiente tabla muestra la compatibilidad de implementación de doble salto para las diversas funciones de ICA®:

| FUNCIÓN ICA | COMPATIBILIDAD DE DOBLE SALTO |
|---|---|
| SmartAccess | Sí |
| SmartControl | Sí |
| Enlightened Data Transport (EDT) | Sí |
| HDX Insight | Sí |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| FUNCIÓN ICA | COMPATIBILIDAD DE DOBLE SALTO |
|---|---|
| Fiabilidad de sesión ICA (puerto 2598) | Sí |
| Migración de sesión ICA | Sí |
| Tiempo de espera de sesión ICA | Sí |
| ICA de múltiples flujos | Sí (solo TCP) |
| Framehawk | No |
| Audio UDP | No |

# Prepararse para una implementación de DMZ de doble salto

Al configurar una implementación de DMZ de doble salto, debe responder las siguientes preguntas:

- ¿Quiero admitir el equilibrio de carga?
- ¿Qué puertos abro en los firewalls?
- ¿Cuántos certificados SSL necesito?
- ¿Qué componentes necesito antes de iniciar la implementación?

Los temas de esta sección contienen información para ayudarle a responder a estas preguntas según corresponda a su entorno.

## Componentes necesarios para iniciar la implementación

Antes de iniciar una implementación de DMZ de doble salto, asegúrese de tener los siguientes componentes:

- Como mínimo, deben estar disponibles dos dispositivos NetScaler Gateway (uno para cada DMZ).
- Los servidores que ejecutan Citrix Virtual Apps™ deben estar instalados y operativos en la red interna.
- StoreFront™ debe instalarse en la segunda DMZ y configurarse para funcionar con la granja de servidores de la red interna.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Como mínimo, se debe instalar un certificado de servidor SSL en NetScaler Gateway en la primera DMZ. Este certificado garantiza que el navegador web y las conexiones de usuario a NetScaler Gateway estén cifradas.

  Necesita certificados adicionales si desea cifrar las conexiones que se producen entre los demás componentes en una implementación de DMZ de doble salto.

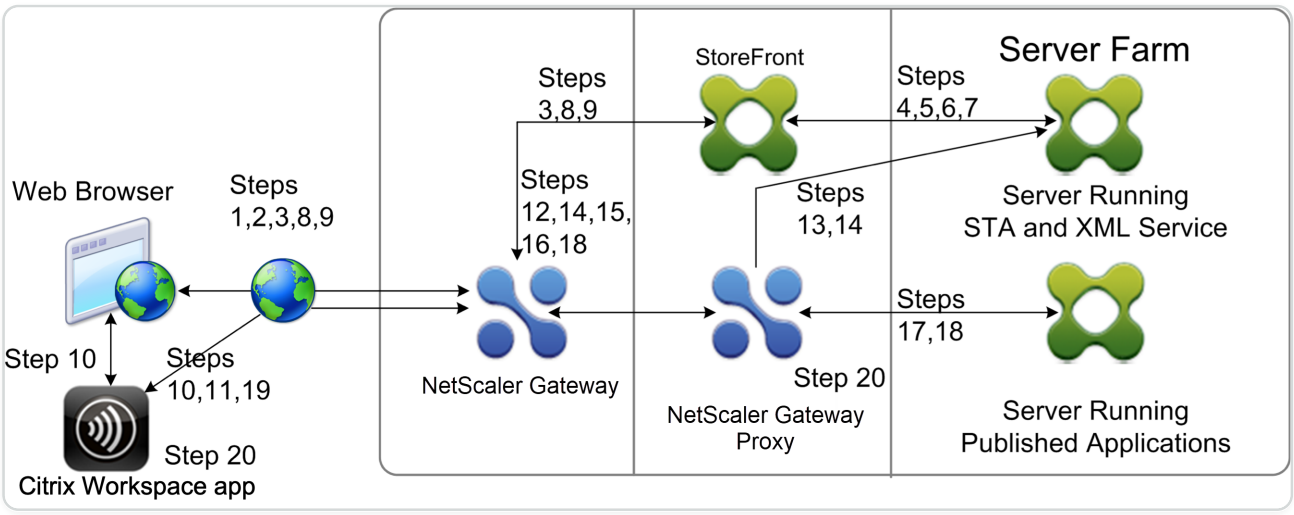
## Flujo de comunicación en una implementación de DMZ de doble salto

Para comprender los problemas de configuración que implica una implementación de DMZ de doble salto, debe tener una comprensión básica de cómo se comunican los diversos componentes de NetScaler Gateway y Citrix Virtual Apps en una implementación de DMZ de doble salto para admitir una conexión de usuario.

El proceso de conexión del usuario a StoreFront™ se produce en un flujo continuo. Los siguientes pasos de alto nivel están involucrados en el proceso.

- Autenticar usuarios
- Crear un ticket de sesión
- Iniciar la aplicación Citrix Workspace
- Completar la conexión

La siguiente figura muestra los pasos que ocurren en el proceso de conexión del usuario a StoreFront. En la red segura, los equipos que ejecutan Citrix Virtual Apps™ también ejecutan Secure Ticket Authority (STA), XML Service y las aplicaciones publicadas.

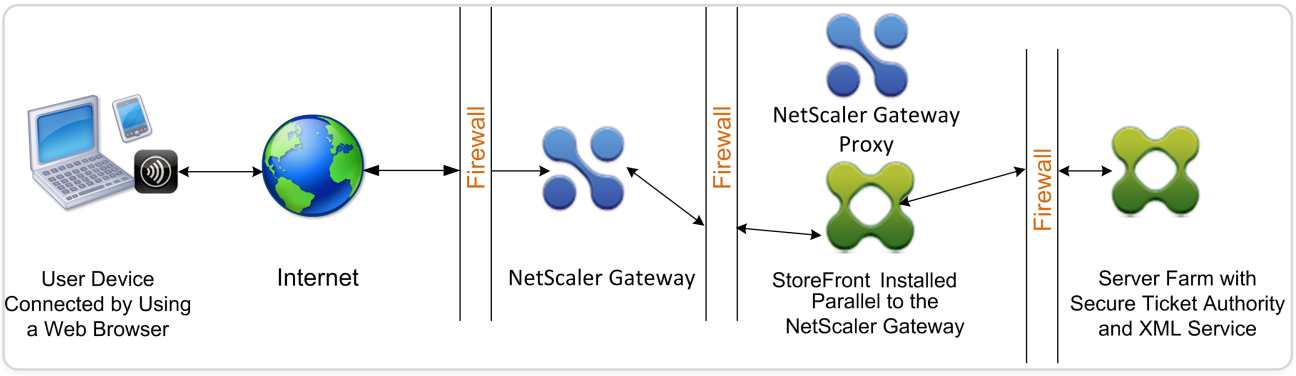



© 1997–2026 Citrix Systems, Inc. All rights reserved.

## Proceso de conexión

**La autenticación de usuarios es el primer paso del proceso de conexión de usuario en una implementación de DMZ de doble salto.**

La siguiente figura muestra el proceso de conexión del usuario en esta implementación.




Durante la etapa de autenticación del usuario, ocurre el siguiente proceso básico:

1. Un usuario escribe la dirección de NetScaler Gateway, como `<https://www.ng.wxyco.com>` en un navegador web para conectarse a NetScaler Gateway en la primera DMZ. Si ha habilitado la autenticación de la página de inicio de sesión en NetScaler Gateway, NetScaler Gateway autentica al usuario.
2. NetScaler Gateway en la primera DMZ recibe la solicitud.
3. NetScaler Gateway redirige la conexión del explorador web a StoreFront.
4. StoreFront envía las credenciales de usuario al servicio XML de Citrix® que se ejecuta en la granja de servidores de la red interna.
5. El servicio XML de Citrix autentica al usuario.
6. El servicio XML crea una lista de las aplicaciones publicadas a las que el usuario está autorizado a acceder y envía esta lista a StoreFront.

   **Nota:**

   - Si habilita la autenticación en NetScaler Gateway, el dispositivo envía la página de inicio de sesión de NetScaler Gateway al usuario. El usuario introduce las credenciales de autenticación en la página de inicio de sesión y el dispositivo autentica al usuario. NetScaler Gateway devuelve las credenciales de usuario a StoreFront.
   - Si no habilita la autenticación, NetScaler Gateway no realiza la autenticación. El dispositivo se conecta a StoreFront, recupera la página de inicio de sesión de StoreFront y la envía al usuario. El usuario introduce las credenciales de autenticación en la página de inicio de

© 1997–2026 Citrix Systems, Inc. All rights reserved.

sesión de StoreFront y NetScaler Gateway devuelve las credenciales de usuario a StoreFront.

**La creación del tíquet de sesión es la segunda etapa del proceso de conexión de usuario en una implementación de DMZ de doble salto.**

Durante la etapa de creación del tíquet de sesión, se produce el siguiente proceso básico:

7. StoreFront se comunica con el servicio XML y la Secure Ticket Authority (STA) en la red interna para producir tíquets de sesión para cada una de las aplicaciones publicadas a las que el usuario está autorizado a acceder. El tíquet de sesión contiene una dirección de alias para el equipo que ejecuta Citrix Virtual Apps que aloja una aplicación publicada.
8. La STA guarda las direcciones IP de los servidores que alojan las aplicaciones publicadas. A continuación, la STA envía los tíquets de sesión solicitados a StoreFront. Cada tíquet de sesión incluye un alias que representa la dirección IP del servidor que aloja la aplicación publicada, pero no la dirección IP real.
9. StoreFront genera un archivo ICA® para cada una de las aplicaciones publicadas. El archivo ICA contiene el tíquet emitido por la STA. A continuación, StoreFront crea y rellena una página web con una lista de enlaces a las aplicaciones publicadas y envía esta página web al explorador web del dispositivo de usuario.

   El inicio de Citrix Workspace app es la tercera etapa del proceso de conexión de usuario en una implementación de DMZ de doble salto. El proceso básico es el siguiente:

10. El usuario hace clic en un enlace a una aplicación publicada en StoreFront. StoreFront envía el archivo ICA de esa aplicación publicada al explorador del dispositivo de usuario.

    El archivo ICA contiene datos que instruyen al navegador web para iniciar Receiver.

    El archivo ICA también contiene el nombre de dominio completo (FQDN) o el nombre del sistema de nombres de dominio (DNS) de NetScaler Gateway en la primera DMZ.
11. El navegador web inicia Receiver y el usuario se conecta a NetScaler Gateway en la primera DMZ utilizando el nombre de NetScaler Gateway en el archivo ICA. Se produce un intercambio de información inicial SSL/TLS para establecer la identidad del servidor que ejecuta NetScaler Gateway.

    **Completar la conexión es la cuarta y última etapa del proceso de conexión del usuario en una implementación de DMZ de doble salto.**

    Durante la etapa de finalización de la conexión, se produce el siguiente proceso básico:

    - El usuario hace clic en un enlace a una aplicación publicada en StoreFront.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- El navegador web recibe el archivo ICA generado por StoreFront e inicia la aplicación Citrix Workspace. Nota: El archivo ICA contiene código que instruye al navegador web para iniciar la aplicación Citrix Workspace.
- La aplicación Citrix Workspace inicia una conexión ICA a NetScaler Gateway en la primera DMZ.
- NetScaler Gateway en la primera DMZ se comunica con la Secure Ticket Authority (STA) en la red interna para resolver la dirección de alias en el ticket de sesión a la dirección IP real de un equipo que ejecuta Citrix Virtual Apps o StoreFront. Esta comunicación se proxy a través de la segunda DMZ por el proxy de NetScaler Gateway.
- NetScaler Gateway en la primera DMZ completa la conexión ICA a la aplicación Citrix Workspace.
- La aplicación Citrix Workspace ahora puede comunicarse a través de ambos dispositivos NetScaler Gateway con el equipo que ejecuta Citrix Virtual Apps en la red interna.

Los pasos detallados para completar el proceso de conexión del usuario son los siguientes:

12. La aplicación Citrix Workspace envía el ticket STA para la aplicación publicada a NetScaler Gateway en la primera DMZ.
13. NetScaler Gateway en la primera DMZ se pone en contacto con la STA en la red interna para la validación del ticket. Para ponerse en contacto con la STA, NetScaler Gateway establece una conexión SOCKS o SOCKS con SSL al proxy de NetScaler Gateway en la segunda DMZ.
14. El proxy de NetScaler Gateway en la segunda DMZ pasa la solicitud de validación del ticket a la STA en la red interna. La STA valida el ticket y lo asigna al equipo que ejecuta Citrix Virtual Apps que aloja la aplicación publicada.
15. El STA envía una respuesta al proxy de NetScaler Gateway en la segunda DMZ, que se pasa a NetScaler Gateway en la primera DMZ. Esta respuesta completa la validación del ticket e incluye la dirección IP del equipo que aloja la aplicación publicada.
16. NetScaler Gateway en la primera DMZ incorpora la dirección del servidor de Citrix Virtual Apps en el paquete de conexión del usuario y envía este paquete al proxy de NetScaler Gateway en la segunda DMZ.
17. El proxy de NetScaler Gateway en la segunda DMZ realiza una solicitud de conexión al servidor especificado en el paquete de conexión.
18. El servidor responde al proxy de NetScaler Gateway en la segunda DMZ. El proxy de NetScaler Gateway en la segunda DMZ pasa esta respuesta a NetScaler Gateway en la primera DMZ para completar la conexión entre el servidor y NetScaler Gateway en la primera DMZ.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

19. NetScaler Gateway en la primera DMZ completa el protocolo de enlace SSL/TLS con el dispositivo de usuario pasando el paquete de conexión final al dispositivo de usuario. Se establece la conexión desde el dispositivo de usuario al servidor.
20. El tráfico ICA fluye entre el dispositivo de usuario y el servidor a través de NetScaler Gateway en la primera DMZ y el proxy de NetScaler Gateway en la segunda DMZ.

# Instalación y configuración de NetScaler Gateway en una DMZ de doble salto

Debe completar varios pasos para implementar NetScaler Gateway en una DMZ de doble salto. Los pasos incluyen la instalación de dispositivos en ambas DMZ y la configuración de los dispositivos para las conexiones de los usuarios.

## Instalar NetScaler Gateway en la primera DMZ

Para instalar NetScaler Gateway en la primera DMZ, siga las instrucciones de Instalar el hardware.

Si va a instalar varios dispositivos NetScaler Gateway en la primera DMZ, puede implementar los dispositivos detrás de un equilibrador de carga.

## Configurar NetScaler Gateway en la primera DMZ

En una implementación de DMZ de doble salto, es obligatorio configurar cada NetScaler Gateway en la primera DMZ para redirigir las conexiones a StoreFronte en la segunda DMZ.

La redirección a StoreFront se realiza a nivel global de NetScaler Gateway o a nivel de servidor virtual. Para conectarse a StoreFront a través de NetScaler Gateway, un usuario debe estar asociado a un grupo de usuarios de NetScaler Gateway para el que esté habilitada la redirección a StoreFront.

## Instalar NetScaler Gateway en la segunda DMZ

El dispositivo NetScaler Gateway en la segunda DMZ se denomina proxy de NetScaler Gateway porque actúa como proxy del tráfico ICA y Secure Ticket Authority (STA) a través de la segunda DMZ. Instalar el hardware para instalar cada dispositivo NetScaler Gateway en la segunda DMZ.

Puede utilizar este procedimiento de instalación para instalar otros dispositivos en la segunda DMZ.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Después de instalar los dispositivos NetScaler Gateway en la segunda DMZ, configure los siguientes ajustes:

- Configure un servidor virtual en el proxy de NetScaler Gateway.
- Configure los dispositivos NetScaler Gateway en la primera y segunda DMZ para que se comuniquen entre sí.
- Enlace el NetScaler Gateway en la segunda DMZ globalmente o a un servidor virtual.
- Configure el STA en el dispositivo de la primera DMZ.
- Abra los puertos en los firewalls que separan la DMZ.
- Instale los certificados en los dispositivos.

## Configurar ajustes en los servidores virtuales del proxy de NetScaler Gateway

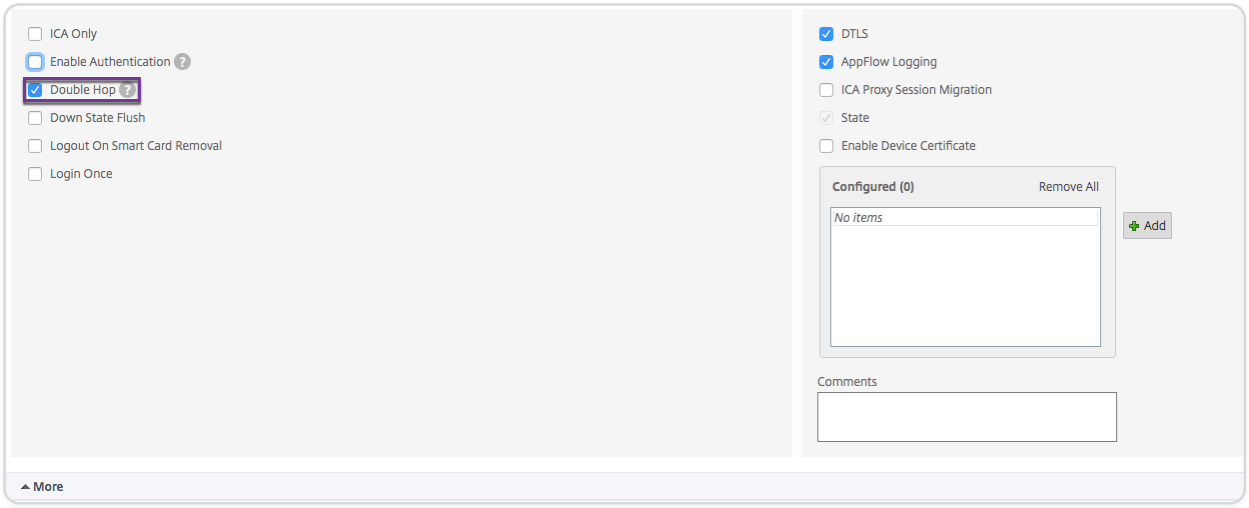
Para permitir que las conexiones pasen entre los dispositivos NetScaler Gateway, habilite el doble salto en el servidor virtual del proxy de NetScaler Gateway.

Cuando los usuarios se conectan, el dispositivo NetScaler Gateway autentica a los usuarios y luego envía la conexión al dispositivo proxy. En el NetScaler Gateway de la primera DMZ, configure el servidor virtual para que se comunique con NetScaler Gateway en la segunda DMZ. No configure la autenticación ni las directivas en el proxy de NetScaler Gateway. Citrix recomienda deshabilitar la autenticación en el servidor virtual.

### Para habilitar el doble salto en el servidor virtual del proxy de NetScaler Gateway mediante la GUI

1. Vaya a **Configuration > NetScaler Gateway > Virtual Servers**.
2. Seleccione un servidor virtual y haga clic en **Editar**.
3. En la sección **Basic Settings**, haga clic en el icono de edición y, a continuación, haga clic en **More**.
4. Seleccione **Double Hop**.

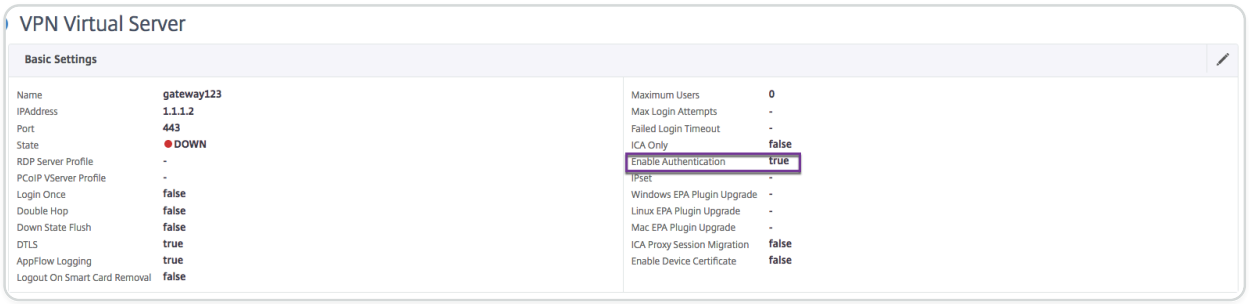
© 1997–2026 Citrix Systems, Inc. All rights reserved.



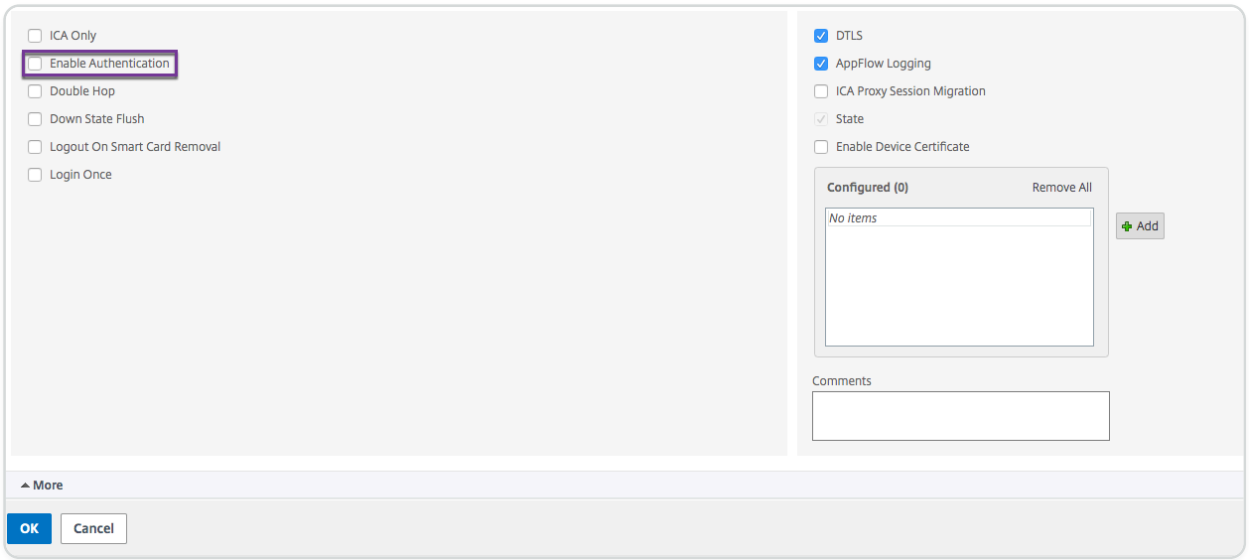

5. Haga clic en **OK**.

## Para deshabilitar la autenticación en el servidor virtual del proxy de NetScaler Gateway mediante la GUI

1. Vaya a **Configuration > NetScaler Gateway > Virtual Servers**.
2. Seleccione un servidor virtual y haga clic en **Editar**.
3. En la sección **Basic Settings**, haga clic en el icono de edición y, a continuación, haga clic en **More**.




4. Desactive la casilla de verificación **Habilitar autenticación**.




© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. Haga clic en **Aceptar**.

## Configurar el dispositivo para que se comunique con el proxy del dispositivo

Cuando implementa NetScaler Gateway en una DMZ de doble salto, debe configurar NetScaler Gateway en la primera DMZ para que se comunique con el proxy de NetScaler Gateway en la segunda DMZ.

Si implementa varios dispositivos en la segunda DMZ, configure cada dispositivo de la primera DMZ para que se comunique con todos los dispositivos proxy de la segunda DMZ.

Nota: Si desea utilizar IPv6, configure el servidor de salto siguiente mediante la utilidad de configuración. Para ello, expanda NetScaler Gateway \> Recursos y, a continuación, haga clic en Servidores de salto siguiente. Siga los pasos del siguiente procedimiento y, a continuación, seleccione la casilla de verificación IPv6.

### Para configurar NetScaler Gateway para que se comunique con el proxy de NetScaler Gateway

1. En la utilidad de configuración, en la ficha Configuración, expanda NetScaler Gateway \> Recursos y, a continuación, haga clic en Servidores de salto siguiente.
2. En el panel de detalles, haga clic en Agregar.
3. En Nombre, escriba un nombre para el primer NetScaler Gateway.
4. En Dirección IP, escriba la dirección IP del servidor virtual del proxy de NetScaler Gateway en la segunda DMZ.
5. En Puerto, escriba el número de puerto, haga clic en Crear y, a continuación, haga clic en Cerrar. Si utiliza un puerto seguro, como el 443, seleccione Seguro.

Debe configurar cada NetScaler Gateway instalado en la primera DMZ para que se comunique con todos los dispositivos proxy de NetScaler Gateway instalados en la segunda DMZ.

Después de configurar los ajustes para el proxy de NetScaler Gateway, vincule la directiva a los servidores de salto siguiente en NetScaler Gateway Global o a un servidor virtual.

### Para vincular globalmente el servidor de salto siguiente de NetScaler Gateway

1. En la utilidad de configuración, en la ficha Configuración, expanda NetScaler Gateway \> Recursos y, a continuación, haga clic en Servidores de salto siguiente.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. En el panel de detalles, seleccione un servidor de salto siguiente y, a continuación, en Acción, seleccione Enlaces globales.
3. En el cuadro de diálogo Configurar enlace global del servidor de siguiente salto, en Nombre del servidor de siguiente salto, seleccione el dispositivo proxy y, a continuación, haga clic en Aceptar.

### Para enlazar el servidor de siguiente salto de NetScaler Gateway a un servidor virtual

1. En la utilidad de configuración, en la ficha Configuración, expanda NetScaler Gateway y, a continuación, haga clic en Servidores virtuales.
2. En el panel de detalles, seleccione un servidor virtual y, a continuación, haga clic en Abrir.
3. En la ficha Aplicaciones publicadas, en Servidores de siguiente salto, haga clic en un elemento y, a continuación, haga clic en Aceptar.

También puede agregar un servidor de siguiente salto desde la ficha Aplicaciones publicadas.

## Configurar NetScaler Gateway para gestionar el tráfico STA e ICA

Cuando implementa NetScaler Gateway en una DMZ de doble salto, debe configurar NetScaler Gateway en la primera DMZ para gestionar las comunicaciones con la Autoridad de tickets seguros (STA) y el tráfico ICA de forma adecuada. El servidor que ejecuta la STA se puede enlazar globalmente o a un servidor virtual.

Después de configurar la STA, puede enlazarla globalmente o a un servidor virtual.

Para configurar y enlazar la STA globalmente:

1. En la GUI, en la ficha Configuration, expanda **NetScaler Gateway** y, a continuación, haga clic en **Global Settings**.
2. En el panel de detalles, en **Servers**, haga clic en **Bind/Unbind STA Servers to be used by the Secure Ticket Authority**.
3. En el cuadro de diálogo **Bind/Unbind STA Servers**, haga clic en **Add**.
4. En el cuadro de diálogo **Configure STA Server**, en **URL**, escriba la ruta al servidor que ejecuta la STA, como `<http://mycompany.com>` o `<http://ipAddress>` y, a continuación, haga clic en **Create**.

Para configurar y enlazar la STA a un servidor virtual:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. En la GUI, en la ficha Configuration, expanda **NetScaler Gateway** y, a continuación, haga clic en **Virtual Servers**.
2. En el panel de detalles, seleccione un servidor virtual y, a continuación, haga clic en **Open**.
3. En la ficha **Published Applications**, en **Secure Ticket Authority**, haga clic en **Add**.
4. En el cuadro de diálogo **Configure STA Server**, en URL, escriba la ruta al servidor que ejecuta la STA, como `<http://mycompany.com>` o `<http://ipAddress>` y, a continuación, haga clic en **Create**.

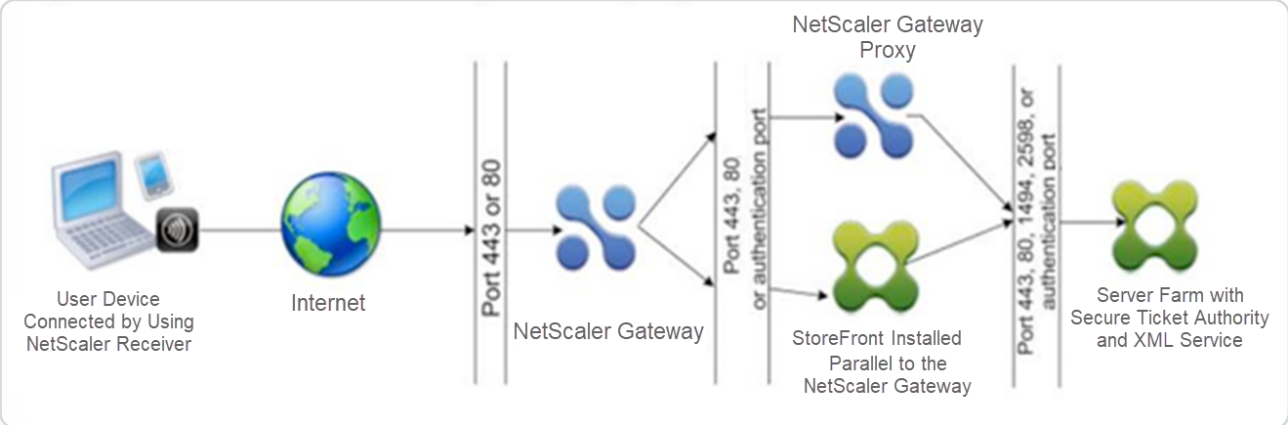
**Nota:**

Si los servidores virtuales VPN comparten el mismo servidor virtual de siguiente salto y los mismos servidores STA, la conexión se restablece cuando el servidor STA común se desvincula de un servidor virtual que comparte el mismo servidor virtual de siguiente salto.

## Abrir los puertos adecuados en los firewalls

Debe asegurarse de que los puertos adecuados estén abiertos en los firewalls para admitir las diferentes conexiones que se producen entre los diversos componentes implicados en una implementación de DMZ de doble salto. Para obtener más información sobre el proceso de conexión y comunicación, consulte Flujo de comunicación en una implementación de DMZ de doble salto.

La siguiente figura muestra los puertos comunes que se pueden utilizar en una implementación de DMZ de doble salto.




La siguiente tabla muestra las conexiones que se producen a través del primer firewall y los puertos que deben estar abiertos para admitir las conexiones.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| CONEXIONES A TRAVÉS DEL PRIMER FIREWALL | PUERTOS UTILIZADOS |
|---|---|
| El navegador web de Internet se conecta a NetScaler Gateway en la primera DMZ. **Nota:** NetScaler Gateway incluye una opción para redirigir las conexiones realizadas en el puerto 80 a un puerto seguro. Si habilita esta opción en NetScaler Gateway, puede abrir el puerto 80 a través del primer firewall. Cuando un usuario realiza una conexión no cifrada a NetScaler Gateway en el puerto 80, NetScaler Gateway redirige automáticamente la conexión a un puerto seguro. | Abra el puerto TCP 443 a través del primer firewall. |
| Citrix Workspace app de Internet se conecta a NetScaler Gateway en la primera DMZ. | Abra el puerto TCP 443 a través del primer firewall. |

La siguiente tabla muestra las conexiones que se producen a través del segundo firewall y los puertos que deben estar abiertos para admitir las conexiones.

| CONEXIONES A TRAVÉS DEL SEGUNDO FIREWALL | PUERTOS UTILIZADOS |
|---|---|
| NetScaler Gateway en la primera DMZ se conecta a StoreFront en la segunda DMZ. | Abra el puerto TCP 80 para una conexión no segura o el puerto TCP 443 para una conexión segura a través del segundo firewall. |
| NetScaler Gateway en la primera DMZ se conecta a NetScaler Gateway en la segunda DMZ. | Abra el puerto TCP 443 para una conexión SOCKS segura a través del segundo firewall. |
| Si habilitó la autenticación en NetScaler Gateway en la primera DMZ, este dispositivo podría necesitar conectarse a un servidor de autenticación en la red interna. | Abra el puerto TCP en el que el servidor de autenticación escucha las conexiones. Los ejemplos incluyen el puerto 1812 para RADIUS y el puerto 389 para LDAP. |

La siguiente tabla muestra las conexiones que se producen a través del tercer firewall y los puertos que deben estar abiertos para admitir las conexiones.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| CONEXIONES A TRAVÉS DEL TERCER FIREWALL | PUERTOS UTILIZADOS |
|---|---|
| StoreFront en la segunda DMZ se conecta al servicio XML alojado en un servidor de la red interna. | Abra el puerto 80 para una conexión no segura o el puerto 443 para una conexión segura a través del tercer firewall. |
| StoreFront en la segunda DMZ se conecta a la Secure Ticket Authority (STA) alojada en un servidor de la red interna. | Abra el puerto 80 para una conexión no segura o el puerto 443 para una conexión segura a través del tercer firewall. |
| NetScaler Gateway en la segunda DMZ se conecta a la STA que reside en la red segura. | Abra el puerto 80 para una conexión no segura o el puerto 443 para una conexión segura a través del tercer firewall. |
| NetScaler Gateway en la segunda DMZ establece una conexión ICA con una aplicación publicada o un escritorio virtual en un servidor de la red interna. | Abra el puerto TCP 1494 para admitir conexiones ICA a través del tercer firewall. Si habilitó la fiabilidad de la sesión en Citrix Virtual Apps, abra el puerto TCP 2598 en lugar del 1494. |
| Si habilitó la autenticación en NetScaler Gateway en la primera DMZ, este dispositivo podría necesitar conectarse a un servidor de autenticación en la red interna. | Abra el puerto TCP en el que el servidor de autenticación escucha las conexiones. Algunos ejemplos son el puerto 1812 para RADIUS y el puerto 389 para LDAP. |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

# Mantenimiento y monitorización del sistema

Una vez que complete la configuración de su NetScaler Gateway, deberá realizar el mantenimiento y la monitorización del dispositivo. Puede hacerlo de las siguientes maneras:

- Puede actualizar NetScaler Gateway a la última versión del software. Cuando inicie sesión en el sitio web de Citrix, puede navegar al sitio de descarga de NetScaler Gateway y descargar el software. Puede encontrar el archivo Léame para las compilaciones de mantenimiento en el Citrix Knowledge Center.
- Puede asignar tareas de configuración y administración de NetScaler Gateway a diferentes miembros de su grupo. Con la administración delegada, puede asignar niveles de acceso a los individuos que los restringen a realizar tareas específicas en NetScaler Gateway.
- Puede guardar la configuración de NetScaler Gateway ya sea en el dispositivo o en un archivo de su equipo. Puede comparar la configuración actual en ejecución y la guardada. También puede borrar la configuración de NetScaler Gateway.
- Puede ver, actualizar y finalizar sesiones de usuario dentro de la utilidad de configuración de NetScaler Gateway.
- Puede configurar el registro en NetScaler Gateway. Los registros proporcionan información importante sobre el dispositivo y son útiles en caso de que experimente problemas.

## Configuración de administradores delegados

NetScaler Gateway tiene un nombre de usuario y una contraseña de administrador predeterminados. El nombre de usuario y la contraseña predeterminados son `nsroot`. Cuando ejecuta el Asistente de configuración por primera vez, puede cambiar la contraseña del administrador.

Puede crear más cuentas de administrador y asignar a cada cuenta diferentes niveles de acceso a NetScaler Gateway. Estas cuentas adicionales se denominan administradores delegados. Por ejemplo, tiene una persona asignada para supervisar las conexiones y los registros de NetScaler Gateway y otra persona responsable de configurar ajustes específicos en NetScaler Gateway. El primer administrador tiene acceso de solo lectura y el segundo administrador tiene acceso limitado al dispositivo.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Para configurar un administrador delegado, utilice directivas de comandos y usuarios y grupos del sistema.

Al configurar un administrador delegado, el proceso de configuración es el siguiente:

- Agregue un usuario del sistema. Un usuario del sistema es un administrador con privilegios específicos. Todos los administradores heredan las directivas de los grupos a los que pertenecen.
- Agregue un grupo del sistema. Un grupo del sistema contiene usuarios del sistema con privilegios específicos. Los miembros del grupo del sistema heredan las directivas del grupo o grupos a los que pertenecen.
- Cree una directiva de comandos. Las directivas de comandos le permiten definir qué partes de la configuración de NetScaler Gateway puede acceder y modificar un usuario o grupo. También puede regular qué comandos, como grupos de comandos, servidores virtuales y otros elementos, los administradores y grupos pueden configurar.
- Enlace la directiva de comandos al usuario o grupo estableciendo la prioridad. Al configurar la administración delegada, asigne prioridades al administrador o grupo para que NetScaler Gateway pueda determinar qué directiva tiene precedencia.

NetScaler Gateway tiene una directiva de comandos del sistema de denegación predeterminada. Las directivas de comandos no se pueden vincular globalmente. Enlace las directivas directamente a los administradores (usuarios) o grupos del sistema. Si los usuarios y grupos no tienen una directiva de comandos asociada, se aplica la directiva de denegación predeterminada y los usuarios no pueden ejecutar ningún comando ni configurar NetScaler Gateway.

Puede configurar directivas de comandos personalizadas para definir un mayor nivel de detalle para las asignaciones de derechos de usuario. Por ejemplo, puede dar a una persona la capacidad de agregar directivas de sesión a NetScaler Gateway, pero no permitir que el usuario realice ninguna otra configuración.

## Configuración de directivas de comandos para administradores delegados

NetScaler Gateway tiene cuatro directivas de comandos integradas que puede utilizar para la administración delegada:

- **Solo lectura** permite el acceso de solo lectura para mostrar todos los comandos, excepto el grupo de comandos del sistema y los comandos `ns.conf show`.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Operador** permite el acceso de solo lectura y también permite el acceso para habilitar y deshabilitar comandos en los servicios. Esta directiva también permite el acceso para establecer servicios y servidores como "acceso inactivo".
- **Red** permite un acceso casi completo al sistema, excluyendo los comandos del sistema y el comando de shell.
- **Superusuario** concede privilegios de sistema completos, como los privilegios concedidos al administrador predeterminado, `nsroot`.

Las directivas de comandos contienen expresiones integradas. Utilice la utilidad de configuración para crear usuarios del sistema, grupos del sistema, directivas de comandos y para definir permisos.

### Para crear un usuario administrativo en NetScaler Gateway

1. En la utilidad de configuración, en el panel de navegación, en la ficha **Configuración**, expanda **Sistema** > **Administración de usuarios** y, a continuación, haga clic en **Usuarios del sistema**.
2. En el panel de detalles, haga clic en **Agregar**.
3. En **Nombre de usuario**, escriba un nombre de usuario.
4. En los campos **Contraseña** y **Confirmar contraseña**, escriba la contraseña.
5. Para agregar usuarios a un grupo, en **Miembro de**, haga clic en **Agregar**.
6. En **Disponible**, seleccione un grupo y, a continuación, haga clic en la flecha derecha.
7. Haga clic en **Directivas de comandos > Acción > Insertar**.
8. En el cuadro de diálogo Insertar directivas de comandos, seleccione el comando, haga clic en **Aceptar > Crear > Cerrar**.

### Creación de grupos administrativos

Los grupos administrativos contienen usuarios que tienen privilegios administrativos en NetScaler Gateway. Puede crear grupos administrativos en la utilidad de configuración.

#### Para configurar un grupo administrativo mediante la utilidad de configuración

1. En la utilidad de configuración, en el panel de navegación, en la ficha **Configuración**, expanda **Sistema** > **Administración de usuarios** y, a continuación, haga clic en **Grupos del sistema**.
2. En el panel de detalles, haga clic en **Agregar**.
3. En **Nombre de grupo**, escriba un nombre para el grupo.
4. Para agregar un usuario existente al grupo, en **Miembros**, haga clic en **Agregar**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. En **Disponible**, seleccione un usuario y, a continuación, haga clic en la flecha derecha.
6. En **Directivas de comandos**, en **Acción**, haga clic en **Insertar**, seleccione una o varias directivas, haga clic en **Aceptar**, haga clic en **Crear** y, a continuación, haga clic en **Cerrar**.

## Configuración de directivas de comandos personalizadas para administradores delegados

Al configurar una directiva de comandos personalizada, proporcione un nombre de directiva y, a continuación, configure los componentes de la directiva para crear la especificación de comandos. Con la especificación de comandos, puede limitar los comandos que los administradores pueden usar. Por ejemplo, si desea denegar a los administradores la capacidad de usar el comando de eliminación. Al configurar la directiva, establezca la acción en denegar y, a continuación, configure los parámetros.

Puede configurar una directiva de comandos simple o avanzada. Al configurar una directiva simple, se configura un componente en el dispositivo, como NetScaler Gateway y la autenticación. Al configurar una directiva avanzada, se selecciona el componente, denominado grupo de entidades, y, a continuación, se seleccionan los comandos que los administradores pueden realizar en el grupo.

### Para crear una directiva de comandos personalizada simple

1. En la utilidad de configuración, en la ficha **Configuración**, en el panel de navegación, expanda **Sistema** > **Administración de usuarios** y, a continuación, haga clic en **Directivas de comandos.**
2. En el panel de detalles, haga clic en **Agregar.**
3. En **Nombre de directiva**, escriba un nombre para la directiva.
4. En **Acción**, seleccione **Permitir** o **Denegar**.
5. En **Especificación de comandos**, haga clic en **Agregar**.
6. En el cuadro de diálogo **Agregar comando**, en la ficha **Simple**, en Operación, seleccione la acción que pueden realizar los administradores delegados.
7. En **Grupo de entidades**, seleccione uno o varios grupos.

   Puede pulsar la tecla CTRL para seleccionar varios grupos.
8. Haga clic en **Crear** y, a continuación, haga clic en **Cerrar**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

### Para crear una directiva de comandos personalizada avanzada

1. En la utilidad de configuración, en el panel de navegación, en la ficha **Configuración**, expanda **Sistema** > **Administración de usuarios** y, a continuación, haga clic en **Directivas de comandos**.
2. En el panel de detalles, haga clic en **Agregar**.
3. En **Nombre de la directiva**, escriba un nombre para la directiva.
4. En **Acción**, seleccione **Permitir** o **Denegar**.
5. En **Especificación de comando**, haga clic en **Agregar**.
6. En el cuadro de diálogo **Agregar comando**, haga clic en la ficha **Avanzado**.
7. En **Grupo de entidades**, seleccione el grupo al que pertenece el comando, como autenticación o alta disponibilidad.
8. En **Entidad**, seleccione la directiva.

   Puede pulsar la tecla CTRL para seleccionar varios elementos de la lista.
9. En **Operación**, seleccione el comando, haga clic en **Crear** y, a continuación, haga clic en **Cerrar**.

   Puede pulsar la tecla CTRL para seleccionar varios elementos de la lista.
10. Haga clic en **Crear** y, a continuación, haga clic en **Cerrar**.
11. En el cuadro de diálogo **Crear directiva de comandos**, haga clic en **Crear** y, a continuación, haga clic en **Cerrar**.

Al hacer clic en **Crear**, la expresión aparece en Especificación de comando en el cuadro de diálogo **Crear directiva de comandos**.

Después de crear la directiva de comandos personalizada, puede vincularla a un usuario o a un grupo.

**Nota**: Solo puede vincular directivas de comandos personalizadas a los usuarios o grupos que cree. No puede vincular una directiva de comandos personalizada al usuario `nsroot`.

### Para vincular una política de comandos personalizada a un usuario o grupo

1. En la utilidad de configuración, en la ficha **Configuración**, en el panel de navegación, expanda **Sistema** > **Administración de usuarios** y, a continuación, haga clic en **Usuarios del sistema** o en **Grupos del sistema**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. En el panel de detalles, seleccione un usuario o grupo de la lista y, a continuación, haga clic en **Abrir**.
3. En **Políticas de comandos**, seleccione la política y, a continuación, haga clic en **Aceptar**.

# Configuración de auditoría en NetScaler Gateway

NetScaler Gateway le permite registrar los estados y la información de estado que recopila el dispositivo. Puede utilizar los registros de auditoría para ver el historial de eventos en orden cronológico. Los mensajes dentro de los registros contienen información sobre el evento que generó el mensaje, una marca de tiempo, el tipo de mensaje y los niveles de registro predefinidos e información del mensaje. Puede configurar los ajustes que determinan la información que se registra y la ubicación donde se almacenan los mensajes.

NetScaler Gateway actualmente admite 2 formatos de registro: un formato de registro propietario para registros locales y el formato syslog para usar con servidores syslog. Puede configurar los registros de auditoría para proporcionar la siguiente información:

| NIVEL | DESCRIPCIÓN |
|---|---|
| EMERGENCIA | Registra solo errores importantes. Las entradas en el registro indican que NetScaler Gateway está experimentando un problema crítico que lo hace inutilizable. |
| ALERTA | Registra problemas que podrían hacer que NetScaler Gateway funcione incorrectamente, pero que no son críticos para su funcionamiento. Se pueden tomar medidas correctivas lo antes posible para evitar que NetScaler Gateway experimente un problema crítico. |
| CRÍTICO | Registra condiciones críticas que no restringen el funcionamiento de NetScaler Gateway, pero que podrían escalar a un problema mayor. |
| ERROR | Registra entradas que resultan de una operación fallida en NetScaler Gateway. |
| ADVERTENCIA | Registra posibles problemas que pueden resultar en un error o un error crítico. |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| NIVEL | DESCRIPCIÓN |
| --- | --- |
| AVISO | Registra problemas más detallados que el registro de nivel de información, pero tiene el mismo propósito que una notificación. |
| INFORMACIÓN | Registra las acciones realizadas por NetScaler Gateway. Este nivel es útil para solucionar problemas. |

El registro de auditoría de NetScaler Gateway también almacena estadísticas de compresión para NetScaler Gateway si configura la compresión TCP. La relación de compresión lograda para diferentes datos se almacena en el archivo de registro para cada sesión de usuario.

NetScaler Gateway utiliza la firma de registro SessionID. Esto le permite rastrear los registros por sesión en lugar de por usuario. Los registros que se generan como parte de una sesión tienen el mismo SessionID. Si un usuario establece dos sesiones desde el mismo dispositivo de usuario con la misma dirección IP, cada sesión tiene un SessionID único.

**IMPORTANTE:**

Si ha escrito scripts de análisis de registros personalizados, debe realizar este cambio de firma dentro de los scripts de análisis personalizados.

## Configuración de registros en NetScaler Gateway

Al configurar el registro en NetScaler Gateway, puede optar por almacenar los registros de auditoría en NetScaler Gateway o enviarlos a un servidor Syslog. Utilice la utilidad de configuración para crear directivas de auditoría y configurar los ajustes para almacenar los registros de auditoría.

### Para crear una directiva de auditoría

1. En la utilidad de configuración, en la ficha Configuración, expanda **NetScaler Gateway** > **Directivas** > **Auditoría**.
2. En **Nombre**, escriba un nombre para la directiva.
3. Seleccione una de las siguientes opciones:
   - Syslog si desea enviar los registros a un servidor Syslog.
   - `Nslog` para almacenar los registros en NetScaler Gateway.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**NOTA:**

Si selecciona esta opción, los registros se almacenan en la carpeta /var/log del dispositivo.

4. En el panel de detalles, haga clic en **Agregar**.
5. Escriba la siguiente información para el servidor donde se almacenan los registros:
   - En Nombre, escriba el nombre del servidor.
   - En Servidor, escriba el nombre o la dirección IP del servidor de registros.
6. Haga clic en Crear y, a continuación, en Cerrar.

Después de crear la directiva de auditoría, puede vincularla a cualquier combinación de lo siguiente:

- Globalmente
- Servidores virtuales
- Grupos
- Usuarios

### Para vincular una directiva de auditoría globalmente

1. En la utilidad de configuración, en la ficha Configuración, expanda **NetScaler Gateway** > **Directivas** > **Auditoría**.
2. Seleccione `Syslog` o `Nslog`.
3. En el panel de detalles, haga clic en **Acción** y, a continuación, en **Enlaces globales**.
4. En el cuadro de diálogo **Vincular/Desvincular directivas de auditoría** a **Global**, en **Detalles**, haga clic en **Insertar directiva**.
5. En **Nombre de directiva**, seleccione una directiva y, a continuación, haga clic en **Aceptar**.

### Para modificar una directiva de auditoría

Puede modificar una directiva de auditoría existente para cambiar el servidor al que se envían los registros.

1. En la utilidad de configuración, en la ficha **Configuración**, expanda **NetScaler Gateway** > **Directivas** > **Auditoría**
2. Seleccione `Syslog` o `Nslog`.
3. En el panel de detalles, haga clic en una directiva y, a continuación, en **Abrir**.
4. En Servidor, seleccione el nuevo servidor y, a continuación, haga clic en **Aceptar**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

### Para eliminar una directiva de auditoría

Puede eliminar una directiva de auditoría de NetScaler Gateway. Al eliminar una directiva de auditoría, la directiva se desvincula automáticamente.

1. En la utilidad de configuración, en la ficha Configuración, expanda **NetScaler Gateway** > **Directivas** > **Auditoría**.
2. Seleccione **Syslog** o `Nslog`.
3. En el panel de detalles, haga clic en una directiva y, a continuación, haga clic en **Eliminar**.

## Configuración del registro de ACL

Puede configurar NetScaler Gateway para registrar detalles de los paquetes que coinciden con una lista de control de acceso (ACL) extendida. Además del nombre de la ACL, los detalles registrados incluyen información específica del paquete, como las direcciones IP de origen y destino. La información se almacena en un syslog o en un archivo `nslog`, según el tipo de registro (syslog o `nslog`) que habilite.

Puede habilitar el registro tanto a nivel global como a nivel de ACL. Sin embargo, para habilitar el registro a nivel de ACL, también debe habilitarlo a nivel global. La configuración global tiene prioridad.

Para optimizar el registro, cuando varios paquetes del mismo flujo coinciden con una ACL, solo se registran los detalles del primer paquete. El contador se incrementa para cada otro paquete que pertenece al mismo flujo. Un flujo se define como un conjunto de paquetes que tienen los mismos valores para los siguientes parámetros:

- IP de origen
- IP de destino
- Puerto de origen
- Puerto de destino
- Protocolo (TCP o UDP)

Si el paquete no es del mismo flujo, o si la duración excede el tiempo medio, se crea un nuevo flujo. El tiempo medio es el tiempo durante el cual los paquetes del mismo flujo no generan mensajes adicionales (aunque el contador se incrementa).

**NOTA:**

El número total de flujos diferentes que se pueden registrar en un momento dado está limitado a 10.000.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

La siguiente tabla describe los parámetros con los que puede configurar el registro de ACL a nivel de regla para ACL extendidas.

| NOMBRE DEL PARÁMETRO | DESCRIPCIÓN |
|---|---|
| `Logstate` | Estado de la función de registro para la ACL. Valores posibles: ENABLED y DISABLED. Predeterminado: DISABLED. |
| `Ratelimit` | Número de mensajes de registro que puede generar una ACL específica. Predeterminado: 100. |

### Para configurar el registro de ACL mediante la utilidad de configuración

Puede configurar el registro para una ACL y especificar el número de mensajes de registro que puede generar la regla.

1. En la utilidad de configuración, en el panel de navegación, expanda **Sistema** > **Red** y, a continuación, haga clic en ACL.
2. En el panel de detalles, haga clic en la ficha **ACL extendidas** y, a continuación, haga clic en Agregar.
3. En el cuadro de diálogo **Crear ACL extendida**, en Nombre, escriba un nombre para la directiva.
4. Seleccione la casilla de verificación **Estado de registro**.
5. En el cuadro de texto **Límite de velocidad de registro**, escriba el límite de velocidad que desea especificar para la regla y, a continuación, haga clic en **Crear**.

Después de configurar el registro de ACL, puede habilitarlo en NetScaler Gateway. Cree una directiva de auditoría y, a continuación, vincúlela a un usuario, grupo, servidor virtual o globalmente.

### Para habilitar el registro de ACL o TCP en NetScaler Gateway

1. En la utilidad de configuración, en el panel de navegación, expanda **NetScaler Gateway** > **Directivas** > **Auditoría**.
2. Seleccione syslog o `nslog`.
3. En la ficha **Servidores**, haga clic en **Agregar**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. En el cuadro de diálogo **Crear servidor de auditoría**, en **Nombre**, escriba un nombre para el servidor y, a continuación, configure los ajustes del servidor.
5. Haga clic en **Registro de ACL** o en **Registro de TCP** y, a continuación, haga clic en **Crear**.

## Habilitación del registro de Citrix Secure Access™

Puede configurar el cliente de Citrix Secure Access para que registre todos los errores en archivos de texto que se almacenan en el dispositivo del usuario. Los usuarios pueden configurar el cliente de Citrix Secure Access para establecer el nivel de registro en el dispositivo del usuario para registrar actividades de usuario específicas. Cuando los usuarios configuran el registro, el complemento crea los dos archivos siguientes en el dispositivo del usuario:

- hooklog\<num\>.txt, que registra los mensajes de intercepción que genera el cliente de Citrix Secure Access.
- nssslvpn.txt, que enumera los errores del complemento.

**NOTA**

. Los archivos hooklog.txt no se eliminan automáticamente. Citrix recomienda eliminar los archivos periódicamente.

Los registros de usuario se encuentran en los siguientes directorios de Windows en el dispositivo del usuario:

- Windows XP (todos los usuarios): %SystemDrive%:\\Documents and Settings\\All Users\ \Application Data\\Citrix\\AGEE
- Windows XP (específico del usuario): %SystemDrive%:\\Documents and Settings\\ %username%\\Local Settings\\Application Data\\Citrix\\AGEE
- Windows Vista (todos los usuarios): %SystemDrive%:\\ProgramData\\Citrix\\AGEE
- Windows Vista (específico del usuario): %SystemDrive%:\\Users\\%username%\\AppData\ \Local\\Citrix\\AGEE
- Windows 7 (todos los usuarios): %SystemDrive%:\\ProgramData\\Citrix\\AGEE
- Windows 7 (específico del usuario): %SystemDrive%:\\Users\\%username%\\AppData\\Local\ \Citrix\\AGEE
- Windows 8 (todos los usuarios): %SystemDrive%:\\ProgramData\\Citrix\\AGEE
- Windows 8 (específico del usuario): %SystemDrive%:\\Users\\%username%\\AppData\\Local\ \Citrix\\AGEE

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Puede usar estos archivos de registro para solucionar problemas del cliente de Citrix Secure Access. Los usuarios pueden enviar los archivos de registro por correo electrónico al Soporte técnico.

En el cuadro de diálogo Configuración, los usuarios pueden establecer el nivel de registro para el cliente Citrix Secure Access. Los niveles de registro son:

- Registrar mensajes de error
- Registrar mensajes de eventos
- Registrar estadísticas del cliente Citrix Secure Access
- Registrar todos los errores, mensajes de eventos y estadísticas

Para obtener más detalles sobre la función de registro del cliente Citrix Secure Access para Windows, consulte Recopilación de registros mejorada para el cliente de Windows.

# Para supervisar las conexiones ICA®

Puede supervisar las sesiones de usuario activas en su granja de servidores mediante el cuadro de diálogo Conexiones ICA. Este cuadro de diálogo proporciona la siguiente información:

- Nombre de usuario de la persona que se conecta a la granja de servidores
- Nombre de dominio de la granja de servidores
- Dirección IP del dispositivo de usuario
- Número de puerto del dispositivo de usuario
- Dirección IP del servidor que ejecuta Citrix Virtual Apps and Desktops
- Número de puerto del servidor que ejecuta Citrix Virtual Apps and Desktops

1. Vaya a **Configuración > NetScaler Gateway**.
2. En la sección **Supervisar conexiones**, haga clic en **Conexiones ICA**.

## Registros de sesión ICA

El archivo `ns.log` imprime los registros de sesión ICA en el siguiente formato:

```
May  2 09:29:02 <local0.info> 10.106.40.223  05/02/2023:09:29:02 GMT  0-
PPE-1 : default ICA Message 141327 0 :  "[Remote ip = 10.10.99.86:514]
[EDT] [CGP][ICAUUID=0006ab3454-d7de-1450-9678-c6333447a76] Received
response from STA server {sta-server=10.11.40.222:80,type=ResponseData}"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

A partir de la versión 13.1 compilación 50.x, se han realizado las siguientes mejoras en los registros ICA:

- Muestra tipos de conexión como TCP, EDT, CGP y SOCKS.
- Muestra el identificador único universal (UUID) de ICA.
- Todos los registros STA se muestran como registros de nivel de información.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

# Autenticación y autorización

NetScaler Gateway emplea un diseño de autenticación flexible que permite una amplia personalización de la autenticación de usuarios para NetScaler Gateway. Puede utilizar servidores de autenticación estándar del sector y configurar NetScaler Gateway para autenticar usuarios con los servidores. NetScaler Gateway también admite la autenticación basada en atributos presentes en un certificado de cliente. La autenticación de NetScaler Gateway está diseñada para adaptarse a procedimientos de autenticación simples que utilizan una única fuente para la autenticación de usuarios, y a procedimientos de autenticación en cascada más complejos que se basan en varios tipos de autenticación.

La autenticación de NetScaler Gateway incorpora la autenticación local para la creación de usuarios y grupos locales. Este diseño se centra en el uso de directivas para controlar los procedimientos de autenticación que configure. Las directivas que cree se pueden aplicar a nivel global de NetScaler Gateway o a nivel de servidor virtual y se pueden utilizar para establecer parámetros del servidor de autenticación condicionalmente en función de la red de origen del usuario.

Dado que las directivas están vinculadas globalmente o a un servidor virtual, también puede asignar prioridades a sus directivas para crear una cascada de varios servidores de autenticación como parte de la autenticación.

NetScaler Gateway incluye soporte para los siguientes tipos de autenticación.

- Local
- Protocolo ligero de acceso a directorios (LDAP)
- RADIUS
- SAML
- TACACS+
- Autenticación de certificado de cliente (incluida la autenticación con tarjeta inteligente)

NetScaler Gateway también admite RSA SecurID, Gemalto Protiva y SafeWord. Utiliza un servidor RADIUS para configurar estos tipos de autenticación.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Mientras que la autenticación permite a los usuarios iniciar sesión en NetScaler Gateway y conectarse a la red interna, la autorización define los recursos dentro de la red segura a los que los usuarios tienen acceso. La autorización se configura con directivas LDAP y RADIUS.

## Configuración de tipos de autenticación global predeterminados

Cuando instaló NetScaler Gateway y ejecutó el asistente de NetScaler Gateway, configuró la autenticación dentro del asistente. Esta directiva de autenticación se enlaza automáticamente al nivel global de NetScaler Gateway. El tipo de autenticación que configura en el asistente de NetScaler Gateway es el tipo de autenticación predeterminado. Puede cambiar el tipo de autorización predeterminado ejecutando el asistente de NetScaler Gateway de nuevo o puede modificar la configuración de autenticación global en la utilidad de configuración.

Si necesita agregar tipos de autenticación adicionales, puede configurar directivas de autenticación en NetScaler Gateway y enlazar las directivas a NetScaler Gateway mediante la utilidad de configuración. Al configurar la autenticación globalmente, define el tipo de autenticación, configura los ajustes y establece el número máximo de usuarios que se pueden autenticar.

Después de configurar y enlazar la directiva, puede establecer la prioridad para definir qué tipo de autenticación tiene precedencia. Por ejemplo, configure directivas de autenticación LDAP y RADIUS. Si la directiva LDAP tiene un número de prioridad de 10 y la directiva RADIUS tiene un número de prioridad de 15, la directiva LDAP tiene precedencia, independientemente de dónde enlace cada directiva. Esto se denomina autenticación en cascada.

Puede seleccionar entregar las páginas de inicio de sesión desde la caché en memoria de NetScaler Gateway o desde el servidor HTTP que se ejecuta en NetScaler Gateway. Si elige entregar la página de inicio de sesión desde la caché en memoria, la entrega de la página de inicio de sesión desde NetScaler Gateway es significativamente más rápida que desde el servidor HTTP. La elección de entregar la página de inicio de sesión desde la caché en memoria reduce el tiempo de espera cuando un gran número de usuarios inician sesión al mismo tiempo. Solo puede configurar la entrega de páginas de inicio de sesión desde la caché como parte de una directiva de autenticación global.

También puede configurar la dirección IP de traducción de direcciones de red (NAT), que es una dirección IP específica para la autenticación. Esta dirección IP es única para la autenticación y no es la subred de NetScaler Gateway, ni las direcciones IP asignadas o virtuales. Esta es una configuración opcional.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**Nota**: No puede usar el asistente de NetScaler Gateway para configurar la autenticación SAML.

Puede usar el asistente de configuración rápida para configurar la autenticación LDAP, RADIUS y de certificados de cliente. Al ejecutar el asistente, puede seleccionar un servidor LDAP o RADIUS existente configurado en NetScaler Gateway. También puede configurar los ajustes para LDAP o RADIUS. Si utiliza la autenticación de dos factores, Citrix recomienda usar LDAP como tipo de autenticación principal.

### Para configurar la autenticación globalmente

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda NetScaler Gateway y, a continuación, haga clic en Configuración global.
2. En el panel de detalles, en Configuración, haga clic en Cambiar la configuración de autenticación.
3. En Número máximo de usuarios, escriba el número de usuarios que se pueden autenticar mediante este tipo de autenticación.
4. En Dirección IP NAT, escriba la dirección IP única para la autenticación.
5. Seleccione Habilitar el almacenamiento en caché estático para entregar las páginas de inicio de sesión más rápido.
6. Seleccione Habilitar comentarios de autenticación mejorados para proporcionar un mensaje a los usuarios si la autenticación falla. El mensaje que reciben los usuarios incluye errores de contraseña, cuenta inhabilitada o bloqueada, o usuario no encontrado, por nombrar algunos.
7. En Tipo de autenticación predeterminado, seleccione el tipo de autenticación.
8. Configure los ajustes para su tipo de autenticación y, a continuación, haga clic en Aceptar.

## Configuración de la autenticación sin autorización

La autorización define los recursos a los que los usuarios pueden conectarse a través de NetScaler Gateway. Se configuran las directivas de autorización mediante una expresión y, a continuación, se establece que la directiva se permita o se deniegue. Puede configurar NetScaler Gateway para que utilice solo la autenticación, sin autorización.

Cuando se configura la autenticación sin autorización, NetScaler Gateway no realiza una comprobación de autorización de grupo. Las directivas que configure para el usuario o grupo se asignan al usuario.

Para obtener más información sobre la configuración de la autorización, consulte Configuración de la autorización.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

# Configuración de la autorización

La autorización especifica los recursos de red a los que los usuarios tienen acceso cuando inician sesión en NetScaler Gateway. La configuración predeterminada para la autorización es denegar el acceso a todos los recursos de red. Citrix recomienda utilizar la configuración global predeterminada y, a continuación, crear directivas de autorización para definir los recursos de red a los que los usuarios pueden acceder.

Puede configurar la autorización en NetScaler Gateway mediante una directiva de autorización y expresiones. Después de crear una directiva de autorización, puede vincularla a los usuarios o grupos que configuró en el dispositivo.

## Configuración de directivas de autorización

Al configurar una directiva de autorización, puede establecerla para permitir o denegar el acceso a los recursos de red en la red interna. Por ejemplo, para permitir a los usuarios acceder a la red 10.3.3.0, utilice la siguiente expresión:

CLIENT.IP.DST.IN_SUBNET(10.3.0.0/16)

Las directivas de autorización se aplican a usuarios y grupos. Después de que un usuario se autentica, NetScaler Gateway realiza una comprobación de autorización de grupo obteniendo la información del grupo del usuario de un servidor RADIUS, LDAP o TACACS+. Si la información del grupo está disponible para el usuario, NetScaler Gateway comprueba los recursos de red permitidos para el grupo.

Para controlar a qué recursos pueden acceder los usuarios, debe crear directivas de autorización. Si no necesita crear directivas de autorización, puede configurar la autorización global predeterminada.

Si crea una expresión dentro de la directiva de autorización que deniega el acceso a una ruta de archivo, solo puede usar la ruta del subdirectorio y no el directorio raíz. Por ejemplo, use fs.path contains "\\\\dir1\\\\dir2" en lugar de fs.path contains "\\\\rootdir\\\\dir1\\\\dir2". Si utiliza la segunda versión en este ejemplo, la directiva falla.

Después de configurar la directiva de autorización, la vincula a un usuario o grupo como se muestra en las tareas siguientes.

De forma predeterminada, las directivas de autorización se validan primero con las directivas que vincula al servidor virtual y luego con las directivas vinculadas globalmente. Si vincula una directiva globalmente y desea que la directiva global tenga prioridad sobre una directiva que vincula a un usuario, grupo o servidor virtual, puede cambiar el número de prioridad de la directiva.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Los números de prioridad comienzan en cero. Un número de prioridad más bajo otorga a la directiva una mayor precedencia.

Por ejemplo, si la directiva global tiene un número de prioridad de uno y el usuario tiene una prioridad de dos, la directiva de autenticación global se aplica primero.

**IMPORTANTE:**

- Las directivas de autorización clásicas se aplican solo al tráfico TCP.
- La directiva de autorización avanzada se puede aplicar a todos los tipos de tráfico (TCP/UDP/ICMP/DNS).
  - Para aplicar la directiva al tráfico UDP/ICMP/DNS, las directivas deben vincularse a los tipos UDP_REQUEST, ICMP_REQUEST y DNS_REQUEST, respectivamente.
  - Al vincular, si no se menciona explícitamente el "type" o si el "type" se establece en REQUEST, el comportamiento no cambia con respecto a las compilaciones anteriores, es decir, estas directivas se aplican solo al tráfico TCP.
  - Las directivas vinculadas en UDP_REQUEST no se aplican al tráfico DNS. Para DNS, las directivas deben vincularse explícitamente a DNS_REQUEST. TCP_DNS es similar a otras solicitudes TCP.

Para obtener más detalles sobre las políticas de autorización avanzadas, consulte el artículo `<https://support.citrix.com/article/CTX232237>`.

### Ejemplos de expresiones de políticas de autorización

A continuación, se muestran ejemplos de expresiones de políticas de autorización:

- `add authorization policy athzPol1 "HTTP.REQ.USER.IS_MEMBER_OF(\"allowedGroup\")" ALLOW`
- `add authorization policy athzPol2 "CLIENT.IP.DST.BETWEEN(192.0.2.10,192.0.2.20)" DENY`
- `add authorization policy athzPol3 "HTTP.REQ.HOSTNAME.CONTAINS(\"portal-srv") || CLIENT.IP.DST.IN_SUBNET(192.0.2.0/25)" ALLOW`

### Para configurar una política de autorización mediante la GUI

1. Vaya a **NetScaler Gateway > Directivas > Autorización**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. En el panel de detalles, haga clic en **Agregar**.
3. En **Nombre**, escriba un nombre para la directiva.
4. En **Acción**, seleccione **Permitir** o **Denegar**.
5. En **Expresión**, haga clic en **Editor de expresiones**.
6. Para empezar a configurar la expresión, haga clic en **Seleccionar** y elija los elementos necesarios.
7. Haga clic en **Listo** cuando la expresión esté completa.
8. Haga clic en **Crear**.

### Para vincular una política de autorización a un usuario mediante la GUI

1. Vaya a **NetScaler Gateway > Administración de usuarios.**
2. Haga clic en **Usuarios AAA**.
3. En el panel de detalles, seleccione un usuario y, a continuación, haga clic en **Editar**.
4. En **Configuración avanzada**, haga clic en **Directivas de autorización**.
5. En la página **Enlace de directivas**, seleccione una directiva o cree una.
6. En **Prioridad**, establezca el número de prioridad.
7. En **Tipo**, seleccione el tipo de solicitud y, a continuación, haga clic en **Aceptar**.

### Para vincular una política de autorización a un grupo mediante la GUI

1. Vaya a **NetScaler Gateway > Administración de usuarios**.
2. Haga clic en **Grupos AAA**.
3. En el panel de detalles, seleccione un grupo y, a continuación, haga clic en **Editar**.
4. En **Configuración avanzada**, haga clic en **Directivas de autorización**.
5. En la página **Enlace de directivas**, seleccione una directiva o cree una.
6. En **Prioridad**, establezca el número de prioridad.
7. En **Tipo**, seleccione el tipo de solicitud y, a continuación, haga clic en **Aceptar**.

## Configuración de la autorización global predeterminada

Para definir los recursos a los que los usuarios tienen acceso en la red interna, puede configurar la autorización global predeterminada. La autorización global se configura permitiendo o denegando el acceso a los recursos de red de forma global en la red interna.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Cualquier acción de autorización global que cree se aplica a todos los usuarios que aún no tienen una política de autorización asociada, ya sea directamente o a través de un grupo. Una política de autorización de usuario o grupo siempre anula la acción de autorización global. Si la acción de autorización predeterminada se establece en Denegar, debe aplicar políticas de autorización para todos los usuarios o grupos a fin de que los recursos de red sean accesibles para esos usuarios o grupos. Este requisito ayuda a mejorar la seguridad.

Para configurar la autorización global predeterminada:

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda NetScaler Gateway y, a continuación, haga clic en Configuración global.
2. En el panel de detalles, en Configuración, haga clic en Cambiar configuración global.
3. En la ficha Seguridad, junto a Acción de autorización predeterminada, seleccione Permitir o Denegar y, a continuación, haga clic en Aceptar.

# Deshabilitar la autenticación

Si su implementación no requiere autenticación, puede deshabilitarla. Puede deshabilitar la autenticación para cada servidor virtual que no la requiera.

**IMPORTANTE:**

Citrix recomienda deshabilitar la autenticación con precaución. Si no utiliza un servidor de autenticación externo, cree usuarios y grupos locales para permitir que NetScaler Gateway autentique a los usuarios. Deshabilitar la autenticación detiene el uso de las funciones de autenticación, autorización y contabilidad que controlan y supervisan las conexiones a NetScaler Gateway. Cuando los usuarios escriben una dirección web para conectarse a NetScaler Gateway, la página de inicio de sesión no aparece.

## Para deshabilitar la autenticación

1. En la utilidad de configuración, en el panel de navegación, expanda NetScaler Gateway y, a continuación, haga clic en Servidores virtuales.
2. En el panel de detalles, haga clic en un servidor virtual y, a continuación, haga clic en Abrir.
3. En la ficha Autenticación, en Autenticación de usuario, haga clic para desmarcar Habilitar autenticación.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

# Configuración de la autenticación para horas específicas

Puede configurar una directiva de autenticación para que los usuarios puedan acceder a la red interna en momentos específicos, como durante el horario laboral normal. Cuando los usuarios intentan iniciar sesión en un momento diferente, se deniega el inicio de sesión.

Para restringir cuándo los usuarios inician sesión en NetScaler Gateway, cree una expresión dentro de la directiva de autenticación y, a continuación, vincúlela a un servidor virtual o globalmente.

## Para configurar la autenticación por hora, fecha o día de la semana

1. En la utilidad de configuración, en la ficha Configuración, expanda NetScaler Gateway \> Directivas \> Autenticación.
2. En Autenticación, seleccione el tipo de autenticación.
3. En el panel de detalles, haga clic en la ficha Directivas, seleccione una directiva de autenticación y, a continuación, haga clic en Abrir.
4. En el cuadro de diálogo Configurar directiva de autenticación, en Expresión, junto a Coincidir con cualquier expresión, haga clic en Agregar.
5. En el cuadro de diálogo Agregar expresión, en Tipo de expresión, seleccione Fecha/Hora.
6. En Calificador, seleccione una de las siguientes opciones:

   - TIME para configurar la hora en que los usuarios no pueden iniciar sesión.
   - DATE para configurar la fecha en que los usuarios no pueden iniciar sesión.
   - DAYOFWEEK para configurar el día en que los usuarios no pueden iniciar sesión.

   Ejemplo: TIME: 2020-10-12-02:30:00GMT DATE: 2020-10-12 DAYOFWEEK: Monday
7. En Operador, seleccione el valor.
8. En Valor, haga clic en el calendario junto al cuadro de texto y, a continuación, seleccione el día, la fecha o la hora.
9. Haga clic en Aceptar dos veces, haga clic en Cerrar y haga clic en Aceptar.

# Cómo funcionan las políticas de autenticación

Cuando los usuarios inician sesión en NetScaler Gateway, se autentican según una política que usted crea. La política define el tipo de autenticación. Una única política de autenticación se puede utilizar para necesidades de autenticación sencillas y normalmente se vincula a nivel global.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

También puede utilizar el tipo de autenticación predeterminado, que es local. Si configura la autenticación local, también debe configurar usuarios y grupos en NetScaler Gateway.

Puede configurar varias políticas de autenticación y vincularlas para crear un procedimiento de autenticación detallado y servidores virtuales. Por ejemplo, puede configurar la autenticación en cascada y de dos factores configurando varias políticas. También puede establecer la prioridad de las políticas de autenticación para determinar qué servidores y el orden en que NetScaler Gateway comprueba las credenciales de usuario. Una política de autenticación incluye una expresión y una acción. Por ejemplo, si establece la expresión en el valor True, cuando los usuarios inician sesión, la acción evalúa el inicio de sesión del usuario como verdadero y, a continuación, los usuarios tienen acceso a los recursos de red.

Después de crear una política de autenticación, la vincula a nivel global o a servidores virtuales. Cuando vincula al menos una política de autenticación a un servidor virtual, las políticas de autenticación que vinculó a nivel global no se utilizan cuando los usuarios inician sesión en el servidor virtual, a menos que el tipo de autenticación global tenga una precedencia superior a la política vinculada al servidor virtual.

Cuando un usuario inicia sesión en NetScaler Gateway, la autenticación se evalúa en el siguiente orden:

- Se comprueba el servidor virtual en busca de políticas de autenticación vinculadas.
- Si las políticas de autenticación no están vinculadas al servidor virtual, NetScaler Gateway comprueba las políticas de autenticación globales.
- Si una política de autenticación no está vinculada a un servidor virtual o globalmente, el usuario se autentica mediante el tipo de autenticación predeterminado.

Si configura políticas de autenticación LDAP y RADIUS y desea vincular las políticas globalmente para la autenticación de dos factores, puede seleccionar la política en la utilidad de configuración y, a continuación, seleccionar si la política es el tipo de autenticación principal o secundario. También puede configurar una política de extracción de grupos.

## Configuración de perfiles de autenticación

Puede crear un perfil de autenticación mediante el asistente de NetScaler Gateway o la utilidad de configuración. El perfil contiene todos los ajustes de la directiva de autenticación. Se configura el perfil al crear la directiva de autenticación.

Con el asistente de NetScaler Gateway, puede usar el tipo de autenticación elegido para configurar la autenticación. Si desea configurar directivas de autenticación adicionales después de

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ejecutar el asistente, puede usar la utilidad de configuración. Para obtener más información sobre el asistente de NetScaler Gateway, consulte Configuración de ajustes mediante el asistente de NetScaler Gateway.

### Para crear una directiva de autenticación mediante la utilidad de configuración

1. En la utilidad de configuración, en la ficha Configuración, expanda NetScaler Gateway \> Directivas \> Autenticación.
2. En el panel de navegación, en Autenticación, seleccione un tipo de autenticación.
3. En el panel de detalles, en la ficha Directivas, haga clic en Agregar.
4. Si utiliza un tipo de autenticación externo, junto a Servidor, haga clic en Nuevo.
5. En el cuadro de diálogo Crear servidor de autenticación, configure los ajustes para su tipo de autenticación, haga clic en Crear y, a continuación, en Cerrar.
6. En el cuadro de diálogo Crear directiva de autenticación, junto a Expresiones con nombre, seleccione Valor verdadero, haga clic en Agregar expresión, haga clic en Crear y, a continuación, en Cerrar. Nota: Cuando selecciona un tipo de autenticación y guarda el perfil de autenticación, no puede cambiar el tipo de autenticación. Para usar un tipo de autenticación diferente, debe crear una nueva directiva.

### Para modificar una directiva de autenticación mediante la utilidad de configuración

Puede modificar las directivas y perfiles de autenticación configurados, como la dirección IP del servidor de autenticación o la expresión.

1. En la utilidad de configuración, en la ficha Configuración, expanda NetScaler Gateway \> Directivas \> Autenticación.
2. En el panel de navegación, en Autenticación, seleccione un tipo de autenticación.
3. En el panel de detalles, en la ficha Servidores, seleccione un servidor y, a continuación, haga clic en Abrir.

### Para eliminar una directiva de autenticación

Si cambió o eliminó un servidor de autenticación de su red, elimine la directiva de autenticación correspondiente de NetScaler Gateway.

1. En la utilidad de configuración, en la ficha Configuración, expanda NetScaler Gateway \> Directivas \> Autenticación.
2. En el panel de navegación, en Autenticación, seleccione un tipo de autenticación.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. En el panel de detalles, en la ficha Directivas, seleccione una directiva y, a continuación, haga clic en Quitar.

## Enlazar directivas de autenticación

Después de configurar las directivas de autenticación, las enlaza globalmente o a un servidor virtual. Puede usar la utilidad de configuración para enlazar una directiva de autenticación.

### Para enlazar una directiva de autenticación globalmente mediante la GUI

1. En la utilidad de configuración, en la ficha Configuration, expanda **NetScaler Gateway > Policies > Authentication**.
2. Haga clic en un tipo de autenticación.
3. En el panel de detalles, en la ficha **Policies**, haga clic en un servidor y, a continuación, en **Action**, haga clic en **Global Bindings**.
4. En la ficha **Primary or Secondary**, en **Details**, haga clic en **Insert Policy**.
5. En **Policy Name**, seleccione la directiva y, a continuación, haga clic en **OK**.

   **Nota**: Al seleccionar la directiva, NetScaler Gateway establece automáticamente la expresión en el valor True.

### Para desenlazar una directiva de autenticación global mediante la GUI

1. En la utilidad de configuración, en la ficha Configuration, expanda **NetScaler Gateway > Policies > Authentication**.
2. En la ficha **Policies**, en **Action**, haga clic en **Global Bindings**.
3. En el cuadro de diálogo **Bind/Unbind Authentication Policies to Global**, en la ficha **Primary or Secondary**, en **Policy Name**, seleccione la directiva, haga clic en **Unbind Policy** y, a continuación, haga clic en **OK**.

## Establecer prioridades para las directivas de autenticación

De forma predeterminada, las directivas de autenticación se validan primero con las directivas que se vinculan al servidor virtual y, a continuación, con las directivas vinculadas globalmente. Si vincula una directiva de autenticación globalmente y desea que la directiva global tenga prioridad sobre una directiva que vincula a un servidor virtual, puede cambiar el número de prioridad de la directiva. Los números de prioridad comienzan en cero. Un número de prioridad más bajo otorga a la directiva de autenticación una precedencia más alta.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Por ejemplo, si la directiva global tiene un número de prioridad de uno y el servidor virtual tiene una prioridad de dos, la directiva de autenticación global se aplica primero.

### Para establecer o cambiar la prioridad de las directivas de autenticación globales

1. En la utilidad de configuración, en la ficha Configuración, expanda NetScaler Gateway \> Directivas \> Autenticación.
2. En la ficha Directivas, en Acción, haga clic en Enlaces globales.
3. En el cuadro de diálogo Enlazar/Desenlazar directivas globales de autenticación, en la ficha Principal o Secundaria, en Prioridad, escriba el número y, a continuación, haga clic en Aceptar.

### Para cambiar la prioridad de una directiva de autenticación vinculada a un servidor virtual

También puede modificar una directiva de autenticación vinculada a un servidor virtual.

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda NetScaler Gateway y, a continuación, haga clic en Servidores virtuales.
2. Seleccione un servidor virtual y, a continuación, haga clic en Abrir.
3. Haga clic en la ficha Autenticación y, a continuación, seleccione Principal o Secundaria.
4. Seleccione la directiva y, en Prioridad, escriba el número de prioridad y, a continuación, haga clic en Aceptar.

# Configuración de usuarios locales

Puede crear cuentas de usuario localmente en NetScaler Gateway para complementar a los usuarios de los servidores de autenticación. Por ejemplo, es posible que desee crear cuentas de usuario locales para usuarios temporales, como consultores o visitantes, sin crear una entrada para esos usuarios en el servidor de autenticación.

Si utiliza la autenticación local, cree usuarios y luego agréguelos a los grupos que cree en NetScaler Gateway. Después de configurar usuarios y grupos, puede aplicar políticas de autorización y sesión, crear marcadores, especificar aplicaciones y especificar la dirección IP de los recursos compartidos de archivos y servidores a los que los usuarios tienen acceso.

## Para crear usuarios locales

1. En la utilidad de configuración, haga clic en la ficha **Configuration** y, en el panel de navegación, expanda **NetScaler Gateway > User Administration** y, a continuación, haga clic en **AAA Users**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. En el panel de detalles, haga clic en **Add**.
3. En **User Name**, escriba el nombre de usuario.
4. Si utiliza la autenticación local, desactive **External Authentication**. **Nota**: Seleccione **External Authentication** para que los usuarios se autentiquen en un servidor de autenticación externo, como LDAP o RADIUS. Desactive la casilla de verificación para que NetScaler Gateway se autentique en la base de datos de usuarios local.
5. En **Password** y **Confirm Password**, escriba la contraseña del usuario, haga clic en **Create** y, a continuación, haga clic en **Close**.

## Para cambiar la contraseña de un usuario

Después de crear un usuario local, puede cambiar la contraseña del usuario o configurar la cuenta de usuario para que se autentique en un servidor de autenticación externo.

1. En la utilidad de configuración, haga clic en la ficha **Configuration** y, en el panel de navegación, expanda **NetScaler Gateway > User Administration** y, a continuación, haga clic en **AAA Users**.
2. En el panel de detalles, seleccione un usuario y, a continuación, haga clic en **Open**.
3. En **Password** y **Confirm Password**, escriba la nueva contraseña del usuario y, a continuación, haga clic en **OK**.

## Para cambiar el método de autenticación de un usuario

Si tiene usuarios configurados para la autenticación local, puede cambiar la autenticación a un servidor de autenticación externo. Para ello, habilite la autenticación externa.

1. En la utilidad de configuración, haga clic en la ficha **Configuración** y, en el panel de navegación, expanda **NetScaler Gateway > Administración de usuarios** y, a continuación, haga clic en **Usuarios AAA**.
2. En el panel de detalles, seleccione un usuario y, a continuación, haga clic en **Abrir**.
3. Seleccione **Autenticación externa** y, a continuación, haga clic en **Aceptar**.

## Para eliminar un usuario

También puede eliminar un usuario de NetScaler Gateway.

1. En la utilidad de configuración, haga clic en la ficha **Configuración** y, en el panel de navegación, expanda **NetScaler Gateway > Administración de usuarios** y, a continuación, haga clic en **Usuarios AAA**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. En el panel de detalles, seleccione un usuario y, a continuación, haga clic en **Quitar**.

Cuando se elimina un usuario de NetScaler Gateway, todas las directivas asociadas también se eliminan del perfil de usuario.

# Configuración de grupos

Puede tener grupos en NetScaler Gateway que son grupos locales y pueden autenticar usuarios con autenticación local. Si utiliza servidores externos para la autenticación, los grupos en NetScaler Gateway se configuran para que coincidan con los grupos configurados en los servidores de autenticación de la red interna. Cuando un usuario inicia sesión y se autentica, si un nombre de grupo coincide con un grupo en un servidor de autenticación, el usuario hereda la configuración del grupo en NetScaler Gateway.

Después de configurar los grupos, puede aplicar políticas de autorización y de sesión, crear marcadores, especificar aplicaciones y especificar la dirección IP de los recursos compartidos de archivos y servidores a los que el usuario tiene acceso.

Si utiliza la autenticación local, cree usuarios y agréguelos a los grupos configurados en NetScaler Gateway. Los usuarios heredarán entonces la configuración de ese grupo.

**IMPORTANTE:**

Si los usuarios son miembros de un grupo de Active Directory, el nombre del grupo en NetScaler Gateway debe ser el mismo que el del grupo de Active Directory.

## Para crear un grupo

1. En la utilidad de configuración, haga clic en la ficha **Configuration** y, en el panel de navegación, expanda **NetScaler Gateway > User Administration** y, a continuación, haga clic en **AAA Groups**.
2. En el panel de detalles, haga clic en **Add**.
3. En **Group Name**, escriba un nombre para el grupo, haga clic en **Create** y, a continuación, haga clic en **Close**.

## Para eliminar un grupo

También puede eliminar grupos de usuarios de NetScaler Gateway.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. En la utilidad de configuración, haga clic en la ficha **Configuration** y, en el panel de navegación, expanda **NetScaler Gateway > User Administration** y, a continuación, haga clic en **AAA Groups**.
2. En el panel de detalles, seleccione el grupo y, a continuación, haga clic en **Remove**.

## Adición de usuarios a grupos

Puede agregar usuarios a un grupo durante la creación del grupo o más tarde. Puede agregar usuarios a varios grupos para que los usuarios puedan heredar las directivas y la configuración vinculadas a esos grupos.

Para agregar usuarios a grupos:

1. En la utilidad de configuración, haga clic en la ficha Configuration y, en el panel de navegación, expanda **NetScaler Gateway > User Administration** y, a continuación, haga clic en **AAA Users**.
2. En el panel de detalles, seleccione un grupo y, a continuación, haga clic en **Open**.
3. En la ficha **Users**, en **Available Users**, seleccione los usuarios, haga clic en **Add** y, a continuación, haga clic en **OK**.

## Configuración de directivas con grupos

Después de configurar los grupos, puede usar el cuadro de diálogo Grupo para aplicar directivas y configuraciones que especifican el acceso de los usuarios. Si utiliza la autenticación local, crea usuarios y los agrega a grupos configurados en NetScaler Gateway. Los usuarios heredan entonces la configuración de ese grupo.

Puede configurar las siguientes directivas o configuraciones para un grupo de usuarios en el cuadro de diálogo Grupo:

- Usuarios
- Directivas de autorización
- Directivas de auditoría
- Directivas de sesión
- Directivas de tráfico
- Marcadores
- Aplicaciones de intranet
- Direcciones IP de intranet

© 1997–2026 Citrix Systems, Inc. All rights reserved.

En su configuración, es posible que tenga usuarios que pertenezcan a más de un grupo. Además, cada grupo puede tener una o más directivas de sesión vinculadas, con diferentes parámetros configurados. Los usuarios que pertenecen a más de un grupo heredan las directivas de sesión asignadas a todos los grupos a los que pertenece el usuario. Para garantizar qué evaluación de directiva de sesión tiene prioridad sobre la otra, debe establecer la prioridad de la directiva de sesión.

Por ejemplo, tiene el grupo1 que está vinculado con una directiva de sesión configurada con la página de inicio www.homepage1.com. El grupo2 está vinculado con una directiva de sesión configurada con la página de inicio www.homepage2.com. Cuando estas directivas se vinculan a los grupos respectivos sin un número de prioridad o con el mismo número de prioridad, la página de inicio que aparece a los usuarios que pertenecen a ambos grupos depende de qué directiva se procese primero. Al establecer un número de prioridad más bajo, lo que da mayor precedencia, para la directiva de sesión con la página de inicio www.homepage1.com, puede asegurarse de que los usuarios que pertenecen a ambos grupos reciban la página de inicio www.homepage1.com.

Si las directivas de sesión no tienen un número de prioridad asignado o tienen el mismo número de prioridad, la precedencia se evalúa en el siguiente orden:

- Usuario
- Grupo
- Servidor virtual
- Global

Si las políticas están vinculadas al mismo nivel, sin un número de prioridad o si las políticas tienen el mismo número de prioridad, el orden de evaluación es según el orden de vinculación de la política. Las políticas que se vinculan primero a un nivel tienen precedencia sobre las políticas vinculadas posteriormente.

Si tenemos un usuario vinculado a varios grupos y cada grupo tiene IIP vinculado, el usuario puede obtener una IP libre de cualquiera de los grupos vinculados.

## Configuración de la autenticación LDAP

Puede configurar NetScaler Gateway para autenticar el acceso de los usuarios con uno o varios servidores LDAP.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

La autorización LDAP requiere nombres de grupo idénticos en Active Directory, en el servidor LDAP y en NetScaler Gateway. Los caracteres y las mayúsculas/minúsculas también deben coincidir.

De forma predeterminada, la autenticación LDAP es segura mediante el uso de Secure Sockets Layer (SSL) o Transport Layer Security (TLS). Hay dos tipos de conexiones LDAP seguras. Con un tipo, el servidor LDAP acepta las conexiones SSL o TLS en un puerto independiente del puerto que el servidor LDAP utiliza para aceptar conexiones LDAP claras. Una vez que los usuarios establecen las conexiones SSL o TLS, el tráfico LDAP se puede enviar a través de la conexión.

Los números de puerto para las conexiones LDAP son:

- 389 para conexiones LDAP no seguras
- 636 para conexiones LDAP seguras
- 3268 para conexiones LDAP no seguras de Microsoft
- 3269 para conexiones LDAP seguras de Microsoft

El segundo tipo de conexiones LDAP seguras utiliza el comando StartTLS y el número de puerto 389. Si configura los números de puerto 389 o 3268 en NetScaler Gateway, el servidor intenta usar StartTLS para establecer la conexión. Si utiliza cualquier otro número de puerto, el servidor intenta establecer conexiones mediante SSL o TLS. Si el servidor no puede usar StartTLS, SSL o TLS, la conexión falla.

Si especifica el directorio raíz del servidor LDAP, NetScaler Gateway busca en todos los subdirectorios para encontrar el atributo de usuario. En directorios grandes, este enfoque puede afectar al rendimiento. Por esta razón, Citrix recomienda que utilice una unidad organizativa (OU) específica.

La siguiente tabla contiene ejemplos de campos de atributos de usuario para servidores LDAP:

| SERVIDOR LDAP | ATRIBUTO DE USUARIO | SENSIBLE A MAYÚSCULAS |
|---|---|---|
| Servidor de Microsoft Active Directory | sAMAccountName | No |
| Novell eDirectory | ou | Sí |
| Servidor de directorios de IBM | ID de usuario | Sí |
| Lotus Domino | CN | Sí |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| SERVIDOR LDAP | ATRIBUTO DE USUARIO | SENSIBLE A MAYÚSCULAS |
|---|---|---|
| Directorio Sun ONE (anteriormente iPlanet) | uid o cn | Sí |

Esta tabla contiene ejemplos del DN base:

| SERVIDOR LDAP | DN BASE |
|---|---|
| Servidor Microsoft Active Directory | DC=`citrix`,DC=local |
| Novell eDirectory | ou=users,ou=dev |
| Servidor de directorios IBM | cn=users |
| Lotus Domino | OU=City,O=`Citrix`, C=US |
| Directorio Sun ONE (anteriormente iPlanet) | ou=People,dc=`citrix`,dc=com |

La siguiente tabla contiene ejemplos de DN de enlace:

| SERVIDOR LDAP | DN DE ENLACE |
|---|---|
| Servidor de Microsoft Active Directory | CN=Administrador, CN=Usuarios, DC=`citrix`, DC=local |
| Novell eDirectory | cn=administrador, o=`citrix` |
| Servidor de directorios de IBM | LDAP_dn |
| Lotus Domino | CN=Administrador de Notes, O=`Citrix`, C=US |
| Directorio Sun ONE (anteriormente iPlanet) | uid=administrador,ou=Administradores, ou=Gestión de Topología,o=NetscapeRoot |

**Nota**: Para obtener más información sobre la configuración del servidor LDAP, consulte Determinación de atributos en su directorio LDAP.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

## Para configurar la autenticación LDAP mediante la utilidad de configuración

1. Vaya a **NetScaler Gateway** >**Directivas** > **Autenticación**.
2. Haga clic en **LDAP**.
3. En el panel de detalles, en la ficha **Directivas**, haga clic en **Agregar**.
4. En **Nombre**, escriba un nombre para la directiva.
5. Junto a **Servidor**, haga clic en **Nuevo**.
6. En **Nombre**, escriba el nombre del servidor.
7. En **Servidor**, en **Dirección IP y puerto**, escriba la dirección IP y el número de puerto del servidor LDAP.
8. En **Tipo**, seleccione **AD** para Active Directory o **NDS** para Novell Directory Services.
9. En **Configuración de conexión**, complete lo siguiente:

    a. En **DN base (ubicación de los usuarios)**, escriba el DN base bajo el cual se encuentran los usuarios. El DN base busca los usuarios ubicados en el directorio seleccionado (AD o NDS).

    El DN base se deriva del DN de enlace eliminando el nombre de usuario y especificando el grupo donde se encuentran los usuarios. Ejemplos de la sintaxis para el DN base son:

    ```
    ou=users,dc=ace,dc=com

    cn=Users,dc=ace,dc=com
    ```

    b. En **DN de enlace de administrador**, escriba el DN de enlace de administrador para las consultas al directorio LDAP. Ejemplos de la sintaxis para el DN de enlace son:

    ```
    domain/user name

    ou=administrator,dc=ace,dc=com

    user@domain.name (for Active Directory)

    cn=Administrator,cn=Users,dc=ace,dc=com
    ```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Para Active Directory, se requiere el nombre de grupo especificado como cn=groupname. El nombre de grupo que defina en NetScaler Gateway y el nombre de grupo en el servidor LDAP deben ser idénticos.

Para otros directorios LDAP, el nombre de grupo no es necesario o, si es necesario, se especifica como ou=groupname.

NetScaler Gateway se enlaza al servidor LDAP mediante las credenciales de administrador y, a continuación, busca al usuario. Después de localizar al usuario, NetScaler Gateway desvincula las credenciales de administrador y se vuelve a enlazar con las credenciales de usuario.

c. En **Contraseña de administrador y Confirmar contraseña de administrador**, escriba la contraseña de administrador para el servidor LDAP.

10. Para recuperar más configuraciones LDAP automáticamente, haga clic en **Recuperar atributos**.

    Cuando hace clic en **Recuperar atributos**, los campos en Configuración adicional se rellenan automáticamente. Si desea omitir este paso, continúe con los pasos 12 y 13. De lo contrario, salte al paso 14.

11. En **Configuración adicional**, en Atributo de nombre de inicio de sesión del servidor, escriba el atributo bajo el cual NetScaler Gateway debe buscar los nombres de inicio de sesión de usuario para el servidor LDAP que está configurando. El valor predeterminado es `samAccountName`.

12. En **Filtro de búsqueda**, escriba el valor para buscar los usuarios asociados con grupos de Active Directory únicos o múltiples.

    Por ejemplo, "memberOf=CN=GatewayAccess,OU=Groups,DC=Users,DC=lab".

    **NOTA**

    Puede utilizar el ejemplo anterior para restringir el acceso de NetScaler Gateway solo a los miembros de un grupo de AD específico.

13. En **Atributo de grupo**, deje el valor predeterminado memberOf para Active Directory o cambie el atributo al atributo del tipo de servidor LDAP que esté utilizando. Este atributo permite a NetScaler Gateway obtener los grupos asociados con un usuario durante la autorización.

14. En **Tipo de seguridad**, seleccione el tipo de seguridad y, a continuación, haga clic en **Crear**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

15. Para permitir que los usuarios cambien su contraseña LDAP, seleccione **Permitir cambio de contraseña**.

    **Nota:**

    - Si selecciona **PLAINTEXT** como tipo de seguridad, no se admite que los usuarios cambien sus contraseñas.
    - Si selecciona **PLAINTEXT** o **TLS** para la seguridad, utilice el número de puerto 389. Si selecciona **SSL**, utilice el número de puerto 636.

## Determinar atributos en su directorio LDAP

Si necesita ayuda para determinar los atributos de su directorio LDAP para poder configurar los ajustes de autenticación en NetScaler® Gateway, puede consultarlos fácilmente con el navegador LDAP gratuito de Softerra.

Puede descargar el navegador LDAP desde el sitio web de Softerra LDAP Administrator. Después de instalar el navegador, configure los siguientes atributos:

- El nombre de host o la dirección IP de su servidor LDAP.
- El puerto de su servidor LDAP. El valor predeterminado es 389.
- El campo DN base, que puede dejar en blanco. La información proporcionada por el navegador LDAP puede ayudarle a determinar el DN base que debe configurar en NetScaler Gateway.
- La casilla de verificación Enlace anónimo determina si el servidor LDAP requiere credenciales de usuario para conectarse a él. Si el servidor LDAP requiere credenciales, deje la casilla de verificación desmarcada.

Después de completar la configuración, el navegador LDAP muestra el nombre del perfil en el panel izquierdo y se conecta al servidor LDAP.

## Configuración de la extracción de grupos LDAP

Si utiliza la autenticación de dos factores, los grupos extraídos de las fuentes de autenticación principal y secundaria se concatenan. Las directivas de autorización se pueden aplicar al grupo que se extrae del servidor de autenticación principal o secundario.

Los nombres de grupo obtenidos del servidor LDAP se comparan con los nombres de grupo creados localmente en NetScaler Gateway. Si los dos nombres de grupo coinciden, las propiedades del grupo local se aplican al grupo obtenido de los servidores LDAP.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Si los usuarios pertenecen a más de un grupo LDAP, NetScaler Gateway extrae la información del usuario de todos los grupos a los que pertenecen los usuarios. Si un usuario es miembro de dos grupos en NetScaler Gateway y cada grupo tiene una directiva de sesión vinculada, el usuario hereda las directivas de sesión de ambos grupos. Para asegurarse de que los usuarios reciban la directiva de sesión correcta, establezca la prioridad de la directiva de sesión.

Para obtener más información sobre los atributos de pertenencia a grupos LDAP, consulte lo siguiente:

- Cómo funciona la extracción de grupos LDAP directamente desde el objeto de usuario
- Cómo funciona la extracción de grupos LDAP indirectamente desde el objeto de grupo

### Cómo funciona la extracción de grupos LDAP directamente desde el objeto de usuario

Los servidores LDAP que evalúan las pertenencias a grupos a partir de objetos de grupo admiten la autorización de NetScaler Gateway.

Algunos servidores LDAP permiten que los objetos de usuario contengan información sobre los grupos a los que pertenecen los objetos, como Active Directory (mediante el atributo memberOf) o IBM eDirectory (mediante el atributo groupMembership). La pertenencia a grupos de un usuario puede ser atributos del objeto de usuario, como IBM Directory Server (mediante ibm-allGroups) o el servidor de directorios Sun ONE (mediante nsRole). Ambos tipos de servidores LDAP admiten la extracción de grupos de NetScaler Gateway.

Por ejemplo, en IBM Directory Server, todas las pertenencias a grupos, incluidos los grupos estáticos, dinámicos y anidados, se pueden devolver mediante el atributo ibm-allGroups. En Sun ONE, todos los roles, incluidos los administrados, filtrados y anidados, se calculan mediante el atributo nsRole.

### Cómo funciona la extracción de grupos LDAP del objeto de grupo indirectamente

Los servidores LDAP que evalúan las pertenencias a grupos de objetos de grupo indirectamente no son compatibles con la autorización de NetScaler Gateway.

Algunos servidores LDAP, como Lotus Domino, permiten que los objetos de grupo contengan solo información sobre los usuarios. Estos servidores LDAP no permiten que el objeto de usuario contenga información sobre los grupos y, por lo tanto, no son compatibles con la extracción de grupos de NetScaler Gateway. Para este tipo de servidor LDAP, las búsquedas de pertenencia a grupos se realizan localizando al usuario en la lista de miembros de los grupos.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

### Campos de atributo de grupo de autorización LDAP

La siguiente tabla contiene ejemplos de campos de atributo de grupo LDAP:

| SERVIDORES LDAP | ATRIBUTO LDAP |
|---|---|
| Servidor Microsoft Active Directory | memberOf |
| Novell eDirectory | groupMembership |
| Servidor de directorios IBM | ibm-allGroups |
| Directorio Sun ONE (anteriormente iPlanet) | nsRole |

### Para configurar la autorización LDAP

Se configura la autorización LDAP en la política de autenticación estableciendo el nombre del atributo de grupo y el subatributo.

1. En la utilidad de configuración, en la ficha Configuración, expanda NetScaler Gateway > Directivas > Autenticación.
2. En Autenticación, haga clic en un tipo de autenticación.
3. En el panel de detalles, haga clic en Agregar.
4. En Nombre, escriba un nombre para la directiva.
5. Junto a Servidor, haga clic en Nuevo.
6. En Nombre, escriba el nombre del servidor.
7. En Servidor, escriba la dirección IP y el puerto del servidor LDAP.
8. En Atributo de grupo, escriba memberOf.
9. En Nombre de subatributo, escriba CN y, a continuación, haga clic en Crear.
10. En el cuadro de diálogo Crear directiva de autenticación, junto a Expresiones con nombre, seleccione la expresión, haga clic en Agregar expresión, haga clic en Crear y, a continuación, haga clic en Cerrar.

### Configuración de la extracción de grupos anidados de LDAP

NetScaler Gateway puede consultar grupos LDAP y extraer información de grupos y usuarios de los grupos antecesores que configure en el servidor de autenticación. Por ejemplo, si creó el grupo1 y dentro de ese grupo creó el grupo2 y el grupo3. Si el usuario pertenece al grupo3,

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler Gateway extrae información de todos los grupos antecesores anidados (grupo2, grupo1) hasta el nivel especificado.

Puede usar una directiva de autenticación para configurar la extracción de grupos anidados de LDAP. Cuando se ejecuta la consulta, NetScaler Gateway busca en los grupos hasta que alcanza el nivel máximo de anidamiento o hasta que busca todos los grupos disponibles.

**Para configurar la extracción de grupos anidados de LDAP**

1. En la utilidad de configuración, en el panel de navegación, expanda **NetScaler Gateway > Directivas > Autenticación/Autorización > Autenticación > Autenticación** y, a continuación, haga clic en **LDAP**.
2. En el panel de detalles, en la ficha Directivas, haga clic en **Agregar**.
3. En Nombre, escriba un nombre para la directiva.
4. Junto a Servidor, haga clic en **Nuevo**.
5. En Nombre, escriba el nombre del servidor.
6. Configure los ajustes para el servidor LDAP.
7. Expanda **Extracción de grupos anidados** y, a continuación, haga clic en **Habilitar**.
8. En **Nivel máximo de anidamiento**, escriba el número de niveles que NetScaler Gateway comprueba.
9. En **Identificador de nombre de grupo**, escriba el nombre de atributo LDAP que identifica de forma única un nombre de grupo en el servidor LDAP, como `sAMAccountName`.
10. En **Atributo de búsqueda de grupo**, escriba el nombre de atributo LDAP que se obtendrá en la respuesta de búsqueda para determinar los grupos principales de cualquier grupo. Por ejemplo, `memberOf`.
11. En **Subatributo de búsqueda de grupo**, escriba el nombre de subatributo LDAP que se buscará como parte del Atributo de búsqueda de grupo para determinar los grupos principales de cualquier grupo. Por ejemplo, escriba CN.
12. En **Filtro de búsqueda de grupo**, escriba la cadena de consulta. Por ejemplo, el filtro puede ser `&(samaccountname=test)(objectClass=*)`.
13. Haga clic en **Crear** y, a continuación, haga clic en **Cerrar**.
14. En el cuadro de diálogo Crear directiva de autenticación, junto a Expresiones con nombre, seleccione la expresión, haga clic en **Agregar expresión**, haga clic en **Crear** y, a continuación, haga clic en **Cerrar**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

# Configuración de la extracción de grupos LDAP para varios dominios

Si tiene varios dominios para la autenticación y está utilizando StoreFront, puede configurar NetScaler Gateway para que utilice la extracción de grupos para enviar el nombre de dominio correcto a StoreFront.

En Active Directory, debe crear un grupo para cada dominio de su red. Después de crear el grupo, añade usuarios que pertenecen al grupo y al dominio especificado. Una vez configurados los grupos en Active Directory, configure la extracción de grupos LDAP para varios dominios en NetScaler Gateway.

Para configurar NetScaler Gateway para la extracción de grupos para varios dominios, debe crear el mismo número de directivas de sesión y autenticación que el número de dominios de su red. Por ejemplo, tiene dos dominios, denominados `Sampa` y Child. Cada dominio recibe una directiva de sesión y una directiva de autenticación.

Después de crear las directivas, crea grupos en NetScaler Gateway y vincula las directivas de sesión al grupo. A continuación, vincula las directivas de autenticación a un servidor virtual.

Si implementa StoreFront™ en varios dominios, debe existir una relación de confianza entre los dominios.

Si implementa Citrix Endpoint Management™ o StoreFront en varios dominios, los dominios no necesitan confiar entre sí.

## Creación de directivas de sesión para la extracción de grupos

El primer paso al crear directivas de sesión para la extracción de grupos es crear dos perfiles de sesión y establecer los siguientes parámetros:

- Habilitar proxy ICA®.
- Agregar la dirección web de StoreFront™.
- Agregar el dominio de Windows.
- Agregue el perfil a una directiva de sesión y establezca la expresión en true.

### Para crear los perfiles de sesión para la extracción de grupos

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda **NetScaler Gateway > Directivas** y, a continuación, haga clic en **Sesión**.
2. En el panel de detalles, haga clic en la ficha **Perfiles** y, a continuación, haga clic en **Agregar**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. En **Nombre**, escriba un nombre para el perfil. Por ejemplo, escriba `Sampa`.
4. En la ficha **Aplicaciones publicadas**, haga lo siguiente:
    a. Junto a **Proxy ICA**, haga clic en **Anular global** y, a continuación, seleccione **ACTIVADO**.
    b. Junto a **Dirección de la interfaz web**, haga clic en **Anular global** y, a continuación, escriba la dirección web de StoreFront.
    c. Junto a **Dominio de inicio de sesión único**, haga clic en **Anular global**, escriba el nombre del dominio de Windows y, a continuación, haga clic en **Crear**.
5. En **Nombre**, borre el nombre del primer dominio y escriba el nombre del segundo dominio, como Secundario.
6. Junto a **Dominio de inicio de sesión único**, borre el nombre del primer dominio de Windows y escriba el nombre del segundo dominio, haga clic en **Crear** y, a continuación, en **Cerrar**.

Después de crear los perfiles de sesión, cree dos directivas de sesión. Cada directiva de sesión utiliza uno de los perfiles.

**Para crear una directiva de sesión**

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda **NetScaler Gateway > Directivas** y, a continuación, haga clic en **Sesión**.
2. En el panel de detalles, en la ficha **Directivas**, haga clic en **Agregar**.
3. En **Nombre**, escriba un nombre para la directiva.
4. En **Perfil de solicitud**, seleccione el perfil para el primer dominio.
5. Junto a **Expresiones con nombre**, haga clic en **General**, seleccione **Valor verdadero**, haga clic en **Agregar expresión** y, a continuación, haga clic en **Crear**.
6. En **Nombre**, cambie el nombre al segundo dominio.
7. En **Perfil de solicitud**, seleccione el perfil para el segundo dominio, haga clic en **Crear** y, a continuación, en **Cerrar**.

### Creación de directivas de autenticación LDAP para varios dominios

Después de crear directivas de sesión en NetScaler Gateway, se crean directivas de autenticación LDAP que son casi idénticas. Al configurar la directiva de autenticación, el campo importante es Filtro de búsqueda. En este campo, debe escribir el nombre del grupo que creó en Active Directory.

Cree primero los perfiles de autenticación y, a continuación, cree la directiva de autenticación.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**Para crear perfiles de autenticación para extracciones de grupos de varios dominios**

1. En la utilidad de configuración, en la ficha Configuración, expanda Citrix® **Gateway > Directivas > Autenticación**.
2. En el panel de navegación, haga clic en **LDAP**.
3. En el panel de detalles, haga clic en la ficha **Servidores** y, a continuación, haga clic en **Agregar**.
4. En **Nombre**, escriba el nombre del primer dominio, como `Sampa`.
5. Configure los parámetros para el servidor LDAP y, a continuación, haga clic en **Crear**.
6. Repita los pasos 3, 4 y 5 para configurar el perfil de autenticación del segundo dominio y, a continuación, haga clic en **Cerrar**.

Después de crear y guardar los perfiles, cree las directivas de autenticación.

**Para crear directivas de autenticación para extracciones de grupos de varios dominios**

1. En la utilidad de configuración, en la ficha Configuración, expanda **NetScaler Gateway > Directivas > Autenticación**.
2. En el panel de detalles, haga clic en la ficha **Directivas** y, a continuación, haga clic en **Agregar**.
3. En **Nombre**, escriba el nombre del primer dominio.
4. En **Tipo de autenticación**, seleccione **LDAP**.
5. En **Servidor**, seleccione el perfil de autenticación para el primer dominio.
6. Junto a **Expresiones con nombre**, haga clic en **General**, seleccione **Valor verdadero**, haga clic en **Agregar expresión** y, a continuación, haga clic en **Crear**.
7. En Nombre, escriba el nombre del segundo dominio.
8. En **Servidor**, seleccione el perfil de autenticación para el segundo dominio, haga clic en **Crear** y, a continuación, haga clic en **Cerrar**.

## Creación de grupos y vinculación de directivas para la extracción de grupos LDAP para varios dominios

Después de crear las directivas de autenticación, cree grupos en NetScaler Gateway. Después de crear los grupos, vincule la directiva de autenticación a un servidor virtual.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**Para crear grupos en NetScaler Gateway**

1. En la utilidad de configuración, en la ficha **Configuración**, en el panel de navegación, expanda **NetScaler Gateway > Administración de usuarios** y, a continuación, haga clic en **Grupos AAA**.
2. En el panel de detalles, haga clic en **Agregar**.
3. En **Nombre de grupo**, escriba el nombre del primer grupo de Active Directory.

   **IMPORTANTE:**

   Al crear grupos en NetScaler Gateway para la extracción de grupos de varios dominios, los nombres de los grupos deben ser los mismos que los grupos que definió en Active Directory. Los nombres de los grupos también distinguen entre mayúsculas y minúsculas, y las mayúsculas y minúsculas deben coincidir con las que introdujo en Active Directory.

4. En la ficha **Directivas**, haga clic en **Sesión** y, a continuación, haga clic en **Insertar directiva**.
5. En **Nombre de directiva**, haga doble clic en la directiva y, a continuación, haga clic en **Crear**.

**Para vincular las directivas de autenticación a un servidor virtual**

1. En la utilidad de configuración, en la ficha **Configuración**, en el panel de navegación, expanda **NetScaler Gateway** y, a continuación, haga clic en **Servidores virtuales**.
2. En el panel de detalles, haga clic en un servidor virtual y, a continuación, haga clic en **Abrir**.
3. En la ficha Autenticación, haga clic en **Principal**, en **Nombre de directiva**, haga doble clic en **Insertar directiva** y, a continuación, seleccione la primera directiva de autenticación.
4. En **Nombre de directiva**, haga clic en **Insertar directiva**, haga doble clic en la segunda directiva de autenticación y, a continuación, haga clic en **Aceptar**.

## Notificación de caducidad de contraseña de 14 días para autenticación LDAP

El dispositivo NetScaler Gateway admite la notificación de caducidad de contraseña de 14 días para la autenticación basada en LDAP. Mediante el uso de esta función, los administradores pueden notificar a los usuarios finales sobre el tiempo umbral de caducidad de la contraseña en días. Para obtener más detalles, consulte Notificación de caducidad de contraseña de 14 días para autenticación LDAP.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

# Configuración de la autenticación de certificados de cliente

Los usuarios que inician sesión en un servidor virtual de NetScaler Gateway también pueden autenticarse en función de los atributos del certificado de cliente presentados al servidor virtual. La autenticación de certificados de cliente también se puede utilizar con otros tipos de autenticación, como LDAP o RADIUS, para proporcionar autenticación de dos factores.

Para autenticar a los usuarios en función de los atributos del certificado del lado del cliente, la autenticación de cliente debe estar habilitada en el servidor virtual y se debe solicitar el certificado de cliente. Debe vincular un certificado raíz al servidor virtual en NetScaler Gateway.

Cuando los usuarios inician sesión en el servidor virtual de NetScaler Gateway, después de la autenticación, la información del nombre de usuario se extrae del campo especificado del certificado. Normalmente, este campo es Subject:CN. Si el nombre de usuario se extrae correctamente, el usuario se autentica. La autenticación falla en los siguientes casos.

- Si el usuario no proporciona un certificado válido durante el protocolo de enlace Secure Sockets Layer (SSL).
- Si la extracción del nombre de usuario falla, la autenticación falla.

Puede autenticar a los usuarios en función del certificado de cliente configurando el tipo de autenticación predeterminado para usar el certificado de cliente. También puede crear una acción de certificado que defina lo que se debe hacer durante la autenticación basada en un certificado SSL de cliente.

## Para configurar el certificado de cliente como tipo de autenticación predeterminado mediante la GUI

1. Vaya a **Configuration > NetScaler Gateway** y, a continuación, haga clic en **Global Settings**.
2. En el panel de detalles, en **Authentication Settings**, haga clic en **Change authentication CERT settings**.
3. Seleccione **ON** para habilitar la autenticación de dos factores mediante el certificado según sus requisitos.
4. En **User Name Field**, seleccione el tipo de campo de certificado que contiene los nombres de usuario.
5. En **Group Name Field**, seleccione el tipo de campo de certificado que contiene el nombre del grupo.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

6. En **Default Authorization Group**, escriba el nombre del grupo predeterminado y, a continuación, haga clic en **OK**.

## Extracción del nombre de usuario del certificado de cliente

Si la autenticación de certificado de cliente está habilitada en NetScaler Gateway, los usuarios se autentican en función de ciertos atributos del certificado de cliente. Una vez que la autenticación es correcta, el nombre de usuario o el nombre de usuario y grupo del usuario se extraen del certificado. Además, se aplican las políticas especificadas para ese usuario.

## Configuración y vinculación de una política de autenticación de certificado de cliente

Puede crear una política de autenticación de certificado de cliente y vincularla a un servidor virtual. Puede usar la política para restringir el acceso a grupos o usuarios específicos. Esta política tiene prioridad sobre la política global.

Para configurar una política de autenticación de certificado de cliente:

1. En la utilidad de configuración, en la ficha Configuración, expanda **NetScaler Gateway > Directivas > Autenticación**.
2. En el panel de navegación, en **Autenticación**, haga clic en **CERT**.
3. En el panel de detalles, haga clic en **Agregar**.
4. En el campo **Nombre**, escriba un nombre para la política.
5. Junto a **Servidor**, haga clic en **Nuevo**.
6. En **Nombre**, escriba un nombre para el perfil.
7. Junto a **Doble factor**, seleccione **DESACTIVADO**.
8. En el campo **Nombre de usuario** y en el campo **Nombre de grupo**, seleccione los valores y, a continuación, haga clic en &**Crear**. Nota: Si configuró previamente los certificados de cliente como el tipo de autenticación predeterminado, use los mismos nombres que usó para la directiva. Si completó el campo Nombre de usuario y el campo Nombre de grupo para el tipo de autenticación predeterminado, use los mismos valores para el perfil.
9. En el cuadro de diálogo **Crear política de autenticación**, junto a **Expresiones con nombre**, seleccione la expresión, haga clic en **Agregar expresión**, haga clic en **Crear** y, a continuación, haga clic en **Cerrar**.

Para vincular una política de certificado de cliente a un servidor virtual:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Después de configurar la política de autenticación de certificado de cliente, puede vincularla a un servidor virtual.

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda **NetScaler Gateway** y, a continuación, haga clic en **Servidores virtuales**.
2. En el panel de detalles, haga clic en un servidor virtual y, a continuación, en **Abrir**.
3. En el cuadro de diálogo de configuración de **Servidor virtual de NetScaler Gateway**, haga clic en la ficha **Autenticación**.
4. Haga clic en **Principal** o **Secundario**.
5. En **Detalles**, haga clic en **Insertar directiva**.
6. En **Nombre de directiva**, seleccione la directiva y, a continuación, haga clic en **Aceptar**.

Para configurar un servidor virtual para solicitar el certificado de cliente:

Cuando desee utilizar un certificado de cliente para la autenticación, debe configurar el servidor virtual para que se soliciten certificados de cliente durante el protocolo de enlace SSL.

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda **NetScaler Gateway** y, a continuación, haga clic en **Servidores virtuales**.
2. En el panel de detalles, haga clic en un **Servidor virtual** y, a continuación, en **Abrir**.
3. En la ficha **Certificados**, haga clic en **Parámetro SSL**.
4. En **Otros**, haga clic en **Autenticación de cliente**.
5. En **Certificado de cliente**, seleccione **Opcional** o **Obligatorio** y, a continuación, haga clic en Aceptar dos veces. Seleccione **Opcional** si desea permitir otros tipos de autenticación en el mismo servidor virtual y no requiere el uso de certificados de cliente.

**NOTA**

- Para obtener más información sobre la URL de devolución de llamada, consulte Importar un NetScaler Gateway.
- Para obtener más información sobre los certificados, consulte Instalar, vincular y actualizar certificados.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

## Configuración de la autenticación de certificado de cliente de doble factor

Puede configurar un certificado de cliente para autenticar a los usuarios primero y luego exigirles que inicien sesión con un tipo de autenticación secundaria, como LDAP o RADIUS. En este escenario, el certificado de cliente autentica a los usuarios primero. Luego, aparece una página de inicio de sesión donde pueden introducir su nombre de usuario y contraseña. Cuando se completa el protocolo de enlace de Secure Sockets Layer (SSL), la secuencia de inicio de sesión puede seguir una de las dos rutas siguientes:

- Ni el nombre de usuario ni el grupo se extraen del certificado. La página de inicio de sesión aparece al usuario con una solicitud para introducir credenciales de inicio de sesión válidas. NetScaler Gateway autentica las credenciales del usuario como en el caso de la autenticación normal por contraseña.
- El nombre de usuario y el nombre de grupo se extraen del certificado de cliente. Si solo se extrae el nombre de usuario, aparece una página de inicio de sesión al usuario en la que el nombre de inicio de sesión está presente y el usuario no puede modificar el nombre. Solo el campo de contraseña está en blanco.

La información de grupo que NetScaler Gateway extrae durante la segunda ronda de autenticación se añade a la información de grupo, si la hubiera, que NetScaler Gateway extrajo del certificado.

## Configuración de la autenticación con tarjeta inteligente

Puede configurar NetScaler Gateway para que utilice una tarjeta inteligente criptográfica para autenticar a los usuarios.

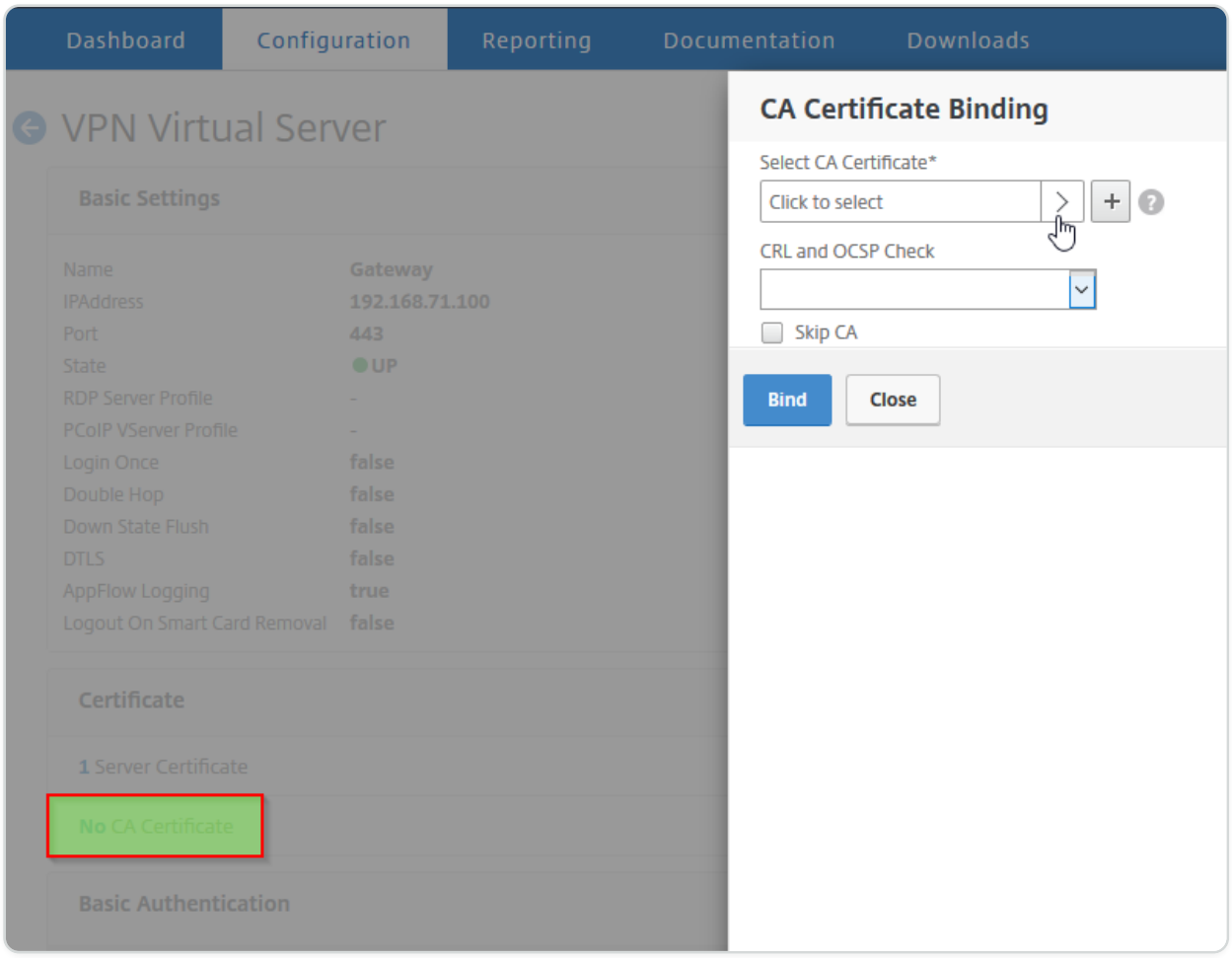
Para configurar una tarjeta inteligente con NetScaler Gateway, debe hacer lo siguiente:

- Cree una directiva de autenticación de certificados. Para obtener más información, consulte Configuración de la autenticación de certificados de cliente.
- Enlace la directiva de autenticación a un servidor virtual.
- Agregue el certificado raíz de la entidad de certificación (CA) que emite los certificados de cliente a NetScaler Gateway. Para obtener más información, consulte Para instalar un certificado raíz en NetScaler Gateway.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**IMPORTANTE:**

Cuando agregue el certificado raíz al servidor virtual para la autenticación con tarjeta inteligente, debe seleccionar el certificado de la lista **Seleccionar certificado de CA**.




Después de crear el certificado de cliente, puede escribir el certificado, conocido como flash, en la tarjeta inteligente. Una vez completado ese paso, puede probar la tarjeta inteligente.

Si configura StoreFront™ para la autenticación de paso de tarjeta inteligente, si se cumple alguna de las siguientes condiciones, el inicio de sesión único en StoreFront fallará:

- Si establece el dominio en la ficha **Aplicaciones publicadas** como `mydomain`.com en lugar de `mydomain`.
- Si no establece el nombre de dominio en la ficha **Aplicaciones publicadas** y ejecuta el comando `wi-sso-split-upn` estableciendo el valor en 1. En este caso, el UserPrincipalName contiene el nombre de dominio "`mydomain`.com".

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Puede utilizar la autenticación con tarjeta inteligente para agilizar el proceso de inicio de sesión de sus usuarios y, al mismo tiempo, mejorar la seguridad del acceso de los usuarios a su infraestructura. El acceso a la red corporativa interna está protegido por una autenticación de dos factores basada en certificados que utiliza la infraestructura de clave pública. Las claves privadas están protegidas por controles de hardware y nunca abandonan la tarjeta inteligente. Sus usuarios obtienen la comodidad de acceder a sus escritorios y aplicaciones desde una variedad de dispositivos corporativos utilizando sus tarjetas inteligentes y PIN.

Puede utilizar tarjetas inteligentes para la autenticación de usuarios a través de StoreFront para escritorios y aplicaciones proporcionados por Citrix Virtual Apps and Desktops. Los usuarios de tarjetas inteligentes que inician sesión en StoreFront también pueden acceder a las aplicaciones proporcionadas por NetScaler Endpoint Management. Sin embargo, los usuarios deben autenticarse de nuevo para acceder a las aplicaciones web de Endpoint Management que utilizan la autenticación de certificados de cliente.

Para obtener más información, consulte Configurar la autenticación con tarjeta inteligente en la documentación de StoreFront.

### Configuración de la autenticación con tarjeta inteligente con conexiones Secure ICA®

Los usuarios que inician sesión y establecen una conexión ICA segura mediante una tarjeta inteligente con inicio de sesión único configurado en NetScaler Gateway podrían recibir dos veces solicitudes de su número de identificación personal (PIN).

- Al iniciar sesión y al intentar iniciar un recurso publicado. Esta situación se produce si el explorador web y la aplicación Citrix Workspace utilizan el mismo servidor virtual configurado para usar certificados de cliente.
- La aplicación Citrix Workspace no comparte un proceso ni una conexión Secure Sockets Layer (SSL) con el explorador web. Por lo tanto, cuando la conexión ICA completa el protocolo de enlace SSL con NetScaler Gateway, el certificado de cliente se requiere una segunda vez.

Para evitar que los usuarios reciban la segunda solicitud de PIN, debe cambiar dos configuraciones:

- La autenticación de cliente en el servidor virtual VPN debe estar inhabilitada.
- La renegociación SSL debe estar habilitada.

Después de configurar el servidor virtual, vincule uno o varios servidores STA al servidor virtual, como se describe en Configurar NetScaler Gateway para gestionar el tráfico STA e ICA.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

También es posible que desee probar la autenticación con tarjeta inteligente.

Para inhabilitar la autenticación de cliente:

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda NetScaler Gateway y, a continuación, haga clic en Servidores virtuales.
2. Seleccione el servidor virtual pertinente en el panel de detalles principal y, a continuación, haga clic en Modificar.
3. En el panel Opciones avanzadas, haga clic en Parámetros SSL.
4. Desactive la casilla de verificación Autenticación de cliente.
5. Haga clic en Listo.

Para habilitar la renegociación SSL:

1. Mediante la utilidad de configuración, en la ficha Configuración, vaya a Administración de tráfico y, a continuación, haga clic en SSL.
2. En el panel principal, haga clic en Cambiar la configuración avanzada de SSL.
3. En el menú Denegar renegociación SSL, seleccione NO.

Para probar la autenticación con tarjeta inteligente:

1. Conecte la tarjeta inteligente al dispositivo de usuario.
2. Abra su explorador web e inicie sesión en NetScaler Gateway.

## Configuración de la autenticación RADIUS

Puede configurar NetScaler Gateway para autenticar el acceso de los usuarios con uno o varios servidores RADIUS. Si utiliza productos RSA SecurID, SafeWord o Gemalto Protiva, cada uno de estos productos se configura mediante un servidor RADIUS.

Su configuración podría requerir el uso de una dirección IP del servidor de acceso a la red (NAS IP) o un identificador del servidor de acceso a la red (NAS ID). Al configurar NetScaler Gateway para usar un servidor de autenticación RADIUS, siga estas directrices:

- Si habilita el uso de la IP de NAS, el dispositivo envía su dirección IP configurada al servidor RADIUS, en lugar de la dirección IP de origen utilizada para establecer la conexión RADIUS.
- Si configura el ID de NAS, el dispositivo envía el identificador al servidor RADIUS. Si no configura el ID de NAS, el dispositivo envía su nombre de host al servidor RADIUS.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Cuando habilita la IP de NAS, el dispositivo ignora cualquier ID de NAS que se configure utilizando la IP de NAS para comunicarse con el servidor RADIUS.

## Configuración de Gemalto Protiva

Protiva es una plataforma de autenticación sólida que Gemalto desarrolló para aprovechar las ventajas de la autenticación con tarjeta inteligente de Gemalto. Con Protiva, los usuarios inician sesión con un nombre de usuario, una contraseña y una contraseña de un solo uso que genera el dispositivo Protiva. De forma similar a RSA SecurID, la solicitud de autenticación se envía al servidor de autenticación Protiva y el servidor valida o rechaza la contraseña. Para configurar Gemalto Protiva para que sea compatible con NetScaler Gateway, siga estas directrices:

- Instale el servidor Protiva.
- Instale el software Protiva SAS Agent, que extiende el servidor de autenticación de Internet (IAS), en un servidor RADIUS IAS de Microsoft. Asegúrese de anotar la dirección IP y el número de puerto del servidor IAS.
- Configure un perfil de autenticación RADIUS en NetScaler Gateway e introduzca la configuración del servidor Protiva.

## Configuración de SafeWord

La línea de productos SafeWord proporciona autenticación segura mediante una contraseña basada en tokens. Una vez que el usuario introduce la contraseña, SafeWord la invalida inmediatamente y no se puede volver a utilizar. Al configurar el servidor SafeWord, necesita la siguiente información:

- La dirección IP de NetScaler Gateway. La dirección IP debe ser la misma que configuró en la configuración del cliente del servidor RADIUS. NetScaler Gateway utiliza la dirección IP interna para comunicarse con el servidor RADIUS. Al configurar el secreto compartido, utilice la dirección IP interna. Si configura dos dispositivos para alta disponibilidad, utilice la dirección IP interna virtual.
- Un secreto compartido.
- La dirección IP y el puerto del servidor SafeWord. El número de puerto predeterminado es 1812.

## Para configurar la autenticación RADIUS

1. En la utilidad de configuración, en la ficha Configuración, expanda NetScaler Gateway \> Directivas \> Autenticación.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Haga clic en RADIUS y, a continuación, en el panel de detalles, en la ficha Directivas, haga clic en Agregar.
3. En el cuadro de diálogo Crear directiva de autenticación, en Nombre, escriba un nombre para la directiva.
4. En Nombre, escriba un nombre para la directiva.
5. Junto a Servidor, haga clic en Nuevo.
6. En el cuadro de diálogo Crear directiva de autenticación, en Nombre, escriba un nombre para el servidor.
7. En Servidor, en Dirección IP, escriba la dirección IP del servidor RADIUS.
8. En Puerto, escriba el puerto. El valor predeterminado es 1812.
9. En Detalles, en Clave secreta y Confirmar clave secreta, escriba el secreto del servidor RADIUS.
10. En ID de NAS, escriba el número de identificador y, a continuación, haga clic en Crear.
11. En el cuadro de diálogo Crear directiva de autenticación, junto a Expresiones con nombre, seleccione la expresión, haga clic en Agregar expresión, haga clic en Crear y, a continuación, haga clic en Cerrar.

## Elección de protocolos de autenticación RADIUS

NetScaler Gateway admite implementaciones de RADIUS configuradas para usar varios protocolos para la autenticación de usuarios, incluidos:

- Protocolo de autenticación de contraseña (PAP)
- Protocolo de autenticación de desafío-respuesta (CHAP)
- Protocolo de autenticación de desafío-respuesta de Microsoft (MS-CHAP versión 1 y versión 2)

Si su implementación de NetScaler Gateway está configurada para usar la autenticación RADIUS y su servidor RADIUS está configurado para usar PAP, puede fortalecer la autenticación de usuario asignando un secreto compartido fuerte al servidor RADIUS. Los secretos compartidos RADIUS fuertes consisten en secuencias aleatorias de letras mayúsculas y minúsculas, números y puntuación, y tienen al menos 22 caracteres de longitud. Si es posible, use un programa de generación de caracteres aleatorios para determinar los secretos compartidos de RADIUS.

Para proteger aún más el tráfico RADIUS, asigne un secreto compartido diferente a cada dispositivo o servidor virtual de NetScaler Gateway. Cuando defina clientes en el servidor RADIUS,

© 1997–2026 Citrix Systems, Inc. All rights reserved.

también puede asignar un secreto compartido independiente a cada cliente. Si hace esto, debe configurar por separado cada directiva de NetScaler Gateway que utilice la autenticación RADIUS.

Cuando crea una directiva RADIUS, configura los secretos compartidos en NetScaler Gateway como parte de la directiva.

## Configuración de la extracción de direcciones IP

Puede configurar NetScaler Gateway para extraer la dirección IP de un servidor RADIUS. Cuando un usuario se autentica con el servidor RADIUS, el servidor devuelve una dirección IP enmarcada que se asigna al usuario. La dirección IP enmarcada también se denomina Atributo RADIUS 8 Framed-IP-Address en las solicitudes de acceso.

Los siguientes son componentes para la extracción de direcciones IP:

- Permite que un servidor RADIUS remoto proporcione una dirección IP de la red interna para un usuario que ha iniciado sesión en NetScaler Gateway.
- Permite la configuración de cualquier atributo RADIUS utilizando el tipo **ipaddress**, incluidos los atributos codificados por el proveedor.

Al configurar el servidor RADIUS para la extracción de direcciones IP, se configura el identificador de proveedor y el tipo de atributo. El ID de proveedor y los atributos se utilizan para establecer la asociación entre el cliente RADIUS y el servidor RADIUS.

- El identificador de proveedor (ID) permite al servidor RADIUS asignar una dirección IP al cliente desde un grupo de direcciones IP configuradas en el servidor RADIUS. El ID de proveedor es el atributo en la respuesta RADIUS que proporciona la dirección IP de la red interna. Un valor de cero indica que el atributo no está codificado por el proveedor.
- El tipo de atributo es el atributo de dirección IP remota en una respuesta RADIUS. El valor mínimo es 1 y el valor máximo es 255.

Una configuración común es extraer el atributo RADIUS **framed IP address**. El ID de proveedor se establece en 0 o no se especifica. El tipo de atributo se establece en 8.

**Para configurar la extracción de direcciones IP de un servidor RADIUS mediante la GUI:**

1. Vaya a **NetScaler Gateway \> Directivas \> Autenticación** y haga clic en **RADIUS**.
2. En el panel **Detalles**, en la ficha **Directivas**, seleccione una directiva RADIUS y, a continuación, haga clic en **Abrir**.
3. En el cuadro de diálogo **Configurar directiva de autenticación**, junto a Servidor, haga clic en **Modificar**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. En **Detalles**, en **Identificador de proveedor de grupo**, escriba el valor.
5. En **Tipo de atributo de grupo**, escriba el valor y, a continuación, haga clic en **Aceptar** dos veces.

## Configuración de la extracción de grupos RADIUS

Puede configurar la autorización RADIUS mediante un método denominado extracción de grupos. La configuración de la extracción de grupos le permite administrar usuarios en su servidor RADIUS en lugar de agregarlos a NetScaler Gateway.

Para configurar la autorización RADIUS, utilice una directiva de autenticación y configure el identificador de proveedor de grupo (ID), el tipo de atributo de grupo, el prefijo de grupo y un separador de grupo. Al configurar la directiva, agregue una expresión y, a continuación, vincule la directiva globalmente o a un servidor virtual.

### Configuración de RADIUS en Windows Server 2003

Si utiliza Microsoft Internet Authentication Service (IAS) para la autorización RADIUS en Windows Server 2003, durante la configuración de NetScaler Gateway, debe proporcionar la siguiente información:

- El ID de proveedor es el código específico del proveedor que introdujo en IAS.
- El tipo es el número de atributo asignado por el proveedor.
- El nombre de atributo es el tipo de nombre de atributo que definió en IAS. El nombre predeterminado es CTXSUserGroups=

Si IAS no está instalado en el servidor RADIUS, puede instalarlo desde Agregar o quitar programas en el Panel de control. Para obtener más información, consulte la Ayuda en línea de Windows.

Para configurar IAS, utilice la Consola de administración de Microsoft (MMC) e instale el complemento para IAS. Siga el asistente, asegurándose de seleccionar la siguiente configuración:

- Seleccione el equipo local.
- Seleccione Directivas de acceso remoto y cree una directiva personalizada.
- Seleccione Grupos de Windows para la directiva.
- Seleccione uno de los siguientes protocolos:
    - Microsoft Challenge-Handshake Authentication Protocol versión 2 (MS-CHAP v2)
    - Protocolo de autenticación de desafío-respuesta de Microsoft (MS-CHAP)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

    - Protocolo de autenticación de desafío-respuesta (CHAP)
    - Autenticación sin cifrar (PAP, SPAP)

- Seleccione el atributo específico del proveedor.

  El atributo específico del proveedor debe coincidir con los usuarios que definió en el grupo del servidor con los usuarios de NetScaler Gateway. Para cumplir este requisito, envíe los atributos específicos del proveedor a NetScaler Gateway. Asegúrese de seleccionar RADIUS=Standard.
- El valor predeterminado de RADIUS es 0. Utilice este número para el código de proveedor.
- El número de atributo asignado por el proveedor es 0.

  Este es el número asignado para el atributo Grupo de usuarios. El atributo está en formato de cadena.
- Seleccione Cadena para el formato del atributo.

  El valor del atributo requiere el nombre del atributo y los grupos.

  Para Access Gateway, el valor del atributo es CTXSUserGroups=groupname. Si se definen dos grupos, como ventas y finanzas, el valor del atributo es CTXSUserGroups=sales;finance. Separe cada grupo con un punto y coma.
- Elimine todas las demás entradas del cuadro de diálogo Editar perfil de acceso telefónico, dejando la que dice Específico del proveedor.

Después de configurar la directiva de acceso remoto en IAS, configure la autenticación y autorización RADIUS en NetScaler Gateway.

Al configurar la autenticación RADIUS, utilice la configuración que estableció en el servidor IAS.

### Configuración de RADIUS para la autenticación en Windows Server 2008

En Windows Server 2008, se configura la autenticación y autorización RADIUS mediante el Servidor de directivas de red (NPS), que reemplaza al Servicio de autenticación de Internet (IAS). Puede usar el Administrador del servidor y agregar NPS como un rol para instalar NPS.

Al instalar NPS, seleccione el Servicio de directivas de red. Después de la instalación, puede configurar los ajustes de RADIUS para su red iniciando el NPS desde Servicios administrativos en el menú Inicio. Cuando abra el NPS, agregue NetScaler Gateway como cliente RADIUS y luego configure los grupos de servidores.

Al configurar el cliente RADIUS, asegúrese de seleccionar las siguientes opciones:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Para el nombre del proveedor, seleccione RADIUS Standard.
- Tome nota del secreto compartido porque deberá configurar el mismo secreto compartido en NetScaler Gateway.

Para los grupos RADIUS, necesita la dirección IP o el nombre de host del servidor RADIUS. No cambie la configuración predeterminada.

Después de configurar el cliente y los grupos RADIUS, configure los ajustes en las dos directivas siguientes:

- Directivas de solicitud de conexión donde se configuran los ajustes para la conexión de NetScaler Gateway, incluido el tipo de servidor de red, las condiciones para la directiva de red y los ajustes para la directiva.
- Directivas de red donde se configura la autenticación del Protocolo de autenticación extensible (EAP) y los atributos específicos del proveedor.

Al configurar la directiva de solicitud de conexión, seleccione Sin especificar para el tipo de servidor de red. Luego configure su condición seleccionando Tipo de puerto NAS como condición y Virtual (VPN) como valor.

Al configurar una directiva de red, debe configurar las siguientes opciones:

- Seleccione Servidor de acceso remoto (VPN de acceso telefónico) como tipo de servidor de acceso a la red.
- Seleccione Autenticación cifrada (CHAP) y Autenticación sin cifrar (PAP y SPAP) para el EAP.
- Seleccione RADIUS Standard para el atributo específico del proveedor.

  El número de atributo predeterminado es 26. Este atributo se utiliza para la autorización RADIUS.

  NetScaler Gateway necesita el atributo específico del proveedor para hacer coincidir los usuarios definidos en el grupo del servidor con los de NetScaler Gateway. Esto se hace enviando los atributos específicos del proveedor a NetScaler Gateway.
- Seleccione Cadena para el formato del atributo.

  El valor del atributo requiere el nombre del atributo y los grupos.

  Para NetScaler Gateway, el valor del atributo es CTXSUserGroups= nombre_grupo. Si se definen dos grupos, como ventas y finanzas, el valor del atributo es CTXSUserGroups=ventas;finanzas. Separe cada grupo con un punto y coma.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- El separador es el que utilizó en el NPS para separar grupos, como un punto y coma, dos puntos, un espacio o un punto.

Cuando haya terminado de configurar la política de acceso remoto en IAS, puede configurar la autenticación y autorización RADIUS en NetScaler Gateway.

### Para configurar la autorización RADIUS

1. En la utilidad de configuración, en la ficha Configuración, expanda NetScaler Gateway \> Directivas \> Autenticación.
2. Haga clic en RADIUS.
3. En la ficha Directivas, haga clic en Agregar.
4. En Nombre, escriba un nombre para la directiva.
5. Debajo de Servidor* haga clic en +
6. En Nombre, escriba el nombre del servidor RADIUS.
7. En Servidor, escriba la dirección IP y el puerto del servidor RADIUS.
8. En Detalles, introduzca los valores de Identificador de proveedor de grupo y Tipo de atributo de grupo.
9. En Codificación de contraseña, seleccione el protocolo de autenticación y, a continuación, haga clic en Crear.
10. En el cuadro de diálogo Crear directiva de autenticación, junto a Expresiones con nombre, seleccione la expresión, haga clic en Agregar expresión, haga clic en Crear y, a continuación, haga clic en Cerrar.

## Configuración de la contabilidad de usuarios RADIUS

NetScaler Gateway puede enviar mensajes de inicio y fin de sesión de usuario a su servidor de contabilidad RADIUS. Los mensajes, que se envían para cada sesión de usuario, incluyen un subconjunto de los atributos definidos en RFC2866. La Tabla 1 enumera los atributos admitidos y los tipos de mensajes de contabilidad RADIUS (RAD_START y RAD_STOP) en los que se envían. La Tabla 2 enumera los valores predefinidos que se pueden asignar al atributo `Acct-Terminate-Cause` y los eventos correspondientes de NetScaler Gateway.

Tabla 1. Atributos RADIUS admitidos

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| ATRIBUTO | SIGNIFICADO | RAD_START | RAD_STOP |
|---|---|---|---|
| User-Name | Nombre del usuario asociado a la sesión. | X | X |
| Session-Id | El ID de sesión de NetScaler. | X | X |
| Acct-Session-Time | Duración de la sesión en segundos. | X | |
| Acct-Terminate-Cause | Motivo de la terminación de la cuenta. | X | |

Tabla 2. Causas de terminación de RADIUS

| MÉTODO DE CIERRE DE SESIÓN DE NETSCALER | CAUSA DE TERMINACIÓN DE RADIUS |
|---|---|
| LOGOUT_SESSN_TIMEDOUT | RAD_TERM_SESSION_TIMEOUT |
| LOGOUT_SESSN_INITIATEDBYUSER | RAD_TERM_USER_REQUEST |
| LOGOUT_SESSN_KILLEDBYADMIN | RAD_TERM_ADMIN_RESET |
| LOGOUT_SESSN_TLOGIN | RAD_TERM_NAS_REQUEST |
| LOGOUT_SESSN_MAXLICRCHD | RAD_TERM_NAS_REQUEST |
| LOGOUT_SESSN_CLISECCHK_FAILED | RAD_TERM_NAS_REQUEST |
| LOGOUT_SESSN_PREAUTH_CHANGED | RAD_TERM_NAS_REQUEST |
| LOGOUT_SESSN_COOKIE_MISMATCH | RAD_TERM_NAS_REQUEST |
| LOGOUT_SESSS_DHT | RAD_TERM_NAS_REQUEST |
| LOGOUT_SESSS_2FACTOR_FAIL | RAD_TERM_NAS_REQUEST |
| LOGOUT_SESSN_ICALIC | RAD_TERM_NAS_REQUEST |
| LOGOUT_SESSN_INTERNALERR | RAD_TERM_NAS_ERROR |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

La configuración de la contabilidad de usuarios de RADIUS requiere la creación de un par de directivas. La primera directiva es una directiva de autenticación RADIUS que designa un servidor RADIUS al que enviar mensajes de contabilidad. La segunda es una directiva de sesión que utiliza la directiva de contabilidad RADIUS como su acción.

Para configurar la contabilidad de usuarios de RADIUS, debe:

1. Cree una directiva RADIUS para definir el servidor de contabilidad RADIUS. El servidor de contabilidad puede ser el mismo servidor que utiliza para la autenticación RADIUS.
2. Cree una directiva de sesión, utilizando la directiva RADIUS como una acción que especifica el servidor de contabilidad de usuarios RADIUS.
3. Enlace la directiva de sesión globalmente, para que se aplique a todo el tráfico, o a un servidor virtual de NetScaler Gateway, para que se aplique solo al tráfico que fluye a través de ese servidor virtual.

### Para crear una directiva RADIUS

1. En la utilidad de configuración, en el panel de navegación, expanda el nodo NetScaler Gateway y, a continuación, Directivas.
2. Expanda Autenticación y seleccione RADIUS.
3. En el panel de detalles, en la ficha Directivas, haga clic en Agregar.
4. Introduzca un nombre para la directiva.
5. Seleccione un servidor del menú Servidor, o haga clic en el icono + y siga las indicaciones para agregar un nuevo servidor RADIUS.
6. En el panel Expresión, en el menú Expresiones de directiva guardadas, seleccione ns_true.
7. Haga clic en Crear.

### Para crear una directiva de sesión

Después de configurar una directiva RADIUS que especifique el servidor de contabilidad RADIUS, cree una directiva de sesión que aplique este servidor de contabilidad en una acción, como se indica a continuación:

1. En la utilidad de configuración, en el panel de navegación, expanda el nodo NetScaler Gateway y, a continuación, Directivas.
2. Seleccione Sesión.
3. En el panel de detalles principal, seleccione Agregar.
4. Introduzca un nombre para la directiva.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. En el menú Acción, haga clic en el icono + para agregar una nueva acción de sesión.
6. Introduzca un nombre para la acción de sesión.
7. Haga clic en la ficha Experiencia del cliente.
8. En el menú Directiva de contabilidad, seleccione la directiva RADIUS que creó anteriormente.
9. Haga clic en Crear.
10. En el panel Expresión, en el menú Expresiones de directiva guardadas, seleccione ns_true.
11. Haga clic en Crear.

### Para enlazar la directiva de sesión globalmente

1. En la utilidad de configuración, en el panel de navegación, expanda el nodo NetScaler Gateway y, a continuación, Directivas.
2. Seleccione Sesión.
3. En el menú Acción del panel de detalles principal, seleccione Enlaces globales.
4. Haga clic en Enlazar.
5. En el panel Directivas, seleccione la directiva de sesión que creó anteriormente y, a continuación, haga clic en Insertar.
6. En la lista de directivas, haga clic en la entrada Prioridad de la directiva de sesión e introduzca un valor de 0 a 64000.
7. Haga clic en Aceptar.

### Para enlazar la directiva de sesión a un servidor virtual de NetScaler Gateway

1. En la utilidad de configuración, en el panel de navegación, expanda el nodo NetScaler Gateway y, a continuación, seleccione Servidores virtuales.
2. En el panel de detalles principal, seleccione un servidor virtual y, a continuación, haga clic en Editar.
3. En el panel Directivas, haga clic en el icono + para seleccionar una directiva.
4. En el menú Elegir directiva, seleccione Sesión y asegúrese de que Solicitud esté seleccionada en el menú Elegir tipo.
5. Haga clic en Continuar.
6. Haga clic en Enlazar.
7. En el panel Directivas, seleccione la directiva de sesión que creó anteriormente y, a continuación, haga clic en Insertar.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

8. Haga clic en Aceptar.

# Configuración de la autenticación SAML

Security Assertion Markup Language (SAML) es un estándar basado en XML para intercambiar autenticación y autorización entre proveedores de identidades (IdP) y proveedores de servicios. NetScaler Gateway admite la autenticación SAML.

Al configurar la autenticación SAML, se crean las siguientes configuraciones:

- Nombre del certificado IdP. Esta es la clave pública que corresponde a la clave privada en el IdP.
- URL de redirección. Esta es la URL del IdP de autenticación. Los usuarios no autenticados se redirigen a esta URL.
- Campo de usuario. Puede usar este campo para extraer el nombre de usuario si el IdP envía el nombre de usuario en un formato diferente al de la etiqueta NameIdentifier de la etiqueta Subject. Esta es una configuración opcional.
- Nombre del certificado de firma. Esta es la clave privada del servidor NetScaler Gateway que se utiliza para firmar la solicitud de autenticación al IdP. Si no configura un nombre de certificado, la aserción se envía sin firmar o la solicitud de autenticación se rechaza.
- Nombre del emisor SAML. Este valor se utiliza cuando se envía la solicitud de autenticación. Debe haber un nombre único en el campo del emisor para indicar la autoridad desde la que se envía la aserción. Este es un campo opcional.
- Grupo de autenticación predeterminado. Este es el grupo en el servidor de autenticación desde el que se autentican los usuarios.
- Doble factor. Esta configuración habilita o deshabilita la autenticación de doble factor.
- Rechazar aserción sin firmar. Si está habilitado, NetScaler Gateway rechaza la autenticación de usuario si el nombre del certificado de firma no está configurado.

NetScaler Gateway admite el enlace HTTP POST. En este enlace, la parte remitente responde al usuario con un 200 OK que contiene un formulario de publicación automática con la información requerida. Específicamente, el formulario predeterminado debe contener dos campos ocultos llamados `SAMLRequest` y `SAMLResponse`, dependiendo de si el formulario es una solicitud o una respuesta. El formulario también incluye RelayState, que es un estado o información utilizada por la parte remitente para enviar información arbitraria que no es procesada por una parte que confía. La parte que confía devuelve la información para que, cuando la parte remitente reciba la

© 1997–2026 Citrix Systems, Inc. All rights reserved.

aserción junto con RelayState, la parte remitente sepa qué hacer a continuación. Se recomienda cifrar u ofuscar el RelayState.

**NOTA**

- Cuando NetScaler Gateway se utiliza como IdP para Citrix Cloud, no es necesario configurar la regla **RelayState** en NetScaler Gateway.
- En caso de encadenamiento de IdP, es suficiente configurar la regla **RelayState** solo en la primera política SAML. En este contexto, el encadenamiento de IdP es un escenario en el que una acción SAML configurada hace referencia a un IdP de servidor virtual de autenticación que contiene otra acción SAML.

## Configuración de Active Directory Federation Services 2.0

Puede configurar Active Directory Federation Services (AD FS) 2.0 en cualquier equipo con Windows Server 2008 o Windows Server 2012 que utilice en una función de servidor federado. Al configurar el servidor ADFS para que sea compatible con NetScaler Gateway, debe configurar los siguientes parámetros mediante el Asistente para confianza de usuario de confianza en Windows Server 2008 o Windows Server 2012.

Parámetros de Windows Server 2008:

- Confianza de usuario de confianza. Proporcione la ubicación del archivo de metadatos de NetScaler Gateway, como `https://vserver.fqdn.com/ns.metadata.xml`, donde vserver.fqdn.com es el nombre de dominio completo (FQDN) del servidor virtual de NetScaler Gateway. Puede encontrar el FQDN en el certificado de servidor vinculado al servidor virtual.
- Reglas de autorización. Puede permitir o denegar el acceso de los usuarios a la parte de confianza.

Parámetros de Windows Server 2012:

- Confianza de usuario de confianza. Proporcione la ubicación del archivo de metadatos de NetScaler Gateway, como `https://vserver.fqdn.com/ns.metadata.xml`, donde vserver.fqdn.com es el nombre de dominio completo (FQDN) del servidor virtual de NetScaler Gateway. Puede encontrar el FQDN en el certificado de servidor vinculado al servidor virtual.
- Perfil de AD FS. Seleccione el perfil de AD FS.
- Certificado. NetScaler Gateway no admite el cifrado. No es necesario seleccionar un certificado.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Habilitar la compatibilidad con el protocolo SAML 2.0 WebSSO. Esto habilita la compatibilidad con SAML 2.0 SSO. Proporcione la URL del servidor virtual de NetScaler Gateway, como `https:netScaler.virtualServerName.com/cgi/samlauth`.

  Esta URL es la URL del Servicio de consumidor de aserciones en el dispositivo NetScaler Gateway. Este es un parámetro constante y NetScaler Gateway espera una respuesta SAML en esta URL.
- Identificador de confianza de usuario de confianza. Introduzca el nombre NetScaler Gateway. Esta es una URL que identifica a las partes de confianza, como `https://netscalerGateway.virtualServerName.com/adfs/services/trust`.
- Reglas de autorización. Puede permitir o denegar el acceso de los usuarios a la parte de confianza.
- Configurar reglas de notificación. Puede configurar los valores de los atributos LDAP mediante las Reglas de transformación de emisión y utilizar la plantilla Enviar atributos LDAP como notificaciones. A continuación, configure los ajustes LDAP que incluyen:
  - Direcciones de correo electrónico
  - sAMAccountName
  - User Principal Name (UPN)
  - MemberOf
- Firma del certificado. Puede especificar los certificados de verificación de firma seleccionando las Propiedades de una parte de confianza y luego agregando el certificado.

  Si el certificado de firma es inferior a 2048 bits, aparece un mensaje de advertencia. Puede ignorar la advertencia para continuar. Si está configurando una implementación de prueba, deshabilite la Lista de revocación de certificados (CRL) en la parte de confianza. Si no deshabilita la comprobación, AD FS intentará usar la CRL para validar el certificado.

  Puede deshabilitar la CRL ejecutando el siguiente comando: Set-ADFWRelayingPartyTrust -SigningCertficateRevocatonCheck None-TargetName NetScaler®

Después de configurar los ajustes, verificar los datos de la parte de confianza antes de completar el Asistente para la confianza de la parte de confianza. Compruebe el certificado del servidor virtual de NetScaler Gateway con la URL del punto final, como `https://vserver.fqdn.com/cgi/samlauth`.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Después de terminar de configurar los ajustes en el Asistente para la confianza de la parte de confianza, seleccione la confianza configurada y, a continuación, edite las propiedades. Realice lo siguiente:

- Establezca el algoritmo hash seguro en SHA-1.

  Nota: NetScaler solo admite SHA-1.
- Elimine el certificado de cifrado. Las aserciones cifradas no son compatibles.
- Edite las reglas de notificación, incluyendo lo siguiente:
  - Seleccionar regla de transformación
  - Agregar regla de notificación
  - Seleccionar plantilla de regla de notificación: Enviar atributos LDAP como notificaciones
  - Asignar un nombre
  - Seleccionar Almacén de atributos: Active Directory
  - Seleccionar atributo LDAP: \<parámetros de Active Directory\>
  - Seleccionar Regla de reclamación saliente como "Name ID"

  Nota: Las etiquetas XML de nombre de atributo no son compatibles.
- Configure la URL de cierre de sesión único. La regla de reclamación es Enviar URL de cierre de sesión. La regla personalizada debe ser la siguiente:

```
=> issue(Type = "logoutURL", Value = "https://<adfs.fqdn.com>/adfs/
ls/", Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/
claimproperties/attributename"] =
"urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified");
```

Después de configurar los ajustes de AD FS, descargue el certificado de firma de AD FS y, a continuación, cree una clave de certificado en NetScaler Gateway. A continuación, puede configurar la autenticación SAML en NetScaler Gateway utilizando el certificado y la clave.

## Configuración de la autenticación SAML de dos factores

Puede configurar la autenticación SAML de dos factores. Al configurar la autenticación SAML con la autenticación LDAP, utilice las siguientes directrices:

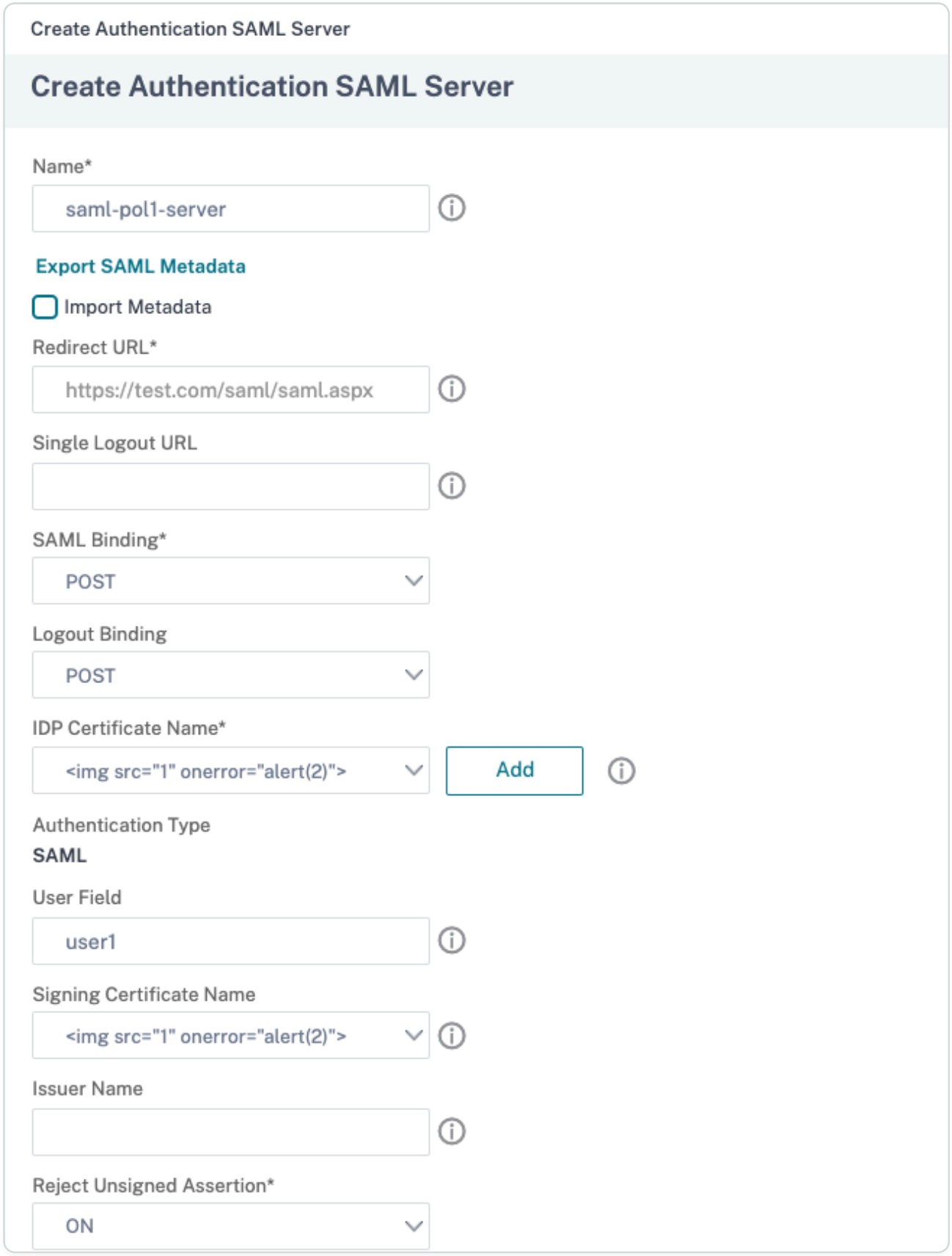
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Si SAML es el tipo de autenticación principal, deshabilite la autenticación en la política LDAP y configure la extracción de grupos. Luego, vincule la política LDAP como el tipo de autenticación secundaria.
- La autenticación SAML no utiliza una contraseña y solo usa el nombre de usuario. Además, la autenticación SAML solo informa a los usuarios cuando la autenticación se realiza correctamente. Si la autenticación SAML falla, los usuarios no son notificados. Dado que no se envía una respuesta de fallo, SAML debe ser la última política en la cascada o la única política.
- Se recomienda configurar nombres de usuario reales en lugar de cadenas opacas.
- SAML no se puede vincular como tipo de autenticación secundaria.

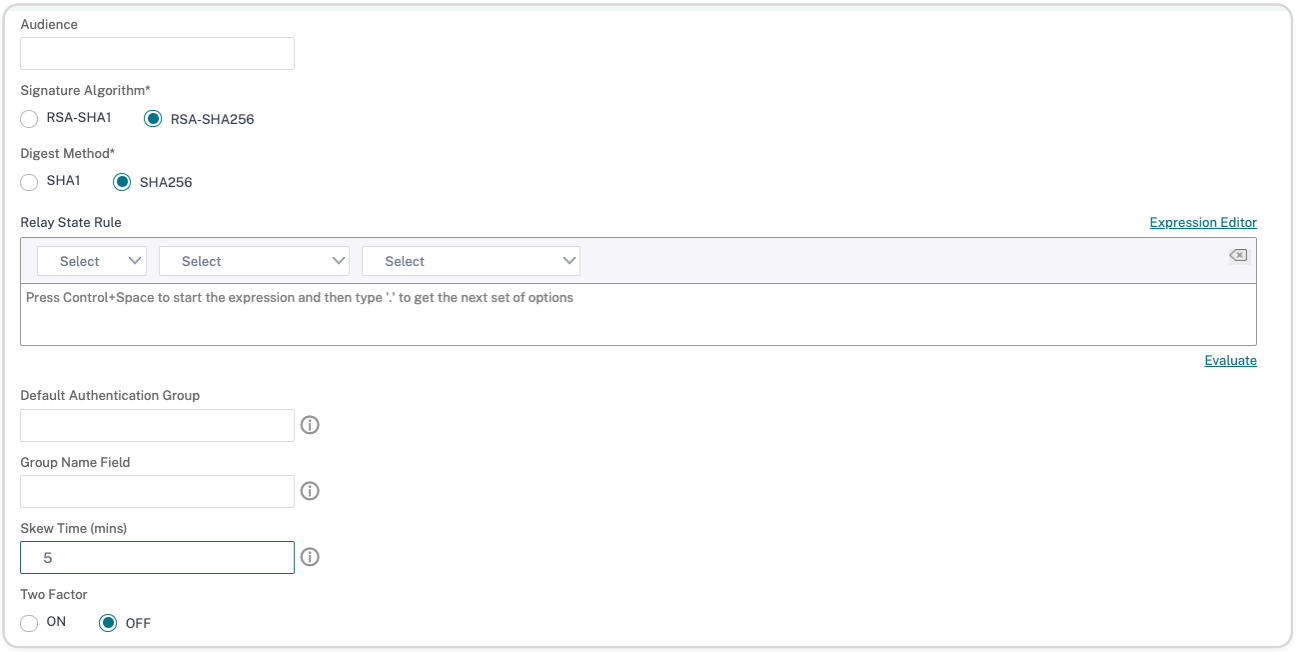
## Para configurar la autenticación SAML

1. En la utilidad de configuración, en la ficha Configuración, expanda **NetScaler Gateway > Directivas > Autenticación**.
2. En el panel de navegación, haga clic en **SAML**.
3. En el panel de detalles, haga clic en **Agregar**.
4. En el cuadro de diálogo Crear directiva de autenticación, en **Nombre**, escriba un nombre para la directiva.

© 1997–2026 Citrix Systems, Inc. All rights reserved.




© 1997–2026 Citrix Systems, Inc. All rights reserved.




1. Junto a Servidor, haga clic en **Nuevo**.
2. En **Nombre**, escriba un nombre para el perfil de servidor.
3. En Nombre del certificado de IdP, seleccione un certificado o haga clic en **Instalar**. Este es el certificado instalado en el servidor SAML o IdP.

   Si hace clic en Instalar, agregue el certificado y la clave privada. Para obtener más información, consulte Instalar y administrar certificados.
4. En **URL de redirección**, introduzca la URL del proveedor de identidades (IdP) de autenticación.

   Esta es la URL para el inicio de sesión del usuario en el servidor SAML. Este es el servidor al que NetScaler Gateway redirige la solicitud inicial.
5. En **URL de cierre de sesión único**, especifique la URL para que el dispositivo pueda reconocer cuándo enviar al cliente de vuelta al IdP para completar el proceso de cierre de sesión.
6. En **Enlace SAML**, seleccione el método que se utilizará para mover el cliente del SP al IdP. Esto debe ser lo mismo en el IdP para que entienda cómo se conecta el cliente a él. Cuando el dispositivo actúa como SP, admite enlaces POST, REDIRECT y ARTIFACT.
7. En **Logout Binding**, seleccione **REDIRECT.**
8. En **IDP Certificate Name**, seleccione el certificado IdPCert (Base64) presente en SAML Signing Certificate.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**NOTA:**

También puede hacer clic en **Import Metadata** y seleccionar la URL donde se almacena la configuración de metadatos.

9. En **User Field**, introduzca el nombre de usuario que desea extraer.
10. En **Signing Certificate Name**, seleccione el certificado SAML SP (con clave privada) que el dispositivo utiliza para firmar las solicitudes de autenticación al IdP. El mismo certificado (sin clave privada) debe importarse al IdP, para que el IdP pueda verificar la firma de la solicitud de autenticación. La mayoría de los IdP no necesitan este campo.

    Este es el certificado que está vinculado a la dirección IP virtual de NetScaler Gateway. El nombre del emisor SAML (SAML Issuer Name) es el nombre de dominio completo (FQDN) al que los usuarios inician sesión, como lb.example.com o ng.example.com.
11. En **Issuer Name**, introduzca el FQDN de la dirección IP virtual de equilibrio de carga o de NetScaler Gateway a la que el dispositivo envía la solicitud de autenticación inicial (GET).
12. En **Reject unsigned assertion**, especifique si requiere que las aserciones del IdP estén firmadas. Puede asegurarse de que solo la aserción debe estar firmada (ON) o de que tanto la aserción como la respuesta del IdP deben estar firmadas (STRICT).
13. En **Audience**, introduzca la audiencia a la que se aplica la aserción enviada por el IdP. Normalmente, es un nombre de entidad o una URL que representa al proveedor de servicios.
14. En **Signature Algorithm**, seleccione RSA-SHA256
15. En **Digest Method**, seleccione SHA256
16. En **Default Authentication Group**, introduzca el grupo predeterminado que se elige cuando la autenticación se realiza correctamente, además de los grupos extraídos.
17. En **Group Name**, introduzca el nombre de la etiqueta en la aserción que contiene los grupos de usuarios.
18. En **Skew Time (mins)**, especifique la desviación de reloj permitida en minutos que el proveedor de servicios permite en una aserción entrante.
19. Haga clic en **Crear** y, a continuación, en **Cerrar**.
20. En el cuadro de diálogo Crear directiva de autenticación, junto a Expresiones con nombre, seleccione General, seleccione Valor verdadero, haga clic en **Agregar expresión**, haga clic en **Crear** y, a continuación, haga clic en **Cerrar**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

### Referencias

- NetScaler como SP de SAML
- NetScaler como IdP de SAML
- Funciones adicionales compatibles con SAML

## Mejoras en la autenticación SAML

Esta función requiere conocimientos de SAML, dominio fundamental de la autenticación y comprensión de FIPS para utilizar esta información.

Puede utilizar las siguientes funciones de NetScaler con aplicaciones y servidores de terceros compatibles con la especificación SAML 2.0:

- Proveedor de servicios SAML (SP)
- Proveedor de identidades SAML (IdP)

SP e IdP permiten un inicio de sesión único (SSO) entre servicios en la nube. La función SAML SP proporciona una forma de abordar las reclamaciones de usuario de un IdP. El IdP puede ser un servicio de terceros u otro dispositivo NetScaler. La función SAML IdP se utiliza para afirmar los inicios de sesión de los usuarios y proporcionar reclamaciones consumidas por los SP.

Como parte del soporte SAML, tanto los módulos IdP como SP firman digitalmente los datos que se envían a los pares. La firma digital incluye una solicitud de autenticación del SP, una aserción del IdP y mensajes de cierre de sesión entre estas dos entidades. La firma digital valida la autenticidad del mensaje.

Las implementaciones actuales de SAML SP e IdP realizan el cálculo de la firma en un motor de paquetes. Estos módulos utilizan certificados SSL para firmar los datos. En un NetScaler compatible con FIPS, la clave privada del certificado SSL no está disponible en el motor de paquetes o en el espacio de usuario, por lo que el módulo SAML actual no está preparado para hardware FIPS.

Este documento describe el mecanismo para descargar los cálculos de firma a la tarjeta FIPS. La verificación de la firma se realiza en el software, ya que la clave pública está disponible.

### Solución

El conjunto de funciones SAML se ha mejorado para utilizar una API SSL para la descarga de firmas. Consulte la documentación del producto NetScaler® para obtener detalles sobre estas subfunciones SAML afectadas:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Enlace de publicación de SAML SP – Firma de AuthnRequest
2. Enlace de publicación de SAML IdP – Firma de aserción/respuesta/ambos
3. Escenarios de cierre de sesión único de SAML SP – Firma de LogoutRequest en el modelo iniciado por SP y firma de LogoutResponse en el modelo iniciado por IdP
4. Enlace de artefacto SAML SP – Firma de la solicitud ArtifactResolve
5. SAML SP Redirect Binding – Firma de AuthnRequest
6. SAML IdP Redirect Binding – Firma de Response/Assertion/Ambos
7. Soporte de cifrado SAML SP – Descifrado de Assertion

### Plataforma

La API solo se puede descargar a una plataforma FIPS.

### Configuración

La configuración de descarga se realiza automáticamente en la plataforma FIPS.

Sin embargo, dado que las claves privadas SSL no están disponibles para el espacio de usuario en el hardware FIPS, hay un ligero cambio en la configuración al crear el certificado SSL en el hardware FIPS.

Aquí está la información de configuración:

- `add ssl fipsKey fips-key`

  Cree un CSR y úselo en el servidor CA para generar un certificado. Luego puede copiar ese certificado en `/nsconfig/ssl`. Supongamos que el archivo es fips3cert.cer.
- `add ssl certKey fips-cert -cert fips3cert.cer -fipsKey fips-key`

  Luego especifique este certificado en la acción SAML para el módulo SAML SP.
- `set samlAction <name> -samlSigningCertName fips-cert`

  Del mismo modo, utiliza esto en el `samlIdpProfile` para el módulo SAML IdP.
- `set samlidpprofile fipstest –samlIdpCertName fips-cert`

La clave FIPS no está disponible la primera vez. Si no hay una clave FIPS, cree una como se describe en Crear una clave FIPS.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
create ssl fipskey <fipsKeyName> -modulus <positive_integer> [-exponent (3
| F4)]



create certreq <reqFileName> -fipskeyName <string>
```

## Uso de la autenticación SAML para iniciar sesión en NetScaler Gateway

Puede usar la autenticación SAML para iniciar sesión en NetScaler Gateway mediante los clientes VPN y la aplicación Workspace. El complemento admite la autenticación SAML solo a través de directivas SAML avanzadas vinculadas al servidor virtual de autenticación, es decir, la autenticación nFactor.

**IMPORTANTE:**

El complemento no admite la autenticación SAML cuando las directivas SAML están vinculadas directamente al servidor virtual VPN, es decir, la autenticación no nFactor.

### Plataformas y aplicaciones compatibles

La siguiente tabla enumera las plataformas y aplicaciones que admiten la autenticación SAML para iniciar sesión en NetScaler Gateway.

| PRODUCTO | VERSIÓN |
|---|---|
| NetScaler Gateway | Versión 12.0 compilación 41.16 y posteriores |
| Cliente VPN | Versión 12.1 compilación 49.37 y posteriores. **Plataformas compatibles**: Windows 7, Windows 8, Windows 8.1, Windows 10 |
| Versiones de la aplicación Workspace | Windows: 1808; Mac: 1808 |

### Configurar la autenticación SAML mediante directivas SAML avanzadas

Para obtener detalles sobre la configuración de la autenticación SAML mediante políticas SAML avanzadas, consulte NetScaler como IdP SAML.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

# Configuración de la autenticación TACACS+

Puede configurar un servidor TACACS+ para la autenticación. Al igual que la autenticación RADIUS, TACACS+ utiliza una clave secreta, una dirección IP y el número de puerto. El número de puerto predeterminado es 49.

Para configurar NetScaler Gateway para que utilice un servidor TACACS+, proporcione la dirección IP del servidor y el secreto de TACACS+. Solo necesita especificar el puerto cuando el número de puerto del servidor en uso sea diferente del número de puerto predeterminado 49.

Para configurar la autenticación TACACS+ mediante la interfaz de usuario, siga estos pasos.

1. En la utilidad de configuración, en la ficha Configuración, expanda **NetScaler Gateway > Directivas > Autenticación**.
2. Haga clic en **TACACS**.
3. En el panel de detalles, haga clic en **Agregar**.
4. En el campo **Nombre**, escriba un nombre para la directiva.
5. Junto al campo **Servidor**, haga clic en **Agregar** para crear un nuevo servidor TACACS o haga clic en **Modificar** para realizar cambios en un servidor TACACS existente.
6. En el campo **Nombre**, escriba un nombre para el servidor.
7. En **Dirección IP**, escriba la dirección IP.
8. En **Puerto**, utilice el número de puerto predeterminado 49.
9. En el campo **Clave TACACS**, escriba la clave. En el campo **Confirmar clave TACACS**, escriba la misma clave para confirmar.
10. Haga clic en **Más**.
11. En **Autorización**, seleccione **ACTIVADO** y, a continuación, haga clic en **Crear**.
12. En el cuadro de diálogo **Crear directiva de autenticación TACACS**, seleccione la expresión, haga clic en Crear y, a continuación, haga clic en Cerrar.

Para configurar la autenticación TACACS+ mediante la interfaz de línea de comandos, escriba el siguiente comando.

```
add authentication tacacsAction <name> [-serverIP <ip_addr|ipv6_addr|*>][-
serverPort <port>] [-authTimeout <positive_integer>] {-tacacsSecret }

[-authorization ( ON | OFF )] [-accounting ( ON | OFF )][-auditFailedCmds
( ON | OFF )] [-groupAttrName <string>][-defaultAuthenticationGroup
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
<string>] [-Attribute1 <string>] [-Attribute2 <string>] [-Attribute3
<string>] [-Attribute4 <string>]

[-Attribute5 <string>] [-Attribute6 <string>] [-Attribute7 <string>] [-
Attribute8 <string>] [-Attribute9 <string>] [-Attribute10 <string>]

[-Attribute11 <string>] [-Attribute12 <string>] [-Attribute13 <string>] [-
Attribute14 <string>] [-Attribute15 <string>] [-Attribute16 <string>]
```

Después de configurar los ajustes del servidor TACACS+ en NetScaler Gateway, enlace la directiva para activarla. Puede enlazar la directiva a nivel global o de servidor virtual. Para obtener más información sobre el enlace de directivas de autenticación, consulte Enlace de directivas de autenticación.

## Borrar Configuración Básica No Debe Borrar la Configuración TACACS

Este tema se centra en no borrar todas las configuraciones relacionadas con RBA (Acceso Basado en Roles) cuando se ejecuta el comando de borrar configuración.

El comando actual de borrar configuración se ejecuta en uno de tres niveles:

- Básico
- Extendido
- Completo

Según el nivel, las configuraciones de NetScaler se borran y se restablecen a los valores predeterminados de fábrica.

El comando utilizado es;

```
clear ns config [-force] <level>
```

El nuevo comando añade una opción para permitir/denegar la eliminación de todas las configuraciones relacionadas con RBA.

### Nuevo Comando

Se describen las características de la configuración de Borrar RBA:

1. Opción SÍ/NO con Valor predeterminado: SÍ.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

El administrador decide si conservar la configuración RBA o no.

2. SOLO se admite el NIVEL BÁSICO de borrar configuración.
3. Las siguientes configuraciones no se borran:

   - Añadir/vincular usuario/grupo del sistema.
   - Añadir política de comandos.
   - Comandos TACACS (añadir acción/política TACACS).
   - Vincular global del sistema

   **Nota:** La configuración relacionada con TACACS (acción/política) se conserva si la política está vinculada al sistema global; de lo contrario, se borra.

### Configuración de CLI

El comando utilizado es;

```
clear config [–force] <level> [-RBAconfig]
```

Por defecto, está configurado en SÍ y borra las configuraciones según el nivel.

Si –`RBAconfig` se establece en NO, la configuración relacionada con RBA se mantiene. Se incluye lo siguiente:

- Añadir/vincular usuario/grupo del sistema
- Vincular global del sistema
- Comandos relacionados con TACACS (añadir acción/política TACACS)
- Añadir política de comandos

## Configuración de la autenticación multifactor

Puede configurar dos tipos de autenticación multifactor en NetScaler Gateway:

- Autenticación en cascada que establece el nivel de prioridad de autenticación
- Autenticación de dos factores que requiere que los usuarios inicien sesión mediante dos tipos de autenticación

Si tiene varios servidores de autenticación, puede establecer la prioridad de sus políticas de autenticación. Los niveles de prioridad que establezca determinarán el orden en que el servidor de

© 1997–2026 Citrix Systems, Inc. All rights reserved.

autenticación valida las credenciales de los usuarios. Una política con un número de prioridad más bajo tiene preferencia sobre una política con un número más alto.

Puede hacer que los usuarios se autentiquen contra dos servidores de autenticación diferentes. Por ejemplo, puede configurar una política de autenticación LDAP y una política de autenticación RSA. Cuando los usuarios inician sesión, primero se autentican con su nombre de usuario y contraseña. Luego, se autentican con un número de identificación personal (PIN) y el código del token RSA.

## Configuración de la autenticación en cascada

La autenticación le permite crear una cascada de varios servidores de autenticación mediante la priorización de políticas. Al configurar una cascada, el sistema recorre cada servidor de autenticación, según lo definido por las políticas en cascada, para validar las credenciales de un usuario. Las políticas de autenticación priorizadas se organizan en cascada en orden ascendente y pueden tener valores de prioridad en el rango de 1 a 9999. Estas prioridades se definen al vincular las políticas a nivel global o de servidor virtual.

Durante la autenticación, cuando un usuario inicia sesión, se comprueba primero el servidor virtual y luego las políticas de autenticación globales. Si un usuario pertenece a una política de autenticación tanto en el servidor virtual como a nivel global, se aplica primero la política del servidor virtual y luego la política de autenticación global. Si desea que los usuarios reciban la política de autenticación vinculada globalmente, cambie la prioridad de la política. Cuando una política de autenticación global tiene un número de prioridad de uno y una política de autenticación vinculada a un servidor virtual tiene un número de prioridad de dos, la política de autenticación global tiene prioridad. Por ejemplo, puede tener tres políticas de autenticación vinculadas al servidor virtual y puede establecer la prioridad de cada política.

Si un usuario no se autentica con una política en la cascada principal, o si ese usuario se autentica correctamente con una política en la cascada principal pero no se autentica con una política en la cascada secundaria, el proceso de autenticación se detiene y el usuario es redirigido a una página de error.

Nota: Citrix® recomienda que, al vincular varias políticas a un servidor virtual o globalmente, defina prioridades únicas para todas las políticas de autenticación.

### Para establecer la prioridad de las políticas de autenticación globales

1. En la utilidad de configuración, en la ficha Configuración, expanda **NetScaler Gateway > Directivas > Autenticación**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Seleccione la directiva vinculada globalmente y, a continuación, en **Acción**, haga clic en **Enlaces globales**.
3. En el cuadro de diálogo **Vincular/Desvincular directivas globales de autenticación**, en Prioridad, escriba el número y, a continuación, haga clic en **Aceptar**.

### Para cambiar la prioridad de una política de autenticación vinculada a un servidor virtual

También puede modificar una política de autenticación vinculada a un servidor virtual.

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda **NetScaler Gateway** y, a continuación, haga clic en **Servidores virtuales**.
2. En el panel de detalles, seleccione un servidor virtual y, a continuación, haga clic en **Abrir**.
3. Haga clic en la ficha **Autenticación** y, a continuación, haga clic en **Principal** o **Secundaria**.
4. Junto a la política de autenticación, en **Prioridad**, escriba el número y, a continuación, haga clic en **Aceptar**.

## Configuración de la autenticación de dos factores

NetScaler Gateway admite la autenticación de dos factores. Normalmente, al autenticar usuarios, NetScaler Gateway detiene el proceso de autenticación tan pronto como autentica correctamente a un usuario a través de cualquiera de los métodos de autenticación configurados. En ciertos casos, es posible que deba autenticar a un usuario en un servidor, pero extraer grupos de un servidor diferente. Por ejemplo, si su red autentica a los usuarios en un servidor RADIUS, pero también utiliza la autenticación de tokens RSA SecurID y los grupos de usuarios se almacenan en ese servidor, es posible que deba autenticar a los usuarios en ese servidor para poder extraer los grupos.

Si los usuarios se autentican mediante dos tipos de autenticación, y si uno de esos tipos es la autenticación de certificado de cliente, puede configurar la directiva de autenticación de certificado como el segundo método de autenticación. Por ejemplo, utiliza LDAP como tipo de autenticación principal y el certificado de cliente como autenticación secundaria. Cuando los usuarios inician sesión con su nombre de usuario y contraseña, tienen acceso a los recursos de red.

Al configurar la autenticación de dos factores, selecciona si el tipo de autenticación es el tipo principal o secundario.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

### Para configurar la autenticación de dos factores

1. En la utilidad de configuración, en la ficha Configuración, expanda NetScaler Gateway \> Directivas \> Autenticación.
2. En la ficha Directivas, haga clic en Enlaces globales.
3. En el cuadro de diálogo Enlazar/Desenlazar directivas de autenticación a global, haga clic en Principal.
4. Haga clic en Insertar directiva.
5. En Nombre de directiva, seleccione la directiva de autenticación.
6. Haga clic en Secundario, repita los pasos 4 y 5 y, a continuación, haga clic en Aceptar.

## Seleccionar el tipo de autenticación para el inicio de sesión único

Si tiene el inicio de sesión único y la autenticación de dos factores configurados en NetScaler Gateway, puede seleccionar qué contraseña usar para el inicio de sesión único. Por ejemplo, tiene LDAP configurado como el tipo de autenticación principal y RADIUS configurado como el tipo de autenticación secundaria. Cuando los usuarios acceden a recursos que requieren inicio de sesión único, el nombre de usuario y la contraseña principal se envían de forma predeterminada. Usted establece qué contraseña se debe usar para el inicio de sesión único en las aplicaciones web dentro de un perfil de sesión.

### Para configurar la autenticación para el inicio de sesión único

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda **NetScaler Gateway > Directivas > Sesión**.
2. En el panel de detalles, haga clic en la ficha **Perfiles** y, a continuación, realice una de las siguientes acciones:
   - Para crear un nuevo perfil, haga clic en **Agregar**.
   - Para modificar un perfil existente, haga clic en **Abrir**.
3. En la ficha Experiencia del cliente, junto a Índice de credenciales, haga clic en **Anular global** y seleccione **Principal** o **Secundario**.
4. Si se trata de un nuevo perfil, haga clic en **Crear** y, a continuación, haga clic en **Cerrar**.
5. Si está modificando un perfil existente, haga clic en **Aceptar**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

### Configuración de certificados de cliente y autenticación de dos factores LDAP

Puede utilizar un certificado de cliente seguro con autenticación y autorización LDAP, como el uso de autenticación con tarjeta inteligente con LDAP. El usuario inicia sesión y, a continuación, el nombre de usuario se extrae del certificado de cliente. El certificado de cliente es la forma principal de autenticación y LDAP es la forma secundaria. La autenticación de certificado de cliente debe tener prioridad sobre la directiva de autenticación LDAP. Al establecer la prioridad de las directivas, asigne un número inferior a la directiva de autenticación de certificado de cliente que el número que asigne a la directiva de autenticación LDAP.

Para utilizar un certificado de cliente, debe tener una entidad de certificación (CA) empresarial, como los Servicios de certificados en Windows Server 2008, ejecutándose en el mismo equipo que ejecuta Active Directory. Puede utilizar la CA para crear un certificado de cliente.

Para utilizar un certificado de cliente con autenticación y autorización LDAP, debe ser un certificado seguro que utilice Secure Sockets Layer (SSL). Para utilizar certificados de cliente seguros para LDAP, instale el certificado de cliente en el dispositivo de usuario e instale un certificado raíz correspondiente en NetScaler Gateway.

Antes de configurar un certificado de cliente, haga lo siguiente:

- Cree un servidor virtual.
- Cree una directiva de autenticación LDAP para el servidor LDAP.
- Establezca la expresión de la directiva LDAP en valor Verdadero.

#### Para configurar la autenticación de certificado de cliente con LDAP

1. En la utilidad de configuración, en la ficha Configuración, expanda **NetScaler Gateway \> Directivas \> Autenticación**.
2. En el panel de navegación, en Autenticación, haga clic en Cert.
3. En el panel de detalles, haga clic en Agregar.
4. En Nombre, escriba un nombre para la directiva.
5. En Tipo de autenticación, seleccione Cert.
6. Junto a Servidor, haga clic en Nuevo.
7. En Nombre, escriba un nombre para el servidor y, a continuación, haga clic en Crear.
8. En el cuadro de diálogo Crear servidor de autenticación, en Nombre, escriba el nombre del servidor.
9. Junto a Doble factor, seleccione ACTIVADO.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

10. En el campo Nombre de usuario, seleccione Asunto:CN y, a continuación, haga clic en Crear.
11. En el cuadro de diálogo Crear directiva de autenticación, junto a Expresiones con nombre, seleccione Valor verdadero, haga clic en Agregar expresión, haga clic en Crear y, a continuación, haga clic en Cerrar.

Después de crear la directiva de autenticación de certificados, vincule la directiva al servidor virtual. Después de vincular la directiva de autenticación de certificados, vincule la directiva de autenticación LDAP al servidor virtual.

**IMPORTANTE:**

Debe vincular la directiva de autenticación de certificados al servidor virtual antes de vincular la directiva de autenticación LDAP al servidor virtual.

### Para instalar un certificado raíz en NetScaler Gateway

Después de crear la directiva de autenticación de certificados, descargue e instale un certificado raíz de su CA en formato Base64 y guárdelo en su equipo. A continuación, puede cargar el certificado raíz en NetScaler Gateway.

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda SSL y, a continuación, haga clic en Certificados.
2. En el panel de detalles, haga clic en Instalar.
3. En Nombre de par de claves de certificado, escriba un nombre para el certificado.
4. En Nombre de archivo de certificado, haga clic en Examinar y, en la lista, seleccione Dispositivo o Local.
5. Vaya al certificado raíz, haga clic en Abrir y, a continuación, haga clic en Instalar.

### Para añadir un certificado raíz a un servidor virtual

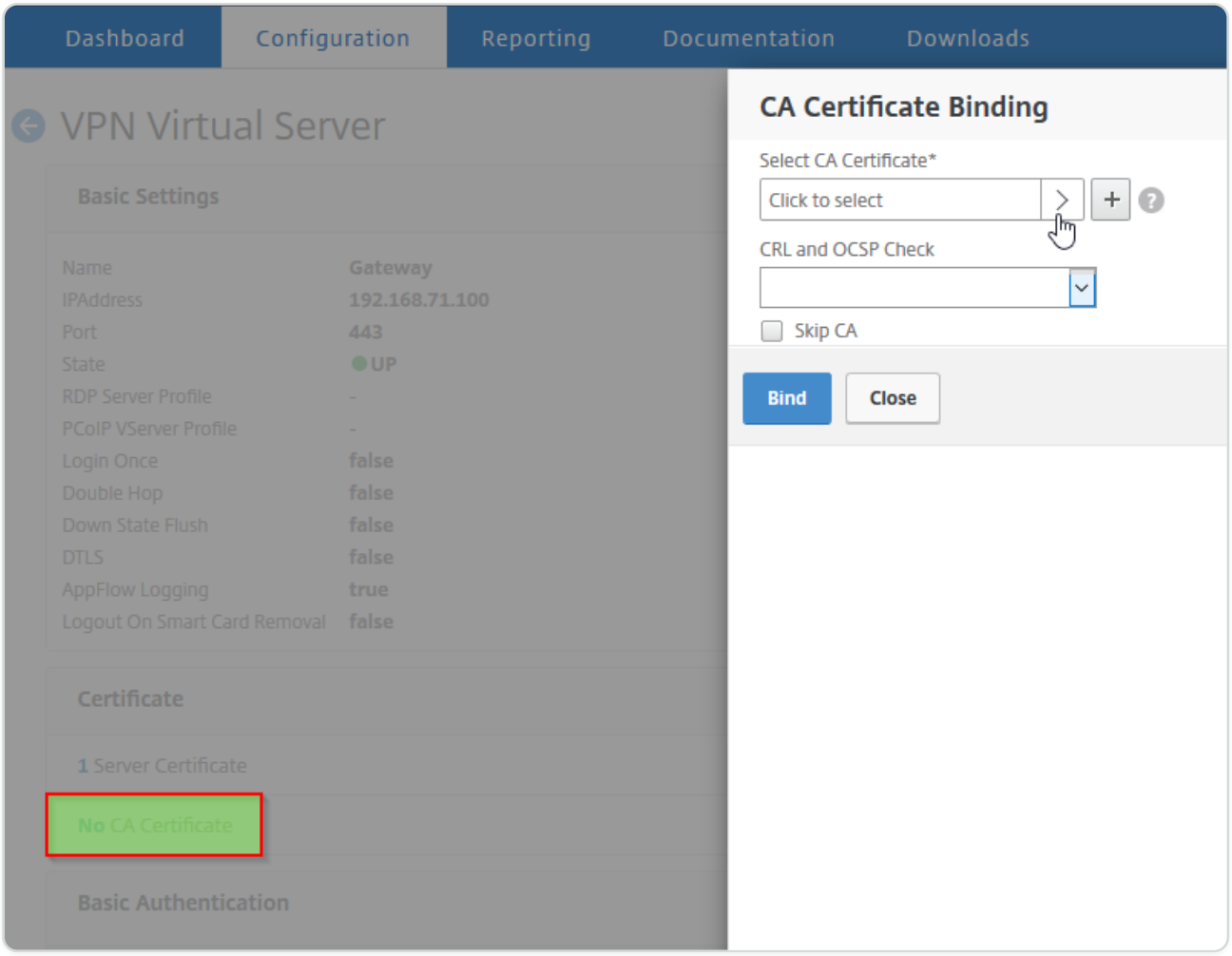
Después de instalar el certificado raíz en NetScaler Gateway, añada el certificado al almacén de certificados del servidor virtual.

**IMPORTANTE:**

Cuando agregue el certificado raíz al servidor virtual para la autenticación con tarjeta inteligente, debe seleccionar el certificado en el cuadro de lista **Seleccionar certificado de CA**, como se muestra en la siguiente figura.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Figura 1. Adición de un certificado raíz como CA




1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda NetScaler Gateway y, a continuación, haga clic en Servidores virtuales.
2. En el panel de detalles, seleccione un servidor virtual y, a continuación, haga clic en Abrir.
3. En la ficha Certificados, en Disponible, seleccione el certificado, junto a Agregar, en la lista, haga clic en CA y, a continuación, haga clic en Aceptar.
4. Repita el paso 2.
5. En la ficha Certificados, haga clic en Parámetros SSL.
6. En Otros, seleccione Autenticación de cliente.
7. En Otros, junto a Certificado de cliente, seleccione Opcional y, a continuación, haga clic en Aceptar dos veces.
8. Después de configurar el certificado de cliente, pruebe la autenticación iniciando sesión en NetScaler Gateway con el cliente Citrix Secure Access. Si tiene más de un certificado instalado, recibirá un mensaje pidiéndole que seleccione el certificado correcto. Después de seleccionar el certificado, aparece la pantalla de inicio de sesión con el nombre de usuario

© 1997–2026 Citrix Systems, Inc. All rights reserved.

rellenado con la información obtenida del certificado. Escriba la contraseña y, a continuación, haga clic en Iniciar sesión.

Si no ve el nombre de usuario correcto en el campo Nombre de usuario de la pantalla de inicio de sesión, compruebe las cuentas de usuario y los grupos en su directorio LDAP. Los grupos definidos en NetScaler Gateway deben ser los mismos que los del directorio LDAP. En Active Directory, configure los grupos en el nivel raíz del dominio. Si crea grupos de Active Directory que no están en el nivel raíz del dominio, puede producirse una lectura incorrecta del certificado de cliente.

Si los usuarios y grupos no están en el nivel raíz del dominio, la página de inicio de sesión de NetScaler Gateway muestra el nombre de usuario configurado en Active Directory. Por ejemplo, en Active Directory, tiene una carpeta llamada Usuarios y el certificado dice CN=Users. En la página de inicio de sesión, en Nombre de usuario, aparece la palabra Usuarios.

Si no desea mover sus cuentas de grupo y de usuario al nivel raíz del dominio, al configurar el servidor de autenticación de certificados en NetScaler Gateway, deje en blanco los campos Nombre de usuario y Nombre de grupo.

# Configuración del inicio de sesión único

Puede configurar NetScaler Gateway para admitir el inicio de sesión único con Windows, para aplicaciones web (como SharePoint), para recursos compartidos de archivos y para StoreFront. El inicio de sesión único también se aplica a los recursos compartidos de archivos a los que los usuarios pueden acceder a través de la utilidad de transferencia de archivos en la interfaz de acceso o desde el menú del icono de NetScaler Gateway en el área de notificación.

Si configura el inicio de sesión único cuando los usuarios inician sesión, se inician sesión automáticamente de nuevo sin tener que introducir sus credenciales por segunda vez.

## Configuración del inicio de sesión único con Windows

Los usuarios abren una conexión iniciando el cliente Citrix Secure Access desde el escritorio. Puede especificar que el cliente Citrix Secure Access se inicie automáticamente cuando el usuario inicie sesión en Windows habilitando el inicio de sesión único. Cuando configura el inicio de sesión único, las credenciales de inicio de sesión de Windows de los usuarios se pasan a NetScaler Gateway para la autenticación. La habilitación del inicio de sesión único para el cliente Citrix Secure Access facilita las operaciones en el dispositivo del usuario, como los scripts de instalación y la asignación automática de unidades.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Habilite el inicio de sesión único solo si los dispositivos de usuario inician sesión en el dominio de su organización. Si el inicio de sesión único está habilitado y un usuario se conecta desde un dispositivo que no está en su dominio, se le pedirá al usuario que inicie sesión.

Puede configurar el inicio de sesión único con Windows de forma global o mediante un perfil de sesión asociado a una directiva de sesión.

### Para configurar el inicio de sesión único con Windows globalmente

1. En la utilidad de configuración, en la ficha **Configuración**, en el panel de navegación, expanda **NetScaler Gateway** y, a continuación, haga clic en **Configuración global**.
2. En el panel de detalles, en **Configuración**, haga clic en **Cambiar configuración global**.
3. En la ficha **Experiencia del cliente**, haga clic en **Inicio de sesión único con Windows** y, a continuación, haga clic en **Aceptar**.

### Para configurar el inicio de sesión único con Windows mediante una directiva de sesión

1. En la utilidad de configuración, en la ficha **Configuración**, en el panel de navegación, expanda **NetScaler Gateway > Directivas** y, a continuación, haga clic en **Sesión**.
2. En el panel de detalles, haga clic en **Agregar**.
3. En **Nombre**, escriba un nombre para la directiva.
4. Junto a **Perfil de solicitud**, haga clic en **Nuevo**.
5. En **Nombre**, escriba un nombre para el perfil.
6. En la ficha **Experiencia del cliente**, junto a **Inicio de sesión único con Windows**, haga clic en **Anular global**, haga clic en **Inicio de sesión único con Windows** y, a continuación, haga clic en **Aceptar**.
7. En el cuadro de diálogo **Crear directiva de sesión**, junto a **Expresiones con nombre**, seleccione **General**, seleccione el valor Verdadero, haga clic en **Agregar expresión**, haga clic en **Crear** y, a continuación, haga clic en **Cerrar**.

## Configuración del inicio de sesión único para aplicaciones web

Puede configurar NetScaler Gateway para proporcionar inicio de sesión único a servidores de la red interna que utilizan autenticación basada en web. Con el inicio de sesión único, puede redirigir al usuario a una página de inicio personalizada, como un sitio de SharePoint o a StoreFront. También puede configurar el inicio de sesión único para los recursos a través del cliente Citrix

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Secure Access desde un marcador configurado en la página de inicio o una dirección web que los usuarios escriban en el explorador web.

Si va a redirigir la página de inicio a un sitio de SharePoint o a StoreFront, proporcione la dirección web del sitio. Cuando los usuarios se autentican, ya sea por NetScaler Gateway o por un servidor de autenticación externo, se les redirige a la página de inicio especificada. Las credenciales de usuario se pasan de forma transparente al servidor web. Si el servidor web acepta las credenciales, los usuarios inician sesión automáticamente. Si el servidor web deniega las credenciales, los usuarios reciben un mensaje de autenticación solicitando su nombre de usuario y contraseña.

Puede configurar el inicio de sesión único para aplicaciones web de forma global o mediante una directiva de sesión.

### Para configurar el inicio de sesión único para aplicaciones web globalmente

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda NetScaler Gateway y, a continuación, haga clic en Configuración global.
2. En el panel de detalles, en Configuración, haga clic en Cambiar configuración global.
3. En la ficha Experiencia de cliente, haga clic en Inicio de sesión único para aplicaciones web y, a continuación, haga clic en Aceptar.

### Para configurar el inicio de sesión único para aplicaciones web mediante una directiva de sesión

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda NetScaler Gateway \> Directivas y, a continuación, haga clic en Sesión.
2. En el panel de detalles, en la ficha Directivas, seleccione una directiva de sesión y, a continuación, haga clic en Abrir.
3. En el cuadro de diálogo Configurar directiva de sesión, junto a Perfil de solicitud, haga clic en Modificar.
4. En la ficha Experiencia de cliente, junto a Inicio de sesión único para aplicaciones web, haga clic en Anulación global, haga clic en Inicio de sesión único para aplicaciones web y, a continuación, haga clic en Aceptar.

### Para definir el puerto HTTP para el inicio de sesión único en aplicaciones web

El inicio de sesión único solo se intenta para el tráfico de red donde el puerto de destino se considera un puerto HTTP. Para permitir el inicio de sesión único en aplicaciones que utilizan un

© 1997–2026 Citrix Systems, Inc. All rights reserved.

puerto distinto del puerto 80 para el tráfico HTTP, agregue uno o varios números de puerto en NetScaler Gateway. Puede habilitar varios puertos. Los puertos se configuran globalmente.

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda NetScaler Gateway y, a continuación, haga clic en Configuración global.
2. En el panel de detalles, en Configuración, haga clic en Cambiar configuración global.
3. En la ficha Configuración de red, haga clic en Configuración avanzada.
4. En Puertos HTTP, escriba el número de puerto, haga clic en Agregar y, a continuación, haga clic en Aceptar dos veces.

   Puede repetir el paso 4 para cada puerto que desee agregar.

**Nota**: Si las aplicaciones web de la red interna utilizan direcciones IP públicas, el inicio de sesión único no funciona. Para habilitar el inicio de sesión único, la tunelización dividida debe estar habilitada como parte de la configuración de la directiva global, independientemente de si se utiliza el acceso sin cliente o el cliente Citrix Secure Access™ para las conexiones de dispositivos de usuario. Si no es posible habilitar la tunelización dividida a nivel global, cree un servidor virtual que utilice un rango de direcciones privadas.

## Configuración del inicio de sesión único en aplicaciones web mediante LDAP

Al configurar el inicio de sesión único y los usuarios inician sesión mediante el nombre principal de usuario (UPN) con un formato de username@domain.com, de forma predeterminada, el inicio de sesión único falla y los usuarios deben autenticarse dos veces. Si necesita usar este formato para el inicio de sesión del usuario, modifique la directiva de autenticación LDAP para aceptar esta forma de nombre de usuario.

### Para configurar el inicio de sesión único en aplicaciones web

1. En la utilidad de configuración, en la ficha **Configuración**, expanda **NetScaler Gateway > Directivas > Autenticación**.
2. En el panel de detalles, en la ficha **Directivas**, seleccione una directiva LDAP y, a continuación, haga clic en **Abrir**.
3. En el cuadro de diálogo **Configurar directiva de autenticación**, junto a **Servidor**, haga clic en **Modificar**.
4. En **Configuración de conexión**, en DN base (ubicación de los usuarios), escriba DC=domainname,DC=com.
5. En **DN de enlace de administrador**, escriba LDAPaccount@domainname.com, donde domainname.com es el nombre de su dominio.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

6. En **Contraseña de administrador** y **Confirmar contraseña de administrador**, escriba la contraseña.
7. En **Otras configuraciones**, en **Atributo de nombre de inicio de sesión del servidor**, escriba UserPrincipalName.
8. En **Atributo de grupo**, escriba memberOf.
9. En **Nombre de subatributo**, escriba CN.
10. En **Atributo de nombre de SSO**, escriba el formato mediante el cual los usuarios inician sesión y, a continuación, haga clic en **Aceptar** dos veces. Este valor es `SamAccountName` o `UserPrincipalName`.

## Configuración de inicio de sesión único en un dominio

Si los usuarios se conectan a servidores que ejecutan Citrix Virtual Apps™ y utilizan SmartAccess, puede configurar el inicio de sesión único para los usuarios que se conectan a la granja de servidores. Al configurar el acceso a las aplicaciones publicadas mediante una directiva y un perfil de sesión, utilice el nombre de dominio de la granja de servidores.

También puede configurar el inicio de sesión único para recursos compartidos de archivos en su red.

### Para configurar el inicio de sesión único en un dominio

1. En la utilidad de configuración, en la ficha Configuration (Configuración), en el panel de navegación, expanda NetScaler Gateway \> Policies (Directivas) y, a continuación, haga clic en Session (Sesión).
2. En el panel de detalles, en la ficha Policies (Directivas), seleccione una directiva de sesión y, a continuación, haga clic en Open (Abrir).
3. En el cuadro de diálogo Configure Session Policy (Configurar directiva de sesión), junto a Request Profile (Perfil de solicitud), haga clic en Modify (Modificar).
4. En el cuadro de diálogo Configure Session Profile (Configurar perfil de sesión), en la ficha Published Applications (Aplicaciones publicadas), en Single-sign-on Domain (Dominio de inicio de sesión único), haga clic en Override Global (Anular global), escriba el nombre de dominio y, a continuación, haga clic en OK (Aceptar) dos veces.

Para obtener más información sobre cómo configurar NetScaler Gateway con Citrix Virtual Apps, consulte Integrar NetScaler Gateway con Citrix Virtual Apps and Desktops.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

# Configuración del inicio de sesión único para Microsoft Exchange 2010

La siguiente sección describe la configuración del inicio de sesión único (SSO) para Microsoft Exchange 2010 en NetScaler Gateway. El SSO para Outlook Web Access (OWA) 2010 no funciona en las siguientes condiciones:

- Uso de la autenticación basada en formularios en Microsoft Exchange 2010.
- Servidor virtual de equilibrio de carga con política de administración de tráfico de autenticación, autorización y auditoría.

**NOTA:**

Esta configuración solo funciona para el servidor virtual de equilibrio de carga con política de administración de tráfico de autenticación, autorización y auditoría. No funciona para SSO en OWA 2010 con VPN sin cliente.

Los siguientes pasos son requisitos previos que debe considerar antes de configurar el SSO para Microsoft Exchange 2010 en NetScaler Gateway.

- La URL de acción para el formulario SSO es diferente en OWA 2010. Modifique la política de administración de tráfico en consecuencia.
- Necesita una política de reescritura para establecer la cookie `PBack` en la solicitud logon.aspx. En escenarios normales, establece la cookie `PBack` en el cliente y hace clic en Enviar.
- Cuando utiliza SSO, la respuesta a logon.aspx se consume y NetScaler Gateway genera la solicitud de formulario. La cookie no se adjunta en la solicitud de envío del formulario.
- El servidor OWA espera la cookie `PBack` en la solicitud de envío del formulario. Se requiere la política de reescritura para adjuntar la cookie `PBack` en la solicitud de envío del formulario.

### Realice lo siguiente mediante la CLI

1. Configure la administración de tráfico de autenticación, autorización y auditoría

   ```
   add tm formSSOAction OWA_Form_SSO_SSOPro -actionURL "/owa/auth.owa"
   -userField username -passwdField password -ssoSuccessRule
   "http.RES.SET_COOKIE.COOKIE(\"cadata\").VALUE(\"cadata\").LENGTH.GT(70"
   -responsesize 15000 -submitMethod POST
   ```

2. Configure la política de administración de tráfico y vincule la política

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- `add tm trafficAction OWA_2010_Prof -appTimeout 1 -SSO ON -formSSO Action OWA_Form_SSO_SSOPro`
- `add tm trafficPolicy owa2k10_pol "HTTP.REQ.URL.CONTAINS(\"owa/auth/logon.aspx\")" OWA_2010_Prof`
- `bind tm global -policyName owa2k10_pol -priority 100`

### Configuración de reescritura mediante la CLI

En el símbolo del sistema, escriba:

- `add rewrite action set_pback_cookie insert_after "http.REQ.COOKIE.VALUE(\"OutlookSession\")" "\";PBack=0\"" -bypassSafetyCheck YES`
- `add rewrite policy set_pback_cookie "http.REQ.URL.CONTAINS(\"logon.aspx\")" set_pback_cookie`
- `bind rewrite global set_pback_cookie 100 END -type REQ_DEFAULT`

#### Configuración de reescritura alternativa

En raras ocasiones, es posible que Microsoft Outlook no emita cookies de sesión de OWA y que las cookies `Pback` tampoco se inserten. El problema podría ocurrir después de haber ejecutado los comandos anteriores para implementar la configuración de reescritura.

Para superar estos escenarios y como solución alternativa, puede configurar los siguientes comandos en lugar de la configuración de reescritura.

En el símbolo del sistema, escriba:

- `add rewrite action set_pback_cookie insert_http_header "Cookie" '"PBack=0"'`
- `add rewrite policy set_pback_cookie "http.REQ.URL.CONTAINS(\"logon.aspx\")" set_pback_cookie`
- `set rewrite policy set_pback_cookie -action set_pback_cookie`
- `bind rewrite global set_pback_cookie 100 END -type REQ_DEFAULT`

## Configuración del uso de contraseñas de un solo uso

Puede configurar NetScaler Gateway para que utilice contraseñas de un solo uso, como un número de identificación personal (PIN) de token o un código de acceso. Después de que un usuario introduce el código de acceso o el PIN, el servidor de autenticación invalida

© 1997–2026 Citrix Systems, Inc. All rights reserved.

inmediatamente la contraseña de un solo uso y el usuario no puede volver a introducir el mismo PIN o contraseña.

Entre los productos que incluyen el uso de una contraseña de un solo uso se incluyen:

- RSA SecurID
- Imprivata OneSign
- SafeWord
- Gemalto Protiva
- Nordic SMS PASSCODE

Para usar cada uno de estos productos, configure el servidor de autenticación en la red interna para que utilice RADIUS. Para obtener más información, consulte Configuración de la autenticación RADIUS.

Si configura la autenticación en NetScaler Gateway para usar una contraseña de un solo uso con RADIUS, como la proporcionada por un token RSA SecurID, por ejemplo, NetScaler Gateway intenta volver a autenticar a los usuarios mediante el uso de la contraseña almacenada en caché. Esta reautenticación se produce cuando realiza cambios en NetScaler Gateway o si la conexión entre el cliente Citrix Secure Access y NetScaler Gateway se interrumpe y luego se restaura.

También puede producirse un intento de reautenticación cuando las conexiones están configuradas para usar la aplicación Citrix Workspace y los usuarios se conectan a StoreFront mediante RADIUS o LDAP. Cuando un usuario inicia una aplicación y la utiliza, y luego vuelve a Receiver para iniciar otra aplicación, NetScaler Gateway utiliza información almacenada en caché para autenticar al usuario.

## Configuración de la autenticación RSA SecurID

Al configurar el servidor RSA/ACE para la autenticación RSA SecureID, debe completar los siguientes pasos:

Configure el cliente RADIUS con la siguiente información:

- Proporcione el nombre del dispositivo NetScaler Gateway.
- Proporcione una descripción (no obligatoria).
- Proporcione la dirección IP del sistema.
- Proporcione el secreto compartido entre NetScaler Gateway y el servidor RADIUS.
- Configure la marca/modelo como RADIUS estándar.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

En la configuración del host del agente, necesita la siguiente información:

- Proporcione el nombre de dominio completo (FQDN) de NetScaler Gateway (tal como aparece en el certificado vinculado al servidor virtual). Después de proporcionar el FQDN, haga clic en la tecla Tab y la ventana Dirección de red se rellenará automáticamente.

  Después de introducir el FQDN, la dirección de red aparece automáticamente. Si no es así, introduzca la dirección IP del sistema.
- Proporcione el tipo de agente utilizando el servidor de comunicación.
- Configure la importación de todos los usuarios o de un conjunto de usuarios a los que se les permite autenticarse a través de NetScaler Gateway.

Si aún no está configurado, cree una entrada de host de agente para el servidor RADIUS, incluyendo la siguiente información:

- Proporcione el FQDN del servidor RSA.

  Después de introducir el FQDN, la dirección de red aparece automáticamente. Si no es así, proporcione la dirección IP del servidor RSA.
- Proporcione el tipo de agente, que es el servidor RADIUS.

Para obtener más información sobre cómo configurar un servidor RADIUS de RSA, consulte la documentación del fabricante.

Para configurar RSA SecurID, cree un perfil y una política de autenticación y, a continuación, vincule la política globalmente o a un servidor virtual. Para crear una política RADIUS para usar RSA SecurID, consulte Configuración de la autenticación RADIUS.

Después de crear la política de autenticación, vincúlela a un servidor virtual o globalmente. Para obtener más información, consulte Vinculación de políticas de autenticación.

## Configuración de la devolución de contraseñas con RADIUS

Puede reemplazar las contraseñas de dominio por una contraseña de un solo uso que un token genera desde un servidor RADIUS. Cuando los usuarios inician sesión en NetScaler Gateway, introducen un número de identificación personal (PIN) y la contraseña de un solo uso del token. Después de que NetScaler Gateway valida sus credenciales, el servidor RADIUS devuelve la contraseña de Windows del usuario a NetScaler Gateway. NetScaler Gateway acepta la respuesta del servidor y, a continuación, utiliza la contraseña devuelta para el inicio de sesión único en lugar de utilizar la contraseña de un solo uso que los usuarios escribieron durante el inicio de sesión.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Esta devolución de contraseña con la función RADIUS le permite configurar el inicio de sesión único sin necesidad de que los usuarios recuerden su contraseña de Windows.

Cuando los usuarios inician sesión mediante la devolución de contraseña, pueden acceder a todos los recursos de red permitidos en la red interna, incluidos Citrix Endpoint Management™ y StoreFront.

Para habilitar el inicio de sesión único mediante contraseñas devueltas, configure una directiva de autenticación RADIUS en NetScaler Gateway mediante los parámetros Identificador de proveedor de contraseña y Tipo de atributo de contraseña. Estos dos parámetros devuelven la contraseña de Windows del usuario a NetScaler Gateway.

NetScaler Gateway admite Imprivata OneSign. La versión mínima requerida de Imprivata OneSign es la 4.0 con Service Pack 3. El identificador de proveedor de contraseña predeterminado para Imprivata OneSign es 398. El código de tipo de atributo de contraseña predeterminado para Imprivata OneSign es 5.

Puede utilizar otros servidores RADIUS para la devolución de contraseñas, como RSA, Cisco o Microsoft. Configure el servidor RADIUS para que devuelva la contraseña de inicio de sesión único del usuario en un par de valores de atributo específicos del proveedor. En una directiva de autenticación de NetScaler Gateway, debe agregar los parámetros **Identificador de proveedor de contraseña y Tipo de atributo de contraseña** para estos servidores.

Puede encontrar una lista completa de identificadores de proveedor en el sitio web de la Internet Assigned Numbers Authority (IANA). Por ejemplo, el identificador de proveedor para la seguridad RSA es 2197, para Microsoft es 311 y para Cisco Systems es 9. El atributo específico del proveedor que admite un proveedor debe confirmarse con el proveedor. Por ejemplo, Microsoft ha publicado una lista de atributos específicos del proveedor en Atributos RADIUS específicos del proveedor de Microsoft.

Puede seleccionar cualquiera de los atributos específicos del proveedor para almacenar la contraseña de inicio de sesión único para los usuarios en el servidor RADIUS del proveedor. Si configura NetScaler Gateway con el identificador de proveedor y el atributo donde se almacena la contraseña de usuario en el servidor RADIUS, NetScaler Gateway solicita el valor del atributo en el paquete de solicitud de acceso que se envía al servidor RADIUS. Si el servidor RADIUS responde con el par atributo-valor correspondiente en el paquete de aceptación de acceso, la devolución de contraseña funciona independientemente del servidor RADIUS que utilice.

Para configurar el inicio de sesión único mediante contraseñas devueltas:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. En la utilidad de configuración, en la ficha Configuración, expanda **NetScaler Gateway \> Directivas \ > Autenticación**.
2. En el panel de navegación, haga clic en **RADIUS**.
3. En el panel de detalles, haga clic en **Agregar**.
4. En el cuadro de diálogo **Crear directiva de autenticación**, en Nombre, escriba un nombre para la directiva.
5. Junto a **Servidor**, haga clic en **Nuevo**.
6. En **Nombre**, escriba el nombre del servidor.
7. Configure los ajustes para el servidor RADIUS.
8. En **Identificador de proveedor de contraseña**, escriba el identificador de proveedor que devuelve el servidor RADIUS. Este identificador debe tener un valor mínimo de 1.
9. En **Tipo de atributo de contraseña**, escriba el tipo de atributo que devuelve el servidor RADIUS en el código AVP específico del proveedor. El valor puede oscilar entre 1 y 255.
10. En el cuadro de diálogo **Crear directiva de autenticación**, junto a **Expresiones con nombre**, seleccione la expresión, haga clic en **Agregar expresión**, haga clic en **Crear** y, a continuación, haga clic en **Cerrar**.

## Configuración de la autenticación SafeWord

La línea de productos SafeWord ayuda a proporcionar una autenticación segura mediante el uso de una contraseña basada en tokens. Después de que los usuarios introducen una contraseña, SafeWord la invalida y no se puede volver a utilizar.

Si NetScaler Gateway está reemplazando a Secure Gateway en una implementación de Secure Gateway y StoreFront, puede optar por no configurar la autenticación en NetScaler Gateway y seguir permitiendo que StoreFront proporcione autenticación SafeWord para el tráfico HTTP entrante.

NetScaler Gateway admite la autenticación SafeWord para los siguientes productos:

- SafeWord 2008
- SafeWord PremierAccess
- SafeWord para Citrix®
- SafeWord RemoteAccess

Puede configurar NetScaler Gateway para autenticarse mediante productos SafeWord de las siguientes maneras:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Configure la autenticación para usar un servidor RADIUS de PremierAccess que esté instalado como parte de SafeWord PremierAccess y permita que maneje la autenticación.
- Configure la autenticación para usar el agente IAS de SafeWord, que es un componente de SafeWord RemoteAccess, SafeWord para Citrix y SafeWord PremierAccess 4.0.
- Instale el agente de interfaz web de SafeWord para admitir StoreFront. No es necesario configurar la autenticación en NetScaler Gateway y StoreFront puede encargarse de ello. Esta configuración no utiliza el servidor RADIUS de PremierAccess ni el agente IAS de SafeWord.

Al configurar el servidor RADIUS de SafeWord, necesita la siguiente información:

- La dirección IP de NetScaler Gateway. Cuando configure los ajustes del cliente en el servidor RADIUS, utilice la dirección IP de NetScaler Gateway.
- Un secreto compartido.
- La dirección IP y el puerto del servidor SafeWord.

### Configuración de la autenticación Gemalto Protiva

Protiva es una plataforma de autenticación sólida que se desarrolló para aprovechar las ventajas de la autenticación con tarjeta inteligente de Gemalto. Con Protiva, los usuarios inician sesión con un nombre de usuario, una contraseña y una contraseña de un solo uso generada por el dispositivo Protiva. De forma similar a RSA SecurID, la solicitud de autenticación se envía al servidor de autenticación de Protiva y la contraseña se valida o se rechaza.

Para configurar Gemalto Protiva para que admita NetScaler Gateway, utilice las siguientes directrices:

- Instale el servidor Protiva.
- Instale el complemento del agente de Protiva Internet Authentication Server (IAS) en un servidor RADIUS IAS de Microsoft. Asegúrese de anotar la dirección IP y el número de puerto del servidor IAS.

## nFactor para la autenticación de Gateway

La autenticación nFactor habilita un conjunto completamente nuevo de posibilidades en cuanto a la autenticación. Los administradores que utilizan nFactor disfrutan de flexibilidad en la autenticación, autorización y auditoría al configurar los factores de autenticación para los servidores virtuales.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Dos bancos de políticas o dos factores ya no restringen a un administrador. El número de bancos de políticas se puede ampliar para adaptarse a diferentes necesidades. Basándose en factores anteriores, nFactor determina un método de autenticación. Los formularios de inicio de sesión dinámicos y las acciones en caso de fallo son posibles utilizando nFactor.

**IMPORTANTE:**

- A partir de la versión 13.0 compilación 67.x, la autenticación nFactor es compatible con la licencia Standard solo para el servidor virtual Gateway/VPN, y no para el servidor virtual de autenticación. En la licencia Standard, la GUI del visualizador nFactor no se puede utilizar para crear la EPA en el flujo nFactor. Además, no puede editar el esquema de inicio de sesión, sino que debe utilizar el esquema de inicio de sesión predeterminado tal cual.
- Para que NetScaler admita la autenticación nFactor, se requiere una licencia Advanced o una licencia Premium. Para obtener más información sobre la autenticación nFactor con NetScaler, consulte (/es-es/citrix-adc/current-release/aaa-tm/authentication-methods/multi-factor-nfactor-authentication.html).

## Requisitos de licencia de las funciones de autenticación, autorización y auditoría

La siguiente tabla enumera los requisitos de licencia para las funciones de autenticación, autorización y auditoría disponibles.

| | LICENCIA STANDARD | LICENCIA ADVANCED | LICENCIA PREMIUM |
|---|---|---|---|
| **Autenticación LOCAL** | Sí | Sí | Sí |
| **Autenticación LDAP** | Sí | Sí | Sí |
| **Autenticación RADIUS** | Sí | Sí | Sí |
| **Autenticación TACACS** | Sí | Sí | Sí |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| | LICENCIA STANDARD | LICENCIA ADVANCED | LICENCIA PREMIUM |
|---|---|---|---|
| **Autenticación web** | Sí | Sí | Sí |
| **Autenticación de certificado de cliente** | Sí | Sí | Sí |
| **Autenticación de negociación** | Sí | Sí | Sí |
| **Autenticación SAML** | Sí | Sí | Sí |
| **Autenticación OAuth** | No | Sí | Sí |
| **OTP nativo** | No | Sí | Sí |
| **OTP por correo electrónico** | No | Sí | Sí |
| **Notificación push para OTP** | No | No | Sí |
| **Pregunta y respuesta basadas en el conocimiento (autenticación KBA)** | No | Sí | Sí |
| **Restablecimiento de contraseña de autoservicio (SSPR)** | No | Sí | Sí |
| **Visualizador de nFactor** | Sí | Sí | Sí |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**NOTA**

- Para conocer los pasos para configurar nFactor para la licencia estándar de NetScaler, consulte la sección Crear un servidor virtual.
- Solo se puede vincular un servidor virtual de autenticación, autorización y auditoría no direccionable a un servidor virtual de Gateway/VPN en la licencia estándar de NetScaler.
- La personalización de LoginSchema no está permitida en la licencia estándar de NetScaler. El soporte de nFactor es básico, con solo los esquemas de inicio de sesión predeterminados y ya agregados que vienen con el dispositivo. El administrador puede usarlos en sus configuraciones, pero no puede agregar un esquema de inicio de sesión. Por lo tanto, la opción de la GUI está deshabilitada.

## Casos de uso

La autenticación nFactor permite flujos de autenticación dinámicos basados en el perfil de usuario. A veces, los flujos pueden ser sencillos e intuitivos para el usuario. En otros casos, pueden combinarse con la seguridad de Active Directory u otros servidores de autenticación. Los siguientes son algunos requisitos específicos de Gateway:

1. **Selección dinámica de nombre de usuario y contraseña.** Tradicionalmente, los clientes (incluidos los exploradores y los receptores) utilizan la contraseña de Active Directory (AD) como primer campo de contraseña. La segunda contraseña está reservada para la contraseña de un solo uso (OTP). Sin embargo, para proteger los servidores AD, es necesario validar primero la OTP. nFactor puede hacer esto sin necesidad de modificaciones del cliente.
2. **Punto final de autenticación multiinquilino.** Algunas organizaciones utilizan diferentes servidores Gateway para usuarios con y sin certificado. Dado que los usuarios utilizan sus propios dispositivos para iniciar sesión, los niveles de acceso de los usuarios varían en el dispositivo NetScaler en función del dispositivo que se utilice. Gateway puede satisfacer diferentes necesidades de autenticación.
3. **Autenticación basada en la pertenencia a grupos.** Algunas organizaciones obtienen propiedades de usuario de los servidores AD para determinar los requisitos de autenticación. Los requisitos de autenticación pueden variar para cada usuario.
4. **Cofactores de autenticación.** A veces, se utilizan diferentes pares de directivas de autenticación para autenticar diferentes conjuntos de usuarios. Proporcionar directivas de pares aumenta la eficacia de la autenticación. Las directivas dependientes se pueden crear a

© 1997–2026 Citrix Systems, Inc. All rights reserved.

partir de un flujo. De esta manera, los conjuntos de directivas independientes se convierten en flujos propios que aumentan la eficiencia y reducen la complejidad.

## Gestión de respuestas de autenticación

La devolución de llamada de NetScaler Gateway registra las respuestas de autenticación. Las respuestas de AAAD (daemon de autenticación) y los códigos de éxito/error/diálogo se envían al controlador de devolución de llamada. Los códigos de éxito/error/diálogo dirigen a Gateway para que realice la acción adecuada.

## Soporte al cliente

La siguiente tabla detalla los datos de configuración.

| CLIENTE | SOPORTE NFACTOR | PUNTO DE ENLACE DE DIRECTIVAS DE AUTENTICACIÓN | EPA |
|---|---|---|---|
| Exploradores | Sí | Autenticación | Sí |
| Aplicación Citrix Workspace | Sí | VPN | Sí |
| Plug-in de Gateway | Sí | VPN | Sí |

**Nota:**

- Citrix Workspace app admite la autenticación nFactor para los sistemas operativos compatibles a partir de las siguientes versiones.
  - Windows 4.12
  - Linux 13.10
  - Mac 1808
  - iOS 2007
  - Android 1808
  - HTML5: Compatible con Store Web
  - Chrome: Compatible con Store Web

© 1997–2026 Citrix Systems, Inc. All rights reserved.

## Compatibilidad del tipo de credencial de WebView con los mecanismos de autenticación

**NOTA:**

Las expresiones de bloqueo (como la variable ns) no son compatibles con las directivas de sesión VPN con compatibilidad con WebView. Para obtener más información sobre las expresiones de bloqueo, póngase en contacto con Soporte de Citrix.

La autenticación de NetScaler es compatible con el protocolo AUTHv3. El tipo de credencial de WebView en el protocolo AUTHv3 es compatible con todos los tipos de mecanismos de autenticación (incluidos SAML y OAuth). El tipo de credencial de WebView forma parte de AUTHv3, que implementan la aplicación Citrix Workspace y el explorador en las aplicaciones web.

El siguiente ejemplo explica el flujo de eventos de WebView a través de NetScaler Gateway y la aplicación Citrix Workspace:

1. La aplicación Citrix Workspace negocia con NetScaler Gateway para la compatibilidad con el protocolo AUTHv3.
2. NetScaler responde positivamente y sugiere una URL de inicio específica.
3. La aplicación Citrix Workspace se conecta al punto final (URL) específico.
4. NetScaler Gateway envía una respuesta al cliente para iniciar WebView.
5. La aplicación Citrix Workspace inicia WebView y envía una solicitud inicial a NetScaler.
6. NetScaler redirige la URI al punto de conexión de inicio de sesión del navegador.
7. Una vez completada la autenticación, NetScaler envía una respuesta de finalización a WebView.
8. Ahora, WebView se cierra y devuelve el control a la aplicación Citrix Workspace para continuar con el protocolo AUTHv3 para el establecimiento de la sesión.

## Configuración de línea de comandos

El servidor virtual de Gateway necesita un servidor virtual de autenticación nombrado como un atributo. El nombre del servidor virtual como atributo es la única configuración necesaria para este modelo.

```
add authnProfile <name-of-profile> -authnVsName <name-of-auth-vserver>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

El authnVsName es el nombre del servidor virtual de autenticación. El servidor virtual authnVsName debe configurarse con políticas de autenticación avanzadas y se utiliza para la autenticación nFactor.

```
add vpn vserver <name> <serviceType> <IP> <PORT> -authnProfile <name-of-profile>

set vpn vserver <name> -authnProfile <name-of-profile>
```

Donde authnProfile es el perfil de autenticación creado anteriormente.

## Desafíos de interoperabilidad

La mayoría de los clientes de Legacy Gateway, además de los clientes rfWeb, se basan en las respuestas enviadas por Gateway. Por ejemplo, se espera una respuesta 302 a /vpn/index.html para muchos clientes. Estos clientes también dependen de varias cookies de Gateway como "`pwcount`" y "NSC_CERT".

## Análisis de puntos finales (EPA)

EPA en nFactor no es compatible con el módulo de autenticación, autorización y auditoría de NetScaler. Por lo tanto, el servidor virtual de NetScaler Gateway realiza EPA. Después de EPA, las credenciales de inicio de sesión se envían al servidor virtual de autenticación mediante la API mencionada anteriormente. Una vez completada la autenticación, Gateway continúa con el proceso de postautenticación y establece la sesión de usuario.

## Consideraciones sobre la configuración incorrecta

El cliente de Gateway envía las credenciales de usuario solo una vez. Gateway obtiene una o dos credenciales del cliente con la solicitud de inicio de sesión. En el modo heredado, hay un máximo de dos factores. Las contraseñas obtenidas se utilizan para estos factores. Sin embargo, con nFactor, el número de factores que se pueden configurar es prácticamente ilimitado. Las contraseñas obtenidas del cliente de Gateway se reutilizan (según la configuración) para los factores configurados. Se debe tener cuidado de que la contraseña de un solo uso (OTP) no se reutilice varias veces. Del mismo modo, un administrador debe asegurarse de que la contraseña reutilizada en un factor sea realmente aplicable a ese factor.

## Definición de clientes

La opción de configuración se proporciona para ayudar a NetScaler a distinguir entre clientes de navegador y clientes pesados como Receiver.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Se proporciona un conjunto de patrones, ns_vpn_client_useragents, para que el administrador configure patrones para todos los clientes.

Del mismo modo, al vincular la cadena «Citrix Receiver» al `patset` anterior para ignorar a todos los clientes que tengan «Citrix Receiver» en el User-Agent.

## Restricción de nFactor para Gateway

La autenticación nFactor para Gateway no se produce si se cumplen las siguientes condiciones.

1. El authnProfile no está configurado en NetScaler Gateway.
2. Las directivas de autenticación avanzadas no están vinculadas al servidor virtual de autenticación y el mismo servidor virtual de autenticación se menciona en `authnProfile`.
3. La cadena User-Agent en la solicitud HTTP coincide con los User-Agents configurados en `patset` ns_vpn_client_useragents.

Si no se cumplen estas condiciones, se utiliza la directiva de autenticación clásica vinculada a Gateway.

Si un User-Agent, o una parte de él, está vinculado al `patset` mencionado anteriormente, las solicitudes procedentes de esos user-agents no participan en el flujo nFactor. Por ejemplo, el siguiente comando restringe la configuración para todos los navegadores (suponiendo que todos los navegadores contengan «Mozilla» en la cadena del user-agent):

```
bind patset ns_vpn_client_useragents Mozilla
```

## LoginSchema

LoginSchema es una representación lógica del formulario de inicio de sesión. El lenguaje XML lo define. La sintaxis de loginSchema se ajusta a la especificación del Protocolo de Formularios Comunes de Citrix.

LoginSchema define la «vista» del producto. Un administrador puede proporcionar una descripción personalizada, texto de ayuda, etc., del formulario. El esquema de inicio de sesión incluye las etiquetas del propio formulario. Un cliente puede proporcionar el mensaje de éxito o error que describe el formulario presentado en un momento dado.

Utilice el siguiente comando para configurar un esquema de inicio de sesión.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
add authentication loginSchema <name> -authenticationSchema <string> [-
userExpression <string>] [-passwdExpression <string>] [-
userCredentialIndex <positive_integer>]

[-passwordCredentialIndex <positive_integer>] [-authenticationStrength
<positive_integer>] [-SSOCredentials ( YES | NO )]
```

### Descripción del parámetro

- name - Nombre para el nuevo esquema de inicio de sesión. Este es un argumento obligatorio. Longitud máxima: 127
- authenticationSchema - Nombre del archivo para leer el esquema de autenticación que se enviará a la interfaz de usuario de la página de inicio de sesión. Este archivo contiene la definición XML de los elementos según el protocolo de autenticación de formularios de Citrix para poder renderizar el formulario de inicio de sesión. Si el administrador no desea solicitar a los usuarios otras credenciales, sino continuar con las credenciales obtenidas previamente, entonces `noschema` se puede dar como argumento. Esto se aplica solo a los loginSchemas que se utilizan con los factores definidos por el usuario, y no con el factor del servidor virtual.

Este es un argumento obligatorio. Longitud máxima: 255

- userExpression - Expresión para la extracción del nombre de usuario durante el inicio de sesión. Puede ser cualquier expresión de política avanzada relevante. Longitud máxima: 127
- passwdExpression - Expresión para la extracción de la contraseña durante el inicio de sesión. Puede ser cualquier expresión de política avanzada relevante. Longitud máxima: 127
- userCredentialIndex - El índice en el que el nombre de usuario introducido por el usuario debe almacenarse en la sesión. Valor mínimo: 1, Valor máximo: 16
- passwordCredentialIndex - El índice en el que la contraseña introducida por el usuario debe almacenarse en la sesión. Valor mínimo: 1, Valor máximo: 16
- authenticationStrength - Peso de la autenticación actual. Valor mínimo: 0, Valor máximo: 65535
- `SSOCredentials` - Esta opción indica si las credenciales del factor actual son las credenciales predeterminadas de SSO (SingleSignOn). Valores posibles: SÍ, NO. Valor predeterminado: NO

© 1997–2026 Citrix Systems, Inc. All rights reserved.

## Conocimientos necesarios sobre LoginSchema y nFactor

Los archivos loginSchema precompilados se encuentran en la siguiente ubicación de NetScaler: **/nsconfig/loginschema/LoginSchema/**. Estos archivos loginSchema precompilados se adaptan a casos de uso comunes y se pueden modificar para pequeñas variaciones si es necesario.

Además, la mayoría de los casos de uso de factor único con pocas personalizaciones no necesitan la configuración del esquema de inicio de sesión.

Se recomienda al administrador que consulte la documentación para conocer otras opciones de configuración que permiten a NetScaler descubrir los factores. Una vez que el usuario envía las credenciales, el administrador puede configurar más de un factor para elegir y procesar de forma flexible los factores de autenticación.

## Configuración de la autenticación de doble factor sin usar LoginSchema

NetScaler determina automáticamente los requisitos de doble factor basándose en la configuración. Una vez que el usuario presenta estas credenciales, el administrador puede configurar el primer conjunto de políticas en el servidor virtual. Contra cada política puede haber un "nextFactor" configurado como "passthrough". Un "passthrough" implica que NetScaler debe procesar el inicio de sesión utilizando el conjunto de credenciales existente sin recurrir al usuario. Al utilizar factores "passthrough", un administrador puede dirigir programáticamente el flujo de autenticación. Se recomienda a los administradores que lean la especificación de nFactor o las guías de implementación para obtener más detalles. Consulte Autenticación multifactor (nFactor).

## Expresiones de nombre de usuario y contraseña

Para procesar las credenciales de inicio de sesión, el administrador debe configurar el loginSchema. Los casos de uso de factor único o doble con pocas personalizaciones de loginSchema no necesitan una definición XML específica. El LoginSchema tiene otras propiedades como userExpression y passwdExpression que se pueden usar para alterar el nombre de usuario o la contraseña que presenta el usuario.

Los esquemas de inicio de sesión son expresiones de directiva avanzadas y también se pueden usar para anular la entrada del usuario. Esto se puede lograr añadiendo una cadena para los parámetros en **-authenticationSchema** como se muestra en el siguiente ejemplo.

A continuación se muestran ejemplos para modificar las entradas de usuario para el nombre de usuario y la contraseña, respectivamente.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Cambiar la entrada del usuario para el nombre de usuario de `username@citrix.com` a `username@xyz.com`

```
add authentication loginSchema user_schema -authenticationSchema
LoginSchema/DualAuth.xml -userExpression
"AAA.LOGIN.USERNAME.BEFORE_STR(\"@\").APPEND(\"@xyz.com\")"
```

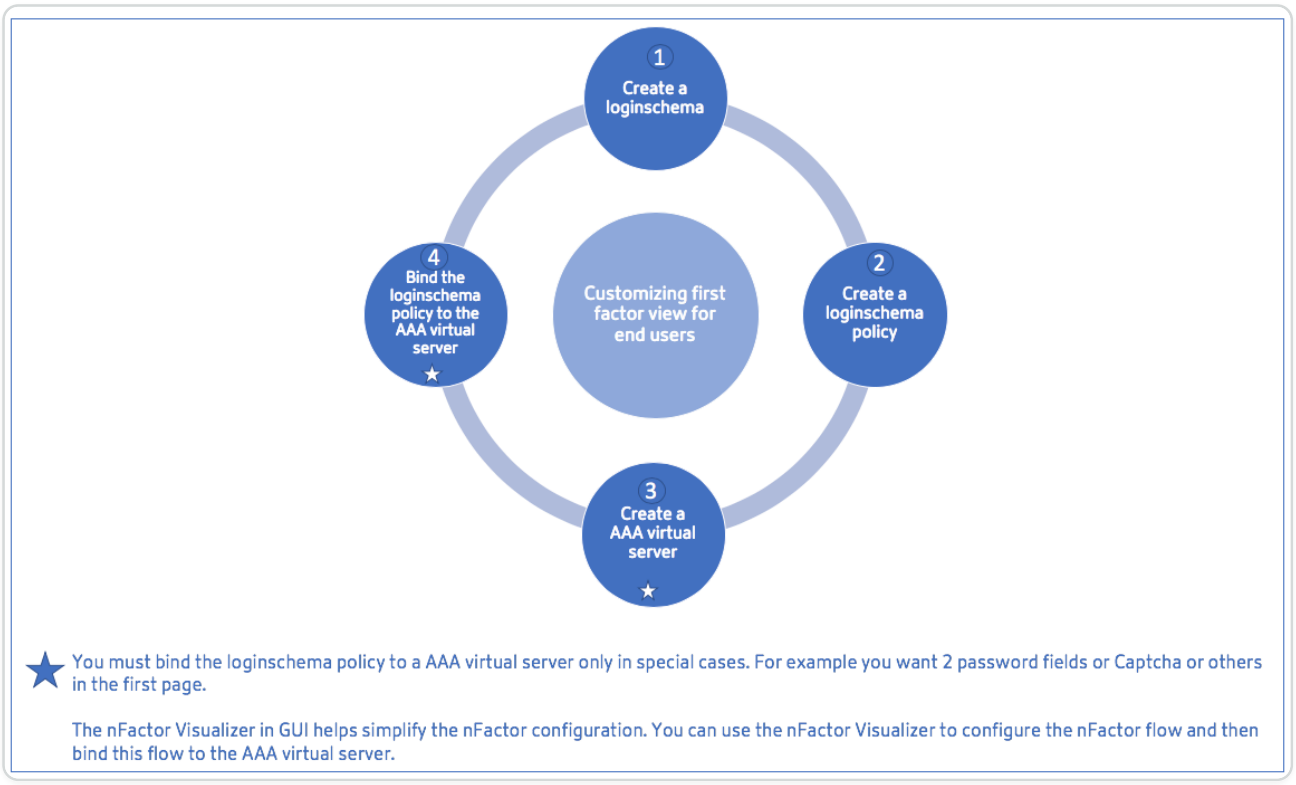
- Considere un escenario en el que el usuario proporciona una contraseña y un código de acceso en el primer factor como parte del esquema de inicio de sesión configurado. Para usar el **código de acceso** proporcionado por el usuario en el primer factor y la **contraseña** en el segundo factor, puede modificar el esquema de inicio de sesión existente mediante los siguientes comandos.

```
add authentication loginSchema user_schema -authenticationSchema
LoginSchema/DualAuth.xml -passwdExpression "AAA.LOGIN.PASSWORD2"
```

```
add authentication loginSchema user_schema_second -authenticationSchema
noschema  -passwdExpression "AAA.LOGIN.PASSWORD"
```

## Pasos de alto nivel en la configuración de nFactor

El siguiente diagrama ilustra los pasos de alto nivel implicados en la configuración de nFactor.




© 1997–2026 Citrix Systems, Inc. All rights reserved.

## Configuración de la GUI

En esta sección se describen los siguientes temas:

- Crear un servidor virtual
- Crear servidor virtual de autenticación
- Crear perfil CERT de autenticación
- Crear una directiva de autenticación
- Agregar un servidor de autenticación LDAP
- Añadir una política de autenticación LDAP
- Añadir un servidor de autenticación RADIUS
- Añadir una política de autenticación RADIUS
- Crear un esquema de inicio de sesión de autenticación
- Crear una etiqueta de política

## Crear un servidor virtual

1. Vaya a **NetScaler Gateway > Servidores virtuales.**
2. Haga clic en el botón **Agregar** para crear un servidor virtual de gateway.
3. Introduzca la siguiente información y haga clic en **Aceptar**.

| NOMBRE DEL PARÁMETRO | DESCRIPCIÓN DEL PARÁMETRO |
|---|---|
| **Nombre** | Nombre del servidor virtual de NetScaler Gateway. Debe comenzar con un carácter alfabético ASCII o un guion bajo (_), y debe contener solo caracteres alfanuméricos ASCII, guion bajo, almohadilla (#), punto (.), espacio, dos puntos (:), arroba (@), igual (=) y guion (-). Se puede cambiar después de crear el servidor virtual. El siguiente requisito se aplica solo a la CLI de NetScaler: si el nombre incluye uno o más espacios, encierre el nombre entre comillas dobles o simples (por ejemplo, "mi servidor" o 'mi servidor'). |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| NOMBRE DEL PARÁMETRO | DESCRIPCIÓN DEL PARÁMETRO |
|---|---|
| **Tipo de dirección IP** | Seleccione la opción **Dirección IP** o **No direccionable** en el menú desplegable. |
| **Dirección IP** | Una dirección de Protocolo de Internet (dirección IP) es una etiqueta numérica asignada a cada dispositivo que participa en la red informática que utiliza el Protocolo de Internet para la comunicación. |
| **Puerto** | Introduzca el número de puerto para el servidor virtual. |
| **Perfil de servidor RDP** | Nombre del perfil de servidor RDP asociado al servidor virtual. |
| **Perfil de servidor virtual PCoIP** | Nombre del perfil de servidor virtual PCoIP asociado al servidor virtual. |
| **Usuarios máximos** | Número máximo de sesiones de usuario simultáneas permitidas en este servidor virtual. El número real de usuarios que pueden iniciar sesión en este servidor virtual depende del número total de licencias de usuario. |
| **Intentos máximos de inicio de sesión** | Número máximo de intentos de inicio de sesión. |
| **Tiempo de espera de inicio de sesión fallido** | Número de minutos que una cuenta permanece bloqueada si el usuario supera el número máximo de intentos permitidos. |
| **Actualización del complemento EPA de Windows** | Opción para configurar el comportamiento de actualización del plug-in para clientes Windows. |
| **Actualización del plug-in EPA de Linux** | Opción para configurar el comportamiento de actualización del plug-in para clientes Linux. |
| | >**Nota:** |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

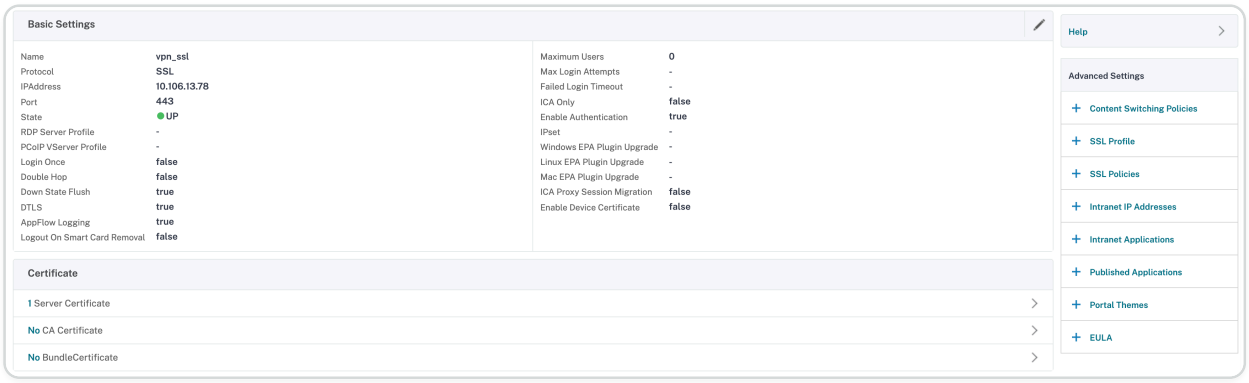
| NOMBRE DEL PARÁMETRO | DESCRIPCIÓN DEL PARÁMETRO |
| --- | --- |
| | >- Para eLux e IGEL OS, este parámetro siempre debe establecerse en **Nunca**. |
| | >- La opción **Esencial** no es compatible con el cliente Citrix Secure Access para Linux. |
| **Actualización del plug-in EPA de Mac** | Opción para configurar el comportamiento de actualización del plug-in para clientes macOS. |
| **Inicio de sesión único** | Esta opción habilita o deshabilita el SSO sin interrupciones para este servidor virtual. |
| **Solo ICA** | - Cuando se establece en **ON**, implica el modo Básico, donde el usuario puede iniciar sesión utilizando la aplicación Citrix Workspace o un navegador y obtener acceso a las aplicaciones publicadas configuradas en el entorno de Citrix Virtual Apps and Desktops indicado por el parámetro `Wihome`. Los usuarios no pueden conectarse utilizando el cliente Citrix Secure Access y no se pueden configurar los análisis de puntos finales. El número de usuarios que pueden iniciar sesión y acceder a las aplicaciones no está limitado por la licencia en este modo. |
| | - Cuando se establece en **OFF**, implica el modo SmartAccess, donde el usuario puede iniciar sesión utilizando la aplicación Citrix Workspace, un navegador o un cliente Citrix Secure Access. El administrador puede configurar escaneos de puntos finales para que se ejecuten en los sistemas cliente y luego usar los resultados para controlar el acceso a las aplicaciones publicadas. En este modo, el cliente puede conectarse a la puerta de enlace en otros modos de cliente, a saber, VPN y VPN sin cliente. El número de usuarios que pueden iniciar sesión y |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| NOMBRE DEL PARÁMETRO | DESCRIPCIÓN DEL PARÁMETRO |
|---|---|
| | acceder a los recursos está limitado por las licencias CCU en este modo. |
| **Habilitar autenticación** | Requerir autenticación para los usuarios que se conectan a NetScaler Gateway. |
| **Doble salto** | Utilice NetScaler Gateway en una configuración de doble salto. Una implementación de doble salto proporciona una capa adicional de seguridad para la red interna mediante el uso de tres firewalls para dividir la DMZ en dos etapas. Dicha implementación puede tener un dispositivo en la DMZ y otro en la red segura. |
| **Vaciar estado inactivo** | Cierre las conexiones existentes cuando el servidor virtual esté marcado como INACTIVO (DOWN), lo que significa que el servidor podría haber agotado el tiempo de espera. Desconectar las conexiones existentes libera recursos y, en ciertos casos, acelera la recuperación de configuraciones de equilibrio de carga sobrecargadas. Habilite esta configuración en servidores en los que las conexiones se puedan cerrar de forma segura cuando estén marcadas como INACTIVAS. No habilite el vaciado de estado INACTIVO en servidores que deban completar sus transacciones. |
| **DTLS** | Esta opción inicia o detiene el servicio de turno en el servidor virtual. |
| **Registro de AppFlow** | Registre los registros de AppFlow que contienen información estándar de NetFlow o IPFIX, como marcas de tiempo para el inicio y el final de un flujo, recuento de paquetes y recuento de bytes. También registre los registros que contienen información a nivel de aplicación, como direcciones web HTTP, métodos de solicitud |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| NOMBRE DEL PARÁMETRO | DESCRIPCIÓN DEL PARÁMETRO |
|---|---|
| | HTTP y códigos de estado de respuesta, tiempo de respuesta del servidor y latencia. |
| **Migración de sesión de proxy ICA** | Esta opción determina si una sesión de proxy ICA existente se transfiere cuando el usuario inicia sesión desde otro dispositivo. |
| **Estado** | El estado actual del servidor virtual, como ACTIVO, INACTIVO, OCUPADO, etc. |
| **Habilitar certificado de dispositivo** | Indica si la comprobación del certificado del dispositivo como parte de EPA está activada o desactivada. |




4. Seleccione la sección **Sin certificado de servidor** de la página.
5. Haga clic en **>** en **Seleccionar certificado de servidor** para seleccionar el certificado de servidor.
6. Seleccione el certificado SSL y haga clic en el botón **Seleccionar**.
7. Haga clic en **Enlazar**.
8. Si ve una advertencia sobre **No hay cifrados utilizables**, haga clic en **Aceptar**
9. Haga clic en el botón **Continuar**.
10. En la sección Autenticación, haga clic en el icono **+** en la parte superior derecha.

## Crear un servidor virtual de autenticación

1. Vaya a **Seguridad > NetScaler AAA – Tráfico de aplicaciones > Servidores virtuales.**
2. Haga clic en el botón **Agregar**.
3. Complete la siguiente Configuración básica para crear el servidor virtual de autenticación.

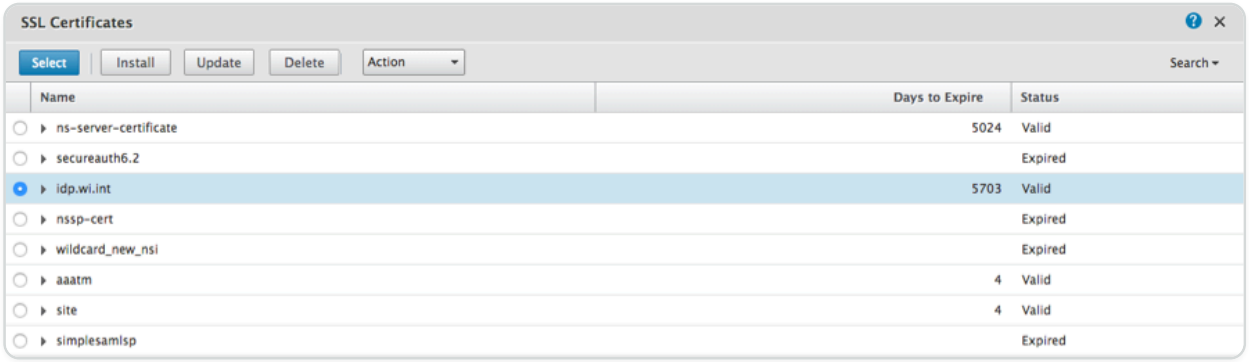
© 1997–2026 Citrix Systems, Inc. All rights reserved.

**Nota**: El signo * a la derecha del nombre de la configuración indica campos obligatorios.

- Introduzca el **Nombre** del nuevo servidor virtual de autenticación.
- Introduzca el **Tipo de dirección IP**. El tipo de dirección IP se puede configurar como No direccionable.
- Introduzca la **dirección IP**. La dirección IP puede ser cero.
- Introduzca el tipo de **Protocolo** del servidor virtual de autenticación.
- Introduzca el **puerto TCP** en el que el servidor virtual acepta conexiones.
- Introduzca el **dominio** de la cookie de autenticación establecida por el servidor virtual de autenticación.

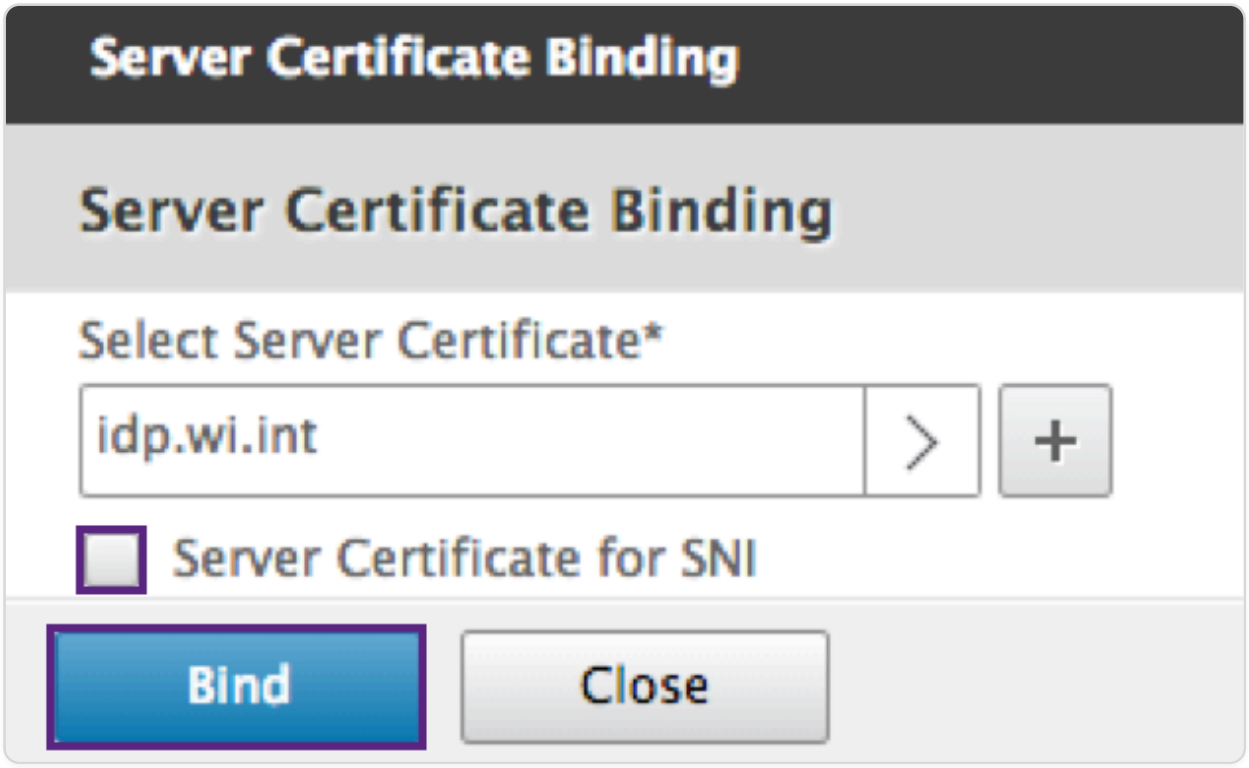
4. Haga clic en **Aceptar**.
5. Haga clic en **Sin certificado de servidor**.
6. Seleccione el certificado de servidor deseado de la lista.
7. Elija el certificado SSL deseado y haga clic en el botón **Seleccionar**.

   **Nota**: El servidor virtual de autenticación no necesita un certificado asociado.




8. Configure el **enlace de certificado de servidor**.
   - Marque la casilla **Certificado de servidor para SNI** para enlazar una o más claves de certificado utilizadas para el procesamiento SNI.
   - Haga clic en el botón **Enlazar**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.




## Crear un perfil CERT de autenticación

1. Vaya a **Security -> NetScaler AAA â€“ Application Traffic -> Policies -> Authentication -> Basic Policies -> CERT.**
2. Seleccione la pestaña Perfiles y, a continuación, seleccione **Agregar**.
3. Complete los siguientes campos para crear el perfil CERT de autenticación. El signo * a la derecha del nombre de la configuración indica los campos obligatorios.
   - **Nombre** - Nombre para el perfil (acción) del servidor de autenticación de certificado de cliente.
   - **Doble factor** – En este caso, la opción de autenticación de doble factor es NOOP.
   - **Campo de nombre de usuario** – introduzca el campo del certificado de cliente del que se extrae el nombre de usuario. Debe establecerse en ""Subject"" o ""Issuer"" (incluya ambos conjuntos de comillas dobles).
   - **Campo de nombre de grupo** - introduzca el campo del certificado de cliente del que se extrae el grupo. Debe establecerse en ""Subject"" o ""Issuer"" (incluya ambos conjuntos de comillas dobles).
   - **Grupo de autenticación predeterminado** - Este es el grupo predeterminado que se elige cuando la autenticación se realiza correctamente, además de los grupos extraídos.
4. Haga clic en **Crear**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

## Crear una directiva de autenticación

**NOTA**

Si configura una directiva de primer factor con una regla de directiva que utiliza AAA.login, la siguiente expresión debe configurarse con la condición OR para que la aplicación Citrix Workspace admita la implementación de nFactor.

```
|| HTTP.REQ.URL.CONTAINS("/cgi/authenticate")
```

1. Vaya a **Security -> NetScaler AAA – Application Traffic -> Policies -> Authentication -> Advanced Policies -> Policy.**
2. Seleccione el botón **Add**.
3. Complete la siguiente información para crear una directiva de autenticación. El signo * a la derecha del nombre de la configuración indica los campos obligatorios.

   a) **Name**: introduzca el nombre de la directiva de AUTENTICACIÓN avanzada. Debe comenzar con una letra, un número o el carácter de subrayado (_), y debe contener solo letras, números y los caracteres de guion (-), punto (.), almohadilla (#), espacio (), arroba (@), igual (=), dos puntos (:) y subrayado. No se puede cambiar después de crear la directiva de autenticación.

   El siguiente requisito se aplica solo a la CLI de NetScaler: si el nombre incluye uno o más espacios, encierre el nombre entre comillas dobles o simples (por ejemplo, "my authentication policy" o 'my authentication policy').

   b) **Action Type**: introduzca el tipo de acción de autenticación.

   c) **Action**: introduzca el nombre de la acción de autenticación que se realizará si la directiva coincide.

   d) **Log Action**: introduzca el nombre de la acción de registro de mensajes que se utilizará cuando una solicitud coincida con esta directiva.

   e) **Expression**: introduzca el nombre de la regla con nombre de NetScaler, o una expresión de sintaxis predeterminada, que la directiva utiliza para determinar si se debe intentar autenticar al usuario con el servidor de AUTENTICACIÓN.

   f) **Comments**: introduzca cualquier comentario para conservar información sobre esta directiva.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. Haga clic en **Create**.

## Agregar un servidor de autenticación LDAP

1. Vaya a **Security -> NetScaler AAA – Application Traffic -> Policies -> Authentication -> Basic Policies -> LDAP.**
2. Agregue un servidor LDAP seleccionando la ficha **Server** y, a continuación, el botón **Add**.

## Agregar una política de autenticación LDAP

1. Vaya a **Security > NetScaler AAA â€“ Application Traffic > Policies > Authentication > Advanced Policies > Policy**.
2. Haga clic en **Add** para agregar una política de autenticación.
3. Complete la siguiente información para crear una política de autenticación. El signo * a la derecha del nombre de la configuración indica los campos obligatorios.

   a) **Name** - Nombre de la política de AUTENTICACIÓN avanzada. Debe comenzar con una letra, un número o el carácter de subrayado (_), y debe contener solo letras, números y los caracteres de guion (-), punto (.), almohadilla (#), espacio (), arroba (@), igual (=), dos puntos (:) y subrayado. No se puede cambiar después de crear la política de autenticación.

   El siguiente requisito se aplica solo a la CLI de NetScaler: Si el nombre incluye uno o más espacios, encierre el nombre entre comillas dobles o simples (por ejemplo, "my authentication policy" o 'my authentication policy').

   b) **Action Type** - Tipo de la acción de autenticación.

   c) **Action** - Nombre de la acción de autenticación que se realizará si la política coincide.

   d) **Log Action** - Nombre de la acción de registro de mensajes que se utilizará cuando una solicitud coincida con esta política.

   e) **Expression** - Nombre de la regla con nombre de NetScaler, o una expresión de sintaxis predeterminada, que la política utiliza para determinar si se debe intentar autenticar al usuario con el servidor de AUTENTICACIÓN.

   f) **Comments** - Cualquier comentario para preservar información sobre esta política.
4. Haga clic en **Create.**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

## Agregar un servidor de autenticación RADIUS

1. Vaya a **Security > NetScaler AAA â€“ Application Traffic > Policies Authentication > Basic Policies > RADIUS**.
2. Para agregar un servidor, seleccione la pestaña **Servers** y haga clic en el botón **Add**.
3. Introduzca lo siguiente para crear un servidor RADIUS de autenticación. El signo * a la derecha del nombre de la configuración indica campos obligatorios.
    a. Introduzca un **Nombre** para la acción RADIUS.
    b. Introduzca el **Nombre del servidor** o la **Dirección IP del servidor** asignada al servidor RADIUS.
    c. Introduzca el número de **Puerto** en el que el servidor RADIUS escucha las conexiones.
    d. Introduzca el valor de **Tiempo de espera** en segundos. El dispositivo NetScaler espera una respuesta del servidor RADIUS hasta que expire el valor de tiempo de espera configurado.
    e. Introduzca la **Clave secreta** que se comparte entre el servidor RADIUS y el dispositivo NetScaler. La clave secreta es necesaria para permitir que el dispositivo NetScaler se comunique con el servidor RADIUS.
    f. **Confirme la clave secreta**.
4. Haga clic en **Crear.**

## Agregar una directiva de autenticación RADIUS

1. Vaya a **Seguridad > NetScaler AAA – Tráfico de aplicaciones > Directivas > Autenticación > Directivas avanzadas > Directiva.**
2. Haga clic en **Agregar** para crear una directiva de autenticación.
3. Complete la siguiente información para crear una directiva de autenticación. El signo * a la derecha del nombre de la configuración indica campos obligatorios.
    a. **Nombre** - Nombre de la directiva de AUTENTICACIÓN avanzada. Debe comenzar con una letra, un número o el carácter de subrayado (_), y debe contener solo letras, números y los caracteres de guion (-), punto (.), almohadilla (#), espacio (), arroba (@), igual (=), dos puntos (:) y subrayado. No se puede cambiar después de crear la directiva de AUTENTICACIÓN.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

El siguiente requisito se aplica solo a la CLI de NetScaler: Si el nombre incluye uno o más espacios, encierre el nombre entre comillas dobles o simples (por ejemplo, "mi directiva de autenticación" o 'mi directiva de autenticación').

a. **Tipo de acción** - Tipo de la acción de autenticación.

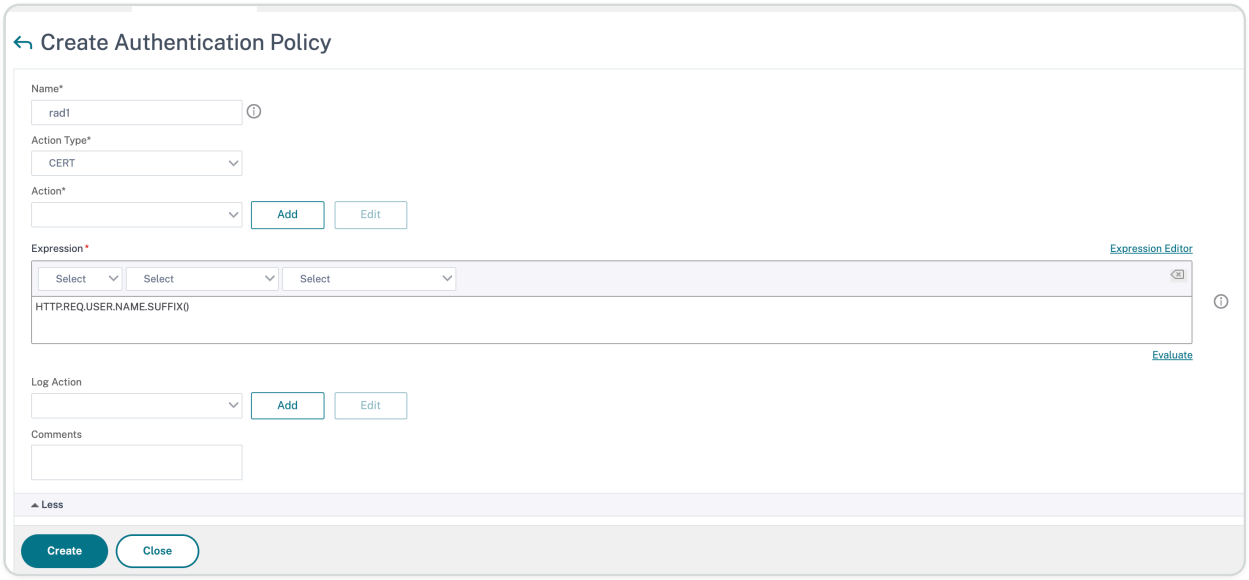
b. **Acción** - Nombre de la acción de autenticación que se realizará si la política coincide.

c. **Acción de registro** - Nombre de la acción de registro de mensajes que se utilizará cuando una solicitud coincida con esta política.

d. **Expresión** - Nombre de la regla con nombre de NetScaler, o una expresión de sintaxis predeterminada, que la política utiliza para determinar si se debe intentar autenticar al usuario con el servidor de AUTENTICACIÓN.

e. **Comentarios** - Cualquier comentario para preservar información sobre esta política.

4. Haga clic en **Aceptar.** La política de autenticación que ha creado aparece en la lista de políticas.




## Crear un esquema de inicio de sesión de autenticación

1. Vaya a **Security > NetScaler AAA – Application Traffic > Login Schema.**
2. Seleccione la ficha Perfiles y haga clic en el botón **Agregar**.
3. Rellene los siguientes campos para crear un esquema de inicio de sesión de autenticación:

a. Introduzca **Nombre** – Nombre para el nuevo esquema de inicio de sesión.

b. Introduzca **Esquema de autenticación** - Nombre del archivo para leer el esquema de autenticación que se enviará para la interfaz de usuario de la página de inicio de sesión. Este archivo debe contener la definición XML de los elementos según el protocolo de

© 1997–2026 Citrix Systems, Inc. All rights reserved.

autenticación de formularios de Citrix para poder renderizar un formulario de inicio de sesión. Si un administrador no desea solicitar más credenciales a los usuarios, sino continuar con las credenciales obtenidas anteriormente, se puede proporcionar "`noschema`" como argumento. Esto se aplica solo a los loginSchemas que se utilizan con factores definidos por el usuario, y no al factor de servidor virtual.

c. Introduzca **Expresión de usuario** - Expresión para la extracción del nombre de usuario durante el inicio de sesión.

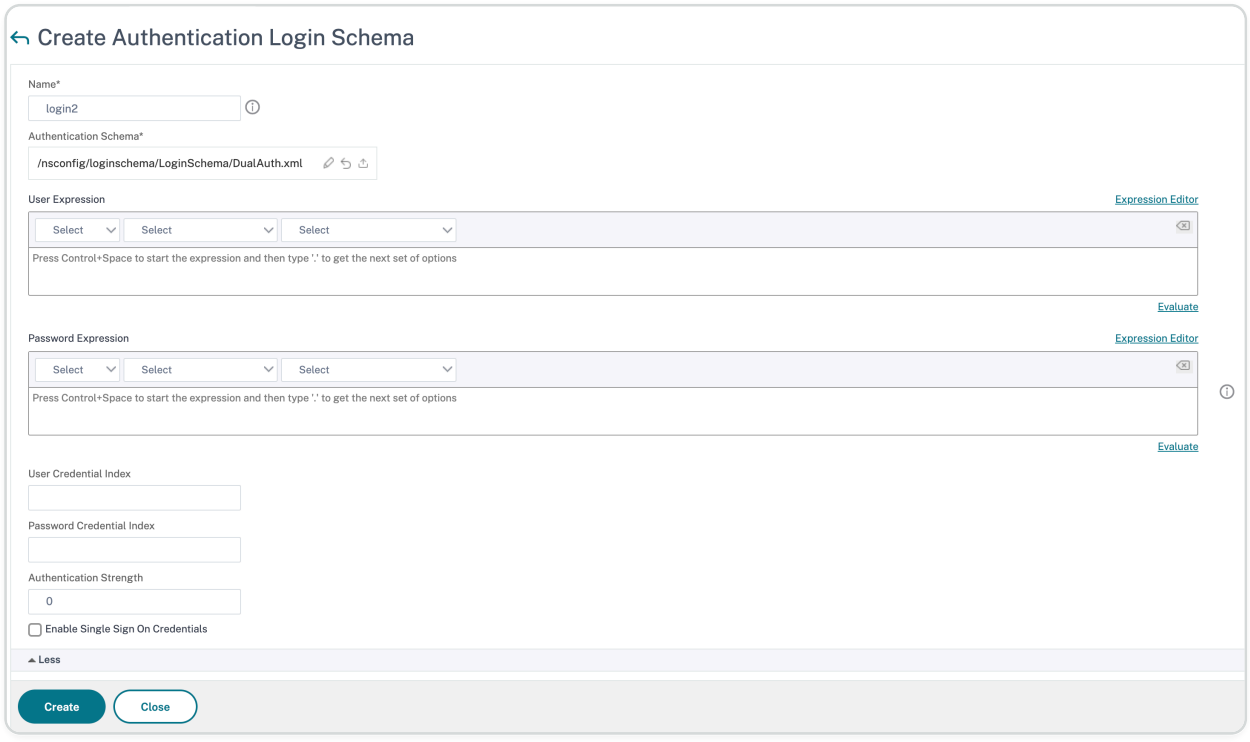
d. Introduzca **Expresión de contraseña** - Expresión para la extracción de la contraseña durante el inicio de sesión.

e. Introduzca **Índice de credenciales de usuario** - Un índice en el que se almacena en la sesión el nombre de usuario introducido por el usuario.

f. Introduzca **Password Credential Index** - Un índice en el que la contraseña introducida por el usuario debe almacenarse en la sesión.

g. Introduzca **Authentication Strength** - Peso de la autenticación actual.

4. Haga clic en **Create.** El perfil de esquema de inicio de sesión que ha creado debe aparecer en la lista de perfiles de esquema de inicio de sesión.



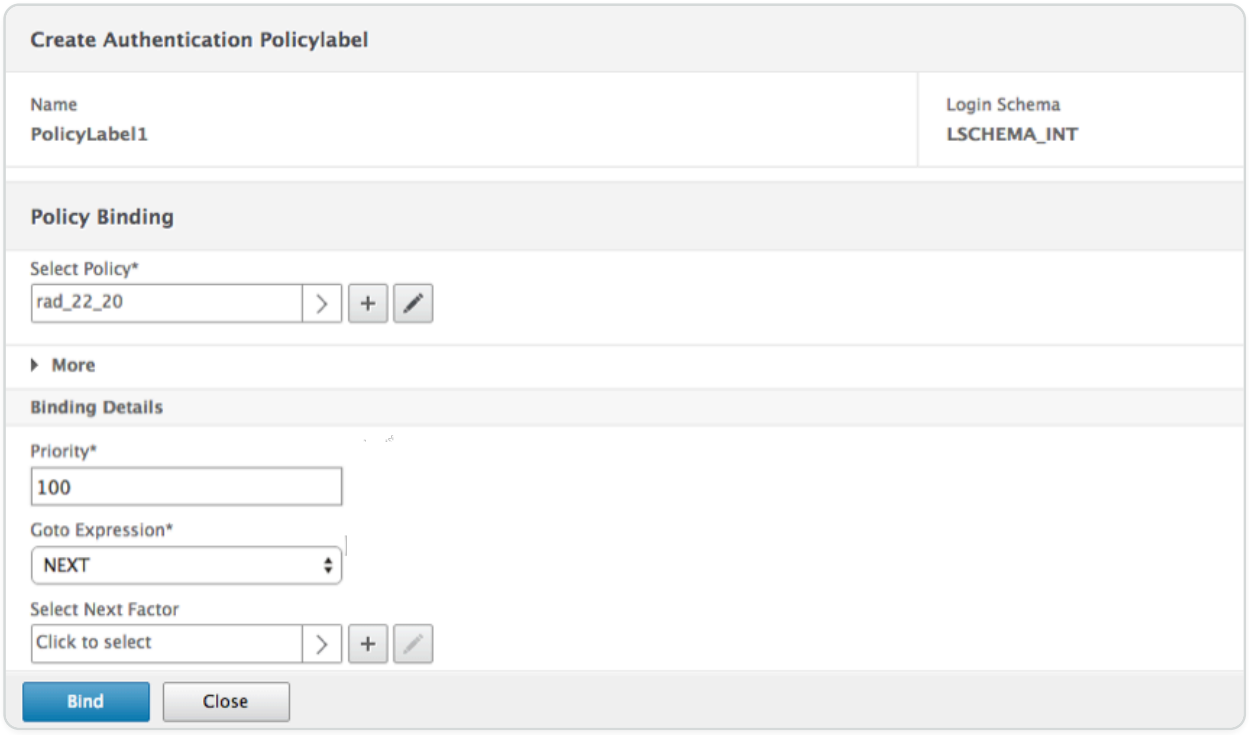

## Crear una etiqueta de directiva

Una etiqueta de directiva especifica las directivas de autenticación para un factor particular. Cada una de estas etiquetas corresponde a un único factor. Esta especifica el formulario de inicio de

© 1997–2026 Citrix Systems, Inc. All rights reserved.

sesión que debe presentarse al usuario. Debe vincularse como el siguiente factor de una directiva de autenticación o de otra etiqueta de directiva de autenticación. Normalmente, una etiqueta de directiva incluye directivas de autenticación para un mecanismo de autenticación específico. Sin embargo, también puede haber una que contenga directivas de autenticación para diferentes mecanismos de autenticación.

1. Vaya a **Security > NetScaler AAA â€“ Application Traffic > Policies > Authentication > Advanced Policies > Policy Label.**
2. Haga clic en el botón **Add**.
3. Complete los siguientes campos para crear una etiqueta de directiva de autenticación:
   a. Introduzca el **Name** de la nueva etiqueta de directiva de autenticación.
   b. Introduzca el **Login Schema** asociado a la etiqueta de directiva de autenticación.
   c. Haga clic en **Continue**.
4. **Select a Policy** en el menú desplegable.
5. Elija la **Authentication Policy** deseada y haga clic en el botón **Select**.
6. Complete los siguientes campos:
   a. Introduzca la **Prioridad** de la vinculación de la directiva.
   b. Introduzca la **expresión Goto** — la expresión especifica la prioridad de la siguiente directiva que se evaluará si la regla de directiva actual se evalúa como VERDADERA.




© 1997–2026 Citrix Systems, Inc. All rights reserved.

7. Seleccione la directiva de autenticación deseada y haga clic en el botón **Seleccionar**.
8. Haga clic en el botón **Enlazar**.
9. Haga clic en **Listo**.
10. Revise la etiqueta de la directiva de autenticación.

## Configuración de re-Captcha para la autenticación nFactor

A partir de la versión 12.1 compilación 50.x de NetScaler, NetScaler Gateway admite una nueva acción de primera clase 'captchaAction' que simplifica la configuración de Captcha. Como Captcha es una acción de primera clase, puede ser un factor por sí mismo. Puede inyectar Captcha en cualquier parte del flujo nFactor.

Anteriormente, tenía que escribir directivas de WebAuth personalizadas con cambios también en la RfWebUI. Con la introducción de captchaACtion, no tiene que modificar el JavaScript.

**IMPORTANTE:**

Si se utiliza Captcha junto con los campos de nombre de usuario o contraseña en el esquema, el botón Enviar se desactiva hasta que se cumple Captcha.

### Configuración de Captcha

La configuración de Captcha consta de dos partes.

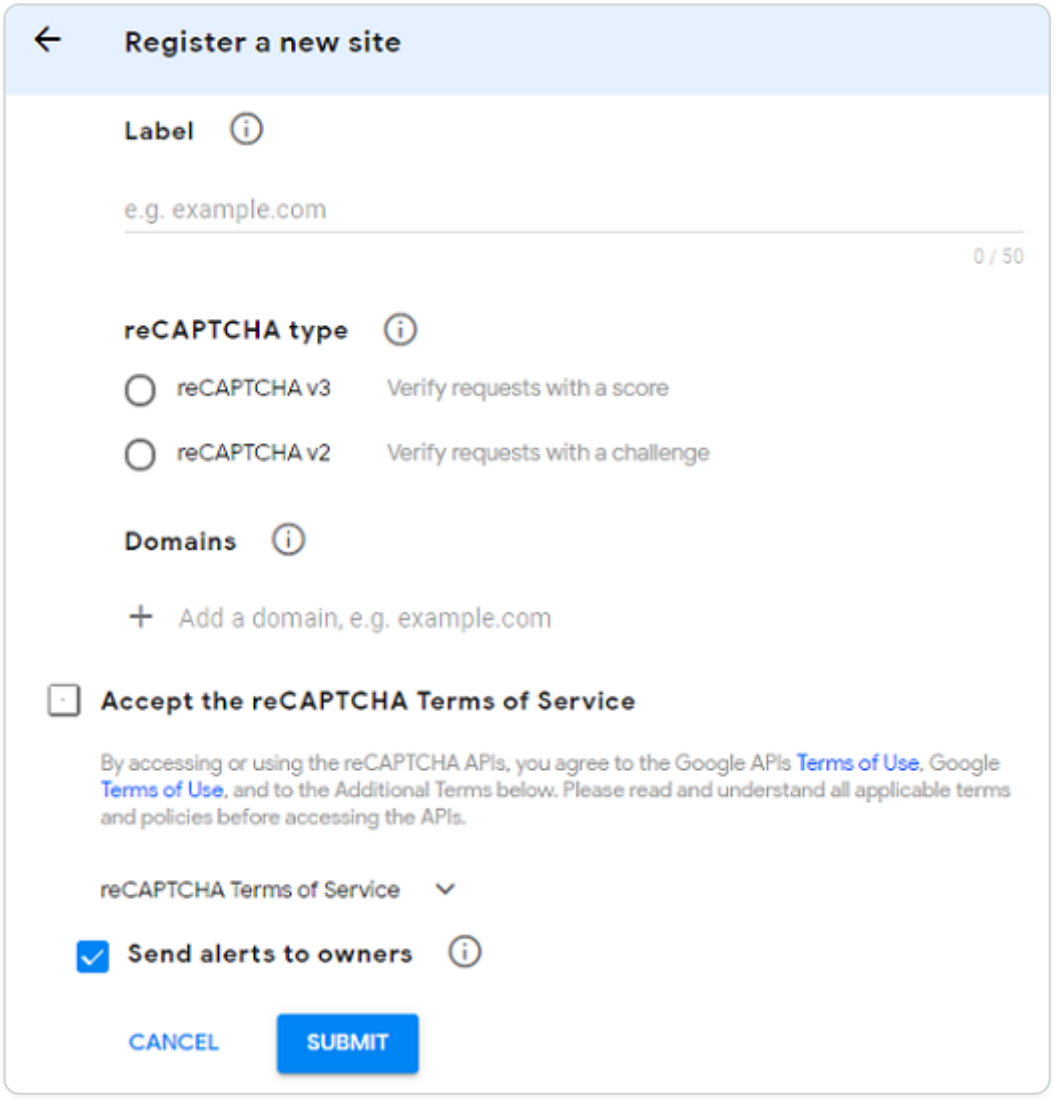
1. Configuración en Google para registrar Captcha.
2. Configuración en el dispositivo NetScaler para usar Captcha como parte del flujo de inicio de sesión.

#### Configuración de Captcha en Google

Registre un dominio para Captcha en `https://www.google.com/recaptcha/admin#list`.

1. Cuando navega a esta página, aparece la siguiente pantalla.

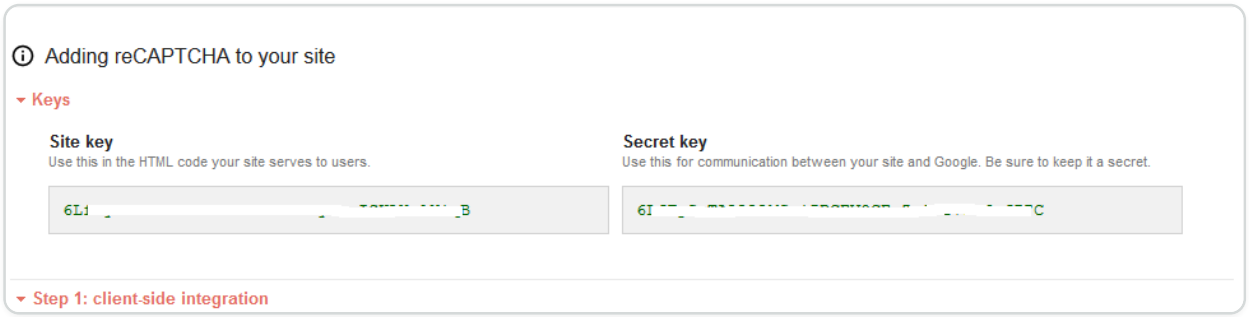
© 1997–2026 Citrix Systems, Inc. All rights reserved.




**NOTA**

Utilice `reCAPTCHA` v2 solamente. `reCAPTCHA` invisible todavía está en vista previa.

2. Después de registrar un dominio, se muestran la "SiteKey" y la "SecretKey".




© 1997–2026 Citrix Systems, Inc. All rights reserved.

**NOTA**

La "SiteKey" y la "SecretKey" aparecen atenuadas por motivos de seguridad. La "SecretKey" debe mantenerse a salvo.

### Configuración de Captcha en el dispositivo NetScaler

La configuración de Captcha en el dispositivo NetScaler se puede dividir en tres partes:

- Mostrar pantalla de Captcha
- Enviar la respuesta de Captcha al servidor de Google
- La configuración LDAP es el segundo factor para el inicio de sesión del usuario (opcional)

### Mostrar pantalla de Captcha

La personalización del formulario de inicio de sesión se realiza a través del esquema de inicio de sesión SingleAuthCaptcha.xml. Esta personalización se especifica en el servidor virtual de autenticación y se envía a la interfaz de usuario para renderizar el formulario de inicio de sesión. El esquema de inicio de sesión integrado, SingleAuthCaptcha.xml, se encuentra en el directorio `/nsconfig/loginSchema/LoginSchema` del dispositivo NetScaler.

**IMPORTANTE:**

- Según su caso de uso y los diferentes esquemas, puede modificar el esquema existente. Por ejemplo, si solo necesita el factor Captcha (sin nombre de usuario ni contraseña) o la autenticación dual con Captcha.
- Si se realizan modificaciones personalizadas o se cambia el nombre del archivo, Citrix recomienda copiar todos los esquemas de inicio de sesión del directorio /nsconfig/loginschema/LoginSchema al directorio principal, /nsconfig/loginschema.

### Para configurar la visualización de Captcha mediante la CLI

```
-  add authentication loginSchema singleauthcaptcha
-authenticationSchema /nsconfig/loginschema/SingleAuthCaptcha.xml



-  add authentication loginSchemaPolicy singleauthcaptcha -rule true
-action singleauthcaptcha
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
-  add authentication vserver auth SSL <IP> <Port>


-  add ssl certkey vserver-cert -cert <path-to-cert-file> -key <path-to-
key-file>

-  bind ssl vserver auth -certkey vserver-cert

-  bind authentication vserver auth -policy singleauthcaptcha -priority 5
-gotoPriorityExpression END
```

### Enviar la respuesta de Captcha al servidor de Google

Después de configurar el Captcha que debe mostrarse a los usuarios, los administradores envían la configuración al servidor de Google para verificar la respuesta de Captcha del navegador.

#### PARA VERIFICAR LA RESPUESTA DE CAPTCHA DEL NAVEGADOR

```
-  add authentication captchaAction myrecaptcha -sitekey <sitekey-copied-
from-google> -secretkey <secretkey-from-google>


-  add authentication policy myrecaptcha -rule true -action myrecaptcha

-  bind authentication vserver auth -policy myrecaptcha -priority 1
```

Los siguientes comandos son necesarios para configurar la autenticación AD si se desea. De lo contrario, puede omitir este paso.

```
-  add authentication ldapAction ldap-new -serverIP x.x.x.x -serverPort
636 -ldapBase "cn=users,dc=aaatm,dc=com" -ldapBindDn adminuser@aaatm.com
-ldapBindDnPassword <password> -encrypted -encryptmethod ENCMTHD_3
-ldapLoginName sAMAccountName -groupAttrName memberof -subAttributeName CN
-secType SSL -passwdChange ENABLED -defaultAuthenticationGroup ldapGroup
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
-  add authenticationpolicy ldap-new -rule true -action ldap-new
```

### La configuración LDAP es el segundo factor para el inicio de sesión del usuario (opcional)

La autenticación LDAP se produce después de Captcha, la añade al segundo factor.

```
-  add authentication policylabel second-factor

-  bind authentication policylabel second-factor -policy ldap-new
-priority 10

-  bind authentication vserver auth -policy myrecaptcha -priority 1
-nextFactor second-factor
```

El administrador debe añadir los servidores virtuales apropiados según se utilice un servidor virtual de equilibrio de carga o un dispositivo NetScaler Gateway para el acceso. El administrador debe configurar el siguiente comando si se requiere un servidor virtual de equilibrio de carga:

```
add lb vserver lbtest HTTP <IP> <Port> -authentication ON
-authenticationHost nssp.aaatm.com`
```

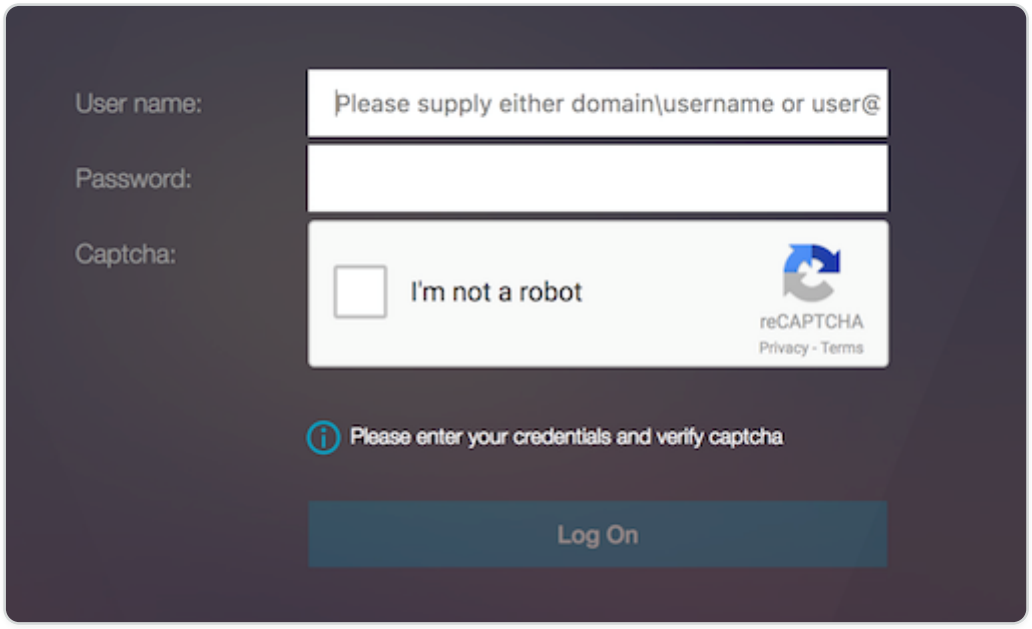
**nssp.aaatm.com** – Se resuelve en el servidor virtual de autenticación.

### Validación de Captcha por parte del usuario

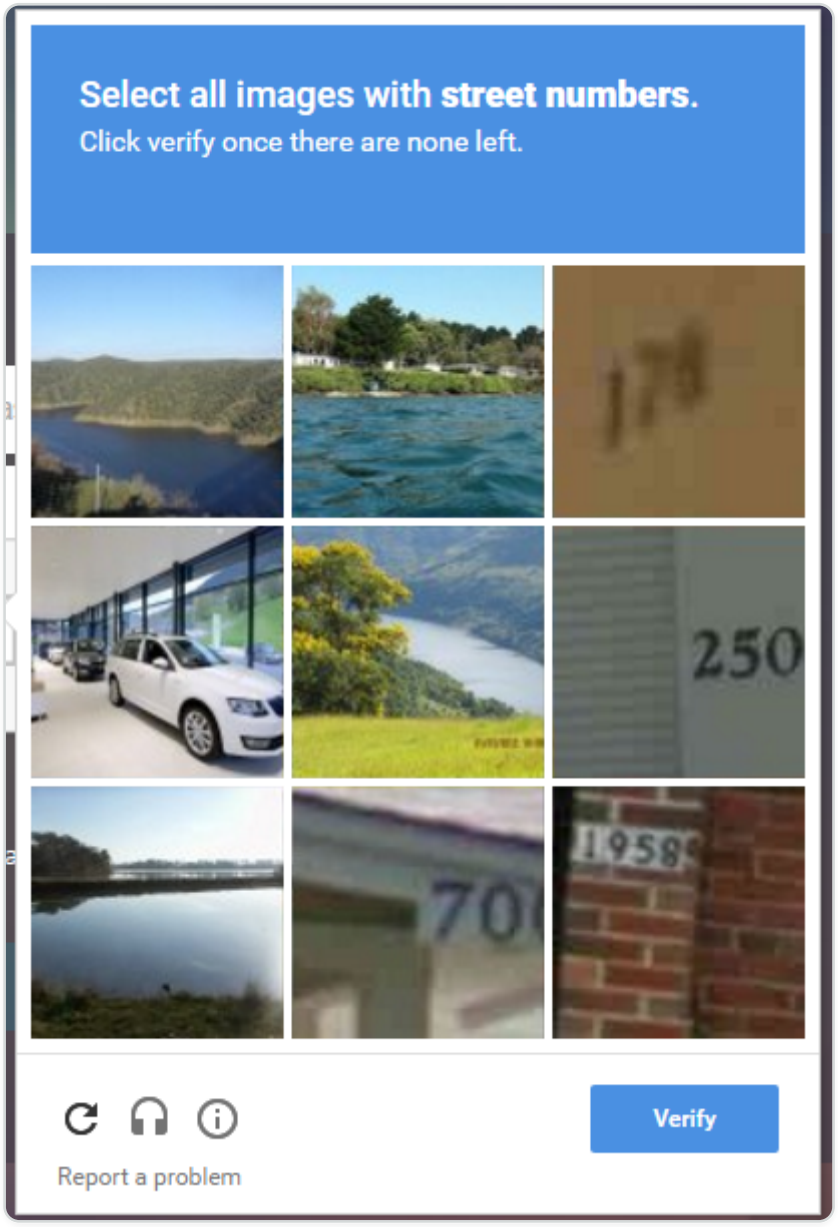
Una vez que haya configurado todos los pasos mencionados en las secciones anteriores, consulte las capturas de pantalla de la interfaz de usuario anteriores.

1. Una vez que el servidor virtual de autenticación carga la página de inicio de sesión, se muestra la pantalla de inicio de sesión. **Iniciar sesión** está deshabilitado hasta que se complete el Captcha.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

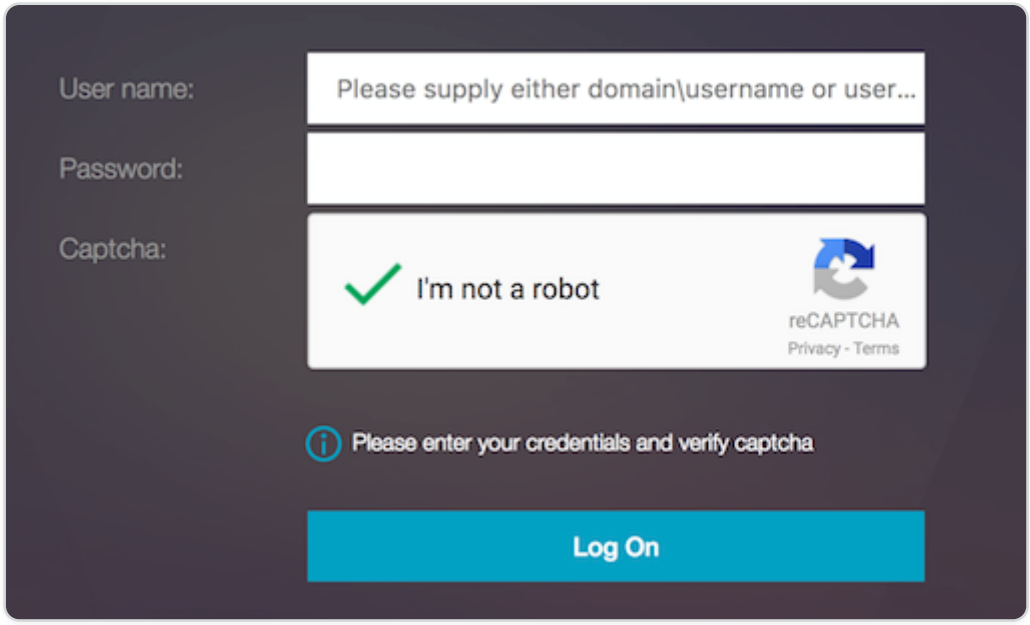



2. Seleccione la opción No soy un robot. Se muestra el widget de Captcha.




© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. Se le guiará a través de una serie de imágenes de Captcha antes de que se muestre la página de finalización.
4. Introduzca las credenciales de AD, marque la casilla **No soy un robot** y haga clic en **Iniciar sesión**. Si la autenticación se realiza correctamente, se le redirigirá al recurso deseado.

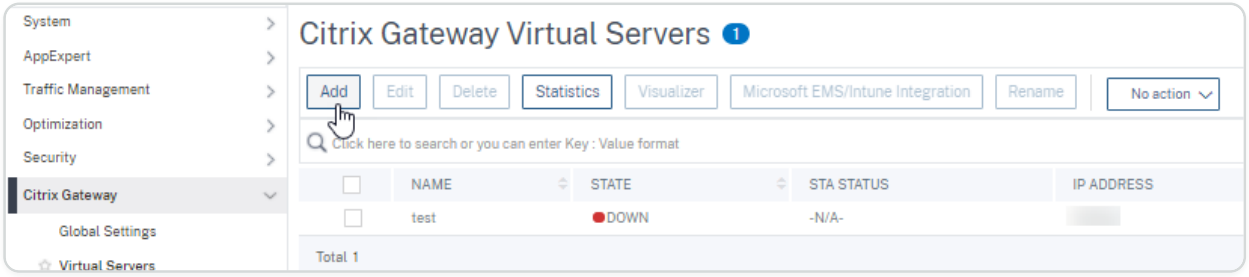



**NOTA:**

- Si se utiliza Captcha con la autenticación de AD, el botón Enviar credenciales se deshabilita hasta que se complete el Captcha.
- El Captcha ocurre en un factor propio. Por lo tanto, cualquier validación posterior, como la de AD, debe ocurrir en el `nextfactor` de Captcha.

## Crear un servidor virtual de Gateway para la autenticación nFactor en la licencia estándar de NetScaler

1. Vaya a **NetScaler Gateway>Servidores virtuales**.
2. En la página **Servidores virtuales de NetScaler Gateway**, haga clic en **Agregar**.

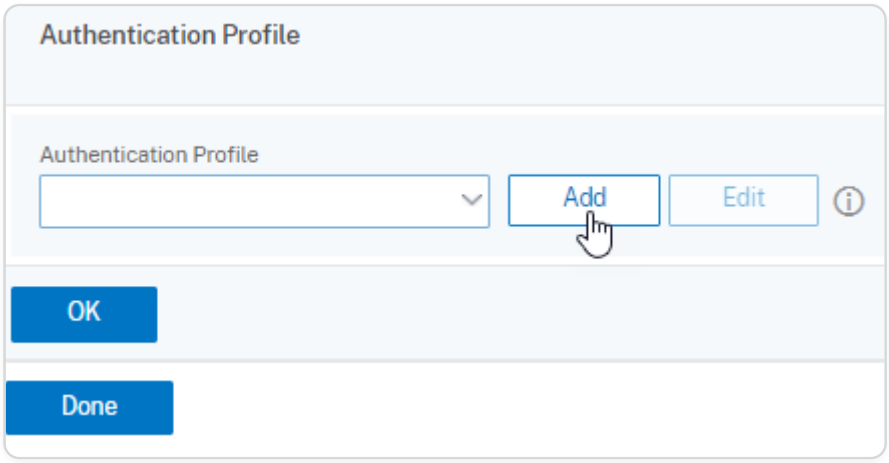



© 1997–2026 Citrix Systems, Inc. All rights reserved.

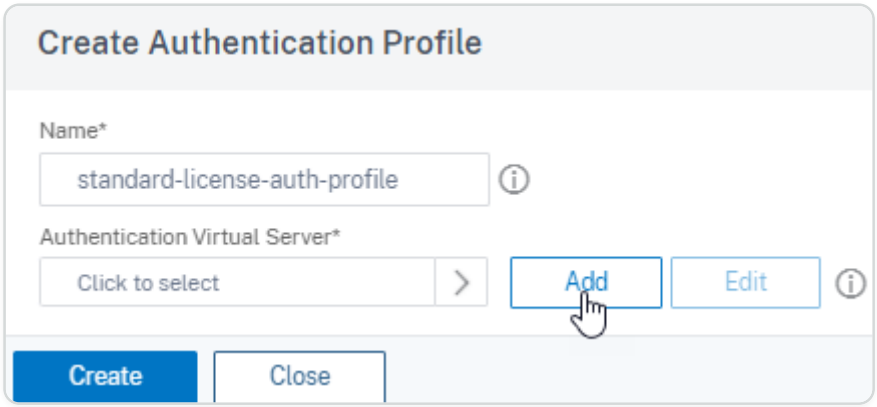
3. Introduzca los siguientes detalles en la página **Servidor virtual VPN**, haga clic en **Aceptar** y, a continuación, en **Continuar**.

   - Nombre: nombre del servidor virtual de NetScaler Gateway
   - Protocolo: seleccione **SSL**
   - Dirección IP: dirección IP del servidor virtual de NetScaler Gateway
   - Puerto: introduzca 443

   ](/en-us/netscaler-gateway/media/add-standard-license-virtual-server-citrix.png)
4. En la página **Servidor virtual VPN**, haga clic en el icono más junto a **Perfil de autenticación**.
5. Haga clic en **Agregar** para configurar el perfil de autenticación.




6. Introduzca un nombre para el perfil de autenticación y haga clic en **Agregar**.

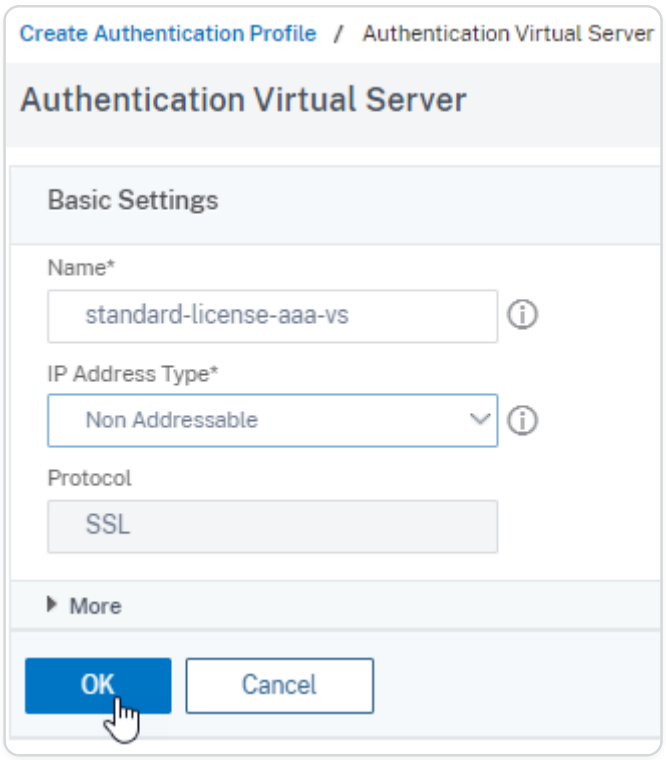



7. Introduzca los siguientes detalles en la página **Servidor virtual VPN**, haga clic en **Aceptar** y, a continuación, en **Continuar**.

   - Nombre: nombre del servidor virtual de autenticación, autorización y auditoría

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Protocolo: seleccione **No direccionable**. Solo se puede vincular un servidor virtual de autenticación, autorización y auditoría no direccionable a un servidor virtual de Gateway/ VPN en la licencia estándar de NetScaler.




**NOTA:**

- En la licencia estándar de NetScaler, los pasos para crear una política son los mismos que en la licencia Premium para los tipos de política admitidos.
- La licencia estándar de NetScaler no admite la adición de nuevos esquemas de inicio de sesión en la configuración de nFactor.

### Referencias

Para ver un ejemplo de configuración de nFactor de extremo a extremo, consulte Configuración de la autenticación nFactor.

## Visualizador de Unified Gateway

El Visualizador de Unified Gateway proporciona una representación visual de las configuraciones mediante el Asistente de Unified Gateway. El Visualizador de Unified Gateway se utiliza para agregar y editar configuraciones, y para diagnosticar un problema de back-end.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

El Visualizador de Unified Gateway muestra lo siguiente:

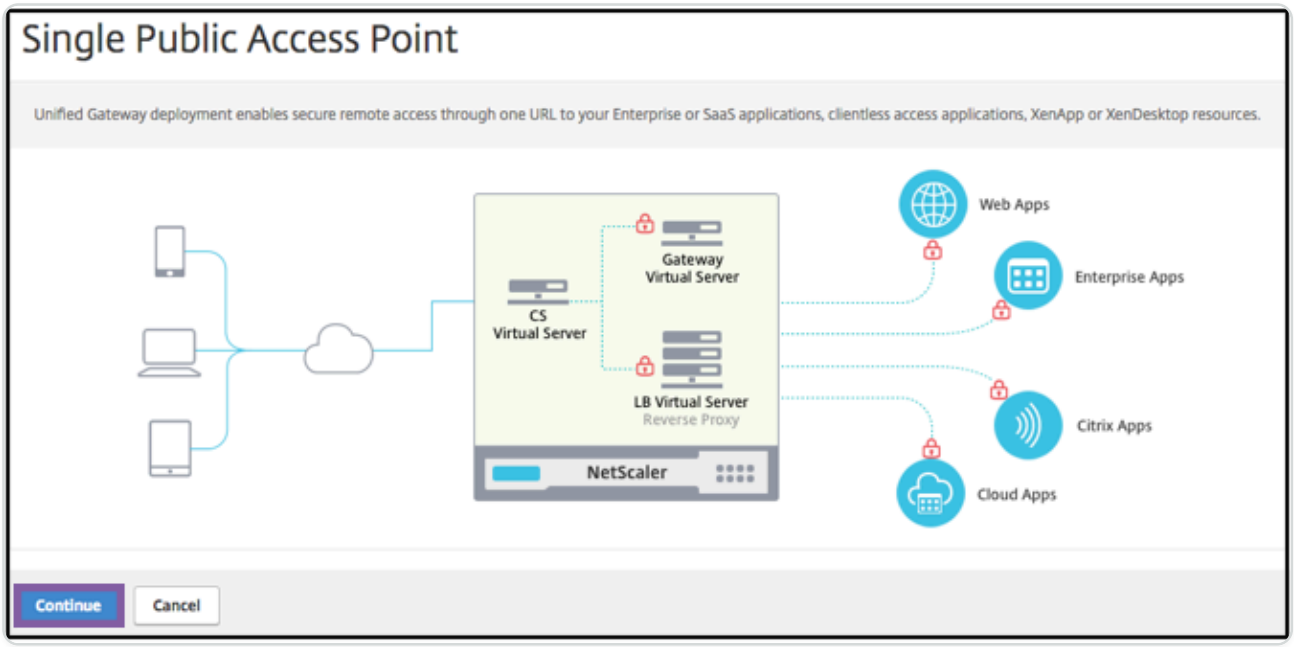
| CONFIGURACIÓN | CONFIGURACIÓN |
|---|---|
| Directivas de preautenticación | Directivas de autenticación |
| Servidores virtuales CS | Servidores virtuales VPN |
| Servidores virtuales LB | Aplicaciones XA/XD |
| Aplicaciones web | Aplicaciones SaaS |

La implementación de Unified Gateway permite el acceso remoto seguro a través de una URL a sus aplicaciones empresariales o SaaS, aplicaciones de acceso sin cliente, Citrix Virtual Apps™ y recursos de escritorios.

## Configurar Unified Gateway

1. Seleccione Unified Gateway en el menú.
2. En la siguiente pantalla, verificar que tiene la siguiente información y, a continuación, haga clic en **Comenzar**:
   - Dirección IP pública para Unified Gateway.
   - Cadena de certificados de servidor (.PFX o .PEM) con certificado de CA raíz opcional.
   - Detalles de autenticación basados en LDAP/RADIUS/Certificado de cliente.
   - Detalles de la aplicación (URL para aplicaciones SaaS o detalles del servidor de Citrix Virtual Apps and Desktops).
3. Haga clic en el botón **Continuar**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



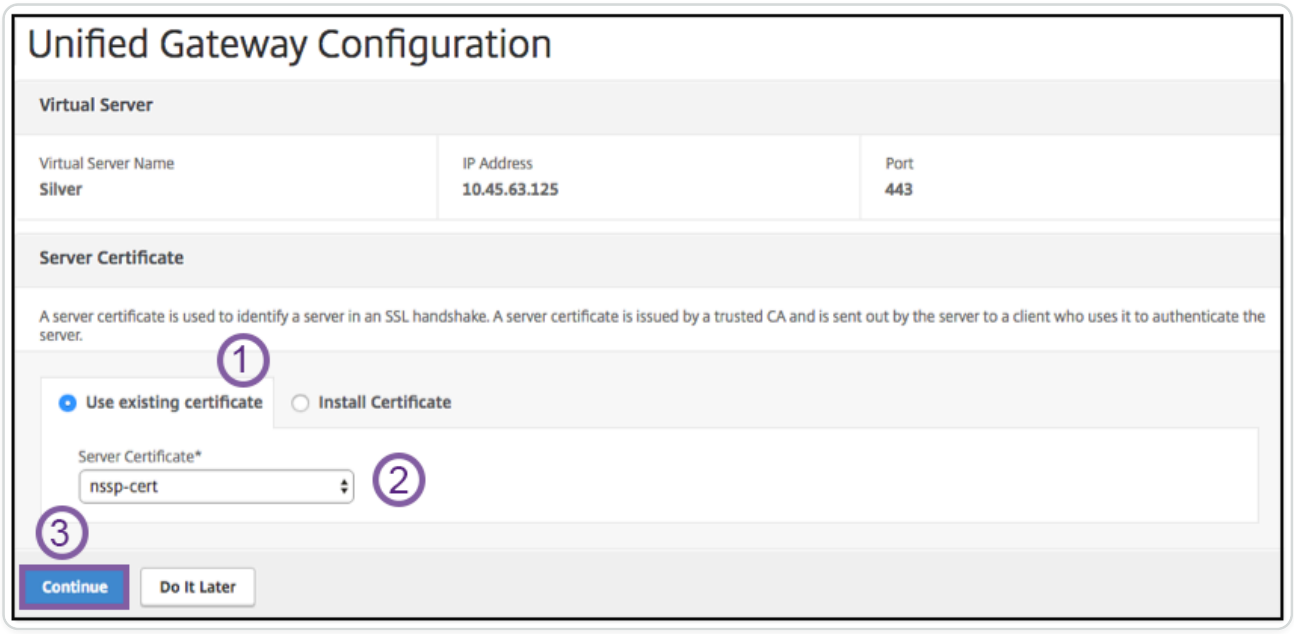

**Cree un servidor virtual de configuración de Unified Gateway.**

1. Introduzca el **Nombre** de configuración para el servidor virtual.
2. Introduzca la **dirección IP de Unified Gateway** pública para la implementación de Unified Gateway.
3. Introduzca el número de **Puerto**. El rango de números de puerto es 1–65535.
4. Haga clic en **Continuar**.

**Complete la siguiente información para especificar el certificado de servidor.**

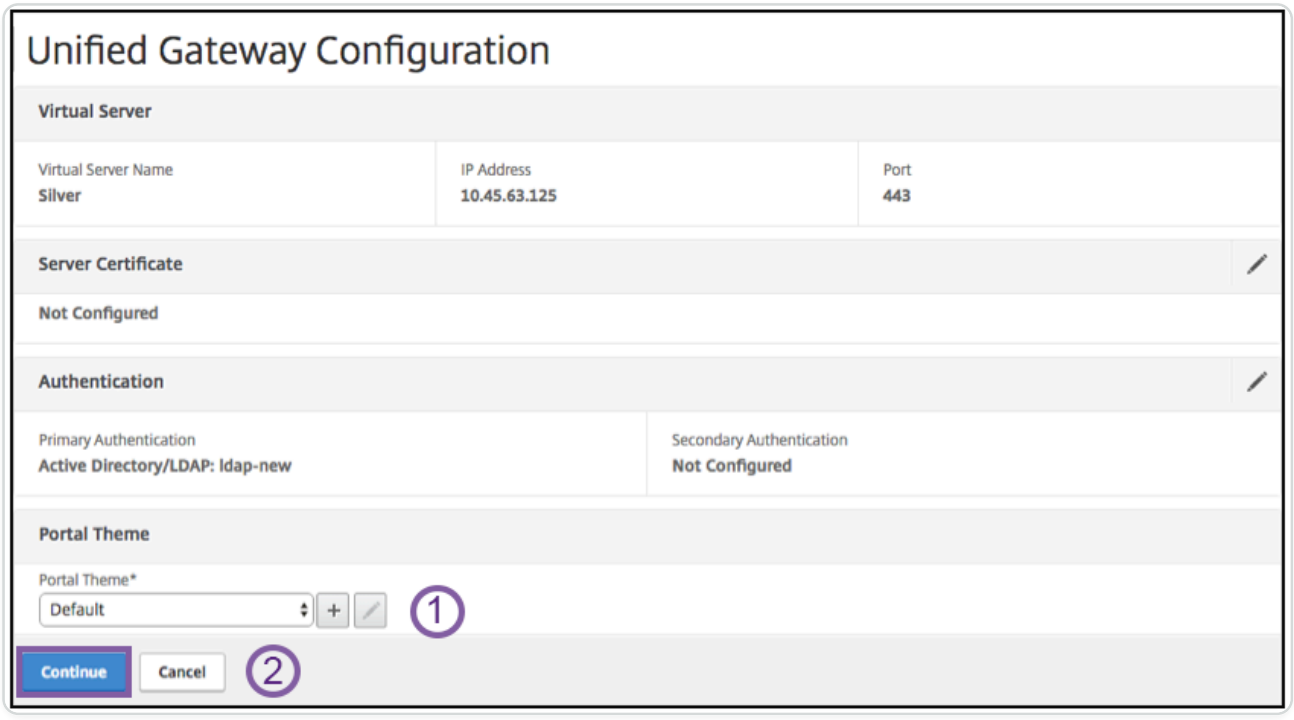
1. Seleccione los botones de radio **Usar certificado existente** o **Instalar certificado**.
2. Seleccione un **Certificado de servidor** del menú.
3. Haga clic en el botón **Continuar**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.




**Complete la siguiente información para especificar la autenticación.**

1. Seleccione un **Método de autenticación principal** del menú.
2. Seleccione los botones de radio **Usar servidor existente** o **Agregar nuevo servidor**.
3. Haga clic en el botón **Continuar**.
4. Seleccione el **Tema del portal** del menú.
5. Haga clic en **Continuar**.
6. Seleccione los botones de radio **Aplicación web** o **Citrix Virtual Apps Desktops**.
7. Haga clic en **Continuar**.




Seleccionar aplicación

© 1997–2026 Citrix Systems, Inc. All rights reserved.

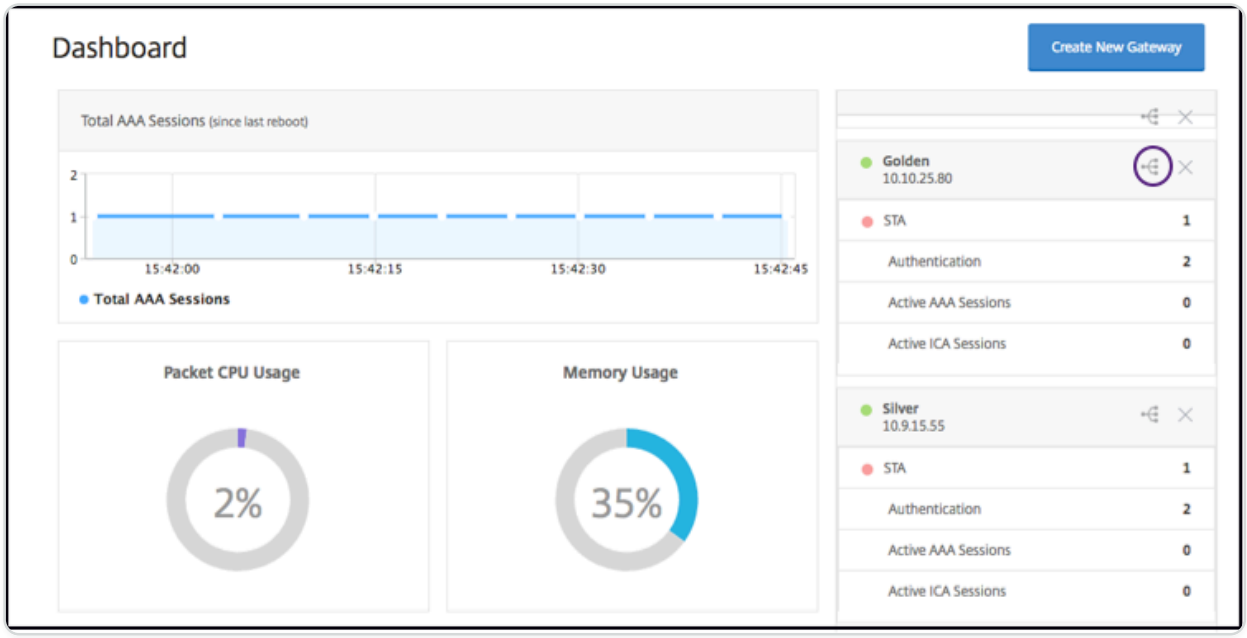
**Complete la siguiente información para especificar la aplicación web.**

1. Introduzca el nombre del enlace de marcador.
2. Seleccione el tipo de aplicación que representa la URL de VPN. Los valores posibles son:
    - Aplicación de Intranet
    - Acceso sin cliente
    - SaaS
    - Aplicación preconfigurada en este NetScaler
3. Marque esta casilla para que esta aplicación sea accesible a través de la URL de Unified Gateway.
4. Introduzca la URL para el enlace de marcador.
5. Desde la URL del icono, elija un archivo para obtener un archivo de icono. La longitud máxima = 255
6. Haga clic en el botón **Continuar**.
7. Haga clic en **Listo**.
8. Haga clic en **Continuar**.
9. Haga clic en **Listo**.

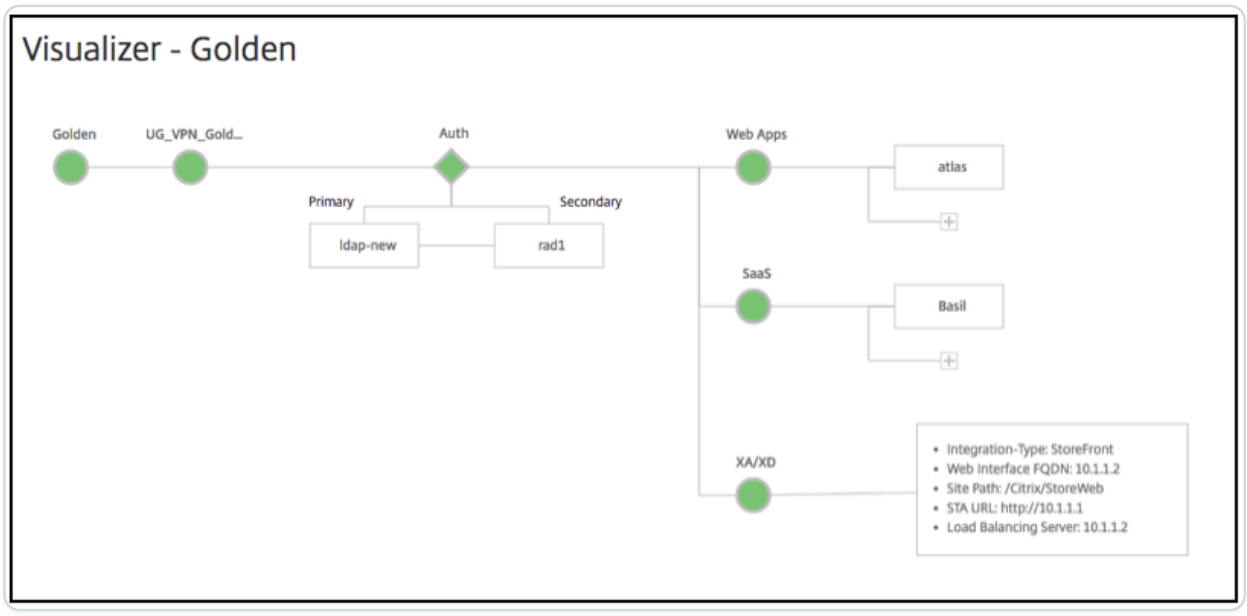
## Configuración de la GUI

1. Seleccione Unified Gateway en el menú.
2. Haga clic en el icono **Unified Gateway Visualizer** para acceder a las instancias de Gateway configuradas.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

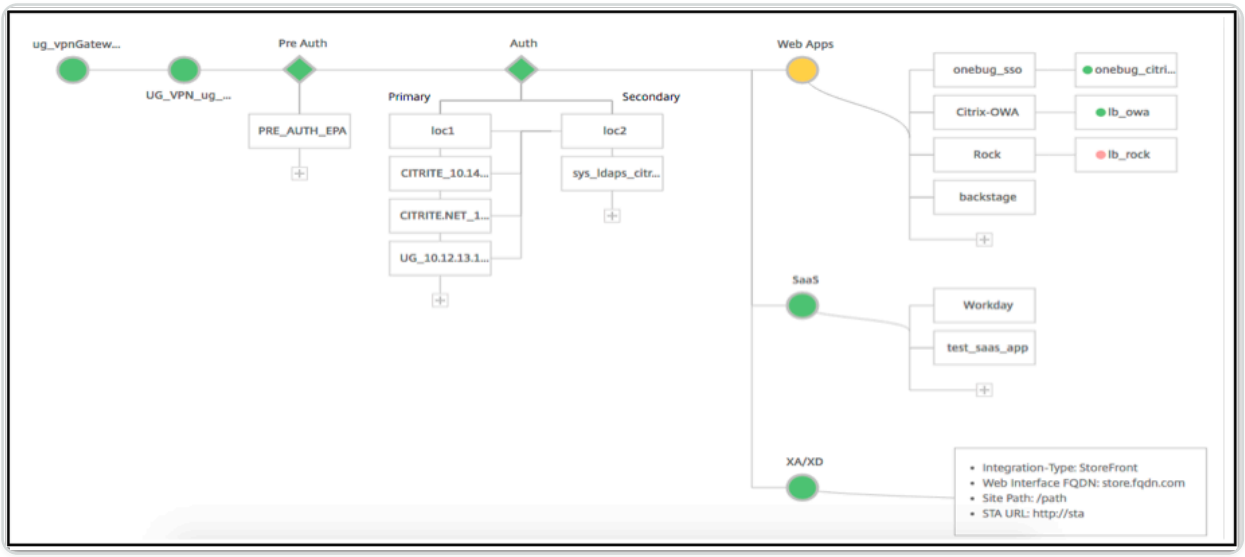



El Visualizador de Unified Gateway se parece a un diagrama de flujo, como se muestra en la siguiente imagen:




El Visualizador de Unified Gateway tiene una sección de PreAuth, `Auth` y una sección de Aplicaciones. Si el servidor virtual VPN tiene una política de preautenticación, solo entonces se muestra `pre-auth` en el Visualizador de Unified Gateway.

© 1997–2026 Citrix Systems, Inc. All rights reserved.




El Visualizador de Unified Gateway utiliza un esquema de codificación de colores para los servidores virtuales de equilibrio de carga y VPN para indicar su estado.

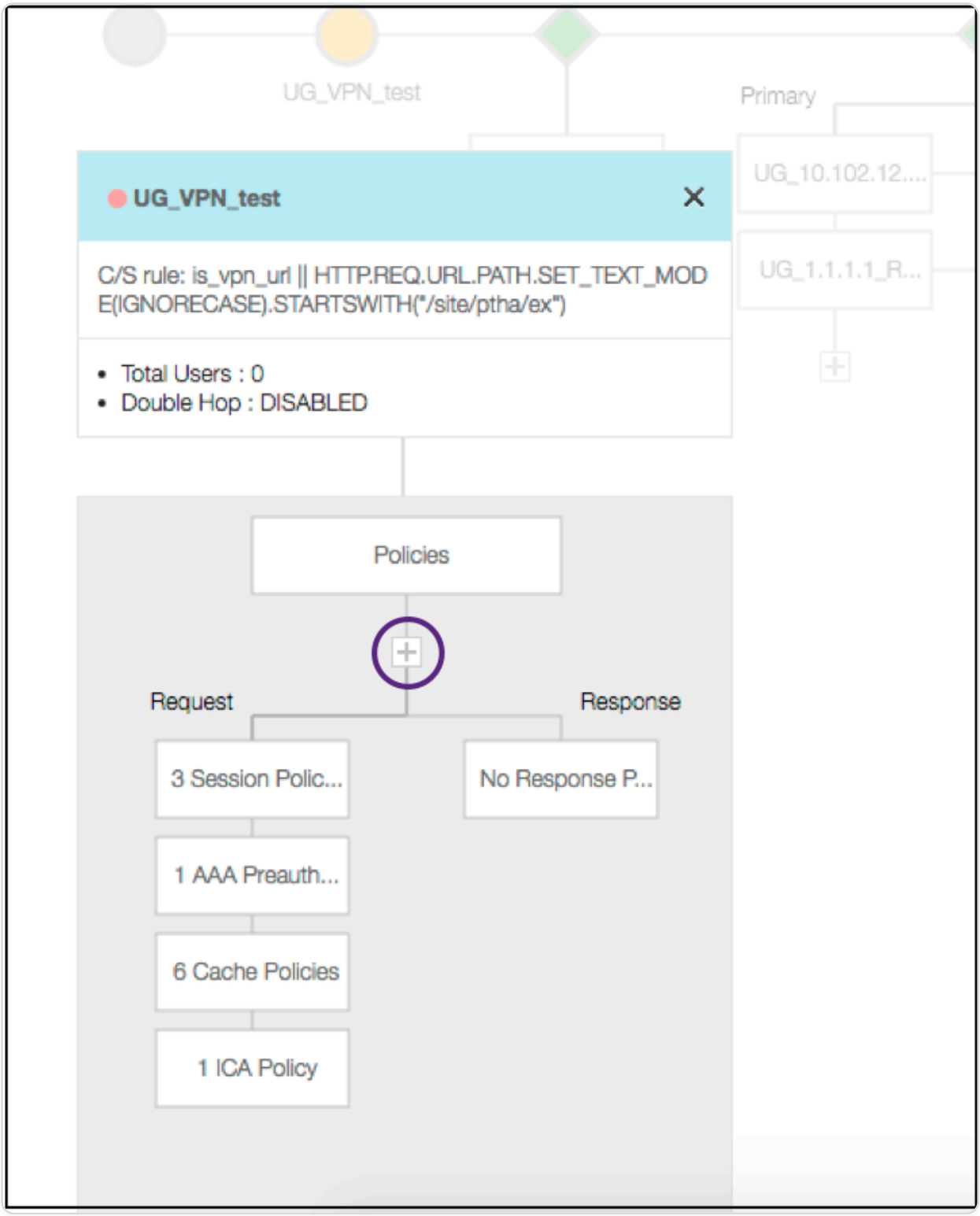
| COLOR | DESCRIPCIÓN |
|---|---|
| Rojo | significa que el servidor está inactivo. |
| Gris | significa que las aplicaciones web/Citrix Virtual Apps no se han configurado. |
| Verde | significa que todo está bien con el servidor virtual. |
| Naranja | significa que uno de los servicios del servidor virtual de equilibrio de carga. está inactivo, pero sigue funcionando correctamente. |

## Detalles de los servidores virtuales VPN

Para obtener los detalles de los servidores virtuales VPN, haga clic en el **nodo de servidores virtuales VPN**. La ventana emergente muestra detalles como la regla C/S y todas las políticas.

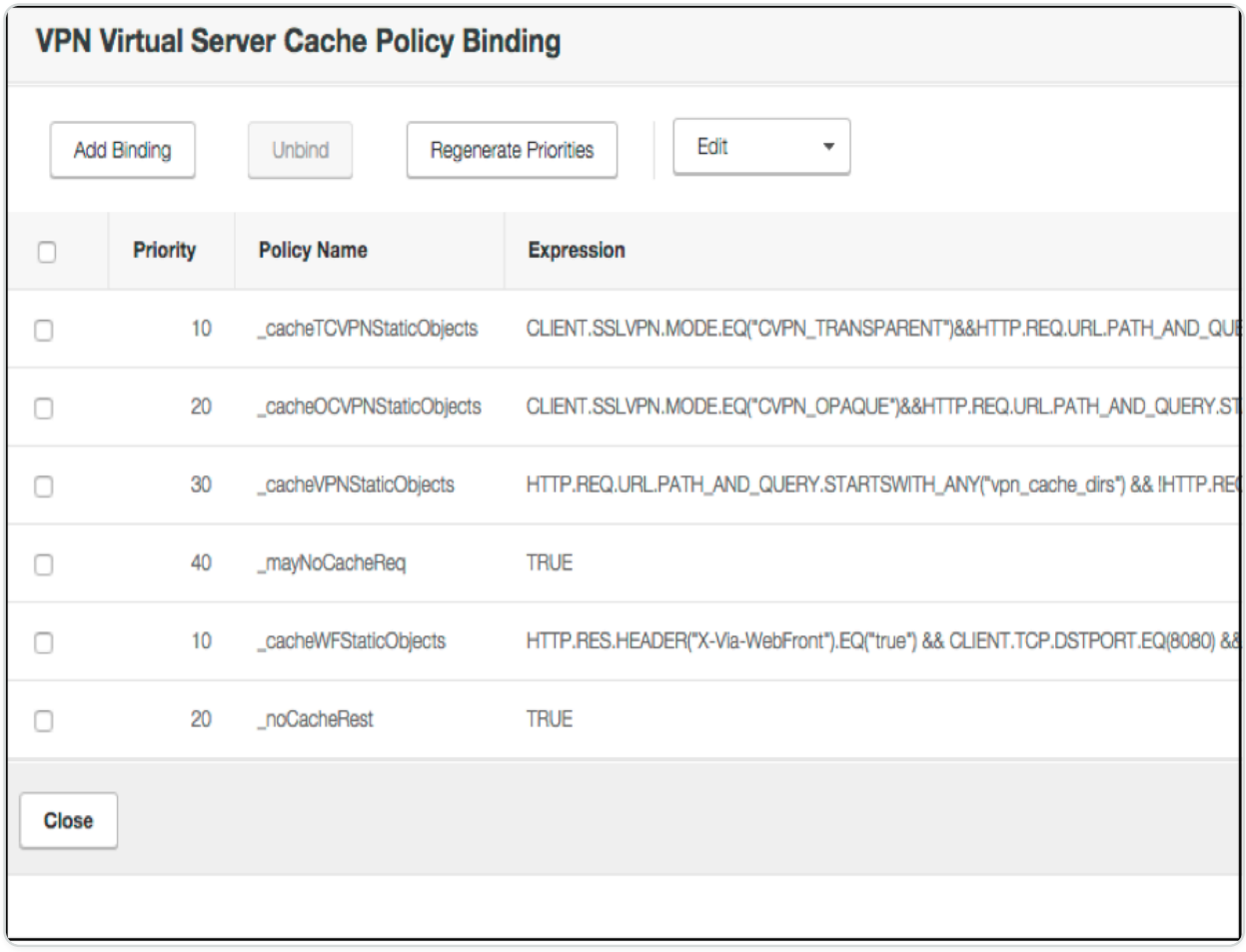
1. Agregue políticas a la entidad VPN haciendo clic en el icono (+).

© 1997–2026 Citrix Systems, Inc. All rights reserved.

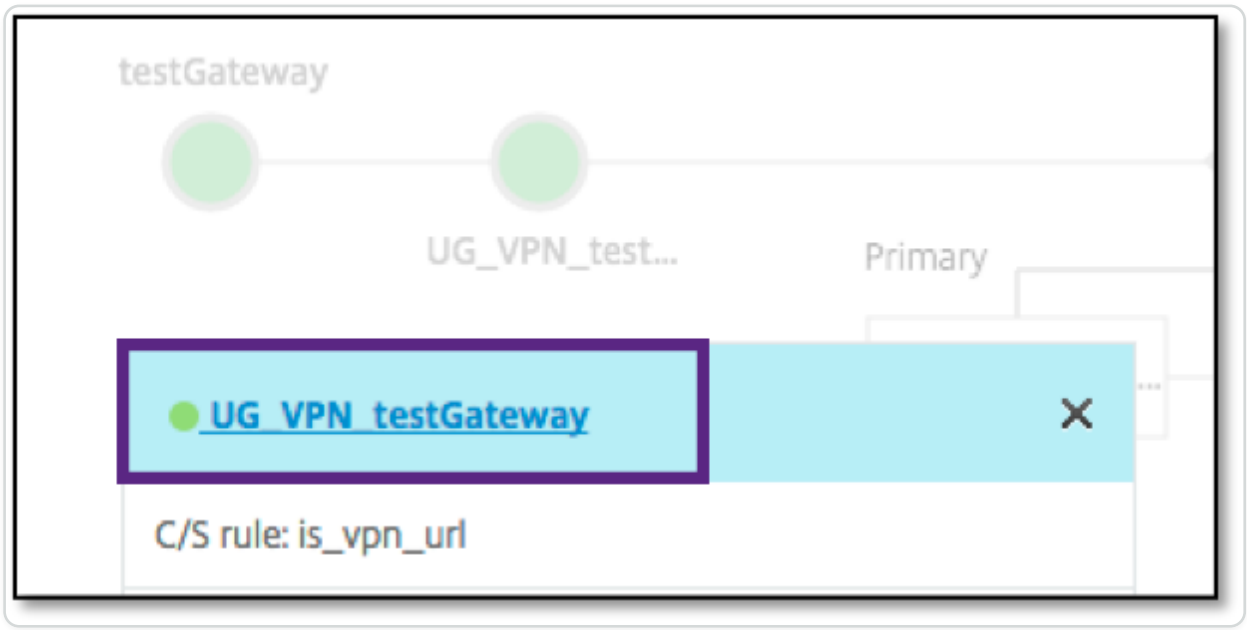



2. Haga clic en el nodo deseado para ver los detalles de las políticas ya configuradas.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

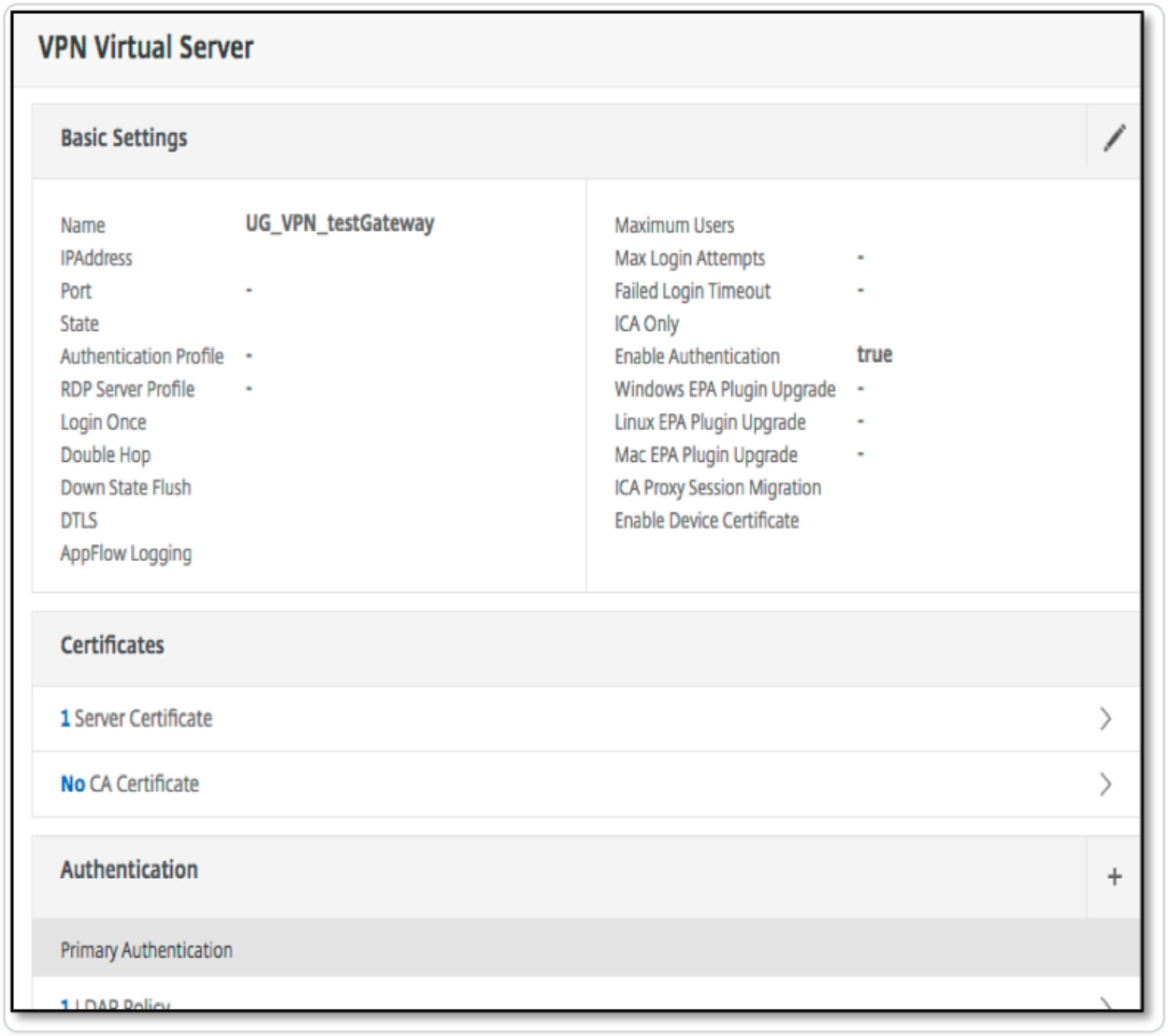



Para obtener información del servidor virtual VPN, el título VPN en la ventana emergente es una entidad en la que se puede hacer clic y que lleva a un control deslizante que detalla el servidor virtual VPN.




Los detalles del servidor VPN se muestran aquí.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

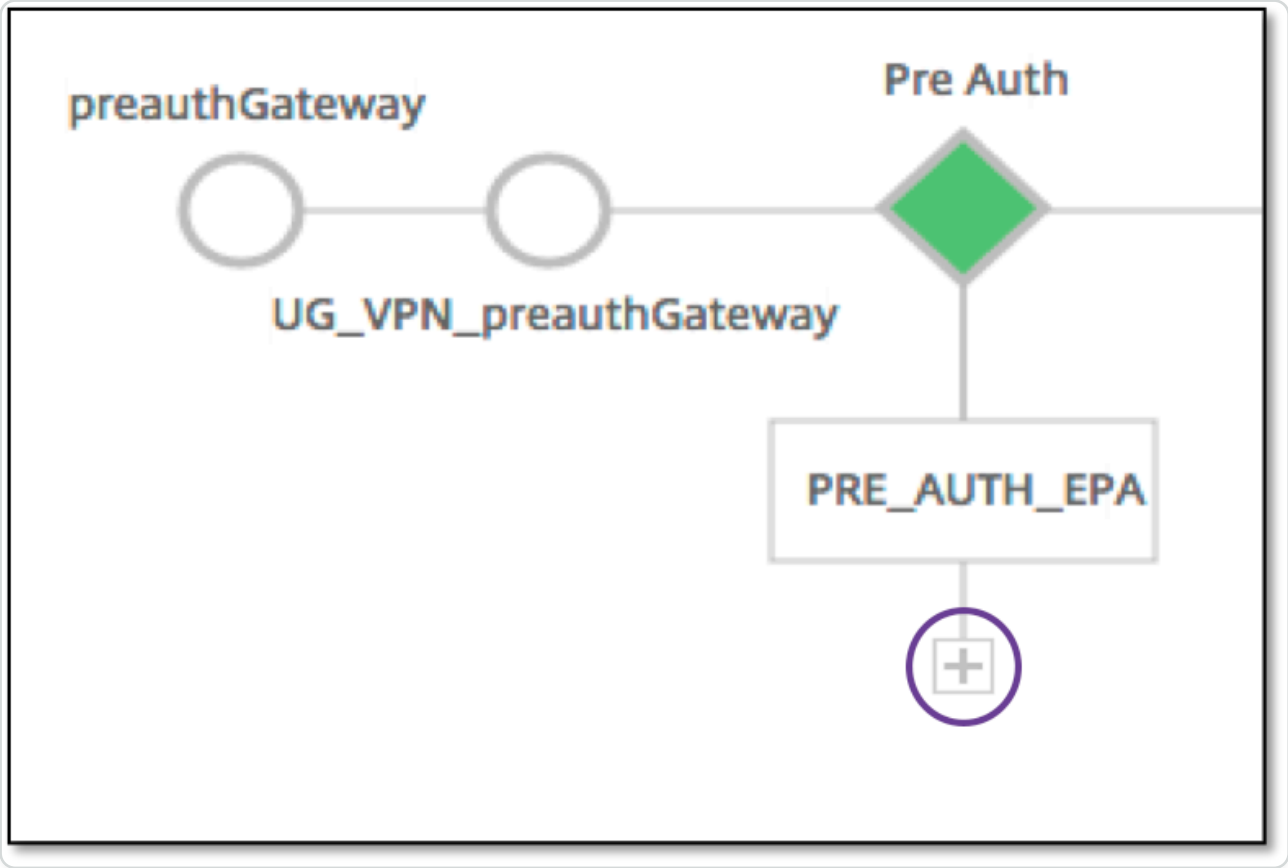



## The Pre Auth Block

Si un servidor virtual VPN tiene políticas de preautenticación asociadas, el Visualizador de Unified Gateway muestra un bloque `Pre Auth`. El bloque `Pre Auth` muestra las políticas y proporciona una opción para agregar políticas de preautenticación a la VPN.

1. Haga clic en el **+** para agregar una política `preauth`.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



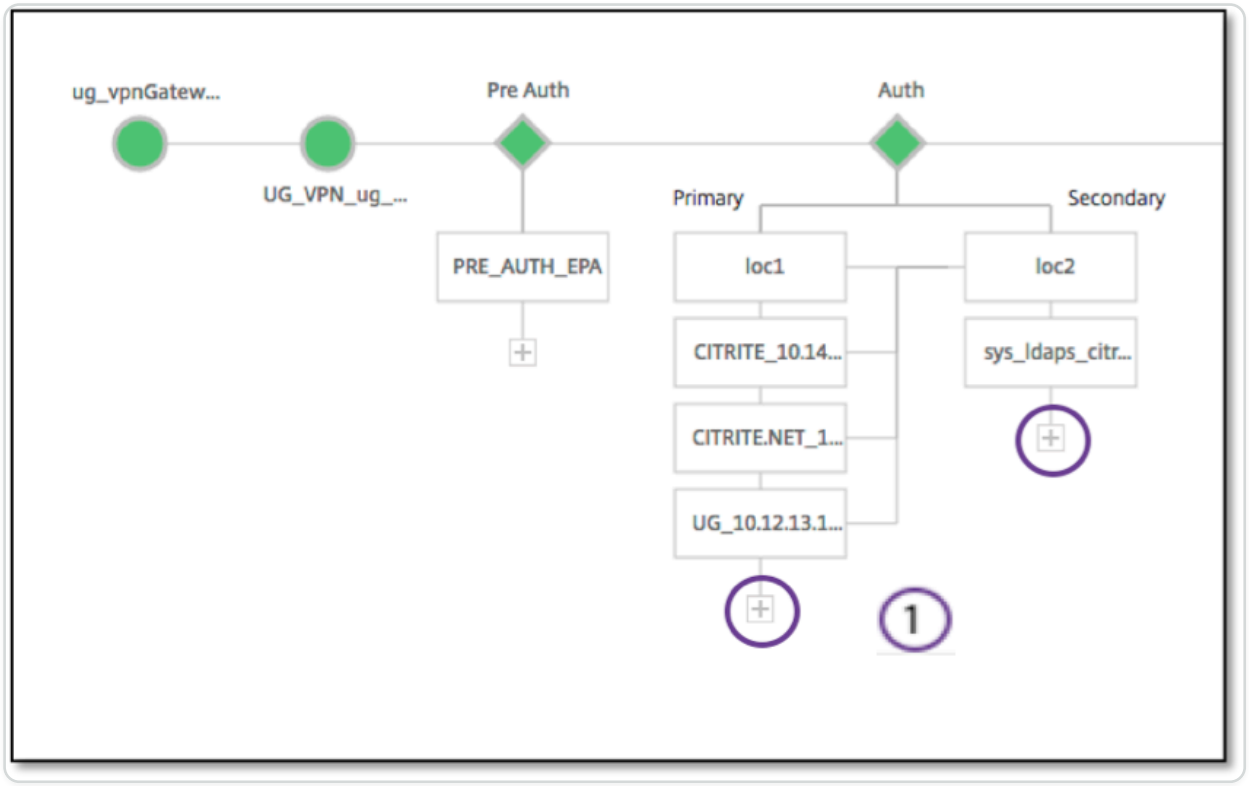

En un caso en el que no haya políticas de preautenticación asociadas, este bloque estaría oculto.

## The Auth Block

El bloque `Auth` enumera las políticas principales y secundarias. El bloque `Auth` ofrece una opción para añadir políticas.

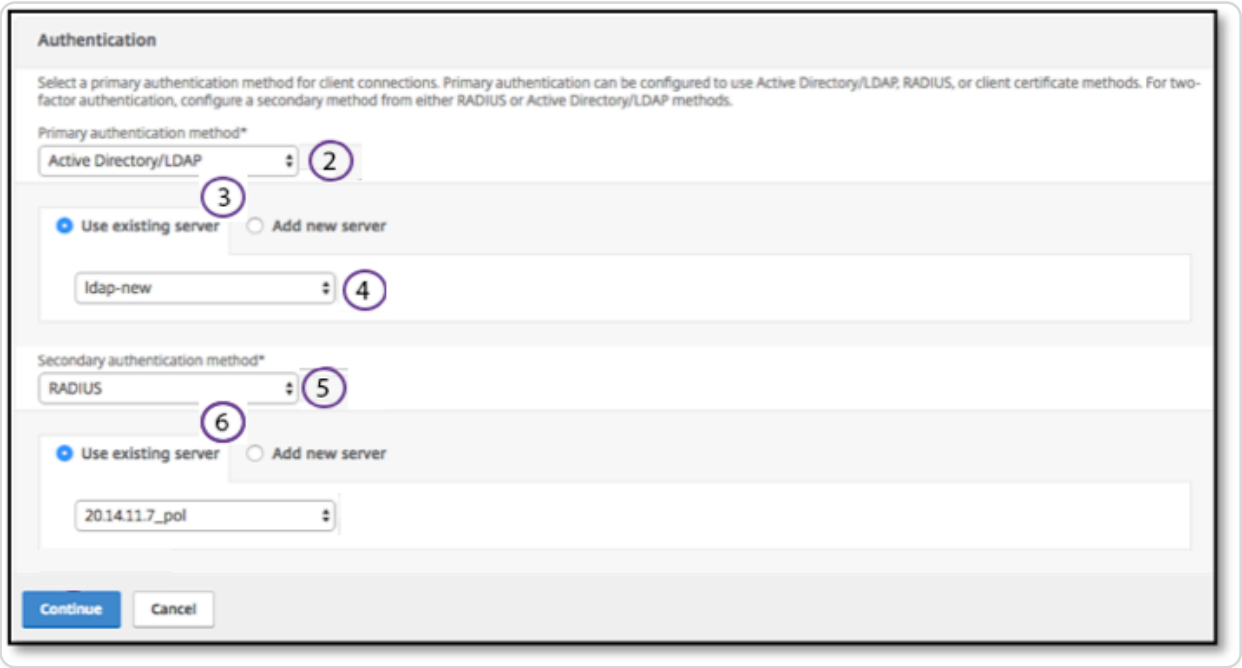
1. Haga clic en **+** en la lista Principal para añadir un enlace de autenticación principal o haga clic en + en la lista Secundaria para añadir un enlace de autenticación secundaria.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



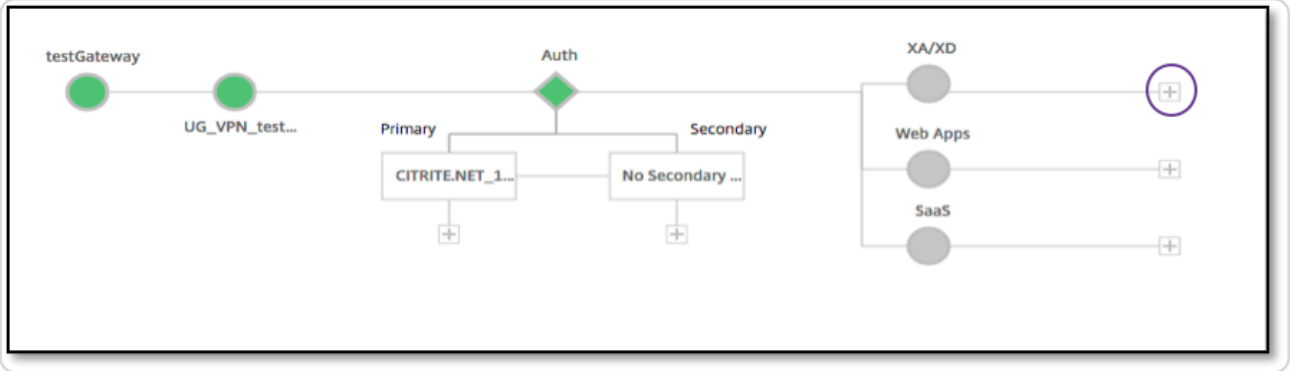

2. Seleccione una opción en el menú **Método de autenticación principal**.
3. Especifique si es un **servidor existente** o **Añadir nuevo servidor** seleccionando el botón de opción.
4. Seleccione una opción en el menú **Nombre de la política LDAP**.
5. Seleccione **RADIUS** en el menú **Método de autenticación secundaria**.
6. Especifique si desea **usar un servidor existente** o **Añadir nuevo servidor** seleccionando el botón de opción.
7. Haga clic en **Continuar**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.




## Adición de StoreFront™

1. Haga clic en **+** cerca de XA/XD, y le llevará a la adición de aplicaciones “XA/XD”.




Puede elegir su punto de integración. Las opciones son StoreFront, WI o WionNS. Haga clic en **Continuar**.

1. Complete los siguientes campos para configurar StoreFront. Los campos que requieren información obligatoria están marcados con un *.

| CAMPO | DESCRIPCIÓN |
| --- | --- |
| FQDN de StoreFront* | Introduzca el FQDN del servidor StoreFront. Longitud máxima: 255 caracteres. Ejemplo:// storefront.xendt.net |
| Ruta del sitio* | Introduzca la ruta a Receiver para el sitio web ya configurado en StoreFront. |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| CAMPO | DESCRIPCIÓN |
| --- | --- |
| Dominio predeterminado para la autenticación de usuarios `Single Sign-on Domain` * | Introduzca el dominio predeterminado para la autenticación de usuarios |
| Nombre del almacén* | Introduzca el nombre de los monitores de StoreFront. El STORENAME es un argumento que define el nombre del almacén del servicio StoreFront para sondear el estado de los servidores StoreFront. Aplicable a los monitores de StoreFront. Longitud máxima: 31 |
| Servidor de Secure Ticket Authority* | Introduzca la URL de Secure Ticket Authority, normalmente presente en el controlador de entrega. Ejemplo: `http://sta` |
| Servidor StoreFront* | Introduzca la dirección IP del servidor StoreFront |
| Protocolo* | Introduzca el protocolo utilizado por el servidor. |
| Puerto* | Introduzca el puerto utilizado por el servidor. |
| Equilibrio de carga | Introduzca la configuración de equilibrio de carga para los servidores StoreFront. |
| Servidor virtual* | Introduzca la dirección IP pública para la implementación de Unified Gateway. |

2. Haga clic en **Continuar.**

## Adición de SaaS

1. Haga clic en **+** para añadir aplicaciones SaaS; esto le llevará a la página Añadir SaaS. Rellene los siguientes campos para configurar SaaS. Los campos que requieren información obligatoria se indican con un*.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| CAMPO | DESCRIPCIÓN |
|---|---|
| Nombre* | Introduzca el nombre del enlace de marcador. |
| Tipo de aplicación | Introduzca el tipo de aplicación que representa esta URL VPN. Los valores posibles son: Aplicación de intranet/Acceso sin cliente/SaaS/ Aplicación preconfigurada en este NetScaler |
| Introduzca la URL* | Introduzca la URL de la aplicación de intranet. |
| Elija **Archivo** | Introduzca la URL para obtener el archivo de icono para mostrar este recurso. Longitud máxima = 255 |

## Adición de aplicaciones web

1. Haga clic en **+** para añadir aplicaciones web; esto le llevará a la página Añadir aplicaciones web. Rellene los siguientes campos para configurar una aplicación web. Los campos que requieren información obligatoria se indican con un *.

| CAMPO | DESCRIPCIÓN |
|---|---|
| Nombre* | Introduzca el nombre del enlace de marcador. |
| Tipo de aplicación | Introduzca el tipo de aplicación que representa esta URL VPN. Los valores posibles son: Aplicación de intranet/Acceso sin cliente/SaaS/ Aplicación preconfigurada en este NetScaler |
| Introducir URL* | Introduzca la URL de la aplicación de Intranet. |
| Elegir **Archivo** | Introduzca la URL para obtener el archivo de icono para mostrar este recurso. MaxLength = 255 |

Si se puede acceder a una aplicación a través de la URL de Unified Gateway, se puede acceder a los detalles del servidor de equilibrio de carga haciendo clic en la aplicación:

© 1997–2026 Citrix Systems, Inc. All rights reserved.




Se pueden añadir nuevas directivas haciendo clic en (+) y todas las directivas vinculadas se pueden ver haciendo clic en el nodo que muestra la información de la directiva.

También se muestra el número de servicios vinculados al equilibrador de carga, junto con la información general del estado. Un clic adicional enumera todos los servicios. Se pueden añadir nuevos servicios al equilibrador de carga.

Para obtener más detalles del equilibrador de carga, el título de la ventana emergente es clicable y lleva a la página de detalles del servidor virtual de equilibrio de carga.

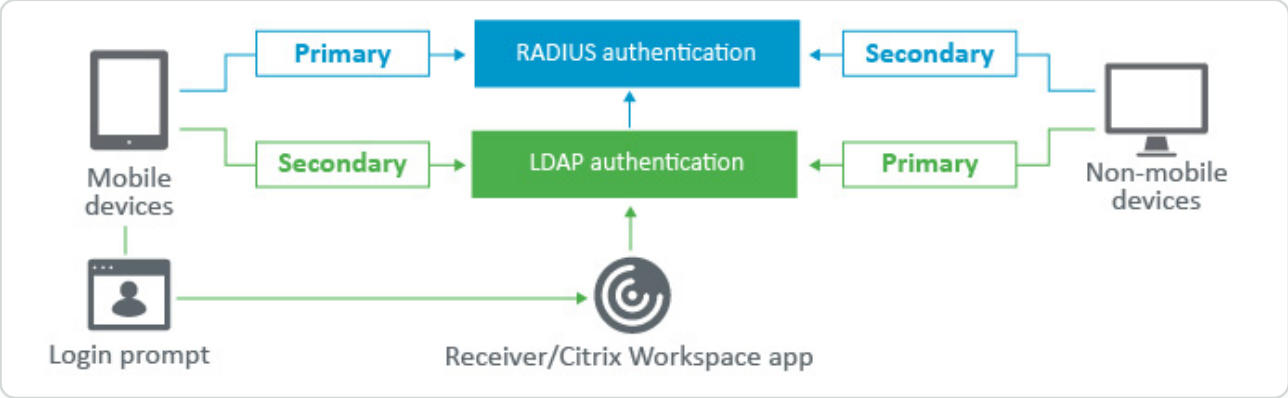
© 1997–2026 Citrix Systems, Inc. All rights reserved.

# Configurar NetScaler Gateway para usar autenticación RADIUS y LDAP con dispositivos móviles/tabletas

Esta sección describe cómo configurar el dispositivo NetScaler Gateway para usar la autenticación RADIUS como principal y la autenticación LDAP como secundaria con dispositivos móviles/tabletas.

La configuración demostrada en la sección sigue permitiendo que todas las demás conexiones utilicen LDAP primero y RADIUS segundo.

Cuando configura la autenticación de dos factores en la aplicación Citrix Workspace para usarla con dispositivos móviles/tabletas, debe agregar RSA SecureID (autenticación RADIUS) como autenticación principal. Pero cuando los usuarios reciben la solicitud de nombre de usuario y contraseña, código de acceso en Receiver, están introduciendo LDAP primero y RADIUS como segundas credenciales. Desde el punto de vista de un administrador, es una configuración diferente en comparación con una configuración no móvil.




Complete el siguiente procedimiento para configurar el dispositivo NetScaler Gateway para usar la autenticación RADIUS como principal y la autenticación LDAP como secundaria con dispositivos móviles/tabletas.

1. Desde la Utilidad de configuración, seleccione **NetScaler Gateway > Directivas > Autenticación** y cree una directiva de autenticación para LDAP y RSA para dispositivos móviles y no móviles. Esto es necesario para evitar una condición lógica que puede permitir a los usuarios omitir la autenticación RADIUS.
2. Introduzca los detalles del servidor LDAP después de hacer clic en la opción **Agregar** en la ficha **Servidores** para LDAP.
3. Cree una directiva LDAP para los dispositivos móviles eligiendo el servidor LDAP requerido.

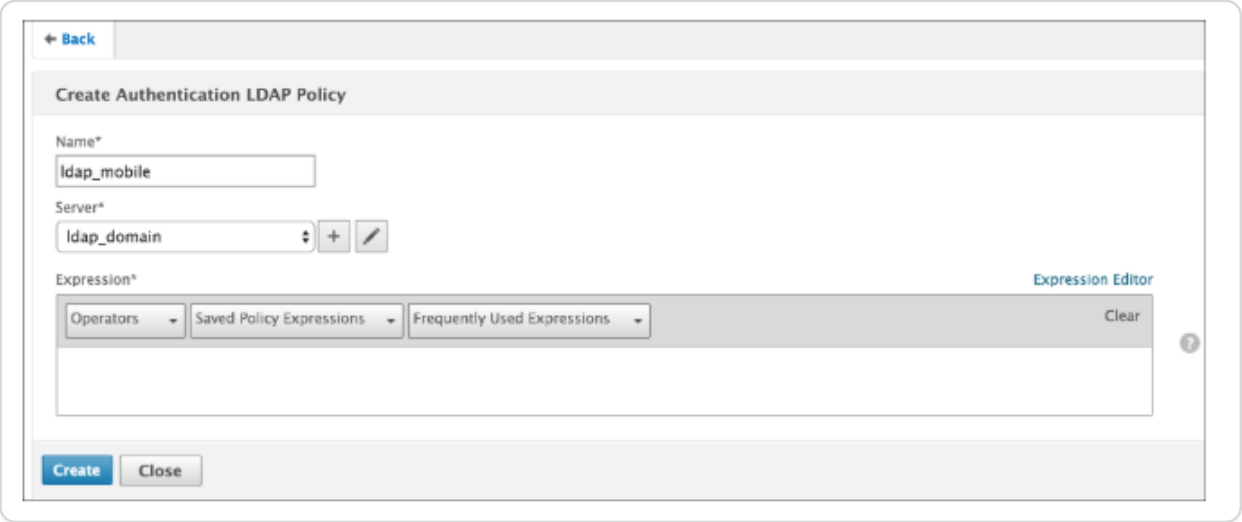
   Para vincular esta directiva solo a dispositivos móviles, utilice la siguiente expresión:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
REQ.HTTP.HEADER User-Agent CONTAINS CitrixReceiver
```

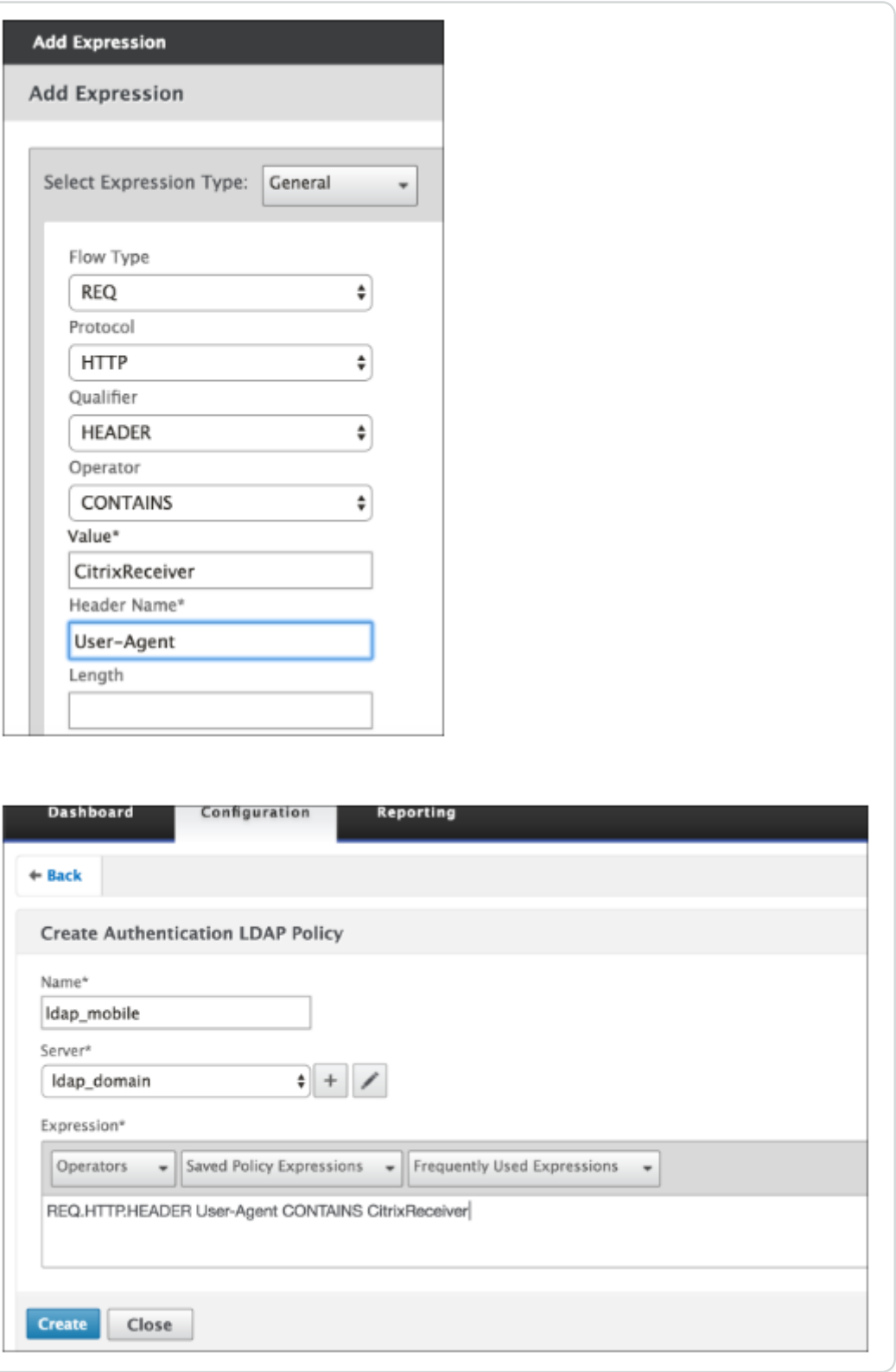
La expresión avanzada correspondiente es:

```
HTTP.REQ.HEADER("User-Agent").CONTAINS("CitrixReceiver")
```




4. Haga clic en **Editor de expresiones** para crear la directiva:

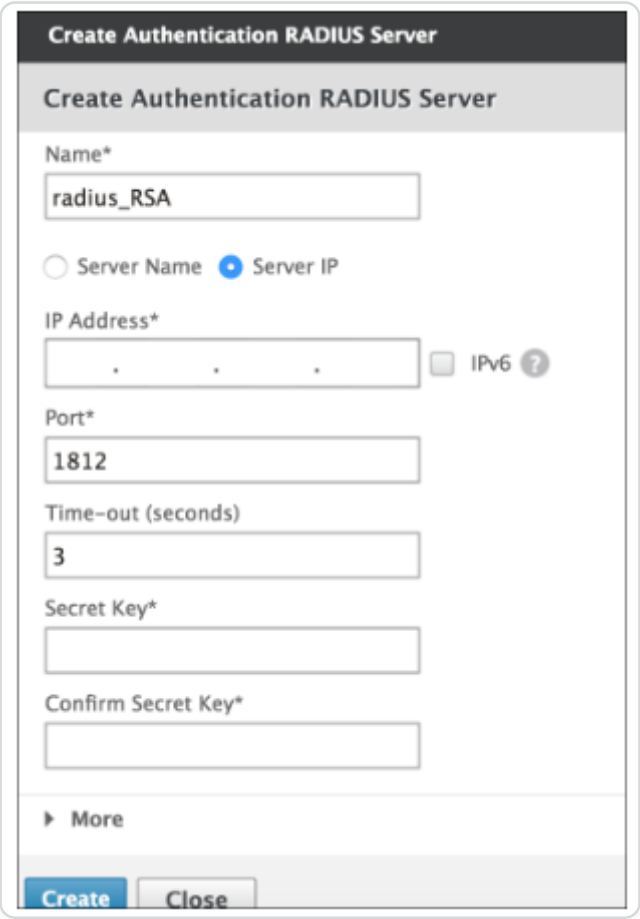
© 1997–2026 Citrix Systems, Inc. All rights reserved.



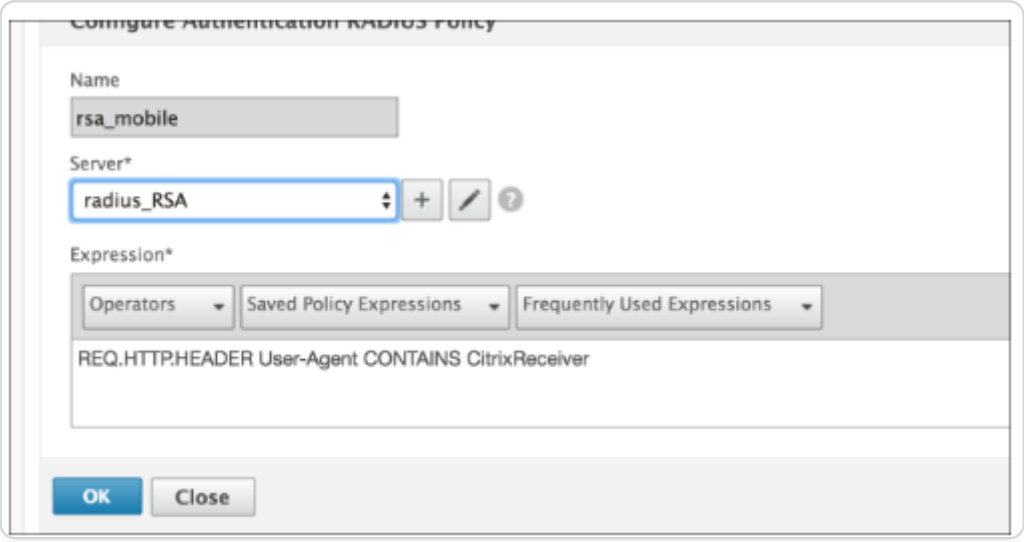

5. Cree una directiva RADIUS y un servidor RADIUS para los dispositivos móviles.

   - Vaya a la opción RADIUS desde **NetScaler Gateway > Directivas > Autenticación > RADIUS**. Haga clic en **Agregar** en la ficha Servidor.
   - Agregue los detalles necesarios. El puerto predeterminado para la autenticación RADIUS es 1812.

© 1997–2026 Citrix Systems, Inc. All rights reserved.




- Para vincular esta directiva solo a dispositivos móviles, utilice la siguiente expresión:



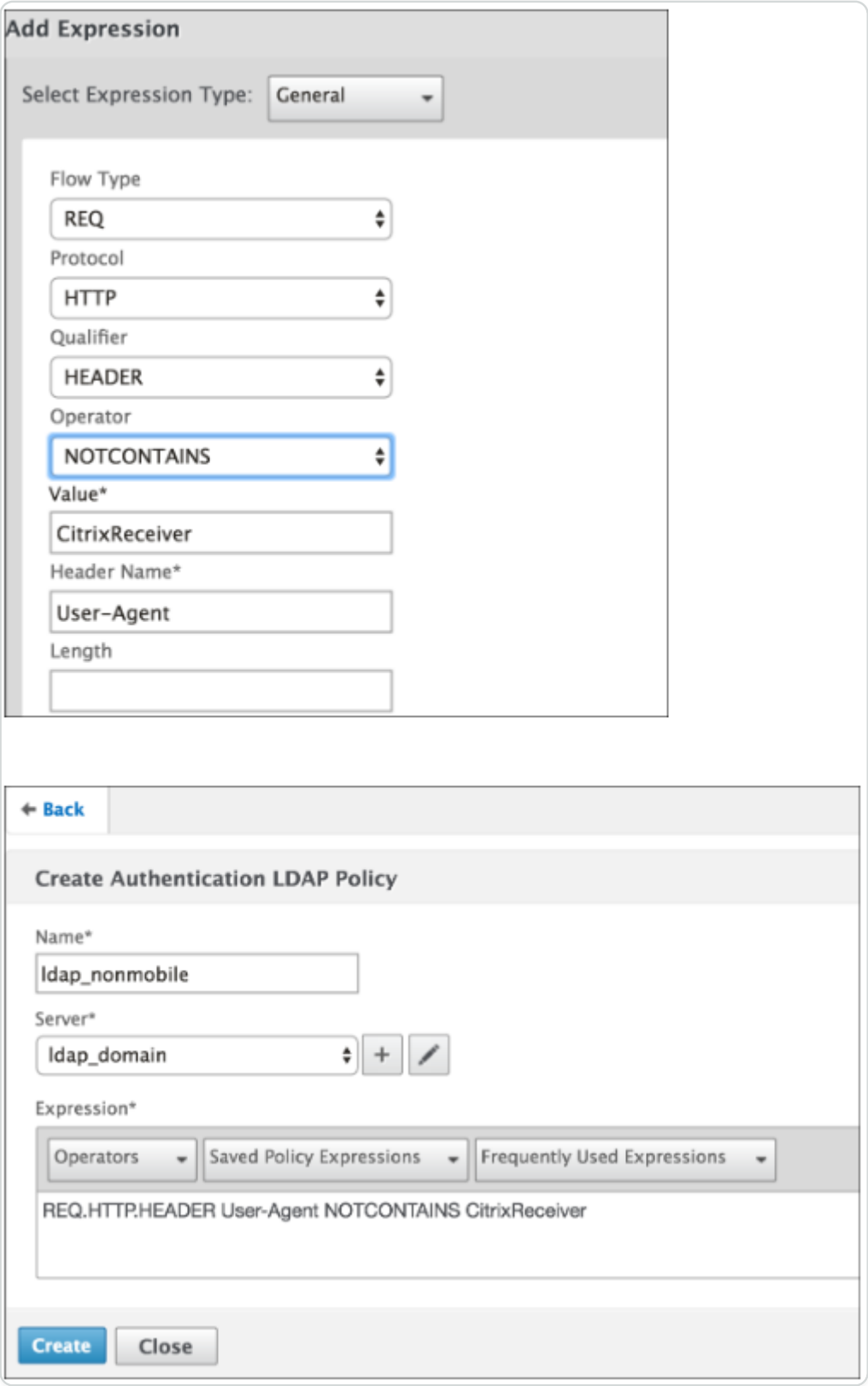

6. Siga el mismo paso para crear una directiva LDAP para dispositivos no móviles. Para vincular esta directiva solo a dispositivos no móviles, utilice la siguiente expresión:

```
REQ.HTTP.HEADER User-Agent NOTCONTAINS CitrixReceiver
```

La expresión avanzada correspondiente es:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
HTTP.REQ.HEADER("User-Agent").CONTAINS("CitrixReceiver").NOT
```



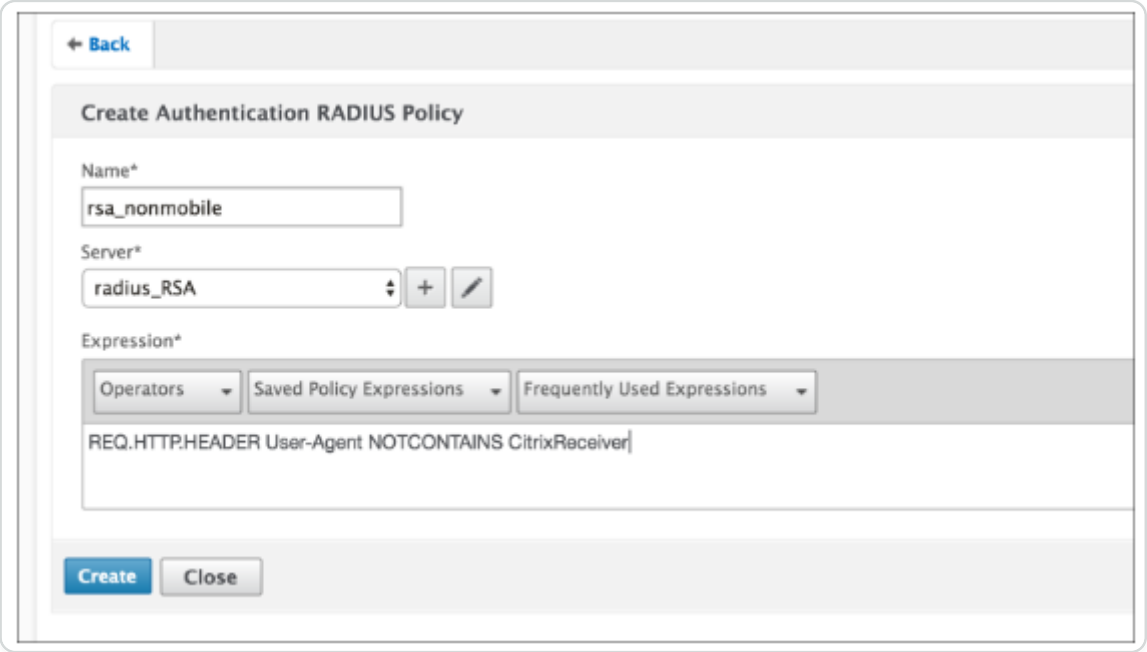

7. Cree una directiva RADIUS para dispositivos no móviles. Para vincular esta directiva solo a dispositivos no móviles, utilice la siguiente expresión:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
REQ.HTTP.HEADER User-Agent NOTCONTAINS CitrixReceiver
```

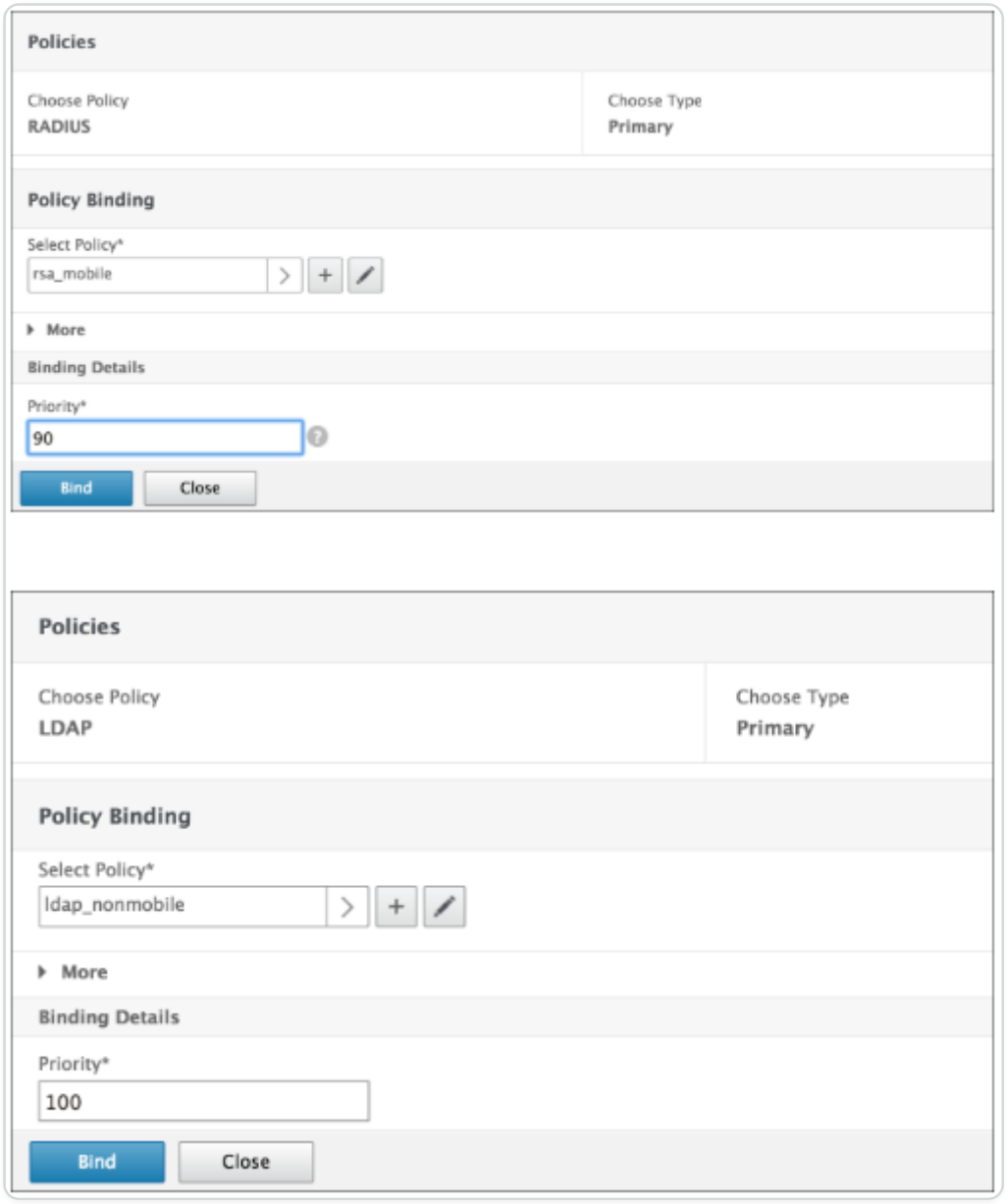
La expresión avanzada correspondiente es:

```
HTTP.REQ.HEADER("User-Agent").CONTAINS("CitrixReceiver").NOT
```

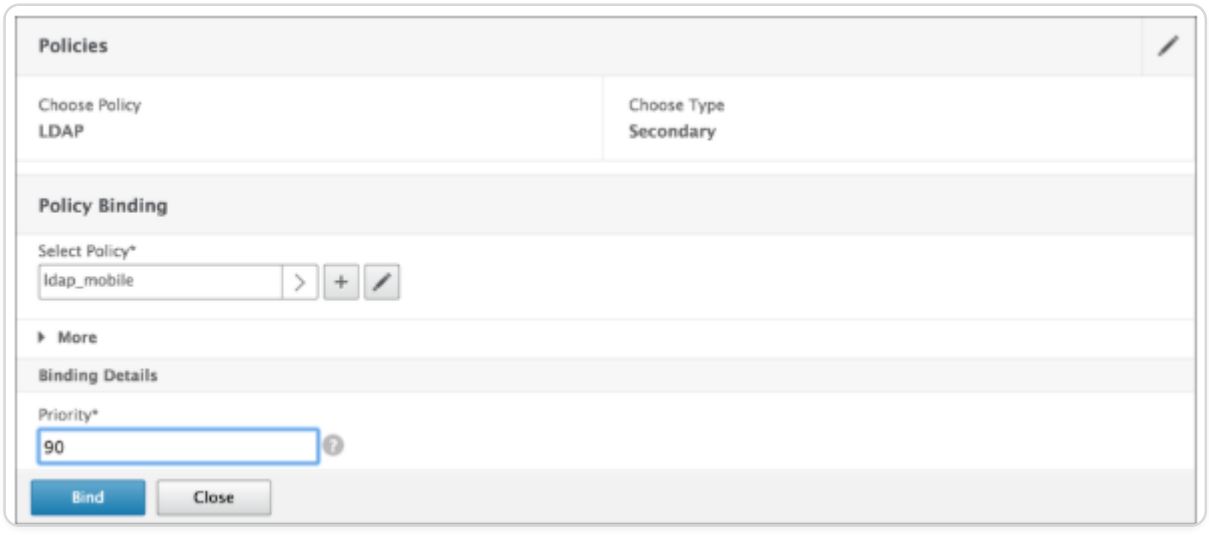



8. Vaya a las propiedades del servidor virtual de NetScaler Gateway y haga clic en la ficha **Autenticación**. En las directivas de autenticación principales, agregue la directiva RSA_Mobile como prioridad máxima y la directiva LDAP_NonMobile como prioridad secundaria:

© 1997–2026 Citrix Systems, Inc. All rights reserved.




9. En las directivas de autenticación secundarias, agregue la directiva LDAP_Mobile como prioridad máxima, seguida de la directiva RSA_NonMobile como prioridad secundaria:

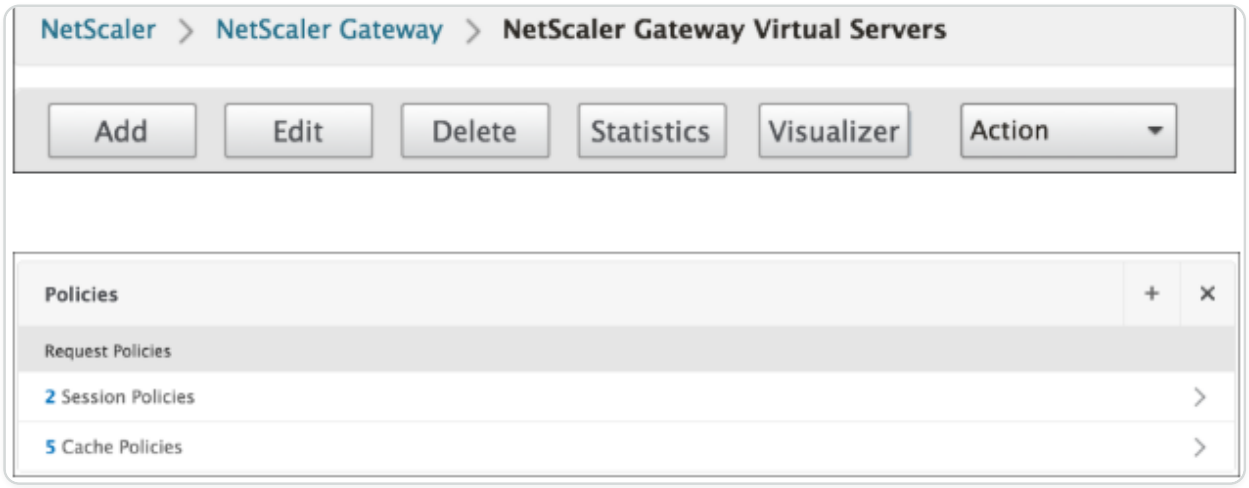



© 1997–2026 Citrix Systems, Inc. All rights reserved.

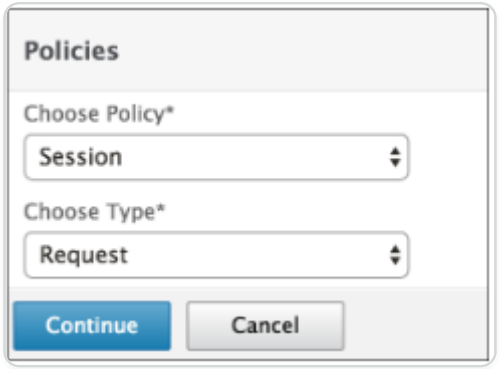
La política de sesión debe tener el Índice de credenciales de inicio de sesión único correcto, es decir, deben ser las credenciales LDAP. Para dispositivos móviles, el **Índice de credenciales** en **Perfil de sesión > Experiencia del cliente** debe establecerse en **Secundario**, que es LDAP.

Por lo tanto, necesita dos políticas de sesión, una para dispositivos móviles y otra para dispositivos no móviles.

- Para dispositivos móviles, la política de sesión y el perfil de sesión aparecen como se muestra en la siguiente captura de pantalla. Para crear una política de sesión, navegue hasta el servidor virtual requerido y haga clic en **Editar**, vaya a la sección de políticas y haga clic en el signo +:

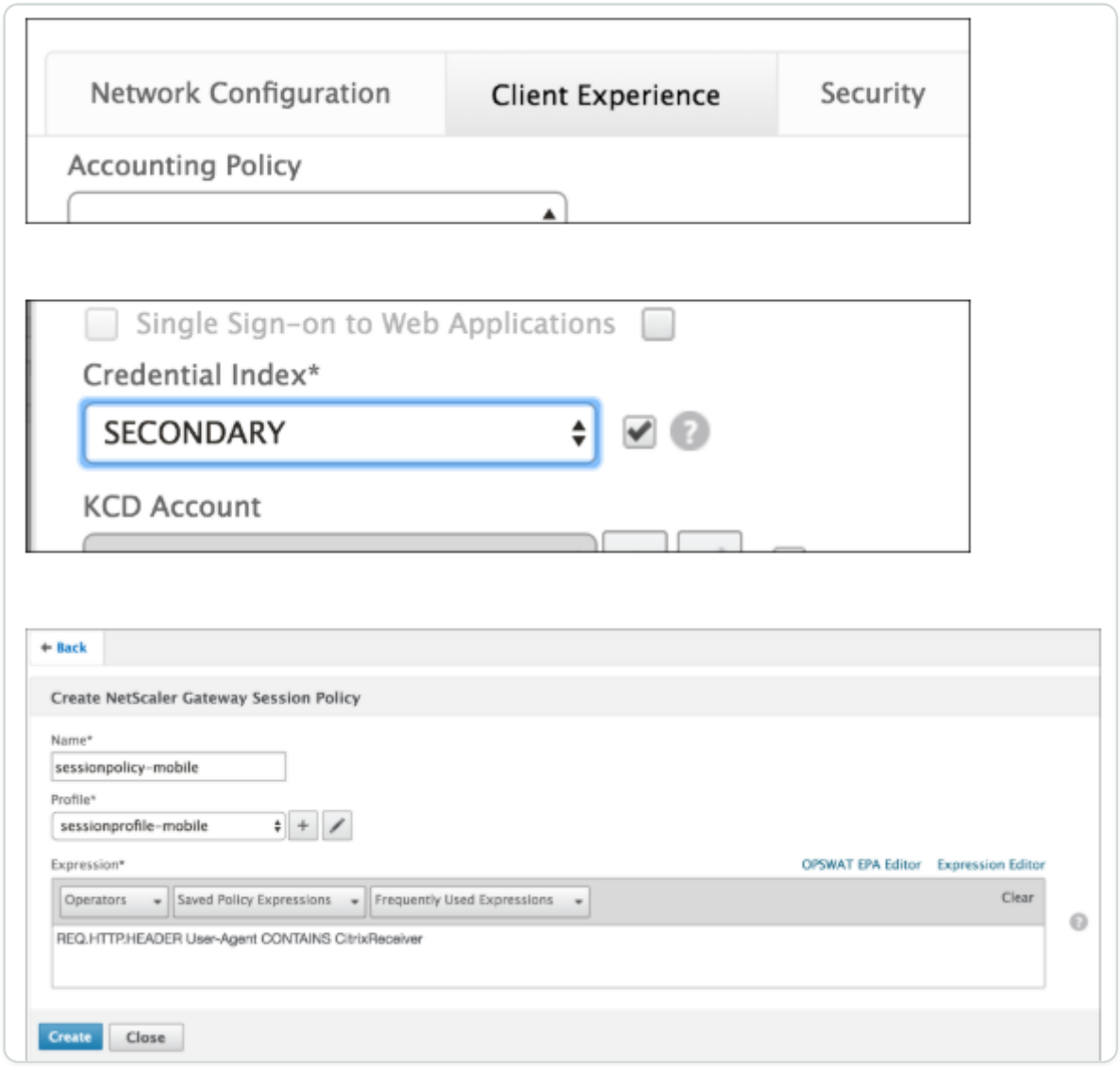



- Elija la opción **Sesión** del menú.




- Introduzca el nombre deseado de la política de sesión y haga clic en + para crear un perfil. Para dispositivos móviles, el **Índice de credenciales** en **Perfil de sesión > Experiencia del cliente** debe establecerse en **Secundario**, que es LDAP.

© 1997–2026 Citrix Systems, Inc. All rights reserved.




- Para dispositivos no móviles, siga los mismos pasos. El **Índice de credenciales** en **Perfil de sesión > Experiencia del cliente** debe establecerse en **Principal**, que es LDAP.

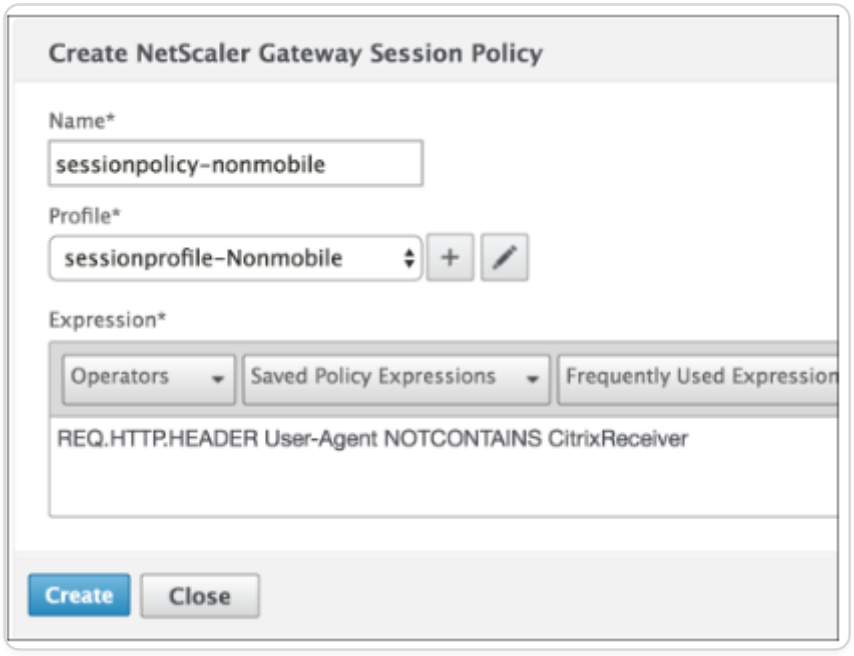
La expresión debe cambiarse a:

```
REQ.HTTP.HEADER User-Agent NOTCONTAINS CitrixReceiver
```

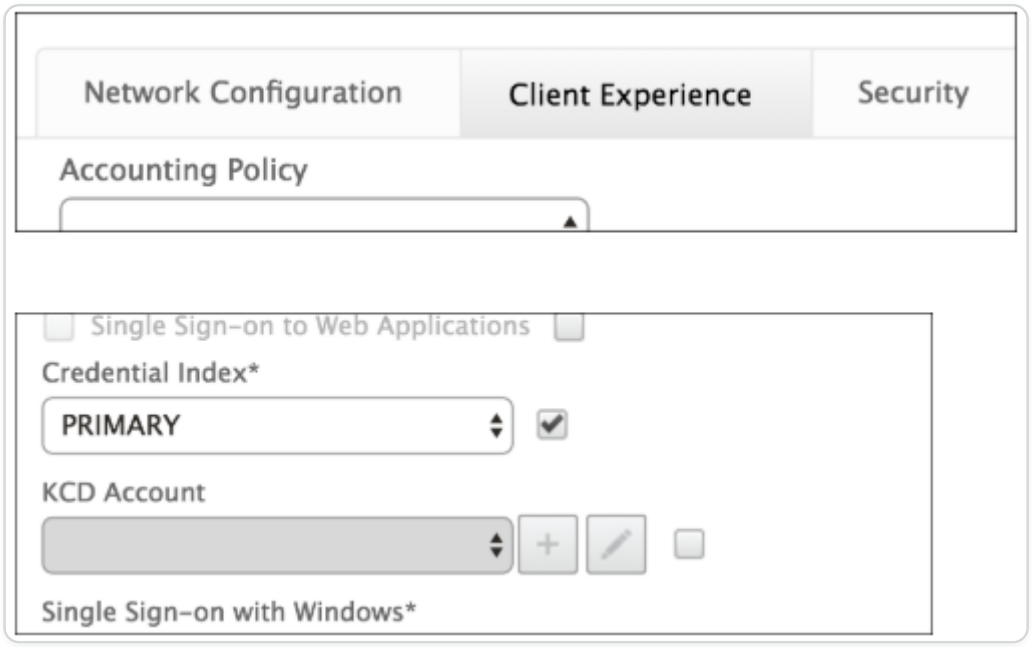
La expresión avanzada correspondiente es:

```
HTTP.REQ.HEADER("User-Agent").CONTAINS("CitrixReceiver").NOT
```

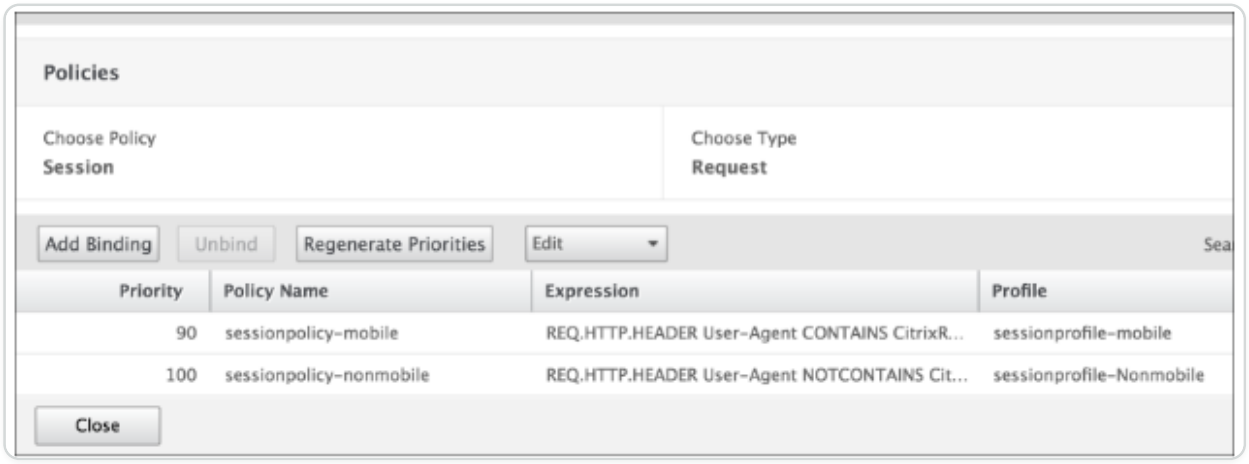
© 1997–2026 Citrix Systems, Inc. All rights reserved.




- Para crear un perfil para usuarios no móviles, haga clic en el signo +.

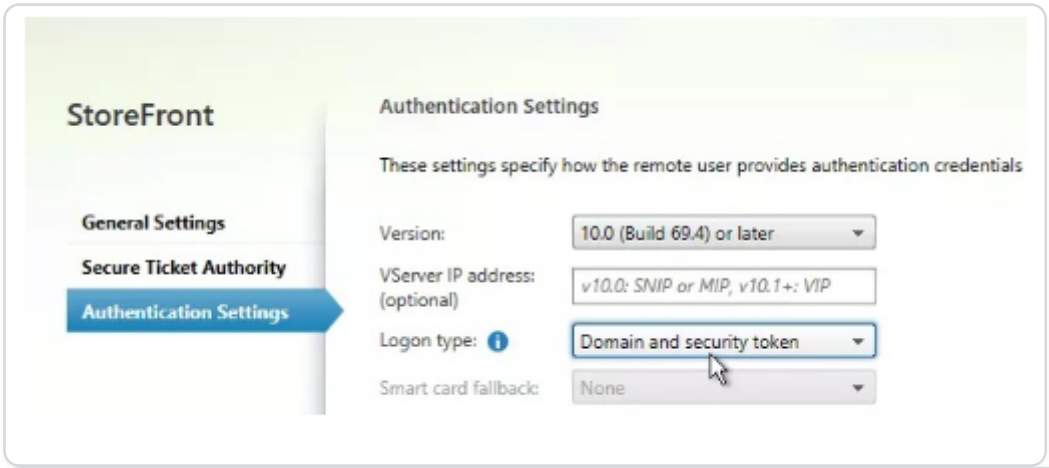


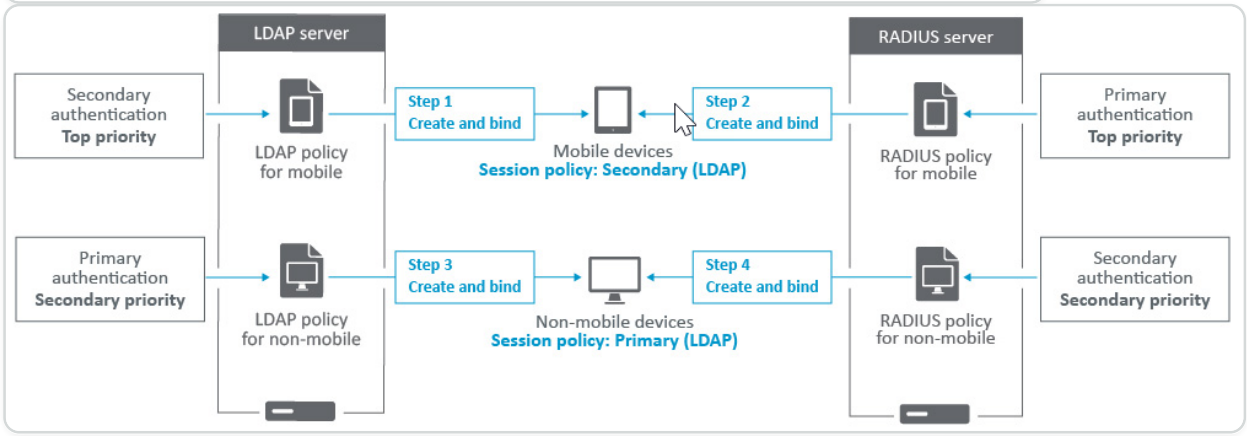

10. La siguiente figura muestra las políticas y perfiles bajo el servidor virtual requerido.




© 1997–2026 Citrix Systems, Inc. All rights reserved.

11. También en StoreFront, en la configuración de NetScaler Gateway, establecido para usar "Logon Type" = "Domain and Security token"




# Restringir el acceso a NetScaler Gateway para miembros de un grupo de Active Directory

NetScaler Gateway admite dos métodos para restringir el acceso de inicio de sesión.

- **Filtro de búsqueda LDAP:** Restringe el acceso de inicio de sesión a NetScaler Gateway solo a los nombres de usuario que coinciden con el filtro de búsqueda LDAP (por ejemplo, la pertenencia a un grupo de Active Directory).
- **Directiva de sesión de NetScaler Gateway:** Restringe el acceso de inicio de sesión a NetScaler Gateway solo a los usuarios de los grupos incluidos en la directiva o el perfil de sesión. Este método admite varios grupos de Active Directory.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

# Método de filtro de búsqueda LDAP

## Información general

Cuando un usuario introduce las credenciales en la página de inicio de sesión del servidor virtual de NetScaler Gateway y pulsa ENTRAR, el dispositivo busca primero el nombre de usuario en Active Directory (LDAP). Si no se define un filtro de búsqueda LDAP en la directiva o el servidor LDAP, el dispositivo busca una coincidencia en todos los nombres de usuario de Active Directory. Una vez que se encuentra una coincidencia, el dispositivo extrae el nombre distintivo (DN) completo del usuario y utiliza el DN y la contraseña del usuario para autenticarse en Active Directory.

Si se define un filtro de búsqueda LDAP, solo se buscarán los nombres de usuario que coincidan con el filtro de búsqueda LDAP. Por ejemplo, si el filtro de búsqueda LDAP está configurado para buscar solo miembros de un grupo de Active Directory, el nombre de usuario introducido por el usuario debe coincidir con los miembros del grupo.

## Requisitos previos

El servidor virtual de NetScaler Gateway debe estar configurado para la autenticación LDAP.

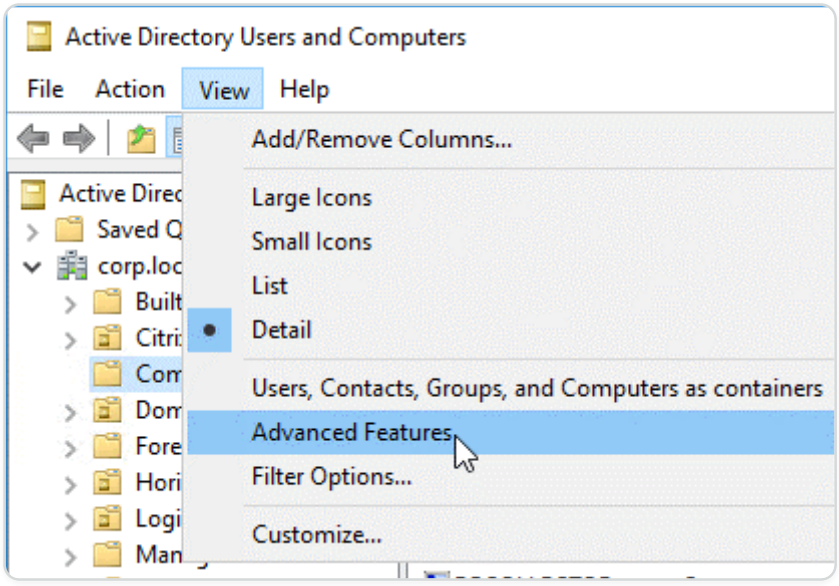
# Pasos para configurar un filtro de búsqueda LDAP para miembros de un grupo de Active Directory

1. Determine el grupo de Active Directory que tiene permiso de acceso y obtenga su nombre distintivo completo.

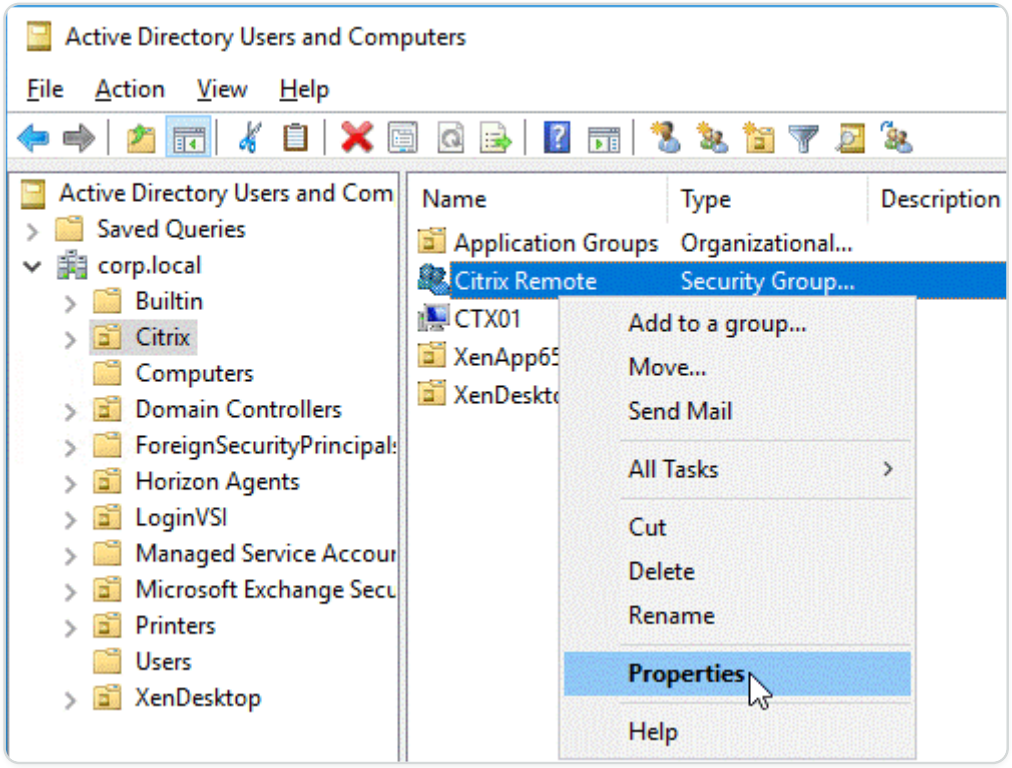
   Una forma sencilla de obtener el nombre distintivo completo del grupo es a través de Usuarios y equipos de Active Directory.

2. En Usuarios y equipos de Active Directory, en el menú **Ver**, habilite **Características avanzadas**.

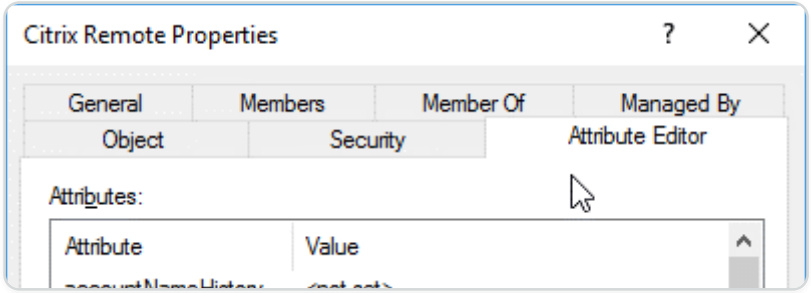
© 1997–2026 Citrix Systems, Inc. All rights reserved.




3. Navegue por el árbol hasta el objeto de grupo, haga clic con el botón derecho y, a continuación, haga clic en **Propiedades**. **Nota:** No puede usar **Buscar**. En su lugar, debe navegar por el árbol para encontrar el objeto.



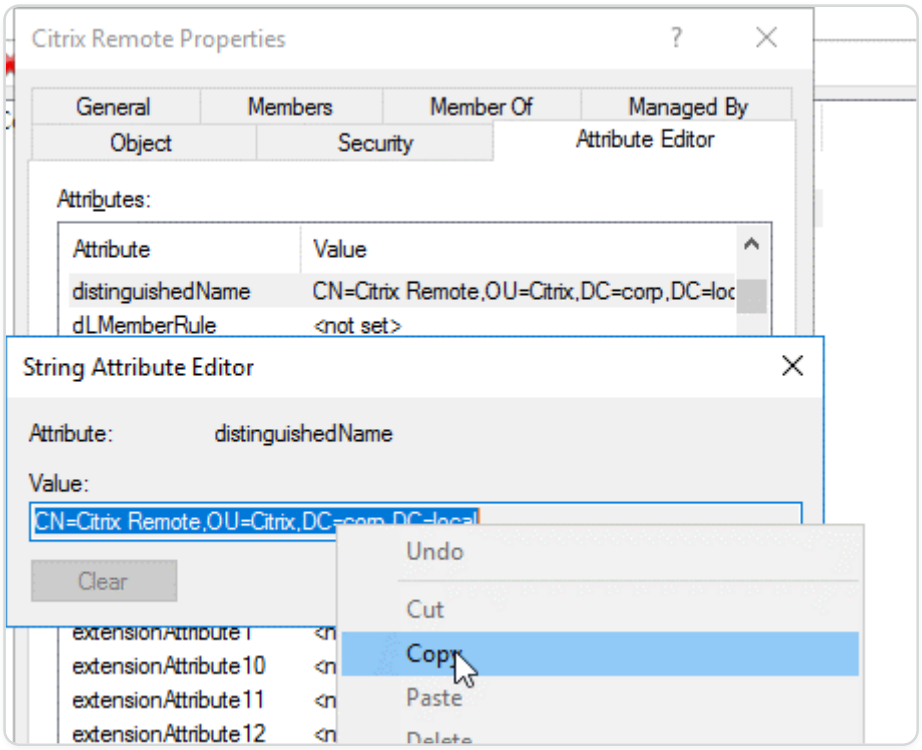

4. A la derecha, cambie a la ficha **Editor de atributos**.




© 1997–2026 Citrix Systems, Inc. All rights reserved.

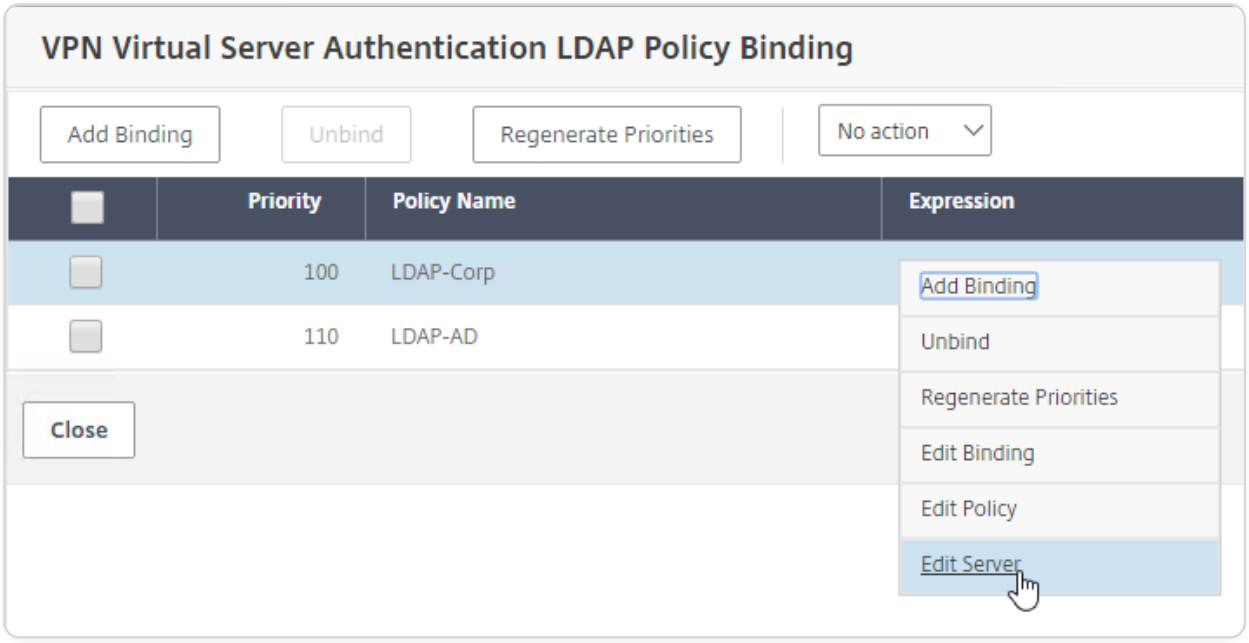
Esta ficha solo es visible si las **Funciones avanzadas** están habilitadas y si no ha utilizado la función **Buscar**.

5. Desplácese hacia abajo hasta **distinguishedName**, haga doble clic en él y, a continuación, cópielo en el portapapeles.

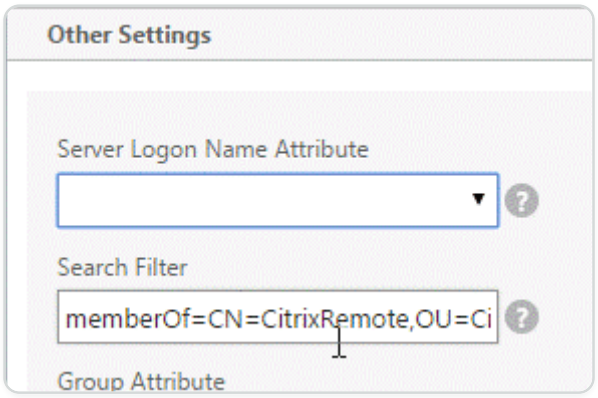



6. En la GUI de NetScaler Gateway, vaya a **NetScaler Gateway > Servidores virtuales**.
7. Seleccione un servidor virtual de NetScaler Gateway existente y haga clic en **Editar**.
8. En la sección Autenticación básica, haga clic en **Directivas LDAP**.
9. Haga clic con el botón derecho en una directiva LDAP existente y haga clic en **Editar servidor**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.




10. En la sección **Otros parámetros**, en el campo **Filtro de búsqueda**, escriba **memberOf=** y, a continuación, pegue el nombre distintivo del grupo de Active Directory después del signo igual (=).




Un ejemplo de filtro de búsqueda es el siguiente: memberOf=CN=Citrix® Remote,OU=Citrix,DC=corp,DC=local **Nota:** De forma predeterminada, NetScaler® solo busca nombres de usuario que sean miembros directos del grupo de Active Directory. Si desea buscar grupos anidados, agregue el OID de Microsoft:: al filtro de búsqueda LDAP. El OID se inserta entre memberOf y =.

**Ejemplo:** memberOf:1.2.840.113556.1.4.1941:=CN=Citrix Remote,OU=Citrix,DC=corp,DC=local

11. Haga clic en **Aceptar**.

## Método de directiva de sesión de NetScaler Gateway

NetScaler Gateway permite a los administradores especificar los usuarios de qué grupos de Active Directory tienen permiso para iniciar sesión a través de una directiva o perfil de sesión. Para

© 1997–2026 Citrix Systems, Inc. All rights reserved.

obtener información sobre cómo crear y añadir usuarios al grupo de Active Directory, consulte Para crear grupos en NetScaler Gateway.

**Mediante la CLI:**

Ejecute el siguiente comando para restringir el acceso a NetScaler Gateway a los usuarios de un grupo determinado:

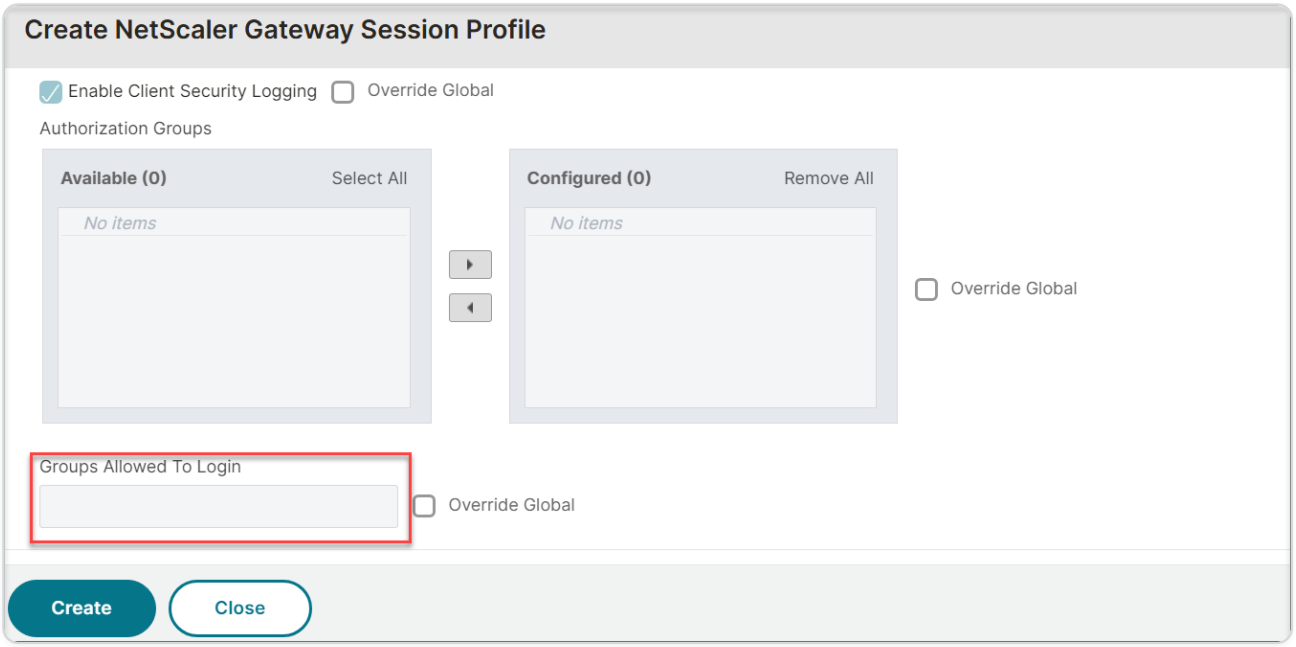
```
set vpn sessionAction sessionActionName -allowedLoginGroups groupName
```

**Mediante la GUI:**

1. Vaya a **NetScaler Gateway** > **Directivas** > **Sesión**.
2. En el panel de detalles, haga clic en **Agregar**.
3. En **Nombre**, escriba un nombre para la directiva.
4. Junto a **Perfil**, haga clic en **Agregar**.
5. En **Nombre**, escriba un nombre para el perfil.
6. Haga clic en la ficha **Seguridad** y seleccione **Configuración avanzada**.
7. Junto a **Grupos permitidos para iniciar sesión**, seleccione **Anular global** y, a continuación, introduzca los grupos de **Active Directory** a los que se les permitirá iniciar sesión en NetScaler Gateway.
8. Haga clic en **Crear**.

Después de crear y cerrar el perfil de sesión, cree la expresión para la directiva de sesión en el cuadro de diálogo **Crear directiva de sesión de NetScaler Gateway**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.




# Soporte OTP nativo para autenticación

NetScaler Gateway es compatible con contraseñas de un solo uso (OTP) sin necesidad de utilizar un servidor de terceros. Una contraseña de un solo uso es una opción muy segura para autenticarse en servidores seguros, ya que el número o código de acceso generado es aleatorio. Anteriormente, empresas especializadas, como RSA, ofrecían las OTP con dispositivos específicos que generaban números aleatorios. Este sistema debe estar en comunicación constante con el cliente para generar un número esperado por el servidor.

Además de reducir los gastos de capital y operativos, esta función mejora el control del administrador al mantener toda la configuración en el dispositivo NetScaler.

**NOTA:**

Dado que ya no se necesitan servidores de terceros, el administrador de NetScaler debe configurar una interfaz para administrar y validar los dispositivos de los usuarios.

El usuario debe estar registrado en un servidor virtual de NetScaler Gateway para utilizar la solución OTP. El registro solo es necesario una vez por dispositivo único y se puede restringir a determinados entornos. La configuración y validación de un usuario registrado es similar a la configuración de una política de autenticación adicional.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

## Ventajas del soporte OTP nativo

- Reduce los costes operativos al eliminar la necesidad de tener una infraestructura adicional en un servidor de autenticación, además del Active Directory.
- Consolida la configuración solo en el dispositivo NetScaler, lo que ofrece un gran control a los administradores.
- Elimina la dependencia del cliente de un servidor de autenticación adicional para generar un número esperado por los clientes.

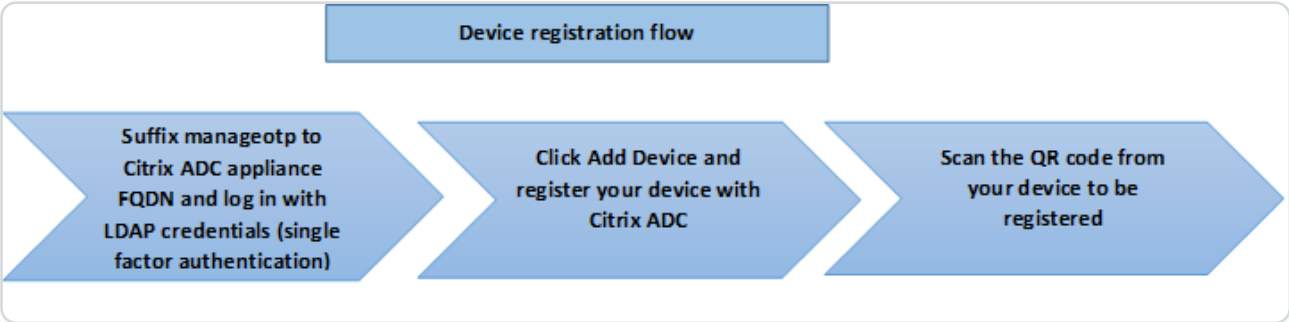
## Flujo de trabajo de OTP nativo

La solución OTP nativa es un proceso doble y el flujo de trabajo se clasifica de la siguiente manera:

- Registro de dispositivos
- Inicio de sesión del usuario final

**Importante:** Puede omitir el proceso de registro si utiliza soluciones de terceros o administra otros dispositivos además del dispositivo NetScaler. La cadena final que agregue debe estar en el formato especificado por NetScaler.

La siguiente figura muestra el flujo de registro de dispositivos para registrar un nuevo dispositivo para recibir OTP.

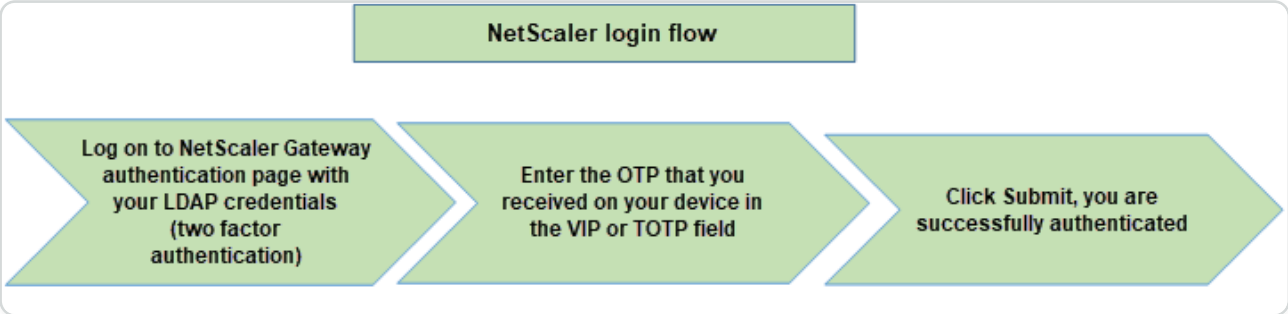



**NOTA:**

El registro del dispositivo se puede realizar utilizando cualquier número de factores. El factor único (como se especifica en la figura anterior) se utiliza como ejemplo para explicar el proceso de registro del dispositivo.

La siguiente figura muestra la verificación de OTP a través del dispositivo registrado.

© 1997–2026 Citrix Systems, Inc. All rights reserved.




## Requisitos previos

Para utilizar la función OTP nativa, asegúrese de que se cumplen los siguientes requisitos previos.

- La versión de lanzamiento de la función de NetScaler es 12.0 compilación 51.24 y posteriores.
- La licencia de edición Advanced o Premium está instalada en NetScaler Gateway.
- NetScaler Gateway está configurado con una IP de administración y la consola de administración es accesible tanto mediante un navegador como mediante la línea de comandos.
- NetScaler está configurado con un servidor virtual de autenticación, autorización y auditoría para autenticar a los usuarios.
- El dispositivo NetScaler está configurado con Unified Gateway y el perfil de autenticación, autorización y auditoría está asignado al servidor virtual de Gateway.
- La solución OTP nativa está restringida al flujo de autenticación nFactor. Se requieren políticas avanzadas para configurar la solución. Para obtener más detalles, consulte el artículo CTX222713.

Asegúrese también de lo siguiente para Active Directory:

- Una longitud mínima de atributo de 256 caracteres.
- El tipo de atributo debe ser 'DirectoryString', como UserParameters. Estos atributos pueden contener valores de cadena.
- El tipo de cadena de atributo debe ser Unicode si el nombre del dispositivo contiene caracteres no ingleses.
- El administrador de NetScaler LDAP debe tener acceso de escritura al atributo AD seleccionado.
- El dispositivo NetScaler y la máquina cliente deben estar sincronizados con un servidor de hora de red común.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

## Configurar OTP nativo mediante la GUI

El registro OTP nativo no es solo una autenticación de un solo factor. Las siguientes secciones le ayudarán a configurar la autenticación de un solo factor y de segundo factor.

### Crear esquema de inicio de sesión para el primer factor

1. Vaya a **Security AAA > Application Traffic > Login Schema**.
2. Vaya a **Profiles** y haga clic en **Add**.
3. En la página **Create Authentication Login Schema**, introduzca *lschema_single_auth_manage_otp* en el campo **Name** y haga clic en **Edit** junto a **noschema**.
4. Haga clic en la carpeta **LoginSchema**.
5. Desplácese hacia abajo para seleccionar **SingleAuth.xml** y haga clic en **Select**.
6. Haga clic en **Create**.
7. Haga clic en **Policies** y haga clic en **Add**.
8. En la pantalla **Create Authentication Login Schema Policy**, introduzca los siguientes valores.

   **Nombre:** `lpol_single_auth_manage_otp_by_url` **Perfil:** seleccione l`pol_single_auth_manage_otp_by_url` de la lista. **Regla:** `HTTP.REQ.COOKIE.VALUE("NSC_TASS").EQ("` manageotp `")`

### Configurar el servidor virtual de autenticación, autorización y auditoría

1. Vaya a **Security > AAA – Application Traffic > Authentication Virtual Servers**. Haga clic para editar el servidor virtual existente.
2. Haga clic en el icono **+** junto a **Login Schemas** en **Advanced Settings** en el panel derecho.
3. Seleccione **No Login Schema.**
4. Haga clic en la flecha y seleccione la política **lpol_single_auth_manage_otp_by_url**.
5. Seleccione la política **lpol_single_auth_manage_otp_by_url** y haga clic en **Select**.
6. Haga clic en **Bind**.
7. Desplácese hacia arriba y seleccione **1 Authentication Policy** en **Advanced Authentication Policy**.
8. Haga clic con el botón derecho en la **nFactor Policy** y seleccione **Edit Binding**.
9. Haga clic en el icono **+** presente en **Select Next Factor,** cree un Next Factor y haga clic en **Bind**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

10. En la pantalla **Create Authentication** `PolicyLabel`, introduzca lo siguiente y haga clic en **Continue**:

    **Nombre**: manage_otp_flow_label

    **Esquema de inicio de sesión**: Lschema_Int

11. En la pantalla **Authentication PolicyLabel**, haga clic en el icono **+** para crear una política.
12. En la pantalla **Create Authentication Policy**, introduzca lo siguiente:

    **Nombre**: auth_pol_ldap_otp_action

13. Seleccione el tipo de acción mediante la lista **Action Type**.
14. En el campo **Action**, haga clic en el icono **+** para crear una acción.
15. En la página **Create Authentication LDAP server**, seleccione el botón de opción **Server IP**, desmarque la casilla de verificación junto a **Authentication**, introduzca los siguientes valores y seleccione **Test Connection**.

    **Nombre**: ldap_otp_action

    **Dirección IP**: 192.168.10.11

    **DN base**: DC=training, DC=lab

    **Administrador**: Administrator@training.lab

    **Contraseña**: `xxxxx`

16. Desplácese hasta la sección **Other Settings**. Utilice el menú desplegable para seleccionar las siguientes opciones. **Server Logon Name Attribute** como **New** y escriba **userprincipalname**.
17. Utilice el menú desplegable para seleccionar **SSO Name Attribute** como **New** y escriba **userprincipalname**.
18. Introduzca «UserParameters» en el campo **OTP Secret** y haga clic en **More**.
19. Introduzca los siguientes atributos.

    **Atributo 1** = mail **Atributo 2** = objectGUID **Atributo 3** = immutableID

20. Haga clic en **Aceptar**.
21. En la página **Crear directiva de autenticación**, establezca la expresión en **true** y haga clic en **Crear**.
22. En la página **Crear etiqueta de directiva de autenticación**, haga clic en **Enlazar** y, a continuación, en **Listo**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

23. En la página **Enlace de directivas**, haga clic en **Enlazar**.
24. En la página **Directiva de autenticación**, haga clic en **Cerrar** y, a continuación, en **Listo**.

**NOTA:**

El servidor virtual de autenticación debe estar enlazado al tema del portal RFWebUI. Enlace un certificado de servidor al servidor. La IP del servidor '1.2.3.5' debe tener un FQDN correspondiente, es decir, otpauth.server.com, para su uso posterior.

### Crear esquema de inicio de sesión para OTP de segundo factor

1. Vaya a **Seguridad > Tráfico de aplicaciones AAA > Servidores virtuales**. Seleccione el servidor virtual que desea editar.
2. Desplácese hacia abajo y seleccione **1 Esquema de inicio de sesión**.
3. Haga clic en **Agregar enlace**.
4. En la sección **Enlace de directivas**, haga clic en el icono **+** para agregar una directiva.
5. En la página **Crear directiva de esquema de inicio de sesión de autenticación**, introduzca el nombre como OTP y haga clic en el icono **+** para crear un perfil.
6. En la página **Crear esquema de inicio de sesión de autenticación**, introduzca el nombre como OTP y haga clic en el icono situado junto a **noschema**.
7. Haga clic en la carpeta **LoginSchema**, seleccione **DualAuthManageOTP.xml** y, a continuación, haga clic en **Seleccionar**.
8. Haga clic en **Crear**.
9. En la sección **Regla**, introduzca **True**. Haga clic en **Crear**.
10. Haga clic en **Enlazar**.
11. Observe los dos factores de autenticación. Haga clic en **Cerrar** y, a continuación, en **Listo**.

### Configurar la política de conmutación de contenido para gestionar OTP

Las siguientes configuraciones son necesarias si utiliza Unified Gateway.

1. Vaya a **Administración del tráfico > Conmutación de contenido > Directivas**. Seleccione la política de conmutación de contenido, haga clic con el botón derecho y seleccione **Editar**.
2. Edite la expresión para evaluar la siguiente instrucción OR y haga clic en **Aceptar**:

is_vpn_url||HTTP.REQ.URL.CONTAINS("`manageotp`")

© 1997–2026 Citrix Systems, Inc. All rights reserved.

## Configurar OTP nativo mediante la CLI

Debe tener la siguiente información para configurar la página de administración de dispositivos OTP:

- IP asignada al servidor virtual de autenticación
- FQDN correspondiente a la IP asignada
- Certificado de servidor para el servidor virtual de autenticación

**NOTA:**

La OTP nativa es una solución únicamente basada en web.

### Para configurar la página de registro y administración de dispositivos OTP

Crear servidor virtual de autenticación

```
add authentication vserver authvs SSL 1.2.3.5 443

bind authentication vserver authvs -portaltheme RFWebUI

bind ssl vserver authvs -certkeyname otpauthcert
```

**NOTA:**

El servidor virtual de autenticación debe estar vinculado al tema del portal RFWebUI. Vincule un certificado de servidor al servidor. La IP del servidor ‘1.2.3.5’ debe tener un FQDN correspondiente, es decir, otpauth.server.com, para su uso posterior.

### Para crear una acción de inicio de sesión LDAP

```
add authentication ldapAction <LDAP ACTION NAME> -serverIP <SERVER IP> -
 serverPort <SERVER PORT> -ldapBase <BASE> -ldapBindDn <AD USER>
-ldapBindDnPassword <PASSWO> -ldapLoginName <USER FORMAT>
```

**Ejemplo**:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
add authentication ldapAction ldap_logon_action -serverIP 1.2.3.4
-serverPort 636 -ldapBase "OU=Users,DC=server,DC=com" -ldapBindDn
administrator@ctxnsdev.com -ldapBindDnPassword PASSWORD -ldapLoginName
userprincipalname
```

### Para agregar una directiva de autenticación para el inicio de sesión LDAP

```
add authentication Policy auth_pol_ldap_logon -rule true -action
ldap_logon_action
```

### Para presentar la interfaz de usuario a través de LoginSchema

Mostrar el campo de nombre de usuario y el campo de contraseña a los usuarios al iniciar sesión

```
add authentication loginSchema lschema_single_auth_manage_otp
-authenticationSchema "/nsconfig/loginschema/LoginSchema/
SingleAuthManageOTP.xml"
```

## Mostrar la página de registro y administración de dispositivos

Citrix® recomienda dos formas de mostrar la pantalla de registro y administración de dispositivos: URL o nombre de host.

- **Uso de URL**

  Cuando la URL contiene ‘/manageotp’

  - `add authentication loginSchemaPolicy lpol_single_auth_manage_otp_by_url -rule 'http.req.cookie.value("NSC_TASS").contains("manageotp")' -action lschema_single_auth_manage_otp`
  - `bind authentication vserver authvs -policy lpol_single_auth_manage_otp_by_url -priority 10 -gotoPriorityExpression END`

- **Uso del nombre de host**

  Cuando el nombre de host es 'alt.server.com'

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- `add authentication loginSchemaPolicy lpol_single_auth_manage_otp_by_host -rule 'http.req.header("host").eq("alt.server.com")' -action lschema_single_auth_manage_otp`
- `bind authentication vserver authvs -policy lpol_single_auth_manage_otp_by_host -priority 20 -gotoPriorityExpression END`

### Para configurar la página de inicio de sesión de usuario mediante la CLI

Debe tener la siguiente información para configurar la página de inicio de sesión de usuario:

- IP para un servidor virtual de equilibrio de carga
- FQDN correspondiente para el servidor virtual de equilibrio de carga
- Certificado de servidor para el servidor virtual de equilibrio de carga

```
bind ssl vserver lbvs_https -certkeyname lbvs_server_cert
```

El servicio de back-end en el equilibrio de carga se representa de la siguiente manera:

```
add service iis_backendsso_server_com 1.2.3.210 HTTP 80

bind lb vserver lbvs_https iis_backendsso_server_com
```

### Para crear una acción de validación de contraseña de OTP

```
add authentication ldapAction <LDAP ACTION NAME> -serverIP <SERVER IP>
-serverPort <SERVER PORT> -ldapBase <BASE> -ldapBindDn <AD USER>
-ldapBindDnPassword <PASSWORD> -ldapLoginName <USER FORMAT>
-authentication DISABLED -OTPSecret <LDAP ATTRIBUTE>
```

### Ejemplo:

```
add authentication ldapAction ldap_otp_action -serverIP 1.2.3.4
-serverPort 636 -ldapBase "OU=Users,DC=server,DC=com" -ldapBindDn
administrator@ctxnsdev.com -ldapBindDnPassword PASSWORD -ldapLoginName
userprincipalname -authentication DISABLED -OTPSecret userParameters
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**IMPORTANTE:**

La diferencia entre el inicio de sesión LDAP y la acción OTP es la necesidad de deshabilitar la autenticación e introducir un nuevo parámetro `OTPSecret`. No utilice el valor del atributo AD.

**Para agregar una política de autenticación para la validación de la contraseña de un solo uso (OTP)**

```
add authentication Policy auth_pol_otp_validation -rule true -action
ldap_otp_action
```

**Para presentar la autenticación de dos factores a través de LoginSchema**

Agregue la interfaz de usuario para la autenticación de dos factores.

```
add authentication loginSchema lscheme_dual_factor -authenticationSchema
"/nsconfig/loginschema/LoginSchema/DualAuth.xml"

add authentication loginSchemaPolicy lpol_dual_factor -rule true -action
lscheme_dual_factor
```

**Para crear un factor de validación de contraseña a través de la etiqueta de política**

Cree una etiqueta de política de flujo de OTP administrada para el siguiente factor (el primer factor es el inicio de sesión LDAP)

```
add authentication loginSchema lschema_noschema -authenticationSchema
noschema

add authentication policylabel manage_otp_flow_label -loginSchema
lschema_noschema
```

**Para vincular la política OTP a la etiqueta de política**

```
bind authentication policylabel manage_otp_flow_label -policyName
 auth_pol_otp_validation -priority 10 -gotoPriorityExpression NEXT
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

### Vincular el flujo de UI

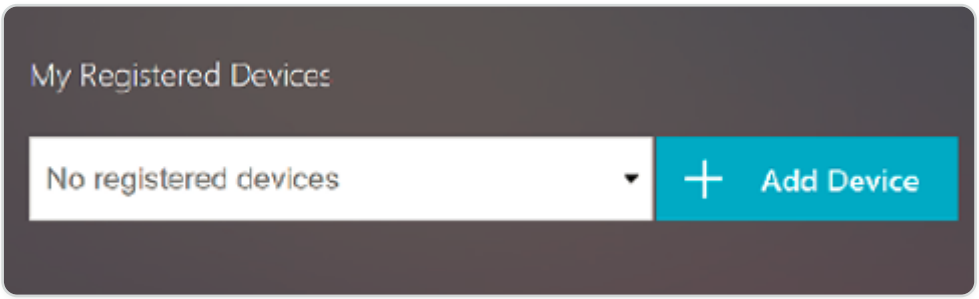
Vincule el inicio de sesión LDAP seguido de la validación OTP con el servidor virtual de autenticación.

```
bind authentication vserver authvs -policy auth_pol_ldap_logon -priority
10 -nextFactor  manage_otp_flow_label -gotoPriorityExpression NEXT

bind authentication vserver authvs -policy lpol_dual_factor -priority 30
-gotoPriorityExpression END
```

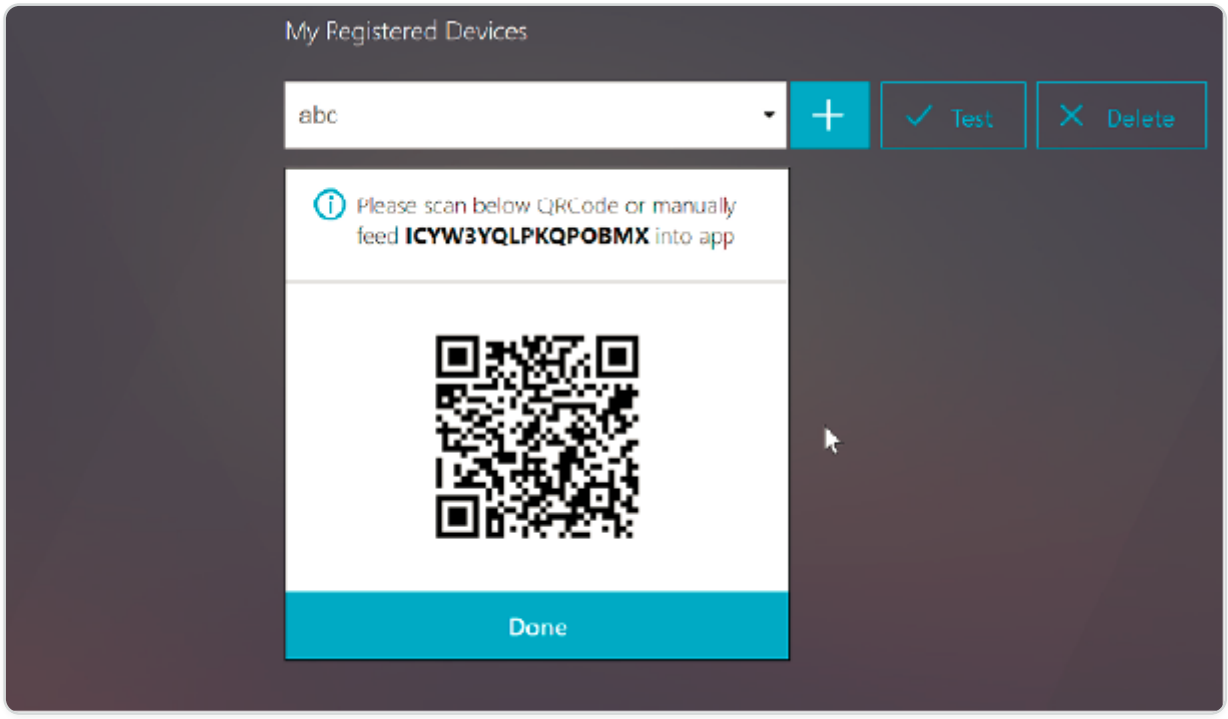
## Registre su dispositivo con NetScaler

1. Navegue a su FQDN de NetScaler (primera IP pública), con un sufijo /manageotp. Por ejemplo, `<https://otpauth.server.com/manageotp>` Inicie sesión con las credenciales de usuario.
2. Haga clic en el icono **+** para agregar un dispositivo.




3. Introduzca un nombre de dispositivo y pulse **Ir**. Aparecerá un código de barras en la pantalla.
4. Haga clic en **Iniciar configuración** y, a continuación, haga clic en **Escanear código de barras**.
5. Pase la cámara del dispositivo sobre el código QR. Opcionalmente, puede introducir el código.

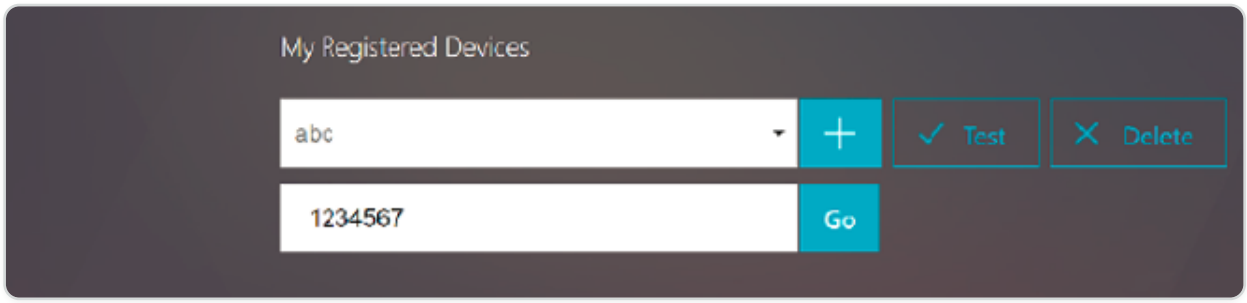
© 1997–2026 Citrix Systems, Inc. All rights reserved.




**NOTA:**

El código QR mostrado es válido durante 3 minutos.

6. Tras un escaneo correcto, se le presenta un código de 6 dígitos sensible al tiempo que se puede utilizar para iniciar sesión.

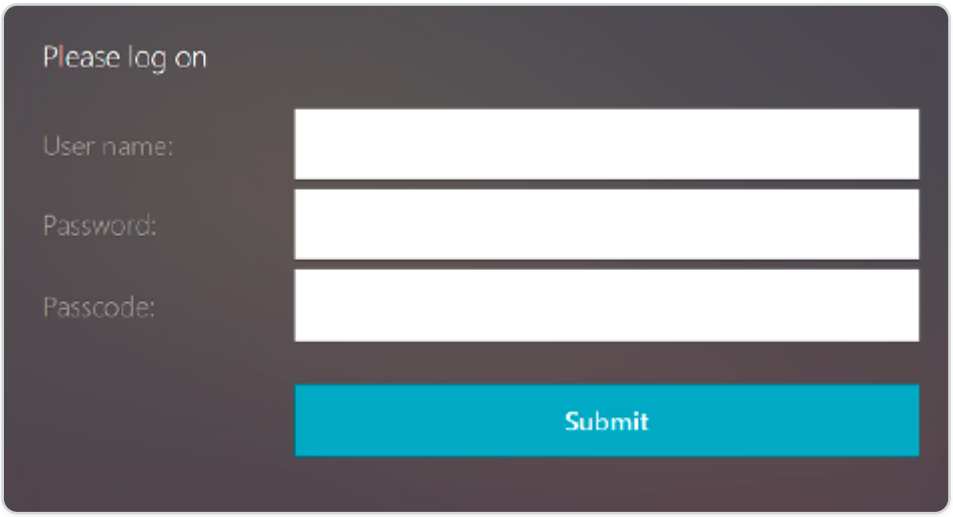



7. Para probar, haga clic en **Listo** en la pantalla QR, luego haga clic en la marca de verificación verde de la derecha.
8. Seleccione su dispositivo en el menú desplegable e introduzca el código de Google Authenticator (debe ser azul, no rojo) y haga clic en **Ir**.
9. Asegúrese de cerrar sesión utilizando el menú desplegable en la esquina superior derecha de la página.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

## Iniciar sesión en NetScaler mediante la OTP

1. Vaya a su primera URL pública e introduzca su OTP de Google Authenticator para iniciar sesión.
2. Autentíquese en la página de bienvenida de NetScaler.




© 1997–2026 Citrix Systems, Inc. All rights reserved.

# Uso de alta disponibilidad

Una implementación de alta disponibilidad de dos dispositivos NetScaler Gateway puede proporcionar un funcionamiento ininterrumpido en cualquier transacción. Cuando se configura un dispositivo como nodo principal y el otro como nodo secundario, el nodo principal acepta conexiones y administra servidores, mientras que el nodo secundario supervisa al principal. Si, por alguna razón, el nodo principal no puede aceptar conexiones, el nodo secundario toma el control.

El nodo secundario supervisa al principal enviando mensajes periódicos (a menudo llamados mensajes de latido o comprobaciones de estado) para determinar si el nodo principal está aceptando conexiones. Si una comprobación de estado falla, el nodo secundario reintenta la conexión durante un período especificado, después del cual determina que el nodo principal no funciona con normalidad. El nodo secundario toma el control del principal (un proceso llamado conmutación por error).

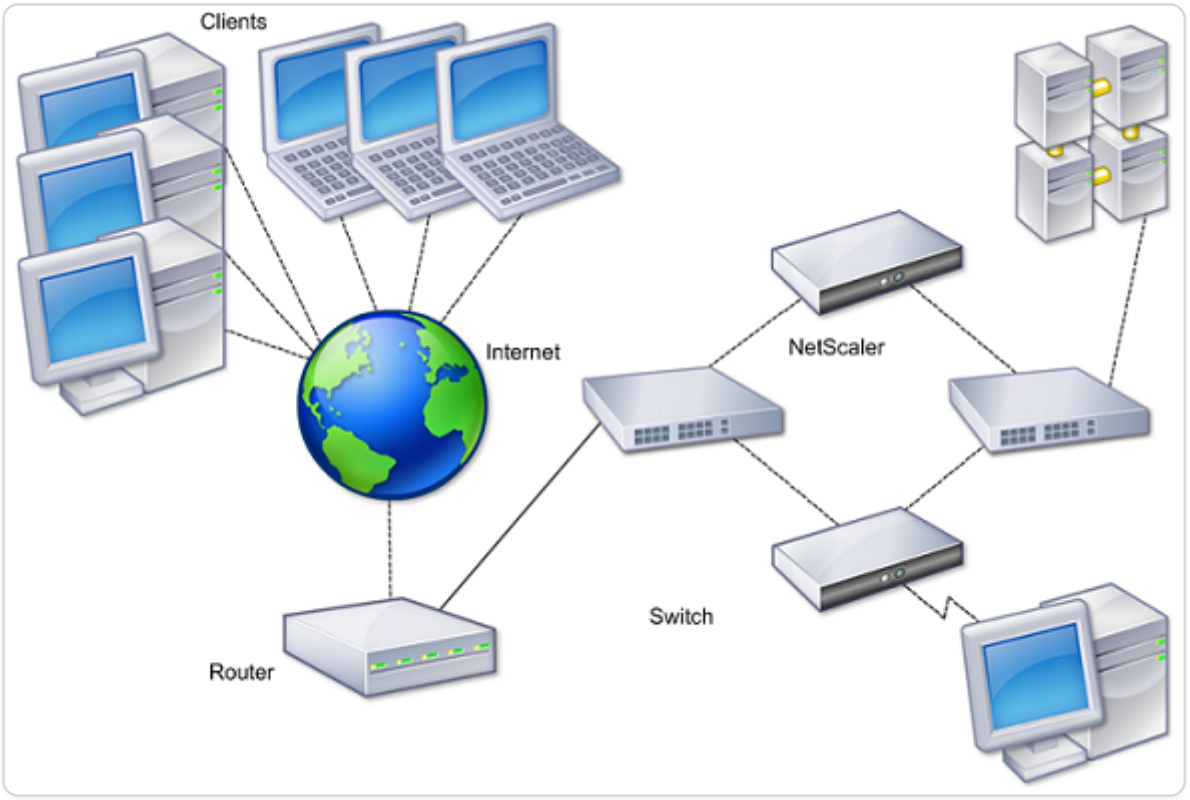
Después de una conmutación por error, todos los clientes deben restablecer sus conexiones a los servidores administrados, pero las reglas de persistencia de sesión se mantienen como estaban antes de la conmutación por error.

Con la persistencia de registro del servidor web habilitada, no se pierden datos de registro debido a la conmutación por error. Para que la persistencia de registro esté habilitada, la configuración del servidor de registro debe contener entradas para ambos sistemas en el archivo log.conf.

La siguiente figura muestra una configuración de red con un par de alta disponibilidad.

Figura 1. Dispositivos NetScaler Gateway en una configuración de alta disponibilidad

© 1997–2026 Citrix Systems, Inc. All rights reserved.




Los pasos básicos para configurar la alta disponibilidad son los siguientes:

1. Crear una configuración básica, con ambos nodos en la misma subred.
2. Personalizar los intervalos en los que los nodos comunican la información de comprobación de estado.
3. Personalizar el proceso mediante el cual los nodos mantienen la sincronización.
4. Personalizar la propagación de comandos del principal al secundario.
5. Opcionalmente, configurar el modo a prueba de fallos para evitar una situación en la que ninguno de los nodos sea principal.
6. Configurar direcciones MAC virtuales si su entorno incluye dispositivos que no aceptan mensajes ARP gratuitos de NetScaler Gateway.

Cuando esté listo para una configuración más compleja, puede configurar nodos de alta disponibilidad en subredes diferentes.

Para mejorar la fiabilidad de su configuración de alta disponibilidad, puede configurar monitores de ruta y crear enlaces redundantes. En algunas situaciones, como al solucionar problemas o realizar tareas de mantenimiento, es posible que desee forzar la conmutación por error de un nodo (asignar el estado principal al otro nodo), o es posible que desee forzar que el nodo secundario permanezca secundario o que el nodo principal permanezca principal.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

# Cómo funciona la alta disponibilidad

Cuando se configura NetScaler Gateway en un par de alta disponibilidad, el NetScaler Gateway secundario supervisa el primer dispositivo enviando mensajes periódicos, también llamados mensajes de latido o comprobación de estado, para determinar si el primer dispositivo está aceptando conexiones. Si una comprobación de estado falla, el NetScaler Gateway secundario intenta la conexión de nuevo durante un tiempo especificado hasta que determina que el dispositivo principal no funciona. Si el dispositivo secundario confirma el fallo de la comprobación de estado, el NetScaler Gateway secundario toma el control del NetScaler Gateway principal. Esto se denomina conmutación por error.

Los siguientes puertos se utilizan para intercambiar información relacionada con la alta disponibilidad entre los dispositivos NetScaler Gateway:

- El puerto UDP 3003 se utiliza para intercambiar paquetes de saludo para comunicar el estado a intervalos.
- El puerto TCP 3010 se utiliza para la sincronización de la configuración de alta disponibilidad.
- El puerto TCP 3011 se utiliza para sincronizar la configuración.

## Directrices para configurar la alta disponibilidad

Antes de configurar un par de alta disponibilidad, debe revisar estas directrices:

- Cada dispositivo NetScaler Gateway debe ejecutar la misma versión del software NetScaler Gateway. Puede encontrar el número de versión en la parte superior de la página en la utilidad de configuración.
- NetScaler Gateway no sincroniza automáticamente las contraseñas entre dos dispositivos. Puede optar por configurar cada NetScaler Gateway con el nombre de usuario y la contraseña del otro dispositivo del par.
- Las entradas del archivo de configuración, ns.conf, tanto en el NetScaler Gateway principal como en el secundario deben coincidir, con las siguientes excepciones:
    - El dispositivo NetScaler Gateway principal y el secundario deben configurarse cada uno con su propia dirección IP de sistema única. Utilice el Asistente de configuración para configurar o modificar la dirección IP del sistema en cualquiera de los NetScaler Gateway.
    - En un par de alta disponibilidad, el ID de NetScaler Gateway y la dirección IP asociada deben apuntar al otro NetScaler Gateway.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Por ejemplo, si tiene dos dispositivos, denominados AG1 y AG2, debe configurar AG1 con el ID de NetScaler Gateway único y la dirección IP de AG2. Debe configurar AG2 con el ID de NetScaler Gateway único y la dirección IP de AG1.

Nota: Cada dispositivo NetScaler Gateway siempre se identifica como Nodo 0. Configure cada dispositivo con un ID de nodo único.

- Cada dispositivo del par de alta disponibilidad debe tener la misma licencia. Para obtener más información sobre las licencias, consulte Licencias.
- Si crea un archivo de configuración en cualquiera de los nodos mediante un método que no pase directamente por la utilidad de configuración o la interfaz de línea de comandos (por ejemplo, importando certificados SSL o cambiando los scripts de inicio), debe copiar el archivo de configuración al otro nodo o crear un archivo idéntico en ese nodo.
- Al configurar un par de alta disponibilidad, asegúrese de que las direcciones IP asignadas y la dirección de la puerta de enlace predeterminada de los dispositivos principal y secundario sean idénticas. Si es necesario, puede cambiar la dirección IP asignada en cualquier momento ejecutando el Asistente de configuración.

Puede usar la lista de comprobación previa a la instalación para ver una lista de la configuración específica que debe configurar en una implementación de alta disponibilidad. Para obtener más información, consulte Lista de comprobación previa a la instalación.

## Configuración de ajustes para alta disponibilidad

Para configurar una configuración de alta disponibilidad, se crean dos nodos, cada uno de los cuales define la dirección IP de NetScaler Gateway del otro como un nodo remoto. Puede empezar iniciando sesión en uno de los dos dispositivos NetScaler que desea configurar para alta disponibilidad y añadir un nodo. Especifique la dirección IP de NetScaler Gateway del otro dispositivo como la dirección del nuevo nodo. Luego, inicie sesión en el otro dispositivo y añada un nodo que tenga la dirección IP de NetScaler Gateway del primer dispositivo. Un algoritmo determina qué nodo se convierte en principal y cuál en secundario.

Antes de configurar los dispositivos, añada un nodo de alta disponibilidad. Este nodo representa el primer o el segundo NetScaler Gateway en el par de alta disponibilidad. Para configurar la alta disponibilidad, primero se crea el nodo y luego se configuran los ajustes de alta disponibilidad.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**IMPORTANTE:**

- Para garantizar una alta disponibilidad sin interrupciones y una funcionalidad de información de HDX™ ininterrumpida, es crucial que ambos nodos operen con la misma versión de software. Las discrepancias de versión durante las actualizaciones pueden interrumpir la recopilación de datos de sesión esenciales, lo que lleva a posibles interrupciones del servicio y a la generación del error "código de omisión 143" después de la conmutación por error. Por lo tanto, los datos de información de HDX no se rellenan para las conexiones ICA existentes durante o después de la actualización.
- Cuando la sincronización de datos entre los nodos principal y secundario está incompleta, el nodo secundario podría carecer de información suficiente para reanudar las conexiones sin problemas. Esto puede resultar en que NetScaler Gateway no pueda recuperar datos esenciales de información de HDX, lo que lleva a un error de "código de omisión 169". Por lo tanto, el soporte de información de HDX podría verse temporalmente interrumpido durante los escenarios de conmutación por error.

## Para añadir un nodo de alta disponibilidad

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda **Sistema > Alta disponibilidad**.
2. En el panel de detalles, en la ficha Nodos, haga clic en **Agregar**.
3. En la página **Crear nodo HA**, en el cuadro de texto **Dirección IP de nodo remoto**, escriba la dirección NSIP del NetScaler que se va a añadir como nodo remoto. Si la dirección IP de NetScaler Gateway es una dirección IPv6, seleccione la casilla de verificación **IPv6** antes de introducir la dirección.
4. Si quiere añadir el nodo local al nodo remoto automáticamente, seleccione Configurar sistema remoto para participar en la configuración de alta disponibilidad. Si no selecciona esta opción, debe iniciar sesión en el dispositivo representado por el nodo remoto y añadir el nodo que está configurando actualmente.
5. Haga clic para habilitar **Desactivar interfaces/canales de monitorización de HA que estén inactivos**.
6. Si el dispositivo remoto tiene un nombre de usuario y una contraseña diferentes, en Credenciales de inicio de sesión del sistema remoto, haga clic en Las credenciales de inicio de sesión del sistema remoto son diferentes de las del nodo propio.
7. En **Nombre de usuario**, escriba el nombre de usuario del dispositivo remoto.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

8. En **Contraseña**, escriba la contraseña del dispositivo remoto.
9. Haga clic en **Aceptar**.

## Para habilitar o deshabilitar el nodo secundario

Solo puede deshabilitar o habilitar el nodo secundario. Cuando deshabilita un nodo secundario, deja de enviar mensajes de latido al nodo principal y, por lo tanto, el nodo principal ya no puede comprobar el estado del nodo secundario. Cuando habilita un nodo, este participa en la configuración de alta disponibilidad.

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda Sistema y, a continuación, haga clic en Alta disponibilidad.
2. En el panel de detalles, en la ficha Nodos, seleccione el nodo local y, a continuación, haga clic en Abrir.
3. En el cuadro de diálogo Configurar nodo de HA, en Estado de alta disponibilidad, seleccione HABILITADO (No participar en HA).
4. Haga clic en Aceptar. Aparece un mensaje en la barra de estado, indicando que el nodo se ha configurado correctamente.

## Para configurar los ajustes de alta disponibilidad

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda **Sistema > Alta disponibilidad**.
2. En el panel de detalles, en la ficha Nodos, seleccione un nodo y, a continuación, haga clic en **Editar**.
3. En el cuadro de diálogo **Configurar nodo de HA**, en ID, escriba el número del identificador de nodo. ID especifica el número de nodo único para el otro dispositivo.
4. En **Dirección IP**, escriba la dirección IP del sistema y, a continuación, haga clic en Aceptar. La Dirección IP especifica la dirección IP del otro dispositivo.

**Nota**: El ID máximo para los nodos en un par de alta disponibilidad es 64.

## Cambiar la contraseña de un nodo RPC

Para comunicarse con otros dispositivos NetScaler Gateway, cada dispositivo requiere conocer los demás dispositivos, incluida la forma de autenticarse en NetScaler Gateway. Los nodos RPC son entidades internas del sistema que se utilizan para la comunicación de configuración e información de sesión entre sistemas. Existe un nodo RPC en cada NetScaler Gateway y almacena información, como las direcciones IP del otro dispositivo NetScaler Gateway y las contraseñas

© 1997–2026 Citrix Systems, Inc. All rights reserved.

utilizadas para la autenticación. El NetScaler Gateway que se pone en contacto con otro NetScaler Gateway comprueba la contraseña dentro del nodo RPC.

NetScaler Gateway requiere contraseñas de nodo RPC en ambos dispositivos de un par de alta disponibilidad. Las contraseñas deben ser las mismas en ambos dispositivos. El dispositivo principal debe conocer la contraseña del nodo RPC secundario y el secundario debe conocer la contraseña del nodo RPC principal. Inicialmente, cada NetScaler Gateway se configura con la misma contraseña de nodo RPC. Para mejorar la seguridad, debe cambiar las contraseñas predeterminadas de los nodos RPC. Puede utilizar la utilidad de configuración para configurar y cambiar los nodos RPC.

Los nodos RPC se crean implícitamente al agregar un nodo o al agregar un sitio de equilibrio de carga de servidor global (GSLB). No se pueden crear ni eliminar nodos RPC manualmente.

**IMPORTANTE:**

También debe proteger la conexión de red entre los dispositivos. Puede configurar la seguridad al configurar la contraseña del nodo RPC seleccionando la casilla de verificación **Seguro**.

### Para cambiar la contraseña de un nodo RPC y habilitar una conexión segura

1. Vaya a **Sistema > Red > RPC.**
2. En el panel de detalles, seleccione el nodo y, a continuación, haga clic en **Editar**.
3. En **Contraseña** y **Confirmar contraseña**, escriba la nueva contraseña.
4. En **Dirección IP de origen**, escriba la dirección IP del sistema del otro dispositivo NetScaler Gateway.
5. Haga clic en **Seguro** y, a continuación, en **Aceptar**.

**NOTA:**

Cuando habilita la opción **Seguro**, el dispositivo cifra toda la comunicación enviada desde el nodo a otros nodos RPC, lo que garantiza la seguridad de la comunicación RPC.

### Para cambiar la contraseña de un nodo RPC mediante la CLI

En el símbolo del sistema, escriba:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
set ns rpcNode <IPAddress> {-password} [-secure ( YES | NO )]



show ns rpcNode
```

**Ejemplo:**

```
> set ns rpcNode 192.0.2.4 -password mypassword -secure YES

 Done

> show rpcNode

.

.

.

 IPAddress:  192.0.2.4 Password:  d336004164d4352ce39e

     SrcIP:  *           Secure:  ON

Done

>
```

## Configuración de los dispositivos principal y secundario para alta disponibilidad

Después de cambiar la contraseña del nodo RPC y habilitar la comunicación segura, utilice la utilidad de configuración para configurar los nodos principal y secundario de alta disponibilidad de NetScaler Gateway.

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda Sistema y, a continuación, haga clic en Alta disponibilidad.
2. En el panel de detalles, en la ficha Nodos, seleccione un nodo y, a continuación, haga clic en Modificar.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. En Estado de alta disponibilidad, haga clic en Habilitado (Participar activamente en HA) y, a continuación, haga clic en Aceptar.

# Configuración de los intervalos de comunicación

Al configurar NetScaler Gateway como un par de alta disponibilidad, puede configurar el NetScaler Gateway secundario para que escuche a intervalos específicos, medidos en milisegundos (ms). Estos intervalos se conocen como intervalos de saludo (hello intervals) e intervalos de inactividad (dead intervals).

El intervalo de saludo (hello interval) es el intervalo en el que se envían los mensajes de latido al nodo par. El intervalo de inactividad (dead interval) es el intervalo de tiempo después del cual el nodo par se marca como INACTIVO si no se reciben paquetes de latido. Los mensajes de latido son paquetes UDP enviados al puerto 3003 del otro nodo en un par de alta disponibilidad.

Al configurar el intervalo de saludo (hello interval), puede usar los valores de 200 a 1000. El valor predeterminado es 200. Los valores del intervalo de inactividad (dead interval) son de 3 a 60. El valor predeterminado es 3.

**NOTA**

El intervalo de inactividad (dead interval) debe establecerse como un múltiplo del intervalo de saludo (hello interval).

## Para configurar los intervalos de comunicación para el NetScaler Gateway secundario

1. En la utilidad de configuración, en la pestaña Configuración, en el panel de navegación, expanda Sistema y, a continuación, haga clic en Alta disponibilidad.
2. En el panel de detalles, en la pestaña Nodos, seleccione un nodo y, a continuación, haga clic en Editar.
3. En Intervalos, realice una o ambas de las siguientes acciones:
   - En Intervalo de saludo (ms), escriba el valor y, a continuación, haga clic en Aceptar. El valor predeterminado es 200 milisegundos.
   - En Intervalo de inactividad (s), escriba el valor y, a continuación, haga clic en Aceptar. La configuración predeterminada es de tres segundos.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

# Sincronización de dispositivos NetScaler Gateway

La sincronización automática de los dispositivos NetScaler Gateway en un par de alta disponibilidad está habilitada de forma predeterminada. Con la sincronización automática, puede realizar cambios en un dispositivo y permitir que los cambios se propaguen automáticamente al segundo dispositivo. La sincronización utiliza el puerto 3010.

La sincronización se inicia cuando ocurre lo siguiente:

- El nodo secundario se reinicia.
- El nodo principal se convierte en secundario después de una conmutación por error.

Puede inhabilitar la sincronización, lo que impide que el NetScaler Gateway secundario sincronice su configuración con el NetScaler Gateway principal cuando se produce un cambio en el dispositivo principal. También puede forzar la sincronización.

Habilita o inhabilita la sincronización de alta disponibilidad en el nodo secundario del par.

## Para habilitar o inhabilitar la sincronización de alta disponibilidad

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda Sistema y, a continuación, haga clic en Alta disponibilidad.
2. En el panel de detalles, en la ficha Nodos, seleccione un nodo y, a continuación, haga clic en Editar.
3. En el cuadro de diálogo Configurar nodo, en Sincronización HA, realice una de las siguientes acciones:
    - Para inhabilitar la sincronización, desactive la casilla de verificación El nodo secundario obtendrá la configuración del principal.
    - Para habilitar la sincronización, active la casilla de verificación El nodo secundario obtendrá la configuración del principal.
4. Haga clic en Aceptar. Aparece un mensaje en la barra de estado indicando que la configuración del nodo se realizó correctamente.

## Para forzar la sincronización entre dispositivos

Además de la sincronización automática, NetScaler Gateway admite la sincronización forzada entre los dos nodos de un par de alta disponibilidad.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Puede forzar la sincronización tanto en los dispositivos NetScaler Gateway principales como en los secundarios. Sin embargo, si la sincronización ya está en curso, el comando falla y NetScaler Gateway muestra una advertencia. La sincronización forzada también falla en las siguientes circunstancias:

- Fuerza la sincronización en un sistema independiente.
- El nodo secundario está inhabilitado.
- Inhabilita la sincronización de alta disponibilidad en el nodo secundario.

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda Sistema y, a continuación, haga clic en Alta disponibilidad.
2. En la ficha Nodos, haga clic en Forzar sincronización.

# Sincronización de archivos de configuración en una configuración de alta disponibilidad

En una configuración de alta disponibilidad, puede sincronizar varios archivos de configuración desde el nodo principal al nodo secundario.

## Parámetros para sincronizar archivos en una configuración de alta disponibilidad

- Modo

```
El tipo de sincronización que se va a realizar. Las siguientes
descripciones incluyen, entre paréntesis, el argumento de línea de
comandos que especifica la opción.

-  **Todo excepto licencias y rc.conf** (all). Sincroniza archivos
relacionados con la configuración del sistema, marcadores de NetScaler
Gateway, certificados SSL, listas CRL de SSL, scripts de inyección HTML y
objetos XML de Application Firewall.

-  **Marcadores** (bookmarks). Sincroniza todos los marcadores de
NetScaler Gateway.

-  **Certificados y claves SSL** (`ssl`). Sincroniza todos los
certificados, claves y CRL para la función SSL.

-  **Licencias y rc.conf** (misc). Sincroniza todos los archivos de
licencia y el archivo rc.conf.
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
-  **Todo, incluidas las licencias y rc.conf** (all\_plus\_misc).
Sincroniza archivos relacionados con la configuración del sistema,
marcadores de NetScaler Gateway, certificados SSL, listas CRL de SSL,
scripts de inyección HTML, objetos XML de Application Firewall, licencias
y el archivo rc.conf.
```

Nota: Hay más opciones disponibles si instala una licencia de NetScaler en el dispositivo.

### Para sincronizar archivos en una configuración de alta disponibilidad mediante la utilidad de configuración

1. En el panel de navegación, expanda **Sistema** y, a continuación, haga clic en **Diagnóstico**.
2. En el panel de detalles, en **Utilidades**, haga clic en **Iniciar sincronización de archivos HA**.
3. En el cuadro de diálogo **Iniciar sincronización de archivos**, en el menú **Modo**, seleccione el tipo de sincronización adecuado (por ejemplo, Todo excepto licencias y rc.conf) y, a continuación, haga clic en **Aceptar**.

## Configuración de la propagación de comandos

En una configuración de alta disponibilidad, cualquier comando emitido en el nodo principal se propaga automáticamente al nodo secundario y se ejecuta en él antes de que el comando se ejecute en el nodo principal. Si la propagación del comando falla, o si la ejecución del comando falla en el nodo secundario, el nodo principal ejecuta el comando y registra un error. La propagación de comandos utiliza el puerto 3011.

En una configuración de par de alta disponibilidad, la propagación de comandos está habilitada de forma predeterminada tanto en el nodo principal como en el secundario. Puede habilitar o deshabilitar la propagación de comandos en cualquiera de los nodos de un par de alta disponibilidad. Si deshabilita la propagación de comandos en el nodo principal, los comandos no se propagan al nodo secundario. Si deshabilita la propagación de comandos en el nodo secundario, los comandos propagados desde el principal no se ejecutan en el nodo secundario.

Nota: Después de volver a habilitar la propagación, recuerde forzar la sincronización.

Nota: Si la sincronización se produce mientras se deshabilita la propagación, cualquier cambio relacionado con la configuración que realice antes de que la deshabilitación de la propagación surta efecto se sincronizará con el nodo secundario. Esto también es cierto para los casos en los que la propagación se deshabilita mientras la sincronización está en curso.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

## Para habilitar o deshabilitar la propagación en el nodo principal

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda **Sistema** y, a continuación, haga clic en **Alta disponibilidad**.
2. En el panel de detalles, en la ficha **Nodos**, seleccione un nodo y, a continuación, haga clic en **Editar**.
3. En **Propagación de HA**, realice una de las siguientes acciones:
   - Para deshabilitar la propagación de alta disponibilidad, desactive la casilla de verificación **El nodo principal propaga la configuración al secundario**.
   - Para habilitar la propagación de alta disponibilidad, seleccione la casilla de verificación **El nodo principal propaga la configuración al secundario**.
4. Haga clic en **Aceptar**.

## Solución de problemas de propagación de comandos

La siguiente lista describe las razones por las que la propagación de comandos podría fallar, y soluciones para restaurar la configuración:

- La conectividad de red no está activa. Si falla la propagación de un comando, compruebe la conexión de red entre los dispositivos NetScaler Gateway principal y secundario.
- Recursos faltantes en el NetScaler Gateway secundario. Si la ejecución de un comando se realiza correctamente en el NetScaler Gateway principal pero no se propaga al NetScaler Gateway secundario, ejecute el comando directamente en el NetScaler Gateway secundario para ver el mensaje de error. El error podría haberse producido porque los recursos necesarios para el comando están presentes en el NetScaler Gateway principal y no están disponibles en el NetScaler Gateway secundario. Además, verificar que los archivos de licencia de cada dispositivo coinciden.

  Por ejemplo, verificar que todos sus certificados Secure Sockets Layer (SSL) estén presentes en cada NetScaler Gateway. verificar que cualquier personalización del script de inicialización exista en ambos dispositivos NetScaler Gateway.
- Error de autenticación. Si recibe un mensaje de error de autenticación, verificar la configuración del nodo RPC en cada dispositivo.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

# Configurar el modo a prueba de fallos

En una configuración de alta disponibilidad, el modo a prueba de fallos garantiza que un nodo sea siempre principal cuando ambos nodos fallen la comprobación de estado. El modo a prueba de fallos garantiza que, cuando un nodo solo está parcialmente disponible, los métodos de copia de seguridad puedan activarse y gestionar el tráfico.

Se configura el modo a prueba de fallos de alta disponibilidad de forma independiente en cada nodo.

La siguiente tabla muestra algunos de los casos de modo a prueba de fallos. El estado NOT_UP significa que el nodo falló la comprobación de estado y, sin embargo, el nodo está parcialmente disponible. El estado UP significa que el nodo pasó la comprobación de estado.

Tabla 1. Casos de modo a prueba de fallos

| ESTADO DE SALUD DEL NODO A (PRINCIPAL) | ESTADO DE SALUD DEL NODO B (SECUNDARIO) | COMPORTAMIENTO PREDETERMINADO DE ALTA DISPONIBILIDAD | COMPORTAMIENTO DE ALTA DISPONIBILIDAD CON MODO A PRUEBA DE FALLOS HABILITADO | DESCRIPCIÓN |
|---|---|---|---|---|
| NOT_UP (falló el último) | NOT_UP (falló el primero) | A (Secundario), B (Secundario) | A (Principal), B (Secundario) | Si ambos nodos fallan, uno tras otro, el nodo que fue el último nodo principal permanece como principal. |
| NO_ACTIVO (falló primero) | NO_ACTIVO (falló último) | A (Secundario), B (Secundario) | A (Secundario), B (Principal) | Si ambos nodos fallan, uno tras otro, el nodo que fue el último nodo principal permanece como principal. |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| ESTADO DE SALUD DEL NODO A (PRINCIPAL) | ESTADO DE SALUD DEL NODO B (SECUNDARIO) | COMPORTAMIENTO PREDETERMINADO DE ALTA DISPONIBILIDAD | COMPORTAMIENTO DE ALTA DISPONIBILIDAD CON MODO A PRUEBA DE FALLOS HABILITADO | DESCRIPCIÓN |
|---|---|---|---|---|
| ACTIVO | ACTIVO | A (Principal), B (Secundario) | A (Principal), B (Secundario) | Si ambos nodos superan la comprobación de estado, no hay cambios en el comportamiento con el modo a prueba de fallos habilitado. |
| ACTIVO | NO_ACTIVO | A (Principal), B (Secundario) | A (Principal), B (Secundario) | Si solo falla el nodo secundario, no hay cambios en el comportamiento con el modo a prueba de fallos habilitado. |
| NOT_UP | UP | A (Secundario), B (Principal) | A (Secundario), B (Principal) | Si solo falla el principal, no hay cambios en el comportamiento con el modo a prueba de fallos habilitado. |
| NOT_UP | UP (STAYSECONDARY) | A (Secundario), B (Secundario) | A (Principal), B (Secundario) | Si el secundario está configurado como |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| | | | | |
|---|---|---|---|---|
| | | | | STAYSECONDARY, el principal sigue siendo principal incluso si falla. |

### Para configurar el modo a prueba de fallos

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda Sistema y, a continuación, haga clic en Alta disponibilidad.
2. En el panel de detalles, en la ficha Nodos, seleccione un nodo y, a continuación, haga clic en Editar.
3. En el cuadro de diálogo Configurar nodo, en Modo a prueba de fallos, seleccione Mantener un nodo principal incluso cuando ambos nodos no estén en buen estado y, a continuación, haga clic en Aceptar.

## Configuración de la dirección MAC virtual

La dirección MAC virtual es compartida por los dispositivos NetScaler Gateway primario y secundario en una configuración de alta disponibilidad.

En una configuración de alta disponibilidad, el NetScaler Gateway principal posee todas las direcciones IP flotantes, como la dirección IP asignada o la dirección IP virtual. Responde a las solicitudes del protocolo de resolución de direcciones (ARP) para estas direcciones IP con su propia dirección MAC. Como resultado, la tabla ARP de un dispositivo externo (como un enrutador) se actualiza con la dirección IP flotante y la dirección MAC del NetScaler Gateway principal. Cuando se produce una conmutación por error, el NetScaler Gateway secundario asume el rol de nuevo NetScaler Gateway principal. Luego utiliza el protocolo de resolución de direcciones gratuito (GARP) para anunciar las direcciones IP flotantes que adquirió del dispositivo principal. La dirección MAC que anuncia el nuevo dispositivo principal es la de su propia interfaz.

Algunos dispositivos no aceptan los mensajes GARP generados por NetScaler Gateway. Como resultado, algunos de los dispositivos externos retienen la antigua asignación de IP a MAC anunciada por el antiguo NetScaler Gateway principal. Esta situación puede hacer que un sitio deje de estar disponible. Para resolver el problema, se configura una dirección MAC virtual en ambos dispositivos NetScaler Gateway de un par de alta disponibilidad. Esta configuración implica que ambos dispositivos NetScaler Gateway tienen direcciones MAC idénticas. Como resultado, cuando se produce una conmutación por error, la dirección MAC del NetScaler Gateway

© 1997–2026 Citrix Systems, Inc. All rights reserved.

secundario permanece inalterada y las tablas ARP de los dispositivos externos no necesitan actualizarse.

Para crear una dirección MAC virtual, cree un identificador de enrutador virtual (ID) y vincúlelo a una interfaz. En una configuración de alta disponibilidad, el usuario debe vincular el ID a las interfaces de ambos dispositivos.

Cuando el ID del enrutador virtual se vincula a una interfaz, el sistema genera una dirección MAC virtual con el ID del enrutador virtual como último octeto. Un ejemplo de la dirección MAC virtual genérica es 00:00:5e:00:01:\<VRID\>. Por ejemplo, si creó un ID de enrutador virtual con el valor 60 y lo vincula a una interfaz, la dirección MAC virtual resultante es 00:00:5e:00:01:3c, donde 3c es la representación hexadecimal del ID del enrutador virtual. Puede crear 255 ID de enrutador virtual que van del 1 al 254.

Puede configurar direcciones MAC virtuales para IPv4 e IPv6.

## Configuración de direcciones MAC virtuales IPv4

Cuando se crea una dirección MAC virtual IPv4 y se vincula a una interfaz, cualquier paquete IPv4 enviado desde la interfaz utiliza la dirección MAC virtual que está vinculada a la interfaz. Si no hay ninguna dirección MAC virtual IPv4 vinculada a una interfaz, se utiliza la dirección MAC física de la interfaz.

La dirección MAC virtual genérica tiene el formato 00:00:5e:00:01:\<VRID\>. Por ejemplo, si crea un VRID con un valor de 60 y lo vincula a una interfaz, la dirección MAC virtual resultante es 00:00:5e:00:01:3c, donde 3c es la representación hexadecimal del VRID. Puede crear 255 VRID con valores de 1 a 255.

### Creación o modificación de una dirección MAC virtual IPv4

Se crea una dirección MAC virtual IPv4 asignándole un ID de enrutador virtual. A continuación, puede vincular la dirección MAC virtual a una interfaz. No se pueden vincular varios ID de enrutador virtual a la misma interfaz. Para verificar la configuración de la dirección MAC virtual, debe mostrar y examinar la dirección MAC virtual y las interfaces vinculadas a la dirección MAC virtual.

#### Parámetros para configurar una dirección MAC virtual

VRID

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
El ID de enrutador virtual que identifica la dirección MAC virtual.
Valores posibles: 1–255.
```

`ifnum`

```
El número de interfaz (notación de ranura/puerto) que se vinculará a la
dirección MAC virtual.
```

**Para configurar una dirección MAC virtual**

1. Vaya a **Sistema > Red** y, a continuación, haga clic en **VMAC**.
2. En el panel de detalles, en la ficha **VMAC**, haga clic en **Agregar**.
3. En el cuadro de diálogo **Crear VMAC**, en **ID de enrutador virtual**, escriba el valor.
4. En **Interfaces asociadas**, en **Interfaces disponibles**, seleccione una interfaz de red, haga clic en **Agregar**, haga clic en **Crear** y, a continuación, haga clic en **Cerrar**.

Después de crear la dirección MAC virtual, aparece en la utilidad de configuración. Si seleccionó una interfaz de red, el ID de enrutador virtual se vincula a esa interfaz.

**Para eliminar una dirección MAC virtual**

Para eliminar una dirección MAC virtual, debe eliminar el ID de enrutador virtual correspondiente.

1. Vaya a **Sistema > Red** y, a continuación, haga clic en **VMAC**.
2. En el panel de detalles, seleccione un elemento y, a continuación, haga clic en **Eliminar**.

**Para vincular y desvincular una dirección MAC virtual**

Cuando creó el ID de enrutador virtual, seleccionó una interfaz de red en NetScaler Gateway y, a continuación, vinculó el ID de enrutador virtual a la interfaz de red. También puede desvincular una dirección MAC virtual de la interfaz de red, pero dejar la dirección MAC configurada en NetScaler Gateway.

1. Vaya a **Sistema > Red** y, a continuación, haga clic en **VMAC**.
2. En el panel de detalles, seleccione un elemento y, a continuación, haga clic en **Abrir**.
3. En **Interfaces configuradas**, seleccione una interfaz de red, haga clic en **Eliminar**, haga clic en **Aceptar** y, a continuación, haga clic en **Cerrar**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

# Configuración de direcciones MAC virtuales IPv6

NetScaler Gateway admite direcciones MAC virtuales para paquetes IPv6. Puede vincular cualquier interfaz a una dirección MAC virtual para IPv6, incluso si una dirección MAC virtual IPv4 está vinculada a la interfaz. Cualquier paquete IPv6 enviado desde la interfaz utiliza la dirección MAC virtual vinculada a esa interfaz. Si no hay ninguna dirección MAC virtual vinculada a una interfaz, un paquete IPv6 utiliza la MAC física.

## Crear o modificar una dirección MAC virtual para IPv6

Cree una dirección MAC virtual IPv6 asignándole un ID de enrutador virtual IPv6. A continuación, vincule la dirección MAC virtual a una interfaz. No puede vincular varios ID de enrutador virtual IPv6 a una interfaz. Para verificar la configuración de la dirección MAC virtual, muestre y examine las direcciones MAC virtuales y las interfaces vinculadas a la dirección MAC virtual.

### Parámetros para configurar una dirección MAC virtual para IPv6

- `Virtual Router ID`

  El ID de enrutador virtual que identifica la dirección MAC virtual. Valores posibles: 1-255.

- `ifnum`

  El número de interfaz (notación de ranura/puerto) que se va a vincular a la dirección MAC virtual.

### Para configurar una dirección MAC virtual para IPv6

1. En la utilidad de configuración, en la ficha Configuración, expanda **Sistema > Red** y, a continuación, haga clic en VMAC.
2. En el panel de detalles, en la ficha VMAC6, realice una de las siguientes acciones:
   - Para crear una nueva dirección MAC virtual, haga clic en Agregar.
   - Para modificar una dirección MAC virtual existente, haga clic en Abrir.
3. En el cuadro de diálogo Crear VMAC6 o Configurar VMAC6, en ID de enrutador virtual, introduzca el valor, como vrID6.
4. En Asociar interfaces, haga clic en **Agregar > Crear > Cerrar**. Aparece un mensaje en la barra de estado, indicando que la dirección MAC virtual está configurada.

### Para eliminar una dirección MAC virtual para IPv6

1. En la utilidad de configuración, en la ficha Configuración, expanda **Sistema > Red** y, a continuación, haga clic en VMAC.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. En el panel de detalles, en la pestaña VMAC6, seleccione el ID de enrutador virtual que desea eliminar y, a continuación, haga clic en Eliminar. Aparece un mensaje en la barra de estado, indicando que la dirección MAC virtual se ha eliminado.

# Configuración de pares de alta disponibilidad en subredes diferentes

Una implementación típica de alta disponibilidad es cuando ambos dispositivos de un par de alta disponibilidad residen en la misma subred. Una implementación de alta disponibilidad también puede consistir en dos dispositivos NetScaler Gateway en los que cada dispositivo está en una red diferente. Este tema describe esta última configuración e incluye configuraciones de ejemplo y una lista de diferencias entre las configuraciones de alta disponibilidad dentro de una red y entre redes.

También puede configurar la redundancia de enlaces y los monitores de rutas. Estas funciones de NetScaler Gateway son útiles en una configuración de alta disponibilidad entre redes. Las funciones también cubren el proceso de comprobación de estado utilizado por cada NetScaler Gateway para garantizar que el dispositivo asociado esté activo.

## Cómo funciona la configuración de red independiente

Los dispositivos NetScaler Gateway están conectados a diferentes enrutadores, llamados R3 y R4, en dos redes diferentes. Los dispositivos intercambian paquetes de latido a través de estos enrutadores. Un paquete de latido es una señal que se produce a intervalos regulares y que garantiza que la conexión sigue activa. Puede ampliar esta configuración para adaptarse a implementaciones que involucren cualquier número de interfaces.

Nota: Si utiliza enrutamiento estático en su red, debe agregar rutas estáticas entre todos los sistemas para garantizar que los paquetes de latido se envíen y reciban correctamente. (Si utiliza enrutamiento dinámico en sus sistemas, las rutas estáticas son innecesarias).

Cuando los dispositivos de un par de alta disponibilidad residen en dos redes diferentes, el NetScaler Gateway secundario debe tener una configuración de red independiente. Esto significa que los dispositivos NetScaler Gateway en diferentes redes no pueden compartir direcciones IP asignadas, VLAN o rutas de red. Este tipo de configuración, en la que los dispositivos NetScaler Gateway de un par de alta disponibilidad tienen diferentes parámetros configurables, se conoce como configuración de red independiente o configuración de red simétrica.

La siguiente tabla resume los parámetros configurables para una configuración de red independiente y muestra cómo debe configurarlos en cada NetScaler Gateway:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| PARÁMETROS CONFIGURABLES | COMPORTAMIENTO |
|---|---|
| Direcciones IP | Específico de NetScaler Gateway. Activo solo en ese dispositivo. |
| Dirección IP virtual | Flotante. |
| Red de área local virtual | Específico de NetScaler Gateway. Activo solo en ese dispositivo. |
| Rutas | Específico de NetScaler Gateway. Activo solo en ese dispositivo. Una ruta de equilibrio de carga de enlaces (LLB) es flotante. |
| listas de control de acceso (ACL) | Flotante (común). Activo en ambos dispositivos. |
| Enrutamiento dinámico | Específico de NetScaler Gateway. Activo solo en ese dispositivo. El NetScaler Gateway secundario también debe ejecutar los protocolos de enrutamiento y establecer una relación de igual con los enrutadores ascendentes. |
| Modo L2 | Flotante (común). Activo en ambos dispositivos. |
| Modo L3 | Flotante (común). Activo en ambos dispositivos. |
| Traducción de direcciones de red inversa (NAT) | Específico de NetScaler Gateway. NAT inverso con una dirección IP virtual porque la dirección IP de NAT es flotante. |

**NOTA:**

IPSET en modo INC es compatible con direcciones IP públicas. Para obtener más información, consulte Configurar nodos HA-INC mediante la plantilla de alta disponibilidad de NetScaler con Azure ILB.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

## Adición de un nodo remoto

Cuando dos nodos de un par de alta disponibilidad residen en subredes diferentes, cada nodo debe tener una configuración de red diferente. Por lo tanto, para configurar dos sistemas independientes para que funcionen como un par de alta disponibilidad, debe especificar el modo de computación de red independiente durante el proceso de configuración.

Al agregar un nodo de alta disponibilidad, debe inhabilitar el monitor de alta disponibilidad para cada interfaz que no esté conectada o que no se utilice para el tráfico.

### Para agregar un nodo remoto para el modo de computación de red independiente

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda **Sistema > Alta disponibilidad**.
2. En el panel de detalles, haga clic en la ficha **Nodos** y, a continuación, haga clic en **Agregar**.
3. En el cuadro de diálogo Configuración de alta disponibilidad, en el cuadro de texto **Dirección IP del nodo remoto**, escriba la dirección IP de NetScaler Gateway del dispositivo que es el nodo remoto.

   Para usar una dirección IPv6, haga clic en la casilla de verificación **IPv6** antes de introducir la dirección IP.
4. Si desea agregar el nodo local al nodo remoto automáticamente, seleccione Configurar sistema remoto para participar en la configuración de alta disponibilidad. Si no selecciona esta opción, debe iniciar sesión en el dispositivo representado por el nodo remoto y agregar el nodo que está configurando actualmente.
5. Haga clic para habilitar el monitor HA claro en las interfaces/canales que están inactivos.
6. Haga clic para habilitar Activar el modo INC (Configuración de red independiente) en modo propio.
7. Haga clic en **Aceptar**. La página **Nodos** muestra los nodos locales y remotos en su configuración de alta disponibilidad.

### Para eliminar un nodo remoto

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda **Sistema > Alta disponibilidad**.
2. En el panel de detalles, haga clic en la ficha **Nodos**.
3. Seleccione el nodo que desea eliminar, haga clic en **Eliminar,** y, a continuación, haga clic en **Sí**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

# Configuración de monitores de ruta

Puede usar monitores de ruta para hacer que el estado de alta disponibilidad dependa de la tabla de enrutamiento interna, ya sea que la tabla contenga rutas estáticas o aprendidas dinámicamente. En una configuración de alta disponibilidad, un monitor de ruta en cada nodo comprueba la tabla de enrutamiento interna para asegurarse de que siempre haya una entrada de ruta para llegar a una red en particular. Si la entrada de ruta no está presente, el estado del monitor de ruta cambia a INACTIVO.

Cuando un dispositivo NetScaler Gateway solo tiene rutas estáticas para llegar a una red y desea crear un monitor de ruta para esa red, debe habilitar las rutas estáticas supervisadas para las rutas estáticas. La ruta estática supervisada elimina las rutas estáticas inaccesibles de la tabla de enrutamiento interna. Si deshabilita las rutas estáticas supervisadas en las rutas estáticas, una ruta estática inaccesible puede permanecer en la tabla de enrutamiento interna, lo que anula el propósito de tener el monitor de ruta.

Los monitores de ruta son compatibles con la configuración de configuración de red independiente habilitada o deshabilitada. La siguiente tabla muestra lo que ocurre con los monitores de ruta en una configuración de alta disponibilidad y con la configuración de red independiente habilitada o deshabilitada.

| MONITORES DE RUTA EN ALTA DISPONIBILIDAD EN MODO DE CONFIGURACIÓN DE RED INDEPENDIENTE DESHABILITADO | MONITORES DE RUTA EN ALTA DISPONIBILIDAD EN MODO DE CONFIGURACIÓN DE RED INDEPENDIENTE HABILITADO |
|---|---|
| Los monitores de ruta son propagados por los nodos e intercambiados durante la sincronización. | Los monitores de ruta no son propagados por los nodos ni intercambiados durante la sincronización. |
| Los monitores de ruta están activos solo en el nodo principal actual. | Los monitores de ruta están activos tanto en el nodo principal como en el secundario. |
| El dispositivo NetScaler Gateway siempre muestra el estado de un monitor de ruta como ACTIVO, independientemente de si la entrada de ruta está presente o no en la tabla de enrutamiento interna. | El dispositivo NetScaler Gateway muestra el estado del monitor de ruta como INACTIVO si la entrada de ruta correspondiente no está presente en la tabla de enrutamiento interna. |
| Un monitor de ruta comienza a monitorear su ruta en los siguientes casos, para permitir que NetScaler Gateway aprenda las rutas | No aplicable. |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| MONITORES DE RUTA EN ALTA DISPONIBILIDAD EN MODO DE CONFIGURACIÓN DE RED INDEPENDIENTE DESHABILITADO | MONITORES DE RUTA EN ALTA DISPONIBILIDAD EN MODO DE CONFIGURACIÓN DE RED INDEPENDIENTE HABILITADO |
|---|---|
| dinámicas, lo que puede tardar hasta 180 segundos: reinicio, conmutación por error, comando set route6 para rutas v6, comando set route `msr` enable/disable para rutas v4, adición de un nuevo monitor de ruta | |

Los monitores de ruta son útiles cuando se deshabilita el modo de configuración de red independiente y se desea que una puerta de enlace de un nodo principal sea inaccesible como una de las condiciones para la conmutación por error de alta disponibilidad.

Por ejemplo, deshabilita la configuración de red independiente en una configuración de alta disponibilidad en una topología de dos brazos que tiene dispositivos NetScaler Gateway NS1 y NS2 en la misma subred, con el router R1 y los conmutadores SW1, SW2 y SW3, como se muestra en la siguiente figura. Dado que R1 es el único router en esta configuración, quiere que la configuración de alta disponibilidad realice una conmutación por error siempre que R1 no sea accesible desde el nodo principal actual. Puede configurar un monitor de ruta (por ejemplo, RM1 y RM2, respectivamente) en cada uno de los nodos para supervisar la accesibilidad de R1 desde ese nodo.

Flujo de red(/en-us/netscaler-gateway/media/ha-rm-ha-non-inc.png)

Con NS1 como nodo principal actual, el flujo de red es el siguiente:

1. El monitor de ruta RM1 en NS1 supervisa la tabla de enrutamiento interna de NS1 para la presencia de una entrada de ruta para el router R1. NS1 y NS2 intercambian mensajes de latido a través del conmutador SW1 o SW3 a intervalos regulares.
2. Si el conmutador SW1 falla, el protocolo de enrutamiento en NS1 detecta que R1 no es accesible y, por lo tanto, elimina la entrada de ruta para R1 de la tabla de enrutamiento interna. NS1 y NS2 intercambian mensajes de latido a través del conmutador SW3 a intervalos regulares.
3. Al detectar que la entrada de ruta para R1 no está presente en la tabla de enrutamiento interna, RM1 inicia una conmutación por error. Si la ruta a R1 está inactiva desde NS1 y NS2, la conmutación por error ocurre cada 180 segundos hasta que uno de los dispositivos pueda alcanzar R1 y restaurar la conexión.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

## Agregar o eliminar monitores de ruta

Cuando los dispositivos de un par de alta disponibilidad residen en redes diferentes, el estado de alta disponibilidad de NetScaler Gateway depende de si se puede acceder al dispositivo o no. En una configuración de alta disponibilidad entre redes, un monitor de ruta en cada NetScaler Gateway escanea la tabla de enrutamiento interna para asegurarse de que siempre haya una entrada para el otro NetScaler Gateway.

### Para agregar un monitor de ruta

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda Sistema y, a continuación, haga clic en Alta disponibilidad.
2. En el cuadro de diálogo Enlazar/Desenlazar monitores de ruta, en la ficha Monitores de ruta, haga clic en Acción y, a continuación, haga clic en Configurar.
3. En Especificar monitor de ruta, en Red, escriba la dirección IP de la red del otro dispositivo NetScaler Gateway.

   Para configurar una dirección IPv6, haga clic en IPv6 y, a continuación, escriba la dirección IP.
4. En Máscara de red, escriba la máscara de subred de la otra red, haga clic en Agregar y, a continuación, haga clic en Aceptar.

Cuando este procedimiento se completa, el monitor de ruta se enlaza a NetScaler Gateway.

Nota: Cuando un monitor de ruta no está enlazado a un NetScaler Gateway, el estado de alta disponibilidad de cualquiera de los dispositivos se determina por el estado de las interfaces.

### Para eliminar un monitor de ruta

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda Sistema y, a continuación, haga clic en Alta disponibilidad.
2. En la ficha Monitores de ruta, haga clic en Acción y, a continuación, haga clic en Configurar.
3. En Monitores de ruta configurados, seleccione el monitor, haga clic en Quitar y, a continuación, haga clic en Aceptar.

# Configuración de la redundancia de enlaces

La redundancia de enlaces agrupa las interfaces de red para evitar la conmutación por error debido a un fallo en una interfaz de red de un NetScaler Gateway que tiene otras interfaces en funcionamiento. El fallo de la primera interfaz en el NetScaler Gateway principal activa la conmutación por error, aunque la primera interfaz aún puede usar su segundo enlace para atender

© 1997–2026 Citrix Systems, Inc. All rights reserved.

las solicitudes de los usuarios. Al configurar la redundancia de enlaces, puede agrupar las dos interfaces en un conjunto de interfaces de conmutación por error, lo que evita que el fallo de un solo enlace provoque la conmutación por error al NetScaler Gateway secundario, a menos que todas las interfaces del NetScaler Gateway principal no funcionen.

Cada interfaz de un conjunto de interfaces de conmutación por error mantiene entradas de puente independientes. Las interfaces de monitorización que están habilitadas y de alta disponibilidad en un NetScaler Gateway que no están vinculadas a un conjunto de interfaces fallidas se conocen como interfaces críticas, porque si alguna de estas interfaces falla, se activa la conmutación por error.

## Para configurar la redundancia de enlaces

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda Sistema y, a continuación, haga clic en Alta disponibilidad.
2. En la ficha Conjunto de interfaces de conmutación por error, haga clic en Agregar.
3. En Nombre, escriba un nombre para el conjunto.
4. En Interfaces, haga clic en Agregar.
5. En Interfaces disponibles, seleccione una interfaz y, a continuación, haga clic en la flecha para mover la interfaz a Configurado.
6. Repita los pasos 4 y 5 para la segunda interfaz y, a continuación, haga clic en Crear.

Puede agregar tantas interfaces como necesite para la conmutación por error entre las interfaces.

## Para quitar interfaces del conjunto de interfaces de conmutación por error

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda Sistema y, a continuación, haga clic en Alta disponibilidad.
2. En la ficha Conjunto de interfaces de conmutación por error, seleccione un conjunto y, a continuación, haga clic en Quitar.

## Para quitar un conjunto de interfaces de conmutación por error

Si ya no necesita un conjunto de interfaz de conmutación por error, puede eliminarlo de NetScaler Gateway.

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda Sistema y, a continuación, haga clic en Alta disponibilidad.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. En la ficha Conjunto de interfaz de conmutación por error, seleccione un conjunto y, a continuación, haga clic en Eliminar.

## Comprensión de las causas de la conmutación por error

Los siguientes eventos pueden causar una conmutación por error en una configuración de alta disponibilidad:

1. Si el nodo secundario no recibe un paquete de latido del nodo principal durante un período de tiempo que excede el intervalo de inactividad establecido en el secundario. Para obtener más información sobre cómo configurar el intervalo de inactividad, consulte Configuración de intervalos de comunicación. Las posibles causas por las que un nodo no recibe paquetes de latido de un nodo par incluyen:
    - Un problema de configuración de red impide que los latidos atraviesen la red entre los nodos de alta disponibilidad.
    - El nodo par experimenta un fallo de hardware o software que hace que se congele (se cuelgue), se reinicie o, de otro modo, deje de procesar y reenviar paquetes de latido.
2. El nodo principal experimenta un fallo de hardware en su tarjeta SSL.
3. El nodo principal no recibe ningún paquete de latido en sus interfaces de red durante tres segundos.
4. En el nodo principal, falla una interfaz de red que no forma parte de un conjunto de interfaces de conmutación por error (FIS) o un canal de agregación de enlaces (LA) y tiene el Monitor de alta disponibilidad (HAMON) habilitado. Las interfaces están habilitadas, pero pasan a un estado INACTIVO.
5. En el nodo principal, fallan todas las interfaces de un FIS. Las interfaces están habilitadas, pero pasan a un estado INACTIVO.
6. En el nodo principal, falla un canal LA con HAMON habilitado. Las interfaces están habilitadas, pero pasan a un estado INACTIVO.
7. En el nodo principal, fallan todas las interfaces. En este caso, la conmutación por error se produce independientemente de la configuración de HAMON.
8. En el nodo principal, todas las interfaces se deshabilitan manualmente. En este caso, la conmutación por error se produce independientemente de la configuración de HAMON.
9. Se fuerza una conmutación por error emitiendo el comando de conmutación por error forzada en cualquiera de los nodos.
10. Un monitor de ruta que está vinculado al nodo principal pasa a estado INACTIVO.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

# Forzar la conmutación por error desde un nodo

Es posible que desee forzar una conmutación por error si, por ejemplo, necesita reemplazar o actualizar el nodo principal. Puede forzar la conmutación por error desde el nodo principal o el secundario. Una conmutación por error forzada no se propaga ni se sincroniza. Para ver el estado de sincronización después de una conmutación por error forzada, puede ver el estado del nodo.

Una conmutación por error forzada falla en cualquiera de las siguientes circunstancias:

- Fuerza la conmutación por error en un sistema independiente.
- El nodo secundario está inhabilitado.
- El nodo secundario está configurado para permanecer como secundario.

El dispositivo NetScaler Gateway muestra un mensaje de advertencia si detecta un problema potencial cuando ejecuta el comando de forzar conmutación por error. El mensaje incluye la información que activó la advertencia y solicita confirmación antes de continuar.

## Forzar la conmutación por error en el nodo principal o secundario

Si fuerza la conmutación por error en el nodo principal, el principal se convierte en el secundario y el secundario se convierte en el principal. La conmutación por error forzada solo es posible cuando el nodo principal puede determinar que el nodo secundario está ACTIVO.

Si el nodo secundario está INACTIVO, el comando de conmutación por error forzada devuelve el siguiente mensaje de error: "Operación no posible debido a un estado de par no válido. Rectifique y vuelva a intentarlo."

Si el sistema secundario está en estado de reclamación o inactivo, el comando devuelve el siguiente mensaje de error: `"Operation not possible now. Please wait for system to stabilize before retrying."`

Si ejecuta el comando de conmutación por error forzada desde el nodo secundario, el nodo secundario se convierte en principal y el nodo principal se convierte en secundario. Una conmutación por error forzada solo puede ocurrir si el estado del nodo secundario es bueno y el nodo no está configurado para permanecer como secundario.

Si el nodo secundario no puede convertirse en el nodo principal, o si el nodo secundario se configuró para permanecer como secundario (mediante la opción STAYSECONDARY), el nodo muestra el siguiente mensaje de error: "Operación no posible ya que mi estado no es válido. Consulte el nodo para obtener más información."

© 1997–2026 Citrix Systems, Inc. All rights reserved.

### Para forzar la conmutación por error en el nodo principal o en un nodo secundario

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda Sistema y, a continuación, haga clic en Alta disponibilidad.
2. En el panel de detalles, en la ficha Nodos, seleccione el nodo principal y, a continuación, en Acciones, haga clic en Forzar conmutación por error.
3. En el cuadro de diálogo Advertencia, haga clic en Sí.

## Forzar al nodo principal a permanecer como principal

En una configuración de alta disponibilidad, puede forzar a que el NetScaler Gateway principal permanezca como principal incluso después de una conmutación por error del dispositivo. Solo puede configurar esta opción en dispositivos NetScaler Gateway independientes y en el NetScaler Gateway que sea el dispositivo principal en un par de alta disponibilidad.

### Para forzar al nodo principal a permanecer como principal

1. En la utilidad de configuración, en la ficha Configuration (Configuración), en el panel de navegación, expanda System (Sistema) y, a continuación, haga clic en High Availability (Alta disponibilidad).
2. En el panel de detalles, en la ficha Nodes (Nodos), seleccione un nodo y, a continuación, haga clic en Edit (Modificar).
3. En High Availability Status (Estado de alta disponibilidad), haga clic en Stay Primary (Permanecer como principal) y, a continuación, haga clic en OK (Aceptar).

Puede borrar esta configuración solo mediante el siguiente comando:

```
clear configuration full
```

Los siguientes comandos no cambian la configuración de alta disponibilidad de NetScaler Gateway:

```
clear configuration basic
```

```
clear configuration extended
```

## Forzar que el nodo secundario permanezca secundario

En una configuración de alta disponibilidad, puede forzar que el NetScaler Gateway secundario permanezca secundario, independientemente del estado del NetScaler Gateway principal. Cuando

© 1997–2026 Citrix Systems, Inc. All rights reserved.

configura NetScaler Gateway para que permanezca secundario, este sigue siendo secundario incluso si el NetScaler Gateway principal falla.

Por ejemplo, en una configuración de alta disponibilidad existente, suponga que necesita actualizar el NetScaler Gateway principal y que este proceso lleva un tiempo determinado. Durante la actualización, el NetScaler Gateway principal puede dejar de estar disponible, pero no desea que el NetScaler Gateway secundario tome el control. Desea que permanezca como el NetScaler Gateway secundario, incluso si detecta un fallo en el NetScaler Gateway principal.

Si el estado de un NetScaler Gateway en un par de alta disponibilidad está configurado para permanecer secundario, no participa en las transiciones de la máquina de estados de alta disponibilidad. Puede comprobar el estado del NetScaler Gateway en la utilidad de configuración, en la pestaña **Nodos**.

Esta configuración funciona tanto en un NetScaler Gateway independiente como en uno secundario.

Cuando se configura el nodo de alta disponibilidad, no se propaga ni se sincroniza y solo afecta al NetScaler Gateway en el que se configura el ajuste.

### Para forzar que el nodo secundario permanezca secundario

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda Sistema y, a continuación, haga clic en Alta disponibilidad.
2. En el panel de detalles, en la ficha Nodos, seleccione un nodo y, a continuación, haga clic en Modificar.
3. En Estado de alta disponibilidad, haga clic en Permanecer secundario (Permanecer en modo de escucha) y, a continuación, haga clic en Aceptar.

### Para devolver NetScaler Gateway al servicio como un dispositivo de alta disponibilidad activo

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda Sistema y, a continuación, haga clic en Alta disponibilidad.
2. En el panel de detalles, en la ficha Nodos, seleccione el dispositivo que va a permanecer como nodo principal y, a continuación, haga clic en Abrir.
3. En Estado de alta disponibilidad, haga clic en Habilitado (Participar activamente en HA) y, a continuación, haga clic en Aceptar.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

# Uso de la agrupación en clúster

NetScaler Gateway se puede implementar en configuraciones de clúster para proporcionar un alto rendimiento, alta disponibilidad y escalabilidad para el tráfico de clientes VPN. En un clúster, un grupo de dispositivos o máquinas virtuales de NetScaler Gateway funciona como una única imagen de sistema para coordinar las sesiones de usuario y administrar el tráfico a los recursos de red. Un clúster de NetScaler Gateway se puede construir con un mínimo de dos y un máximo de 32 dispositivos o máquinas virtuales de NetScaler Gateway configurados como nodos de clúster.

Lea la documentación de NetScaler Clustering antes de empezar a configurar su clúster de NetScaler Gateway. Preste especial atención a los siguientes temas de esa documentación.

- Consulte (/es-es/citrix-adc/current-release/clustering.html) para verificar que los sistemas que planea usar cumplen los requisitos.
- Consulte (/es-es/citrix-adc/current-release/clustering/cluster-overview.html) para obtener una descripción de los conceptos de agrupación en clúster.
- Consulte (/es-es/citrix-adc/current-release/clustering/cluster-overview/cluster-node-states.html) para planificar la implementación e identificar cualquier advertencia que pueda ser relevante para su entorno.

Un clúster de NetScaler Gateway funciona como un clúster de NetScaler de tipo de configuración VIP con puntos.

**IMPORTANTE:**

El asistente de **XenApp y XenDesktop®** no es compatible con la agrupación en clúster y, por lo tanto, no encontrará el asistente de **XenApp y XenDesktop** en la sección **GUI > Panel de navegación > Integrar con productos NetScaler**.

## Configuración de clúster

Las tareas principales para configurar el clúster de NetScaler Gateway son:

1. Decida qué dispositivo NetScaler Gateway o máquina virtual es el coordinador de configuración y cree una instancia de clúster en ese sistema (si aún no existe).
2. Una los sistemas NetScaler Gateway al clúster como nodos.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. Cree un grupo de nodos en la instancia del clúster, con la opción STICKY establecida.
4. Enlace un único nodo de clúster al grupo de nodos del clúster.
5. Configure un servidor virtual de NetScaler Gateway en el coordinador de configuración y enlácelo al grupo de nodos del clúster.

Existen varios métodos para configurar un clúster de NetScaler. El siguiente conjunto de tareas utiliza el método más directo disponible en la utilidad de configuración.

## Para crear una instancia de clúster de NetScaler Gateway mediante la utilidad de configuración

Una vez que tenga los detalles de la implementación en orden, comience la configuración en el NetScaler Gateway que es el coordinador de configuración.

Precaución: La creación de la instancia del clúster borra la configuración. Si necesita guardar la configuración del sistema existente como referencia, archive una copia antes de continuar con la configuración del clúster. Cualquier configuración existente que se vaya a utilizar en el clúster se puede volver a aplicar en el coordinador de configuración una vez establecido el clúster.

1. Inicie sesión en la utilidad de configuración de NetScaler en la dirección NSIP.
2. Expanda el nodo Sistema y, a continuación, el subnodo Clúster.
3. En el panel de detalles, haga clic en Administrar clúster.
4. En el cuadro de diálogo Configuración del clúster, establezca los parámetros necesarios para crear el clúster.
    a. Introduzca un ID de instancia de clúster. El ID de instancia de clúster es el identificador numérico de la instancia de clúster. El valor predeterminado es 1, pero puede establecerlo en cualquier número del 1 al 16.
    b. Introduzca la dirección IP del clúster. La dirección IP del clúster es la dirección IP del coordinador de configuración del clúster, que es la dirección IP de administración del clúster.
    c. Seleccione la interfaz de backplane preferida. Esta es la interfaz de NetScaler Gateway que se utilizará para la comunicación entre los nodos del clúster.
5. Haga clic en Crear.
6. Cuando se le solicite confirmar el reinicio del sistema, haga clic en Sí.
7. Una vez que el nodo esté ACTIVO y la sincronización sea correcta, desde la dirección IP del clúster, cambie las credenciales RPC tanto para el nodo como para la dirección IP del clúster.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Para obtener más información sobre cómo cambiar una contraseña de nodo RPC, consulte Cambiar una contraseña de nodo RPC.

8. Espere a que el sistema se reinicie. Una vez disponible, inicie sesión en la utilidad de configuración en la dirección IP del clúster configurada en el paso 4(2).

**Nota:** En el panel de **detalles de información del sistema**, el nodo local en la dirección NSIP se informa como coordinador de configuración. Esto confirma que la instancia base del clúster está ahora operativa.

El nodo local del coordinador de configuración se añade automáticamente al clúster. Se pueden añadir más nodos en la siguiente tarea.

## Adición de nodos a un clúster de NetScaler Gateway

Una vez establecida la instancia del clúster, puede empezar a añadir otros nodos de NetScaler Gateway al clúster.

Para añadir más sistemas NetScaler Gateway al clúster, puede utilizar la utilidad de configuración para configurar de forma remota los ajustes de creación de nodos de clúster y de unión al clúster.

**Nota**: La adición de nodos al clúster debe completarse antes de configurar su configuración de NetScaler Gateway. De esta manera, no tendrá que repetir la configuración de NetScaler Gateway si algo sale mal con la configuración de su clúster y desea eliminar el clúster y empezar de nuevo.

1. Inicie sesión en la utilidad de configuración de NetScaler en la dirección IP del clúster.
2. Expanda el nodo **Sistema** y luego el subnodo Clúster.
3. En el panel de detalles, haga clic en **Administrar clúster**.
4. En el panel de detalles de Nodos de clúster, haga clic en **Agregar**.
5. En el panel **Crear nodo de clúster**, introduzca un ID de nodo único para este nodo.
6. Introduzca la dirección IP de NetScaler del sistema que se va a agregar como nodo de clúster.
7. En el panel **Credenciales de nodo de clúster**, introduzca el nombre de usuario y la contraseña de NetScaler Gateway para el sistema NetScaler Gateway remoto.
8. En el panel Credenciales del coordinador de configuración, introduzca la contraseña del usuario autorizado local.
9. Haga clic en **Crear**.
10. Cuando se le solicite, haga clic en **SÍ** para permitir que se guarde la configuración del sistema y realizar un reinicio en caliente del NetScaler Gateway remoto.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

11. Una vez que el nodo esté ACTIVO y la sincronización sea correcta, desde la dirección IP del clúster, cambie las credenciales de RPC tanto para el nodo como para la dirección IP del clúster. Para obtener más información sobre cómo cambiar una contraseña de nodo RPC, consulte Cambiar una contraseña de nodo RPC.

Repita los pasos 4 a 11 para cada sistema NetScaler Gateway remoto adicional que desee configurar como nodo de clúster.

verificar que los nodos del clúster estén incluidos en la Lista de nodos activos en el panel de detalles de Nodos de clúster. Si falta algún nodo, repita los pasos 4 a 10 hasta que se listen todos los nodos necesarios.

## Creación de un grupo de nodos de clúster

Una vez que se hayan agregado los nodos del clúster, se puede crear un grupo de nodos del clúster.

1. Inicie sesión en la utilidad de configuración de NetScaler en la dirección IP del clúster.
2. Expanda el nodo **Sistema** y, a continuación, el subnodo Clúster.
3. Haga clic en **Grupos de nodos**.
4. En el panel de detalles, haga clic en **Agregar**.
5. Introduzca un nombre para el grupo de nodos del clúster.
6. Seleccione la opción **Sticky** para admitir el tipo de servidor virtual de NetScaler Gateway.
7. Haga clic en **Continuar**.

El grupo de nodos del clúster ya está establecido. Antes de salir de esta área de la utilidad de configuración, puede vincular el nodo local de NetScaler Gateway al nuevo grupo de nodos del clúster. Este es el único nodo vinculado al grupo de clústeres.

## Vincular el nodo de clúster local al grupo de nodos del clúster

Dado que una configuración de clúster de NetScaler Gateway es de tipo 'spotted', solo se puede vincular un nodo al grupo de nodos. El siguiente procedimiento vincula el nodo local del coordinador de configuración al grupo de nodos, pero cualquier nodo del clúster se puede utilizar para esta vinculación.

1. En el panel Avanzado, expanda Nodos de clúster.
2. En el panel central Nodos de clúster, seleccione Sin nodo de clúster.
3. En la pantalla de configuración del nodo de clúster, haga clic en Vincular.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. Seleccione el nodo local representado por la dirección NSIP para este sistema NetScaler Gateway.
5. Haga clic en Insertar.
6. Haga clic en Aceptar.
7. Haga clic en Listo.

El clúster ya está rellenado y listo para compartir un servidor virtual de NetScaler Gateway según lo configurado por la siguiente tarea.

## Vinculación de un servidor virtual de NetScaler Gateway al grupo de nodos del clúster

Una vez establecido un clúster, puede proceder a crear la configuración de NetScaler Gateway que el despliegue del clúster pretende servir. Para vincular la configuración al clúster, debe crear el servidor virtual de NetScaler Gateway y vincularlo a un grupo de nodos del clúster que esté configurado como tipo Sticky. Una vez que el servidor virtual esté vinculado al grupo de nodos del clúster, puede continuar configurando NetScaler Gateway.

Si se configuran varios servidores virtuales de NetScaler Gateway, estos también deben vincularse al grupo de nodos del clúster.

**Nota:** Si los servidores virtuales de NetScaler Gateway aún no se han configurado, es posible que primero deba habilitar las funciones de NetScaler Gateway y Autenticación, Autorización y Auditoría en **Sistema > Configuración > Configurar funciones básicas**.

1. Inicie sesión en la utilidad de configuración de NetScaler en la dirección IP del clúster.
2. Expanda el nodo **Sistema**, y luego el subnodo Clúster.
3. Haga clic en **Grupos de nodos**.
4. En el panel **Grupo de nodos**, seleccione el nombre del grupo de nodos deseado y, a continuación, haga clic en **Editar**.
5. En el panel **Avanzado** de la derecha, expanda la opción **Servidores virtuales** y, a continuación, haga clic en el icono + para agregar un servidor virtual.
6. Elija el tipo de servidor virtual VPN y, a continuación, haga clic en **Continuar**.
7. Haga clic en **Vincular**.
8. Si el servidor virtual necesario aparece en la lista, selecciónelo, haga clic en **Insertar** y, a continuación, haga clic en **Aceptar**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

9. Si tiene que crear un nuevo servidor virtual, haga clic en **Agregar**. Continúe con la configuración del servidor virtual de NetScaler. Como mínimo, todo lo que se necesita es crear el servidor virtual para que pueda vincularse al grupo de nodos del clúster.
10. Una vez que el servidor virtual esté disponible en la lista de servidores virtuales de NetScaler Gateway, selecciónelo y, a continuación, haga clic en **Insertar**.
11. Haga clic en **Aceptar**.
12. Haga clic en **Listo**.

**Nota**: Si hay varios servidores virtuales de NetScaler Gateway configurados, estos también deben vincularse al grupo de nodos del clúster utilizando este mismo método.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

# Unified Gateway

## NetScaler con Unified Gateway: una única URL

NetScaler con Unified Gateway permite un acceso seguro simplificado a cualquier aplicación a través de una única URL para usuarios de escritorio y móviles. Detrás de esta única URL, los administradores tienen un único punto para la configuración, la seguridad y el control del acceso remoto a las aplicaciones. Y los usuarios remotos tienen una experiencia mejorada con un inicio de sesión único sin interrupciones para todas las aplicaciones que necesitan, junto con la facilidad de uso de iniciar y cerrar sesión una sola vez.

Para lograr esto, NetScaler con Gateway, junto con las capacidades de conmutación de contenido de NetScaler y su amplia infraestructura de autenticación, proporciona acceso a sitios y aplicaciones organizacionales a través de esta única URL. Además, los usuarios remotos pueden usar dispositivos móviles iOS o Android y sistemas Linux, PC o Mac con el cliente Citrix Secure Access para un acceso uniforme a la URL de Unified Gateway, dondequiera que se encuentren.

Una implementación de Unified Gateway permite el acceso con una única URL a las siguientes categorías de aplicaciones:

- Aplicaciones de intranet.
- Aplicaciones sin cliente
- Aplicación de software como servicio
- Aplicaciones preconfiguradas servidas por NetScaler
- Aplicaciones publicadas de Citrix Virtual Apps and Desktops

Las **aplicaciones de intranet** pueden ser cualquier aplicación web que resida dentro de la red empresarial segura. Estos son recursos internos como un sitio de intranet organizacional, una aplicación de seguimiento de errores o una wiki.

Normalmente, también residen dentro de la red empresarial segura, las **aplicaciones sin cliente** a las que Unified Gateway proporciona acceso con una única URL son Outlook Web Access y SharePoint. Estas aplicaciones proporcionan acceso al correo electrónico de Exchange y a los recursos del equipo sin software cliente dedicado, que deben estar disponibles para los usuarios remotos.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Las **aplicaciones SaaS**, también conocidas comúnmente como aplicaciones en la nube, son aplicaciones externas basadas en la nube de las que dependen las organizaciones, como ShareFile, Salesforce o NetSuite. Se admite el inicio de sesión único basado en SAML con aquellas aplicaciones SaaS que lo ofrecen.

Algunas organizaciones pueden tener **aplicaciones preconfiguradas servidas por NetScaler** implementadas en una configuración de equilibrio de carga de NetScaler. A menudo, esto también se conoce como aplicación de 'proxy inverso'. Unified Gateway admite estas aplicaciones cuando un servidor virtual para la implementación reside en la misma instancia o dispositivo de NetScaler Unified Gateway. Estas aplicaciones pueden tener su propia configuración de autenticación, que es independiente de la configuración de Unified Gateway.

Cualquier **aplicación publicada de Citrix Virtual Apps and Desktops** puede estar disponible a través de una URL de Unified Gateway. Opcionalmente, se pueden aplicar políticas de SmartAccess y SmartControl para un control de acceso y políticas granulares a estos recursos.

## El asistente de configuración de Unified Gateway

El método recomendado para configurar una implementación de NetScaler con Unified Gateway es usar el asistente de configuración de Unified Gateway. El asistente le guía a través de la configuración y crea todos los servidores virtuales, directivas y expresiones necesarios, y aplica la configuración según los detalles proporcionados. Después de la configuración inicial, el asistente se puede usar para administrar su implementación y supervisar su funcionamiento.

**NOTA:**

El asistente de configuración de Unified Gateway no realiza una configuración inicial del sistema. Su dispositivo NetScaler Gateway o instancia VPX debe tener la instalación básica completada antes de configurar Unified Gateway. Consulte las instrucciones de instalación de Configuración de NetScaler Gateway con el asistente de configuración inicial para completar la configuración básica.

Los elementos de Unified Gateway configurados por el asistente son:

- El servidor virtual principal de Unified Gateway
- Un certificado de servidor SSL para el servidor virtual de Unified Gateway
- Una configuración de autenticación principal y cualquier configuración de autenticación secundaria opcional
- Una selección de tema de portal y personalización opcional

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Las aplicaciones de usuario a las que se accederá a través del portal de Unified Gateway

Para cada uno de estos elementos, debe proporcionar información de configuración. Para una implementación básica de Unified Gateway, se necesita la siguiente información.

- Para el servidor virtual principal de Unified Gateway, la dirección IP pública y el número de puerto IP para la implementación. Esta es la dirección IP que se resuelve en DNS al nombre de host de la URL de Unified Gateway. Por ejemplo, si la URL de su implementación de Unified Gateway es `https://mycompany.com/`, la dirección IP debe resolverse en mycompany.com.
- El certificado de servidor SSL firmado para la implementación. NetScaler Gateway admite certificados con formato PEM o PFX.
- Información del servidor de autenticación principal. Los sistemas de autenticación admitidos para esta configuración de autenticación son LDAP/Active Directory, RADIUS y basados en certificados. También se puede crear una configuración de autenticación secundaria LDAP o RADIUS. Se debe proporcionar la dirección IP del servidor de autenticación junto con las credenciales de administrador o los atributos de directorio relevantes. Para la autenticación de certificados, se deben proporcionar los atributos del certificado del dispositivo y un certificado de CA.
- Se puede seleccionar un tema de portal. Si se desea un diseño de portal personalizado o de marca, se pueden cargar gráficos personalizados en el sistema con el asistente.
- Para las aplicaciones de usuario basadas en web, se deben especificar las URL de las aplicaciones individuales. Para las aplicaciones web que van a utilizar la autenticación de inicio de sesión único (SSO) de SAML, la utilidad recopila la URL del Servicio de consumidor de aserciones junto con otros parámetros SAML opcionales. Reúna los detalles de configuración con antelación para las aplicaciones que utilizan un sistema de autenticación SAML.
- Para que los recursos publicados de Citrix Virtual Apps and Desktops estén disponibles a través de la implementación de Unified Gateway, debe especificar el punto de integración (StoreFront). La utilidad requiere el nombre de dominio completo del punto de integración, la ruta del sitio, el dominio de inicio de sesión único, la URL del servidor Secure Ticket Authority (STA) y otros, según el tipo de punto de integración.

## Administración de configuración adicional

Para la configuración específica del sitio no disponible en la utilidad de configuración de Unified Gateway, como la configuración SSL alternativa o las directivas de sesión, puede administrar la configuración necesaria en la utilidad de configuración de NetScaler Gateway. Puede modificar

© 1997–2026 Citrix Systems, Inc. All rights reserved.

esta configuración en los servidores virtuales de conmutación de contenido o VPN una vez que hayan sido creados por la utilidad de configuración de Unified Gateway.

## Servidor virtual de conmutación de contenido

Esta es la entidad de configuración de NetScaler detrás de la dirección IP principal y la URL de la implementación. Los certificados y parámetros del servidor SSL se administran en este servidor virtual. Como este servidor virtual es el host de red que responde a la implementación, la respuesta del servidor ICMP y el estado RHI se pueden modificar en este servidor virtual, si es necesario. El servidor virtual de conmutación de contenido se encuentra en la ficha **Configuración** en **Administración del tráfico** > **Conmutación de contenido** > **Servidores virtuales**.

**IMPORTANTE:**

Al actualizar su entorno de Unified Gateway a la versión 13.0 compilación 58.x o posterior, el conmutador DTLS se inhabilita en el servidor virtual de conmutación de contenido que se configuró antes del servidor virtual de puerta de enlace o VPN. Habilite manualmente el conmutador DTLS en el servidor virtual de conmutación de contenido después de la actualización. No habilite el conmutador DTLS si está utilizando el asistente para la configuración.

### Servidor virtual VPN

Todos los demás parámetros, perfiles y enlaces de directivas de VPN para la configuración de Unified Gateway se administran en este servidor virtual, incluida la configuración de autenticación principal. Esta entidad se administra en la ficha **Configuración** en **NetScaler Gateway** > **Servidores virtuales**. El nombre del servidor virtual VPN relevante incluye el nombre asignado al servidor virtual de conmutación de contenido durante la configuración inicial de Unified Gateway.

**NOTA:**

Los servidores virtuales VPN creados para una implementación de Unified Gateway no son direccionables y se les asigna la dirección IP 0.0.0.0.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

# Preguntas frecuentes sobre Unified Gateway

## ¿Qué es Unified Gateway?

Unified Gateway es una nueva función de la versión 11.0 de NetScaler que proporciona la capacidad de recibir tráfico en un único servidor virtual (denominado servidor virtual Unified Gateway) y, a continuación, dirigir internamente ese tráfico, según corresponda, a los servidores virtuales que están enlazados al servidor virtual Unified Gateway.

La función Unified Gateway permite a los usuarios finales acceder a varios servicios mediante una única dirección IP o URL (asociada al servidor virtual Unified Gateway). Los administradores pueden liberar direcciones IP y simplificar la configuración de la implementación de NetScaler Gateway.

Cada servidor virtual Unified Gateway puede actuar como front-end de un servidor virtual NetScaler Gateway junto con cero o más servidores virtuales de equilibrio de carga como parte de una formación. Unified Gateway funciona mediante la función de conmutación de contenido del dispositivo NetScaler.

Algunos ejemplos de implementaciones de Unified Gateway:

- Servidor virtual Unified Gateway ->
- Servidor virtual Unified Gateway ->
- Servidor virtual Unified Gateway ->
- Servidor virtual Unified Gateway ->

Cada uno de los servidores virtuales de equilibrio de carga puede ser cualquier servidor de equilibrio de carga estándar que aloje un servicio de back-end, como Microsoft Exchange o Citrix® ShareFile.

## ¿Por qué usar Unified Gateway?

La función Unified Gateway permite a los usuarios finales acceder a varios servicios mediante una única dirección IP o URL (asociada al servidor virtual Unified Gateway). Para los administradores, la ventaja es que pueden liberar direcciones IP y simplificar la configuración de la implementación de NetScaler Gateway.

## ¿Puede haber más de un servidor virtual Unified Gateway?

Sí. Puede haber tantos servidores virtuales Unified Gateway como necesite.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

## ¿Por qué se necesita la conmutación de contenido para Unified Gateway?

La función de conmutación de contenido es necesaria porque el servidor virtual de conmutación de contenido es el que recibe el tráfico y lo dirige internamente al servidor virtual apropiado. El servidor virtual de conmutación de contenido es el componente principal de la función Unified Gateway.

## En versiones anteriores a la 11.0, la conmutación de contenido se puede utilizar para recibir tráfico para varios servidores virtuales. ¿Ese uso también se denomina Unified Gateway?

El uso de un servidor virtual de conmutación de contenido para recibir tráfico para varios servidores virtuales es compatible con versiones anteriores a la 11.0. Sin embargo, la conmutación de contenido no puede dirigir el tráfico a un servidor virtual de NetScaler Gateway.

Las mejoras en la versión 11.0 permiten que un servidor virtual de conmutación de contenido dirija el tráfico a cualquier servidor virtual, incluido un servidor virtual de NetScaler Gateway.

## ¿Qué ha cambiado con las directivas de conmutación de contenido en Unified Gateway?

1. Se agrega un nuevo parámetro de línea de comandos "-targetVserver" para la acción de conmutación de contenido. El nuevo parámetro se utiliza para especificar el servidor virtual de NetScaler Gateway de destino. Ejemplo:

   añadir acción cs UG_CSACT_MyUG -targetVserver UG_VPN_MyUG

   En la utilidad de configuración de NetScaler Gateway, la acción de conmutación de contenido tiene una nueva opción, Target Virtual Server, que puede hacer referencia a un servidor virtual de NetScaler Gateway.
2. Se puede utilizar una nueva expresión de directiva avanzada, is_vpn_url, para hacer coincidir las solicitudes específicas de NetScaler Gateway y de autenticación.

## ¿Qué funciones de NetScaler Gateway no son compatibles actualmente con Unified Gateway?

Todas las funciones son compatibles con Unified Gateway. Sin embargo, se ha informado de un problema menor (ID de problema 544325) con el inicio de sesión nativo a través del plug-in VPN. En este caso, el inicio de sesión único (SSO) sin interrupciones no funciona.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

## Con Unified Gateway, ¿cuál es el comportamiento de los escaneos de EPA?

Con Unified Gateway, el análisis de puntos finales se activa solo para los métodos de acceso de NetScaler Gateway, no para el acceso de NetScaler AAA TM. Si un usuario intenta acceder a un servidor virtual de NetScaler AAA TM, aunque la autenticación se realice en el servidor virtual de NetScaler Gateway, el escaneo de EPA no se activa. Sin embargo, si el usuario intenta obtener acceso VPN sin cliente/VPN completa, se activa el escaneo de EPA configurado. En ese caso, se realiza la autenticación o el SSO sin interrupciones.

## ¿Cuáles son los requisitos de licencia para Unified Gateway?

Unified Gateway solo es compatible con licencias Advanced y Premium. No está disponible para ediciones solo de NetScaler Gateway o de licencia Standard.

## ¿El servidor virtual de NetScaler Gateway utilizado con Unified Gateway necesita una configuración de IP/Puerto/SSL?

Para un servidor virtual de NetScaler Gateway utilizado con el servidor virtual de Unified Gateway, no se necesita una configuración de IP/Puerto/SSL en el servidor virtual de NetScaler Gateway. Sin embargo, para la funcionalidad de proxy RDP, puede vincular el mismo certificado de servidor SSL/TLS al servidor virtual de NetScaler Gateway.

## ¿Necesito reaprovisionar los certificados SSL/TLS que están en el servidor virtual de NetScaler Gateway para usarlos con un servidor virtual de Unified Gateway?

No es necesario reaprovisionar los certificados que están actualmente vinculados a su servidor virtual de NetScaler Gateway. Puede reutilizar cualquier certificado SSL existente y vincularlos al servidor virtual de Unified Gateway.

## ¿Cuál es la diferencia entre una URL única y una implementación de varios hosts? ¿Cuál necesito?

Una URL única se refiere a la capacidad del servidor virtual de Unified Gateway para manejar el tráfico de un nombre de dominio completo (FQDN). Esta restricción existe cuando Unified Gateway utiliza un certificado de servidor SSL/TLS cuyo asunto de certificado está rellenado con el FQDN. Por ejemplo: ug.citrix.com

Si Unified Gateway utiliza un certificado de servidor comodín, puede manejar el tráfico de varios subdominios. Por ejemplo: *.citrix.com

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Otra opción es la configuración SSL/TLS con la funcionalidad de Indicador de Nombre de Servidor (SNI) para permitir la vinculación de varios certificados de servidor SSL/TLS. Ejemplos: auth.citrix.com, auth.citrix.de, auth.citrix.co.uk, auth.citrix.co.jp

Un solo host frente a varios hosts es análogo a la forma en que los sitios web se alojan típicamente en un servidor web (por ejemplo, el servidor HTTP Apache o Microsoft Internet Information Services (IIS)). Si hay un solo host, puede usar una ruta de sitio para cambiar el tráfico de la misma manera que usa un alias o un "directorio virtual" en Apache. Si hay varios hosts, usa un encabezado de host para cambiar el tráfico de manera similar a como usa los Hosts Virtuales en Apache.

## ¿Qué mecanismos de autenticación se pueden usar con Unified Gateway?

Todos los mecanismos de autenticación existentes que son compatibles con NetScaler Gateway también lo son con Unified Gateway.

Estos incluyen LDAP, RADIUS, SAML, Kerberos, Autenticación basada en certificados, y así sucesivamente.

Cualquier mecanismo de autenticación configurado en el servidor virtual de NetScaler Gateway antes de la actualización se utiliza automáticamente cuando el servidor virtual de NetScaler Gateway se coloca detrás del servidor virtual de Unified Gateway. No hay pasos de configuración adicionales involucrados, aparte de asignar una dirección IP no direccionable (0.0.0.0) al servidor virtual de NetScaler Gateway.

## ¿Qué es la autenticación “SelfAuth”?

SelfAuth no es un tipo de autenticación por sí mismo. SelfAuth describe cómo se crea una URL. Un nuevo parámetro de línea de comandos, `ssotype`, está disponible para la configuración de URL de VPN. Ejemplo:

```
> add vpn url RGB RGB "http://blue.citrix.lab/" -vServerName Blue -ssotype selfauth
```

SelfAuth es uno de los valores del parámetro `ssotype`. Este tipo de URL se puede utilizar para acceder a recursos que no están en el mismo dominio que el servidor virtual de Unified Gateway. La configuración se puede ver en la utilidad de configuración al configurar un marcador.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

## ¿Qué es la autenticación «StepUp»?

When extra, more secure levels of authentication are required for accessing a NetScaler AAA TM resource, you can use StepUp authentication. On the command line, use an authnProfile command to set the authenticationLevel parameter. Example:

```
add authentication authnProfile AuthProfile -authnVsName AAATMVserver
-AuthenticationHost auth.citrix.lab -AuthenticationDomain citrix.lab **-
**AuthenticationLevel 100
```

Este perfil de autenticación está vinculado al servidor virtual de equilibrio de carga.

## Is StepUp authentication supported for NetScaler AAA TM virtual servers?

Sí, es compatible.

## ¿Qué es `login once/logout once`?

`Login Once`: Los usuarios de VPN inician sesión una vez en un servidor virtual NetScaler AAA TM o NetScaler Gateway. Y a partir de entonces, los usuarios de VPN tienen acceso sin interrupciones a todas las aplicaciones empresariales/en la nube/web. El usuario no necesita volver a autenticarse. Sin embargo, la reautenticación se realiza en casos especiales, como NetScaler AAA TM StepUp.

`Logout Once`: Después de crear la primera sesión de NetScaler AAA TM o NetScaler Gateway, se utiliza para crear sesiones posteriores de NetScaler AAA TM o NetScaler Gateway para ese usuario. Si alguna de esas sesiones se cierra, el dispositivo NetScaler también cierra las demás aplicaciones o sesiones del usuario.

## ¿Se pueden especificar políticas de autenticación comunes a nivel de Unified Gateway con un servidor virtual de equilibrio de carga NetScaler AAA TM específicamente autenticado y vinculado a nivel de servidor virtual de equilibrio de carga? ¿Cuáles son los pasos de configuración para admitir este caso de uso?

Si necesita especificar políticas de autenticación separadas para el servidor virtual NetScaler AAA TM detrás de Unified Gateway, necesita tener un servidor virtual de autenticación separado y direccionable de forma independiente (similar a la configuración ordinaria de NetScaler AAA TM). La configuración del host de autenticación en el servidor virtual de equilibrio de carga debe apuntar a este servidor virtual de autenticación.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

## ¿Cómo se configura Unified Gateway para que los servidores virtuales de NetScaler AAA TM vinculados tengan sus propias políticas de autenticación?

En este escenario, el servidor de equilibrio de carga debe tener la opción FQDN de autenticación configurada para apuntar al servidor virtual de NetScaler AAA TM. El servidor virtual de NetScaler AAA TM debe tener una dirección IP independiente y ser accesible desde NetScaler y los clientes.

## ¿Se requiere un servidor virtual de autenticación NetScaler AAA TM para autenticar a los usuarios que acceden a través de un servidor virtual de Unified Gateway?

No. El servidor virtual de NetScaler Gateway autentica incluso a los usuarios de NetScaler AAA TM.

## ¿Dónde se especifican las directivas de autenticación de NetScaler Gateway: en el servidor virtual de Unified Gateway o en el servidor virtual de NetScaler Gateway?

Las directivas de autenticación deben vincularse al servidor virtual de NetScaler Gateway.

## ¿Cómo se habilita la autenticación en los servidores virtuales de NetScaler AAA TM detrás de un servidor virtual de conmutación de contenido de Unified Gateway?

Habilite la autenticación en NetScaler AAA TM y apunte el host de autenticación al FQDN de conmutación de contenido de Unified Gateway.

## ¿Cómo agrego servidores virtuales TM detrás de la conmutación de contenido (URL única frente a varios hosts)?

No hay diferencia entre agregar los servidores virtuales de NetScaler AAA TM para una URL única y agregarlos para varios hosts. En cualquier caso, el servidor virtual se agrega como destino en una acción de conmutación de contenido. La diferencia entre URL única y varios hosts se implementa mediante reglas de directiva de conmutación de contenido.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

## ¿Qué sucede con las directivas de autenticación vinculadas a un servidor virtual de equilibrio de carga de NetScaler AAA TM si ese servidor virtual se mueve detrás de un servidor virtual de Unified Gateway?

Las directivas de autenticación se asocian al servidor virtual de autenticación, y este, a su vez, al de equilibrio de carga. Para el servidor virtual de Unified Gateway, Citrix recomienda que el de NetScaler Gateway sea el único punto de autenticación, lo que elimina la necesidad de autenticar en un servidor virtual de autenticación (o incluso la necesidad de uno específico). Apuntar el host de autenticación al FQDN del servidor virtual de Unified Gateway garantiza que la autenticación la realice el de NetScaler Gateway. Si se apunta el host de autenticación a la conmutación de contenido para Unified Gateway y aún hay un servidor virtual de autenticación vinculado, las directivas de autenticación asociadas a este se ignoran. Sin embargo, si se apunta un host de autenticación a un servidor virtual de autenticación independiente y direccionable, las directivas de autenticación vinculadas surten efecto.

## ¿Cómo se configuran las directivas de sesión para las sesiones de NetScaler AAA TM?

Si, en Unified Gateway, no se especifica ningún servidor virtual de autenticación para el servidor virtual de NetScaler AAA TM, las sesiones de NetScaler AAA TM heredan las directivas de sesión de NetScaler Gateway. Si se especifica el servidor virtual de autenticación, se aplican las directivas de sesión de NetScaler AAA TM vinculadas a ese servidor virtual.

## ¿Cuáles son los cambios en el portal de NetScaler Gateway en NetScaler 11.0?

En las versiones de NetScaler anteriores a la 11.0, se podía configurar una única personalización del portal a nivel global. Cada servidor virtual de gateway en un dispositivo NetScaler dado utiliza la personalización global del portal.

En NetScaler 11.0, con la función de temas del portal, puede configurar varios temas del portal. Los temas se pueden vincular globalmente o a servidores virtuales específicos.

## ¿NetScaler 11.0 admite la personalización del portal de NetScaler Gateway?

Mediante la utilidad de configuración, puede usar la nueva función de temas del portal para personalizar y crear los temas del portal por completo. Puede cargar diferentes imágenes, establecer esquemas de color, cambiar etiquetas de texto, etc.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Las páginas del portal que se pueden personalizar son:

- Inicio de sesión
- Página de análisis de puntos finales
- Página de error de análisis de puntos finales
- Página posterior al análisis de puntos finales
- Página de conexión VPN
- Página de inicio del portal

Con esta versión, puede personalizar los servidores virtuales de NetScaler Gateway con diseños de portal únicos.

## ¿Se admiten los temas del portal en implementaciones de alta disponibilidad o clúster de NetScaler?

Sí. Los temas del portal son compatibles con las implementaciones de alta disponibilidad y clúster de NetScaler.

## ¿Se migrarán mis personalizaciones como parte del proceso de actualización de NetScaler 11.0?

No. Las personalizaciones existentes en la página del portal de NetScaler Gateway que se invocan mediante la modificación del archivo rc.conf/rc.netscaler o mediante el uso de la funcionalidad de temas personalizados en 10.1/10.5 no se migrarán automáticamente al actualizar a NetScaler 11.0.

## ¿Hay algún paso previo a la actualización que seguir para preparar los temas del portal en NetScaler 11.0?

Cualquier personalización existente debe eliminarse de los archivos rc.conf o rc.netscaler.

La otra opción es que, si se utilizan temas personalizados, deben asignarse a la configuración predeterminada:

1. Vaya a **Configuración > NetScaler Gateway > Configuración global**
2. Haga clic en **Cambiar configuración global**.
3. Haga clic en **Experiencia del cliente** y seleccione **Predeterminado** en la lista **Tema de la interfaz de usuario**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

## Tengo personalizaciones almacenadas en la instancia de NetScaler, invocadas por rc.conf o rc.netscaler. ¿Cómo me muevo a los temas del portal?

El documento Crear un tema personalizado para la página de inicio de sesión de Citrix Gateway detalla dicha configuración para las versiones de NetScaler 9.3 y 10.0 hasta la compilación 10.0 73.5001.e. Desde la compilación 10.0 73.5002.e de NetScaler 10.0 (incluidas 10.1 y 10.5), el parámetro UITHEME CUSTOM ha estado disponible para ayudar a los clientes a conservar sus personalizaciones entre reinicios. Si las personalizaciones se almacenan en el disco duro de NetScaler y desea seguir utilizándolas, haga una copia de seguridad de los archivos GUI de la versión 11.0 e insértelos en el archivo de tema personalizado existente. Si desea pasar a los temas del portal, primero debe anular la configuración del parámetro UITHEME en la Configuración global o en el perfil de sesión, en **Experiencia del cliente**. O bien, puede establecerlo en DEFAULT o GREENBUBBLE. Entonces podrá empezar a crear y vincular un tema del portal.

## ¿Cómo puedo exportar mis personalizaciones actuales y guardarlas antes de actualizar a NetScaler 11.0? ¿Puedo mover los archivos exportados a otro dispositivo NetScaler?

Los archivos personalizados que se cargaron en la carpeta **ns_gui_custom** están en el disco y persisten durante las actualizaciones. Sin embargo, es posible que estos archivos no sean totalmente compatibles con el nuevo kernel de NetScaler 11.0 y otros archivos GUI que forman parte del kernel. Por lo tanto, Citrix recomienda hacer una copia de seguridad de los archivos GUI de la versión 11.0 y personalizar las copias de seguridad.

Además, no hay ninguna utilidad en la utilidad de configuración para exportar la carpeta **ns_custom_gui** a otro dispositivo NetScaler. Utilice SSH o una utilidad de transferencia de archivos como WinSCP para extraer los archivos de la instancia de NetScaler.

## ¿Se admiten los temas del portal para los servidores virtuales NetScaler AAA TM?

Sí. Los temas del portal son compatibles con los servidores virtuales NetScaler AAA TM.

## ¿Qué cambió en la función de proxy RDP para NetScaler Gateway 11.0?

Se han realizado muchas mejoras en el proxy RDP desde la versión de mejora de NetScaler 10.5.e. En NetScaler 11.0, esta función está disponible desde la primera compilación publicada.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

### Cambios en las licencias

La función de proxy RDP en NetScaler 11.0 solo se puede usar con las ediciones Premium y Advanced. Se deben obtener licencias de usuario concurrente de Citrix (CCU) para cada usuario.

### Comando de habilitación

En NetScaler 10.5.e no existía ningún comando para habilitar el proxy RDP. En NetScaler 11.0, se ha añadido el comando de habilitación:

```
enable feature rdpproxy
```

La función debe tener licencia para ejecutar este comando.

### Otros cambios en el proxy RDP

Se ha hecho obligatorio un atributo de clave precompartida (PSK) en el perfil del servidor.

Para migrar las configuraciones existentes de NetScaler 10.5.e para el proxy RDP a NetScaler 11.0, se deben comprender y abordar los siguientes detalles.

Si un administrador desea agregar una configuración de proxy RDP existente a una implementación de Unified Gateway elegida:

- La dirección IP del servidor virtual de NetScaler Gateway debe editarse y establecerse en una dirección IP no direccionable (0.0.0.0).
- Cualquier certificado de servidor SSL/TLS y las políticas de autenticación deben estar vinculados al servidor virtual de NetScaler Gateway que forma parte de la formación de Unified Gateway elegida.

## ¿Cómo se migra una configuración de proxy de Protocolo de escritorio remoto (RDP) basada en NetScaler 10.5.e a NetScaler 11.0?

Opción 1: Mantener el servidor virtual de NetScaler Gateway existente con la configuración de proxy RDP tal cual, con una licencia Premium o Advanced.

Opción 2: Mover el servidor virtual de NetScaler Gateway existente con la configuración de proxy RDP, colocándolo detrás de un servidor virtual de Unified Gateway.

Opción 3: Agregar un servidor virtual de NetScaler Gateway independiente con configuración de proxy RDP a un dispositivo Standard Edition existente.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

## ¿Cómo se configura NetScaler Gateway para la configuración de proxy RDP mediante la versión NetScaler 11.0?

Hay dos opciones para implementar el proxy RDP usando la versión NS 11.0:

1. Uso de un servidor virtual NetScaler Gateway con acceso externo. Esto requiere una dirección IP/FQDN visible externamente para el servidor virtual NetScaler Gateway. Esta opción es la que está disponible en NetScaler 10.5.e.
2. Uso de un servidor virtual Unified Gateway que actúa como front-end del servidor virtual NetScaler Gateway.

Con la Opción 2, el servidor virtual NetScaler Gateway no requiere su propia dirección IP/FQDN, ya que utiliza una dirección IP no direccionable (0.0.0.0).

## ¿Es HDX™ Insight compatible con Unified Gateway?

Cuando NetScaler Gateway se implementa con Unified Gateway, se deben cumplir las siguientes condiciones:

- El servidor virtual NetScaler Gateway debe tener un certificado SSL válido asociado.
- El servidor virtual NetScaler Gateway debe estar en estado ACTIVO para generar registros de AppFlow en NetScaler ADM, para la elaboración de informes de HDX Insight.

## ¿Cómo migro mi configuración existente de HDX Insight?

No es necesaria ninguna migración. Las directivas de AppFlow vinculadas a un servidor virtual NetScaler Gateway se transfieren si ese servidor virtual NetScaler Gateway se coloca detrás de un servidor virtual Unified Gateway.

Para los datos existentes en NetScaler ADM para el servidor virtual NetScaler Gateway, hay dos posibilidades:

- Si la dirección IP del servidor virtual NetScaler Gateway se asigna a un servidor virtual Unified Gateway como parte de la migración a Unified Gateway, los datos permanecen vinculados al servidor virtual NetScaler Gateway.
- Si al servidor virtual Unified Gateway se le asigna una dirección IP independiente, los datos de AppFlow del servidor virtual NetScaler Gateway se vinculan a esa nueva dirección IP. Por lo tanto, los datos existentes no forman parte de los datos nuevos.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

# Configuración de VPN en un dispositivo NetScaler Gateway

**IMPORTANTE:**

Las capturas de pantalla de esta sección se mantienen en un esquema de escala de grises por las siguientes razones:

- Ayudar a los lectores con discapacidad visual, especialmente a aquellos con daltonismo o deficiencia de color.
- El uso de una imagen en escala de grises representa la imagen de forma genérica, sin mostrar el impacto de la personalización de la codificación de colores que podría haberse realizado en el navegador o el sistema operativo del usuario.

Los usuarios pueden utilizar los siguientes métodos para conectarse a los recursos de red de su organización a través de NetScaler Gateway:

- Aplicación Citrix Workspace que contiene todos los plug-ins de Citrix instalados en el dispositivo del usuario.
- Aplicación Citrix Workspace para web que permite las conexiones de los usuarios a aplicaciones, escritorios y ShareFile mediante un explorador web.
- Secure Hub para permitir a los usuarios acceder a Secure Mail, WorxWeb y aplicaciones móviles desde sus dispositivos iOS y Android.
- Cliente Citrix Secure Access™ para Windows, macOS X o Linux.
- Aplicación NetScaler Gateway para iOS y Android.
- Acceso sin cliente que proporciona a los usuarios el acceso que necesitan sin instalar software de usuario.
- Interoperabilidad con el plug-in Citrix SD-WAN™.

Si los usuarios instalan el cliente Citrix Secure Access y, a continuación, instalan la aplicación Citrix Workspace desde Citrix Virtual Apps 6.5 para Windows Server 2008 (incluidos Feature Pack y Feature Pack 2), Citrix Virtual Desktops 7.0 o posterior, la aplicación Citrix Workspace agrega

© 1997–2026 Citrix Systems, Inc. All rights reserved.

automáticamente el cliente Citrix Secure Access. Los usuarios pueden conectarse con el cliente Citrix Secure Access desde un explorador web o desde la aplicación Citrix Workspace.

SmartAccess determina automáticamente los métodos de acceso permitidos para un dispositivo de usuario en función de los resultados de un análisis de punto final. Para obtener más información sobre SmartAccess, consulte Configuración de SmartAccess.

NetScaler Gateway es compatible con las aplicaciones de productividad móvil de Citrix Endpoint Management para dispositivos móviles iOS y Android. NetScaler Gateway incluye Secure Browse, que permite conexiones a NetScaler Gateway desde dispositivos móviles iOS que establecen el túnel micro VPN. Los dispositivos Android que se conectan con Secure Hub también establecen automáticamente un túnel micro VPN que proporciona acceso seguro a nivel de aplicación web y móvil a los recursos de su red interna. Si los usuarios se conectan desde un dispositivo Android con aplicaciones de productividad móvil, debe configurar los ajustes de DNS en NetScaler Gateway. Para obtener más información, consulte Compatibilidad con consultas DNS mediante sufijos DNS para dispositivos Android.

## Cómo se conectan los usuarios con el cliente Citrix Secure Access™

NetScaler Gateway funciona de la siguiente manera:

- Cuando los usuarios intentan acceder a los recursos de red a través del túnel VPN, el cliente Citrix Secure Access cifra todo el tráfico de red destinado a la red interna de la organización y reenvía los paquetes a NetScaler Gateway.
- NetScaler Gateway finaliza el túnel SSL, acepta cualquier tráfico entrante destinado a la red privada y reenvía el tráfico a la red privada. NetScaler Gateway envía el tráfico de vuelta al equipo remoto a través de un túnel seguro.

Cuando los usuarios escriben la dirección web, reciben una página de inicio de sesión donde introducen sus credenciales e inician sesión. Si las credenciales son correctas, NetScaler Gateway finaliza el protocolo de enlace con el dispositivo del usuario.

Si el usuario está detrás de un servidor proxy, puede especificar el servidor proxy y las credenciales de autenticación. Para obtener más información, consulte Habilitar la compatibilidad con proxy para conexiones de usuario.

El cliente Citrix Secure Access está instalado en el dispositivo del usuario. Después de la primera conexión, si los usuarios inician sesión con un equipo basado en Windows, pueden usar el icono del área de notificación para establecer la conexión.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

## Establecer el túnel seguro

Cuando los usuarios se conectan con el cliente Citrix Secure Access, Secure Hub o la aplicación Citrix Workspace, el software cliente establece un túnel seguro a través del puerto 443 (o cualquier puerto configurado en NetScaler Gateway) y envía información de autenticación. Cuando se establece el túnel, NetScaler Gateway envía información de configuración al cliente Citrix Secure Access, Secure Hub o la aplicación Citrix Workspace que describe las redes que se van a proteger y que contiene una dirección IP si habilita los grupos de direcciones.

### Tunelizar el tráfico de red privada a través de conexiones seguras

Cuando se inicia el cliente Citrix Secure Access y el usuario se autentica, todo el tráfico de red destinado a redes privadas especificadas se captura y se redirige a través del túnel seguro a NetScaler Gateway. La aplicación Citrix Workspace debe ser compatible con el cliente Citrix Secure Access para establecer la conexión a través del túnel seguro cuando los usuarios inician sesión.

Secure Hub, Secure Mail y WorxWeb utilizan Micro VPN para establecer el túnel seguro para dispositivos móviles iOS y Android.

NetScaler Gateway intercepta todas las conexiones de red que realiza el dispositivo del usuario y las multiplexa a través de Secure Sockets Layer (SSL) a NetScaler Gateway, donde el tráfico se desmultiplexa y las conexiones se reenvían a la combinación correcta de host y puerto.

Las conexiones están sujetas a políticas de seguridad administrativas que se aplican a una sola aplicación, a un subconjunto de aplicaciones o a una intranet completa. Usted especifica los recursos (rangos de pares de direcciones IP/subred) a los que los usuarios remotos pueden acceder a través de la conexión VPN.

El cliente Citrix Secure Access intercepta y tuneliza los siguientes protocolos para las aplicaciones de intranet definidas:

- TCP (todos los puertos)
- UDP (todos los puertos)
- ICMP (tipos 8 y 0 - solicitud/respuesta de eco)

Las conexiones de las aplicaciones locales en el dispositivo del usuario se tunelizan de forma segura a NetScaler Gateway, que restablece las conexiones al servidor de destino. Los servidores de destino ven las conexiones como originadas desde el NetScaler Gateway local en la red privada, ocultando así el dispositivo del usuario. Esto también se denomina Traducción de

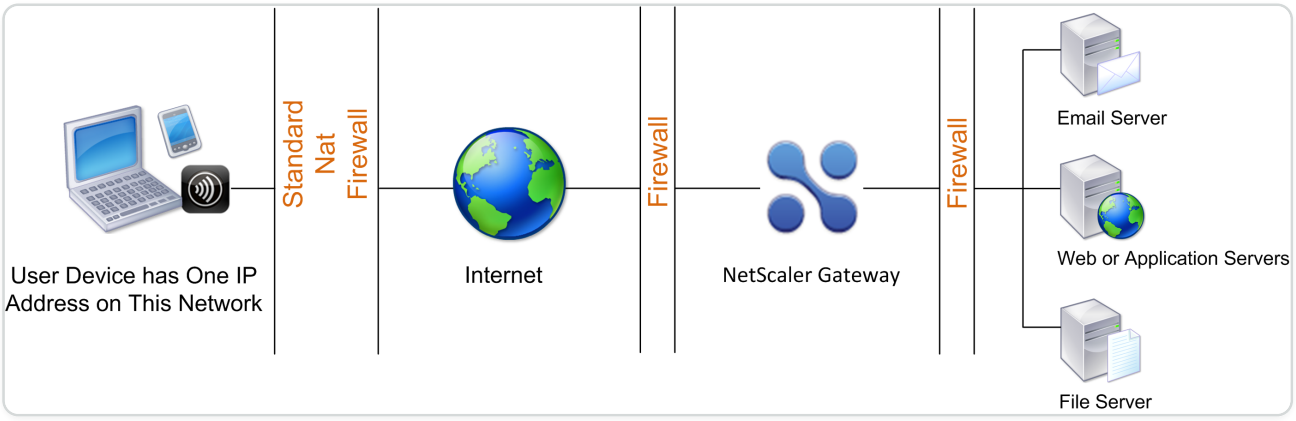
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Direcciones de Red (NAT) inversa. Ocultar las direcciones IP añade seguridad a las ubicaciones de origen.

Localmente, en el dispositivo del usuario, todo el tráfico relacionado con la conexión, como los paquetes SYN-ACK, PUSH, ACK y FIN, es recreado por el cliente de Citrix Secure Access para que parezca provenir del servidor privado.

## Conectarse a través de firewalls y proxies

Los usuarios del cliente de Citrix Secure Access a veces se encuentran dentro del firewall de otra organización, como se muestra en la siguiente figura:




Los firewalls NAT mantienen una tabla que les permite enrutar paquetes seguros desde NetScaler Gateway de vuelta al dispositivo del usuario. Para las conexiones orientadas a circuitos, NetScaler Gateway mantiene una tabla de traducción NAT inversa mapeada por puertos. La tabla de traducción NAT inversa permite a NetScaler Gateway hacer coincidir las conexiones y enviar paquetes de vuelta a través del túnel al dispositivo del usuario con los números de puerto correctos para que los paquetes regresen a la aplicación correcta.

## Controlar la actualización de los clientes de Citrix Secure Access

Los administradores del sistema controlan cómo se comporta el complemento de NetScaler cuando su versión no coincide con la revisión de NetScaler Gateway. Las nuevas opciones controlan el comportamiento de actualización del complemento para sistemas operativos Mac y Windows.

Para los complementos VPN, la opción de actualización se puede configurar en dos lugares de la interfaz de usuario del dispositivo NetScaler:

- En la configuración global
- En el nivel de perfil de sesión

© 1997–2026 Citrix Systems, Inc. All rights reserved.

## Requisitos

- La versión del complemento EPA y VPN de Windows debe ser superior a 11.0.0.0
- La versión del complemento EPA de Mac debe ser superior a 3.0.0.31
- La versión del complemento VPN de Mac debe ser superior a 3.1.4 (357)

**NOTA:**

Si el dispositivo NetScaler se actualiza a la versión 11.0, todos los complementos VPN (y EPA) anteriores se actualizan a la última versión, independientemente de la configuración de control de actualización. Para las actualizaciones posteriores, respetan la configuración de control de actualización anterior.

### Comportamientos del complemento

Para cada tipo de cliente, NetScaler Gateway permite las siguientes tres opciones para controlar el comportamiento de actualización del complemento:

- **Siempre**

  El complemento siempre se actualiza cuando la versión del complemento del usuario final no coincide con el complemento que se envía con NetScaler. Este es el comportamiento predeterminado. Elija esta opción si no desea que se ejecuten varias versiones del complemento en su empresa.

- **Esencial**

  El complemento solo se actualiza cuando se considera necesario. Las actualizaciones se consideran necesarias en las dos circunstancias siguientes:

  - El complemento instalado es incompatible con la versión actual de NetScaler.
  - El complemento instalado debe actualizarse para la corrección de seguridad necesaria.

  Elija esta opción si desea minimizar el número de actualizaciones de complementos, pero no quiere perderse ninguna actualización de seguridad de complementos.

  **NOTA:**

  La opción de actualización del plug-in **Essential** no es compatible con el cliente Citrix Secure Access para Linux.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Para garantizar la funcionalidad correcta de la opción **Essential** del parámetro **Windows Plugin Upgrade**, siga estos pasos:

a. Descargue la versión requerida de `win-vpn.tgz` desde la página Descargas de Citrix.

b. Extraiga el archivo `win-vpn.tgz`. Esta extracción incluye tres archivos: `AGEE-setup.exe`, `nsepa_setup.exe` y `package.json`.

c. Edite el archivo `package.json` para agregar los parámetros `compatibleFrom` y `compatibleTill`. Puede obtener los valores `compatibleFrom` del archivo `pluginList.xml` en "https://<vserv_url>/vpn/pluginList.xml".

   El siguiente es un ejemplo del archivo `package.json` modificado:

```
{

"Description": "This zip file contains VPN and EPA Plugins for
Windows",

"packages": [

    {

    "metadata": {

        "version": "25.5.1.15"

            "compatibleFrom": "25.5.1.15",

            "compatibleTill": ""

    },

    "type": "WIN-VPN"

    },

    {

    "metadata": {

        "version": "25.5.1.15"

            "compatibleFrom": "25.5.1.15",
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
            "compatibleTill": ""

    },

    "type": "WIN-EPA"

    },

    {

    "metadata": {

        "version": "25.5.1.15"

            "compatibleFrom": "25.5.1.15",

            "compatibleTill": ""

    },

    "type": "WIN-EPA64"

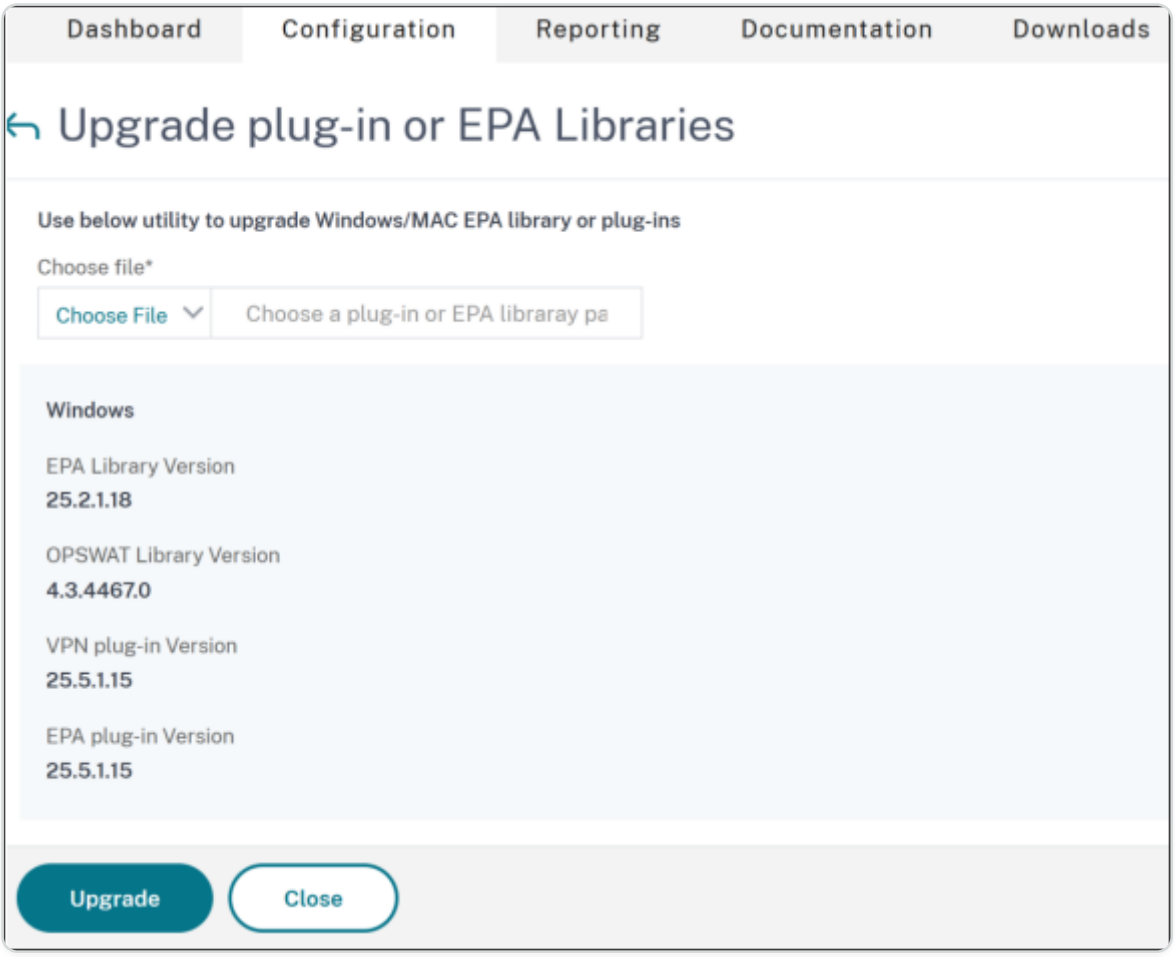
    }

]

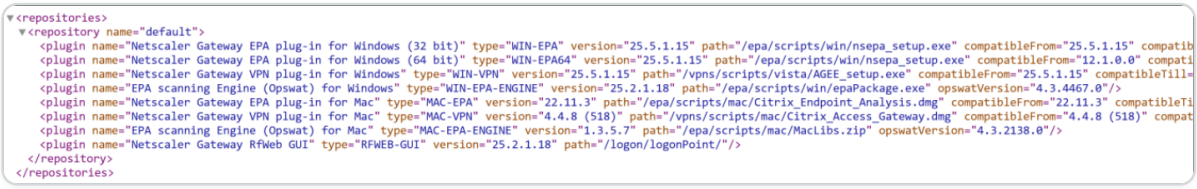
}
```

d. Comprima los tres archivos de nuevo en formato .tgz y, a continuación, cargue este nuevo archivo .tgz en NetScaler. Para obtener más información, consulte Actualizar el cliente Citrix Secure Access y el cliente EPA para Windows en NetScaler Gateway.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

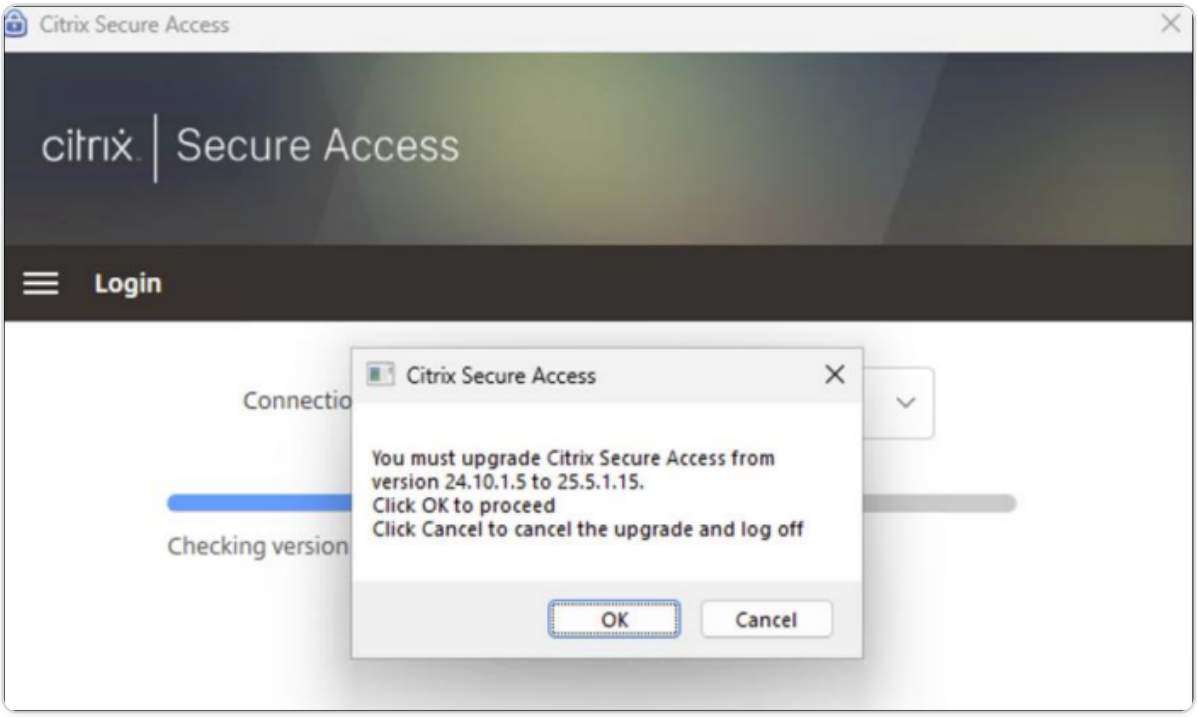



e. Después de la carga, valide que el archivo `pluginList.xml` en NetScaler se haya actualizado con los valores `compatibleFrom` correctos.




f. Conéctese a la URL del servidor virtual desde el cliente Citrix Secure Access para Windows. Se le pedirá al usuario que continúe con la actualización del plug-in.

© 1997–2026 Citrix Systems, Inc. All rights reserved.




- **Nunca**

  El plug-in no se actualiza.

  **NOTA:**

  Para eLux® e IGEL OS, la opción **Actualización del complemento de Linux** en la ficha **Experiencia del cliente** siempre debe establecerse en **Nunca**.

### Parámetros de CLI para controlar la actualización del complemento VPN

NetScaler Gateway admite dos tipos de complementos (EPA y VPN) para los sistemas operativos Windows y Mac. Para admitir el control de actualización del complemento VPN a nivel de sesión, NetScaler Gateway admite dos parámetros de perfil de sesión denominados WindowsinPluginUpgrade y MacPluginUpgrade.

Estos parámetros están disponibles a nivel global, de servidor virtual, de grupo y de usuario. Cada parámetro puede tener un valor de Siempre, Esencial o Nunca. Para obtener una descripción de estos parámetros, consulte Comportamientos del complemento.

### Parámetros de CLI para controlar la actualización del complemento EPA

NetScaler Gateway admite complementos EPA para los sistemas operativos Windows y Mac. Para admitir el control de actualización del complemento EPA a nivel de servidor virtual, NetScaler

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Gateway admite dos parámetros de servidor virtual denominados windowsEPAPluginUpgrade y macEPAPluginUpgrade.

Los parámetros están disponibles a nivel de servidor virtual. Cada parámetro puede tener un valor de Siempre, Esencial o Nunca. Para obtener una descripción de estos parámetros, consulte Comportamientos del complemento

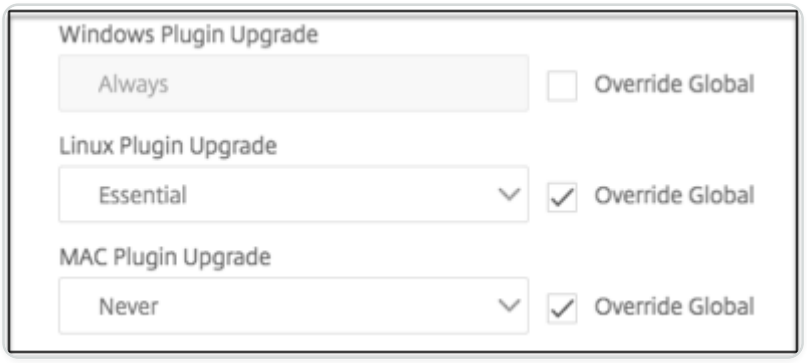
### Configuración de VPN

Siga estos pasos para la **configuración de VPN** de los complementos de Windows, Linux y Mac.

1. Vaya a **NetScaler > Directivas > Sesión.**
2. Seleccione la directiva de sesión deseada y, a continuación, haga clic en **Editar**.
3. Seleccione la ficha **Experiencia del cliente**.
4. Estas opciones de cuadros de diálogo afectan al comportamiento de actualización.

   - Siempre
   - Esencial
   - Nunca

   El valor predeterminado es Siempre.
5. Seleccione la casilla de verificación a la derecha de cada opción. Seleccione la frecuencia para aplicar el comportamiento de actualización.

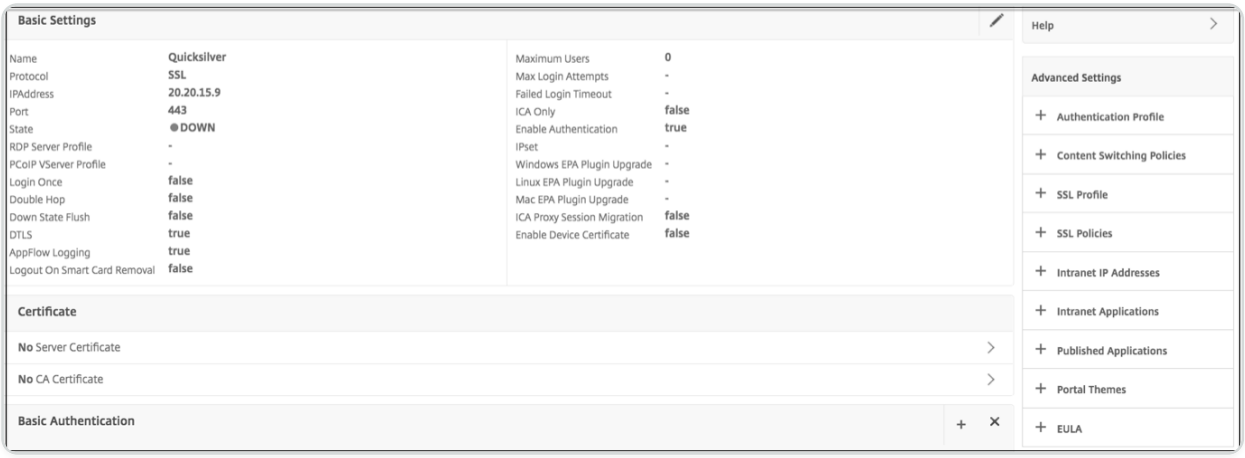



### Configuración de EPA

Siga estos pasos para la configuración de EPA de los plug-ins de Windows, Linux y Apple.

1. Vaya a **NetScaler Gateway > Servidores virtuales**.
2. Seleccione un servidor y haga clic en el botón **Editar**.
3. Haga clic en el icono del **lápiz**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.




4. Haga clic en **Más**
5. Los cuadros de diálogo que aparecen afectan al comportamiento de actualización. Las opciones disponibles son:
    - Siempre
    - Esencial
    - Nunca

# Configuración completa de VPN en NetScaler Gateway

Esta sección describe cómo configurar una configuración completa de VPN en un dispositivo NetScaler Gateway. Contiene consideraciones de red y el enfoque ideal para resolver problemas desde la perspectiva de la red.

## Requisitos previos

- Instale un certificado SSL y vincúlelo al servidor virtual VPN.
    - CTX109260 - Cómo generar e instalar un certificado SSL público en un dispositivo NetScaler
    - CTX122521 - Cómo reemplazar el certificado predeterminado de un dispositivo NetScaler por un certificado de CA de confianza que coincida con el nombre de host del dispositivo
    - Documentación de NetScaler - Vincular el par de claves de certificado al servidor virtual basado en SSL
- Cree un perfil de autenticación para NetScaler Gateway.
    - Para obtener información adicional, consulte la documentación de NetScaler - Configuración de la autenticación de usuarios externos

© 1997–2026 Citrix Systems, Inc. All rights reserved.

    - Para obtener información adicional, consulte la lista de comprobación: Usar AD FS para implementar y administrar el inicio de sesión único

- Descargue Cliente VPN.
- Cree una directiva de sesión que permita conexiones VPN completas.

Cuando los usuarios se conectan con el cliente Citrix Secure Access, Secure Hub o la aplicación Citrix Workspace, el software cliente establece un túnel seguro a través del puerto 443 (o cualquier puerto configurado en NetScaler Gateway) y envía información de autenticación. Una vez establecido el túnel, NetScaler Gateway envía información de configuración al cliente Citrix Secure Access, Citrix Secure Hub o la aplicación Citrix Workspace que describe las redes que se van a proteger. Esa información también contiene una dirección IP si habilita las IP de intranet.

Puede configurar las conexiones de los dispositivos de usuario definiendo los recursos a los que los usuarios pueden acceder en la red interna. La configuración de las conexiones de los dispositivos de usuario incluye lo siguiente:

- Tunelización dividida
- Direcciones IP para usuarios, incluidas las agrupaciones de direcciones (IP de intranet)
- Conexiones a través de un servidor proxy
- Definición de los dominios a los que los usuarios tienen acceso
- Configuración de tiempo de espera
- Inicio de sesión único
- Software de usuario que se conecta a través de NetScaler Gateway
- Acceso para dispositivos móviles

La mayoría de las conexiones de dispositivos de usuario se configuran mediante un perfil que forma parte de una directiva de sesión. También puede definir la configuración de conexión de dispositivos de usuario mediante directivas de autenticación, tráfico y autorización. También se pueden configurar mediante aplicaciones de intranet.

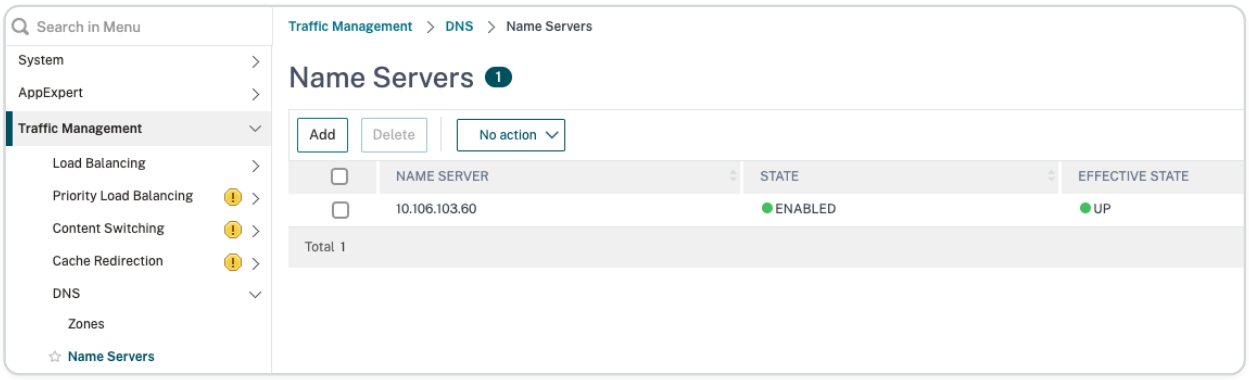
## Configurar una configuración VPN completa en un dispositivo NetScaler Gateway

Para configurar una configuración VPN en el dispositivo NetScaler Gateway, complete el siguiente procedimiento:

1. Vaya a **Administración del tráfico > DNS**.

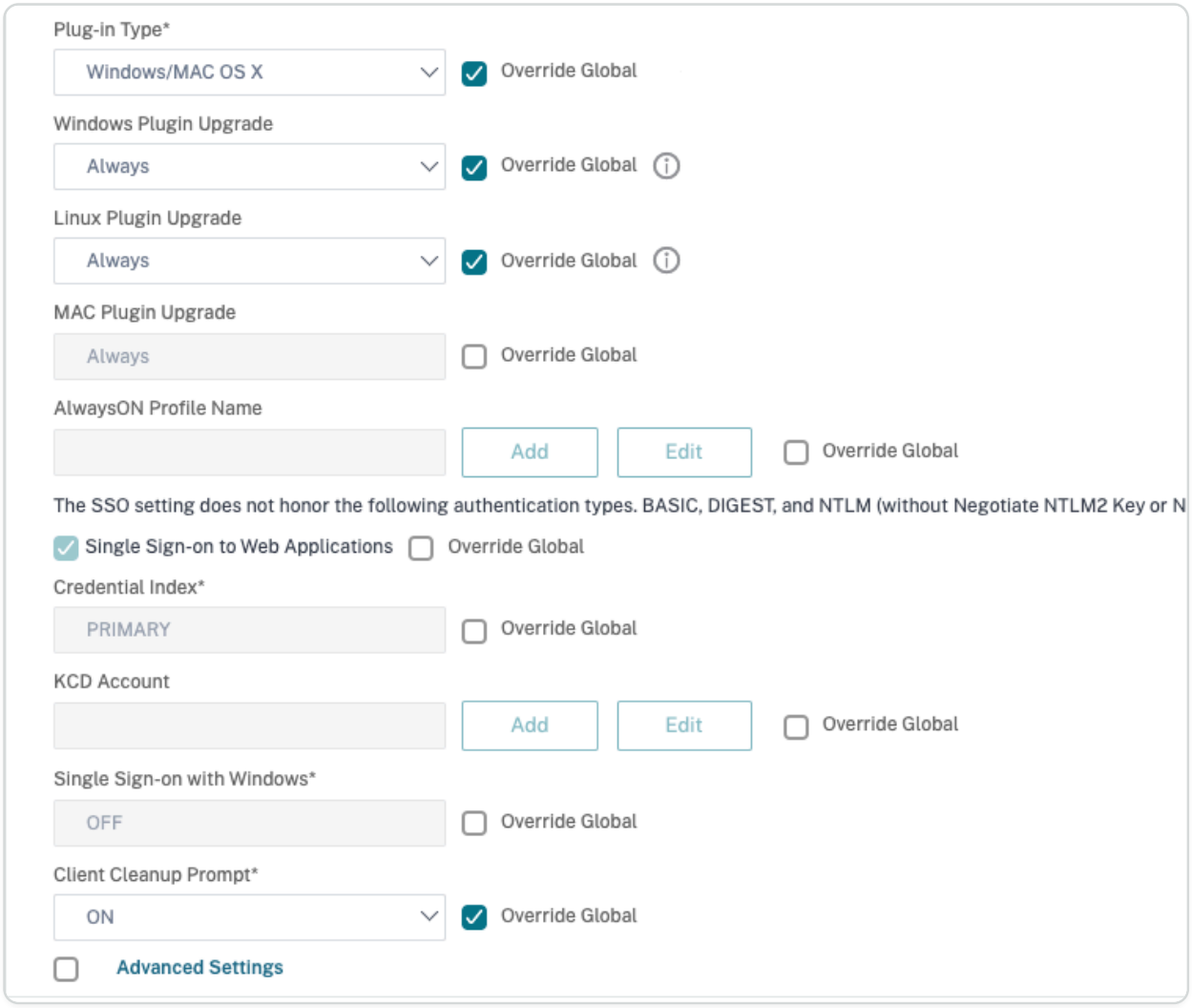
© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Seleccione el nodo Servidores de nombres, como se muestra en la siguiente captura de pantalla. Asegúrese de que el servidor de nombres DNS esté en la lista. Si no está disponible, agregue un servidor de nombres DNS.



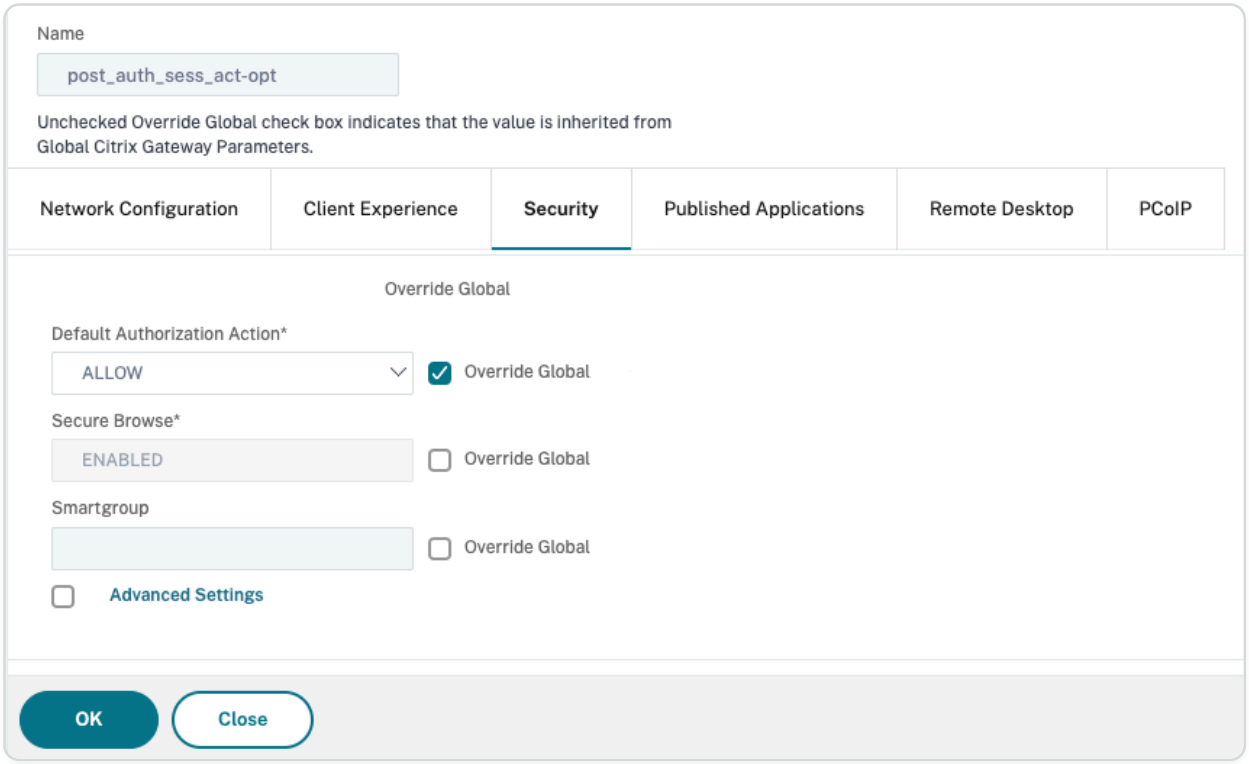

3. Expanda **NetScaler Gateway > Directivas**.
4. Seleccione el nodo **Sesión**.
5. En la página Directivas y perfiles de sesión de NetScaler Gateway, haga clic en la ficha **Perfiles** y, a continuación, en **Agregar**. Para cada componente que configure en el cuadro de diálogo Configurar perfil de sesión de NetScaler Gateway, asegúrese de seleccionar la opción **Anular global** para el componente respectivo.
6. Haga clic en la ficha **Experiencia del cliente**.
7. Escriba la URL del portal de la intranet en el campo Página de inicio si desea presentar alguna URL cuando el usuario inicie sesión en la VPN. Si el parámetro de la página de inicio se establece en "nohomepage.html", la página de inicio no se muestra. Cuando se inicia el complemento, se inicia una instancia del explorador y se cierra automáticamente.
8. Asegúrese de seleccionar la configuración deseada de la lista Túnel dividido.
9. Seleccione **DESACTIVADO** en la lista **Acceso sin cliente** si desea FullVPN.
10. Asegúrese de que **Windows/Mac OS X** esté seleccionado en la lista **Tipo de complemento**.
11. Seleccione la opción **Inicio de sesión único en aplicaciones web** si lo desea.
12. Asegúrese de que la opción **Solicitud de limpieza del cliente** esté seleccionada si es necesario, como se muestra en la siguiente captura de pantalla:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

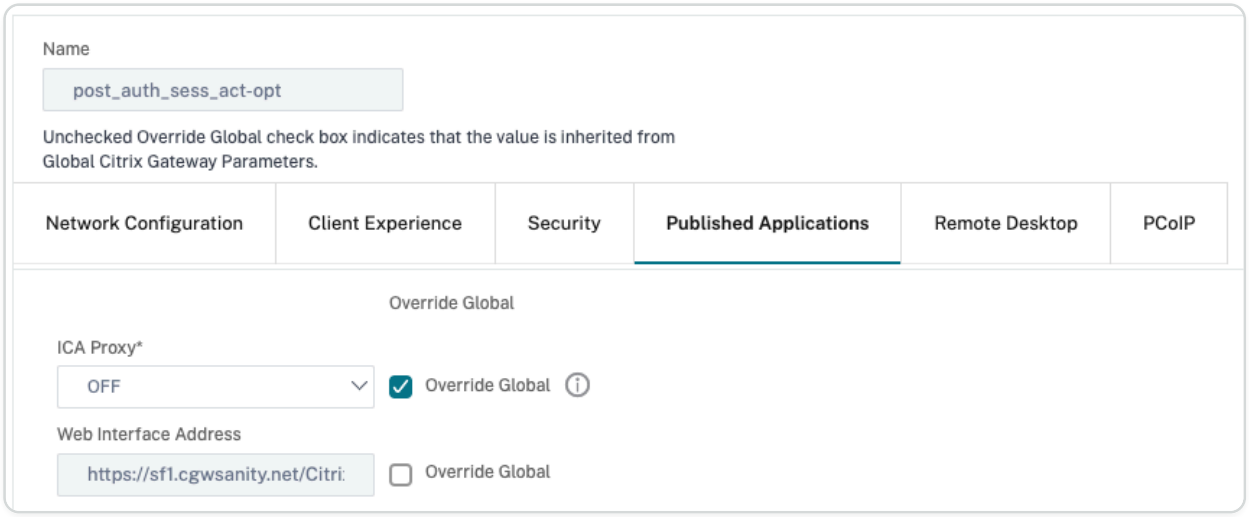



13. Haga clic en la ficha **Seguridad**.
14. Asegúrese de que **PERMITIR** esté seleccionado en la lista **Acción de autorización predeterminada**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

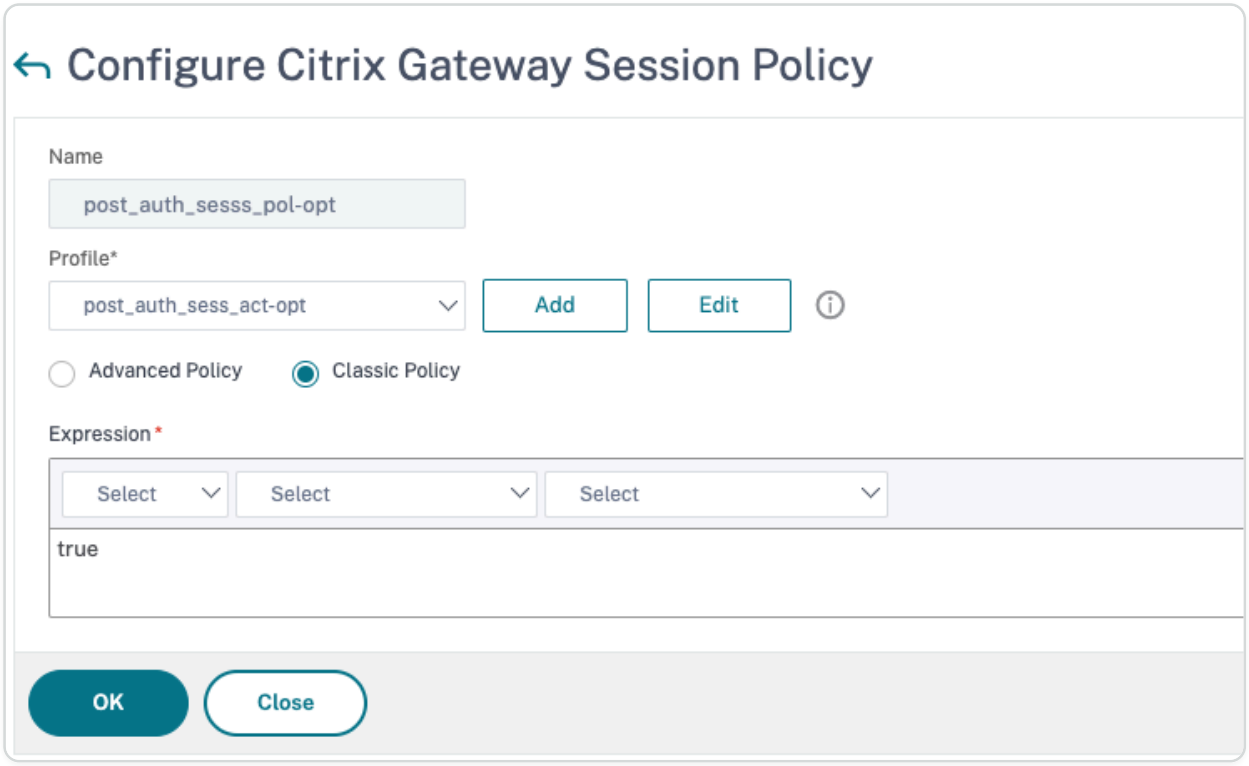



15. Haga clic en la ficha **Aplicaciones publicadas**.
16. Asegúrese de que **DESACTIVADO** esté seleccionado en la lista **Proxy ICA®** en la opción **Aplicaciones publicadas**.




17. Haga clic en **Crear**.
18. Haga clic en **Cerrar**.
19. Haga clic en la pestaña **Directivas** de la página Directivas y perfiles de sesión de NetScaler Gateway en el servidor virtual o active las directivas de sesión en el nivel GRUPO/USUARIO según sea necesario.
20. Cree una directiva de sesión con una expresión requerida o verdadera, como se muestra en la siguiente captura de pantalla:

© 1997–2026 Citrix Systems, Inc. All rights reserved.



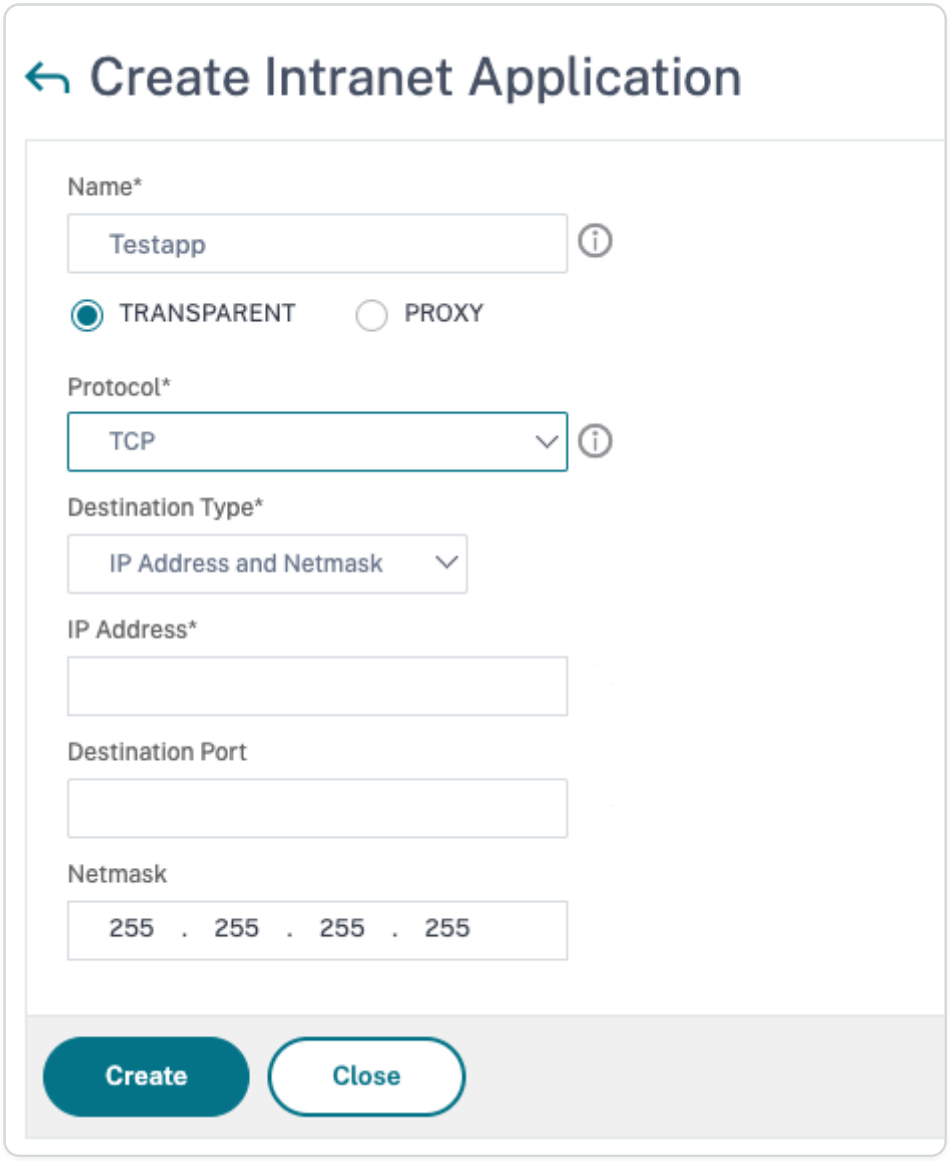

21. Enlace la directiva de sesión al servidor virtual VPN. Para obtener más información, consulte Enlazar directivas de sesión.

    Si el túnel dividido se configuró en ON, debe configurar las aplicaciones de intranet a las que desea que los usuarios accedan cuando estén conectados a la VPN. Para obtener más información sobre las aplicaciones de intranet, consulte Configurar aplicaciones de intranet para el cliente de Citrix Secure Access.

    a. Vaya a **NetScaler Gateway > Recursos > Aplicaciones de intranet**.

    b. Cree una aplicación de intranet. Seleccione Transparente para FullVPN con cliente Windows. Seleccione el protocolo que desea permitir (TCP, UDP o CUALQUIERA), tipo de destino (dirección IP y máscara, rango de direcciones IP o nombre de host).

© 1997–2026 Citrix Systems, Inc. All rights reserved.




c. Si es necesario, establezca una nueva directiva para VPN en iOS y Android mediante la siguiente expresión: `HTTP.REQ.HEADER("User-Agent").CONTAINS("CitrixVPN")&&HTTP.REQ.HEADER("User-Agent").CONTAINS("NSGiOSplugin")&&HTTP.REQ.HEADER("User-Agent").CONTAINS("Android")`

d. Enlace las aplicaciones de intranet creadas en el nivel USUARIO/GRUPO/VSERVER según sea necesario.

**NOTA:**

Las aplicaciones web publicadas en el puerto 80 (HTTP) se bloquean automáticamente incluso cuando una directiva de acceso las permite explícitamente. Para resolver este problema, ejecute el siguiente comando en el shell de NetScaler Gateway:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
nsapimgr -y -s vpn_http_port80=0
```

Para que persista entre reinicios, añada este comando a `/nsconfig/rc.netscaler`.

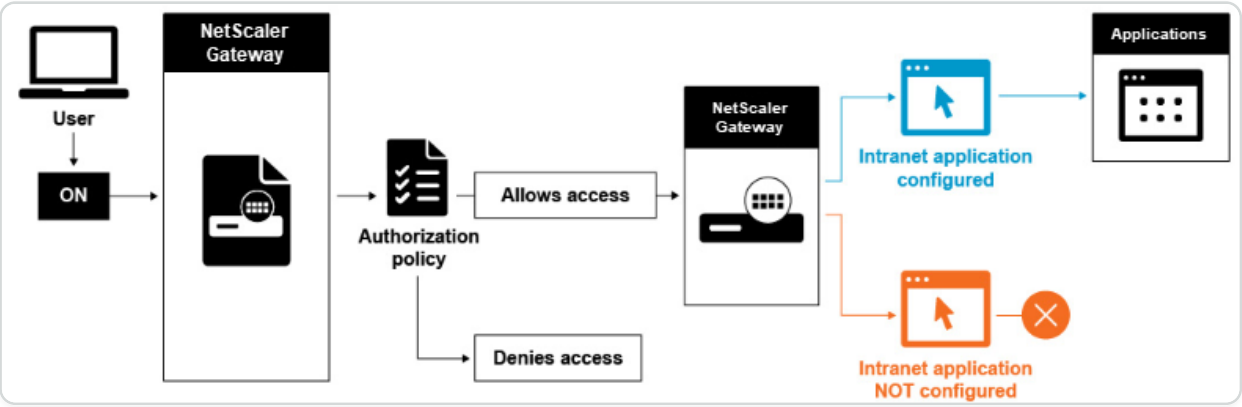
## Configurar la tunelización dividida

1. Vaya a **Configuración** > **NetScaler Gateway > Directivas > Sesión**.
2. En el panel de detalles, en la ficha Perfiles, seleccione un perfil y, a continuación, haga clic en **Modificar**.
3. En la ficha **Experiencia del cliente**, junto a **Tunelización dividida**, seleccione **Anulación global**, seleccione una opción y, a continuación, haga clic en **Aceptar**.

   Configuración de la tunelización dividida y la autorización

   Al planificar la implementación de NetScaler Gateway, es importante tener en cuenta la tunelización dividida y la acción de autorización predeterminada y las directivas de autorización.

   Por ejemplo, tiene una directiva de autorización que permite el acceso a un recurso de red. Tiene la tunelización dividida establecida en ACTIVADA y no configura las aplicaciones de intranet para enviar tráfico de red a través de NetScaler Gateway. Cuando NetScaler Gateway tiene este tipo de configuración, se permite el acceso al recurso, pero los usuarios no pueden acceder al recurso.




Si la directiva de autorización deniega el acceso a un recurso de red, el cliente de Citrix Secure Access envía tráfico a NetScaler Gateway, pero el acceso al recurso se deniega en las siguientes condiciones.

- Tiene la tunelización dividida establecida en ACTIVADA.
- Las aplicaciones de intranet están configuradas para enrutar el tráfico de red a través de NetScaler Gateway

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Para obtener más información sobre las directivas de autorización, revise lo siguiente:

- Configuración de la autorización
- Configuración de directivas de autorización
- Configuración de la autorización global predeterminada

Para configurar el acceso a la red a los recursos de red internos

1. Vaya a **Configuración** > **NetScaler Gateway > Recursos > Aplicaciones de intranet**.
2. En el panel de detalles, haga clic en **Agregar**.
3. Complete los parámetros para permitir el acceso a la red, haga clic en **Crear** y, a continuación, haga clic en **Cerrar**.

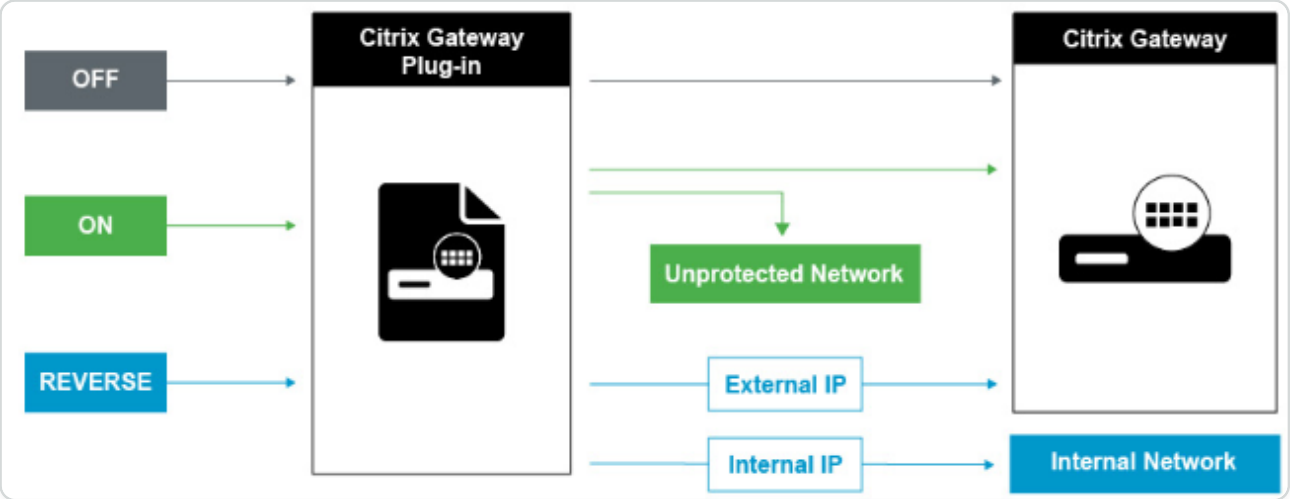
Cuando no configuramos las IP de intranet para los usuarios de VPN, el usuario envía el tráfico al VIP de NetScaler Gateway y, desde allí, el dispositivo NetScaler crea un nuevo paquete al recurso de la aplicación de intranet en la LAN interna. Este nuevo paquete se originará desde el SNIP hacia la aplicación de intranet. Desde aquí, la aplicación de intranet recibe el paquete, lo procesa y luego intenta responder al origen de ese paquete (el SNIP en este caso). El SNIP recibe el paquete y envía la respuesta al cliente que realizó la solicitud.

Cuando se utiliza una dirección IP de intranet, el usuario envía el tráfico al VIP de NetScaler Gateway y, desde allí, el dispositivo NetScaler asigna la IP del cliente a una de las IPs de INTRANET configuradas del grupo. Tenga en cuenta que el dispositivo NetScaler será el propietario del grupo de IP de intranet y, por esta razón, estos rangos no deben utilizarse en la red interna. El dispositivo NetScaler asigna una IP de intranet para las conexiones VPN entrantes, como lo haría un servidor DHCP. El dispositivo NetScaler crea un nuevo paquete para la aplicación de intranet en la LAN a la que accedería el usuario. Este nuevo paquete se originará desde una de las IPs de intranet hacia la aplicación de intranet. Desde aquí, las aplicaciones de intranet reciben el paquete, lo procesan y luego intentan responder al origen de ese paquete (la IP de INTRANET). En este caso, el paquete de respuesta debe enrutarse de vuelta al dispositivo NetScaler, donde se encuentran las IPs de INTRANET (Recuerde, el dispositivo NetScaler es el propietario de las subredes de IP de intranet). Para realizar esta tarea, el administrador de red debe tener una ruta a la IP de INTRANET, apuntando a uno de los SNIP. Se recomienda dirigir el tráfico de vuelta al SNIP que contiene la ruta desde la cual el paquete sale del dispositivo NetScaler por primera vez para evitar cualquier tráfico asimétrico.

## Opciones de tunelización dividida

Las siguientes son las diversas opciones de tunelización dividida.

© 1997–2026 Citrix Systems, Inc. All rights reserved.




### Tunelización dividida DESACTIVADA

Cuando la tunelización dividida está desactivada, el cliente de Citrix Secure Access captura todo el tráfico de red originado desde un dispositivo de usuario y lo envía a través del túnel VPN a NetScaler Gateway. En otras palabras, el cliente VPN establece una ruta predeterminada desde el PC cliente que apunta al VIP de NetScaler Gateway, lo que significa que todo el tráfico debe enviarse a través del túnel para llegar al destino. Dado que todo el tráfico se enviará a través del túnel, las políticas de autorización deben determinar si el tráfico puede pasar a los recursos de red internos o si debe denegarse.

Cuando está configurado en «desactivado», todo el tráfico pasa por el túnel, incluido el tráfico web estándar a los sitios web. Si el objetivo es supervisar y controlar este tráfico web, debe reenviar estas solicitudes a un proxy externo mediante el dispositivo NetScaler. Los dispositivos de usuario también pueden conectarse a través de un servidor proxy para acceder a redes internas.

NetScaler Gateway admite los protocolos HTTP, SSL, FTP y SOCKS. Para habilitar la compatibilidad con proxy para las conexiones de usuario, debe especificar esta configuración en NetScaler Gateway. Puede especificar la dirección IP y el puerto utilizados por el servidor proxy en NetScaler Gateway. El servidor proxy se utiliza como proxy de reenvío para todas las conexiones posteriores a la red interna.

Para obtener más información, consulte los siguientes enlaces:

- Habilitación de la compatibilidad con proxy para conexiones de usuario

### Tunelización dividida ACTIVADA

Puede habilitar la tunelización dividida para evitar que el cliente de Citrix Secure Access envíe tráfico de red innecesario a NetScaler Gateway. Si la tunelización dividida está habilitada, el cliente de Citrix Secure Access solo envía el tráfico destinado a redes protegidas (aplicaciones de

© 1997–2026 Citrix Systems, Inc. All rights reserved.

intranet) por NetScaler Gateway a través del túnel VPN. El cliente de Citrix Secure Access no envía tráfico de red destinado a redes no protegidas a NetScaler Gateway. Cuando se inicia el cliente de Citrix Secure Access, obtiene la lista de aplicaciones de intranet de NetScaler Gateway y establece una ruta para cada subred definida en la ficha de aplicación de intranet en el PC cliente. El cliente de Citrix Secure Access examina todos los paquetes transmitidos desde el dispositivo de usuario y compara las direcciones dentro de los paquetes con la lista de aplicaciones de intranet (tabla de enrutamiento creada cuando se inició la conexión VPN). Si la dirección de destino del paquete se encuentra dentro de una de las aplicaciones de intranet, el cliente de Citrix Secure Access envía el paquete a través del túnel VPN a NetScaler Gateway. Si la dirección de destino no se encuentra en una aplicación de intranet definida, el paquete no se cifra y el dispositivo de usuario enruta el paquete de forma adecuada utilizando el enrutamiento predeterminado definido originalmente en el PC cliente. «Cuando se habilita la tunelización dividida, las aplicaciones de intranet definen el tráfico de red que se intercepta y se envía a través del túnel».

### Tunelización dividida inversa

NetScaler Gateway también admite la tunelización dividida inversa, que define el tráfico de red que NetScaler Gateway no intercepta. Si establece la tunelización dividida en inversa, las aplicaciones de intranet definen el tráfico de red que NetScaler Gateway no intercepta. Cuando habilita la tunelización dividida inversa, todo el tráfico de red dirigido a direcciones IP internas omite el túnel VPN, mientras que el resto del tráfico pasa por NetScaler Gateway. La tunelización dividida inversa se puede utilizar para registrar todo el tráfico LAN no local. Por ejemplo, si los usuarios tienen una red inalámbrica doméstica y han iniciado sesión con el cliente de Citrix Secure Access, NetScaler Gateway no intercepta el tráfico de red destinado a una impresora u otro dispositivo dentro de la red inalámbrica.

**NOTA:**

El cliente de Citrix Secure Access para Windows, macOS, iOS y Android admite la tunelización dividida inversa basada en FQDN. Para los clientes de Windows, a partir de Citrix Secure Access 22.6.1.5, esta función solo funciona si el controlador WFP está habilitado.

#### Puntos a tener en cuenta

**Tunelización dividida inversa basada en IP:**

- El número de reglas basadas en direcciones IP está limitado a 1024.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Compatible con los controladores DNE y WFP.

**Tunelización dividida inversa basada en nombre de host:**

- El número de nombres de host a los que se puede acceder durante una sesión VPN está restringido por el número de direcciones IP utilizables especificadas en el rango de suplantación de FQDN. Esto se debe a que cada nombre de host ocupa una dirección IP del rango de suplantación de FQDN. Una vez que el rango de IP se agota, la dirección IP asignada menos recientemente se reutiliza para el siguiente nombre de host nuevo.
- Los sufijos DNS deben configurarse.

> **NOTA:**
>
> Para los clientes de Windows, la tunelización dividida inversa basada en nombres de host solo es compatible con el controlador WFP. Habilite el modo de controlador WFP estableciendo el valor de registro «EnableWFP» en `1`. Para obtener más información, consulte Cliente de Citrix Secure Access para Windows mediante la plataforma de filtrado de Windows.

**Tunelización dividida inversa basada en IP y en nombre de host:**

- Compatible solo con el controlador WFP. Todas las demás directrices mencionadas en el túnel dividido inverso basado en IP y el túnel dividido inverso basado en nombre de host son aplicables.

## Configurar la resolución de servicio de nombres

Durante la instalación de NetScaler Gateway, puede usar el asistente de NetScaler Gateway para configurar otros ajustes, incluidos los proveedores de servicios de nombres. Los proveedores de servicios de nombres traducen el nombre de dominio completo (FQDN) a una dirección IP. En el asistente de NetScaler Gateway, también puede realizar lo siguiente:

- Configurar un servidor DNS o WINS
- Establecer la prioridad de la búsqueda DNS
- Establecer el número de veces que se reintentará la conexión al servidor.

Cuando ejecuta el asistente de NetScaler Gateway, puede agregar un servidor DNS en ese momento. Puede agregar otros servidores DNS y un servidor WINS a NetScaler Gateway

© 1997–2026 Citrix Systems, Inc. All rights reserved.

mediante un perfil de sesión. Luego puede dirigir a los usuarios y grupos para que se conecten a un servidor de resolución de nombres diferente al que configuró originalmente con el asistente.

Antes de configurar otro servidor DNS en NetScaler Gateway, cree un servidor virtual que actúe como servidor DNS para la resolución de nombres.

Para agregar un servidor DNS o WINS dentro de un perfil de sesión

1. En la utilidad de configuración, ficha Configuración > **NetScaler Gateway > Directivas > Sesión**.
2. En el panel de detalles, en la ficha Perfiles, seleccione un perfil y, a continuación, haga clic en Abrir.
3. En la ficha Configuración de red, realice una de las siguientes acciones:
   - Para configurar un servidor DNS, junto a **Servidor virtual DNS**, haga clic en **Anular global**, seleccione el servidor y, a continuación, haga clic en **Aceptar**.
   - Para configurar un servidor WINS, junto a **IP del servidor WINS**, haga clic en **Anular global**, escriba la dirección IP y, a continuación, haga clic en **Aceptar**.

### Referencias

- Tunelización dividida
- Cómo se conectan los usuarios con el cliente Citrix Secure Access
- Acerca de NetScaler Gateway
- Seleccionar el método de acceso de usuario

## Seleccionar el método de acceso de usuario

Puede configurar NetScaler Gateway para proporcionar conexiones de usuario a través de los siguientes escenarios:

- Conexiones de usuario mediante la aplicación Citrix Workspace. Esta aplicación es compatible con StoreFront para proporcionar a los usuarios acceso a aplicaciones publicadas o escritorios virtuales en una granja de servidores. Es un software que utiliza el protocolo de red ICA para establecer conexiones de usuario. Los usuarios instalan la aplicación Citrix Workspace en el dispositivo de usuario. Cuando los usuarios instalan la aplicación en su equipo basado en Windows o Mac, esta engloba todos los plug-ins, incluido el cliente Citrix Secure Access para conexiones de usuario. NetScaler Gateway también admite conexiones desde la aplicación Citrix Workspace para Android y la aplicación Citrix Workspace para iOS. Los usuarios pueden

© 1997–2026 Citrix Systems, Inc. All rights reserved.

conectarse a sus escritorios virtuales y aplicaciones basadas en Windows, web, móviles y SaaS a través de Citrix Endpoint Management o StoreFront.

- Conexiones de usuario con Secure Hub. Los usuarios pueden conectarse a aplicaciones móviles, web y SaaS configuradas en Endpoint Management. Los usuarios instalan Secure Hub en su dispositivo móvil (Android o iOS). Cuando los usuarios inician sesión en Secure Hub, pueden instalar WorxMail y WorxWeb, junto con cualquier otra aplicación móvil que haya instalado en Endpoint Management. Secure Hub, Secure Mail y WorxWeb utilizan la tecnología Micro VPN para establecer conexiones a través de NetScaler Gateway.
- Conexiones de usuario mediante el cliente Citrix Secure Access™ como aplicación independiente. El cliente Citrix Secure Access es un software que los usuarios pueden descargar e instalar en un dispositivo de usuario. Cuando los usuarios inician sesión con el plug-in, pueden acceder a los recursos de la red segura como si estuvieran en la oficina. Los recursos incluyen servidores de correo electrónico, recursos compartidos de archivos y sitios web de intranet.
- Conexiones de usuario mediante acceso sin cliente. El acceso sin cliente proporciona a los usuarios el acceso que necesitan sin necesidad de instalar software, como el cliente Citrix Secure Access o la aplicación Citrix Workspace, en el dispositivo de usuario. El acceso sin cliente permite conexiones a un conjunto limitado de recursos web, como Outlook Web Access o SharePoint, aplicaciones publicadas en Citrix Virtual Apps, escritorios virtuales de Citrix Virtual Apps and Desktops y recursos compartidos de archivos en la red segura a través de la interfaz de acceso. Los usuarios se conectan introduciendo la dirección web de NetScaler Gateway en un navegador web y, a continuación, seleccionan el acceso sin cliente en la página de opciones.
- Conexiones de usuario si falla un análisis de preautenticación o postautenticación. Este escenario se denomina reserva de escenario de acceso. La reserva de escenario de acceso permite que un dispositivo de usuario vuelva del cliente Citrix Secure Access a StoreFront, mediante la aplicación Citrix Workspace, si el dispositivo de usuario no supera el análisis inicial de análisis de puntos finales.

  Si los usuarios inician sesión en NetScaler Gateway a través de la aplicación Citrix Workspace, el análisis de preautenticación no funciona. Los análisis de postautenticación sí funcionan cuando NetScaler Gateway establece el túnel VPN.

Los usuarios pueden descargar e instalar el cliente Citrix Secure Access mediante los siguientes métodos:

- Conectarse a NetScaler Gateway mediante un explorador web.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Conectarse a StoreFront configurado para aceptar conexiones de NetScaler Gateway.
- Instalar el plug-in mediante un objeto de directiva de grupo (GPO).
- Cargar el plug-in de NetScaler en el servidor de merchandising.

# Implementar el cliente Citrix Secure Access™ para el acceso de los usuarios

NetScaler Gateway incluye los siguientes plug-ins para el acceso de los usuarios:

- Cliente Citrix Secure Access para Windows
- Cliente Citrix Secure Access para Mac

Cuando los usuarios inician sesión en NetScaler Gateway por primera vez, descargan e instalan el cliente Citrix Secure Access desde una página web. Los usuarios inician sesión haciendo clic en el icono de NetScaler Gateway en el área de notificación de un equipo basado en Windows. En un equipo macOS X, los usuarios pueden iniciar sesión desde el menú **Dock o Aplicaciones**. Si actualiza NetScaler Gateway a una nueva versión de software, el cliente Citrix Secure Access se actualiza automáticamente en el dispositivo del usuario.

## Implementar el cliente Citrix Secure Access mediante el paquete de instalación MSI

Puede implementar el cliente Citrix Secure Access mediante una infraestructura de Microsoft Active Directory o una herramienta de implementación MSI estándar de terceros, como Windows Server Update Services. Si utiliza una herramienta compatible con los paquetes de Windows Installer, puede implementar los paquetes con cualquier herramienta compatible con archivos MSI. Luego, utilice su herramienta de implementación para implementar e instalar el software en los dispositivos de usuario adecuados.

### Ventajas de usar una herramienta de implementación centralizada

- Capacidad para cumplir los requisitos de seguridad. Por ejemplo, puede instalar software de usuario sin habilitar privilegios de instalación de software para usuarios no administrativos.
- Control sobre las versiones de software. Puede implementar una versión actualizada del software a todos los usuarios simultáneamente.
- Escalabilidad. Una estrategia de implementación centralizada se escala fácilmente para admitir más usuarios.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Experiencia de usuario positiva. Puede implementar, probar y solucionar problemas relacionados con la instalación sin involucrar a los usuarios en este proceso.

Citrix® recomienda esta opción cuando se prefiere el control administrativo sobre la instalación del software de usuario y el acceso a los dispositivos de usuario está fácilmente disponible.

Para obtener más información, consulte Implementación del cliente Citrix Secure Access desde Active Directory.

### Determinar qué plug-in de software implementar

Si su implementación de NetScaler Gateway no requiere ningún plug-in de software en los dispositivos de los usuarios, se considera que su implementación proporciona acceso sin cliente. En este escenario, los usuarios solo necesitan un navegador web para acceder a los recursos de red. Sin embargo, ciertas funciones requieren el software del plug-in en el dispositivo del usuario.

## Seleccionar el Citrix Secure Access™ client para los usuarios

Al configurar NetScaler Gateway, puede elegir cómo inician sesión los usuarios. Los usuarios pueden iniciar sesión con uno de los siguientes plug-ins:

- Citrix Secure Access client para Windows
- Citrix Secure Access client para macOS

La configuración se completa creando una directiva de sesión y, a continuación, vinculando la directiva a usuarios, grupos o servidores virtuales. También puede habilitar los plug-ins configurando los ajustes globales. Dentro del perfil global o de sesión, seleccione Windows o macOS X como tipo de plug-in. Cuando los usuarios inician sesión, reciben el plug-in tal como se define globalmente o en el perfil y la directiva de sesión. Cree perfiles separados para el tipo de plug-in.

### Configurar el plug-in globalmente

1. Vaya a **NetScaler Gateway > Global Settings**.
2. En el panel de detalles, en **Settings**, haga clic en **Change global settings**.
3. En la ficha **Client Experience**, junto a **Plug-in Type**, seleccione **Windows/MAC OS X** y, a continuación, haga clic en **OK**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

## Configurar el tipo de plug-in para Windows o macOS en un perfil de sesión

1. Vaya a **NetScaler Gateway > Policies > Session**.
2. Realice una de las siguientes acciones:
   - Si está creando una directiva de sesión, en el panel de detalles, haga clic en **Add**.
   - Si está cambiando una directiva existente, seleccione una directiva y, a continuación, haga clic en **Open**.
3. Cree un perfil o modifique uno existente. Para ello, realice una de las siguientes acciones:
   - Junto a **Perfil**, haga clic en **Agregar**.
   - Junto a **Perfil**, haga clic en **Editar**.
4. En la ficha **Client Experience**, junto a **Plug-in Type**, haga clic en **Override Global** y, a continuación, seleccione **Windows/MAC OS X**.
5. Realice una de las siguientes acciones:
   - Si está creando un perfil, haga clic en **Crear**, establezca la expresión en el cuadro de diálogo de la directiva, haga clic en **Crear** y, a continuación, haga clic en **Cerrar**.
   - Si está modificando un perfil existente, después de realizar la selección, haga clic en **Aceptar** dos veces.

## Cliente Citrix Secure Access para Windows

Cuando los usuarios inician sesión en NetScaler Gateway, descargan e instalan el cliente Citrix Secure Access en el dispositivo del usuario.

Para instalar el plug-in, los usuarios deben ser un administrador local o un miembro del grupo Administradores. Esta restricción se aplica solo a la primera instalación. Las actualizaciones del plug-in no requieren acceso de nivel de administrador.

Para permitir que los usuarios se conecten y utilicen NetScaler Gateway, debe proporcionarles la siguiente información:

- Dirección web de NetScaler Gateway, como `<https://NetScalerGatewayFQDN/>`
- Cualquier requisito del sistema para ejecutar el cliente Citrix Secure Access si configuró recursos y directivas de punto final

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Según la configuración del dispositivo del usuario, es posible que también deba proporcionar la siguiente información:

- Si los usuarios ejecutan un firewall en su equipo, deben cambiar la configuración del firewall para que no bloquee el tráfico hacia o desde las direcciones IP correspondientes a los recursos a los que se les concedió acceso. El cliente Citrix Secure Access gestiona automáticamente el Firewall de conexión a Internet en Windows XP y el Firewall de Windows en Windows XP Service Pack 2, Windows Vista, Windows 7, Windows 8 o Windows 8.1.
- Los usuarios que deseen enviar tráfico a FTP a través de una conexión de NetScaler Gateway deben configurar su aplicación FTP para realizar transferencias pasivas. Una transferencia pasiva significa que el equipo remoto establece la conexión de datos con su servidor FTP, en lugar de que el servidor FTP establezca la conexión de datos con el equipo remoto.
- Los usuarios que deseen ejecutar aplicaciones cliente X a través de la conexión deben ejecutar un servidor X, como `XManager`, en sus equipos.
- Los usuarios que instalan Receiver para Windows o Receiver para Mac pueden iniciar el cliente Citrix Secure Access desde Receiver o mediante un explorador web. Proporcione instrucciones a los usuarios sobre cómo iniciar sesión con el cliente Citrix Secure Access a través de Receiver o un explorador web.

Dado que los usuarios trabajan con archivos y aplicaciones como si fueran locales en la red de la organización, no es necesario volver a capacitarlos ni configurar las aplicaciones.

Para establecer una conexión segura por primera vez, inicie sesión en NetScaler Gateway mediante la página de inicio de sesión web. El formato típico de una dirección web es `<https://companyname.com>`. Cuando los usuarios inician sesión, pueden descargar e instalar el cliente Citrix Secure Access en su equipo.

### Instalar el cliente Citrix Secure Access para Windows

1. En un explorador web, escriba la dirección web de NetScaler Gateway.
2. Escriba el nombre de usuario y la contraseña y, a continuación, haga clic en Iniciar sesión.
3. Seleccione Acceso a la red y, a continuación, haga clic en Descargar.
4. Siga las instrucciones para instalar el plug-in.

Cuando la descarga se completa, el cliente Citrix Secure Access se conecta y muestra un mensaje en el área de notificación de un equipo basado en Windows.

Si desea que los usuarios se conecten con el cliente Citrix Secure Access sin usar un explorador web, puede configurar el plug-in para que muestre el cuadro de diálogo de inicio de sesión cuando

© 1997–2026 Citrix Systems, Inc. All rights reserved.

los usuarios hagan clic con el botón secundario en el icono de **NetScaler Gateway** en el área de notificación de un equipo basado en Windows o inicien el plug-in desde el menú Inicio.

### Configurar el cuadro de diálogo de inicio de sesión para el cliente Citrix Secure Access para Windows

Para configurar el cliente Citrix Secure Access para que use el cuadro de diálogo de inicio de sesión, los usuarios deben haber iniciado sesión para completar este procedimiento.

1. En un equipo basado en Windows, en el área de notificación, haga clic con el botón secundario en el icono de NetScaler Gateway y, a continuación, haga clic en **Configurar NetScaler Gateway**.
2. Haga clic en la ficha **Perfil** y, a continuación, haga clic en **Cambiar perfil**.
3. En la pestaña **Opciones**, haga clic en **Usar el cliente Citrix Secure Access para el inicio de sesión**.

> **NOTA:**
>
> Si los usuarios abren el cuadro de diálogo **Configurar NetScaler Gateway** desde Receiver, la pestaña **Opciones** no está disponible.

### Establecer el modo de intercepción para el cliente Citrix Secure Access para Windows

Si está configurando el cliente Citrix Secure Access para Windows, también debe configurar el modo de intercepción y establecerlo en transparente.

1. En la utilidad de configuración, haga clic en la ficha Configuración, expanda **NetScaler Gateway > Recursos** y, a continuación, haga clic en **Aplicaciones de intranet**.
2. En el panel de detalles, haga clic en **Agregar**.
3. En **Nombre**, escriba un nombre para la directiva.
4. Haga clic en **Transparente**.
5. En **Protocolo**, seleccione **CUALQUIERA**.
6. En **Tipo de destino**, seleccione **Dirección IP y máscara de red**.
7. En **Dirección IP**, escriba la dirección IP.
8. En **Máscara de red**, escriba la máscara de subred, haga clic en **Crear** y, a continuación, haga clic en **Cerrar**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

### Compatibilidad con Microsoft Edge WebView para Citrix Secure Access de Windows

La compatibilidad con Microsoft Edge WebView para Citrix Secure Access de Windows introduce una experiencia de usuario final mejorada. Para obtener más información, consulte Compatibilidad con Microsoft Edge WebView para Citrix Secure Access de Windows

### Cliente de Citrix Secure Access para Windows que utiliza la Plataforma de filtrado de Windows

La Plataforma de filtrado de Windows (WFP) es un conjunto de API y servicios del sistema que proporcionan una plataforma para crear aplicaciones de filtrado de red. WFP está diseñada para reemplazar las tecnologías anteriores de filtrado de paquetes, el filtro de la Especificación de interfaz de controlador de red (NDIS), que se utilizaba con el controlador DNE. El modo WFP es compatible con la compilación 22.6.1.5 del cliente de Citrix Secure Access para Windows.

#### Instalar la compilación WFP

Puede instalar la compilación WFP utilizando uno de los siguientes métodos.

- Instale el complemento VPN con los controladores DNE y WFP (método predeterminado)

  Cuando el complemento se instala con los controladores DNE y WFP, los administradores pueden usar el controlador WFP o el controlador DNE para la tunelización mediante un ajuste del registro. De forma predeterminada, el controlador DNE se utiliza para la tunelización.
- Instale el complemento VPN solo con el controlador WFP (omitir la instalación del controlador DNE)

  Los controladores DNE no son compatibles con algunas aplicaciones de terceros, incluso cuando no están en uso. Para esas implementaciones, los administradores pueden usar este tipo de instalación. Como el controlador DNE no está instalado, solo se utiliza el controlador WFP para la tunelización.

#### Seleccionar un controlador WFP en lugar de un controlador DNE

Realice los siguientes pasos para seleccionar el controlador WFP en lugar del controlador DNE.

**NOTA:**

Esto solo funciona con el método de instalación predeterminado.

1. Descargue la compilación del complemento VPN compatible con WFP e instale el nuevo complemento VPN.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. De forma predeterminada, el controlador DNE se utiliza para tunelizar el tráfico. Para usar el controlador WFP para la tunelización, los administradores deben crear la siguiente entrada de registro:

   - REG_PATH - HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Client
     - REG_TYPE - REG_DWORD
     - REG_NAME - EnableWFP
     - REG_VALUE – Establezca el valor en 1 para usar WFP y en 0 para usar DNE (por defecto, DNE está habilitado si este valor de registro no está presente o está establecido en 0)

**NOTA:**

Después de cambiar el modo de tunelización de DNE a WFP o viceversa, el sistema debe reiniciarse para que los cambios surtan efecto correctamente.

### Omitir completamente la instalación de DNE

Realice los siguientes pasos para omitir la instalación de DNE.

1. Realice una desinstalación limpia del complemento VPN.

   a. Desinstale el complemento VPN actual presente en la máquina y reinicie la máquina.

   b. Compruebe si el controlador DNE está desinstalado mediante cualquiera de las siguientes opciones.

      - Abra un símbolo del sistema elevado (o PowerShell). Ejecute los siguientes comandos (la salida de ejemplo muestra que el controlador basado en DNE está instalado en el sistema)

```
PS C:\Users\Administrator> sc qc cag

[SC] QueryServiceConfig SUCCESS

SERVICE_NAME: cag

TYPE               : 1  KERNEL_DRIVER

START_TYPE         : 2   AUTO_START
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
ERROR_CONTROL      : 1   NORMAL

BINARY_PATH_NAME   : \??\C:\Program Files\Common Files\Deterministic
Networks\Common Files\cag.sys

LOAD_ORDER_GROUP   :

TAG                : 0

DISPLAY_NAME       : Citrix cag plugin for Access Gateway

DEPENDENCIES       :

SERVICE_START_NAME :

PS C:\Users\Administrator> sc qc dne

[SC] QueryServiceConfig SUCCESS



SERVICE_NAME: dne

TYPE               : 1  KERNEL_DRIVER

START_TYPE         : 1   SYSTEM_START

ERROR_CONTROL      : 1   NORMAL

BINARY_PATH_NAME   : \SystemRoot\system32\DRIVERS\dnelwf64.sys

LOAD_ORDER_GROUP   : NDIS

TAG                : 38

DISPLAY_NAME       : DNE LightWeight Filter

DEPENDENCIES       :

SERVICE_START_NAME :
```

Si el controlador no está instalado, se muestra la siguiente salida:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

`The specified service does not exist as an installed service.`.

Dado que el controlador DNE (dnelwf64.sys) también es utilizado por otros proveedores, podría estar presente incluso cuando el cliente Citrix Secure Access no está instalado en el sistema. Por otro lado, el complemento CAG solo es utilizado por el cliente Citrix Secure Access.

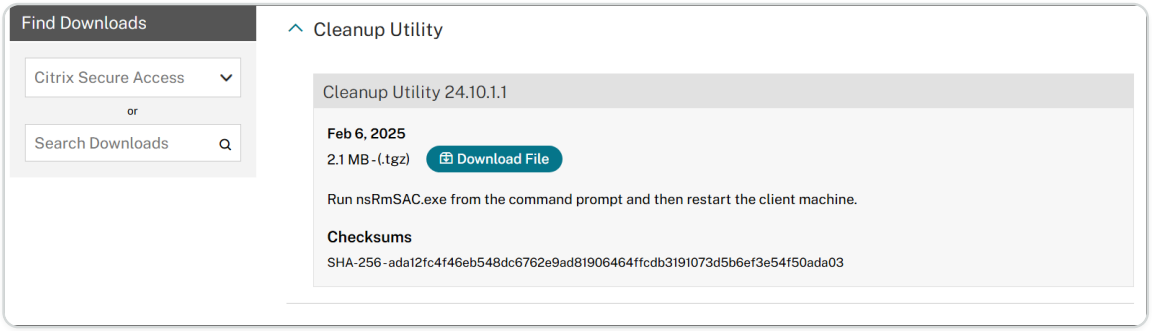
- La presencia de DNE también se puede comprobar intentando iniciar los controladores CAG y DNE. Abra el símbolo del sistema con derechos de administrador y ejecute los siguientes comandos:

```
net start cag

net start dne
```

  - Si el mensaje de salida indica que no se pueden localizar los servicios (El nombre del servicio no es válido.), entonces los componentes del complemento y del controlador se desinstalan correctamente. En este caso, pase al paso 2.
  - Si los componentes del complemento y del controlador no se desinstalan correctamente, ejecute la utilidad de limpieza nsRmSac.exe en la máquina cliente siguiendo estas instrucciones:
    - Descomprima la utilidad de limpieza y cópiela en una carpeta.
    - Ejecute nsRmSAC.exe desde el símbolo del sistema con privilegios de administrador.
    - Reinicie la máquina cliente.

    La utilidad de limpieza nsRmSac.exe está disponible en la página Citrix Downloads en la sección **Utilidad de limpieza**.




© 1997–2026 Citrix Systems, Inc. All rights reserved.

**NOTA:**

A partir de la versión 24.10.1.5 del cliente Citrix Secure Access para Windows, la utilidad de limpieza nsRmSac.exe admite los argumentos de línea de comandos `/quiet` y `/autoreboot`. El comando nsRmSac.exe `/quiet /autoreboot` permite que la utilidad de limpieza se ejecute sin intervención manual.

- La opción `/quiet` elimina la aplicación Citrix Secure Access y el controlador asociado.
- La opción `/autoreboot` reinicia el sistema una vez que la utilidad nsRmSac.exe finaliza la función de limpieza. El argumento `/autoreboot` solo funciona con la opción `/quiet`.

2. Cree las siguientes entradas de registro.

- REG_PATH - HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Client
  - REG_TYPE - REG_DWORD
  - REG_NAME - SkipDNE
  - REG_VALUE - Establezca en 1 para asegurarse de que DNE no esté instalado en la máquina
- REG_PATH - HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Client
  - REG_TYPE - REG_DWORD
  - REG_NAME - EnableWFP
  - REG_VALUE - Establezca en 1 para habilitar WFP (esta entrada debe crearse si se omite la instalación de DNE)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**NOTA:**

- Si las entradas del registro no se crean antes de la instalación, DNE se instala de forma predeterminada. Además, puede comprobar los archivos de registro de VPN para validar si se utiliza WFP o DNE.
- Si se omite la instalación de DNE, EnableWFP debe establecerse en 1. En este caso, no puede cambiar al complemento basado en DNE sin reinstalar el cliente de Citrix Secure Access.

3. Instale el nuevo complemento VPN.
4. Confirme si el controlador WFP está instalado en el sistema. Abra un símbolo del sistema con privilegios elevados y ejecute el siguiente comando. La salida de ejemplo muestra que el controlador WFP está instalado en el sistema.

```
PS C:\Users\Administrator> sc qc ctxsgwcallout

[SC] QueryServiceConfig SUCCESS



SERVICE_NAME: ctxsgwcallout

    TYPE               : 1  KERNEL_DRIVER

    START_TYPE         : 1   SYSTEM_START

    ERROR_CONTROL      : 0   IGNORE

    BINARY_PATH_NAME   : \??\C:\Program Files\Citrix\Secure Access
Client\ctxsgwcallout.sys

    LOAD_ORDER_GROUP   :

    TAG                : 0

    DISPLAY_NAME       : Citrix Secure Access Callout Driver

    DEPENDENCIES       :
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
SERVICE_START_NAME :
```

Si el controlador no está instalado, se muestra la siguiente salida:

`The specified service does not exist as an installed service.`.

5. Reinicie la máquina cliente.

### Ventajas de WFP

Las siguientes son algunas de las ventajas de WFP si la instalación del controlador WFP independiente se realiza en el cliente.

- **Soporte de túnel dividido inverso basado en FQDN:** El controlador WFP permite el soporte para el tunelado dividido INVERSO basado en FQDN. No es compatible con el controlador DNE. Para obtener más detalles, consulte Opciones de tunelado dividido.
- **Soporte de Wireshark:** DNE no permite capturar tráfico bidireccional en una máquina cliente debido a su vinculación con el adaptador Ethernet/Wi-Fi. Esto no es un problema con el nuevo controlador WFP. Cualquier captura de tráfico (unidireccional o bidireccional) está cifrada y requiere claves SSL para descifrarla.
- **Soporte de NMAP:** El nuevo controlador WFP admite el escaneo NMAP mientras el complemento VPN se utiliza para tunelar el tráfico, mientras que DNE no permite el escaneo NMAP mientras el complemento VPN se utiliza para tunelar el tráfico.
- **Velocidad de red:** En algunos escenarios, si DNE está instalado en una máquina cliente, la velocidad de descarga y carga se ve afectada, lo que no ocurre con WFP.
- **Rendimiento mejorado de nslookup:** A veces, con DNE, `nslookup` no responde con un menor número de intentos, y esto no se observa con WFP.
- **Rendimiento mejorado de iperf sobre UDP:** Con DNE, se observó cierta pérdida de paquetes durante las pruebas de escalabilidad usando iperf sobre UDP. No se observa pérdida de paquetes con WFP.

## Cliente de Citrix Secure Access para macOS

1. Descargue la aplicación Citrix Secure Access para macOS/iOS desde la App Store.
2. Haga clic en **Abrir** una vez que la descarga se haya completado.

Para obtener detalles sobre cómo usar Citrix Secure Access para macOS, consulte Cómo usar la aplicación Citrix Secure Access desde su dispositivo macOS.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

## Aplicar el acceso a la LAN local a los usuarios finales según la configuración de ADC

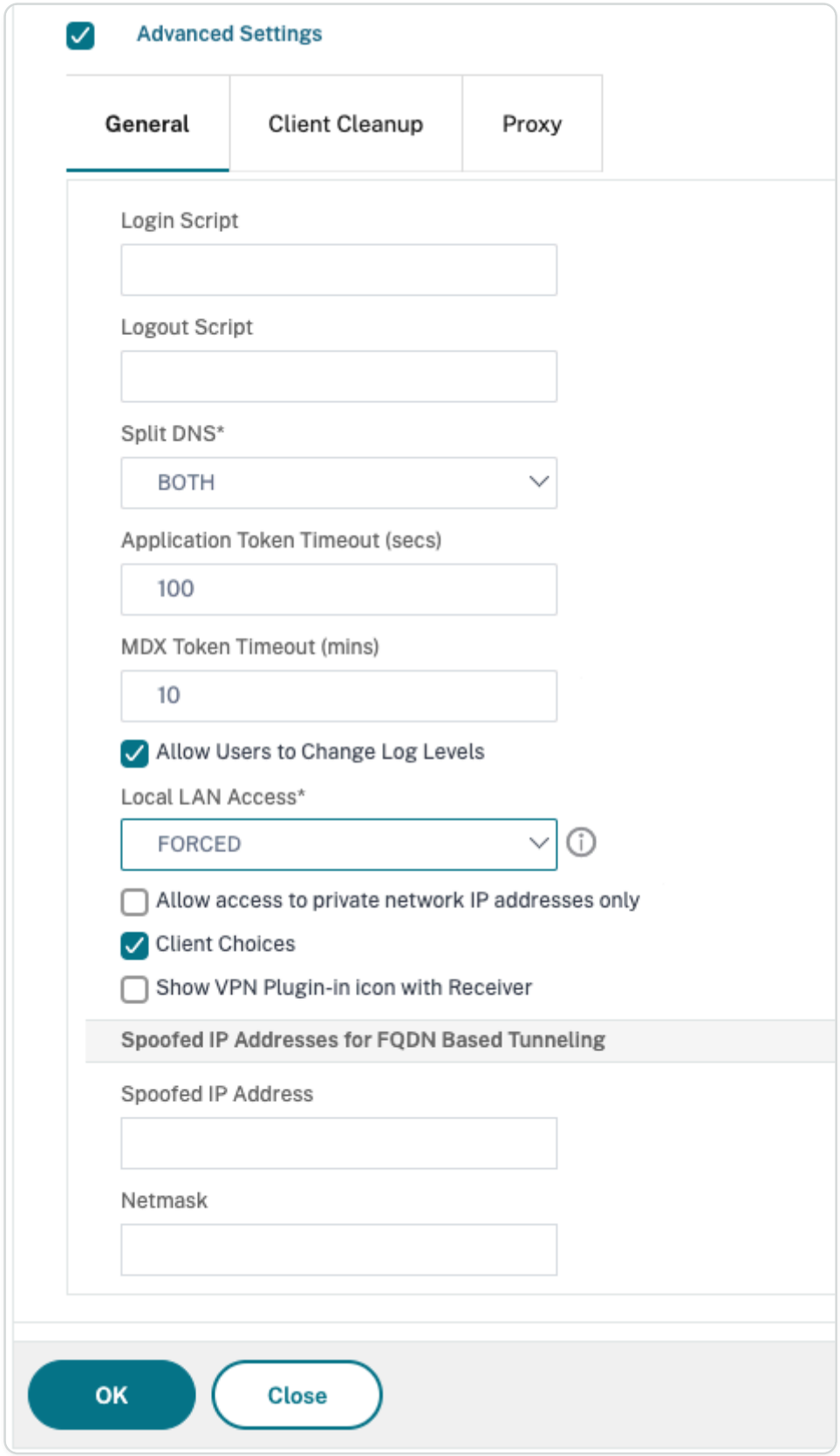
Los administradores pueden restringir a los usuarios finales la desactivación de la opción de acceso a la LAN local en sus máquinas cliente. Se añade una nueva opción, FORZADO, a los valores existentes del parámetro Acceso a la LAN local. Cuando el valor de Acceso a la LAN local se establece en FORZADO, el acceso a la LAN local siempre está habilitado para los usuarios finales en las máquinas cliente. Los usuarios finales no pueden deshabilitar la configuración de la LAN local utilizando la interfaz de usuario del cliente de Citrix Secure Access.

Los administradores pueden permitir a los usuarios finales acceder a los recursos de la LAN local en su máquina cliente configurando el parámetro de acceso a la LAN local en ON. Para impedir que los usuarios finales accedan a los recursos de la LAN local en su máquina cliente, los administradores pueden configurar el parámetro de acceso a la LAN local en OFF. Para obtener detalles sobre las configuraciones de usuario final, consulte Acceso a la LAN local para macOS y Acceso a la LAN local para iOS.

**Para habilitar la opción Forzado mediante la GUI:**

1. Vaya a **NetScaler Gateway > Configuración global > Cambiar configuración global**.
2. Haga clic en la ficha **Experiencia del cliente** y, a continuación, haga clic en **Configuración avanzada**.
3. En **Acceso a la LAN local**, seleccione **FORZADO**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.




**Para habilitar la opción Forzado mediante la CLI, ejecute el siguiente comando:**

```
set vpn parameter -localLanAccess FORCED
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**NOTAS:**

- El cliente de Citrix Secure Access para macOS/iOS y versiones posteriores admite la funcionalidad de acceso a la LAN local de NetScaler Gateway.
- A partir del cliente de Citrix Secure Access para Windows 23.10.1.7, el acceso a la LAN local es compatible en un túnel a nivel de máquina si el parámetro Acceso a la LAN local se establece en **Forzado** en NetScaler Gateway.

## Implementar el cliente Citrix Secure Access™ desde Active Directory

Si los usuarios no tienen privilegios administrativos para instalar el cliente Citrix Secure Access en el dispositivo del usuario, puede implementar el complemento para los usuarios desde Active Directory. Cuando utiliza este método para implementar el cliente Citrix Secure Access, puede extraer el programa de instalación y, a continuación, utilizar una directiva de grupo para implementar el programa. Los pasos generales para este tipo de implementación son:

- Extracción del paquete MSI.
- Distribución del complemento mediante una directiva de grupo.
- Creación de un punto de distribución.
- Asignación del paquete del cliente Citrix Secure Access mediante un objeto de directiva de grupo.

  **Nota:** La distribución del cliente Citrix Secure Access desde Active Directory solo es compatible con Windows 7, Windows 8 y Windows 10.

Puede descargar el paquete MSI desde la utilidad de configuración o desde el sitio web de Citrix®.

### Para descargar el paquete MSI del cliente Citrix Secure Access desde la utilidad de configuración

1. En la utilidad de configuración, haga clic en **Descargas**.
2. En Cliente Citrix Secure Access, haga clic en **Descargar complemento de NetScaler Gateway para Windows** y, a continuación, guarde el archivo **nsvpnc_setup.exe** en su servidor Windows.

   **Nota:**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Para máquinas de 64 bits, debe guardar el archivo Agee_setup.exe en su servidor Windows.
- Si no aparece el cuadro de diálogo **Descarga de archivos**, pulse la tecla CTRL al hacer clic en el enlace **Descargar cliente Citrix Secure Access para Windows**.

3. En un símbolo del sistema, vaya a la carpeta donde guardó **nsvpnc_setup.exe** y, a continuación, escriba:

   ```
   nsvpnc_setup /c
   ```

   Esto extrae el archivo agee.msi.

   **Nota:** Para máquinas de 64 bits, vaya a la carpeta donde guardó **Agee_setup.exe** y, a continuación, escriba:

   ```
   Agee_setup.exe /c
   ```

   Esto extrae el archivo agee64.msi.
4. Guarde el archivo extraído en una carpeta del servidor Windows.

Después de extraer el archivo, utilice una directiva de grupo en Windows Server para distribuir el archivo.

Antes de iniciar la distribución, instale la Consola de administración de directivas de grupo en Windows Server 2003, Windows Server 2008 o Windows Server 2012. Para obtener más información, consulte la ayuda en línea de Windows.

**Nota:** Cuando utiliza una directiva de grupo para publicar el cliente de Citrix Secure Access, Citrix recomienda asignar el paquete al dispositivo de usuario. El paquete MSI se instala por dispositivo.

Antes de poder distribuir el software, cree un punto de distribución en un recurso compartido de red en un servidor de publicación, como Microsoft Internet Security and Acceleration (ISA) Server.

### Para crear un punto de distribución

1. Inicie sesión en el servidor de publicación como administrador.
2. Cree una carpeta y compártala en la red con permiso de lectura para todas las cuentas que necesiten acceso al paquete de distribución.
3. En el símbolo del sistema, vaya a la carpeta donde guardó el archivo extraído y, a continuación, escriba: msiexec -a agee.msi

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. En la pantalla **Ubicación de red**, haga clic en **Cambiar** y, a continuación, vaya a la carpeta compartida donde desea crear la instalación administrativa del cliente de Citrix Secure Access.
5. Haga clic en **Aceptar** y, a continuación, haga clic en **Instalar**.

Después de haber colocado el paquete extraído en el recurso compartido de red, asigne el paquete a un objeto de directiva de grupo en Windows.

Después de configurar correctamente el cliente Citrix Secure Access como un paquete de software administrado, el complemento se instala automáticamente la próxima vez que se inicie el dispositivo del usuario.

**NOTA:**

Cuando el paquete de instalación se asigna a un equipo, el usuario debe reiniciar el equipo.

Cuando se inicia la instalación, los usuarios reciben un mensaje de que el cliente Citrix Secure Access se está instalando.

## Administrar el cliente Citrix Secure Access™ mediante Active Directory

Cada versión del cliente Citrix Secure Access se empaqueta como una instalación completa del producto, en lugar de como un parche. Cuando los usuarios inician sesión y el cliente Citrix Secure Access detecta una nueva versión del plug-in, el plug-in se actualiza automáticamente. También puede implementar el cliente Citrix Secure Access para actualizarlo mediante Active Directory.

Para ello, cree un punto de distribución para el cliente Citrix Secure Access. Cree un objeto de directiva de grupo y asígnele la nueva versión del plug-in. A continuación, cree un vínculo entre el nuevo paquete y el paquete existente. Después de crear el vínculo, el cliente Citrix Secure Access se actualiza.

### Eliminar el cliente Citrix Secure Access de los dispositivos de usuario

Para eliminar el cliente Citrix Secure Access de los dispositivos de usuario, elimine el paquete asignado del Editor de objetos de directiva de grupo.

Cuando se elimina el plug-in del dispositivo de usuario, los usuarios reciben un mensaje de que el plug-in se está desinstalando.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

### Solucionar problemas de instalación del cliente Citrix Secure Access mediante Active Directory

Si el paquete asignado no se instala cuando se inicia el dispositivo de usuario, es posible que vea la siguiente advertencia en el registro de eventos de la aplicación:

No se pudieron aplicar los cambios a la configuración de instalación del software. La aplicación de la directiva de instalación de software se ha retrasado hasta el siguiente inicio de sesión porque un administrador ha habilitado la optimización del inicio de sesión para la directiva de grupo. El error fue: El marco de la directiva de grupo debe llamar a la extensión en la actualización de la directiva de primer plano sincrónica.

Este error es causado por la optimización de inicio de sesión rápido (Fast Logon Optimization) en Windows XP, en la que se permite a los usuarios iniciar sesión antes de que el sistema operativo inicialice todos los componentes de red, incluido el procesamiento de objetos de directiva de grupo. Algunas directivas pueden requerir más de un reinicio para surtir efecto. Para resolver este problema, deshabilite la optimización de inicio de sesión rápido en Active Directory.

Para solucionar otros problemas de instalación de software administrado, Citrix® recomienda usar una directiva de grupo para habilitar el registro del instalador de Windows.

## Integrar el cliente Citrix Secure Access con la aplicación Citrix Workspace

NetScaler Gateway es compatible con la aplicación Citrix Workspace. El sistema orquestado consta de los siguientes componentes:

- Aplicación Citrix Workspace para Windows 3.4 o posterior
- Aplicación Citrix Workspace para Mac
- Aplicación Citrix Workspace para Android
- Aplicación Citrix Workspace para iOS
- StoreFront 2.1 o posterior
- Endpoint Management 2.8 y posterior o Citrix Endpoint Management 10
- Servicio Citrix Update alojado en el sitio web de Citrix

Para obtener más información sobre la compatibilidad de NetScaler Gateway con los productos de Citrix, consulte (/es-es/netscaler-gateway/13-1/citrix-prod-compatibility.html)Compatibilidad con los productos de Citrix.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Puede configurar NetScaler Gateway para que, cuando los usuarios inicien sesión en el dispositivo, el cliente Citrix Secure Access abra un explorador web que permita el inicio de sesión único en la página de inicio de la aplicación Citrix Workspace. Los usuarios pueden descargar la aplicación Citrix Workspace desde la página de inicio.

Cuando los usuarios inician sesión con la aplicación Citrix Workspace, las conexiones de usuario se pueden enrutar a través de NetScaler Gateway de la siguiente manera:

- Directamente a Endpoint Management
- Directamente a StoreFront™
- A StoreFront y luego a Endpoint Management si no configura las aplicaciones móviles MDX en Endpoint Management
- A Endpoint Management y luego a StoreFront si configura aplicaciones móviles MDX en Endpoint Management

**NOTA:**

Las conexiones que se enrutan directamente a Endpoint Management solo son compatibles con Endpoint Management 2.0, Endpoint Management 2.5, Endpoint Management 2.6, Endpoint Management 2.8 y Endpoint Management 2.9. Si tiene Endpoint Management 1.1 implementado en su red, las conexiones de usuario deben enrutarse a través de StoreFront.

## Cómo se conectan los usuarios con la aplicación Citrix Workspace

Los usuarios pueden conectarse a las siguientes aplicaciones, escritorios y datos desde la aplicación Citrix Workspace:

- Aplicaciones basadas en Windows y escritorios virtuales publicados en StoreFront™
- Datos de ShareFile a los que se accede a través de Citrix Endpoint Management™

Los usuarios pueden iniciar sesión con cualquiera de las siguientes aplicaciones Citrix Workspace:

- Aplicación Citrix Workspace para Web
- Aplicación Citrix Workspace para Windows
- Aplicación Citrix Workspace para Mac
- Aplicación Citrix Workspace para iOS
- Aplicación Citrix Workspace para Android

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Los usuarios pueden iniciar sesión con la aplicación Citrix Workspace para Web mediante un explorador web o desde el icono de la aplicación Citrix Workspace en el dispositivo del usuario.

Cuando los usuarios inician sesión con cualquier versión de la aplicación Citrix Workspace, las aplicaciones, los datos de ShareFile y los escritorios aparecen en el explorador o en la ventana de la aplicación Citrix Workspace.

## Desacoplar el icono de la aplicación Citrix Workspace

Cuando una implementación de Citrix Virtual Apps and Desktops está configurada con el cliente Citrix Secure Access integrado con la aplicación Citrix Workspace, el icono del complemento no es visible para un usuario conectado a la VPN. El icono de **Citrix Secure Access** normalmente reside en la bandeja del sistema de Windows o en la barra de menú del Finder de macOS X. Este icono es la interfaz para la configuración y los controles del complemento. Para los usuarios de Windows, cuando la aplicación Citrix Workspace y el cliente Citrix Secure Access están integrados, el cuadro de diálogo **Acerca de** en la aplicación Citrix Workspace muestra los controles del cliente Citrix Secure Access. Para los usuarios de macOS X, no hay controles disponibles para el cliente Citrix Secure Access después de la integración.

Algunas implementaciones integradas pueden requerir exponer los controles del complemento mientras se mantiene la integración de la funcionalidad subyacente. Para ello, utilice el siguiente comando de CLI o la tarea de la utilidad de configuración de NetScaler para alternar la integración del icono para los clientes VPN.

### Configurar la integración del icono mediante la CLI

En el símbolo del sistema, escriba;

```
set vpn parameter [-iconWithReceiver (ON/OFF)]
```

### Configurar la integración del icono mediante la GUI

1. En la ficha Configuración, vaya a **NetScaler Gateway > Configuración global**.
2. Haga clic en **Cambiar configuración global** y, a continuación, seleccione la ficha **Experiencia del cliente**.
3. Haga clic en **Configuración avanzada.**
4. Seleccione **Mostrar icono del complemento VPN** con la aplicación Citrix Workspace.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

## Configurar IPv6 para conexiones ICA®

NetScaler Gateway admite direcciones IPv6 para conexiones ICA. Las conexiones con IPv6 a StoreFront funcionan igual que las conexiones IPv4. Cuando los usuarios se conectan mediante la dirección web de NetScaler Gateway, NetScaler Gateway actúa como proxy de la conexión a StoreFront.

Puede configurar IPv6 para NetScaler Gateway implementado en una DMZ o implementado en una DMZ de doble salto.

Puede habilitar IPv6 en NetScaler Gateway mediante la línea de comandos. Puede utilizar las siguientes directrices:

- Habilite IPv6 en el dispositivo.
- Configure las direcciones IP de subred.
- Establezca el orden de resolución de DNS.
- Establezca una dirección web de StoreFront™.
- Vincule la Autoridad de tickets seguros (STA) a NetScaler Gateway.

De forma predeterminada, la dirección IP asignada no admite direcciones IPv6. Para enrutar las comunicaciones de los usuarios a la red interna, debe crear direcciones IP de subred y, a continuación, configurar NetScaler Gateway para que utilice las direcciones IP de subred.

Si implementa varias subredes IPv6 en su red, cree varias direcciones IP de subred IPv6 en NetScaler Gateway, una para cada subred de su red. El enrutamiento de red envía los paquetes IPv6 a las subredes respectivas mediante las direcciones IP de subred.

### Para configurar IPv6 para ICA Proxy mediante la CLI

1. Inicie sesión en NetScaler Gateway mediante una conexión Secure Shell (SSH), como desde PuTTY. En el símbolo del sistema, escriba;

```
enable ns feature IPv6PT. This enables IPv6.



enable ns mode USNIP.



set dns parameter –resolutionOrder AAAAThenAQuery AThenAAAAQuery
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
OnlyAAAAQuery OnlyAQuery



set vpn parameter -wihome `http://XD_domain/Citrix/StoreWeb`
```

Donde <XD_domain> es el nombre de dominio o la dirección IP de StoreFront.

**Ejemplo:**

```
set vpn parameter -wihome `http://storefront.domain.com/Citrix/StoreWeb`.
```

O

```
set vpn parameter -wihome `http://[1000:2000::3000]/Citrix/StoreWeb`
```

**NOTA:**

Si utiliza la dirección IPv6 para configurar este parámetro, la dirección IP debe ir entre corchetes.

## Configurar la página de inicio de la aplicación Citrix Workspace en NetScaler Gateway

Puede configurar la página de inicio de la aplicación Citrix Workspace de forma global o como parte de un perfil de sesión. Si quiere configurar la aplicación Citrix Workspace para Web y versiones anteriores de la aplicación Citrix Workspace que no reconocen StoreFront a través de NetScaler Gateway, debe crear dos perfiles de sesión independientes. El campo Página de inicio de la aplicación Citrix Workspace debe tener la dirección web correcta para cada perfil para que los usuarios puedan iniciar sesión correctamente.

Para las aplicaciones Citrix Workspace que reconocen StoreFront a través de NetScaler Gateway, la aplicación Citrix Workspace para Web y la aplicación Citrix Workspace pueden compartir un perfil. Sin embargo, Citrix recomienda configurar un perfil de sesión para la aplicación Citrix Workspace para Web y un perfil de sesión independiente para todas las demás aplicaciones Citrix Workspace.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

### Para configurar la página de inicio de la aplicación Citrix Workspace globalmente

Para configurar la página de inicio de la aplicación Citrix Workspace globalmente:

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda NetScaler Gateway y, a continuación, haga clic en Configuración global.
2. En el panel de detalles, en Configuración, haga clic en Cambiar configuración global.
3. En el cuadro de diálogo Configuración global de NetScaler Gateway, haga clic en la ficha Aplicaciones publicadas.
4. En Página de inicio de la aplicación Citrix Workspace, escriba la dirección web de la aplicación Citrix Workspace o la página de inicio de la aplicación Citrix Workspace para Web y, a continuación, haga clic en Aceptar.

### Para configurar la página de inicio de la aplicación Citrix Workspace en un perfil de sesión

Para configurar la página de inicio de la aplicación Citrix Workspace en un perfil de sesión:

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda **NetScaler Gateway > Directivas** y, a continuación, haga clic en **Sesión**.
2. En el panel de detalles, en la ficha **Perfiles**, haga clic en **Agregar**.
3. En el cuadro de diálogo **Crear perfil de sesión de NetScaler Gateway**, en la ficha **Aplicación publicada**, junto a **Página de inicio de Citrix Receiver**, haga clic en **Anular global**.
4. En la página de inicio de la aplicación Citrix Workspace, escriba la dirección web de la aplicación Citrix Workspace o la página de inicio de la aplicación Citrix Workspace para Web y, a continuación, haga clic en **Crear**.

## Aplicar el tema de la aplicación Citrix Workspace a la página de inicio de sesión de NetScaler Gateway

Puede usar la interfaz de usuario de NetScaler Gateway para aplicar el tema de la aplicación Citrix Workspace a la página de inicio de sesión de NetScaler Gateway. Puede alternar entre el tema de la aplicación Citrix Workspace y el tema personalizado que cree. Una vez creado el tema personalizado, borre la caché del navegador para evitar que aparezcan páginas almacenadas en caché.

De forma predeterminada, la página de inicio de sesión de NetScaler Gateway utiliza el tema visual RfWebUI que coincide con el estilo de la interfaz de usuario unificada (Unifed UI) utilizada por StoreFront. Si utiliza la plataforma Citrix Workspace o StoreFront local con la nueva interfaz de

© 1997–2026 Citrix Systems, Inc. All rights reserved.

usuario de Workspace, siga las instrucciones proporcionadas en este artículo de soporte. Alternativamente, puede crear su propio tema personalizado. Para obtener más información, consulte Crear un tema personalizado para la página de inicio de sesión de NetScaler Gateway.

Asegúrese de que el tema del portal de NetScaler Gateway esté vinculado a un servidor virtual VPN. Para obtener más información, consulte Vincular un tema de portal a un servidor virtual VPN.

## Crear un tema personalizado para la página de inicio de sesión de NetScaler Gateway

Puede usar la GUI para crear un tema personalizado para la página de inicio de sesión de NetScaler Gateway. También puede dejar el tema predeterminado o usar el tema de la aplicación Citrix Workspace. Cuando elige aplicar un tema personalizado a la página de inicio de sesión, usa la línea de comandos de NetScaler Gateway para crear e implementar el tema. Luego, usa la GUI para configurar la página del tema personalizado.

Puede configurar la página del tema personalizado mediante la configuración global de NetScaler Gateway.

Puede usar esta función con las siguientes versiones de NetScaler Gateway:

- NetScaler Gateway 10.1
- Access Gateway 10, compilación 73.5002.e (debe instalar esta compilación después de la compilación 71.6104.e para usar esta función con Endpoint Management versiones 2.5, 2.6 o 2.8)
- Access Gateway 10, compilación 71.6104.e

### Crear e implementar el tema personalizado mediante la CLI

Para crear e implementar el tema personalizado mediante la línea de comandos:

1. Inicie sesión en la línea de comandos de NetScaler Gateway.
2. En el símbolo del sistema, escriba shell.
3. En el símbolo del sistema, escriba `mkdir /var/ns_gui_custom; cd /netscaler; tar -cvzf /var/ns_gui_custom/customtheme.tar.gz ns_gui/*`.
4. Use la utilidad de configuración para cambiar al tema personalizado y, a continuación, realice cambios de personalización en /var/ns_gui_custom/ns_gui/vpn. Puede:
    - Realizar ediciones en el archivo css/ctx.authentication.css.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Copie un logotipo personalizado en la carpeta /var/ns_gui_custom/ns_gui/vpn/media. **Nota:** Puede usar WinSCP para transferir los archivos.

5. Si tiene varios dispositivos NetScaler Gateway, repita los pasos 3 y 4 para todos los dispositivos.

## Claves del registro del cliente VPN de NetScaler Gateway para Windows

Las claves del registro del cliente VPN están disponibles en **HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Client**. La siguiente tabla enumera las claves del registro del cliente VPN de NetScaler Gateway, sus valores y una breve descripción de cada valor.

| CLAVE DEL REGISTRO | TIPO DE REGISTRO | CONTROL DE REGISTRO | VALORES Y DESCRIPCIÓN | VALOR PREDETERMINADO |
|---|---|---|---|---|
| addedRoutes/ modifiedRoutes | REG_SZ | Administrado por el cliente Citrix Secure Access. | Creado para la comunicación interna del complemento. Los usuarios no deben modificar esta clave. | Este registro no tiene un valor predeterminado. |
| AlwaysOnService | REG_DWORD | El administrador puede implementar este registro a través de un objeto de directiva de grupo (GPO) mediante la Consola de administraci | • 1 => Establecer un túnel a nivel de máquina pero no un túnel a | Este registro no tiene un valor predeterminado. |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| CLAVE DEL REGISTRO | TIPO DE REGISTRO | CONTROL DE REGISTRO | VALORES Y DESCRIPCIÓN | VALOR PREDETERMINADO | |
|---|---|---|---|---|---|
| | | ón de directivas de grupo (GPMC) o la inserción de System Center Configuration Manager (SCCM). | nivel de usuario.<br>• 2 => Establecer un túnel a nivel de máquina o un túnel a nivel de usuario en cualquier momento.<br>• 3 => Establecer un túnel a nivel de máquina y un túnel a nivel de usuario para habilitar el SO multisecuencia en Citrix | | |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| CLAVE DEL REGISTRO | TIPO DE REGISTRO | CONTROL DE REGISTRO | VALORES Y DESCRIPCIÓN | VALOR PREDETERMINADO | |
|---|---|---|---|---|---|
| | | | Secure Private Access para máquinas unidas a un dominio.<br>**Nota:** La compatibilidad con la función de SO multisecuencia está en versión preliminar. | | |
| AlwaysOnURL | REG_SZ | Puede controlar este registro de una de las dos maneras siguientes. | URL del servidor virtual de NetScaler Gateway al que el usuario desea conectarse. Ejemplo: `https://` | Este registro no tiene un valor predeterminado, ya que está configurado para una solución personalizada. | |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| CLAVE DEL REGISTRO | TIPO DE REGISTRO | CONTROL DE REGISTRO | VALORES Y DESCRIPCIÓN | VALOR PREDETERMINADO | |
|---|---|---|---|---|---|
| | | • El administrador puede implementar este registro a través de GPO mediante GPMC o SCCM push (o)<br>• Uso de la CLI. Para obtener más información, consulte la nota*. | `xyz.companyDomain.com` | | |
| AlwaysOn | REG_DWORD | Mediante la CLI. Para obtener más información, consulte la nota*. | • 1 => Permitir el acceso a la red en caso | Este registro no tiene un valor predeterminado. | |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| CLAVE DEL REGISTRO | TIPO DE REGISTRO | CONTROL DE REGISTRO | VALORES Y DESCRIPCIÓN | VALOR PREDETERMINADO | |
|---|---|---|---|---|---|
| | | | de fallo de la VPN.<br>• 2=> Bloquear el acceso a la red en caso de fallo de la VPN. | | |
| AlwaysOnAllowlist | REG_SZ | El administrador puede implementar este registro a través de GPO mediante GPMC o el envío de SCCM. | Lista separada por punto y coma de FQDN, rangos de direcciones IP o direcciones IP permitidas por el controlador en modo estricto Always On. Ejemplos: `example.citrix.com;192.0.2.0;192.0.2.100-192.0.2.255` | vacío o NULO | |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| CLAVE DEL REGISTRO | TIPO DE REGISTRO | CONTROL DE REGISTRO | VALORES Y DESCRIPCIÓN | VALOR PREDETERMINADO | |
|---|---|---|---|---|---|
| ClientControl | REG_DWORD | Uso de la CLI. Para obtener más información, consulte la nota*. | • 1 => Permite a los usuarios cerrar sesión o conectarse a otras puertas de enlace.<br>• 0 => Impide a los usuarios cerrar sesión o conectarse a otras puertas de enlace. | 1 | |
| ConfigSize | REG_DWORD | El administrador puede implementar este registro a través de GPO utilizando GPMC o | El cliente de Windows admite un tamaño de archivo de configuración de 64 KB de forma predetermin | 64 KB | |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| CLAVE DEL REGISTRO | TIPO DE REGISTRO | CONTROL DE REGISTRO | VALORES Y DESCRIPCIÓN | VALOR PREDETERMINADO | |
|---|---|---|---|---|---|
| | | SCCM push. Este registro se utiliza solo para Citrix Secure Private Access. | ada. Utilice este registro para aumentar el tamaño del archivo de configuración.<br>Si el tamaño del archivo de configuración supera el valor predeterminado de 64 KB, establezca el valor del registro `ConfigSize` en 5 veces 64 KB (en bytes) por cada 64 KB adicionales.<br><br>Por ejemplo, si va a añadir 64 KB adicionales, debe establecer el valor del | | |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| CLAVE DEL REGISTRO | TIPO DE REGISTRO | CONTROL DE REGISTRO | VALORES Y DESCRIPCIÓN | VALOR PREDETERMINADO | |
|---|---|---|---|---|---|
| | | | registro en 64 x 1024 x 5 = 327680. Del mismo modo, si va a añadir 128 KB, debe establecer el valor del registro en 64 x 1024 x (5+5) = 655360. | | |
| Conectado | REG_DWORD | Gestionado por el cliente de Citrix Secure Access. | Si la conexión es correcta, esta clave se establece en 1; de lo contrario, se establece en 0. Esta clave se utiliza internamente. Los usuarios no deben modificar esta clave. | Este registro no tiene un valor predeterminado. | |
| DisableCredProv | REG_DWORD | El administrador puede implementar | Cuando **AlwaysOn VPN antes del inicio** | 0 | |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| CLAVE DEL REGISTRO | TIPO DE REGISTRO | CONTROL DE REGISTRO | VALORES Y DESCRIPCIÓN | VALOR PREDETERMINADO |
|---|---|---|---|---|
| | | este registro a través de GPO mediante GPMC o un envío de SCCM. | **de sesión de Windows** está habilitado, el complemento VPN de Windows agrega el proveedor de credenciales para mostrar el estado del túnel en la pantalla de inicio de sesión. Si no necesita esta funcionalidad adicional, cree y establezca este registro en 1. | |
| DisableIconHide | REG_DWORD | Mediante CLI: `set vpn parameter iconWithReceiver ON` | • 1 => La aplicación Citrix Workspace y el complemento NetScaler | 0 |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| CLAVE DEL REGISTRO | TIPO DE REGISTRO | CONTROL DE REGISTRO | VALORES Y DESCRIPCIÓN | VALOR PREDETERMINADO |
|---|---|---|---|---|
| | | | Gateway se muestran en la barra de tareas. | |
| | | | 0 => El icono del complemento de NetScaler Gateway está integrado con la aplicación Citrix Workspace para Windows. El complemento de NetScaler Gateway no es visible en la barra de tareas cuando la sesión VPN completa está en ejecución. | |
| DisableDNSRoutes | REG_DWORD | El administrador puede implementar | • 0 => Valor predeter | 0 |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| CLAVE DEL REGISTRO | TIPO DE REGISTRO | CONTROL DE REGISTRO | VALORES Y DESCRIPCIÓN | VALOR PREDETERMINADO |
|---|---|---|---|---|
| | | este registro a través de GPO mediante GPMC o el envío de SCCM. | minado. El complemento VPN agrega rutas para los servidores DNS si son diferentes de la puerta de enlace predeterminada para una interfaz física. Sin embargo, según la topología de red de la máquina cliente de Window | |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| CLAVE DEL REGISTRO | TIPO DE REGISTRO | CONTROL DE REGISTRO | VALORES Y DESCRIPCIÓN | VALOR PREDETERMINADO |
|---|---|---|---|---|
| | | | s, es posible que las rutas del servidor DNS no siempre sean necesarias. | |
| | | | 1 => El complemento VPN no agrega rutas explícitas para los servidores DNS. | |
| DisallowCaptivePortals | REG_DWORD | El administrador puede implementar este registro a través de GPO mediante GPMC o el envío de SCCM. | • 1 => El complemento VPN comprueba si hay portales cautivos intentando conectarse a la | 0 |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| CLAVE DEL REGISTRO | TIPO DE REGISTRO | CONTROL DE REGISTRO | VALORES Y DESCRIPCIÓN | VALOR PREDETERMINADO | |
|---|---|---|---|---|---|
| | | | página (http://www.msftconnecttest.com/connecttest.txt) de prueba de Microsoft Connect antes de iniciar una sesión VPN.<br>• 0 => El complemento VPN omite la comprobación de portales cautivos. | | |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| CLAVE DEL REGISTRO | TIPO DE REGISTRO | CONTROL DE REGISTRO | VALORES Y DESCRIPCIÓN | VALOR PREDETERMINADO |
|---|---|---|---|---|
| DisableIntuneDeviceEnrollment | REG_DWORD | El administrador puede implementar este registro a través de GPO mediante GPMC o SCCM push. | Si se establece en 1, no se realiza la inscripción de dispositivos Intune. | 0 |
| EnableAutoUpdate | REG_DWORD | El administrador puede implementar este registro a través de GPO mediante GPMC o SCCM push. | Se utiliza para controlar la funcionalidad de actualización del complemento desde el lado del cliente.<br>• 0 => Deshabilitar la funcionalidad de actualización automática. | 0 |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| CLAVE DEL REGISTRO | TIPO DE REGISTRO | CONTROL DE REGISTRO | VALORES Y DESCRIPCIÓN | VALOR PREDETERMINADO | |
|---|---|---|---|---|---|
| | | | • 1 => Habilitar la funcionalidad de actualización automática. **Nota:** Esta clave de registro está disponible en **HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Client\AutoUpdate**. | | |
| EnableEdgeWebview | REG_DWORD | El administrador puede implementar este registro | • 0 => Deshabilitar | 1 | |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| CLAVE DEL REGISTRO | TIPO DE REGISTRO | CONTROL DE REGISTRO | VALORES Y DESCRIPCIÓN | VALOR PREDETERMINADO | |
|---|---|---|---|---|---|
| | | a través de GPO usando GPMC o mediante un envío de SCCM. | Microsoft Edge WebView.<br>• 1 => Habilitar Microsoft Edge WebView. | | |
| EnableKerberosAuth | REG_DWORD | El administrador puede implementar este registro a través de GPO usando GPMC o un envío de SCCM. | • 0 => Valor predeterminado.<br>• 1 => El cliente VPN utiliza el método de autenticación Kerberos para el inicio de sesión automático. | 0 | |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| CLAVE DEL REGISTRO | TIPO DE REGISTRO | CONTROL DE REGISTRO | VALORES Y DESCRIPCIÓN | VALOR PREDETERMINADO | |
|---|---|---|---|---|---|
| EnableMultiSessionFlow | REG_DWORD | El administrador puede implementar este registro a través de GPO usando GPMC o un envío de SCCM. | • 0 => Deshabilitar el acceso al SO multisecuencia en Citrix Secure Private Access<br>• 1 => Habilitar el acceso al SO multisecuencia en Citrix Secure Private Access | Este registro no tiene un valor predeterminado, ya que está configurado para una solución personalizada. | |
| EnableTCPDNS | REG_DWORD | El administrador puede implementar este registro a través de GPO mediante GPMC o el envío de SCCM. | • 0 => Deshabilita la compatibilidad con DNS dividido para | 1 | |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| CLAVE DEL REGISTRO | TIPO DE REGISTRO | CONTROL DE REGISTRO | VALORES Y DESCRIPCIÓN | VALOR PREDETERMINADO | |
|---|---|---|---|---|---|
| | | | solicitudes DNS basadas en TCP.<br>• 1 => Habilita la compatibilidad con DNS dividido para solicitudes DNS basadas en TCP. | | |
| EnableVA | REG_DWORD | Administrado por el cliente de Citrix Secure Access. | Esta clave se utiliza internamente si el adaptador virtual de Citrix debe habilitarse cuando IIP está presente. Los usuarios no deben | 1 | |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| CLAVE DEL REGISTRO | TIPO DE REGISTRO | CONTROL DE REGISTRO | VALORES Y DESCRIPCIÓN | VALOR PREDETERMINADO |
|---|---|---|---|---|
| | | | modificar esta clave. | |
| EnableWFP | REG_DWORD | El administrador puede implementar este registro a través de GPO mediante GPMC o SCCM push o mediante un indicador de función. | • 1 => El complemento VPN utiliza WFP. A partir de la versión 25.1.1.27 del cliente de Citrix Secure Access para Windows, WFP está habilitado de forma predeterminada. | 1 |
| | | | 0 => El complemento VPN utiliza DNE. | |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| CLAVE DEL REGISTRO | TIPO DE REGISTRO | CONTROL DE REGISTRO | VALORES Y DESCRIPCIÓN | VALOR PREDETERMINADO |
|---|---|---|---|---|
| ExcludeDomainsFromRemoteDns | REG_SZ | El administrador puede implementar este registro a través de GPO mediante GPMC o SCCM push. | Excluye la resolución DNS de ser realizada por el cliente de Citrix Secure Access a través de un servidor DNS remoto.<br><br>Si `example.com` es un dominio de intranet y quiere excluir aplicaciones específicas como `sshhost.example.com`, `rdphost.example.com` o `*.ftphost.example.com`, utilice este registro. `*.ftphost.example.com` es un patrón | Este registro no tiene un valor predeterminado, ya que está configurado para una solución personalizada. |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| CLAVE DEL REGISTRO | TIPO DE REGISTRO | CONTROL DE REGISTRO | VALORES Y DESCRIPCIÓN | VALOR PREDETERMINADO |
|---|---|---|---|---|
| | | | comodín que coincide con cualquier subdominio bajo `ftphost.example.com`.<br><br>Asegúrese de ajustar los nombres de dominio y los patrones según sus requisitos. Una vez que haya realizado los cambios, reinicie Citrix Secure Access o el sistema para que la configuración surta efecto. | |
| ExcludeDomainsFromTunnel (Vista previa) | REG_SZ | El administrador puede implementar este registro a través de GPO | Excluye el tráfico de dominios específicos de ser tunelizado a través del | Este registro no tiene un valor predeterminado, ya que está configurado |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| CLAVE DEL REGISTRO | TIPO DE REGISTRO | CONTROL DE REGISTRO | VALORES Y DESCRIPCIÓN | VALOR PREDETERMINADO |
|---|---|---|---|---|
| | | utilizando GPMC o el envío de SCCM. | cliente Citrix Secure Access. Si `example.com` es un dominio de intranet y desea excluir aplicaciones específicas como `sshhost.example.com`, `rdphost.example.com` o `*.ftphost.example.com`, utilice este registro. Asegúrese de establecer el valor del registro como una lista de nombres de dominio o patrones separados por comas. | para una solución personalizada. |
| HttpTimeout | REG_DWORD | El administrador puede | El tiempo de espera HTTP se | 100 segundos |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| CLAVE DEL REGISTRO | TIPO DE REGISTRO | CONTROL DE REGISTRO | VALORES Y DESCRIPCIÓN | VALOR PREDETERMINADO |
|---|---|---|---|---|
| | | implementar este registro a través de GPO utilizando GPMC o el envío de SCCM. | configura en segundos. Si el tiempo de espera no está configurado, se utiliza el tiempo de espera predeterminado. El valor de tiempo de espera predeterminado es de 100 segundos, según los estándares de Windows. | |
| InstallDir | REG_SZ | Administrado por el cliente Citrix Secure Access. | Ubicación donde está instalado el cliente de Citrix Secure Access. | "C:\Program Files\Citrix\Secure Access Client" |
| locationDetection | REG_DWORD | Uso de la CLI. Para obtener más información, consulte la nota*. | • 1 => Para habilitar la detección de | Este registro no tiene un valor predeterminado y solo se configura cuando el modo Always On |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| CLAVE DEL REGISTRO | TIPO DE REGISTRO | CONTROL DE REGISTRO | VALORES Y DESCRIPCIÓN | VALOR PREDETERMINADO | |
|---|---|---|---|---|---|
| | | | ubicación.<br>• 0 => Para deshabilitar la detección de ubicación. | está habilitado. | |
| NoDHCPRoute | REG_DWORD | 1. Desde el dispositivo NetScaler, cree un nuevo archivo llamado `plugin Customization.json` con el valor `\ { "NoDHCPRoute" :` | Si se establece en 1, no se añade la ruta del servidor DHCP. | Este registro no tiene un valor predeterminado, ya que se personaliza en función de la topología de red. | |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| CLAVE DEL REGISTRO | TIPO DE REGISTRO | CONTROL DE REGISTRO | VALORES Y DESCRIPCIÓN | VALOR PREDETERMINADO | |
|---|---|---|---|---|---|
| | | `true }` .<br>2. Coloque el archivo `plugin Customizatio n.json` en las carpetas **/ netscaler/ ns_gui/ vpn** y **/ var/ netscaler/gui/ vpn**. | | | |
| overrideIPV6DnsDrop | REG_DWORD | El administrador puede implementar este registro a través de GPO utilizando GPMC o SCCM push. | • 1 => Permite que el tráfico DNS IPv6 fluya a través de la VPN. | Este registro no tiene un valor predeterminado, ya que se personaliza en función de la topología de red. | |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| CLAVE DEL REGISTRO | TIPO DE REGISTRO | CONTROL DE REGISTRO | VALORES Y DESCRIPCIÓN | VALOR PREDETERMINADO |
|---|---|---|---|---|
| | | | 0 => Restringir el flujo de tráfico DNS IPv6. | |
| ProductVersion | REG_SZ | Administrado por el cliente Citrix Secure Access. | Versión actualmente instalada del cliente Citrix Secure Access. | Información de la versión del producto |
| ProductCode | REG_SZ | Administrado por el cliente Citrix Secure Access. | Esta clave se utiliza internamente. Los usuarios no deben modificar esta clave. | {B04137FF-B5C9-4058-ACEB-04118790118D} |
| secureDNSUpdate | REG_DWORD | El administrador puede implementar este registro a través de GPO mediante GPMC o SCCM push. | • 0 => El complemento VPN solo intenta la actualización DNS no segura.<br>• 1 => El complemento | 1 |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| CLAVE DEL REGISTRO | TIPO DE REGISTRO | CONTROL DE REGISTRO | VALORES Y DESCRIPCIÓN | VALOR PREDETERMINADO | |
|---|---|---|---|---|---|
| | | | VPN intenta primero la actualización DNS no segura. Si la actualización DNS no segura falla, el complemento VPN intenta entonces la actualización DNS segura. Este es el comportamiento predeterminado a partir de la compilación | | |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| CLAVE DEL REGISTRO | TIPO DE REGISTRO | CONTROL DE REGISTRO | VALORES Y DESCRIPCIÓN | VALOR PREDETERMINADO | |
|---|---|---|---|---|---|
| | | | 21.3.1.2 del complemento de Windows.<br>• 2 => El complemento VPN solo intenta la actualización DNS segura. | | |
| SecureChannelResetTimeoutSeconds | REG_DWORD | El administrador puede implementar este registro a través de GPO utilizando GPMC o el envío de SCCM. | Por defecto, este valor de registro no está establecido ni añadido. Cuando el valor de `SecureChannelResetTimeoutSeconds` es `0xFFFFFFFF` o no está presente en el registro, el | Este registro no tiene un valor predeterminado, ya que está configurado para una solución personalizada. | |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| CLAVE DEL REGISTRO | TIPO DE REGISTRO | CONTROL DE REGISTRO | VALORES Y DESCRIPCIÓN | VALOR PREDETERMINADO |
|---|---|---|---|---|
| | | | complemento VPN espera a que la llamada a la API `SecureChannelReset()` se complete antes de empezar a tunelizar el tráfico de datos. Este es el comportamiento predeterminado. El administrador debe establecer este registro en el cliente para que el complemento VPN comience a tunelizar el tráfico de datos después de esperar el tiempo especificado para que la llamada a la | |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| CLAVE DEL REGISTRO | TIPO DE REGISTRO | CONTROL DE REGISTRO | VALORES Y DESCRIPCIÓN | VALOR PREDETERMINADO |
|---|---|---|---|---|
| | | | API se complete. | |
| SecureAccessLogInScript | REG_SZ | El administrador puede implementar este registro a través de GPO utilizando GPMC o el envío de SCCM. | El servicio Citrix Secure Access accede a la configuración del script de inicio de sesión utilizando esta clave de registro cuando se conecta al servicio Citrix Secure Private Access. Para obtener más información, consulte Registros de configuración de scripts de inicio y cierre de sesión. | Este registro no tiene un valor predeterminado, ya que está configurado para una solución personalizada. |
| SecureAccessLogOutScript | REG_SZ | El administrador puede implementar este registro a través de | El servicio Citrix Secure Access accede a la configuració | Este registro no tiene un valor predeterminado, ya que está |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| CLAVE DEL REGISTRO | TIPO DE REGISTRO | CONTROL DE REGISTRO | VALORES Y DESCRIPCIÓN | VALOR PREDETERMINADO |
|---|---|---|---|---|
| | | GPO utilizando GPMC o el envío de SCCM. | n del script de cierre de sesión utilizando esta clave de registro cuando se conecta al servicio Citrix Secure Private Access. Para obtener más información, consulte Registros de configuración de scripts de inicio y cierre de sesión. | configurado para una solución personalizada. |
| suffixList | REG_SZ | Mediante CLI: `add dns suffix` | Lista de dominios de intranet separados por punto y coma. Se utiliza cuando la detección de ubicación está habilitada. | Recupera el valor del sufijo DNS configurado en el servidor. |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| CLAVE DEL REGISTRO | TIPO DE REGISTRO | CONTROL DE REGISTRO | VALORES Y DESCRIPCIÓN | VALOR PREDETERMINADO |
|---|---|---|---|---|
| SicBeginPort | REG_DWORD | 1. Desde el dispositivo NetScaler, cree un nuevo archivo llamado `pluginCustomization.json` con el valor `\{"SicBeginPort" : 51000}` .<br>2. Coloque el archivo `pluginCustomization.json` en las carpetas */* | Evita conflictos que puedan surgir al usar puertos para crear sockets entre el cliente de Citrix Secure Access y aplicaciones de terceros en las máquinas cliente. El rango permitido es 49152–64535 (C000 a FC17 en formato hexadecimal ). El cliente VPN utiliza hasta 1000 puertos a partir de `SicBeginPort` solo si `EnableWFP` también está configurado en `1` . | Este registro no tiene un valor predeterminado, ya que está configurado para una solución personalizada. |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| CLAVE DEL REGISTRO | TIPO DE REGISTRO | CONTROL DE REGISTRO | VALORES Y DESCRIPCIÓN | VALOR PREDETERMINADO | |
|---|---|---|---|---|---|
| | | **netscaler/ns_gui/vpn** y **/var/netscaler/gui/vpn**. | | | |
| userCertCAList | REG_SZ | El administrador puede implementar este registro a través de GPO utilizando GPMC o SCCM push. | Se utiliza en el contexto del servicio Always On, donde un cliente puede especificar la lista de CA de las que elegir el certificado de cliente. | Este registro no tiene un valor predeterminado, ya que está configurado para una solución personalizada. | |

**NOTA:**

*Utilice el siguiente comando para aplicar las claves de registro `AlwaysOnURL`, `AlwaysOn`, `ClientControl` y `locationDetection` mediante la CLI:

```
add alwaysONProfile <alwaysONProfileName>-clientControl ( ALLOW | DENY )-locationBasedVPN ( Remote | Everywhere )-networkAccessOnVPNFailure ( onlyToGateway | fullAccess )
```

**Importante:**

- Puede aplicar claves de registro según sus implementaciones. Por ejemplo, la clave de registro `AlwaysOnService` solo es aplicable al servicio Always On, mientras que la clave de

© 1997–2026 Citrix Systems, Inc. All rights reserved.

registro `ClientControl` no es aplicable al servicio Always On. Consulte la documentación de implementación individual para obtener más detalles.

- `secureDNSUpdate` solo es aplicable a dispositivos cliente unidos a un dominio.
- Para el cliente Citrix Secure Access para Windows 23.1.1.8 y versiones posteriores, el nombre de la clave de registro es `overrideIPV6DnsDrop`. Para el cliente Citrix Secure Access para Windows 22.10.1.9 y versiones anteriores, el nombre de la clave de registro es `overrideIP6DnsDrop`.
- A partir del cliente Citrix Secure Access para Windows 24.8.1.15, las claves de registro `DisableGA`, `ForcedLogging` y `OverrideSpoofIPRange` están obsoletas.
- A partir del cliente Citrix Secure Access para Windows 24.8.1.19, el administrador puede habilitar VDI multisecuencia alojado en la nube en Secure Private Access mediante el registro `EnableMultiSessionFlow` para el acceso contextual a los recursos en función de su ubicación, dispositivo y otros factores. Para las máquinas unidas a un dominio, utilice los registros `EnableMultiSessionFlow` y `AlwaysOnService`.
- Para el cliente Citrix Secure Access para Windows en versiones anteriores a la 24.8.1.19, el administrador puede habilitar Microsoft Edge WebView mediante el registro `EnableEdgeWebview`.

# Aplicar la marca HttpOnly en las cookies de autenticación

A partir de la versión 13.1-37.x y posteriores de NetScaler Gateway, la marca HttpOnly está disponible en las cookies de autenticación de los escenarios VPN, es decir, las cookies NSC_AAAC y NSC_TMAS. La cookie de autenticación NSC_TMAS se utiliza durante la autenticación nFactor y la cookie NSC_AAAC se utiliza para la sesión autenticada. La marca HttpOnly en una cookie restringe el acceso a la cookie mediante la opción de cookie de documento de JavaScript. Esto ayuda a prevenir el robo de cookies debido a la creación de scripts entre sitios.

## Escenario compatible

La marca HTTPOnly es compatible con la autenticación nFactor.

**Comportamiento cuando el parámetro HttpOnlyCookie de NetScaler AAA se utiliza junto con el parámetro HttpOnlyCookie de tmsession:**

- Cuando el parámetro httpOnlyCookie de autenticación, autorización y auditoría está habilitado y se utiliza la autenticación nFactor, el parámetro HttpOnlyCookie de autenticación, autorización y auditoría anula el parámetro HttpOnlyCookie de la sesión TM. Además, tanto

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NSC_TMAS como NSC_AAAC se marcan como HttpOnly independientemente del tipo de sesión; ya sea una sesión VPN, una sesión TM o durante la autenticación nFactor.

- Si el parámetro HttpOnlyCookie está deshabilitado, la marca HttpOnly no se establece para una sesión VPN. Para el escenario de autenticación, autorización y auditoría, la marca HttpOnly se establece en función del valor del parámetro de sesión TM.

## Configurar la función HttpOnly mediante la CLI

- Habilitar la marca HttpOnly.

```
set aaa parameter -httpOnlyCookie ENABLED
```

**NOTA:**

- De forma predeterminada, la marca HttpOnly está habilitada en las siguientes compilaciones de NetScaler Gateway:
  - 14.1-43.56 y posteriores
  - 13.1-59.19 y posteriores
- Para deshabilitar la marca HttpOnly, ejecute el siguiente comando:

```
set aaa parameter -httpOnlyCookie DISABLED
```

- Comprobar el estado de la función HttpOnly.

```
show aaa parameter
```

## Limitaciones

- Cuando la función HttpOnly está habilitada, el botón de la página de inicio en el cliente Citrix Secure Access™ no funciona.
- La bandera HttpOnly no se establece en ninguna autenticación clásica.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

# Personalizar el portal de usuario para usuarios VPN

NetScaler Gateway permite a los administradores personalizar la apariencia del portal de usuario al que acceden los usuarios VPN. Puede seleccionar entre un conjunto de temas preestablecidos o utilizar uno como plantilla para crear un portal totalmente personalizado o de marca.

Mediante la utilidad de configuración, puede personalizar un tema añadiendo nuevos logotipos, imágenes de fondo, etiquetas de cuadros de entrada personalizadas y varios otros atributos del diseño del portal basado en CSS. Los temas de portal integrados incluyen contenido para cinco idiomas: inglés, francés, español, alemán y japonés. El idioma que se presenta al usuario se determina automáticamente en función de la configuración regional de sus navegadores web.

Puede crear un EULA personalizado que se presenta a los usuarios VPN antes de que se les permita iniciar sesión. La función EULA admite versiones de EULA específicas de la configuración regional, que se presentan a los usuarios en función de las configuraciones regionales informadas por sus navegadores web.

Tanto los temas del portal como las configuraciones de EULA se pueden vincular de forma independiente en el servidor virtual VPN y en los niveles globales de VPN.

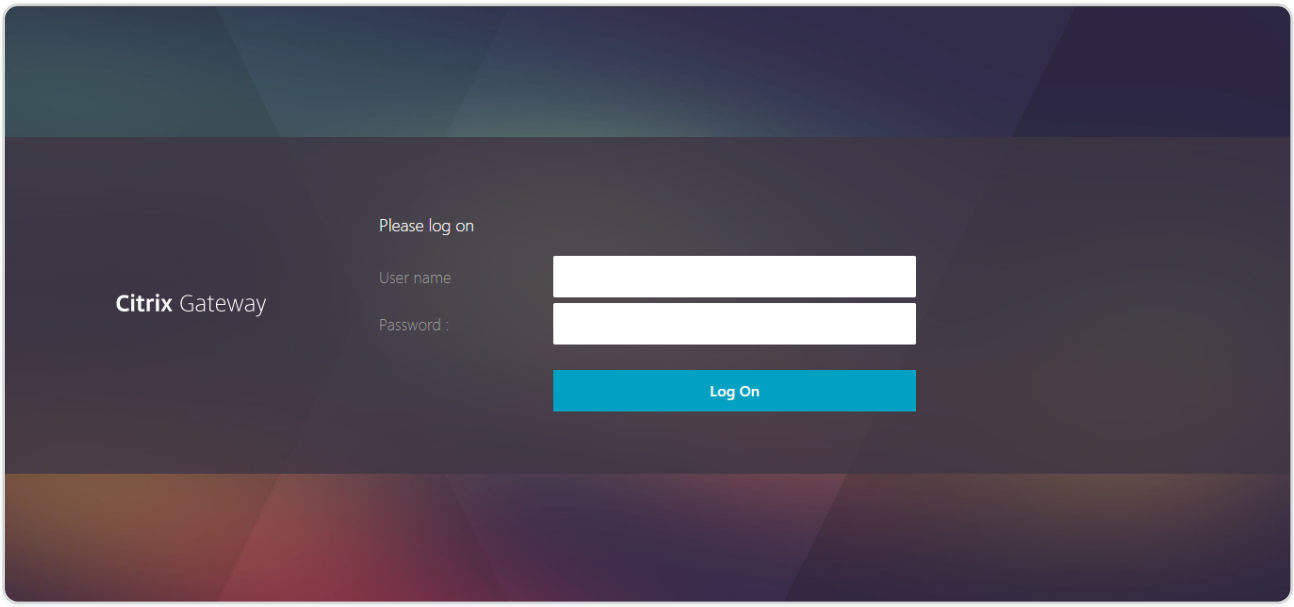
**IMPORTANTE:**

NetScalerÂ® no admite personalizaciones que requieran modificaciones de código y no ofrece soporte para resolver problemas más allá de volver a un tema predeterminado.

## Aplicar un tema de portal

A partir de la versión 13.0 compilación 67.43, el portal VPN está configurado para usar el tema RfWebUI, de forma predeterminada. Anteriormente, el `Caxton theme` era el tema predeterminado. También puede aplicar los temas Green bubble y X1.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

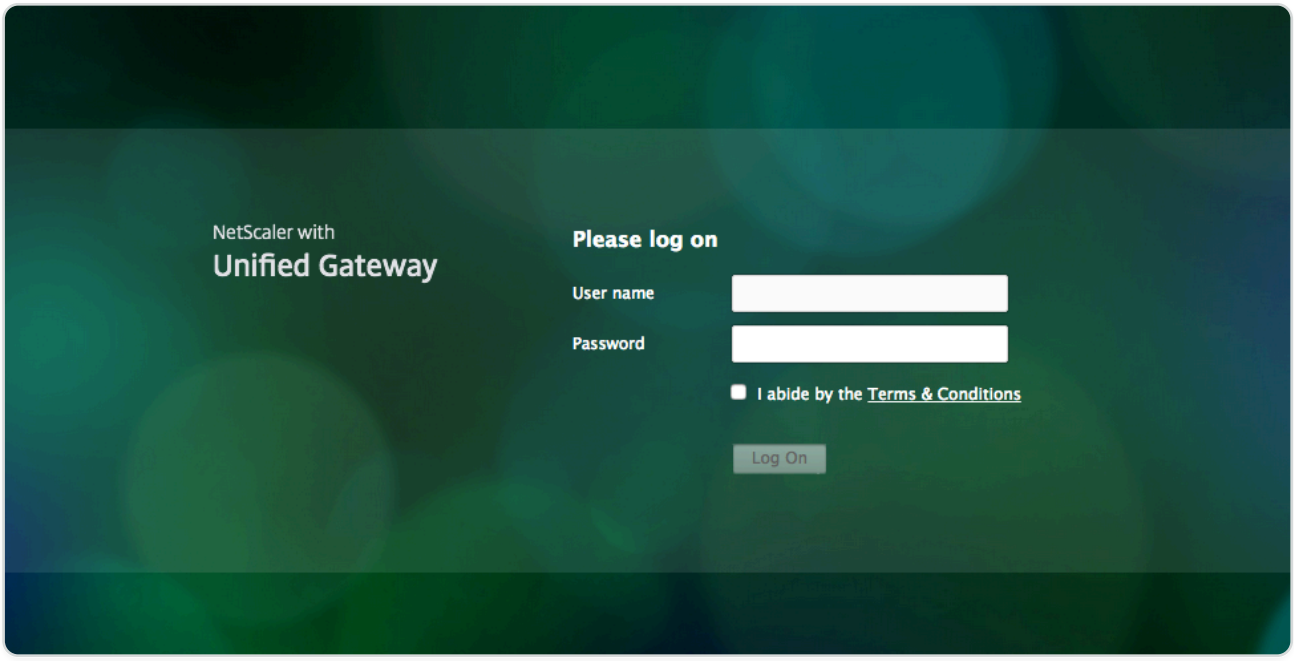



## Tema Caxton

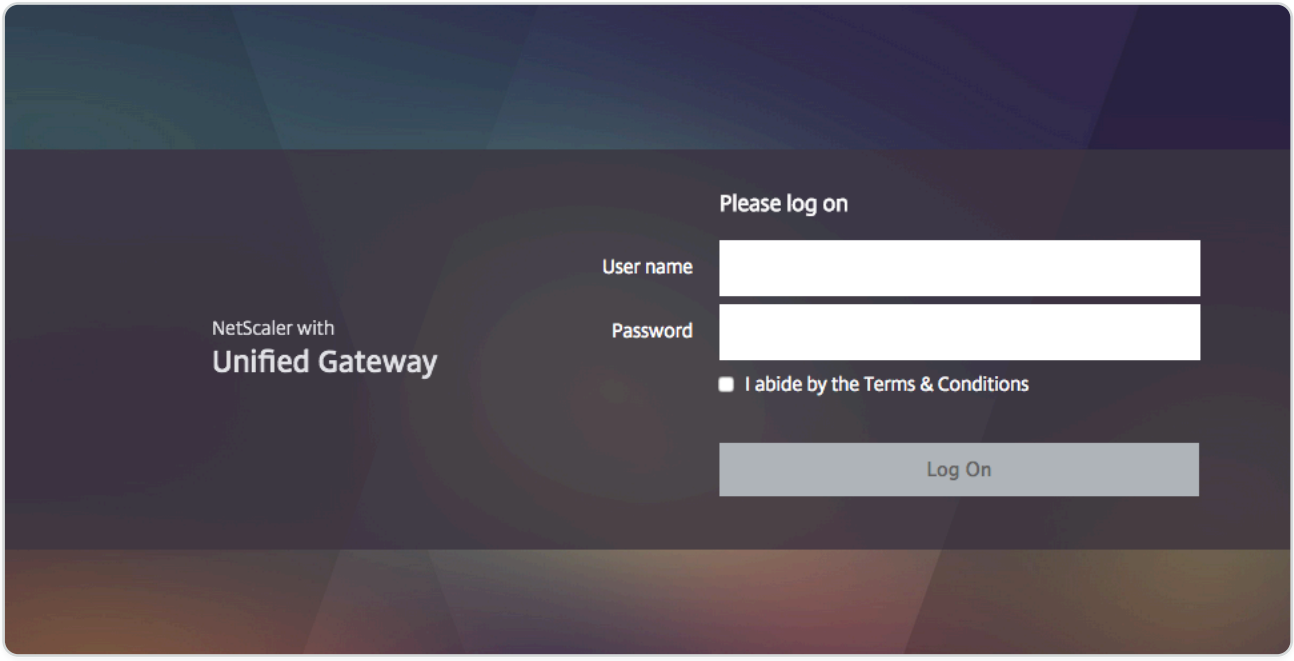



© 1997–2026 Citrix Systems, Inc. All rights reserved.

### Tema Green bubble




### Tema X1




Puede aplicar cualquiera de los temas suministrados directamente a un servidor virtual VPN o como una vinculación VPN global.

## Vincular un tema de portal a un servidor virtual VPN

Puede vincular un tema de portal en un servidor virtual existente o al crear un nuevo servidor virtual.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

### Vincular un tema de portal a un servidor virtual VPN mediante la CLI

En el símbolo del sistema, escriba;

```
bind vpn vserver <name> - portaltheme <name>
```

### Vincular un tema de portal a un servidor virtual VPN mediante la GUI

1. En la ficha **Configuración**, vaya a **NetScaler Gateway** y haga clic en **Servidores virtuales.**
2. Seleccione un servidor virtual y, a continuación, haga clic en **Editar**.
3. Si aún no se ha vinculado un tema de portal al servidor virtual, haga clic en **Tema del portal** en **Configuración avanzada** en el panel de detalles. De lo contrario, la opción **Tema del portal** ya está expandida en el panel de detalles.
4. En el panel de detalles, en **Temas del portal**, haga clic en **Sin tema de portal** para expandir la ventana de vinculación de temas del portal.
5. `Click` **Haga clic para seleccionar**.
6. En la ventana **Temas del portal**, haga clic en un nombre de tema y, a continuación, haga clic en **Seleccionar**.
7. Haga clic en **Vincular**.
8. Haga clic en **Listo**.

Si está creando un servidor virtual VPN, puede seguir los pasos del procedimiento anterior a partir del paso 3 mientras se encuentra en el panel **Editar servidor virtual VPN** para vincular un tema de portal.

## Vincular un tema de portal a VPN global

### Vincular un tema de portal a VPN global mediante la CLI

Â En el símbolo del sistema, escriba;

```
bind vpn global portaltheme <name>
```

### Vincular un tema de portal a VPN global mediante la GUI

1. En la ficha **Configuración**, vaya a **NetScaler Gateway.**
2. En el panel de detalles principal, haga clic en **NetScaler Gateway Policy Manager**.
3. Haga clic en el icono '**+**'.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. En la lista **Punto de enlace**, seleccione **Recursos**.
5. En la lista Â **Tipo de conexión**Â , seleccione Â **Tema del portal.**
6. Haga clic en **Continuar**.
7. En la pantalla Â **Punto de enlace**Â , haga clic en **Agregar enlace**.
8. Haga clic en **Haga clic para seleccionar**.
9. En la ventana **Temas del portal**, haga clic en un nombre de tema y, a continuación, haga clic en **Seleccionar**.
10. Haga clic en **Enlazar**.
11. Haga clic en **Cerrar**.
12. Haga clic en **Listo.**

**SUGERENCIA:**

Después de realizar los cambios, utilice el comando «save ns config» en la línea de comandos o haga clic en el icono de guardar en la utilidad de configuración para asegurarse de que los cambios se guarden en el archivo de configuración de NetScaler.

## Crear un tema de portal

Para crear un diseño de portal personalizado, utilice uno de los temas de portal suministrados como plantilla. El sistema hace una copia del tema de plantilla seleccionado con un nombre que usted especifique.

## Usar un tema de portal estándar como plantilla para un tema de portal personalizado

Para crear un tema de portal, puede usar la utilidad de configuración o la línea de comandos para crear la entidad del tema. Sin embargo, los controles de personalización detallados solo están disponibles dentro de la utilidad de configuración.

### Crear un tema de portal mediante la CLI

En el símbolo del sistema, escriba:

```
add portaltheme <name> basetheme <name>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

### Crear un tema de portal mediante la GUI

1. En la ficha **Configuración**, vaya a **NetScaler Gateway** y haga clic en **Temas del portal**.
2. En el panel de detalles principal, haga clic en **Agregar**.
3. Introduzca un nombre para el tema y seleccione una plantilla de la lista de plantillas y, a continuación, haga clic en **Aceptar**.
4. En este punto, se le presenta la vista por primera vez de la ventana de edición del tema del portal. Haga clic en **Aceptar** para salir.

Puede proceder a personalizar el nuevo tema del portal con la vista por primera vez.

Una vez creado un nuevo tema, puede vincularlo a un servidor virtual VPN o a la VPN global. Puede vincular un nuevo tema inmediatamente después de su creación o después de completar sus personalizaciones.

## Personalización del tema del portal

Para personalizar un tema del portal, utilice la interfaz de temas del portal en la utilidad de configuración. Para obtener los mejores resultados, debe comprender los distintos elementos de esta interfaz antes de usarla.

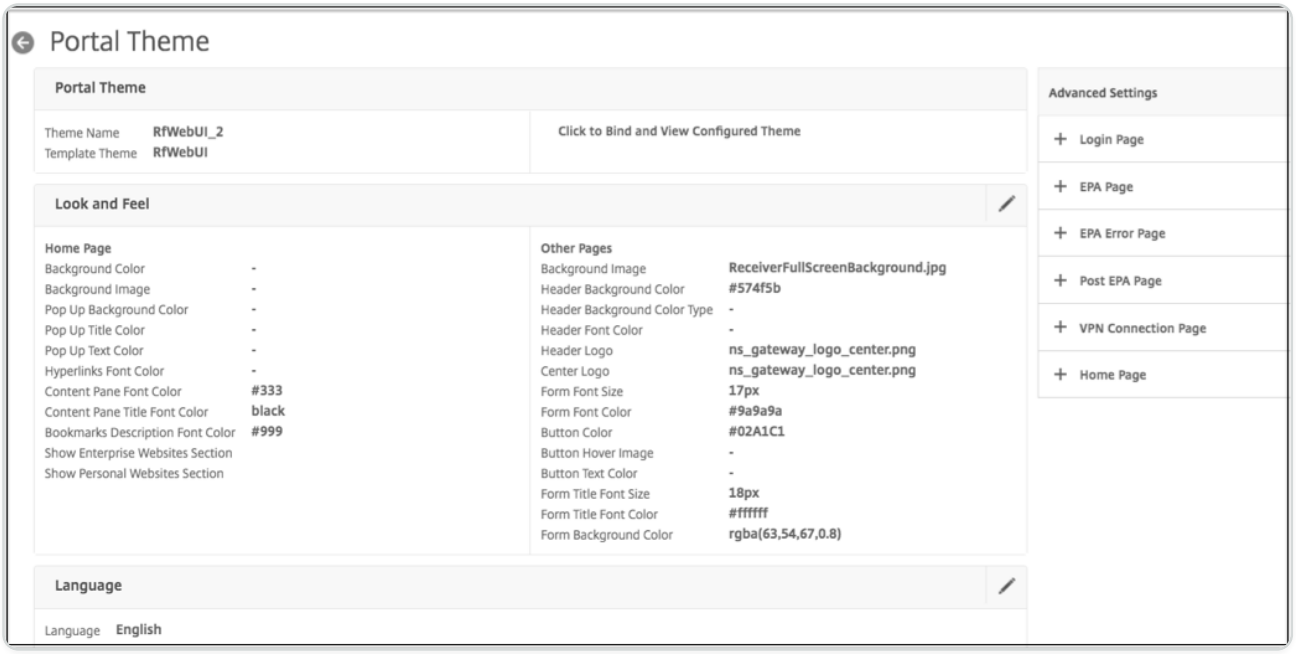
## Acerca de la interfaz de temas del portal

Para abrir la **interfaz de temas del portal** en la utilidad de configuración de NetScaler Gateway, en la ficha **Configuración**, vaya a **NetScaler Gateway** y haga clic en **Temas del portal**. Puede crear un tema como se describe en *Crear un tema del portal* o seleccionar un tema existente en el panel de detalles principal y hacer clic en **Modificar**.

La página de personalización del tema del portal tiene cuatro paneles de componentes principales para modificar el diseño de un portal:

- Panel Tema del portal
- Panel Aspecto y comportamiento
- Panel Configuración avanzada
- Panel Idioma

© 1997–2026 Citrix Systems, Inc. All rights reserved.




El panel **Tema del portal** en la parte superior de la página informa qué tema está cargado para su edición y en qué tema de plantilla se basa. La opción de visualización aquí le permite ver sus personalizaciones sin acceder a la VPN con una conexión de usuario. El uso de la opción de visualización requiere vincular el tema a un servidor virtual VPN y la vinculación permanece activa después de cerrar la ventana de visualización.

Con el panel **Aspecto y comportamiento** en el centro de la página, puede configurar las propiedades generales de un tema, como encabezados, colores e imágenes de fondo, propiedades de fuente y logotipos. Cuando este panel está en modo de edición, hay leyendas de atributos disponibles para guiarle sobre dónde se utilizan los atributos de Aspecto y comportamiento en las páginas del portal.

El panel **Configuración avanzada** contiene los controles de contenido en pantalla para las páginas individuales del portal. Para cargar el contenido de una página para su edición, haga clic en una de las páginas enumeradas. Los controles de la página se abren debajo de los otros paneles centrales. Una página permanece contraída en el panel **Configuración avanzada** durante las ediciones del tema del portal siempre que la página no se haya modificado.

En el panel **Idioma**, puede seleccionar cuál de los idiomas se carga cuando se selecciona una página para editar desde el panel **Configuración avanzada**. Las páginas en inglés se cargan por defecto.

### Tipos de atributos de página personalizables

Al personalizar un Tema del portal, puede modificar una serie de atributos en la interfaz del Tema del portal. Junto con el texto y los idiomas admitidos que se pueden editar, los elementos gráficos

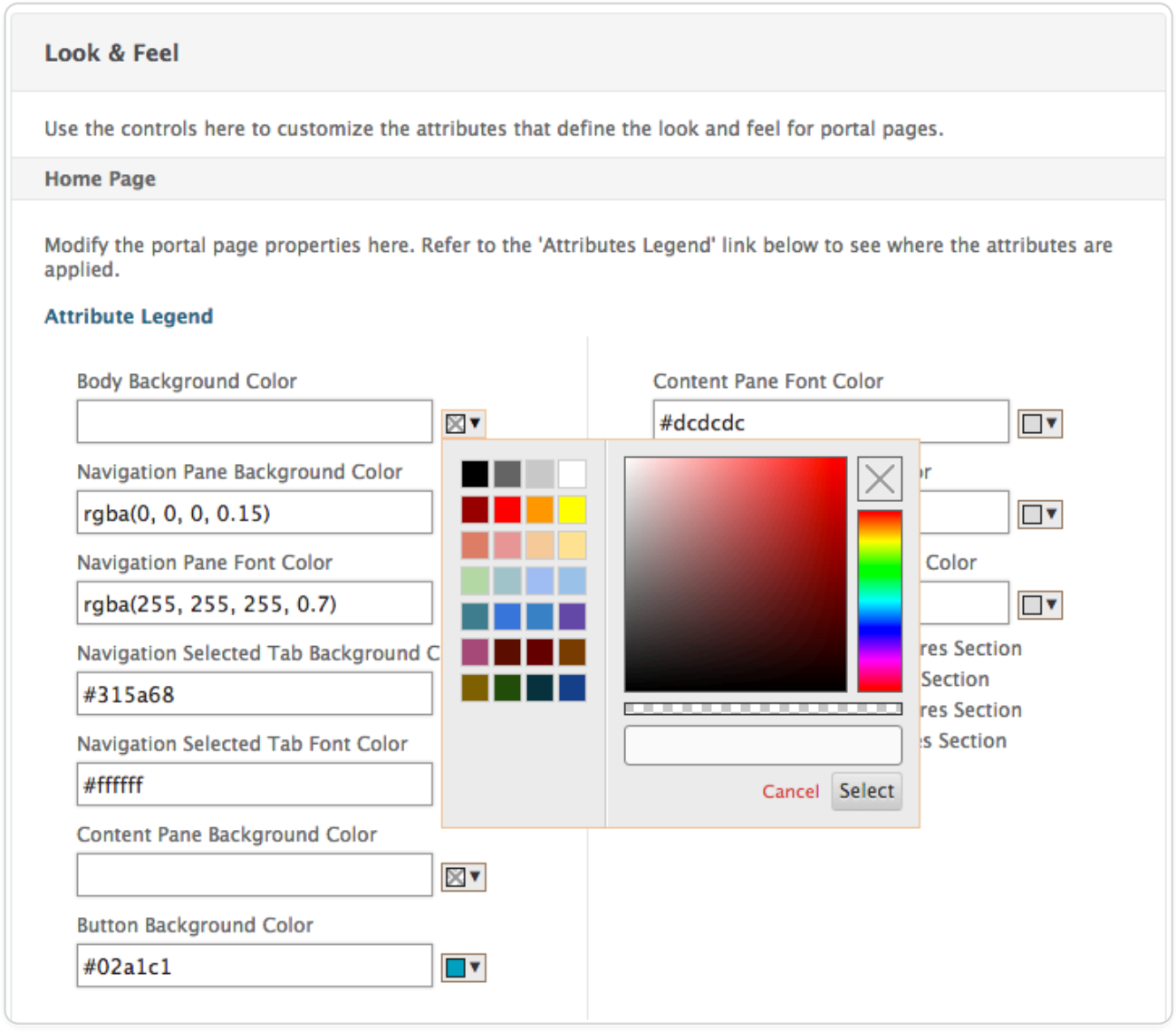
© 1997–2026 Citrix Systems, Inc. All rights reserved.

del diseño del portal se pueden adaptar a sus necesidades. Cada uno de los tipos de elementos de página tiene parámetros o recomendaciones a considerar antes de modificarlos.

### *Colores*

El diseño del portal especifica los colores para atributos como fondos de página, resaltados, texto para títulos y contenido del cuerpo, controles de botón y respuestas al pasar el ratón.

Para personalizar un atributo de color, puede introducir un valor de color directamente para un elemento seleccionado, o puede utilizar el selector de color suministrado para generar un valor de color. La interfaz admite la introducción de valores de color HTML válidos en formato RGBA, formato de triplete hexadecimal HTML y nombres de color X11. Se puede acceder al selector de color para cualquier atributo de color aplicable haciendo clic en el cuadro de color junto al campo de entrada del atributo.




### *Fuentes*

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Junto con los colores de fuente, puede modificar los tamaños de fuente para algunos atributos de página. Para cada uno de estos atributos, un menú ofrece los tamaños disponibles para cada atributo, según lo determinado por el diseño del portal.

***Imágenes***

Para las imágenes, una descripción emergente disponible para cada control proporciona recomendaciones de tamaño y otros requisitos. Las descripciones varían según la ubicación de un atributo en la página y su función. Puede utilizar formatos de archivo de imagen PNG o JPEG. Puede seleccionar una imagen para cargar marcando la casilla de verificación debajo del nombre de archivo de un elemento y luego navegando hasta donde reside la imagen en la unidad de su equipo local.

***Etiquetas***

En la sección **Configuración avanzada**, puede seleccionar el texto de una página específica del portal para modificarlo. Si modifica el texto predeterminado en inglés de una página, el texto para otros idiomas no se vuelve a traducir. El contenido de la página en idioma alternativo se proporciona como una conveniencia, pero requiere actualizaciones manuales para cualquier personalización.

Para editar otra versión de idioma de una página, primero contraiga la ventana, si está abierta, haciendo clic en el icono **X** de la página del portal abierta. Luego, seleccione el idioma en el panel **Idioma** y haga clic en **Aceptar**. Todas las páginas del portal abiertas desde el panel **Configuración avanzada** estarán en ese idioma hasta que seleccione uno diferente.

**IMPORTANTE:**

En implementaciones de alta disponibilidad o en clúster, los Temas del portal se distribuyen a través de la configuración compartida solo cuando la configuración de los Temas del portal se realiza en las entidades NetScaler principales o coordinadoras de configuración, respectivamente.

## Crear un EULA

El sistema del portal VPN ofrece la opción de aplicar un EULA a una configuración de portal. Una vez que un EULA está vinculado a la configuración de NetScaler Gateway, ya sea en el ámbito global de VPN o a un servidor virtual VPN relevante, los usuarios de VPN deben aceptar el EULA como Términos y condiciones antes de que se les permita autenticarse en la VPN.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Al igual que con los temas del portal, a los usuarios se les presenta un EULA específico del idioma basado en la configuración regional informada por su navegador web. En los casos en que una configuración regional no coincida con ninguno de los idiomas admitidos, el idioma predeterminado que se presenta es el inglés.

Para cada EULA, puede introducir un mensaje personalizado en los idiomas admitidos. No se proporciona contenido pretraducido para las configuraciones de EULA como sí lo es para los temas del portal. Si la configuración regional informada por un usuario coincide con un idioma en el que no se ha introducido contenido de EULA, al usuario se le devuelve una página en blanco cuando hace clic en el enlace "Términos y condiciones" en la página de inicio de sesión de VPN.

Para crear un EULA, puede utilizar cualquiera de los controles de la utilidad de configuración en la ficha **Configuración** en **NetScaler Gateway > Configuración global > EULA** o **NetScaler Gateway > Recursos > EULA**. Los controles del panel **Configuración global** se utilizan para administrar las vinculaciones globales de EULA de VPN, mientras que el control del nodo **Recursos > EULA** es para operaciones generales en las configuraciones de EULA.

Puede administrar las vinculaciones de EULA del servidor virtual VPN editando un servidor virtual VPN en **NetScaler Gateway > Servidores virtuales**. Algunos comandos también están disponibles con la línea de comandos para administrar entidades EULA. Sin embargo, los controles completos de administración de EULA solo están disponibles en la utilidad de configuración.

### Crear una entidad EULA mediante la CLI

En el símbolo del sistema, escriba;

```
add vpn eula <name>
```

### Crear una entidad EULA mediante la GUI

1. Vaya a **NetScaler Gateway > Recursos > EULA**.
2. Haga clic en **Agregar** para crear una entidad.
3. Introduzca un nombre para la entidad.
4. Para cada uno de los idiomas, pegue el contenido en las fichas correspondientes. Puede utilizar texto sin formato o etiquetas HTML para dar formato al contenido, incluida una etiqueta `<br>` para añadir saltos de línea.
5. Haga clic en **Crear**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Una vez que se ha creado una entidad EULA, se puede vincular globalmente a la configuración de VPN, o se puede vincular a un servidor virtual de VPN.

### Vincular un EULA a la VPN global mediante la CLI

En el símbolo del sistema, escriba;

```
bind vpn global eula <name>
```

### Vincular un EULA a la VPN global mediante la GUI

1. En la pestaña **Configuración**, vaya a **NetScaler Gateway > Configuración global**.
2. En el panel de detalles principal, haga clic en **Configurar un Contrato de licencia de usuario final**.
3. Haga clic en **Agregar enlace**.
4. Haga clic en **Haga clic para seleccionar**.
5. Seleccione una entidad EULA y, a continuación, haga clic en **Seleccionar**.
6. Haga clic en **Vincular**.
7. Haga clic en **Cerrar**.

### Vincular un EULA a un servidor virtual de VPN mediante la CLI

En el símbolo del sistema, escriba;

```
bind vpn vserver <name> eula <name>
```

### Vincular un EULA a un servidor virtual de VPN mediante la GUI

1. En la pestaña **Configuración**, vaya a **NetScaler Gateway > Servidores virtuales**.
2. En el panel de detalles principal, seleccione un servidor virtual VPN y haga clic en **Editar**.
3. Desde el panel de **Configuración avanzada** en el lado derecho de la página, haga clic en **EULA**.
4. En el panel de EULA recién añadido, haga clic en **Sin EULA**.
5. `Click` **Haga clic para seleccionar**.
6. Seleccione una entidad EULA y haga clic en **Seleccionar**.
7. Haga clic en **Enlazar**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

8. Haga clic en **Listo**.

## Pedir a los usuarios que actualicen los navegadores antiguos o no compatibles mediante la creación de una página personalizada

Si un cliente se conecta a una dirección VIP de NetScaler® mediante un cifrado inseguro como SSLv3, puede ser redirigido a una página personalizada que le pida que actualice a la última versión de Internet Explorer, Firefox, Chrome o Safari.

**Nota:** Según la RFC6176 del Grupo de Trabajo de Ingeniería de Internet (ITEF), los servidores TLS no deben admitir SSLv2. Por lo tanto, el dispositivo NetScaler no admite SSLv2 a partir de la versión 12.1 y posteriores.

### Cómo crear una página personalizada para pedir a los usuarios que actualicen los navegadores antiguos no compatibles basados en SSL

- Cree una directiva de respondedor de NetScaler con la regla `client.ssl.version.eq()`. La versión devuelve la versión del protocolo SSL.
  - Devuelve 0 si la transacción no está basada en SSL.
  - Devuelve 0x002 si la transacción es SSLv2.
  - Devuelve 0x300 si la transacción es SSLv3.
  - Devuelve 0x301 si la transacción es TLSv1.
- Debe habilitar SSLv3 (u otra versión anterior) para activar la directiva de respondedor.

  Por ejemplo, si SSLv3 está inhabilitado en el dispositivo NetScaler y un cliente con un navegador antiguo que usa SSLv3 intenta conectarse, se deniega el acceso.
- Si su implementación requiere SSLv3 o una versión anterior durante un período específico (uno o dos meses), configure lo siguiente:
  - Habilite el protocolo SSLv3.
  - Actualice la página personalizada para incluir información de que, después del período especificado, el navegador no podrá conectarse al dispositivo.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

# Configurar el acceso VPN sin cliente con NetScaler Gateway

El acceso sin cliente permite a los usuarios acceder a lo que necesitan sin tener que instalar software de usuario, como el cliente Citrix Secure Access™ o Receiver. Los usuarios pueden usar su navegador web para conectarse a aplicaciones web, como Outlook Web Access.

Siga estos pasos para configurar el acceso sin cliente:

- Habilitar el acceso sin cliente de forma global o mediante una directiva de sesión vinculada a un usuario, grupo o servidor virtual.
- Seleccionar el método de codificación de la dirección web.

Para habilitar el acceso sin cliente solo para un servidor virtual específico, inhabilite el acceso sin cliente globalmente y, a continuación, cree una directiva de sesión para habilitarlo.

Si utiliza el asistente de NetScaler Gateway para configurar el dispositivo, tiene la opción de configurar el acceso sin cliente dentro del asistente. La configuración del asistente se aplica globalmente. Dentro del asistente de NetScaler Gateway, puede configurar los siguientes métodos de conexión de cliente:

- Cliente Citrix Secure Access. Los usuarios solo pueden iniciar sesión con el cliente Citrix Secure Access.
- Utilice el cliente Citrix Secure Access y permita la reserva de escenarios de acceso. Los usuarios inician sesión en NetScaler Gateway con el cliente Citrix Secure Access. Si el dispositivo del usuario falla en un análisis de Endpoint Analysis, los usuarios pueden iniciar sesión mediante el acceso sin cliente. Cuando esto ocurre, los usuarios tienen acceso limitado a los recursos de red.
- Permitir a los usuarios iniciar sesión mediante un navegador web y acceso sin cliente. Los usuarios solo pueden iniciar sesión mediante el acceso sin cliente y reciben acceso limitado a los recursos de red.

## Cómo funcionan las directivas de acceso VPN sin cliente

Puede configurar el acceso sin cliente a las aplicaciones web creando directivas. Puede configurar los ajustes de una directiva de acceso sin cliente en la utilidad de configuración. Una directiva de acceso sin cliente se compone de una regla y un perfil. Puede utilizar las directivas de acceso sin cliente preconfiguradas que vienen con NetScaler Gateway. También puede crear sus propias directivas de acceso sin cliente personalizadas.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler Gateway proporciona directivas preconfiguradas para lo siguiente:

- Outlook Web Access y Outlook Web App
- SharePoint 2007
- Todas las demás aplicaciones web

**NOTA:**

OWA 2016 y SharePoint 2016 solo son compatibles mediante el acceso sin cliente avanzado.

Tenga en cuenta las siguientes características de las directivas de acceso sin cliente preconfiguradas:

- Se configuran automáticamente y no se pueden cambiar.
- Cada directiva está enlazada a nivel global.
- Cada directiva no se aplica a menos que habilite el acceso sin cliente globalmente o creando una directiva de sesión.
- No puede eliminar ni modificar los enlaces globales, incluso si no habilita el acceso sin cliente.

La compatibilidad con otras aplicaciones web depende de las directivas de reescritura que configure en NetScaler Gateway. Citrix recomienda probar cualquier directiva personalizada que cree para asegurarse de que todos los componentes de la aplicación se reescriban correctamente.

Si permite conexiones desde Receiver para Android, Receiver para iOS o Citrix Secure Hub™, debe habilitar el acceso sin cliente. Para Citrix Secure Hub que se ejecuta en un dispositivo iOS, también debe habilitar Secure Browse dentro del perfil de sesión. Secure Browse y el acceso sin cliente funcionan juntos para permitir conexiones desde dispositivos iOS. No es necesario habilitar Secure Browse si los usuarios no se conectan con dispositivos iOS.

El asistente de configuración rápida configura las directivas y la configuración de acceso sin cliente correctas para dispositivos móviles. Citrix® recomienda ejecutar el asistente de configuración rápida para configurar las directivas correctas para las conexiones a StoreFront y Citrix Endpoint Management.

Puede enlazar directivas de acceso sin cliente personalizadas globalmente o a un servidor virtual. Si desea enlazar directivas de acceso sin cliente a un servidor virtual, debe crear una directiva personalizada y luego enlazarla. Para aplicar diferentes directivas de acceso sin cliente, ya sea globalmente o para un servidor virtual, cambie el número de prioridad de la directiva personalizada para que tenga un número inferior al de las directivas preconfiguradas, lo que le dará a la directiva

© 1997–2026 Citrix Systems, Inc. All rights reserved.

personalizada una prioridad más alta. Si no hay otras directivas de acceso sin cliente enlazadas al servidor virtual, las directivas globales preconfiguradas tienen prioridad.

**NOTA:**

No puede cambiar los números de prioridad de las directivas de acceso sin cliente preconfiguradas.

## Habilitar el acceso VPN sin cliente

Cuando habilita el acceso sin cliente a nivel global, todos los usuarios reciben la configuración para el acceso sin cliente. Puede usar el asistente de NetScaler Gateway, una directiva global o una directiva de sesión para habilitar el acceso sin cliente.

En una configuración global o un perfil de sesión, el acceso sin cliente tiene las siguientes configuraciones:

- **Activado**. Habilita el acceso sin cliente. Si deshabilita las opciones de cliente y no configura o deshabilita StoreFront™, los usuarios inician sesión mediante el acceso sin cliente.
- **Desactivado**. El acceso sin cliente no está habilitado de forma predeterminada. El acceso sin cliente se habilita después de que los usuarios inicien sesión con el cliente Citrix Secure Access. Si deshabilita las opciones de cliente y no configura o deshabilita StoreFront, los usuarios inician sesión con el cliente Citrix Secure Access. Si el análisis de puntos finales falla cuando los usuarios inician sesión, los usuarios reciben la página de opciones con el acceso sin cliente disponible.
- **Inhabilitado**. El acceso sin cliente está inhabilitado. Cuando selecciona **Inhabilitado**, los usuarios no pueden iniciar sesión mediante el acceso sin cliente y el icono de acceso sin cliente no aparece en la página de opciones.

Si no habilita el acceso sin cliente mediante el asistente de NetScaler Gateway, puede habilitarlo globalmente o en una directiva de sesión mediante la utilidad de configuración.

### Para habilitar el acceso sin cliente globalmente

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda NetScaler Gateway y, a continuación, haga clic en **Configuración global**.
2. En el panel de detalles, en **Configuración**, haga clic en **Cambiar configuración global**.
3. En la ficha **Experiencia del cliente**, junto a **Acceso sin cliente**, seleccione **ACTIVADO** y, a continuación, haga clic en **Aceptar**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

### Para habilitar el acceso sin cliente mediante una directiva de sesión

Si desea que solo un grupo selecto de usuarios, grupos o servidores virtuales utilicen el acceso sin cliente, inhabilite o borre el acceso sin cliente globalmente. Luego, mediante una directiva de sesión, habilite el acceso sin cliente y vincúlelo a usuarios, grupos o servidores virtuales.

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda **NetScaler Gateway > Directivas > Sesión**.
2. En el panel de detalles, en la ficha Directivas, haga clic en **Agregar**.
3. En **Nombre**, escriba un nombre para la directiva.
4. Junto a **Perfil de solicitud**, haga clic en **Nuevo**.
5. En **Nombre**, escriba un nombre para el perfil.
6. En la ficha **Experiencia del cliente**, junto a Acceso sin cliente, haga clic en **Anular global**, seleccione **Activado** y, a continuación, haga clic en **Crear**.
7. En el cuadro de diálogo **Crear directiva de sesión**, junto a **Expresiones con nombre**, seleccione General, seleccione Valor verdadero, haga clic en Agregar expresión, haga clic en **Crear** y, a continuación, haga clic en **Cerrar**.
8. Haga clic en **Crear** y, a continuación, haga clic en **Cerrar**.

Después de crear la directiva de sesión que habilita el acceso sin cliente, la vincula a un usuario, grupo o servidor virtual.

## Codificar la dirección web

Cuando habilita el acceso sin cliente, puede optar por codificar las direcciones de las aplicaciones web internas o dejar la dirección como texto sin formato. La configuración es:

- Ocultar. Esto utiliza mecanismos de codificación estándar para ocultar la parte del dominio y el protocolo del recurso.
- Borrar. La dirección web no está codificada y es visible para los usuarios.
- Cifrar. El dominio y el protocolo se cifran mediante una clave de sesión. Cuando la dirección web está cifrada, la URL es diferente para cada sesión de usuario para el mismo recurso web. Si los usuarios marcan la dirección web codificada, la guardan en el navegador web y luego cierran la sesión, cuando los usuarios inician sesión e intentan conectarse a la dirección web de nuevo usando el marcador, no pueden conectarse a la dirección web. Nota: Si los usuarios guardan el marcador cifrado en la interfaz de acceso durante su sesión, el marcador funciona cada vez que el usuario inicia sesión.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Puede configurar esta opción globalmente o como parte de una directiva de sesión. Si configura la codificación como parte de la directiva de sesión, puede vincularla a los usuarios, grupos o a un servidor virtual.

### Configurar la codificación de direcciones web globalmente

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda NetScaler Gateway y, a continuación, haga clic en Configuración global.
2. En el panel de detalles, en Configuración, haga clic en Cambiar configuración global.
3. En la pestaña Experiencia del cliente, junto a Codificación de URL de acceso sin cliente, seleccione el nivel de codificación y, a continuación, haga clic en Aceptar.

## Configurar la codificación de direcciones web mediante la creación de una directiva de sesión

1. En la utilidad de configuración, en la pestaña Configuración, en el panel de navegación, expanda **NetScaler Gateway > Policies** y, a continuación, haga clic en Sesión.
2. En el panel de detalles, en la pestaña Directivas, haga clic en Agregar.
3. En Nombre, escriba un nombre para la directiva.
4. Junto a Perfil de solicitud, haga clic en Nuevo.
5. En Nombre, escriba un nombre para el perfil.
6. En la pestaña Experiencia del cliente, junto a Codificación de URL de acceso sin cliente, haga clic en Anular global, seleccione el nivel de codificación y, a continuación, haga clic en Aceptar.
7. En el cuadro de diálogo Crear directiva de sesión, junto a Expresiones con nombre, seleccione General, seleccione Valor verdadero, haga clic en Agregar expresión, haga clic en Crear y, a continuación, haga clic en Cerrar.

## Crear directivas de acceso sin cliente

Si desea utilizar la misma configuración que para las directivas de acceso sin cliente predeterminadas, pero desea vincular la directiva a un servidor virtual, puede copiar las directivas predeterminadas, proporcionando un nuevo nombre para la directiva. Puede utilizar la utilidad de configuración para copiar las directivas predeterminadas.

Después de vincular la nueva directiva al servidor virtual, puede establecer la prioridad de la directiva para que se ejecute primero cuando un usuario inicie sesión.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

### Crear una directiva de acceso sin cliente utilizando la configuración predeterminada

1. En la utilidad de configuración, en el panel de navegación, expanda **NetScaler Gateway > Policies** y, a continuación, haga clic en Acceso sin cliente.
2. En el panel de detalles, en la pestaña Directivas, haga clic en una directiva predeterminada y, a continuación, haga clic en Agregar.
3. En Nombre, escriba un nuevo nombre para la directiva, haga clic en Crear y, a continuación, haga clic en Cerrar.

## Vincular una directiva de acceso sin cliente a un servidor virtual

Después de crear la directiva, vincúlela al servidor virtual.

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda NetScaler Gateway y, a continuación, haga clic en Servidores virtuales.
2. En el panel de detalles, seleccione un servidor virtual y, a continuación, haga clic en Abrir.
3. En el cuadro de diálogo Configurar servidor virtual de NetScaler Gateway, haga clic en la ficha Directivas y, a continuación, haga clic en Sin cliente.
4. Haga clic en Insertar directiva, seleccione una directiva de la lista y, a continuación, haga clic en Aceptar.

### Crear y evaluar expresiones de directivas de acceso sin cliente

Al crear una directiva para el acceso sin cliente, puede crear su propia expresión para la directiva. Cuando haya terminado de crear la expresión, puede evaluarla para comprobar su precisión.

1. En la utilidad de configuración, en el panel de navegación, expanda **NetScaler Gateway > Directivas** y, a continuación, haga clic en Acceso sin cliente.
2. En el panel de detalles, en la ficha Directivas, haga clic en una directiva predeterminada y, a continuación, haga clic en Agregar.
3. En Nombre, escriba un nombre para la directiva.
4. Junto a Perfil, haga clic en Nuevo.
5. En Nombre, escriba un nombre para el perfil.
6. Configure los ajustes de reescritura y, a continuación, haga clic en Crear.
7. En el cuadro de diálogo Crear política de acceso sin cliente, en Expresión, haga clic en Agregar.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

8. En el cuadro de diálogo Agregar expresión, cree la expresión y, a continuación, haga clic en Aceptar.
9. En el cuadro de diálogo Crear política de acceso sin cliente, haga clic en Evaluar y, si la expresión se evalúa como correcta, haga clic en Crear.

## Acceso VPN sin cliente avanzado con NetScaler Gateway

La VPN sin cliente es una forma de proporcionar acceso remoto a los recursos de la intranet corporativa a través de NetScaler Gateway sin una aplicación cliente VPN en la máquina cliente. La VPN sin cliente proporciona acceso remoto a aplicaciones web empresariales, portales y otros recursos utilizando un navegador web en el lado del cliente. La solución avanzada de VPN sin cliente elimina las siguientes limitaciones relacionadas con la VPN sin cliente:

- Las URL relativas no se pueden identificar a veces.
- Las URL relativas generadas dinámicamente no se pueden identificar.

La VPN sin cliente avanzada identifica la URL absoluta y los nombres de host y los reescribe de una manera nueva y única en lugar de intentar reescribir las URL relativas presentes en las respuestas HTTP/páginas web. SharePoint ya no necesita usar la carpeta predeterminada para reescribir URL y se admite un acceso personalizado a SharePoint.

### Requisitos previos

Los siguientes son los requisitos previos para configurar la VPN sin cliente avanzada.

- **Certificado de servidor comodín** - La VPN sin cliente avanzada reescribe las URL de una manera única. Esta singularidad se mantiene para cada URL por usuario. Por ejemplo, si la aplicación web está alojada en `https://webapp.customer.com`, y el servidor virtual VPN está alojado en `https://vpn.customer.com`, entonces la VPN sin cliente avanzada lo reescribe como `https://cvpneqwerty.vpn.customer.com`. Esto significa que cada URL se reescribe como un subdominio del servidor virtual VPN. En esta nueva URL, `cvpneqwerty` se puede descifrar de nuevo a `https://webapp.customer.com`. La cadena `cvpneqwerty` es dinámica y, por lo tanto, para SSL, debe vincular el servidor virtual VPN con un certificado comodín.

  Si el servidor está alojado con `https://vpn.customer.com`, el certificado del servidor ahora debe tener entradas para (vpn.customer.com y .vpn.customer.com) como parte del CN o SAN de los certificados (donde CN=nombre común, SAN=Nombre alternativo del sujeto). El proceso de vinculación de este certificado sigue siendo el mismo en NetScaler Gateway. **Nota:** Los certificados comodín solo admiten un nivel (es decir, ..customer.com no está permitido). Si ya

© 1997–2026 Citrix Systems, Inc. All rights reserved.

está utilizando un certificado comodín (para *.customer.com) y aloja `https://vpn.customer.com`, esto no funciona para la VPN sin cliente avanzada. Debe obtener un nuevo certificado con `*.vpn.customer.com`.

- **Entrada DNS comodín** - Los clientes (navegadores web) deben resolver el FQDN de la aplicación VPN sin cliente avanzada. Al configurar el servidor NetScaler Gateway, debe haber configurado una entrada DNS para resolver vpn.customer.com. Esto permite que el navegador resuelva vpn.customer.com a la dirección IP de su servidor virtual VPN. Para resolver URL como `https://cvpnqwerty.vpn.customer.com` a la misma IP (dirección IP del servidor virtual VPN), debe agregar un nuevo registro para el dominio de `vpn.customer.com`. Busque la configuración de dominio en su servidor DNS y agregue un nuevo registro de host para "*" con la misma dirección IP que antes. Después de agregar el registro de host, debe ver respuestas de ping exitosas para `https://cpvnanything.vpn.customer.com`.

### Configurar el acceso VPN sin cliente avanzado

**Para configurar el acceso VPN sin cliente avanzado mediante la interfaz de línea de comandos, en el símbolo del sistema, escriba:**

```
set vpn parameter -clientlessVpnMode ON

set vpn parameter -advancedClientlessVpnMode ENABLED
```

Si se vincula una acción de sesión al servidor virtual, también debe habilitar la opción de modo VPN sin cliente avanzado para esa acción de sesión.

**Ejemplo:**

```
set vpn sessionaction SessionActionName -advancedclientlessvpn ENABLED
```

**Para configurar el acceso VPN sin cliente avanzado mediante la GUI de NetScaler:**

1. En la GUI de NetScaler®, vaya a **Configuration > NetScaler > Global Settings**.
2. En la **página Global Settings**, haga clic en **Change Global Settings** y, a continuación, seleccione la ficha **Client Experience**.
3. En la ficha **Client Experience**, en la lista **Clientless Access**, haga clic en **On**.
4. En la ficha **Client Experience**, en la lista **Advanced Clientless VPN Mode**, haga clic en **Enabled**. Si selecciona **STRICT** en la lista **Advanced Clientless VPN Mode**, el dispositivo NetScaler solo responde a las URL de StoreFront en el formato VPN sin cliente clásico y

© 1997–2026 Citrix Systems, Inc. All rights reserved.

bloquea todas las demás solicitudes de VPN sin cliente clásicas. Esta opción proporciona una configuración más segura en el dispositivo para entregar recursos web internos.

**NOTA:**

- Si una acción de sesión está vinculada al servidor virtual, también debe habilitar la opción **Advanced Clientless VPN Mode** para esa acción de sesión desde la ficha **Client Experience** en la página **Configure NetScaler Gateway Session Profile**.
- Puede seleccionar la opción **Override Global** para anular la configuración global.
- También puede configurar la función VPN sin cliente avanzada a nivel de sesión.

### Advertencias

La VPN sin cliente avanzada tiene como objetivo proporcionar acceso a las aplicaciones web empresariales. Dichas aplicaciones tienen un solo FQDN para cada tipo de recurso que necesitan (JavaScript, CSS, imágenes, etc.). Dado que codificamos el FQDN completo de las aplicaciones internas en un solo octeto (VPN sin cliente), perdemos la relación de subdominio. Como resultado, cada vez que una aplicación web empresarial se configura con CORS, a veces puede notar problemas al acceder a ella a través de la VPN sin cliente avanzada.

## Configurar el acceso a dominios para los usuarios

Si los usuarios se conectan mediante acceso sin cliente, puede restringir los recursos de red, los dominios y los sitios web a los que los usuarios pueden acceder. Puede usar el asistente de NetScaler Gateway o la configuración global para crear listas para incluir o excluir el acceso a dominios.

Puede permitir el acceso a todos los recursos de red, dominios y sitios web y, a continuación, crear una lista de exclusión. La lista de exclusión cita un conjunto específico de recursos a los que los usuarios no pueden acceder. Los usuarios no pueden acceder a ningún dominio que se encuentre en la lista de exclusión.

También puede denegar el acceso a todos los recursos de red, dominios y sitios web y, a continuación, crear una lista de inclusión específica. La lista de inclusión cita los recursos a los que los usuarios pueden acceder. Los usuarios no pueden acceder a ningún dominio que no aparezca en la lista.

Nota: Si configura directivas de acceso sin cliente para Citrix Endpoint Management o StoreFront y los usuarios se conectan con Receiver para Web, debe permitir los dominios a los que Receiver

© 1997–2026 Citrix Systems, Inc. All rights reserved.

para Web puede acceder. Esto es necesario para que NetScaler Gateway pueda reescribir el tráfico de red para StoreFront y Endpoint Management.

### Para configurar el acceso a dominios mediante el asistente de NetScaler Gateway

1. En la utilidad de configuración, haga clic en la ficha Configuración y, a continuación, en el panel de navegación, haga clic en NetScaler Gateway.
2. En el panel de detalles, en Introducción, haga clic en el asistente de NetScaler Gateway.
3. Haga clic en Siguiente y, a continuación, siga las instrucciones del asistente hasta llegar a la página Configurar acceso sin cliente.
4. Haga clic en Configurar dominios para acceso sin cliente y realice una de las siguientes acciones:
   - Para crear una lista de dominios excluidos, haga clic en Excluir dominios.
   - Para crear una lista de dominios incluidos, haga clic en Permitir dominios.
5. En Nombres de dominio, escriba el nombre de dominio y, a continuación, haga clic en Agregar.
6. Repita el paso 5 para cada dominio que quiera agregar a la lista y, a continuación, haga clic en Aceptar cuando termine.
7. Continúe configurando el dispositivo mediante el asistente de NetScaler Gateway.

### Para configurar los ajustes de dominio mediante la utilidad de configuración

También puede crear o modificar la lista de dominios mediante la configuración global en la utilidad de configuración.

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda NetScaler Gateway y, a continuación, haga clic en Configuración global.
2. En el panel de detalles, en Acceso sin cliente, haga clic en Configurar dominios para acceso sin cliente.
3. Realice una de las siguientes acciones:
   - Para crear una lista de dominios excluidos, haga clic en Excluir dominios.
   - Para crear una lista de dominios incluidos, haga clic en Permitir dominios.
4. En Nombres de dominio, escriba el nombre de dominio y, a continuación, haga clic en Agregar.
5. Repita el paso 4 para cada dominio que desee agregar a la lista y, a continuación, haga clic en Aceptar cuando haya terminado.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

# Acceso VPN sin cliente para SharePoint 2003, SharePoint 2007 y SharePoint 2013

NetScaler Gateway puede reescribir contenido de uno o más sitios de SharePoint 2003, SharePoint 2007 o SharePoint 2013 para que el contenido esté disponible para los usuarios sin necesidad del cliente Citrix Secure Access. Para que el proceso de reescritura se complete correctamente, debe configurar NetScaler Gateway con el nombre de host de cada servidor SharePoint de su red.

Puede usar el asistente de NetScaler Gateway o la utilidad de configuración para configurar el nombre de host de los sitios de SharePoint.

En el asistente de NetScaler Gateway, navegue por el asistente para configurar sus ajustes. Cuando llegue a la página Configurar acceso sin cliente, escriba la dirección web del sitio de SharePoint y, a continuación, haga clic en **Agregar**.

Para agregar más sitios web o para configurar SharePoint por primera vez después de ejecutar el asistente de NetScaler Gateway, utilice la utilidad de configuración.

**IMPORTANTE:**

El acceso sin cliente clásico admite versiones hasta SharePoint 2013 y OWA 2013. El acceso sin cliente avanzado admite SharePoint 2016 y OWA 2016, y versiones posteriores.

## Configurar el acceso sin cliente para SharePoint mediante la GUI de NetScaler

1. Vaya a **NetScaler Gateway** > **Configuración global**.
2. En el panel de detalles, en Acceso sin cliente, haga clic en **Configurar acceso sin cliente para SharePoint**.
3. En Acceso sin cliente para SharePoint, en Nombre de host del servidor SharePoint, escriba el nombre de host del sitio SharePoint y, a continuación, haga clic en **Agregar**.
4. Repita el paso 3 para cada sitio de SharePoint que desee agregar a la lista y, a continuación, haga clic en **Aceptar** cuando haya terminado.

## Establecer un sitio de SharePoint como página de inicio

Si desea establecer un sitio de SharePoint como página de inicio de los usuarios, configure un perfil de sesión e introduzca el nombre de host del sitio de SharePoint.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**Para configurar un sitio de SharePoint como página de inicio**

1. Vaya a **NetScaler Gateway > Directivas** y, a continuación, haga clic en **Sesión**.
2. En el panel de detalles, haga clic en **Agregar**.
3. En **Nombre**, escriba un nombre para la directiva.
4. Junto a **Perfil de solicitud**, haga clic en **Nuevo**.
5. En Nombre, escriba un nombre para el perfil.
6. En la ficha Experiencia del cliente, junto a Página principal, haga clic en **Anular global** y, a continuación, escriba el nombre del sitio de SharePoint.
7. Junto a Acceso sin cliente, haga clic en **Anular global**, seleccione **Activado** y, a continuación, haga clic en **Crear**.
8. En el cuadro de diálogo Crear directiva de sesión, junto a Expresiones con nombre, seleccione **General**, seleccione **Valor verdadero**, haga clic en **Agregar expresión**, haga clic en **Crear** y, a continuación, haga clic en **Cerrar**.

Después de completar la directiva de sesión, vincúlela a usuarios, grupos, servidores virtuales o globalmente. Cuando los usuarios inicien sesión, verán el sitio web de SharePoint como su página de inicio.

### Habilitar la resolución de nombres para los servidores de SharePoint 2007

Los servidores de SharePoint 2007 envían el nombre del servidor configurado como nombre de host dentro de varias URL como parte de la respuesta. Si un nombre de servidor de SharePoint configurado no es el nombre de dominio completo (FQDN), NetScaler Gateway no puede resolver la dirección IP utilizando el nombre del servidor de SharePoint, y algunas funciones de usuario agotan el tiempo de espera con el mensaje de error “HTTP:1.1 Gateway Time-out”. Estas funciones pueden incluir la entrada y salida de archivos, la visualización del espacio de trabajo y la carga de varios archivos cuando los usuarios inician sesión mediante el acceso sin cliente.

Para resolver este problema, puede probar una de las siguientes opciones:

- Configure un sufijo DNS en NetScaler Gateway para que el nombre de host de SharePoint se convierta en un FQDN antes de la resolución de nombres.
- Configure una entrada DNS local en NetScaler Gateway para cada nombre de servidor de SharePoint.
- Cambie todos los nombres de servidor de SharePoint para usar el FQDN, como SharePoint.intranetdomain en lugar de SharePoint,

© 1997–2026 Citrix Systems, Inc. All rights reserved.

### Configurar un sufijo DNS

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda **DNS** y, a continuación, haga clic en **Sufijo DNS**.
2. En el panel de detalles, haga clic en **Agregar**.
3. En **Sufijo DNS**, escriba el nombre de dominio de la intranet como sufijo, haga clic en **Crear** y, a continuación, haga clic en **Cerrar**.

Puede repetir el paso 3 para cada dominio que desee agregar.

**Para configurar un registro DNS local para cada nombre de servidor de SharePoint en NetScaler Gateway**

1. En la utilidad de configuración, en el panel de navegación, expanda **DNS > Registros** y, a continuación, haga clic en **Registros de direcciones**.
2. En el panel de detalles, haga clic en **Agregar**.
3. En **Nombre de host**, escriba el nombre de host de SharePoint para el registro de dirección DNS.
4. En **Dirección IP**, escriba la dirección IP del servidor de SharePoint, haga clic en **Agregar**, haga clic en **Crear** y, a continuación, haga clic en **Cerrar**.

El nombre de host para el que se agrega un registro A no debe tener un registro CNAME. Además, no puede haber registros A duplicados en el dispositivo.

## Habilitar cookies persistentes de acceso VPN sin cliente

Las cookies persistentes son necesarias para acceder a ciertas funciones de SharePoint, como abrir y editar documentos de Microsoft Word, Excel y PowerPoint alojados en el servidor de SharePoint.

Una cookie persistente permanece en el dispositivo del usuario y se envía con cada solicitud HTTP. NetScaler Gateway cifra la cookie persistente antes de enviarla al complemento en el dispositivo del usuario y la actualiza periódicamente mientras la sesión exista. La cookie caduca si la sesión finaliza.

En el asistente de NetScaler Gateway, los administradores pueden habilitar las cookies persistentes globalmente. También puede crear una directiva de sesión para habilitar las cookies persistentes por usuario, grupo o servidor virtual.

Las siguientes opciones están disponibles para las cookies persistentes:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Permitir habilita las cookies persistentes y los usuarios pueden abrir y editar documentos de Microsoft almacenados en SharePoint.
- Denegar deshabilita las cookies persistentes y los usuarios no pueden abrir ni editar documentos de Microsoft almacenados en SharePoint.
- Preguntar solicita a los usuarios que permitan o denieguen las cookies persistentes durante la sesión.

Las cookies persistentes no son necesarias para el acceso sin cliente si los usuarios no se conectan a SharePoint.

### Configurar cookies persistentes para el acceso VPN sin cliente para SharePoint

Puede configurar cookies persistentes para el acceso sin cliente para SharePoint, ya sea globalmente o como parte de una directiva de sesión.

#### Para configurar cookies persistentes globalmente

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda NetScaler Gateway y, a continuación, haga clic en Configuración global.
2. En el panel de detalles, en Configuración, haga clic en Cambiar configuración global.
3. En la ficha Experiencia del cliente, junto a Cookies persistentes de acceso sin cliente, seleccione una opción y, a continuación, haga clic en Aceptar.

#### Para configurar cookies persistentes como parte de una directiva de sesión

1. En la utilidad de configuración, en la pestaña Configuración, en el panel de navegación, expanda **NetScaler Gateway > Directivas** y, a continuación, haga clic en Sesión.
2. En el panel de detalles, en la pestaña Directivas, haga clic en Agregar.
3. En Nombre, escriba un nombre para la directiva.
4. Junto a Perfil de solicitud, haga clic en Nuevo.
5. En Nombre, escriba un nombre para el perfil.
6. En la pestaña Experiencia del cliente, junto a Cookies persistentes de acceso sin cliente, haga clic en Anular global, seleccione una opción y, a continuación, haga clic en Crear.
7. En el cuadro de diálogo Crear directiva de autenticación, junto a Expresiones con nombre, seleccione General, seleccione Valor verdadero, haga clic en Agregar expresión, haga clic en Crear y, a continuación, haga clic en Cerrar.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

# Cliente VPN Citrix® SSO para dispositivos móviles

Citrix SSO es el cliente VPN para dispositivos móviles (macOS, iOS y iOS). Citrix SSO proporciona compatibilidad completa con la administración de dispositivos móviles (MDM) en macOS, iOS y Android. Con un servidor MDM, un administrador puede configurar y administrar de forma remota perfiles VPN a nivel de dispositivo y perfiles VPN por aplicación. Citrix SSO también es compatible con la mayoría de las funciones de uso común.

## Referencias

- Cliente de Citrix Secure Access
- Clientes VPN de NetScaler Gateway y funciones compatibles

# Configurar la página de opciones de cliente

Puede configurar NetScaler Gateway para proporcionar a los usuarios varias opciones de inicio de sesión. Al configurar la página de opciones de cliente, los usuarios tienen la opción de iniciar sesión desde una ubicación con las siguientes opciones:

- Cliente Citrix Secure Access™ para Windows
- Cliente Citrix Secure Access para macOS X
- StoreFront™
- Acceso sin cliente

Los usuarios inician sesión en NetScaler Gateway mediante la dirección web del certificado vinculado a NetScaler Gateway o al servidor virtual. Al crear una directiva y un perfil de sesión, puede determinar las opciones de inicio de sesión que reciben los usuarios. Dependiendo de cómo configure NetScaler Gateway, la página de opciones de cliente muestra hasta tres iconos que representan las siguientes opciones de inicio de sesión:

- Acceso a la red. Cuando los usuarios inician sesión en NetScaler Gateway por primera vez mediante un explorador web y, a continuación, seleccionan Acceso a la red, aparece la página de descarga. Cuando los usuarios hacen clic en Descargar, el plug-in se descarga e instala en el dispositivo del usuario. Cuando la descarga y la instalación se completan, aparece la interfaz de acceso. Si instala una versión más reciente o revierte a una versión anterior de NetScaler Gateway, el cliente Citrix Secure Access para Windows se actualiza o degrada silenciosamente a la versión del dispositivo. Si los usuarios se conectan mediante el cliente Citrix Secure Access para Mac, el plug-in se actualiza silenciosamente si se detecta una nueva

© 1997–2026 Citrix Systems, Inc. All rights reserved.

versión del dispositivo cuando los usuarios inician sesión. Esta versión del plug-in no se degrada silenciosamente.

- StoreFront. Si los usuarios seleccionan StoreFront para iniciar sesión, se abre Receiver y los usuarios pueden acceder a aplicaciones y escritorios.

  **NOTA:**

  Si configura StoreFront como una opción de cliente, las aplicaciones y los escritorios no aparecen en el panel izquierdo de la interfaz de acceso.

- Acceso sin cliente. Si los usuarios seleccionan el acceso sin cliente para iniciar sesión, aparece la interfaz de acceso o su página de inicio personalizada. En la interfaz de acceso, los usuarios pueden navegar a recursos compartidos de archivos, sitios web y usar Outlook Web Access.

Secure Browse permite a los usuarios conectarse a través de NetScaler Gateway desde un dispositivo iOS. Si habilita Secure Browse, cuando los usuarios inician sesión mediante Secure Hub, Secure Browse inhabilita la página de opciones de cliente.

## Mostrar la página de opciones de cliente al iniciar sesión

Cuando habilita la opción de opciones de cliente, los usuarios pueden iniciar sesión con el cliente Citrix Secure Access, Receiver o acceso sin cliente desde una página web después de una autenticación correcta en NetScaler Gateway. Cuando el inicio de sesión es correcto, aparecen iconos en la página web desde la que los usuarios pueden elegir el método para establecer una conexión.

Puede habilitar las opciones de cliente sin usar el análisis de puntos finales ni implementar la reserva de escenarios de acceso. Si no define una expresión de seguridad de cliente, los usuarios reciben opciones de conexión para la configuración establecida en NetScaler Gateway. Si existe una expresión de seguridad de cliente para la sesión de usuario y el dispositivo del usuario falla el análisis de puntos finales, la página de opciones solo ofrece acceso sin cliente para iniciar sesión.

Puede configurar las opciones de cliente de forma global o mediante un perfil y una directiva de sesión.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**IMPORTANTE:**

Al configurar las opciones de cliente, no configure grupos de cuarentena. Los dispositivos de usuario que fallan el análisis de puntos finales y se ponen en cuarentena se tratan igual que los dispositivos de usuario que pasan el análisis de puntos finales.

### Habilitar las opciones de cliente globalmente

1. En la GUI, en la ficha Configuration, en el panel de navegación, expanda **NetScaler Gateway** y, a continuación, haga clic en **Global Settings**.
2. En el panel de detalles, en Settings, haga clic en **Change global settings**.
3. En la ficha Client Experience, haga clic en **Advanced Settings**.
4. En la ficha General, haga clic en **Client Choices** y, a continuación, haga clic en **OK**.

### Habilitar las opciones de cliente como parte de una directiva de sesión

También puede configurar las opciones de cliente como parte de una directiva de sesión y, a continuación, vincularla a usuarios, grupos y servidores virtuales.

1. En la GUI, en la ficha Configuration, en el panel de navegación, expanda **NetScaler Gateway > Policies** y, a continuación, haga clic en **Session**.
2. En el panel de detalles, en la ficha Policies, haga clic en **Add**.
3. En Name, escriba un nombre para la directiva.
4. Junto a Request Profile, haga clic en **New**.
5. En Nombre, escriba un nombre para el perfil.
6. En la ficha Experiencia del cliente, haga clic en **Avanzado**.
7. En la ficha General, junto a Opciones de cliente, haga clic en **Anular global**, haga clic en **Opciones de cliente**, haga clic en **Aceptar** y, a continuación, haga clic en **Crear**.
8. En el cuadro de diálogo Crear directiva de sesión, junto a Expresiones con nombre, seleccione **General**, seleccione **True value**, haga clic en **Agregar expresión**, haga clic en **Crear** y, a continuación, haga clic en **Cerrar**.

## Configurar las opciones de Opciones de cliente

Además de habilitar las opciones de cliente mediante un perfil y una directiva de sesión, debe configurar los ajustes del software de usuario. Por ejemplo, quiere que los usuarios inicien sesión mediante el cliente Citrix Secure Access, StoreFront o el acceso sin cliente. Cree un perfil de

© 1997–2026 Citrix Systems, Inc. All rights reserved.

sesión que habilite las tres opciones y las opciones de cliente. A continuación, cree una directiva de sesión con la expresión establecida en True value con el perfil adjunto. Después, vincule la directiva de sesión a un servidor virtual.

Antes de crear la directiva y el perfil de sesión, debe crear un grupo de autorización para los usuarios.

### Crear un grupo de autorización

1. En la utilidad de configuración, en la ficha Configuración del panel de navegación, **NetScaler Gateway > Administración de usuarios** y, a continuación, haga clic en **AAA Groups**.
2. En el panel de detalles, haga clic en **Agregar**.
3. En **Nombre del grupo**, escriba el nombre del grupo.
4. En la ficha **Usuarios**, seleccione los usuarios, haga clic en **Agregar** para cada uno, haga clic en **Crear** y, a continuación, haga clic en **Cerrar**.

El siguiente procedimiento es un ejemplo de perfil de sesión para las opciones de cliente con el cliente Citrix Secure Access, StoreFront y el acceso sin cliente.

## Crear un perfil de sesión para las opciones de cliente

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda **NetScaler Gateway > Directivas > Sesión**.
2. En el panel de detalles, haga clic en la pestaña **Perfiles** y, a continuación, en **Agregar**.
3. En **Nombre**, escriba un nombre para el perfil.
4. En la ficha **Experiencia del cliente**, haga lo siguiente:
    a. Junto a Página principal, haga clic en **Anular global** y, a continuación, desactive **Mostrar página principal**. Esto inhabilita la interfaz de acceso.
    b. Junto a **Acceso sin cliente**, haga clic en **Anular global** y, a continuación, seleccione **DESACTIVADO**.
    c. Junto a **Tipo de plug-in**, haga clic en **Anular global** y, a continuación, seleccione Windows/Mac OS X.
    d. Haga clic en **Configuración avanzada** y, junto a **Opciones de cliente**, haga clic en **Anular global** y, a continuación, en **Opciones de cliente**.
5. En la ficha **Seguridad**, junto a **Acción de autorización predeterminada**, haga clic en **Anular global** y, a continuación, seleccione **PERMITIR**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

6. En la ficha **Seguridad**, haga clic en **Configuración avanzada**.
7. En **Grupos de autorización**, haga clic en **Anular global**, haga clic en **Agregar** y, a continuación, seleccione el grupo.
8. En la ficha **Aplicaciones publicadas**, haga lo siguiente:
    a. Junto a **Proxy ICA®**, haga clic en **Anular global** y, a continuación, seleccione **DESACTIVADO**.
    b. Junto a **Dirección de la interfaz web**, haga clic en **Anular global** y, a continuación, escriba la dirección web de StoreFront, como `<http://ipAddress/Citrix/>`.
    c. Junto a **Modo de portal de interfaz web**, haga clic en **Anular global** y, a continuación, seleccione **COMPACTO**.
    d. Junto a **Dominio de inicio de sesión único**, haga clic en **Anular global** y, a continuación, escriba el nombre del dominio.
9. Haga clic en **Crear** y, a continuación, en **Cerrar**.

Si quiere usar el cliente Citrix Secure Access para Java como opción de cliente, en la ficha **Experiencia del cliente**, en Tipo de complemento, seleccione **Java**. Si selecciona esta opción, debe configurar una aplicación de intranet y establecer el modo de intercepción en Proxy.

Después de crear el perfil de sesión, cree una directiva de sesión. Dentro de la directiva, seleccione el perfil y establezca la expresión en el valor Verdadero.

Para usar StoreFront como opción de cliente, también debe configurar la Secure Ticket Authority (STA) en NetScaler Gateway. La STA está vinculada al servidor virtual.

**NOTA:**

Si el servidor que ejecuta StoreFront no está disponible, la opción Citrix Virtual Apps™ no aparece en la página de opciones.

### Configurar el servidor STA globalmente

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda **NetScaler Gateway** y, a continuación, haga clic en **Configuración global**.
2. En el panel de detalles, en Servidores, haga clic en **Enlazar/Desenlazar servidores STA** para que los use la Secure Ticket Authority.
3. En el cuadro de diálogo **Enlazar/Desenlazar servidores STA**, haga clic en **Agregar**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. En el cuadro de diálogo **Configurar servidor STA**, en la URL, escriba la dirección web del servidor STA y, a continuación, haga clic en **Crear**.
5. Repita los pasos 3 y 4 para agregar más servidores STA y, a continuación, haga clic en **Aceptar**.

### Vincular la STA a un servidor virtual

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda **NetScaler Gateway** y, a continuación, haga clic en **Servidores virtuales**.
2. En el panel de detalles, haga clic en un servidor virtual y, a continuación, haga clic en **Abrir**.
3. En la pestaña **Aplicaciones publicadas**, en **Secure Ticket Authority**, en **Activo**, seleccione los servidores STA y, a continuación, haga clic en **Aceptar**.

También puede agregar servidores STA en la pestaña **Aplicaciones publicadas**.

## Configurar la reserva de escenario de acceso

SmartAccess permite a NetScaler Gateway determinar automáticamente los métodos de acceso permitidos para un dispositivo de usuario basándose en los resultados de un análisis de punto final. La reserva de escenario de acceso amplía aún más esta capacidad al permitir que un dispositivo de usuario recurra del cliente Citrix Secure Access a StoreFront mediante la aplicación Citrix Workspace si el dispositivo de usuario no supera el análisis inicial de punto final.

Para habilitar la reserva de escenario de acceso, se configura una política de postautenticación que determina si los usuarios reciben un método de acceso alternativo al iniciar sesión en NetScaler Gateway. Esta política de postautenticación se define como una expresión de seguridad de cliente que se configura globalmente o como parte de un perfil de sesión. Si se configura un perfil de sesión, el perfil se asocia a una política de sesión que luego se vincula a usuarios, grupos o servidores virtuales. Cuando se habilita la reserva de escenario de acceso, NetScaler Gateway inicia un análisis de punto final después de la autenticación del usuario. Los resultados para los dispositivos de usuario que no cumplen los requisitos de un análisis de postautenticación de reserva son los siguientes:

- Si las opciones de cliente están habilitadas, los usuarios pueden iniciar sesión en StoreFront utilizando únicamente la aplicación Citrix Workspace.
- Si el acceso sin cliente y las opciones de cliente están deshabilitados, los usuarios pueden ser puestos en cuarentena en un grupo que proporciona acceso solo a StoreFront.
- Si el acceso sin cliente y StoreFront están habilitados en NetScaler Gateway y el proxy ICA está deshabilitado, los usuarios recurren al acceso sin cliente.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Si StoreFront no está configurado y el acceso sin cliente está establecido en permitido, los usuarios recurren al acceso sin cliente.

Cuando el acceso sin cliente está deshabilitado, se debe configurar la siguiente combinación de ajustes para la reserva de escenario de acceso:

- Definir los parámetros de seguridad del cliente para el análisis de postautenticación de reserva.
- Definir la página de inicio de la interfaz web.
- Deshabilitar las opciones de cliente.
- Si los dispositivos de usuario fallan la comprobación de seguridad del cliente, los usuarios se colocan en un grupo de cuarentena que permite el acceso solo a StoreFront y a las aplicaciones publicadas.

## Crear políticas para la reserva de escenario de acceso

Para configurar NetScaler Gateway para la reserva de escenario de acceso, debe crear políticas y grupos de las siguientes maneras:

- Crear un grupo de cuarentena en el que se colocan los usuarios si el análisis de punto final falla.
- Crear una configuración global de StoreFront que se utilice si el análisis de punto final falla.
- Cree una directiva de sesión que anule la configuración global y, a continuación, vincule la directiva de sesión a un grupo.
- Cree una directiva de seguridad de cliente global que se aplique si el análisis de punto final falla.

Al configurar la reserva de escenarios de acceso, utilice las siguientes directrices:

- El uso de opciones de cliente o la reserva de escenarios de acceso requiere el complemento de análisis de punto final para todos los usuarios. Si el análisis de punto final no se puede ejecutar o si los usuarios seleccionan Omitir análisis durante el análisis, se les deniega el acceso. Nota: La opción de omitir el análisis se elimina en NetScaler Gateway 10.1, compilación 120.1316.e
- Cuando habilita las opciones de cliente, si el dispositivo de usuario falla el análisis de punto final, los usuarios se colocan en el grupo de cuarentena. Los usuarios pueden seguir iniciando sesión con el cliente Citrix Secure Access o la aplicación Citrix Workspace en StoreFront. Nota: CitrixÂ® recomienda no crear un grupo de cuarentena si habilita las opciones de cliente.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Los dispositivos de usuario que fallan el análisis de punto final se ponen en cuarentena y se tratan de la misma manera que los dispositivos de usuario que pasan el análisis de punto final.

- Si el análisis de punto final falla y el usuario se coloca en el grupo de cuarentena, las directivas vinculadas al grupo de cuarentena solo son efectivas si no hay directivas vinculadas directamente al usuario que tengan un número de prioridad igual o inferior al de las directivas vinculadas al grupo de cuarentena.
- Puede utilizar diferentes direcciones web para la interfaz de acceso y StoreFront. Al configurar las páginas de inicio, la página de inicio de la interfaz de acceso tiene prioridad para el cliente Citrix Secure Access y la página de inicio de la aplicación Citrix Workspace tiene prioridad para StoreFront.

### Crear un grupo de cuarentena

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda **NetScaler Gateway > Administración de usuarios** y, a continuación, haga clic en **Grupos AAA**.
2. En el panel de detalles, haga clic en **Agregar**.
3. En **Nombre de grupo**, escriba un nombre para el grupo, haga clic en **Crear** y, a continuación, haga clic en **Cerrar**.

**IMPORTANTE:**

El nombre del grupo de cuarentena no debe coincidir con el nombre de ningún grupo de dominio al que puedan pertenecer los usuarios. Si el grupo de cuarentena coincide con un nombre de grupo de Active Directory, los usuarios se ponen en cuarentena incluso si el dispositivo de usuario pasa el análisis de seguridad de punto final.

Después de crear el grupo, configure NetScaler Gateway para que recurra a la interfaz de acceso si el dispositivo de usuario falla el análisis de punto final.

### Configurar ajustes para poner en cuarentena las conexiones de usuario

1. En la utilidad de configuración, en la pestaña Configuración, en el panel de navegación, expanda NetScaler Gateway y, a continuación, haga clic en **Configuración global**.
2. En el panel de detalles, en **Configuración**, haga clic en **Cambiar configuración global**.
3. En el cuadro de diálogo **Configuración global de NetScaler Gateway**, en la pestaña **Aplicaciones publicadas**, junto a **Proxy ICA**, seleccione **DESACTIVADO**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. Junto a **Dirección de interfaz web**, escriba la dirección web de StoreFront.
5. Junto a **Dominio de inicio de sesión único**, escriba el nombre de su dominio de Active Directory y, a continuación, haga clic en **Aceptar**.

Después de configurar los ajustes globales, cree una directiva de sesión que anule la configuración global de ICAÂ® Proxy y, a continuación, vincule la directiva de sesión al grupo de cuarentena.

### Crear una directiva de sesión para la reserva de escenarios de acceso

1. En la utilidad de configuración, en la pestaña Configuración, en el panel de navegación, expanda **NetScaler Gateway > Directivas** y, a continuación, haga clic en **Sesión**.
2. En el panel de detalles, haga clic en **Agregar**.
3. En **Nombre**, escriba un nombre para la directiva.
4. Junto a **Perfil de solicitud**, haga clic en **Nuevo**.
5. En la pestaña **Aplicaciones publicadas**, junto a **Proxy ICA**, haga clic en **Anular global**, seleccione **Activado** y, a continuación, haga clic en **Crear**.
6. En el cuadro de diálogo **Crear directiva de sesión**, junto a **Expresiones con nombre**, seleccione **General**, seleccione **Valor verdadero**, haga clic en **Agregar expresión**, haga clic en **Crear** y, a continuación, haga clic en **Cerrar**.

Después de crear la directiva de sesión, vincule la directiva a un grupo de cuarentena.

### Vincular la política de sesión al grupo de cuarentena

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda **NetScaler Gateway > Administración de usuarios** y, a continuación, haga clic en **Grupos AAA**.
2. En el panel de detalles, seleccione un grupo y, a continuación, haga clic en **Abrir**.
3. Haga clic en Sesión.
4. En la ficha **Directivas**, seleccione **Sesión** y, a continuación, haga clic en **Insertar directiva**.
5. En **Nombre de directiva**, seleccione la directiva y, a continuación, haga clic en **Aceptar**.

Después de crear la política de sesión y el perfil que habilita StoreFront en NetScaler Gateway, cree una política de seguridad de cliente global.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

### Crear una política de seguridad de cliente global

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda NetScaler Gateway y, a continuación, haga clic en **Configuración global**.
2. En el panel de detalles, en **Configuración**, haga clic en **Cambiar configuración global**.
3. En la ficha **Seguridad**, haga clic en **Configuración avanzada**.
4. En **Seguridad del cliente**, introduzca la expresión. Para obtener más información sobre cómo configurar expresiones del sistema, consulte Configuración de expresiones del sistema y Configuración de expresiones de seguridad de cliente compuestas
5. En **Grupo de cuarentena**, seleccione el grupo que configuró en el procedimiento de grupo y, a continuación, haga clic en **Aceptar**.

## Configurar conexiones para el cliente Citrix Secure Access™

Las conexiones de los dispositivos de usuario se configuran definiendo los recursos a los que los usuarios pueden acceder en la red interna. La configuración de las conexiones de los dispositivos de usuario incluye:

- Definir los dominios a los que los usuarios tienen acceso permitido.
- Configurar direcciones IP para los usuarios, incluidas las agrupaciones de direcciones (IP de intranet).
- Configurar la configuración de tiempo de espera.
- Configurar el inicio de sesión único.
- Configurar la intercepción de clientes.
- Configurar la tunelización dividida.
- Configurar las conexiones a través de un servidor proxy.
- Configurar el software de usuario para conectarse a través de NetScaler Gateway.
- Configurar el acceso para dispositivos móviles.

La mayoría de las conexiones de los dispositivos de usuario se configuran mediante un perfil que forma parte de una directiva de sesión. También puede definir la configuración de conexión de los dispositivos de usuario mediante aplicaciones de intranet, la autenticación previa y las directivas de tráfico.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**NOTA:**

El complemento VPN de Windows y los complementos EPA recopilan datos de telemetría para sus diversas operaciones. Para deshabilitar la funcionalidad, haga lo siguiente en la máquina cliente.

Establezca el registro “HKLM\Software\Citrix\Secure Access Client\DisableGA” de tipo REG_DWORD en 1.

## Configurar el número de sesiones de usuario

Puede configurar el número máximo de usuarios a los que se les permite conectarse a NetScaler Gateway en un momento determinado, ya sea a nivel global o por servidor virtual. Las sesiones no se crean en NetScaler Gateway cuando el número de usuarios que se conectan al dispositivo supera el valor que usted configura. Si el número de usuarios supera el número permitido, los usuarios reciben un mensaje de error.

### Para establecer el límite global de usuarios

Cuando se configura el límite de usuarios globalmente, la restricción se aplica a todos los usuarios que establecen sesiones con diferentes servidores virtuales en el sistema. Cuando el número de sesiones de usuario alcanza el valor establecido, no se pueden establecer nuevas sesiones en ningún servidor virtual presente en NetScaler Gateway.

El número máximo de usuarios se establece a nivel global al configurar el tipo de autenticación predeterminado para NetScaler Gateway.

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda NetScaler Gateway y, a continuación, haga clic en Configuración global.
2. En el panel de detalles, en Configuración, haga clic en Cambiar configuración de autenticación.
3. En el cuadro de diálogo Configuración de autenticación global, en Número máximo de usuarios, escriba el número de usuarios y, a continuación, haga clic en Aceptar.

### Para establecer el límite de usuarios por servidor virtual

También puede aplicar el límite de usuarios a cada servidor virtual del sistema. Cuando se configura el límite de usuarios por servidor virtual, la restricción se aplica solo a los usuarios que establecen sesiones con ese servidor virtual en particular. Los usuarios que establecen sesiones con otros servidores virtuales no se ven afectados por este límite.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda NetScaler Gateway y, a continuación, haga clic en Servidores virtuales.
2. En el panel de detalles, haga clic en un servidor virtual y, a continuación, haga clic en Abrir.
3. En Usuarios máximos, escriba el número de usuarios y, a continuación, haga clic en Aceptar.

## Configurar ajustes de tiempo de espera

Puede configurar NetScaler Gateway para forzar una desconexión si no hay actividad en la conexión durante un número de minutos especificado. Un minuto antes de que una sesión expire (se desconecte), el usuario recibe una alerta que indica que la sesión se cerrará. Si la sesión se cierra, el usuario debe iniciar sesión de nuevo.

Las siguientes opciones de tiempo de espera están disponibles.

- **Tiempo de espera forzado:** Si habilita esta configuración, NetScaler Gateway desconecta la sesión después de que transcurra el intervalo de tiempo de espera (en minutos), independientemente de lo que esté haciendo el usuario. No hay ninguna acción que el usuario pueda realizar para evitar que se produzca la desconexión cuando transcurra el intervalo de tiempo de espera. Esta configuración se aplica a los usuarios que se conectan con el cliente Citrix Secure Access, la aplicación Citrix Workspace, Secure Hub o a través de un navegador web. El valor mínimo es 1 y el valor máximo es 65535.
- **Tiempo de espera de sesión:** Si habilita esta configuración, NetScaler Gateway desconecta la sesión si no se detecta actividad de red durante el intervalo especificado (en minutos). Esta configuración se aplica a los usuarios que se conectan con el cliente Citrix Secure Access, la aplicación Citrix Workspace, Citrix Secure Hub o a través de un navegador web. La configuración predeterminada de tiempo de espera es de 30 minutos. El valor mínimo es 1 y el valor máximo es 65535.
- **Tiempo de espera de sesión inactiva:** La duración (en minutos) tras la cual el cliente Citrix Secure Access™ finaliza una sesión inactiva si no hay actividad del usuario, como la del ratón, el teclado o la táctil, durante el intervalo especificado. Esta configuración se aplica únicamente a los usuarios que se conectan con el cliente Citrix Secure Access. El valor mínimo es 1 y el valor máximo es 9999.

Puede habilitar cualquiera de las configuraciones de tiempo de espera introduciendo un valor entre 1 y 65536 para especificar los minutos del intervalo de tiempo de espera. Si habilita más de una de estas configuraciones, el primer intervalo de tiempo de espera que transcurra cerrará la conexión del dispositivo de usuario.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Puede configurar los ajustes de tiempo de espera configurando los ajustes globales o utilizando un perfil de sesión. Cuando agrega el perfil a una política de sesión, la política se vincula a un usuario, grupo o servidor virtual. Cuando configura los ajustes de tiempo de espera globalmente, los ajustes se aplican a todas las sesiones de usuario.

**NOTA:**

- En Always On (modo de servicio o modo de usuario), el cliente VPN ignora todos los tiempos de espera. Las decisiones de tiempo de espera forzado y tiempo de espera de sesión se producen en el dispositivo NetScaler y, por lo tanto, esos tiempos de espera funcionan según lo previsto. Si se produce dicho tiempo de espera, el complemento VPN intenta realizar la autenticación automática.

  En Always On, dado que el dispositivo de usuario debe estar conectado a través del túnel VPN todo el tiempo, no configure el tiempo de espera forzado ni el tiempo de espera de inactividad del cliente. Sin embargo, se puede configurar el tiempo de espera de sesión para eliminar sesiones obsoletas.
- Algunas aplicaciones, como Microsoft Outlook, envían automáticamente sondeos de tráfico de red a los servidores de correo electrónico sin ninguna intervención del usuario. Citrix® recomienda que configure el tiempo de espera de sesión inactiva con el tiempo de espera de sesión para asegurarse de que una sesión desatendida en un dispositivo de usuario expire en un tiempo razonable.

## Configurar tiempos de espera forzados

Un tiempo de espera forzado desconecta el cliente Citrix Secure Access automáticamente después de una cantidad de tiempo especificada en minutos. Puede configurar un tiempo de espera forzado globalmente o como parte de una política de sesión.

### Configurar un tiempo de espera forzado global

1. En la utilidad de configuración, en la pestaña **Configuration**, en el panel de navegación, expanda NetScaler Gateway y, a continuación, haga clic en **Global Settings**.
2. En el panel de detalles, en **Settings**, haga clic en **Change global settings**.
3. En la pestaña **Network Configuration**, haga clic en **Advanced Settings**.
4. En Forced Time-out (mins), escriba el número de minutos que los usuarios pueden permanecer conectados.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. En Forced Time-out Warning (mins), escriba el número de minutos antes de que se advierta a los usuarios de que la conexión se desconectará y, a continuación, haga clic en **OK**.

#### Configurar un tiempo de espera forzado dentro de una directiva de sesión

Si desea tener un mayor control sobre quién recibe el tiempo de espera forzado, cree una directiva de sesión y, a continuación, aplique la directiva a un usuario o grupo.

1. En la utilidad de configuración, en la pestaña **Configuration**, en el panel de navegación, expanda **NetScaler Gateway** > **Policies** y, a continuación, haga clic en **Session**.
2. En el panel de detalles, haga clic en **Add**.
3. En Name, escriba un nombre para la directiva.
4. Junto a Request Profile, haga clic en **New**.
5. En Name, escriba un nombre para el perfil.
6. En la pestaña **Network Configuration**, haga clic en **Advanced**.
7. En Timeouts, haga clic en **Override Global** y en Forced Time-out (mins) escriba el número de minutos que los usuarios pueden permanecer conectados.
8. Junto a **Forced Time-out Warning (mins)**, haga clic en **Override Global** y escriba el número de minutos antes de que se advierta a los usuarios de que la conexión se desconectará. Haga clic en **OK** dos veces.
9. En el cuadro de diálogo **Crear directiva de sesión**, junto a **Expresiones con nombre**, seleccione General, seleccione **Valor verdadero**, haga clic en **Agregar expresión**, haga clic en **Crear** y, a continuación, haga clic en **Cerrar**.

### Configurar tiempos de espera de sesión o de inactividad

Puede usar la GUI de NetScaler para configurar los ajustes de tiempo de espera de sesión y de cliente globalmente o para crear una directiva de sesión. Al crear una directiva y un perfil de sesión, establezca la expresión en True.

**NOTA:**

Si no anula explícitamente la configuración global y establece el tiempo de espera de la sesión en **Experiencia del cliente > Tiempo de espera de la sesión (minutos)**, esto puede provocar bucles de autenticación que requieren volver a iniciar sesión. Esto ocurre incluso con el tiempo de espera de sesión predeterminado de 30 minutos.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

### Para configurar un tiempo de espera de sesión o de inactividad del cliente globalmente mediante la GUI

1. En la ficha **Configuración**, en el panel de navegación, expanda **NetScaler Gateway** y, a continuación, haga clic en **Configuración global**.
2. En el panel de detalles, en **Configuración**, haga clic en **Cambiar configuración global**.
3. En la ficha **Experiencia del cliente**, realice una o ambas de las siguientes acciones:
   - En **Tiempo de espera de la sesión (minutos)**, escriba el número de minutos.
   - En **Tiempo de espera de inactividad del cliente (minutos)**, escriba el número de minutos y, a continuación, haga clic en **Aceptar**.

### Para configurar los ajustes de tiempo de espera de sesión o de inactividad del cliente mediante una directiva de sesión con la GUI

1. En la ficha **Configuración**, en el panel de navegación, expanda **NetScaler Gateway** > **Directivas** y, a continuación, haga clic en **Sesión**.
2. En la página **Directivas y perfiles de sesión de NetScaler Gateway**, haga clic en **Perfiles de sesión** y, a continuación, haga clic en **Agregar**.
3. En Nombre, escriba un nombre para el perfil.
4. En la pestaña **Experiencia del cliente**, realice una o ambas de las siguientes acciones:
   - Junto a **Tiempo de espera de sesión (min)**, haga clic en **Anular global** y, a continuación, escriba el número de minutos y haga clic en **Crear**.
   - Junto a **Tiempo de espera de inactividad del cliente (min)**, haga clic en **Anular global**, escriba el número de minutos y, a continuación, haga clic en **Crear**.
5. a. En la página **Directivas y perfiles de sesión de NetScaler Gateway**, haga clic en **Directivas de sesión** y, a continuación, haga clic en **Agregar**.
6. En **Crear directiva de sesión de NetScaler Gateway**,
   - En **Nombre**, introduzca el nombre de la directiva.
   - En **Perfil**, seleccione el perfil que especifica la acción que aplicará la nueva directiva de sesión si se cumplen los criterios de la regla.
   - seleccione **Directiva avanzada**.
   - En el campo **Expresión**, agregue su expresión o el nombre de una expresión con nombre, especificando el tráfico que coincide con la directiva.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Haga clic en **Crear** y, a continuación, haga clic en **Cerrar**.

## Conectar a recursos de red internos

Puede configurar NetScaler Gateway para permitir a los usuarios acceder a los recursos de la red interna. Si inhabilita el túnel dividido, todo el tráfico de red del dispositivo de usuario se envía a NetScaler Gateway y las directivas de autorización determinan si se permite que el tráfico pase a los recursos de red internos. Cuando habilita el túnel dividido, solo el tráfico destinado a la red interna es interceptado por el dispositivo de usuario y enviado a NetScaler Gateway. Puede configurar qué direcciones IP intercepta NetScaler Gateway mediante aplicaciones de intranet.

Si utiliza el cliente Citrix Secure Access™ para Windows, establezca el modo de intercepción en transparente. Si utiliza el cliente Citrix Secure Access para Java, establezca el modo de intercepción en proxy. Cuando establece el modo de intercepción en transparente, puede permitir el acceso a los recursos de red mediante:

- Una única dirección IP y máscara de subred
- Un rango de direcciones IP

Si establece el modo de intercepción en proxy, puede configurar las direcciones IP de destino y origen y los números de puerto.

### Configurar el acceso a la red para recursos de red internos

1. En la utilidad de configuración, en la ficha **Configuración**, en el panel de navegación, expanda NetScaler Gateway, expanda Recursos y, a continuación, haga clic en **Aplicaciones de intranet**.
2. En el panel de detalles, haga clic en **Agregar**.
3. Complete los parámetros para permitir el acceso a la red, haga clic en **Crear** y, a continuación, haga clic en **Cerrar**.

## Configurar la tunelización dividida

Puede habilitar la tunelización dividida para evitar que el cliente Citrix Secure Access envíe tráfico de red innecesario a NetScaler Gateway.

Cuando no se habilita la tunelización dividida, el cliente Citrix Secure Access captura todo el tráfico de red originado en un dispositivo de usuario y lo envía a través del túnel VPN a NetScaler Gateway.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Si habilita la tunelización dividida, el cliente Citrix Secure Access solo envía el tráfico destinado a redes protegidas por NetScaler Gateway a través del túnel VPN. El cliente Citrix Secure Access no envía tráfico de red destinado a redes no protegidas a NetScaler Gateway.

Cuando se inicia el cliente Citrix Secure Access, obtiene la lista de aplicaciones de intranet de NetScaler Gateway. El cliente Citrix Secure Access examina todos los paquetes transmitidos en la red desde el dispositivo de usuario y compara las direcciones dentro de los paquetes con la lista de aplicaciones de intranet. Si la dirección de destino del paquete se encuentra dentro de una de las aplicaciones de intranet, el cliente Citrix Secure Access envía el paquete a través del túnel VPN a NetScaler Gateway. Si la dirección de destino no está en una aplicación de intranet definida, el paquete no se cifra y el dispositivo de usuario lo enruta de forma adecuada. Cuando se habilita la tunelización dividida, las aplicaciones de intranet definen el tráfico de red que se intercepta.

**NOTA:**

Si los usuarios se conectan a aplicaciones publicadas en una granja de servidores mediante la aplicación Citrix Workspace, no es necesario configurar la tunelización dividida.

NetScaler Gateway también admite la tunelización dividida inversa, que define el tráfico de red que NetScaler Gateway no intercepta. Si establece la tunelización dividida en inversa, las aplicaciones de intranet definen el tráfico de red que NetScaler Gateway no intercepta. Cuando se habilita la tunelización dividida inversa, todo el tráfico de red dirigido a direcciones IP internas omite el túnel VPN, mientras que el resto del tráfico pasa por NetScaler Gateway. La tunelización dividida inversa se puede utilizar para registrar todo el tráfico LAN no local. Por ejemplo, si los usuarios tienen una red inalámbrica doméstica y han iniciado sesión con el cliente Citrix Secure Access, NetScaler Gateway no intercepta el tráfico de red destinado a una impresora u otro dispositivo dentro de la red inalámbrica.

Para obtener más información sobre las aplicaciones de intranet, consulte Configuración de la interceptación de clientes.

La tunelización dividida se configura como parte de la directiva de sesión.

### Para configurar la tunelización dividida

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda **Directivas de NetScaler Gateway** y, a continuación, haga clic en **Sesión**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. En el panel de detalles, en la ficha **Perfiles**, seleccione un perfil y, a continuación, haga clic en **Abrir**.
3. En la ficha **Experiencia del cliente**, junto a **Túnel dividido**, seleccione **Anulación global**, elija una opción y, a continuación, haga clic en **Aceptar** dos veces.

### Configuración de la tunelización dividida y la autorización

Al planificar la implementación de NetScaler Gateway, es importante tener en cuenta el túnel dividido y la acción de autorización predeterminada y las directivas de autorización.

Por ejemplo, tiene una directiva de autorización que permite el acceso a un recurso de red. Tiene el túnel dividido configurado en ON y no configura las aplicaciones de intranet para enviar tráfico de red a través de NetScaler Gateway. Cuando NetScaler Gateway tiene este tipo de configuración, se permite el acceso al recurso, pero los usuarios no pueden acceder a él.

Si la directiva de autorización deniega el acceso a un recurso de red, tiene el túnel dividido configurado en ON y las aplicaciones de intranet están configuradas para enrutar el tráfico de red a través de NetScaler Gateway, el cliente de Citrix Secure Access envía tráfico a NetScaler Gateway, pero se deniega el acceso al recurso.

Para obtener más información sobre las opciones de túnel dividido, consulte Opciones de túnel dividido.

## Configurar la intercepción de cliente

Se configuran reglas de intercepción para las conexiones de usuario en NetScaler Gateway mediante aplicaciones de intranet. De forma predeterminada, al configurar la dirección IP del sistema, una dirección IP asignada o una dirección IP de subred en el dispositivo, se crean rutas de subred basadas en estas direcciones IP. Las aplicaciones de intranet se crean automáticamente en función de estas rutas y se pueden vincular a un servidor virtual. Si habilita la tunelización dividida, debe definir aplicaciones de intranet para que se produzca la intercepción del cliente.

Puede configurar aplicaciones de intranet mediante la GUI. Puede vincular aplicaciones de intranet a usuarios, grupos o servidores virtuales.

Si habilita la tunelización dividida y los usuarios se conectan mediante WorxWeb o WorxMail, al configurar la intercepción de cliente, debe agregar las direcciones IP de Citrix Endpoint Management™ y de su servidor Exchange. Si no habilita la tunelización dividida, no es necesario

© 1997–2026 Citrix Systems, Inc. All rights reserved.

que configure las direcciones IP de Endpoint Management y Exchange en las aplicaciones de intranet.

Para obtener información sobre la configuración de la tunelización dividida, consulte Configurar la tunelización dividida.

### Configurar aplicaciones de intranet para el cliente Citrix Secure Access™

Cree aplicaciones de intranet para el acceso de los usuarios a los recursos definiendo lo siguiente:

- Una dirección IP
- Un rango de direcciones IP
- Un nombre de host

Cuando se define una aplicación de intranet en NetScaler Gateway, el cliente Citrix Secure Access para Windows intercepta el tráfico de usuario destinado al recurso y lo envía a través de NetScaler Gateway.

Al configurar aplicaciones de intranet, tenga en cuenta lo siguiente:

- Cuando la tunelización dividida está ACTIVADA,
  - Configure las aplicaciones de intranet.
  - Asigne aplicaciones de intranet a cada grupo de autenticación, autorización y auditoría.
- Cuando el túnel dividido está DESACTIVADO,
  - Todo el tráfico se intercepta a través del túnel VPN.
  - No es necesario configurar las aplicaciones de intranet.
- Cuando el túnel dividido está INVERTIDO,
  - Configure las aplicaciones de intranet. El tráfico no especificado por las aplicaciones de intranet pasa a través del túnel VPN.
  - Asigne las aplicaciones de intranet que se excluirán de la VPN a cada grupo de autenticación, autorización y auditoría.

**IMPORTANTE:**

La intercepción debe establecerse en **TRANSPARENTE** independientemente de la configuración del túnel dividido.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**Nota:**

- Al configurar una aplicación de intranet, debe seleccionar un modo de intercepción que corresponda al tipo de software de complemento utilizado para establecer conexiones.
- No puede configurar una aplicación de intranet para intercepción de proxy y transparente.

### Para crear una aplicación de intranet para una dirección IP

1. En la ficha Configuración, en el panel de navegación, expanda **Recursos de NetScaler Gateway** y, a continuación, haga clic en **Aplicaciones de intranet.**
2. En el panel de detalles, haga clic en **Agregar.**
3. En Nombre, escriba un nombre para el perfil.
4. En el cuadro de diálogo **Crear aplicación de intranet**, seleccione **TRANSPARENTE.**
5. En **Tipo de destino**, seleccione **Dirección IP** y **Máscara de red.**
6. En Protocolo, seleccione el protocolo que se aplica al recurso de red.
7. En **Dirección IP**, escriba la dirección IP.
8. En **Máscara de red**, escriba la máscara de subred, haga clic en **Crear** y, a continuación, en **Cerrar.**

### Para configurar un rango de direcciones IP

Si tiene varios servidores en su red, como servidores web, de correo electrónico y de recursos compartidos de archivos, puede configurar un recurso de red que incluya el rango IP para los recursos de red. Esta configuración permite a los usuarios acceder a los recursos de red contenidos en el rango de direcciones IP.

1. En la ficha **Configuración**, en el panel de navegación, expanda **Recursos de NetScaler Gateway** y, a continuación, haga clic en **Aplicaciones de intranet.**
2. En el panel de detalles, haga clic en **Agregar.**
3. En **Nombre**, escriba un nombre para el perfil.
4. En Protocolo, seleccione el protocolo que se aplica al recurso de red.
5. En el cuadro de diálogo **Crear aplicación de intranet**, seleccione **TRANSPARENTE**.
6. En **Tipo de destino**, seleccione **Rango de direcciones IP.**
7. En **IP inicial**, escriba la dirección IP inicial y en IP final, escriba la dirección IP final, haga clic en **Crear** y, a continuación, en **Cerrar.**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

### Para crear una aplicación de intranet para un nombre de host

1. En la pestaña Configuración, en el panel de navegación, expanda **Recursos de NetScaler Gateway** y, a continuación, haga clic en **Aplicaciones de intranet.**
2. En el panel de detalles, haga clic en **Agregar**.
3. En **Nombre**, escriba un nombre para el perfil.
4. En el cuadro de diálogo **Crear aplicación de intranet**, seleccione **TRANSPARENTE**.
5. En **Tipo de destino**, seleccione **nombre de host**.
6. En Protocolo, seleccione **CUALQUIERA**, haga clic en **Crear** y, a continuación, haga clic en **Cerrar**.

**IMPORTANTE:**

- A partir de la versión 13.0 compilación 36.27 y posteriores, el plug-in VPN de Windows admite reglas basadas en el nombre de host (FQDN) para la tunelización dividida. Debe actualizar tanto el dispositivo NetScaler como el plug-in VPN de Windows a la versión 13.0 compilación 36.27 o posterior.
- También se admiten nombres de host comodín. Por ejemplo, si se configura una aplicación de intranet con el nombre de host “*.example.com”, `a1.example.com`, `b2.example.com`, etc., se tuneliza.
- La aplicación de intranet basada en el nombre de host solo funciona cuando la tunelización dividida está configurada en ON o REVERSE.

## Configurar la resolución de servicio de nombres

Durante la instalación de NetScaler Gateway, puede usar el asistente de NetScaler Gateway para configurar otros ajustes, incluidos los proveedores de servicios de nombres. Los proveedores de servicios de nombres traducen el nombre de dominio completo (FQDN) a una dirección IP. En el asistente de NetScaler Gateway, puede configurar un servidor DNS o WINS, establecer la prioridad de la búsqueda DNS y el número de veces que se debe reintentar la conexión al servidor.

Cuando ejecuta el asistente de NetScaler Gateway, puede agregar un servidor DNS en ese momento. Puede agregar más servidores DNS y un servidor WINS a NetScaler Gateway mediante un perfil de sesión. Luego, puede dirigir a los usuarios y grupos para que se conecten a un servidor de resolución de nombres diferente al que configuró originalmente con el asistente.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Antes de configurar un servidor DNS adicional en NetScaler Gateway, cree un servidor virtual que actúe como servidor DNS para la resolución de nombres.

### Agregar un servidor DNS o WINS dentro de un perfil de sesión

1. En la utilidad de configuración, en la ficha **Configuration** (Configuración), en el panel de navegación, expanda **NetScaler Gateway Policies** (Directivas de NetScaler Gateway) y, a continuación, haga clic en **Session** (Sesión).
2. En el panel de detalles, en la ficha Profiles (Perfiles), seleccione un perfil y, a continuación, haga clic en Open (Abrir).
3. En la ficha Network Configuration (Configuración de red), realice una de las siguientes acciones:

    - Para configurar un servidor DNS, junto a DNS Virtual Server (Servidor virtual DNS), haga clic en **Override Global** (Anular global), seleccione el servidor y, a continuación, haga clic en **OK** (Aceptar).
    - Para configurar un servidor WINS, junto a WINS Server IP (IP del servidor WINS), haga clic en **Override Global** (Anular global), escriba la dirección IP y, a continuación, haga clic en **OK** (Aceptar).

**IMPORTANTE:**

Las directivas de respondedor no se evalúan para los servidores virtuales DNS no direccionables asociados al perfil de sesión VPN.

## Habilitar la compatibilidad con proxy para conexiones de usuario

Los dispositivos de usuario pueden conectarse a través de un servidor proxy para acceder a redes internas. NetScaler Gateway admite los protocolos HTTP, SSL, FTP y SOCKS. Para habilitar la compatibilidad con proxy para las conexiones de usuario, debe especificar la configuración en NetScaler Gateway. Puede especificar la dirección IP y el puerto utilizados por el servidor proxy en NetScaler Gateway. El servidor proxy se utiliza como proxy de reenvío para todas las conexiones posteriores a la red interna.

### Configuración del proxy

Puede configurar los ajustes del proxy en el explorador o en el dispositivo NetScaler. Para configurar los ajustes del proxy en el explorador o en el dispositivo, vaya a **Configuración global**

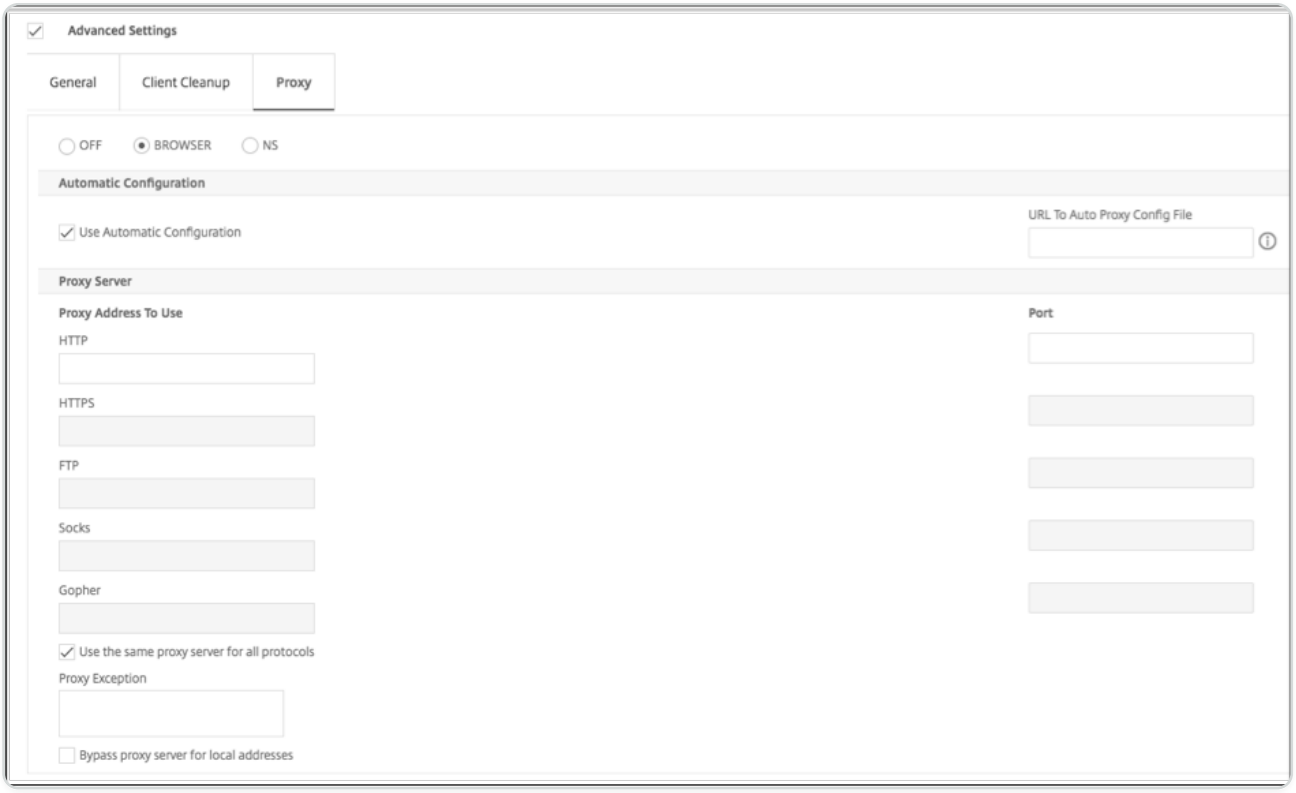
© 1997–2026 Citrix Systems, Inc. All rights reserved.

**de NetScaler Gateway > ficha Experiencia del cliente > Configuración avanzada > Proxy** y, a continuación, seleccione **Explorador** o **NS** según corresponda.

- **Explorador**: Cuando elige configurar los ajustes del proxy en el explorador, puede usar la opción de configuración automática proporcionando un enlace al archivo de configuración de proxy automático. La configuración automática podría sobrescribir la configuración manual.

  Además, al seleccionar **Explorador**, puede omitir los proxies configurados previamente seleccionando la opción de excepción de proxy.

  **Nota**: Los diferentes tipos de clientes tienen diferentes capacidades con respecto a la configuración del proxy del **explorador**. Para obtener más información, consulte Clientes VPN de NetScaler Gateway y funciones admitidas.
- **NS**: No puede usar la opción de configuración automática si configura los ajustes del proxy en el dispositivo NetScaler. No puede omitir los proxies configurados previamente al configurar los ajustes del proxy en el dispositivo.
- **DESACTIVADO**: Cuando se selecciona esta opción, NetScaler Gateway deshabilita la configuración del proxy en el complemento VPN.




### Para configurar la compatibilidad con proxy para conexiones de usuario

1. En el panel de navegación, expanda **NetScaler Gateway** y, a continuación, haga clic en **Configuración global.**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. En el panel de detalles, en **Configuración**, haga clic en Cambiar configuración global.
3. En la ficha Experiencia del cliente, haga clic en **Configuración avanzada**.
4. En la ficha **Proxy**, en **Configuración del proxy**, seleccione **Explorador.**
5. Para los protocolos, escriba la dirección IP y el número de puerto y, a continuación, haga clic en **Aceptar**.

**NOTA:**

- Si selecciona **NS**, puede configurar servidores proxy que solo admiten conexiones HTTP seguras y no seguras.
- Después de habilitar la compatibilidad con proxy en NetScaler Gateway, especifique los detalles de configuración en el dispositivo de usuario para el servidor proxy que corresponda al protocolo.

  Después de habilitar la compatibilidad con proxy, NetScaler Gateway envía los detalles del servidor proxy al explorador web del cliente y cambia la configuración del proxy en el explorador.

  - Cuando el dispositivo de usuario se conecta a NetScaler Gateway, el dispositivo de usuario puede comunicarse con el servidor proxy directamente para la conexión a la red del usuario.
  - Cuando el dispositivo de usuario se desconecta de NetScaler Gateway, la configuración del proxy se restaura a la configuración predeterminada anterior, que estaba presente antes de conectarse al complemento VPN.

### Para configurar un servidor proxy para usar todos los protocolos para NetScaler Gateway

Puede configurar un servidor proxy para admitir todos los protocolos que utiliza NetScaler Gateway. Esta configuración proporciona una combinación de dirección IP y puerto para todos los protocolos.

1. En el panel de navegación, expanda **NetScaler Gateway** y, a continuación, haga clic en **Configuración global**.
2. En el panel de detalles, en **Configuración**, haga clic en Cambiar configuración global.
3. En la ficha **Experiencia del cliente**, haga clic en **Configuración avanzada**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. En la ficha **Proxy**, en **Configuración de proxy**, seleccione **Explorador**.
5. Para los protocolos, escriba la dirección IP y el número de puerto.
6. Haga clic en Usar el mismo servidor proxy para todos los protocolos y, a continuación, haga clic en **Aceptar**.

Cuando deshabilita la tunelización dividida y establece todas las configuraciones de proxy en Activado, las configuraciones de proxy se propagan a los dispositivos de usuario. Si las configuraciones de proxy se establecen en Dispositivo, las configuraciones no se propagan a los dispositivos de usuario.

NetScaler Gateway establece conexiones con el servidor proxy en nombre del dispositivo de usuario. Las configuraciones de proxy no se propagan al navegador del usuario, por lo que no es posible la comunicación directa entre el dispositivo de usuario y el servidor proxy.

### Para configurar NetScaler Gateway como servidor proxy

Cuando configura NetScaler Gateway como servidor proxy, HTTP no seguro y seguro son los únicos protocolos compatibles.

1. En el panel de navegación, expanda **NetScaler Gateway** y, a continuación, haga clic en **Configuración global.**
2. En el panel de detalles, en **Configuración**, haga clic en Cambiar configuración global.
3. En la ficha **Experiencia del cliente**, haga clic en **Configuración avanzada.**
4. En la ficha **Proxy**, en **Configuración de proxy**, seleccione **NS**.
5. Para los protocolos, escriba la dirección IP y el número de puerto y, a continuación, haga clic en **Aceptar.**

## Configurar grupos de direcciones

En algunas situaciones, los usuarios que se conectan con el cliente Citrix Secure Access necesitan una dirección IP única para NetScaler Gateway. Por ejemplo, en un entorno Samba, cada usuario que se conecta a una unidad de red asignada debe parecer que se origina en una dirección IP diferente. Cuando habilita los grupos de direcciones (también conocidos como agrupación de IP) para un grupo, NetScaler Gateway puede asignar un alias de dirección IP único a cada usuario.

Los grupos de direcciones se configuran mediante direcciones IP de intranet. Los siguientes tipos de aplicaciones pueden necesitar usar una dirección IP única extraída del grupo de IP:

- Voz sobre IP

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- FTP activo
- Mensajería instantánea
- Secure Shell (SSH)
- Virtual Network Computing (VNC) para conectarse a un escritorio de equipo
- Escritorio remoto (RDP) para conectarse a un escritorio de cliente

Puede configurar NetScaler Gateway para asignar una dirección IP interna a los usuarios que se conectan a NetScaler Gateway. Se pueden asignar direcciones IP estáticas a los usuarios o se puede asignar un rango de direcciones IP a un grupo, un servidor virtual o al sistema globalmente.

NetScaler Gateway le permite asignar direcciones IP de su red interna a sus usuarios remotos. Una dirección IP en la red interna puede direccionar a un usuario remoto. Si elige usar un rango de direcciones IP, el sistema asigna dinámicamente una dirección IP de ese rango a un usuario remoto bajo demanda.

Al configurar grupos de direcciones, tenga en cuenta lo siguiente:

- Las direcciones IP asignadas deben enrutarse correctamente. Para garantizar el enrutamiento correcto, considere lo siguiente:
  - Si no habilita la tunelización dividida, asegúrese de que las direcciones IP se puedan enrutar a través de dispositivos de traducción de direcciones de red (NAT).
  - Cualquier servidor al que accedan las conexiones de usuario con direcciones IP de intranet debe tener las puertas de enlace adecuadas configuradas para llegar a esas redes.
  - Configure pasarelas o una ruta estática en NetScaler Gateway para que el tráfico de red del software de usuario se enrute a la red interna.
- Solo se pueden usar máscaras de subred contiguas al asignar rangos de direcciones IP. Se puede asignar un subconjunto de un rango a una entidad de nivel inferior. Por ejemplo, si un rango de direcciones IP está vinculado a un servidor virtual, vincule un subconjunto del rango a un grupo.
- Los rangos de direcciones IP no se pueden vincular a varias entidades dentro de un nivel de vinculación. Por ejemplo, un subconjunto de un rango de direcciones que está vinculado a un grupo no se puede vincular a un segundo grupo.
- NetScaler Gateway no permite eliminar o desvincular direcciones IP mientras están en uso activo por una sesión de usuario.
- Las direcciones IP de la red interna se asignan a los usuarios mediante la siguiente jerarquía:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

    - Vinculación directa del usuario
    - Grupo de direcciones asignado al grupo
    - Grupo de direcciones asignado al servidor virtual
    - Rango global de direcciones

- Solo se pueden usar máscaras de subred contiguas al asignar rangos de direcciones. Sin embargo, un subconjunto de un rango asignado podría asignarse a una entidad de nivel inferior. Un rango de direcciones global vinculado puede tener un rango vinculado a lo siguiente:
    - Servidor virtual
    - Grupo
    - Usuario
- Un rango de direcciones de servidor virtual vinculado puede tener un subconjunto vinculado a lo siguiente:
    - Grupo
    - Usuario

Un rango de direcciones de grupo enlazado puede tener un subconjunto enlazado a un usuario.

Cuando se asigna una dirección IP a un usuario, la dirección se reserva para el siguiente inicio de sesión del usuario hasta que se agota el rango del grupo de direcciones. Cuando las direcciones se agotan, NetScaler Gateway recupera la dirección IP del usuario que ha estado desconectado de NetScaler Gateway durante más tiempo.

Si no se puede recuperar una dirección y todas las direcciones están activamente en uso, NetScaler Gateway no permite que el usuario inicie sesión. Puede evitar esta situación permitiendo que NetScaler Gateway utilice la dirección IP asignada como una dirección IP de intranet cuando todas las demás direcciones IP no estén disponibles.

### Registro DNS de IP de intranet

Si se asigna una IP de intranet a una máquina cliente y, después del establecimiento del túnel VIP, el complemento VPN comprueba si esa máquina cliente está unida a un dominio. Si la máquina cliente es una máquina unida a un dominio, el complemento VPN inicia el proceso de registro DNS para vincular el nombre de host de la máquina de intranet con la dirección IP de intranet asignada. Este registro se revierte antes de la desestablecimiento del túnel.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Para un registro DNS exitoso, asegúrese de que los siguientes `nsapimgr` estén configurados. Asegúrese también de que el servidor DNS autoritativo esté configurado para permitir actualizaciones DNS "no seguras".

- **`nsapimgr` -ys enable_vpn_dns_override=1**: Este indicador se envía al cliente VPN de NetScaler Gateway junto con los demás parámetros de configuración. Si este indicador no está configurado y el cliente VPN intercepta una solicitud DNS/WINS, envía una solicitud HTTP "GET /DNS" correspondiente al servidor virtual de NetScaler Gateway a través del túnel para obtener la dirección IP resuelta. Sin embargo, si el indicador 'enable_vpn_dnstruncate_fix' está configurado, el cliente VPN reenvía las solicitudes DNS/WINS de forma transparente al servidor virtual de NetScaler Gateway. En este caso, el paquete DNS se envía tal cual al servidor virtual de NetScaler Gateway a través del túnel VPN. Esto ayuda en los casos en que los registros DNS que regresan de los servidores de nombres configurados en NetScaler Gateway son enormes y no caben en el paquete de respuesta UPD. En este caso, cuando el cliente recurre al uso de TCP-DNS, este paquete TCP-DNS llega al servidor de NetScaler Gateway tal cual, y por lo tanto el servidor de NetScaler Gateway realiza una consulta TCP-DNS a un servidor DNS.
- **nsapimgr -ys enable_vpn_dnstruncate_fix=1**: Este indicador es utilizado por el propio servidor NetScaler Gateway. Si este indicador está configurado, NetScaler Gateway anula el destino de las "conexiones TCP en el puerto DNS" a los servidores DNS configurados en NetScaler Gateway (en lugar de intentar enviarlas a la IP del servidor DNS originalmente presente en el paquete TCP-DNS entrante). Para las solicitudes DNS UDP, el valor predeterminado es utilizar los servidores DNS configurados para la resolución DNS. El complemento NetScaler Gateway para Windows admite actualizaciones DNS seguras y no seguras. La compatibilidad con actualizaciones DNS seguras existe por defecto en las compilaciones 21.7.1.1 o superiores.

  La actualización DNS segura en el complemento de Windows está deshabilitada de forma predeterminada. Para habilitarla, cree un valor de tipo REG_DWORD en `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access` y configúrelo en 1.

  - Cuando se establece el valor en 1, el complemento VPN intenta primero la actualización DNS no segura. Si la actualización DNS no segura falla, el complemento VPN intenta la actualización DNS segura.
  - Para intentar solo la actualización DNS segura, puede establecer el valor en 2.

Para obtener más información sobre cómo configurar estos parámetros, consulte `<https://support.citrix.com/article/CTX200243>`.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

### Configurar grupos de direcciones para un usuario, grupo o servidor virtual mediante la GUI

1. Vaya a **Configuration** > **NetScaler® Gateway** y realice una de las siguientes acciones:
   - Vaya a **NetScaler Gateway** > **User Administration** y, a continuación, haga clic en **AAA Users**.
   - Vaya a **NetScaler Gateway** > **User Administration** y, a continuación, haga clic en **AAA Groups**.
   - Expanda **NetScaler Gateway** y, a continuación, haga clic en **Virtual Servers**.
2. En el panel de detalles, haga clic en un usuario, grupo o servidor virtual y, a continuación, haga clic en **Open**.
3. En los cuadros de texto **IP Address** y **Netmask** de la ficha **Intranet IPs**, escriba la dirección IP y la máscara de subred y, a continuación, haga clic en **Add**.
4. Repita el paso 3 para cada dirección IP que quiera agregar al grupo y, a continuación, haga clic en **OK**.

### Configurar grupos de direcciones globalmente mediante la GUI

1. Vaya a **Configuration** > **NetScaler Gateway** > **Global Settings**.
2. En el panel de detalles, en **Intranet IPs**, haga clic en **Para asignar una dirección IP estática única o un grupo de direcciones IP para su uso por todas las sesiones de NetScaler Gateway del cliente, configure Intranet IPs**.
3. En el cuadro de diálogo **Bind Intranet IPs**, haga clic en **Action** y, a continuación, haga clic en **Insert**.
4. En los cuadros de texto **IP Address** y **Netmask**, escriba la dirección IP y la máscara de subred y, a continuación, haga clic en **Add**.
5. Repita los pasos 3 y 4 para cada dirección IP que quiera agregar al grupo y, a continuación, haga clic en **OK**.

### Configurar grupos de direcciones mediante la CLI

1. Ejecute uno de los siguientes comandos para configurar los grupos de direcciones:
   - **Para un usuario AAA:** `bind aaa user <username> -intranetIP <ip_address> <netmask>`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Para un grupo AAA:** `bind aaa group <groupname> -intranetIP <ip_address> <netmask>`
- **Para un servidor virtual VPN:** `bind vpn vserver <vservername> -intranetIP <ip_address> -netmask <netmask>`
- **Para VPN global:** `bind vpn global -intranetIP <ip_address> -netmask <netmask>`

2. A partir de la versión 13.1-53.x de NetScaler Gateway, puede usar el siguiente comando para establecer el límite en el número máximo de direcciones IP de intranet que se pueden asignar a un usuario:

   `set vpn parameter -maxIIPperUser <number>`

   **NOTA:**

   - El valor mínimo para `maxIIPperUser` es 1 y el máximo es 10.
   - Si el parámetro `maxIIPperUser` no está configurado, de forma predeterminada el número de direcciones IP de intranet que se asignan al usuario es 1.
   - La configuración `maxIIPperUser` solo se aplica a las direcciones IP de intranet configuradas a nivel de grupo AAA, servidor virtual VPN o VPN global. Las direcciones IP de intranet configuradas a nivel de usuario AAA no se ven afectadas por esta configuración.
   - Aumentar o disminuir el límite `maxIIPPerUser` no afecta a las sesiones existentes ni al número de direcciones IP de intranet asignadas. Las sesiones existentes permanecen activas hasta que se agota el tiempo de espera de la sesión/inactividad o la intervención del administrador. Sin embargo, la configuración surte efecto inmediatamente para las nuevas sesiones.

### Definir opciones de grupo de direcciones

Puede usar una directiva de sesión o la configuración global de NetScaler Gateway para controlar si se asignan direcciones IP de intranet durante una sesión de usuario. La definición de opciones de grupo de direcciones le permite asignar direcciones IP de intranet a NetScaler Gateway, al tiempo que deshabilita el uso de direcciones IP de intranet para un grupo particular de usuarios.

Puede configurar grupos de direcciones mediante una directiva de sesión de una de las tres maneras siguientes:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- `Nospillover` - Cuando configura grupos de direcciones para una dirección IP de intranet, obtiene una sesión con una IP disponible del grupo. Para los usuarios que han utilizado todas las direcciones IP de intranet disponibles, aparece la página de inicio de sesión de transferencia.
- **Desbordamiento** - Cuando se configuran grupos de direcciones y la IP asignada se utiliza como dirección IP de intranet, la dirección IP asignada se utiliza para los usuarios que han utilizado todas las direcciones IP de intranet disponibles.
- **Desactivado** - Los grupos de direcciones no están configurados.

**NOTA:**

Si la dirección IP asignada no está configurada, se utiliza SNIP.

### Para definir grupos de direcciones

1. En la utilidad de configuración, en la ficha **Configuration**, en el panel de navegación, expanda **NetScaler Gateway > Policies** y, a continuación, haga clic en **Session**.
2. En el panel de detalles, en la ficha **Policies**, haga clic en **Add**.
3. En **Name**, escriba un nombre para la directiva.
4. Junto a **Request Profile**, haga clic en **New**.
5. En Name, escriba un nombre para el perfil.
6. En la ficha **Network Configuration**, haga clic en **Advanced**.
7. Junto a Intranet IP, haga clic en **Override Global** y, a continuación, seleccione una opción.
8. Si selecciona **SPILLOVER** en el paso 9, junto a Mapped IP, haga clic en **Override Global**, seleccione el nombre de host del dispositivo, haga clic en **OK** y, a continuación, haga clic en **Create**.
9. En el cuadro de diálogo **Create Session Policy**, cree una expresión. Haga clic en **Create** y, a continuación, haga clic en **Close**.

### Configurar la página de inicio de sesión de transferencia

Si un usuario no tiene una dirección IP de intranet disponible y luego intenta establecer otra sesión con NetScaler Gateway, aparece la página de inicio de sesión de transferencia. La página de inicio de sesión de transferencia permite a los usuarios reemplazar su sesión existente de NetScaler Gateway por una nueva sesión.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

La página de inicio de sesión de transferencia también se puede usar si la solicitud de cierre de sesión se pierde o si el usuario no realiza un cierre de sesión limpio. Por ejemplo:

- A un usuario se le asigna una dirección IP de intranet estática y tiene una sesión de NetScaler Gateway existente. Si el usuario intenta establecer una segunda sesión desde un dispositivo diferente, aparece la página de inicio de sesión de transferencia y el usuario puede transferir la sesión al nuevo dispositivo.
- A un usuario se le asignan cinco direcciones IP de intranet y tiene cinco sesiones a través de NetScaler Gateway. Si el usuario intenta establecer una sexta sesión, aparece la página de inicio de sesión de transferencia y el usuario puede optar por reemplazar una sesión existente por una nueva.

**NOTAS:**

- Si el usuario no tiene una dirección IP asignada disponible por lo que no se puede establecer una nueva sesión, aparece un mensaje de error.
- Citrix Secure Access para Android 23.12.1 y versiones posteriores admiten la funcionalidad de inicio de sesión de transferencia de NetScaler Gateway en el modo Always On VPN.

La página de inicio de sesión de transferencia aparece solo si configura grupos de direcciones y deshabilita el desbordamiento.

### Configurar un sufijo DNS

Cuando un usuario inicia sesión en NetScaler Gateway y se le asigna una dirección IP, se agrega un registro DNS para la combinación de nombre de usuario y dirección IP a la caché DNS de NetScaler Gateway. Puede configurar un sufijo DNS para anexar al nombre de usuario cuando el registro DNS se agrega a la caché. Esto permite que los usuarios sean referenciados por el nombre DNS, lo que puede ser más fácil de recordar que una dirección IP. Cuando el usuario cierra sesión en NetScaler Gateway, el registro se elimina de la caché DNS.

#### Para configurar un sufijo DNS

1. En la utilidad de configuración, en la ficha **Configuración**, en el panel de navegación, expanda **NetScaler Gateway > Directivas** y, a continuación, haga clic en **Sesión**.
2. En el panel de detalles, en la ficha **Directivas**, seleccione una directiva de sesión y, a continuación, haga clic en **Abrir**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. Junto a Perfil de solicitud, haga clic en **Modificar**.
4. En la ficha **Configuración de red**, haga clic en **Avanzado**.
5. Junto a Sufijo DNS de IP de intranet, haga clic en **Anular global**, escriba el sufijo DNS y, a continuación, haga clic en **Aceptar** tres veces.

## Compatibilidad con teléfonos VoIP

Cuando se instala NetScaler Gateway como un dispositivo independiente y los usuarios se conectan con el cliente Citrix Secure Access, NetScaler Gateway admite la comunicación bidireccional con softphones de voz sobre IP (VoIP).

A continuación, se muestran algunos de los softphones VoIP compatibles con Citrix Secure Access™:

- Cisco Softphone
- Avaya IP Softphone

Se admite la tunelización segura entre la IP PBX y el software de softphone que se ejecuta en el dispositivo del usuario. Para permitir que el tráfico VoIP atraviese el túnel seguro, debe instalar el cliente Citrix Secure Access y uno de los softphones compatibles en el mismo dispositivo de usuario.

Cuando el tráfico VoIP se envía a través del túnel seguro, Citrix Secure Access admite las siguientes funciones de softphone:

- Llamadas salientes realizadas desde el softphone IP
- Llamadas entrantes realizadas al softphone IP
- Tráfico de voz bidireccional
- Flujos de control TCP y UDP con aplicaciones VoIP

**NOTA:**

Para el flujo de control UDP con DNE, la aplicación VoIP se desconecta si la duración de la inactividad es de 30 segundos o más. Por lo tanto, si la aplicación VoIP admite la mensajería de control UDP y encuentra algún problema, le recomendamos que utilice Citrix Secure Access en modo WFP.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

La compatibilidad con softphones VoIP se configura mediante direcciones IP de intranet. Debe configurar una dirección IP de intranet para cada usuario. Si utiliza Cisco Softphone Communication, después de configurar la dirección IP de intranet y vincularla a un usuario, no se requiere ninguna configuración adicional. Para obtener más información sobre cómo configurar una dirección IP de intranet, consulte Configuración de grupos de direcciones.

Si habilita la tunelización dividida, cree una aplicación de intranet y especifique la aplicación Avaya Softphone. Además, debe habilitar la intercepción transparente.

## Configurar la interfaz de acceso

NetScaler Gateway incluye una página de inicio predeterminada que aparece después de que los usuarios inician sesión. La página de inicio predeterminada se denomina Interfaz de acceso. Puede usar la Interfaz de acceso como página de inicio, o configurar StoreFront como página de inicio, o una página de inicio personalizada.

La Interfaz de acceso contiene tres paneles. Si tiene StoreFront™ en su implementación, los usuarios pueden iniciar sesión en Receiver en el panel izquierdo de la Interfaz de acceso. Si tiene StoreFront en su implementación, los usuarios no pueden iniciar sesión en Receiver desde el panel izquierdo.

La Interfaz de acceso se utiliza para proporcionar enlaces a sitios web, tanto internos como externos, y enlaces a recursos compartidos de archivos en la red interna. Puede personalizar la Interfaz de acceso de las siguientes maneras:

- Cambiar la Interfaz de acceso.
- Crear enlaces de la Interfaz de acceso.

Los usuarios también pueden personalizar la Interfaz de acceso añadiendo sus propios enlaces a sitios web y recursos compartidos de archivos. Los usuarios también pueden usar la página de inicio para transferir archivos de la red interna a su dispositivo.

**NOTA:**

Cuando los usuarios inician sesión e intentan abrir recursos compartidos de archivos desde la Interfaz de acceso, el recurso compartido de archivos no se abre y los usuarios reciben el mensaje de error “Failed to make TCP connection to the server.” Para resolver este problema, configure su firewall para permitir el tráfico desde la dirección IP del sistema NetScaler Gateway a la dirección IP del servidor de archivos en los puertos TCP 445 y 139.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

## Cambiar la Interfaz de acceso

Es posible que desee dirigir a los usuarios a una página de inicio personalizada, en lugar de depender de la Interfaz de acceso. Para ello, instale la página de inicio en NetScaler Gateway y, a continuación, configure la directiva de sesión para usar la nueva página de inicio.

### Para instalar una página de inicio personalizada

1. En la utilidad de configuración, haga clic en la ficha **Configuración** y, a continuación, en el panel de navegación, haga clic en **NetScaler Gateway.**
2. En el panel de detalles, en **Personalizar Interfaz de acceso**, haga clic en **Cargar** la **Interfaz de acceso.**
3. Para instalar la página de inicio desde un archivo en un equipo de su red, en Archivo local, haga clic en **Examinar**, vaya al archivo y, a continuación, haga clic en **Seleccionar.**
4. Para usar una página de inicio instalada en NetScaler Gateway, en Ruta remota, haga clic en **Examinar**, seleccione el archivo y, a continuación, haga clic en **Seleccionar**.
5. Haga clic en **Cargar** y, a continuación, haga clic en **Cerrar**.

## Reemplace la interfaz de acceso con una página de inicio personalizada

Puede usar la configuración global o una directiva y un perfil de sesión para configurar una página de inicio personalizada que reemplace la página de inicio predeterminada, la interfaz de acceso. Después de configurar la directiva, puede vincularla a un usuario, grupo, servidor virtual o globalmente. Cuando configura una página de inicio personalizada, la interfaz de acceso no aparece cuando los usuarios inician sesión.

### Configurar la página de inicio personalizada globalmente

1. En la utilidad de configuración, en la ficha **Configuración**, en el panel de navegación, expanda **NetScaler Gateway** y, a continuación, haga clic en **Configuración global**.
2. En el panel de detalles, en **Configuración**, haga clic en Cambiar configuración global.
3. En la ficha **Experiencia del cliente**, en **Página de inicio**, haga clic en **Mostrar página de inicio** y, a continuación, introduzca la dirección web de su página de inicio personalizada.
4. Haga clic en **Aceptar** y, a continuación, haga clic en **Cerrar**.

### Configurar una página de inicio personalizada en un perfil de sesión

1. En la utilidad de configuración, en la ficha **Configuración**, en el panel de navegación, expanda **Directivas de NetScaler Gateway** y, a continuación, haga clic en **Sesión**.
2. En el panel de detalles, en la ficha **Directivas**, haga clic en **Agregar**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. En Nombre, escriba un nombre para la directiva.
4. Junto a **Perfil de solicitud**, haga clic en **Nuevo**.
5. En **Nombre**, escriba un nombre para el perfil.
6. En la pestaña **Client Experience**, junto a **Home Page**, haga clic en **Override Global**, haga clic en **Display Home Page** y, a continuación, escriba la dirección web de la página de inicio.
7. En el cuadro de diálogo **Create Session Policy**, junto a **Named Expressions**, seleccione **General**, seleccione el valor True, haga clic en **Add Expression**, haga clic en **Create** y, a continuación, haga clic en **Close**.

## Crear y aplicar enlaces web

Puede configurar la Interfaz de acceso para mostrar un conjunto de enlaces a recursos internos que están disponibles para los usuarios. La creación de estos enlaces requiere que primero los defina como recursos. Luego, los vincula a un usuario, grupo, servidor virtual o globalmente para activarlos en la Interfaz de acceso. Los enlaces que cree aparecerán en los paneles de **Sitios web** en **Sitios web empresariales**.

**IMPORTANTE:**

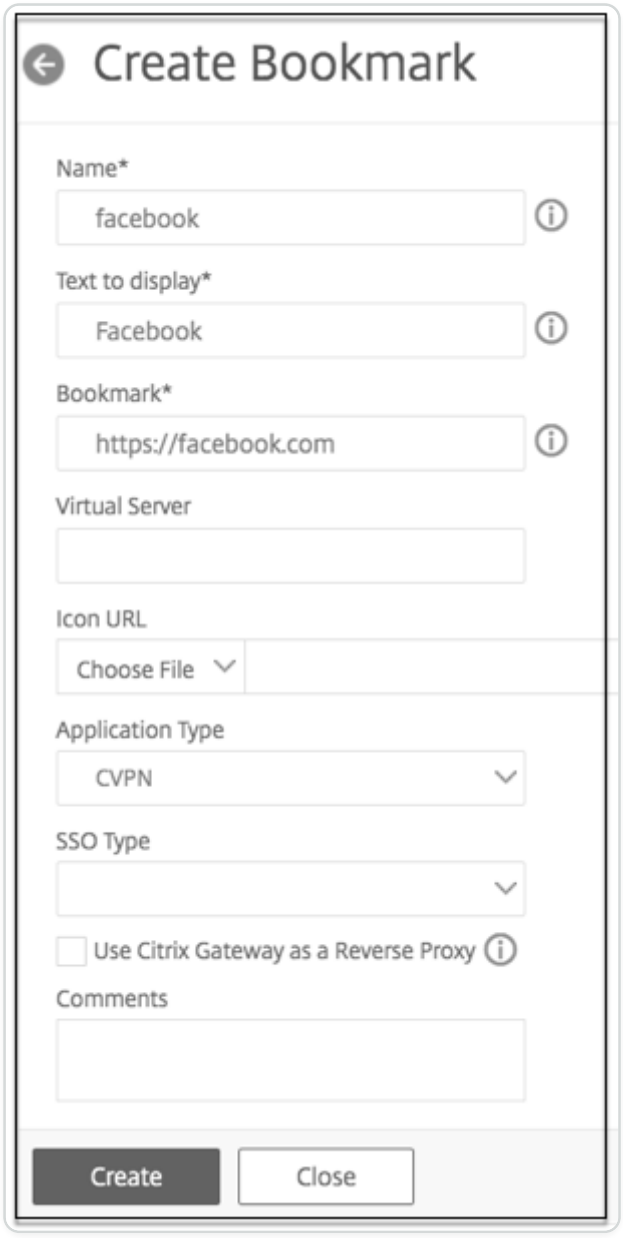
A partir de la versión 13.0 compilación 64.xx de NetScaler, no se admiten los recursos compartidos de archivos a través de NetScaler Gateway.

### Creación de marcadores empresariales

#### Para crear un enlace de Interfaz de acceso en una directiva de sesión

1. En la utilidad de configuración, en la ficha **Configuración**, en el panel de navegación, expanda **NetScaler Gateway > Recursos** y, a continuación, haga clic en **Marcadores de portal**.
2. En el panel de detalles, haga clic en **Agregar**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.




3. En **Nombre**, escriba un nombre para el marcador.
4. En **Texto a mostrar**, escriba la descripción del enlace. La descripción aparece en la **Interfaz de acceso**.
5. En **Marcador**, escriba la dirección web de la aplicación.
6. En **Servidor virtual**, escriba el nombre del servidor virtual de equilibrio de carga/conmutación de contenido asociado. Este campo es opcional.
7. En **URL del icono**, los iconos cargados son compatibles con todos los temas, excepto el tema predeterminado. El tamaño máximo recomendado es de 70x70 píxeles. Recomendamos utilizar imágenes transparentes. Este campo es opcional.
8. En **Tipo de aplicación**, seleccione el tipo de aplicación (VPN, VPN sin cliente o SaaS) que representa la URL. Este campo es opcional.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

9. En **Tipo de SSO**, seleccione el tipo de SSO que desea configurar para el marcador. Cuando el SSO está configurado, los usuarios pueden acceder a las aplicaciones sin tener que introducir sus credenciales en los inicios de sesión posteriores. Se admiten los siguientes tipos de SSO:

    - Unified Gateway: Esta configuración de SSO permite el acceso remoto seguro a múltiples recursos de una aplicación a través de una única URL.
    - Autoautenticación: En esta configuración de SSO, se solicita a los usuarios de NetScaler Gateway que proporcionen las credenciales de inicio de sesión para acceder a la aplicación.
    - Autenticación basada en SAML: En esta configuración de SSO, NetScaler Gateway utiliza un IdP para validar los detalles del usuario, genera una aserción SAML y la envía al SP. Si la validación es correcta, el SSO se realiza correctamente.

    **NOTA:**

    Si habilita el acceso sin cliente, puede asegurarse de que las solicitudes a los sitios web pasen por NetScaler Gateway. Por ejemplo, ha añadido un marcador para Google. Seleccione la casilla de verificación **Usar NetScaler Gateway como proxy inverso**. Cuando selecciona esta casilla de verificación, las solicitudes del sitio web van desde el dispositivo del usuario a NetScaler Gateway y luego al sitio web. Cuando desactiva la casilla de verificación, las solicitudes van desde el dispositivo del usuario al sitio web. Esta casilla de verificación solo está disponible si habilita el acceso sin cliente.

10. Haga clic en **Crear** y, a continuación, haga clic en **Cerrar.**

**Para vincular un enlace de interfaz de acceso**

Puede vincular enlaces de interfaz de acceso a las siguientes ubicaciones:

- Usuarios
- Grupos
- Servidores virtuales

Después de guardar la configuración, los enlaces están disponibles para los usuarios en la interfaz de acceso en la ficha **Inicio**, que es la primera página que ven los usuarios después de iniciar sesión correctamente.

1. En la utilidad de configuración, en el panel de navegación, realice una de las siguientes acciones:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Expanda **Administración de usuarios de NetScaler Gateway** y, a continuación, haga clic en **Usuarios AAA.**
- Expanda **NetScaler Gateway User Administration** y, a continuación, haga clic en **AAA Groups.**
- Expanda **NetScaler Gateway** y, a continuación, haga clic en **Virtual Servers.**

2. En el panel de detalles, realice una de las siguientes acciones:
   - Seleccione un usuario y, a continuación, haga clic en Abrir.
   - Seleccione un grupo y, a continuación, haga clic en Abrir.
   - Seleccione un servidor virtual y, a continuación, haga clic en Abrir.
3. En el cuadro de diálogo, haga clic en la ficha **Bookmarks**.
4. En **Available Bookmarks**, seleccione uno o varios marcadores, haga clic en la flecha derecha para mover los marcadores a Configured Bookmarks y, a continuación, en **OK.**

**Para enlazar marcadores globalmente mediante la GUI**

1. En la ficha **Configuration**, en el panel de navegación, expanda **NetScaler Gateway** y, a continuación, haga clic en **Global Settings.**
2. En el panel de detalles, en **Bookmarks**, haga clic en **Crear enlaces a las aplicaciones HTTP y de uso compartido de archivos de Windows que desea que sean accesibles en la página del portal de NetScaler Gateway**.




3. En el cuadro de diálogo **Configure VPN Global Binding***, haga clic en **Add.**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. En **Available**, seleccione uno o varios marcadores, haga clic en la flecha derecha para mover los marcadores a Configured y, a continuación, en **OK**.

**Para agregar un marcador empresarial mediante la CLI**

En el símbolo del sistema, escriba:

```
add vpn url <urlName> <linkName> <actualURL>  [-ssotype <ssotype>]
```

**Ejemplo:**

Marcador web

```
add vpn url google google "https://www.google.com"
```

**Para vincular un marcador de empresa mediante la CLI**

Puede vincular marcadores de empresa a nivel de usuario, grupo, servidor virtual y global.

```
bind aaa user <userName> -urlName <string>

bind aaa group <groupName> -urlName <string>

bind vpn vserver <vserverName> -urlName <string>

bind vpn global –urlName <string>
```

**Ejemplo:**

```
bind vpn global -urlName google
```

### Creación de marcadores personales

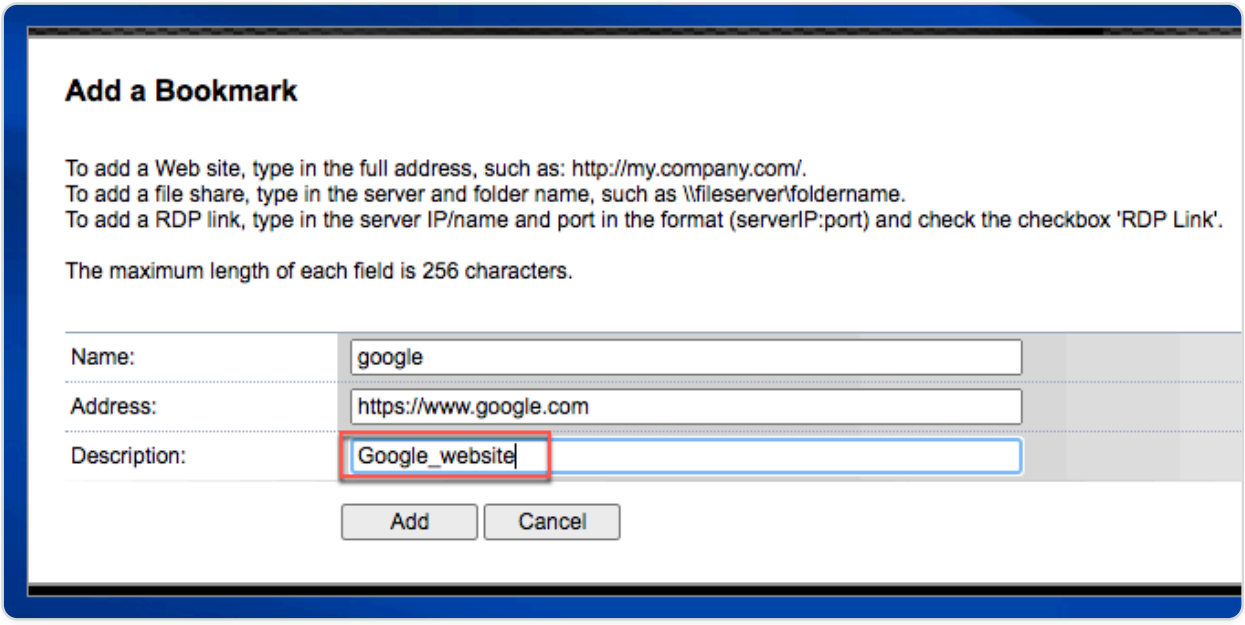
Puede crear sitios web personales solo desde el servidor virtual VPN. No hay una GUI de administración de NetScaler Gateway para agregar marcadores personales.

1. Inicie sesión en un servidor virtual VPN.
2. Haga clic en **Acceso a la red** o **Acceso sin cliente** para agregar un marcador.
3. Haga clic en **Agregar**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.




4. Introduzca los detalles del marcador, como el nombre del sitio web, la dirección y la descripción.




5. Haga clic en **Agregar**.

Los sitios web que ha añadido aparecen bajo las pestañas respectivas.

© 1997–2026 Citrix Systems, Inc. All rights reserved.




### Configurar tokens de nombre de usuario en marcadores

Puede configurar URL de marcadores y de recursos compartidos de archivos utilizando un token especial, %`username`%. Cuando los usuarios inician sesión, el token se reemplaza con el nombre de inicio de sesión de cada usuario. Por ejemplo, crea un marcador para un empleado llamado Jack para una carpeta como \\\\EmployeeServer\\%`username`%\\. Cuando Jack inicia sesión, la URL del recurso compartido de archivos se asigna a \\\\EmployeeServer\\Jack\\. Cuando configure tokens de nombre de usuario en marcadores, tenga en cuenta las siguientes situaciones:

- Si utiliza un tipo de autenticación, el nombre de usuario reemplaza el token %`username`%.
- Si utiliza la autenticación de dos factores, el nombre de usuario del tipo de autenticación principal se utiliza para reemplazar el token %`username`%.
- Si utiliza la autenticación de certificado de cliente, el campo de nombre de usuario del perfil de autenticación de certificado de cliente se utiliza para reemplazar el token %`username`%.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

# Configurar SmartAccess

Puede usar SmartAccess con Citrix Virtual Apps and Desktops para entregar de forma inteligente aplicaciones publicadas y escritorios virtuales a los usuarios.

SmartAccess le permite controlar el acceso a las aplicaciones y escritorios publicados en un servidor mediante las directivas de sesión de NetScaler Gateway. Utiliza comprobaciones de autenticación previa y posterior como condición, junto con otras condiciones, para el acceso a los recursos publicados. Otras condiciones incluyen cualquier cosa que pueda controlar con una directiva de Citrix Virtual Apps and Desktops, como límites de ancho de banda de la impresora, asignación de unidades de dispositivos de usuario, portapapeles, audio y asignación de impresoras. Puede aplicar una directiva de Citrix Virtual Apps and Desktops en función de si los usuarios superan una comprobación de NetScaler Gateway.

NetScaler Gateway puede entregar Citrix Virtual Desktops mediante las mismas opciones disponibles con StoreFront, acceso ICA Proxy, acceso sin cliente y acceso a NetScaler Gateway.

Esta funcionalidad se logra integrando los componentes de NetScaler Gateway con StoreFront y Citrix Virtual Apps and Desktops. Esta integración proporciona autenticación avanzada y una opción de control de acceso a StoreFront. Para obtener más información, consulte la documentación de StoreFront en el nodo Technologies de la documentación del producto NetScaler.

La conectividad remota a una granja de servidores no requiere el cliente de Citrix Secure Access. Los usuarios pueden conectarse con la aplicación Citrix Workspace. Los usuarios pueden usar el cliente de Citrix Secure Access para iniciar sesión y recibir sus aplicaciones publicadas y escritorios virtuales a través de la interfaz de acceso, que es la página de inicio predeterminada de NetScaler Gateway.

# Directivas de tráfico

Las directivas de tráfico le permiten configurar los siguientes ajustes para las conexiones de usuario:

- Aplicar tiempos de espera más cortos para aplicaciones confidenciales a las que se accede desde redes que no son de confianza.
- Cambiar el tráfico de red para usar TCP en algunas aplicaciones. Si selecciona TCP, debe habilitar o deshabilitar el inicio de sesión único para determinadas aplicaciones.
- Identificar situaciones en las que desea usar otras funciones HTTP para el tráfico de clientes de Citrix Secure Access™.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Definir las extensiones de nombre de archivo que se utilizan con la asociación de tipos de archivo.

## Crear una directiva de tráfico

Para configurar una directiva de tráfico, cree un perfil y configure los siguientes parámetros:

- Protocolo (HTTP o TCP)
- Tiempo de espera de la aplicación
- Inicio de sesión único en aplicaciones web
- Inicio de sesión único de formulario
- Asociación de tipos de archivo
- Complemento de repetidor
- Cuentas de delegación restringida de Kerberos (KCD)

Después de crear la política de tráfico, puede vincularla a servidores virtuales, usuarios, grupos o globalmente.

Por ejemplo, tiene la aplicación web PeopleSoft Human Resources instalada en un servidor de la red interna. Puede crear una política de tráfico para esta aplicación que defina la dirección IP de destino, el puerto de destino y puede establecer la cantidad de tiempo que un usuario puede permanecer conectado a la aplicación, como 15 minutos.

Si desea configurar otras funciones, como la compresión HTTP para una aplicación, puede utilizar una política de tráfico para configurar los ajustes. Al crear la política, utilice el parámetro HTTP para la acción. En la expresión, cree la dirección de destino para el servidor que ejecuta la aplicación.

### Ejemplos de expresiones de políticas de tráfico

A continuación se muestran ejemplos de expresiones de políticas de tráfico:

- `add vpn trafficPolicy trafPol1 "HTTP.REQ.URL.CONTAINS(\"/Citrix/\") || HTTP.REQ.URL.CONTAINS(\"10.102.\")")" trafAct1`
- `add vpn trafficPolicy trafPol2 "HTTP.REQ.HOSTNAME.CONTAINS(\"portal-srv\") || HTTP.REQ.URL.CONTAINS(\"homePage\"))" trafAct2`
- `add vpn trafficPolicy trafPol3 true trafAct3`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

### Configurar una política de tráfico mediante la GUI

1. Expanda **NetScaler Gateway > Directivas** y, a continuación, haga clic en **Tráfico**.
2. En el panel de detalles, en la ficha **Directivas**, haga clic en **Agregar**.
3. En el cuadro de diálogo **Crear política de tráfico**, en **Nombre**, escriba un nombre para la política.
4. Junto a **Perfil de solicitud**, haga clic en **Nuevo**.
5. En **Nombre**, escriba un nombre para el perfil.
6. En **Protocolo**, seleccione **HTTP** o **TCP**.

   **Nota:** Si selecciona TCP como protocolo, no puede configurar el inicio de sesión único y la configuración se deshabilita en el cuadro de diálogo del perfil.
7. En **Tiempo de espera de la aplicación (minutos)**, escriba el número de minutos. Esta configuración limita el tiempo que los usuarios pueden permanecer conectados a la aplicación web.
8. Para habilitar el inicio de sesión único en la aplicación web, en **Inicio de sesión único**, seleccione **ACTIVADO**.

   Nota: Si quiere usar el inicio de sesión único basado en formularios, puede configurar los ajustes dentro del perfil de tráfico. Para obtener más información, consulte Configuración del inicio de sesión único basado en formularios.
9. Para especificar una asociación de tipo de archivo, en **Asociación de tipo de archivo**, seleccione **ACTIVADO**.
10. Para usar el complemento repetidor para optimizar el tráfico de red, en Citrix SD-WAN™, seleccione **ACTIVADO**, haga clic en **Crear** y, a continuación, haga clic en **Cerrar**.
11. Si configura KCD en el dispositivo, en Cuenta KCD, seleccione la cuenta.

    Para obtener más información sobre cómo configurar KCD en el dispositivo, consulte Cómo configurar NetScaler Gateway para la delegación restringida de Kerberos.
12. En el cuadro de diálogo Crear directiva de tráfico, cree o agregue una expresión, haga clic en **Crear** y, a continuación, haga clic en **Cerrar**.

## Configurar el inicio de sesión único basado en formularios

El inicio de sesión único basado en formularios permite a los usuarios iniciar sesión una sola vez en todas las aplicaciones protegidas de su red. Cuando se configura el inicio de sesión único basado en formularios en NetScaler Gateway, los usuarios pueden acceder a aplicaciones web

© 1997–2026 Citrix Systems, Inc. All rights reserved.

que requieren un inicio de sesión basado en formularios HTML sin tener que volver a escribir su contraseña. Sin el inicio de sesión único, los usuarios deben iniciar sesión por separado para acceder a cada aplicación.

Después de crear el perfil de inicio de sesión único de formulario, debe crear un perfil y una directiva de tráfico que incluyan el perfil de inicio de sesión único de formulario. Para obtener más información, consulte Creación de una directiva de tráfico.

### Configurar el inicio de sesión único basado en formularios

1. Expanda **NetScaler Gateway > Directivas** y, a continuación, haga clic en **Tráfico**.
2. En el panel de detalles, haga clic en la ficha **Perfiles SSO de formulario** y, a continuación, haga clic en **Agregar**.
3. En **Nombre**, escriba un nombre para el perfil.
4. En **URL de acción**, escriba la URL a la que se envía el formulario completado.

   **Nota:** La URL es la URL relativa a la raíz.
5. En **Nombre de usuario**, escriba el nombre del atributo para el campo de nombre de usuario.
6. En **Contraseña**, escriba el nombre del atributo para el campo de contraseña.
7. En **Regla de éxito de SSO**, cree una expresión que describa la acción que realiza este perfil cuando es invocado por una directiva. También puede crear la expresión utilizando los botones Prefijo, Añadir y Operador debajo de este campo.

   Esta regla comprueba si el inicio de sesión único se ha realizado correctamente o no.
8. En **Par nombre-valor**, escriba el valor del campo de nombre de usuario, seguido de un ampersand (&), y luego el valor del campo de contraseña.

   Los nombres de los valores se separan con un ampersand (&), como nombre1=valor1&nombre2=valor2.
9. En **Tamaño de respuesta**, escriba el número de bytes que se permiten para el tamaño completo de la respuesta. Escriba el número de bytes en la respuesta que se analizarán para extraer los formularios.
10. En **Extracción**, seleccione si el par nombre/valor es estático o dinámico. La configuración predeterminada es Dinámica.
11. En **Método de envío**, seleccione el método HTTP utilizado por el formulario de inicio de sesión único para enviar las credenciales de inicio de sesión al servidor de inicio de sesión. El valor predeterminado es Get.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

12. Haga clic en **Crear** y, a continuación, haga clic en **Cerrar**.

## Configurar el inicio de sesión único de SAML

Puede crear un perfil SAML 1.1 o SAML 2.0 para el inicio de sesión único (SSO). Los usuarios pueden conectarse a aplicaciones web que admiten el protocolo SAML para el inicio de sesión único. NetScaler Gateway admite el inicio de sesión único del proveedor de identidades (IdP) para aplicaciones web SAML.

### Configurar el inicio de sesión único de SAML

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda **NetScaler Gateway \ > Directivas** y, a continuación, haga clic en Tráfico.
2. En el panel de detalles, haga clic en la ficha Perfil de SSO de SAML.
3. En el panel de detalles, haga clic en Agregar.
4. En Nombre, escriba un nombre para el perfil.
5. En Nombre del certificado de firma, introduzca el nombre del certificado X.509.
6. En URL de ACS, introduzca el servicio de consumidor de aserciones del proveedor de identidades o del proveedor de servicios. La AssertionConsumerServiceURL (URL de ACS) proporciona la capacidad de SSO para los usuarios.
7. En Regla de estado de retransmisión, cree la expresión para la directiva a partir de Expresiones de directiva guardadas y Expresiones de uso frecuente. Seleccione de la lista Operador para definir cómo se evalúa la expresión. Para probar la expresión, haga clic en Evaluar.
8. En Enviar contraseña, seleccione ACTIVADO o DESACTIVADO.
9. En Nombre del emisor, introduzca la identidad de la aplicación SAML.
10. Haga clic en Crear y, a continuación, en Cerrar.

## Enlazar una directiva de tráfico

Puede enlazar directivas de tráfico a servidores virtuales, grupos, usuarios y a NetScaler Gateway Global. Puede utilizar la utilidad de configuración para enlazar una directiva de tráfico.

### Enlazar una directiva de tráfico globalmente mediante la GUI

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda **NetScaler Gateway > Directivas** y, a continuación, haga clic en Tráfico.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. En el panel de detalles, seleccione una directiva y, a continuación, en Acción, haga clic en Enlaces globales.
3. En el cuadro de diálogo Enlazar/Desenlazar directivas de tráfico, en Detalles, haga clic en Insertar directiva.
4. En Nombre de la directiva, seleccione la directiva y, a continuación, haga clic en Aceptar.

## Eliminar directivas de tráfico

Puede utilizar la utilidad de configuración para eliminar directivas de tráfico de NetScaler Gateway. Si utiliza la utilidad de configuración para eliminar una directiva de tráfico y la directiva está enlazada al nivel de usuario, grupo o servidor virtual, primero debe desenlazar la directiva. A continuación, puede eliminar la directiva.

### Desenlazar una directiva de tráfico mediante la GUI

1. Expanda **NetScaler Gateway,** y, a continuación, haga clic en **Servidores virtuales**.
   - **Expanda NetScaler Gateway > Administración de usuarios** y, a continuación, haga clic en **Grupos AAA**.
   - Expanda **NetScaler Gateway > Administración de usuarios** y, a continuación, haga clic en **Usuarios AAA**.
2. En el panel de detalles, seleccione un servidor virtual, grupo o usuario y, a continuación, haga clic en **Abrir**.
3. En el cuadro de diálogo **Configurar servidor virtual de NetScaler Gateway, Configurar grupo AAA** o **Configurar usuario AAA**, haga clic en la ficha **Directivas**.
4. Haga clic en **Tráfico**, seleccione la directiva y, a continuación, haga clic en **Desenlazar directiva**.
5. Haga clic en **Aceptar,** y, a continuación, haga clic en **Cerrar**.

Una vez desenlazada la directiva de tráfico, puede eliminar la directiva.

### Eliminar una directiva de tráfico mediante la GUI

1. Expanda **NetScaler Gateway > Directivas** y, a continuación, haga clic en **Tráfico**.
2. En el panel de detalles, en la ficha Directivas, seleccione la directiva de tráfico y, a continuación, haga clic en **Quitar**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

# Directivas de sesión

Una directiva de sesión es una colección de expresiones y configuraciones que se aplican a usuarios, grupos, servidores virtuales y globalmente.

Utilice una directiva de sesión para configurar los ajustes de las conexiones de usuario. Puede definir ajustes para configurar el software con el que inician sesión los usuarios, como el cliente Citrix Secure Access para Windows o el cliente Citrix Secure Access para Mac. También puede configurar ajustes para exigir a los usuarios que inicien sesión con la aplicación Citrix Workspace o Secure Hub. Las directivas de sesión se evalúan y aplican después de que el usuario se autentique.

Las directivas de sesión se aplican según las siguientes reglas:

- Las directivas de sesión siempre anulan la configuración global.
- Cualquier atributo o parámetro que no se establezca mediante una directiva de sesión se establece en las directivas establecidas para el servidor virtual.
- Cualquier otro atributo que no esté establecido por una directiva de sesión o por el servidor virtual se establece mediante la configuración global.

**IMPORTANTE:**

Las siguientes instrucciones son pautas generales para crear directivas de sesión. Hay instrucciones específicas para configurar directivas de sesión para diferentes configuraciones, como el acceso sin cliente o el acceso a aplicaciones publicadas. Las instrucciones pueden contener indicaciones para configurar un ajuste específico. Sin embargo, ese ajuste puede ser uno de muchos ajustes que se encuentran dentro de un perfil y una directiva de sesión. Las instrucciones le indican que cree un ajuste dentro de un perfil de sesión y luego aplique el perfil a una directiva de sesión. Puede cambiar los ajustes dentro de un perfil y una directiva sin crear una directiva de sesión. Además, puede crear todos sus ajustes a nivel global y luego crear una directiva de sesión para anular los ajustes globales.

Si implementa Citrix Endpoint Management o StoreFront en su red, Citrix recomienda utilizar el asistente de configuración rápida para configurar directivas y perfiles de sesión. Al ejecutar el asistente, define la configuración para su implementación. NetScaler Gateway crea entonces las directivas de autenticación, sesión y acceso sin cliente necesarias.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

## Crear una directiva de sesión

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda NetScaler Gateway > Directivas y, a continuación, haga clic en Sesión.
2. En el panel de detalles, en la ficha Directivas, haga clic en Agregar.
3. En Nombre, escriba un nombre para la directiva.
4. Junto a Request Profile, haga clic en Nuevo.
5. En Nombre, escriba un nombre para el perfil.
6. Complete la configuración del perfil de sesión y, a continuación, haga clic en Crear.
7. En el cuadro de diálogo Crear perfil de sesión, agregue una expresión para la directiva, haga clic en Crear y, a continuación, haga clic en Cerrar. Nota: En la expresión, seleccione Valor verdadero para que la directiva se aplique siempre al nivel al que está vinculada.

### Ejemplos de expresiones de directivas de sesión

A continuación, se muestran ejemplos de expresiones de directivas de sesión:

- `add vpn sessionPolicy sessPol1 "HTTP.REQ.HEADER(\"User-Agent\").CONTAINS(\"CitrixReceiver\") || HTTP.REQ.HEADER(\"User-Agent\").CONTAINS(\"CitrixWorkspace\")" sessAct1`
- `add vpn sessionPolicy sessPol2 "HTTP.REQ.HEADER(\"User-Agent\").CONTAINS(\"CitrixReceiver\").NOT" sessAct2`
- `add vpn sessionPolicy sessPol3 true sessAct3`

## Vincular directivas de sesión

Después de crear una directiva de sesión, vincúlela a un usuario, grupo, servidor virtual o globalmente. Las directivas de sesión se aplican como una jerarquía en el siguiente orden:

- Usuarios
- Grupos
- Servidores virtuales
- Globalmente

### Vincular una directiva de sesión a un servidor virtual mediante la GUI

1. Vaya a **NetScaler Gateway > Virtual Servers**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Seleccione un servidor virtual y haga clic en **Edit**. También puede crear un nuevo servidor virtual.
3. Desplácese hasta la sección **Policies** y haga clic en el icono **+**.
4. En **Choose Policy**, seleccione **Session**.
5. En **Choose Type**, seleccione **Request** y haga clic en **Continue**.
6. En **Select Policy**, seleccione la directiva que quiere enlazar a este servidor virtual.
7. En **Priority**, introduzca el número de prioridad de la directiva.
8. Haga clic en **Bind**.

### Enlazar una directiva de sesión a un grupo de autenticación, autorización y auditoría mediante la GUI

1. Vaya a **NetScaler Gateway > User Administration > AAA Groups**.
2. Seleccione un grupo de autenticación, autorización y auditoría existente y haga clic en **Edit**. También puede crear un grupo de autenticación, autorización y auditoría.
3. En **Advanced Settings**, haga clic en **Policies** y, a continuación, haga clic en el icono **+**.
4. En **Choose Policy**, seleccione **Session** y haga clic en **Continue**.
5. En **Select Policy**, seleccione la directiva que quiere enlazar a este grupo de autenticación, autorización y auditoría.
6. En **Priority**, introduzca el número de prioridad de la directiva.
7. Haga clic en **Enlazar**.

### Enlazar una directiva de sesión a un usuario de autenticación, autorización y auditoría mediante la GUI

1. Vaya a **NetScaler Gateway > User Administration > AAA Users**.
2. Seleccione un usuario de NetScaler existente y haga clic en **Editar**. También puede crear un usuario de autenticación, autorización y auditoría.
3. En **Configuración avanzada**, haga clic en **Directivas** y, a continuación, haga clic en el icono **+**.
4. En **Elegir directiva**, seleccione **Sesión** y haga clic en **Continuar**.
5. En **Seleccionar directiva**, seleccione la directiva que desea enlazar a este usuario de autenticación, autorización y auditoría.
6. En **Prioridad**, introduzca el número de prioridad de la directiva.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

7. Haga clic en **Enlazar**.

**Nota**: Para obtener más información sobre la prioridad, consulte `<https://support.citrix.com/article/CTX214588>`.

## Crear un perfil de sesión

Un perfil de sesión contiene la configuración para las conexiones de usuario.

Los perfiles de sesión especifican las acciones que se aplican a una sesión de usuario si el dispositivo de usuario cumple las condiciones de la expresión de directiva. Los perfiles se utilizan con las directivas de sesión. Puede utilizar la utilidad de configuración para crear perfiles de sesión por separado de una directiva de sesión y, a continuación, utilizar el perfil para varias directivas. Solo puede utilizar un perfil con una directiva.

### Configurar la configuración de red para las conexiones de usuario en un perfil de sesión

Puede utilizar la ficha **Configuración de red** en el perfil de sesión para configurar la siguiente configuración de red para las conexiones de usuario:

- Servidor DNS
- Dirección IP del servidor WINS
- Dirección IP asignada que puede usar como dirección IP de intranet
- Configuración de desbordamiento para grupos de direcciones (direcciones IP de intranet)
- Sufijo DNS IP de intranet
- Puertos HTTP
- Configuración de tiempo de espera forzado

### Configurar los ajustes de conexión en un perfil de sesión

Puede usar la ficha **Experiencia del cliente** del perfil de sesión para configurar los siguientes ajustes de conexión:

- Interfaz de acceso o página de inicio personalizada
- Dirección web para correo electrónico basado en web, como Outlook Web Access
- tipo de complemento (cliente Citrix Secure Access™ para Windows o cliente Citrix Secure Access para macOS X)
- Tunelización dividida

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Configuración de tiempo de espera de sesión e inactividad
- Acceso sin cliente
- Codificación de URL de acceso sin cliente
- tipo de complemento (Windows o Mac)
- Inicio de sesión único en aplicaciones web
- Índice de credenciales para la autenticación
- Inicio de sesión único con Windows
- Comportamiento de limpieza del cliente
- Scripts de inicio de sesión
- Configuración de depuración del cliente
- DNS dividido
- Acceso a direcciones IP de red privada y acceso a LAN local
- Opciones del cliente
- Configuración del proxy

Para obtener más información sobre la configuración de las conexiones de usuario, consulte Configuración de conexiones para el cliente Citrix Secure Access.

### Configurar la configuración de seguridad en un perfil de sesión

Puede utilizar la ficha **Seguridad** de un perfil de sesión para configurar los siguientes ajustes de seguridad:

- Acción de autorización predeterminada (permitir o denegar)
- Navegación segura para conexiones desde dispositivos iOS
- Grupos de cuarentena
- Grupos de autorización

Para obtener más información sobre cómo configurar la autorización en NetScaler Gateway, consulte Configuración de la autorización.

### Configurar los ajustes de Citrix Virtual Apps and Desktops en un perfil de sesión

Puede usar la ficha **Aplicaciones publicadas** en un perfil de sesión para configurar los siguientes ajustes para las conexiones a servidores que ejecutan Citrix Virtual Apps and Desktops:

- Proxy ICA, que son conexiones de cliente que utilizan la aplicación Citrix Workspace

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Dirección de Web Interface
- Modo de portal de Web Interface
- Inicio de sesión único en el dominio de la granja de servidores
- Página de inicio de la aplicación Citrix Workspace
- Dirección de servicios de cuenta

Para obtener más información sobre cómo configurar los ajustes para conectarse a aplicaciones publicadas en una granja de servidores, consulte Integrar NetScaler Gateway con Citrix Virtual Apps and Desktops.

Puede crear perfiles de sesión independientemente de una directiva de sesión. Al crear la directiva, puede seleccionar el perfil que desea adjuntar a la directiva.

**Para crear un perfil de sesión mediante la GUI**

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda **NetScaler Gateway > Directivas** y, a continuación, haga clic en **Sesión**.
2. En el panel de detalles, haga clic en la ficha **Perfiles** y, a continuación, haga clic en **Agregar**.
3. Configure los parámetros del perfil, haga clic en **Crear** y, a continuación, haga clic en **Cerrar**.

Después de crear un perfil, puede incluirlo en una directiva de sesión.

**Para agregar un perfil a una directiva de sesión mediante la GUI**

1. En la utilidad de configuración, en el panel de navegación, expanda **Access Gateway > Directivas** y, a continuación, haga clic en **Sesión**.
2. En la ficha **Directivas**, realice una de las siguientes acciones:
   - Haga clic en **Agregar** para crear una directiva de sesión.
   - Seleccione una directiva y, a continuación, haga clic en **Abrir**.
3. En **Perfil de solicitud**, seleccione un perfil de la lista.
4. Termine de configurar la directiva de sesión y, a continuación, realice una de las siguientes acciones:
   a. Haga clic en **Crear** y, a continuación, haga clic en **Cerrar** para crear la directiva.
   b. Haga clic en **Aceptar** y, a continuación, haga clic en **Cerrar** para modificar la directiva.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

# Soporte de políticas avanzadas para marcadores empresariales

Los marcadores empresariales (URL VPN) se pueden configurar como políticas avanzadas.

**NOTAS:**

- NetScaler Gateway admite los protocolos HTTP, HTTPS y RDP para los marcadores empresariales.
- NetScaler Gateway solo admite URL absolutas para los marcadores empresariales.

## Configurar la URL VPN como una política avanzada

### En la GUI

1. Crear un perfil de URL VPN.
    - Vaya a **Configuración > NetScaler Gateway > Políticas > URL VPN**.
    - En la página **Políticas y perfiles de URL VPN**, seleccione la ficha **Perfiles de URL VPN** y haga clic en **Agregar**.
    - Actualice los campos obligatorios y haga clic en **Crear**.
        - Nombre: Un nombre para el perfil de URL VPN.
        - Texto a mostrar: Una breve descripción del enlace. La descripción aparece en la interfaz de acceso.
        - Marcador: Dirección web de la aplicación.
        - Servidor virtual: Nombre del servidor virtual de equilibrio de carga o de conmutación de contenido asociado que está configurado. Este campo es opcional.
        - URL del icono: Los iconos cargados en este campo son compatibles con todos los temas, excepto con el tema predeterminado. El tamaño máximo recomendado es de 70x70 píxeles. Le recomendamos que utilice imágenes transparentes. Este campo es opcional.
        - Tipo de aplicación: seleccione el tipo de aplicación (VPN, VPN sin cliente o SaaS) que representa la URL. Este campo es opcional.

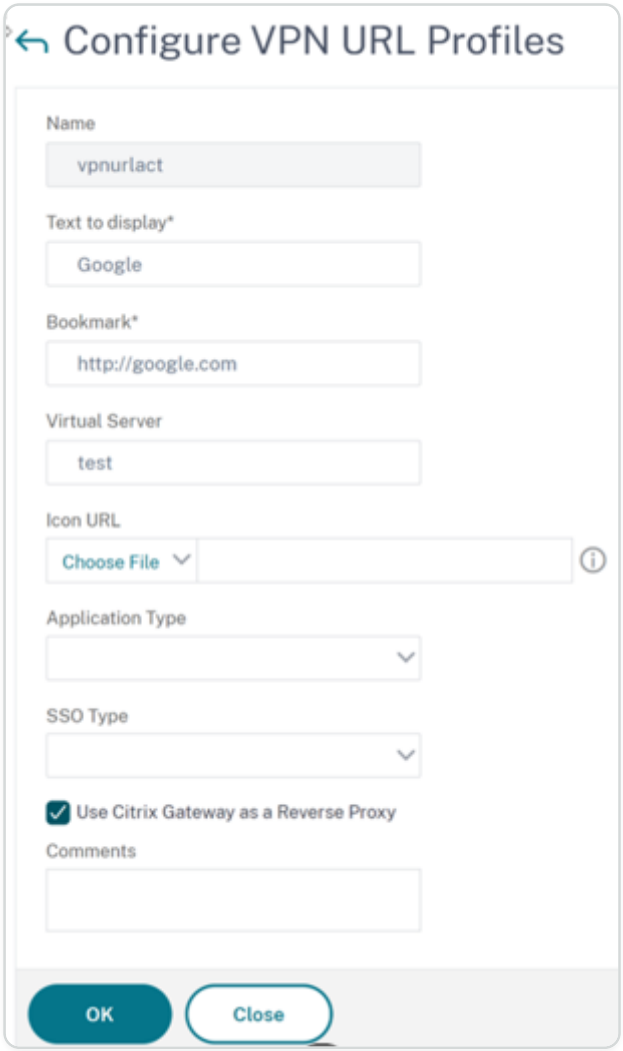
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Tipo de SSO: Tipo de SSO que desea configurar para el marcador. Cuando el SSO está configurado, los usuarios pueden acceder a las aplicaciones sin tener que introducir sus credenciales en los inicios de sesión posteriores. Se admiten los siguientes tipos de SSO:
  - Gateway unificado: Esta configuración de SSO permite un acceso remoto seguro a múltiples recursos de una aplicación a través de una única URL.
  - Autoautenticación: En esta configuración de SSO, se solicita a los usuarios de NetScaler Gateway que proporcionen las credenciales de inicio de sesión para acceder a la aplicación.
  - Autenticación basada en SAML: En esta configuración de SSO, NetScaler Gateway utiliza un IdP para validar los detalles del usuario, genera una aserción SAML y la envía al SP. Si la validación es correcta, el SSO se realiza correctamente.

**NOTA:**

Si habilita el acceso sin cliente, puede asegurarse de que las solicitudes a los sitios web pasen por NetScaler Gateway. Por ejemplo, ha agregado un marcador para Google. Seleccione la casilla de verificación Usar NetScaler Gateway como proxy inverso. Cuando selecciona esta casilla de verificación, las solicitudes del sitio web van desde el dispositivo del usuario a NetScaler Gateway y luego al sitio web. Cuando desactiva la casilla de verificación, las solicitudes van desde el dispositivo del usuario al sitio web. Esta casilla de verificación solo está disponible si habilita el acceso sin cliente.

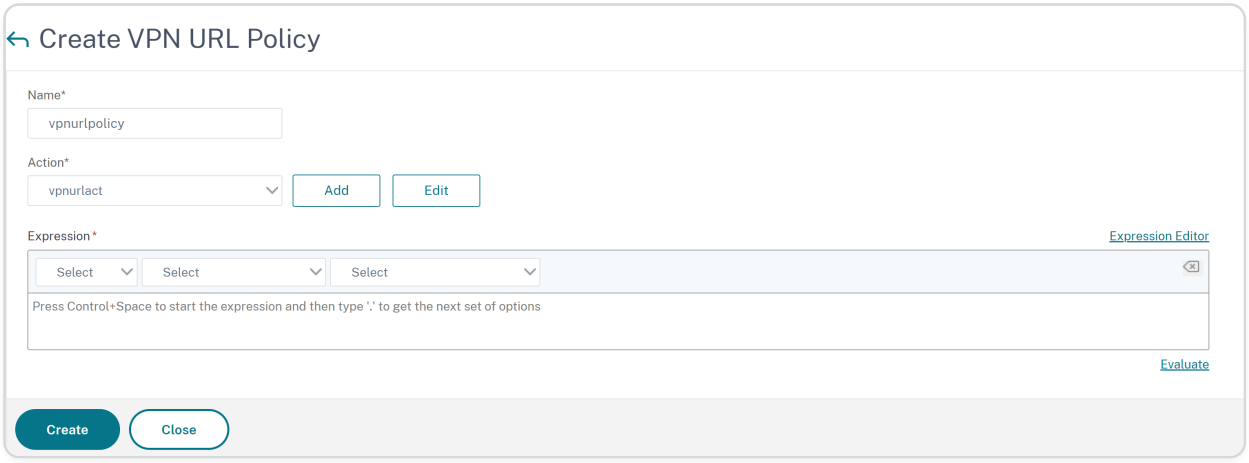
© 1997–2026 Citrix Systems, Inc. All rights reserved.




2. Crear una directiva de URL VPN.

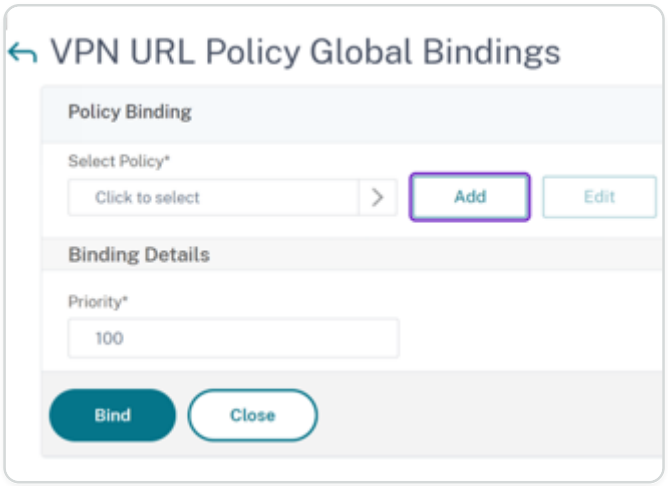
   - Vaya a **Configuration > NetScaler Gateway > Policies > VPN URL**.
   - En la página **VPN URL Policies and Profiles**, seleccione la ficha **VPN URL Policy** y haga clic en **Add**.
   - Actualice los campos obligatorios y haga clic en **Create**.
     - Nombre: Un nombre para la directiva de URL VPN.
     - Acción: Seleccione el perfil de URL VPN configurado. Si no hay ningún perfil en la lista desplegable, haga clic en Agregar y repita el paso 1.
     - Expresión: Consulte (/es-es/citrix-adc/current-release/appexpert/policies-and-expressions.html) para obtener información sobre las expresiones de directiva avanzadas.

© 1997–2026 Citrix Systems, Inc. All rights reserved.




3. Enlace la directiva de URL VPN a un punto de enlace.

   - Vaya a **Configuración > NetScaler Gateway > Directivas > URL VPN**.
   - En la página **Directivas y perfiles de URL VPN**, seleccione la ficha **Directiva de URL VPN**.
   - Seleccione **Enlaces globales** en la lista desplegable **Seleccionar acción**.
   - Seleccione la directiva de URL VPN. Si no hay ninguna directiva en la lista, haga clic en **Agregar** y repita el paso 2.
   - En la sección **Detalles de enlace**, asigne una prioridad a la directiva de URL VPN.




## En la CLI

### Crear una acción de URL VPN:

En el símbolo del sistema, escriba lo siguiente:

```
add vpn urlAction &lt;name> -linkName &lt;string> -actualURL &lt;string>
[-vServerName &lt;string>] [-clientlessAccess ( ON | OFF )] [-comment
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
&lt;string>] [-iconURL &lt;URL>] [-ssotype &lt;ssotype>] [-applicationtype
&lt;applicationtype>] [-samlSSOProfile &lt;string>]
```

NetScaler Gateway admite las siguientes operaciones para la acción de URL VPN:

- **agregar**

```
add vpn urlAction &lt;name> -linkName &lt;string> -actualURL
&lt;string> [-vServerName &lt;string>] [-clientlessAccess ( ON | OFF )]
[-comment &lt;string>] [-iconURL &lt;URL>] [-ssotype &lt;ssotype>] [-
applicationtype &lt;applicationtype>] [-samlSSOProfile &lt;string>]
```

- **establecer**

```
set vpn urlAction &lt;name> [-vServerName &lt;string>] [-
clientlessAccess ( ON | OFF )] [-comment &lt;string>] [-iconURL
&lt;URL>] [-ssotype &lt;ssotype>] [-applicationtype
&lt;applicationtype>] [-samlSSOProfile &lt;string>]
```

- **anular**

```
unset vpn urlAction &lt;name> [-vServerName] [-clientlessAccess] [-
comment] [-iconURL] [-ssotype] [-applicationtype] [-samlSSOProfile]
```

**NOTA:**

Si establece el acceso sin cliente en ON, puede asegurarse de que las solicitudes a los sitios web vayan desde el dispositivo del usuario a NetScaler Gateway y luego al sitio web.

- **mostrar**

```
show vpn urlAction [&lt;name>]
```

- **eliminar**

```
remove vpn urlAction &lt;name>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **renombrar**

```
rename vpn urlAction &lt;name>@ &lt;newName>@
```

**Crear una política de URL VPN:**

NetScaler Gateway admite las siguientes operaciones para la política de URL VPN:

- **añadir**

```
add vpn urlPolicy &lt;name> -rule &lt;expression> -action &lt;string>
[-comment &lt;string>] [-logAction &lt;string>]
```

- **establecer**

```
set vpn urlPolicy &lt;name> [-rule &lt;expression>] [-action
&lt;string>] [-comment &lt;string>] [-logAction &lt;string>]
```

- **anular**

```
unset vpn urlPolicy &lt;name> [-comment] [-logAction]
```

- **mostrar**

```
show vpn urlPolicy [&lt;name>]
```

- **eliminar**

```
remove vpn urlPolicy &lt;name>
```

- **renombrar**

```
rename vpn urlpolicy &lt;name>@ &lt;newName>@
```

- **estado**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
stat vpn urlpolicy [&lt;name>] [-detail] [-fullValues] [-ntimes
&lt;positive_integer>] [-logFile &lt;input_filename>] [-clearstats
( basic | full )]
```

**Vincular la directiva a un punto de enlace:**

NetScaler Gateway admite las siguientes operaciones para el enlace de directivas de URL VPN:

- **vincular**

```
bind vpn vserver &lt;vserver name> -policy &lt;string> -priority
&lt;positive_integer> [-gotoPriorityExpression &lt;expression>]

bind vpn global -policyName &lt;string> -priority &lt;positive_integer>
[-gotoPriorityExpression &lt;expression>]

bind aaa user &lt;userName> -policy &lt;string> [-priority
&lt;positive_integer>] [-type &lt;type>] [-gotoPriorityExpression
&lt;expression>]

bind aaa group &lt;groupName> -policy &lt;string> [-priority
&lt;positive_integer>] [-type &lt;type>] [-gotoPriorityExpression
&lt;expression>]
```

- **desvincular**

```
unbind vpn vserver &lt;name> -policy &lt;string>

unbind vpn global -policyName &lt;string>

unbind aaa user &lt;name> -policy &lt;string>

unbind aaa group &lt;name> -policy &lt;string>
```

**NOTA:**

Los puntos de enlace son `aaauser`, `aaagroup`, `vpnvserver` y `vpnglobal`.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

# Políticas de puntos finales

El Análisis de puntos finales (EPA) es un proceso que escanea el dispositivo de un usuario y detecta información, como la presencia y el nivel de versión de las actualizaciones del sistema operativo, el software antivirus, el firewall y el navegador web. El Análisis de puntos finales le permite determinar si el dispositivo de un usuario cumple con sus requisitos antes de que se conecte a su red. También se puede configurar para comprobar periódicamente si hay cambios mientras el usuario permanece conectado. Puede comprobar archivos, procesos y entradas del registro en el dispositivo del usuario durante la sesión del usuario para asegurarse de que el dispositivo sigue cumpliendo los requisitos.

**IMPORTANTE:**

- El Análisis de puntos finales está diseñado para analizar el dispositivo del usuario según criterios de cumplimiento predeterminados y no aplica ni valida la seguridad de los dispositivos de usuario final. Se recomienda utilizar sistemas de seguridad de puntos finales para proteger los dispositivos de ataques de administradores locales.
- El cliente EPA está disponible como cliente independiente y también se incluye con el cliente Citrix Secure Access™. El cliente Citrix® EPA y el cliente Citrix Secure Access son independientes entre sí.

## Cómo funcionan las políticas de puntos finales

Puede configurar NetScaler Gateway para comprobar si un dispositivo de usuario cumple ciertos requisitos antes de que un usuario inicie sesión. Esto se denomina política de preautenticación. Puede configurar NetScaler Gateway para comprobar en un dispositivo de usuario la presencia de antivirus, firewall, antispam, procesos, archivos, entradas del registro, seguridad de Internet o sistemas operativos que especifique en la política. Si el dispositivo del usuario no supera el análisis de preautenticación, los usuarios no podrán iniciar sesión.

Para verificar otros requisitos que no se utilizan en una política de preautenticación, puede configurar una política de sesión y vincularla a un usuario o grupo. Este tipo de política se denomina política de postautenticación, que se ejecuta durante la sesión del usuario para garantizar que los criterios requeridos, como el software antivirus o un proceso, sigan siendo conformes.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Cuando configura una política de preautenticación o postautenticación, NetScaler Gateway descarga el complemento de Análisis de puntos finales y luego ejecuta el análisis en el dispositivo de los usuarios. Cada vez que un usuario inicia sesión, el complemento de Análisis de puntos finales se ejecuta automáticamente.

Puede utilizar los tres tipos de políticas siguientes para configurar las políticas de puntos finales:

- Política de preautenticación que utiliza un parámetro Sí o No. El análisis determina si el dispositivo del usuario cumple los requisitos especificados. Si el análisis falla, el usuario no puede introducir credenciales en la página de inicio de sesión.
- Política de sesión que es condicional y se puede utilizar para SmartAccess.
- Expresión de comprobación del dispositivo cliente dentro de una política de sesión. Si el dispositivo del usuario no cumple los requisitos de la expresión de comprobación del dispositivo cliente, puede configurar que los usuarios se coloquen en un grupo de cuarentena. Si el dispositivo del usuario supera el análisis, los usuarios pueden colocarse en un grupo diferente que podría requerir otras comprobaciones.

Puede incorporar la información detectada en las políticas, lo que le permite conceder diferentes niveles de acceso en función del dispositivo del usuario. Por ejemplo, puede proporcionar acceso completo con permiso de descarga a los usuarios que se conectan de forma remota desde dispositivos de usuario que cumplen los requisitos actuales de software antivirus y firewall. Para los usuarios que se conectan desde dispositivos no conformes, puede proporcionar un nivel de acceso más restringido que les permita editar documentos en servidores remotos sin descargarlos. Todos los dispositivos que ejecutan EPA se consideran dispositivos no conformes.

El Análisis de puntos finales realiza los siguientes pasos básicos:

- Examina un conjunto inicial de información sobre el dispositivo del usuario para determinar qué análisis aplicar.
- Ejecuta todos los análisis aplicables. Cuando los usuarios intentan conectarse, el complemento Endpoint Analysis comprueba el dispositivo del usuario para ver si cumple los requisitos especificados en la directiva de autenticación previa o de sesión. Si el dispositivo del usuario supera el análisis, se permite a los usuarios iniciar sesión. Si el dispositivo del usuario no supera el análisis, no se permite a los usuarios iniciar sesión.

  **Nota:** Los análisis de Endpoint Analysis se completan antes de que la sesión del usuario utilice una licencia.
- Compara los valores de propiedad detectados en el dispositivo del usuario con los valores de propiedad deseados que aparecen en los análisis configurados.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Produce un resultado que verifica si se encuentran los valores de propiedad deseados.

**ATENCIÓN:**

Las instrucciones para crear directivas de Endpoint Analysis son pautas generales. Puede tener muchas configuraciones dentro de una directiva de sesión. Las instrucciones específicas para configurar directivas de sesión pueden contener indicaciones para configurar una configuración específica. Sin embargo, esa configuración puede ser una de las muchas configuraciones que se encuentran dentro de un perfil y una directiva de sesión.

### Ejemplos de expresiones EPA

A continuación, se muestran ejemplos de expresiones de algunos componentes de EPA, como la eliminación de procesos, la eliminación de archivos y el certificado de dispositivo:

- Windows:
  - Eliminar proceso: `sys.client_expr(\“proc_0_perl\“) -killProcess processToKill.exe`
  - Certificado de dispositivo: `sys.client_expr(“device-cert_0_0”)`
  - Eliminar archivos: `sys.client_expr(\“proc_0_perl\“) -deletefiles “C:/removefile.txt”`
- MAC
  - Eliminar proceso: `sys.client_expr(\“proc_0_perl\“) -killProcess processToKill.exe`
  - Certificado de dispositivo: `sys.client_expr(“device-cert_0_0”)`
  - Eliminar archivos: `sys.client_expr(\“proc_0_perl\“) -deletefiles “C:/removefile.txt”`

## Evaluar las opciones de inicio de sesión de usuario

Cuando los usuarios inician sesión, pueden optar por omitir el análisis de Endpoint Analysis. Si los usuarios omiten el análisis, NetScaler Gateway procesa esta acción como un error de Endpoint Analysis. Cuando los usuarios fallan el análisis, solo obtienen acceso a través del acceso sin cliente.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Por ejemplo, quiere proporcionar a los usuarios acceso mediante el cliente Citrix Secure Access. Para iniciar sesión en NetScaler Gateway con el plug-in, los usuarios deben tener una aplicación antivirus en ejecución, como Norton Antivirus. Si el dispositivo del usuario no ejecuta la aplicación, los usuarios pueden iniciar sesión solo con Receiver y usar las aplicaciones publicadas. También puede configurar el acceso sin cliente, que restringe el acceso a aplicaciones específicas, como Outlook Web Access.

Para configurar NetScaler Gateway para lograr este escenario de inicio de sesión, asigne una directiva de sesión restrictiva como directiva predeterminada. A continuación, configure los ajustes para actualizar a los usuarios a una directiva de sesión privilegiada cuando el dispositivo del usuario supere el análisis de Endpoint Analysis. En ese momento, los usuarios tienen acceso a la capa de red y pueden iniciar sesión con el cliente Citrix Secure Access.

**Para configurar NetScaler Gateway para aplicar primero la directiva de sesión restrictiva, realice los siguientes pasos:**

- Configure los ajustes globales con ICA® Proxy habilitado y todos los demás ajustes necesarios si la aplicación especificada no se está ejecutando en el dispositivo del usuario.
- Cree una directiva de sesión y un perfil que habiliten el cliente Citrix Secure Access.
- Cree una expresión dentro de la parte de la regla de la directiva de sesión para especificar la aplicación, como `(client.application.process(symantec.exe) exists)`

  Cuando los usuarios inician sesión, la directiva de sesión se aplica primero. Si Endpoint Analysis falla o el usuario omite el análisis, NetScaler Gateway ignora la configuración de la directiva de sesión (la expresión de la directiva de sesión se considera falsa). Como resultado, los usuarios tienen acceso restringido mediante el acceso sin cliente. Si Endpoint Analysis se supera, NetScaler Gateway aplica la directiva de sesión y los usuarios tienen acceso completo con el cliente Citrix Secure Access.

## Omitir el análisis de EPA

Puede omitir el análisis de EPA solo para la postautenticación y la autenticación avanzada. La omisión de EPA está disponible en los exploradores de todos los sistemas operativos compatibles. Los usuarios deben hacer clic en el botón **Omitir EPA** que aparece al acceder a la puerta de enlace. Si los usuarios omiten el análisis, NetScaler Gateway procesa esta acción como un error de Endpoint Analysis. Cuando los usuarios fallan el análisis, solo obtienen acceso a través del acceso sin cliente.

Consulte también `<https://support.citrix.com/article/CTX200748>`.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

## Análisis de Endpoint Analysis compatibles con Ubuntu

Los siguientes análisis de Endpoint Analysis (EPA) son compatibles con el complemento EPA instalado para el sistema operativo Ubuntu. Se incluye una expresión de ejemplo para configurar cada uno de los análisis junto con los análisis EPA. Puede configurar estas expresiones en las políticas de autenticación.

- **Archivo**
  - **Existencia**: sys.client_expr("file_0_/home/user/test.txt")
  - **Suma de comprobación MD5**: sys.client_expr("file_0_/home/user/test.txt_md5_ce780e271debcc29f551546e8db3368f")
  - **Texto dentro de un archivo (compatibilidad con expresiones regulares)**: sys.client_expr("file_0_/home/user/test.txt_search_cloud”)
- **Proceso**
  - **Existencia**: sys.client_expr("proc_0_perl")
  - **Suma de comprobación MD5**: sys.client_expr("proc_0_perl_md5_c060d3a5f97e27066cef8c116785567a")
  - **Ruta**: sys.client_expr("proc_0_perl_path_/usr/bin/perl")
- **Dispositivo del sistema de archivos o nombre del punto de montaje**: sys.client_expr("mountpoint_0_/sys”)

Si utiliza políticas avanzadas, las expresiones para cada análisis se pueden generar desde la GUI (**Security > AAA > Policies > Authentication > Advanced Policies > EPA**).

**NOTA:**

- En la página del Editor de expresiones, para el cliente Linux, puede seleccionar **Common** y, a continuación, seleccionar **Process, File** o **Mount Point**.
- El análisis EPA para direcciones MAC no es compatible con clientes Linux.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

# Directivas y perfiles de preautenticación

**IMPORTANTE:**

El análisis de puntos finales está diseñado para analizar el dispositivo del usuario según criterios de cumplimiento predeterminados y no aplica ni valida la seguridad de los dispositivos del usuario final. Se recomienda utilizar sistemas de seguridad de puntos finales para proteger los dispositivos de ataques de administradores locales.

Puede configurar NetScaler Gateway para que compruebe los dispositivos de un usuario antes de que se autentiquen en NetScaler Gateway. Esto se puede usar para restringir el acceso si el dispositivo del usuario no cumple con los requisitos de su organización. Las comprobaciones de dispositivos se pueden implementar mediante directivas individuales específicas de un servidor virtual o globalmente, como se describe en los dos procedimientos siguientes.

Las directivas de preautenticación constan de un perfil y una expresión. Se configura el perfil para usar una expresión que permita o deniegue la ejecución de un proceso en el dispositivo del usuario. Por ejemplo, el archivo de texto, clienttext.txt, se está ejecutando en el dispositivo del usuario. Cuando el usuario inicia sesión en NetScaler Gateway, puede permitir o denegar el acceso según si el archivo de texto se está ejecutando. Si no desea permitir que los usuarios inicien sesión cuando el proceso se está ejecutando, puede configurar un perfil de preautenticación para detener el proceso antes de que los usuarios inicien sesión.

**Puede configurar los siguientes ajustes para las directivas de preautenticación:**

- Expresión. Incluye los siguientes ajustes para ayudarle a crear expresiones:
  - Expresión. Muestra todas las expresiones.
  - Coincidir con cualquier expresión. Configura la directiva para que coincida con cualquiera de las expresiones presentes en la lista de expresiones seleccionadas.
  - Coincidir con todas las expresiones. Configura la directiva para que coincida con todas las expresiones presentes en la lista de expresiones seleccionadas.
  - Expresiones tabulares. Crea una expresión compuesta con las expresiones existentes mediante los operadores `OR (||) or AND (&&)`.
  - Formato libre avanzado. Crea expresiones compuestas personalizadas utilizando los nombres de las expresiones y los operadores `OR (||) and AND (&&)`. Elija solo las expresiones que necesite y omita otras expresiones de la lista de expresiones seleccionadas.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Agregar. Crea una expresión.
- Modificar. Modifica una expresión existente.
- Eliminar. Elimina la expresión seleccionada de la lista de expresiones compuestas.
- Expresiones con nombre. Seleccione una expresión con nombre configurada. Puede seleccionar expresiones con nombre del menú de expresiones ya presentes en NetScaler Gateway.
- Agregar expresión. Agrega la expresión con nombre seleccionada a la directiva.
- Reemplazar expresión. Reemplaza la expresión con nombre seleccionada en la directiva.
- Vista previa de la expresión. Muestra la cadena detallada que está configurada en NetScaler Gateway al seleccionar una expresión con nombre.

## Configurar perfil de preautenticación

### Para configurar un perfil de preautenticación globalmente mediante la GUI

1. En la ficha Configuración, haga clic en **NetScaler Gateway,** y, a continuación, haga clic en **Configuración global**.
2. En el panel de detalles, en **Configuración**, haga clic en **Cambiar la configuración de preautenticación**.
3. En el cuadro de diálogo **Configuración global de preautenticación**, configure los parámetros:

   a. En **Acción**, seleccione **Permitir o Denegar**.

      Deniega o permite a los usuarios iniciar sesión después de que se realice el análisis de puntos finales.

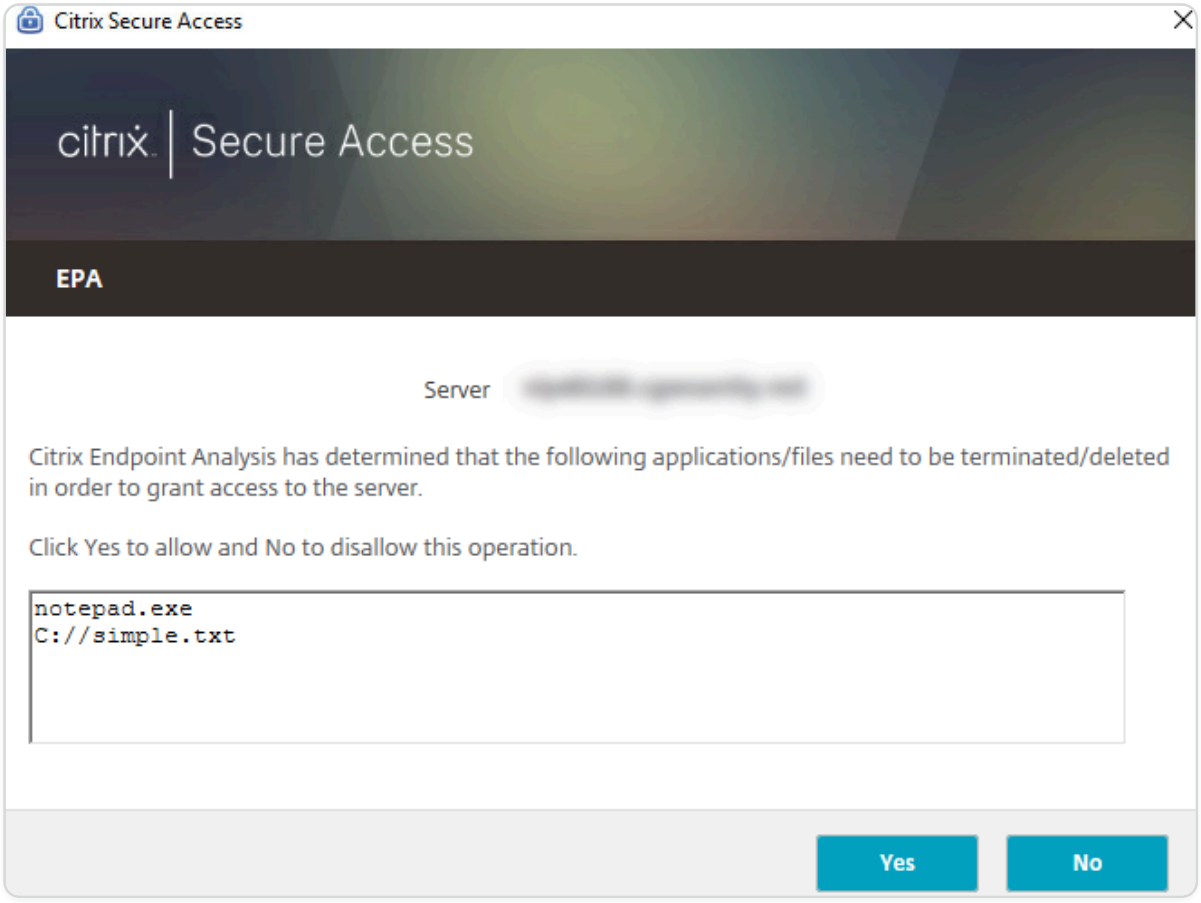
   b. En **Procesos que se van a cancelar**, introduzca el proceso.

      Esto especifica los procesos que el complemento de análisis de puntos finales debe detener.

   c. En **Archivos que se van a eliminar**, introduzca el nombre del archivo.

      Esto especifica los archivos que el complemento de análisis de puntos finales debe eliminar. Al eliminar o cancelar un proceso, se muestra una notificación a los usuarios finales.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



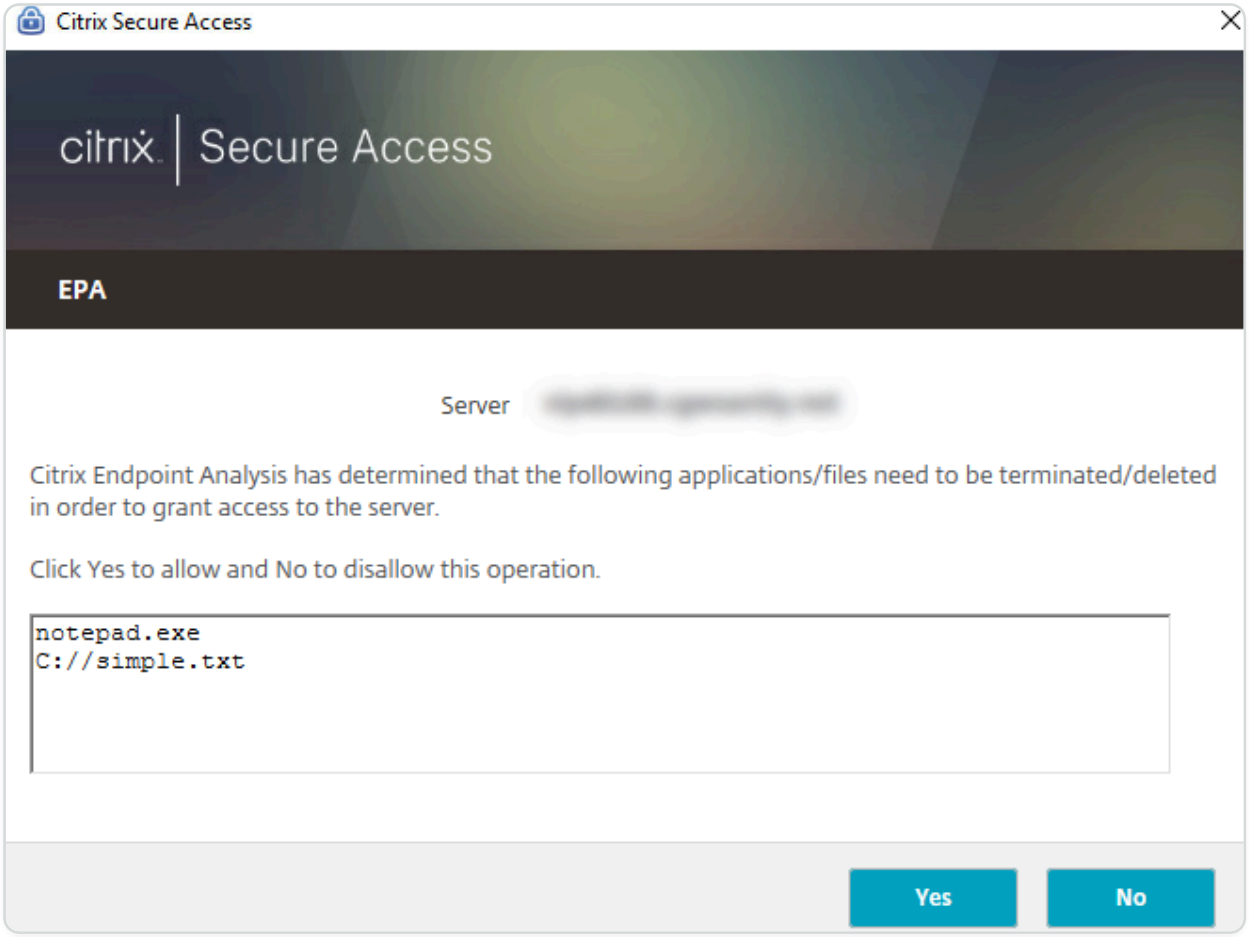

4. En Expresión, puede dejar la expresión ns_true o crear una expresión para una aplicación específica, como un antivirus o un software de seguridad, y luego hacer clic en **OK**.

### Para configurar un perfil de preautenticación mediante la GUI

1. Vaya a **NetScaler Gateway > Directivas > Autenticación/Autorización** y, a continuación, haga clic en **EPA de preautenticación**.
2. En el panel de detalles, en la ficha **Profiles**, haga clic en **Add**.
3. En **Name**, escriba el nombre de la aplicación que se va a comprobar.
4. En **Action**, seleccione **ALLOW** o **DENY**.
5. En **Processes to be canceled**, escriba el nombre del proceso que se va a detener.
6. En **Files to be deleted**, escriba el nombre del archivo que se va a eliminar, como c:\clientext.txt, haga clic en **Create** y, a continuación, haga clic en **Close**.

   Esto especifica los archivos que el complemento Endpoint Analysis debe eliminar. Al eliminar o cancelar un proceso, se muestra una notificación a los usuarios finales.

© 1997–2026 Citrix Systems, Inc. All rights reserved.




Si utiliza la GUI para configurar un perfil de preautenticación, debe crear la directiva de preautenticación haciendo clic en **Add** en la ficha **Policies**. En el cuadro de diálogo **Create Pre-Authentication Policy**, seleccione el perfil en el menú **Request Profile**.

### Agregar una expresión preconfigurada a una directiva de preautenticación

NetScaler Gateway incluye expresiones preconfiguradas, denominadas expresiones con nombre. Al configurar una directiva, puede usar una expresión con nombre para la directiva. Por ejemplo, desea que la directiva de preautenticación compruebe si Symantec Antivirus 10 tiene definiciones de virus actualizadas. Cree una directiva de preautenticación y agregue la expresión como se describe en el siguiente procedimiento.

Al crear una directiva de preautenticación o de sesión, puede crear la expresión al crear la directiva. A continuación, puede aplicar la directiva, con la expresión, a los servidores virtuales o globalmente.

El siguiente procedimiento describe cómo añadir una expresión antivirus preconfigurada a una política mediante la utilidad de configuración.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**Añadir una expresión con nombre a una directiva de autenticación previa**

1. Vaya a **NetScaler Gateway > Policies > Authentication/Authorization** y, a continuación, haga clic en **Pre-Authentication EPA**.
2. En el panel de detalles, seleccione una política y, a continuación, haga clic en **Open**.
3. Junto a **Named Expressions**, seleccione **Anti-Virus**, seleccione el producto antivirus de la lista.
4. Haga clic en **Add Expression**, haga clic en **Create** y, a continuación, haga clic en **Close**.

## Configurar expresiones personalizadas

Una expresión personalizada es aquella que se crea dentro de la política. Al crear una expresión, se configuran los parámetros de la expresión.

También puede crear expresiones personalizadas para hacer referencia a cadenas de uso común. Esto facilita el proceso de configuración de las políticas de autenticación previa y también el mantenimiento de las expresiones configuradas.

Por ejemplo, desea crear una expresión personalizada para el antivirus Symantec 10 y asegurarse de que las definiciones de virus no tengan más de tres días. Cree una política y, a continuación, configure la expresión para especificar las definiciones de virus.

El siguiente procedimiento muestra cómo crear una expresión en una política de autenticación previa. Puede utilizar los mismos pasos en una política de sesión.

**Crear una política de autenticación previa y una expresión personalizada**

1. Vaya a **NetScaler Gateway > Policies > Authentication/Authorization** y, a continuación, haga clic en **Pre-Authentication EPA**.
2. En el panel de detalles, haga clic en **Add**.
3. En **Name**, escriba un nombre para la política.
4. Junto a **Perfil de solicitud**, haga clic en **Nuevo**.
5. En el cuadro de diálogo Crear perfil de autenticación, en **Nombre**, escriba un nombre para el perfil y en **Acción**, seleccione **Permitir** y, a continuación, haga clic en **Crear**.
6. En el cuadro de diálogo Crear directiva de autenticación previa, junto a M**atch Any Expression**, haga clic en **Agregar**.
7. En **Tipo de expresión**, seleccione **Seguridad del cliente**.
8. Configure lo siguiente:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

a. En **Componente**, seleccione **Antivirus**.
b. En **Nombre**, escriba un nombre para la aplicación.
c. En **Calificador**, seleccione **Versión**.
d. En **Operador**, seleccione **==**.
e. En **Valor**, escriba el valor.
f. En **Actualización**, escriba 3 y, a continuación, haga clic en **Aceptar**.

9. En el cuadro de diálogo Crear directiva de autenticación previa, haga clic en **Crear** y, a continuación, haga clic en **Cerrar**.

Cuando se configura una expresión personalizada, esta se agrega al cuadro **Expresión** en el cuadro de diálogo de la directiva.

### Configurar expresiones compuestas

Una directiva de autenticación previa puede tener un perfil y varias expresiones. Si configura expresiones compuestas, utiliza operadores para especificar las condiciones de la expresión. Por ejemplo, puede configurar expresiones compuestas para requerir que el dispositivo de usuario ejecute una de las siguientes aplicaciones antivirus:

- Symantec Antivirus 10
- McAfee Antivirus 11
- Sophos Antivirus 4

Se configura la expresión con el operador OR para comprobar las tres aplicaciones anteriores. Si NetScaler Gateway detecta la versión correcta de cualquiera de las aplicaciones en el dispositivo del usuario, se permite a los usuarios iniciar sesión. La expresión en el cuadro de diálogo de la directiva aparece de la siguiente manera:

```
av_5_Symantec_10 || av_5_McAfeevirusscan_11 || av_5_sophos_4
```

Para obtener más información sobre las expresiones compuestas, consulte Configuración de expresiones compuestas.

### Enlazar directivas de autenticación previa

Después de crear la directiva de autenticación previa, enlácela al nivel al que se aplica. Puede enlazar las directivas de autenticación previa a servidores virtuales o globalmente.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

#### Crear y enlazar una directiva de autenticación previa globalmente

1. En la ficha Configuración, haga clic en **NetScaler Gateway,** y, a continuación, haga clic en **Configuración global**.
2. En el panel de detalles, haga clic en **Cambiar configuración de autenticación previa**.
3. En el cuadro de diálogo Configuración global de autenticación previa, en **Acción**, seleccione **Permitir** o **Denegar**.
4. En **Nombre**, escriba un nombre para la directiva.
5. En el cuadro de diálogo **Configuración global de autenticación previa**, junto a **Expresiones con nombre**, seleccione **General**, seleccione el valor **True**, haga clic en **Agregar expresión**, haga clic en **Crear** y, a continuación, haga clic en **Cerrar**.

#### Enlazar una directiva de autenticación previa a un servidor virtual

1. En la ficha Configuration, haga clic en **NetScaler Gateway** y, a continuación, en **Virtual Servers**.
2. En el panel de detalles, seleccione un servidor virtual y, a continuación, haga clic en **Open**.
3. En el cuadro de diálogo configure NetScaler Gateway Virtual Server, haga clic en la ficha **Policies** y, a continuación, en **Pre-authentication**.
4. En Details, haga clic en **Insert Policy** y, a continuación, en Policy Name, seleccione la directiva de autenticación previa.
5. Haga clic en **OK**.

### Desvincular y eliminar directivas de autenticación previa

Puede eliminar una directiva de autenticación previa de NetScaler Gateway si es necesario. Antes de eliminar una directiva de autenticación previa, desvínculela del servidor virtual o globalmente.

#### Desvincular una directiva de autenticación previa global

1. Vaya a **NetScaler Gateway > Policies > Authentication/Authorization** y, a continuación, haga clic en **Pre-Authentication EPA**.
2. En el panel de detalles, seleccione una directiva y, a continuación, en **Action**, haga clic en **Global Bindings**.
3. En el cuadro de diálogo **Bind/Unbind Pre-authentication Policies to Global**, seleccione una directiva, haga clic en **Unbind Policy** y, a continuación, en **OK**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

### Desvincular una directiva de autenticación previa de un servidor virtual

1. En la ficha Configuration, haga clic en **NetScaler Gateway** y, a continuación, en **Virtual Servers**.
2. En el cuadro de diálogo **Configure NetScaler Gateway Virtual Server**, haga clic en la ficha **Policies** y, a continuación, en **Preauthentication**.
3. Seleccione la directiva y, a continuación, haga clic en **Unbind Policy**.

Cuando la política de preautenticación no está vinculada, puede eliminar la política de NetScaler Gateway.

### Eliminar una política de preautenticación

1. Vaya a **NetScaler Gateway > Directivas > Autenticación/Autorización** y, a continuación, haga clic en **EPA de preautenticación**.
2. En el panel de detalles, seleccione una política y, a continuación, haga clic en **Eliminar**.

## Establecer la prioridad de las políticas de preautenticación

Puede tener varias políticas de preautenticación vinculadas a diferentes niveles. Por ejemplo, tiene una política que comprueba una aplicación antivirus específica vinculada globalmente y una política de firewall vinculada al servidor virtual. Cuando los usuarios inician sesión, la política vinculada al servidor virtual se aplica primero. La política vinculada globalmente se aplica en segundo lugar.

Puede cambiar el orden en que se producen los análisis de preautenticación. Para que NetScaler Gateway aplique primero la política global, cambie el número de prioridad de la política vinculada al servidor virtual, dándole un número de prioridad más alto que la política vinculada globalmente. Por ejemplo, establezca el número de prioridad para la política global en uno y la política del servidor virtual en dos. Cuando los usuarios inician sesión, NetScaler Gateway ejecuta primero el análisis de la política global y, en segundo lugar, el análisis de la política del servidor virtual.

### Cambiar la prioridad de una política de preautenticación

1. En la ficha Configuración, haga clic en **NetScaler Gateway** y, a continuación, haga clic en **Servidores virtuales**.
2. En el panel de detalles, seleccione un servidor virtual y, a continuación, haga clic en **Abrir**.
3. En la ficha Directivas, haga clic en **Preautenticación**.
4. En Prioridad, escriba el número de prioridad de la política y, a continuación, haga clic en **Aceptar**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

# Directivas de postautenticación

**IMPORTANTE:**

El análisis de puntos finales está diseñado para analizar el dispositivo del usuario según criterios de cumplimiento predeterminados y no aplica ni valida la seguridad de los dispositivos del usuario final. Se recomienda utilizar sistemas de seguridad de puntos finales para proteger los dispositivos de ataques de administrador local.

Una directiva de postautenticación es un conjunto de reglas genéricas que el dispositivo del usuario debe cumplir para mantener la sesión activa. Si la directiva falla, la conexión a NetScaler Gateway finaliza. Al configurar la directiva de postautenticación, puede configurar cualquier ajuste para las conexiones de usuario que se puedan hacer condicionales.

Utilice directivas de sesión para configurar directivas de postautenticación. Primero, cree los usuarios a los que se aplica la directiva. Luego, agregue los usuarios a un grupo. A continuación, vincule las directivas de sesión, de tráfico y las aplicaciones de intranet al grupo.

También puede especificar grupos como grupos de autorización. Este tipo de grupo le permite asignar usuarios a grupos en función de una expresión de comprobación de dispositivo cliente dentro de la directiva de sesión.

También puede configurar una directiva de postautenticación para colocar a los usuarios en un grupo de cuarentena si el dispositivo del usuario no cumple los requisitos de la directiva. Una directiva simple incluye una expresión de comprobación de dispositivo cliente y un mensaje. Cuando los usuarios están en el grupo de cuarentena, pueden iniciar sesión en NetScaler Gateway; sin embargo, reciben acceso limitado a los recursos de red.

No puede crear un grupo de autorización y un grupo de cuarentena utilizando el mismo perfil y directiva de sesión. Los pasos para crear la directiva de postautenticación son los mismos. Al crear la directiva de sesión, seleccione un grupo de autorización o un grupo de cuarentena. Puede crear dos directivas de sesión y vincular cada directiva al grupo.

Las directivas de postautenticación también se utilizan con SmartAccess. Para obtener más información sobre SmartAccess, consulte Configuración de SmartAccess.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**NOTA:**

Esta funcionalidad solo funciona con el cliente Citrix Secure Access. Si los usuarios inician sesión con la aplicación Citrix Workspace, el análisis de Endpoint Analysis solo se ejecuta al iniciar sesión.

## Configurar una directiva de postautenticación

Utilice una directiva de sesión para configurar una directiva de postautenticación. Una directiva simple incluye una expresión de comprobación de dispositivo cliente y un mensaje.

### Para configurar una directiva de postautenticación mediante la GUI

1. Expanda **NetScaler Gateway > Directivas** y, a continuación, haga clic en **Sesión**.
2. En el panel de detalles, en la ficha **Directivas**, haga clic en **Agregar**.
3. En **Nombre**, escriba un nombre para la directiva.
4. Junto a **Perfil de solicitud**, haga clic en **Nuevo**.
5. En **Nombre**, escriba un nombre para el perfil.
6. En la ficha Seguridad, haga clic en **Configuración avanzada**.
7. En **Seguridad del cliente**, haga clic en **Anular global** y, a continuación, haga clic en **Nuevo**.
8. Configure la expresión de comprobación del dispositivo cliente y, a continuación, haga clic en **Crear**.
9. En **Seguridad del cliente**, en Grupo de cuarentena, seleccione un grupo.
10. En **Mensaje de error**, escriba el mensaje que desea que reciban los usuarios si el análisis posterior a la autenticación falla.
11. En Grupos de autorización, haga clic en **Anular global**, seleccione un grupo, haga clic en **Agregar**, haga clic en **Aceptar** y, a continuación, haga clic en **Crear**.
12. En el cuadro de diálogo **Crear directiva de sesión**, junto a Expresiones con nombre, seleccione **General**, seleccione **Valor verdadero**, haga clic en **Agregar expresión**, haga clic en **Crear** y, a continuación, haga clic en **Cerrar**.

## Configurar la frecuencia de los análisis posteriores a la autenticación

Puede configurar NetScaler Gateway para ejecutar la directiva posterior a la autenticación a intervalos especificados. Por ejemplo, ha configurado una directiva de comprobación de

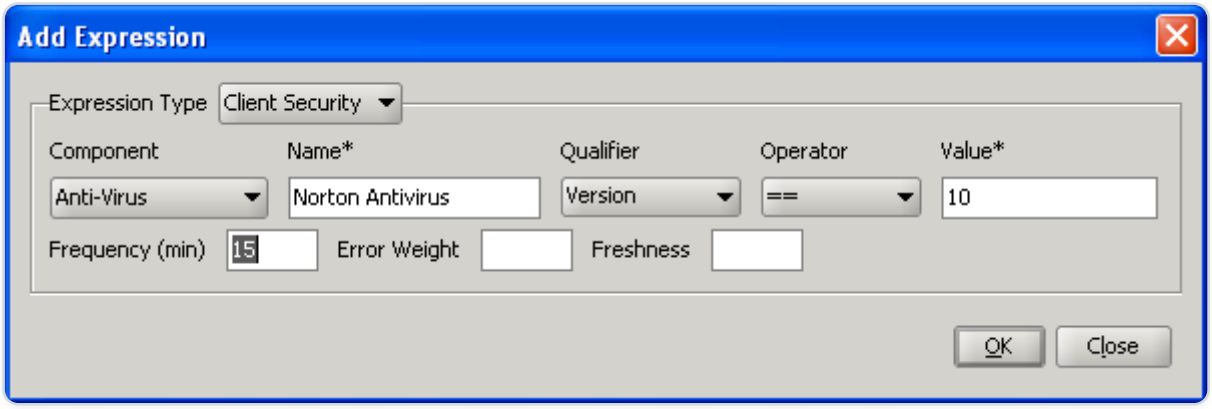
© 1997–2026 Citrix Systems, Inc. All rights reserved.

dispositivos cliente y desea que se ejecute en el dispositivo de usuario cada 10 minutos. Puede configurar esta frecuencia creando una expresión personalizada dentro de la directiva.

**NOTA:**

La funcionalidad de comprobación de frecuencia para las directivas posteriores a la autenticación solo funciona con el cliente de Citrix Secure Access. Si los usuarios inician sesión con la aplicación Citrix Workspace, el análisis de Endpoint Analysis se ejecuta solo al iniciar sesión.

Puede establecer la frecuencia (en minutos) al configurar la política de comprobación de dispositivos cliente. La siguiente figura muestra dónde puede introducir un valor de frecuencia en el cuadro de diálogo **Agregar expresión**.




## Grupos de cuarentena y autorización

Cuando los usuarios inician sesión en NetScaler Gateway, se les asigna a un grupo que se configura en NetScaler Gateway o en un servidor de autenticación en la red segura. Si un usuario falla un análisis posterior a la autenticación, puede asignarlo a un grupo restringido, denominado grupo de cuarentena, que restringe el acceso a los recursos de red.

También puede usar grupos de autorización para restringir el acceso de los usuarios a los recursos de red. Por ejemplo, podría tener un grupo de personal contratado que solo tenga acceso a su servidor de correo electrónico y a un recurso compartido de archivos. Cuando los dispositivos de los usuarios cumplen los requisitos de comprobación de dispositivos que definió en NetScaler Gateway, los usuarios pueden convertirse en miembros de grupos de forma dinámica.

Utilice la configuración global o las directivas de sesión para configurar grupos de cuarentena y autorización que estén vinculados a un usuario, grupo o servidor virtual. Puede asignar usuarios a grupos en función de una expresión de comprobación de dispositivos cliente dentro de la directiva

© 1997–2026 Citrix Systems, Inc. All rights reserved.

de sesión. Cuando el usuario es miembro de un grupo, NetScaler Gateway aplica la directiva de sesión en función de la pertenencia al grupo.

### Configurar grupos de autorización

Al configurar un análisis de Endpoint Analysis, puede agregar usuarios dinámicamente a un grupo de autorización cuando el dispositivo del usuario pasa el análisis. Por ejemplo, cree un análisis de Endpoint Analysis que compruebe la pertenencia al dominio del dispositivo del usuario. En NetScaler Gateway, cree un grupo local llamado Equipos unidos a un dominio y agréguelo como grupo de autorización para cualquiera que pase el análisis. Cuando los usuarios se unen al grupo, heredan las directivas asociadas a este.

No puede vincular directivas de autorización globalmente ni a un servidor virtual. Puede usar grupos de autorización para proporcionar un conjunto predeterminado de directivas de autorización cuando los usuarios no están configurados para ser miembros de otro grupo en NetScaler Gateway.

#### PARA CONFIGURAR UN GRUPO DE AUTORIZACIÓN MEDIANTE UNA DIRECTIVA DE SESIÓN

1. Vaya a **NetScaler Gateway > Directivas** y, a continuación, haga clic en **Sesión**.
2. En el panel de detalles, en la ficha Directivas, haga clic en **Agregar**.
3. En **Nombre**, escriba un nombre para la directiva.
4. Junto a **Perfil de solicitud**, haga clic en **Nuevo**.
5. En **Nombre**, escriba un nombre para el perfil.
6. En la pestaña Seguridad, haga clic en **Configuración avanzada**.
7. En Grupos de autorización, haga clic en **Anular global** y seleccione un grupo de la lista desplegable.
8. Haga clic en **Agregar**, haga clic en **Aceptar** y, a continuación, haga clic en **Crear**.
9. En el cuadro de diálogo **Crear directiva de sesión**, junto a Expresiones con nombre, seleccione **General**, seleccione **Valor verdadero**, haga clic en **Agregar expresión**, haga clic en **Crear** y, a continuación, haga clic en **Cerrar**.

Después de crear la directiva de sesión, puede vincularla a un usuario, grupo o servidor virtual.

#### PARA CONFIGURAR UN GRUPO DE AUTORIZACIÓN GLOBAL

1. Expanda **NetScaler Gateway** y, a continuación, haga clic en **Configuración global**.
2. En el panel de detalles, en Configuración, haga clic en **Cambiar configuración global**.
3. En la pestaña Seguridad, haga clic en **Configuración avanzada**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. En Grupo de autorización, seleccione un grupo de la lista desplegable.
5. Haga clic en **Agregar** y, a continuación, haga clic en **Aceptar**.

Si desea eliminar un grupo de autorización globalmente o de la directiva de sesión, en el cuadro de diálogo Configuración de seguridad - Avanzada, seleccione el grupo de autorización de la lista y, a continuación, haga clic en **Quitar**.

### Configuración de grupos de cuarentena

Al configurar un grupo de cuarentena, se configura la expresión de comprobación del dispositivo cliente mediante el cuadro de diálogo Configuración de seguridad - Configuración avanzada dentro de un perfil de sesión.

#### PARA CONFIGURAR LA EXPRESIÓN DE COMPROBACIÓN DEL DISPOSITIVO CLIENTE PARA UN GRUPO DE CUARENTENA

1. Vaya a **NetScaler Gateway > Directivas** y, a continuación, haga clic en **Sesión**.
2. En el panel de detalles, en la ficha Directivas, haga clic en **Agregar**.
3. En **Nombre**, escriba un nombre para la directiva.
4. Junto a **Perfil de solicitud**, haga clic en **Nuevo**.
5. En **Nombre**, escriba un nombre para el perfil.
6. En la ficha Seguridad, haga clic en **Configuración avanzada**.
7. En **Seguridad del cliente**, haga clic en **Anular global** y, a continuación, haga clic en **Nuevo**.
8. En el cuadro de diálogo **Expresión de cliente**, configure la expresión de comprobación del dispositivo cliente y, a continuación, haga clic en **Crear**.
9. En **Grupo de cuarentena**, seleccione el grupo.
10. En Mensaje de error, escriba un mensaje que describa el problema para los usuarios y, a continuación, haga clic en **Crear**.
11. En el cuadro de diálogo **Crear directiva de sesión**, junto a Expresiones con nombre, seleccione **General**, seleccione **Valor verdadero** y haga clic en **Agregar expresión**.
12. Haga clic en **Crear** y, a continuación, haga clic en **Cerrar**.

Después de crear la directiva de sesión, vincúlela a un usuario, grupo o servidor virtual.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**NOTA:**

Si el análisis de Endpoint Analysis falla y el usuario se coloca en el grupo de cuarentena, las directivas vinculadas al grupo de cuarentena solo son efectivas si no hay directivas vinculadas directamente al usuario que tengan un número de prioridad igual o inferior al de las directivas vinculadas al grupo de cuarentena.

#### PARA CONFIGURAR UN GRUPO DE CUARENTENA GLOBAL

1. Expanda **NetScaler Gateway** y, a continuación, haga clic en **Global Settings**.
2. En el panel de detalles, en Configuración, haga clic en **Change global settings**.
3. En la ficha **Security**, haga clic en **Advanced Settings**.
4. En **Client Security**, configure la expresión de comprobación del dispositivo cliente.
5. En **Quarantine Group**, seleccione el grupo.
6. En **Error Message**, escriba un mensaje que describa el problema a los usuarios y, a continuación, haga clic en **OK**.

## Expresiones de comprobación de dispositivos de preautenticación para dispositivos de usuario

**IMPORTANTE:**

El Análisis de puntos finales está diseñado para analizar el dispositivo del usuario según criterios de cumplimiento predeterminados y no aplica ni valida la seguridad de los dispositivos de usuario final. Se recomienda utilizar sistemas de seguridad de puntos finales para proteger los dispositivos de ataques de administradores locales.

NetScaler Gateway proporciona varias comprobaciones de cumplimiento de puntos finales durante el inicio de sesión del usuario o en otros momentos configurados durante una sesión que ayudan a validar los dispositivos de usuario. Solo los dispositivos de usuario que superan estas comprobaciones pueden establecer una sesión de NetScaler Gateway.

Los siguientes son los tipos de comprobaciones en los dispositivos de usuario que puede configurar en NetScaler Gateway:

- Antispam
- Antivirus

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Directivas de archivos
- Seguridad de Internet
- Sistema operativo
- Firewall personal
- Directivas de procesos
- Directivas de registro
- Directivas de servicio

Si una comprobación de dispositivo falla en el dispositivo de usuario, no se establecen nuevas conexiones hasta que una comprobación posterior sea exitosa (en el caso de comprobaciones que se realizan a intervalos regulares); sin embargo, el tráfico que fluye a través de las conexiones existentes continúa tunelizando a través de NetScaler Gateway.

Puede usar la utilidad de configuración para configurar políticas de preautenticación o expresiones de comprobación de dispositivos dentro de las políticas de sesión que están diseñadas para realizar comprobaciones en los dispositivos de usuario.

### Configurar expresiones de antivirus, firewall, seguridad de Internet o antispam

Puede configurar los ajustes para las políticas de antivirus, firewall, seguridad de Internet y antispam en el cuadro de diálogo **Agregar expresión**. Los ajustes para cada política son los mismos: las diferencias son los valores que seleccione. Por ejemplo, si desea comprobar el dispositivo de usuario en busca de Norton antivirus versión 10 y ZoneAlarm Pro, cree dos expresiones dentro de la política de sesión o preautenticación que especifiquen el nombre y el número de versión de cada aplicación.

Cuando selecciona Seguridad de cliente como tipo de expresión, puede configurar lo siguiente:

- Componente: El tipo de seguridad del cliente, como antivirus, firewall o entrada de registro.
- Nombre: El nombre de la aplicación, proceso, archivo, entrada de registro o sistema operativo.
- Calificador: La versión o el valor del componente que comprueba la expresión.
- Operador: Comprueba si el valor existe o es igual al valor.
- Valor: La versión de la aplicación para software antivirus, firewall, seguridad de Internet o antispam en el dispositivo de usuario.
- Frecuencia: Frecuencia con la que se ejecuta un análisis posterior a la autenticación, en minutos.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Peso de error: Un peso asignado a cada mensaje de error contenido en una expresión anidada cuando varias expresiones tienen diferentes cadenas de error. El peso determina qué mensaje de error aparece.
- Actualización: Define la antigüedad máxima de una definición de virus. Por ejemplo, puede configurar la expresión para que las definiciones de virus no tengan más de tres días.

**Para agregar una política de comprobación de dispositivos de cliente a una política de preautenticación o de sesión**

1. En la utilidad de configuración, en el panel de navegación, realice una de las siguientes acciones:

   a. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda **NetScaler Gateway > Policies** y, a continuación, haga clic en **Sesión**.

   b. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda **NetScaler Gateway > Directivas > Autenticación/Autorización** y, a continuación, haga clic en **EPA de autenticación previa**.

2. En el panel de detalles, en la ficha Directivas, haga clic en **Agregar**.
3. En Nombre, escriba un nombre para la directiva.
4. Junto a Coincidir con cualquier expresión, haga clic en Agregar.
5. En el cuadro de diálogo Agregar expresión, en Tipo de expresión, seleccione **Seguridad del cliente**.
6. Configure los ajustes para lo siguiente:

   a. En Componente, seleccione el elemento que desea escanear.

   b. En Nombre, escriba el nombre de la aplicación.

   c. En Calificador, seleccione **Versión**.

   d. En Operador, seleccione el valor.

   e. En Valor, escriba la cadena de comprobación del dispositivo cliente, haga clic en **Aceptar**, haga clic en **Crear** y, a continuación, haga clic en **Cerrar**.

## Configurar directivas de servicio

Un servicio es un programa que se ejecuta silenciosamente en el dispositivo del usuario. Al crear una directiva de sesión o de autenticación previa, puede crear una expresión que garantice que los dispositivos de los usuarios ejecuten un servicio determinado cuando se establezca la sesión.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**Para configurar una directiva de servicio**

1. En la utilidad de configuración, en el panel de navegación, realice una de las siguientes acciones:
    a. En la utilidad de configuración, en la pestaña Configuración, en el panel de navegación, expanda **NetScaler Gateway > Directivas** y, a continuación, haga clic en Sesión.
    b. En la utilidad de configuración, en la pestaña Configuración, en el panel de navegación, expanda **NetScaler Gateway > Directivas > Autenticación/Autorización** y, a continuación, haga clic en EPA de autenticación previa.
2. En el panel de detalles, en la pestaña Directivas, haga clic en Agregar.
3. En Nombre, escriba un nombre para la directiva.
4. Junto a Coincidir con cualquier expresión, haga clic en Agregar.
5. En el cuadro de diálogo Agregar expresión, en Tipo de expresión, seleccione Seguridad de cliente.
6. Configure los ajustes para lo siguiente:
    a. En Componente, seleccione Servicio.
    b. En Nombre, escriba el nombre del servicio.
    c. En Calificador, déjelo en blanco o seleccione Versión.
    d. Según su selección en Calificador, realice una de las siguientes acciones:
        - Si se deja en blanco, en Operador, seleccione == o \!=
        - Si seleccionó Versión, en Operador, en Valor, escriba el valor, haga clic en Aceptar y, a continuación, haga clic en Cerrar.

Puede consultar una lista de todos los servicios disponibles y el estado de cada uno en un equipo basado en Windows en la siguiente ubicación:

**Panel de control > Herramientas administrativas > Servicios**

**NOTA:**

El nombre de cada servicio varía de su nombre listado. Compruebe el nombre del servicio consultando el cuadro de diálogo Propiedades.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

### Configurar políticas de proceso

Al crear una política de sesión o de preautenticación, puede definir una regla que requiera que todos los dispositivos de usuario tengan un proceso específico en ejecución cuando los usuarios inicien sesión. El proceso puede ser cualquier aplicación y puede incluir aplicaciones personalizadas.

Nota: La lista de todos los procesos que se ejecutan en un equipo basado en Windows aparece en la pestaña **Procesos** del Administrador de tareas de Windows.

#### Para configurar una política de proceso

1. En la utilidad de configuración, en el panel de navegación, realice una de las siguientes acciones:
    a. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda **NetScaler Gateway \ > Directivas** y, a continuación, haga clic en Sesión.
    b. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda **NetScaler Gateway \> Directivas \ > Autenticación/Autorización** y, a continuación, haga clic en EPA de preautenticación.
2. En el panel de detalles, en la ficha Directivas, haga clic en Agregar.
3. En Nombre, escriba un nombre para la directiva.
4. Junto a Coincidir con cualquier expresión, haga clic en Agregar.
5. En el cuadro de diálogo Agregar expresión, en Tipo de expresión, seleccione Seguridad del cliente.
6. Configure los ajustes para lo siguiente:
    a. En Componente, seleccione Proceso.
    b. En Nombre, escriba el nombre de la aplicación.
    c. En Operador, seleccione EXISTS o NOTEXISTS, haga clic en Aceptar y, a continuación, en Cerrar.

Al configurar una directiva de análisis de puntos finales (de preautenticación o postautenticación) para comprobar un proceso, puede configurar una suma de comprobación MD5.

Al crear la expresión para la directiva, puede agregar la suma de comprobación MD5 al proceso que está comprobando. Por ejemplo, si está comprobando si notepad.exe se está ejecutando en el dispositivo del usuario, la expresión es:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CLIENT.APPLICATION.PROCESS(notepad.exe_md5_388b8fbc36a8558587afc90fb23a3b00) EXISTS

### Configurar directivas del sistema operativo

Al crear una directiva de sesión o de preautenticación, puede configurar cadenas de comprobación de dispositivos cliente para determinar si el dispositivo del usuario ejecuta un sistema operativo determinado cuando los usuarios inician sesión. También puede configurar la expresión para comprobar un Service Pack o una revisión en particular.

Los valores para Windows y Macintosh son:

| SISTEMA OPERATIVO | VALOR |
|---|---|
| macOS X | macOS |
| Windows 8.1 | win8.1 |
| Windows 8 | win8 |
| Windows 7 | win7 |
| Windows Vista | Vista |
| Windows XP | `winxp` |
| Windows Server 2008 | win2008 |
| Windows Server 2003 | win2003 |
| Windows 2000 Server | win2000 |
| Plataforma Windows de 64 bits | win64 |

#### Para configurar una política de sistema operativo mediante la GUI

1. En el panel de navegación, realice una de las siguientes acciones:
    a. Vaya a **NetScaler Gateway > Directivas** y, a continuación, haga clic en **Sesión**.
    b. Vaya a **NetScaler Gateway > Directivas > Preautenticación**.
2. En el panel de detalles, en la ficha **Directivas**, haga clic en **Agregar**.
3. En **Nombre**, escriba un nombre para la directiva.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. En **Acción de solicitud**, seleccione una acción existente o cree una.
5. Haga clic en **Editor de expresiones**.
6. En **Seleccionar tipo de expresión**, seleccione **Seguridad del cliente**.
7. Configure los siguientes ajustes:
    a. En **Componente**, seleccione **Sistema operativo**.
    b. En **Nombre**, escriba el nombre del sistema operativo.
    c. En Calificador, realice una de las siguientes acciones:
        - Deje el campo en blanco
        - Seleccione **Service Pack**
        - Seleccione **Revisión**
        - Seleccione **Versión** (solo para macOS)
    d. Según su selección en el paso 7, en Operador, realice una de las siguientes acciones:
        - Si Calificador está en blanco, en Operador, seleccione EQUAL (= =), NOTEQUAL (\!=), EXISTS o NOTEXISTS.
        - Si seleccionó Service Pack o Hotfix, seleccione el operador y en Valor, escriba el valor.
8. Haga clic en **Listo** y, a continuación, haga clic en **Cerrar**.

Si está configurando un Service Pack, como client.os `(winxp).sp`, si no hay un número en el campo **Valor**, NetScaler Gateway devuelve un mensaje de error porque la expresión no es válida.

Si el sistema operativo tiene Service Packs presentes, como Service Pack 3 y Service Pack 4, puede configurar una comprobación solo para Service Pack 4, porque la presencia de Service Pack 4 indica automáticamente que los Service Packs anteriores están presentes.

### Configurar directivas de registro

Al crear una directiva de sesión o de preautenticación, puede comprobar la existencia y el valor de las entradas del registro en el dispositivo del usuario. La sesión se establece solo si la entrada particular existe o tiene el valor configurado o superior.

Al configurar una expresión de registro, utilice las siguientes directrices:

- Se utilizan cuatro barras invertidas para separar claves y subclaves, como

  HKEY_LOCAL_MACHINE\\\\\\\\SOFTWARE

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Se utilizan guiones bajos para separar la subclave y el nombre de valor asociado, como

  HKEY_LOCAL_MACHINE\\\\\\\\SOFTWARE\\\\\\\\VirusSoftware_Version

- Se utiliza una barra invertida (\\) para indicar un espacio, como en los dos ejemplos siguientes:

  HKEY_LOCAL_MACHINE\\\\\\\\SOFTWARE\\\\Citrix\\\\\\\\Secure\\ Access\\ Client_ProductVersion

  CLIENT.REG(HKEY_LOCAL_MACHINE\\\\\\\\Software\\\\\\\\Symantec\\\\Norton\\ AntiVirus_Version).VALUE == 12.8.0.4 -frequency 5

La siguiente es una expresión de registro que busca la clave de registro del cliente Citrix Secure Access™ cuando los usuarios inician sesión:

CLIENT.REG(`secureaccess`).VALUE==HKEY_LOCAL_MACHINE\\\\\\\\SOFTWARE\\\\\\\\CITRIX\\\\\\\\Secure\\Access\\Client_ProductVersion

**NOTA:**

Si está buscando claves y valores de registro y selecciona Formato libre avanzado en el cuadro de diálogo Expresión, la expresión debe comenzar con CLIENT.REG.

Las comprobaciones de registro son compatibles en los cinco tipos más comunes siguientes:

- HKEY_CLASSES_ROOT
- HKEY_CURRENT_USER
- HKEY_LOCAL_MACHINE
- HKEY_USERS
- HKEY_CURRENT_CONFIG

Los valores de registro que se van a comprobar utilizan los siguientes tipos:

- Cadena

  Para el tipo de valor de cadena, se comprueba la distinción entre mayúsculas y minúsculas.

- DWORD

  Para el tipo DWORD, el valor se compara y debe ser igual.

- Cadena expandida

© 1997–2026 Citrix Systems, Inc. All rights reserved.

No se admiten otros tipos, como Binario y Cadena múltiple.

- Solo se admite el operador de comparación '=='.
- No se admiten otros operadores de comparación, como \<, \> y las comparaciones que distinguen entre mayúsculas y minúsculas.
- La longitud total de la cadena del registro debe ser inferior a 256 bytes.

Puede agregar un valor a la expresión. El valor puede ser una versión de software, una versión de Service Pack o cualquier otro valor que aparezca en el registro. Si el valor de los datos en el registro no coincide con el valor con el que está probando, se deniega el inicio de sesión a los usuarios.

**NOTA:**

No puede buscar un valor dentro de una subclave. La búsqueda debe coincidir con el valor con nombre y el valor de datos asociado.

**Para configurar una directiva de registro**

1. En la utilidad de configuración, en el panel de navegación, realice una de las siguientes acciones:
   a. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda **NetScaler Gateway \ > Directivas** y, a continuación, haga clic en Sesión.
   b. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda **NetScaler Gateway \> Directivas \ > Autenticación/Autorización** y, a continuación, haga clic en EPA de autenticación previa.
2. En el panel de detalles, en la ficha Directivas, haga clic en Agregar.
3. En Nombre, escriba un nombre para la directiva.
4. Junto a Coincidir con cualquier expresión, haga clic en Agregar.
5. En el cuadro de diálogo Agregar expresión, en Tipo de expresión, seleccione Seguridad de cliente.
6. Configure los ajustes para lo siguiente:
   a. En Componente, seleccione Registro.
   b. En Nombre, escriba el nombre de la clave de registro.
   c. En Calificador, déjelo en blanco o seleccione Valor.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

d. En Operador, realice una de las siguientes acciones:

   - Si Calificador se deja en blanco, seleccione EXISTE o NOEXISTE
   - Si seleccionó Valor en Calificador, seleccione == o \!=

e. En Valor, escriba el valor tal como aparece en el editor del registro, haga clic en Aceptar y, a continuación, en Cerrar.

### Configurar expresiones compuestas de comprobación de dispositivos cliente

Puede combinar cadenas de comprobación de dispositivos cliente para formar expresiones compuestas de comprobación de dispositivos cliente.

Los operadores booleanos admitidos en NetScaler Gateway son:

- Y (&&)
- O (||)
- No (!)

Para mayor precisión, puede agrupar las cadenas utilizando paréntesis.

**NOTA:**

Si utiliza la línea de comandos para configurar expresiones, use paréntesis para agrupar las expresiones de comprobación de dispositivos al formar una expresión compuesta. El uso de paréntesis mejora la comprensión y la depuración de la expresión del cliente.

#### Configurar directivas con el operador AND (&&)

El operador AND (&&) funciona combinando dos cadenas de comprobación de dispositivos cliente de modo que la comprobación compuesta solo se supera cuando ambas comprobaciones son verdaderas. La expresión se evalúa de izquierda a derecha y, si la primera comprobación falla, la segunda comprobación no se realiza.

Puede configurar el operador AND (&&) utilizando la palabra clave 'AND' o los símbolos '&&'.

Ejemplo:

La siguiente es una comprobación de dispositivo cliente que determina si el dispositivo de usuario tiene la versión 7.0 del antivirus Sophos instalada y en ejecución. También comprueba si el servicio Net Logon se está ejecutando en el mismo equipo.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
CLIENT.APPLICATION.AV(sophos).version==7.0 AND CLIENT.SVC(netlogon) EXISTS
```

Esta cadena también se puede configurar como:

```
CLIENT.APPLICATION.AV(sophos).version==7.0 && CLIENT.SVC(netlogon) EXISTS
```

### Configurar directivas con el operador OR ( || )

El operador OR `(||)` funciona combinando dos cadenas de comprobación de dispositivos. La comprobación compuesta se supera cuando cualquiera de las comprobaciones es verdadera. La expresión se evalúa de izquierda a derecha y, si la primera comprobación se supera, la segunda comprobación no se realiza. Si la primera comprobación no se supera, la segunda comprobación se realiza.

Puede configurar el operador OR `(||)` utilizando la palabra clave `OR` o el símbolo `||`.

Ejemplo:

La siguiente es una comprobación de dispositivo cliente que determina si el dispositivo de usuario tiene el archivo `c:\\file.txt` o el proceso `putty.exe` ejecutándose en él.

```
client.file(c:\\\\\\\\file.txt) EXISTS) OR (client.proc(putty.exe) EXISTS
```

Esta cadena también se puede configurar como

```
client.file(c:\\\\\\\\file.txt) EXISTS) || (client.proc(putty.exe) EXISTS
```

### Configurar directivas mediante el operador NOT (\!)

El operador NOT (\!) o de negación niega la cadena de comprobación del dispositivo cliente.

Ejemplo:

La siguiente comprobación del dispositivo cliente se supera si el archivo c:\ \sophos_virus_defs.dat NO tiene más de dos días de antigüedad:

```
\!(client.file(c:\\\\\\\\sophos\_virus\_defs.dat).timestamp==2dy)
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

# Certificado de dispositivo en nFactor como componente EPA

**IMPORTANTE:**

El análisis de puntos finales (EPA) está diseñado para analizar el dispositivo del usuario según criterios de cumplimiento predeterminados y no aplica ni valida la seguridad de los dispositivos del usuario final. Se recomienda utilizar sistemas de seguridad de puntos finales para proteger los dispositivos de ataques de administradores locales.

El certificado de dispositivo se puede configurar en nFactor como un componente EPA. El certificado de dispositivo puede aparecer como cualquier factor como parte de EPA.

A continuación, se indican los beneficios de configurar el certificado de dispositivo en nFactor como un componente EPA.

- El error en la validación del certificado de dispositivo no provoca un error de inicio de sesión. Según la configuración, el inicio de sesión puede continuar y el usuario puede ser colocado en grupos con acceso limitado.
- Dado que la comprobación del certificado de dispositivo se basa en políticas, puede permitir o bloquear selectivamente el acceso a los recursos de su intranet corporativa en función de la autenticación del certificado de dispositivo. Por ejemplo, la autenticación del certificado de dispositivo se puede utilizar para proporcionar acceso condicional a la aplicación de Office 365 solo en los equipos portátiles administrados por la empresa.

La validación del certificado de dispositivo no puede formar parte de un análisis EPA periódico.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**IMPORTANTE:**

- De forma predeterminada, Windows exige privilegios de administrador para acceder a los certificados de dispositivo. Para agregar la comprobación del certificado de dispositivo para usuarios no administradores, debe instalar el complemento VPN de la misma versión que el complemento EPA en el dispositivo.
- Puede agregar varios certificados de CA a la puerta de enlace y validar el certificado de dispositivo.
- Si instala dos o más certificados de dispositivo en los equipos cliente, los usuarios deben seleccionar el certificado correcto al iniciar sesión en NetScaler Gateway o antes de que se ejecute el análisis de puntos finales.
- Cuando cree el certificado de dispositivo, debe ser un certificado X.509.
- Si tiene un certificado de dispositivo emitido por una CA intermedia, se deben vincular tanto el certificado de CA intermedio como el raíz.
- También debe vincular el certificado de CA al servidor virtual VPN.

### Configurar el certificado de dispositivo en nFactor como componente EPA

**Para configurar el certificado de dispositivo en nFactor como componente EPA mediante la CLI:**

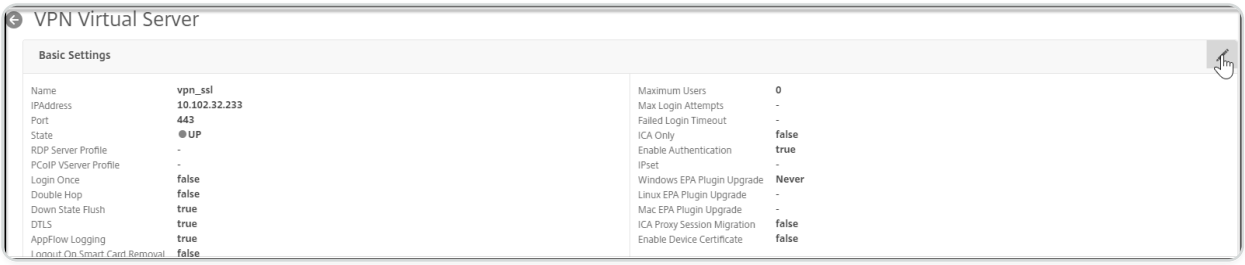
En el símbolo del sistema, escriba;

```
add authentication epaAction epa-act -csecexpr sys.client_expr("device-cert_0_0") -defaultgroup epa_pass -quarantine_group epa_fail
```

**Para configurar el certificado de dispositivo en nFactor como componente EPA para el servidor virtual VPN mediante la GUI:**

1. En la GUI de NetScaler, vaya a **Configuration > NetScaler Gateway > Virtual Servers**.
2. En la página **NetScaler Gateway Virtual Servers**, seleccione el servidor virtual que desea modificar y haga clic en **Edit**.
3. En la página **VPN Virtual Server**, haga clic en el icono Editar.

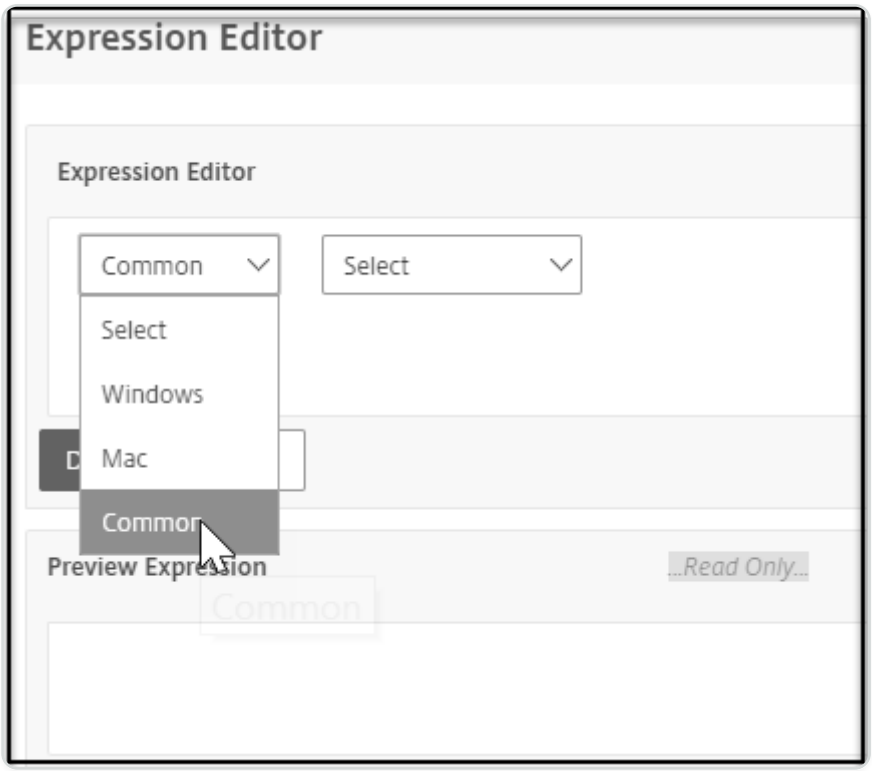
© 1997–2026 Citrix Systems, Inc. All rights reserved.




4. Haga clic en **More**.
5. Haga clic en **+** en la sección CA for Device Certificate y haga clic en OK.

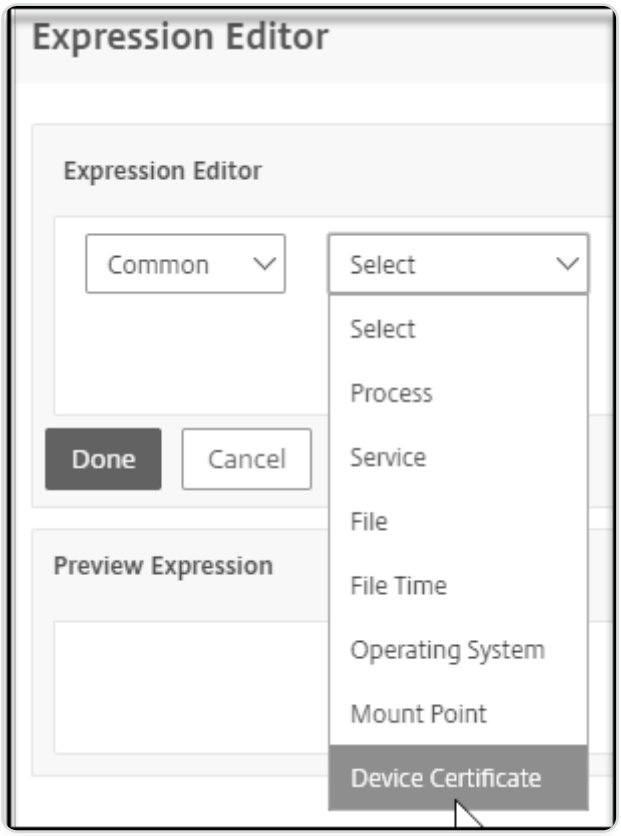
> **NOTA:**
>
> No seleccione la casilla de verificación **Enable Device Certificate**. Al habilitarla, se activa la validación del certificado de dispositivo en el EPA clásico.

6. En la GUI de NetScaler, vaya a **Configuration > Security >AAA – Application Traffic > Policies > Authentication > Advanced Policies > Actions > EPA**.
7. En la página **Authentication EPA Action**, haga clic en **Add**. Puede hacer clic en **Edit** para editar una acción EPA existente.
8. En la página **Create Authentication EPA Action**, proporcione los valores para los campos obligatorios para crear una acción EPA de autenticación y haga clic en el enlace **EPA Editor**.
9. Seleccione **Common** en el menú **Expression Editor**.




© 1997–2026 Citrix Systems, Inc. All rights reserved.

10. Seleccione **Device Certificate** en el menú subsiguiente que aparece y haga clic en **Done** para completar la configuración.




**Para configurar el certificado de dispositivo en nFactor como un componente EPA para el servidor virtual de autenticación mediante la GUI:**

1. En la GUI de NetScaler, vaya a **Security > AAA-Application Traffic > Virtual Servers**.
2. En la página **NetScaler Gateway Virtual Servers**, seleccione el servidor virtual que desea modificar y haga clic en Edit.
3. En la página **Authentication Virtual Server**, haga clic en el icono Edit.
4. Haga clic en **More**.
5. Haga clic en **Add** junto a la sección **CA for Device Certificate**.
6. Seleccione el certificado que desea agregar y haga clic en **OK** para completar la configuración.
7. Repita los **pasos 6 a 10** para completar la configuración.

## Referencias

- Configurar perfil de preautenticación
- Vincular directivas de preautenticación

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Establecer la prioridad de las políticas de preautenticación(/es-es/netscaler-gateway/13-1/vpn-user-config/endpoint-policies/preauthentication-policies-and-profiles.html#set-the-priority-of-preauthentication-policies)
- Configurar una política de postautenticación(/es-es/netscaler-gateway/13-1/vpn-user-config/endpoint-policies/post-authentication-policies.html#configure-a-post-authentication-policy)
- Configurar la frecuencia de los análisis de postautenticación(/es-es/netscaler-gateway/13-1/vpn-user-config/endpoint-policies/post-authentication-policies.html#configure-the-frequency-of-post-authentication-scans)

## Análisis EPA como factor en la autenticación nFactor

**IMPORTANTE:**

El análisis de puntos finales (Endpoint Analysis) está diseñado para analizar el dispositivo del usuario según criterios de cumplimiento predeterminados y no aplica ni valida la seguridad de los dispositivos del usuario final. Se recomienda utilizar sistemas de seguridad de puntos finales para proteger los dispositivos de ataques de administradores locales.

Las siguientes son algunas de las entidades básicas de nFactor EPA.

**Acción EPA:** La acción EPA es un tipo de acción introducido para nFactor EPA. Contiene lo siguiente:

- Expresión de comprobación del dispositivo cliente: Esta expresión se envía al complemento EPA de la puerta de enlace para su evaluación.
- Grupo de éxito: Este grupo, si está configurado, se hereda a la sesión de la puerta de enlace si el resultado de EPA es verdadero.
- Grupo de cuarentena: Este grupo, si está configurado, se hereda a la sesión de la puerta de enlace si el resultado de EPA es falso.
- killProcess: Representa el nombre del proceso que el proceso EPA debe finalizar.
- deleteFiles: Especifica rutas separadas por comas a los archivos que el proceso EPA debe eliminar.

Los grupos se pueden usar durante la vida útil de la sesión para determinar si el cliente cumple con ciertas condiciones de EPA. Si en un factor dado, el EPA falla y la última acción no contiene "Grupo de cuarentena", la autenticación se termina para ese usuario. Si existe un "Grupo de

© 1997–2026 Citrix Systems, Inc. All rights reserved.

cuarentena", la autenticación continúa y el administrador puede verificar el grupo para otorgar acceso limitado. Para obtener más detalles, consulte Ejecución de EPA.

**Política EPA:** En nFactor, todas las políticas se añaden con la misma sintaxis "add authentication policy". Sin embargo, el tipo de acción califica la política como una política EPA.

**Factor EPA:** El factor EPA es una etiqueta de política regular. No existe una entidad llamada factor EPA. Una vez que la política EPA se vincula a un factor, hereda ciertas propiedades que la convierten en un factor EPA.

**NOTA:**

El término "Factor EPA" se usa comúnmente en este documento para referirse a un factor con políticas EPA.

**EPA – Cuarentena:** Si en un factor dado, todas las expresiones de comprobación del dispositivo cliente de todas las acciones fallan, y si la última acción contiene “grupo de cuarentena”, ese grupo se añade a la sesión y se examina el nextFactor. Es decir, a pesar del fallo, la presencia del "grupo de cuarentena" califica la sesión para la siguiente etapa. Sin embargo, debido a la herencia de un grupo especial, el administrador puede relegar la sesión a acceso restringido o a políticas de autenticación adicionales como OTP o SAML.

Si no hay ningún grupo de cuarentena en la última acción, la autenticación finaliza con un error.

**EPA en nFactor también utiliza las siguientes entidades:**

- **LoginSchema:** Representación XML del formulario de inicio de sesión. Define la "vista" del formulario de inicio de sesión y también tiene propiedades de un "factor".
- **Etiqueta de política o factor de política:** Es una colección de políticas que se prueban en una etapa determinada de la autenticación.
- **Etiqueta de servidor virtual:** El servidor virtual también es una etiqueta de política a la que se pueden vincular políticas. Sin embargo, el servidor virtual es la colección de varias etiquetas de política, ya que es el punto de entrada para el acceso de los usuarios.
- **siguiente factor:** Se utiliza para especificar la etiqueta de política/factor que se debe tomar una vez que la política de autenticación dada tenga éxito.
- **Política NO_AUTHN:** Política especial cuya acción siempre tiene éxito.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Factor de paso:** Es una etiqueta de política/factor cuyo esquema de inicio de sesión no contiene vista. Es una indicación para el dispositivo NetScaler de que debe continuar la autenticación en el factor dado sin intervención del usuario.

Para obtener más información, consulte conceptos, entidades y terminología de nFactor.

### Exclusividad mutua del factor EPA

El factor EPA contiene una o más políticas EPA. Una vez que las políticas EPA se vinculan a un factor, las políticas de autenticación regulares no están permitidas en ese factor. Esta restricción es para ofrecer la mejor experiencia de usuario y una clara separación del análisis de puntos finales. La única excepción a esta regla es la política NO_AUTHN. Dado que la política NO_AUTHN es una política especial utilizada para simular un 'salto en caso de fallo', está permitida en el factor EPA.

### Ejecución de EPA

En cualquier factor dado (incluido el factor de servidor virtual), antes de servir el formulario de inicio de sesión, el dispositivo NetScaler comprueba si el factor está configurado para EPA. Si es así, envía una respuesta específica al cliente (UI) para que se active la secuencia EPA. Esta secuencia comprende la solicitud del cliente de expresiones de comprobación del dispositivo cliente y el envío de los resultados. Las expresiones de comprobación del dispositivo cliente para todas las políticas de un factor se envían a la vez al cliente. Una vez que se obtienen los resultados en el dispositivo NetScaler, cada una de las expresiones de todas las acciones se evalúa en una secuencia. La primera acción que da como resultado una EPA exitosa finaliza ese factor, y DefaultGroup, si está configurado, se hereda en la sesión. Si se encuentra una política NO_AUTHN, se califica como éxito automático. Si se especifica el nextFactor, el dispositivo continúa con ese factor. De lo contrario, la autenticación finaliza. Esta condición también es aplicable para el primer factor. Si no hay ningún factor de política de autenticación después de EPA en el servidor virtual, la autenticación se termina. Esto es diferente del comportamiento de la política clásica, donde al usuario siempre se le muestra la página de inicio de sesión después de EPA. Sin embargo, en caso de que no haya una política EPA exitosa, NetScaler Gateway examina el Grupo de Cuarentena configurado para la última política EPA en ese factor o cascada. Si la última política está configurada con el Grupo de Cuarentena, ese grupo se añade a la sesión y se inspecciona el nextFactor. Si existe un nextFactor, la autenticación procede a ese factor. De lo contrario, la autenticación se completa.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

### Configurar el análisis EPA para que se ejecute después de la autenticación

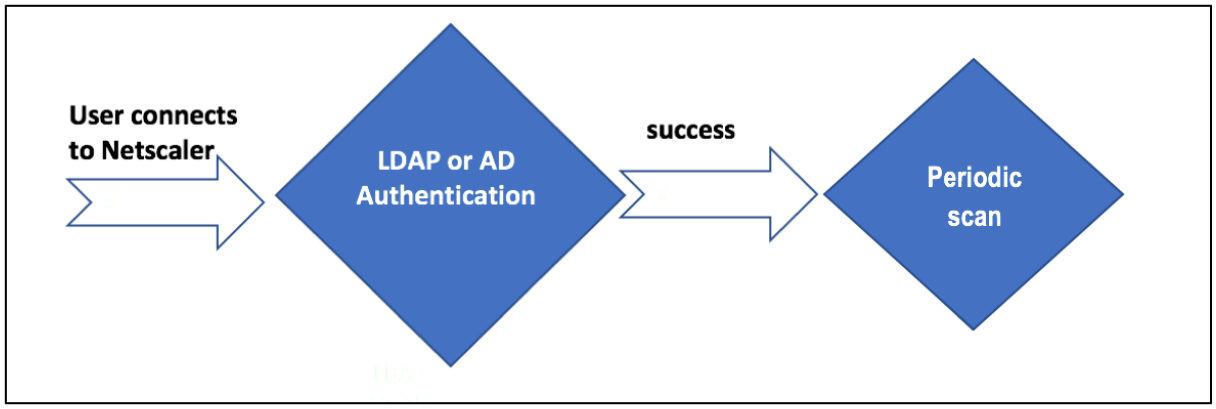
Puede configurar el escaneo EPA para que se ejecute después de la autenticación. En el siguiente ejemplo, el escaneo EPA se utiliza como una verificación final en una autenticación nFactor o multifactor. En esta configuración, si el escaneo EPA falla durante cualquiera de estas verificaciones, la sesión se termina.

**NOTA:**

Al configurar la autenticación nFactor con varias políticas EPA, se recomienda no posicionarlas secuencialmente, ya que esto podría dar lugar a múltiples solicitudes para que el usuario inicie el complemento EPA. En su lugar, se recomienda alternar las políticas EPA con otros métodos de autenticación.

**Ejemplos:**

- **Recomendado:** Factor EPA 1 > LDAP > Factor EPA 2
- **No recomendado:** LDAP > Factor EPA 1 > Factor EPA 2




- El usuario intenta conectarse a la IP virtual de NetScaler® Gateway.
- Se muestra al usuario una página de inicio de sesión con campos de nombre de usuario y contraseña para que proporcione sus credenciales. Con estas credenciales, se realiza una autenticación basada en LDAP o AD en el back-end. Si tiene éxito, se le presenta al usuario una ventana emergente para autorizar el escaneo EPA.
- Una vez que el usuario autoriza, se realiza el escaneo EPA y, en función del éxito o fracaso de la configuración del cliente del usuario, se proporciona el acceso.
- Si el escaneo es exitoso, el escaneo EPA se realiza periódicamente para verificar que los requisitos de verificación del dispositivo configurados aún se cumplen.
- Si el escaneo EPA falla durante cualquiera de estas verificaciones, la sesión se termina.

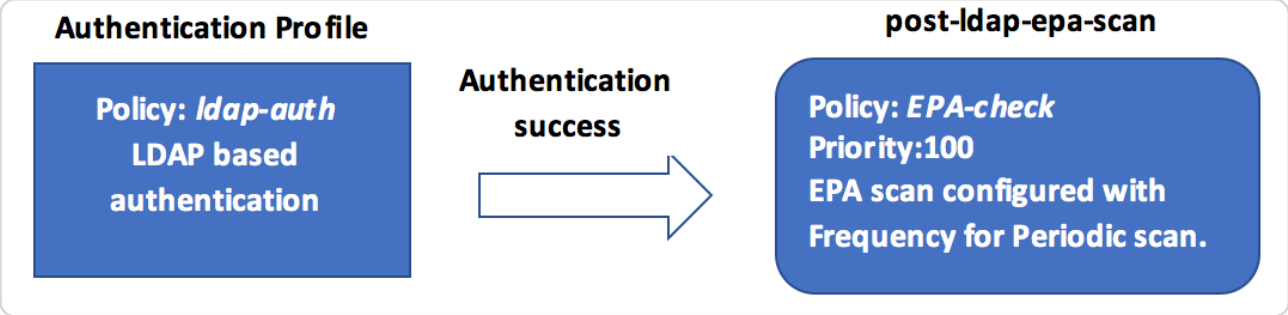
© 1997–2026 Citrix Systems, Inc. All rights reserved.

### Requisitos previos

Se asume que la siguiente configuración está implementada:

- Configuración del servidor virtual VPN, la puerta de enlace y el servidor virtual de autenticación
- Configuraciones del servidor LDAP y políticas asociadas.

La siguiente sección recoge las políticas y configuraciones de etiquetas de política requeridas, así como la asignación de políticas y etiquetas de política a un perfil de autenticación.




### En la CLI

1. Cree una acción para realizar un escaneo EPA antes de la autenticación LDAP y asóciela con una política de escaneo EPA.

   ```
   add authentication epaAction pre-ldap-epa-action -csecexpr
   "sys.client_expr (\"proc_2_firefox\")"



   add authentication Policy pre-ldap-epa-pol -rule true -action pre-ldap-
   epa-action
   ```

   La expresión anterior escanea si el proceso 'Firefox' se está ejecutando. El cliente EPA comprueba la existencia del proceso cada 2 minutos, lo que se indica con el dígito '2' en la expresión de escaneo.

2. Configure la etiqueta de política `pre-ldap-epa-label`, que aloja la política para el escaneo EPA.

   ```
   add authentication policylabel pre-ldap-epa-label -loginSchema
   LSCHEMA_INT
   ```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**NOTA:**

LSCHEMA_INT es un esquema integrado sin esquema (noschema), lo que significa que no se presenta ninguna página web adicional al usuario en este paso.

3. Asocie la política configurada en el paso 1 con la etiqueta de política configurada en el paso 2. Esto completa el mecanismo de autenticación.

```
bind authentication policylabel pre-ldap-epa-label -policyName pre-
ldap-epa-pol -priority 100 -gotoPriorityExpression END
```

4. Configure una acción y política LDAP.

```
add authentication ldapAction ldap-act -serverIP 192.0.2.0 -ldapBase
"dc=example,dc=net" -ldapBindDn user1@example.net -ldapBindDnPassword
1.cloud -ldapLoginName samAccountName -groupAttrName memberOf
-subAttributeName CN -passwdChange ENABLED



add authentication Policy ldap-pol -rule true -action ldap-act
```

5. Cree un esquema de inicio de sesión con SSO habilitado.

```
add authentication loginSchema ldap-schema -authenticationSchema "/
nsconfig/loginschema/LoginSchema/SingleAuth.xml" -SSOCredentials Yes
```

6. Configure la etiqueta de política `ldap-pol-label`, que aloja la política para la autenticación LDAP.

```
add authentication policylabel ldap-pol-label -loginSchema ldap-schema
```

7. Vincule el esquema de inicio de sesión configurado en el paso 5 a la etiqueta de política configurada en el paso 6.

```
bind authentication policylabel ldap-pol-label -policyName ldap-pol
-priority 100 -gotoPriorityExpression NEXT
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

8. Cree una acción para realizar un escaneo EPA después de la autenticación LDAP y asóciela con una política de escaneo EPA.

```
add authentication epaAction post-ldap-epa-action -csecexpr
"sys.client_expr (\"proc_2_chrome\")"



add authentication Policy post-ldap-epa-pol -rule true -action post-
ldap-epa-action



add authentication policylabel post-ldap-epa-label -loginSchema
LSCHEMA_INT



bind authentication policylabel post-ldap-epa-label -policyName post-
ldap-epa-pol -priority 100 -gotoPriorityExpression
```

9. Para resumir, asocie la política `pre-ldap-epa-pol` al servidor virtual de autenticación con el siguiente paso apuntando a la etiqueta de política `ldap-pol-label` para realizar un escaneo EPA.

```
bind authentication vserver user.auth.test -policy pre-ldap-epa-pol
-priority 100 -nextFactor ldap-pol-label -gotoPriorityExpression NEXT



bind authentication policylabel ldap-pol-label -policyName ldap-pol
-priority 100 -gotoPriorityExpression NEXT -nextFactor post-ldap-epa-
label
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**NOTA:**

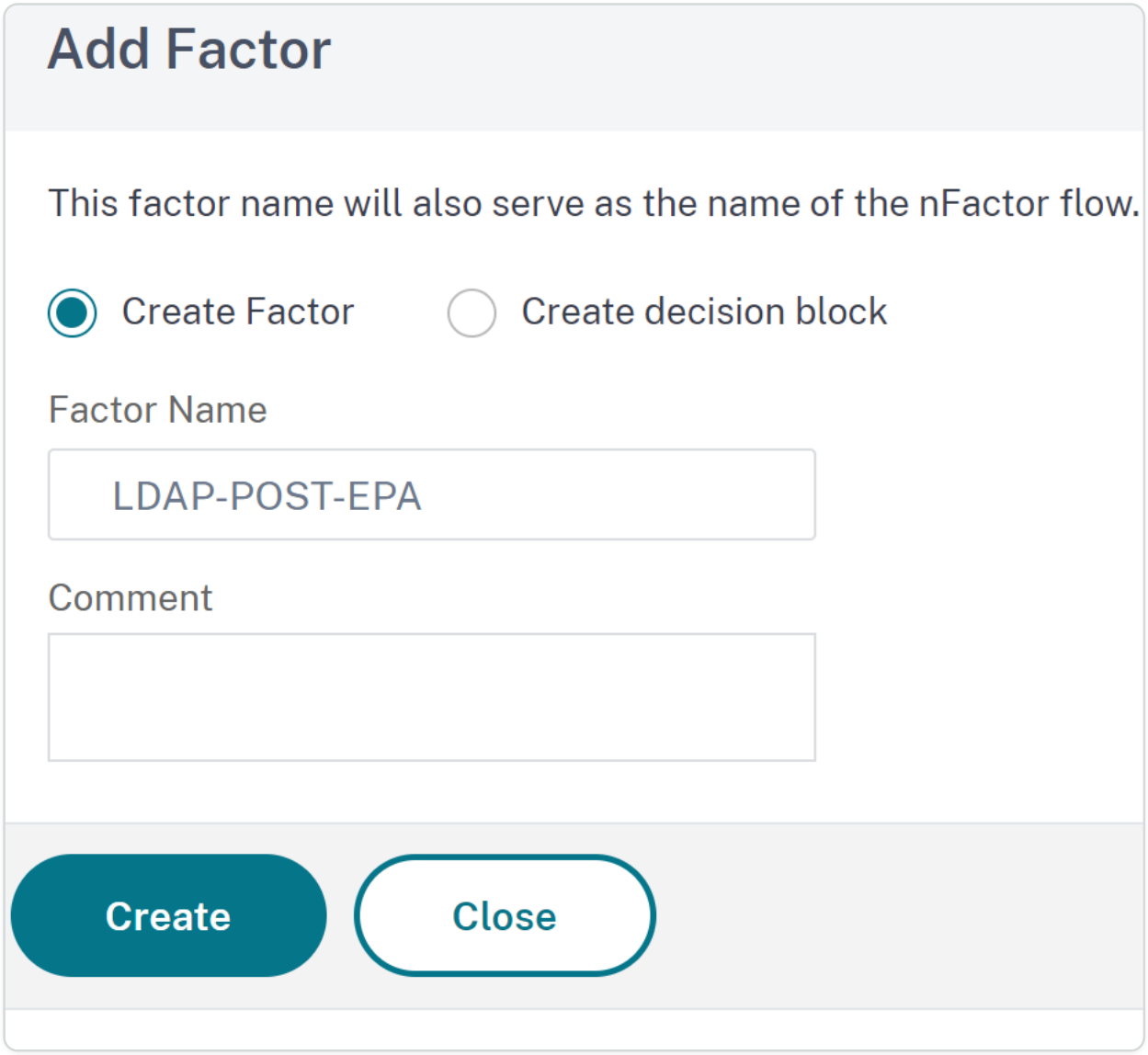
- En el EPA periódico configurado como múltiples factores, se considera el último factor con la configuración de EPA periódica.
- Los escaneos periódicos solo se pueden ejecutar utilizando el complemento EPA y no en el navegador.
- En el primer ejemplo, EPA es el primer factor donde el escaneo busca el proceso 'Firefox'.
- Si el escaneo EPA es exitoso, conduce a la autenticación LDAP, seguida del siguiente escaneo EPA, que busca el proceso 'Chrome'.
- Cuando se configuran múltiples escaneos periódicos como diferentes factores, el último escaneo tiene prioridad. En este caso, el complemento EPA escanea el proceso 'Chrome' cada 2 minutos después de que el inicio de sesión sea exitoso.

### En la GUI (mediante el Visualizador nFactor)

Puede configurar un escaneo EPA avanzado como un factor utilizando el visualizador nFactor en la GUI. En el siguiente ejemplo, hemos utilizado LDAP como primer factor y EPA como siguiente factor.

1. Cree un primer factor para el flujo nFactor.
    - Vaya a **Security > AAA-Application Traffic > nFactor Visualizer > nFactor Flows** y haga clic en **Add**.
    - Haga clic en **+** para añadir el flujo nFactor.
    - Añada un factor y haga clic en **Create**.

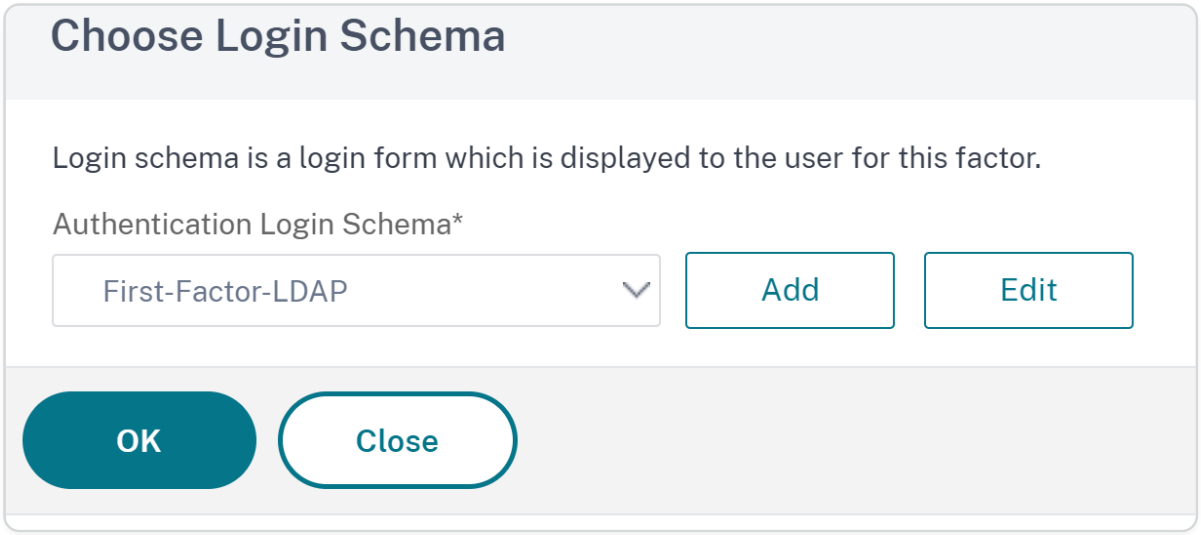
© 1997–2026 Citrix Systems, Inc. All rights reserved.




2. Cree un esquema de inicio de sesión y una política para el primer factor.

   - En el mosaico del primer factor, haga clic en **Agregar esquema** para agregar un esquema de inicio de sesión. Puede seleccionar un esquema de inicio de sesión de autenticación existente de la lista desplegable o crear un esquema de inicio de sesión.
   - Para crear un esquema de inicio de sesión de autenticación, haga clic en **Agregar**. Para obtener información detallada sobre el esquema de inicio de sesión de autenticación, consulte Configuración de la autenticación nFactor.

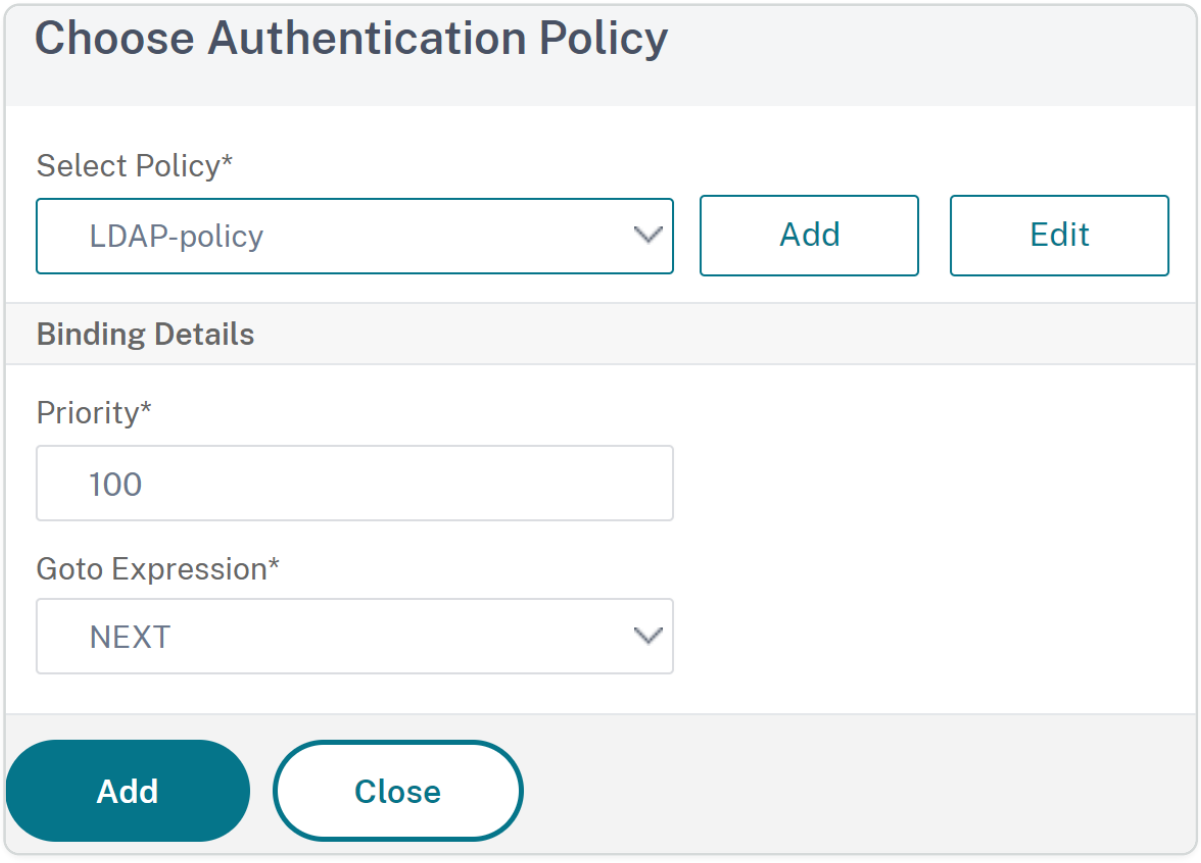
© 1997–2026 Citrix Systems, Inc. All rights reserved.




- Haga clic en **Agregar política** para agregar la política LDAP. Si la política LDAP ya está creada, puede seleccionarla. Haga clic en **Agregar**.

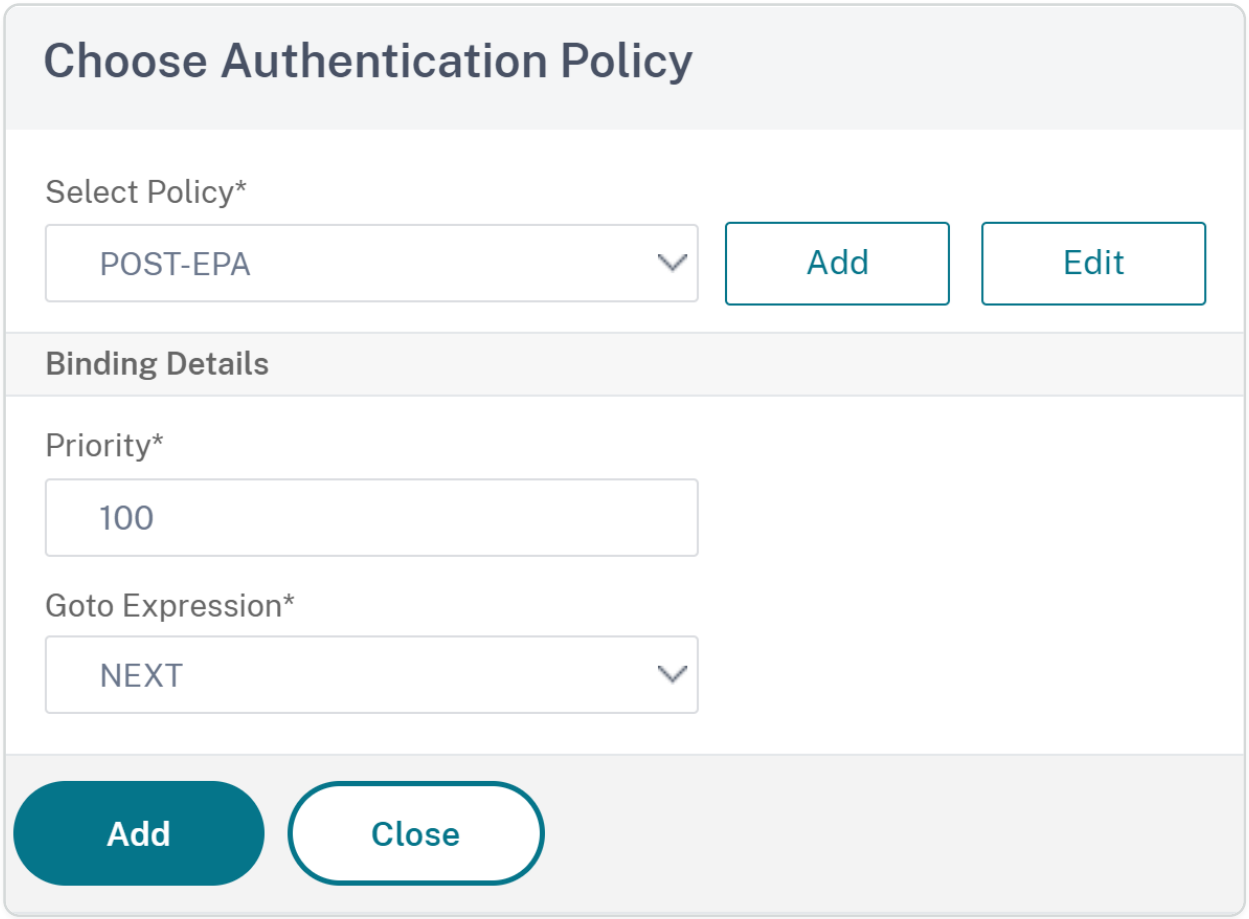
**NOTA:**

Si no se ha creado una política LDAP, puede crear una. Haga clic en el botón **Agregar** junto a la lista desplegable **Seleccionar política**. En el campo **Acción**, seleccione LDAP. Para obtener detalles sobre cómo agregar un servidor LDAP de autenticación, consulte `https://support.citrix.com/article/CTX123782`.




© 1997–2026 Citrix Systems, Inc. All rights reserved.

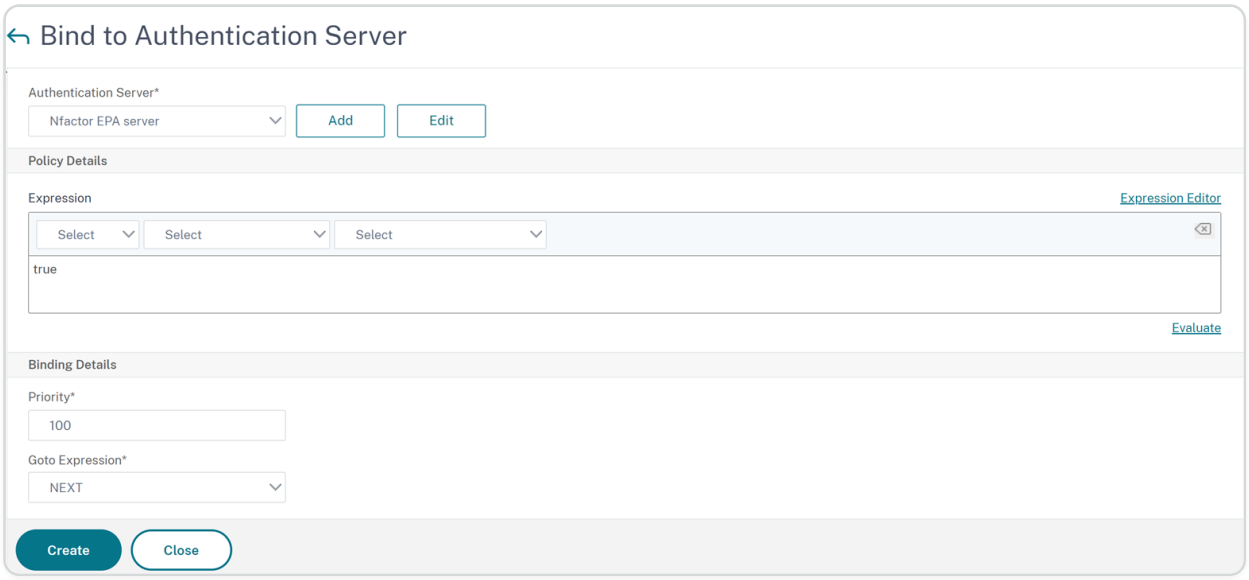
3. Cree un siguiente factor y conéctelo al primer factor.
    - Haga clic en el icono **+** de color verde o rojo para agregar EPA como el siguiente factor.
    - Cree el siguiente factor en la página **Siguiente factor a conectar**.
    - Deje la sección **Agregar esquema** en blanco para que no se aplique ningún esquema predeterminado a este factor.
4. Agregue una política para el siguiente factor.
    - Haga clic en **Agregar política** para agregar la política y acción de EPA posterior a la autenticación.
    - Puede elegir entre una lista existente de políticas o crear una política. Para elegir entre las políticas existentes, seleccione una política de la lista desplegable **Seleccionar política**, proporcione los detalles de enlace y haga clic en **Agregar**.
    - Para crear una política, haga clic en el botón **Agregar** junto a la lista desplegable **Seleccionar política**.




5. Una vez completado el flujo nFactor, haga clic en **Listo**.
6. Enlace el flujo nFactor a un servidor de autenticación.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Vaya a **Seguridad AAA - Tráfico de aplicaciones > Visualizador nFactor > Flujos nFactor**.
- Seleccione el nFactor y haga clic en **Enlazar a servidor de autenticación**.




### Referencias

- Conceptos, entidades y terminología de nFactor
- Cómo configurar la autenticación LDAP en NetScaler Gateway
- Autenticación LDAP
- Análisis avanzados de Endpoint Analysis

## Tipos de clasificación de análisis EPA en el cliente de Windows

**IMPORTANTE:**

El análisis de puntos finales está diseñado para analizar el dispositivo del usuario según criterios de cumplimiento predeterminados y no aplica ni valida la seguridad de los dispositivos del usuario final. Se recomienda utilizar sistemas de seguridad de puntos finales para proteger los dispositivos de ataques de administradores locales.

Los siguientes nuevos tipos de clasificación se añaden al análisis EPA para los parches que faltan. El análisis EPA falla si el cliente tiene alguno de los siguientes parches que faltan.

- Aplicación
- Conectores
- Actualizaciones críticas

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Actualizaciones de definición
- Kits de desarrollo
- Paquetes de características
- Guía
- Actualizaciones de seguridad
- Service Packs
- Herramientas
- Actualizaciones acumulativas
- Actualizaciones

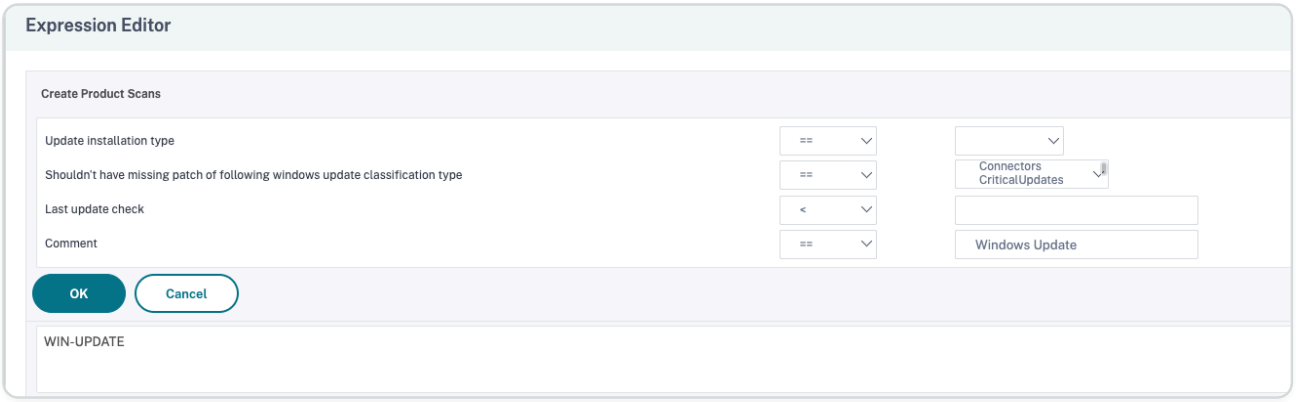
**NOTAS:**

- Anteriormente, los análisis de EPA para parches faltantes se realizaban según los niveles de gravedad: Crítico, Importante, Moderado y Bajo en el cliente de Windows.
- Si utiliza Citrix Secure Access para Windows 23.8.1.1 y versiones posteriores, el análisis `CLIENT.SYSTEM('WIN-UPDATE_SCAN-TIME')` se limita a las máquinas cliente que tienen las actualizaciones automáticas habilitadas. Si las actualizaciones automáticas están deshabilitadas, este análisis devuelve un resultado diferente.

### Configurar los tipos de clasificación de análisis de EPA mediante la GUI

1. Vaya a **NetScaler Gateway > Directivas > Preautenticación**.
2. Cree una nueva directiva de preautenticación o edite una existente.
3. Haga clic en el enlace **Editor de EPA de OPSWAT**.
4. En el Editor de expresiones, seleccione **Windows > Windows Update**.
5. En **No debería tener un parche faltante del siguiente nivel de seguridad**, seleccione el tipo de clasificación para los parches faltantes.
6. Haga clic en **Aceptar**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.




Los clientes pueden actualizar a la versión 4.3.2744.0s de OPSWAT para usar estas opciones.

### Referencias

- Para obtener detalles sobre los GUID de clasificación de los servicios de actualización de Windows Server, consulte `<https://docs.microsoft.com/es-es/previous-versions/windows/desktop/ff357803(v=vs.85)>`.
- Para la descripción de la terminología de las actualizaciones de software de Microsoft, consulte `<https://docs.microsoft.com/es-es/troubleshoot/windows-client/deployment/standard-terminology-software-updates>`.

## Análisis avanzados de Endpoint Analysis

El análisis avanzado de Endpoint Analysis (EPA) se utiliza para escanear los dispositivos de usuario en busca del requisito de seguridad de punto final configurado en NetScaler Gateway. Si un dispositivo de usuario intenta acceder a NetScaler Gateway, el dispositivo se escanea en busca de información de seguridad, como el sistema operativo, el antivirus, las versiones del navegador web, etc., antes de que un administrador pueda conceder acceso a NetScaler Gateway. Para obtener más información sobre los requisitos del sistema del cliente Citrix EPA, consulte Requisitos de Endpoint Analysis.

El análisis avanzado de EPA es un análisis basado en directivas que puede configurar en NetScaler Gateway para sesiones de autenticación. La directiva realiza una comprobación del registro en un dispositivo de usuario y, en función de la evaluación, la directiva permite o deniega el acceso a la red de NetScaler.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**IMPORTANTE:**

Los análisis de OPSWAT que requieren privilegios de administrador no son compatibles con los clientes Citrix EPA para Windows y macOS. Para verificar los análisis de OPSWAT compatibles, consulte la “Supported application list.xlsx” disponible en la página Citrix Downloads para la versión específica de las bibliotecas de OPSWAT en uso.

Si un calificador de análisis en el archivo "Supported application list.xlsx" está marcado como "FALSE", indica que el calificador de análisis de OPSWAT correspondiente no es compatible. En tales casos, se recomienda ajustar los análisis para usar configuraciones compatibles.
Puede configurar el análisis avanzado de EPA mediante la GUI o la CLI.

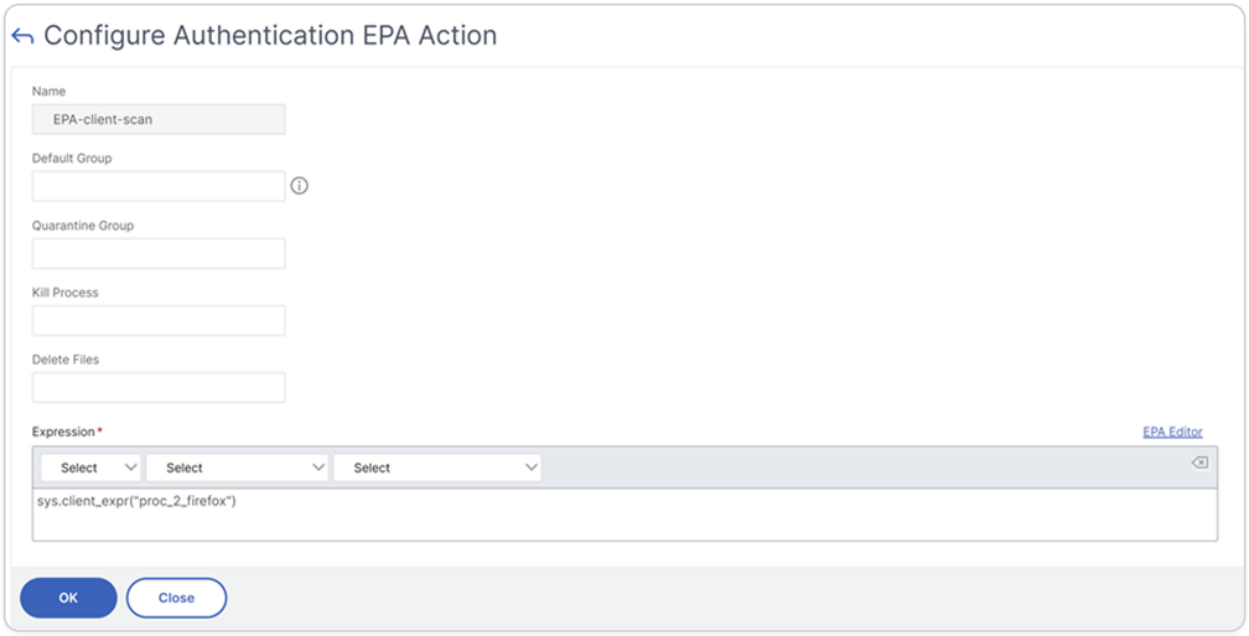
## En la GUI

1. Crear acción EPA.

   Vaya a **Security > AAA - Application Traffic > Policies > Authentication > Advanced Policies > Actions > EPA** y haga clic en **Add**. En la página **Create Authentication EPA Action**, actualice la siguiente información y haga clic en **Create**.

   - Nombre: Nombre de la acción EPA.
   - Grupo predeterminado: El grupo predeterminado que se elige cuando la comprobación de EPA se realiza correctamente.
   - Grupo de cuarentena: El grupo de cuarentena que se elige cuando la comprobación de EPA falla.
   - Terminar proceso: Cadena que especifica el nombre de un proceso que debe terminar el complemento EPA. Varios procesos deben separarse con comas.
   - Eliminar archivos: Cadena que especifica las rutas y los nombres de los archivos que debe eliminar el complemento EPA. Varios archivos deben separarse con comas.
   - Expresión: Consulte Referencia de expresiones de directivas de análisis avanzado de puntos finales para ver el formato de expresión de EPA.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

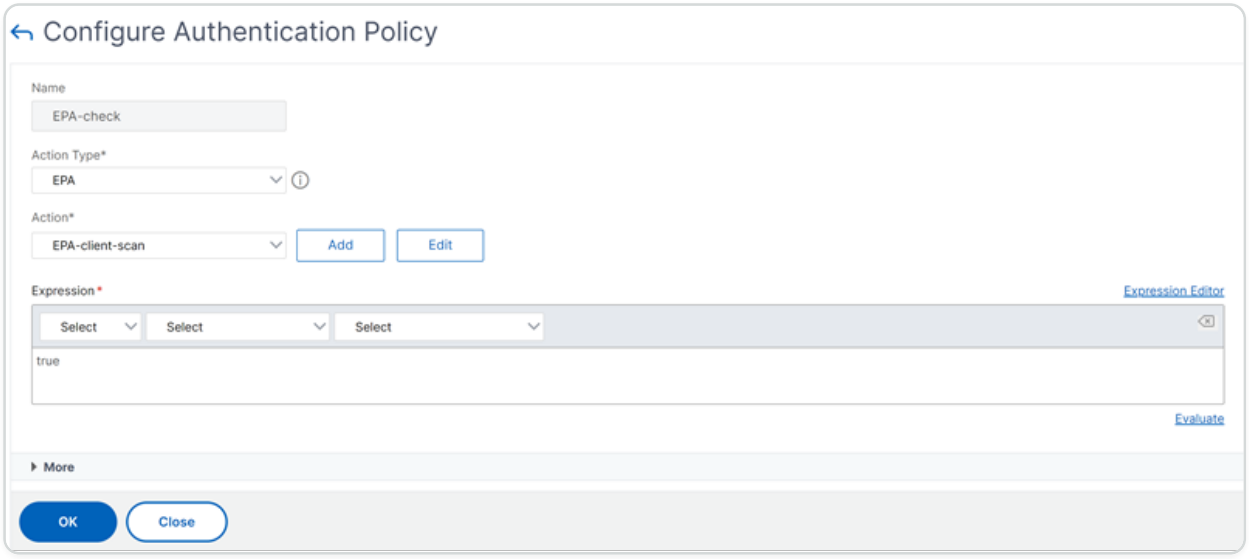



2. Cree una directiva EPA correspondiente.

   Vaya a **Seguridad > AAA - Tráfico de aplicaciones > Directivas > Autenticación > Directivas avanzadas > Directivas** y haga clic en **Agregar**. En la página **Crear directiva de autenticación**, actualice la siguiente información y haga clic en **Crear**.

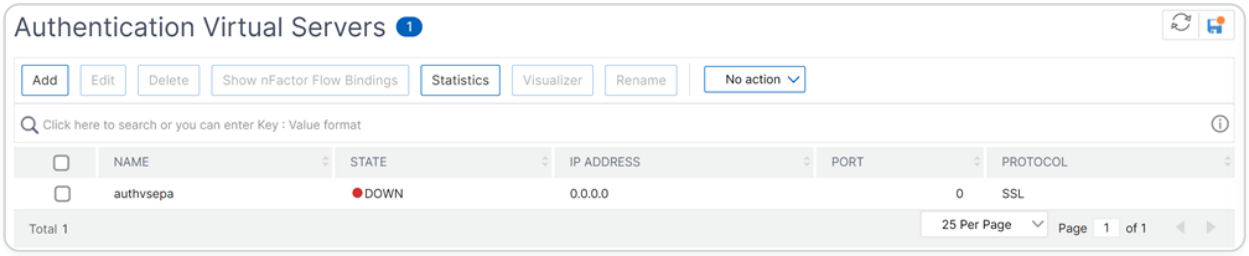
   - Nombre: Nombre de la directiva EPA avanzada.
   - Tipo de acción: Tipo de la acción de autenticación.
   - Acción: Nombre de la acción de autenticación que se realizará si la directiva coincide.
   - Expresión: Consulte Referencia de expresiones de directivas de análisis avanzado de puntos finales para ver el formato de expresión de EPA.
   - Acción de registro: Nombre de la acción de registro de mensajes que se utilizará cuando una solicitud coincida con esta directiva. La longitud máxima permitida es de 127 caracteres.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



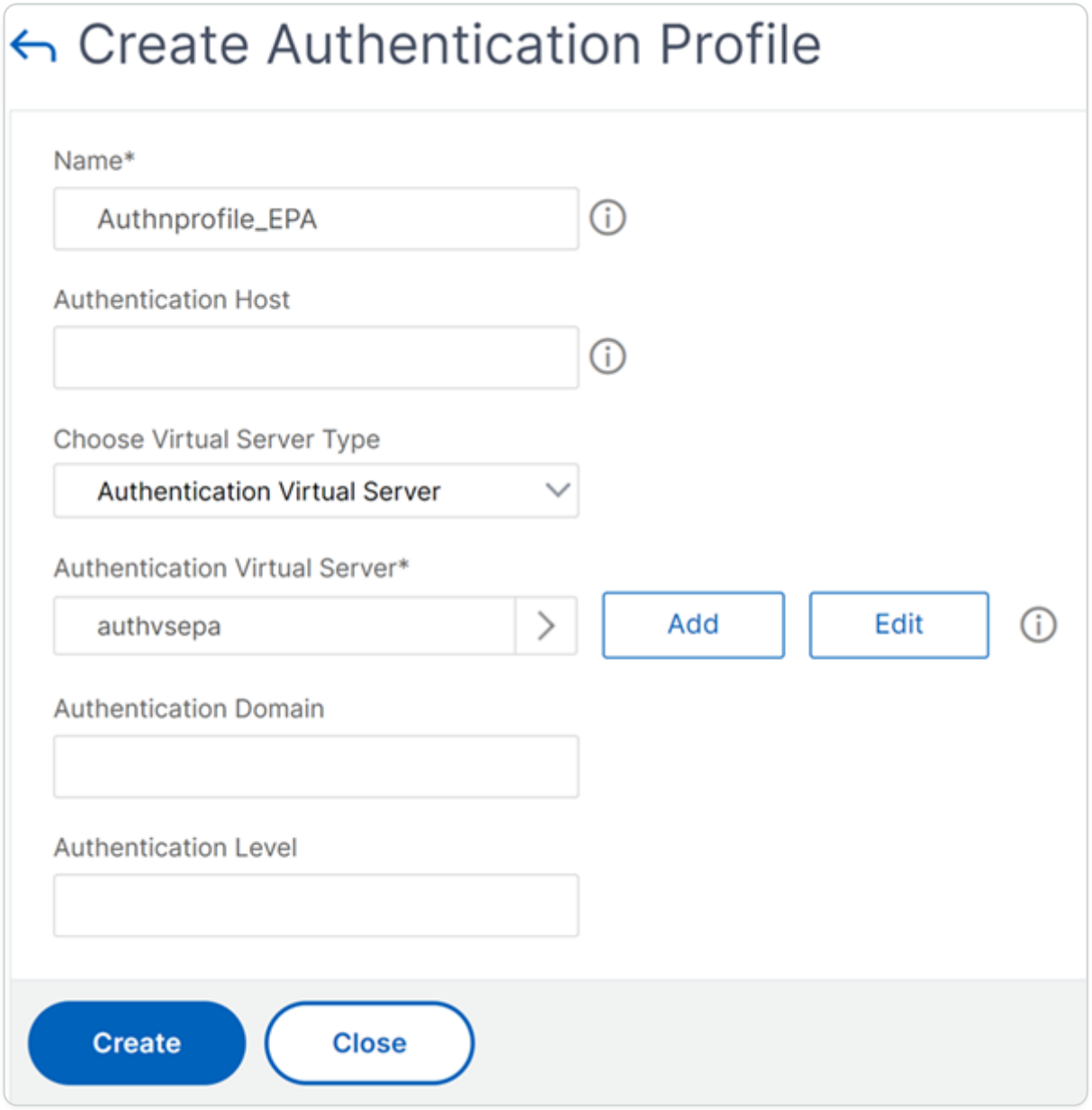

3. Configure un servidor virtual de autenticación y un perfil de autenticación.

   - Vaya a **Seguridad > AAA - Tráfico de aplicaciones > Servidores virtuales de autenticación** y haga clic en **Agregar**.




   - Vaya a **Seguridad > AAA - Tráfico de aplicaciones > Perfil de autenticación** y haga clic en **Crear**.

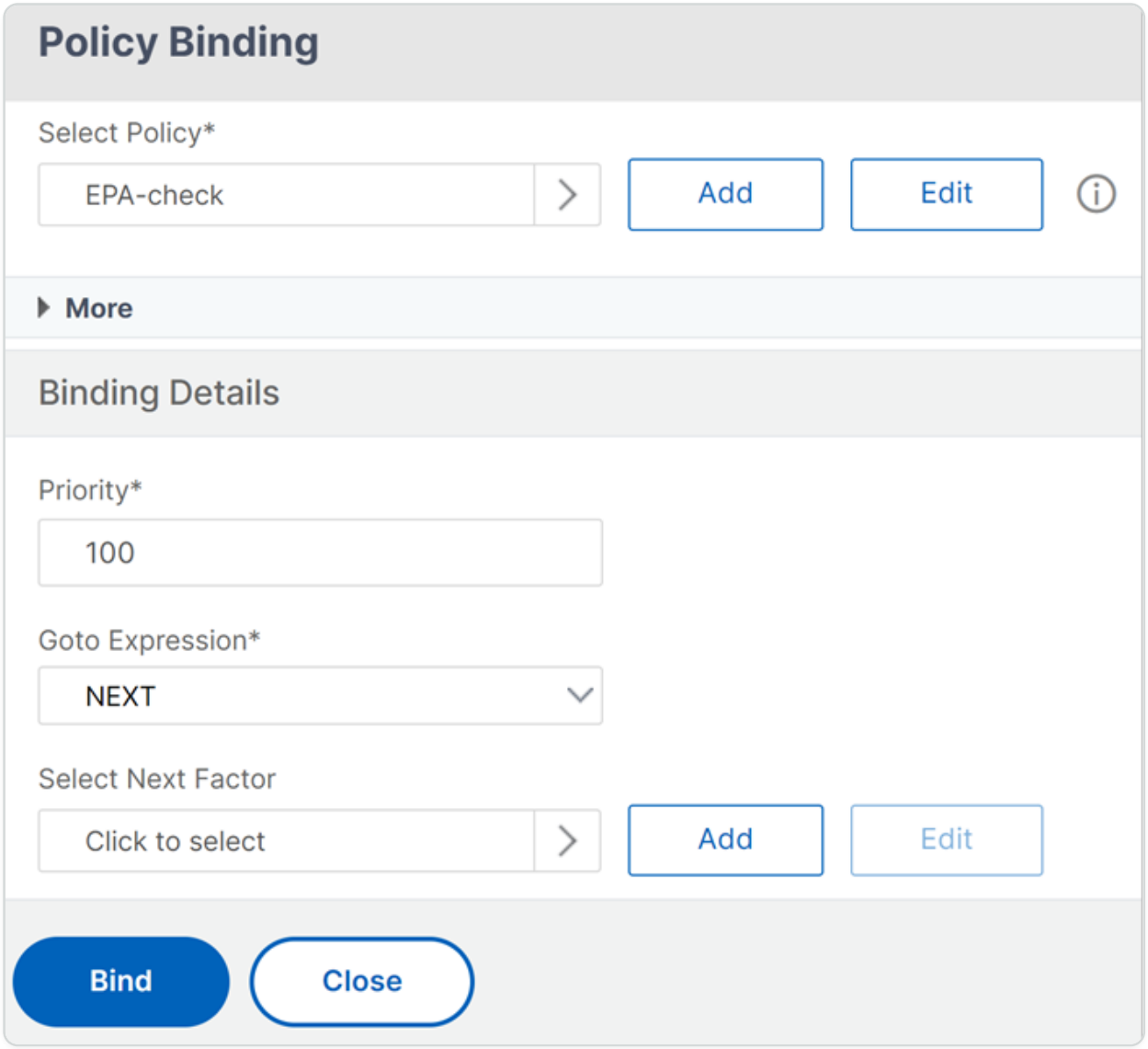
© 1997–2026 Citrix Systems, Inc. All rights reserved.




4. Vincule la política EPA avanzada al servidor virtual de autenticación.

   - Vaya a **Security > AAA – Application Traffic > Authentication Virtual Servers** y seleccione el servidor virtual de autenticación.
   - Seleccione la política en la sección **Advanced Authentication Policies**.
   - Haga clic en **Bind** en la sección **Policy Binding**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.




5. Vincule la política EPA al flujo nFactor.

   Para obtener más información sobre cómo agregar una política EPA avanzada como factor al flujo nFactor, consulte Escaneo EPA como factor en la autenticación nFactor.

## En la CLI

1. Cree una acción para realizar el escaneo EPA.

   ```
   add authentication epaAction EPA-client-scan -csecexpr "sys.client_expr
   (\"proc_2_firefox\")"
   ```

   La expresión anterior escanea si el proceso 'Firefox' se está ejecutando. El complemento EPA comprueba la existencia del proceso cada 2 minutos, lo que se indica con el dígito '2' en la expresión de escaneo.

2. Asocie la acción EPA a una política EPA avanzada.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
add authentication Policy EPA-check -rule true -action EPA-client-scan
```

3. Configure un servidor virtual de autenticación y un perfil de autenticación.

```
add authentication vserver authnvsepa ssl -ip address 192.0.2.0 -port
443
```

```
add Authnprofile_EPA -authnVsName authnvsepa
```

4. Vincule la política EPA avanzada al servidor virtual de autenticación.

```
bind authentication vs authnvsepa -policy EPA-check -pr 1
```

## Actualizar bibliotecas EPA

Para usar la GUI de NetScaler para actualizar las bibliotecas EPA:

1. Vaya a **Configuración > NetScaler Gateway > Actualizar componentes de cliente**.
2. En **Actualizar componentes de cliente**, haga clic en el enlace **Actualizar bibliotecas EPA**.
3. Elija el archivo requerido y haga clic en **Actualizar**.

**IMPORTANTE:**

- En una alta disponibilidad de NetScaler Gateway, las bibliotecas EPA deben actualizarse tanto en los nodos principal como secundario.
- En una configuración de clúster de NetScaler Gateway, las bibliotecas EPA deben actualizarse en todos los nodos del clúster.
- Si experimenta problemas después de actualizar la biblioteca EPA, no puede volver a una versión anterior. Póngase en contacto con Soporte de Citrix para obtener ayuda.

Para ver la lista de aplicaciones compatibles con Windows y MAC de OPSWAT para los análisis de NetScaler, consulte `<https://support.citrix.com/article/CTX234466>`.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

## Solución de problemas de análisis avanzados de Endpoint Analysis

Para ayudar con la solución de problemas de los análisis avanzados de Endpoint Analysis, los plug-ins de cliente escriben información de registro en un archivo en los sistemas de punto final del cliente. Estos archivos de registro se pueden encontrar en los siguientes directorios, según el sistema operativo del usuario.

**Windows Vista, Windows 7, Windows 8, Windows 8.1 y Windows 10:**

C:\\Users\\\<username\>\\AppData\\Local\\Citrix\\AGEE\\nsepa.txt

**Windows XP:**

C:\\Documentos y configuración\\Todos los usuarios\\Datos de programa\\Citrix\\AGEE\\nsepa.txt

**Sistemas Mac OS X:**

~/Library/Application Support/Citrix/EPAPlugin/epaplugin.log

(Donde el símbolo ~ indica la ruta del directorio de inicio del usuario de macOS correspondiente.)
(Donde el símbolo ~ indica la ruta del directorio de inicio del usuario de macOS correspondiente.)

**Ubuntu:**

- ~/.citrix/nsepa.txt
- ~/.citrix/nsgcepa.txt

## Análisis EPA para direcciones MAC

A partir de la versión 13.0-88.x de NetScaler, puede configurar las configuraciones de análisis EPA para las direcciones MAC permitidas o específicas. NetScaler utiliza expresiones de directiva y conjuntos de patrones para especificar la lista de direcciones MAC.

Antes de la versión 13.0-88.x de NetScaler, la lista de direcciones MAC permitidas debía definirse dentro de una expresión EPA. Para los clientes con un gran número de direcciones MAC permitidas, era engorroso incluir todas las direcciones MAC en una sola expresión. Además, existía una limitación en el número de direcciones MAC que se podían añadir en una sola expresión.

Por ejemplo,

© 1997–2026 Citrix Systems, Inc. All rights reserved.

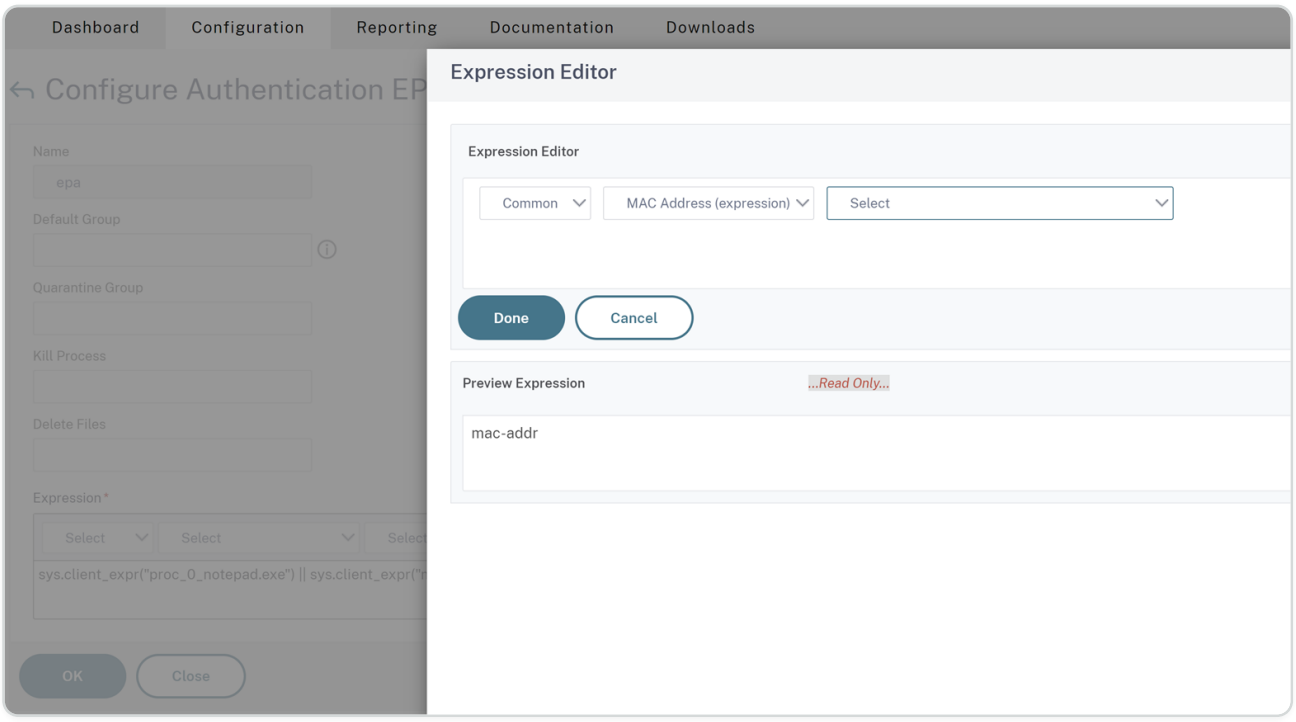
```
add authentication epaAction epa -csecexpr q/
sys.client_expr("proc_0_notepad.exe") || sys.client_expr("proc_0_chrome")
|| sys.client_expr("proc_0_firefox") &&
sys.client_expr("sys_0_MAC_ADDR_anyof_1AC89C83BOF7,0250F20A777C[COMMENT:
MAC Address]")/
```

### Configurar el análisis EPA para direcciones MAC mediante la GUI

La opción **Direcciones MAC (expresión)** que antes estaba disponible en la categoría de análisis de **Windows** ahora está disponible en la categoría de análisis **Común** de la GUI de NetScaler. Esta opción permite a los usuarios configurar un análisis EPA para una lista de direcciones MAC permitidas o específicas.

**NOTA:**

El cliente de Citrix Secure Access 22.10.1 y versiones posteriores admiten este método de NetScaler para gestionar las configuraciones de análisis EPA en la GUI.




1. Configure un conjunto de patrones. Para obtener más información, consulte Configuración de un conjunto de patrones.
2. Cree una expresión de directiva correspondiente para cada conjunto de patrones.

   Al configurar la expresión, en el Editor de expresiones, seleccione **AAA > LOGIN > CLIENT_MAC_ADDR > EQUAL_ANY(string) > Pattern Set**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Para obtener más información sobre cómo configurar una expresión avanzada, consulte Configurar expresiones de directiva avanzadas en una directiva.

3. Cree un análisis EPA para la expresión configurada en los pasos anteriores. Para obtener más información, consulte Análisis avanzados de Endpoint Analysis.

### Configurar el análisis EPA para direcciones MAC mediante la CLI

1. Almacene las direcciones MAC dentro de conjuntos de patrones.

   En el símbolo del sistema, escriba;

   ```
   add policy patset <name> [-comment <string>]
   ```

   Ejemplo:

   ```
   add policy patset patset1

   bind policy patset patset1 1A-C8-9C-83-BO-F7

   bind policy patset patset1 02-50-F2-0A-77-7C … and so on up to 3K
   entries.

   add policy patset patset2

   bind policy patset patset2 1A-2B-3C-4D-5E-6A

   bind policy patset patset2 1A-2B-3C-4D-5E-6B … and so on up to 3K
   entries.
   ```

2. Cree una expresión de directiva correspondiente para cada conjunto de patrones utilizando AAA.LOGIN.CLIENT_MAC_ADDR.equals_any()

   En el símbolo del sistema, escriba;

   ```
   Add policy expression <name> <value> [-comment <string>] [-
   clientSecurityMessage <string>]
   ```

   Ejemplo:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
add policy expression exp1
AAA.LOGIN.CLIENT_MAC_ADDR.equals_any("patset1")

add policy expression exp2
AAA.LOGIN.CLIENT_MAC_ADDR.equals_any("patset2")
```

3. Cree análisis EPA utilizando las expresiones de directiva configuradas

   En el símbolo del sistema, escriba;

   ```
   add authentication epaAction <name>  -csecexpr <expression>
   ```

   Ejemplo:

   ```
   add authentication epaAction epa -csecexpr q/
   sys.client_expr("proc_0_notepad.exe") ||
   sys.client_expr("proc_0_chrome")  || sys.client_expr("mac-addr_0_exp1")
   || sys.client_expr("mac-addr_0_exp2") ||
   sys.client_expr("proc_0_firefox")/
   ```

   Configure una directiva de preautenticación,

   ```
   add authentication Policy epapol -rule true -action epa
   ```

   Enlace la directiva de preautenticación,

   ```
   bind authentication vserver <name> -policy epapol -priority 10
   -gotoPriorityExpression NEXT
   ```

### Puntos a tener en cuenta

- La configuración de un análisis EPA para una lista permitida de direcciones MAC solo es aplicable para los flujos de autenticación nFactor.
- Se recomienda almacenar no más de 3000 entradas en un conjunto de patrones.
- Las direcciones MAC deben configurarse en el formato 1A-2B-3C-4D-5E-6F.
- El formato para el escaneo EPA es `mac-addr_0_<policy-expression-name>`. En este formato, `mac-addr_0_` es un valor estático y debe introducir el nombre de la expresión de la política después de `mac-addr_0_`.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Los escaneos EPA se pueden separar adecuadamente usando los símbolos `( ||, &&)`.
- Para añadir muchas direcciones MAC a un conjunto de patrones, puede utilizar la importación de conjuntos de patrones basada en archivos. Se recomienda almacenar un máximo de 3000 entradas/conjunto de patrones para un rendimiento óptimo.
- Si las direcciones MAC están presentes dentro de un archivo, puede crear un conjunto de patrones utilizando la importación de conjuntos de patrones basada en archivos y especificando el delimitador apropiado durante la importación.

### Limitaciones

- El escaneo EPA para direcciones MAC no es compatible con máquinas Linux.

### Referencias

- Configurar un conjunto de patrones.
- Crear un conjunto de patrones mediante importación basada en archivos.

## Referencia de expresiones de directiva de análisis avanzado de puntos finales

Este tema describe el formato y la construcción de las expresiones de análisis avanzado de puntos finales. La utilidad de configuración de NetScaler Gateway crea automáticamente los elementos de expresión que se incluyen aquí y no requiere configuración manual.

### Formato de expresión

Una expresión de análisis avanzado de puntos finales tiene el siguiente formato:

```
CLIENT.APPLICATION (SCAN-type_ Product-id_ Method-name _ Method-comparator_ Method-param _…)
```

Donde:

SCAN-type es el tipo de aplicación que se está analizando.

Product-id es la identificación del producto para la aplicación analizada.

Method-name es el atributo de producto o sistema que se está analizando.

Method-comparator es el comparador elegido para el análisis.

Method-param es el valor o los valores de atributo que se están analizando.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Ejemplo:

client.application(ANTIVIR_2600_RTP_==_TRUE)

**NOTA:**

Para los tipos de análisis que no son de aplicación, el prefijo de expresión es CLIENT.SYSTEM en lugar de CLIENT.APPLICATION.

### Cadenas de expresión

Cada uno de los tipos de análisis admitidos en el Análisis avanzado de puntos finales utiliza un identificador único en las expresiones. La siguiente tabla enumera las cadenas para cada tipo de análisis.

| TIPO DE ANÁLISIS | CADENA DE EXPRESIÓN DEL TIPO DE ANÁLISIS |
|---|---|
| Antiphishing | ANTIPHI |
| Antispyware | ANTISPY |
| Antivirus | ANTIVIR |
| Cliente de copia de seguridad | BACKUP |
| Control de acceso a dispositivos | DEV-CONT |
| Prevención de pérdida de datos | DATA-PREV |
| Uso compartido de escritorio | DESK-SHARE |
| Firewall | FIREWALL |
| Agente de estado | HEALTH |
| Cifrado de disco duro | HD-ENC |
| Mensajería instantánea | IM |
| Navegador web | BROWSER |
| P2P | P2P |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| TIPO DE ANÁLISIS | CADENA DE EXPRESIÓN DEL TIPO DE ANÁLISIS |
|---|---|
| Gestión de parches | PATCH |
| Filtrado de URL | URL-FILT |
| Dirección MAC (expresión) | MAC |
| Comprobación de dominio | DOMAIN |
| Análisis de registro | REG |

**NOTA:**

Para los análisis específicos de macOS X, las expresiones incluyen el prefijo MAC- antes del tipo de método. Por lo tanto, para los análisis de antivirus y antiphishing, los métodos son MAC-ANTIVIR y MAC-ANTIPHI, respectivamente.

Por ejemplo:
client.application(MAC-ANTIVIR_2600_RTP_==_TRUE)

### Métodos de análisis de aplicaciones

Al configurar expresiones de Análisis Avanzado de Puntos Finales, se utilizan métodos para definir los parámetros de los escaneos de puntos finales. Estos métodos incluyen un nombre de método, un comparador y un valor. Las siguientes tablas enumeran los métodos disponibles para su uso en expresiones.

#### Métodos de escaneo comunes:

Los siguientes métodos se utilizan para varios tipos de escaneos de aplicaciones.

| MÉTODO | DESCRIPCIÓN | COMPARADOR | VALORES POSIBLES |
|---|---|---|---|
| VERSION* | Especifica la versión de la aplicación. | <, <=, >, >=, !=, == | Cadena de versión |
| AUTHENTIC** | Comprueba si la aplicación es auténtica o no. | \== | TRUE |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| MÉTODO | DESCRIPCIÓN | COMPARADOR | VALORES POSIBLES |
|---|---|---|---|
| HABILITADO | Compruebe si la aplicación está habilitada. | \== | TRUE |
| EN EJECUCIÓN | Compruebe si la aplicación se está ejecutando. | \== | TRUE |
| COMENTARIO | Campo de comentario (ignorado por el análisis). Delimitado por [] dentro de las expresiones. | \== | Cualquier texto |

* La cadena VERSION puede especificar una cadena decimal de hasta cuatro valores, como 1.2.3.4.

** Una comprobación AUTHENTIC verifica la autenticidad de los archivos binarios de la aplicación.

**NOTA:**

Puede seleccionar una versión genérica para los tipos de análisis de aplicaciones. Cuando se seleccionan análisis genéricos, el ID de producto es 0.

Gateway ofrece una opción para configurar análisis genéricos para cada tipo de software. Mediante el análisis genérico, un administrador puede analizar la máquina cliente sin restringir la comprobación de análisis a ningún producto en particular.

Para los análisis genéricos, los métodos de análisis solo funcionan si el producto instalado en el sistema del usuario admite ese método de análisis. Para saber qué productos admiten un método de análisis en particular, póngase en contacto con el soporte de NetScaler®.

**Métodos de análisis únicos:**

Los siguientes métodos son únicos para los tipos de análisis especificados.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| MÉTODO | DESCRIPCIÓN | COMPARADOR | VALORES POSIBLES |
|---|---|---|---|
| ENABLED-FOR | Compruebe si el software antiphishing está habilitado para la aplicación seleccionada. | `allof, anyof,noneof` | **Para Windows**: Internet Explorer, Mozilla Firefox, Google Chrome, Opera, Safari. **Para Mac:** Safari, Mozilla Firefox, Google, Chrome, Opera |

Tabla 2. Antispyware y Antivirus

| MÉTODO | DESCRIPCIÓN | COMPARADOR | VALORES POSIBLES |
|---|---|---|---|
| RTP | Comprueba si la protección en tiempo real está activada o no. | \== | TRUE |
| SCAN-TIME | ¿Cuántos **minutos** han pasado desde que se realizó un análisis completo del sistema? | <, <=, >, >=, !=, == | Cualquier número positivo |
| VIRDEF-FILE-TIME | ¿Cuántos **minutos** han pasado desde que se actualizó el archivo de definición de virus (es decir, número de minutos entre la marca de tiempo del archivo de definición de virus y la marca de tiempo actual)? | <, <=, >, >=, !=, == | Cualquier número positivo |
| VIRDEF-FILE-VERSION | Versión del archivo de definición. | <, <=, >, >=, !=, == | Cadena de versión |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| MÉTODO | DESCRIPCIÓN | COMPARADOR | VALORES POSIBLES |
|---|---|---|---|
| ENGINE-VERSION | Versión del motor. | <, <=, >, >=, !=, == | Cadena de versión |

Tabla 3. Cliente de copia de seguridad

| MÉTODO | DESCRIPCIÓN | COMPARADOR | VALORES POSIBLES |
|---|---|---|---|
| LAST-BK-ACTIVITY | Número de **minutos** transcurridos desde que se completó la última actividad de copia de seguridad. | <, <=, >, >=, !=, == | Cualquier número positivo |

Tabla 4. Prevención de pérdida de datos

| MÉTODO | DESCRIPCIÓN | COMPARADOR | VALORES POSIBLES |
|---|---|---|---|
| HABILITADO | Comprueba si la aplicación está habilitada o no y si la protección de tiempo está activada o no. | \== | VERDADERO |

Tabla 5. Agente de comprobación de estado

| MÉTODO | DESCRIPCIÓN | COMPARADOR | VALORES POSIBLES |
|---|---|---|---|
| SYSTEM-COMPL | Comprobar si el sistema cumple con la normativa. | \== | VERDADERO |

Tabla 6. Cifrado de disco duro

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| MÉTODO | DESCRIPCIÓN | COMPARADOR | VALORES POSIBLES |
|---|---|---|---|
| ENC-PATH | RUTA para comprobar el estado del cifrado. | SIN OPERADOR | Cualquier texto |
| ENC-TYPE | Comprobar el tipo de cifrado para la ruta especificada. | `allof, anyof, noneof` | **Lista con las siguientes opciones**: UNENCRYPTED, PARTIAL, ENCRYPTED, VIRTUAL, SUSPENDED, PENDING |

Tabla 7. Navegador web

| MÉTODO | DESCRIPCIÓN | COMPARADOR | VALORES POSIBLES |
|---|---|---|---|
| DEFAULT | Comprobar si está configurado como navegador predeterminado. | \== | TRUE |

Tabla 8. Gestión de parches

| MÉTODO | DESCRIPCIÓN | COMPARADOR | VALORES POSIBLES |
|---|---|---|---|
| SCAN-TIME | Cuántos minutos han pasado desde que se realizó el último análisis del parche. | <, <=, >, >=, !=, == | Cualquier número positivo |
| MISSED-PATCH | Al sistema cliente no le faltan parches de estos tipos. | `anyof, noneof` | Cualquiera preseleccionado (parches preseleccionados en |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| MÉTODO | DESCRIPCIÓN | COMPARADOR | VALORES POSIBLES |
|---|---|---|---|
| | | | el servidor de Patch Manager) |

Tabla 9. Dirección MAC (expresión)

| MÉTODO | DESCRIPCIÓN | COMPARADOR | VALORES POSIBLES |
|---|---|---|---|
| ADDR | Compruebe si las direcciones MAC de la máquina cliente están o no en la lista proporcionada. | `anyof, noneof` | Lista editable |

Tabla 10. Pertenencia al dominio

| MÉTODO | DESCRIPCIÓN | COMPARADOR | VALORES POSIBLES |
|---|---|---|---|
| SUFFIX | Compruebe si la máquina cliente existe o no en la lista proporcionada. | `anyof, noneof` | Lista editable |

Tabla 11. Entrada de registro numérica

| MÉTODO | DESCRIPCIÓN | COMPARADOR | VALORES POSIBLES |
|---|---|---|---|
| PATH | Ruta para la comprobación del registro. En el formato: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Client\EnableAutoUpdate. No se requiere el escape de | SIN OPERADOR | Cualquier texto |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| MÉTODO | DESCRIPCIÓN | COMPARADOR | VALORES POSIBLES |
|---|---|---|---|
| | caracteres especiales. Todas las claves raíz del registro: HKEY_LOCAL_MACHINE, HKEY_CURRENT_USER, HKEY_USERS, HKEY_CLASSES_ROOT, HKEY_CURRENT_CONFIG | | |
| REDIR-64 | Seguir la redirección de 64 bits. Si se establece en TRUE, se sigue la redirección WOW (es decir, la ruta del Registro se comprueba en sistemas de 32 bits, pero la ruta redirigida por WOW se comprueba en sistemas de 64 bits). Si no se establece, no se sigue la redirección WOW (es decir, se comprueba la misma ruta del Registro para sistemas de 32 y 64 bits). Para las entradas del registro que no se redirigen, esta configuración no tiene ningún efecto. Consulte el | == | TRUE |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| MÉTODO | DESCRIPCIÓN | COMPARADOR | VALORES POSIBLES |
|---|---|---|---|
| | siguiente artículo para obtener la lista de claves de registro que se redirigen en sistemas de 64 bits: `http://msdn.microsoft.com/es-es/library/aa384253%28v=vs.85%29.aspx` | | |
| VALOR | Valor esperado para la ruta anterior. Este análisis solo funciona para tipos de registro REG_DWORD y REG_QWORD. | <, <=, >, >=, !=, == | Cualquier número |

## Administrar sesiones de usuario

Puede administrar las sesiones de usuario en la GUI de NetScaler desde el cuadro de diálogo **Sesiones de usuarios activos**. Este cuadro de diálogo muestra una lista de las sesiones de usuario activas en NetScaler Gateway. Puede ver las sesiones de usuario final o de grupo utilizando el nombre de usuario, el nombre de grupo o la dirección IP. También puede ver las sesiones activas dentro de este cuadro de diálogo. La información de la sesión incluye:

- Nombre de usuario
- Dirección IP del dispositivo de usuario
- Número de puerto del dispositivo de usuario
- Dirección IP del servidor virtual
- Número de puerto del servidor virtual
- Dirección IP de intranet asignada al usuario

© 1997–2026 Citrix Systems, Inc. All rights reserved.

# Administrar sesiones de usuario mediante la GUI

### Para ver las sesiones de usuario

1. En el panel de navegación de la GUI de NetScaler, haga clic en **NetScaler Gateway**.
2. En el panel de detalles, en Supervisar conexiones, haga clic en **Sesiones de usuario activas**.
3. En **Sesiones de usuario activas**, seleccione entre los siguientes tipos.
   - **Usuarios activos**
   - **Grupos activos**
   - **IP de intranet**- Cuando selecciona IP de intranet, debe introducir la dirección IP de intranet y la máscara de subred.
4. Haga clic en **Continuar**.

### Para actualizar la lista de sesiones

Puede recuperar información actualizada sobre las sesiones de NetScaler Gateway.

1. En el panel de navegación de la GUI de NetScaler, haga clic en **NetScaler Gateway**.
2. En el panel de detalles, en Monitor Connections, haga clic en **Sesiones de usuario activas**.
3. Haga clic en **Actualizar**.

### Para finalizar sesiones de usuario o de grupo o una sesión que tenga una dirección IP de intranet específica

Puede finalizar sesiones de usuario y de grupo. También puede finalizar una sesión que tenga una dirección IP de intranet y una máscara de subred específicas.

1. En el panel de navegación de la GUI de NetScaler, haga clic en **NetScaler Gateway**.
2. En el panel de detalles, en Monitor Connections, haga clic en **Sesiones de usuario activas**.
3. En Sesiones, seleccione un usuario, grupo o una sesión que tenga una dirección IP de intranet específica y, a continuación, haga clic en **Finalizar**.

# Administrar sesiones de usuario mediante la CLI

Puede utilizar los siguientes comandos de la CLI para ver sesiones de usuario, finalizar sesiones de usuario o de grupo.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- `show aaa session` - Muestra todas las conexiones de autenticación, autorización y auditoría de NetScaler o VPN que están vinculadas al usuario, grupo, dirección IP o rango de IP especificados.
- `show vpn icaConnection` - Muestra todas las conexiones activas que utilizan el proxy ICA.
- `show system session` - Muestra información sobre todas las sesiones actuales del sistema o sobre la sesión especificada.

# Inicio de sesión automático de Windows

La funcionalidad de inicio de sesión automático de Windows permite que el cliente de Citrix Secure Access establezca un túnel con NetScaler automáticamente una vez que el usuario inicia sesión en la máquina Windows. Los métodos de autenticación que admiten la funcionalidad de inicio de sesión automático de Windows son LDAP y Kerberos.

## Configurar el inicio de sesión automático de Windows mediante la CLI

Puede configurar el inicio de sesión automático de Windows mediante el siguiente comando de la CLI:

```
set vpn parameter -windowsAutoLogon ON
```

## Inicio de sesión automático con autenticación Kerberos

A partir de las versiones 23.10.1.7 y posteriores del cliente de Citrix Secure Access para Windows, puede utilizar el método de autenticación Kerberos para el inicio de sesión automático.

Con este método de autenticación, el SSO de Kerberos de back-end funciona sin problemas sin que el administrador tenga que enviar configuraciones de URL de back-end adicionales a las máquinas cliente. Además, la URL de Gateway se añade automáticamente en la sección **Propiedades de Internet > Sitios de confianza** de las máquinas cliente.

### Requisitos previos

- **Configuraciones de administrador**: Si la autenticación Kerberos está configurada en NetScaler con `windowsAutoLogon` establecido en ON, el método de autenticación Kerberos se habilita automáticamente con NetScaler. Para obtener más información, consulte Configuración de la autenticación Kerberos en el dispositivo NetScaler.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Los administradores también deben configurar la autenticación Kerberos en sus máquinas cliente. Para obtener más información, consulte Configurar la autenticación Kerberos en un cliente.

- **Configuraciones de usuario final**: Los usuarios finales deben tener Microsoft Edge WebView habilitado en el cliente de Citrix Secure Access. Para obtener más información, consulte Compatibilidad de Microsoft Edge WebView con Citrix Secure Access para Windows.

### Configurar la autenticación Kerberos con el cliente Citrix Secure Access™

Para configurar la autenticación Kerberos con el cliente de Citrix Secure Access, los administradores deben establecer la clave de registro del cliente VPN `EnableKerberosAuth`. Para obtener más información sobre la clave de registro de VPN, consulte Claves de registro del cliente VPN de NetScaler Gateway para Windows.

### Referencias

- Paso de dominio a Citrix Workspace usando Citrix Gateway local como proveedor de identidades
- Cómo configurar NetScaler para la delegación restringida de Kerberos

# Always On

La función Always On de NetScaler Gateway garantiza que los usuarios estén siempre conectados a la red empresarial. Esta conectividad VPN persistente se logra mediante el establecimiento automático de un túnel VPN.

**NOTA**

La función Always On admite portales cautivos para NetScaler 12.0 Build 51.24 y versiones posteriores.

## Cuándo usar Always On

Use Always On cuando necesite proporcionar conectividad VPN sin interrupciones según la ubicación del usuario y deba evitar el acceso a la red por parte de un usuario que no esté conectado a una VPN.

Los siguientes escenarios ilustran el uso de Always On.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Un empleado inicia el portátil fuera de la red empresarial y necesita ayuda para establecer la conectividad VPN.

  **Solución:** Cuando el portátil se inicia fuera de la red empresarial, Always On establece un túnel sin problemas y proporciona conectividad VPN.
- Un empleado que utiliza conectividad VPN se traslada a la red empresarial. El empleado se cambia a una red empresarial, pero permanece conectado al túnel VPN, lo cual no es un estado deseable.

  **Solución:** Cuando el empleado se traslada a la red empresarial, Always On desactiva el túnel VPN y cambia sin problemas al empleado a la red empresarial.
- Un empleado se traslada fuera de la red empresarial y cierra el portátil (no lo apaga). El empleado necesita ayuda para establecer la conectividad VPN al reanudar el trabajo en el portátil.

  **Solución:** Cuando el empleado se traslada fuera de la red empresarial, Always On establece un túnel sin problemas y proporciona conectividad VPN.
- Una empresa quiere regular el acceso a la red que se proporciona a sus usuarios cuando no están conectados a un túnel VPN.

  **Solución:** Dependiendo de la configuración, Always On restringe el acceso, permitiendo a los usuarios acceder solo a la red de la puerta de enlace.

## Descripción del marco de Always On

Always On conecta automáticamente a un usuario a un túnel VPN que el cliente ha establecido previamente. La primera vez que el usuario necesita un túnel VPN, debe conectarse a la URL de NetScaler Gateway y establecer el túnel. Una vez que la configuración de Always On se descarga en el cliente, esta configuración impulsa el establecimiento posterior del túnel.

El ejecutable del cliente Citrix Secure Access™ siempre se está ejecutando en la máquina cliente. Cuando el usuario inicia sesión o la red cambia, el cliente Citrix Secure Access determina si el portátil del usuario está en la red empresarial. Dependiendo de la ubicación y la configuración, el cliente Citrix Secure Access establece un túnel o desactiva un túnel existente.

El establecimiento del túnel se inicia solo después de que el usuario inicia sesión en el equipo. El cliente Citrix Secure Access utiliza las credenciales de la máquina cliente para autenticarse con el servidor de la puerta de enlace e intenta establecer un túnel.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

### Restablecimiento automático de un túnel

El restablecimiento automático de un túnel se activa cuando NetScaler Gateway interrumpe un túnel VPN.

**NOTA**

Cuando el análisis de puntos finales falla, el cliente de NetScaler Gateway no vuelve a intentar establecer el túnel, pero muestra un mensaje de error. Si hay un error de autenticación, el cliente de NetScaler Gateway solicita al usuario las credenciales.

### Métodos de autenticación de usuario admitidos para el establecimiento de túneles sin interrupciones

Los métodos de autenticación de usuario admitidos son los siguientes:

- Nombre de usuario + contraseña de AD: Si se utilizan el nombre de usuario y la contraseña de Windows para la autenticación, el cliente de Citrix Secure Access establece el túnel sin problemas utilizando estas credenciales.
- Certificado de usuario: Si se utiliza un certificado de usuario para la autenticación y solo hay un certificado en la máquina cliente, el cliente de Citrix Secure Access establece un túnel sin problemas utilizando este certificado. Si se instalan varios certificados de cliente, el túnel se establece después de que el usuario haya seleccionado el certificado preferido. El cliente de Citrix Secure Access utiliza este certificado preferido para túneles posteriores.

  Si las tarjetas inteligentes comparten un certificado de usuario, no se puede lograr el inicio de sesión automático si los certificados se instalan dinámicamente en el almacén en comparación con los certificados que ya están presentes en el almacén.
- Certificado de usuario y nombre de usuario + contraseña de AD: Este método de autenticación es la combinación de los métodos de autenticación descritos anteriormente.

**NOTA**

Todos los demás mecanismos de autenticación son compatibles, pero el establecimiento del túnel no es fluido para ningún otro método de autenticación.

### Requisitos de configuración para Always On

El administrador de la empresa debe aplicar lo siguiente para los dispositivos administrados:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- El usuario no debe poder finalizar el proceso/servicio para una configuración específica
- El usuario no debe poder desinstalar el paquete para una configuración específica.
- El usuario no debe poder cambiar entradas de registro específicas.

**NOTA**

Es posible que la función no funcione como se espera si el usuario tiene privilegios de administración, como en el caso de dispositivos no administrados.

## Consideraciones al habilitar la función Always On

Revise la siguiente sección antes de habilitar la función Always On.

Acceso a la red principal: Cuando se establece el túnel, el tráfico a la red empresarial se decide en función de la configuración de túnel dividido. No se proporcionan otras configuraciones para anular este comportamiento.

Configuración del proxy de la máquina cliente: La configuración del proxy de la máquina cliente se ignora para conectarse al servidor de la puerta de enlace.

**NOTA**

La configuración del proxy del dispositivo NetScaler no se ignora. Solo se ignoran las configuraciones de proxy de la máquina cliente. Los usuarios que tienen un proxy configurado en sus sistemas reciben una notificación de que el complemento VPN ha ignorado su configuración de proxy.

## Configuración de Always On

Para configurar Always On, cree un perfil Always On en el dispositivo NetScaler Gateway y aplique el perfil.

Para crear un perfil Always On:

1. En la GUI de NetScaler, vaya a **Configuration > NetScaler Gateway > Policies > AlwaysON.**
2. En la página **AlwaysON Profiles**, haga clic en **Add**.
3. En la página **Crear perfil AlwaysON**, introduzca los siguientes detalles:
    - **Nombre** – El nombre de su perfil.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **VPN basada en la ubicación (nombre de registro del lado del cliente: LocationDetection) – Seleccione una de las siguientes configuraciones:
  - **Remoto** para permitir que un cliente detecte si está en la red empresarial y establezca el túnel si no lo está. Remoto es la configuración predeterminada.
  - **En todas partes** para permitir que un cliente omita la detección de ubicación y establezca el túnel independientemente de la ubicación del cliente.
- **Control de cliente** – Seleccione una de las siguientes configuraciones:
  - **Denegar** para evitar que el usuario cierre sesión y se conecte a otra puerta de enlace. Denegar es la configuración predeterminada.
  - **Permitir** para que el usuario pueda cerrar sesión y conectarse a otra puerta de enlace.
- **Acceso a la red en caso de fallo de VPN (nombre de registro del lado del cliente: AlwaysOn)** – Seleccione una de las siguientes configuraciones:
  - **Acceso completo** para permitir que el tráfico de red fluya hacia y desde el cliente cuando el túnel no está establecido. Acceso completo es la configuración predeterminada.
  - **Solo a la puerta de enlace** para evitar que el tráfico de red fluya hacia o desde el cliente cuando el túnel no está establecido. Sin embargo, se permite el tráfico hacia o desde la dirección IP de la puerta de enlace.

    **Nota:** En el modo **Solo a la puerta de enlace**, solo se desbloquea el tráfico del servidor virtual, DNS y DHCP. Para desbloquear otros sitios web, rangos de direcciones IP o direcciones IP, debe configurar el registro **AlwaysOnAllowlist** con una lista de FQDN, rangos de direcciones IP o direcciones IP separados por punto y coma. Por ejemplo, mycompany.com,mycdn.com,10.120.67.0-10.120.67.255,67.67.67.67

4. Haga clic en **Crear** para finalizar la creación de su perfil.

Para aplicar el perfil Always On:

1. En la interfaz de NetScaler, seleccione **Configuración > NetScaler Gateway > Configuración global**.
2. En la página Configuración global, haga clic en el enlace **Cambiar configuración global** y, a continuación, seleccione la ficha **Experiencia del cliente**.
3. En el menú desplegable **Nombre de perfil de AlwaysON**, seleccione el perfil recién creado y haga clic en **Aceptar**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**Nota:** Se puede realizar una configuración similar en el perfil de sesión para aplicar las directivas a nivel de grupo, nivel de servidor o nivel de usuario.

## Nota sobre las IIP

El túnel a nivel de máquina utiliza autenticación basada en certificados y la sesión que se crea tiene el nombre común del certificado como nombre de usuario. Por lo tanto, si los certificados de dispositivo tienen nombres comunes únicos, las sesiones de diferentes máquinas tienen nombres de usuario diferentes y, por lo tanto, diferentes IIP. Asegúrese de generar un certificado de dispositivo con nombres únicos. Idealmente, debe usar los nombres de las máquinas como nombre común del certificado del dispositivo.

### Resumen del comportamiento de diferentes configuraciones para usuarios administradores y no administradores

La siguiente tabla resume el comportamiento de las diferentes configuraciones. También detalla la posibilidad de ciertas acciones del usuario, que pueden afectar la funcionalidad de Always On.

| NETWORKACCESS ONVPNFAILURE | CONTROL DEL CLIENTE | USUARIO NO ADMINISTRADOR | USUARIO ADMINISTRADOR |
|---|---|---|---|
| `fullaccess` | Permitir | El túnel se establece automáticamente. El usuario puede cerrar sesión y permanecer fuera de la red. El usuario también puede apuntar a otra NetScaler Gateway. | El túnel se establece automáticamente. El usuario puede cerrar sesión y permanecer fuera de la red empresarial. El usuario también puede apuntar a otra NetScaler Gateway. |
| `fullaccess` | Denegar | El túnel se establece automáticamente. El usuario no puede cerrar sesión ni apuntar a otra NetScaler Gateway. | El túnel se establece automáticamente. El usuario puede desinstalar el cliente Citrix Secure Access o moverse a otra NetScaler Gateway. |
| onlyToGateway | Permitir | El túnel se establece automáticamente. El usuario puede cerrar sesión (sin acceso a | El túnel se establece automáticamente. El usuario puede desinstalar el cliente |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| NETWORKACCESS ONVPNFAILURE | CONTROL DEL CLIENTE | USUARIO NO ADMINISTRADOR | USUARIO ADMINISTRADOR |
|---|---|---|---|
| | | la red). El usuario también puede apuntar a otra NetScaler Gateway, en cuyo caso, el acceso se concede únicamente a la NetScaler Gateway recién apuntada. | Citrix Secure Access o moverse a otra NetScaler Gateway. |
| onlyToGateway | Denegar | El túnel se establece automáticamente. El usuario no puede cerrar sesión ni apuntar a otra NetScaler Gateway. | El túnel se establece automáticamente. El usuario puede desinstalar el cliente Citrix Secure Access o moverse a otra NetScaler Gateway. |

## Permitir URL seleccionadas cuando Always On está inactivo

Los usuarios pueden acceder a algunos sitios web incluso cuando Always On está inactivo y la red está bloqueada. Los administradores pueden usar el registro **AlwaysOnAllowlist** para agregar los sitios web a los que desea habilitar el acceso cuando Always On está inactivo.

**NOTA:**

- El registro **AlwaysOnAllowlist** es compatible a partir de la versión 13.0 compilación 47.x y posteriores.
- La ubicación del registro **AlwaysOnAllowlist** es Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Client.
- Las URL/FQDN con comodines no son compatibles en el registro **AlwaysOnAllowlist**.

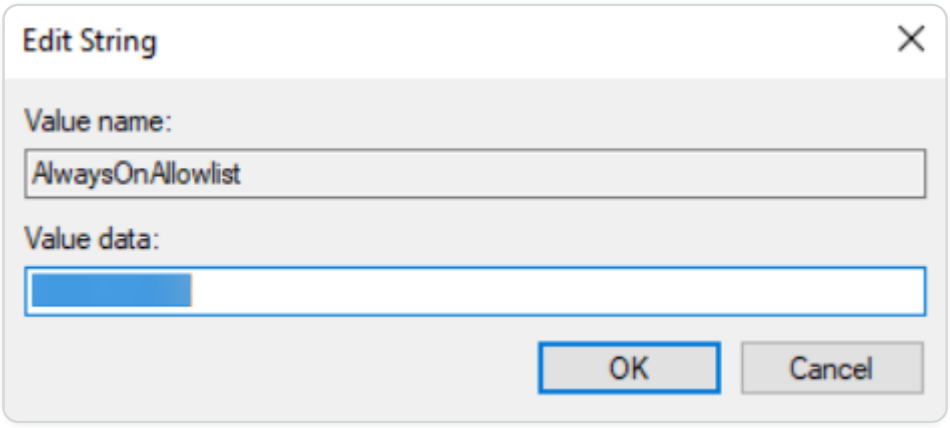
### Para configurar el registro AlwaysOnAllowlist

Configure el registro **AlwaysOnAllowlist** con una lista de FQDN, rangos de direcciones IP o direcciones IP, separada por punto y coma, a los que desea permitir el acceso.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**Ejemplo:** example.citrix.com;192.0.2.0;192.0.2.100-192.0.2.255

La siguiente figura muestra un registro **AlwaysOnAllowlist** de ejemplo.




# Always On VPN antes del inicio de sesión de Windows (formalmente servicio Always On)

La función **AlwaysOn VPN antes del inicio de sesión de Windows** (formalmente servicio Always On) permite a un usuario establecer un túnel VPN a nivel de máquina incluso antes de que un usuario inicie sesión en un sistema Windows. El túnel permanece activo hasta que la máquina se apaga. Después de que el usuario inicia sesión, el túnel VPN a nivel de máquina es asumido por un túnel VPN a nivel de usuario. Después de que el usuario cierra sesión, el túnel a nivel de usuario se desactiva y se establece un túnel a nivel de máquina. **Always On VPN antes del inicio de sesión de Windows** solo se puede configurar utilizando políticas de autenticación avanzadas. Para obtener más detalles, consulte Configurar Always On VPN antes del inicio de sesión de Windows.

## Capacidades de Always On VPN antes del inicio de sesión de Windows

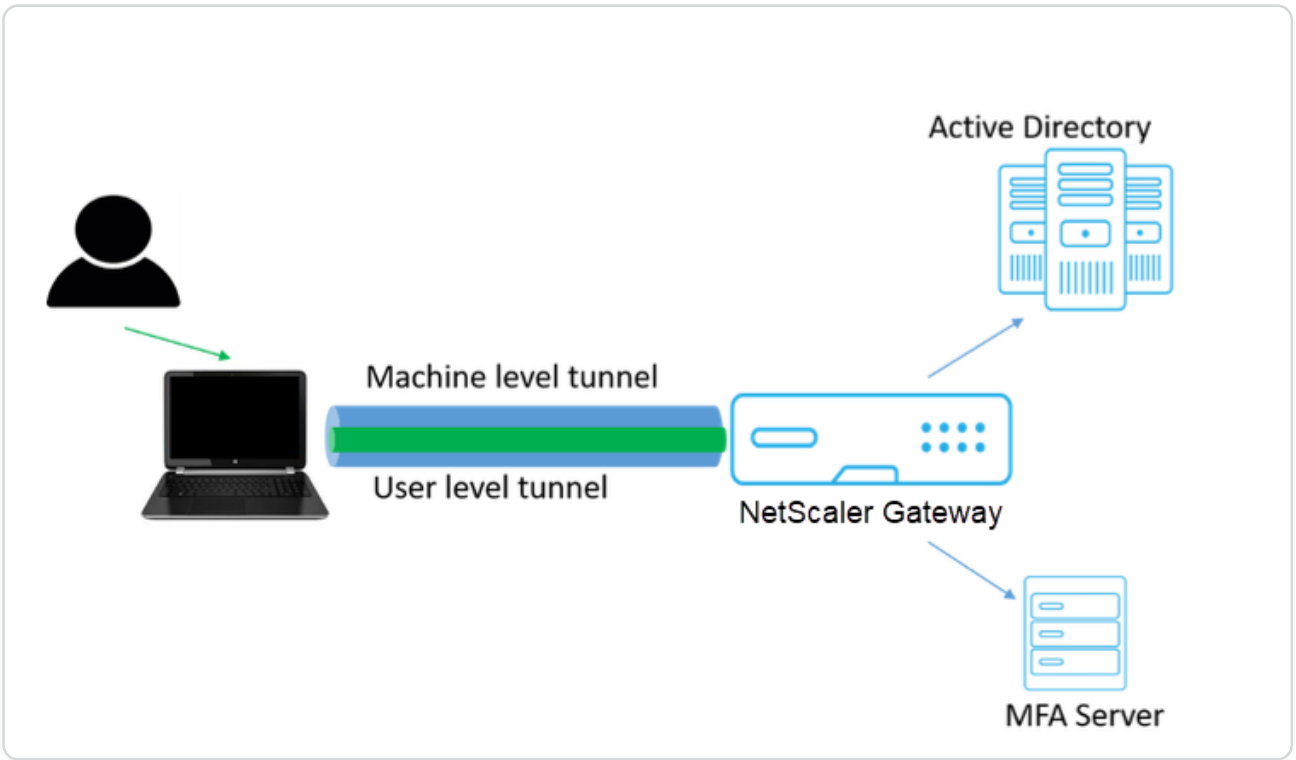
- El administrador puede proporcionar una contraseña de un solo uso a los usuarios que trabajan de forma remota por primera vez, con la cual los usuarios pueden conectarse al controlador de dominio para cambiar su contraseña.
- El administrador puede gestionar/aplicar políticas de AD de forma remota al dispositivo incluso antes de que el usuario inicie sesión.
- El administrador puede proporcionar un nivel de control granular a los usuarios en función del grupo de usuarios después de que el usuario inicie sesión. Por ejemplo, utilizando un túnel a nivel de usuario, puede restringir o proporcionar acceso a un recurso a un grupo de usuarios específico.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- El túnel de usuario se puede configurar para MFA según los requisitos del usuario.
- Varios usuarios pueden usar la misma máquina. El acceso a recursos selectivos se proporciona en función del perfil de usuario. Por ejemplo, varios usuarios pueden usar una máquina en un quiosco sin problemas.
- Los usuarios que trabajan de forma remota se conectan al controlador de dominio para cambiar su contraseña.
- La máquina Windows puede verificar la credencial de inicio de sesión del usuario utilizando el directorio activo corporativo (AD) y las credenciales de Windows en la máquina no se almacenan en caché. Además, los nuevos usuarios de AD corporativo pueden iniciar sesión en la máquina sin problemas.
- La máquina Windows pasa a formar parte de la intranet corporativa incluso antes de que los usuarios inicien sesión, lo que permite a los administradores de TI acceder a la máquina cliente desde la red corporativa con fines de depuración.
- El túnel VPN para una máquina Windows permanece conectado incluso cuando diferentes usuarios inician o cierran sesión en la máquina.

## Comprensión de Always On VPN antes del inicio de sesión de Windows

El siguiente es el flujo de eventos para la funcionalidad **Always On VPN antes del inicio de sesión de Windows**.




© 1997–2026 Citrix Systems, Inc. All rights reserved.

- El usuario enciende el portátil. El túnel a nivel de máquina se establece hacia NetScaler Gateway utilizando el certificado del dispositivo como identidad.
- El usuario inicia sesión en el portátil con credenciales de AD.
- Después del inicio de sesión, se solicita al usuario la MFA.
- Tras una autenticación correcta, el túnel a nivel de máquina se reemplaza por el túnel a nivel de usuario.
- Una vez que el usuario cierra sesión, el túnel a nivel de usuario se reemplaza por el túnel a nivel de máquina.

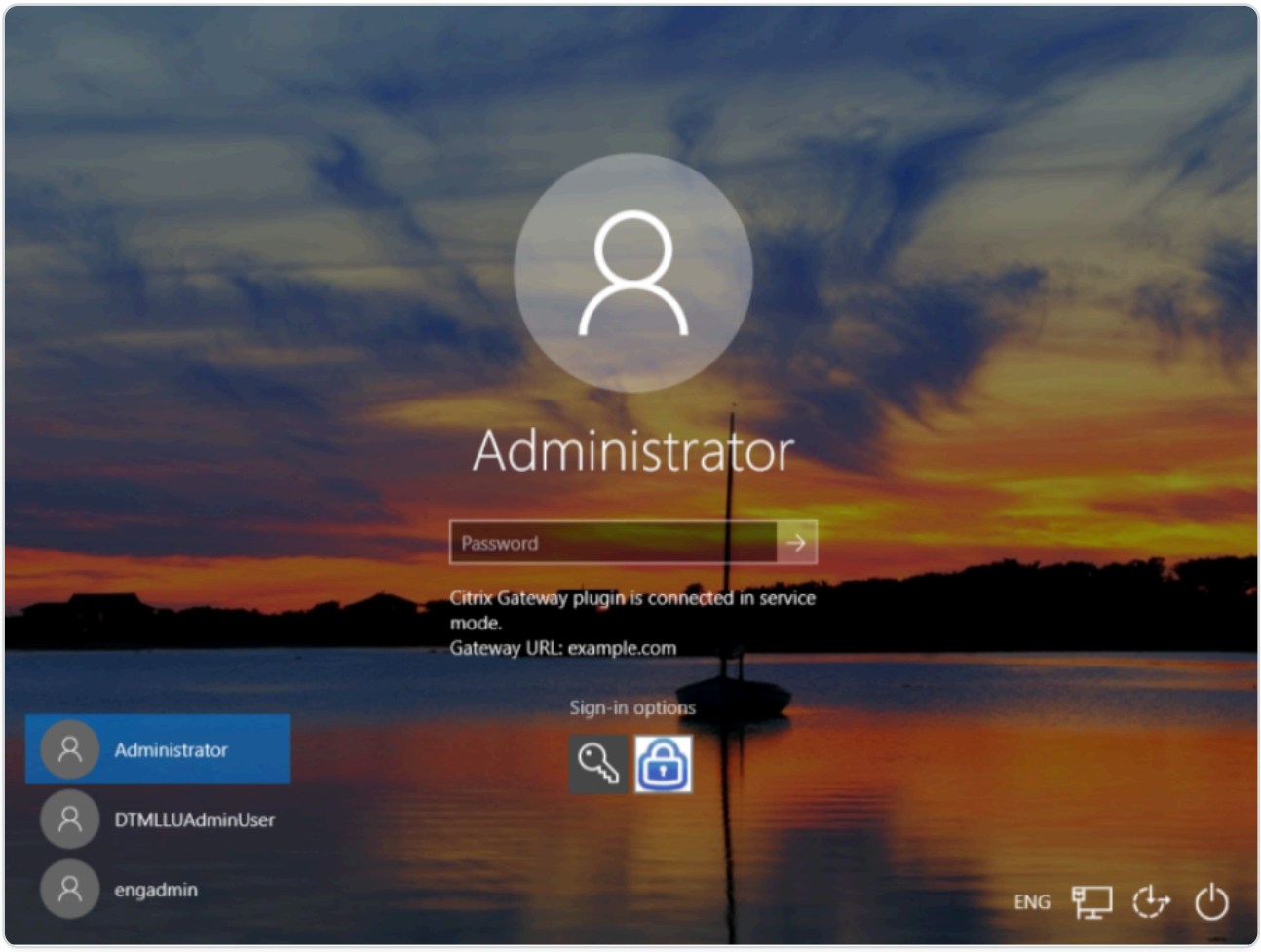
**Puntos a tener en cuenta:**

- NetScaler Gateway y el complemento VPN deben ser la versión 13.0.41.20 o posterior.
- Si una máquina cliente no tiene conectividad a Internet, **Always On VPN antes del inicio de sesión de Windows** espera a que la conectividad a Internet esté disponible antes de establecer el túnel VPN.
- Si una máquina cliente está conectada a una red de portal cautivo, **Always On VPN antes del inicio de sesión de Windows** espera a que el usuario se autentique en el portal cautivo. Después de que el usuario inicia sesión y se habilita el acceso a Internet, **Always On VPN antes del inicio de sesión de Windows** establece el túnel VPN.
- La función Always On VPN antes del inicio de sesión de Windows admite portales cautivos para NetScaler.
- Si la opción de credenciales de inicio de sesión en caché no está habilitada para Windows, los usuarios no podrán iniciar sesión en los siguientes escenarios:
  - La máquina no tiene conectividad a Internet
  - La máquina está conectada a una red de portal cautivo
- Los administradores deben verificar el estado de revocación del certificado del dispositivo antes de presentar la página de inicio de sesión a los usuarios finales.

## Pantalla del administrador de credenciales de Windows después de la configuración de Always On VPN antes del inicio de sesión de Windows

Después de que se configure la función **Always On VPN before Windows Logon**, la pantalla del **administrador de credenciales de Windows** se modifica de la siguiente manera.

© 1997–2026 Citrix Systems, Inc. All rights reserved.




Al hacer clic en **Opciones de inicio de sesión** en la pantalla de inicio de sesión, se muestra la siguiente información:

- El icono de NetScaler Gateway sugiere si la máquina está conectada a NetScaler Gateway o no.
- Según el modo de configuración del usuario, una de las siguientes declaraciones se muestra en la pantalla de inicio de sesión.
  - NetScaler Gateway está conectado en modo de servicio
  - NetScaler Gateway está conectado en modo de usuario

## Configurar Always On VPN antes del inicio de sesión de Windows

Esta sección contiene los detalles para configurar **Always On VPN antes del inicio de sesión de Windows** mediante una política avanzada.

### Requisitos previos

- NetScaler Gateway y el plug-in VPN deben ser de la versión 13.0.41.20 o posterior.
- Se requiere NetScaler Advanced Edition o superior para que la solución funcione.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Puede configurar la funcionalidad solo mediante políticas avanzadas.
- El servidor virtual VPN debe estar en funcionamiento.

### Pasos de configuración de alto nivel

La configuración de **Always On VPN antes del inicio de sesión de Windows** implica los siguientes pasos de alto nivel:

1. Configurar un túnel a nivel de máquina
2. Configurar un túnel a nivel de usuario (opcional)
3. Habilitar la autenticación de usuario
    a. Configure el servidor virtual VPN, instale un certificado de CA y vincule la clave del certificado al servidor virtual.
    b. Crear un perfil de autenticación
    c. Crear un servidor virtual de autenticación
    d. Crear directivas de autenticación
    e. Enlazar las directivas al perfil de autenticación

### Túnel a nivel de máquina

El túnel a nivel de máquina se establece hacia NetScaler Gateway utilizando el certificado del dispositivo como identidad. El certificado del dispositivo debe instalarse en la máquina cliente en el almacén de la máquina. Esto solo es aplicable para el servicio Always On antes del inicio de sesión de Windows.

Para obtener más detalles sobre el certificado del dispositivo, consulte Usar certificados de dispositivo para la autenticación.

**IMPORTANTE:**

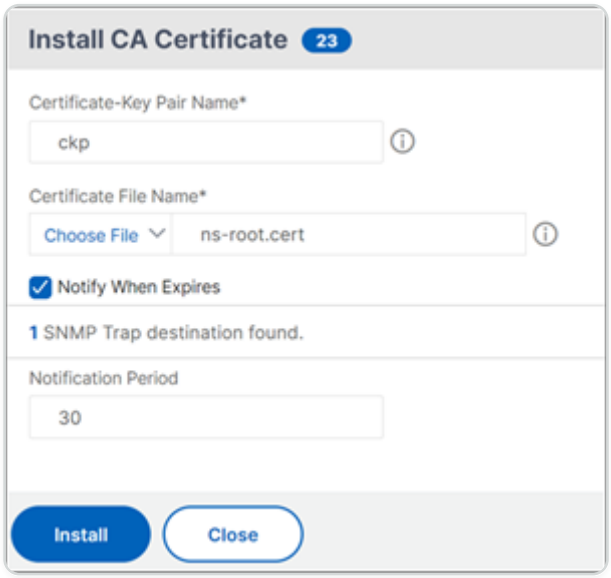
Si el servidor virtual VPN del dispositivo NetScaler Gateway está configurado en un puerto no estándar (distinto de 443), el túnel a nivel de máquina no funciona según lo previsto.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

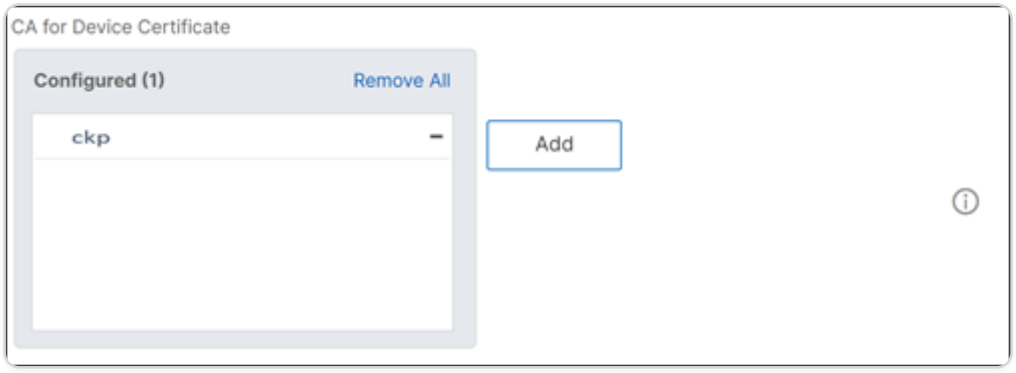
## Configurar el túnel a nivel de máquina mediante el certificado del dispositivo

### CONFIGURACIÓN DE AUTENTICACIÓN BASADA EN CERTIFICADO DE DISPOSITIVO MEDIANTE LA GUI

1. En la ficha **Configuration** (Configuración), vaya a **NetScaler Gateway > Virtual Servers** (Servidores virtuales).
2. En la página NetScaler Gateway Virtual Servers (Servidores virtuales de NetScaler Gateway), seleccione un servidor virtual existente y haga clic en **Edit** (Editar).
3. En **Certificate** (Certificado), haga clic en **CA Certicicate** (Certificado CA).
4. En la página **CA Certificate Binding** (Enlace de certificado CA), haga clic en **Add** (Agregar) junto al campo **Select CA Certificate** (Seleccionar certificado CA), actualice la información requerida y haga clic en **Install** (Instalar).




5. En la página **VPN Virtual Server** (Servidor virtual VPN), haga clic en el icono de edición.
6. En la sección **Configuración básica**, haga clic en **Más**.
7. Haga clic en **Agregar** junto a la sección **CA para certificado de dispositivo** y haga clic en **Aceptar**.




**Nota:** No seleccione la casilla de verificación **Habilitar certificado de dispositivo**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

8. Para vincular un certificado de CA al servidor virtual, haga clic en **Certificado de CA** en la sección **Certificado**. Haga clic en **Agregar enlace** en la página **Enlace de certificado de CA de servidor virtual SSL**.

   **NOTA:**

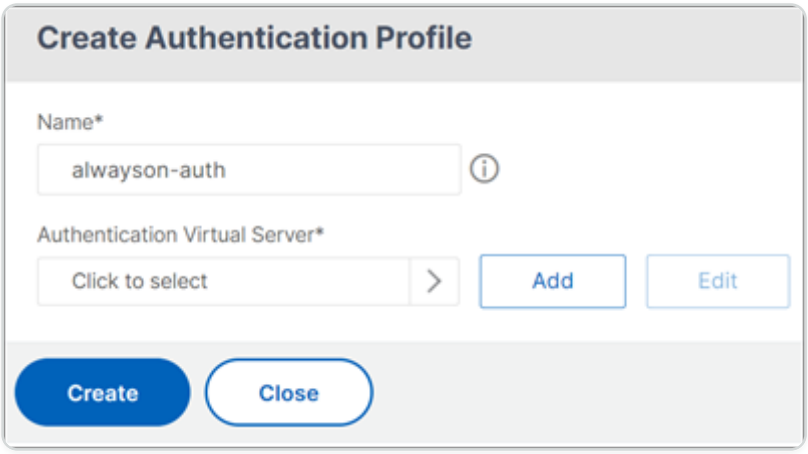
   - El campo de nombre común (CN) del asunto del certificado de dispositivo no debe estar vacío. Si un dispositivo intenta iniciar sesión con certificados de dispositivo CN vacíos, su sesión VPN se crea con el nombre de usuario como «anónimo». En IIP, si varias sesiones tienen el mismo nombre de usuario, las sesiones anteriores se desconectan. Por lo tanto, cuando IIP está habilitado, se observa el impacto en la funcionalidad debido a un nombre común vacío.
   - Todos los certificados de CA (raíz e intermedios) que puedan firmar el certificado de dispositivo emitido a los clientes deben vincularse en la sección **CA para certificado de dispositivo** y también en la sección **Enlace de certificado de CA** para el servidor virtual en los pasos 4 y 5. Para obtener más información sobre cómo vincular el certificado de CA con intermedio/subordinado, consulte Instalar, vincular y actualizar certificados.
   - Si se configuran varios certificados de dispositivo, se intenta utilizar el certificado con la fecha de caducidad más larga para la conexión VPN. Si este certificado permite el análisis EPA correctamente, se establece la conexión VPN. Si este certificado falla en el proceso de análisis, se utiliza el siguiente certificado. Este proceso continúa hasta que se prueban todos los certificados.

9. En la página **Enlace de certificado de CA**, seleccione el certificado.
10. Haga clic en **Enlazar**.
11. Cree un servidor virtual de autenticación.

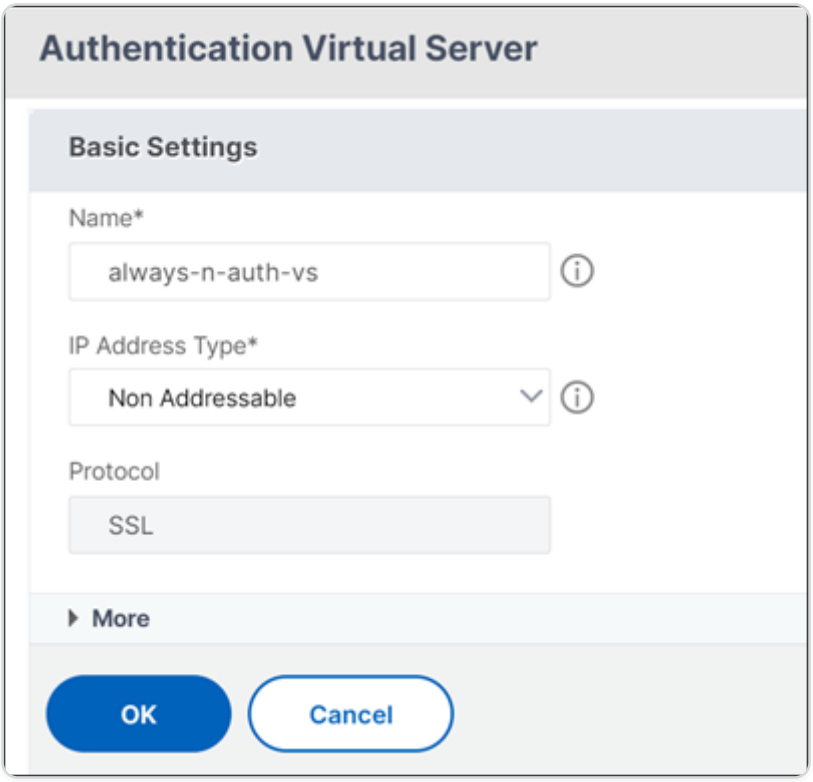
    a. En la página **Servidores virtuales VPN**, vaya a **Configuración avanzada > Perfil de autenticación** y haga clic en **Agregar**.

    b. En la página **Crear perfil de autenticación**, asigne un nombre al perfil de autenticación y haga clic en **Crear**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.




c. En la página **Servidor virtual de autenticación**, asigne un nombre al servidor virtual de autenticación. Seleccione el tipo de dirección IP como **No direccionable,** y haga clic en **Aceptar**.




**NOTA:**

El servidor virtual de autenticación siempre permanece en estado INACTIVO.

12. Cree una directiva de autenticación.

a. En la sección **Directivas de autenticación avanzadas** de la página **Security > AAA-Application Traffic > Authentication Virtual Servers**, seleccione la directiva de autenticación y haga clic en **Add Binding**.

b. En la página **Policy Binding**, haga clic en **Add** junto al campo **Select Policy**.

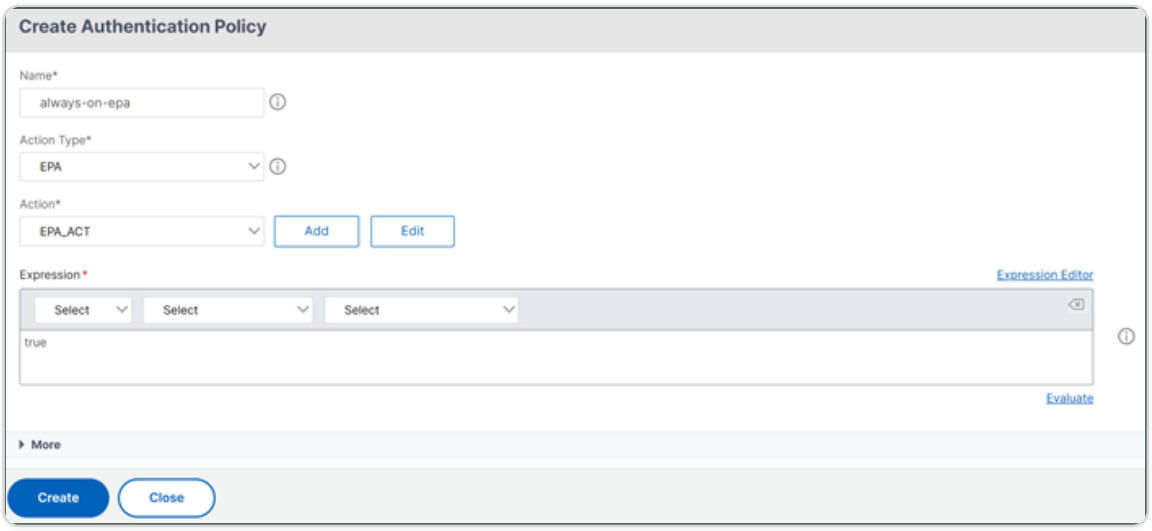
© 1997–2026 Citrix Systems, Inc. All rights reserved.

c. En la página Create Authentication Policy:

i. Asigne un nombre a la directiva de autenticación avanzada.

ii. Seleccione **EPA** en la lista **Action Type**.

iii. Haga clic en **Add** junto a **Action**.

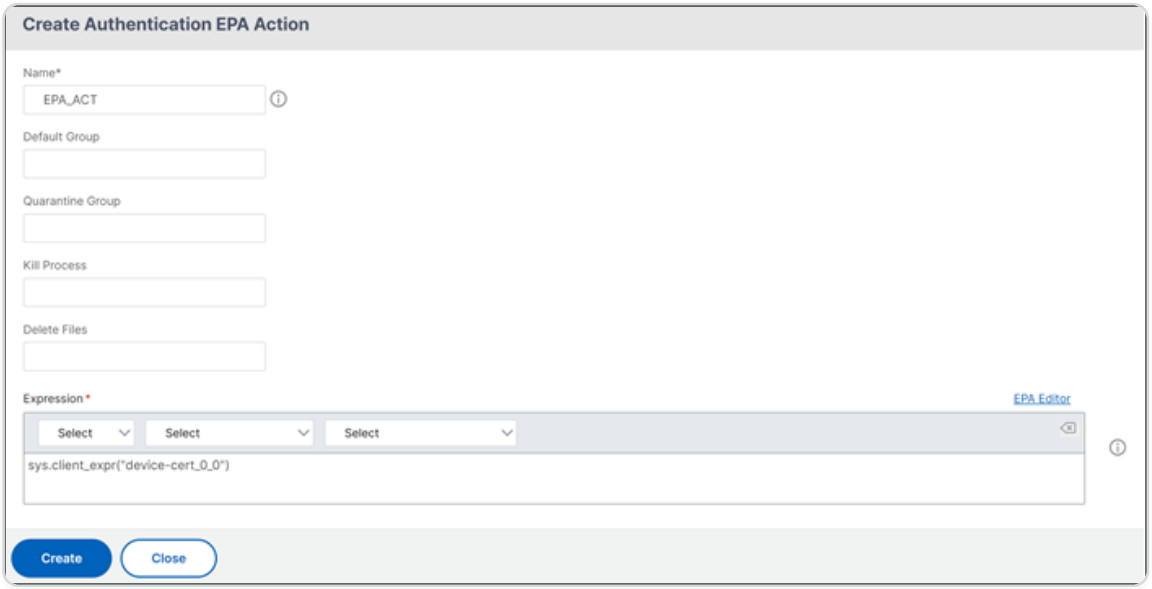



d. En la página Create Authentication EPA Action:

i. Asigne un nombre a la acción EPA.

ii. Introduzca `sys.client_expr("device-cert_0_0")` en el campo **Expression**.

iii. Haga clic en **Create**.



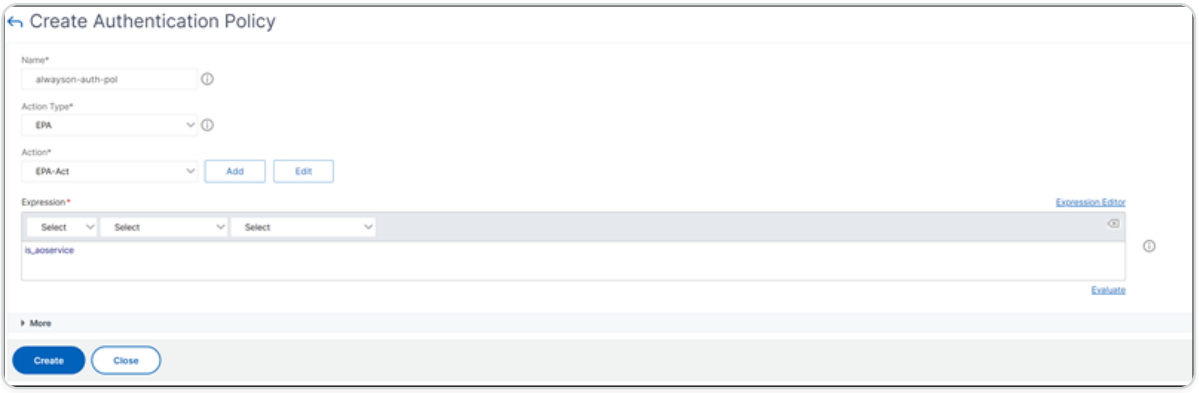

13. En la página **Create Authentication Policy**:

a. Asigne un nombre a la política de autenticación.

b. Introduzca **is_aoservice** en el campo **Expresión**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

c. Haga clic en **Crear**.




14. En la página Enlace de directivas, introduzca **100** en **Prioridad** y haga clic en **Enlazar**.

## CONFIGURACIÓN DE AUTENTICACIÓN BASADA EN CERTIFICADOS DE DISPOSITIVO MEDIANTE LA CLI

1. Instale un certificado de CA en un servidor virtual VPN.

```
add ssl certkey ckp -cert t_CA.cer
```

2. Enlace el certificado de CA al servidor virtual VPN.

```
bind ssl vserver <vServerName> -certkeyName <string> -ocspCheck
( Mandatory | Optional )
```

Ejemplo

```
bind ssl vserver TestClient -CertkeyName ag51.xm.nsi.test.com -CA
-ocspCheck Mandatory
```

3. Agregue un servidor virtual de autenticación.

```
add authentication authnProfile <name>  {-authnVsName <string>}
```

Ejemplo

```
add authentication authnProfile always_on -authnVsName
always_on_auth_server
```

4. Cree una acción EPA de autenticación.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
add authentication epaAction <name> -csecexpr <expression>
```

Ejemplo

```
add authentication epaAction epa-act -csecexpr
 `sys.client_expr("device-cert_0_0")` -defaultgroup epa_pass
```

5. Cree una política de autenticación

```
add authentication Policy <name> -rule <expression> -action <string>
```

Ejemplo:

```
add authentication Policy always_on_epa_auth -rule is_aoservice -action
epa_auth
```

**IMPORTANTE:**

- La configuración del túnel a nivel de máquina ya está completa. Para configurar el túnel a nivel de usuario después del inicio de sesión de Windows, consulte la sección **Túnel a nivel de usuario**.
- En la máquina cliente, el certificado del dispositivo está en formato .pfx. El certificado .pfx se instala en la máquina Windows, ya que Windows entiende el formato .pfx. Este archivo contiene los archivos de certificado y clave. Este certificado debe ser del mismo dominio que está vinculado al servidor virtual. Los certificados y claves .pfx y de servidor se pueden generar mediante el asistente de certificados de cliente. Estos certificados se pueden usar con la autoridad de certificación para generar el .pfx respectivo con el certificado de servidor y el dominio. El certificado .pfx se instala en la cuenta del equipo en la carpeta personal. El comando `show aaa session` muestra el túnel del dispositivo en el dispositivo NetScaler.

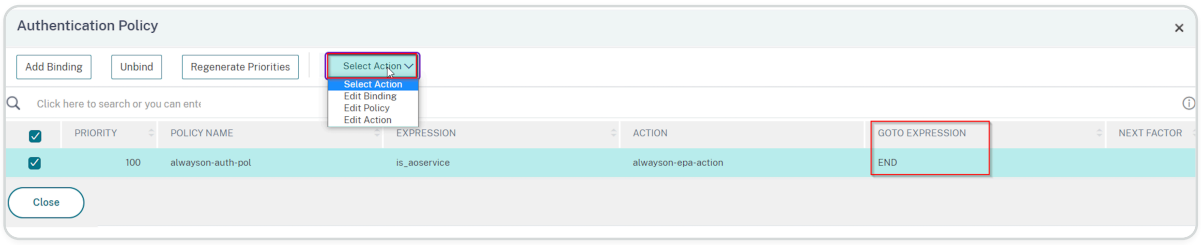
© 1997–2026 Citrix Systems, Inc. All rights reserved.

## Túnel a nivel de usuario

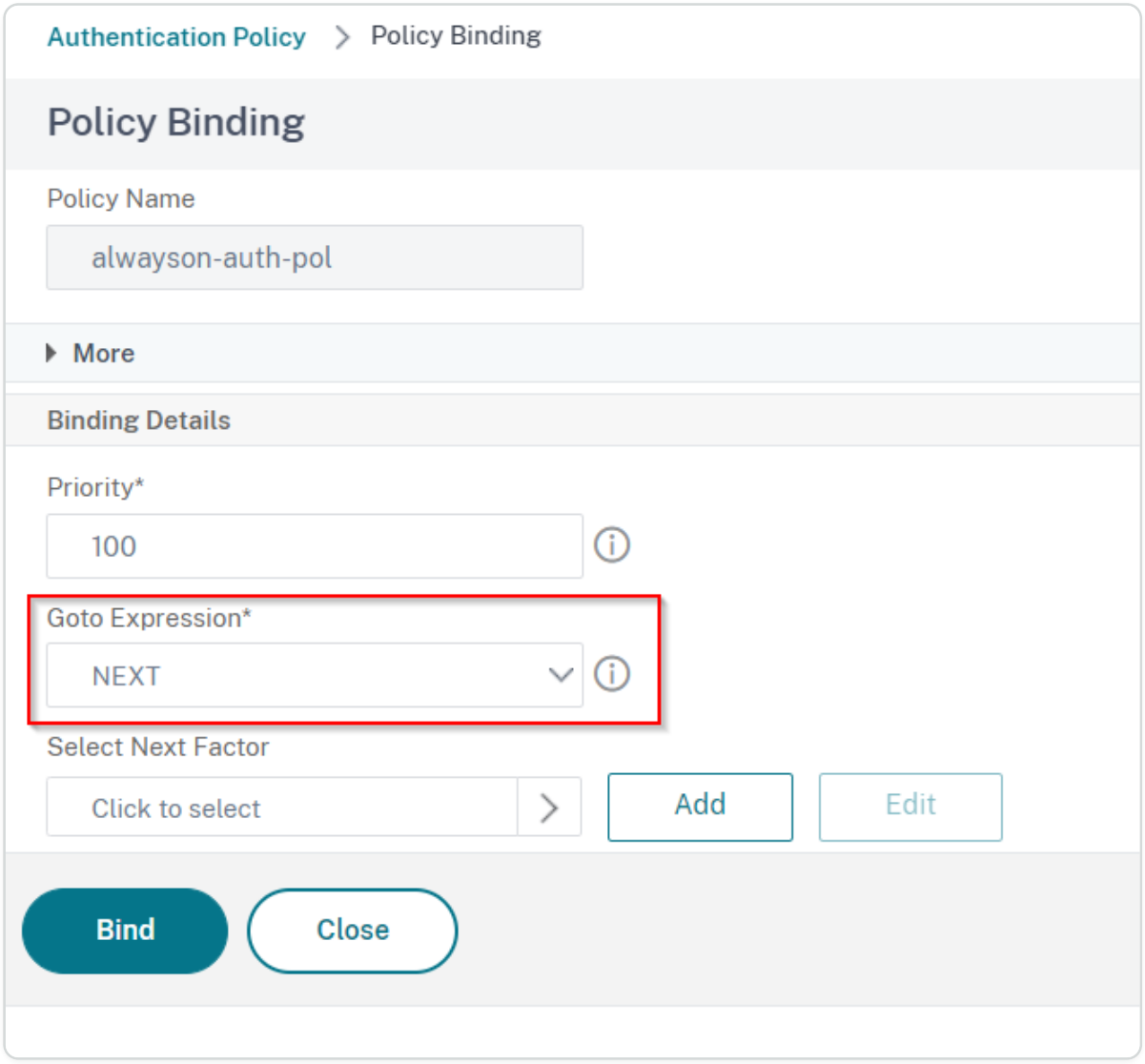
### Reemplace un túnel a nivel de máquina por un túnel a nivel de usuario mediante la GUI

**Nota:** La expresión `is_aoservice.not` es aplicable a partir de NetScaler Gateway versión 13.0.41.20 y posteriores.

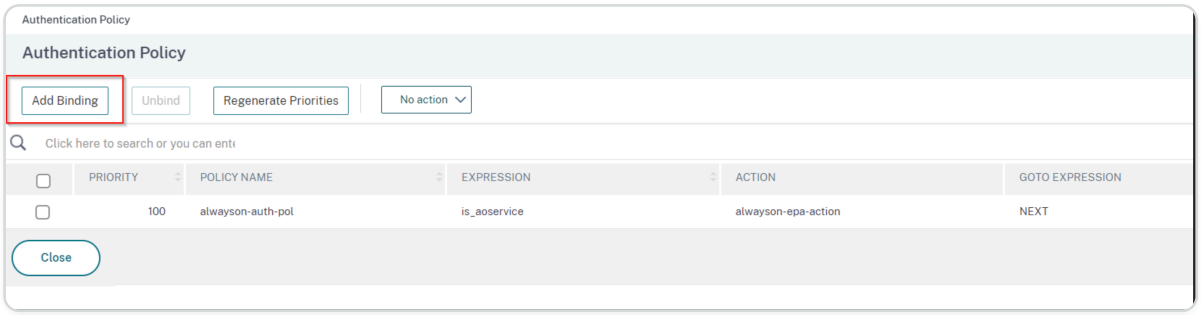
1. Configure una directiva para la autenticación de usuarios.
    a. Vaya a **NetScaler Gateway > Servidores virtuales** y seleccione un servidor virtual.
    b. En **Configuración avanzada**, haga clic en **Perfil de autenticación**.
    c. Configure el perfil de autenticación.
    d. En la página **Configuración > Seguridad > Tráfico de aplicaciones AAA > Servidores virtuales de autenticación**, seleccione la directiva de autenticación.
    e. En **Seleccionar acción**, haga clic en **Editar enlace** y cambie **Expresión GoTo** a **NEXT** en lugar de **END** para la directiva vinculada.




© 1997–2026 Citrix Systems, Inc. All rights reserved.




f. Haga clic en **Vincular** y, a continuación, en la página **Directiva de autenticación**, seleccione la directiva de autenticación y haga clic en **Agregar enlace**.




g. En la página Enlace de política, haga clic en **Agregar** junto a **Seleccionar política**.

En la página Crear política de autenticación;

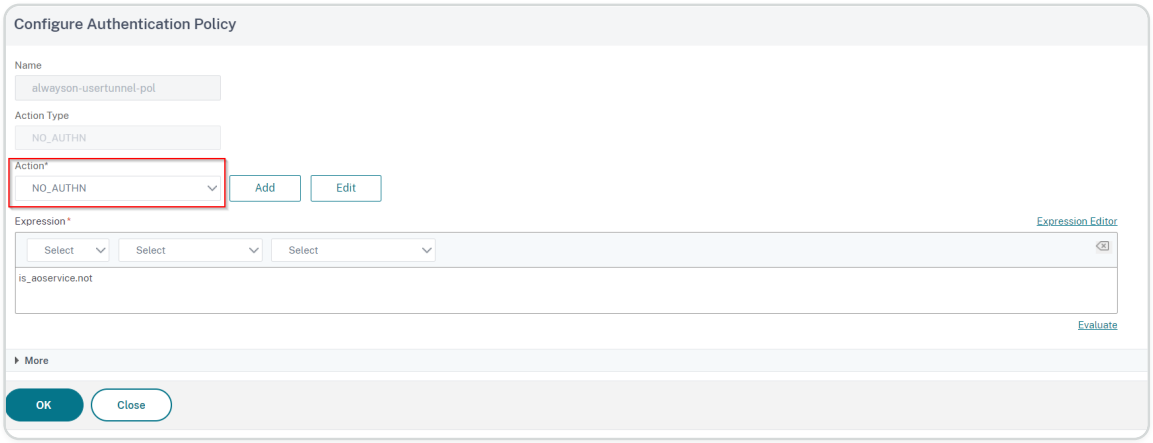
i. Introduzca un nombre para la política de "no autenticación" que se va a crear.

ii. Seleccione el tipo de acción como **No_AUTHN**.

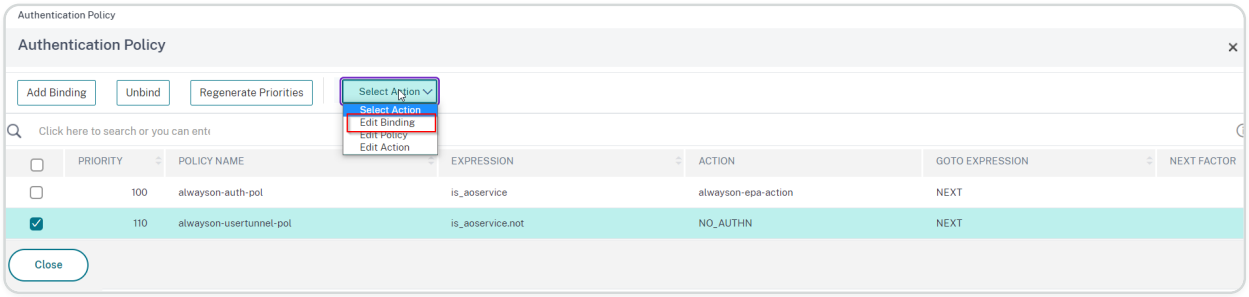
iii. Introduzca **is_aoservice.not** en el campo **Expresión**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

iv. Haga clic en **Crear**.




2. En **Seleccionar acción**, haga clic en **Editar enlace**.




3. En la página Enlace de política, introduzca **110** en **Prioridad**. Haga clic en **Agregar** junto a **Seleccionar siguiente factor**.

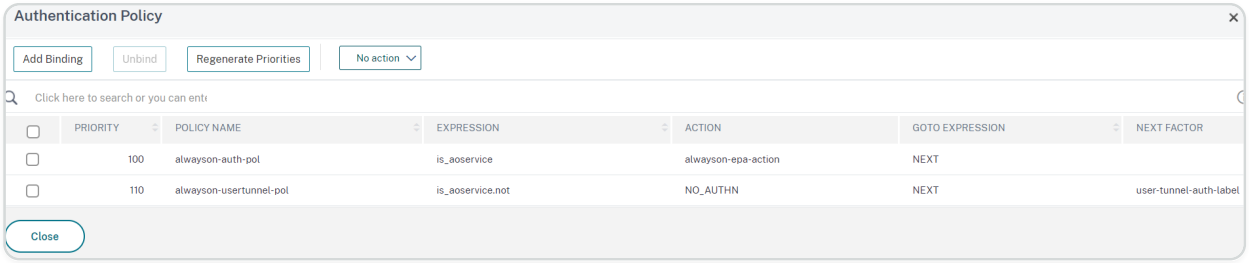
   a. En la página Etiqueta de política de autenticación, introduzca un nombre descriptivo para la etiqueta de política, seleccione el esquema de inicio de sesión y haga clic en **Continuar**.

   b. En **Seleccionar política**, haga clic en **Agregar** y cree una política de autenticación LDAP.

   c. Haga clic en **Crear,** y, a continuación, haga clic en **Enlazar.**

   d. Haga clic en **Listo,** y, a continuación, haga clic en **Enlazar**.

   En la página Política de autenticación, la columna **Siguiente factor** muestra la política de siguiente factor configurada.




4. Puede configurar la política LDAP como el siguiente factor de la política de autenticación.

   a. En la página Crear política de autenticación, introduzca un nombre para la política LDAP.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

b. Seleccione **Tipo de acción** como **LDAP**.

c. Introduzca **Acción** como la acción LDAP configurada.

**NOTA:**

- Para crear un archivo XML de esquema de inicio de sesión, consulte Archivo XML de esquema de inicio de sesión.
- Para crear etiquetas de política, consulte Autenticar la etiqueta de política.
- Para crear una política de autenticación LDAP, consulte Para configurar la autenticación LDAP mediante la utilidad de configuración.

**Sustituir un túnel a nivel de máquina por un túnel a nivel de usuario mediante la CLI**

1. Vincular una política al servidor virtual de autenticación

```
bind authentication vserver <name> -policy <name> -priority
 <positive_integer> -gotoPriorityExpression <expression>
```

Ejemplo

```
bind authentication vserver alwayson-auth-vserver -policy alwayson-
auth-pol -priority 100 -gotoPriorityExpression NEXT
```

2. Agregue una política de autenticación con la acción como `NO_AUTH` y la expresión `is_aoservice.not,` y vincúlela a la política.

```
add authentication Policy <name> -rule <expression> -action <string>



bind authentication vserver <name> -policy <name> -priority
<positive_integer> -gotoPriorityExpression <expression>
```

Ejemplo

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
add authentication Policy alwayson-usertunnel-pol -rule
is_aoservice.not -action NO_AUTHN



bind authentication vserver alwayson-auth-vserver -policy alwayson-
usertunnel-pol -priority 110
```

3. Agregue un siguiente factor y vincule la etiqueta de política al siguiente factor.

```
add authentication policylabel <labelName> -loginSchema <string>



bind authentication  policylabel <string>  -policyName <string>  -
priority <positive_integer> -gotoPriorityExpression <expression>
-nextFactor <string>
```

Ejemplo

```
add authentication policylabel user-tunnel-auth-label -loginSchema
singleauth_alwayson



bind authentication policylabel user -policyName alwayson-usertunnel-
pol -priority 100
```

4. Configure una política LDAP y vincúlela a la etiqueta de política de túnel de usuario.

```


add authentication policy <name>  -rule <expression>  -action <string>



bind authentication vserver <vserver_name> -policy <string>  -priorit <
positive integer>  gotoPriorityExpression <string>
```

Ejemplo

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
add authentication Policy LDAP_new -rule true -action LDAP_new



bind authentication policylabel user-tunnel-auth-label -policyName
LDAP_new -priority 100 -gotoPriorityExpression NEXT
```

### Configuración del lado del cliente

Los `AlwaysOn, locationDetection, and suffixList registries` son opcionales y solo se requieren si se necesita la funcionalidad de detección de ubicación.

Para acceder a las entradas de clave de registro, vaya a la siguiente ruta: **Computer>HKEY_LOCAL_MACHINE>SOFTWARE>Citrix®>Secure Access Client**

| CLAVE DE REGISTRO | TIPO DE REGISTRO | VALORES Y DESCRIPCIÓN |
|---|---|---|
| AlwaysOnService | REG_DWORD | 1 => Establecer túnel a nivel de máquina pero no a nivel de usuario; 2 => Establecer túnel a nivel de máquina y a nivel de usuario |
| AlwaysOnURL | REG SZ | URL del servidor virtual de NetScaler Gateway al que el usuario quiere conectarse. **Ejemplo:** `https://xyz.companyDomain.com` **Importante:** Solo una URL es responsable del túnel a nivel de máquina y del túnel a nivel de usuario. El registro AlwaysOnURL ayuda tanto al servicio como al componente a nivel de usuario a funcionar y a conectar un túnel independiente, es decir, un túnel a nivel de máquina y un túnel a nivel de usuario según el diseño. |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| CLAVE DE REGISTRO | TIPO DE REGISTRO | VALORES Y DESCRIPCIÓN |
|---|---|---|
| AlwaysOn | REG_DWORD | 1 => Permitir acceso a la red en caso de fallo de VPN; 2=> Bloquear acceso a la red en caso de fallo de VPN |
| AlwaysOnAllowlist | REG_SZ | Lista de direcciones IP o FQDN separadas por punto y coma que deben incluirse en la lista blanca mientras la máquina se ejecuta en modo estricto. **Ejemplo:** `8.8.8.8;linkedin.com` |
| UserCertCAList | REG_SZ | Lista de nombres de CA raíz separados por comas o punto y coma, es decir, el nombre del emisor del certificado. Se utiliza en el contexto de un servicio Always On donde un cliente puede especificar la lista de CA de las que elegir el certificado de cliente. **Ejemplo**: `example.net;xyz.gov.in` |
| locationDetection | REG_DWORD | 1 => Para habilitar la detección de ubicación; 0 => Para deshabilitar la detección de ubicación |
| suffixList | REG SZ | Lista de dominios separados por punto y coma y es responsable de comprobar si la máquina está en la intranet o no en cualquier momento dado cuando la detección de ubicación está habilitada. **Ejemplo:** `citrite.net,example.net` |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Para obtener más información sobre estas entradas del registro, consulte Always On.

**NOTA:**

- Cuando se configura el servicio Always On, el perfil Always On configurado en el servidor virtual de NetScaler Gateway o en NetScaler se ignora en el lado del cliente. Por lo tanto, asegúrese de habilitar también los registros VPN `locationDetection` y `AlwaysOn` al configurar el servicio Always On.
- La configuración del registro `ClientControl` solo se admite en el modo Always On y no en el modo de servicio Always On. Como resultado, la opción **Cerrar sesión** no es compatible cuando el modo de servicio Always On está habilitado.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

# Uso de la política avanzada para crear políticas VPN

El motor de políticas clásico (PE) y la infraestructura de políticas avanzada (PI) son dos marcos diferentes de configuración y evaluación de políticas que NetScaler admite actualmente.

La infraestructura de políticas avanzada consta de un potente lenguaje de expresiones. El lenguaje de expresiones se puede utilizar para definir reglas en la política, definir varias partes de la acción y otras entidades admitidas. El lenguaje de expresiones puede analizar cualquier parte de la solicitud o respuesta y también le permite examinar en profundidad los encabezados y la carga útil. El mismo lenguaje de expresiones se expande y funciona a través de cada módulo lógico que NetScaler admite.

**NOTA:**

Se recomienda utilizar políticas avanzadas para crear políticas.

## ¿Por qué migrar de la política clásica a la política avanzada?

La política avanzada tiene un conjunto de expresiones enriquecido y ofrece mucha más flexibilidad que la política clásica. A medida que NetScaler escala y atiende a una gran variedad de clientes, es imperativo admitir expresiones que superen ampliamente las políticas avanzadas. Para obtener más información, consulte Políticas y expresiones.

A continuación se presentan las capacidades añadidas para la política avanzada.

- Capacidad para acceder al cuerpo de los mensajes.
- Admite muchos otros protocolos.
- Accede a muchas otras funciones del sistema.
- Tiene un mayor número de funciones básicas, operadores y tipos de datos.
- Permite el análisis de archivos HTML, JSON y XML.
- Facilita la coincidencia rápida y paralela de múltiples cadenas ( `patsets` , y así sucesivamente).

Ahora, las siguientes políticas VPN se pueden configurar utilizando la política avanzada.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Política de sesión
- Política de autorización
- Política de tráfico
- Política de túnel
- Política de auditoría

Además, el análisis de puntos finales (EPA) se puede configurar como un nFactor para la función de autenticación. EPA se utiliza como guardián para los dispositivos de punto final que intentan conectarse al dispositivo Gateway. Antes de que se muestre la página de inicio de sesión de Gateway en un dispositivo de punto final, se comprueba que el dispositivo cumpla con los requisitos mínimos de hardware y software, según los criterios de elegibilidad configurados por el administrador de Gateway. El acceso a Gateway se concede en función del resultado de las comprobaciones realizadas. Anteriormente, EPA se configuraba como parte de la política de sesión. Ahora se puede vincular a nFactor, lo que proporciona más flexibilidad en cuanto a cuándo se puede realizar. Para obtener más información sobre EPA, consulte el tema Cómo funcionan las políticas de punto final. Para obtener más información sobre nFactor, consulte el tema Autenticación nFactor.

**Casos de uso:**

## EPA de preautenticación mediante EPA avanzada

El análisis EPA de preautenticación se realiza antes de que un usuario proporcione las credenciales de inicio de sesión. Para obtener información sobre cómo configurar NetScaler Gateway para la autenticación nFactor con el análisis EPA de preautenticación como uno de los factores de autenticación, consulte el tema CTX224268.

## EPA de postautenticación mediante EPA avanzada

El análisis EPA de postautenticación se realiza después de que se verifican las credenciales del usuario. En la infraestructura de políticas clásica, el EPA de postautenticación se configuraba como parte de la política de sesión o la acción de sesión. En la infraestructura de políticas avanzadas, el análisis EPA debe configurarse como un factor EPA en la autenticación nFactor. Para obtener información sobre cómo configurar NetScaler Gateway para la autenticación nFactor con el análisis EPA de postautenticación como uno de los factores de autenticación, consulte el tema CTX224303.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

# EPA de preautenticación y postautenticación mediante políticas avanzadas

El EPA se puede realizar antes de la autenticación y después de la autenticación. Para obtener información sobre cómo configurar NetScaler Gateway para la autenticación nFactor con análisis EPA de preautenticación y postautenticación, consulte el tema CTX231362.

# Análisis EPA periódico como factor en la autenticación nFactor

En la infraestructura de políticas clásica, el análisis EPA periódico se configuraba como parte de la acción de política de sesión. En la infraestructura de políticas avanzadas, se puede configurar como parte del factor EPA en la autenticación nFactor.

Para obtener más información sobre cómo configurar el análisis EPA periódico como factor en la autenticación nFactor, consulte Configurar el análisis periódico de Endpoint Analysis como factor en la autenticación nFactor.

**Solución de problemas:**

Se deben tener en cuenta los siguientes puntos para la solución de problemas.

- Las políticas clásicas y avanzadas del mismo tipo (por ejemplo, política de sesión) no se pueden vincular a la misma entidad/punto de enlace.
- La prioridad es obligatoria para todas las políticas PI.
- La política avanzada para la VPN se puede vincular a todos los puntos de enlace.
- La política avanzada con la misma prioridad se puede vincular a un único punto de enlace.
- Si no se selecciona ninguna de las políticas de autorización configuradas, entonces se aplica la acción de autorización global configurada en el parámetro VPN.
- En la política de autorización, la acción de autorización no se revierte si la regla de autorización falla.

**Expresiones equivalentes de política avanzada de uso común para la política clásica:**

| EXPRESIONES DE POLÍTICA CLÁSICA | EXPRESIONES DE POLÍTICA AVANZADA |
|---|---|
| ns_true | verdadero |
| ns_false | falso |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| EXPRESIONES DE POLÍTICA CLÁSICA | EXPRESIONES DE POLÍTICA AVANZADA |
|---|---|
| REQ.HTTP | HTTP.REQ |
| RES.HTTP | HTTP.RES |
| ENCABEZADO "foo" | HEADER("foo") |
| CONTAINS "bar" | .CONTAINS("bar") [Note use of “..”] |
| REQ.IP | CLIENT.IP |
| RES.IP | SERVER.IP |
| SOURCEIP | SRC |
| DESTIP | DST |
| REQ.TCP | CLIENT.TCP |
| RES.TCP | SERVER.TCP |
| PUERTO DE ORIGEN | PUERTO DE ORIGEN |
| PUERTO DE DESTINO | PUERTO DE DESTINO |
| CÓDIGO DE ESTADO | ESTADO |
| REQ.SSL.CLIENT.CERT | CLIENT.SSL.CLIENT_CERT |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

# Configurar el servidor virtual VPN DTLS mediante el servidor virtual VPN SSL

Puede configurar un servidor virtual VPN DTLS para NetScaler Gateway utilizando la misma dirección IP y número de puerto de un servidor virtual VPN SSL configurado. La configuración de servidores virtuales VPN DTLS le permite vincular los cifrados y certificados DTLS avanzados al tráfico DTLS para una seguridad mejorada.

**IMPORTANTE:**

- De forma predeterminada, la funcionalidad DTLS está activada para el servidor virtual VPN SSL existente. Deshabilite la funcionalidad para el servidor antes de crear el servidor virtual VPN DTLS.
- SNI para el servidor virtual de puerta de enlace DTLS es compatible con la versión 13.0 compilación 64.x y posteriores de NetScaler Gateway.
- A partir de la versión 13.0 compilación 79.x de NetScaler, el parámetro `helloverifyrequest` está habilitado de forma predeterminada. La habilitación del parámetro `helloverifyrequest` en el perfil DTLS ayuda a mitigar el riesgo de que un atacante o bots saturen el rendimiento de la red, lo que podría provocar el agotamiento del ancho de banda de salida. Es decir, ayuda a mitigar el ataque de amplificación DDoS de DTLS. Para obtener detalles sobre el parámetro `helloverifyrequest`, consulte Perfil DTLS.
- Al manejar el tráfico UDP, el consumo de memoria del dispositivo NetScaler aumenta si los servidores back-end envían mucho tráfico. Como resultado, el dispositivo NetScaler no puede enviar este tráfico al cliente debido a la conexión TCP MUX en el lado del cliente. En tales casos, Citrix recomienda que utilice el protocolo DTLS.

## Puntos a tener en cuenta

- El servidor virtual VPN DTLS en un dispositivo NetScaler Gateway se puede configurar a partir de la versión 13.0 compilación 58.x.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Antes de configurar un servidor virtual VPN DTLS en un dispositivo NetScaler Gateway, debe haber configurado un servidor virtual VPN SSL en el dispositivo.
- El servidor virtual VPN DTLS utiliza la dirección IP y el número de puerto del servidor virtual VPN SSL configurado.
- Si el protocolo de enlace DTLS falla, la conexión vuelve a TLS.
- Para usar solo DTLS, puede deshabilitar TLS vinculando solo los cifrados DTLS al tráfico DTLS.
- La multiplexación DTLS no es compatible cuando el tráfico TCP se tuneliza a través de VPN.

## Configurar un servidor virtual VPN DTLS mediante la GUI

1. En la pestaña Configuración, vaya a **NetScaler Gateway > Servidores virtuales**.
2. En la página **Servidores virtuales de NetScaler Gateway**, seleccione el servidor virtual SSL VPN existente y haga clic en **Editar**.
3. En la página **Servidor virtual VPN**, haga clic en el icono de edición, desactive la casilla de verificación **DTLS** y haga clic en **Aceptar**.
4. Vuelva a **NetScaler Gateway > Servidores virtuales** y haga clic en **Agregar**.
5. En **Configuración básica**, introduzca los valores de los siguientes campos y haga clic en **Aceptar**.
    - Nombre: un nombre para el servidor virtual DTLS VPN
    - Protocolo: seleccione DTLS
    - Dirección IP: introduzca la dirección IP del servidor virtual SSL VPN
    - Puerto: introduzca el número de puerto del servidor virtual SSL VPN
6. En la página **Servidores virtuales de NetScaler® Gateway**, seleccione el servidor virtual que agregó anteriormente y haga clic en **Editar**.
7. En **Certificados**, haga clic en el icono de flecha para seleccionar la clave de certificado requerida.
8. En **Enlace de certificado de servidor > Seleccionar certificado de servidor**, seleccione una clave de certificado SSL existente o cree una.
9. Haga clic en **Enlazar** en la página **Enlace de certificado de servidor**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**NOTA:**

- Para usar DTLS 1.2, haga clic en el icono de edición en Parámetros SSL y seleccione la casilla de verificación **DTLS 1.2**.
- La indicación de nombre de servidor (SNI) es compatible con el servidor virtual VPN de tipo DTLS.

## Configurar un servidor virtual VPN DTLS mediante la CLI

En el símbolo del sistema, escriba el siguiente conjunto de comandos:

```
set vpn vserver <ssl vpnvserver name> -dtls off

add vpn vserver <dtls vpnvserver name> dtls <ssl vpn vserver IP> <ssl vpn
vserver port>

bind ssl vservser <dtls vpnvserver name> -certkeyName <existing ssl cert
key or newly created cert key>
```

DTLS 1.0 funciona como de costumbre; para usar DTLS 1.2, escriba el siguiente comando:

```
set ssl vserver < dtls vpnvserver name > -dtls12 ENABLED
```

Ejemplo

```
set vpn vserver vpnvserver  -dtls off

add vpn vserver vpnvserver_dtls dtls 10.108.45.220 443

bind ssl vservser vpnvserver_dtls -certkeyName sslcertkey

set ssl vserver vpnvserver_dtls -dtls12 ENABLED
```

**Para habilitar SNI para el servidor virtual VPN de tipo DTLS, escriba el siguiente comando:**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
set ssl vserver <vServerName>@ [-SNIEnable ( ENABLED | DISABLED )

bind ssl vservser <dtls vpnvserver name> -certkeyName <existing ssl cert
key or newly created cert key> <-SNICert>
```

Ejemplo

```
set ssl vserver _XD_10.106.40.225_443_DTLS -sniEnable eNABLED

bind ssl vserver _XD_10.106.40.225_443_DTLS -certkeyName "Insight/
*.insight.net.cer_CERT_" -snICert
```

## Parámetros de servidor virtual VPN DTLS admitidos

Solo se admiten los siguientes parámetros para el servidor virtual VPN de tipo DTLS.

- Ipaddress
- Puerto
- Estado
- Salto doble
- vaciar estado inactivo
- Comentario
- Appflowlog
- Icmpvsrresponse

## Parámetros de servidor virtual VPN DTLS no admitidos

Los siguientes parámetros no son compatibles con el servidor virtual VPN de tipo DTLS.

- LinuxEPAPluginUpgrade
- WindowsEPAPluginUpgrade
- maxAAAUsers
- icaProxySessionMigration
- loginOnce
- cginfraHomePageRedirect

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- logoutOnSmartcardRemoval
- l2Conn
- MacEPAPluginUpgradeRHIstate
- icaOnly
- maxLoginAttempts
- failedLoginTimeout
- vserverFqdn
- deviceCert
- rdpServerProfileName
- pcoipVserverProfileName
- tcpProfileName
- netProfile
- authnProfile
- Listenpriority
- Listenpolicy
- Conjunto de IP
- certkeyNames

## Configurar un servidor virtual DTLS mediante el asistente de XenApp y XenDesktop®

1. Haga clic en **XenApp® y XenDesktop** en **Integrar con productos Citrix®**.
2. En el asistente de configuración de XenApp y XenDesktop, seleccione **StoreFront™** y haga clic en **Continuar**.
3. En la página **NetScaler Gateway Settings**, habilite la casilla **Configure a DTLS Listener for this VPN VServer** y haga clic en **Continue**.

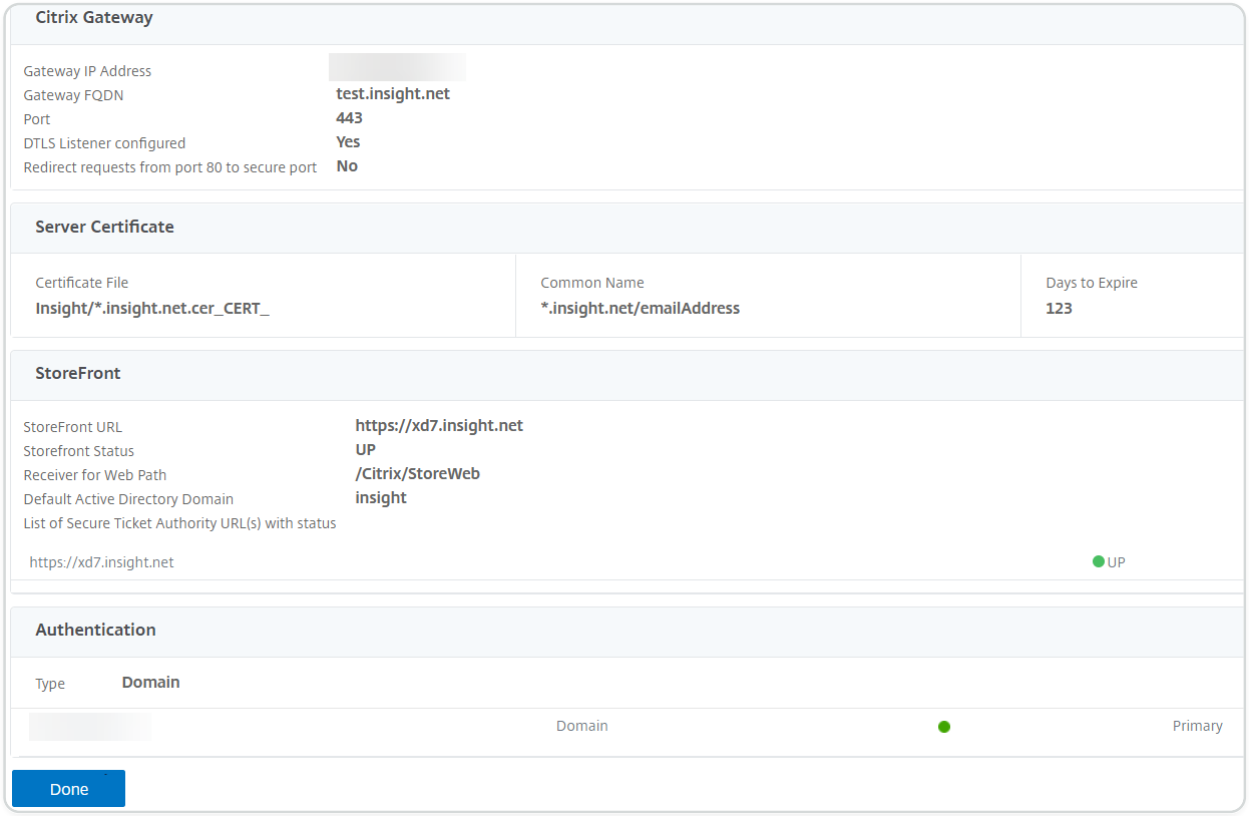
   El agente de escucha DTLS ya está configurado.
4. En Certificado de servidor, haga clic en **Elegir archivo** para seleccionar el certificado de servidor y haga clic en **Continuar**.
5. Especifique el archivo de certificado y el nombre del archivo de clave y haga clic en **Continuar**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

6. En la sección **StoreFront**, proporcione los valores para los parámetros requeridos de la siguiente manera y haga clic en **Continuar**.
7. En la sección **Autenticación**, proporcione los valores para los parámetros requeridos de la siguiente manera y haga clic en **Probar conexión**.

   Asegúrese de que el servidor sea accesible, proporcione el valor de tiempo de espera y el atributo de nombre de inicio de sesión del servidor, y haga clic en **Continuar**.

8. Haga clic en **Listo** para completar la configuración.




# Limitaciones

- DTLS 1.2 solo es compatible con clientes de Windows, macOS e iOS.
- El servidor virtual VPN con DTLS no admite direcciones IPv6.
- La política SSL y el perfil SSL no son compatibles con un servidor virtual VPN DTLS. Además, la vinculación de la política del servidor virtual VPN no es compatible.
- El servidor virtual VPN DTLS de NetScaler Gateway no admite las siguientes funciones. Sin embargo, el servidor virtual VPN SSL de NetScaler Gateway sí admite estas funciones:
  - Unified Gateway con servidor virtual de conmutación de contenido

© 1997–2026 Citrix Systems, Inc. All rights reserved.

    - MUX UDP
    - Vídeo UDP
    - Audio UDP
    - PCOIP

- No se admite el comando `stat vpn vserver` relacionado con las estadísticas del servidor virtual VPN DTLS.
- Las claves HSM no son compatibles con el servidor virtual DTLS.
- La configuración de clúster no es compatible.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

# Integración con productos Citrix®

Si usted es un administrador de sistemas responsable de instalar y configurar NetScaler Gateway, puede configurar el dispositivo para que sea compatible con Citrix Endpoint Management y StoreFront.

Los usuarios pueden conectarse directamente a Endpoint Management desde la red interna o desde una ubicación remota. Cuando los usuarios se conectan, pueden acceder a sus aplicaciones web, SaaS y móviles. También pueden admitir documentos ubicados en ShareFile desde cualquier dispositivo.

Para permitir las conexiones de usuario a una granja de servidores a través de NetScaler Gateway, debe configurar los ajustes en StoreFront y en NetScaler Gateway. Cuando los usuarios se conectan, tienen acceso a las aplicaciones publicadas y a los escritorios virtuales.

Los pasos de configuración para integrar NetScaler Gateway con Endpoint Management y StoreFront asumen lo siguiente:

- NetScaler Gateway reside en la DMZ y está conectado a una red existente.
- NetScaler Gateway se implementa como un dispositivo independiente y los usuarios remotos se conectan directamente a NetScaler Gateway.
- StoreFront, Endpoint Management, Citrix Virtual Apps y Citrix Virtual Desktops™ residen en la red segura.
- ShareFile está configurado en Endpoint Management. Para obtener más información sobre ShareFile, consulte el tema ShareFile y el tema Configuring ShareFile for User Access.

La forma en que implemente StoreFront™ y Endpoint Management depende de las aplicaciones que proporcione a los dispositivos móviles. Si los usuarios tienen acceso a aplicaciones MDX que están encapsuladas con MDX Toolkit, Endpoint Management reside delante de StoreFront en la red segura. Si no proporciona acceso a aplicaciones MDX, StoreFront reside delante de Endpoint Management en la red segura.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

# Cómo se conectan los usuarios a las aplicaciones, escritorios y ShareFile

Si tiene Citrix Endpoint Management™ en su implementación, los usuarios pueden conectarse de las siguientes maneras:

- Cliente Citrix Secure Access™ que establece un túnel VPN completo a los recursos de la red interna. Se crea un perfil de sesión para seleccionar el cliente Citrix Secure Access para Windows o el cliente Citrix Secure Access para Mac. Cuando los usuarios inician sesión mediante el complemento, se pueden ejecutar análisis de punto final en el dispositivo del usuario.

**Nota:** Para permitir que se ejecuten análisis de punto final en equipos Mac, debe instalar NetScaler Gateway 10.1, Build 120.1316.e o posterior.

- Aplicación Citrix Workspace para conectarse a aplicaciones web, SaaS y empresariales, enlaces web y documentos de ShareFile a través de Endpoint Management. Cuando los usuarios inician sesión con la aplicación Citrix Workspace, NetScaler Gateway enruta la conexión a Endpoint Management. Cuando la aplicación Citrix Workspace establece la conexión, las aplicaciones y los documentos de los usuarios aparecen en la aplicación Citrix Workspace. Si los usuarios inician sesión con la aplicación Citrix Workspace y se conectan directamente a Endpoint Management, debe habilitar el acceso sin cliente en NetScaler Gateway. Esta implementación no requiere StoreFront.
- Aplicación Citrix Workspace para conectarse a aplicaciones publicadas y escritorios virtuales a través de StoreFront. Cuando los usuarios inician sesión con la aplicación Citrix Workspace, NetScaler Gateway enruta la conexión a StoreFront. Cuando la aplicación Citrix Workspace establece la conexión, las aplicaciones y los escritorios de los usuarios aparecen en la aplicación Citrix Workspace.
- Secure Hub para conectarse a aplicaciones iOS y Android, incluidas WorxMail y WorxWeb, desde dispositivos móviles a través de Endpoint Management. Cuando los usuarios inician sesión en Secure Hub, tienen acceso a las aplicaciones móviles que configure en Endpoint Management. Cuando NetScaler Gateway establece la conexión Micro VPN, las aplicaciones móviles de los usuarios aparecen en la ventana de Secure Hub. Los usuarios pueden iniciar las aplicaciones desde Secure Hub. Algunas aplicaciones requieren que los usuarios descarguen e instalen la aplicación en el dispositivo móvil.

En cualquiera de los escenarios anteriores, si los usuarios quieren conectarse a través de NetScaler Gateway, hacen lo siguiente:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Los usuarios inician sesión mediante el cliente Citrix Secure Access o la aplicación Citrix Workspace. Para iniciar sesión por primera vez, los usuarios abren un explorador web y escriben el nombre de dominio completo (FQDN) de NetScaler Gateway o la aplicación Citrix Workspace. Los usuarios con dispositivos móviles inician sesión con Secure Hub.
- En la página de inicio de sesión, los usuarios introducen sus credenciales y se autentican.
- Después de la autenticación, la sesión del usuario se redirige a StoreFront™ o Endpoint Management, según su implementación.
- Si implementa StoreFront y Endpoint Management, NetScaler Gateway se pone en contacto con el primer servidor de la implementación. Por ejemplo, si configura aplicaciones móviles MDX en Endpoint Management, implementa StoreFront detrás de Endpoint Management. Si no proporciona acceso a aplicaciones móviles MDX, implementa Endpoint Management detrás de StoreFront.
- Todos los escritorios, documentos y aplicaciones web, SaaS y basados en Windows de los usuarios aparecen en la aplicación Citrix Workspace o en Secure Hub.

Si los usuarios necesitan acceder a otros recursos de la red interna, como Exchange, recursos compartidos de archivos o sitios web internos, también pueden iniciar sesión con el cliente Citrix Secure Access. Por ejemplo, si los usuarios quieren conectarse a un servidor de Microsoft Exchange en la red, inician Microsoft Outlook en su equipo. La conexión segura se realiza con el cliente Citrix Secure Access, que se conecta a NetScaler Gateway. El túnel SSL VPN se crea al servidor de Exchange y los usuarios pueden acceder a su correo electrónico.

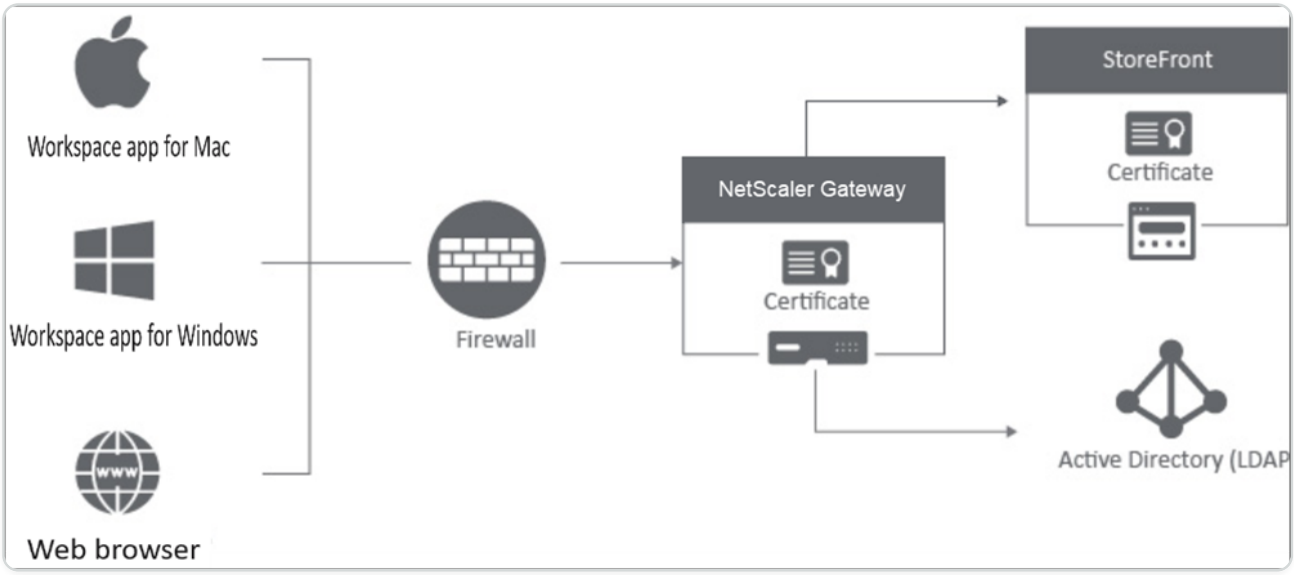
**IMPORTANTE:**

Citrix recomienda configurar la autenticación en el servidor virtual de NetScaler Gateway. Cuando se deshabilita la autenticación en NetScaler Gateway, las solicitudes HTTP no autenticadas se envían directamente a los servidores que ejecutan StoreFront o Endpoint Management en la red interna.

## Integrar NetScaler Gateway con StoreFront

Este artículo describe cómo crear un servidor virtual de NetScaler Gateway para acceder de forma remota a StoreFront, para usuarios que utilizan la aplicación Citrix Workspace o un navegador web.

© 1997–2026 Citrix Systems, Inc. All rights reserved.




Los usuarios se conectan a NetScaler Gateway a través de un navegador web o la aplicación Citrix Workspace. NetScaler Gateway autentica a los usuarios basándose en las políticas configuradas. Si la autenticación es correcta, NetScaler Gateway permite a los usuarios iniciar sesión única en el almacén y actúa como proxy del almacén de StoreFront para el usuario.

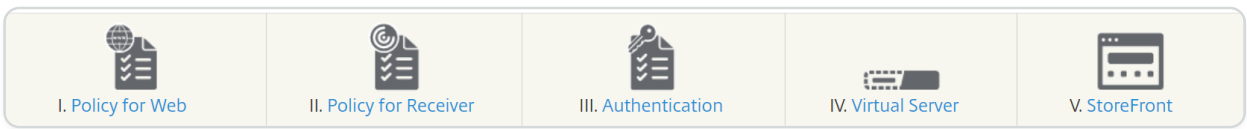
**IMPORTANTE:**

Recomendamos no utilizar el asistente de Citrix Virtual Apps and Desktops para integrar NetScaler Gateway con StoreFront, ya que crea una configuración no válida al usar las políticas de autenticación clásicas (obsoletas).

## Configurar NetScaler Gateway para usar con StoreFront

Para integrar NetScaler Gateway con StoreFront, complete los siguientes pasos:

1. Crear una directiva de sesión para el acceso basado en navegador web
2. Crear una directiva de sesión para el acceso basado en la aplicación Citrix Workspace
3. Crear un perfil de autenticación
4. Crear un servidor virtual de NetScaler Gateway
5. Agregar la instancia de NetScaler Gateway en StoreFront




### 1. Crear una directiva de sesión para el acceso basado en navegador web

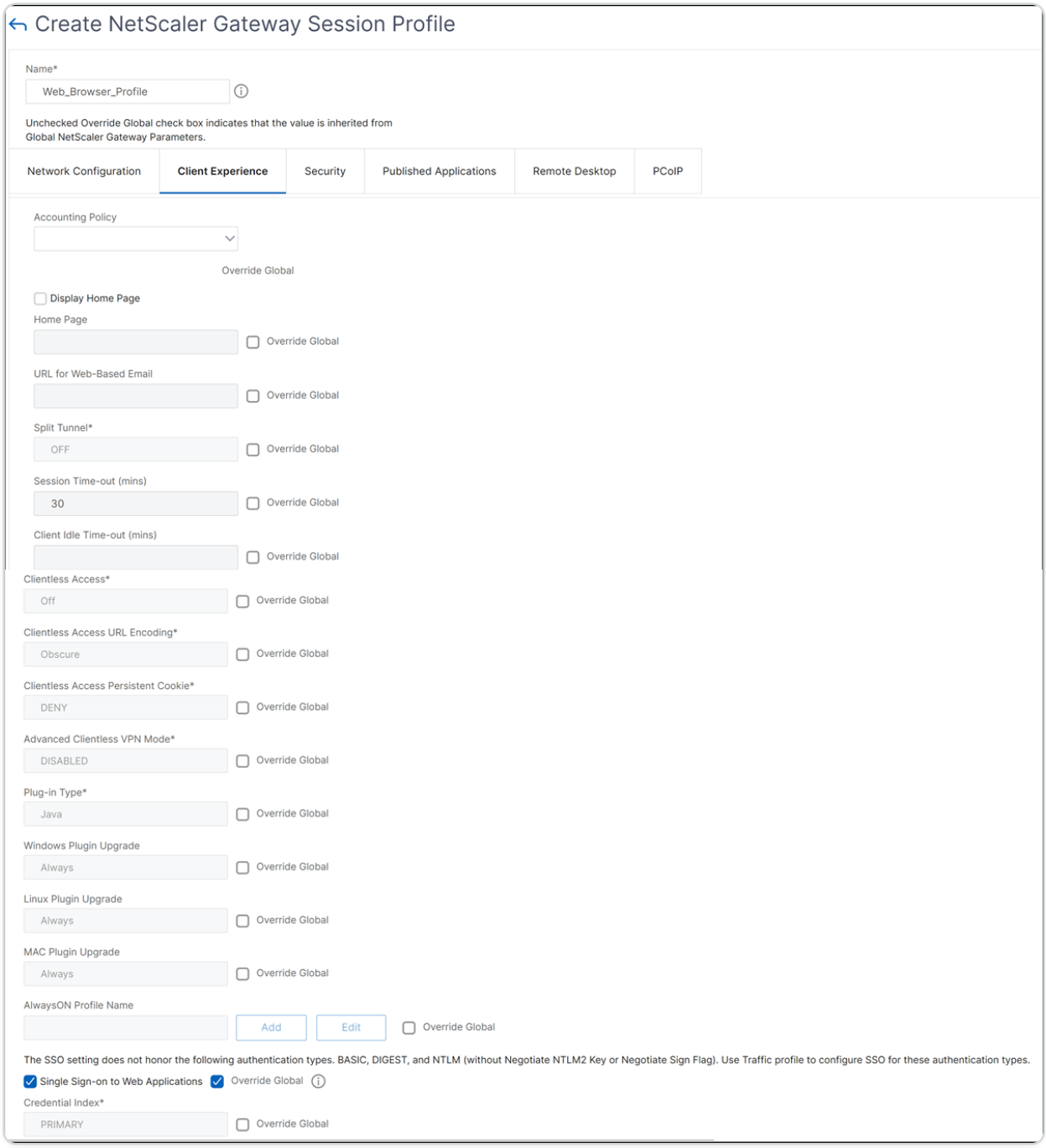
1. Vaya a **Configuración > NetScaler Gateway > Directivas > Sesión**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. En la ficha **Perfiles de sesión**, haga clic en **Agregar**.
3. Asigne un nombre al perfil de sesión.
4. En la ficha **Experiencia del cliente**, habilite las siguientes opciones:

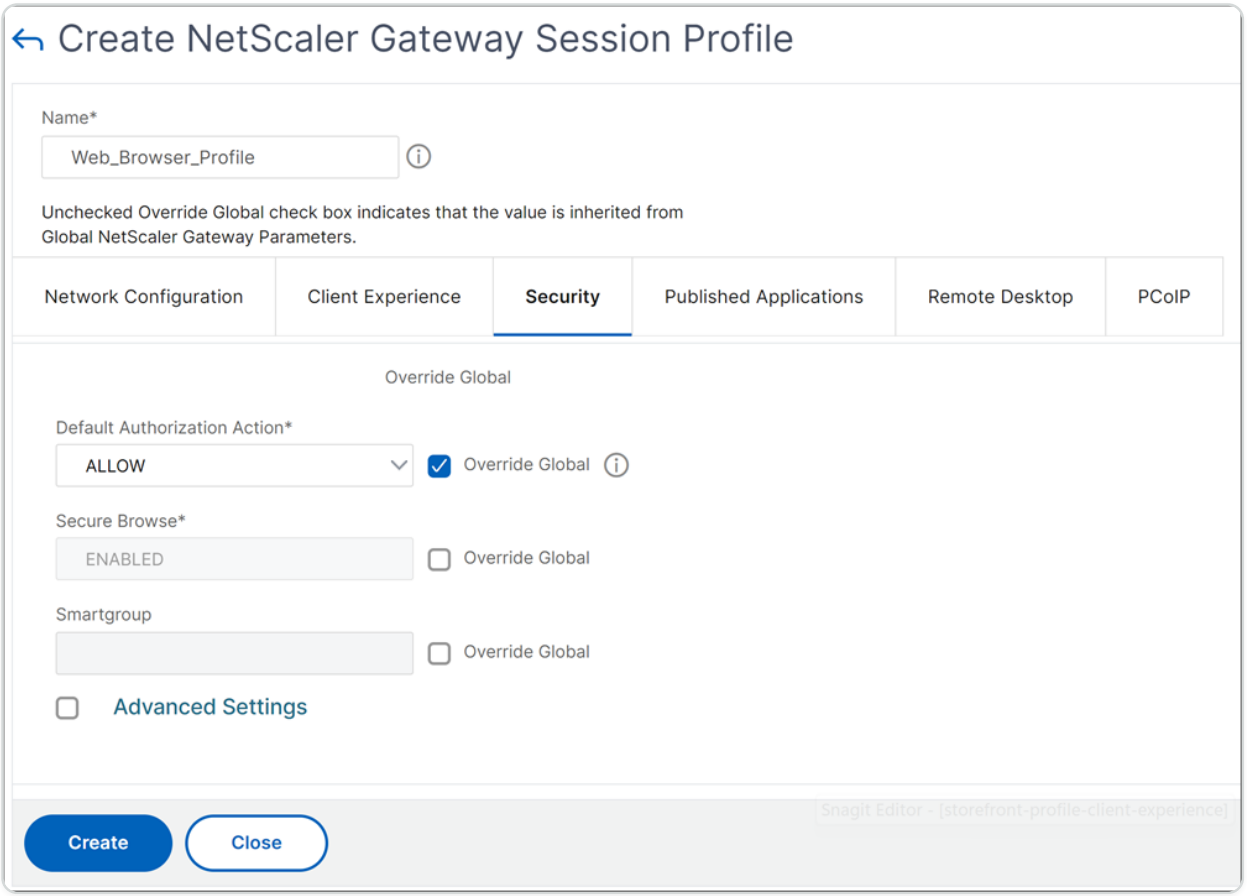
    - **Tiempo de espera de sesión (minutos)**: Se recomienda seleccionar **Anular global** aunque tenga la intención de usar la configuración global de tiempo de espera de sesión. Si no se anula explícitamente esta configuración, incluso cuando se utiliza el tiempo de espera predeterminado de 30 minutos, se pueden producir bucles de autenticación y obligar a los usuarios a volver a iniciar sesión.
    - **Tipo de plug-in**: El tipo de plug-in se establece en **Java**, de forma predeterminada. Aunque esta configuración es opcional, se recomienda si los usuarios quieren inhabilitar la VPN completa.
    - **Inicio de sesión único en la aplicación web**: Al seleccionar esta opción, cuando un usuario inicia sesión en NetScaler Gateway, se reenvían las credenciales al sitio web de StoreFront. Esta configuración evita que los usuarios tengan que introducir sus credenciales dos veces. Sin embargo, también debe habilitar el método de autenticación Pass-through from NetScaler Gateway en StoreFront. Inhabilite esta opción si requiere que los usuarios inicien sesión en NetScaler Gateway y en el almacén de StoreFront con credenciales diferentes.

© 1997–2026 Citrix Systems, Inc. All rights reserved.




5. En la ficha **Seguridad**, habilite **Acción de autorización predeterminada** y establézcala en **PERMITIR**.

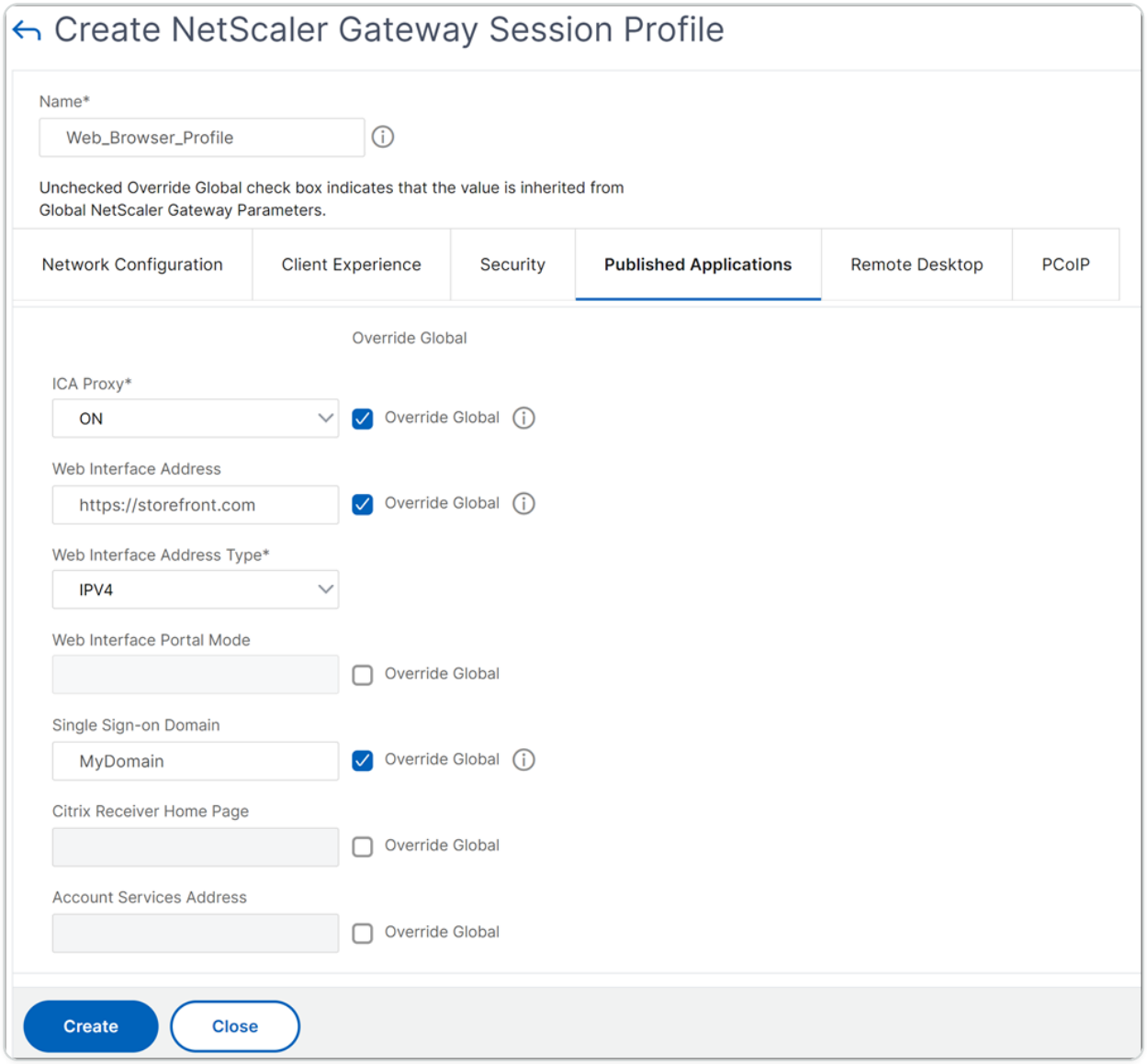
© 1997–2026 Citrix Systems, Inc. All rights reserved.




6. En la ficha **Aplicaciones publicadas**, habilite las siguientes opciones:

   - **Proxy ICA®**: Establecido en ON.
   - **Dirección de la interfaz web**: FQDN del servidor StoreFront™ seguido de la ruta al sitio web del almacén.
   - **Dominio de inicio de sesión único**: Si solo usa un dominio, introduzca opcionalmente el nombre NetBIOS del dominio.

© 1997–2026 Citrix Systems, Inc. All rights reserved.




7. Haga clic en **Crear**.
8. En la ficha **Directivas de sesión**, haga clic en **Agregar**. La directiva de sesión es necesaria para que NetScaler diferencie entre las conexiones basadas en explorador web y las basadas en la aplicación Citrix Workspace. Esta directiva se aplica a las conexiones basadas en explorador web.
9. En **Nombre**, asigne un nombre a la directiva de sesión.
10. En **Perfil**, seleccione el perfil de sesión que creó.
11. Haga clic en la opción **Directiva avanzada** e introduzca la siguiente sintaxis en **Expresión**:

    ```
    HTTP.REQ.HEADER("User-Agent").CONTAINS("CitrixReceiver").NOT
    ```

12. Haga clic en **Crear**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

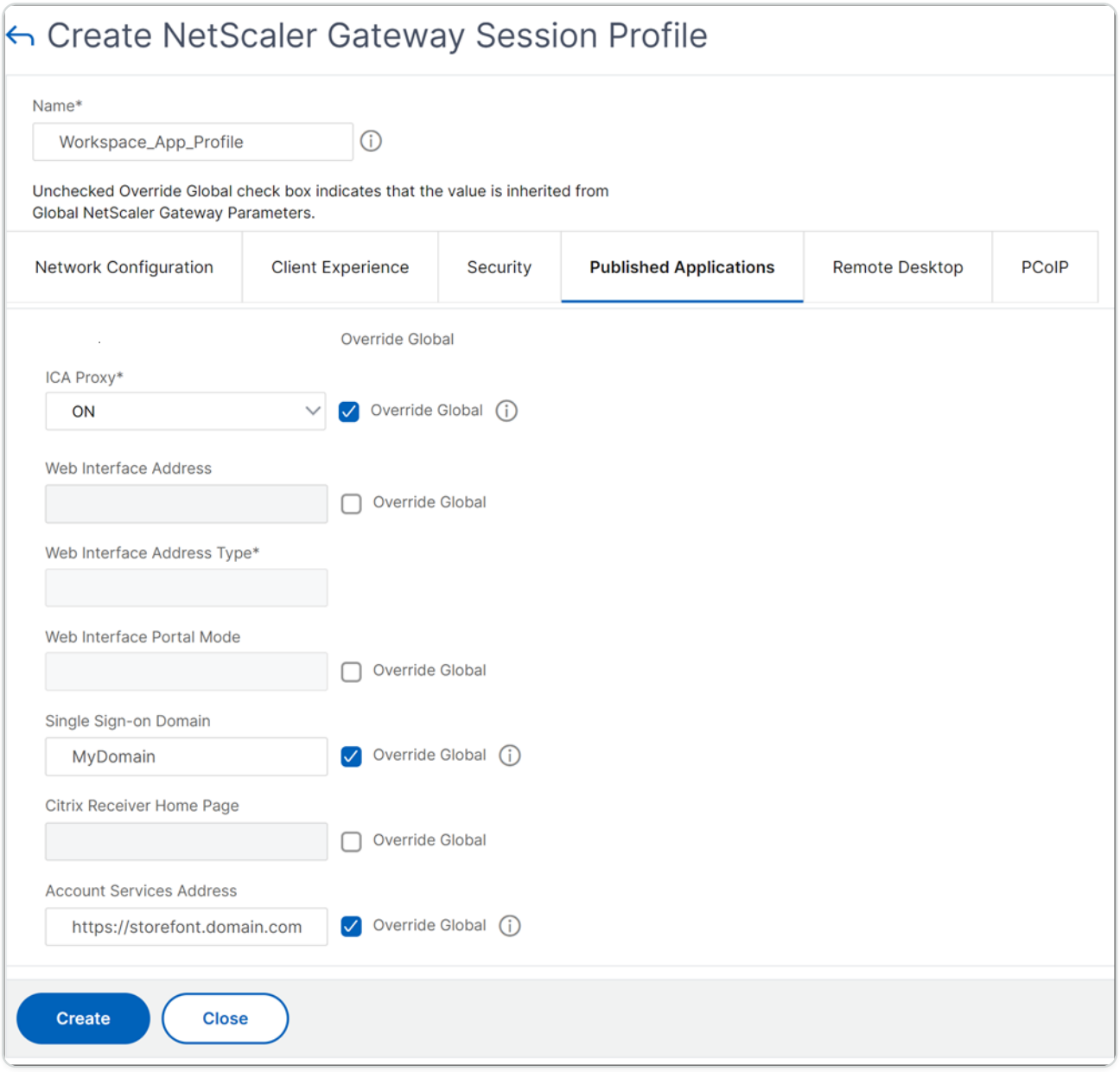



Para obtener más información sobre las directivas de sesión de NetScaler Gateway, consulte Directivas de sesión.

### 2. Crear una directiva de sesión para el acceso basado en la aplicación Citrix Workspace™

Repita los pasos anteriores para crear una directiva de sesión y un perfil de sesión para el acceso basado en la aplicación Citrix Workspace. Sin embargo, en la ficha **Aplicaciones publicadas**, en lugar de configurar la dirección de la interfaz web, debe configurar el ajuste **Dirección del servicio de cuenta**. Este paso requiere que proporcione el FQDN del servidor StoreFront. La aplicación Citrix Workspace utiliza esta dirección para detectar los almacenes disponibles en el servidor.

© 1997–2026 Citrix Systems, Inc. All rights reserved.




### 3. Crear un perfil de autenticación

Cree un perfil de autenticación en NetScaler según el tipo de método de autenticación que necesite configurar.

Aunque este paso es opcional, lo recomendamos como una buena práctica para usar NetScaler Gateway para autenticar la identidad de los usuarios antes de conceder acceso a StoreFront.

Consulte Autenticación y autorización para obtener más detalles.

### 4. Crear un servidor virtual de NetScaler® Gateway

1. Vaya a **NetScaler Gateway > Servidores virtuales**.
2. Haga clic en **Agregar** para añadir un servidor virtual de NetScaler Gateway.
3. Asigne un nombre y una dirección al servidor virtual.

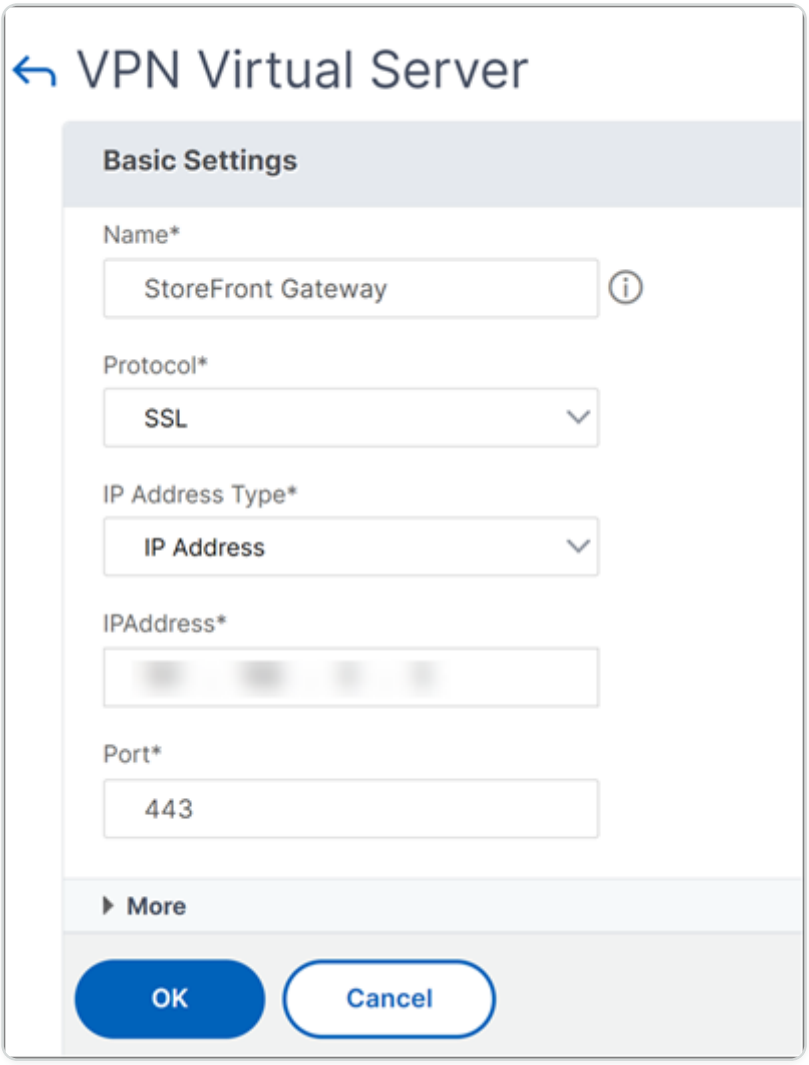
© 1997–2026 Citrix Systems, Inc. All rights reserved.

**NOTA:**

Si decide no usar NetScaler Gateway para autenticar a los usuarios, haga clic en **Más** y desactive la casilla **Habilitar autenticación**.

4. En **Certificado**, haga clic en **Certificado de servidor**.
5. Cargue un certificado de servidor y haga clic en **Enlazar**.
6. Agregue las directivas de sesión:
    a. En **Directivas**, haga clic en **+**.
    b. En la lista desplegable **Elegir directiva**, seleccione **Sesión**. En la lista desplegable **Tipo**, seleccione **Solicitud** y, a continuación, haga clic en **Continuar**.
    c. En **Enlace de directivas**, haga clic en **Seleccionar directiva** y seleccione la directiva de sesión basada en explorador web y la directiva de sesión basada en la aplicación Citrix Workspace que creó anteriormente y haga clic en **Enlazar** para enlazar las directivas de sesión al servidor virtual.
7. En **Aplicaciones publicadas**, haga clic en **Servidor STA**. Especifique al menos una URL de Security Ticket Authority (STA). Si utiliza Citrix Virtual Apps and Desktops, introduzca las URL de los Desktop Delivery Controllers. Si utiliza Citrix DaaS, introduzca las URL de los Citrix Cloud Connectors.
8. En **Perfil de autenticación**, seleccione el perfil de autenticación que creó. Este paso es necesario porque las directivas clásicas ya no son compatibles.
9. Haga clic en **Listo**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.




### 5. Agregar una instancia de NetScaler Gateway en StoreFront

Para obtener instrucciones sobre cómo agregar una instancia de NetScaler Gateway en StoreFront, consulte Configurar NetScaler Gateways.

## Referencias

Para obtener más detalles sobre la integración de StoreFront y NetScaler Gateway, consulte los siguientes temas:

- Agregar NetScaler Gateway
- Diseño de la integración de StoreFront y NetScaler Gateway

© 1997–2026 Citrix Systems, Inc. All rights reserved.

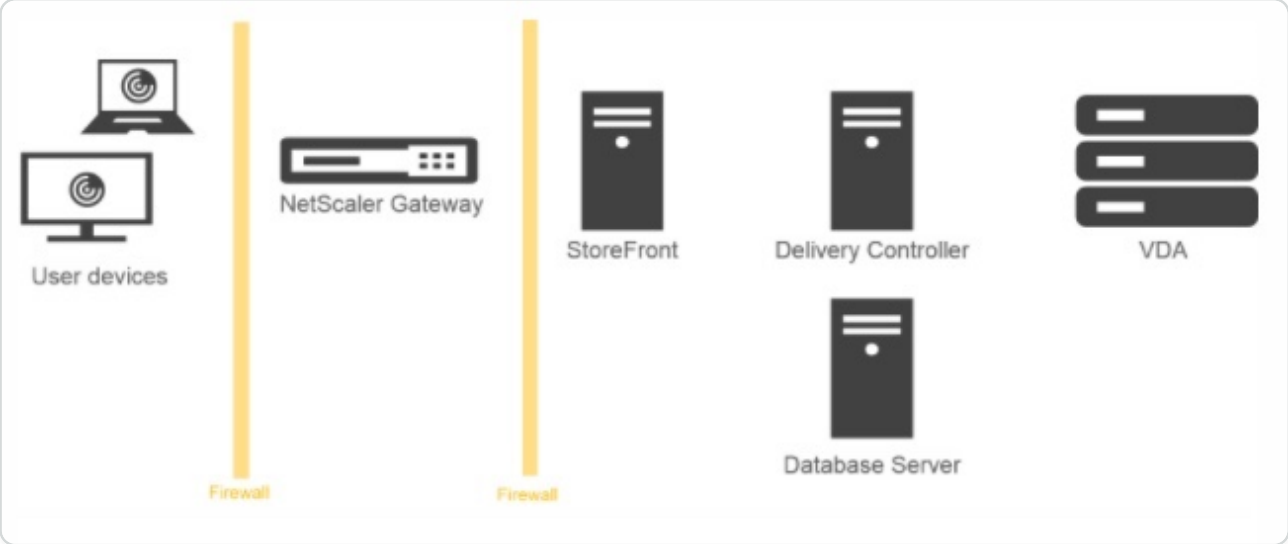
# Integrar NetScaler Gateway con Citrix Virtual Apps and Desktops

Los servidores de StoreFront se implementan y configuran para gestionar el acceso a los recursos y datos publicados. Para el acceso remoto, se recomienda añadir NetScaler Gateway delante de StoreFront.

**NOTA**

Para obtener pasos de configuración detallados sobre cómo integrar Citrix Virtual Apps and Desktops con NetScaler Gateway, consulte la documentación de StoreFront.

El siguiente diagrama ilustra un ejemplo de una implementación simplificada de Citrix que incluye NetScaler Gateway. NetScaler Gateway se comunica con StoreFront para proteger las aplicaciones y los datos entregados por Citrix Virtual Apps and Desktops. Los dispositivos de usuario ejecutan la aplicación Citrix Workspace para crear una conexión segura y acceder a sus aplicaciones, escritorios y archivos.




Los usuarios inician sesión y se autentican mediante NetScaler Gateway. NetScaler Gateway se implementa y protege en la DMZ. La autenticación de dos factores está configurada. Según las credenciales del usuario, se le proporcionan los recursos y las aplicaciones pertinentes. Las aplicaciones y los datos se encuentran en los servidores adecuados (no se muestran en el diagrama). Se utilizan servidores separados para las aplicaciones y los datos sensibles a la seguridad.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

# Implementación con Citrix Endpoint Management™, Citrix Virtual Apps and Desktop

Puede hacer que los usuarios se conecten a aplicaciones Windows, web, SaaS y móviles, y a escritorios virtuales alojados en su red. Puede proporcionar acceso a sus aplicaciones y escritorios a usuarios remotos e internos mediante NetScaler Gateway, Citrix Endpoint Management y Citrix Virtual Apps and Desktops. NetScaler Gateway autentica a los usuarios y, a continuación, les permite acceder a sus aplicaciones mediante la aplicación Citrix Workspace o Secure Hub.

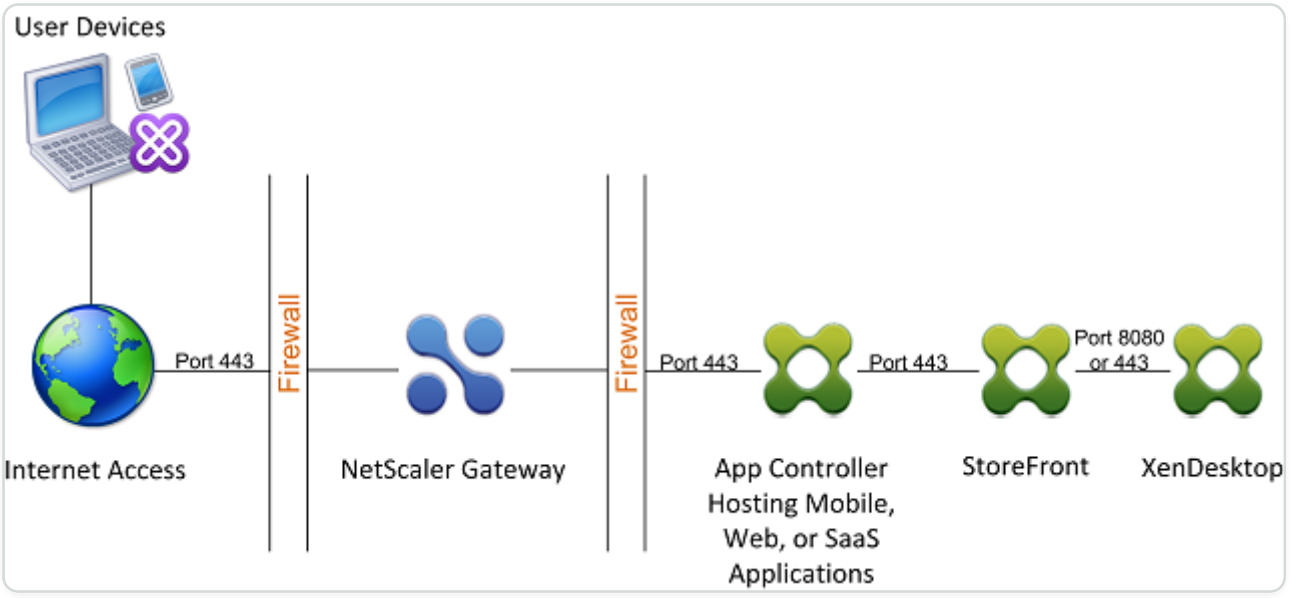
Los usuarios se conectan a sus aplicaciones basadas en Windows publicadas en Citrix Virtual Apps y a los escritorios virtuales publicados en Citrix Virtual Desktops mediante la aplicación Citrix Workspace y StoreFront.

Citrix Endpoint Management contiene Citrix Endpoint Management, que permite a los usuarios conectarse a aplicaciones web, SaaS y MDX. Endpoint Management le permite administrar aplicaciones web, SaaS y MDX para el inicio de sesión único (SSO), junto con los documentos de ShareFile. Instale Endpoint Management en la red interna. Los usuarios remotos se conectan a Endpoint Management a través de NetScaler Gateway para acceder a sus aplicaciones y datos de ShareFile. Los usuarios remotos pueden conectarse con el cliente Citrix Secure Access, la aplicación Citrix Workspace o Secure Hub para acceder a las aplicaciones y a ShareFile. Los usuarios que se encuentran en la red interna pueden conectarse directamente a Endpoint Management mediante la aplicación Citrix Workspace. La siguiente figura muestra NetScaler Gateway implementado con Endpoint Management y StoreFront.

Si su implementación proporciona acceso a aplicaciones MDX desde Endpoint Management y acceso a aplicaciones basadas en Windows desde StoreFront™, implemente Endpoint Management delante de StoreFront, como se muestra en la siguiente ilustración:

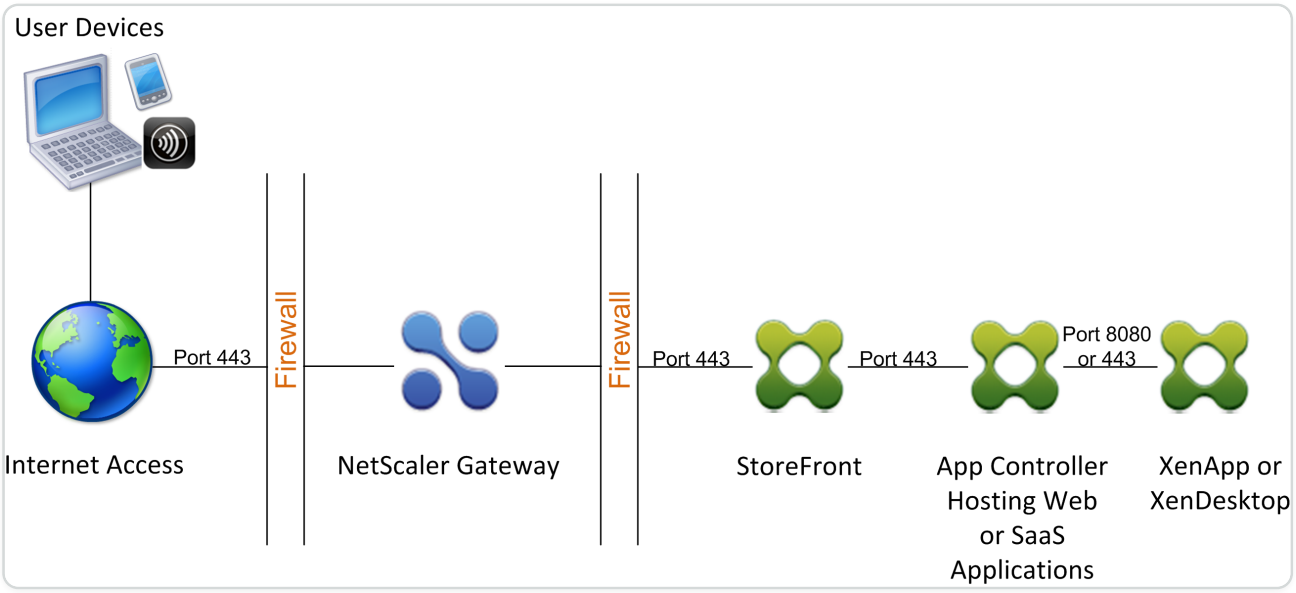
Figura 1. Implementación de NetScaler Gateway con Endpoint Management delante de StoreFront

© 1997–2026 Citrix Systems, Inc. All rights reserved.




Si su implementación no proporciona acceso a aplicaciones MDX, StoreFront reside delante de Endpoint Management, como se muestra en la siguiente ilustración:

Figura 2. Implementación de NetScaler Gateway con StoreFront delante de Endpoint Management




Con cada implementación, StoreFront y Endpoint Management deben residir en la red interna y NetScaler Gateway debe estar en la DMZ. Para obtener más información sobre la implementación de Endpoint Management, consulte el tema Instalación de Endpoint Management. Para obtener más información sobre la implementación de StoreFront, consulte el tema StoreFront.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

# Configuración de los ajustes para su entorno de Citrix Endpoint Management™

El asistente de NetScaler para Citrix Endpoint Management le guía a través de la configuración de las funciones de NetScaler para su implementación de Citrix Endpoint Management. Puede usar el asistente para:

- **Configurar una Micro VPN.** En este escenario, los usuarios remotos pueden acceder a aplicaciones y escritorios en la red interna.
  - Para el modo solo MAM de Citrix Endpoint Management, debe usar NetScaler Gateway para la autenticación.
  - Para implementaciones de MDM, Citrix recomienda NetScaler Gateway para VPN de dispositivos móviles.
  - Para implementaciones ENT, si un usuario opta por no inscribirse en MDM, el dispositivo funciona en el modo MAM heredado y se inscribe utilizando el FQDN de NetScaler Gateway.
- **Configurar la autenticación basada en certificados.** La configuración predeterminada para Citrix Endpoint Management es la autenticación de nombre de usuario y contraseña. Para añadir otra capa de seguridad para la inscripción y el acceso al entorno de Citrix Endpoint Management, considere usar la autenticación basada en certificados.
- **Equilibre la carga de los servidores de Citrix Endpoint Management.** El equilibrio de carga de NetScaler es necesario para todos los modos de dispositivo de Citrix Endpoint Management si tiene varios servidores de este o si la plataforma está dentro de su DMZ o red interna (y, por lo tanto, el tráfico fluye desde los dispositivos a NetScaler y a ella). En este escenario, el dispositivo NetScaler reside en la DMZ entre el dispositivo de usuario y los servidores de Citrix Endpoint Management para equilibrar la carga de los datos cifrados enviados desde los dispositivos móviles a estos.
- **Equilibrar la carga de los servidores de Microsoft Exchange con filtrado de correo electrónico.** En este escenario, el dispositivo NetScaler se encuentra entre el dispositivo de usuario y el conector NetScaler de Citrix Endpoint Management (XNC), y entre el dispositivo de usuario y los servidores CAS de Microsoft Exchange. Todas las solicitudes de los dispositivos de usuario van al dispositivo NetScaler Gateway, que luego se comunica con el XNC para recuperar información sobre el dispositivo. Dependiendo de la respuesta del XNC, el dispositivo NetScaler reenvía la solicitud de un dispositivo en la lista blanca al servidor de la red interna, o descarta la conexión de un dispositivo en la lista negra.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Equilibrar la carga de los conectores de ShareFile StorageZones según el tipo de contenido solicitado.** Este escenario le solicita información básica sobre su entorno de controlador de zonas de almacenamiento y luego genera una configuración que realiza lo siguiente:
  - Equilibra la carga del tráfico entre los controladores de zonas de almacenamiento.
  - Proporciona autenticación de usuario para los conectores de StorageZones.
  - Valida las firmas URI para las cargas y descargas de ShareFile.
  - Finaliza las conexiones SSL en el dispositivo NetScaler.

Para obtener más información sobre la configuración de ShareFile, consulte Configurar NetScaler para el controlador de zonas de almacenamiento.

**IMPORTANTE:**

Antes de usar el asistente de Citrix Endpoint Management, asegúrese de consultar estos artículos de implementación de Citrix Endpoint Management para obtener información y recomendaciones de diseño e implementación:

Integración de Citrix Endpoint Management
Integración con NetScaler Gateway y NetScaler
Consideraciones de SSO y proxy para aplicaciones MDX
Autenticación
Puede usar el asistente de NetScaler para Citrix Endpoint Management solo una vez. Si desea varias instancias de Citrix Endpoint Management, como para entornos de prueba, desarrollo y producción, debe configurar NetScaler para los entornos adicionales manualmente. Los siguientes artículos de soporte enumeran los comandos ejecutados por el asistente y proporcionan instrucciones para ejecutarlos y crear una instancia de NetScaler:
Comandos generados por el asistente de Citrix Endpoint Management en NetScaler - Puente SSL
Comandos generados por el asistente de Citrix Endpoint Management en NetScaler - Descarga SSL

## Requisitos de licencia para las funciones de NetScaler

Debe instalar licencias para habilitar las siguientes funciones de NetScaler:

- El equilibrio de carga de MDM de Citrix Endpoint Management requiere una licencia estándar de NetScaler.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- El equilibrio de carga de ShareFile con StorageZones requiere una licencia estándar de NetScaler.
- El equilibrio de carga de Exchange requiere una licencia de NetScaler o una licencia Advanced con la adición de una licencia de Integrated Caching.

## Asistente de NetScaler para Citrix Endpoint Management

Esta sección proporciona un ejemplo de cómo usar el asistente de NetScaler para Citrix Endpoint Management para:

- Configurar el acceso micro VPN para conexiones de usuarios remotos a recursos administrados por Citrix Endpoint Management en su red interna
- Configurar la autenticación basada en certificados. Para obtener información sobre cómo obtener e instalar un certificado SSL público, consulte Instalación y administración de certificados.
- Configurar el equilibrio de carga para los servidores de Citrix Endpoint Management.

Para usar el asistente:

1. En la GUI de NetScaler®, haga clic en la ficha **Configuration** y, a continuación, en **XenMobile** en la sección **Integrate with Citrix® Products**.
2. Seleccione su versión de Citrix Endpoint Management y, a continuación, haga clic en **Get Started**.
3. Seleccione las funciones que desea configurar. Solo puede usar este asistente una vez, por lo que debe realizar la configuración posterior manualmente. Estas instrucciones asumen que selecciona las siguientes opciones: **Access through NetScaler Gateway** (para Citrix Endpoint Management que se ejecuta en los modos ENT o MAM) y **Load Balance Citrix Endpoint Management Servers**.
4. En la página **NetScaler Gateway Configuration**, introduzca los valores para la dirección IP de NetScaler Gateway, el puerto y el nombre del servidor virtual.
5. En la página **Server Certificate for NetScaler Gateway**, en **Certificate File**, elija el archivo de certificado de **Local** o **Appliance**.
    - Local: Seleccione el certificado en su equipo
    - Appliance: Seleccione el certificado en NetScaler Gateway (dispositivo).
6. En la página **Authentication**, en **Primary authentication method**, seleccione **Client Certificate** y, a continuación, introduzca un nombre para el perfil de certificado.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Los siguientes pasos asumen que ya tiene una directiva de certificado.

Si debe crear una directiva de certificado, haga clic en crear una directiva de certificado. En la pantalla Citrix Endpoint Management Certificate, elija un certificado de servidor existente o instale uno nuevo. Si ejecuta varios servidores de Citrix Endpoint Management, agregue un certificado para cada uno. Para el atributo de nombre de inicio de sesión del servidor, especifique userPrincipalName o sAMAccountName, según sus requisitos.

7. Haga clic en **Doble factor** para habilitar la autenticación de doble factor, la autenticación de certificado de cliente seguida de LDAP o RADIUS como tipo de autenticación secundaria.
8. En **Método de autenticación secundaria**, seleccione el método de autenticación secundaria.

   - Con el certificado de cliente como tipo de autenticación principal, tiene la opción de configurar LDPA (o RADIUS) como tipo de autenticación secundaria.

     Para usar solo la autenticación de certificado de cliente, deje **Segundo método de autenticación** como **Ninguno** y, a continuación, haga clic en **Continuar**.

     Para usar la autenticación de certificado de cliente + dominio (LDAP), cambie **Método de autenticación secundaria** a **LDAP** y configure los ajustes del servidor de autenticación.

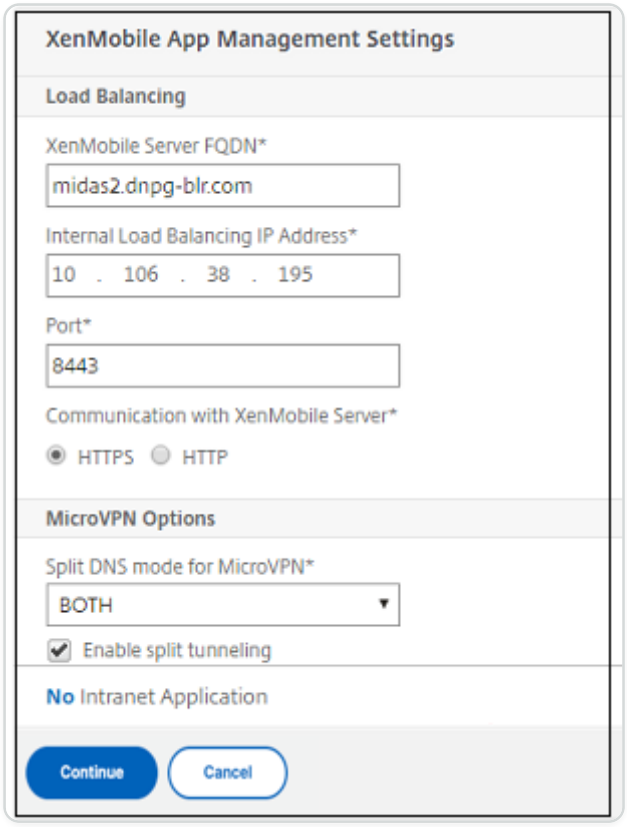
9. Configure la **Configuración de administración de aplicaciones de Citrix Endpoint Management**.

   - Introduzca el **FQDN de Citrix Endpoint Management**. Este es el FQDN de equilibrio de carga para MAM.
   - Introduzca una **Dirección IP de equilibrio de carga interna** solo para MAM para el servidor virtual que equilibra la carga de los servidores de Citrix Endpoint Management. NetScaler Gateway se comunica con Citrix Endpoint Management a través de esta IP virtual de equilibrio de carga de MAM.
   - Esta es una implementación de descarga SSL, así que seleccione **HTTP** en **Comunicación con el servidor de Citrix Endpoint Management**.
   - El campo **Modo DNS dividido para MicroVPN** se establece automáticamente en **AMBOS**.

   Si su implementación requiere tunelización dividida, seleccione **Habilitar tunelización dividida**. A continuación, configure el enlace de aplicaciones de intranet si habilita la tunelización dividida.

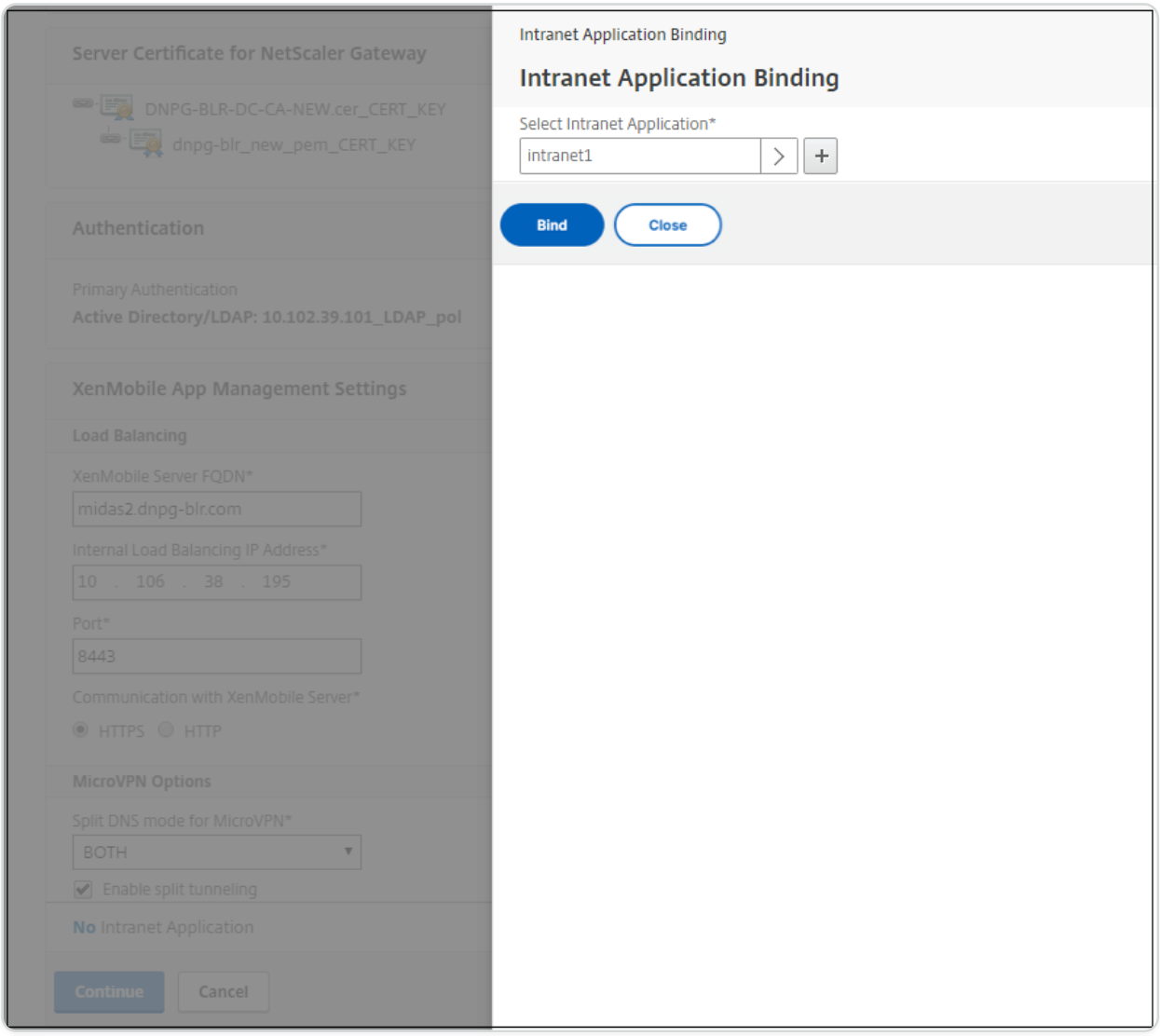
   De forma predeterminada, el acceso a Secure Web se tuneliza a la red interna, lo que significa que Secure Web utiliza un túnel VPN por aplicación de vuelta a la red interna para todo el acceso a la red y el dispositivo NetScaler utiliza la configuración de túnel dividido.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

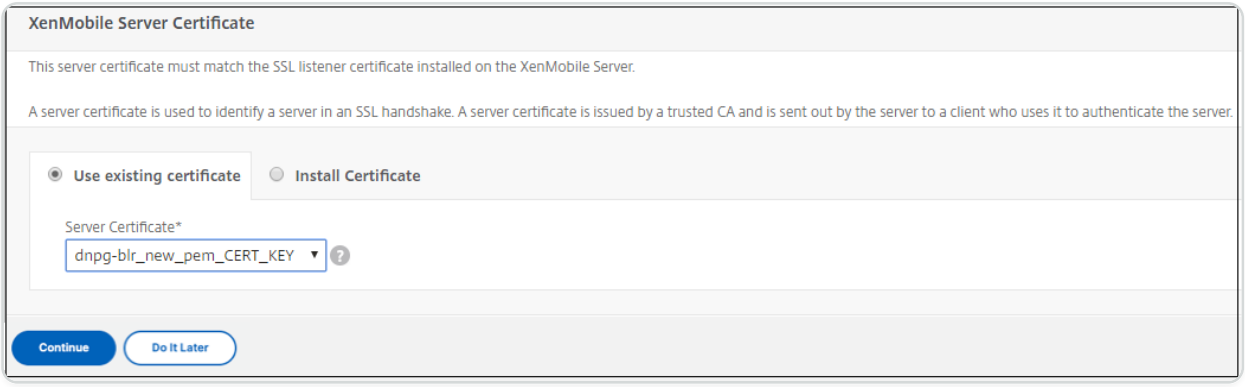



10. Para configurar reglas de intercepción para las conexiones de usuario en NetScaler Gateway, debe configurar el **Enlace de aplicaciones de intranet**. Haga clic en **+** para agregar un enlace.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

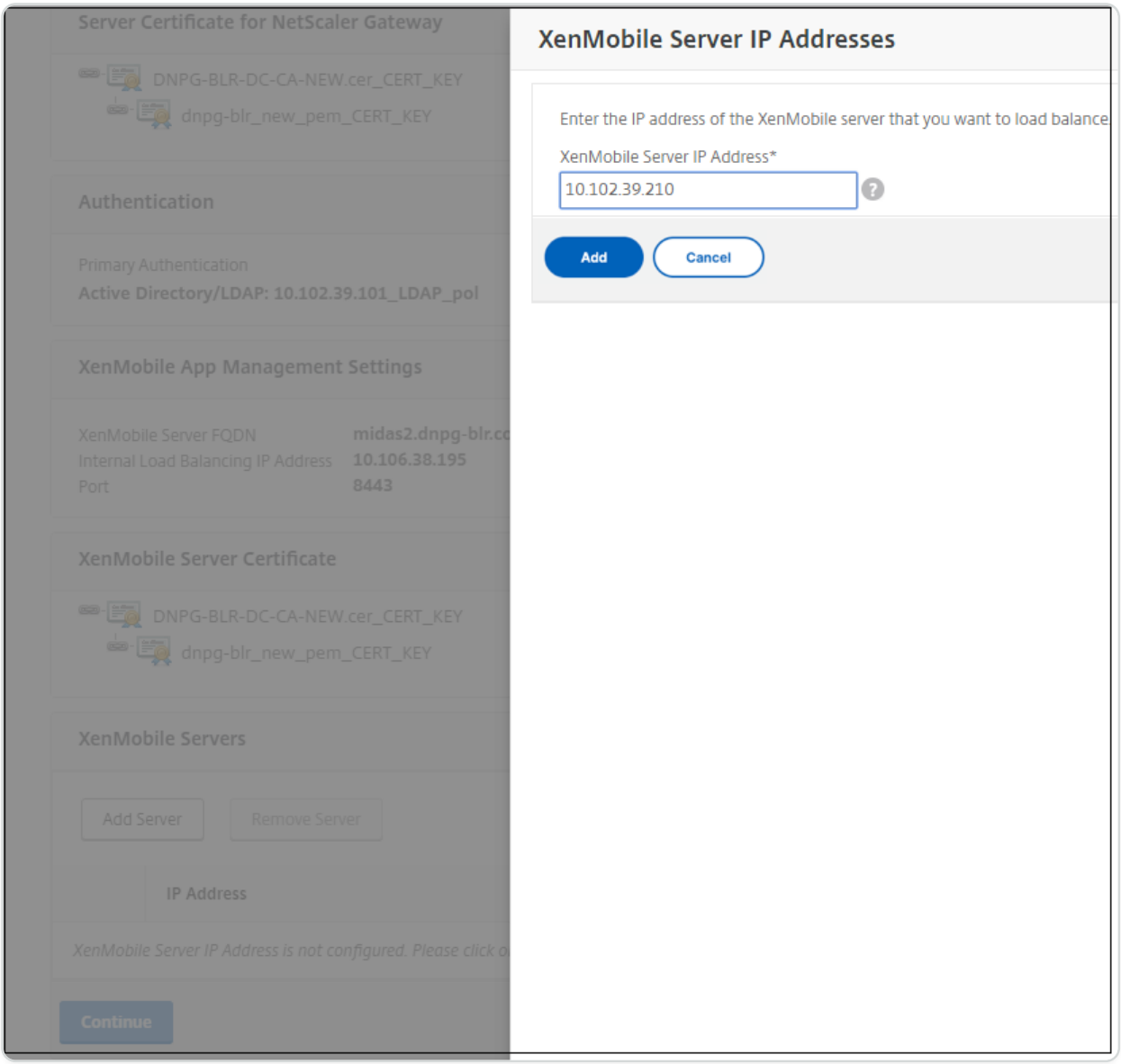



11. Complete los parámetros para permitir el acceso a la red y, a continuación, haga clic en **Crear**.
12. Agregue el certificado de Citrix Endpoint Management. Se utiliza para el servidor virtual de equilibrio de carga de MAM.



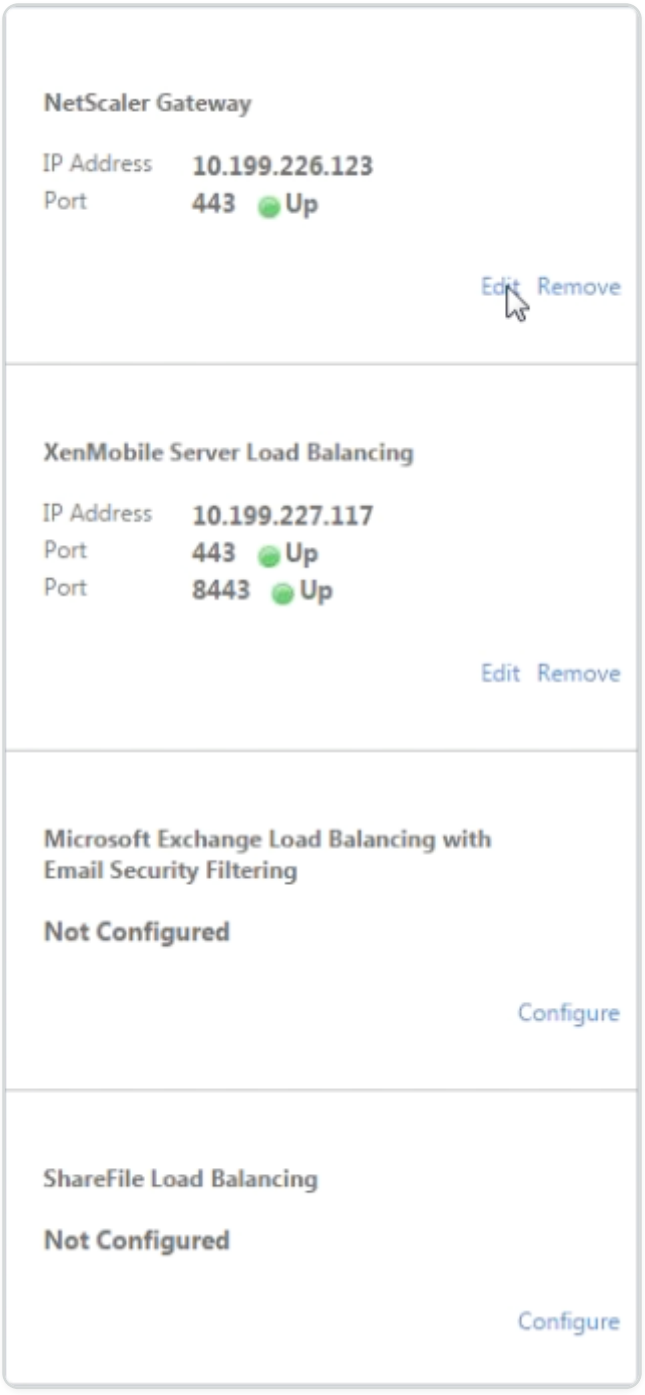

13. En **Citrix Endpoint Management Servers**, haga clic en **Add Server** para agregar la **Citrix Endpoint Management IP Address** para enlazarla a la IP virtual de equilibrio de carga.

© 1997–2026 Citrix Systems, Inc. All rights reserved.




En el panel de NetScaler, confirme que NetScaler Gateway y el equilibrio de carga de Citrix Endpoint Management están configurados.

© 1997–2026 Citrix Systems, Inc. All rights reserved.




Si utiliza los sAMAccount attributes en los certificados de usuario como alternativa a User Principal Name (UPN), configure el perfil de certificado como se describe en Configurar el certificado de cliente o el certificado de cliente y la autenticación de dominio.

## Configurar servidores de equilibrio de carga para Citrix Endpoint Management o Citrix XenMobile Server

Después de usar el asistente de **NetScaler para Citrix Endpoint Management** para la configuración inicial, utilice la utilidad de configuración de NetScaler Gateway para configurar el equilibrio de carga, como se describe en esta sección. Para Citrix Endpoint Management, utilice la descarga SSL. Para Citrix Endpoint Management Server, asegúrese de consultar las

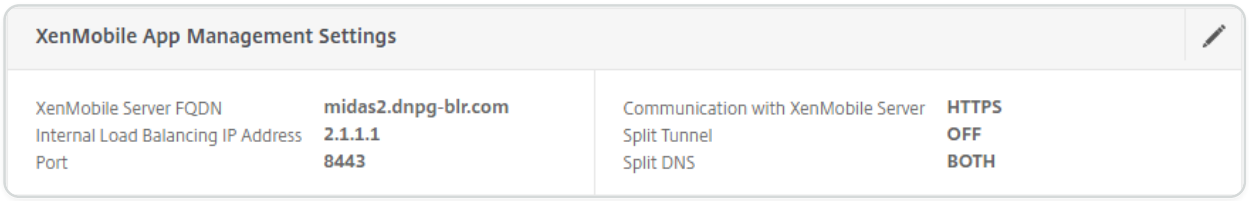
© 1997–2026 Citrix Systems, Inc. All rights reserved.

recomendaciones para los modos de equilibrio de carga en "Resumen de implementación" en Integración con NetScaler Gateway y NetScaler.

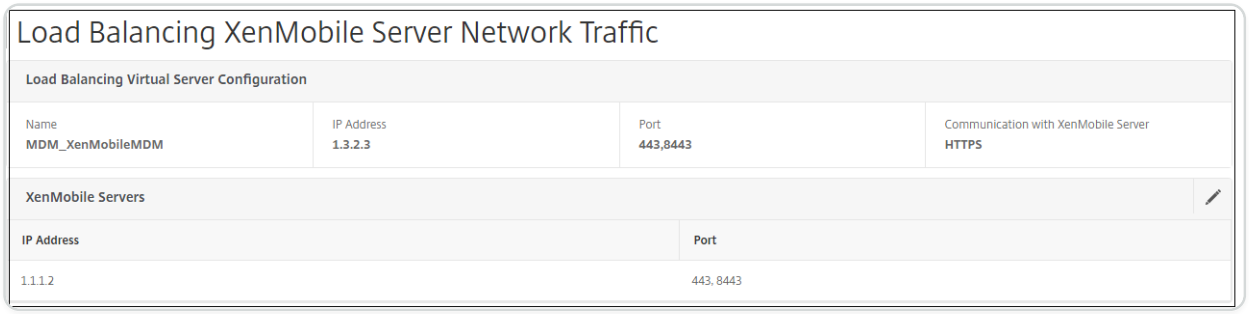
### Para usar el modo puente SSL para VIP de NetScaler

Utilice el modo puente SSL si Citrix Endpoint Management está en la DMZ. Cuando equilibra la carga de Citrix Endpoint Management con VIP de NetScaler en modo puente SSL, el tráfico de Internet fluye directamente al servidor de Citrix Endpoint Management, donde terminan las conexiones. El modo puente SSL es el modo más sencillo de configurar y solucionar problemas.

1. Antes de configurar el modo puente SSL, vaya a **Configuración de administración de aplicaciones de Citrix Endpoint Management** y verificar que la **Comunicación con el servidor de Citrix Endpoint Management** sea **HTTPS**.

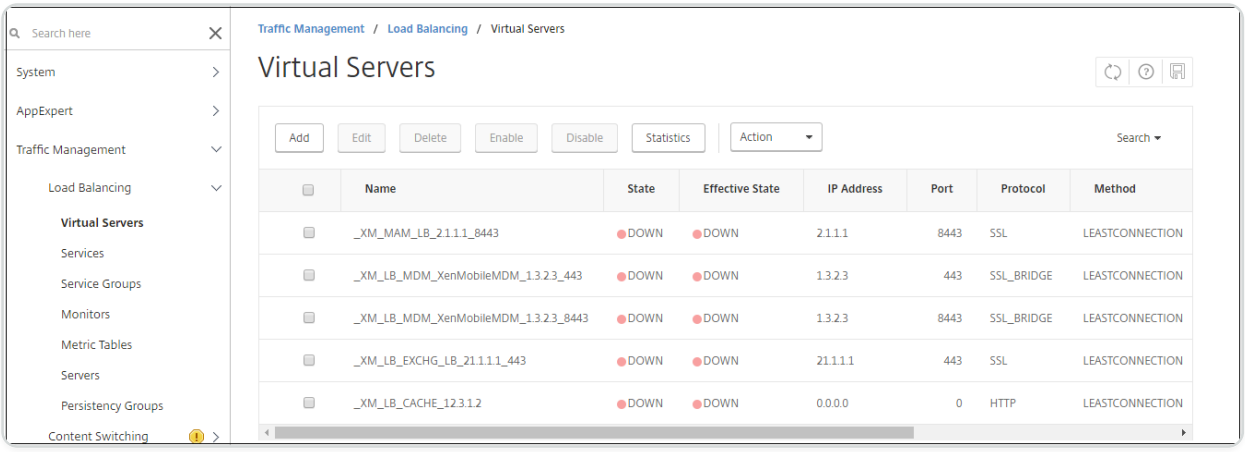



2. Después de iniciar sesión en la utilidad de configuración, en la ficha **Inicio**, en **MDM Server LB**, haga clic en **Configurar**.
3. En **Servidor virtual LB para administración de dispositivos**, en **Nombre**, escriba un nombre para el servidor.
4. En **Dirección IP**, escriba la dirección IP del servidor virtual y, a continuación, haga clic en **Continuar**.
5. En la página **Equilibrar carga de servidores MDM de Citrix Endpoint Management**, repita los pasos 3 y 4 y, a continuación, haga clic en **Crear**.
6. verificar que la configuración sea correcta y, a continuación, haga clic en **Listo**.




7. Para verificar la configuración de equilibrio de carga, vaya a **Administración de tráfico \> Servidores virtuales**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.




### Para usar el modo de descarga SSL para VIP de NetScaler

Utilice la descarga SSL para Citrix Endpoint Management. Utilice también la descarga SSL, si es necesario para cumplir los estándares de seguridad, cuando Citrix Endpoint Management local se encuentre en la red interna. Cuando equilibra la carga de Citrix Endpoint Management con VIP de NetScaler en modo de descarga SSL, el tráfico de Internet fluye directamente al dispositivo NetScaler, donde finalizan las conexiones. NetScaler Gateway establece nuevas sesiones desde el dispositivo a Citrix Endpoint Management. El modo de descarga SSL implica una mayor complejidad durante la configuración y la solución de problemas.

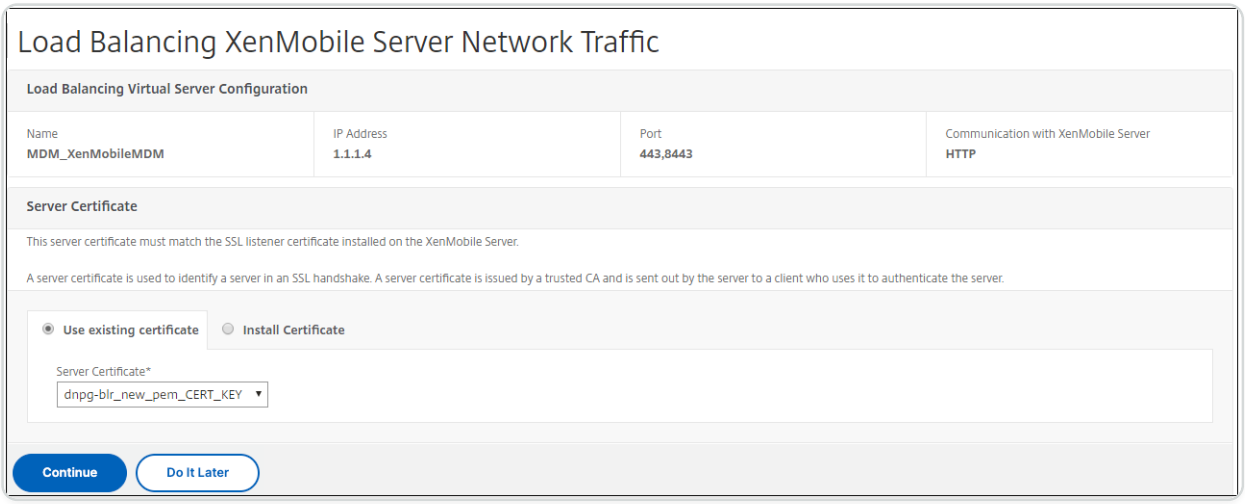
1. Antes de configurar el modo de descarga SSL, vaya a **Configuración de administración de aplicaciones de Citrix Endpoint Management** y verificar que la **Comunicación con el servidor de Citrix Endpoint Management** sea **HTTP**.



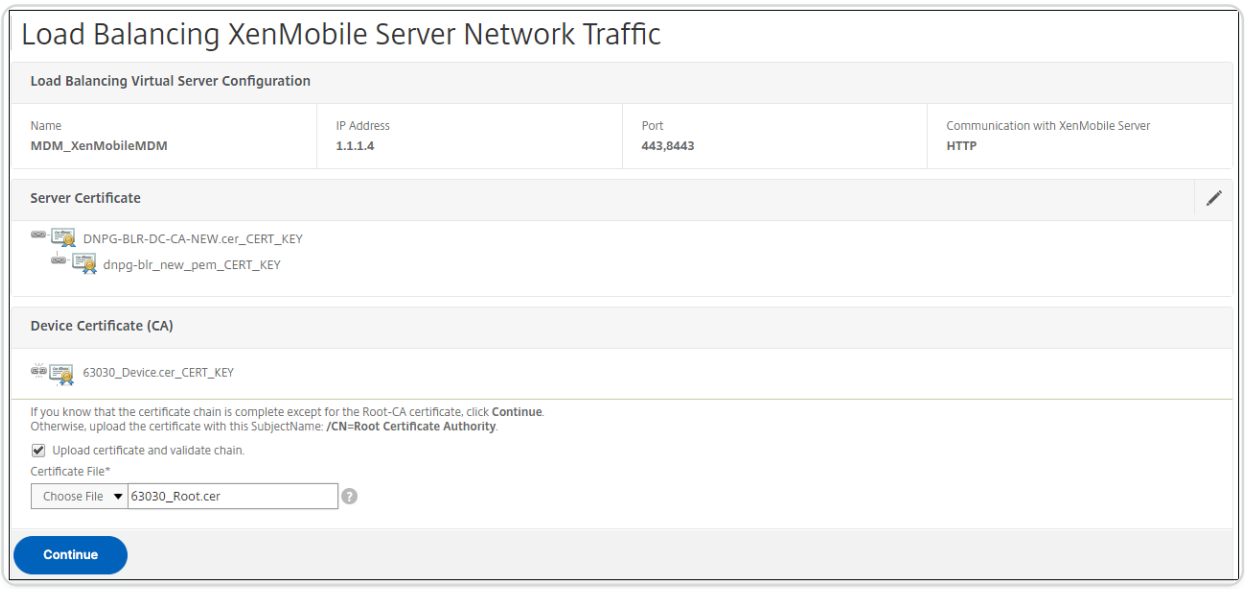

2. Inicie sesión en la utilidad de configuración. En la ficha **Inicio**, en **MDM Server LB**, haga clic en **Configurar**.
3. En **Servidor virtual LB para la administración de dispositivos**, en **Nombre**, escriba un nombre para el servidor.
4. En **Dirección IP**, escriba la dirección IP del servidor virtual y, a continuación, haga clic en **Continuar**.
5. En la página **Equilibrar la carga de los servidores MDM de Citrix Endpoint Management**, repita los pasos 3 y 4 y, a continuación, haga clic en **Crear**.
6. verificar la configuración y, a continuación, haga clic en **Listo**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

7. Cuando se le solicite agregar un certificado de servidor, elija el certificado de servidor y haga clic en **Continuar**.

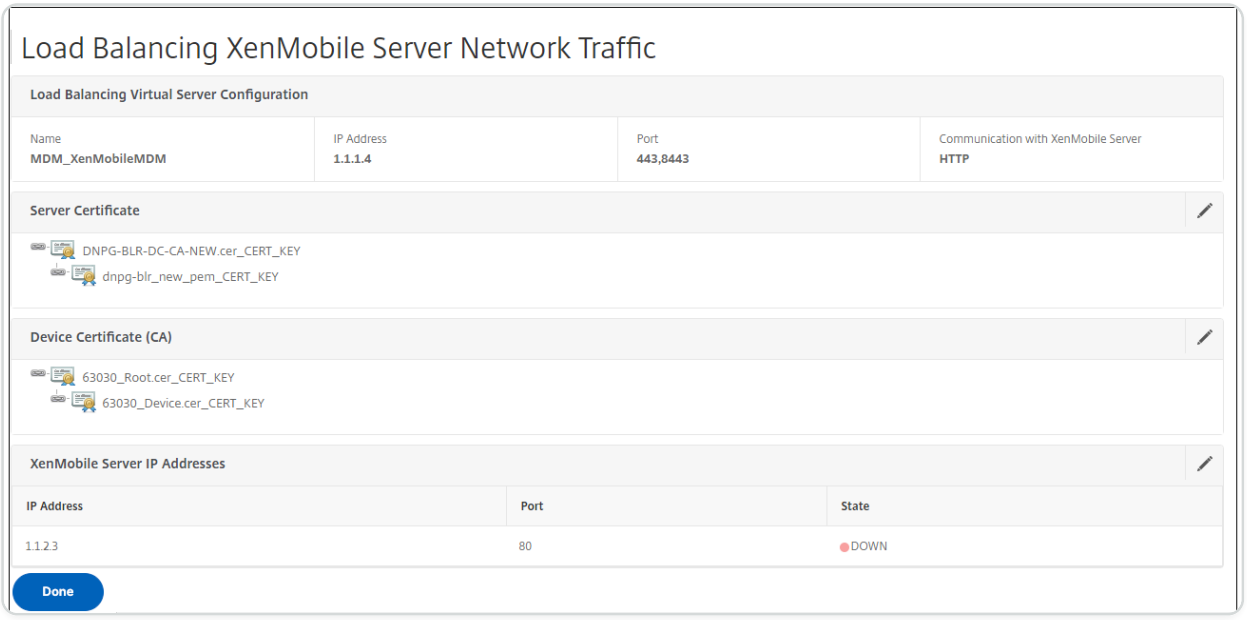



8. Especifique el certificado de CA y haga clic en **Continuar**.




9. Mantenga la misma dirección IP de Citrix Endpoint Management. Haga clic en **Listo**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.




10. Para verificar la configuración de equilibrio de carga, vaya a **Administración de tráfico \> Servidores virtuales**.

    Validar en la página de servidores virtuales(/en-us/netscaler-gateway/media/ssl-offload-setup-5.png)

## Configurar servidores de equilibrio de carga para Microsoft Exchange con filtrado de seguridad de correo electrónico

1. En la ficha **Inicio**, en **MDM Server LB**, haga clic en **Configurar**.
2. En **Servidor virtual LB para Exchange CAS**, en **Nombre**, escriba un nombre para el servidor.
3. En **Dirección IP**, escriba la dirección IP del servidor virtual.
4. En **Puerto**, escriba el número de puerto. Para agregar más puertos, haga clic en el signo más (**+**) y, a continuación, escriba el número de puerto.
5. Haga clic en **Continuar**.

   Página de LB del servidor MDM(/en-us/netscaler-gateway/media/exchange-client-access-servers-1.png)
6. En **Certificados**, elija un certificado existente o instale uno que esté en su equipo (**Local**) o en el dispositivo NetScaler (**Appliance**).
7. Haga clic en **Continuar**.

   Usar certificado existente(/en-us/netscaler-gateway/media/exchange-client-access-servers-2.png)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

8. En **Instancias del servicio Exchange Citrix Analytics**, escriba un nombre, una dirección IP y un número de puerto para el servidor virtual. A continuación, haga clic en **Agregar** y **Continuar**.

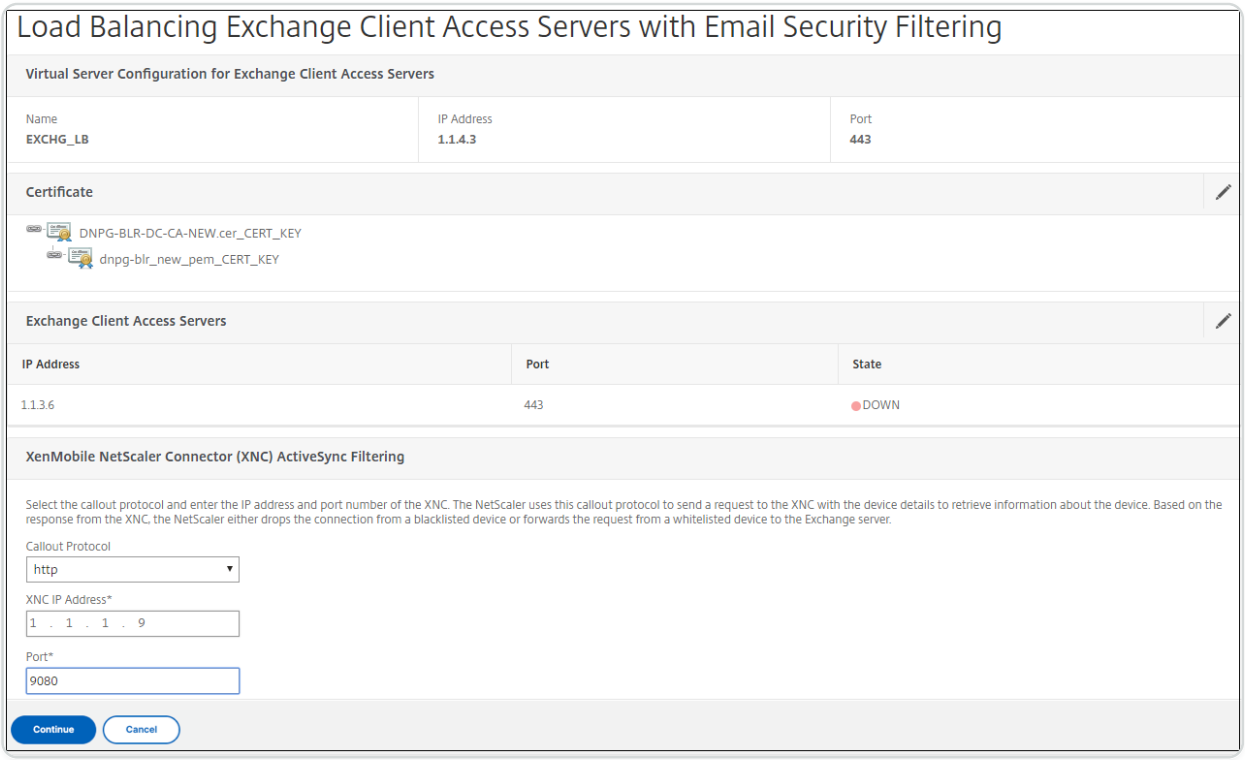
   Actualizar detalles de la instancia(/en-us/netscaler-gateway/media/exchange-client-access-servers-3.png)

Al hacer clic en **Listo**, aparecen los campos para configurar el filtrado de ActiveSync del conector NetScaler (XNC) de Citrix Endpoint Management.

## Configurar el filtrado de ActiveSync del Conector de NetScaler de Citrix Endpoint Management (XNC)

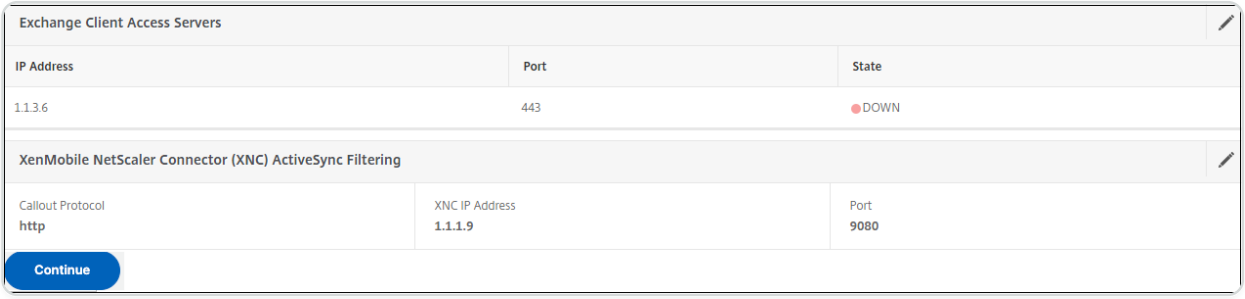
El Conector de NetScaler de Citrix Endpoint Management (XNC) proporciona un servicio de autorización a nivel de dispositivo de clientes de ActiveSync a NetScaler, que actúa como proxy inverso para el protocolo Exchange ActiveSync. La combinación de directivas definidas en Citrix Endpoint Management y reglas definidas localmente por el XNC controla la autorización.

1. En **Filtrado de ActiveSync del Conector de NetScaler de Citrix Endpoint Management (XNC)**, para **Protocolo de llamada**, seleccione **http** o **https**.
2. En **Dirección IP de XNC**, escriba la dirección IP del Conector de NetScaler de Citrix Endpoint Management.
3. En **Puerto**, escriba **9080** para el tráfico de red HTTP o **9443** para el tráfico de red HTTPS y, a continuación, haga clic en **Continuar**.




© 1997–2026 Citrix Systems, Inc. All rights reserved.

Aparece la configuración.




## Permitir el acceso desde dispositivos móviles con las aplicaciones de productividad móvil de Citrix

El asistente de NetScaler para XenMobile configura los ajustes necesarios para permitir a los usuarios conectarse desde dispositivos compatibles a través de NetScaler Gateway a aplicaciones móviles y recursos en la red interna. Los usuarios se conectan mediante Secure Hub (anteriormente, Citrix Secure Hub), que establece un túnel Micro VPN. Cuando los usuarios se conectan, se abre un túnel VPN a NetScaler Gateway y luego se pasa a XenMobile en la red interna. Los usuarios pueden acceder a sus aplicaciones web, móviles y SaaS desde XenMobile.

Para asegurarse de que los usuarios consuman una única licencia Universal al conectarse a NetScaler Gateway con varios dispositivos simultáneamente, puede habilitar la transferencia de sesión en el servidor virtual. Para obtener más información, consulte Configuración de tipos de conexión en el servidor virtual.

Si necesita cambiar su configuración después de usar el asistente de NetScaler para XenMobile, utilice las secciones de este artículo como guía. Antes de cambiar la configuración, asegúrese de comprender las implicaciones de sus cambios. Para obtener más información, consulte la documentación de XenMobile.

### Configurar Secure Browse en NetScaler Gateway

Puede cambiar Secure Browse como parte de la configuración global o como parte de un perfil de sesión. Puede vincular la directiva de sesión a usuarios, grupos o servidores virtuales. Al configurar Secure Browse, también debe habilitar el acceso sin cliente. Sin embargo, el acceso sin cliente no requiere que habilite Secure Browse. Al configurar el acceso sin cliente, establezca **Codificación de URL de acceso sin cliente** en **Borrar**.

Para configurar Secure Browse globalmente:

1. En la utilidad de configuración, en la ficha **Configuración**, en el panel de navegación, expanda **NetScaler Gateway** y, a continuación, haga clic en **Configuración global**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. En el panel de detalles, en **Configuración**, haga clic en **Cambiar configuración global**.
3. En el cuadro de diálogo **Configuración global de NetScaler Gateway**, en la ficha **Seguridad**, haga clic en **Secure Browse** y, a continuación, en **Aceptar**.

Para configurar Secure Browse en una directiva y perfil de sesión:

1. En la utilidad de configuración, en la ficha **Configuración**, en el panel de navegación, expanda **NetScaler Gateway > Directivas** y, a continuación, haga clic en **Sesión**.
2. En el panel de detalles, realice una de las siguientes acciones:
   - Si está creando una nueva directiva de sesión, haga clic en **Agregar**.
   - Si está cambiando una directiva existente, seleccione una directiva y, a continuación, haga clic en **Abrir**.
3. En la directiva, cree un perfil o modifique uno existente. Para ello, realice una de las siguientes acciones:
   - Junto a **Perfil de solicitud**, haga clic en **Nuevo**.
   - Junto a **Perfil de solicitud**, haga clic en **Modificar**.
4. En la ficha **Seguridad**, junto a **Navegación segura**, haga clic en **Anular global** y, a continuación, seleccione **Navegación segura**.
5. Realice una de las siguientes acciones:
   - Si está creando un nuevo perfil, haga clic en **Crear**, establezca la expresión en el cuadro de diálogo de directivas, haga clic en **Crear** y, a continuación, haga clic en **Cerrar**.
   - Si está modificando un perfil existente, después de realizar la selección, haga clic en **Aceptar** dos veces.

Para configurar directivas de tráfico para Secure Web en modo de navegación segura:

Siga estos pasos para configurar directivas de tráfico para enrutar el tráfico de Secure Web a través de un servidor proxy en modo de navegación segura.

1. En la utilidad de configuración, en la ficha **Configuración**, expanda **NetScaler Gateway > Directivas** y, a continuación, haga clic en **Tráfico**.
2. En el panel derecho, haga clic en la ficha **Perfiles de tráfico** y, a continuación, haga clic en **Agregar**.
3. En **Nombre**, introduzca un nombre para el perfil, seleccione **TCP** como **Protocolo** y deje el resto de la configuración tal cual.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. Haga clic en **Crear**.
5. Haga clic en la ficha **Perfiles de tráfico** y, a continuación, haga clic en **Agregar**.
6. En **Nombre**, introduzca un nombre para el perfil y, a continuación, seleccione **HTTP** como **Protocolo**. Este perfil de tráfico es para HTTP y SSL. El tráfico VPN sin cliente es tráfico HTTP por diseño, independientemente del puerto de destino o del tipo de servicio. Por lo tanto, se especifica el tráfico SSL y HTTP como **HTTP** en el perfil de tráfico.
7. En **Proxy**, introduzca la dirección IP del servidor proxy. En **Puerto**, introduzca el número de puerto del servidor proxy.
8. Haga clic en **Crear**.
9. Haga clic en la ficha **Directivas de tráfico** y, a continuación, en **Agregar**.
10. Introduzca el **Nombre** de la directiva de tráfico y, en **Perfil de solicitud**, seleccione el Perfil de tráfico que creó en el paso 3. Introduzca la siguiente **Expresión** y, a continuación, haga clic en **Crear**:

    ```
    REQ.HTTP.HEADER HOST contains ActiveSyncServer || REQ.HTTP.HEADER User-Agent CONTAINS WorxMail || REQ.HTTP.HEADER User-Agent CONTAINS com.zenprise || REQ.HTTP.HEADER User-Agent CONTAINS Citrix Secure Hub || REQ.HTTP.URL CONTAINS AGServices || REQ.HTTP.URL CONTAINS StoreWeb
    ```

    Esa regla realiza una comprobación basada en el encabezado del host. Para omitir el tráfico de sincronización activa del proxy, reemplace `ActiveSyncServer` por el nombre de servidor de sincronización activa adecuado.
11. Haga clic en la ficha **Directivas de tráfico** y, a continuación, en **Agregar**. Introduzca el **Nombre** de la directiva de tráfico y, en **Perfil de solicitud**, seleccione el Perfil de tráfico creado en el paso 6. Introduzca la siguiente **Expresión** y, a continuación, haga clic en **Crear**:

    (REQ.HTTP.HEADER User-Agent CONTAINS Mozilla || REQ.HTTP.HEADER User-Agent CONTAINS com.citrix.browser || REQ.HTTP.HEADER User-Agent CONTAINS WorxWeb) && REQ.TCP.DESTPORT == 80
12. Haga clic en la ficha **Directivas de tráfico** y, a continuación, en **Agregar**. Introduzca el **Nombre** de la Directiva de tráfico y, en **Perfil de solicitud**, seleccione el Perfil de tráfico creado en el paso 6. Introduzca la siguiente **Expresión** y, a continuación, haga clic en **Crear**:

    (REQ.HTTP.HEADER User-Agent CONTAINS Mozilla || REQ.HTTP.HEADER User-Agent CONTAINS com.citrix.browser || REQ.HTTP.HEADER User-Agent CONTAINS WorxWeb) && REQ.TCP.DESTPORT == 443

© 1997–2026 Citrix Systems, Inc. All rights reserved.

13. Vaya a **NetScaler Gateway > Servidores virtuales**, seleccione el servidor virtual en el panel derecho y, a continuación, haga clic en **Modificar**.
14. En la fila **Directivas**, haga clic en **+**.
15. En el menú **Elegir directiva**, seleccione **Tráfico**.
16. Haga clic en **Continuar**.
17. En **Enlace de directivas**, junto a **Seleccionar directiva**, haga clic en **\>**.
18. Seleccione la directiva que creó en el paso 10 y, a continuación, haga clic en **Aceptar**.
19. Haga clic en **Enlazar**.
20. En **Directivas**, haga clic en **Directiva de tráfico**.
21. En **Enlace de directiva de tráfico del servidor virtual VPN**, haga clic en **Agregar enlace**.
22. En **Enlace de directiva**, junto al menú **Seleccionar directiva**, haga clic en **\>** para ver la lista de directivas.
23. Seleccione la directiva que creó en el paso 11 y, a continuación, haga clic en **Aceptar**.
24. Haga clic en **Enlazar**.
25. En **Directivas**, haga clic en **Directivas de tráfico**.
26. En **Enlace de directiva de tráfico del servidor virtual VPN**, haga clic en **Agregar enlace**.
27. En **Enlace de directiva**, junto al menú **Seleccionar directiva**, haga clic en **\>** para ver la lista de directivas.
28. Seleccione la directiva que creó en el paso 12 y, a continuación, haga clic en **Aceptar**.
29. Haga clic en **Enlazar**.
30. Haga clic en **Cerrar**.
31. Haga clic en **Listo**.

Asegúrese de configurar la aplicación Secure Web (WorxWeb) en la consola de XenMobile. Vaya a **Configurar > Aplicaciones**, seleccione la aplicación Secure Web, haga clic en **Editar** y, a continuación, realice estos cambios:

- En la página **Información de la aplicación**, cambie **Modo VPN inicial** a **Secure Browse**.
- En la página de **iOS**, cambie el **Modo VPN inicial** a **Navegación segura**.
- En la página de **Android**, cambie el **Modo VPN preferido** a **Navegación segura**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

### Configurar los tiempos de espera de los tokens de aplicación y MDX

Cuando los usuarios inician sesión desde un dispositivo iOS o Android, se emite un token de aplicación o un token MDX. El token es similar a la Autoridad de tickets seguros (STA).

Puede establecer el número de segundos o minutos que los tokens están activos. Si el token caduca, los usuarios no pueden acceder al recurso solicitado, como una aplicación o una página web.

Los tiempos de espera de los tokens son configuraciones globales. Cuando configura el ajuste, se aplica a todos los usuarios que inician sesión en NetScaler Gateway.

1. En la utilidad de configuración, en la ficha **Configuración**, en el panel de navegación, expanda **NetScaler Gateway** y, a continuación, haga clic en **Configuración global**.
2. En el panel de detalles, en **Configuración**, haga clic en **Cambiar configuración global**.
3. En el cuadro de diálogo **Configuración global de NetScaler Gateway**, en la ficha **Experiencia del cliente**, haga clic en **Configuración avanzada**.
4. En la ficha **General**, en **Tiempo de espera del token de aplicación (seg)**, introduzca el número de segundos antes de que caduque el token. El valor predeterminado es **100** segundos.
5. En **Tiempo de espera del token MDX (min)**, introduzca el número de minutos antes de que caduque el token y, a continuación, haga clic en **Aceptar**. El valor predeterminado es **10** minutos.

### Inhabilitar el análisis de puntos finales para dispositivos móviles

Si configura el análisis de puntos finales, debe configurar las expresiones de directiva para que los análisis de puntos finales no se ejecuten en dispositivos móviles Android o iOS. Los análisis de puntos finales no son compatibles con dispositivos móviles.

Si vincula una directiva de análisis de puntos finales a un servidor virtual, debe crear un servidor virtual secundario para dispositivos móviles. No vincule directivas de preautenticación o postautenticación al servidor virtual del dispositivo móvil.

Cuando configura la expresión de directiva en una directiva de preautenticación, agrega la cadena de agente de usuario para excluir Android o iOS. Cuando los usuarios inician sesión desde uno de estos dispositivos y usted excluye el tipo de dispositivo, el análisis de puntos finales no se ejecuta.

Por ejemplo, se crea la siguiente expresión de directiva para comprobar si el User-Agent contiene Android, si la aplicación virus.exe no existe y para finalizar el proceso keylogger.exe si se está

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ejecutando mediante el perfil de preautenticación. La expresión de directiva podría ser similar a esta:

REQ.HTTP.HEADER User-Agent NO CONTIENE Android y CLIENT.APPLICATION.PROCESS(keylogger.exe) contiene o CLIENT.APPLICATION.PROCESS (virus.exe) contiene

Después de crear la directiva y el perfil de preautenticación, vincule la directiva al servidor virtual. Cuando los usuarios inician sesión desde un dispositivo Android o iOS, el análisis no se ejecuta. Si los usuarios inician sesión desde un dispositivo basado en Windows, el análisis sí se ejecuta.

Para obtener más información sobre la configuración de directivas de preautenticación, consulte Configuración de directivas de punto final.

### Admitir consultas DNS mediante sufijos DNS para dispositivos Android

Cuando los usuarios establecen una conexión Micro VPN desde un dispositivo Android, NetScaler Gateway envía la configuración de DNS dividido al dispositivo de usuario. NetScaler Gateway admite consultas de DNS dividido basadas en la configuración de DNS dividido que configure. NetScaler Gateway también puede admitir consultas de DNS dividido basadas en los sufijos DNS que configure en el dispositivo. Si los usuarios se conectan desde un dispositivo Android, debe configurar los ajustes de DNS en NetScaler Gateway.

El DNS dividido funciona de la siguiente manera:

- Si establece el DNS dividido en **Local**, el dispositivo Android envía todas las solicitudes DNS al servidor DNS local.
- Si establece el DNS dividido en **Remoto**, todas las solicitudes DNS se envían a los servidores DNS configurados en NetScaler Gateway (servidor DNS remoto) para su resolución.
- Si establece el DNS dividido en **Ambos**, el dispositivo Android comprueba el tipo de solicitud DNS.
    - Si el tipo de solicitud DNS no es "A", envía el paquete de solicitud DNS a los servidores DNS locales y remotos.
    - Si el tipo de solicitud DNS es "A", el complemento de Android extrae el FQDN de la consulta y lo compara con la lista de sufijos DNS configurada en el dispositivo NetScaler. Si el FQDN de la solicitud DNS coincide, la solicitud DNS se envía al servidor DNS remoto. Si el FQDN no coincide, la solicitud DNS se envía a los servidores DNS locales.

La siguiente tabla resume el funcionamiento del DNS dividido según el registro de tipo A y la lista de sufijos.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| CONFIGURACIÓN DE DNS DIVIDIDO | ¿ES UN REGISTRO DE TIPO A? | ¿ESTÁ EN LA LISTA DE SUFIJOS? | DÓNDE SE ENVÍA LA SOLICITUD DNS |
|---|---|---|---|
| Local | ambos Sí o No | ambos Sí o No | Local |
| Remoto | ambos Sí o No | ambos Sí o No | Remoto |
| Ambos | No | N/A | Ambos |
| Ambos | Sí | Sí | Remoto |
| Ambos | Sí | No | Local |

Para configurar un sufijo DNS:

1. En la utilidad de configuración, en la ficha **Configuración**, en el panel de navegación, expanda **NetScaler Gateway > Directivas** y, a continuación, haga clic en **Sesión**.
2. En el panel de detalles, en la ficha **Directivas**, seleccione una directiva de sesión y, a continuación, haga clic en **Abrir**.
3. Junto a **Perfil de solicitud**, haga clic en **Modificar**.
4. En la ficha **Configuración de red**, haga clic en **Avanzado**.
5. Junto a **Sufijo DNS de IP de intranet**, haga clic en **Anular global**, escriba el sufijo DNS y, a continuación, haga clic en **Aceptar** tres veces.

Para configurar el DNS dividido globalmente en NetScaler Gateway:

1. En la utilidad de configuración, en la ficha **Configuración**, en el panel de navegación, expanda **NetScaler Gateway** y, a continuación, haga clic en **Configuración global**.
2. En el panel de detalles, en **Configuración**, haga clic en **Cambiar configuración global**.
3. En la ficha **Experiencia del cliente**, haga clic en **Configuración avanzada**.
4. En la ficha **General**, en **Split DNS**, seleccione **Ambos**, **Remoto** o **Local** y, a continuación, haga clic en **Aceptar**.

Para configurar Split DNS en una directiva de sesión en NetScaler Gateway:

1. En la utilidad de configuración, en la ficha **Configuración**, en el panel de navegación, expanda **NetScaler Gateway > Directivas** y, a continuación, haga clic en **Sesión**.
2. En el panel de detalles, en la ficha **Directivas**, haga clic en **Agregar**.
3. En **Nombre**, escriba un nombre para la directiva.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. Junto a **Perfil de solicitud**, haga clic en **Nuevo**.
5. En **Nombre**, escriba un nombre para el perfil.
6. En la ficha **Experiencia del cliente**, haga clic en **Configuración avanzada**.
7. En la ficha **General**, junto a **Split DNS**, haga clic en **Anular global**, seleccione **Ambos**, **Remoto** o **Local** y, a continuación, haga clic en **Aceptar**.
8. En el cuadro de diálogo **Crear directiva de sesión**, junto a **Expresiones con nombre**, seleccione **General**, seleccione **Verdadero**, haga clic en **Agregar expresión**, haga clic en **Crear** y, a continuación, haga clic en **Cerrar**.

## Configurar la autenticación de dominio y de token de seguridad para Citrix Endpoint Management

Puede configurar Citrix Endpoint Management para exigir a los usuarios que se autentiquen con sus credenciales LDAP más una contraseña de un solo uso, utilizando el protocolo RADIUS. Esta sección describe la configuración necesaria de NetScaler Gateway para ese tipo de autenticación de dos factores.

### Requisitos previos

Si aún no ha ejecutado el asistente de NetScaler para Citrix Endpoint Management, consulte la sección *Asistente de NetScaler para Citrix Endpoint Management* en Configuración de los ajustes para su entorno de Citrix Endpoint Management. Asegúrese de que su configuración de NetScaler incluye lo siguiente:

- **Número de puerto LDAP** = **636** (que es el puerto predeterminado para conexiones LDAP seguras)
- **Atributo de nombre de inicio de sesión del servidor** = **samAccountName** o **userPrincipalName** según sus requisitos

### Para configurar la autenticación de dominio y de token de seguridad

1. Vaya a **NetScaler Gateway > Servidores virtuales**. Seleccione el servidor virtual y, a continuación, haga clic en **Editar**.
2. Haga clic en **Sin certificado de CA**.
3. En **Seleccionar certificado de CA**, elija un certificado, haga clic en **Aceptar**, haga clic en **Enlazar** y, a continuación, haga clic en **Listo**.
4. Vaya a **Directivas > Sesión > Perfiles de sesión**, seleccione el perfil y haga clic en **Editar**.
5. Haga clic en la ficha **Experiencia del cliente**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

6. En **Índice de credenciales**, elija **SECUNDARIO**.
7. Haga clic en **Aceptar**.
8. Vaya a **Directivas > Autenticación > LDAP**, haga clic en la ficha **Directiva LDAP** y, a continuación, haga clic en **Editar**.
9. Utilice la siguiente expresión para usar VIP de NetScaler Gateway separadas para Citrix Endpoint Management y Citrix Virtual Apps and Desktops.

   REQ.HTTP.HEADER User-Agent CONTAINS `CitrixReceiver`
10. Vaya a **Directivas > Autenticación > RADIUS** y, a continuación, haga clic en la ficha **Servidores**.
11. Haga clic en **Agregar**, introduzca los detalles del servidor RADIUS y haga clic en **Crear**.
12. Vaya a **Directivas** y, a continuación, haga clic en **Agregar**.
13. Introduzca un **Nombre** para la directiva. En el menú desplegable **Servidor**, seleccione el nombre del servidor RADIUS que ha creado.
14. En **Expresión**, introduzca **REQ.HTTP.HEADER User-Agent CONTAINS CitrixReceiver** y haga clic en **Crear**.
15. Seleccione el servidor virtual y, a continuación, haga clic en **Editar**.
16. En **Autenticación principal**, haga clic en **Directiva LDAP**.
17. Seleccione la directiva, haga clic en **Desvincular** y haga clic en **Cerrar**.
18. En la fila **Autenticación**, haga clic en **+** para agregar la autenticación RADIUS.
19. En **Elegir tipo**, en **Elegir directiva**, seleccione **RADIUS**.
20. Haga clic en **Vincular**.
21. Seleccione la directiva de autenticación RADIUS que creó anteriormente y, a continuación, haga clic en **Insertar**.
22. Haga clic en **Aceptar**.
23. Para añadir LDAP como política de autenticación secundaria: En la fila **Autenticación**, haga clic en **+**.
24. En **Elegir política**, elija **LDAP**.
25. En **Elegir tipo**, elija **Secundario**.
26. En **Seleccionar política**, elija la política LDAP.
27. Seleccione la política y, a continuación, haga clic en **Aceptar**.
28. Haga clic en **Enlazar**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

29. Haga clic en **Listo**.
30. verificar que las políticas que creó tienen la prioridad más alta. Esto garantiza que tengan la prioridad más alta incluso si se añaden más políticas para usuarios no móviles. Para obtener más información, consulte Establecer prioridades para las políticas de autenticación

## Configurar el certificado de cliente o el certificado de cliente y la autenticación de dominio

Puede usar el asistente de NetScaler para Citrix Endpoint Management para realizar la configuración necesaria para Citrix Endpoint Management cuando se usa la autenticación solo con certificado de NetScaler o la autenticación con certificado más dominio. Puede ejecutar el asistente de NetScaler para Citrix Endpoint Management una sola vez. Para obtener información sobre cómo usar el asistente, consulte (/es-es/netscaler-gateway/13-1/integrate-citrix-gateway-with-citrix-products/configure-citrix-endpoint-management-settings-to-integrate-with-citrix-gateway.html).

Si ya ha utilizado el asistente, siga las instrucciones de este artículo para la configuración adicional necesaria para la autenticación con certificado de cliente o la autenticación con certificado de cliente más dominio.

Para asegurarse de que el usuario de un dispositivo en modo solo MAM no pueda autenticarse con un certificado existente en el dispositivo, consulte "Lista de revocación de certificados (CRL) de NetScaler" más adelante en este artículo.

### Configurar NetScaler Gateway para la autenticación con certificado de cliente mediante la GUI

1. Vaya a **Traffic Management > Load Balancing > Virtual Servers**.
2. Seleccione el servidor virtual de tipo **SSL** y, en la sección **SSL Parameters**, establezca **Enable Session Reuse** en **DISABLED**.
3. Vaya a **NetScaler Gateway > Virtual Servers**.
4. Seleccione el servidor virtual de tipo **SSL** y haga clic en **Edit**.
5. En la sección **SSL Parameters**, haga clic en el icono de edición.
6. Seleccione **Client Authentication** y, en **Client Certificate**, seleccione **Mandatory**.
7. Cree una directiva de certificado de autenticación para que Citrix Endpoint Management pueda extraer el **User Principal Name** o el **sAMAccount** del certificado de cliente proporcionado por Secure Hub a NetScaler Gateway.
8. Vaya a **NetScaler Gateway> Policies> Authentication > CERT**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

9. Haga clic en la ficha **Profiles** y, a continuación, en **Add**.
10. Establezca los siguientes parámetros para el perfil de certificado:

    Tipo de autenticación: **CERT**

    Doble factor: **OFF** (solo para autenticación de certificado)

    Campo de nombre de usuario: Asunto: **CN**

    Campo de nombre de grupo: **SubjectAltName:PrincipalName**
11. Enlace solo la política de autenticación de certificado como la **autenticación principal** en el servidor virtual de NetScaler Gateway.
12. Enlace el certificado de CA raíz para validar la confianza del certificado de cliente presentado a NetScaler Gateway.

### Configurar NetScaler Gateway para la autenticación de certificado de cliente y dominio mediante la GUI

1. Vaya a **Administración de tráfico > Equilibrio de carga > Servidores virtuales**.
2. Seleccione el servidor virtual de tipo **SSL** y, en la sección **Parámetros SSL**, establezca **Habilitar reutilización de sesión** como **DESHABILITADO**.
3. Vaya a **NetScaler Gateway > Directivas > Autenticación > Cert**.
4. Haga clic en la ficha **Perfiles** y, a continuación, en **Agregar**.
5. Introduzca el **Nombre** del perfil, establezca **Doble factor** en **ON** y, en **Campo de nombre de usuario**, seleccione **SubjectAltNamePrincipalName**.
6. Haga clic en la ficha **Directivas** y, a continuación, en **Agregar**.
7. Introduzca el **Nombre** de la directiva, en **Servidor** seleccione el perfil de certificado, establezca la **Expresión** y haga clic en **Crear**.
8. Vaya a **Servidores virtuales**, seleccione el servidor virtual de tipo **SSL** y haga clic en **Modificar**.
9. Junto a **Authentication**, haga clic en **+** para añadir la autenticación de certificado.
10. Para seleccionar el método de autenticación, en **Choose Policy**, seleccione **Certificate**, y en **Choose Type** seleccione **Primary**. Esto vincula la autenticación de certificado como autenticación principal con la misma prioridad que el tipo de autenticación LDAP.
11. En **Policy Binding**, haga clic en **Click to Select** para seleccionar la directiva de certificado creada anteriormente.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

12. Seleccione la directiva de certificado creada anteriormente y haga clic en **OK**.
13. Establezca la **Priority** en **100** y, a continuación, haga clic en **Bind**. Utilice el mismo número de prioridad al configurar la directiva de autenticación LDAP en los pasos siguientes.
14. En la fila de **LDAP Policy**, haga clic en **>**.
15. Seleccione la directiva y, a continuación, en el menú desplegable **Edit**, haga clic en **Edit Binding**.
16. Introduzca el mismo valor de **Priority** que especificó para la directiva de certificado. Haga clic en **Bind**.
17. Haga clic en **Close**.
18. Haga clic en el icono de edición en la sección **SSL Parameters**.
19. Seleccione la casilla de verificación **Client Authentication**, y en **Client Certificate** elija **Mandatory**, y haga clic en **OK**.
20. Haga clic en **Done**.

### Lista de revocación de certificados (CRL) de NetScaler

Citrix Endpoint Management solo admite la lista de revocación de certificados (CRL) para una entidad de certificación de terceros. Si tiene una CA de Microsoft configurada, Citrix Endpoint Management utiliza NetScaler para administrar la revocación. Al configurar la autenticación basada en certificados de cliente, considere si necesita configurar la opción de lista de revocación de certificados (CRL) de NetScaler, **Enable CRL Auto Refresh**. Este paso garantiza que el usuario de un dispositivo en modo solo MAM no pueda autenticarse utilizando un certificado existente en el dispositivo. Citrix Endpoint Management vuelve a emitir un nuevo certificado, ya que no restringe a un usuario la generación de un certificado de usuario si se revoca uno. Esta configuración aumenta la seguridad de las entidades PKI cuando la CRL comprueba las entidades PKI caducadas.

## Configuración de SmartControl

SmartControl permite a los administradores definir políticas granulares para configurar y aplicar atributos del entorno de usuario para Citrix Virtual Apps and Desktops en NetScaler Gateway. SmartControl permite a los administradores gestionar estas políticas desde una única ubicación, en lugar de en cada instancia de estos tipos de servidor.

SmartControl se implementa a través de políticas ICA en NetScaler Gateway. Cada política ICA es una combinación de expresión y perfil de acceso que se puede aplicar a usuarios, grupos,

© 1997–2026 Citrix Systems, Inc. All rights reserved.

servidores virtuales y globalmente. Las políticas ICA se evalúan después de que el usuario se autentica al establecer la sesión.

**NOTA:**

Cuando la función de detección de clientes está habilitada, evite usar políticas ICA con reglas que incluyan expresiones de autenticación, autorización y auditoría (como AAA.USER, AAA.GROUP).

La siguiente tabla enumera los atributos del entorno de usuario que SmartControl puede aplicar:

| ATRIBUTO | DESCRIPCIÓN |
|---|---|
| ConnectClientDrives | Especifica la conexión predeterminada a las unidades cliente cuando el usuario inicia sesión. |
| ConnectClientLPTPorts | Especifica la conexión automática de puertos LPT desde el cliente cuando el usuario inicia sesión. Los puertos LPT son los puertos de impresora local. |
| ClientAudioRedirection | Especifica las aplicaciones alojadas en el servidor para transmitir audio a través de un dispositivo de sonido instalado en el equipo cliente. |
| ClientClipboardRedirection | Especifica y configura el acceso al portapapeles en el dispositivo cliente y asigna el portapapeles en el servidor. |
| ClientCOMPortRedirection | Especifica la redirección de puertos COM hacia y desde el cliente. Los puertos COM son los puertos de COMunicación. Los puertos COM son puertos serie. |
| ClientDriveRedirection | Especifica la redirección de unidades hacia y desde el cliente. |
| Multistream | Especifica la función multistream para usuarios específicos. |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| ATRIBUTO | DESCRIPCIÓN |
| --- | --- |
| ClientUSBDeviceRedirection | Especifica la redirección de dispositivos USB hacia y desde el cliente (solo hosts de estación de trabajo). |
| `Localremotedata` | Especifica la capacidad de carga y descarga de archivos HTML5 para la aplicación Citrix Workspace. |
| ClientPrinterRedirection | Especifica las impresoras cliente que se asignarán a un servidor cuando un usuario inicie sesión en una sesión. |

## Directivas

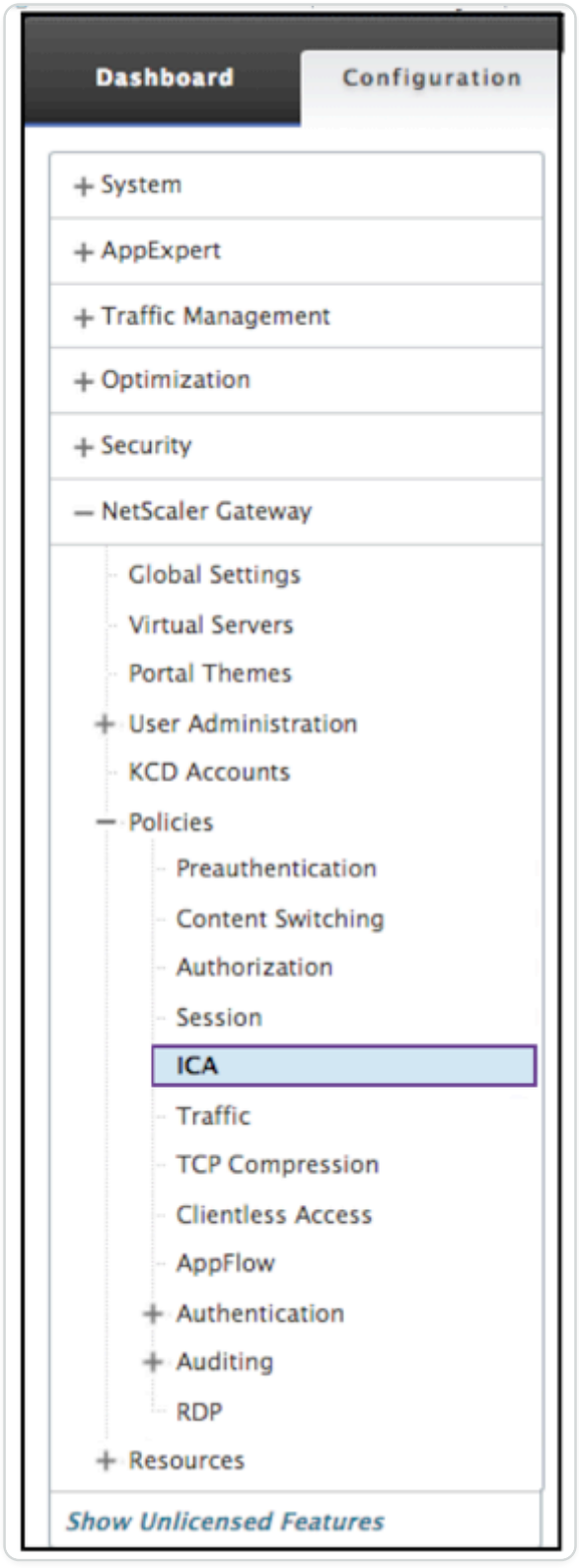
Una directiva ICA® especifica una Acción, un Perfil de acceso, una Expresión y, opcionalmente, una Acción de registro. Los siguientes comandos están disponibles en la pestaña **Directivas**:

- Agregar
- Editar
- Eliminar
- Mostrar enlaces
- Administrador de directivas
- Acción

### Agregar

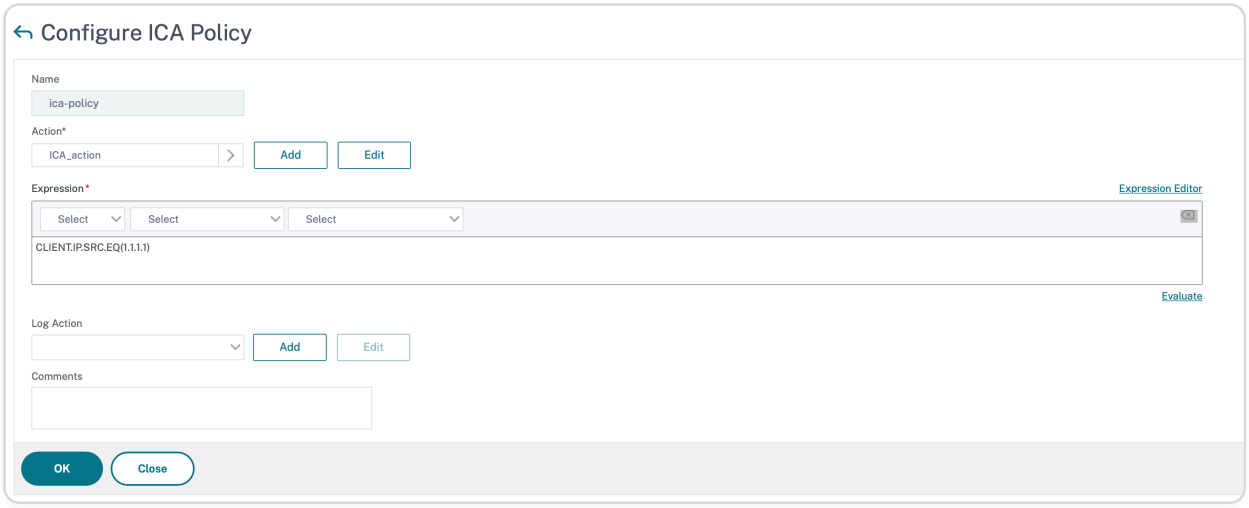
1. Vaya a **NetScaler Gateway > Directivas** y, a continuación, haga clic en **ICA**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.




2. En el panel de detalles, en la ficha Directivas, haga clic en **Agregar**.
3. En el cuadro de diálogo **Nombre**, escriba un nombre para la directiva.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

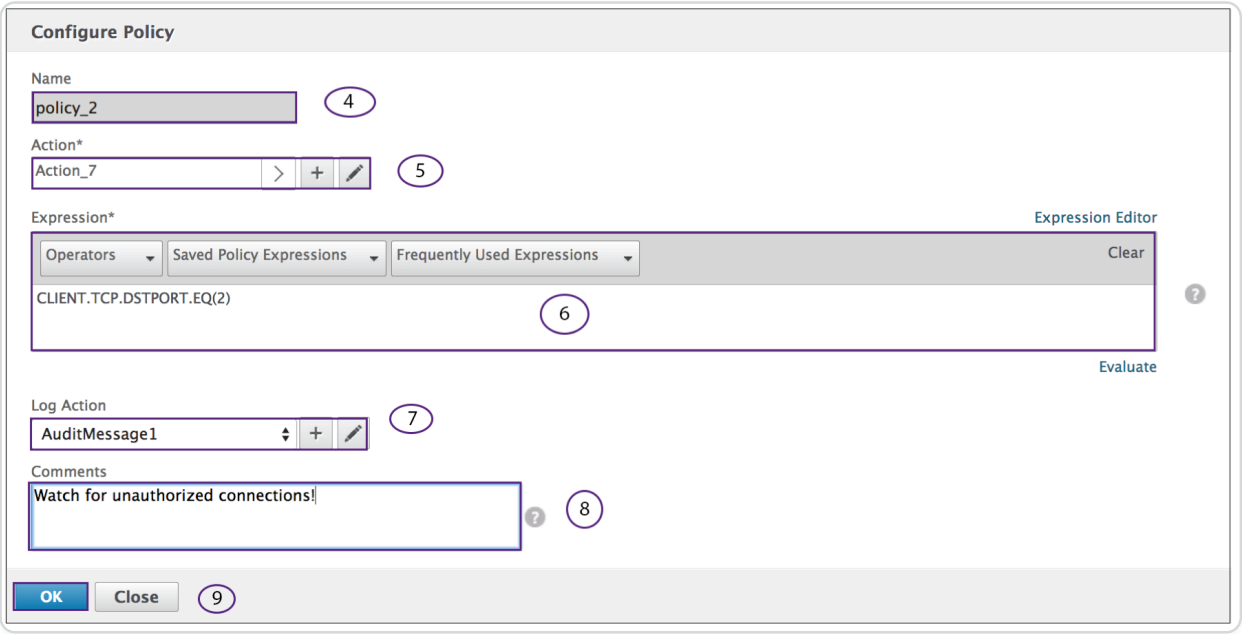



4. Junto a Acción, realice una de las siguientes acciones:
   - Haga clic en el icono **>** para seleccionar una acción existente. Para obtener más información, consulte en (#common-processes).
   - Haga clic en el icono **+** para crear una acción. Para obtener más información, consulte en (#common-processes).
   - El icono del **lápiz** está deshabilitado.
5. Crear una expresión.
6. Crear una **acción de registro**. Para obtener más detalles, consulte Crear una acción de registro.
7. Introduzca un mensaje en el cuadro Comentarios. El comentario se escribe en el registro de mensajes. Este campo es opcional.
8. Haga clic en **Crear**.

## Editar

1. Vaya a **NetScaler Gateway > Directivas** y, a continuación, haga clic en **ICA**.
2. Seleccione la directiva ICA de la lista.
3. En el panel de detalles, en la ficha **Directivas**, haga clic en **Editar**.
4. verificar el nombre de la directiva.

© 1997–2026 Citrix Systems, Inc. All rights reserved.




5. Para revisar la **acción**, realice una de las siguientes acciones:
   - Haga clic en el icono **>** para revisar una **acción** existente. Para obtener más detalles, consulte en (#common-processes).
   - Haga clic en el icono **+** para crear una **acción**. Para obtener más detalles, consulte en (#common-processes).
   - Haga clic en el icono del **lápiz** para revisar .
6. Revise la **Expresión** según desee. Para obtener más detalles, consulte en (#common-processes).
7. Para revisar la **Acción de registro**, realice una de las siguientes acciones:
   - Haga clic en el + para crear una **Acción de registro**.
   - Haga clic en el icono del **lápiz** para configurar un mensaje de auditoría.
8. Revise los comentarios según desee.
9. Haga clic en **Aceptar**.

## Eliminar

1. Vaya a **NetScaler Gateway > Directivas** y, a continuación, haga clic en **ICA**.
2. Seleccione la directiva ICA deseada de la lista.
3. En el panel de detalles, en la ficha **Directivas**, haga clic en **Eliminar**.
4. Confirme que desea eliminar la directiva haciendo clic en **Sí**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

### Mostrar enlace

1. Vaya a **NetScaler Gateway > Directivas** y, a continuación, haga clic en **ICA**.
2. Seleccione la directiva ICA de la lista.
3. En el panel de detalles, en la ficha **Directivas**, haga clic en **Mostrar enlaces**.

### Administrador de directivas

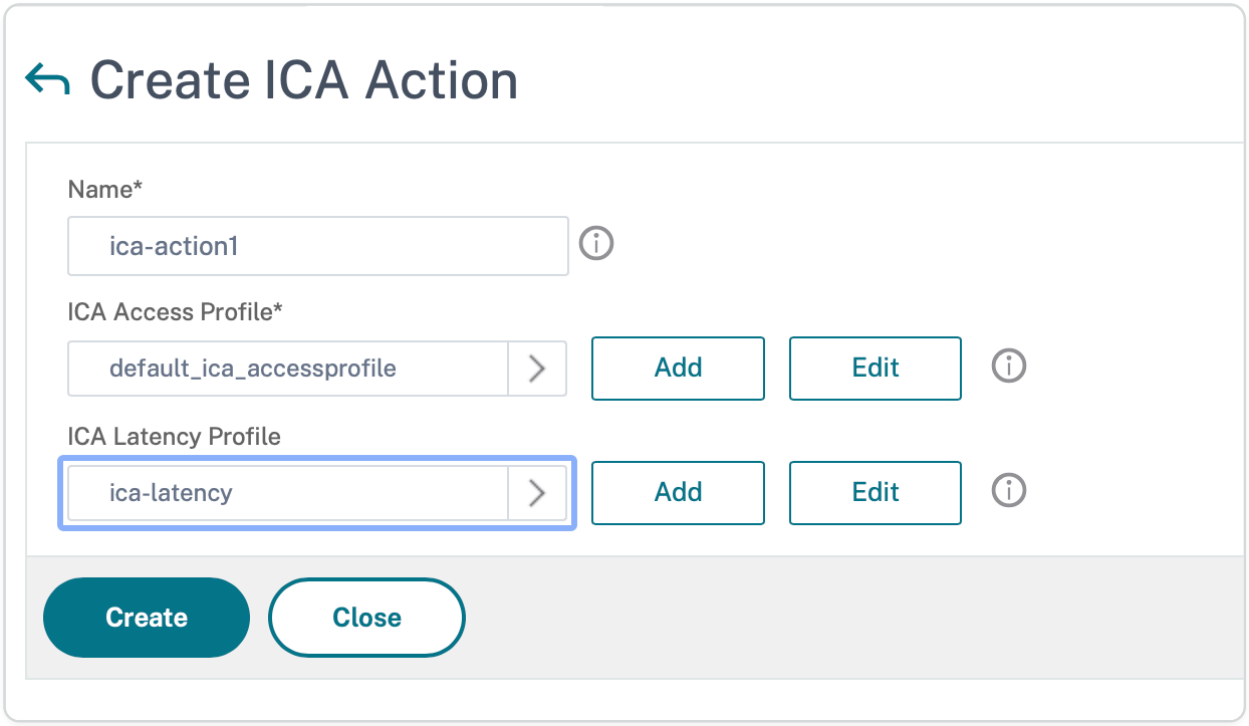
1. Vaya a **NetScaler Gateway > Directivas** y, a continuación, haga clic en **ICA**.
2. Seleccione la directiva ICA deseada de la lista.
3. En el panel de detalles, en la ficha Directivas, haga clic en **Administrador de directivas**
4. En el cuadro de diálogo **Punto de enlace**, seleccione una de las siguientes directivas.
    - Anular global
    - Servidor virtual VPN
    - Servidor virtual de redirección de caché
    - Global predeterminado
5. En el cuadro de diálogo Tipo de conexión, seleccione una directiva de enlace en el menú.
6. Si selecciona el Servidor virtual VPN o el Servidor virtual de redirección de caché, se conectará al servidor mediante el menú.
7. Haga clic en **Continuar**.

    Página de configuración de directivas ICA(/en-us/netscaler-gateway/media/fig50-ica-policy-manager.png)

### Agregar enlace

1. Después de seleccionar Continuar, aparece esta pantalla.
2. Seleccione una política para adjuntar el enlace.
3. Seleccione Agregar enlace.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

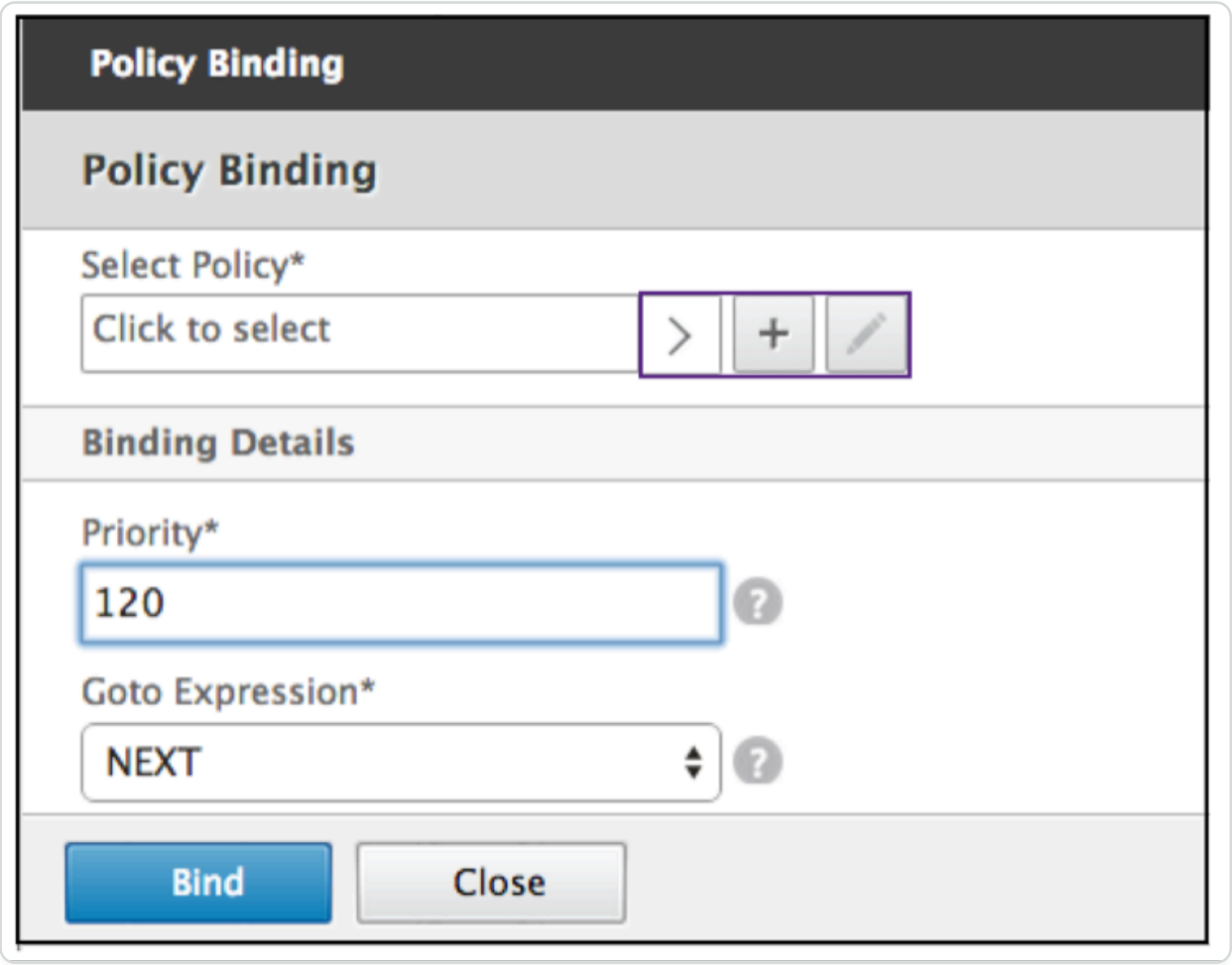



### Enlace de política

1\. Después de seleccionar Listo, aparece esta pantalla.

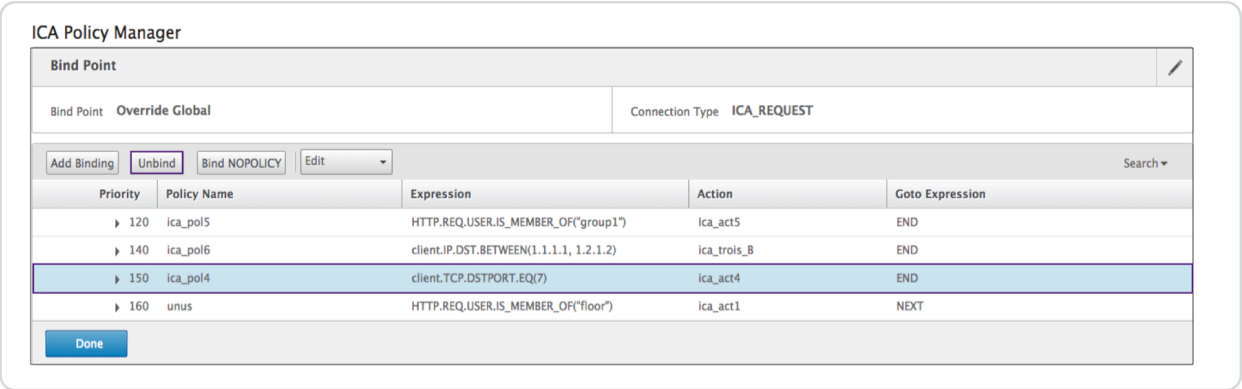
- Haga clic en el icono **>** para seleccionar una política existente. Para obtener más información, consulte Seleccionar una política existente.
- Haga clic en el icono **+** para crear una política. Para obtener más información, consulte Crear una política.

© 1997–2026 Citrix Systems, Inc. All rights reserved.




### Desvincular política

1. Seleccione la política que desea desvincular y haga clic en el botón **Desvincular**.

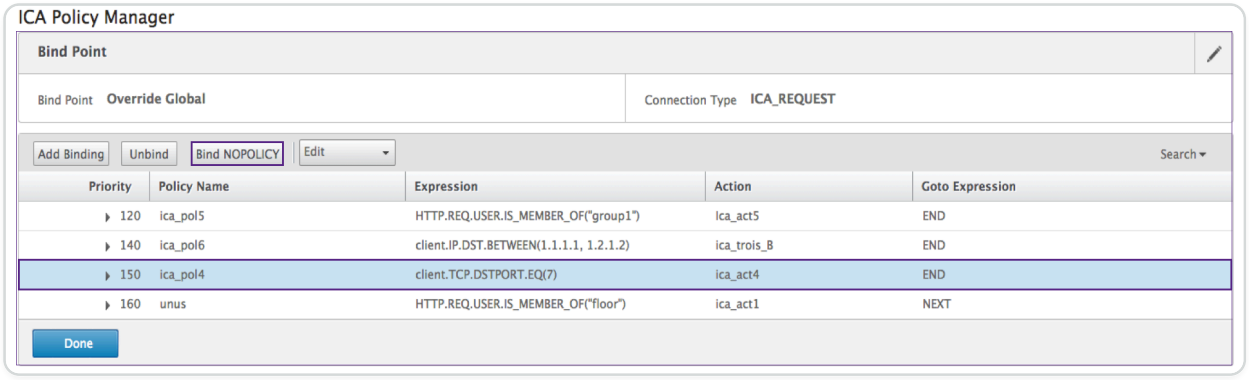



2. Haga clic en **Listo**
3. Haga clic en el botón **Sí** en la pantalla emergente para confirmar que desea desvincular la entidad seleccionada.

### Vincular NOPOLICY

1. Seleccione la política que requiere NOPOLICY y haga clic en el botón **Vincular NOPOLICY**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

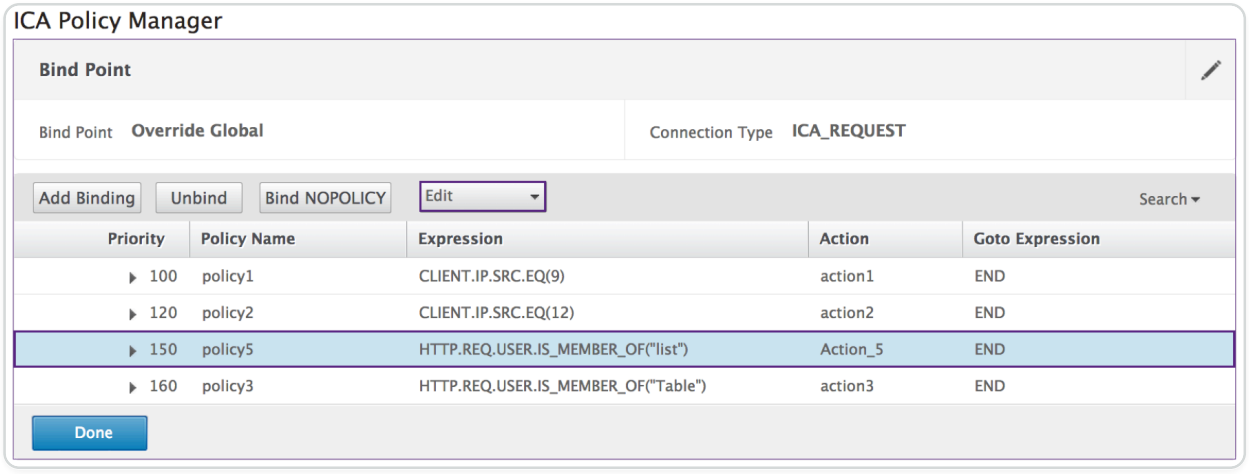



2. Haga clic en **Listo**

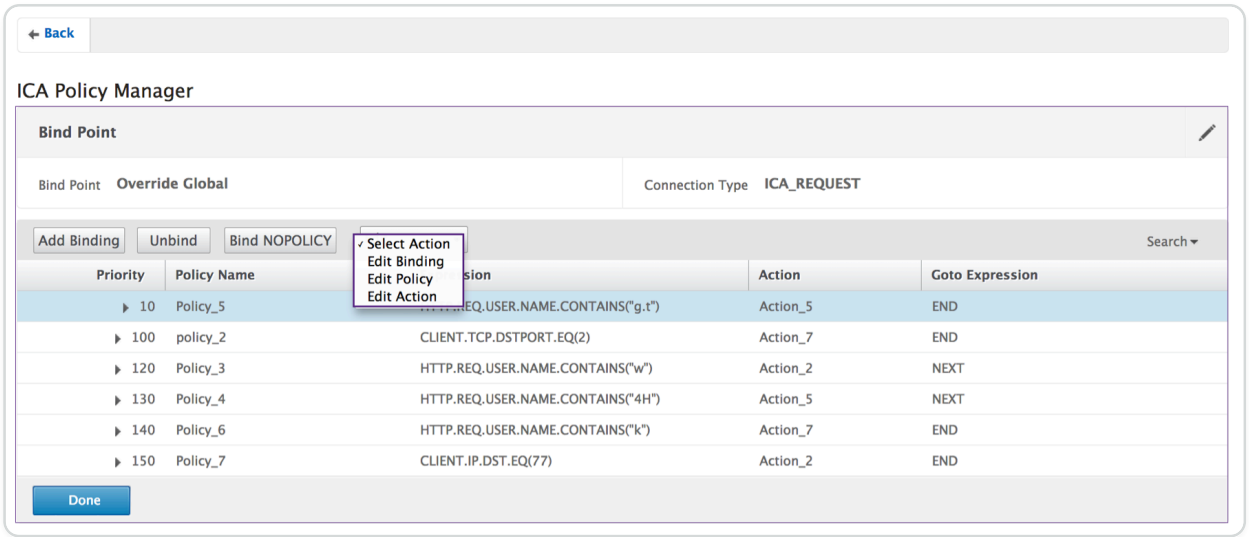
## Editar

Puede editar desde el Administrador de directivas ICA.

1. Seleccione la directiva que desea editar y seleccione **Editar**.



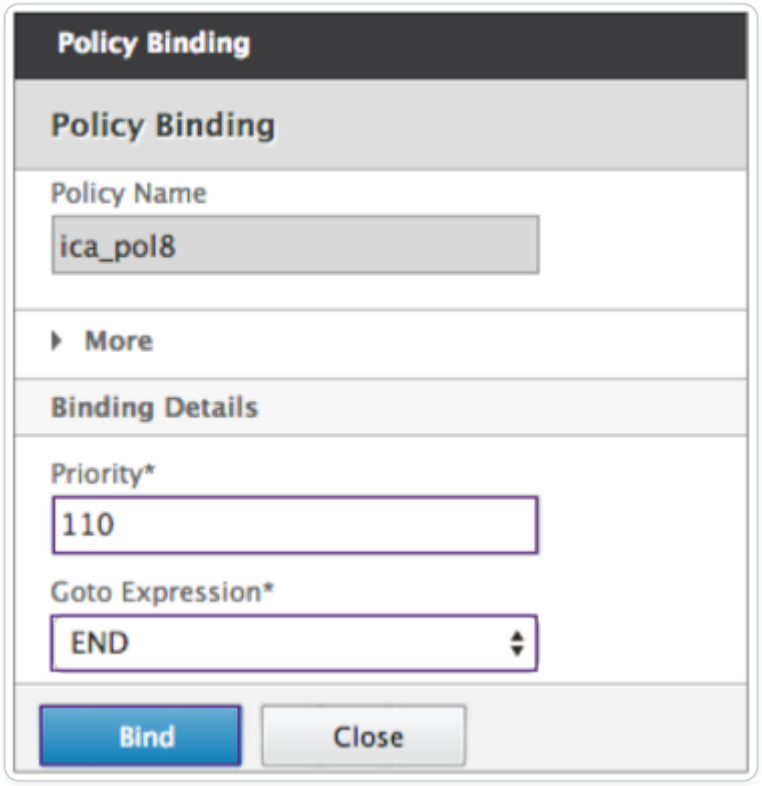

2. Puede realizar las siguientes ediciones: , .




© 1997–2026 Citrix Systems, Inc. All rights reserved.

### Editar enlace

1. Con la directiva seleccionada, haga clic en **Editar enlace**.
2. verificar que está editando la directiva deseada. Este nombre de directiva no es editable.

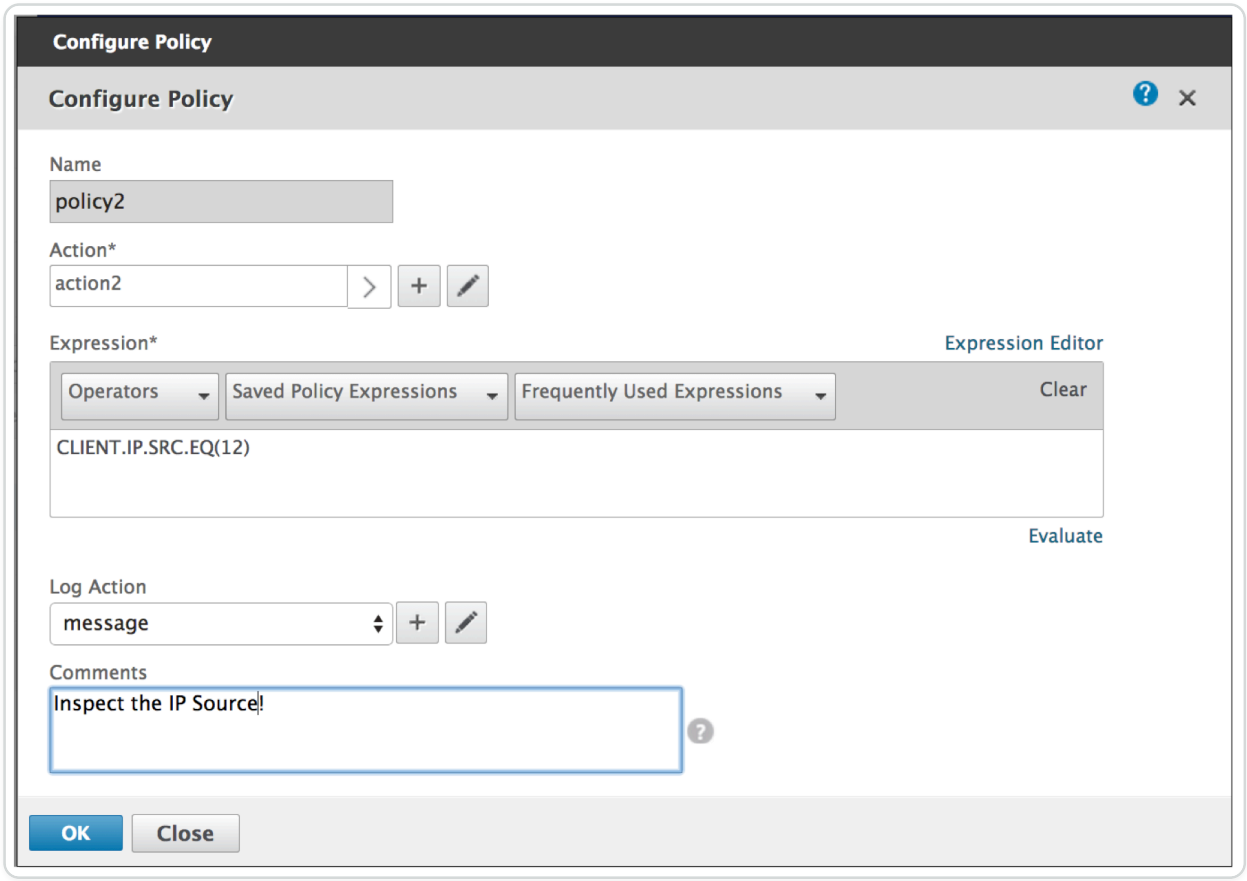



3. Establezca la prioridad según desee.
4. Establezca la expresión Goto según desee.
5. Haga clic en el botón **Enlazar**.

### Editar política

1. Con la política seleccionada, haga clic en **Editar política**.
2. verificar el nombre de la política para asegurarse de que está editando la política deseada. Este campo no es editable.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

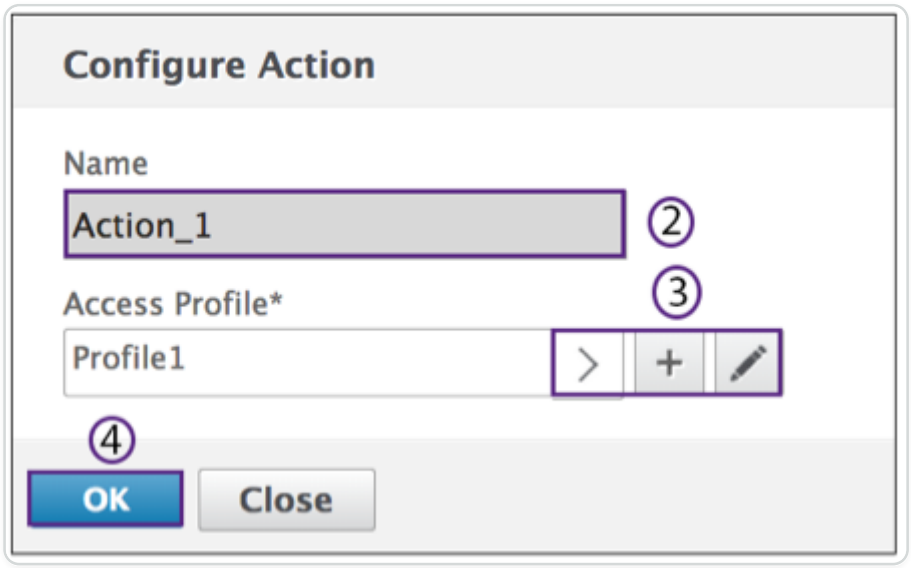



3. Para revisar la política de acción, realice una de las siguientes acciones:
   - Haga clic en el icono **>** para seleccionar una acción existente. Para obtener más información, consulte en (#common-processes).
   - Haga clic en el icono **+** para crear una acción. Para obtener más información, consulte en (#common-processes).
   - Haga clic en el icono del **lápiz** para revisar el perfil de acceso. Para obtener más información, consulte en (#common-processes).
4. Revise la expresión según desee. Para obtener más información, consulte en (#common-processes).
5. Seleccione el tipo de mensaje deseado en el menú. Para crear una acción de registro, realice una de las siguientes acciones:
   - Haga clic en el icono **+** para crear una acción. Para obtener más información, consulte Crear una acción de registro.
   - Haga clic en el icono del **lápiz** para revisar la acción de configurar mensaje de auditoría. Para obtener más información, consulte Configurar acción de mensaje de auditoría.
6. Introduzca comentarios sobre la política ICA.
7. Haga clic en **Aceptar** cuando haya terminado de editar.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

### Editar acción

1. Con la política seleccionada, haga clic en **Editar acción**.
2. verificar el nombre de la acción para confirmar que está editando la acción deseada. Este campo no es editable.
3. Junto a Perfil de acceso, realice una de las siguientes acciones:
   - Haga clic en el icono **\>** para seleccionar un perfil de acceso diferente. Para obtener más información, consulte Configurar acción.
   - Haga clic en el icono **+** para seleccionar un nuevo perfil de canal. Crear un perfil de acceso.
   - Haga clic en el icono del **lápiz** para revisar el perfil de acceso. Para obtener más información, consulte en (#common-processes).
4. Haga clic en **Aceptar**.

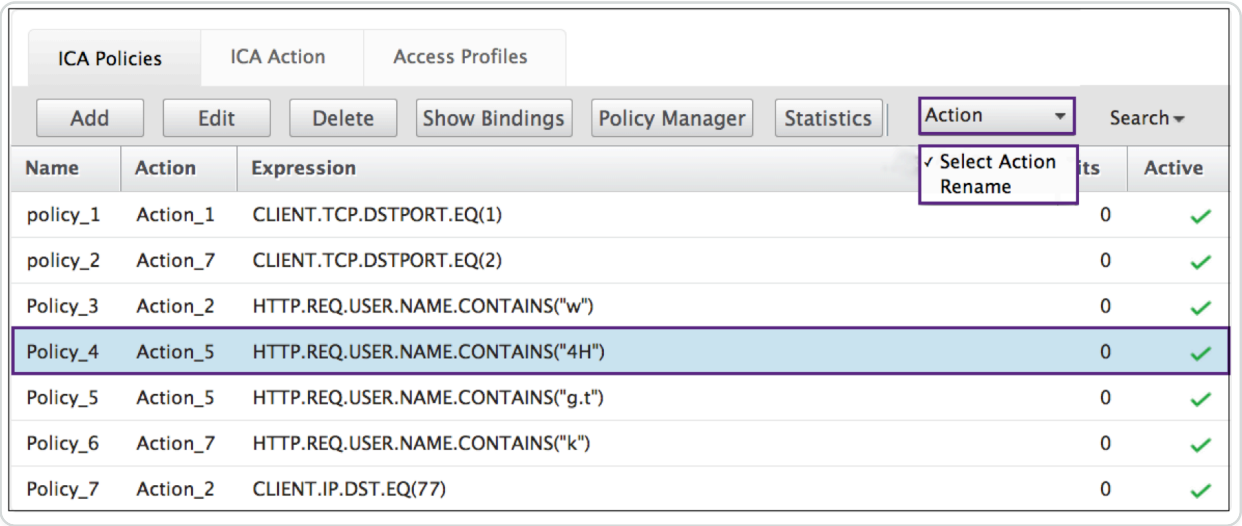



### Acción

Los comandos **Directivas > Acción** se utilizan para cambiar el nombre de la acción.

1. Seleccione la acción ICA deseada de la lista.
2. En la ficha Directivas ICA, haga clic en **Acción**. Seleccione **Cambiar nombre** en el menú.

© 1997–2026 Citrix Systems, Inc. All rights reserved.




3. Cambie el nombre de la acción.
4. Haga clic en **Aceptar**.

## Acción

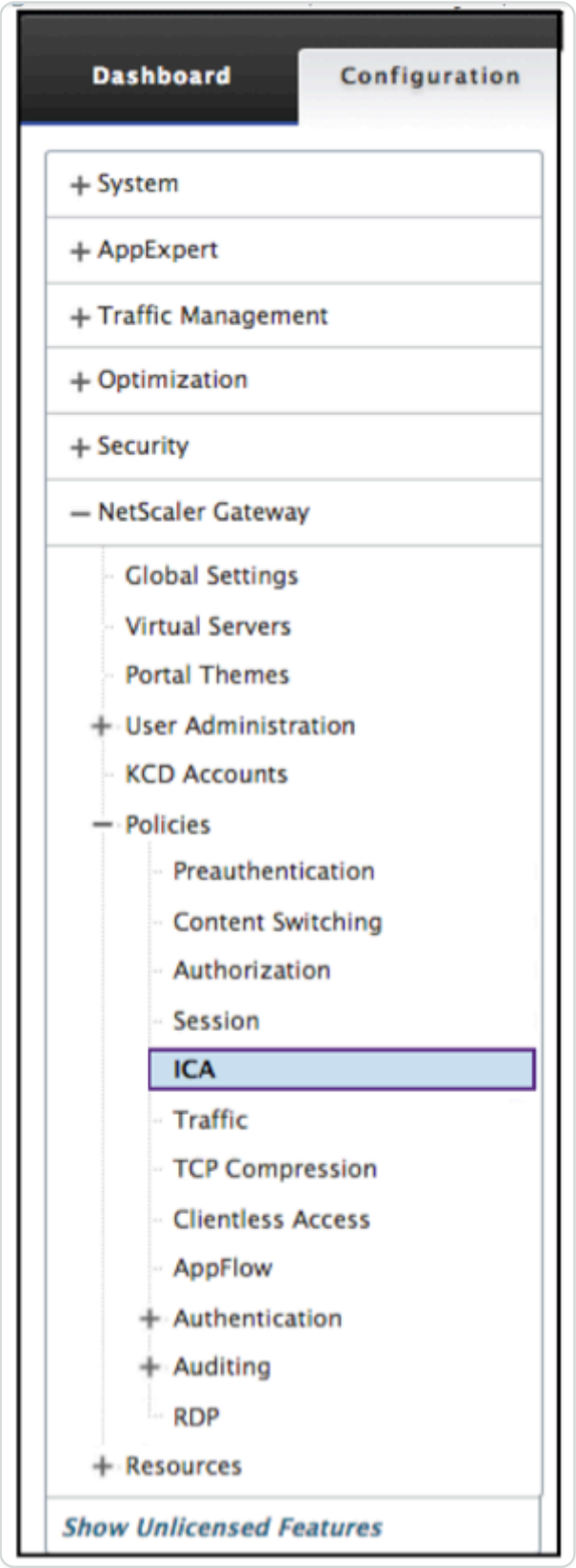
Una Acción conecta una política con un Perfil de acceso. Los siguientes comandos están disponibles en la ficha **Directivas**:

- Agregar
- Editar
- Eliminar
- Acción

## Agregar

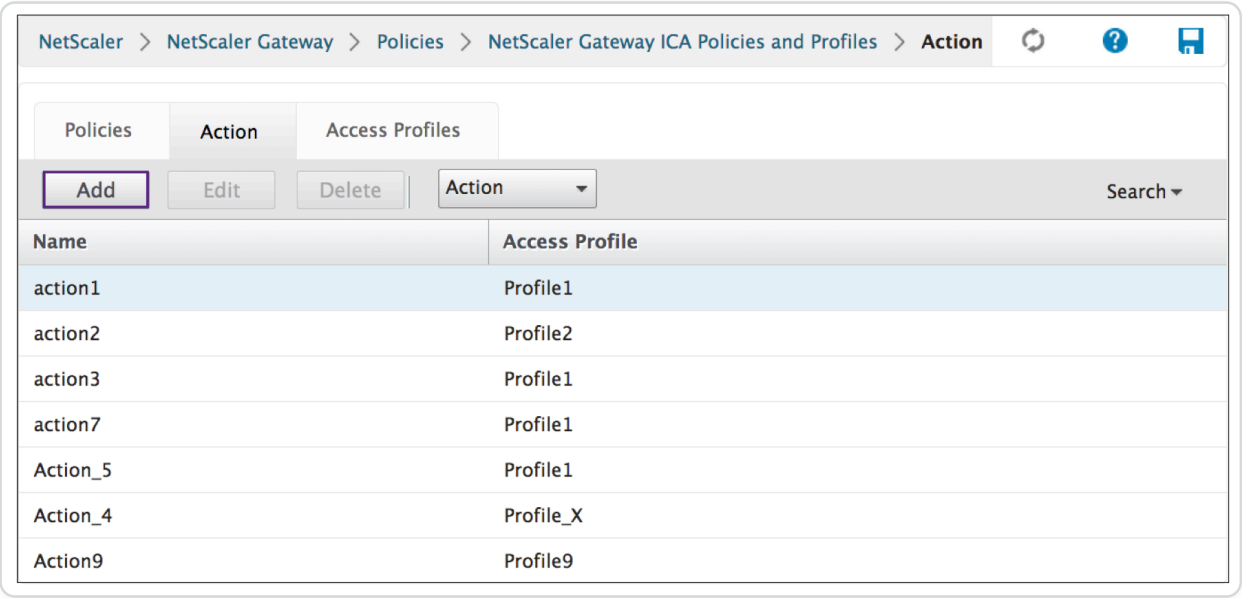
1. Vaya a **NetScaler Gateway > Acción** y, a continuación, haga clic en **ICA**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



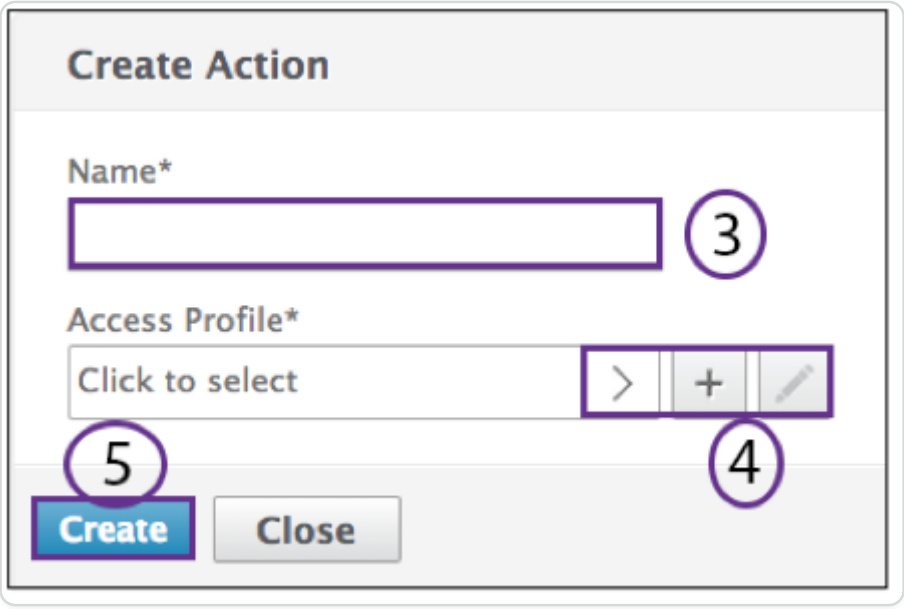

2. En el panel de detalles, en la ficha Acción, haga clic en **Agregar**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.




- Haga clic en el icono **\>** para seleccionar un Perfil de acceso existente. Para obtener más detalles, consulte en (#common-processes).
- Haga clic en el icono **+** para crear un Perfil de acceso. Para obtener más detalles, consulte Crear un perfil de acceso..
- El icono del **lápiz** está inhabilitado para esta pantalla.

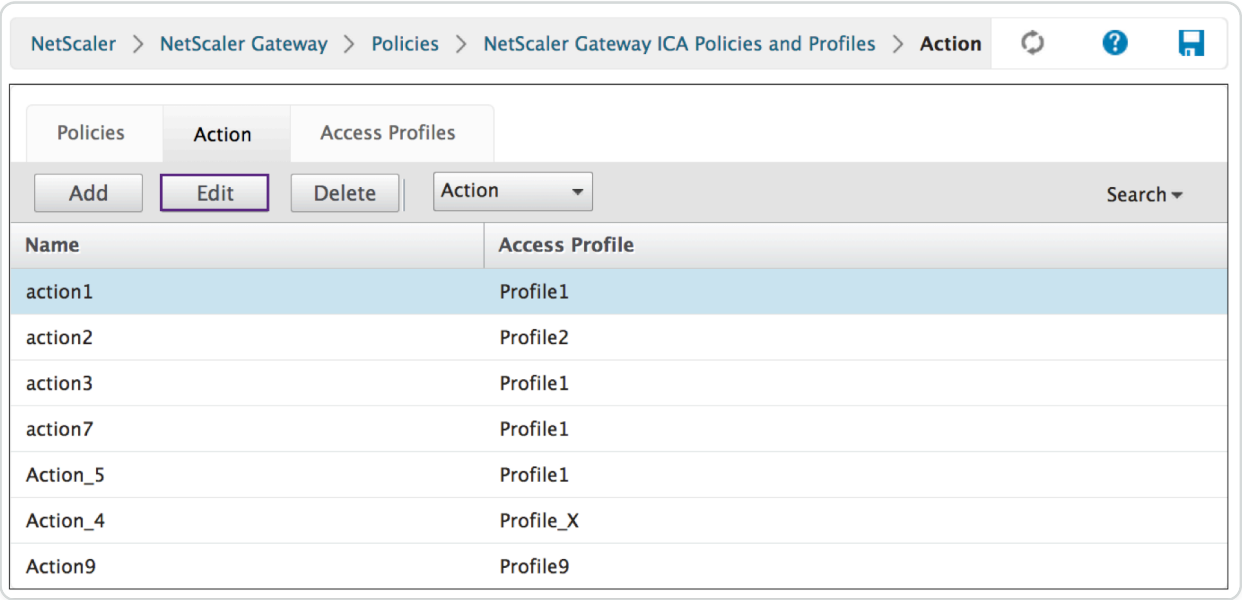
3. Haga clic en **Crear**.




## Editar

1. Seleccione la política ICA deseada de la lista.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

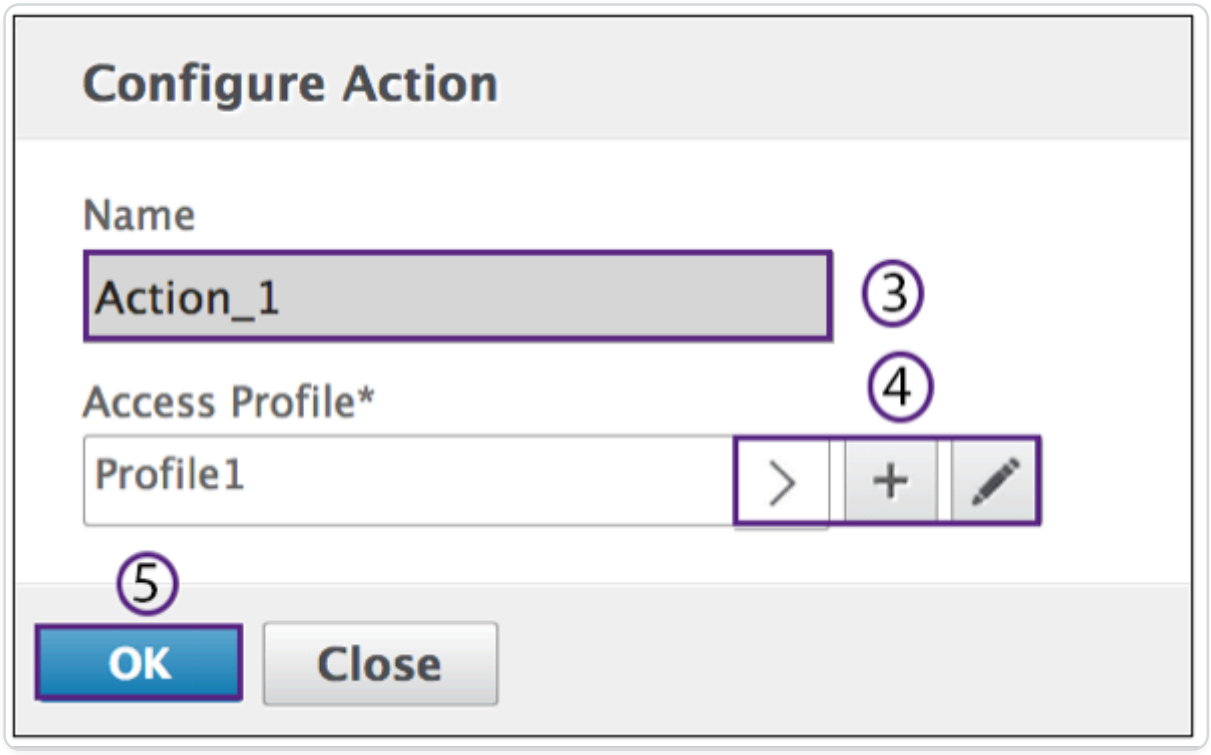



2. En el panel de detalles, en la ficha Acción, haga clic en **Editar**.

## Configurar acción

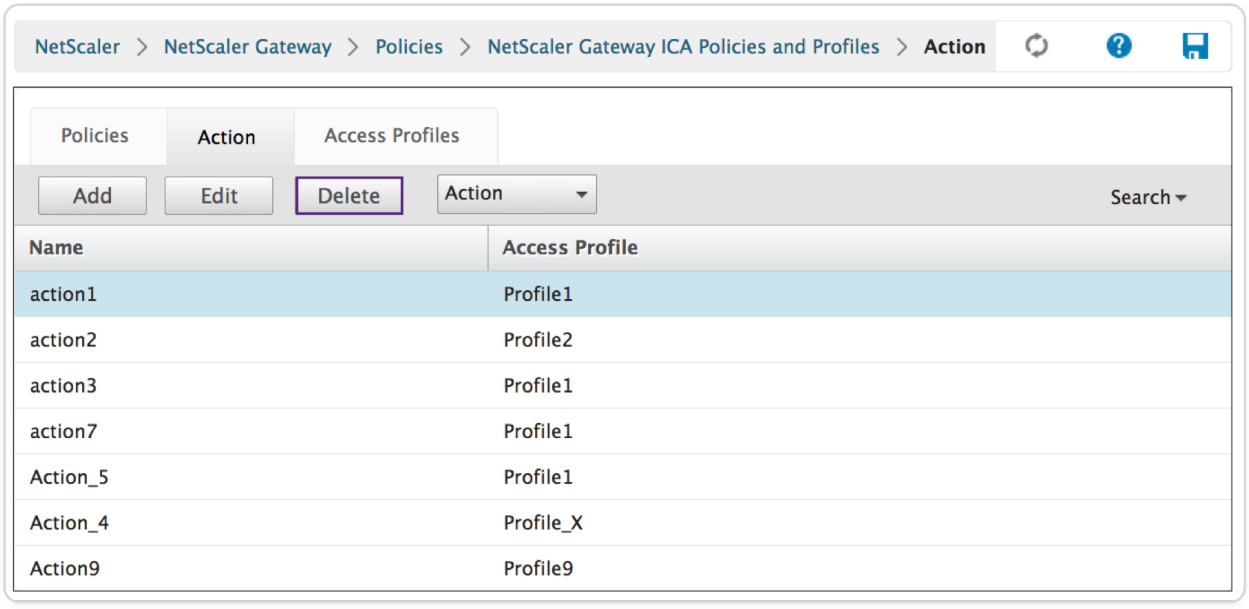
1. verificar el nombre de la acción para confirmar que está editando la acción deseada. Este campo no es editable.
2. Junto a Perfil de acceso, realice una de las siguientes acciones:
   - Haga clic en el **\>** para seleccionar un perfil de acceso existente. Para obtener más información, consulte en (#common-processes).
   - Haga clic en el **+** para crear un perfil de acceso. Para obtener más información, consulte Crear un perfil de acceso.
   - Haga clic en el icono del **lápiz** para Configurar perfil de acceso.
3. Haga clic en **Aceptar**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.




### Eliminar

1. Vaya a **NetScaler Gateway > Acción** y, a continuación, haga clic en **ICA**.
2. Seleccione la acción ICA deseada de la lista.
3. En el panel de detalles, en la ficha Acción, haga clic en **Eliminar**.



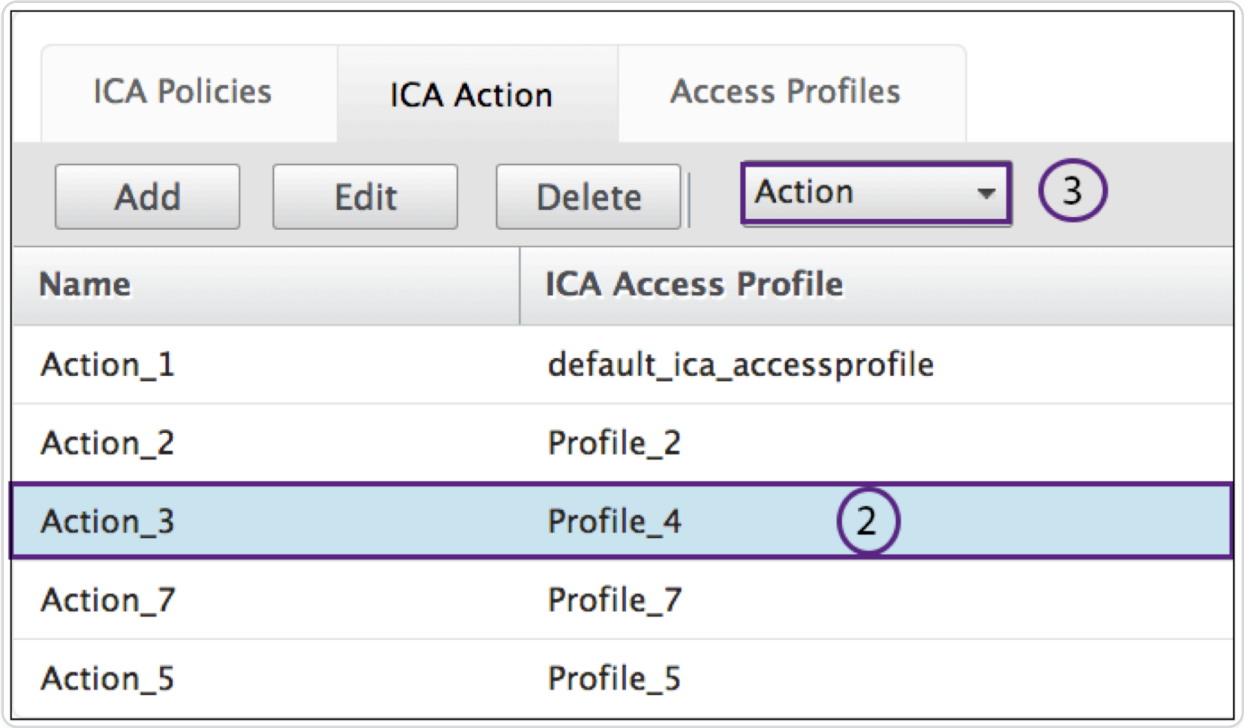

4. Confirme la acción para eliminar la directiva haciendo clic en **Sí**.

### Acción

Los comandos **Acción ICA > Acción** se utilizan para cambiar el nombre de la acción.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Vaya a **NetScaler Gateway > Acción** y, a continuación, haga clic en **ICA**.
2. Seleccione la acción ICA deseada de la lista.
3. En el panel de detalles, en la ficha Acción, haga clic en **Acción**.




4. Seleccione **Acción > Cambiar nombre** en el menú.
5. Cambie el nombre de la acción.
6. Haga clic en **Aceptar**

### Perfiles de acceso

Un perfil ICA define la configuración para las conexiones de usuario.

Los perfiles de acceso especifican las acciones que se aplican al entorno ICA de Citrix Virtual Apps and Desktops de un usuario si el dispositivo del usuario cumple las condiciones de la expresión de la directiva. Puede usar la GUI para crear perfiles ICA por separado de una directiva ICA y luego usar el perfil para varias directivas. Solo puede usar un perfil con una directiva.

Puede crear perfiles de acceso independientemente de una directiva ICA. Al crear la directiva, puede seleccionar el perfil de acceso que desea adjuntar a la directiva. Un perfil de acceso especifica los recursos disponibles para un usuario. Los siguientes comandos están disponibles en la ficha **Directivas**:

- Agregar
- Modificar

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Eliminar

## Crear un perfil de acceso con la GUI

1. Vaya a **NetScaler Gateway > Directivas** y, a continuación, haga clic en **ICA**.
2. En el panel de detalles, haga clic en la ficha **Perfiles de acceso** y, a continuación, haga clic en **Agregar**.
3. Configure la configuración del perfil, haga clic en Crear y, a continuación, haga clic en **Cerrar**. Después de crear un perfil, puede incluirlo en una directiva ICA.

## Agregar un perfil de acceso a una directiva mediante la GUI

1. Vaya a **NetScaler Gateway > Directivas** y, a continuación, haga clic en **ICA**.
2. En la ficha Directivas, realice una de las siguientes acciones:
   - Haga clic en **Agregar** para crear una directiva ICA.
   - Seleccione una directiva y, a continuación, haga clic en **Abrir**.
3. En el menú **Acción**, seleccione un perfil de acceso de la lista.
4. Termine de configurar la política ICA y, a continuación, realice una de las siguientes acciones:

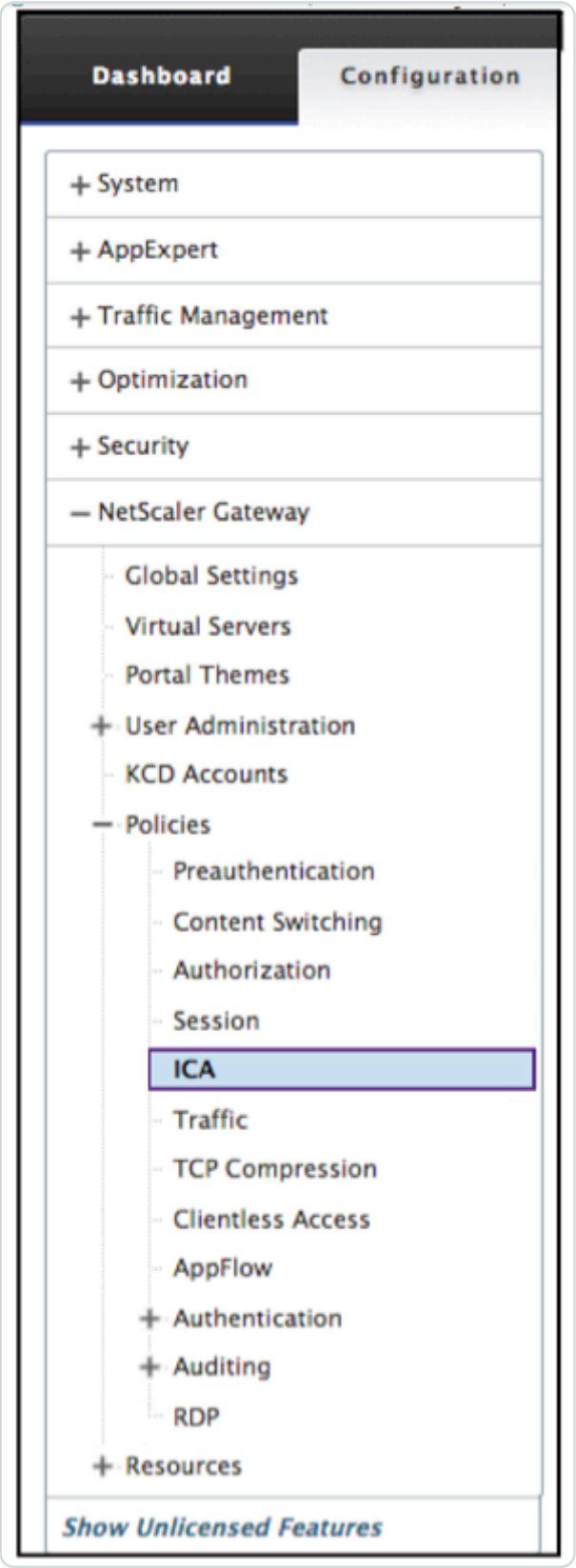
   a. Haga clic en **Crear** y, a continuación, haga clic en **Cerrar** para crear la política.

   1. Haga clic en **Aceptar** y, a continuación, haga clic en **Cerrar** para modificar la política.

## Agregar

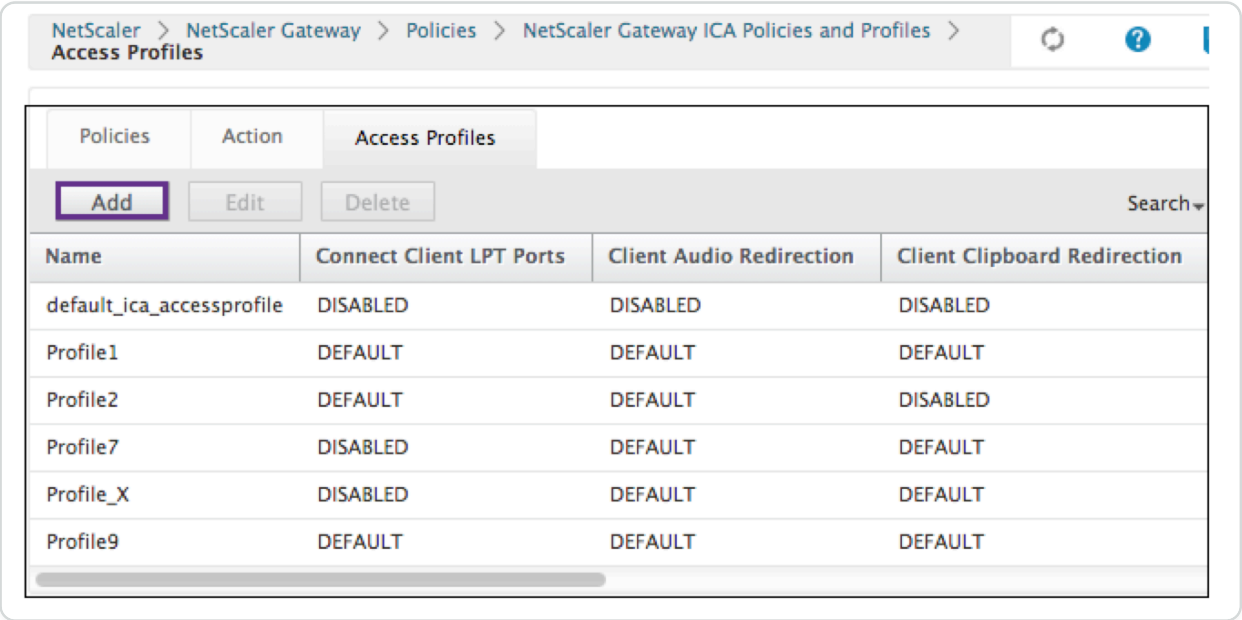
1. Vaya a **NetScaler Gateway > Directivas** y, a continuación, haga clic en **ICA**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

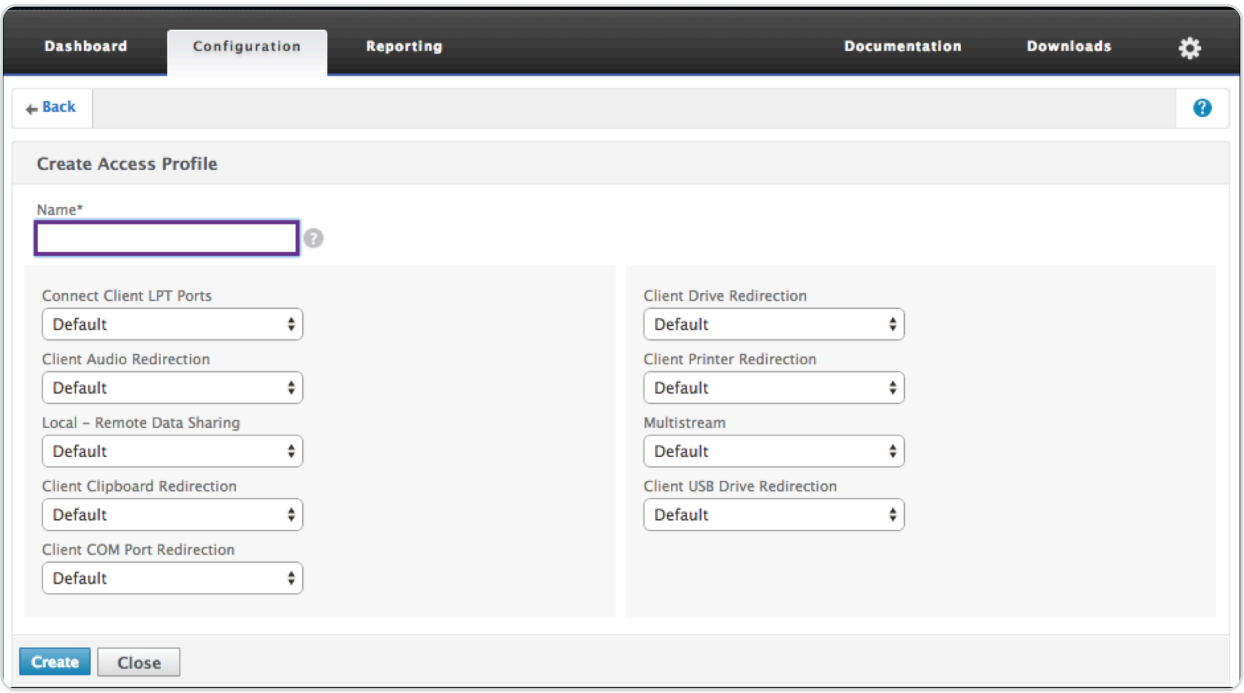



2. En el panel de detalles, en la ficha Perfiles de acceso, haga clic en **Agregar**.****

© 1997–2026 Citrix Systems, Inc. All rights reserved.




3. En Nombre, escriba un nombre para el perfil de acceso.

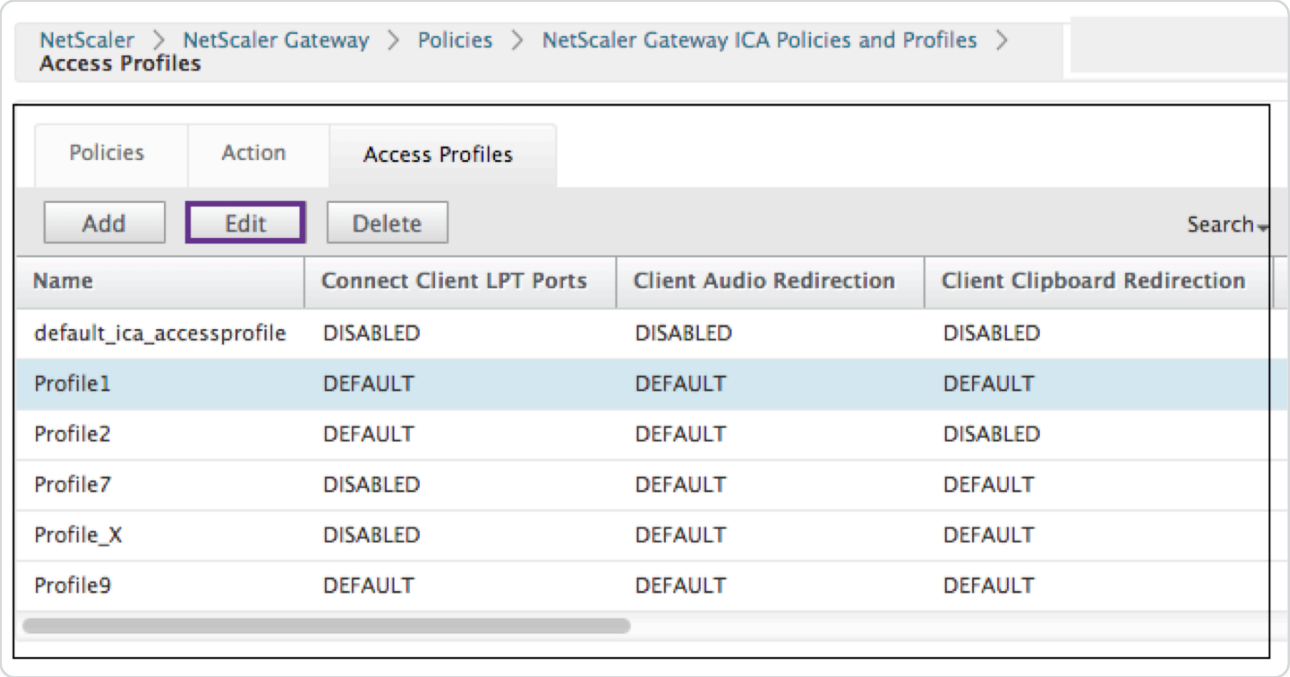



4. Seleccione Predeterminado o Deshabilitar en los menús mostrados para crear el perfil de acceso.
5. Haga clic en **Crear**.

## Editar

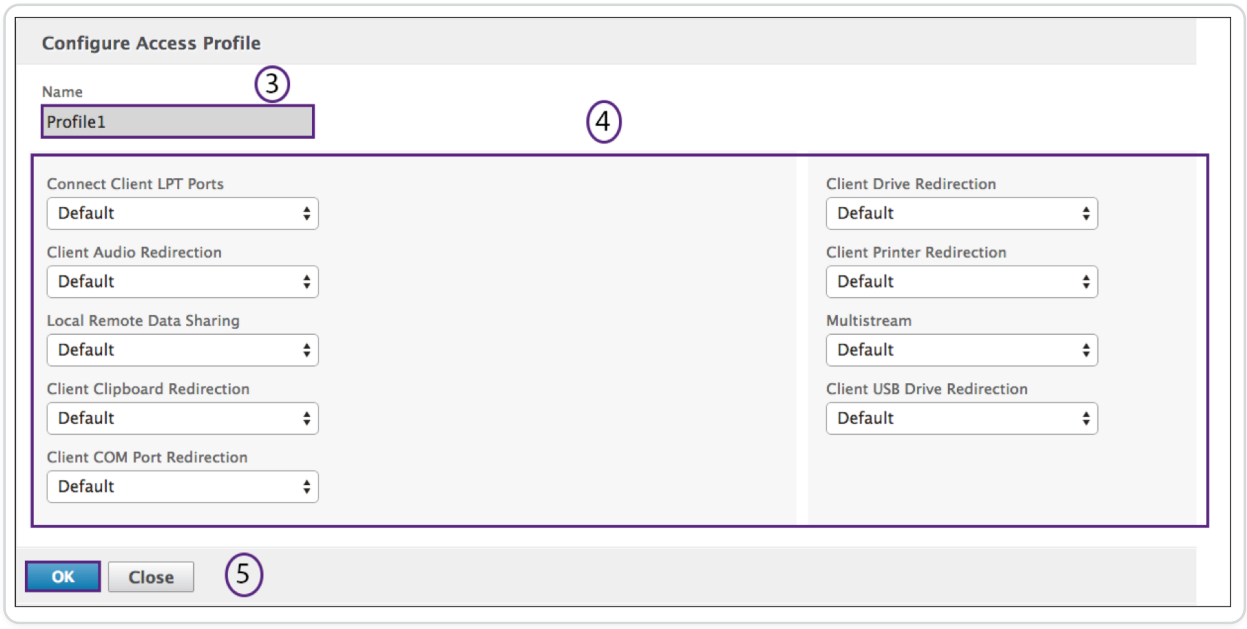
1. Seleccione el perfil de acceso que desea editar.
2. En el panel de detalles, en la ficha Perfiles de acceso, haga clic en **Editar**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.




## Configurar perfil de acceso

1. verificar que el **Nombre** es el que desea revisar.

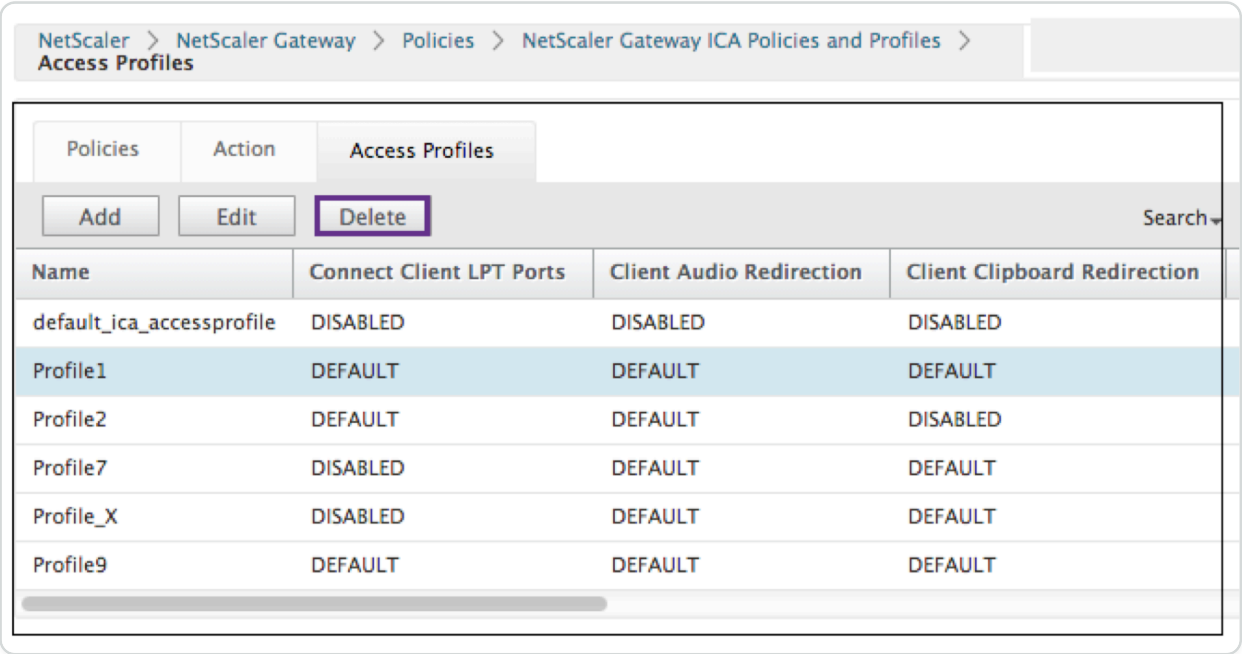



2. Seleccione **Predeterminado** o **Deshabilitar** en el menú para configurar según sea necesario.
3. Haga clic en **Aceptar**.

## Eliminar

1. Vaya a **NetScaler Gateway > Acción** y, a continuación, haga clic en **ICA**.
2. Seleccione la acción ICA deseada de la lista.
3. En el panel de detalles, en la ficha **Acción**, haga clic en **Eliminar**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



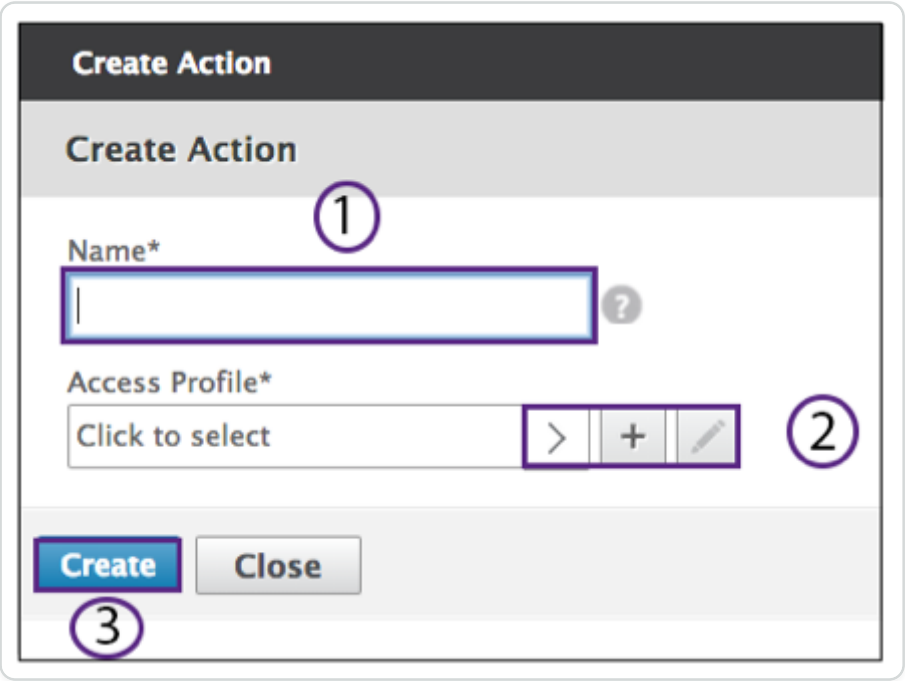

4. Confirme el perfil de acceso que desea eliminar haciendo clic en **Sí**.

## Procesos comunes

### Crear una acción

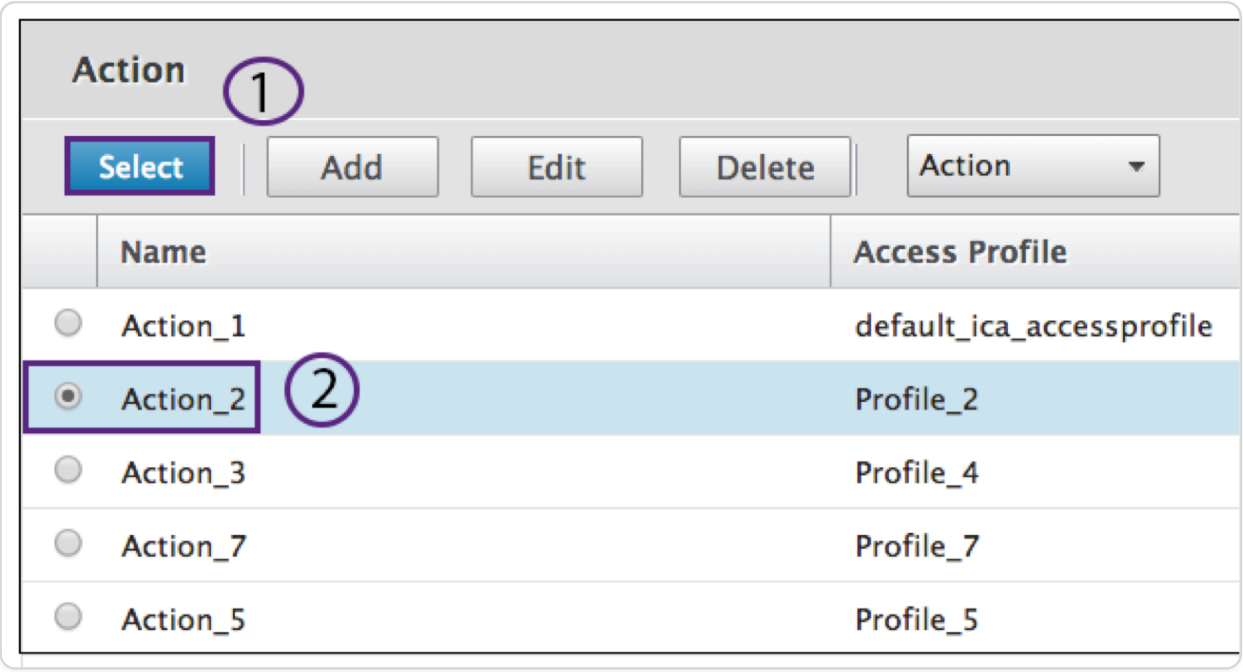
1. Escriba un nombre para la acción.
2. Seleccione una de las siguientes opciones para proporcionar el perfil de acceso:
   - Haga clic en > para seleccionar un perfil de acceso existente. Consulte los detalles en (#common-processes).
   - Haga clic en + para crear un perfil de acceso. Consulte los detalles Crear un perfil de acceso.
   - El icono del **lápiz** está inhabilitado.
3. Haga clic en **Crear**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.




### Seleccionar una acción

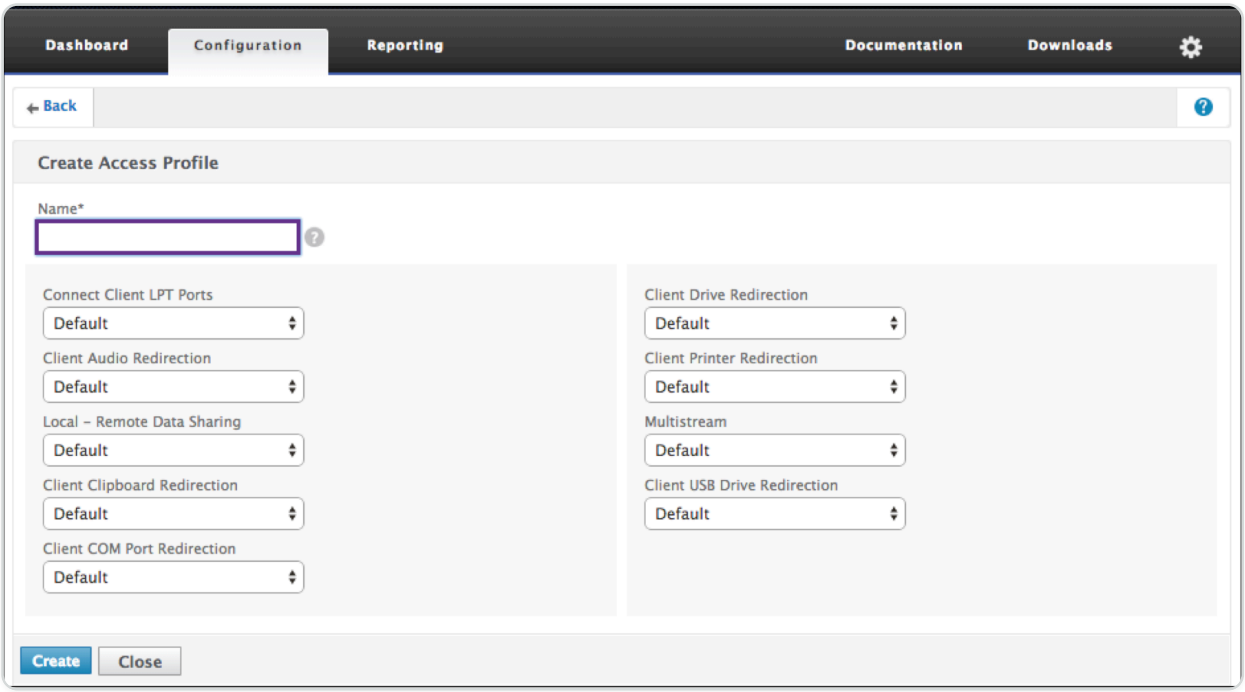
1. Seleccione una acción haciendo clic en el botón de radio a la izquierda de la misma. El perfil de acceso asociado especifica las funciones de usuario permitidas.
2. Haga clic en el botón **Seleccionar**.




### Crear un perfil de acceso

1. Asigne un nombre al perfil de acceso.

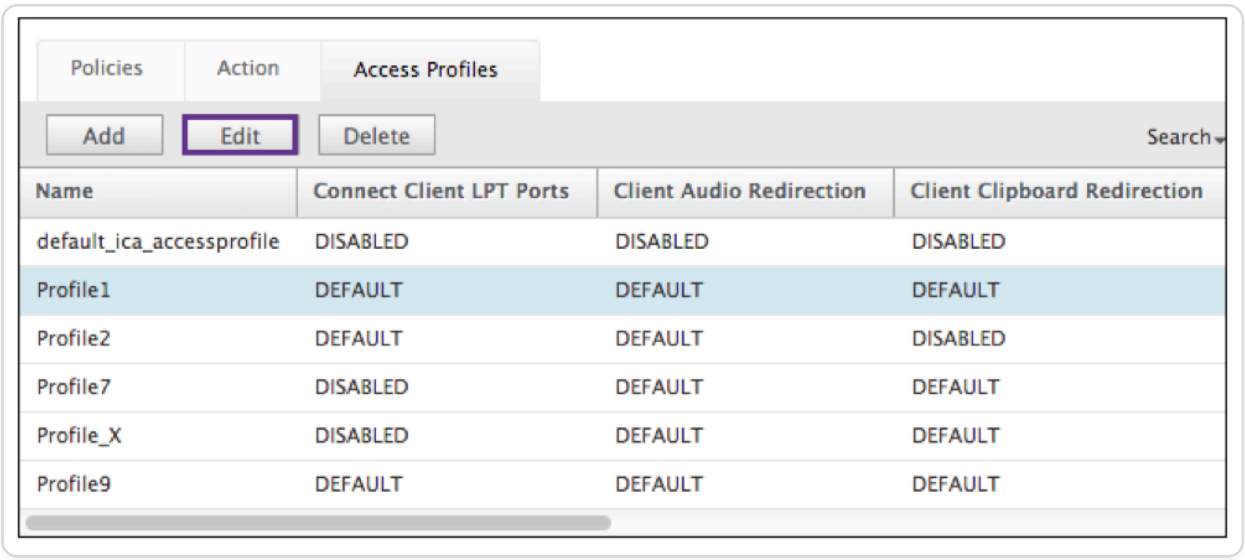
© 1997–2026 Citrix Systems, Inc. All rights reserved.




2. Puede configurar el perfil de acceso desde este menú.
3. Haga clic en **Crear**.

### Seleccionar un perfil de acceso existente

1. Seleccione un perfil de acceso haciendo clic en él.




2. Haga clic en Editar.
3. Configure el perfil de acceso. Para obtener más información, consulte Configurar perfil de acceso.

### Expresiones

1. Para crear o revisar una expresión existente, seleccione Borrar.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

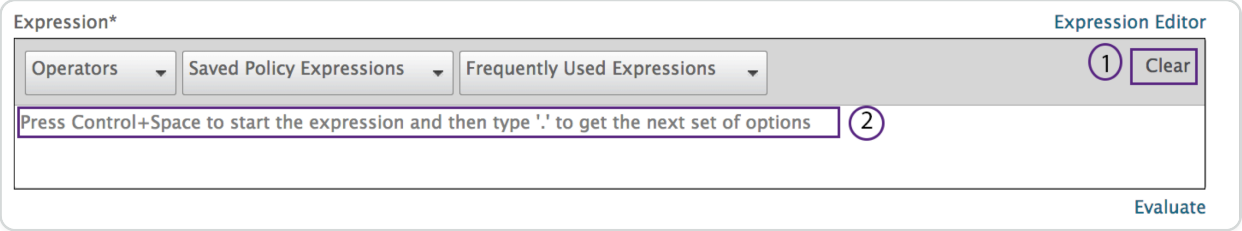
Las expresiones son las expresiones ICA típicas. Para las expresiones HTTP, introduzca el nombre con las comillas y elimine los paréntesis.

| | |
|---|---|
| ICA.SERVER.PORT | Esta expresión comprueba que el puerto especificado coincide con el número de puerto de las aplicaciones y escritorios virtuales de Citrix a los que el usuario intenta conectarse. |
| ICA.SERVER.IP | Esta expresión comprueba que la IP especificada coincide con la dirección IP de las aplicaciones y escritorios virtuales de Citrix a los que el usuario intenta conectarse. |
| `HTTP.REQ.USER.IS\_MEMBER\_OF(“”)` .NOT | Esta expresión comprueba que la conexión actual es accedida por un usuario que NO es miembro del nombre de grupo especificado. |
| HTTP.REQ.USER .IS_MEMBER_OF(“ `group name` ”) | Esta expresión comprueba que el usuario que accede a la conexión actual es miembro del grupo especificado. |
| HTTP.REQ.USER.NAME.CONTAINS(“”).NOT | Esta expresión comprueba que el usuario que accede a la conexión actual NO es miembro del grupo especificado. |
| HTTP.REQ.USER.NAME.CONTAINS(“enter `user name` ”) Especifica los recursos para un nombre de usuario. | Esta expresión comprueba que la conexión actual es accedida por el nombre especificado. |
| CLIENT.IP.DST.EQ(introduzca la dirección IP aquí).NOT | Esta expresión comprueba que la IP de destino del tráfico actual NO es igual a la dirección IP especificada. |
| CLIENT.IP.DST.EQ(introduzca la dirección IP aquí) | Esta expresión comprueba que la IP de destino del tráfico actual es igual a la dirección IP especificada. |
| CLIENT.TCP.DSTPORT.EQ (introduzca el número de puerto).NOT | Esta expresión comprueba que el puerto de destino NO es igual al número de puerto especificado. |

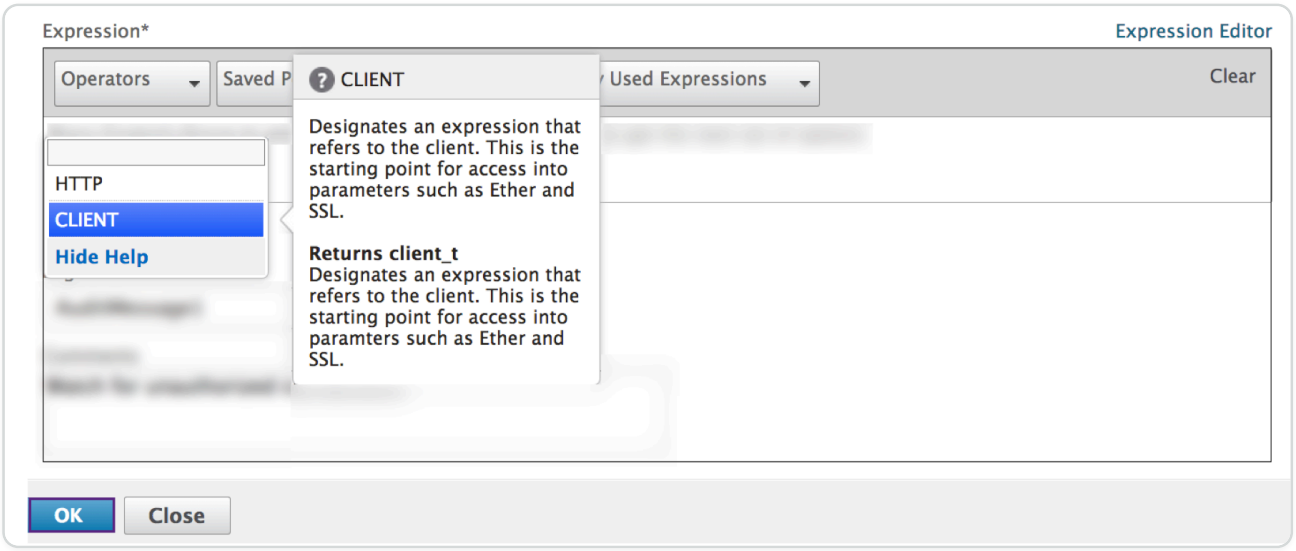
© 1997–2026 Citrix Systems, Inc. All rights reserved.

| | |
|---|---|
| CLIENT.TCP.DSTPORT.EQ (introduzca el número de puerto) | Esta expresión comprueba que el puerto de destino es igual al número de puerto especificado. |

2. Al mismo tiempo, seleccione **Control** y la barra **Espacio**. A continuación, sus opciones serán visibles.




3. Escriba el punto. Haga su selección y pulse la **Space** barra.
4. En cada punto de la expresión de la tabla anterior, escriba el punto. Haga su selección y pulse la barra espaciadora.
5. Haga clic en **Aceptar**.



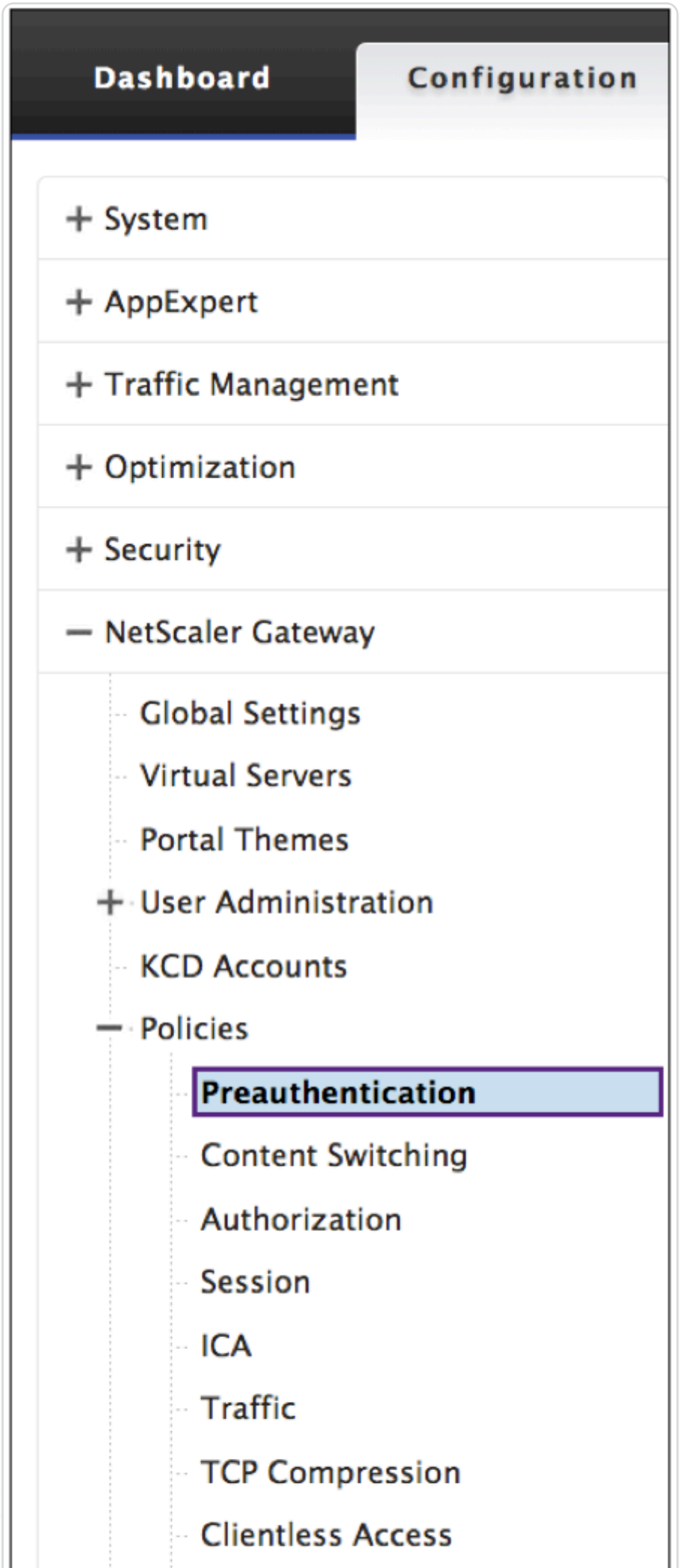

### Identificación de grupo

Las funciones de preautenticación o de sesión definen la expresión con una variable de nombre de grupo.

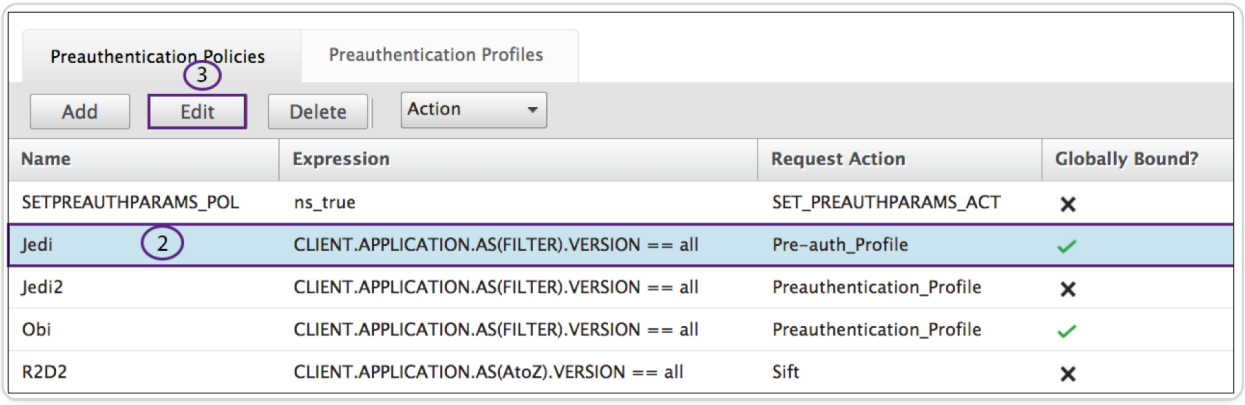
### Preautenticación

1. Seleccione Preautenticación en el panel de configuración.

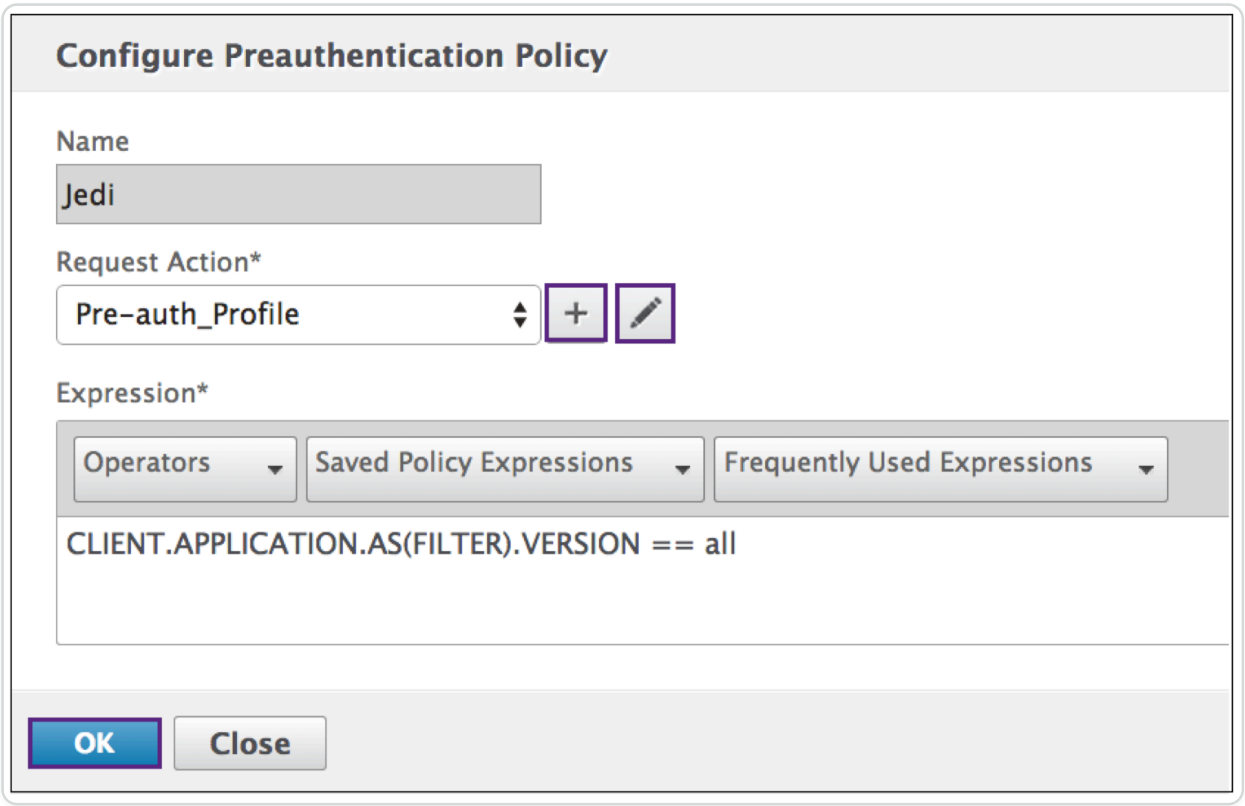
© 1997–2026 Citrix Systems, Inc. All rights reserved.


Dashboard
Configuration
+ System
+ AppExpert
+ Traffic Management
+ Optimization
+ Security
– NetScaler Gateway
Global Settings
Virtual Servers
Portal Themes
+ User Administration
KCD Accounts
– Policies
Preauthentication
Content Switching
Authorization
Session
ICA
Traffic
TCP Compression
Clientless Access

1. Seleccione un nombre de las directivas de preautenticación.
2. Seleccione **Modificar** en la ficha Directivas de preautenticación.

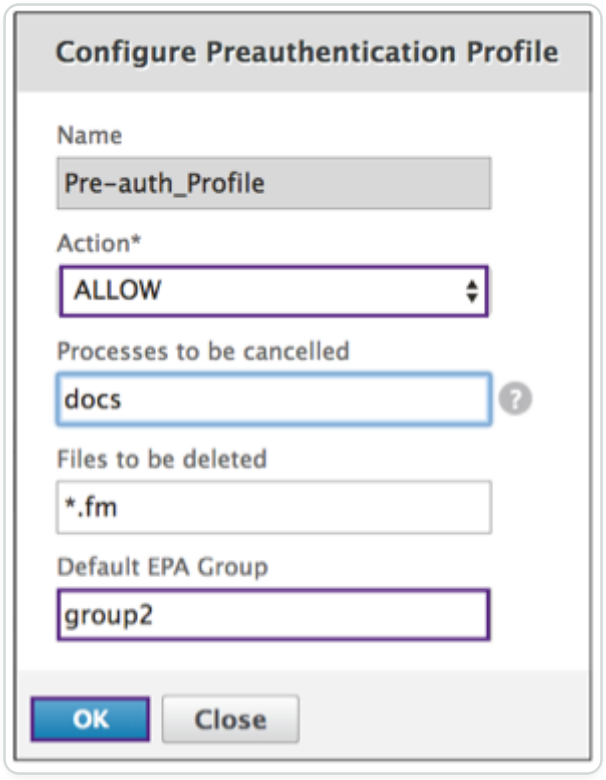



3. Seleccione el icono del **lápiz** o **+** junto al cuadro de diálogo Acción de solicitud.




4. Defina el (“\< `groupname` \>”) en el cuadro de diálogo Grupo EPA predeterminado.

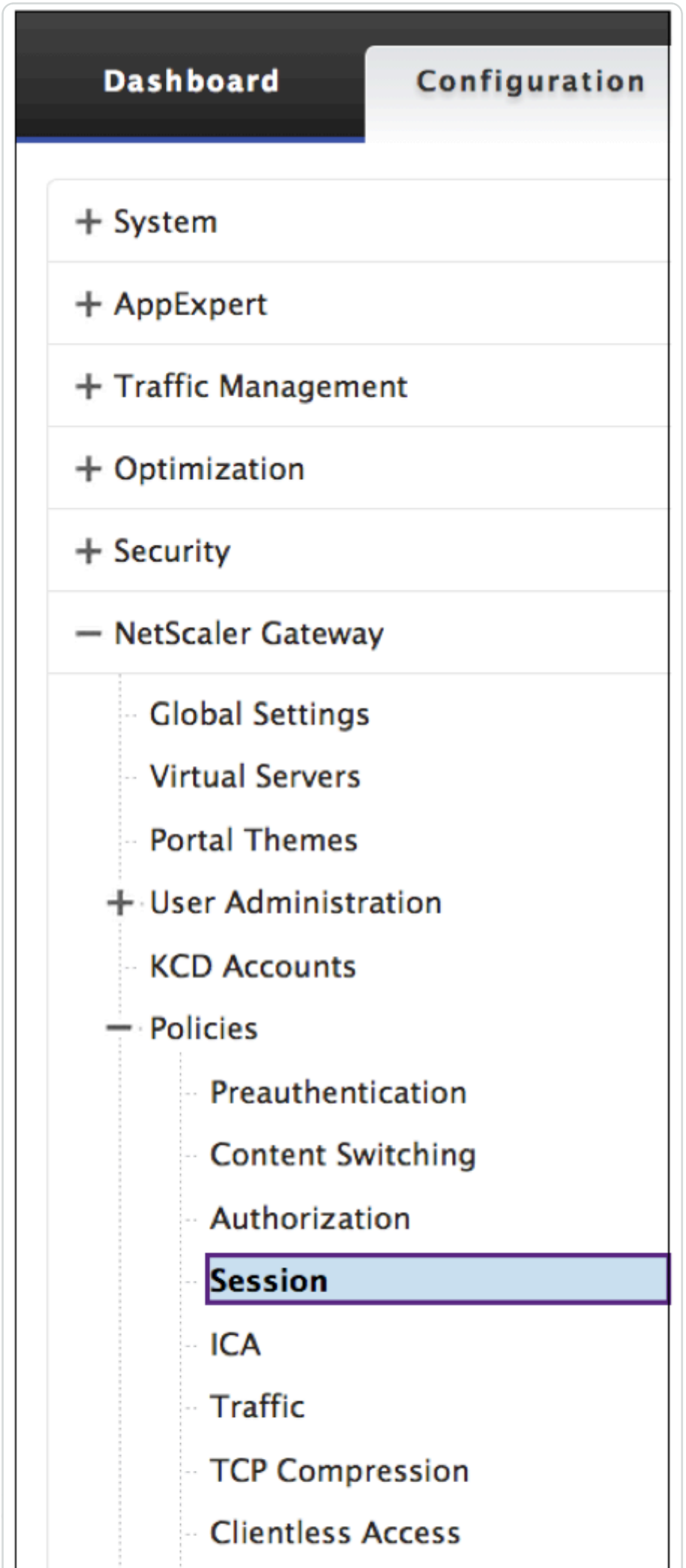
© 1997–2026 Citrix Systems, Inc. All rights reserved.




## Sesión

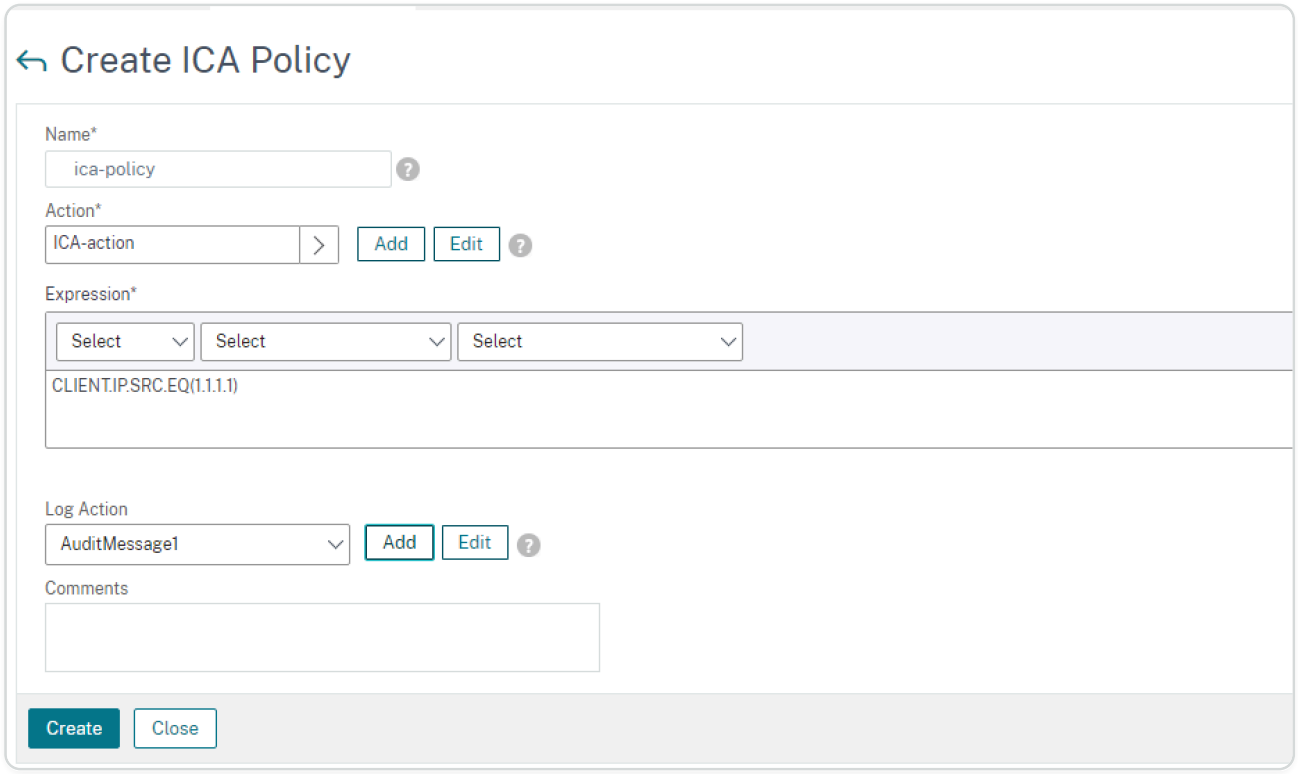
1. Seleccione **Sesión** en el panel de configuración.

© 1997–2026 Citrix Systems, Inc. All rights reserved.


Dashboard
Configuration
+ System
+ AppExpert
+ Traffic Management
+ Optimization
+ Security
– NetScaler Gateway
Global Settings
Virtual Servers
Portal Themes
+ User Administration
KCD Accounts
– Policies
Preauthentication
Content Switching
Authorization
Session
ICA
Traffic
TCP Compression
Clientless Access

## Crear una acción de registro

1. En la pantalla **Configurar directiva**, junto al cuadro de diálogo **Acción de registro**, seleccione el icono **+**




### Crear acción de mensaje de auditoría

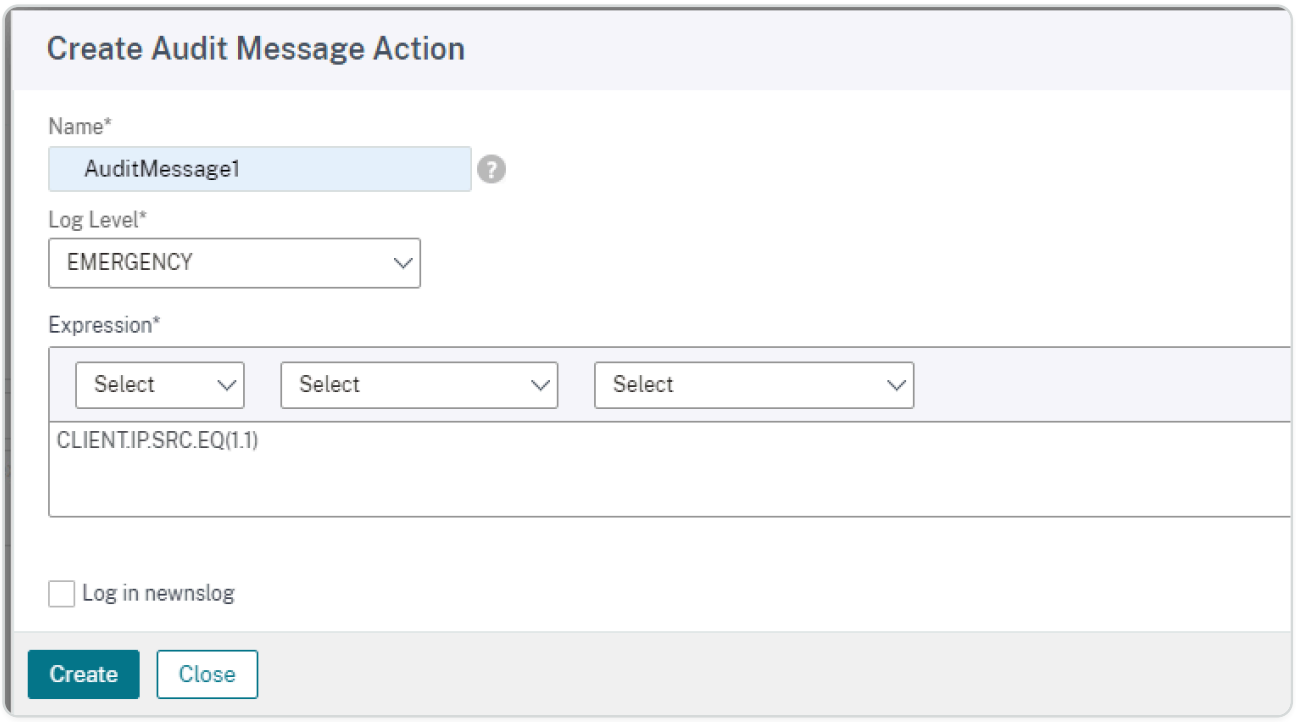
1. Aparece la pantalla **Crear acción de mensaje de auditoría**. Asigne un nombre al mensaje de auditoría. El mensaje de auditoría solo acepta números, letras o un carácter de subrayado.
2. En el menú, especifique el nivel de registro de auditoría.

| | |
|---|---|
| Emergencia | Eventos que indican una crisis inmediata en el servidor. |
| Alerta | Eventos que podrían requerir una acción. |
| Crítico | Eventos que indican una crisis inminente del servidor. |
| Error | Eventos que indican algún tipo de error. |
| Advertencia | Eventos que requieren una acción pronto. |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| | |
|---|---|
| Aviso | Eventos de los que el administrador debe estar al tanto. |
| Informativo | Todos los eventos excepto los de bajo nivel. |
| Depuración | Todos los eventos, con extremo detalle. |

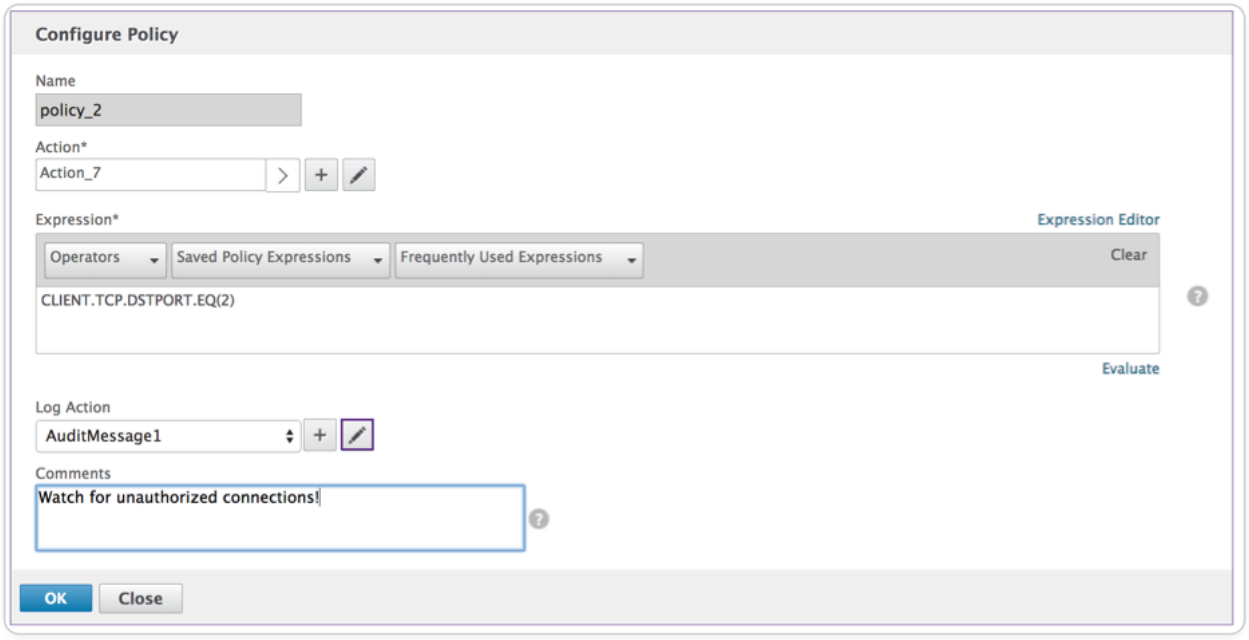
1. Introduzca una expresión. La expresión define el formato y el contenido del registro.
2. Las casillas de verificación.
   - Marque el registro en `newnslog` para enviar el mensaje a un nuevo registro ns.
   - Seleccione **Omitir comprobación de seguridad** para omitir la comprobación de seguridad. Esto permite expresiones no seguras.
3. Haga clic en **Crear**.




## Revisar una acción de registro

1. En la pantalla Configurar directiva, junto al cuadro de diálogo Acción de registro, haga clic en el icono.

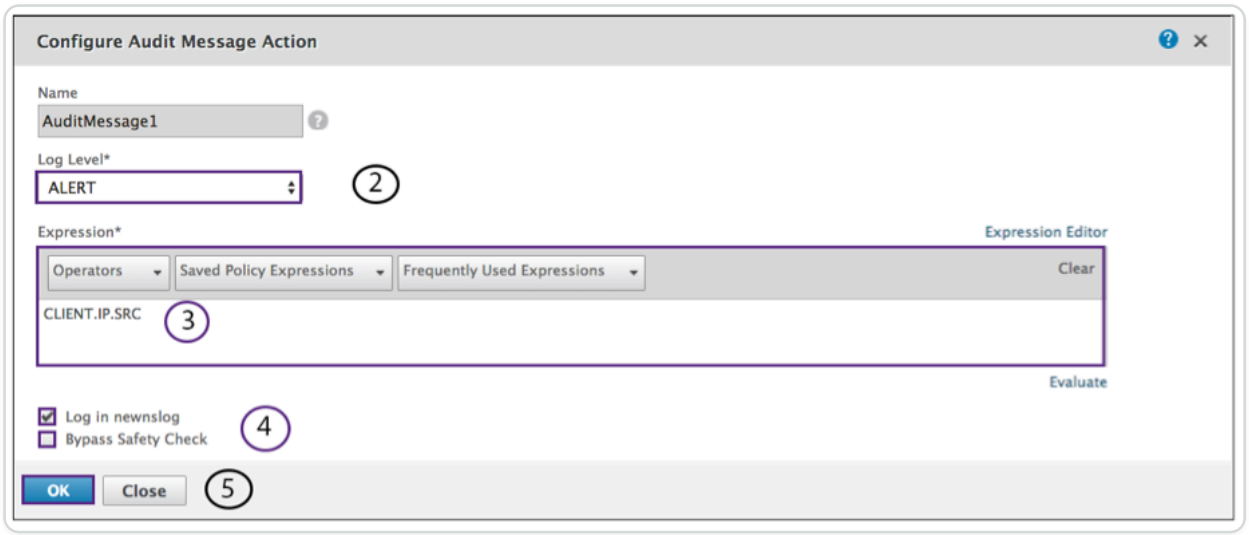
© 1997–2026 Citrix Systems, Inc. All rights reserved.




## Configurar acción de mensaje de auditoría

Los siguientes son campos editables:

1. En el menú, especifique el nivel de registro de auditoría.
2. Introduzca una expresión. La expresión define el formato y el contenido del registro.
3. Las casillas de verificación:
   - Marque la casilla Registrar en `newnslog` para enviar el mensaje a un nuevo registro ns.
   - Seleccione **Omitir comprobación de seguridad** para omitir la comprobación de seguridad. Esto permite expresiones no seguras.
4. Haga clic en **Aceptar**.




© 1997–2026 Citrix Systems, Inc. All rights reserved.

## Seleccionar una directiva existente

1. Haga clic en el icono > para seleccionar una política existente.

   Página de directivas(/en-us/netscaler-gateway/media/fig91-policy-binding.png)

2. Seleccione el botón de opción de la política deseada.

   Seleccionar una directiva(/en-us/netscaler-gateway/media/fig92-policies.png)

## Crear una política

1. En **Nombre**, escriba un nombre para la política.
2. Haga clic en + para crear una política.

   Crear política(/en-us/netscaler-gateway/media/fig93-create-policies.png)

3. Cree una acción. Para obtener más información, consulte **Crear una nueva acción**.
4. Asigne un nombre al perfil de acceso.

   Nombre del perfil de acceso(/en-us/netscaler-gateway/media/fig94-create-access-profile.png)

5. Configure el perfil de acceso desde este menú.
6. Haga clic en **Crear**.
7. Haga clic en **Enlazar**.

   Página de enlace(/en-us/netscaler-gateway/media/fig95-policy-binding.png)

## Configuración del análisis de puntos finales de preautenticación y postautenticación

Esta sección describe cómo configurar el análisis de puntos finales (EPA) de postautenticación y preautenticación.

Para configurar el EPA de postautenticación con SmartControl, utilice el parámetro `Smartgroup` de la acción de sesión VPN. La expresión EPA se configura en la política de sesión VPN.

Puede especificar un nombre de grupo para el parámetro de grupo inteligente. Este nombre de grupo puede ser cualquier cadena. El nombre de grupo no necesita ser un grupo existente en el directorio activo.

Configure la política ICA con la expresión HTTP.REQ.IS_MEMBER_OF ("`groupname`"). Utilice el nombre de grupo que se especificó anteriormente para el grupo inteligente.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Para configurar el EPA de preautenticación con SmartControl, utilice el parámetro de grupo EPA predeterminado del perfil de preautenticación. La expresión EPA se configura en la política de preautenticación.

Puede especificar un nombre de grupo para el parámetro de grupo EPA predeterminado. Este nombre de grupo puede ser cualquier cadena. El nombre de grupo no necesita ser un grupo existente en el directorio activo.

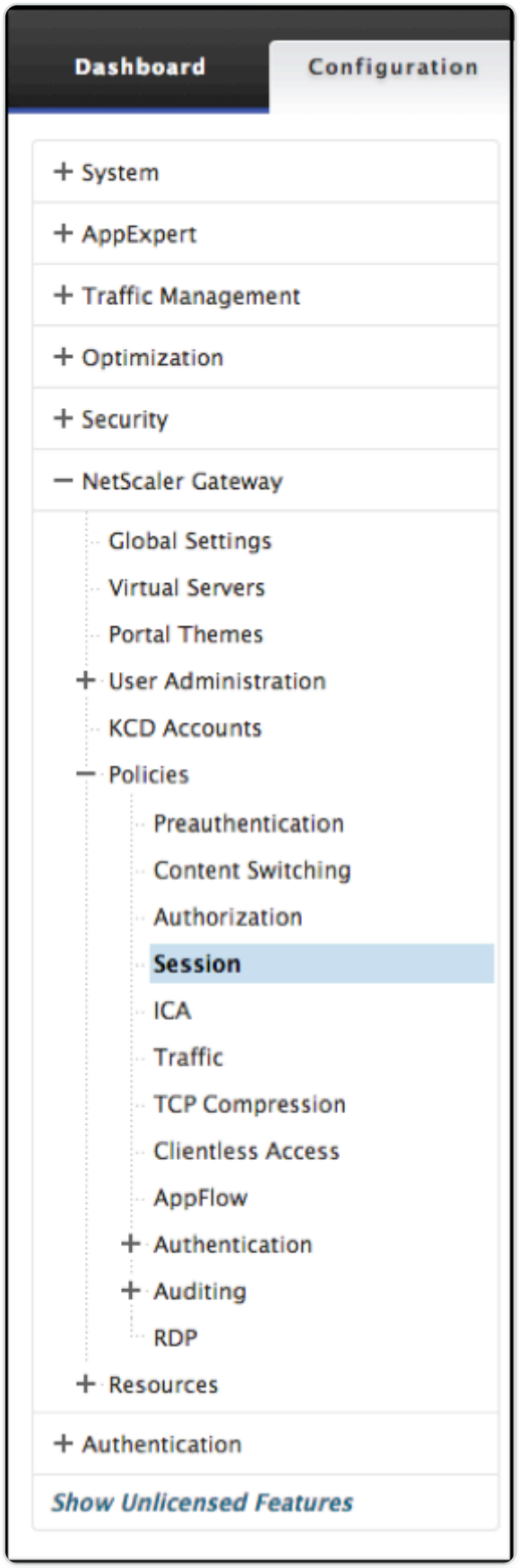
Configure la política ICA con la expresión HTTP.REQ.IS_MEMBER_OF ("`groupname`"), utilice el nombre de grupo que se especificó anteriormente para el grupo EPA predeterminado.

### Configuración de postautenticación

**Utilice el siguiente procedimiento para configurar grupos inteligentes para la configuración de postautenticación.**

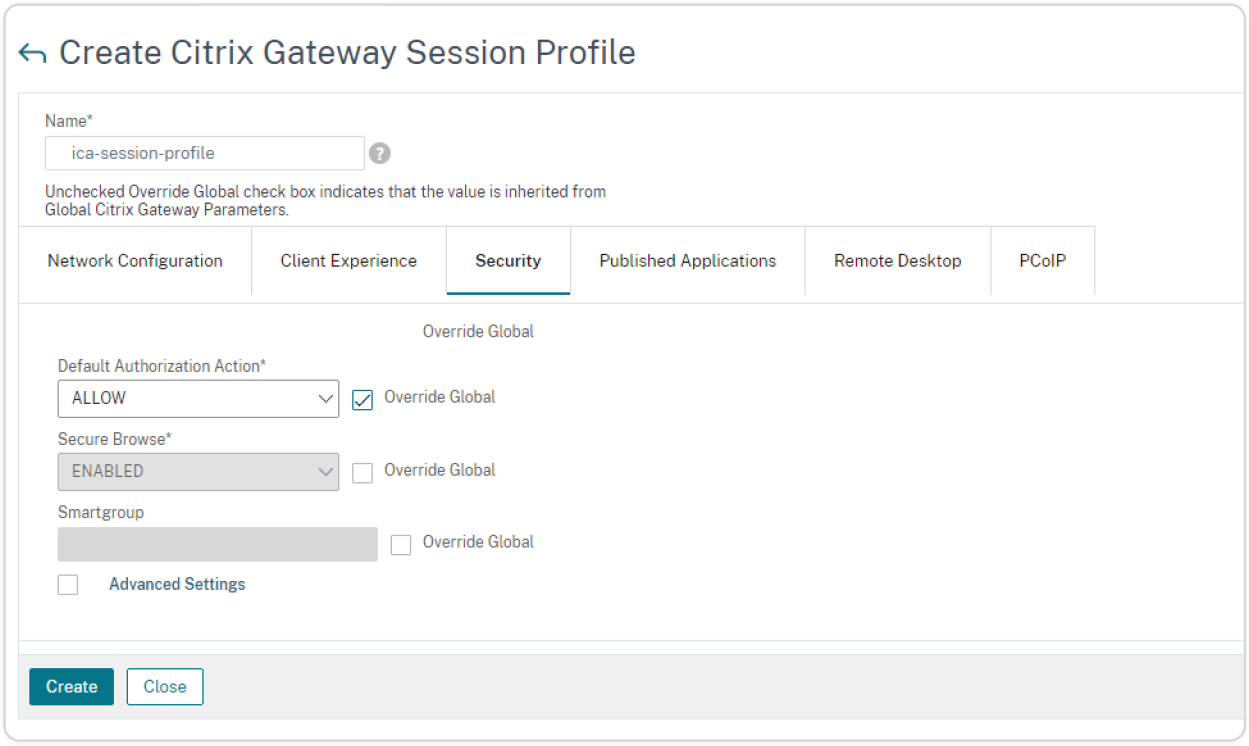
1. Vaya a **NetScaler Gateway > Directivas > Sesión**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.




2. Vaya a **Perfiles de sesión > Agregar**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.




## Crear perfil de sesión de NetScaler Gateway

1. Seleccione la pestaña **Security**.
2. Introduzca un **Name** para su perfil de NetScaler Gateway (acción).
3. Seleccione la casilla a la derecha del menú y seleccione la **Default Authorization Action** deseada.

   Especifique los recursos de red a los que los usuarios tienen acceso cuando inician sesión en la red interna. La configuración predeterminada para la autorización es denegar el acceso a todos los recursos de red. Citrix® recomienda utilizar la configuración global predeterminada y luego crear políticas de autorización para definir los recursos de red a los que los usuarios pueden acceder. Si establece la política de autorización predeterminada en DENY, debe autorizar explícitamente el acceso a cualquier recurso de red, lo que mejora la seguridad.
4. Seleccione la casilla a la derecha del menú y seleccione la opción **Secure Browse.** deseada.

   Permita a los usuarios conectarse a través de NetScaler Gateway a los recursos de red desde dispositivos móviles iOS y Android con la aplicación Citrix Workspace. Los usuarios no necesitan establecer un túnel VPN completo para acceder a los recursos de la red segura.
5. Seleccione la casilla a la derecha del menú e introduzca el nombre `Smartgroup`.

   Este es el grupo en el que se coloca al usuario cuando la política de sesión asociada a esta acción de sesión se ejecuta correctamente. La política de sesión VPN realiza la comprobación EPA posterior a la autenticación y, si la comprobación se realiza correctamente, el usuario se

© 1997–2026 Citrix Systems, Inc. All rights reserved.

coloca en el grupo especificado con un grupo inteligente. La expresión is_member_of (http.req.user.is_member_of) se puede utilizar luego con políticas para comprobar si la EPA ha pasado para el usuario que pertenece a este grupo inteligente.

6. Haga clic en **Create**.
7. Vaya a **NetScaler Gateway > Policies > Session**.
8. Vaya a **Session Policies > Add**.
9. Introduzca el **Name** para la nueva política de sesión que se aplica después de que el usuario inicie sesión en NetScaler Gateway.
10. Seleccione la acción **Profile** usando el menú.

    La acción aplicada por la nueva política de sesión si se cumple el criterio de la regla.

    **Nota:** Si el perfil deseado debe crearse, seleccione el +. Para obtener más detalles, consulte Crear perfil de sesión de NetScaler Gateway.
11. Introduzca **Expresión** en este campo.

    Este campo define la expresión con nombre que especifica el tráfico que coincide con la directiva. La expresión se puede escribir en sintaxis predeterminada o clásica. La longitud máxima de una cadena literal para la expresión es de 255 caracteres. Una cadena más larga se puede dividir en cadenas más pequeñas de hasta 255 caracteres cada una, y las cadenas más pequeñas se concatenan con el operador +. Por ejemplo, puede crear una cadena de 500 caracteres de la siguiente manera: """" + """"

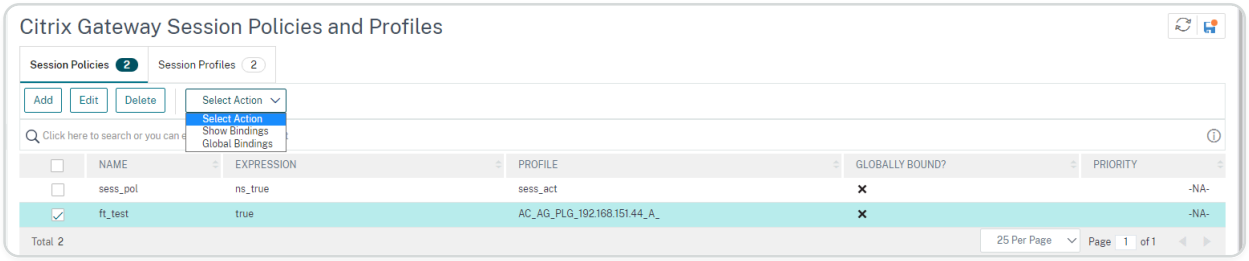
    Los siguientes requisitos se aplican solo a la CLI de NetScaler:

    - Si la expresión incluye uno o más espacios, encierre toda la expresión entre comillas dobles.
    - Si la expresión en sí incluye comillas dobles, escape las comillas usando el carácter.* Alternativamente, puede usar comillas simples para encerrar la regla, en cuyo caso no tendrá que escapar las comillas dobles.
12. Haga clic en **Crear**.
13. Vaya a **Directivas de sesión**.
14. Seleccione el **Nombre** de la directiva de sesión.
15. Seleccione **Enlaces globales** en el menú **Acción**.
16. Seleccione **Agregar enlace**.
17. Seleccione el **>** para elegir una directiva existente.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**Nota:** Seleccione + para crear una directiva. Para obtener más detalles, consulte la sección Crear perfil de sesión de NetScaler Gateway.

18. Elija un nombre de la lista y pulse el botón **Seleccionar**.
19. Introduzca la **Prioridad** y haga clic en **Enlazar**.
20. Haga clic en **Listo**
21. La comprobación muestra que su selección está Enlazada globalmente.

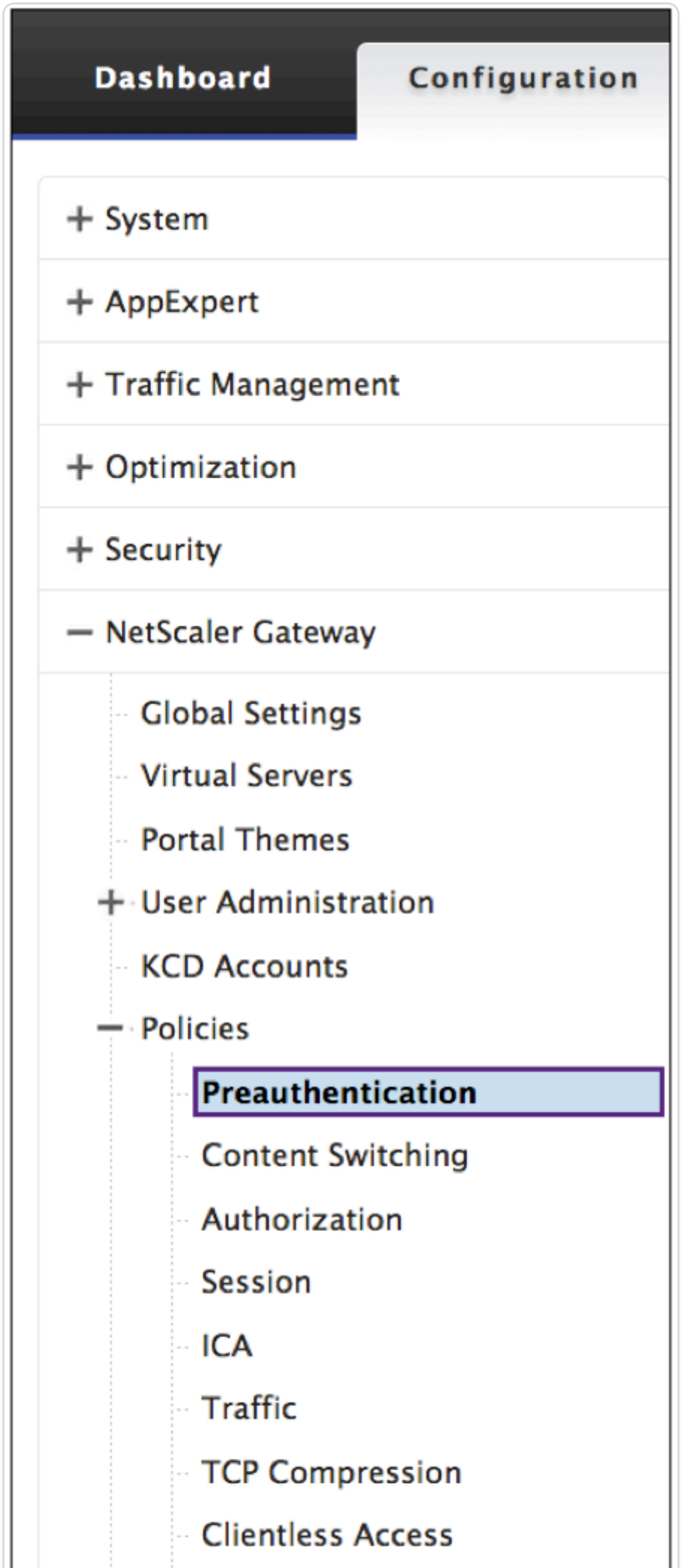



## Configuración de la autenticación previa

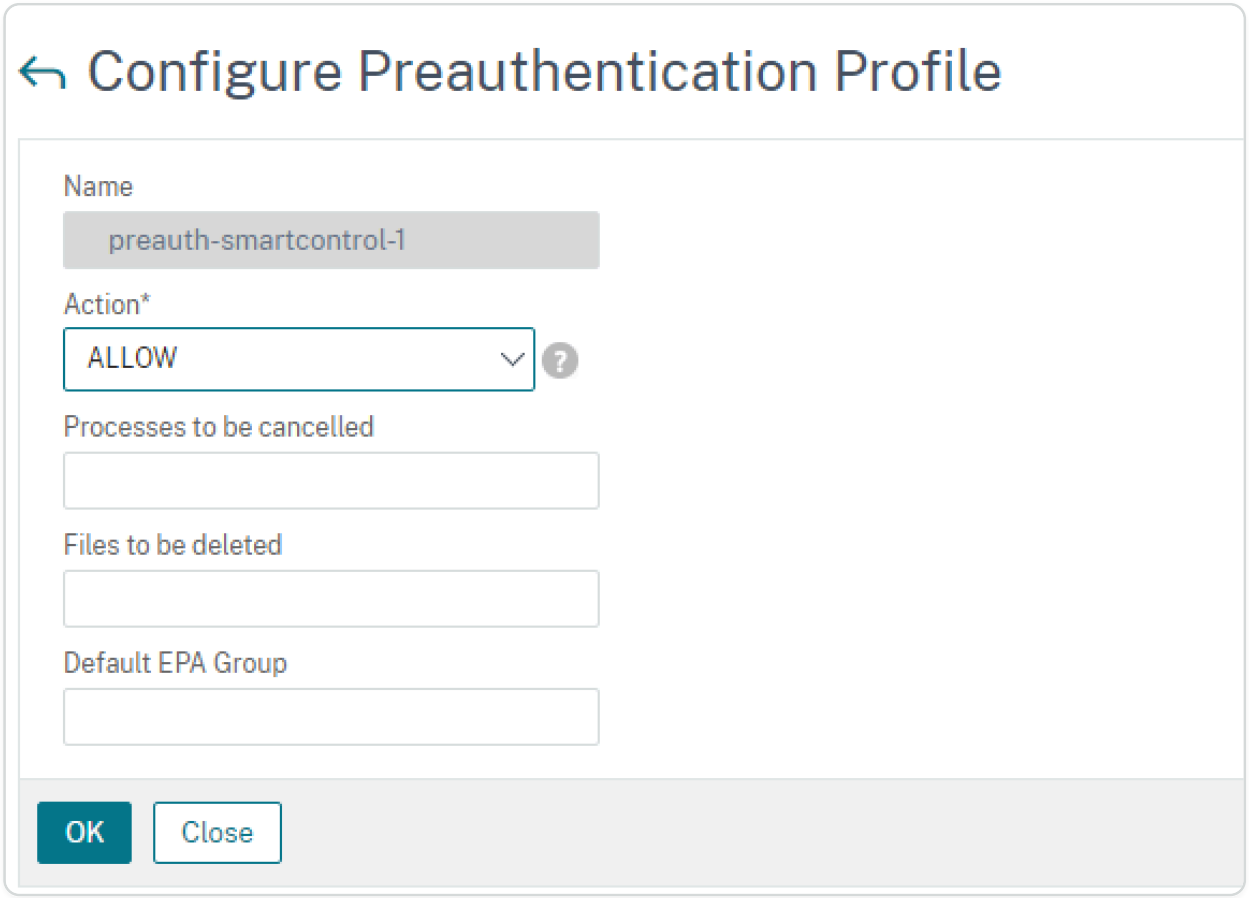
Siga este procedimiento para configurar la autenticación previa.

1. Vaya a **NetScaler Gateway > Directivas > Autenticación previa**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.


Dashboard
Configuration
+ System
+ AppExpert
+ Traffic Management
+ Optimization
+ Security
− NetScaler Gateway
Global Settings
Virtual Servers
Portal Themes
+ User Administration
KCD Accounts
− Policies
Preauthentication
Content Switching
Authorization
Session
ICA
Traffic
TCP Compression
Clientless Access

2. Seleccione la ficha **Perfiles de autenticación previa** y, a continuación, seleccione **Agregar**.




3. Introduzca el **Nombre** de la acción de autenticación previa.

   El nombre debe comenzar con una letra, un número o un guion bajo (_), y debe constar únicamente de letras, números y los caracteres guion (-), punto (.), almohadilla (#), espacio ( ), arroba (@), igual (=), dos puntos (:) y guion bajo. No se puede cambiar después de crear la acción de autenticación previa.

   **Nota:** El siguiente requisito se aplica únicamente a la CLI de NetScaler: Si el nombre incluye uno o varios espacios, escríbalo entre comillas dobles o simples.

4. Seleccione una **Acción de solicitud** que la directiva deba invocar cuando una conexión coincida con la directiva.

   **Nota:** Si quiere crear un perfil de autenticación previa, seleccione el signo +. Para obtener más información, consulte Crear perfil de autenticación previa

5. Introduzca una **Expresión** que sea el nombre de la regla con nombre de NetScaler o una expresión de sintaxis predeterminada que defina las conexiones que coinciden con la directiva.
6. Haga clic en **Crear**.
7. Vaya a la pestaña **Directivas de preautenticación** y seleccione la directiva deseada.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

8. Seleccione **Enlace global** en el menú **Acción**.
9. Seleccione **Agregar enlaces**.
10. Seleccione > para seleccionar una directiva existente.

    Seleccione + para crear una directiva. Para obtener más información, consulte Crear perfil de sesión de NetScaler Gateway.
11. **Seleccione** Directiva.
12. Introduzca la **Prioridad** y haga clic en **Enlazar**.
13. Haga clic en **Listo**.
14. La comprobación muestra que la **Directiva de preautenticación** está **Enlazada globalmente**.

## Crear perfil de preautenticación

1. Introduzca el **Nombre** para la acción de preautenticación

   El nombre debe comenzar con una letra, un número o el carácter de subrayado (_), y debe constar únicamente de letras, números y los caracteres de guion (-), punto (.), almohadilla (#), espacio ( ), arroba (@), igual (=), dos puntos (:) y subrayado. No se puede cambiar después de crear la acción de preautenticación.

   **Nota:** Si el nombre incluye uno o varios espacios, escríbalo entre comillas dobles o simples. Esto solo se aplica a la CLI de NetScaler.
2. Introduzca la **Acción** en el menú.

   Esta opción permitirá o denegará el inicio de sesión después de los resultados del análisis de puntos finales (EPA).
3. **Procesos a cancelar**

   Esta opción identifica una cadena de procesos que la herramienta de análisis de puntos finales (EPA) debe finalizar.
4. **Archivos a eliminar**

   Esta opción identifica una cadena que especifica las rutas y los nombres de los archivos que la herramienta de análisis de puntos finales (EPA) debe eliminar.
5. **Grupo EPA predeterminado**

   El grupo EPA predeterminado es el grupo que se elige cuando la comprobación de EPA se realiza correctamente.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

6. Haga clic en **Crear**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

# Integración de Microsoft Intune

La integración de Microsoft Intune con NetScaler Gateway proporciona una solución de acceso a aplicaciones y protección de datos de primera clase ofrecida por NetScaler Gateway e Intune.

Obtendrá la suite más completa de aplicaciones de productividad seguras, que incluye correo electrónico, calendario, contactos, toma de notas, edición de documentos y acceso remoto, todo ello gestionable de forma centralizada en diferentes plataformas. La integración de Intune y NetScaler Gateway proporciona funcionalidades de gestión de dispositivos móviles (MDM) de primera clase, mientras que la tecnología del lado del cliente de Citrix Secure Access permite a estas aplicaciones habilitadas para Intune acceder a los datos y aplicaciones corporativos de forma segura a través de NetScaler Gateway.

La integración permite a NetScaler Gateway extraer datos de cumplimiento de Intune, lo que habilita las directivas de acceso condicional. Las directivas de acceso condicional otorgan a NetScaler Gateway un control más preciso para regular el acceso en función de las funcionalidades del dispositivo, etc. Por ejemplo, un administrador puede crear una directiva en la que solo se conceda acceso a los dispositivos con la “Cámara” deshabilitada.

NetScaler Gateway admite la autenticación de tokens de la Biblioteca de autenticación de Microsoft (MSAL) una vez configurado el servidor virtual de NetScaler Gateway. Tras la configuración, una aplicación móvil encapsulada con el contenedor o SDK de Citrix Network-Only accede a NetScaler Gateway mediante un token MSAL que la aplicación puede obtener directamente de Microsoft Entra ID.

## Integración de micro VPN de Citrix® con Microsoft Endpoint Manager

Los clientes de NetScaler Gateway pueden usar micro VPN con Microsoft Endpoint Manager (Intune). La integración de micro VPN de Citrix con Microsoft Endpoint Management permite que sus aplicaciones accedan a los recursos locales.

La tecnología micro VPN de Citrix proporciona una VPN a petición que reduce los costes de transferencia de datos y simplifica la seguridad, ya que el túnel VPN no siempre está activo. En su lugar, solo está activo cuando es necesario, lo que reduce el riesgo y optimiza el rendimiento del dispositivo para una mejor experiencia de usuario. Esto también ayuda a mejorar la duración de la batería del móvil. La tecnología micro VPN de NetScaler® proporciona a los usuarios móviles

© 1997–2026 Citrix Systems, Inc. All rights reserved.

acceso seguro a los recursos empresariales internos, al tiempo que les ofrece la mejor experiencia de usuario.

Micro VPN solo es compatible con los siguientes casos de uso:

- Solo gestión de aplicaciones móviles (MAM) de Intune
- Gestión de dispositivos móviles (MDM) y gestión de aplicaciones móviles (MAM) de Intune

**IMPORTANTE:**

Para la funcionalidad SSL VPN, micro VPN requiere una edición NetScaler Gateway Advanced o Premium (VPX 3000 o superior) y un derecho de Citrix Endpoint Management. El derecho de Citrix Endpoint Management garantiza el soporte continuo del SDK de micro VPN en un navegador móvil Microsoft Edge (iOS y Android). Para obtener más información, póngase en contacto con su representante de ventas, de cuenta o de socio.

Para obtener más información sobre cómo configurar la integración de micro VPN de Citrix con Microsoft Endpoint Manager, consulte Configurar NetScaler Gateway para usar micro VPN con Microsoft Endpoint Manager.

## Cuándo usar la solución MDM de Intune integrada

Los siguientes escenarios ilustran el uso de la solución MDM de Intune integrada:

- Un nuevo cliente decide incorporar Intune con la implementación local de NetScaler Gateway
- Un usuario existente de NetScaler Gateway quiere añadir la administración de dispositivos móviles con Intune
- Un usuario existente de Intune quiere permitir que los dispositivos móviles o las aplicaciones accedan a los datos ubicados dentro de la red de la empresa con un dispositivo físico o virtual de NetScaler Gateway en la DMZ de la empresa

**NOTA**

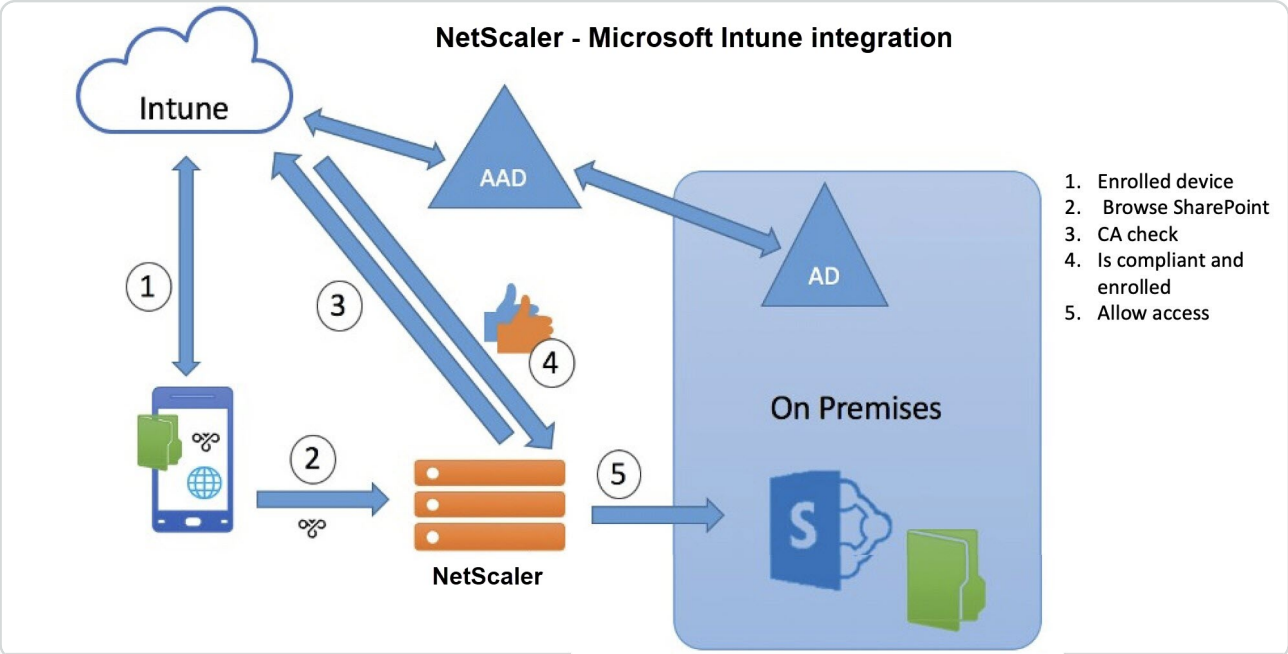
Solo se admiten clientes iOS y Android.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

# Descripción de la integración de MDM de NetScaler Gateway con Intune

A continuación, se muestra un ejemplo del flujo de eventos en una integración típica de MDM de NetScaler Gateway con Intune:

1. Inscriba un dispositivo móvil en Intune.
2. Las aplicaciones aprobadas por la empresa y las políticas de dispositivos se envían al dispositivo.
3. Explore SharePoint (aplicación local) desde el dispositivo.
4. La solicitud del navegador va a NetScaler Gateway.
5. El dispositivo NetScaler Gateway comprueba con Intune el estado de inscripción del dispositivo.
6. Si un dispositivo compatible se inscribe correctamente, se concede el acceso a SharePoint.




Cuando un dispositivo no cumple una política de acceso condicional, el cliente VPN de NetScaler Gateway muestra un mensaje de error. El mensaje proporciona un enlace desde el dispositivo a una página alojada por Intune que ofrece al usuario la opción de inscribir o corregir el estado de cumplimiento del dispositivo.

**NOTA:**

Los administradores deben asegurarse de lo siguiente al enviar los certificados a Intune para que los usuarios puedan diferenciar entre los distintos certificados de su dispositivo.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Los certificados deben tener un resumen del asunto.
- Los resúmenes de asunto para diferentes certificados deben ser distintos.

### Compatibilidad con la API Intune NAC v2

Como parte del soporte de la API Intune NAC v2, debe vincular un archivo de Autoridad de Certificación (certificado CA) para asegurarse de que el dispositivo NetScaler obtenga un certificado válido de los dispositivos móviles. En Intune NAC v2, los dispositivos móviles envían ID de dispositivo como parte del certificado CA. El certificado CA vinculado aquí debe ser el utilizado para emitir certificados de cliente a los dispositivos iOS y Android del usuario final. Si hay certificados intermedios, también deben vincularse aquí.

Para obtener más detalles, consulte Soporte de la API Intune NAC v2

## Configurar la comprobación de dispositivos de Control de Acceso a la Red para el servidor virtual de NetScaler Gateway para el inicio de sesión de factor único

Este tema proporciona información sobre la configuración de NetScaler Gateway para conectarse a una red interna desde un dispositivo móvil (iOS y Android) con la seguridad de Cumplimiento de Acceso a la Red (NAC) ofrecida por Microsoft Intune. Cuando un usuario intenta conectarse a NetScaler Gateway desde un cliente VPN de iOS o Android, el gateway primero comprueba con el servicio de Intune si el dispositivo es un dispositivo administrado y compatible.

- Administrado: El dispositivo está inscrito mediante el cliente del Portal de empresa de Intune.
- Compatible: Se aplican las directivas requeridas enviadas desde el servidor MDM de Intune.

Solo si el dispositivo está administrado y es compatible, se establece la sesión VPN y se le proporciona al usuario acceso a los recursos internos.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**NOTA:**

- En esta configuración, NetScaler Gateway en el back-end se comunica con el servicio de Intune. Los perfiles SSL gestionan las conexiones entrantes a NetScaler Gateway. La comunicación de back-end de NetScaler Gateway gestiona cualquier requisito de SNI de los servicios en la nube de back-end (Intune).
- SNI para el servidor virtual de gateway DTLS es compatible con NetScaler Gateway versión 13.0 compilación 64.x y posteriores.
- La comprobación NAC de Intune, para la VPN por aplicación o incluso la VPN para todo el dispositivo, solo es compatible cuando el perfil VPN es aprovisionado por el portal de administración de Intune (ahora conocido como Microsoft Endpoint Manager). Estas funciones no son compatibles con los perfiles VPN añadidos por el usuario final. El dispositivo del usuario final debe tener el perfil VPN implementado en su dispositivo desde Microsoft Endpoint Manager por su administrador de Intune para usar la comprobación NAC.

## Licencias

Se requiere una licencia de Citrix® Enterprise Edition para esta funcionalidad.

## Requisitos del sistema

- NetScaler Gateway versión 11.1 compilación 51.21 o posterior
- VPN de iOS – 10.6 o posterior
- VPN de Android – 2.0.13 o posterior
- Microsoft
  - Acceso a Microsoft Entra ID (con privilegios de inquilino y administrador)
  - Inquilino con Intune habilitado
- Firewall

  Habilite las reglas del firewall para todo el tráfico DNS y SSL desde la dirección IP de la subred a `https://login.microsoftonline.com` y `https://graph.windows.net` (puerto 53 y puerto 443)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

## Requisitos previos

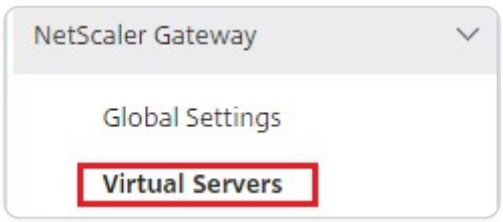
- Todas las directivas de autenticación existentes deben convertirse de directivas clásicas a directivas avanzadas. Para obtener información sobre cómo convertir de directivas clásicas a directivas avanzadas, consulte `<https://support.citrix.com/article/CTX131024>`.
- Cree una aplicación NetScaler Gateway en el portal de Azure. Para obtener más información, consulte Configuración de una aplicación NetScaler Gateway en el portal de Azure.
- Configure la directiva OAuth en la aplicación NetScaler Gateway que creó utilizando la siguiente información específica de la aplicación.
  - ID de cliente / ID de aplicación
  - Secreto de cliente / Clave de aplicación
  - ID de inquilino de Microsoft Entra

## Referencias

- Este documento describe la configuración de NetScaler Gateway. La mayor parte de la configuración del cliente Citrix SSO (iOS/Android) se realiza en el lado de Intune. Para obtener más información sobre la configuración de VPN de Intune para NAC, consulte `<https://docs.microsoft.com/es-es/mem/intune/protect/network-access-control-integrate>`.
- Para configurar el perfil VPN para una aplicación iOS, consulte `<https://docs.microsoft.com/es-es/mem/intune/configuration/vpn-settings-ios>`.
- Para configurar la aplicación NetScaler Gateway en el portal de Azure, consulte Configuración de una aplicación NetScaler Gateway en el portal de Azure.

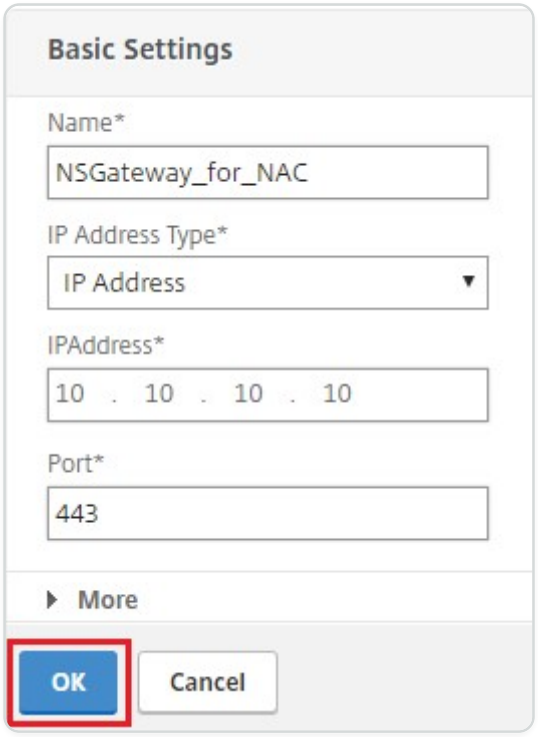
## Para agregar un servidor virtual NetScaler Gateway con nFactor para la implementación de la puerta de enlace

1. Vaya a **NetScaler Gateway > Servidores virtuales**.




2. Haga clic en **Agregar**.
3. Proporcione la información requerida en el área de **Configuración básica** y haga clic en **Aceptar**.

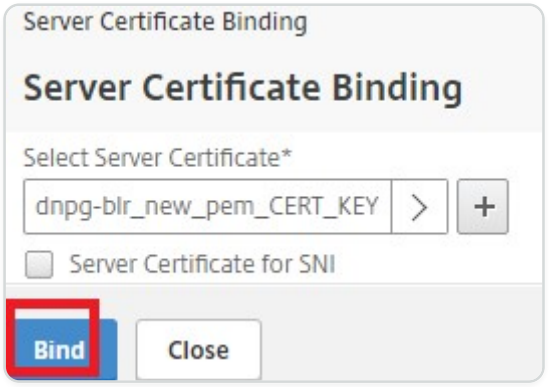
© 1997–2026 Citrix Systems, Inc. All rights reserved.




4. Seleccione **Certificado de servidor**.



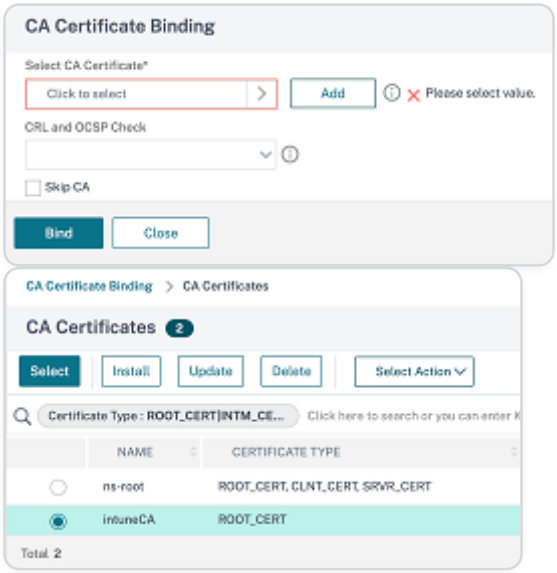

5. Seleccione el certificado de servidor requerido y haga clic en **Enlazar**.




6. Como parte de la compatibilidad con la API v2 de Intune NAC, debe enlazar un archivo de entidad de certificación (certificado de CA) para asegurarse de que el dispositivo NetScaler obtenga un certificado válido de los dispositivos móviles. En Intune NAC v2, los dispositivos móviles envían ID de dispositivo como parte del certificado de cliente. El certificado de CA enlazado aquí debe ser el que se utilizó para emitir certificados de cliente a los dispositivos iOS y Android del usuario final. Si hay certificados intermedios, también deben enlazarse aquí. Para obtener más información sobre la configuración de Intune, consulte Configuración de una

© 1997–2026 Citrix Systems, Inc. All rights reserved.

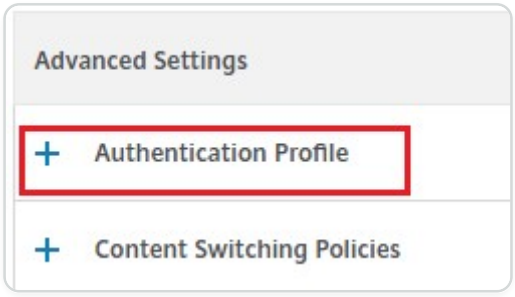
aplicación NetScaler Gateway en el portal de Azure. Para la compatibilidad con la API v2 de Intune NAC, seleccione el certificado de CA requerido y haga clic en **Enlazar**.



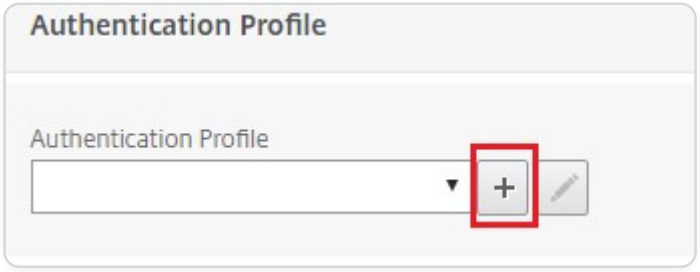

7. Haga clic en **Continuar**.
8. Haga clic en **Continuar**.
9. Haga clic en **Continuar**.
10. Haga clic en el icono de más junto a **Directivas** y seleccione **Sesión** de la lista **Elegir directiva** y seleccione **Solicitud** de la lista **Elegir tipo** y haga clic en **Continuar**.
11. Haga clic en el icono de más junto a **Seleccionar directiva**.
12. En la página **Crear directiva de sesión de NetScaler Gateway**, proporcione un nombre para la directiva de sesión.
13. Haga clic en el icono de más junto a **Perfil** y, en la página **Crear perfil de sesión de NetScaler Gateway**, proporcione un nombre para el perfil de sesión.
14. En la ficha **Experiencia del cliente**, haga clic en la casilla de verificación junto a **Acceso sin cliente** y seleccione **Desactivado** de la lista.
15. Haga clic en la casilla de verificación junto a **Tipo de complemento** y seleccione Windows/Mac OS X de la lista.
16. Haga clic en **Configuración avanzada** y seleccione la casilla de verificación junto a **Opciones de cliente** y establezca su valor en **ACTIVADO**.
17. En la ficha **Seguridad**, haga clic en la casilla de verificación junto a **Acción de autorización predeterminada** y seleccione **Permitir** de la lista.
18. En la ficha **Aplicaciones publicadas**, haga clic en la casilla de verificación junto a **Proxy ICA®** y seleccione **DESACTIVADO** de la lista.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

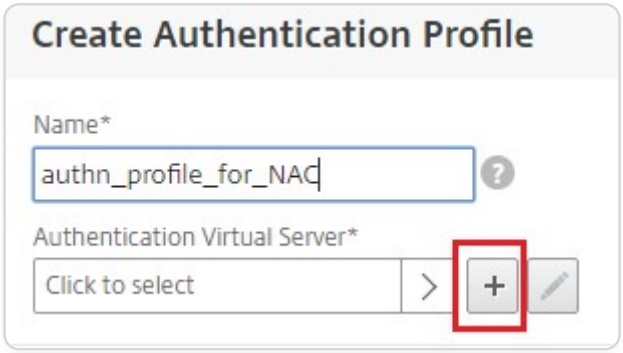
19. Haga clic en **Crear.**
20. En la página **Crear directiva de sesión de NetScaler Gateway**, en el área **Expresión**, configure la expresión de calificación.
21. Haga clic en **Crear**.
22. Haga clic en **Enlazar**.
23. Seleccione **Perfil de autenticación** en **Configuración avanzada**.




24. Haga clic en el icono más y proporcione un nombre para el perfil de autenticación.

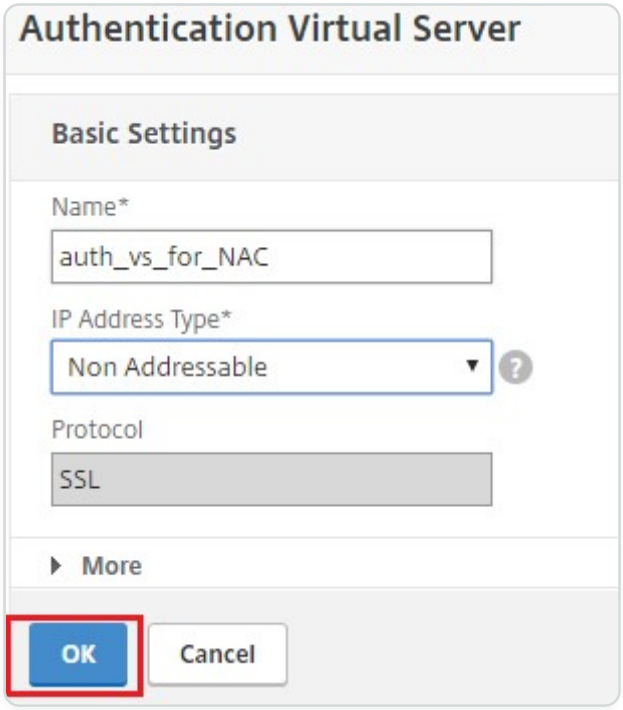



25. Haga clic en el icono más para crear un servidor virtual de autenticación.

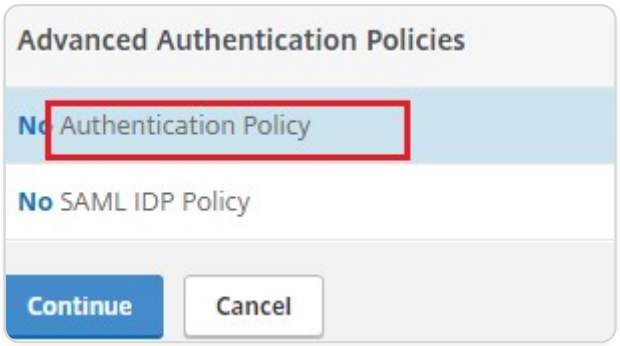



26. Especifique el nombre y el tipo de dirección IP para el servidor virtual de autenticación en el área **Configuración básica** y haga clic en **Aceptar**. El tipo de dirección IP también puede ser **No direccionable**.

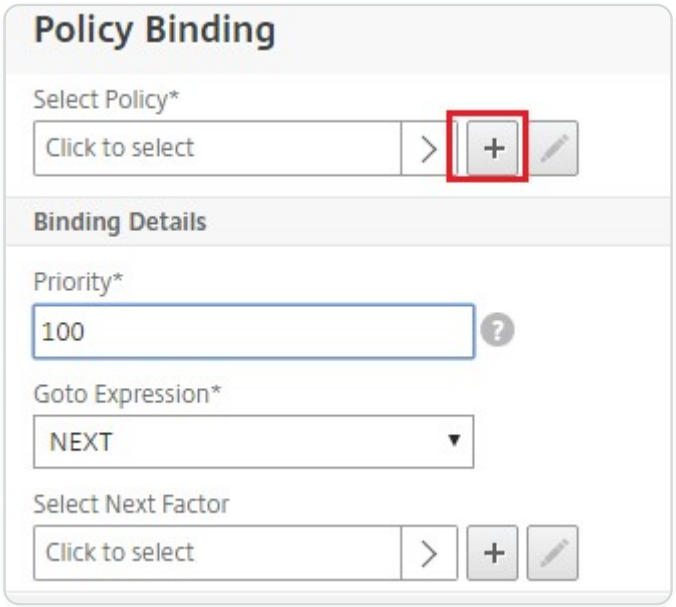
© 1997–2026 Citrix Systems, Inc. All rights reserved.




27. Haga clic en **Directiva de autenticación**.

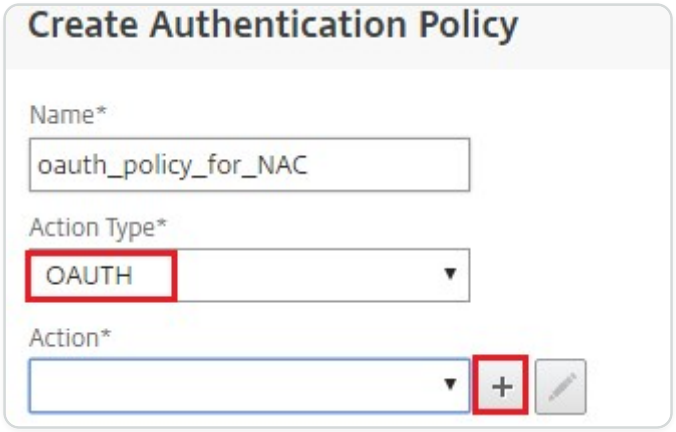



28. En la vista Enlace de directivas, haga clic en el icono más para crear una directiva de autenticación.




© 1997–2026 Citrix Systems, Inc. All rights reserved.

29. Seleccione **OAUTH** como **Tipo de acción** y haga clic en el icono más para crear una acción OAuth para NAC.




30. Cree una acción OAuth utilizando el **ID de cliente**, el **Secreto de cliente** y el **ID de inquilino**.

**NOTA:**

- **ID de cliente**, **Secreto de cliente** e **ID de inquilino** se generan después de configurar la aplicación NetScaler Gateway en el portal de Azure.
- Anote la información del ID de cliente/ID de aplicación, el Secreto de cliente/Secreto de aplicación y el ID de inquilino de Microsoft Entra, ya que son necesarios al crear una acción OAuth en NetScaler Gateway más adelante.

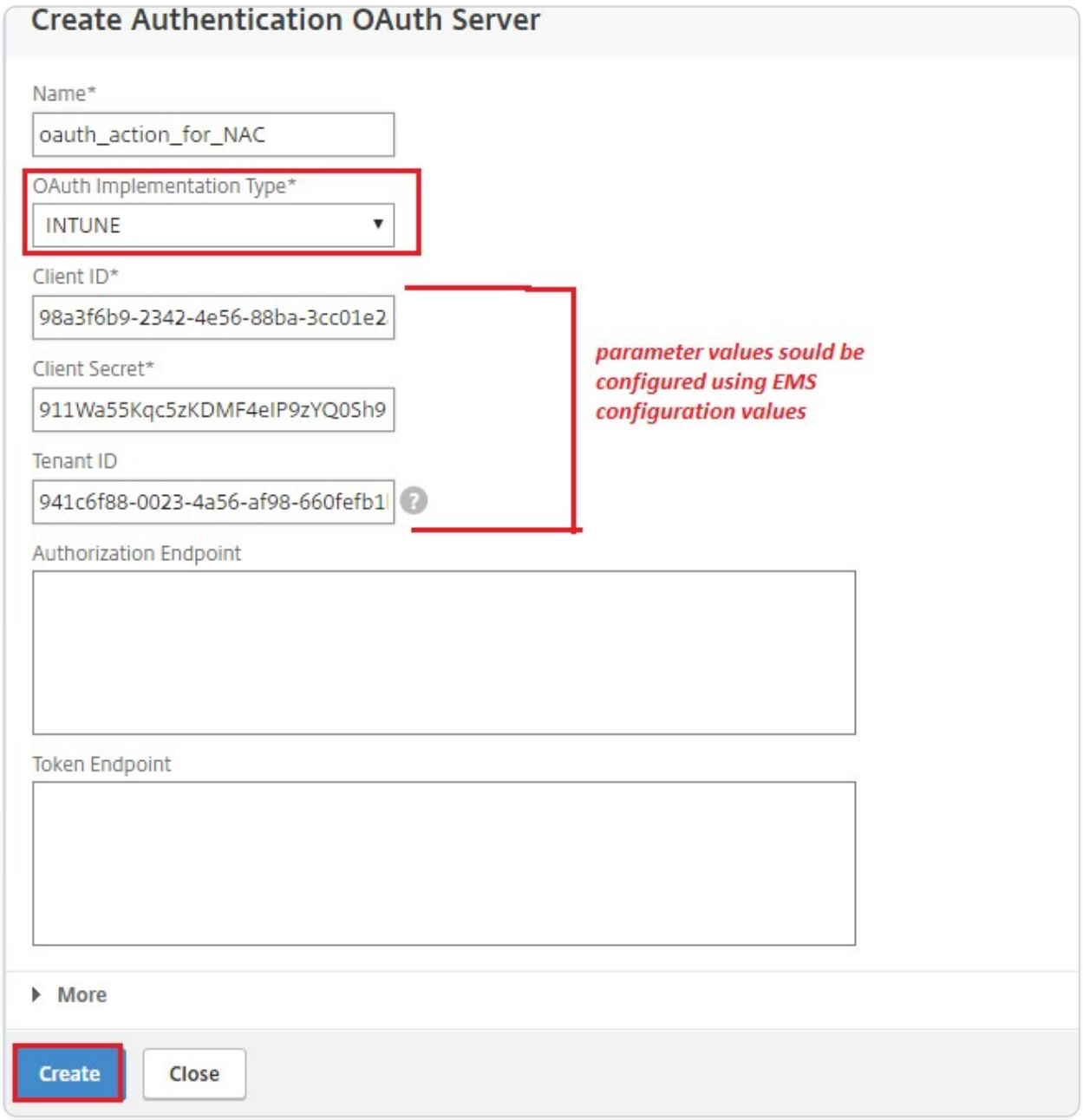
Asegúrese de tener un servidor de nombres DNS apropiado configurado en su dispositivo para resolver y alcanzar;

```
-  `https://login.microsoftonline.com/,`


-  `https://graph.windows.net/`,


-  *.manage.microsoft.com.
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

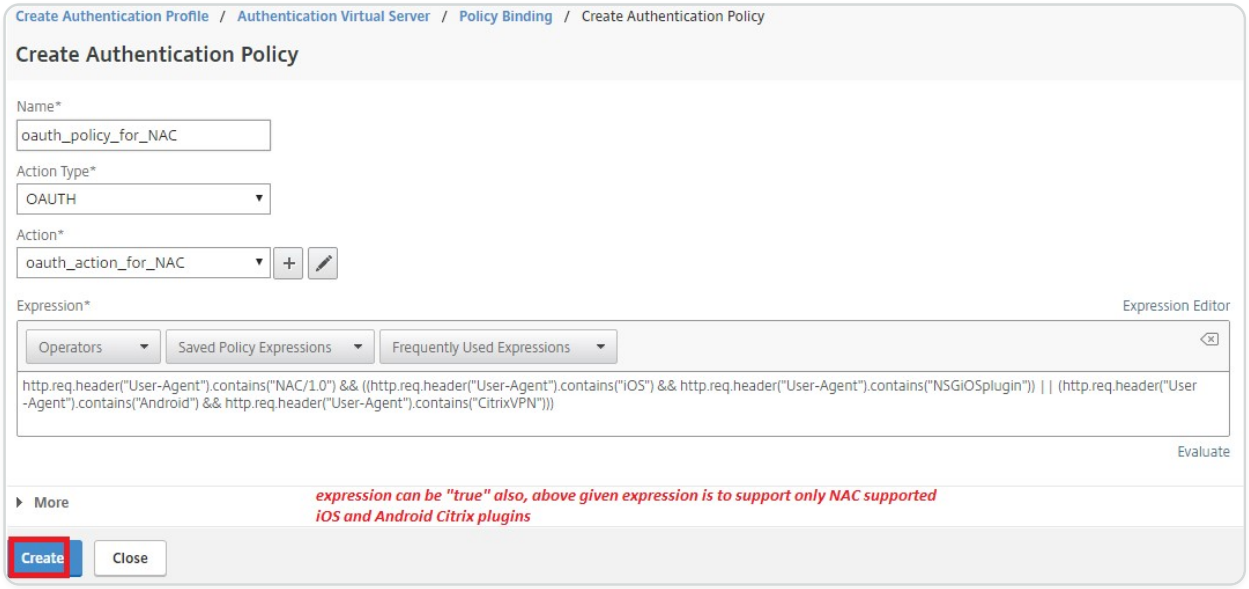



31. Cree una directiva de autenticación para la **Acción OAuth**.

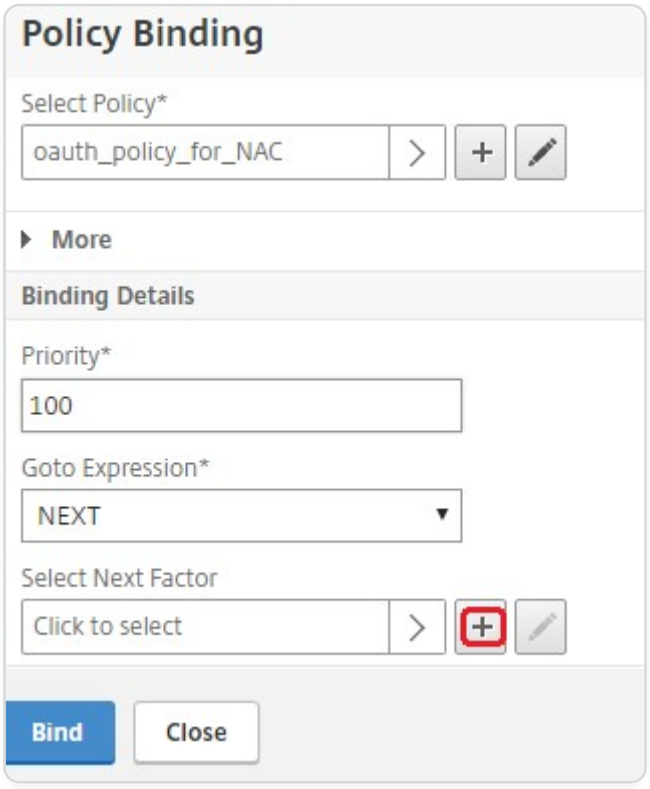
**Regla:**

```
http.req.header("User-Agent").contains("NAC/1.0")&&
((http.req.header("User-Agent").contains("iOS") &&
http.req.header("User-Agent").contains("NSGiOSplugin")) ||
(http.req.header("User-Agent").contains("Android") &&
http.req.header("User-Agent").contains("CitrixVPN")))
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

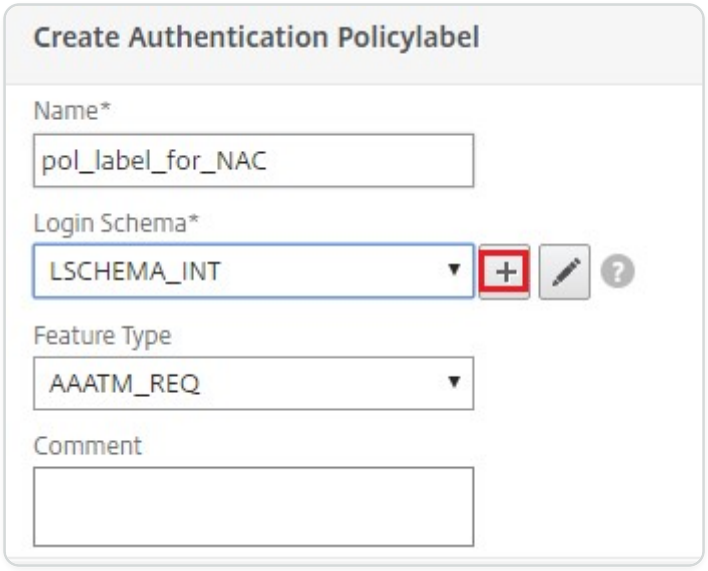



32. Haga clic en el icono más para crear una etiqueta de directiva nextFactor.

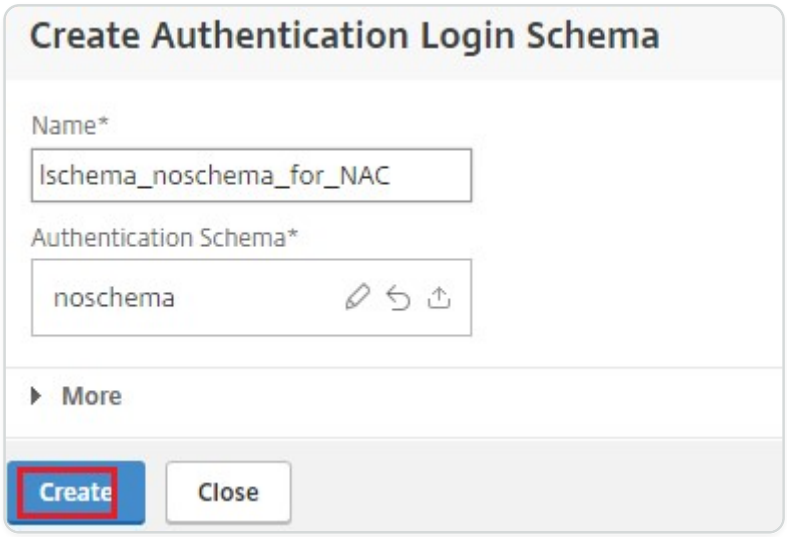



33. Haga clic en el icono más para crear un esquema de inicio de sesión.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

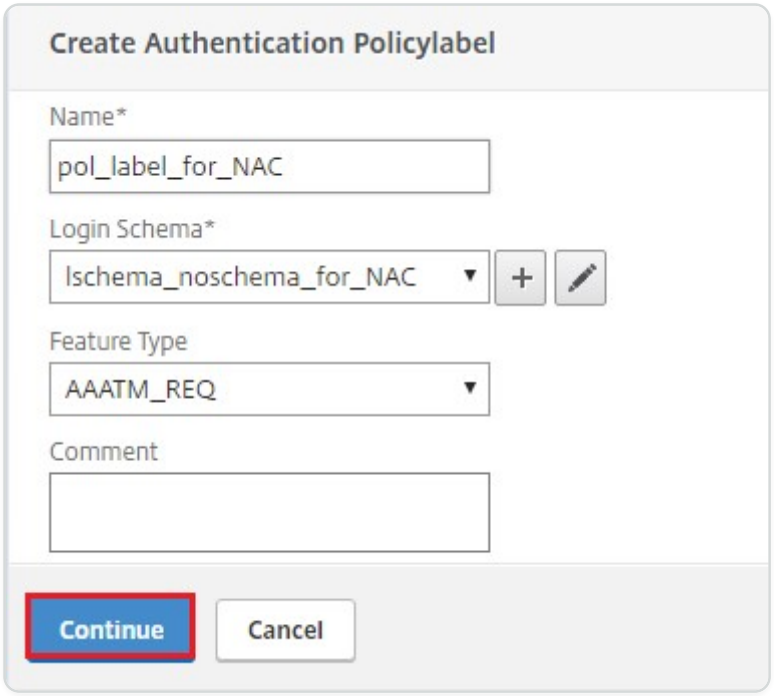



34. Seleccione **noschema** como esquema de autenticación y haga clic en **Crear**.



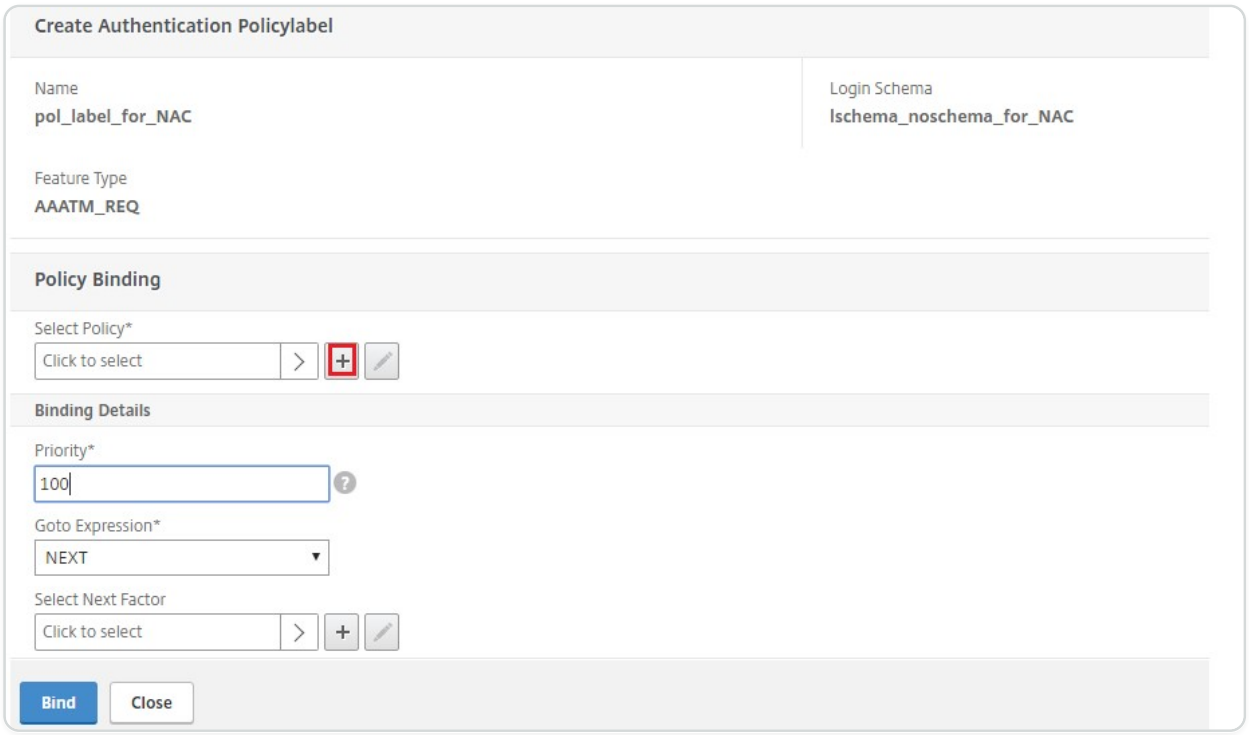

35. Después de seleccionar el esquema de inicio de sesión creado, haga clic en **Continuar**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



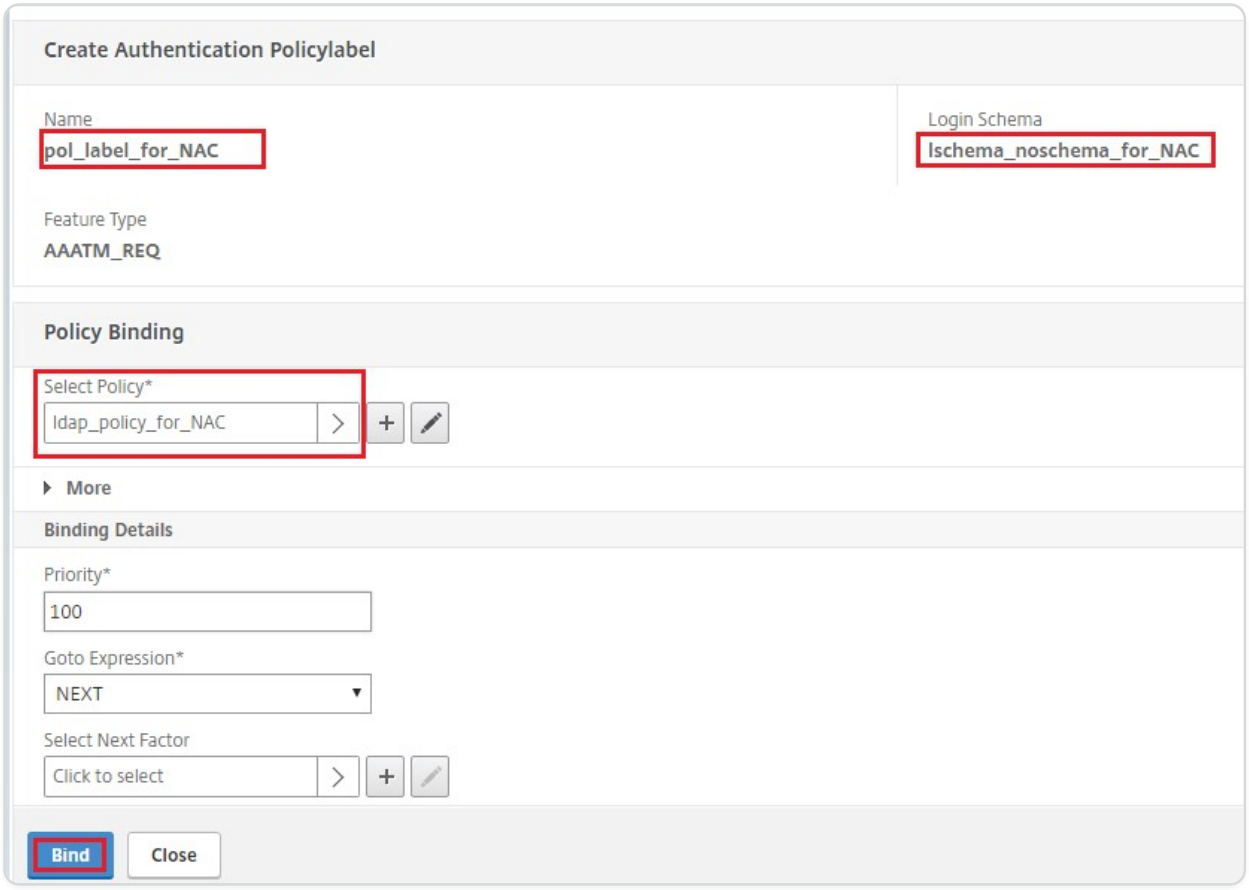

36. En **Seleccionar directiva**, seleccione una directiva de autenticación existente para el inicio de sesión del usuario o haga clic en el icono más **+** para crear una directiva de autenticación.

    Para obtener más información sobre cómo crear una directiva de autenticación, consulte Configuración de directivas de autenticación avanzadas y Configuración de la autenticación LDAP.

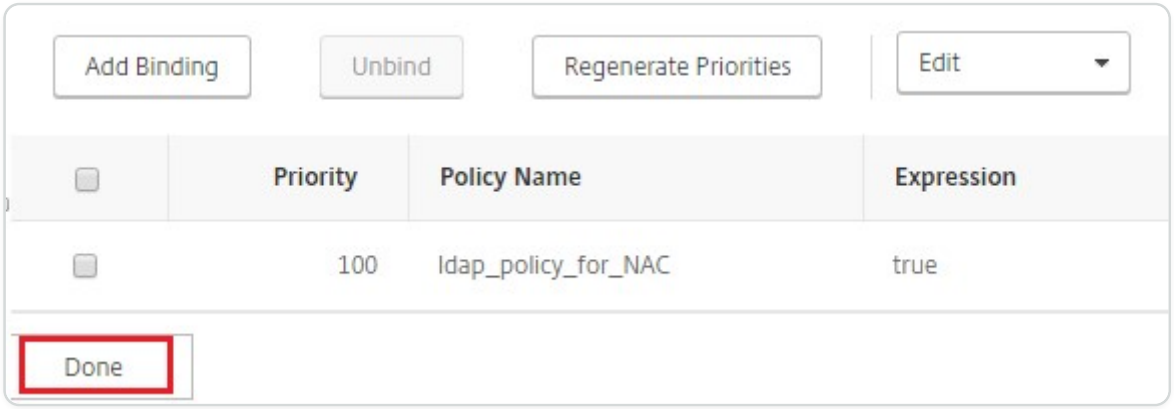



37. Haga clic en **Enlazar**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

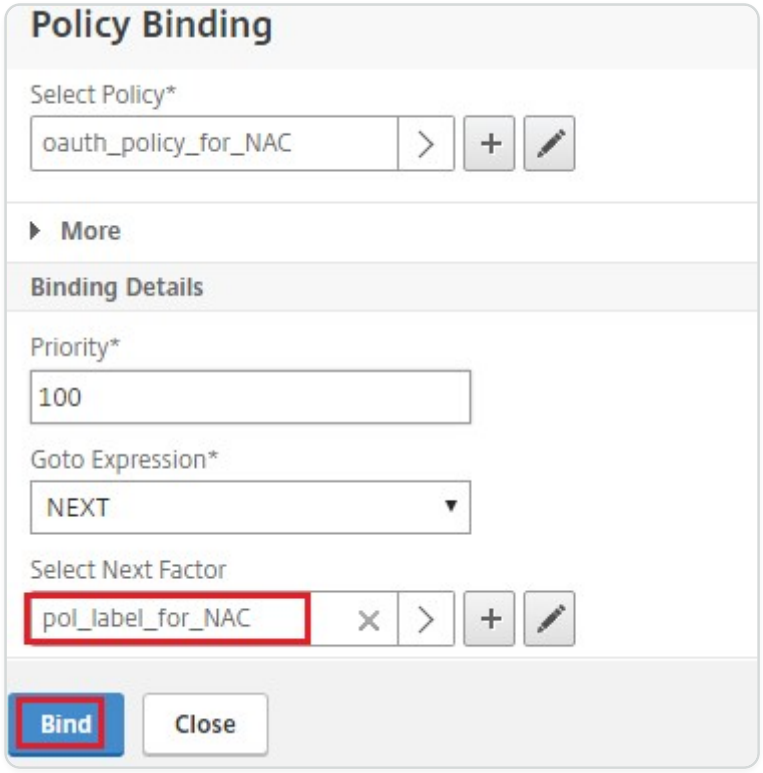



38. Haga clic en **Listo**.

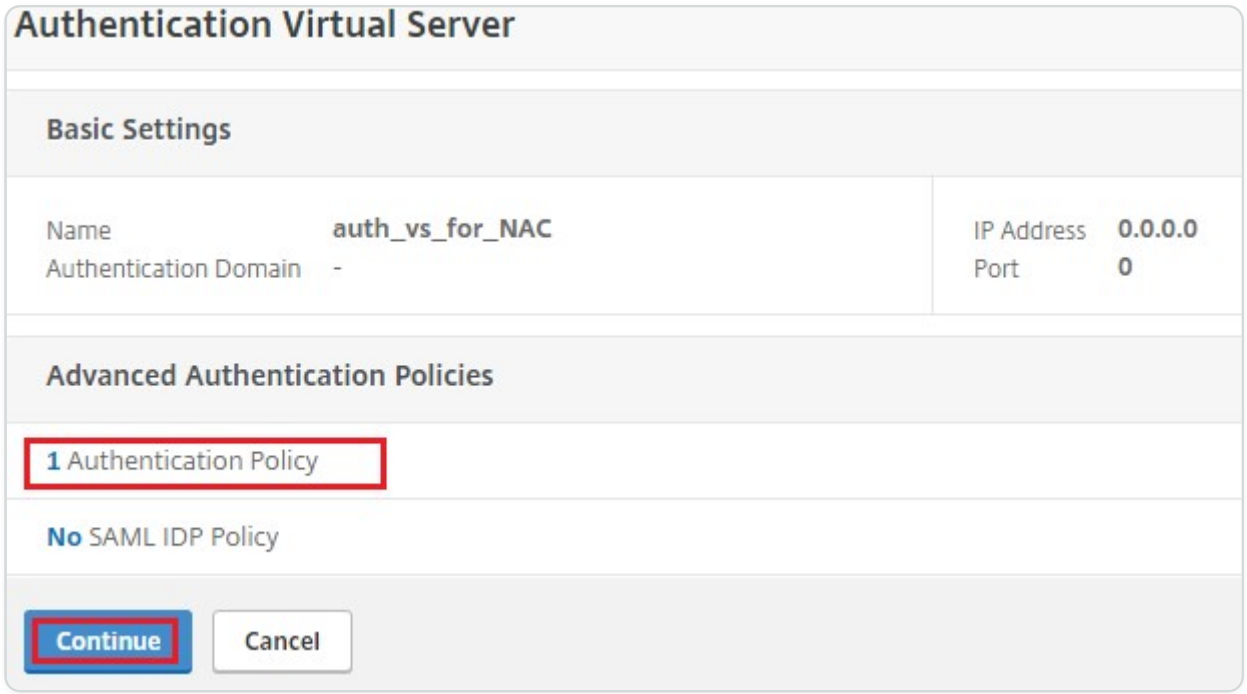



39. Haga clic en **Enlazar**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

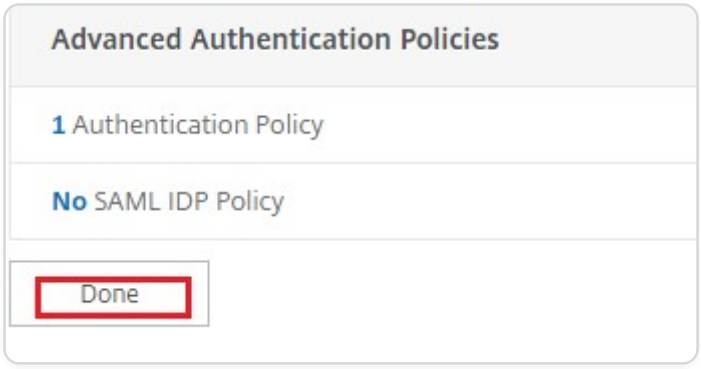



40. Haga clic en **Continuar**.

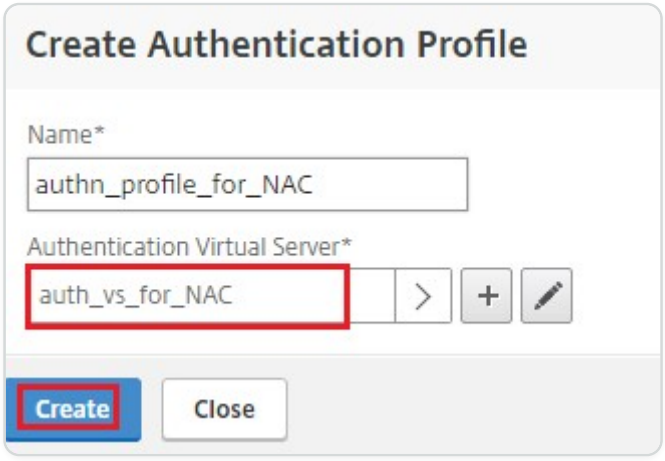



41. Haga clic en **Listo**.

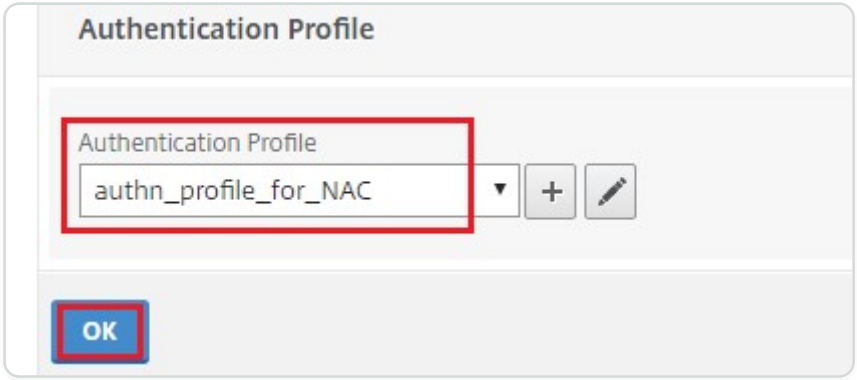
© 1997–2026 Citrix Systems, Inc. All rights reserved.



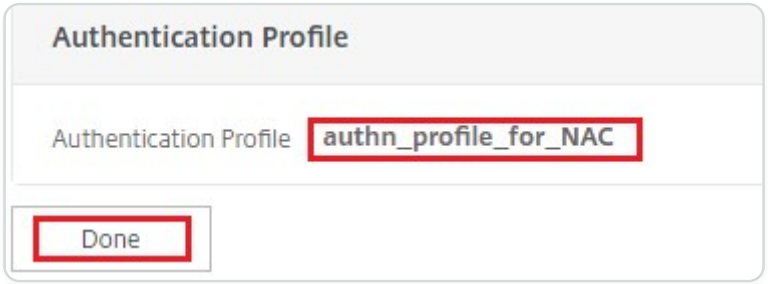

42. Haga clic en **Crear**.




43. Haga clic en **OK**.




44. Haga clic en **Done**.



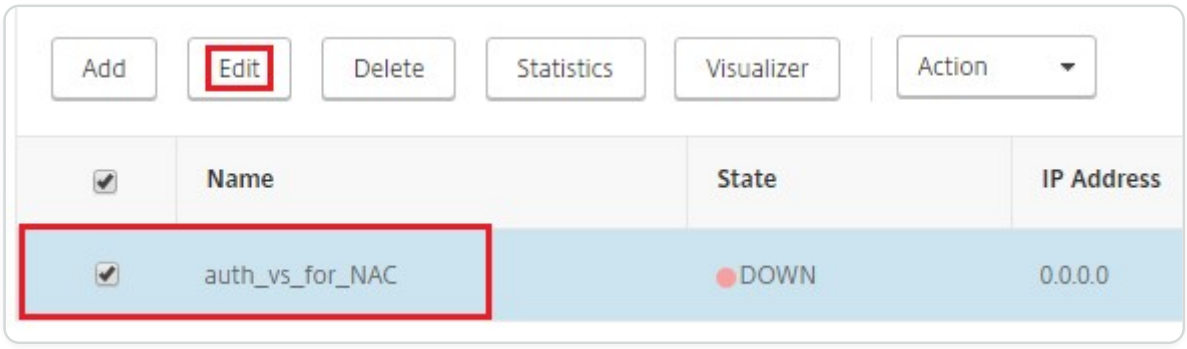

© 1997–2026 Citrix Systems, Inc. All rights reserved.

## Para vincular el esquema de inicio de sesión de autenticación al servidor virtual de autenticación para indicar a los complementos VPN que envíen el ID del dispositivo como parte de la solicitud /cgi/login

1. Vaya a **Seguridad** > **AAA - Tráfico de aplicaciones** > **Servidores virtuales**.




2. Seleccione el servidor virtual seleccionado anteriormente y haga clic en **Editar**.




3. Haga clic en **Esquemas de inicio de sesión** en **Configuración avanzada**.

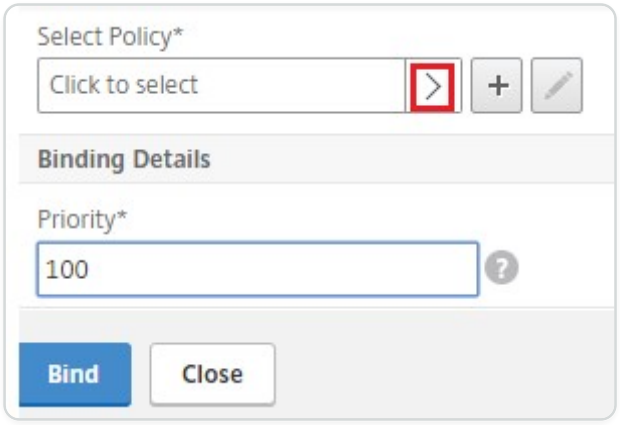



4. Haga clic en **Esquemas de inicio de sesión** para vincular.



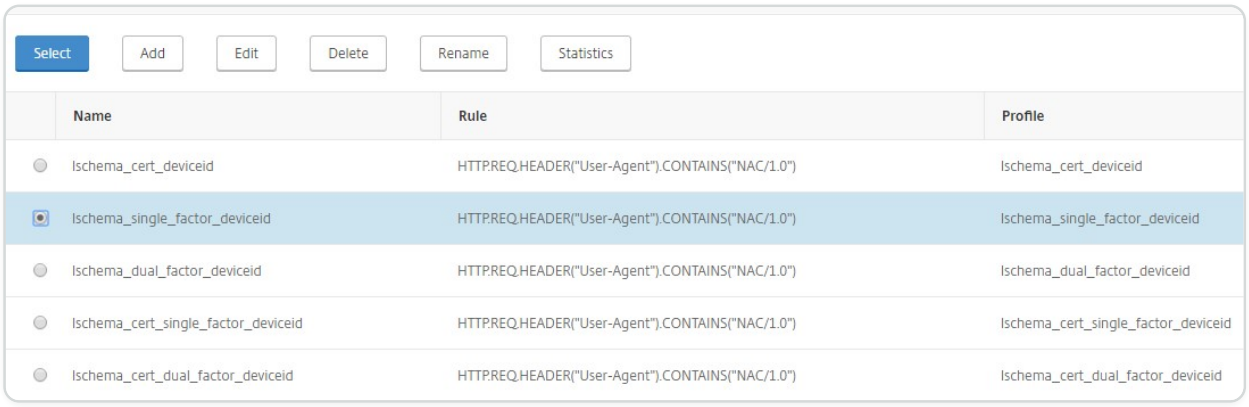

5. Haga clic en para seleccionar y vincular las políticas de esquema de inicio de sesión integradas existentes para la comprobación de dispositivos NAC.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

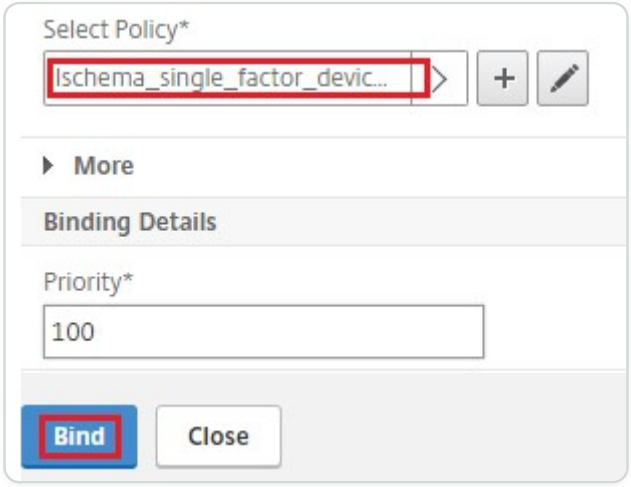



6. Seleccione la política de esquema de inicio de sesión requerida y adecuada para su implementación de autenticación y haga clic en **Seleccionar**.

   En la implementación explicada anteriormente, se utiliza la autenticación de factor único (LDAP) junto con una política de acción OAuth de NAC. Por lo tanto, se selecciona **lschema_single_factor_deviceid**.

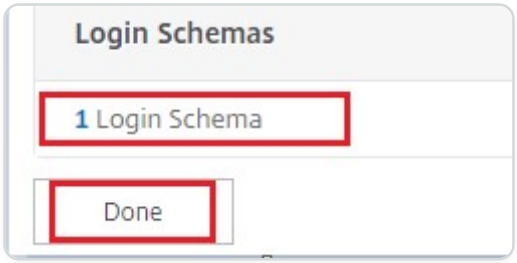



7. Haga clic en **Vincular**.




8. Haga clic en **Listo**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.




## Compatibilidad con la API v2 de Intune NAC

Como parte de la compatibilidad con la API v2 de Intune NAC, debe vincular un archivo de entidad de certificación (certificado CA) para asegurarse de que el dispositivo NetScaler obtenga un certificado válido de los dispositivos móviles. En Intune NAC v2, los dispositivos móviles envían ID de dispositivo como parte del certificado CA. El certificado CA vinculado aquí debe ser el que se utilizó para emitir certificados de cliente a los dispositivos iOS y Android del usuario final. Si hay certificados intermedios, también deben vincularse aquí.

Puede utilizar el siguiente comando de ejemplo para vincular su certificado CA.

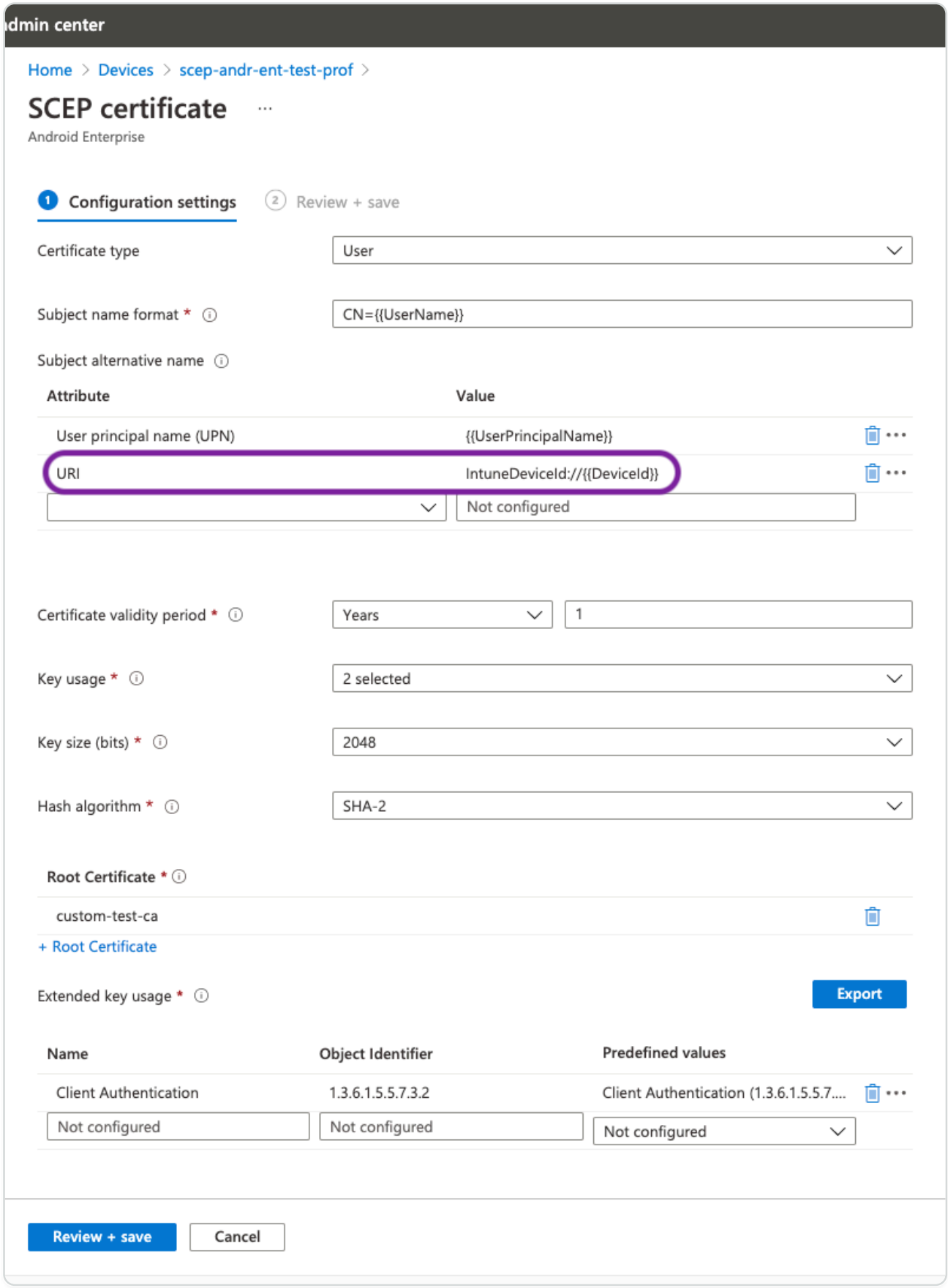
```
bind ssl vserver intune_nac_check_443 -certkeyName clientca -CA -ocspCheck
Optional
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**IMPORTANTE:**

- La compatibilidad con la API v2 de Intune NAC está disponible en las versiones de NetScaler Gateway 13.1 compilación 12.50 o posterior y 13.0 compilación 84.11 o posterior.
- Debe habilitar la autenticación basada en certificados de cliente configurando `clientAuth` en ENABLED y `clientCert` en OPTIONAL en los servidores virtuales VPN y de autenticación. El parámetro `clientCert` se establece en OPTIONAL para que otros puntos finales que no necesiten la comprobación de Intune NAC puedan autenticarse a través del mismo servidor virtual sin proporcionar el certificado de cliente. Los dispositivos Android e iOS deben proporcionar el certificado de cliente. De lo contrario, la comprobación de Intune NAC fallará.
- Debe asegurarse de que los certificados de cliente aprovisionados a través de Intune en el dispositivo móvil deben tener el ID de dispositivo de Intune en el campo SAN de tipo URI, como se indica en el documento del nuevo servicio Microsoft Intune para el control de acceso a la red. Para obtener más detalles, consulte `<https://techcommunity.microsoft.com/t5/intune-customer-success/new-microsoft-intune-service-for-network-access-control/ba-p/2544696>`. El formato del campo de valor URI debe ser el mismo que se indica en la siguiente figura. Además, la aplicación Citrix SSO debe usar el mismo certificado para autenticarse con la puerta de enlace.

© 1997–2026 Citrix Systems, Inc. All rights reserved.




© 1997–2026 Citrix Systems, Inc. All rights reserved.

# Solución de problemas

## Problemas generales

| PROBLEMA | RESOLUCIÓN |
| --- | --- |
| Aparece el mensaje "Se requiere agregar directiva" al abrir una aplicación | Agregue directivas en la API de Microsoft Graph |
| Hay conflictos de directivas | Solo se permite una directiva por aplicación |
| Su aplicación no puede conectarse a recursos internos | Asegúrese de que los puertos de firewall correctos estén abiertos, de que se haya utilizado el ID de inquilino correcto, etc. |

## Problemas de NetScaler Gateway

| PROBLEMA | RESOLUCIÓN |
| --- | --- |
| | |
| NetScaler Gateway no puede acceder a `login.microsoftonline.comandgraph.windows.net`. | Desde NS Shell, compruebe si puede acceder al siguiente sitio web de Microsoft: cURL -v -k `<https://login.microsoftonline.com>`. Luego, compruebe si DNS está configurado en NetScaler Gateway. Compruebe también que la configuración del firewall sea correcta (en caso de que las solicitudes DNS estén bloqueadas por el firewall). |
| Aparece un error en ns.log después de configurar OAuthAction. | Compruebe si las licencias de Intune están habilitadas y si la aplicación Azure Gateway tiene los permisos adecuados configurados. |
| El comando `Sh OAuthAction` no muestra el estado de OAuth como completo. | Compruebe la configuración de DNS y los permisos configurados en la aplicación Azure Gateway. |
| El dispositivo Android o iOS no muestra la solicitud de autenticación dual. | Compruebe si el logonSchema de ID de dispositivo de doble factor está vinculado al servidor virtual de autenticación. |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

### Estado de OAuth de NetScaler Gateway y condición de error

| ESTADO | CONDICIÓN DE ERROR |
|---|---|
| AADFORGRAPH | Secreto no válido, URL no resuelta, tiempo de espera de conexión agotado |
| MDMINFO | `*manage.microsoft.com` está caído o inalcanzable |
| GRAPH | El punto final de Graph está caído o inalcanzable |
| CERTFETCH | No se puede comunicar con "Token Endpoint: `<https://login.microsoftonline.com>` debido a un error de DNS. Para validar esta configuración, vaya al símbolo del sistema de Shell y escriba cURL `<https://login.microsoftonline.com>`. Este comando debe ser válido. |

**Nota:** Cuando el estado de OAuth es correcto, el estado se muestra como COMPLETE.

### Comprobación de la configuración de Intune

Asegúrese de seleccionar la casilla de verificación **Acepto** en **Configuración de VPN base de iOS para Citrix SSO > Habilitar control de acceso a la red (NAC)**. De lo contrario, la comprobación de NAC no funciona.

# Configuración de una aplicación NetScaler Gateway en el portal de Azure

La siguiente sección enumera los pasos para configurar una aplicación NetScaler Gateway en el portal de Azure.

## Requisitos previos

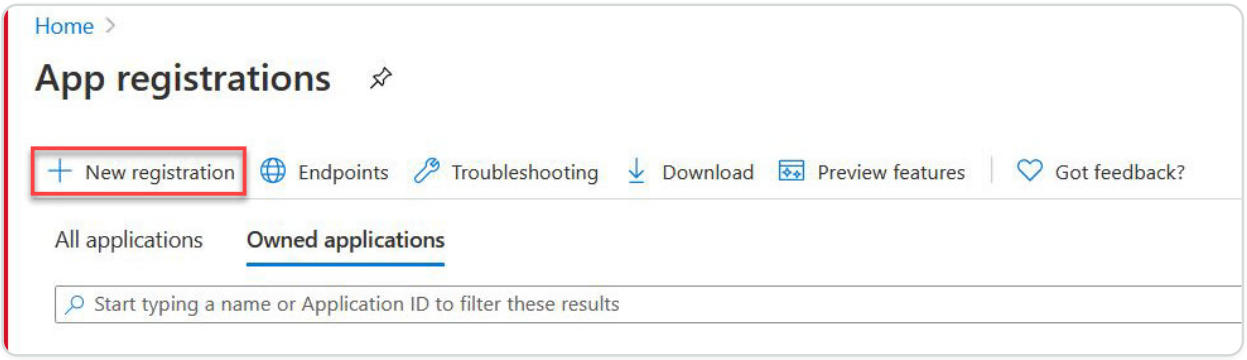
- Credenciales de administrador global de Azure
- Licencia de Intune habilitada
- Para la integración de Intune, debe crear una aplicación NetScaler Gateway en el portal de Azure.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Una vez creada la aplicación NetScaler Gateway, configure la directiva OAuth en NetScaler Gateway utilizando la siguiente información específica de la aplicación:
  - ID de cliente / ID de aplicación
  - Secreto de cliente / Clave de aplicación
  - ID de inquilino de Microsoft Entra
- NetScaler Gateway utiliza el ID de cliente de la aplicación y el secreto de cliente para comunicarse con Azure y comprobar el cumplimiento de NAC.

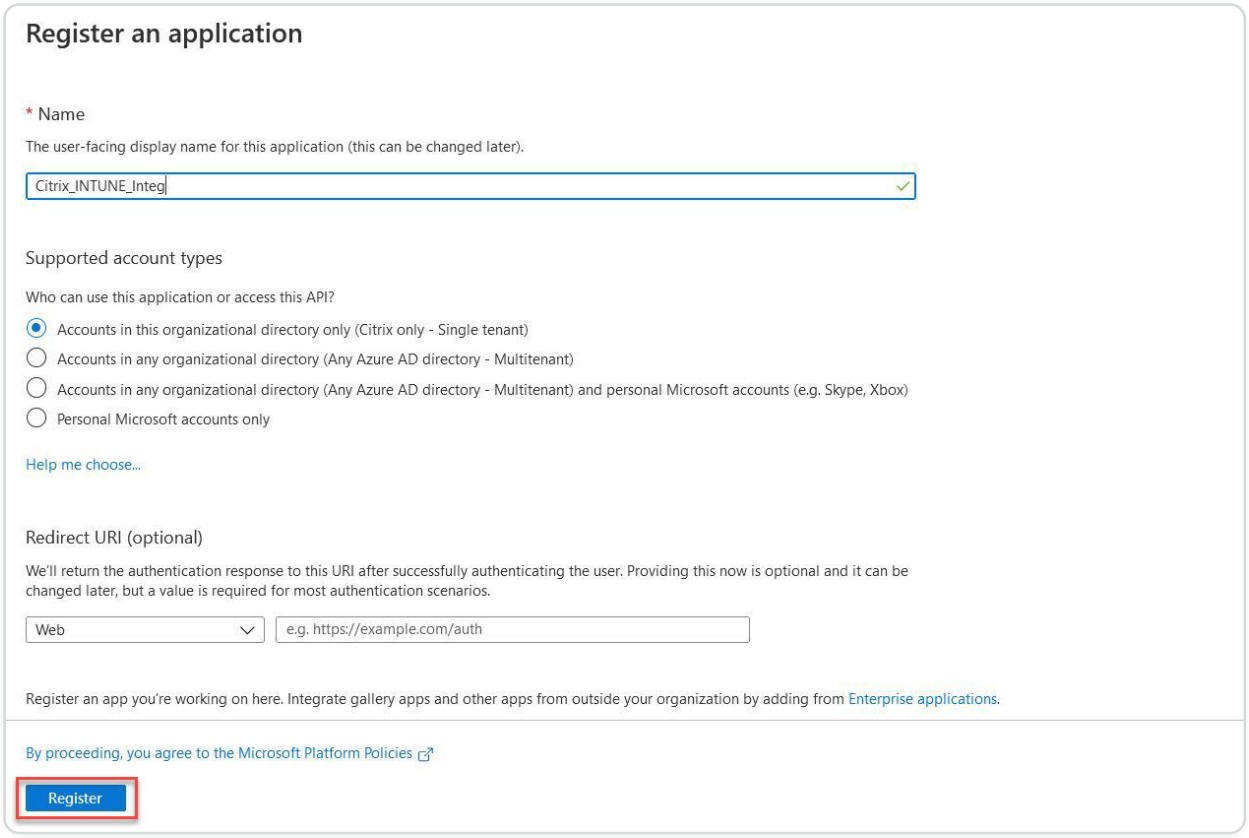
## Para crear una aplicación NetScaler Gateway en Azure

1. Inicie sesión en portal.azure.com
2. Haga clic en **Microsoft Entra ID**.
3. Haga clic en **Registros de aplicaciones** y, a continuación, en **Nuevo registro**.

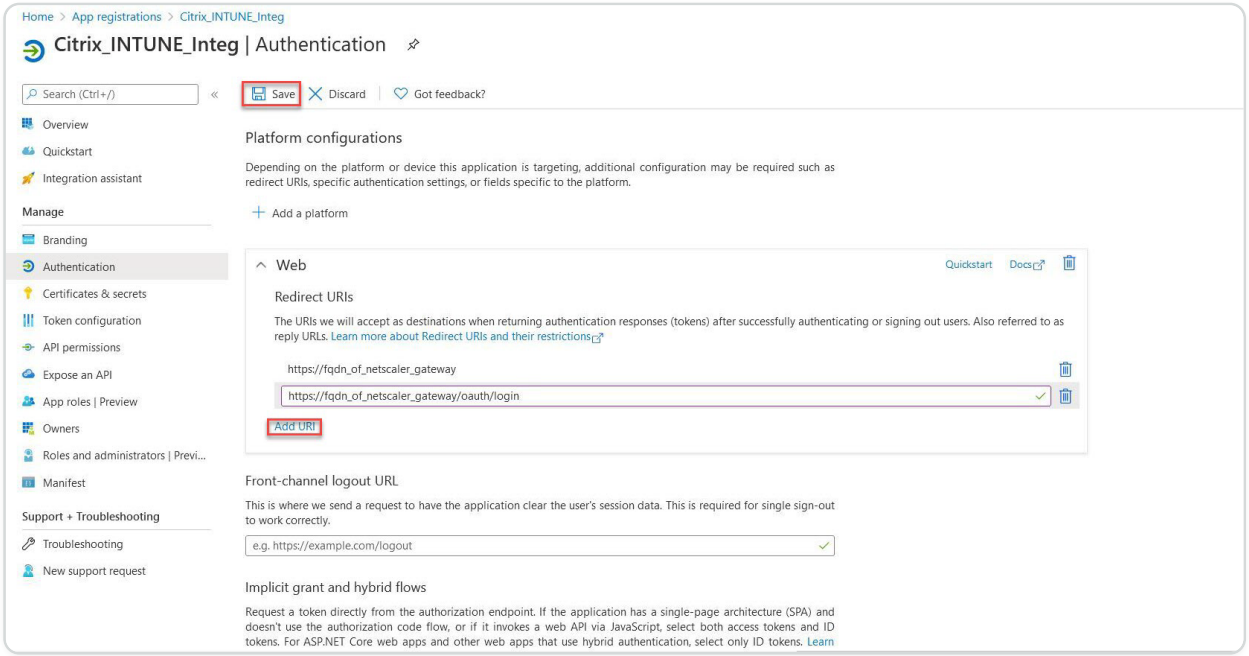



4. En la página **Registrar una aplicación**, introduzca un nombre de aplicación y haga clic en **Registrar**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

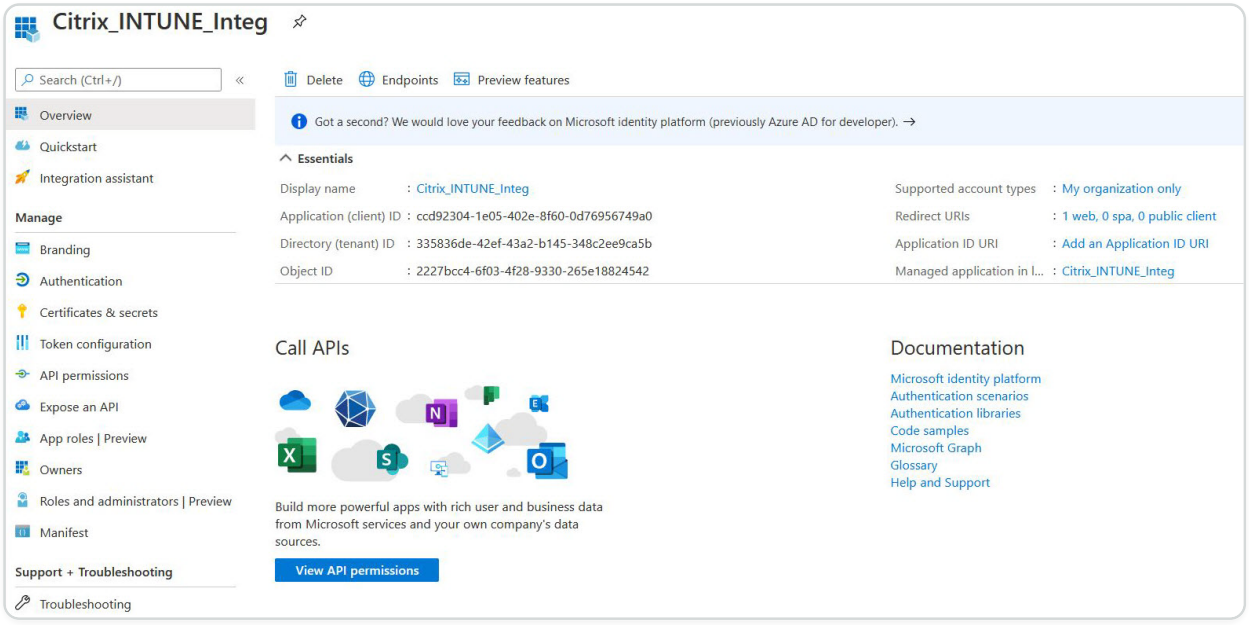



5. Vaya a **Autenticación**, haga clic en **Agregar URI**, introduzca el FDQN para NetScaler Gateway y haga clic en **Guardar**.

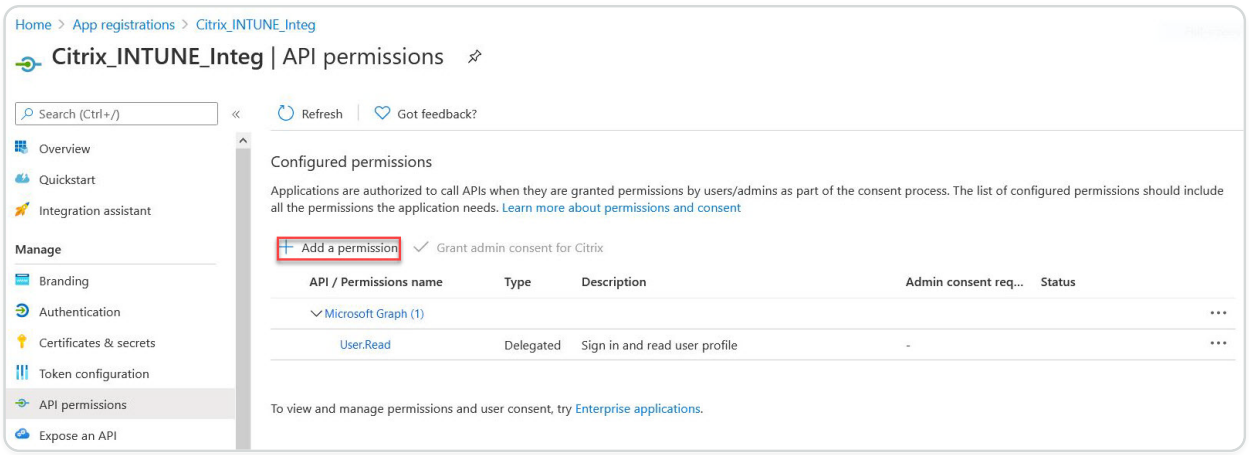



6. Vaya a la página **Información general** para obtener el ID de cliente, el ID de inquilino y el ID de objeto.

© 1997–2026 Citrix Systems, Inc. All rights reserved.




7. Vaya a **Permisos de API** y haga clic en **Agregar un permiso**.




**NOTA:**

Todas las aplicaciones de Microsoft Entra ID que llaman a los puntos de conexión de servicio `https://login.microsoftonline.com`, `https://graph.microsoft.com` o `https://graph.windows.net` requieren que se asigne el permiso de API para que el gateway pueda llamar a la API de NAC. Los permisos de API disponibles son:

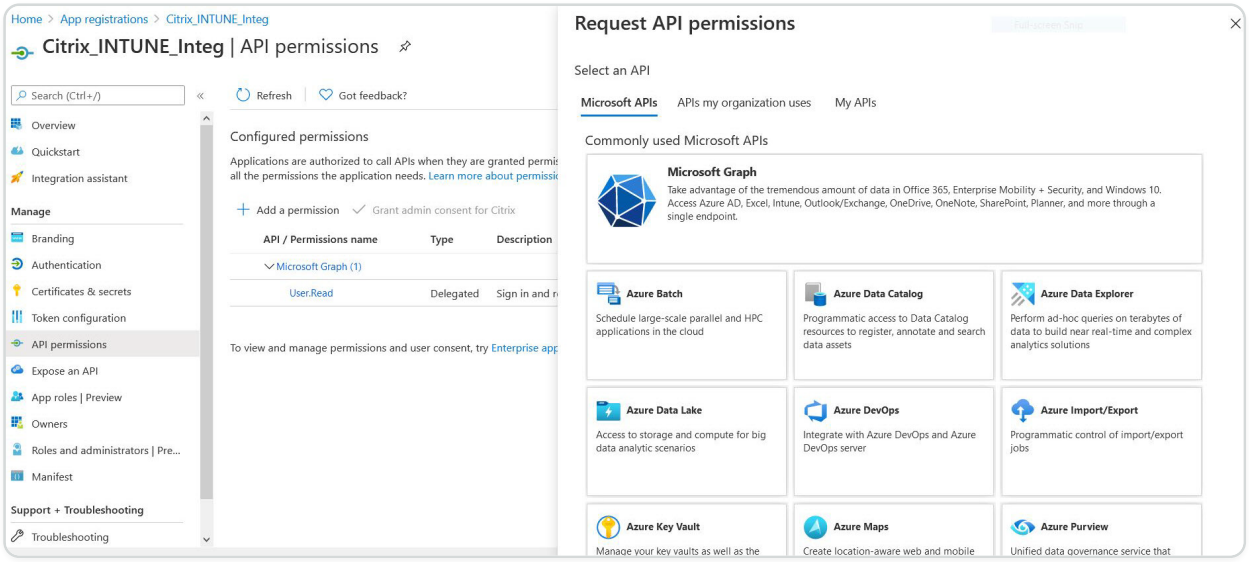
- Application.Read.All
- Application.ReadWrite.All
- Application.OwnedBy
- Directory.Read.All

El permiso preferido es **Application.Read.All**.

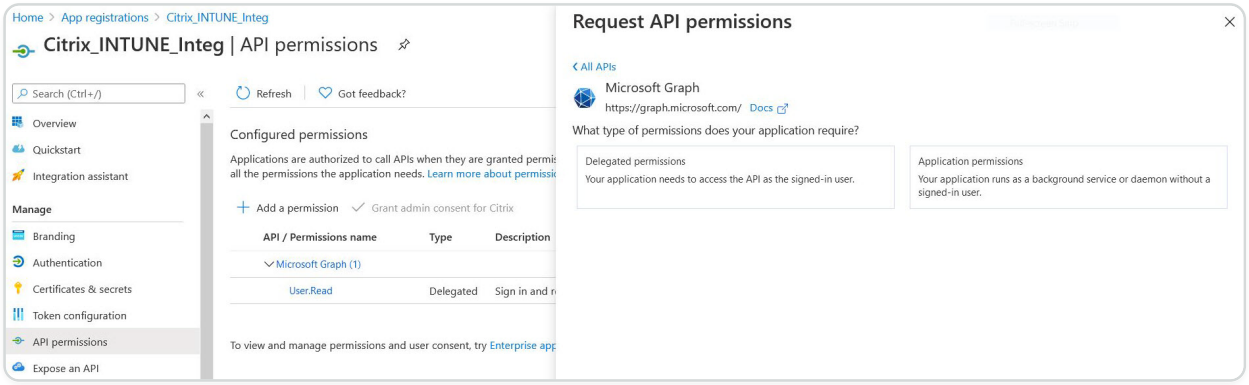
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Para obtener más detalles, consulte `<https://techcommunity.microsoft.com/t5/intune-customer-success/support-tip-intune-service-discovery-api-endpoint-will-require/ba-p/2428040>`

8. Haga clic en el mosaico **Microsoft Graph** para configurar los permisos de API para Microsoft Graph.



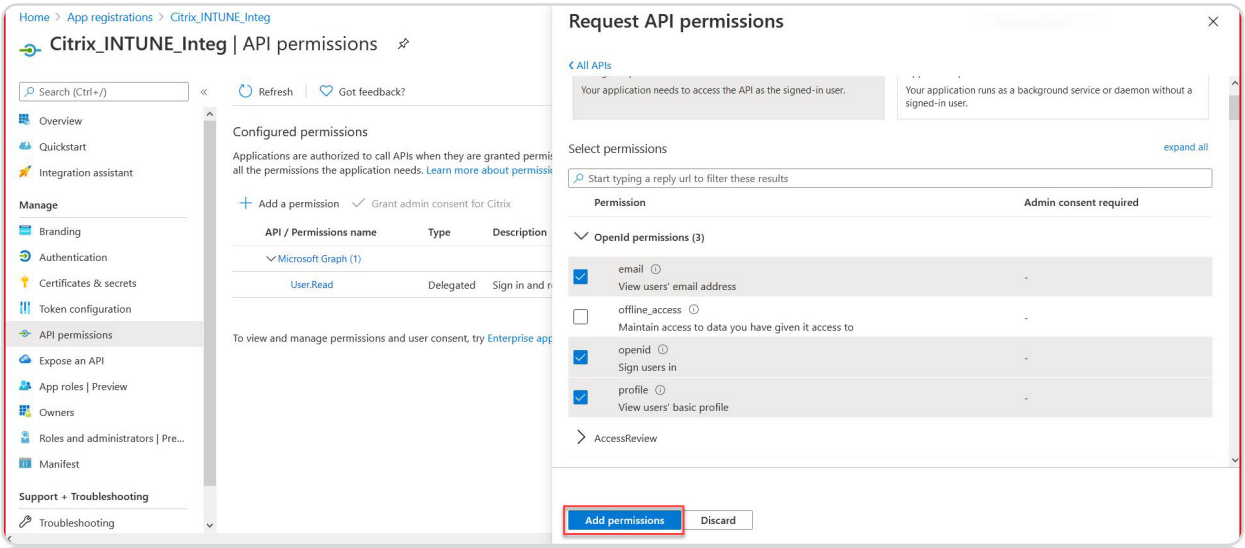

9. Haga clic en el mosaico **Permisos delegados**.

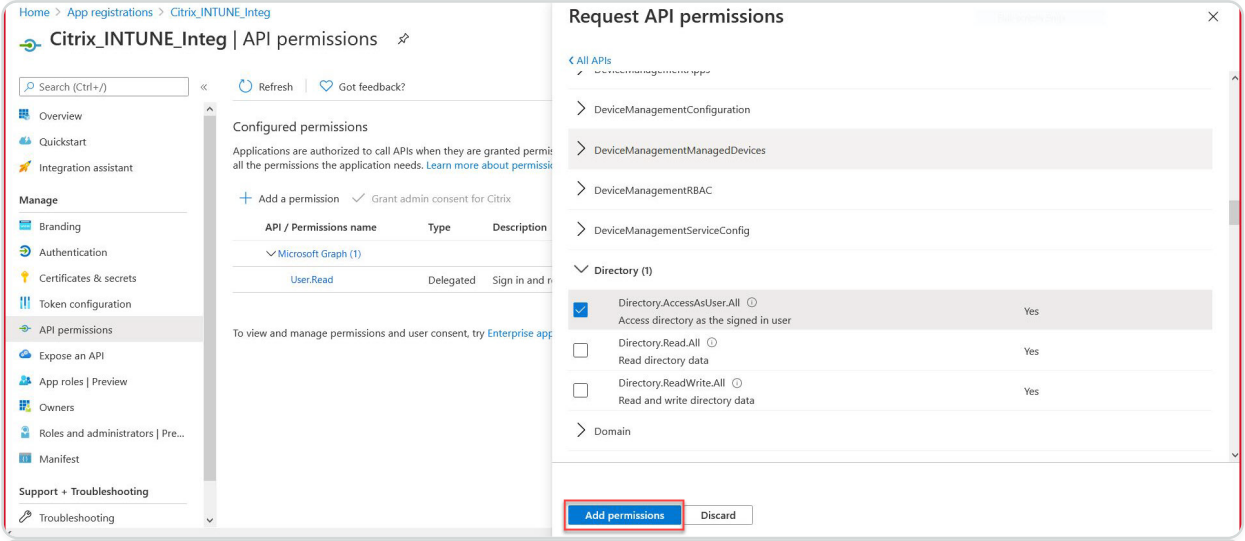


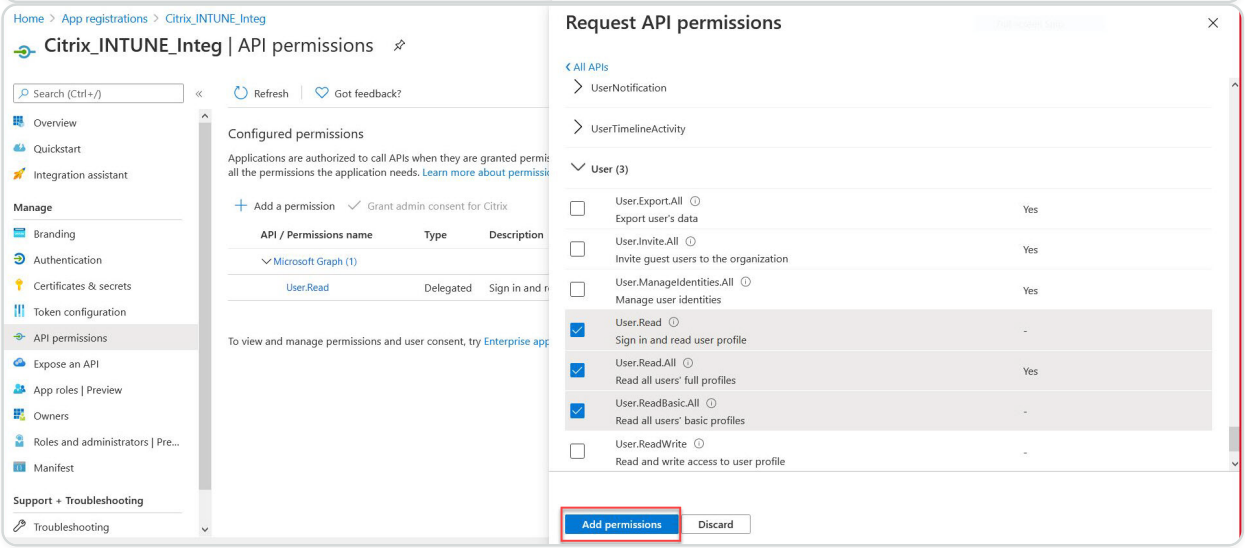

10. Seleccione los siguientes permisos y haga clic en **Agregar permisos**.

    - Correo electrónico
    - `openid`
    - Perfil
    - Directory.AccessAsUser.All
    - User.Read
    - User.Read.All
    - User.ReadBasic.All

© 1997–2026 Citrix Systems, Inc. All rights reserved.




© 1997–2026 Citrix Systems, Inc. All rights reserved.

**PERMISOS PARA LA COMPROBACIÓN NAC DE INTUNE:**

Todas las aplicaciones de Microsoft Entra ID que llaman a los puntos de conexión de servicio `https://login.microsoftonline.com`, `https://graph.microsoft.com` o `https://graph.windows.net` requieren que se asigne el permiso de API para que la puerta de enlace pueda llamar a la API de NAC. Los permisos de API disponibles son:

- Application.Read.All
- Application.ReadWrite.All
- Application.OwnedBy
- Directory.Read.All

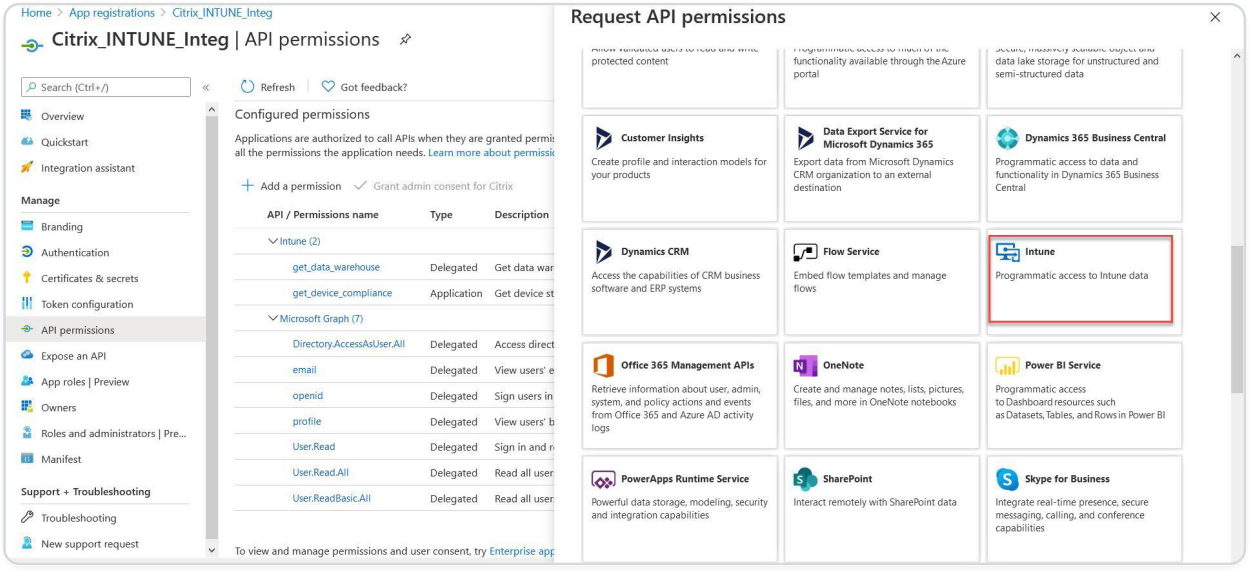
El permiso preferido es **Application.Read.All**.

Para obtener más detalles, consulte `<https://techcommunity.microsoft.com/t5/intune-customer-success/support-tip-intune-service-discovery-api-endpoint-will-require/ba-p/2428040>`

**Nota:**

Si un cliente solo utiliza la Intune Action para la comprobación NAC, el único permiso necesario es **Application.Read.All** en Microsoft Graph.

11. Haga clic en el mosaico de **Intune** para configurar los permisos de API para Intune.




12. Haga clic en el mosaico de **Application permissions** y en el mosaico de **Delegated permissions** para agregar permisos para Get_device_compliance y Get_data_warehouse, respectivamente.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Permiso de API para Intune(/en-us/netscaler-gateway/media/12-request-api-permission-for-intune.png)

13. Seleccione los siguientes permisos y haga clic en **Agregar permisos**.

    - Get_device_compliance - Permisos de aplicación
    - Get_data_warehouse - Permisos delegados

    **NOTA:**

    Para la comprobación de NAC de Intune, el único permiso requerido es **Get_device_compliance**.

    Permisos de API para obtener dispositivo(/en-us/netscaler-gateway/media/13-a-select-api-permission-for-intune.png)

    Permiso de API para obtener almacén(/en-us/netscaler-gateway/media/13-b-select-api-permission-for-intune.png)

14. La siguiente página enumera los permisos de API configurados.

    Lista de permisos de API(/en-us/netscaler-gateway/media/14-list-of-api-permission.png)

15. Vaya a **Certificados y secretos** y haga clic en **Nuevo secreto de cliente**.

    Nuevo secreto de cliente(/en-us/netscaler-gateway/media/15-new-client-secret.png)

16. En la página **Agregar un secreto de cliente**, introduzca una descripción, seleccione la caducidad y haga clic en **Agregar**.

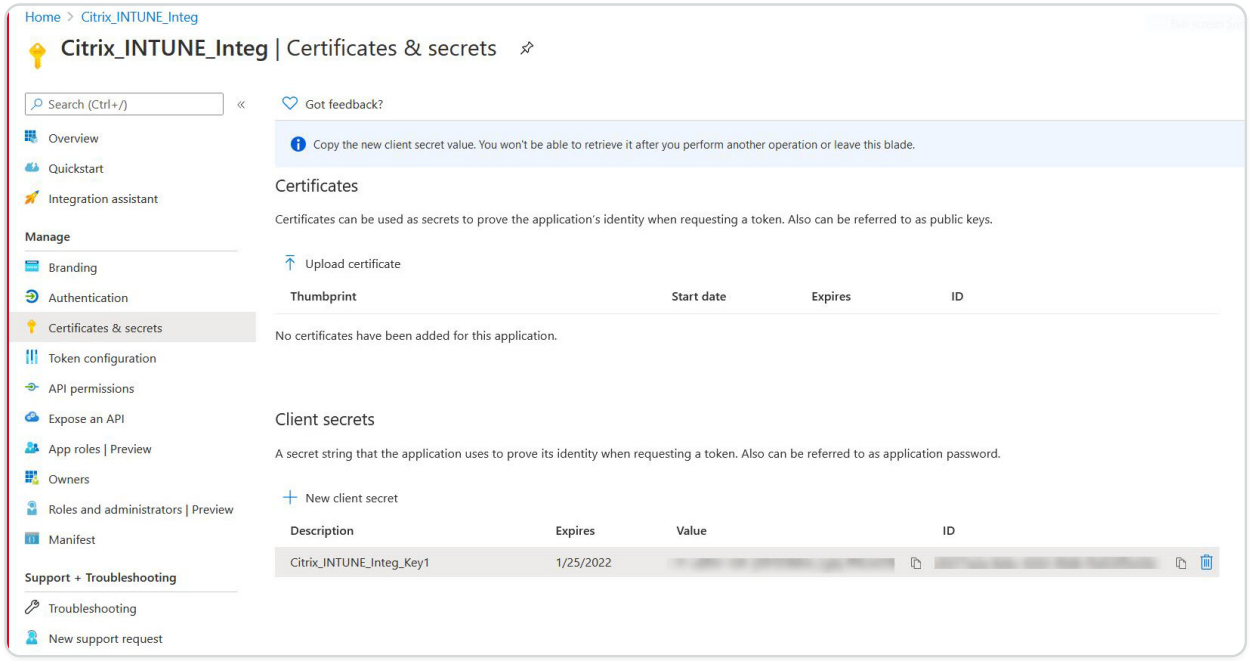
    Permiso de API(/en-us/netscaler-gateway/media/16-add-client-secret.png)

17. La siguiente pantalla muestra el secreto de cliente configurado.

    **NOTA**

    El secreto de cliente se muestra solo una vez cuando se genera. Copie el secreto de cliente mostrado localmente. Utilice el mismo secreto de cliente junto con el ID de cliente asociado a la aplicación recién registrada al configurar la acción OAuth en el dispositivo NetScaler Gateway para Intune.

© 1997–2026 Citrix Systems, Inc. All rights reserved.




La configuración de la aplicación en el portal de Azure ya está completa.

## Descripción de la autenticación de tokens MSAL

A continuación, se muestra el flujo de eventos en una autenticación de tokens MSAL de NetScaler Gateway típica:

1. Cuando se inicia una aplicación en iOS o Android, la aplicación se pone en contacto con Microsoft. Se solicita al usuario que inicie sesión con sus credenciales. Después de un inicio de sesión correcto, la aplicación obtiene un token MSAL.
2. Este token MSAL se presenta a un NetScaler Gateway, que se ha configurado para validar el token MSAL.
3. NetScaler Gateway valida la firma del token MSAL con el certificado correspondiente de Microsoft.
4. Después de una validación correcta, NetScaler Gateway extrae el nombre principal de usuario (UPN) y concede a la aplicación acceso VPN a los recursos internos.

## Configuración del servidor virtual de NetScaler Gateway para la autenticación de tokens MSAL

Para configurar un servidor virtual de NetScaler Gateway para supervisar la autenticación de tokens MSAL, necesita la siguiente información:

- **authorizationEndpoint**: La URL del punto final al que se debe redirigir al usuario no autenticado. NetScaler Gateway redirige al usuario a esta URL añadiendo parámetros de

© 1997–2026 Citrix Systems, Inc. All rights reserved.

consulta, incluido el ID de cliente. Si este parámetro no se especifica, por defecto el usuario se redirige a la URL configurada en **tokenEndpoint**.

- **tokenEndpoint**: La URL del punto final al que NetScaler Gateway publica el token OAuth para verificar su autenticidad. El usuario puede obtener el token OAuth del servidor de autorización tras una autenticación correcta.
- **GraphEndpoint**: La URL del servicio de la API de Graph para conocer los puntos finales de Enterprise Mobility Services (EMS).
- **certEndpoint**: La URL del punto final que contiene la clave web JSON (JWK) para la verificación de tokens MSAL.
- **Audience**: FQDN del servidor virtual de NetScaler al que la aplicación envía el token MSAL.
- **Issuer**: Nombre del emisor de Microsoft Entra ID. Se rellena por defecto.
- **TenantID**: ID de inquilino para el registro de MSAL.
- **ClientID**: Un ID único asignado a la aplicación Gateway como parte del registro de MSAL.
- **ClientSecret**: Una clave secreta asignada a la aplicación Gateway como parte del registro de MSAL.
- **ResourceURI**: Un parámetro opcional para capturar la URI del recurso. Si no se configura, NetScaler utiliza la URI del recurso comercial de Azure.

Realice los siguientes pasos mediante la CLI:

1. Cree una acción OAuth.

```
add authentication OAuthAction <oauth_action_name> -OAuthType <INTUNE>
-authorizationEndpoint <authorization_endpoint_fqdn> -tokenEndpoint
<token_endpoint_fqdn> -clientID <client_id_val> -clientSecret
<client_secret_val> -tenantID <tenant_id_value> -GraphEndpoint
<graph_endpoint_fqdn> -CertEndpoint <cert_endpoint_fqdn>
```

2. Agregue una etiqueta de política de autenticación a la acción OAuth.

```
add authentication policylabel <policy_label_name>
```

3. Crear una política de autenticación para asociar con la acción OAuth recién creada.

```
add authentication Policy <policy_name> -rule <true> -action
<oauth_intune_action>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. Vincular la política de autenticación a la etiqueta de política.

```
bind authentication policylabel <policy_label_name> -policyName
<policy_name> -priority 100
```

5. Configurar el servidor virtual de autenticación.

```
add authentication vserver <authvserver> SSL <0.0.0.0>

bind ssl vserver <authvserver> -certkeyName <cert_key_file_name>

bind authentication vserver <authvserver> -policy <ldap_policy_name>
-priority 100 -nextFactor <policy_label_name>
```

6. Configurar el servidor virtual VPN.

```
add authentication authnProfile <vpn_profile_name> -authnVsName
<authvserver>

add vpn vserver <vserver_name> SSL <vpn_ip_address> -authnProfile
<vpn_profile_name>
```

**Configuración de ejemplo:**

```
add authentication OAuthAction oauth_action_for_NAC -OAuthType INTUNE
-authorizationEndpoint "https://login.microsoftonline.com/
ed10c531-5d7b-4a5c-bb29-564c20480754/oauth2/v2.0/authorize" -tokenEndpoint
"https://login.microsoftonline.com/ed10c531-5d7b-4a5c-bb29-564c20480754/
oauth2/v2.0/token" -clientID 1dc2adc3-0298-4ff5-9bf5-b98852ff58ba
-clientSecret 6zM8Q~b4Hr9wwHEGFla.VDsiMWjvG~PS6PKv7c2m -tenantID
ed10c531-5d7b-4a5c-bb29-564c20480754



add authentication policylabel intune_oauth_pol_label



add authentication Policy oauth_intune_pol -rule true -action
oauth_action_for_NAC
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
bind authentication policylabel intune_oauth_pol_label -policyName
oauth_intune_pol -priority 100



add authentication vserver av_vs SSL 0.0.0.0

bind ssl vserver av_vs -certkeyName crt_key_file_name

bind authentication vserver av_vs -policy ldap_policy_name -priority 100
-nextFactor intune_oauth_pol_label



add authentication authnProfile vpn_authnprofile -authnVsName av_vs

add vpn vserver vpn_sp SSL VPN_IP_Address 443 -authnProfile
vpn_authnprofile
```

**Nota:**

Los parámetros de la configuración de ejemplo deben modificarse según los requisitos. En la configuración de ejemplo:

- `OAuthType`, `clientID`, `clientSecret` y `tenantID` son parámetros obligatorios.
- Los siguientes parámetros se rellenan con los valores predeterminados si el usuario no los configuró al crear la acción OAuth:
  - `GraphEndpoint`: `<https://graph.microsoft.com/>`
  - `AllowedTokenAlgorithms`: HS256, RS256, RS512
  - `TokenEndpointAuthMethod`: client_secret_post
  - `GrantType`: Code
- El `tenantID` utilizado en `authorizationEndpoint` y `tokenEndpoint` es `ed10c531-5d7b-4a5c-bb29-564c20480754`.
- El `loginSchema` utilizado es el esquema predeterminado. Dependiendo del caso de uso, se debe elegir un esquema de inicio de sesión apropiado.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Se selecciona `LDAP` como el primer factor de autenticación y `OAuth` como el siguiente factor, vinculado al servidor virtual de autenticación. Esto se puede modificar según el uso.

# Configurar NetScaler Gateway para usar micro VPN con Microsoft Endpoint Manager

La integración de micro VPN de Citrix con Microsoft Endpoint Management permite que sus aplicaciones accedan a los recursos locales. Para obtener más información, consulte Integración de micro VPN de Citrix con Microsoft Endpoint Manager.

## Requisitos del sistema

- Versiones de NetScaler Gateway
  - 13.1
  - 13.0
  - 12.1.50.x o posterior
  - 12.0.59.x o posterior

  Puede descargar la última versión de NetScaler Gateway desde la página de descarga de NetScaler Gateway.
- Un escritorio Windows con Windows 7 o posterior (solo para el empaquetado de aplicaciones Android)
- Microsoft
  - Acceso a Microsoft Entra ID (con privilegios de administrador de inquilinos)
  - Inquilino habilitado para Intune
- Reglas de firewall
  - Habilite una regla de firewall para el tráfico SSL desde una IP de subred de NetScaler Gateway a `*.manage.microsoft.com`, `https://login.microsoftonline.com` y `https://graph.microsoft.com` (puerto 443)
  - NetScaler Gateway debe poder resolver externamente las URL anteriores.

## Requisitos previos

- **Entorno de Intune:** Si no tiene un entorno de Intune, configure uno. Para obtener instrucciones, consulte la página Introducción a Microsoft Intune.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Aplicación Edge Browser:** El SDK de Micro VPN está integrado en la aplicación Microsoft Edge y en la aplicación Intune Managed Browser para iOS y Android. Para obtener más información sobre Managed Browser, consulte la página Administrar Microsoft Edge en iOS y Android con Intune.
- **Derecho de Citrix Endpoint Management™**: Asegúrese de tener un derecho activo de Citrix Endpoint Management para obtener soporte continuo para el SDK de micro VPN en un navegador móvil Microsoft Edge (iOS y Android). Para obtener más información, póngase en contacto con su representante de ventas, de cuenta o de socio.

## Conceder permisos de aplicación de Microsoft Entra ID

1. Dé su consentimiento para la integración multiinquilino de Citrix con la aplicación Microsoft Entra ID para permitir que NetScaler Gateway se autentique con el dominio de Microsoft Entra. El administrador global de Azure debe visitar la siguiente URL y dar su consentimiento:

   `<https://login.windows.net/common/adminconsent?client_id=b6a53a76-5d50-499e-beb3-c8dbdad5c40b&redirect_uri=https://www.citrix.com&state=consent>`.

2. Dé su consentimiento para la integración multiinquilino de Citrix con la aplicación Microsoft Entra ID para permitir que las aplicaciones móviles se autentiquen con la micro VPN de NetScaler Gateway. Este enlace solo es necesario si el administrador global de Azure ha cambiado el valor predeterminado de Los usuarios pueden registrar aplicaciones de Sí a No. Esta configuración se encuentra en el portal de Azure en **Microsoft Entra ID > Usuarios > Configuración de usuario**. El administrador global de Azure debe visitar la siguiente URL y dar su consentimiento (añada su ID de inquilino) `<https://login.microsoftonline.com/[tenant_id]/adminconsent?client_id=9215b80e-186b-43a1-8aed-9902264a5af7>`.

## Configurar NetScaler Gateway para micro VPN

Para usar micro VPN con Intune, debe configurar NetScaler Gateway para que se autentique en Microsoft Entra ID.

1. Descargue el archivo de script de configuración desde la página de descargas de NetScaler.
2. En el archivo de script, actualice los siguientes valores:

   - `<NSG_IP>`: Dirección IP virtual que se asignará al servidor virtual de NetScaler Gateway. Esta dirección IP debe ser accesible desde sus dispositivos, ya sea directamente o a través de un dispositivo NAT. No puede utilizar un servidor virtual de NetScaler Gateway existente.
   - `<ENV_NAME>`: Nombre para mostrar del servidor virtual de NetScaler Gateway.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- `<SERVER_CERT_NAME>`: Nombre del certificado de servidor que se vinculará al nuevo servidor virtual de NetScaler Gateway.
- `<AAD_CLIENT_SECRET>`: Valor del secreto de cliente generado mediante el script de PowerShell `NsgCreateSecret.ps1` (incluido en el script de configuración).
- `<AAD_TENANT_ID>`: ID de inquilino de Microsoft Entra donde se almacena el ID de Microsoft Entra del cliente. Puede obtenerlo desde la consola de administración de Microsoft Entra ID o generarlo mediante el script de PowerShell `NsgCreateSecret.ps1`.

3. Después de reemplazar todos los marcadores de posición con valores reales, ejecute todo el script ejecutando el siguiente comando en la CLI:

```
/netscaler/nscli -U :<NetScaler Management Username>:<NetScaler
Management Password> batch -f "/var/<NsgCreateScriptFileName>"
```

**NOTA:**

Asegúrese de que se devuelva el valor `Done` después de ejecutar el script.

4. Un servidor virtual de NetScaler Gateway existente no funciona para este caso de uso. Cree un servidor virtual de NetScaler Gateway y asegúrese de que el estado del servidor virtual sea **UP**. Para obtener más información, consulte Crear servidores virtuales.

## Validar la comunicación de NetScaler Gateway con los servicios de Microsoft

1. Acceda a su nuevo servidor virtual de NetScaler Gateway desde Internet utilizando herramientas en línea como SSL Checker. Esto confirma si el certificado del servidor está instalado correctamente y verifica la conectividad entre Internet y el servidor virtual de NetScaler Gateway alojado en su red DMZ.
2. Abra una conexión SSH a NetScaler Gateway utilizando un cliente SSH, como PuTTY.
3. Ejecute los siguientes comandos para comprobar la conexión saliente del dispositivo NetScaler Gateway a las URL de Microsoft: `https://login.microsoftonline.com`, `*.manage.microsoft.com` y `https://graph.microsoft.com`.

```
root@netscaler# curl -s -k https://login.microsoftonline.com

root@netscaler# curl -s -k https://graph.windows.net
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
root@netscaler# curl -s -k https://manage.microsoft.com
```

4. Salga de la conexión SSH y ejecute el comando `show oauthAction` en la CLI. El `OAuth Status` debe ser `COMPLETE`. Si ve el `OAuth Status` distinto de `COMPLETE`, consulte la sección Solución de problemas. Para usar micro VPN con Intune, debe configurar NetScaler Gateway para que se autentique en Microsoft Entra ID.

## Configuración del navegador Microsoft Edge

1. Inicie sesión en `<https://endpoint.microsoft.com/>` y, a continuación, vaya a **Intune > Aplicaciones móviles**.
2. Publique la aplicación Edge como lo hace normalmente y, a continuación, agregue una política de configuración de aplicaciones.
3. En **Administrar**, haga clic en **Directivas de configuración de aplicaciones**.
4. Haga clic en **Agregar** y, a continuación, introduzca un nombre para la directiva que desea crear. En **Tipo de inscripción de dispositivo**, seleccione **Aplicaciones administradas**.
5. Haga clic en **Aplicación asociada**.
6. Seleccione las aplicaciones a las que desea aplicar la directiva (Microsoft Edge o el explorador administrado por Intune) y, a continuación, haga clic en **Aceptar**.
7. Haga clic en **Configuración**.
8. En el campo **Nombre**, introduzca el nombre de una de las directivas que se enumeran en la siguiente tabla.
9. En el campo **Valor**, introduzca el valor que desea aplicar para esa directiva. Haga clic fuera del campo para agregar la directiva a la lista. Puede agregar varias directivas.
10. Haga clic en **Aceptar** y, a continuación, haga clic en **Agregar**.

La directiva se agrega a la lista de directivas.

| NOMBRE (IOS/ANDROID) | VALOR | DESCRIPCIÓN |
|---|---|---|
| MvpnGatewayAddress | `https://external.companyname.com` | URL externa de su NetScaler Gateway |
| MvpnNetworkAccess | MvpnNetworkAccessTunneledWebSSOor Unrestricted | MvpnNetworkAccessTunneledWebSSO es el valor |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| NOMBRE (IOS/ANDROID) | VALOR | DESCRIPCIÓN |
|---|---|---|
| | | predeterminado para la tunelización |
| MvpnExcludeDomains | Lista de nombres de dominio separados por comas que se excluirán | Opcional. Predeterminado=en blanco |
| TunnelExcludeDomains | `app.launchdarkly.com,cis.citrix.com,cis-staging.citrix.com,cis-test.citrix.com,clientstream.launchdarkly.com,crashlytics.com,events.launchdarkly.com,fabric.io,firehose.launchdarkly.com, hockeyapp.net,mobile.launchdarkly.com,pushreg.xm.citrix.com,rttf.citrix.com,rttf-staging.citrix.com,rttf-test.citrix.com,ssl.google-analytics.com,stream.launchdarkly.com` | Opcional. Utilice esta propiedad de cliente para anular la lista predeterminada de dominios excluidos. |

**NOTA:**

Web SSO es el nombre de Secure Browse en la configuración. El comportamiento es el mismo.

- **MvpnNetworkAccess** - MvpnNetworkAccessTunneledWebSSO habilita la redirección HTTP/HTTPS a través de NetScaler Gateway, también conocido como Tunneled-Web SSO. El gateway responde a los desafíos de autenticación HTTP en línea, proporcionando una experiencia de inicio de sesión único (SSO). Para usar Web SSO, establezca esta política en **MvpnNetworkAccessTunneledWebSSO**. La redirección de túnel completo no es compatible. Utilice **Unrestricted** para desactivar la tunelización de micro VPN.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **MvpnExcludeDomains** - Lista de nombres de host o dominio separados por comas que se excluirán de ser enrutados a través del proxy web inverso de NetScaler Gateway. Los nombres de host o dominio se excluyen aunque la configuración de DNS dividido de NetScaler Gateway configurada pudiera seleccionar el dominio o host.

  **NOTA:**

  - Esta política solo se aplica a las conexiones **MvpnNetworkAccessTunneledWebSSO**. Si `MvpnNetworkAccess` es **Unrestricted**, esta política se ignora.
  - Esta política se aplica solo al modo SSO web tunelizado con NetScaler Gateway configurado para tunelización dividida inversa.

- **TunnelExcludeDomains**: de forma predeterminada, MDX excluye algunos puntos de conexión de servicio de la tunelización micro VPN. Los SDK de aplicaciones móviles y las aplicaciones utilizan estos puntos de conexión de servicio para varias funciones. Por ejemplo, los puntos de conexión de servicio incluyen servicios que no requieren enrutamiento a través de redes empresariales, como Google Analytics, servicios de Citrix Cloud™ y servicios de Active Directory. Utilice esta propiedad de cliente para anular la lista predeterminada de dominios excluidos.

  Para configurar esta política de cliente global, en la consola de Microsoft Endpoint Management, vaya a **Configuración > Propiedades del cliente**, agregue la clave personalizada **TUNNEL_EXCLUDE_DOMAINS** y establezca el valor.

  **Valor**: para reemplazar la lista predeterminada con los dominios que desea excluir de la tunelización, escriba una lista de sufijos de dominio separados por comas. Para incluir todos los dominios en la tunelización, escriba ninguno. La lista predeterminada es: **Valor**: para reemplazar la lista predeterminada con los dominios que desea excluir de la tunelización, escriba una lista de sufijos de dominio separados por comas. Para incluir todos los dominios en la tunelización, escriba ninguno. La lista predeterminada es:

  `app.launchdarkly.com,cis.citrix.com,cis-staging.citrix.com,cis-test.citrix.com,clientstream.launchdarkly.com,crashlytics.com,events.launchdarkly.com,fa hockeyapp.net,mobile.launchdarkly.com,pushreg.xm.citrix.com,rttf.citrix.com,rttf-staging.citrix.com,rttf-test.citrix.com,ssl.google-analytics.com,stream.launchdarkly.com`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

# Solución de problemas

## Problemas generales

| PROBLEMA | RESOLUCIÓN |
| --- | --- |
| Aparece el mensaje "Se requiere agregar política" al abrir una aplicación | Agregar políticas en la API de Microsoft Graph |
| Hay conflictos de políticas | Solo se permite una política por aplicación |
| Aparece el mensaje "Error al empaquetar la aplicación" al encapsular una aplicación. Para ver el mensaje completo, consulte la siguiente tabla | La aplicación está integrada con el SDK de Intune. No es necesario encapsular la aplicación con Intune |
| Su aplicación no puede conectarse a recursos internos | Asegúrese de que los puertos de firewall correctos estén abiertos, de que su ID de inquilino sea correcto, etc. |

### Mensaje de error al empaquetar la aplicación:

*Error al empaquetar la aplicación. com.microsoft.intune.mam.apppackager.utils.AppPackagerException: Esta aplicación ya tiene el MAM SDK integrado. com.microsoft.intune.mam.apppackager.AppPackager.packageApp(AppPackager.java:113) com.microsoft.intune.mam.apppackager.PackagerMain.mainInternal(PackagerMain.java:198) com.microsoft.intune.mam.apppackager.PackagerMain.main(PackagerMain.java:56) La aplicación no se puede encapsular.*

## Problemas de NetScaler Gateway

| PROBLEMA | RESOLUCIÓN |
| --- | --- |
| | |
| NetScaler Gateway no puede acceder a `login.microsoftonline.com and graph.windows.net`. | Desde NS Shell, compruebe si puede acceder al siguiente sitio web de Microsoft: cURL -v -k `<https://login.microsoftonline.com>`. A continuación, compruebe si DNS está configurado en NetScaler Gateway. Compruebe también que la configuración del firewall sea correcta (en caso de que las |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| | |
|---|---|
| | solicitudes DNS estén bloqueadas por el firewall). |
| Aparece un error en ns.log después de configurar OAuthAction. | Compruebe si la licencia de Intune está habilitada y si la aplicación Azure Gateway tiene los permisos adecuados configurados. |
| El comando Sh OAuthAction no muestra el estado de OAuth como completado. | Compruebe la configuración de DNS y los permisos configurados en la aplicación Azure Gateway. |
| El dispositivo Android o iOS no muestra la solicitud de autenticación dual. | Compruebe si el logonSchema de ID de dispositivo de doble factor está vinculado al servidor virtual de autenticación. |

### Estado de OAuth de NetScaler Gateway y condición de error

| ESTADO | CONDICIÓN DE ERROR |
|---|---|
| AADFORGRAPH | Secreto no válido, URL no resuelta, tiempo de espera de conexión agotado |
| MDMINFO | `*manage.microsoft.com` está inactivo o inaccesible |
| GRAPH | El punto final de Graph está inactivo o inaccesible |
| CERTFETCH | No se puede comunicar con "Token Endpoint: `<https://login.microsoftonline.com>`" debido a un error de DNS. Para validar esta configuración, vaya al shell y escriba cURL `<https://login.microsoftonline.com>`. Este comando debe validarse. |

**Nota:** Cuando el estado de OAuth es correcto, el estado se muestra como COMPLETE.

## Último punto final del servicio de control de acceso a la red (NAC) de OAuth

A partir de la versión 13.1 compilación 55.x, el servidor virtual VPN admite el último punto final de servicio NAC de OAuth. Esta compatibilidad permite la funcionalidad MDM de extremo a extremo.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

A continuación, se muestra una configuración de CLI de ejemplo de los puntos finales del servicio NAC:

```
add authentication OAuthAction &lt;oauth_action_for_NAC> -OAuthType INTUNE
-authorizationEndpoint "https://login.microsoftonline.com/
&lt;ed10c590-5d7b-4a5c-bb29-564c20480756>/oauth2/v2.0/authorize"
-tokenEndpoint "https://login.microsoftonline.com/&lt;ed10c590-5d7b-4a5c-
bb29-564c20480756>/oauth2/v2.0/token" -clientID <1dc2adc3-0298-4ff5-9bf5-
b98852ff58ba> -clientSecret <6zM8Q~b4Hr9wwHEGFVDsiMWjvG~IS6PKv2m>
-tenantID &lt;ed10c590-5d7b-4a5c-bb29-564c20480756> -GraphEndpoint
"https://graph.microsoft.com" -refreshInterval 1440 -grantType CODE
-authentication DISABLED -allowedAlgorithms HS256 RS256 RS512 -PKCE
ENABLED -tokenEndpointAuthMethod client_secret_post
```

Para obtener más información, consulte Autenticación OAuth.

## Soporte extendido para Azure AD Graph

Dado que Azure AD Graph está obsoleto, los clientes que activan una nueva aplicación no pueden usar los permisos anteriores que estaban disponibles con Azure AD Graph. Sin embargo, los clientes con aplicaciones existentes que deseen usar los permisos antiguos de Azure AD Graph durante un tiempo más pueden seguir haciéndolo realizando algunos cambios de configuración en el dispositivo de puerta de enlace. Esta configuración es compatible con la versión 13.1-27.xx y posteriores de NetScaler Gateway.

Realice los siguientes cambios de configuración en el dispositivo NetScaler Gateway:

1. En el símbolo del sistema, ejecute el siguiente comando.

   ```
   shell nsapimgr_wr.sh -ys call=”ns_intune_enable_old_endpoints”
   ```

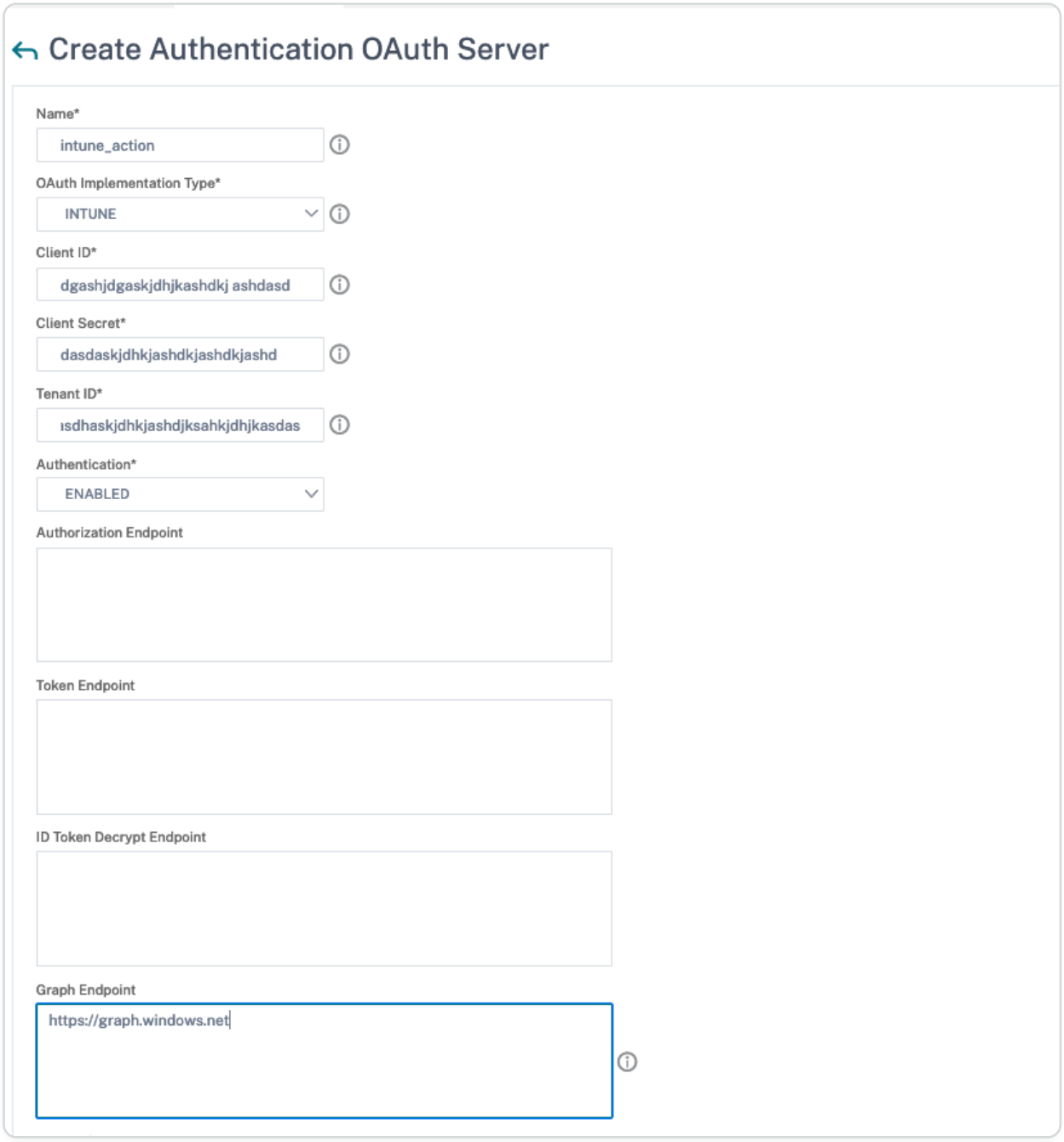
2. Vaya a **Security > AAA-Application Traffic > Policies > Authentication > Advanced Policies > Actions > OAUTH Actions**.

   a. Seleccione un servidor OAuth existente.

   b. Haga clic en **More**.

   c. En **Graph Endpoint**, asegúrese de que la URL se parezca a la que se muestra en la figura.

© 1997–2026 Citrix Systems, Inc. All rights reserved.




© 1997–2026 Citrix Systems, Inc. All rights reserved.

# Soporte de transporte de datos optimizado HDX™

El soporte de transporte de datos optimizado (EDT) para NetScaler Gateway garantiza una experiencia de usuario en sesión de alta definición de escritorios virtuales para los usuarios que ejecutan la aplicación Citrix Workspace.

Además, se facilita el cifrado de extremo a extremo con DTLS 1.0 para la terminación de EDT entre la aplicación Citrix Workspace y VDA. Para obtener más información, consulte Soporte para el protocolo DTLS.

NetScaler Gateway con EDT habilitado ofrece una buena experiencia de usuario tanto en condiciones de LAN como de WAN. Con EDT, no necesita ninguna configuración administrativa o de usuario al pasar de una a otra. El beneficio es más visible en redes de alta latencia con pérdida moderada de paquetes, donde la experiencia del usuario generalmente se retrasaría con alternativas.

## Cuándo utilizar el soporte de transporte de datos iluminado

Los siguientes escenarios ilustran el uso de NetScaler Gateway con EDT habilitado.

- Un usuario desea una experiencia tan buena como en un entorno LAN al acceder de forma remota a los recursos empresariales.
- Un usuario desea una experiencia de usuario enriquecida con aplicaciones y escritorios virtuales en redes Wi-Fi y móviles donde la calidad de la red es deficiente debido a la congestión, la alta pérdida de paquetes y la alta latencia.

Los siguientes puntos deben tenerse en cuenta al usar EDT.

- El control DTLS a nivel de servidor virtual está habilitado de forma predeterminada.
- IPv6 con DTLS no es compatible.
- El dispositivo ahora se puede configurar para la funcionalidad de doble salto para el tráfico EDT entre Receiver y VDA. Para obtener más información, haga clic en Implementación en una DMZ de doble salto.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**Nota:** EDT es compatible con la plataforma MPX FIPS en la versión 12.1 compilación 49.xx y posteriores. En los dispositivos MPX basados en el chip Intel Coleto SSL, EDT es compatible a partir de la versión 12.1 compilación 51.16 y posteriores.

## Configurar NetScaler Gateway para admitir Enlightened Data Transport

El tráfico EDT a través de Gateway ahora tiene visibilidad de extremo a extremo. La disponibilidad de datos de visibilidad tanto en tiempo real como históricos permite a NetScaler ADM admitir una amplia variedad de casos de uso.

Se admiten los siguientes escenarios:

| ESCENARIO | COMPATIBILIDAD CON EDT |
|---|---|
| NetScaler Gateway | Sí |
| NetScaler Gateway con alta disponibilidad (HA) | Sí |
| NetScaler Gateway con optimización de alta disponibilidad (HA) | Sí |
| NetScaler con Unified Gateway | Sí |
| NetScaler Gateway con GSLB | Sí |
| NetScaler Gateway con clúster | Sí |
| Cifrado DTLS de la aplicación Citrix Workspace a NetScaler Gateway | Sí |
| Autoridad de tickets seguros (STA) dual en NetScaler Gateway | Sí |
| Tiempo de espera de la sesión ICA de NetScaler Gateway | Sí |
| ICA de flujo múltiple de NetScaler Gateway | No |
| Fiabilidad de la sesión de NetScaler Gateway (Puerto 2598) | Sí |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| ESCENARIO | COMPATIBILIDAD CON EDT |
|---|---|
| Salto doble de NetScaler Gateway | Sí |
| Cifrado DTLS de NetScaler a VDA | Sí |
| HDX Insight | Sí |
| NetScaler Gateway en modo IPv6 | No |
| NetScaler Gateway SOCKS (Puerto 1494) | No |
| Proxy LAN puro de NetScaler (consulte la nota) | No |

**NOTA:**

EDT no es compatible si el proxy LAN de NetScaler está configurado en modo de usuario LAN o en modo transparente. Sin embargo, TCP es compatible. Para obtener más información, consulte Configuración del proxy ICA saliente.

## Configurar NetScaler Gateway para admitir Enlightened Data Transport

Si utiliza Enlightened Data Transport (EDT), debe habilitar Datagram Transport Layer Security (DTLS) para cifrar la conexión UDP utilizada por EDT. El parámetro DTLS debe habilitarse a nivel de servidor virtual VPN de Gateway. Además, los componentes de Citrix Virtual Apps and Desktops deben actualizarse y configurarse correctamente para lograr tráfico cifrado entre el servidor virtual VPN de Gateway y el dispositivo de usuario.

**NOTA:**

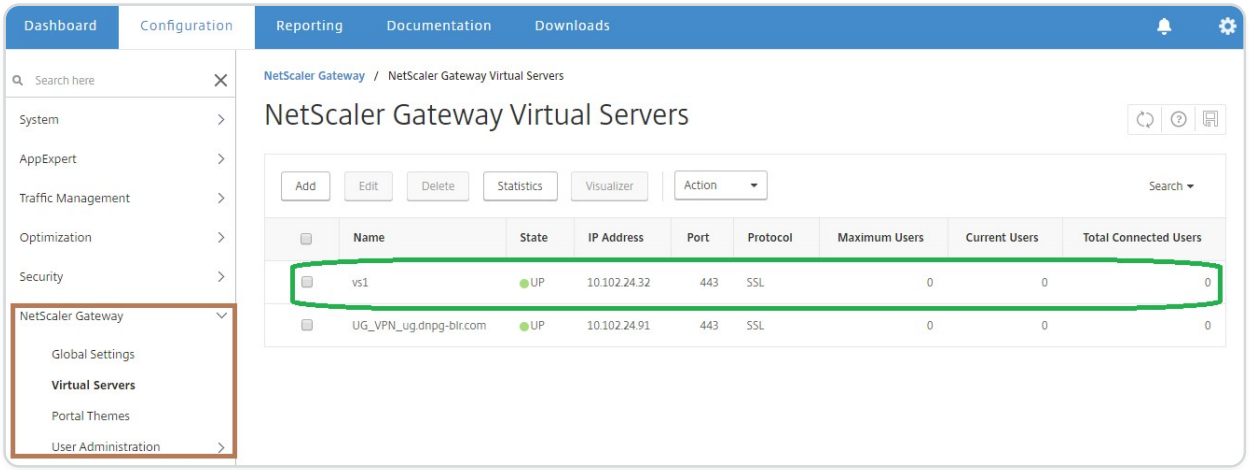
El puerto UDP (por ejemplo, el puerto 443) configurado para el servidor virtual de front-end de NetScaler Gateway debe abrirse en la DMZ para que el servidor virtual reciba las conexiones DTLS. DTLS y CGP son requisitos previos para que EDT sea compatible con NetScaler Gateway.

### Para configurar NetScaler Gateway para admitir EDT mediante la GUI

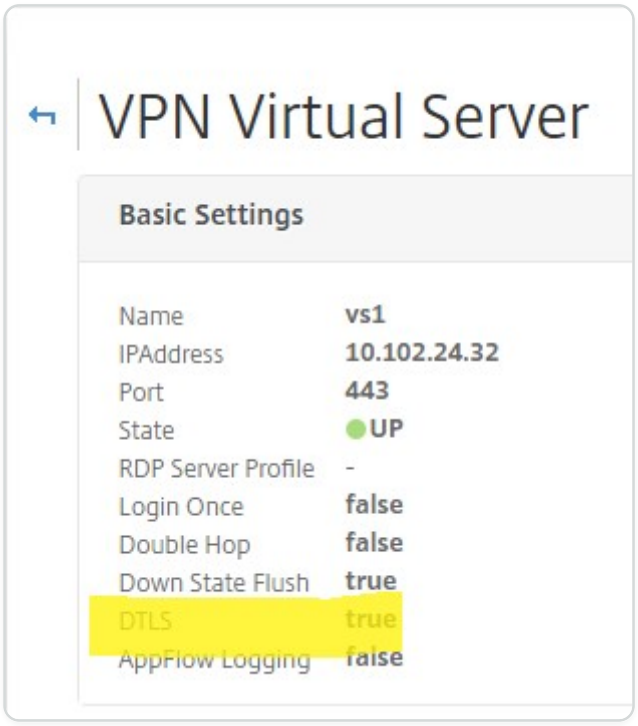
1. Implemente y configure NetScaler Gateway para comunicarse con StoreFront y autenticar a los usuarios de Citrix Virtual Apps and Desktops.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. En la ficha Configuración de la GUI de NetScaler, expanda **NetScaler Gateway** y seleccione **Virtual Servers**.

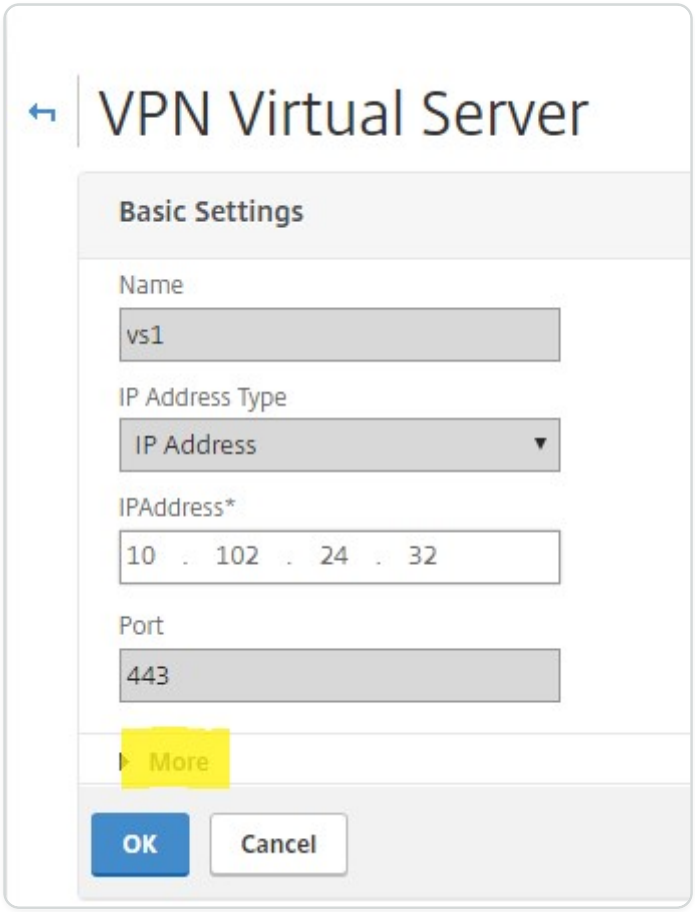



3. Haga clic en **Editar** para mostrar la configuración básica del servidor virtual VPN y, a continuación, verificar el estado de la configuración de DTLS.




4. Haga clic en **Más** para mostrar otras opciones de configuración.

© 1997–2026 Citrix Systems, Inc. All rights reserved.




5. Seleccione **DTLS** para proporcionar seguridad de las comunicaciones para los protocolos de datagramas. Haga clic en **Aceptar**. El área **Configuración básica** del servidor virtual VPN muestra que el indicador DTLS está establecido en **True**.




### Para configurar NetScaler Gateway para la compatibilidad con EDT mediante la CLI

```
set vpn vserver vs1 -DTLS ON
```

## Configurar NetScaler Gateway para admitir HDX Insight

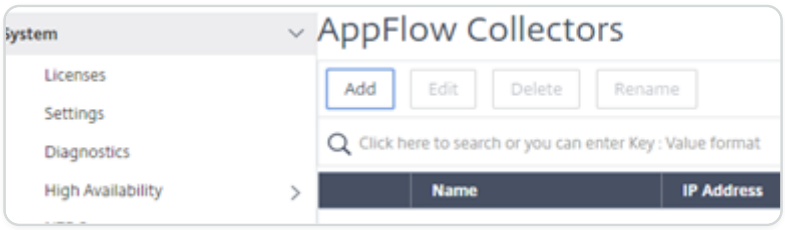
HDX Insight proporciona visibilidad de extremo a extremo para el tráfico HDX a aplicaciones y escritorios virtuales que pasa a través de NetScaler. También permite a los administradores ver

© 1997–2026 Citrix Systems, Inc. All rights reserved.

métricas de latencia de cliente y red en tiempo real, informes históricos, datos de rendimiento de extremo a extremo y solucionar problemas de rendimiento.

## Para configurar NetScaler Gateway para admitir HDX Insight mediante la GUI

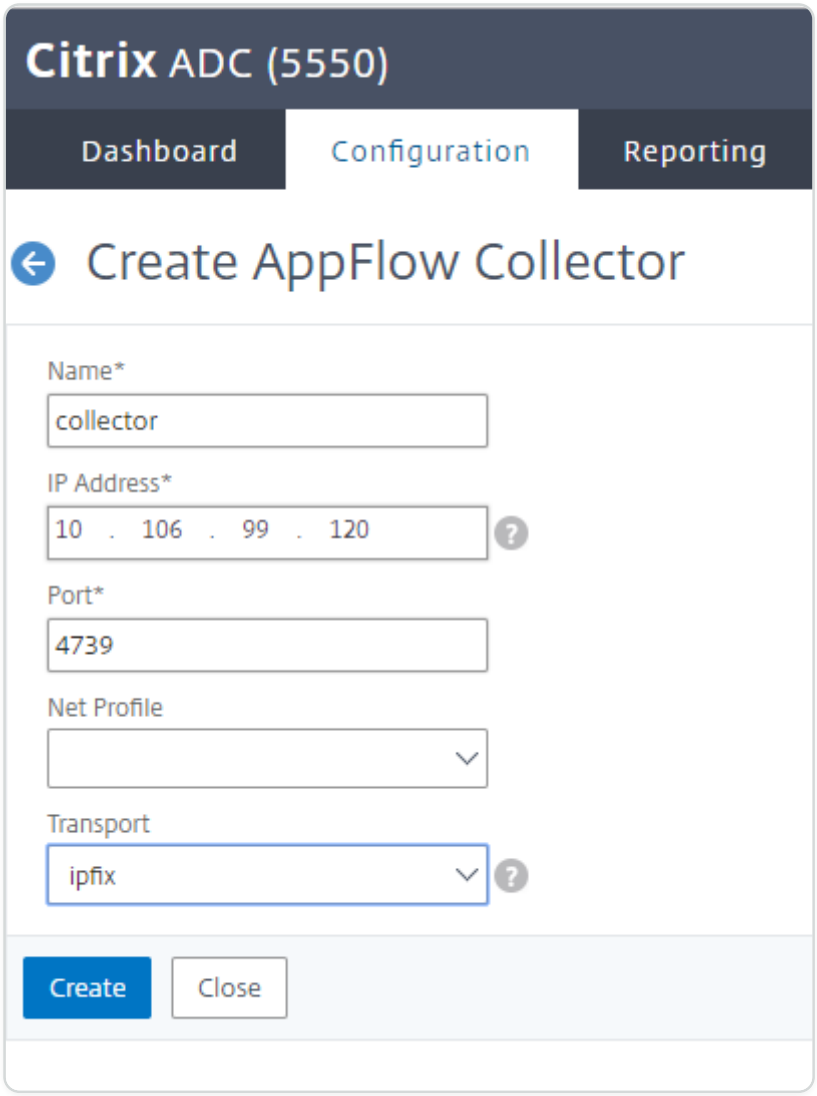
1. En la ficha **Configuration**, vaya a **System> AppFlow®>Collectors** y haga clic en **Add**.



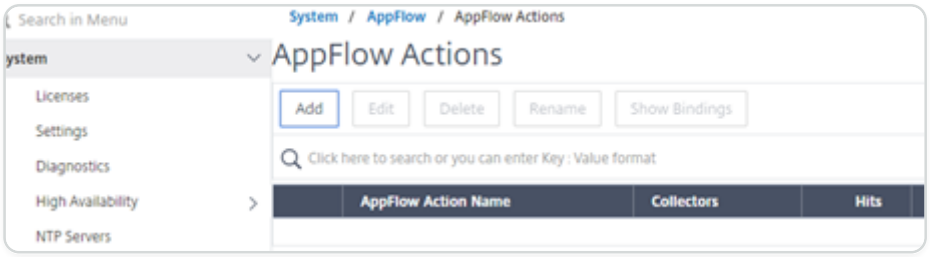

2. En la página **Create AppFlow Collector**, rellene los siguientes campos y haga clic en **Create**.

   - **Nombre:** Nombre del recopilador
   - **Dirección IP:** Dirección IPv4 del recopilador
   - **Puerto:** Puerto en el que escucha el recopilador
   - **Perfil de red:** Perfil de red para asociar con el recopilador. La dirección IP definida en el perfil se utiliza como dirección IP de origen para el tráfico de AppFlow de este recopilador. Si no establece este parámetro, la dirección IP de NetScaler (NSIP) se utiliza como dirección IP de origen.
   - **Transporte:** Tipo de transporte del recopilador.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



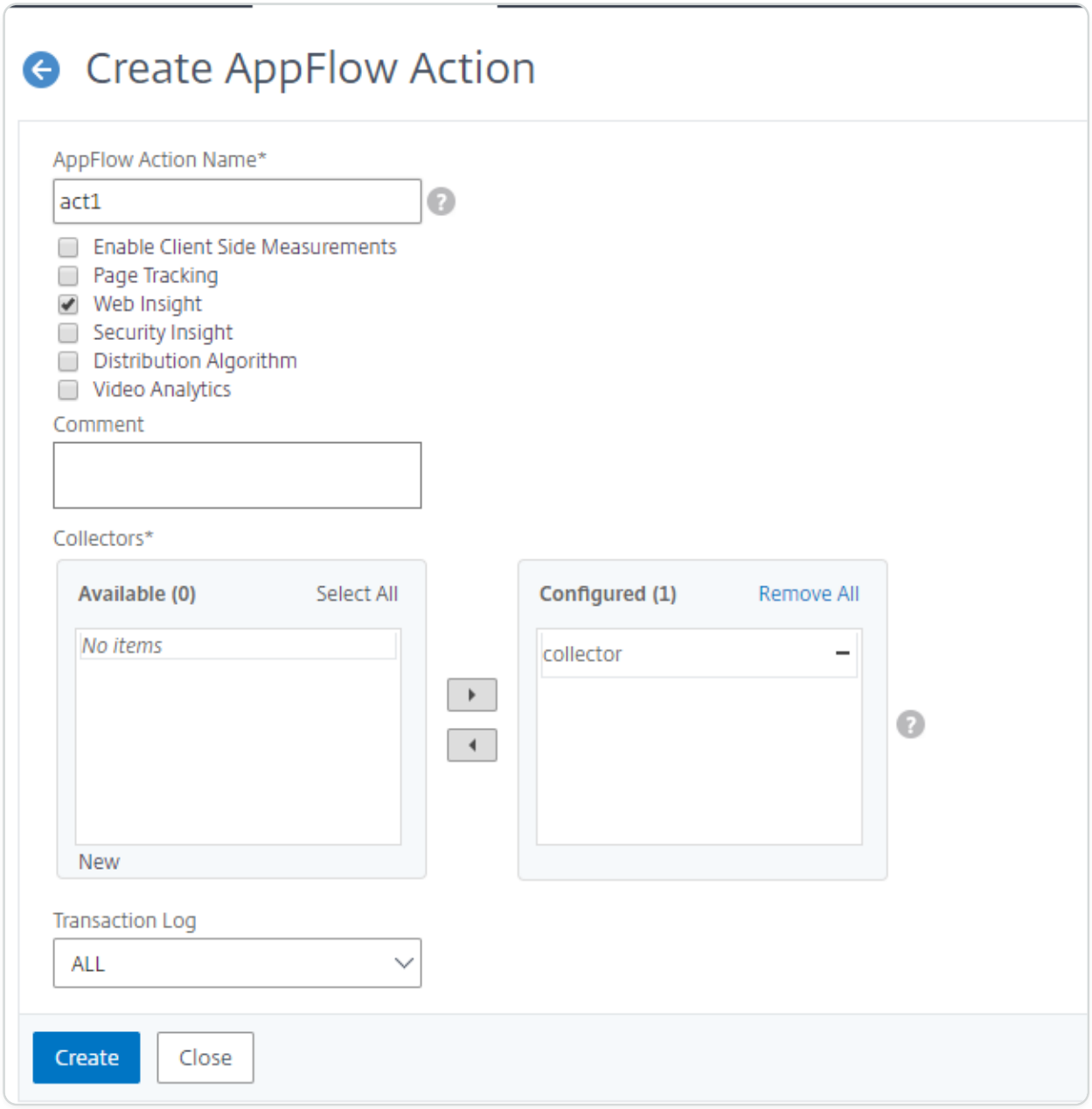

3. Vaya a **System > AppFlow > Actions** y haga clic en **Add**.




4. En la página **Create AppFlow Action**, rellene los siguientes campos y haga clic en **Create**.

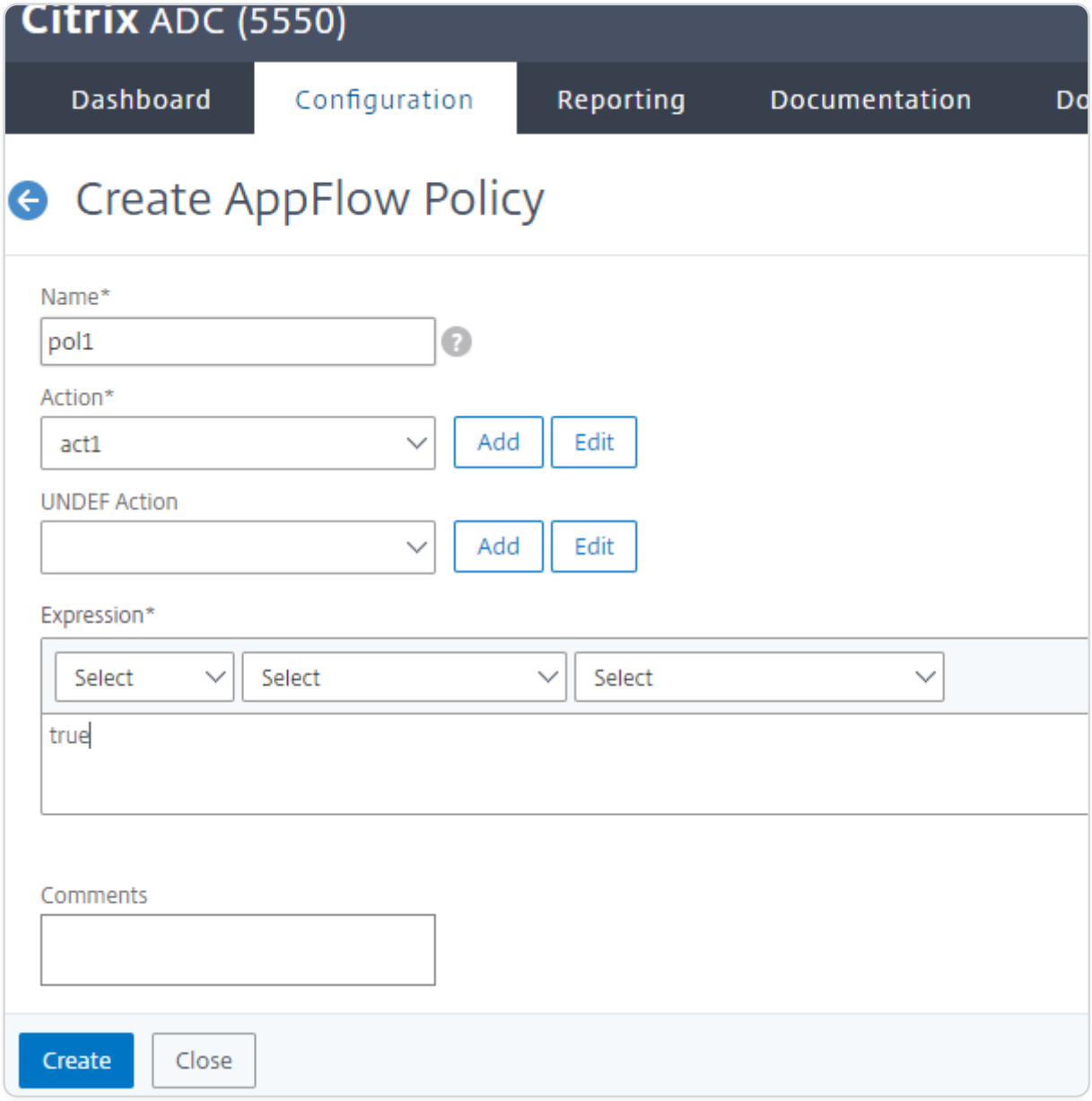
   - **Nombre de la acción de AppFlow:** Nombre de la acción
   - **Comentario:** Cualquier comentario sobre la acción
   - **Colector:** Seleccione los nombres de los colectores que se asociarán a la acción de AppFlow.
   - **Registro de transacciones:** Tipo de transacciones que se registrarán.

© 1997–2026 Citrix Systems, Inc. All rights reserved.




5. Vaya a **Sistema > AppFlow > Directivas** y haga clic en **Agregar**.

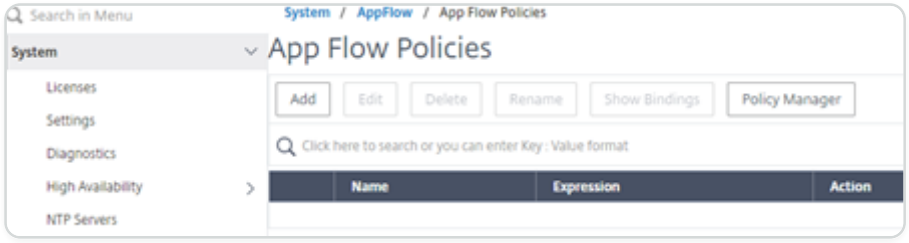
© 1997–2026 Citrix Systems, Inc. All rights reserved.



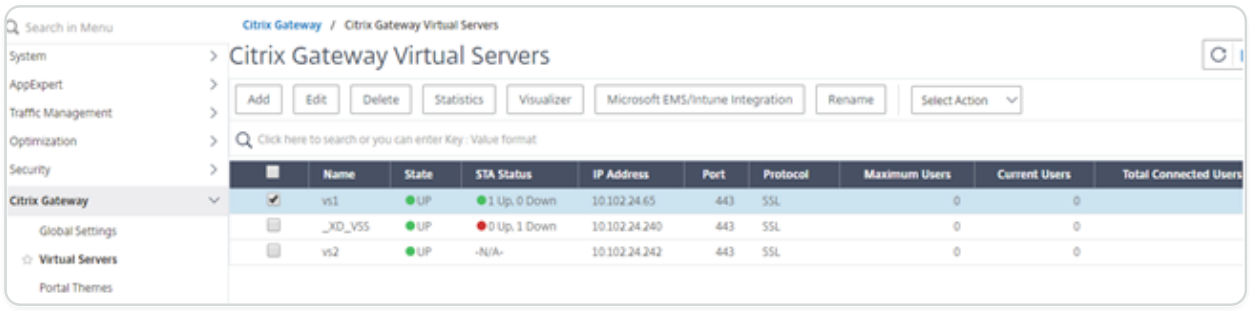

6. En la página **Crear directiva de AppFlow**, rellene los siguientes campos y haga clic en **Crear**.

   - **Nombre:** Nombre de la directiva.
   - **Acción:** Nombre de la acción que se asociará a la directiva.
   - **INDETERMINADO:** Nombre de la acción de AppFlow que se asociará a esta directiva cuando se produzca un evento indefinido.
   - **Expresión:** Expresión u otro valor con el que se evalúa el tráfico. Debe ser una expresión booleana.
   - **Comentarios:** Cualquier comentario sobre esta directiva.

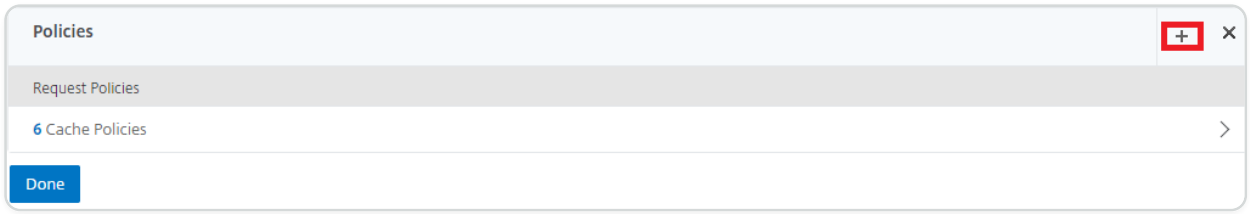
© 1997–2026 Citrix Systems, Inc. All rights reserved.



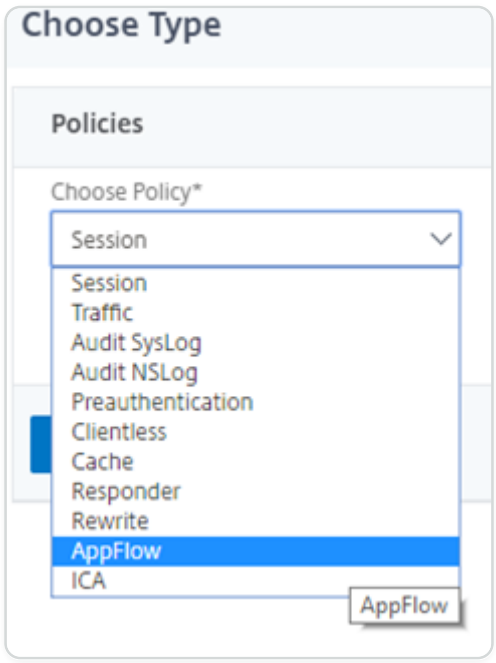

7. Vaya a **NetScaler Gateway > Servidores virtuales**, seleccione el servidor virtual y haga clic en **Modificar**.




8. Desplácese hacia abajo en la página **Servidor virtual VPN** y, en la sección **Directivas**, haga clic en **+**.

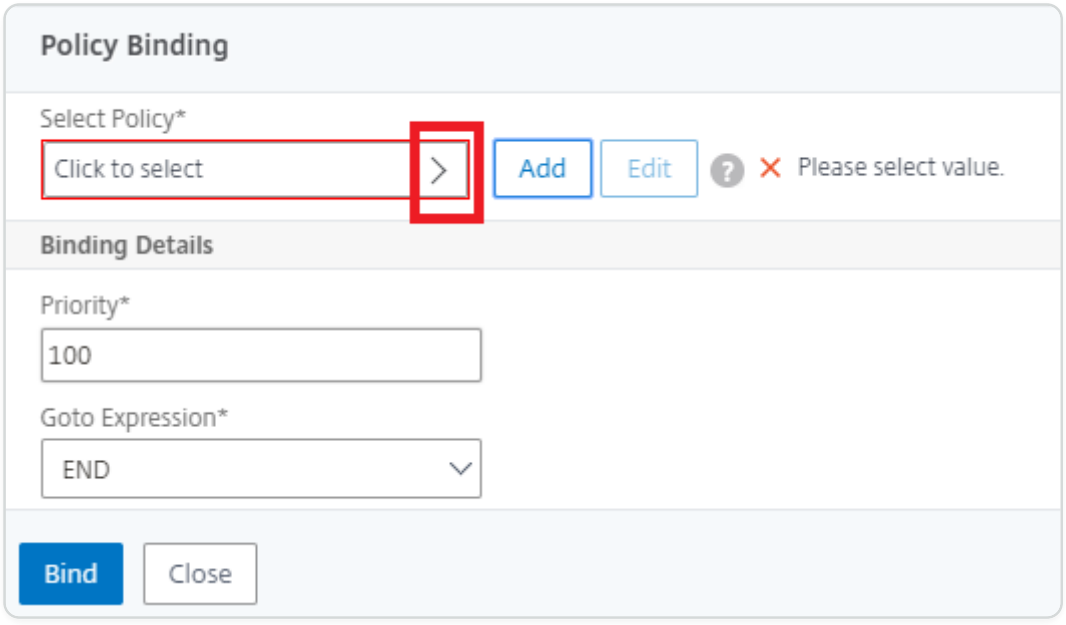



9. En la pantalla **Elegir tipo**, en el menú desplegable **Elegir directiva**, seleccione **AppFlow**. En el menú desplegable **Elegir tipo**, elija **Solicitud** o **Solicitud ICA®** y haga clic en **Continuar**.

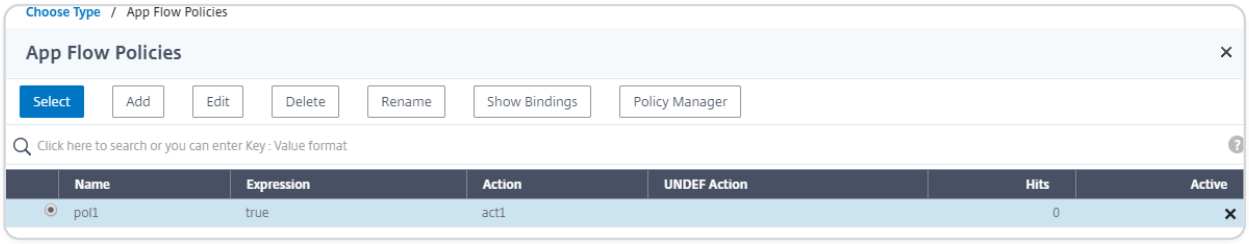



10. Haga clic en la flecha resaltada en **Seleccionar directiva**.

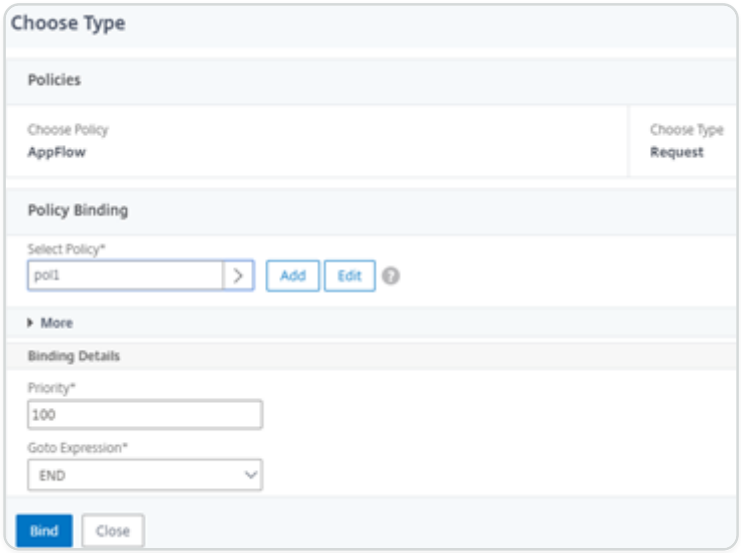
© 1997–2026 Citrix Systems, Inc. All rights reserved.




11. Seleccione la **directiva de AppFlow** y haga clic en **Seleccionar**.




12. Finalmente, haga clic en **Enlazar**.




## Para configurar NetScaler Gateway para admitir HDX Insight mediante la CLI

En el símbolo del sistema, escriba:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
add appflow collector col3 -IPAddress<ip_mas>

add appflow action act1 <action_name>

add appflow policy <policy_name> true <action_name>

bind vpn Vserver <vserver_name>  -pol <policy_name> - priority101 END
-type <ICA_Request>
```

### Deshabilitar HDX Insight para sesiones HDX de AppFlow (NSAP) que no son de NetScaler®

En un dispositivo NetScaler, ahora puede deshabilitar HDX Insight para las sesiones HDX que no son NSAP.

En el símbolo del sistema, escriba:

```
set ica parameter HDXInsightNonNSAP (YES | NO )
```

De forma predeterminada, HDX™ Insight para sesiones que no son NSAP está habilitado.

## Detección de PMTUD y propagación de bits DF para EDT a través de NetScaler Gateway

A partir de la versión 13.1 compilación 17.x, el dispositivo NetScaler Gateway admite la aplicación de bits DF para la detección de la unidad de transmisión máxima de la ruta EDT (PMTUD). La detección de MTU de ruta ayuda a determinar dinámicamente la unidad de transmisión máxima (MTU) al establecer una sesión. La aplicación de bits DF evita la fragmentación de EDT que podría provocar una degradación del rendimiento o un fallo al establecer una sesión.

En versiones anteriores, NetScaler Gateway admitía MTUD de ruta EDT, pero no admitía la aplicación de bits DF.

Para obtener más detalles, consulte Enlightened Data Transport.

### Habilitar la compatibilidad con PMTUD mediante la CLI

En el símbolo del sistema, escriba;

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
set ica parameter [-EnableSRonHAFailover ( YES | NO )] [-HDXInsightNonNSAP
( YES | NO )] [-EDTPmtudDF ( ENABLED | DISABLED )] [-EDTPmtudDFTimeout
<positive_integer>] [-L7LatencyFrequency <positive_integer>]
```

Ejemplo:

```
set ica parameter -EnableSRonHAFailover YES -EDTPmtudDF ENABLED
-EDTPmtudDFTimeout 100
```

**NOTA:**

A partir de la versión 13.1 compilación 42.x y posteriores, el parámetro EDTPmtudDF está habilitado de forma predeterminada. Anteriormente, esta opción estaba deshabilitada de forma predeterminada.

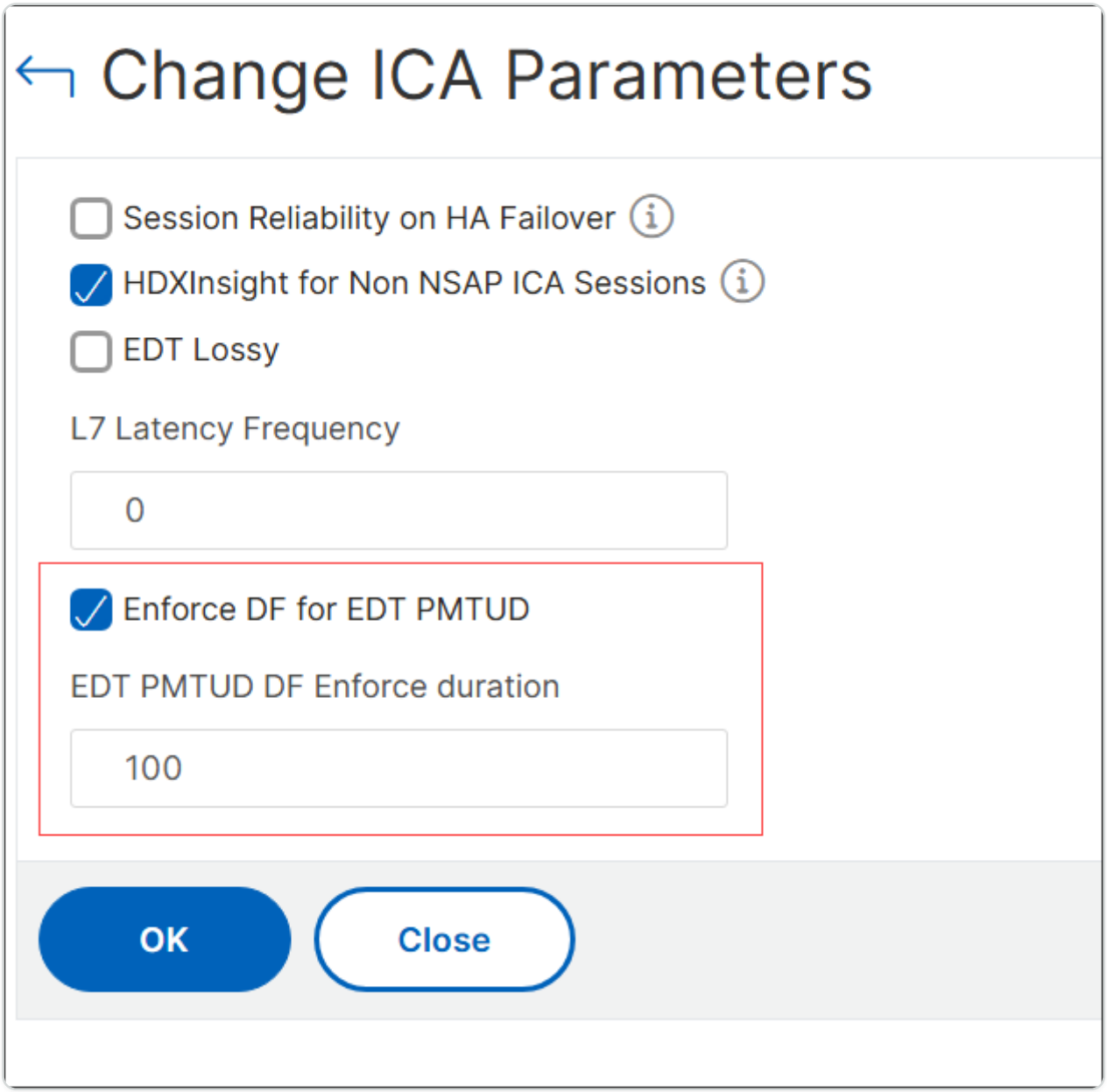
## Habilitar la compatibilidad con PMTUD mediante la GUI

1. Vaya a **Sistema > Configuración > Cambiar parámetros de ICA®**.
2. En **Duración de aplicación de DF de PMTUD de EDT**, introduzca el tiempo de espera en segundos para la aplicación de DF de PMTUD.

**NOTA:**

A partir de la versión 13.1 compilación 42.x y posteriores, la opción **Aplicar DF para PMTUD de EDT** está habilitada de forma predeterminada. Anteriormente, esta opción estaba deshabilitada de forma predeterminada.

© 1997–2026 Citrix Systems, Inc. All rights reserved.




## Umbral de latencia L7

La función de umbral de latencia L7 en HDX™ Insight detecta activamente los problemas de latencia de red de extremo a extremo a nivel de aplicación y toma medidas proactivas. La función de umbral de latencia L7 realiza una supervisión de latencia en tiempo real para detectar los picos y envía notificaciones a HDX Insight si la latencia supera la latencia mínima observada.

Anteriormente, los valores promedio de latencia L7 del lado del cliente y del lado del servidor se enviaban cada 60 segundos a HDX Insight. Cualquier pico detectado dentro de este intervalo se promediaba y, por lo tanto, no se detectaba. Además, no había una supervisión de latencia en tiempo real para detectar estos picos.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

## Diferencia entre la latencia L7 y la latencia L4

Las latencias de red también se capturan y muestran en el nivel L4. Estas latencias se calculan a partir de la capa TCP y no requieren el análisis del tráfico ICA. Por lo tanto, son relativamente fáciles de obtener y requieren menos CPU. Sin embargo, el principal inconveniente de la latencia L4 es la comprensión de la latencia de extremo a extremo. Si hay proxies TCP en la ruta, la latencia L4 solo captura la latencia desde NetScaler hasta el proxy TCP. Esto podría dar lugar a información incompleta y, por lo tanto, a dificultades para depurar el problema.

La latencia L7 se calcula analizando el tráfico ICA®. El cálculo de la latencia L7 se realiza en la capa ICA y, por lo tanto, los proxies intermedios no dan como resultado valores de latencia incompletos. De este modo, proporciona detección de latencia de extremo a extremo.

Las siguientes figuras muestran un tipo de implementación con y sin proxies TCP.

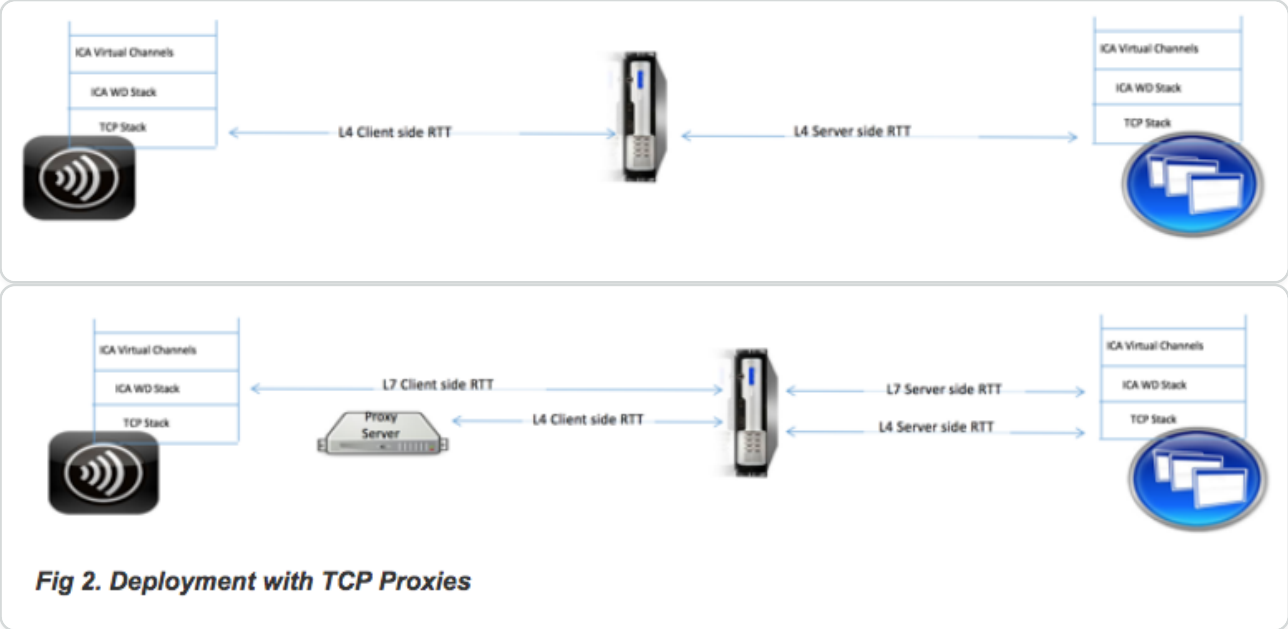



*Fig 2. Deployment with TCP Proxies*

## Diferencia entre los cálculos de ICA RTT y latencia L7

ICA RTT representa el tiempo total de ida y vuelta desde la aplicación Citrix Workspace hasta el Virtual Delivery Agent (VDA). La latencia L7 proporciona detalles granulares sobre las latencias en el lado del cliente y del servidor. La latencia del cliente L7 es la latencia entre la aplicación Citrix Workspace y NetScaler Gateway. La latencia del servidor L7 es la latencia entre NetScaler Gateway y VDA.

**NOTA**

. El cálculo de la latencia L7 del lado del servidor solo es compatible con las versiones 7.13 y posteriores de Citrix Virtual Apps and Desktops.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

## Configurar el umbral de latencia L7 mediante la CLI

1. Agregar un perfil de latencia ICA.

```
add ica latencyprofile <name> [-l7LatencyMonitoring ( ENABLED |
DISABLED )] [-l7LatencyThresholdFactor <positive_integer>] [-
l7LatencyWaitTime <positive_integer>] [-l7LatencyNotifyInterval
<positive_integer>] [-l7LatencyMaxNotifyCount <positive_integer>]
```

2. Agregar una acción ICA.

```
add ica action <name> [-latencyprofileName <string>]
```

3. Agregar una política ICA.

```
add ica policy <name> -rule <expression> -action <string> [-
comment<string>] [-logAction <string>
```

4. Vincular la política ICA al servidor VPN o al punto de enlace global de ICA.

```
bind ica global -policyName <string> -priority <positive_integer> [-
gotoPriorityExpression <expression>] [-type ( ICA_REQ_OVERRIDE |
ICA_REQ_DEFAULT )]
```

O

```
bind vpn vserver <name> -policy <string>  [-priority
<positive_integer>]
```

O

```
bind cr vserver <name> -policy <string> [-priority <positive _integer>]
```

### Argumentos

- **Supervisión de latencia**: Parámetro para habilitar o deshabilitar la supervisión de umbrales L7. Cuando este parámetro está habilitado, se envían notificaciones a HDX Insight cuando se cumplen las condiciones establecidas.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Valor predeterminado: DESHABILITADO

- **Factor de umbral de latencia**: Factor por el cual la latencia activa debe ser mayor que la latencia mínima observada para concluir que se ha superado el umbral y, por lo tanto, se debe enviar una notificación a HDX Insight.

  Valor predeterminado: 4

  Valor mínimo: 2

  Valor máximo: 65535

- **Tiempo de espera de latencia**: Tiempo en segundos que el dispositivo debe esperar después de que se supere el umbral de latencia para enviar una notificación a HDX Insight.

  Valor predeterminado: 20

  Valor mínimo: 1

  Valor máximo: 65535

- **LatencyNotifyInterval**: Intervalo de tiempo en segundos para que el dispositivo envíe notificaciones posteriores a HDX Insight una vez transcurrido el tiempo de espera.

  Valor predeterminado: 20

  Valor mínimo: 1

  Valor máximo: 65535

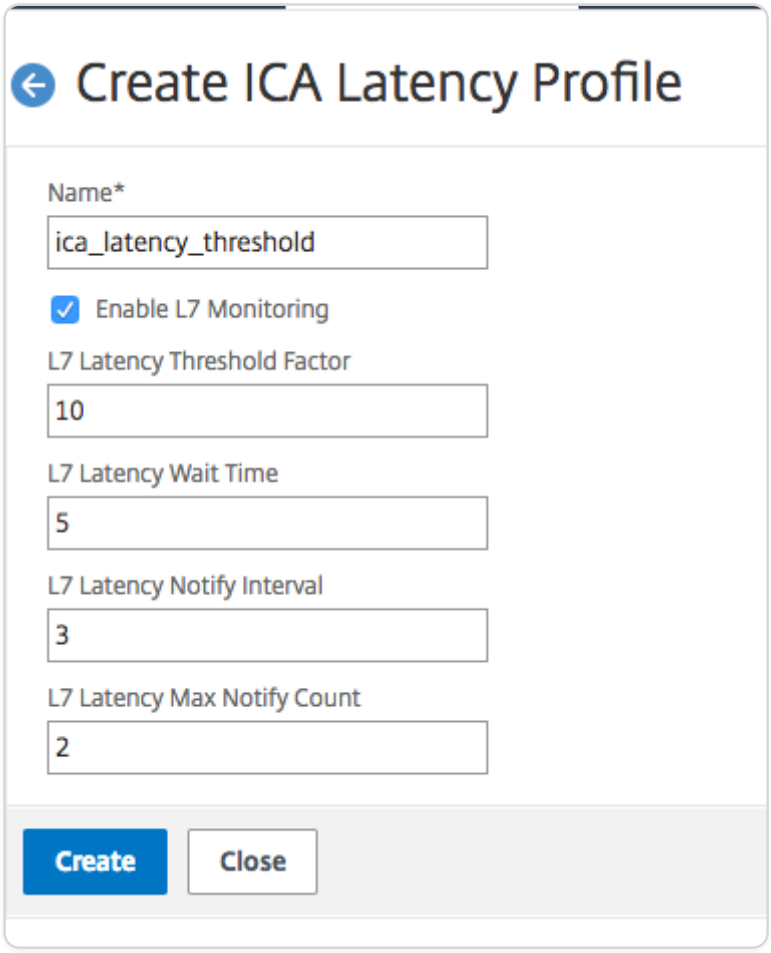
- **LatencyMaxNotifyCount**: Número máximo de notificaciones que se pueden enviar a HDX Insight dentro de un intervalo en el que la latencia supera el umbral.

  Valor predeterminado: 5

## Configurar el umbral de latencia L7 mediante la GUI

1. Vaya a **Configuración** > **NetScaler® Gateway** > **Directivas** > **ICA**.
2. Seleccione la ficha **Perfiles de latencia de ICA** y haga clic en **Agregar**.
3. En la página **Crear perfil de latencia de ICA**, realice lo siguiente.

© 1997–2026 Citrix Systems, Inc. All rights reserved.




- Seleccione **Supervisión de latencia L7** para habilitar la supervisión de umbrales L7.
- En **Factor de umbral L7**, introduzca el valor por el que la latencia activa debe superar la latencia mínima observada para enviar una notificación a HDX Insight.
- En **Tiempo de espera de latencia L7**, introduzca el tiempo en segundos que el dispositivo debe esperar después de que se supere el umbral para enviar una notificación a HDX Insight.
- En **Intervalo de notificación de latencia L7**, introduzca el tiempo en segundos para que el dispositivo envíe notificaciones posteriores a HDX Insight una vez transcurrido el tiempo de espera.
- En **Recuento máximo de notificaciones de latencia L7**, introduzca el número máximo de notificaciones que se pueden enviar a HDX Insight dentro de un intervalo en el que la latencia esté por encima del umbral. **Nota:** El recuento máximo de notificaciones de latencia L7 es aplicable una vez que se supera el umbral y se restablece cuando la latencia activa cae por debajo del umbral. La periodicidad de estas notificaciones se rige por el intervalo de notificación.

4. Haga clic en **Crear**.

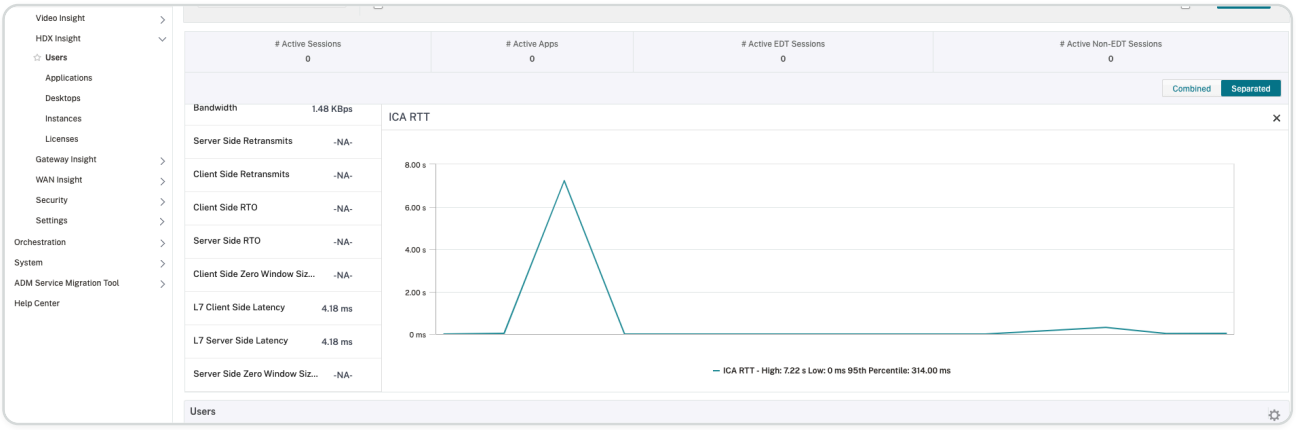
© 1997–2026 Citrix Systems, Inc. All rights reserved.

**IMPORTANTE:**

Después de configurar los parámetros del umbral de latencia L7, debe configurar HDX Insight. Para obtener más información, consulte Configurar NetScaler Gateway para admitir HDX Insight.

### Ver parámetros de latencia L7 en NetScaler ADM

Para ver los parámetros de latencia L7 en NetScaler ADM, vaya a **Analytics > HDX Insight > Aplicaciones** o **Analytics > HDX Insight > Usuarios**.



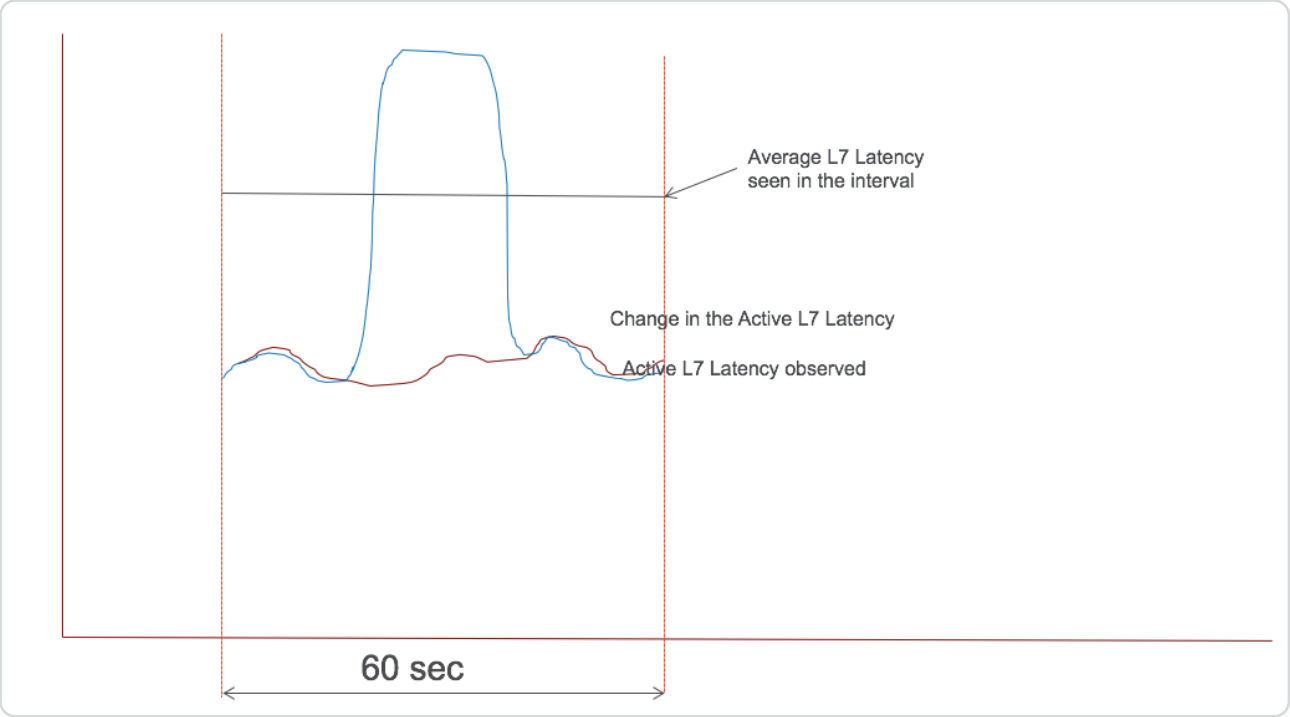

## El modelo de medición de latencia L7 frente al modelo de informes de umbral de latencia L7

### El modelo de medición de latencia L7

En el módulo de medición de latencia L7, los valores promedio de latencia L7 del lado del cliente y del lado del servidor se envían a HDX Insight cada 60 segundos. Como resultado, los picos observados dentro de este intervalo se promedian y, por lo tanto, no se detectan. Además, el módulo de medición de latencia L7 no tiene la capacidad de monitoreo de latencia en vivo.

La siguiente figura ilustra un modelo de medición de latencia L7 de ejemplo.

© 1997–2026 Citrix Systems, Inc. All rights reserved.




### Modelo de informes de umbral de latencia L7

El modelo de informes de umbral de latencia L7 tiene la capacidad de monitoreo de latencia en vivo para detectar picos. Se envían notificaciones a HDX Insight si la latencia supera la latencia mínima observada.

Siempre que se supera un factor de umbral, se detecta el aumento de la latencia. Una vez que expira el tiempo de espera del umbral configurado, se envía una notificación a HDX Insight. Se envía una notificación posterior a HDX Insight después de que haya expirado el tiempo de espera y el factor de umbral aún se supere. En caso de que el valor de latencia caiga por debajo del factor de umbral antes de que expire el tiempo de espera, no se envía ninguna notificación a HDX Insight.

La siguiente figura ilustra un modelo de informe de umbral de latencia L7 de ejemplo.

Informe de umbral de ICA(/en-us/netscaler-gateway/media/l7-latency-threshold-reporting-model.png)

Los siguientes parámetros se pueden configurar en tiempo de ejecución:

- Supervisión de umbral (ACTIVADO/DESACTIVADO)
- Factor de umbral
- Tiempo de espera del umbral
- Intervalo de notificación

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Recuento máximo de notificaciones

© 1997–2026 Citrix Systems, Inc. All rights reserved.

# Proxy RDP

La funcionalidad de proxy RDP se proporciona como parte de NetScaler Gateway. En una implementación típica, el cliente RDP se ejecuta en la máquina de un usuario remoto. El dispositivo NetScaler Gateway se implementa dentro de la DMZ y la granja de servidores RDP se encuentra en la red corporativa interna.

El usuario remoto;

1. se conecta a la dirección IP pública de NetScaler Gateway
2. establece una conexión VPN SSL
3. se autentica
4. accede a los escritorios remotos a través del dispositivo NetScaler Gateway

La función de proxy RDP es compatible con los modos VPN sin cliente y proxy ICA®.

**NOTA:**

NetScaler Gateway no es compatible con Remote Desktop Session Host (RDSH), Remote App, RDS multiusuario, sesiones RDP o aplicaciones RDP.

Las siguientes funciones de proxy RDP proporcionan acceso a una granja de escritorios remotos a través de NetScaler Gateway.

- Asegure el tráfico RDP a través de VPN sin cliente o el modo proxy ICA (sin túnel completo).
- SSO (inicio de sesión único) a servidores RDP a través de NetScaler Gateway. También proporciona una opción para deshabilitar el SSO si es necesario.

  **NOTA:**

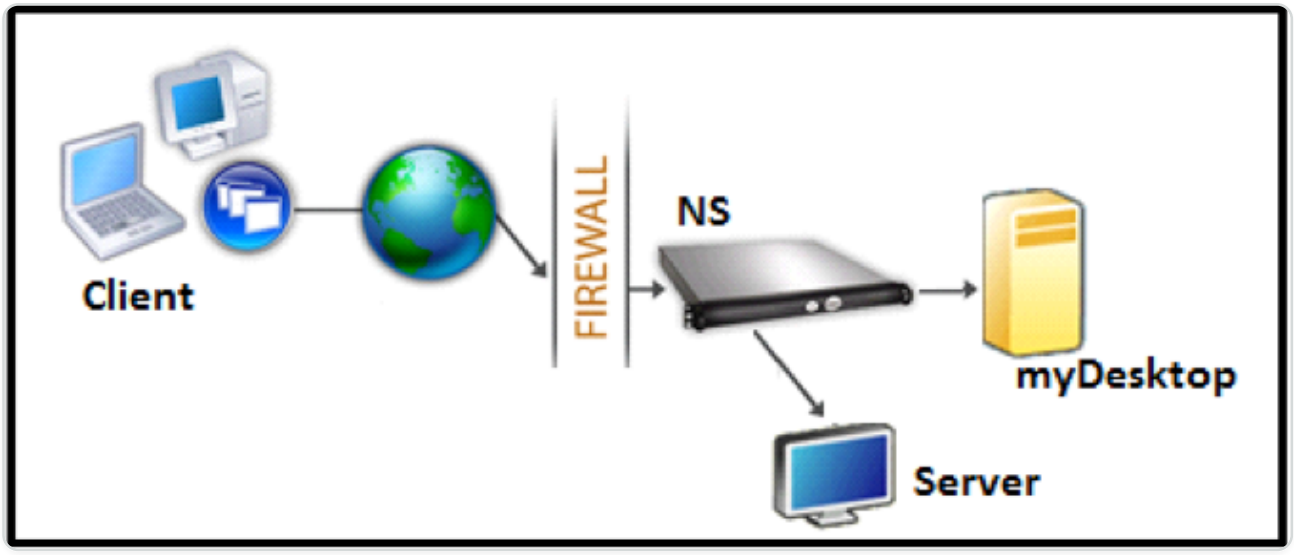
  NetScaler Gateway no es compatible con la delegación restringida de Kerberos (KCD) para SSO en servidores RDP.

- Función de aplicación (SmartAccess), donde los administradores de NetScaler pueden deshabilitar ciertas capacidades RDP a través de la configuración de NetScaler Gateway.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Solución de Gateway único/sin estado (dual) para todas las necesidades (VPN/ICA/RDP/Citrix Endpoint Management).
- Compatibilidad con el cliente MSTSC nativo de Windows para RDP sin necesidad de clientes personalizados.
- Uso del cliente RDP existente proporcionado por Microsoft en macOS, iOS y Android.

La siguiente figura muestra una descripción general de la implementación:




## Implementación a través de VPN sin cliente

En este modo, los enlaces RDP se publican en la página de inicio o portal de Gateway, como marcadores, a través de la configuración `add vpn url` o a través de un portal externo. El usuario puede hacer clic en estos enlaces para obtener acceso al Escritorio remoto.

## Implementación a través de proxy ICA

En este modo, se configura una página de inicio personalizada en el VIP de Gateway mediante el parámetro `wihome`. Esta página de inicio se puede personalizar con la lista de recursos de escritorio remoto a los que el usuario tiene permitido acceder. Esta página personalizada se puede alojar en NetScaler o, si es externa, puede ser un iFrame en la página del portal de Gateway existente. Para obtener más información, consulte Configurar interfaz de acceso.

En cualquiera de los modos, después de que el usuario hace clic en el enlace o icono RDP aprovisionado, una solicitud HTTPS para el recurso correspondiente llega a NetScaler Gateway. El Gateway genera el contenido del archivo RDP para la conexión solicitada y lo envía al cliente. Se invoca el cliente RDP nativo, que se conecta a un oyente RDP en Gateway. Gateway realiza SSO al servidor RDP al admitir la aplicación (SmartAccess). El gateway bloquea el acceso del cliente a

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ciertas funciones RDP, según la configuración de NetScaler, y luego actúa como proxy para el tráfico RDP entre el cliente RDP y el servidor.

# Detalles de la aplicación

El administrador de NetScaler puede configurar ciertas capacidades RDP a través de la configuración de NetScaler Gateway. NetScaler Gateway proporciona la función de "aplicación RDP" para parámetros RDP importantes. NetScaler garantiza que el cliente no pueda habilitar los parámetros bloqueados. Si los parámetros bloqueados están habilitados, la función de aplicación RDP anula los parámetros habilitados por el cliente y no se respetan.

**IMPORTANTE:**

La función de aplicación solo es aplicable si SSO está habilitado.

## Parámetros RDP admitidos para la aplicación

Se admite la aplicación de los siguientes parámetros de redirección. Estos parámetros se pueden configurar como parte de un perfil de cliente RDP.

- Redirección del portapapeles
- Redirección de impresoras
- Redirección de unidades de disco
- Redirección de puertos COM
- Redirección de dispositivos PNP

## Flujo de conexión

El flujo de conexión se puede dividir en dos pasos:

- Enumeración de recursos RDP y descarga de archivos RDP.
- Inicio de la conexión RDP.

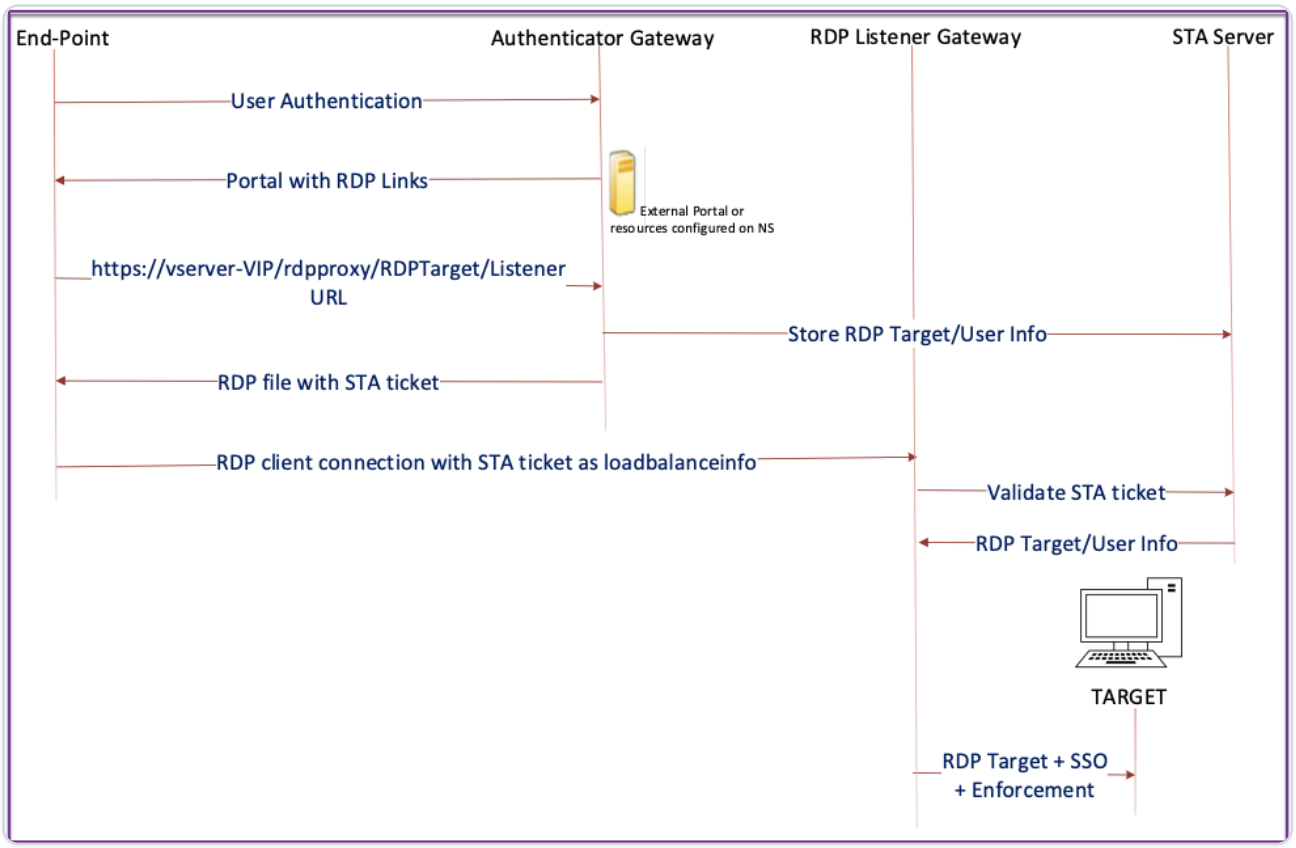
Según el flujo de conexión anterior, existen dos soluciones de implementación:

- Solución de puerta de enlace sin estado (dual): la enumeración de recursos RDP y la descarga de archivos RDP se realizan a través de la puerta de enlace de autenticación, pero el inicio de la conexión RDP se realiza a través de la puerta de enlace del oyente RDP.
- Solución de puerta de enlace única: la enumeración de recursos RDP, la descarga de archivos RDP y el inicio de la conexión RDP se realizan a través de la misma puerta de enlace.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

# Compatibilidad con puerta de enlace sin estado (dual)

La siguiente figura muestra la implementación:




- Un usuario se conecta a la VIP de la puerta de enlace del autenticador y proporciona las credenciales.
- Después de iniciar sesión correctamente en la puerta de enlace, el usuario es redirigido a la página de inicio o al portal externo, que enumera los recursos de escritorio remoto a los que el usuario puede acceder.
- Una vez que el usuario selecciona un recurso RDP, la VIP de la puerta de enlace del autenticador recibe la solicitud en el formato `https://vserver-vip/rdpproxy/rdptarget/listener` indicando el recurso publicado en el que hizo clic el usuario. Esta solicitud contiene la información sobre la dirección IP y el puerto del servidor RDP que el usuario ha seleccionado.
- La puerta de enlace del autenticador procesa la solicitud /rdpproxy/. Dado que el usuario ya está autenticado, esta solicitud viene con una cookie de Gateway válida.
- La información de `RDPTarget` y `RDPUser` se almacena en el servidor STA y se genera un ticket STA. La información almacenada en el servidor STA se cifra utilizando la clave precompartida configurada. La puerta de enlace del autenticador utiliza uno de los servidores STA que está configurado en el servidor virtual de la puerta de enlace.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- La información de 'Listener' obtenida en la solicitud /rdpproxy/ se coloca en `.rdp file` como "`fulladdress`", y el ticket STA (precedido por el STA AuthID) se coloca en `.rdp file` como "`loadbalanceinfo`".
- El `.rdp file` se envía de vuelta al punto final del cliente.
- El cliente RDP nativo se inicia y se conecta a `RDPListener Gateway`. Envía el ticket STA en el paquete inicial.

  La puerta de enlace `RDPListener` valida el ticket STA y obtiene la información de `RDPTarget` y `RDPUser`. El servidor STA que se utilizará se recupera utilizando el 'AuthID' presente en `loadbalanceinfo`.
- Se crea una sesión de puerta de enlace para almacenar políticas de autorización/auditoría. Si ya existe una sesión para el usuario, se reutiliza.
- La puerta de enlace `RDPListener` se conecta a `RDPTarget` e inicia sesión única utilizando CREDSSP.

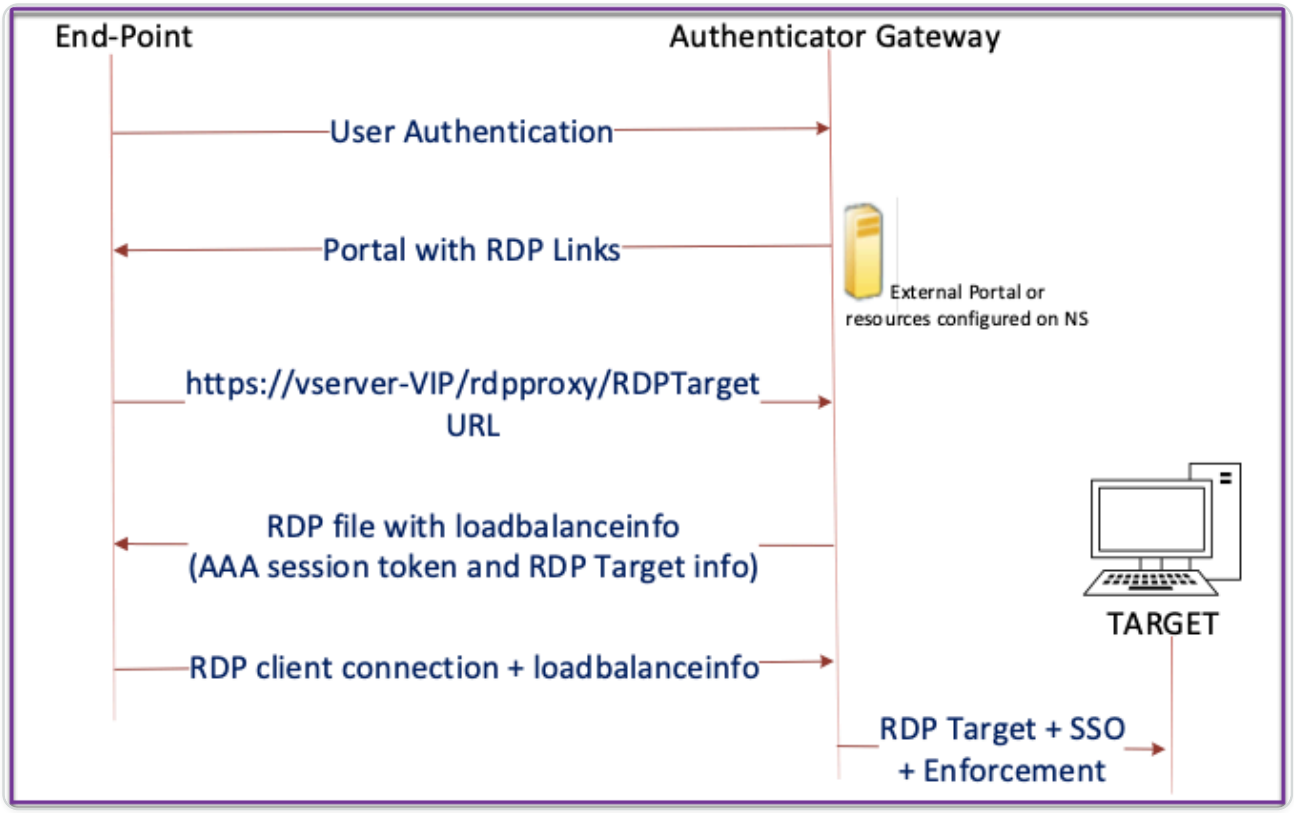
**IMPORTANTE:**

- Para el proxy RDP sin estado, el servidor STA valida el ticket STA, enviado por el cliente RDP, para obtener la información de `RDPTarget/RDPUser`. Debe enlazar el servidor STA además del servidor virtual VPN.
- Para que el agente de escucha RDP funcione correctamente, el puerto especificado en el perfil del servidor RDP debe estar abierto en el firewall del cliente. Esto permite que NetScaler Gateway se comunique con los servidores RDP de backend.

## Compatibilidad con una única puerta de enlace

La siguiente figura muestra la implementación:

© 1997–2026 Citrix Systems, Inc. All rights reserved.




**IMPORTANTE:**

- En el caso de una implementación de puerta de enlace única, el servidor STA no es necesario. La puerta de enlace autenticadora codifica `RDPTarget` y la cookie de sesión de autenticación, autorización y auditoría de NetScaler de forma segura y los envía como `loadbalanceinfo` en `.rdp file`. Cuando el cliente RDP envía este token en el paquete inicial, la puerta de enlace autenticadora decodifica la información `RDPTarget`, busca la sesión y se conecta a `RDPTarget`.
- En una implementación de puerta de enlace única, un perfil de servidor RDP es obligatorio y no se requiere un agente de escucha RDP.

## Compatibilidad con un único agente de escucha

- Agente de escucha único para tráfico RDP y SSL.
- La descarga de archivos RDP y el tráfico RDP se pueden gestionar a través de la misma tupla de 2 (es decir, IP y puerto) en el dispositivo NetScaler.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

# Requisitos de licencia para RDP Proxy

Edición Premium, Edición Advanced

**NOTA:**

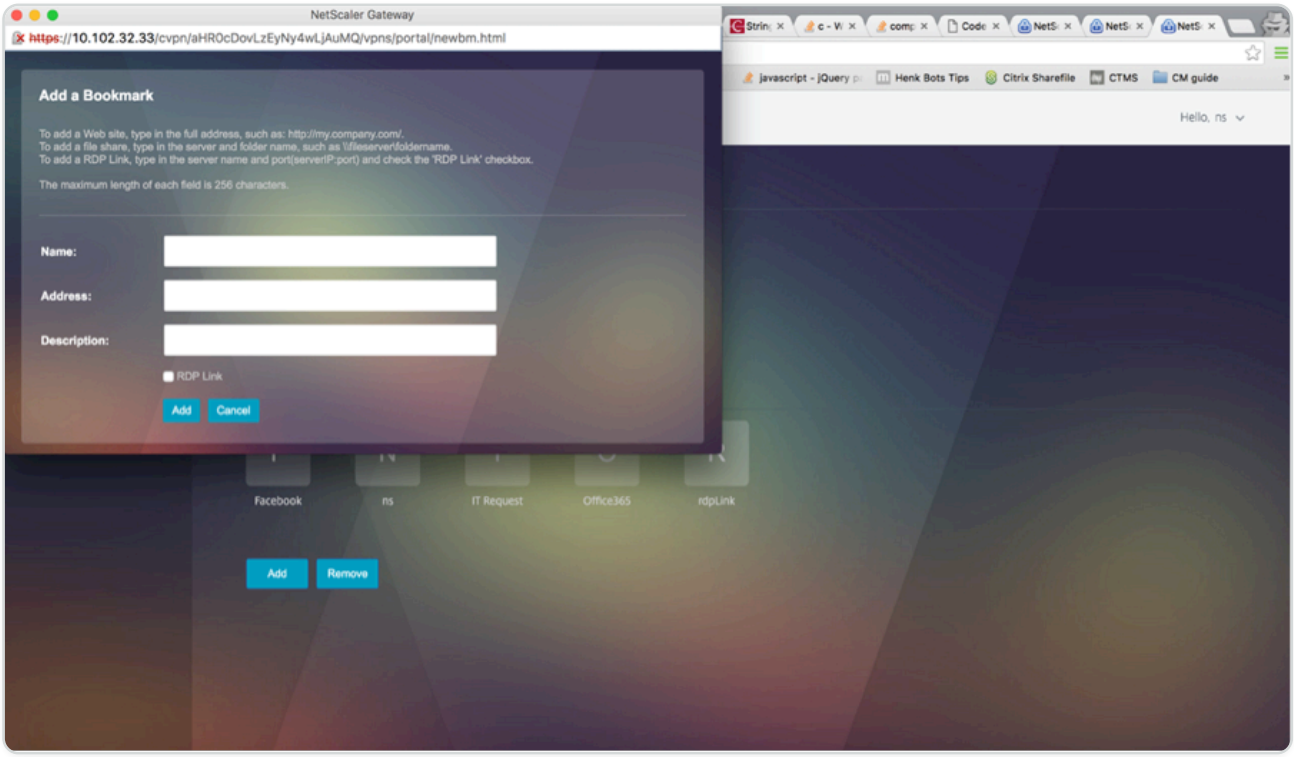
La función de RDP Proxy no está disponible para los clientes que solo tienen una licencia de plataforma Gateway o solo la edición Standard.

Puede utilizar el siguiente comando para habilitar el proxy RDP.

```
enable feature rdpProxy
```

# Marcador

**Generación de enlaces RDP a través del portal.** En lugar de configurar los enlaces RDP para el usuario o publicarlos a través de un portal externo, puede dar a los usuarios la opción de generar sus propias URL proporcionando `targetIP:Port`. Para la implementación de proxy RDP sin estado, el administrador puede incluir información del oyente RDP en formato FQDN:Puerto como parte del perfil de cliente RDP. Esto se hace bajo la opción `rdpListener`. Esta configuración se utiliza para la generación de enlaces RDP a través del portal en modo Dual Gateway.




© 1997–2026 Citrix Systems, Inc. All rights reserved.

### Crear marcadores

1. Cree marcadores en la página del portal para acceder a los recursos RDP: (La URL real comienza con `rdp`://).
2. Añadir URL VPN `<urlName> <linkName>  <actualURL>`
   - La URL debe tener el siguiente formato: `rdp://<TargetIP:Port>`.
   - Para el modo de proxy RDP sin estado, la URL debe tener el siguiente formato: `rdp://<TargetIP:Port>/<ListenerIP:Port>`
   - La URL se publica en el portal en el formato: `https://<VPN-VIP>/rdpproxy/<TargetIP:Port>` `https://<VPN-VIP>/rdpproxy/<TargetIP:Port>/<ListenerIP:Port>`
3. Vincule los marcadores al usuario, o grupo, o al servidor virtual VPN, o VPN global.

### Funciones y modos que deben habilitarse para el proxy RDP

```
-  enable ns feature ssl



-  enable ns feature sslvpn



-  enable ns feature rdpproxy



-  enable mode usnip
```

## Pasos de configuración de alto nivel del proxy RDP

Los siguientes son los pasos de alto nivel involucrados en la configuración del proxy RDP sin estado.

- Crear un perfil de servidor RDP
- Crear un perfil de cliente RDP
- Crear y vincular un servidor virtual

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Crear un marcador
- Crear o editar un perfil o política de sesión
- Vincular un marcador

## Configurar un perfil de cliente

Configure el perfil de cliente en el gateway autenticador. La siguiente es una configuración de ejemplo:

```
add rdpClient profile <name> [-addUserNameInRdpFile ( YES | NO )] [-
audioCaptureMode ( ENABLE | DISABLE )] [-keyboardHook <keyboardHook>] [-
multiMonitorSupport ( ENABLE | DISABLE )] [-psk <string>] [-
rdpCookieValidity <positive_integer>] [-rdpCustomParams <string>] [-
rdpFileName <string>] [-rdpHost <optional FQDN that will be put in the RDP
file as 'fulladdress>] [-rdpUrlOverride ( ENABLE | DISABLE )] [-
redirectClipboard ( ENABLE | DISABLE )] [-redirectComPorts ( ENABLE |
DISABLE )] [-redirectDrives ( ENABLE | DISABLE )] [-redirectPnpDevices
( ENABLE | DISABLE )] [-redirectPrinters ( ENABLE | DISABLE )] [-
videoPlaybackMode ( ENABLE | DISABLE )]
```

Asocie el perfil de cliente RDP con el servidor virtual VPN.

Esto se puede hacer configurando un sessionAction+sessionPolicy o estableciendo el parámetro VPN global.

Ejemplo:

```
add vpn sessionaction <actname> -rdpClientprofile <rdpprofilename>



add vpn sessionpolicy <polname> NS_TRUE <actname>



bind vpn vserver <vservername> -policy <polname> -priority
<prioritynumber>
```

O

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
set vpn parameter –rdpClientprofile <name>
```

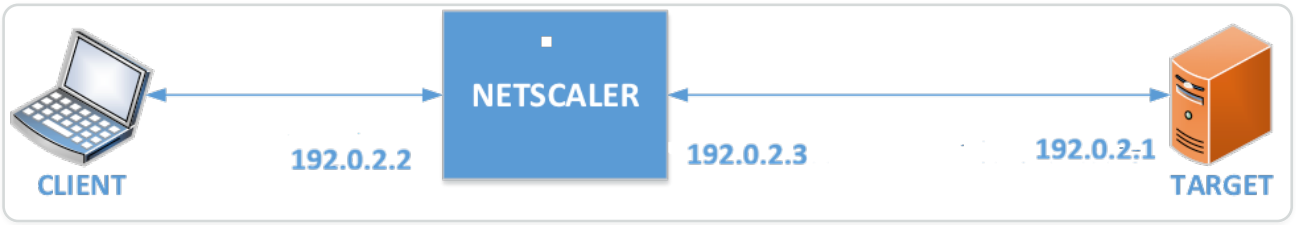
### Configurar un perfil de servidor

Configure el perfil de servidor en el gateway de escucha.

```
add rdp ServerProfile <profilename> -rdpIP <IPV4 address of the RDP
listener> -rdpPort <port for terminating RDP client connections> -psk <key
to decrypt RDPTarget/RDPUser information, needed while using STA>`
```

El `rdp ServerProfile` debe configurarse en el servidor virtual VPN.

```
add vpn vserver v1 SSL <publicIP> <portforterminatingvpnconnections>
-rdpServerProfile <rdpServer Profile>`
```




## Configuración del proxy RDP mediante la CLI

La siguiente es una configuración de proxy RDP de ejemplo mediante la CLI.

- Agregue la URL de VPN para el usuario con la información de destino.

```
add aaa user Administrator –password freebsd123$%^


add vpn url rdp RdpLink rdp://rdpserverinfo


add dns addrec rdpserverinfo 192.0.2.1
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
bind aaa user Administrator  –urlName rdp
```

- Configure el perfil de cliente y servidor RDP para la conexión VPN.

```
add rdp clientprofile p1 –psk citrix -redirectClipboard ENABLE


add rdp serverprofile p1 -rdpIP 192.0.2.2 -psk citrix


add vpn vserver mygateway SSL  192.0.2.2 443 –rdpserverprofile p1


set vpn parameter -clientlessVpnMode ON -defaultAuthorizationAction
ALLOW -rdpClientProfileName p1


add ssl certKey gatewaykey -cert rdp_rootcert.pem  -key rdp_rootkey


bind ssl vserver mygateway -certkeyName gatewaykey
```

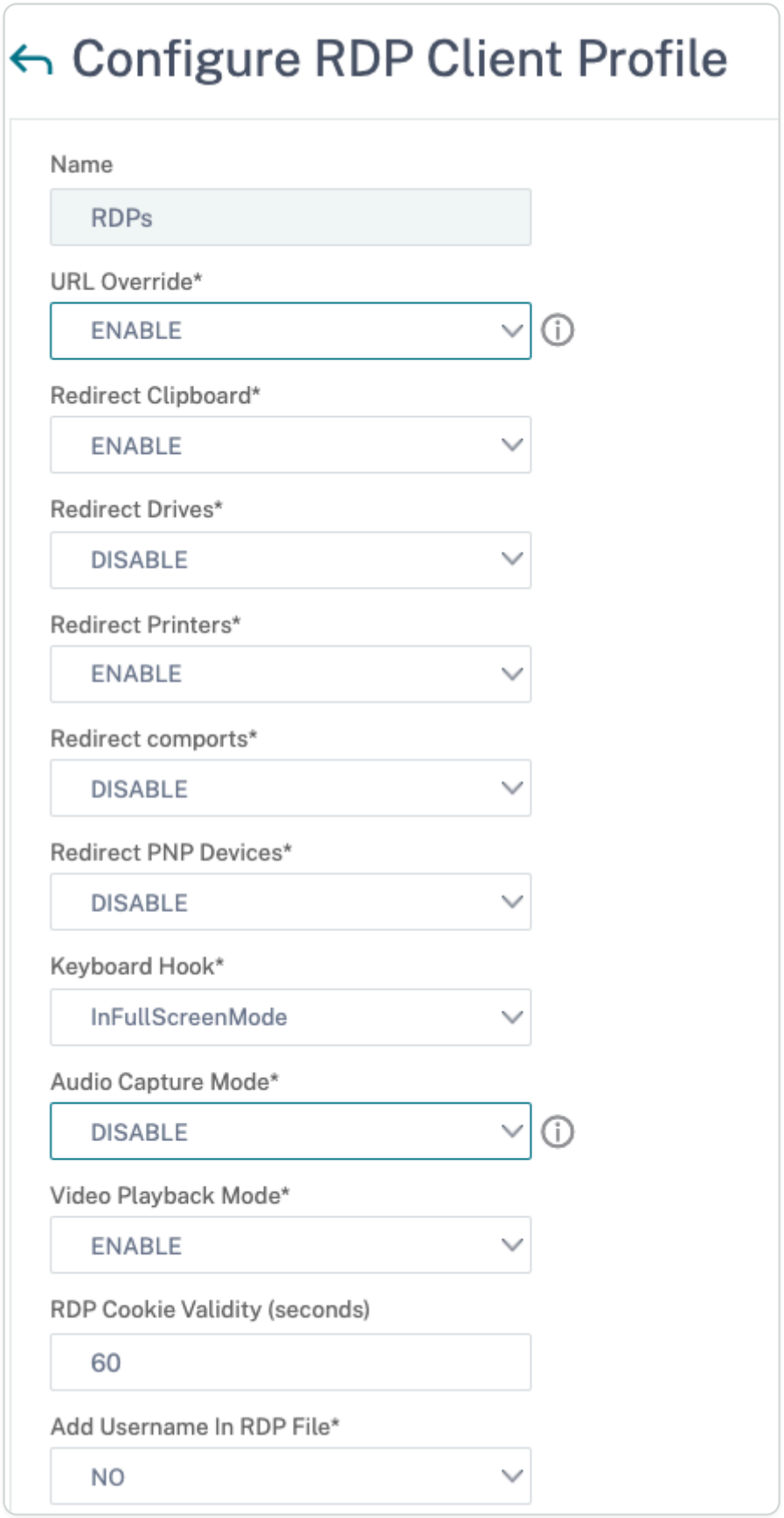
- AGREGUE SNIP para la conexión de NetScaler al destino.

```
add ns ip 192.0.2.3  255.255.255.0 –type SNIP
```

## Configuración del proxy RDP mediante la GUI

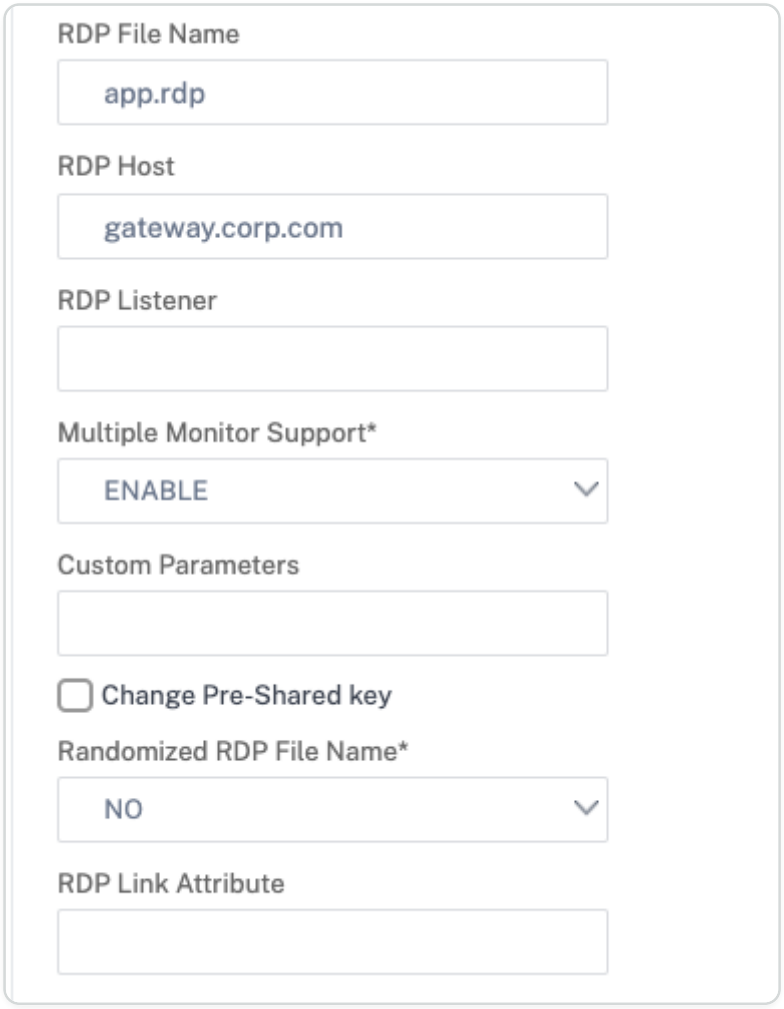
1. Vaya a **NetScaler Gateway > Directivas**, haga clic con el botón derecho en **RDP** y haga clic en **Habilitar función**.
2. Haga clic en RDP en el panel de navegación. A la derecha, seleccione la ficha **Perfiles de cliente** y haga clic en **Agregar**.
3. Introduzca un nombre para el perfil de cliente y configúrelo.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



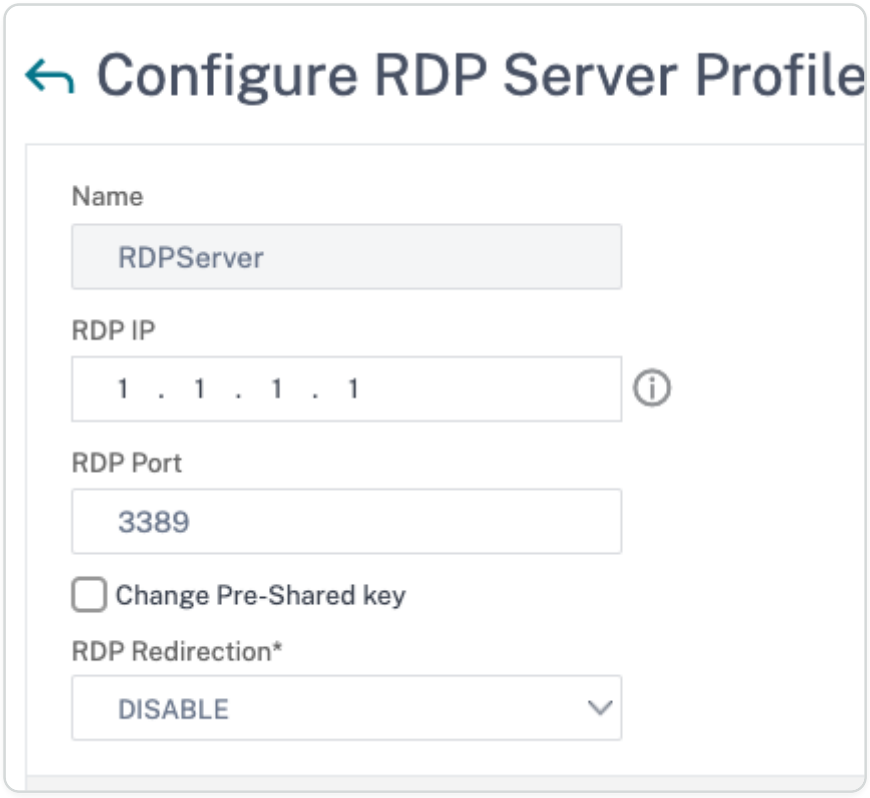

4. En el campo Host RDP, introduzca el FQDN que se resuelve en el agente de escucha del proxy RDP, que suele ser el mismo FQDN que el FQDN del dispositivo NetScaler Gateway.
5. En **Clave precompartida**, introduzca una contraseña y haga clic en **Aceptar**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



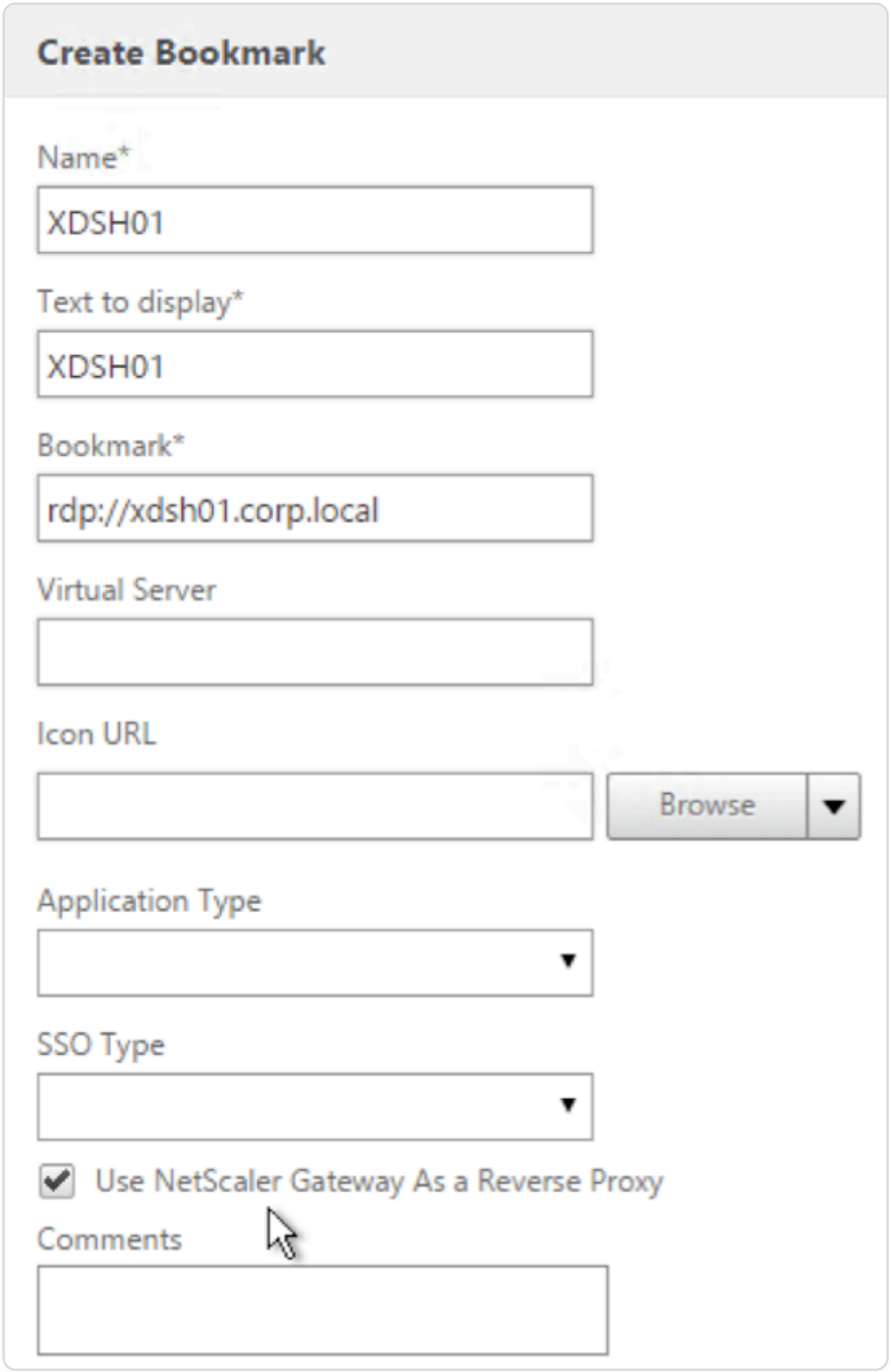

6. Introduzca un nombre para el perfil de servidor.
7. Introduzca la dirección IP del servidor virtual de puerta de enlace al que va a vincular este perfil.
8. Introduzca la misma clave precompartida que configuró para el perfil de cliente RDP. Haga clic en **Crear**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



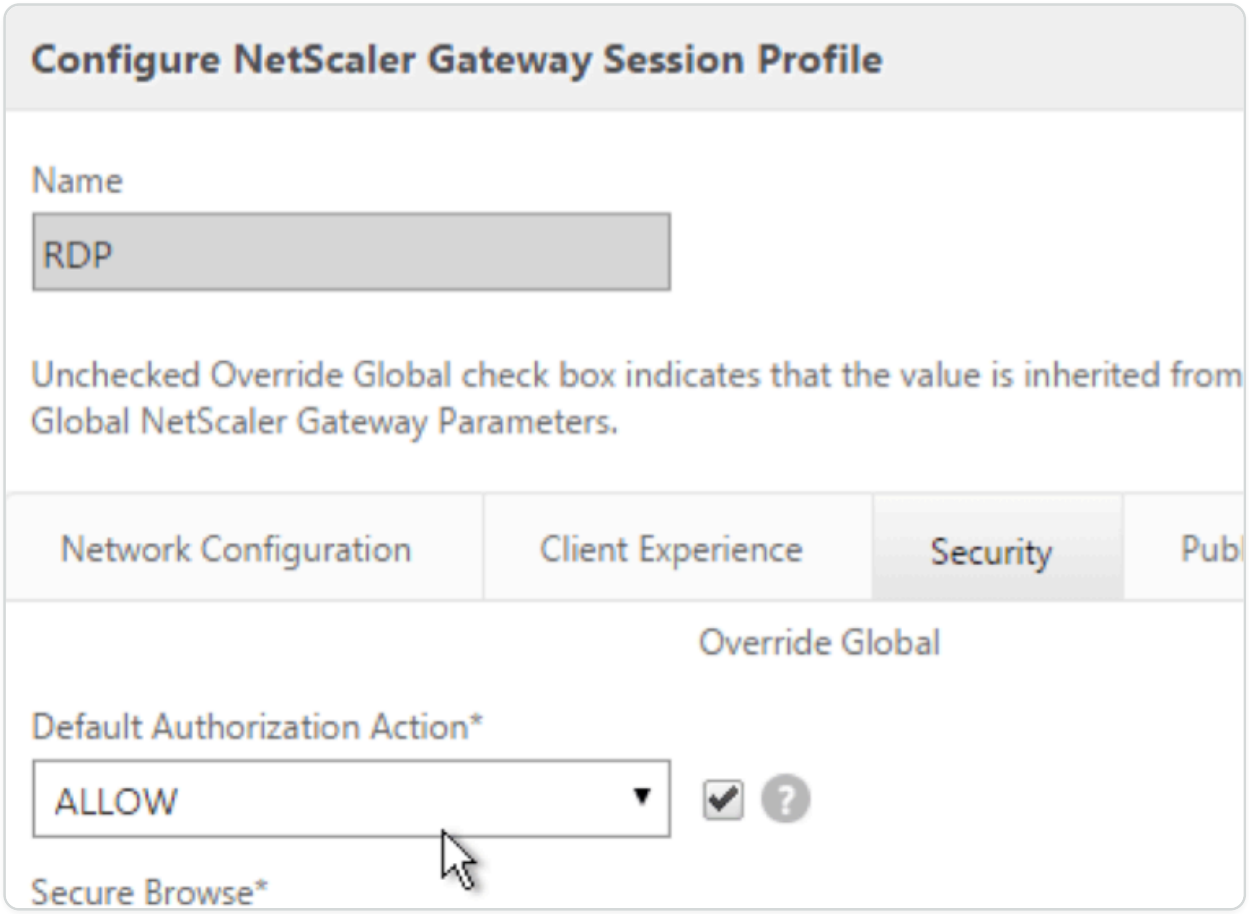

9. Si desea agregar marcadores RDP en la página del portal de acceso sin cliente, a la izquierda, expanda **NetScaler Gateway**, expanda **Resources** y haga clic en **Bookmarks**.
10. A la derecha, haga clic en **Add**.
11. Asigne un nombre al marcador.
12. Para la URL, introduzca **rdp://MyRDPServer using IP or DNS**.
13. Seleccione Usar **NetScaler Gateway As a Reverse Proxy** y haga clic en **Create**.
14. Cree marcadores según sus requisitos.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

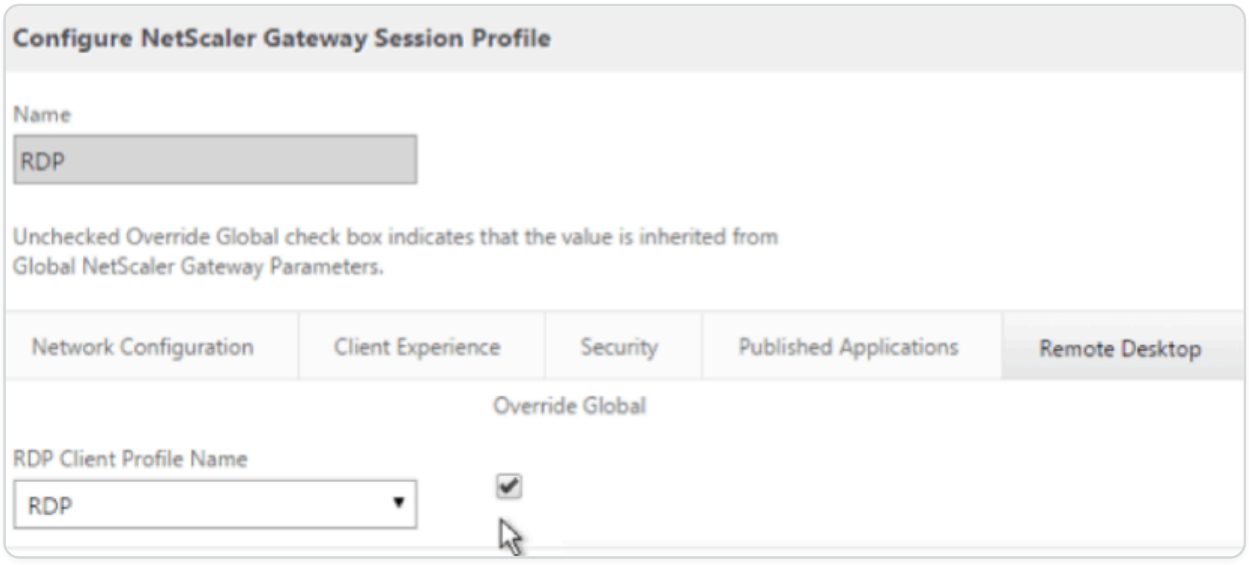



15. Cree o edite un perfil de sesión. Vaya a **NetScaler Gateway > Policies > Session**.
16. En la ficha Seguridad, establezca **Default Authorization Action** en **ALLOW**. O bien, puede usar directivas de autorización para controlar el acceso.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

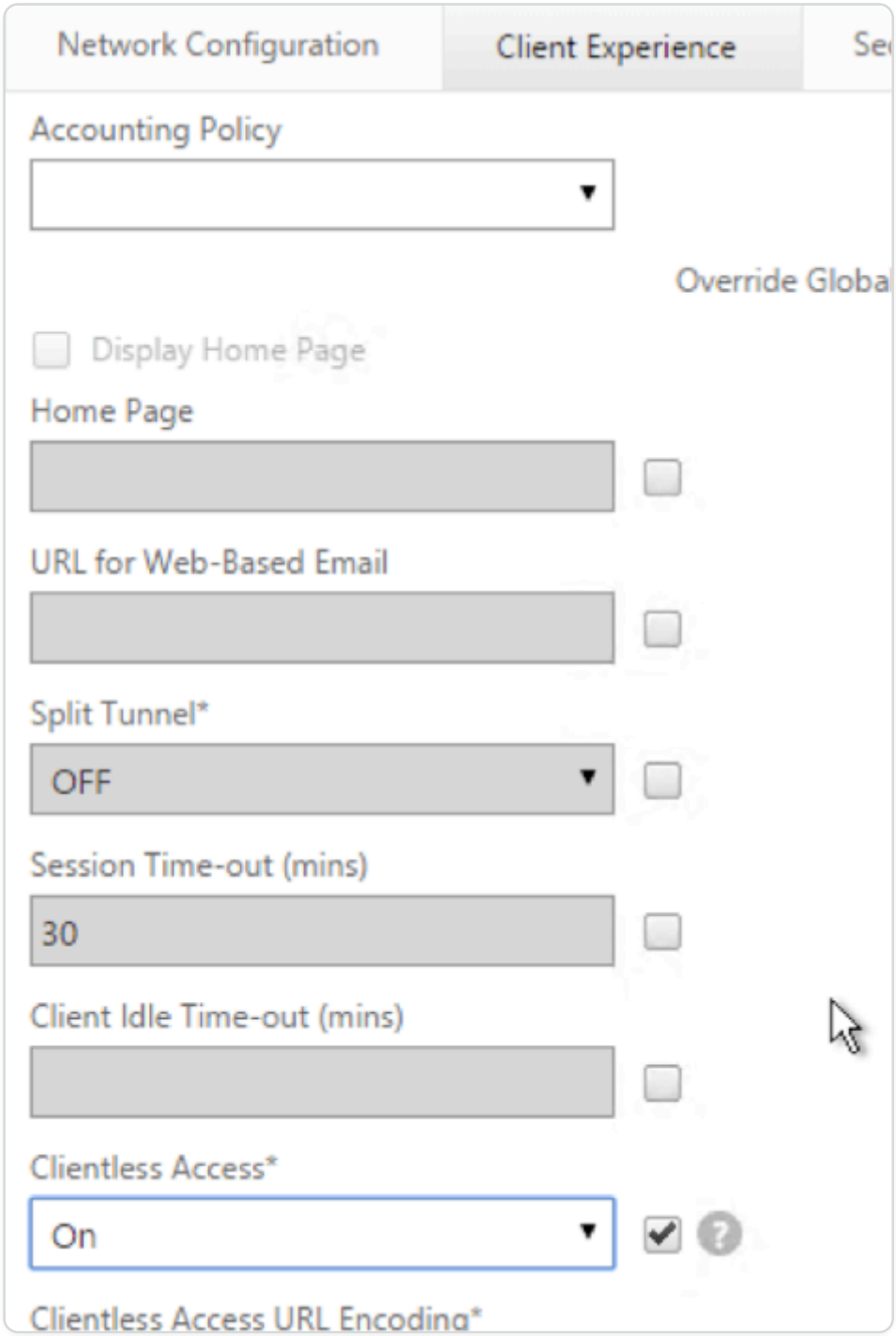



17. En la ficha Escritorio remoto, seleccione el perfil de cliente RDP que creó anteriormente.

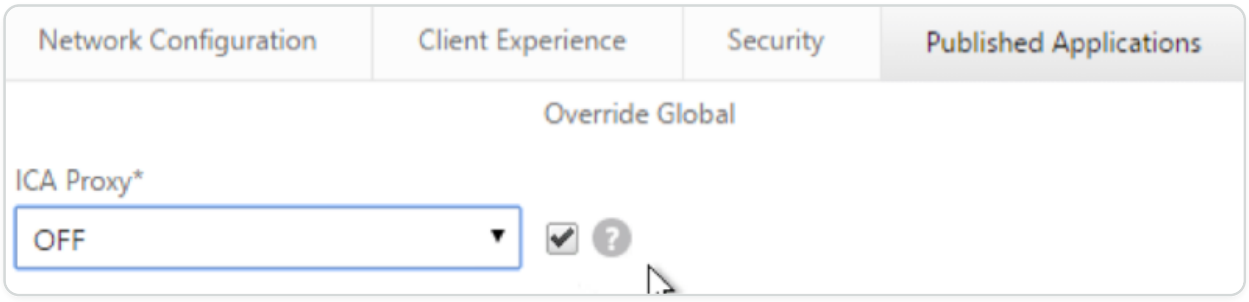



18. Si desea usar marcadores, en la ficha **Client Experience**, establezca **Clientless Access** en **On**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

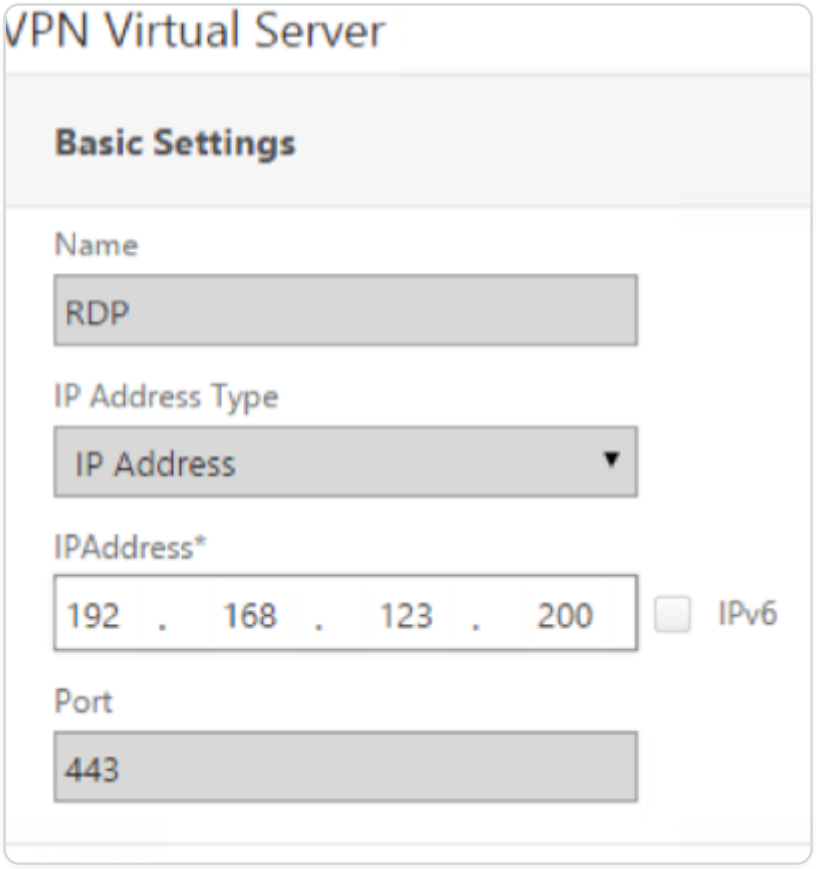



19. En la ficha **Published Applications**, asegúrese de que ICA Proxy esté **DESACTIVADO**.



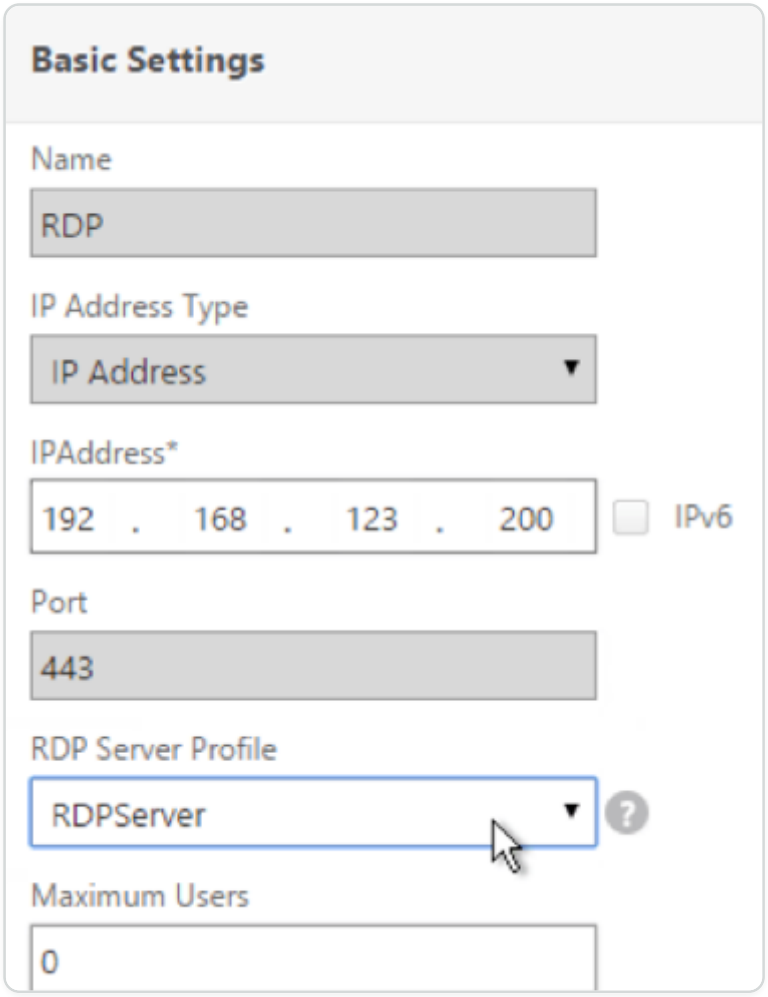

20. Modifique o cree su servidor virtual de gateway.
21. En la sección **Configuración básica**, haga clic en **Más**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

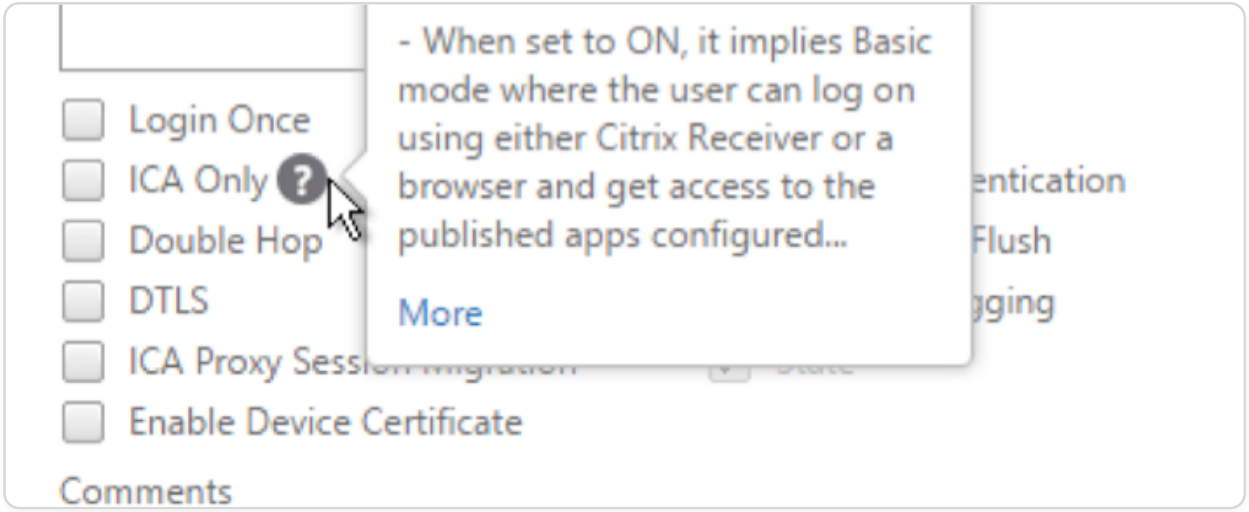



22. Utilice la lista de perfiles de servidor RDP para seleccionar el perfil de servidor RDP que creó anteriormente.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

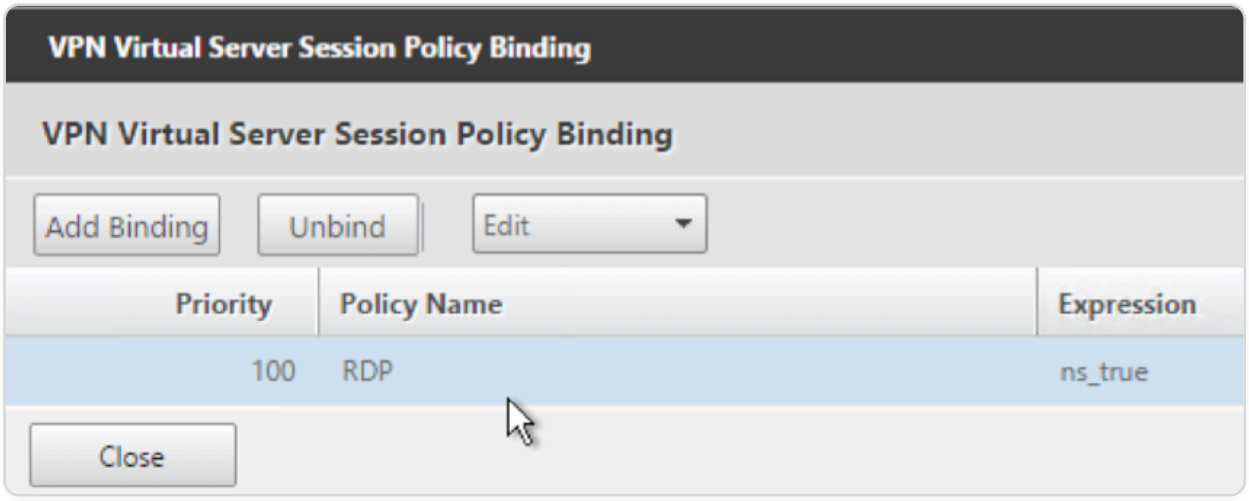



23. Desplácese hacia abajo. Asegúrese de que **Solo ICA** no esté marcado.



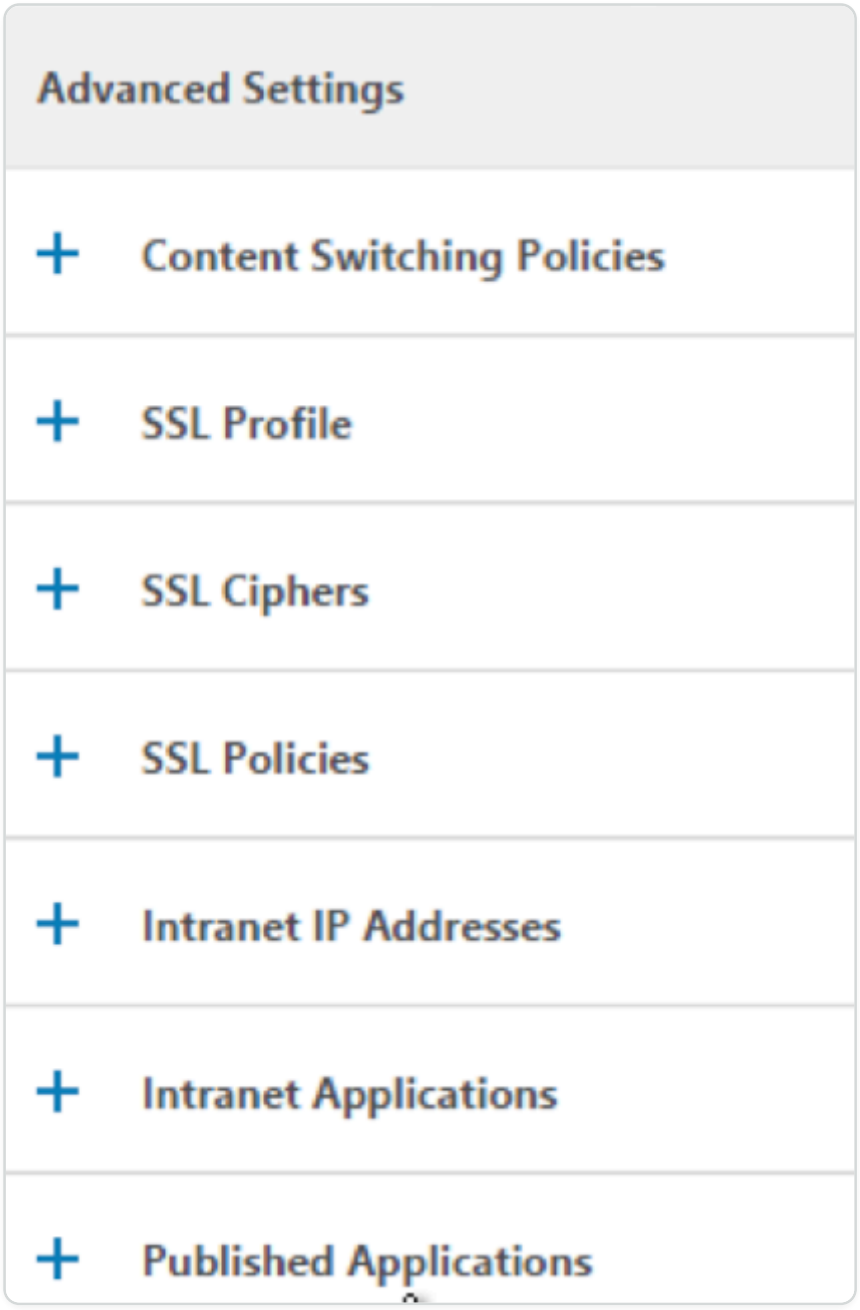

24. Enlazar un certificado.
25. Enlazar directivas de autenticación.
26. Enlace la directiva/perfil de sesión que tiene configurado el perfil de cliente RDP.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



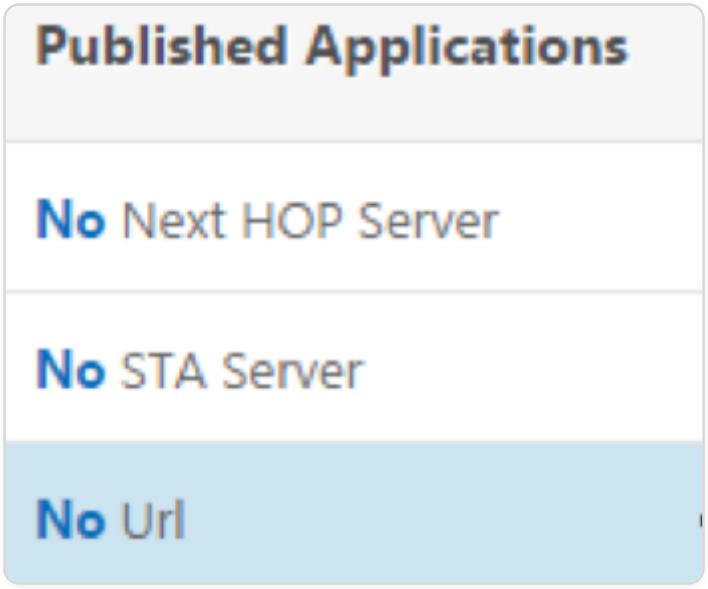

27. Puede enlazar marcadores al servidor virtual de NetScaler Gateway o a un grupo de autenticación, autorización y auditoría. Para enlazar al servidor virtual de NetScaler Gateway, a la derecha, en la sección Configuración avanzada, haga clic en **Aplicaciones publicadas**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

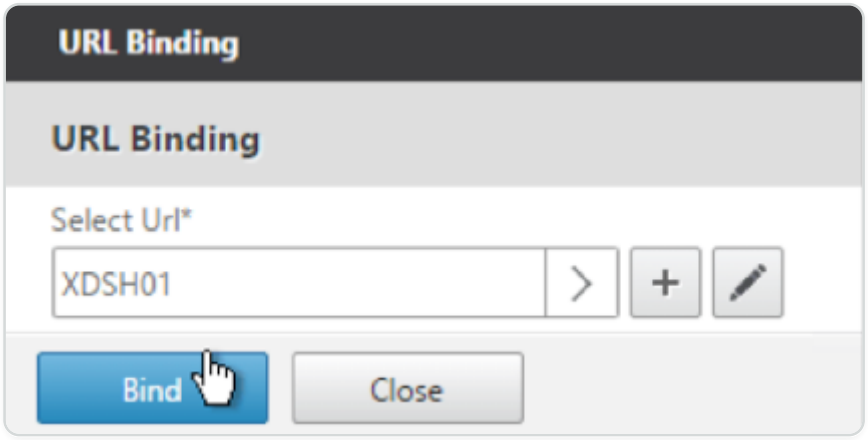



28. A la izquierda, en la sección **Aplicaciones publicadas**, haga clic en **Sin URL**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

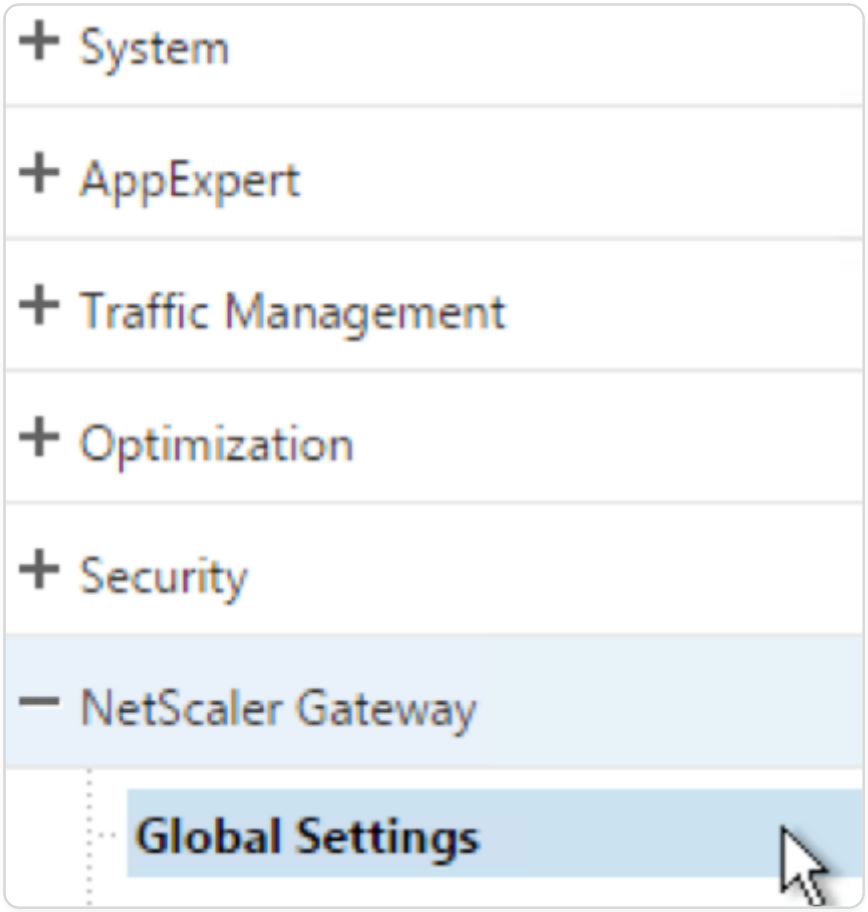



29. Enlace sus marcadores.

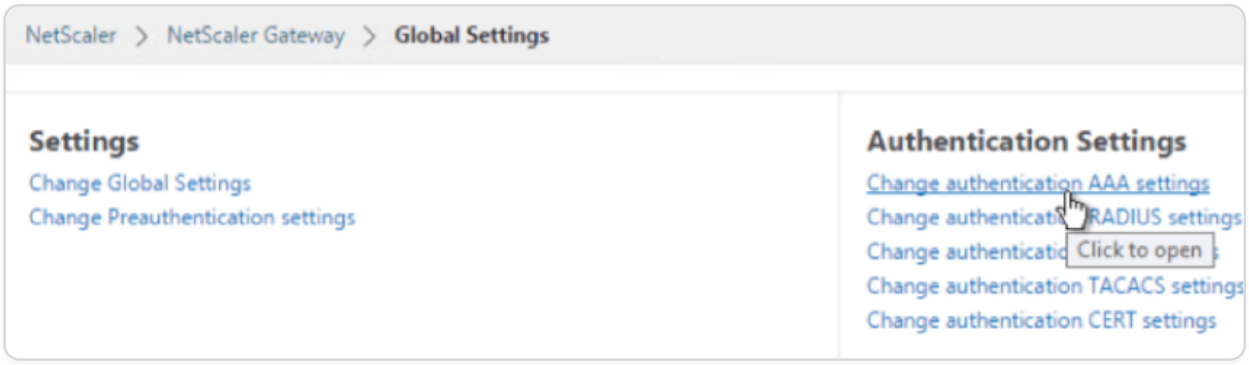



30. Dado que ICA Only no está especificado para este servidor virtual de NetScaler Gateway, asegúrese de que sus licencias universales de NetScaler Gateway estén configuradas correctamente. A la izquierda, expanda **NetScaler Gateway** y haga clic en **Global Settings**.

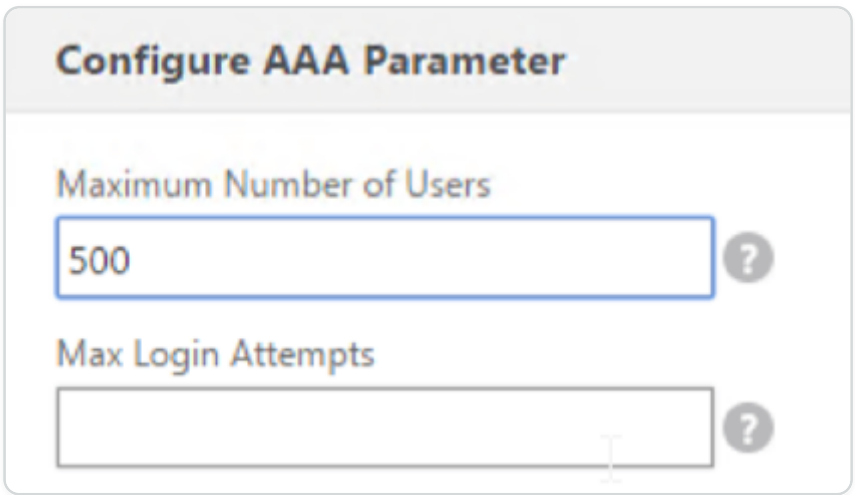
© 1997–2026 Citrix Systems, Inc. All rights reserved.




31. A la derecha, haga clic en **Change authentication AAA settings**.

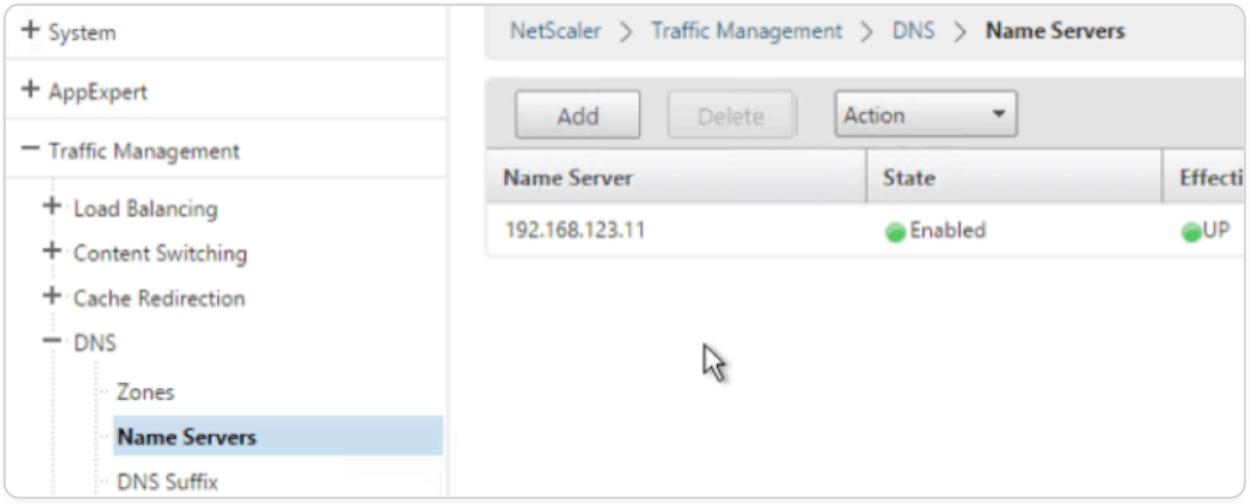



32. Cambie el **Maximum Number of Users** a su límite de licencia.

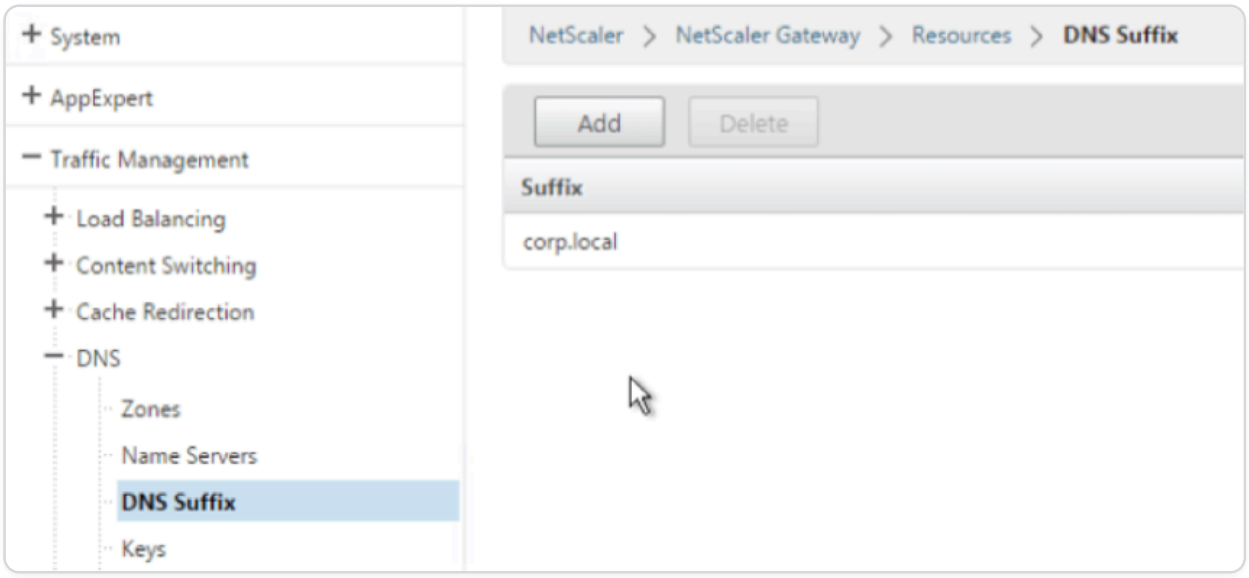



© 1997–2026 Citrix Systems, Inc. All rights reserved.

33. Si quiere conectarse a servidores RDP mediante DNS, asegúrese de que los servidores DNS estén configurados en el dispositivo (**Traffic Management > DNS > Name Servers**).

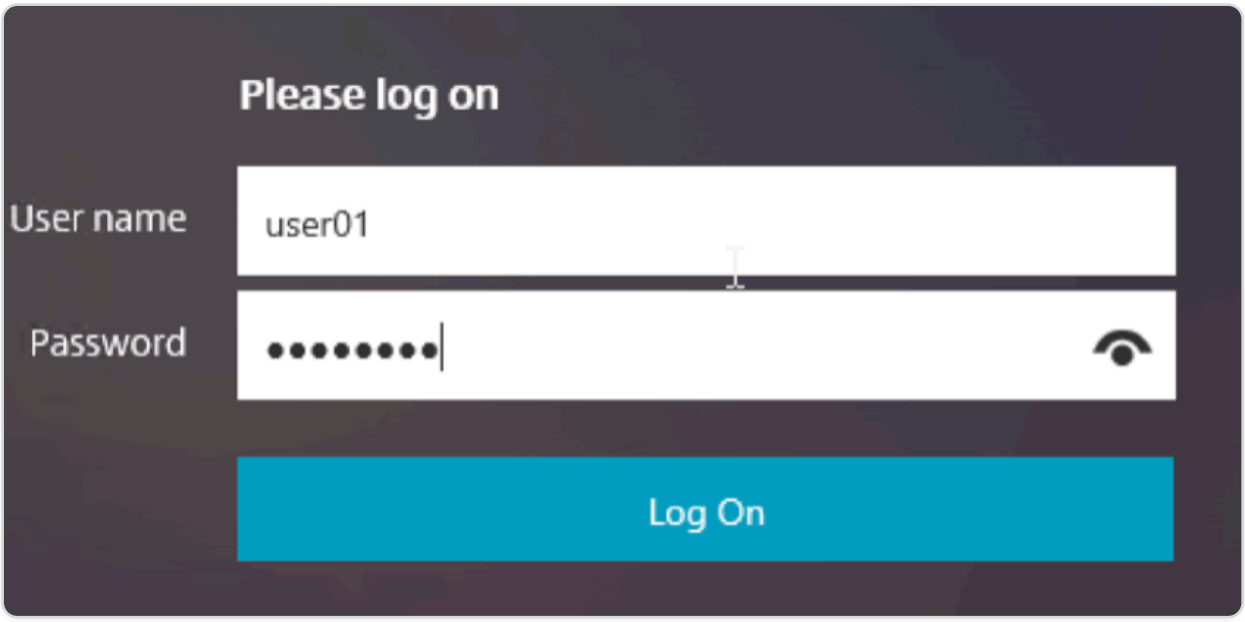



34. Si quiere usar los nombres cortos en lugar de los FQDN, agregue un **DNS Suffix (Traffic Management > DNS > DNS Suffix)**.

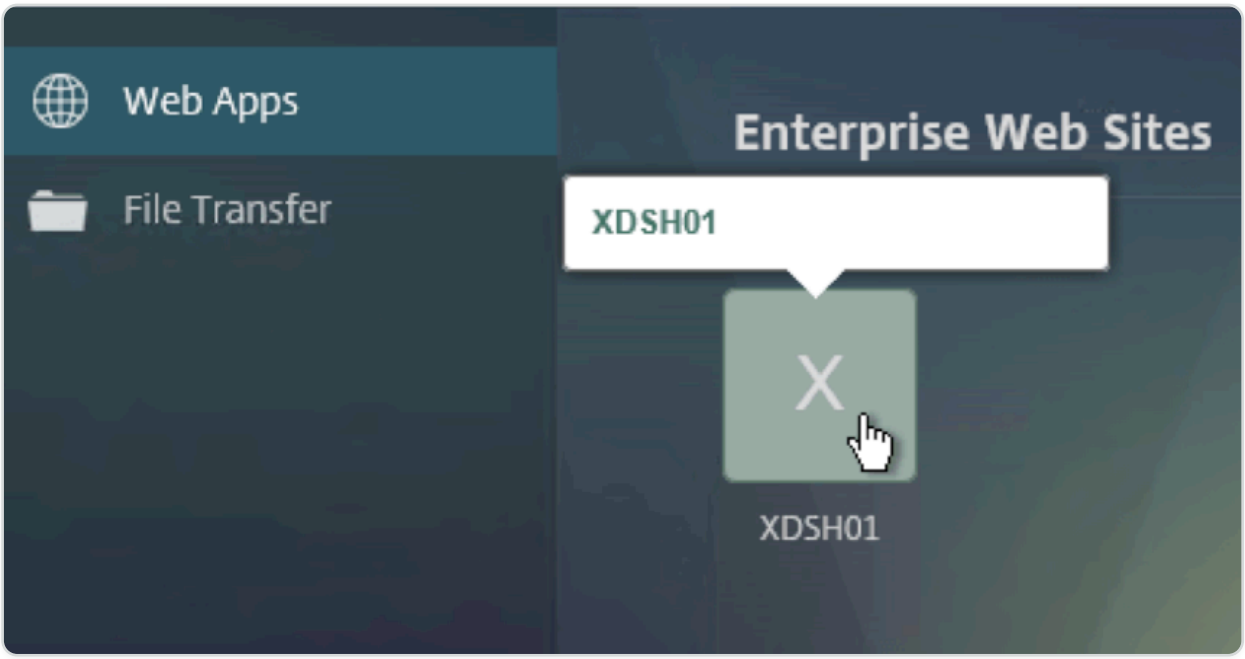



35. Conéctese a su gateway e inicie sesión.

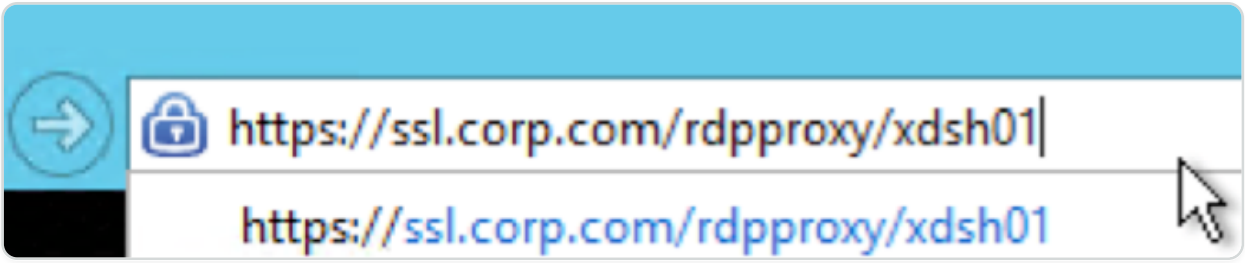
© 1997–2026 Citrix Systems, Inc. All rights reserved.




36. Si ha configurado **Marcadores**, haga clic en el **Marcador**.




37. Puede cambiar la barra de direcciones a **/rdpproxy/MyRDPServer**. Puede introducir una dirección IP (por ejemplo, rdpproxy/192.168.1.50) o un nombre DNS (/rdpproxy/myserver).

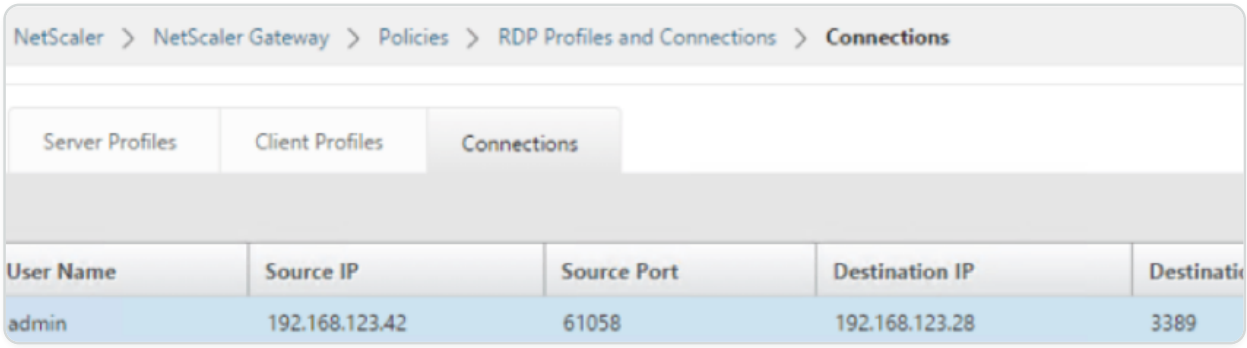



38. Abra el `.rdp file` descargado.

© 1997–2026 Citrix Systems, Inc. All rights reserved.




39. Puede ver los usuarios conectados actualmente yendo a **NetScaler Gateway Policies > RDP.** A la derecha está la pestaña **Conexiones**.




## Opción para deshabilitar SSO

La función SSO (inicio de sesión único) con el proxy RDP se puede deshabilitar configurando las políticas de tráfico de NetScaler para que al usuario siempre se le soliciten las credenciales. Cuando SSO está deshabilitado, la aplicación de RDP (SmartAccess) no funciona.

Ejemplo:

```
add vpn trafficaction <TrafficActionName> HTTP -SSO OFF
```

La política de tráfico se puede configurar según los requisitos; los siguientes son dos ejemplos:

- Para deshabilitar SSO para todo el tráfico:

```
add vpn trafficpolicy <TrafficPolicyName>  "url contains rdpproxy"
<TrafficActionName>
```

- Para deshabilitar SSO según la IP/FQDN de origen/destino

```
add vpn trafficPolicy <TrafficPolicyName>
 "HTTP.REQ.URL.CONTAINS(\"rdpproxy\") && CLIENT.IP.SRC.EQ(<IP>)"
<TrafficActionName>

bind vpnvserver rdp -policy <TrafficPolicyName> -priority 10
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

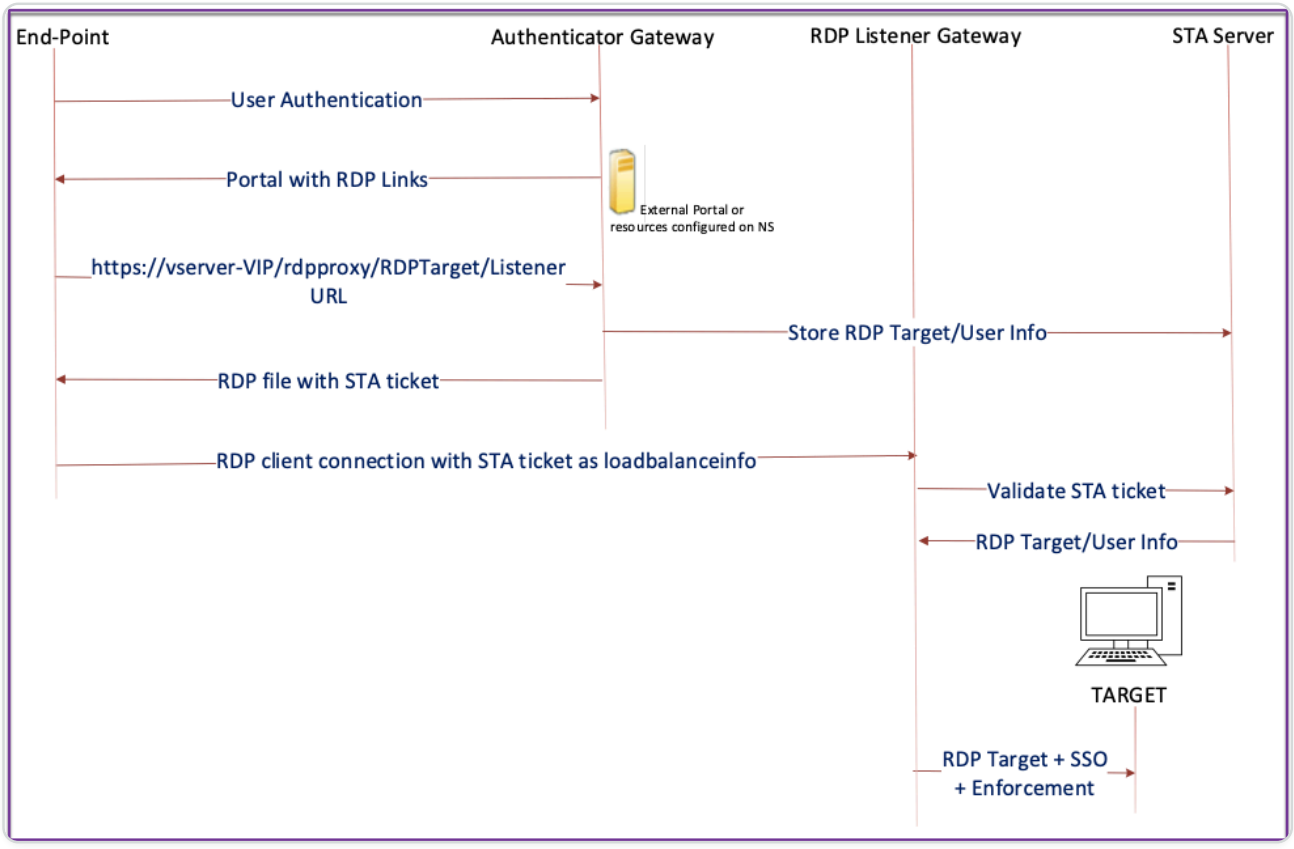
# Proxy RDP sin estado

El Proxy RDP sin estado accede a un host RDP. El acceso se concede a través del `RDPListener` en NetScaler Gateway cuando el usuario se autentica en un autenticador de NetScaler Gateway independiente. La información requerida por el `RDPListener` para NetScaler Gateway se almacena de forma segura en un servidor STA. Un servidor STA se puede colocar en cualquier lugar siempre que NetScaler Gateway y los servidores de enumeración de aplicaciones puedan acceder a él. Para obtener más detalles, consulte `<https://support.citrix.com/article/CTX101997>`.

## Flujo de conexión

Hay dos conexiones involucradas en el flujo del Proxy RDP. La primera conexión es la conexión SSL VPN del usuario al VIP de NetScaler Gateway y la enumeración de los recursos RDP.

La segunda conexión es la conexión del cliente RDP nativo al oyente RDP (configurado usando rdpIP y rdpPort) en NetScaler Gateway, y el posterior proxy seguro de los paquetes del cliente RDP al servidor.




1. El usuario se conecta al VIP del Authenticator Gateway y proporciona las credenciales.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Después de iniciar sesión correctamente en el gateway, el usuario es redirigido a la página de inicio/portal externo que enumera los recursos de escritorio remoto a los que el usuario puede acceder.
3. Una vez que el usuario selecciona un recurso RDP, el VIP del Authenticator Gateway recibe una solicitud, en el formato `https://AGVIP/rdpproxy/ip:port/rdptargetproxy` que indica el recurso publicado en el que hizo clic el usuario. Esta solicitud contiene la información sobre la IP y el puerto del servidor RDP que el usuario ha seleccionado.
4. El gateway autenticador procesa la solicitud /rdpproxy/. Dado que el usuario ya está autenticado, esta solicitud viene con una cookie de gateway válida.
5. La información `RDPTarget` y `RDPUser` se almacena en el servidor STA y se genera un ticket STA. La información se almacena como un blob XML que se cifra opcionalmente utilizando la clave precompartida configurada. Si está cifrado, el blob se codifica en base64 y se almacena. El Authenticator Gateway utiliza uno de los servidores STA configurados en el servidor virtual del Gateway.
6. El blob XML tiene el siguiente formato

   ```
   <Value name=”IPAddress”>ipaddr</Value>\n<Value name=”Port”>port</
   Value\>n



   <Value name=”`Username`”>username</Value\>\n<Value
   name=”Password”>pwd\</Value\>
   ```

7. El `rdptargetproxy` obtenido en la solicitud /rdpproxy/ se coloca como '`fulladdress`' y el ticket STA (precedido por el STA AuthID) se coloca como `loadbalanceinfo` en el archivo .rdp.
8. El archivo `.rdp` se envía de vuelta al punto final del cliente.
9. El cliente RDP nativo se inicia y se conecta a `RDPListener Gateway`. Envía el ticket STA en el paquete x.224 inicial.
10. El `RDPListener Gateway` valida el ticket STA y obtiene la información de `RDPTarget` y `RDPUser`. El servidor STA que se utilizará se recupera utilizando el 'AuthID' presente en el `loadbalanceinfo`.
11. Se crea una sesión de Gateway para almacenar las políticas de autorización/auditoría. Si ya existe una sesión para el usuario, se reutiliza.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

12. El `RDPListener Gateway` se conecta al `RDPTarget` e inicia sesión única utilizando CREDSSP.

## Requisitos previos

- El usuario está autenticado en el autenticador de NetScaler Gateway.
- La URL inicial /rdpproxy y el cliente RDP están conectados a un `RDPListener NetScaler Gateway` diferente.
- El Gateway autenticador, utilizando un servidor STA, pasa de forma segura la información `RDPListener Gateway`.

## Configurar el proxy RDP sin estado mediante la CLI

- Añada un perfil `rdpServer`. El perfil del servidor se configura en el `RDPListener Gateway`.

  **Nota:**

  - Una vez configurado el perfil rdpServer en el servidor virtual VPN, no se puede modificar. Además, el mismo serverProfile no se puede reutilizar en otro servidor virtual VPN.

  ```
  add rdpServer Profile [profilename] -rdpIP [IPV4 address of the RDP
  listener] -rdpPort [port for terminating RDP client connections] -psk
  [key to decrypt RDPTarget/RDPUser information, needed while using STA].
  ```

  Configure el perfil del servidor RDP en el servidor virtual VPN utilizando el siguiente comando:

  ```
  add vpn vserver v1 SSL [publicIP] [portforterminatingvpnconnections]
  -rdpServerProfile [rdpServer Profile]
  ```

  Ejemplo

  ```
  add vpn vserver v1 SSL 1.1.1.1 443 -rdpServerProfile rdp_server_prof
  ```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**IMPORTANTE:**

- El mismo servidor STA debe estar vinculado tanto al gateway autenticador RDP como al gateway de escucha.
- Para el proxy RDP sin estado, el servidor STA valida el ticket STA que envía el cliente RDP para obtener la información del servidor de destino RDP y del usuario RDP. Debe vincular el servidor STA además del servidor virtual VPN. En el siguiente ejemplo, el servidor de destino RDP es 1.1.1.0 y el servidor virtual de puerta de enlace de escucha RDP es 1.1.1.2.

```
add vpn url url4 RDP2 "rdp://1.1.1.0/1.1.1.2:443"
```

Configure el perfil de cliente en la puerta de enlace de autenticación mediante el siguiente comando:

```
add rdpClient profile <name> -rdpHost <optional FQDN that will be put in
the RDP file as ‘fulladdress’> [-rdpUrlOverride ( ENABLE | DISABLE )] [-
redirectClipboard ( ENABLE | DISABLE )] [-redirectDrives ( ENABLE |
DISABLE )]



        [-redirectPrinters ( ENABLE | DISABLE )] [-keyboardHook
<keyboardHook>] [-audioCaptureMode ( ENABLE | DISABLE )] [-
videoPlaybackMode ( ENABLE | DISABLE )]



        [-rdpCookieValidity <positive_integer>][-multiMonitorSupport
( ENABLE | DISABLE )] [-rdpCustomParams <string>]
```

La configuración –rdpHost se utiliza en una implementación de puerta de enlace única. Solo `psk` es un argumento obligatorio y debe ser la misma PSK que se agrega en el perfil del servidor RDP en la puerta de enlace de escucha RDP.

- Asocie el perfil RDP con el servidor virtual VPN.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Puede asociar un perfil RDP configurando una sessionAction+sessionPolicy o estableciendo el parámetro VPN global.

**Ejemplo:**

```
add vpn sessionaction <actname> -rdpClientprofile <rdpprofilename>

add vpn sessionpolicy <polname> NS_TRUE <actname>

bind vpn vserver <vservername> -policy <polname> -priority
<prioritynumber>
```

O

```
set vpn parameter –rdpClientprofile <name>
```

## Configurar el proxy RDP sin estado mediante la GUI

Los siguientes pasos de alto nivel están implicados en la configuración del proxy RDP sin estado. Para conocer los pasos detallados, consulte Configuración del proxy RDP.

- Crear un perfil de servidor RDP
- Crear un perfil de cliente RDP
- Crear un servidor virtual
- Crear un marcador
- Crear o editar un perfil o política de sesión
- Vincular un marcador

**IMPORTANTE:**

Para el proxy RDP sin estado, debe vincular un servidor STA además del servidor virtual VPN.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

### Contador de conexiones

Se agregó un nuevo contador de conexiones, ns_rdp_tot_curr_active_conn, que mantiene el registro del número de conexiones activas en uso. Se puede ver como parte del comando `nsconmsg` en el shell de NetScaler. Está previsto que más adelante se añada un comando CLI para ver estos contadores.

### Notas de actualización

Los parámetros rdpIP y rdpPort, que antes se configuraban en el servidor virtual VPN, forman parte del rdpServerProfile. El `rdp Profile` se renombra como `rdp ClientProfile` y se elimina el parámetro clientSSL. Por lo tanto, la configuración anterior no funciona.

## Redirección de conexión RDP

Un dispositivo NetScaler Gateway ahora admite la redirección de conexiones RDP en presencia de un agente de conexión o un directorio de sesiones. Una comunicación de proxy RDP ya no requiere una URL exclusiva para cada conexión del cliente al servidor. En su lugar, el proxy utiliza una única URL para conectarse a una granja de servidores RDP, lo que reduce la sobrecarga de mantenimiento y configuración para un administrador.

**Punto a tener en cuenta**:

- La redirección de conexión RDP solo se admite cuando SSO está habilitado y se admite tanto en modo Gateway único como en modo Gateway sin estado o dual junto con la aplicación (SmartAccess).
- La función de proxy RDP solo se admite con redirección basada en tokens que admita cookies IP. Los tokens de enrutamiento basados en IP “msts=” son devueltos por el agente de sesión de Windows o el agente de conexión cuando la funcionalidad **Usar redirección de dirección IP** está deshabilitada.
- Puede deshabilitar la configuración **Usar redirección de dirección IP** para habilitar la redirección basada en tokens en la siguiente ubicación. `Computer Configuration > Policies > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > RD Connection Broker`.
- Deshabilite la configuración Usar redirección de dirección IP en las máquinas RDSH y no en la máquina del agente de conexión.
- Se pueden configurar redireccionadores dedicados para la conexión de proxy RDP.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

## Requisitos previos

- Cree un perfil de servidor RDP para habilitar el oyente 3389 en el servidor virtual de NetScaler Gateway. Si la máquina a la que desea acceder por RDP no es miembro de ninguna infraestructura de agente de conexión de RDS, entonces no necesita el oyente 3389.
- Habilite la redirección de conexión RDP en el dispositivo NetScaler Gateway para admitir el proxy RDP en presencia de un agente de conexión.

## Implementar proxy RDP en presencia de un agente de conexión

El proxy RDP en presencia de un agente de conexión se puede implementar de las dos maneras siguientes.

- Con servidores host de sesión RD que participan en el equilibrio de carga del agente de conexión RD.
- En presencia de la función de equilibrio de carga RDP.

**Con servidores host de sesión RD que participan en el equilibrio de carga del agente de conexión RD**:

En este caso, el enlace URL de RDP se puede configurar para que apunte a uno de los servidores RDP como servidor de destino, que actúa como redirigidor. Además, es posible tener uno de los servidores RDP de la granja como servidor de destino (en este caso, el servidor no acepta ninguna sesión RDP).

**En presencia de la función de equilibrio de carga de RDP**:

Cuando el equilibrio de carga del agente de conexión no está habilitado, podemos tener la función de equilibrio de carga de RDP disponible en NetScaler para realizar el equilibrio de carga necesario de las sesiones RDP en presencia de un agente de conexión. En este caso, el enlace URL de RDP debe configurarse para que el equilibrador de carga de RDP sea el servidor de destino. El equilibrador de carga de RDP puede estar en el mismo dispositivo NetScaler Gateway que el proxy RDP. Para obtener más información, consulte Equilibrio de carga de servidores RDP.

### Configurar el proxy RDP en presencia de un agente de conexión mediante la CLI

En el símbolo del sistema, escriba;

```
add rdpserverprofile <Name> -psk <string> -rdpRedirection ( ENABLE |
DISABLE )
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
add rdpserverprofile serverProfileName -psk “secretString” -rdpRedirection
ENABLE
```

### Configurar la redirección de conexión RDP mediante la GUI de NetScaler

1. Vaya a **NetScaler Gateway > Directivas > RDP**.
2. Haga clic con el botón derecho en **RDP** para **habilitar** o **deshabilitar** la funcionalidad de redirección de RDP.

## Rellenar URL de RDP basadas en el atributo LDAP

Puede configurar un dispositivo NetScaler Gateway para recuperar una lista de servidores RDP (IP/FQDN) de un atributo de servidor LDAP. Basándose en la lista recuperada, el dispositivo muestra las URL de RDP para los servidores a los que un usuario puede acceder.

### Para rellenar URL de RDP basadas en el atributo LDAP mediante la CLI

En el símbolo del sistema, escriba:

```
add rdpclientprofile <Name> –rdpUrlLinkAttribute <string>



add rdpclientprofile clientProfileName –rdpUrlLinkAttribute
rdpServerAttribute
```

En el ejemplo anterior, rdpServerAttribute corresponde a los detalles del servidor RDP para un usuario determinado en el servidor LDAP.

**Nota**: Para obtener los detalles del atributo LDAP del servidor LDAP, la acción LDAP debe configurarse con la misma cadena que está configurada con `pUrlLinkAttribute` de la siguiente manera.

```
add authentication ldapAction dnpg_ldap -serverIP <IP address>-ldapBase
<"domain name"> -ldapBindDn <username> -ldapLoginName sAMAccountName
-ldapbindDnpassword <password>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
add authentication ldapAction dnpg_ldap -serverIP 10.102.39.101 -ldapBase
"dc=dnpg-blr,dc=com" -ldapBindDn sqladmin@dnpg-blr.com -ldapLoginName
sAMAccountName -ldapbindDnpassword xxxx



add authentication ldapPolicy dnpg_ldap_pol ns_true dnpg_ldap



bind vpn vs vserver<name> -pol dnpg_ldap_pol



set ldapaction dnpg_ldap -attributes "rdpServerAttribute"



set rdpclientprofile ldap -rdpLinkAttribute rdpServerAttribute
```

## Configuración del servidor LDAP

En el servidor LDAP, realice los siguientes pasos:

1. Vaya a un **Usuario** en particular.
2. En **Usuarios y equipos de AD**, haga clic en **Ver** y, a continuación, en **Detalle.**
3. Haga clic con el botón derecho en el **nombre de usuario** y haga clic en **Editor de atributos.**
4. Cambie el valor del atributo requerido (displayName) y haga clic en **Aceptar.**

## Para rellenar URL de RDP basadas en el atributo LDAP mediante la GUI

1. Vaya a **NetScaler Gateway > Directivas > RDP**.
2. En la página **Perfiles y conexiones RDP**, haga clic en la ficha **Perfiles de cliente** y seleccione el perfil de cliente donde desea configurar el atributo de enlace RDP.
3. En la página **Configurar perfil de cliente RDP**, en **Atributo de enlace RDP**, introduzca el nombre del atributo LDAP.

   **Nota:** El valor del atributo LDAP puede ser una lista separada por comas.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

# Aleatorizar el nombre de archivo RDP con proxy RDP

Al hacer clic en una URL RDP, se descarga un archivo RDP. Al hacer clic de nuevo en la **URL RDP**, se descarga un nuevo archivo RDP con el mismo nombre, lo que provoca una ventana emergente para reemplazar el archivo nuevo por el existente. Para evitar esto, el administrador puede optar por aleatorizar el nombre del archivo RDP. El nombre del archivo ahora se aleatoriza añadiendo la salida de la función time () en el formato \<rdpFileName\>_\< `outputof` time() \>.rdp. Al hacerlo, el dispositivo genera un nombre de archivo RDP único cada vez que descarga un archivo.

## Configurar la compatibilidad con la aleatorización del nombre de archivo RDP con proxy RDP

**Para configurar la compatibilidad con la aleatorización del nombre de archivo RDP con proxy RDP mediante la interfaz de línea de comandos en el símbolo del sistema, escriba**:

```
    add rdpclientprofile <profileName> -rdpfileName <filename> -
randomizeRDPFilename <YES/NO>



    add rdpclientprofile clientProfileName -rdpfileName testRDP -
randomizeRDPFilename YES
```

**Para configurar la compatibilidad con la aleatorización del nombre de archivo RDP con proxy RDP mediante la GUI de NetScaler:**

1. Vaya a **NetScaler Gateway** > **Directivas** > **RDP**.
2. En la página **Perfiles y conexiones RDP**, haga clic en la ficha **Perfiles de cliente** y seleccione el perfil de cliente donde desea configurar la funcionalidad de aleatorización del nombre de archivo RDP.
3. En la página **Configurar perfil de cliente RDP**, seleccione **SÍ** en el menú junto al campo **Nombre de archivo RDP aleatorizado**.

# Configurar el nombre de los archivos RDP

Al descargar un archivo RDP, se puede almacenar localmente con el nombre de archivo configurado.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

## Configurar un nombre para los archivos RDP

Para configurar un nombre para los archivos RDP mediante la CLI, en el símbolo del sistema, escriba**:

```
set rdpclientprofile <Name> -rdpfilename <filename>.rdp
```

**Para configurar un nombre para los archivos RDP mediante la GUI:**

1. Vaya a **NetScaler Gateway** > **Policies** > **RDP**.
2. En la página **RDP Profiles and Connections**, haga clic en la ficha **Client Profiles**. Seleccione el perfil de cliente donde desea configurar una funcionalidad de nombre de archivo RDP aleatorio.
3. En la página **Configure RDP Client Profile**, introduzca un nombre para el perfil RDP en el campo **RDP File Name**. El nombre del archivo debe tener el siguiente formato: <filename.rdp>. Se permite un máximo de 31 caracteres para el nombre.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

# Soporte de proxy ICA® saliente

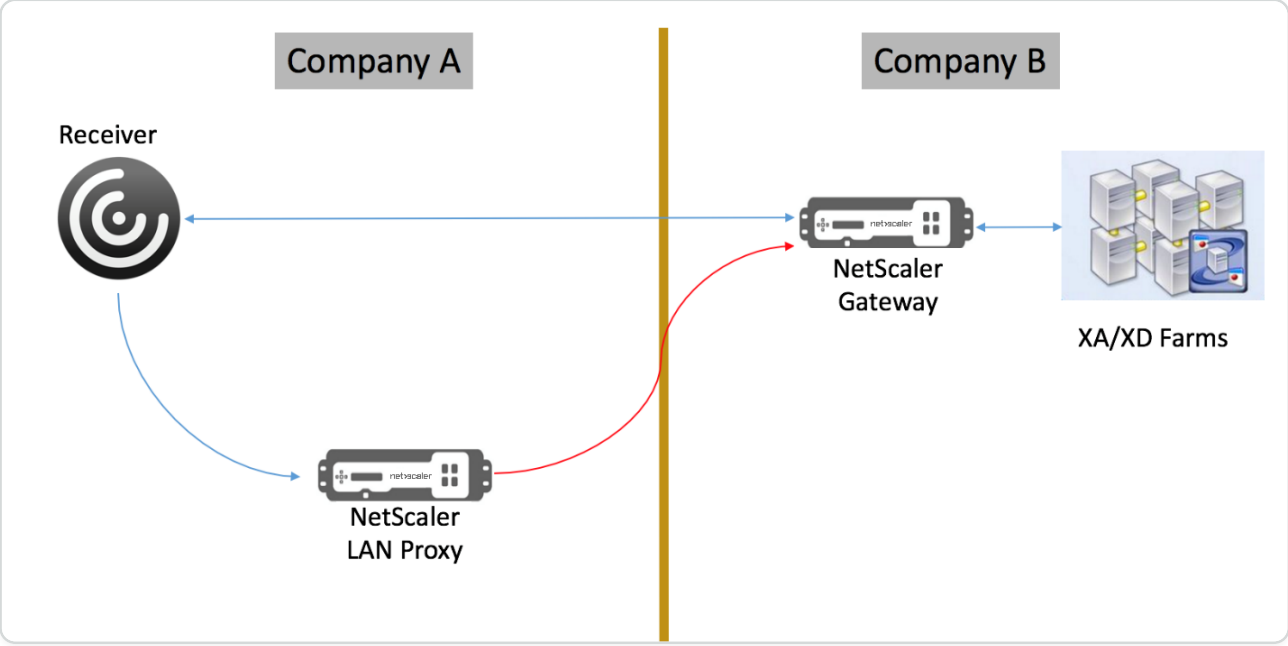
El soporte de proxy ICA saliente para NetScaler Gateway permite a los administradores de red aprovechar las funcionalidades de SmartControl incluso cuando Receiver y NetScaler Gateway se implementan en organizaciones diferentes.

El siguiente escenario ilustra el uso de la solución de proxy ICA saliente:

Un administrador de red requiere control sobre las capacidades relacionadas con la sesión ICA cuando Receiver y NetScaler Gateway se implementan en organizaciones diferentes.

## Descripción del soporte de proxy ICA saliente

Para llevar la funcionalidad SmartControl a la organización empresarial, la empresa A, que tiene el receptor, necesitamos añadir un dispositivo NetScaler que actúe como proxy LAN. El proxy LAN de NetScaler aplica SmartControl y envía el tráfico al NetScaler Gateway de la empresa B. En este escenario de implementación, el receptor reenvía el tráfico al proxy LAN de NetScaler, lo que permite al administrador de red de la empresa A aplicar SmartControl. La implementación se muestra en la siguiente figura.




En este escenario, el tráfico entre el proxy LAN y el NetScaler Gateway se realiza a través de SSL.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**NOTA:**

No habilite la autenticación basada en certificados de cliente en el NetScaler Gateway.

## Soporte SSL en el proxy LAN de NetScaler

A partir de la versión 13.0 compilación xx.xx, el tráfico entre la aplicación Citrix Workspace y el proxy LAN de NetScaler también es compatible con SSL. La aplicación Citrix Workspace cifra el tráfico que envía al proxy LAN a través de SSL. El soporte SSL en el proxy LAN puede coexistir con la implementación existente.

Para habilitar el cifrado de tráfico a través de SSL entre la aplicación Citrix Workspace y el proxy LAN de NetScaler, debe realizar lo siguiente en el proxy LAN de NetScaler:

- Deshabilite la autenticación y habilite el doble salto en el servidor virtual VPN.
- Establezca el host en el cliente Windows en la dirección IP del servidor virtual VPN.
- Habilite SNI y la validación de certificados.
- Añada los certificados de CA apropiados y habilítelos globalmente.

## Configuración del proxy ICA® saliente

La configuración del proxy ICA saliente implica configurar el proxy LAN de NetScaler y NetScaler Gateway.

### Configurar el proxy LAN de NetScaler para el proxy ICA saliente

Puede realizar los siguientes pasos para configurar el proxy ICA saliente mediante la CLI.

- Añadir un servidor virtual VPN.

```
add vpn vserver <name> <serviceType> [<IPAddress> [-range
<positive_integer>] [-ipset <string>]] [<port>] [-state ( ENABLED |
DISABLED )] [-authentication ( ON | OFF )] [-doubleHop ( ENABLED |
DISABLED )]
```

- Establecer los parámetros VPN.

```
set vpn parameter[-backendServerSni ( ENABLED | DISABLED )][-
backendCertValidation ( ENABLED | DISABLED )]
```

- Añadir un par de clave-certificado SSL.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
add ssl certKey ca_cert_verify -cert <certificate name>
```

- Vincular el par de clave-certificado SSL globalmente.

```
bind vpn global -cacert ca_cert_verify
```

**Ejemplo:**

```
-  add vpn vserver ssl_lan_proxy SSL 65.219.17.34 443 -authentication OFF
- doubleHop ENABLED



-  set vpn parameter backendserverSni ENABLED backendcertValidation
ENABLED



-  add ssl certKey dnpg_ca -cert dnpg_ca_cert.cer



-  bind vpn global -cacert dnpg_ca
```

**NOTA:**

Para la compatibilidad con SSL en el proxy LAN de NetScaler, no se requieren cambios en la configuración de NetScaler Gateway.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

# Soporte de proxy PCoIP habilitado en NetScaler Gateway para VMware Horizon View

NetScaler Gateway 12.0 es compatible con el protocolo PC-over-IP (PCoIP), que es el protocolo de visualización remota para varias soluciones VDI que no son de Citrix, incluido VMware Horizon View. PCoIP es análogo al protocolo Citrix HDX/ICA y al protocolo Microsoft RDP. PCoIP utiliza el puerto UDP 4172.

Cuando PCoIP se proxy a través de NetScaler Gateway, NetScaler Gateway puede reemplazar las soluciones tradicionales de acceso remoto PCoIP, como View Security Server o VMware Access Point.

**Los siguientes escenarios ilustran el uso de la solución VMWare Horizon View habilitada para NetScaler Gateway.**

- Usuarios de VMware Horizon PCoIP que necesitan acceder remotamente a grupos de escritorios y grupos de aplicaciones de VMware Horizon View a través de NetScaler Gateway sin implementar un Horizon View Security Server o VMware Access Point.
- Usuarios de PCoIP que acceden remotamente a otras soluciones de escritorio virtual basadas en PCoIP a través de NetScaler Gateway.

**NOTA**

NetScaler Gateway se implementa como una solución de acceso remoto.

## Configurar el proxy PCoIP habilitado para NetScaler Gateway para VMware Horizon View

### Requisitos previos

**Versión** - NetScaler 12.0 o superior

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**Licencia Universal** - El proxy PCoIP utiliza la función de acceso sin cliente de NetScaler Gateway, lo que significa que cada conexión de NetScaler Gateway debe tener licencia para NetScaler Gateway Universal. En el servidor virtual de NetScaler Gateway, asegúrese de que **Solo ICA** esté desactivado.

**Infraestructura de Horizon View** - Una infraestructura interna de Horizon View funcional. Asegúrese de poder conectarse a los agentes de Horizon View internamente sin NetScaler Gateway. Asegúrese de que el **Túnel seguro HTTP(S)** y la **Puerta de enlace segura PCoIP** de Horizon View no estén habilitados en los servidores de conexión de View a los que NetScaler reenviará las conexiones. Se admiten las siguientes versiones de VMware Horizon View.

- Servidor de conexión: 7.0.1 y superior
- Cliente Horizon: 4.2.0 y superior (Windows y Mac)

**Puertos de firewall**:

Asegúrese de lo siguiente:

- UDP 4172 y TCP 443 deben estar abiertos desde los clientes de Horizon View al VIP de NetScaler Gateway.
- UDP 4172 debe estar abierto desde el SNIP de NetScaler a todos los agentes internos de Horizon View.
- El proxy PCoIP es compatible con NetScaler implementado detrás de NAT. A continuación, se presentan los puntos importantes a considerar:
    - La compatibilidad se basa en la configuración del parámetro FQDN del servidor virtual VPN
    - Solo admite FQDN de acceso público y no IP
    - Solo admite los puertos 443 y 4172
    - Debe ser una NAT estática

**Certificado** – Un certificado válido para el servidor virtual de NetScaler Gateway.

**Autenticación** – Una política/servidor de autenticación LDAP que utilice sintaxis avanzada.

**Unified Gateway (opcional)** – Si es Unified Gateway, cree el Unified Gateway antes de añadir la funcionalidad PCoIP.

**Tema del portal RfWebUI** – Para el acceso a Horizon View desde un navegador web, el servidor virtual de NetScaler Gateway debe configurarse con el tema RfWebUI.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**Cliente de Horizon View** – El cliente de Horizon View debe estar instalado en el dispositivo cliente, incluso si se accede a los iconos publicados de Horizon mediante el portal RfWebUI de NetScaler.

**Para configurar NetScaler Gateway para que admita el proxy PCoIP para VMWare Horizon View:**

1. Vaya a **Configuración > Directivas de NetScaler Gateway > PCoIP**.
2. Cree un perfil de servidor virtual y un perfil PCoIP en la página **Perfiles y conexiones PCoIP**.
    a. Para crear un perfil de servidor virtual, en la ficha **Perfiles de VServer**, haga clic en **Agregar**.
    b. Introduzca un nombre para el perfil del servidor virtual.
    c. Introduzca un nombre de dominio de Active Directory que se utilice para el inicio de sesión único en View Connection Server y, a continuación, haga clic en **Crear. Nota:** Solo se admite un único dominio de Active Directory por servidor virtual de NetScaler Gateway. Además, el nombre de dominio especificado aquí se muestra en el cliente de Horizon View.
    d. Haga clic en **Iniciar sesión**.
    e. Para crear un perfil PCoIP, en la ficha **Perfiles**, haga clic en **Agregar**.
        i. Introduzca un nombre para el perfil PCoIP.
        ii. Introduzca la URL de conexión para el servidor de conexión interno de VMware Horizon View y, a continuación, haga clic en **Crear**.
    f. Vaya a **Configuración > NetScaler Gateway > Directivas > Sesión**.
    g. A la derecha, seleccione la pestaña **Perfiles de sesión**.
    h. En la página **Directivas y perfiles de sesión de NetScaler Gateway**, cree o edite un perfil de sesión de NetScaler Gateway.
        i. Para crear un perfil de sesión de NetScaler Gateway, haga clic en **Agregar** y proporcione un nombre.
        ii. Para editar un perfil de sesión de NetScaler Gateway, seleccione el perfil y haga clic en **Editar**.
    i. En la pestaña **Experiencia del cliente**, asegúrese de que el valor de **Acceso sin cliente** esté establecido en **Activado**.
    j. En la pestaña **Seguridad**, asegúrese de que el valor de **Acción de autorización predeterminada** esté establecido en **PERMITIR**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

k. En la pestaña **PCoIP**, seleccione el perfil PCoIP requerido y, a continuación, haga clic en **Crear**. También puede crear o editar perfiles PCoIP desde esta pestaña.

l. Haga clic en **Crear** o **Aceptar** para finalizar la creación o edición del perfil de sesión.

m. Si ha creado un perfil de sesión, también debe crear una directiva de sesión correspondiente.

   i. Vaya a **Configuración > NetScaler Gateway > Directivas > Sesión**.

   ii. seleccione la pestaña **Directivas de sesión** y, a continuación, haga clic en **Agregar**.

   iii. En la página Crear directiva de sesión de NetScaler Gateway, introduzca un nombre para la directiva.

   iv. En **Perfil**, seleccione un perfil existente o haga clic en **Agregar** y cree un perfil.

   v. Agregue una expresión.

      i. Haga clic en **Directiva avanzada** y, a continuación, en **Editor de expresiones**.

      ii. En **Expresión**, seleccione la expresión según sus requisitos.

   vi. Haga clic en **Aceptar**.

n. Enlace el perfil de servidor virtual PCoIP creado y la directiva de sesión a un servidor virtual de NetScaler Gateway.

   i. Vaya a **NetScaler Gateway > Servidores virtuales**.

   ii. A la derecha, **Agregue** un nuevo servidor virtual de NetScaler Gateway o **Edite** un servidor virtual de NetScaler Gateway existente.

   iii. Si está editando un servidor virtual de NetScaler Gateway existente, en la sección **Configuración básica**, haga clic en el icono de lápiz.

   iv. Para agregar y editar, en la sección **Configuración básica**, haga clic en **Más**.

   v. Utilice el menú **Perfil de servidor virtual PCoIP** para seleccionar el perfil de servidor virtual PCoIP requerido.

   vi. Desplácese hacia abajo y asegúrese de que ICA® Only esté desmarcado. A continuación, haga clic en **Aceptar** para cerrar la sección **Configuración básica**.

   vii. Si está creando un servidor virtual de NetScaler Gateway, enlace un **certificado** y enlace una directiva de autenticación LDAP.

   viii. Desplácese hasta la sección **Directivas** y haga clic en el icono más.

   ix. La página **Elegir tipo** tiene como valores predeterminados **Sesión** y **Solicitud**. Haga clic en **Continuar**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

x. En la sección **Enlace de directivas**, haga clic en **Haga clic para seleccionar**.

xi. Seleccione la política de sesión requerida que tenga el perfil PCoIP configurado y haga clic en **Select**.

xii. En la página **Policy Binding**, haga clic en **Bind**.

xiii. Si desea utilizar un navegador web para conectarse a VMware Horizon View, en **Advanced Settings**, añada la sección **Portal Themes**. Si solo utiliza Horizon View Client para conectarse a NetScaler Gateway, no es necesario realizar este paso.

xiv. Utilice el menú **Portal Theme** para seleccionar **RfWebUI** y haga clic en **OK**.

xv. Los iconos publicados de Horizon View se añaden al portal RfWebUI.

**NOTA:**

VMware utiliza dos o más protocolos cuando se usa cualquier protocolo que no sea RDP. Esto puede provocar que las solicitudes se equilibren la carga entre dos servidores back-end diferentes. Puede resolver este problema configurando un único grupo de persistencia en todos los protocolos, asegurando que todas las conexiones permanezcan en el mismo servidor virtual de Citrix®.

## Pasos para habilitar la redirección USB

Se puede acceder a los dispositivos USB conectados a la máquina cliente desde los escritorios y aplicaciones virtuales. A continuación, se detallan los pasos para habilitar la redirección USB:

1. Inicie sesión en VMware Horizon Administrator Console.
2. Vaya a **Inventory > View Configuration Servers**.
3. Seleccione la ficha **Connection Servers**.
4. Seleccione un Connection Server de la lista y haga clic en **Edit**.
5. En la ficha **General**, seleccione la opción **Use Secure Tunnel connection to machine** en **HTTP(S) Secure Tunnel**. Proporcione la URL externa de NetScaler Gateway en el campo **External URL**.

## Actualizar la expresión de conmutación de contenido para Unified Gateway

Si su servidor virtual de NetScaler Gateway está detrás de un Unified Gateway (Content Switching Virtual Server), debe actualizar la Content Switching Expression para incluir las rutas de URL de PCoIP.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. En la GUI de NetScaler, vaya a **Configuración > Administración de tráfico > Conmutación de contenido > Directivas**.
2. Agregue la siguiente expresión en el área **Expresión** y, a continuación, haga clic en **Aceptar**.

||http.req.url.path.eq("/broker/xml")|| http.req.url.path.contains("/broker/resources")|| http.req.url.path.eq("/pcoip-client")||http.req.url.path.contains("/ice-tunnel")

### Usar la puerta de enlace PCoIP

1. Para conectarse, debe tener el cliente de Horizon View instalado en el dispositivo cliente. Una vez instalado, puede usar la interfaz de usuario del cliente de Horizon View para conectarse a NetScaler Gateway, o puede usar la página del portal RfWebUI de NetScaler Gateway para ver los iconos publicados desde Horizon.
2. Para ver las conexiones PCoIP activas, vaya a **NetScaler Gateway > PCoIP.**
3. A la derecha, cambie a la ficha **Conexiones**. Las sesiones activas se muestran con los siguientes datos: nombre de usuario, IP del cliente de Horizon View e IP de destino del agente de Horizon View.
4. Para finalizar una conexión, haga clic con el botón derecho en la ficha **Conexión** y haga clic en **Terminar conexión**. O haga clic en **Terminar todas las conexiones** para finalizar todas las conexiones PCoIP.

## Configuración del servidor de conexión de VMware Horizon View

Para admitir el proxy PCoIP a través de NetScaler Gateway:

1. Inicie sesión en la **Consola de administración de VMware Horizon**.
2. Vaya a I**nventario** --\> **Configuración de vista** --\> **Servidores**.
3. Seleccione la pestaña **Servidores de conexión**.
4. Seleccione un servidor de conexión de la lista y haga clic en **Editar**.
5. En la pestaña **General**, deseleccione la opción **Usar conexión de túnel seguro** a la máquina en Túnel seguro HTTP(S).
6. Haga clic en **Aceptar** para cerrar la ventana **Editar configuración del servidor de conexión**.
7. Realice los pasos del 4 al 6 en todos los servidores de conexión de la lista.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

# Configuración automática de proxy para la compatibilidad con proxy de salida para NetScaler Gateway

Cuando se configura el dispositivo NetScaler Gateway para admitir la configuración automática de proxy (PAC), la URL de un archivo PAC se envía al navegador del cliente. El tráfico del cliente se redirige entonces a los proxies respectivos según lo determinado por las condiciones definidas en el archivo PAC.

A continuación se presentan algunos casos de uso comunes para PAC para proxy de salida:

- Para configurar varios servidores proxy que gestionan el tráfico del cliente.
- Para equilibrar la carga del tráfico del proxy entre subredes.

## Configurar los parámetros globales de NetScaler Gateway para admitir PAC para proxy de salida mediante la CLI

En el símbolo del sistema, escriba:

```
set vpn parameter -proxy BROWSER -autoProxyUrl <URL>
```

## Configurar NetScaler Gateway para admitir PAC en un perfil de sesión mediante la CLI

En el símbolo del sistema, escriba:

```
add vpn sessionAction <name> -proxy BROWSER -autoProxyUrl <URL>
```

Donde;

- **URL** – URL del servidor proxy
- **Nombre** – Nombre de la acción de sesión VPN

© 1997–2026 Citrix Systems, Inc. All rights reserved.

# Configurar los parámetros globales de NetScaler Gateway para admitir PAC para proxy de salida mediante la GUI

1. Vaya a **Configuración > NetScaler Gateway > Configuración global**.
2. En la página **Configuración global**, haga clic en **Cambiar configuración global** y, a continuación, seleccione la pestaña **Experiencia del cliente**.
3. En la pestaña **Client Experience**, seleccione **Advanced Settings** y, a continuación, seleccione la pestaña **Proxy**.
4. En la pestaña **Proxy**, seleccione **Browser** y, a continuación, seleccione **Use Automatic Configuration**.
5. En el campo **URL To Auto Proxy Config File**, escriba la URL del archivo PAC requerido.
6. Haga clic en **Create**.

# Configurar NetScaler Gateway para admitir PAC en el perfil de sesión mediante la GUI

1. Vaya a **Configuration > NetScaler Gateway > Policies > Session**.
2. En la página **Session Policies and Profiles** de NetScaler Gateway, cree un perfil de sesión de NetScaler Gateway.
3. Seleccione la pestaña **Session Profiles**, haga clic en **Add** e introduzca un nombre.
4. En la pestaña **Client Experience**, seleccione **Advanced Settings** y, a continuación, seleccione la pestaña **Proxy**.
5. En la pestaña **Proxy**, seleccione **Browser** y, a continuación, seleccione **Use Automatic Configuration**.
6. En el campo **URL To Auto Proxy Config File**, escriba la URL del archivo PAC requerido.
7. Haga clic en **Create**.
8. Haga clic en **Create**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

# Soporte de configuración para el atributo de cookie SameSite

El atributo `SameSite` indica al navegador si la cookie se puede usar en un contexto entre sitios o solo en un contexto del mismo sitio. Si una aplicación tiene la intención de ser accedida en un contexto entre sitios, solo puede hacerlo a través de la conexión HTTPS. Para obtener más detalles, consulte RFC6265.

Hasta febrero de 2020, el atributo `SameSite` no se configuraba explícitamente en el dispositivo NetScaler. El navegador tomaba el valor predeterminado (None). La no configuración del atributo `SameSite` no afectó a las implementaciones de NetScaler Gateway y NetScaler AAA.

Con la actualización de ciertos navegadores, como Google Chrome 80, hay un cambio en el comportamiento predeterminado de las cookies entre dominios. El atributo `SameSite` se puede establecer en uno de los siguientes valores. El valor predeterminado para Google Chrome se establece en Lax. Para ciertas versiones de otros navegadores, el valor predeterminado para el atributo `SameSite` aún podría establecerse en None.

- **None**: Indica al navegador que use la cookie en un contexto entre sitios solo en conexiones seguras.
- **Lax**: Indica al navegador que use la cookie para solicitudes en el contexto del mismo sitio. En el contexto entre sitios, solo los métodos HTTP seguros como las solicitudes GET pueden usar la cookie.
- **Strict**: Use la cookie solo en el contexto del mismo sitio.

Si no hay un atributo `SameSite` en la cookie, Google Chrome asume la funcionalidad de `SameSite` = Lax. Como resultado, para implementaciones dentro de un iframe con contexto entre sitios que requieren que el navegador inserte cookies, Google Chrome no comparte cookies entre sitios. Como resultado, el iframe dentro del sitio web podría no cargarse.

## Configurar el atributo de cookie `SameSite`

Se agrega un nuevo atributo de cookie llamado `SameSite` a los servidores virtuales VPN y NetScaler AAA. Este atributo se puede establecer a nivel global y a nivel de servidor virtual.

Para configurar el atributo `SameSite`, debe realizar lo siguiente:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Establezca el atributo `SameSite` para el servidor virtual
2. Vincule las cookies a `patset` (si el navegador elimina las cookies entre sitios)

## Configuración del atributo `SameSite` mediante la CLI

Para establecer el atributo `SameSite` a nivel de servidor virtual, utilice los siguientes comandos.

```
set vpn vserver VP1 -SameSite  [ STRICT | LAX | None ]

set aaa vserver VP1 -SameSite  [ STRICT | LAX | None ]
```

Para establecer el atributo `SameSite` a nivel global, utilice los siguientes comandos.

```
set vpn param VP1 -SameSite  [ STRICT | LAX | None ]

set aaa param VP1 -SameSite  [ STRICT | LAX | None ]
```

**Nota**: La configuración a nivel de servidor virtual tiene preferencia sobre la configuración a nivel global. Citrix recomienda establecer el atributo de cookie `SameSite` a nivel de servidor virtual.

## Vinculación de cookies a `patset` mediante la CLI

Si el navegador elimina las cookies entre sitios, puede vincular esa cadena de cookies a la `ns_cookies_SameSite patset` existente para que el atributo `SameSite` se añada a la cookie.

**Ejemplo:**

```
bind patset ns_cookies_SameSite "NSC_TASS"

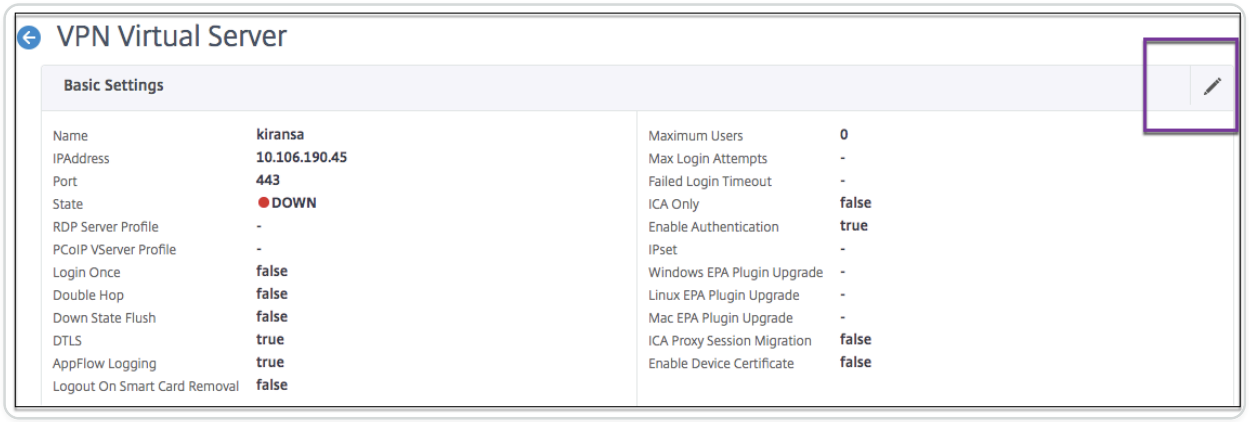
bind patset ns_cookies_SameSite "NSC_TMAS"
```

## Configuración del atributo SameSite mediante la GUI

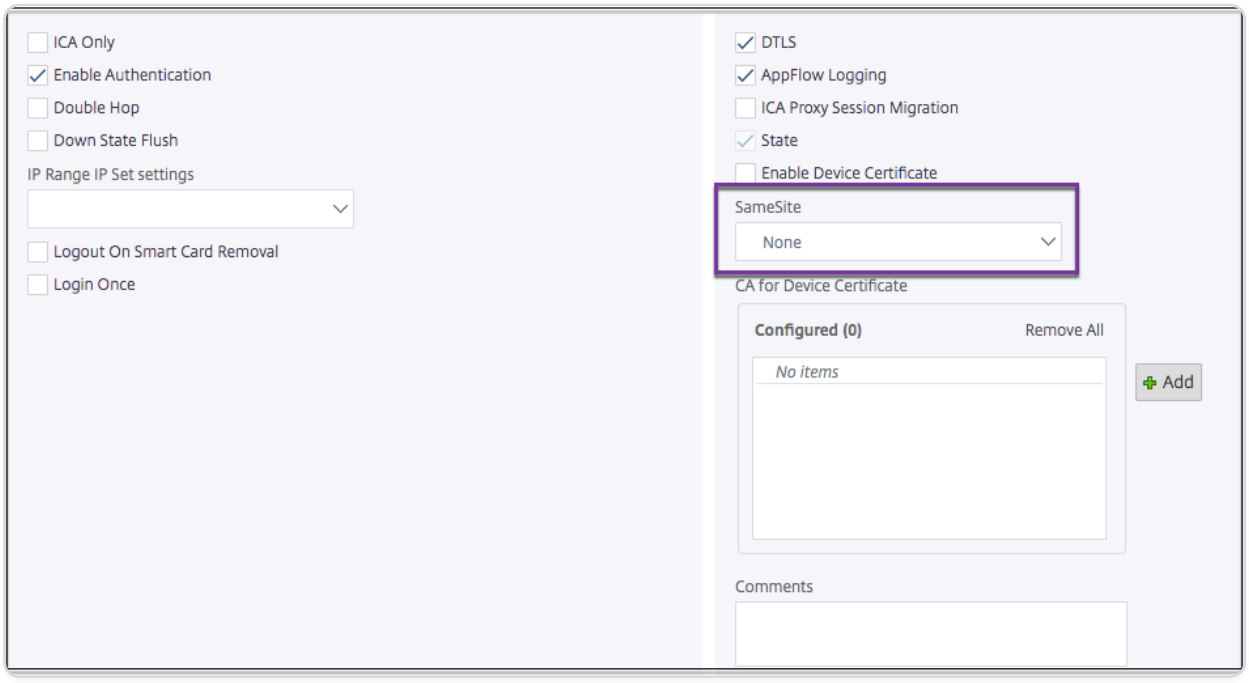
**Para establecer el atributo `SameSite` a nivel de servidor virtual:**

1. Navegue hasta **NetScaler Gateway > Servidores virtuales**.
2. Seleccione un servidor virtual y haga clic en **Editar**.
3. Seleccione el icono de edición en la sección **Configuración básica** y haga clic en **Más**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



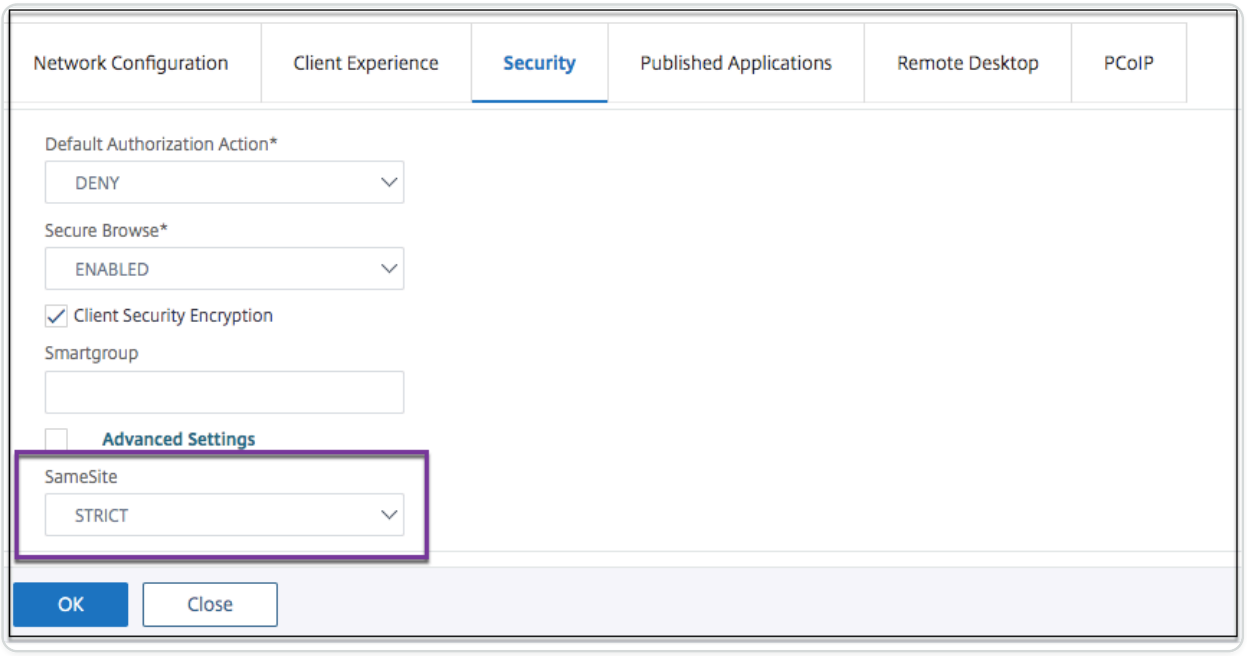

4. En **SameSite**, seleccione la opción según sea necesario.




**Para establecer el atributo `SameSite` a nivel global:**

1. Navegue hasta **NetScaler Gateway > Configuración global > Cambiar configuración global.**
2. Haga clic en la pestaña **Seguridad**.
3. En `SameSite`, seleccione la opción según sea necesario.

© 1997–2026 Citrix Systems, Inc. All rights reserved.




© 1997–2026 Citrix Systems, Inc. All rights reserved.

# Optimizar el tráfico de red con Citrix SD-WAN™ WANOP

Cuando los usuarios inician sesión con el cliente Citrix Secure Access, la conexión se puede optimizar mediante el complemento Citrix SD-WAN WANOP, que se instala en el dispositivo del usuario desde Citrix SD-WAN WANOP. Cuando la conexión se optimiza mediante el complemento Citrix SD-WAN WANOP, el tráfico de red se comprime y acelera a través de NetScaler Gateway. Cuando Citrix SD-WAN WANOP está habilitado para una conexión, las directivas de compresión TCP en NetScaler Gateway se deshabilitan.

El complemento Citrix SD-WAN WANOP se implementa y es compatible con el cliente Citrix Secure Access™.

NetScaler Gateway admite las versiones 5.5 y 6.1 del complemento Repeater y las versiones 6.2 y 7.0 del complemento Citrix SD-WAN WANOP.

La optimización WAN y el control de flujo de Citrix SD-WAN tienen prioridad sobre las funciones de optimización de NetScaler Gateway que requieren la modificación dinámica del contenido. Si la optimización WAN de Citrix SD-WAN está habilitada para el tráfico HTTP, las siguientes funciones de NetScaler Gateway no están disponibles:

- Inicio de sesión único en aplicaciones web
- Asociación de tipos de archivo
- Autorización HTTP

Para permitir el inicio de sesión único en aplicaciones web, puede inhabilitar la aceleración en HTTP. Para ello, utilice la línea de comandos. Inicie sesión en la consola serie de NetScaler Gateway y, a continuación, en un símbolo del sistema, escriba:

```
add vpn trafficAction ssoact http -SSO ON
```

El tráfico de red destinado a un puerto HTTP configurado en NetScaler Gateway se excluye automáticamente de la optimización WAN de Citrix SD-WAN. Esta es la configuración predeterminada. Si configura una directiva de tráfico para la optimización WAN de Citrix SD-WAN en un puerto HTTP, la directiva de tráfico se respeta y el tráfico de red se optimiza mediante Citrix SD-WAN WANOP. Sin embargo, las funciones de optimización de NetScaler Gateway se

© 1997–2026 Citrix Systems, Inc. All rights reserved.

inhabilitan para todo el tráfico afectado por esa directiva. Citrix SD-WAN WANOP puede acelerar el tráfico de red destinado a puertos no HTTP sin afectar a otras funciones de NetScaler Gateway.

Utilice una directiva de tráfico para configurar las conexiones de usuario para que utilicen el complemento Citrix SD-WAN WANOP. A continuación, puede vincular la directiva a usuarios, grupos, servidores virtuales o globalmente. La directiva se prioriza en función de dónde la vincule o del número de prioridad que le asigne.

## Para crear una directiva de tráfico

1. Vaya a **NetScaler Gateway > Directivas > Tráfico**.
2. En el panel de detalles, haga clic en **Agregar**.
3. En **Nombre**, escriba un nombre para la directiva.
4. Junto a Perfil de solicitud, haga clic en **Nuevo**.
5. En **Nombre**, escriba un nombre para el perfil.
6. En **Repetidor de sucursal**, seleccione **ACTIVADO** y, a continuación, haga clic en **Crear**.
7. En el cuadro de diálogo **Crear directiva de tráfico**, junto a **Agregar expresión**, seleccione o introduzca una expresión que represente los tipos de tráfico para habilitar la aceleración de Citrix SD-WAN WANOP.
8. Haga clic en **Agregar expresión**, haga clic en **Crear.** y, a continuación, haga clic en **Cerrar**.

Al agregar una expresión, elija una expresión de red para usar las mismas direcciones IP y rangos de puertos para los que Citrix SD-WAN WANOP está configurado para acelerar. Para que se produzca la aceleración de Citrix SD-WAN WANOP, los tipos de tráfico configurados en NetScaler Gateway deben coincidir con las directivas de clase de servicio configuradas en Citrix SD-WAN WANOP.

Todo el tráfico TCP se beneficia de la aceleración de Citrix SD-WAN WANOP. Si tiene previsto utilizar el inicio de sesión único, no acelere el tráfico HTTP porque la aceleración deshabilita el inicio de sesión único.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

# Configuración de la experiencia de usuario de RfWebUI Persona en Gateway

RfWebUI Persona es un tema que proporciona una nueva página de inicio de sesión y portal para los usuarios de NetScaler Gateway que inician sesión a través de NetScaler Gateway. El portal presenta a los usuarios de Receiver, StoreFront y Citrix Endpoint Management la misma GUI que verían al acceder directamente a uno de esos productos.

## Cuándo usar RfWebUI Persona

Utilice la persona RfWebUI en NetScaler Gateway cuando necesite una vista de panel único de todas las aplicaciones proporcionadas por diferentes productos de NetScaler, como aplicaciones web y de Software como servicio (SaaS), aplicaciones virtuales de Windows y escritorios.

Los siguientes escenarios ilustran el uso de RfWebUI Persona.

- Un usuario accede a StoreFront™ mediante Gateway y encuentra una GUI diferente a la que ve al acceder al producto sin Gateway.

  **Solución:** Cuando el usuario accede a StoreFront mediante Gateway, el tema RfWebUI proporciona una interfaz de usuario similar a la que ve al acceder al producto sin usar Gateway.

- Un usuario accede a las aplicaciones Citrix Workspace, StoreFront y Citrix Endpoint Management mediante Gateway y tiene dificultades para localizar las aplicaciones deseadas, ya que no están agrupadas de forma lógica.

  **Solución:** La persona RfWebUI proporciona una experiencia de usuario de vista de panel único al crear una agrupación lógica de aplicaciones proporcionadas por diferentes productos, como Receiver, StoreFront, Citrix Endpoint Management™ y otros.

## Funcionalidades proporcionadas por RfWebUI Persona

La nueva RfWebUI proporciona las siguientes características:

- GO

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Agregación de aplicaciones
- Enlaces de proxy de Protocolo de escritorio remoto (RDP) configurados por el usuario
- Aplicaciones favoritas

## GO

**GO:** La función Go proporciona acceso a páginas web a través de VPN sin cliente. El usuario simplemente escribe la URL en la sección **URL** de la pestaña **Marcador** y hace clic en **GO**.

Actualmente, la función **GO** solo admite aplicaciones web de Outlook (OWA) y URL de SharePoint.

**Nota** La ficha **GO** solo es visible si el parámetro `clientlessAccessVPNMode` de la directiva de sesión está **Habilitado**.

## Agregación de aplicaciones

**Agregación de aplicaciones:** El tema RfWebUI proporciona una vista de panel único al agrupar las aplicaciones proporcionadas por diferentes productos bajo banners descriptivos. Por ejemplo, todas las URL VPN configuradas por un administrador de NetScaler se encuentran en un paquete denominado **Aplicaciones web y SaaS**, y los marcadores web específicos del usuario se encuentran en **Marcadores personales**. Si los paquetes de aplicaciones de Citrix Virtual Apps and Desktops están configurados en StoreFront, la vista de panel único en NetScaler Gateway también enumera estos paquetes.

## Enlaces de proxy RDP configurados por el usuario

Los usuarios pueden agregar un enlace de proxy RDP como marcador personal. Los marcadores personales aparecen en la ficha **Escritorios**.

Se admiten los siguientes modos RDP:

- Puerta de enlace única
- Puerta de enlace sin estado (doble)

**Nota:** Un usuario puede agregar enlaces de proxy RDP solo si se configura un `RDPclientprofile`. Para obtener más información sobre las configuraciones RDP, consulte la documentación del proxy RDP.

## Aplicaciones favoritas

Los usuarios pueden agregar las aplicaciones deseadas que aparecen en **Aplicación web y SaaS** y en **Marcadores personales** a la ficha **FAVORITOS** haciendo clic en el enlace **Agregar a**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**favoritos** que aparece junto al nombre de la aplicación. Las aplicaciones, una vez agregadas, se pueden ver en la ficha **FAVORITOS**. También se pueden eliminar de la ficha **FAVORITOS** haciendo clic en el enlace **ELIMINAR** que aparece junto a la aplicación dentro de la ficha **FAVORITOS**.

# Consideraciones al habilitar la persona RfWebUI

La persona RfWebUI no es totalmente compatible con lo siguiente:

**Función de uso compartido de archivos:** La función de uso compartido de archivos, para acceder a recursos compartidos de archivos SMB, no es compatible. **Email Home:** El parámetro VPN **Email Home** no está disponible como vista incrustada para el portal de NetScaler Gateway. Se puede acceder a él como una aplicación en el paquete **Aplicaciones web y SaaS** en la ficha **APLICACIONES** de RfWebUI. **Cliente Java:** El cliente Java basado en navegador para establecer un túnel SSL no está disponible en este tema.

## Configuración de la persona RfWebUI

**Para aplicar la persona RfWebUI**:

1. En la interfaz de NetScaler, vaya a **Configuration > NetScaler Gateway Portal Themes**.
2. En la página **Portal Themes**, seleccione la casilla de verificación **RfWebUI**.
3. Haga clic en el icono **Save** en la esquina superior derecha de la página **Portal Themes**.
4. En el cuadro de diálogo **Save Confirmation**, haga clic en **Yes**.

# Parámetros de configuración de RfWebUI

El comportamiento general del portal de NetScaler Gateway está influenciado por dos archivos de configuración: el archivo de configuración local de NetScaler Gateway y el archivo de StoreFront.

Según su implementación, puede modificar el comportamiento del portal de NetScaler Gateway cambiando las propiedades en el archivo «plugins.xml». Este archivo aparece como un archivo de configuración en el navegador, que es la solicitud de `/var/netscaler/logon/themes/<custom_theme>/plugins.xml`.

Durante el inicio de sesión, se utilizan los archivos de configuración de NetScaler Gateway. Pero cuando se conecta a StoreFront, StoreFront envía una nueva configuración y la configuración anterior se sobrescribe. Este comportamiento difiere para la VPN sin cliente y para ICA.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Para ICA, la configuración de StoreFront siempre tiene prioridad, pero algunos de los comportamientos en la VPN sin cliente que están influenciados por la configuración de NetScaler Gateway se mantienen incluso después de que la nueva configuración se actualiza desde StoreFront.

La siguiente tabla enumera los parámetros que describen la configuración que tiene prioridad sobre la VPN sin cliente y ICA.

| TIPO DE CONFIGURACIÓN | SUBTIPO DE CONFIGURACIÓN | PARÁMETRO | VPN SIN CLIENTE | ICA | DESCRIPCIÓN |
|---|---|---|---|---|---|
| Sesión para VPN sin cliente / AuthManager para ICA | - | loginFormTimeout | NetScaler Gateway | - | Define el tiempo en minutos para el tiempo de espera de la página de inicio de sesión |
| Asistente de plug-in | - | habilitado | StoreFront | StoreFront | Habilitar o deshabilitar el asistente de plug-in |
| Asistente de plug-in | - | upgradeAtLogin | StoreFront | StoreFront | Solicita la actualización del plug-in al iniciar sesión |
| Asistente de plug-in | - | showAfterLogin | NetScaler Gateway | StoreFront | Muestra el mensaje del plug-in después de iniciar sesión |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| TIPO DE CONFIGURACIÓN | SUBTIPO DE CONFIGURACIÓN | PARÁMETRO | VPN SIN CLIENTE | ICA | DESCRIPCIÓN |
|---|---|---|---|---|---|
| Asistente de plug-in | - | showOnlyIfRequiredByApps | NetScaler Gateway | StoreFront | Muestra el mensaje del plug-in después de iniciar sesión, si lo requieren las aplicaciones |
| Asistente de plug-in | macOS/win32 | ruta | NetScaler Gateway | StoreFront | Define la ruta de descarga para los plug-ins |
| Asistente de plug-in | protocolHandler | habilitado | NetScaler Gateway | StoreFront | Alternar la página del controlador de protocolo antes de iniciar el plug-in |
| Asistente de plug-in | protocolHandler | plataformas | NetScaler Gateway | StoreFront | Identifica la plataforma compatible para el plug-in |
| Asistente de plug-in | - | skipDoubleHopCheckWhenDisabled | • NetScaler Gateway | StoreFront | Alternar la comprobación de configuración de doble salto de NetScaler Gateway |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| TIPO DE CONFIGURACIÓN | SUBTIPO DE CONFIGURACIÓN | PARÁMETRO | VPN SIN CLIENTE | ICA | DESCRIPCIÓN |
|---|---|---|---|---|---|
| | | | | | para el paso a través de ICA |
| Interfaz de usuario | - | frameOptions | NA | NA | - |
| Interfaz de usuario | | autoLaunchDesktop | StoreFront | StoreFront | Habilitar o deshabilitar el inicio del escritorio |
| Interfaz de usuario | workspaceControl | habilitado | StoreFront | StoreFront | Habilitar o deshabilitar el control del espacio de trabajo |
| Interfaz de usuario | workspaceControl | autoReconnectAtLogon | StoreFront | StoreFront | Alternar para reconectar automáticamente la sesión anterior si está disponible |
| Interfaz de usuario | workspaceControl | logoffAction | StoreFront | StoreFront | Define el comportamiento de cierre de sesión de Citrix Workspace |
| Interfaz de usuario | workspaceControl | showReconnectButton | StoreFront | StoreFront | Mostrar u ocultar el botón |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| TIPO DE CONFIGURACIÓN | SUBTIPO DE CONFIGURACIÓN | PARÁMETRO | VPN SIN CLIENTE | ICA | DESCRIPCIÓN |
|---|---|---|---|---|---|
| | | | | | **Volver a conectar** |
| Interfaz de usuario | workspaceControl | showDisconnectButton | StoreFront | StoreFront | Mostrar u ocultar el botón **desconectar** |
| Interfaz de usuario | workspaceControl | showDesktopsView | StoreFront | StoreFront | Mostrar u ocultar la vista de escritorios |
| Interfaz de usuario | workspaceControl | showAppsView | StoreFront | StoreFront | Mostrar u ocultar la vista de aplicaciones |
| Interfaz de usuario | control del espacio de trabajo | vista predeterminada | StoreFront | StoreFront | Seleccione la vista de Escritorio o la vista de Aplicación |
| Interfaz de usuario | configuración del receptor | habilitado | StoreFront | StoreFront | Alternar la configuración del receptor |
| Interfaz de usuario | configuración del receptor | mostrar solo si lo requieren las aplicaciones | NetScaler Gateway | NetScaler Gateway | Mostrar el mensaje del receptor si lo requieren las aplicaciones |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| TIPO DE CONFIGURACIÓN | SUBTIPO DE CONFIGURACIÓN | PARÁMETRO | VPN SIN CLIENTE | ICA | DESCRIPCIÓN |
|---|---|---|---|---|---|
| Interfaz de usuario | receiverConfiguration | downloadURL | StoreFront | StoreFront | Descargar la URL para el receptor |
| Interfaz de usuario | appShortcuts | habilitado | StoreFront | StoreFront | Habilitar o deshabilitar la pestaña de acceso directo a la aplicación |
| Interfaz de usuario | appShortcuts | allowSessionReconnect | StoreFront | StoreFront | Permitir reconexión de sesión |

Para reflejar la configuración modificada de StoreFront en RfWebUI para VPN sin cliente e ICA, actualice manualmente el parámetro correspondiente en el archivo de configuración de NetScaler Gateway. Por ejemplo, si `if pluginAssistant.html5.enabled` está establecido en `Off` en la configuración de StoreFront, actualice el parámetro correspondiente en el archivo de configuración de NetScaler Gateway.

Personalice los parámetros de RfWebUI en el archivo de configuración de NetScaler Gateway para que coincidan con la configuración de StoreFront siguiendo estos pasos:

1. Abra `/var/netscaler/logon/themes/<customtheme>/plugins.xml`.

   **NOTA:**

   Si el tema personalizado se creó en una versión anterior, el archivo "plugins.xml" de la carpeta del tema personalizado podría estar vacío. Ejecute el siguiente comando para rellenar "plugins.xml" con el contenido necesario.

   `cp /var/netscaler/logon/LogonPoint/homeconfig.xml /var/netscaler/logon/themes/<customtheme>/plugins.xml`

   No modifique `/var/netscaler/logon/LogonPoint/homeconfig.xml`.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Edite solo los parámetros necesarios y vacíe la caché de NetScaler® mediante el siguiente comando:

```
flush cache contentgroup loginstaticobjects
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

# Personalización del portal de Gateway mediante plug-ins personalizados

El marco RfWebUi de NetScaler Gateway proporciona la capacidad de agregar plug-ins personalizados para personalizar su portal de Gateway. Estos plug-ins personalizados se pueden usar para agregar una gran funcionalidad al Gateway, por ejemplo, si desea agregar una página completamente nueva en el flujo del Gateway. Para otros casos de uso, el código se puede agregar al archivo de script personalizado proporcionado para los temas del Gateway en la ubicación /`var/netscaler/logon/themes/<custom_theme>/script.js`.

**NOTA:**

NetScaler Gateway solo admite la creación y el uso de plug-ins personalizados para la personalización del portal. NetScaler Gateway no crea ni proporciona ningún plug-in personalizado basado en los requisitos del cliente.

1. Para agregar un plug-in personalizado, cree el archivo JavaScript en la ubicación `/var/netscaler/logon/LogonPoint/plugins/ns-gateway/`. Por ejemplo, puede encontrar los siguientes plug-ins en `/var/netscaler/logon/LogonPoint/plugins/ns-gateway/`.

   - ns-nfactor.js
   - nsg-epa.js
   - nsg-setclient.js

   Se recomienda introducir el nombre del plug-in en el formato `<plugin_name>`.js.

   Todos estos archivos de plug-in son obtenidos por el marco RfWebUI según lo requiera la funcionalidad.

2. Después de crear el archivo del plug-in, use el siguiente código como ejemplo para registrar el plug-in con el marco RfWebUI.

```
(function ($) {

            CTXS.ExtensionAPI.addPlugin( {
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
                        Name : “plugin name”,

                        initialize: function() {}

            });

    })(jQuery);
```

donde,

**name** es el nombre que se le da al plug-in. Se utiliza como identificador del plug-in.

**initialize** toma la función como parámetro que se utiliza para inicializar el plug-in.

3. Introduzca el nombre del plug-in y la función de inicialización en la función `CTXS.ExtensionAPI.addPlugin()` para registrar el plug-in. El nombre y la ubicación del plug-in agregado deben registrarse en el archivo plugins.xml en la ubicación `/var/netscaler/logon/themes/<custom_theme>/plugins.xml`.
4. Después de escribir el código del plug-in, el nombre y la ubicación del plug-in recién agregado deben registrarse con el archivo `plugins.xml` en la ubicación `/var/netscaler/logon/themes/<custom_theme>/plugins.xml`. El plug-in debe registrarse con la etiqueta `plug-in`.

```
<plugins>

<plugin name="nsg-epa" src="plugins/ns-gateway/nsg-epa.js"/>

<plugin name="nsg-setclient" src="plugins/ns-gateway/nsg-setclient.js"/
>

<plugin name="ns-nfactorn" src="plugins/ns-gateway/ns-nfactor.js"/>

</plugins>
```

5. Introduzca un nombre y un src para el plug-in para que RFWebUI pueda identificar y recuperar el plug-in.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

# Ejemplo de configuración

Las siguientes configuraciones de ejemplo se pueden utilizar para agregar un plug-in personalizado para añadir un pie de página a la página de inicio de sesión de NetScaler Gateway.

1. Cree el archivo de plug-in de JavaScript en la ubicación, `/var/netscaler/logon/LogonPoint/plugins/ns-gateway/.`.
2. Asigne el nombre ns-footer.js al plug-in `/var/netscaler/logon/LogonPoint/plugins/ns-gateway/ns-footer.js`
3. Agregue el siguiente código al plug-in registrado en RfWebUI y, en la función de inicialización, agregue el pie de página a la puerta de enlace.

```
(function ($) {

CTXS.ExtensionAPI.addPlugin({

    name: "ns-footer", // Name of plugin - must match name sent in
configuration

    initialize: function () {



    // Add the footer for the login page

    $("#customExplicitAuthBottom").append("<div style='text-
align:center;color:white;font-size:15px;'><br />Disclaimer<br /><br /
>"+" Access to this website is restricted to employees of Login
Consultants<br/></div>");



    // To Add the footer to the login timeout page

    $("#customAuthBottom").append("<div style='text-
align:center;color:white;font-size:15px;'><br >Disclaimer<br /><br /
>"+" Access to this website is restricted to employees of Login
Consultants<br /></div>");



    callback();
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    }

});

})(jQuery);
```

4. Guarde el archivo.
5. Agregue el nombre y el src en plugins.xml en la ubicación `var/netscaler/logon/themes/<custom_theme>/plugins.xml`.

```
<plugins>

<plugin name="nsg-epa" src="plugins/ns-gateway/nsg-epa.js" />

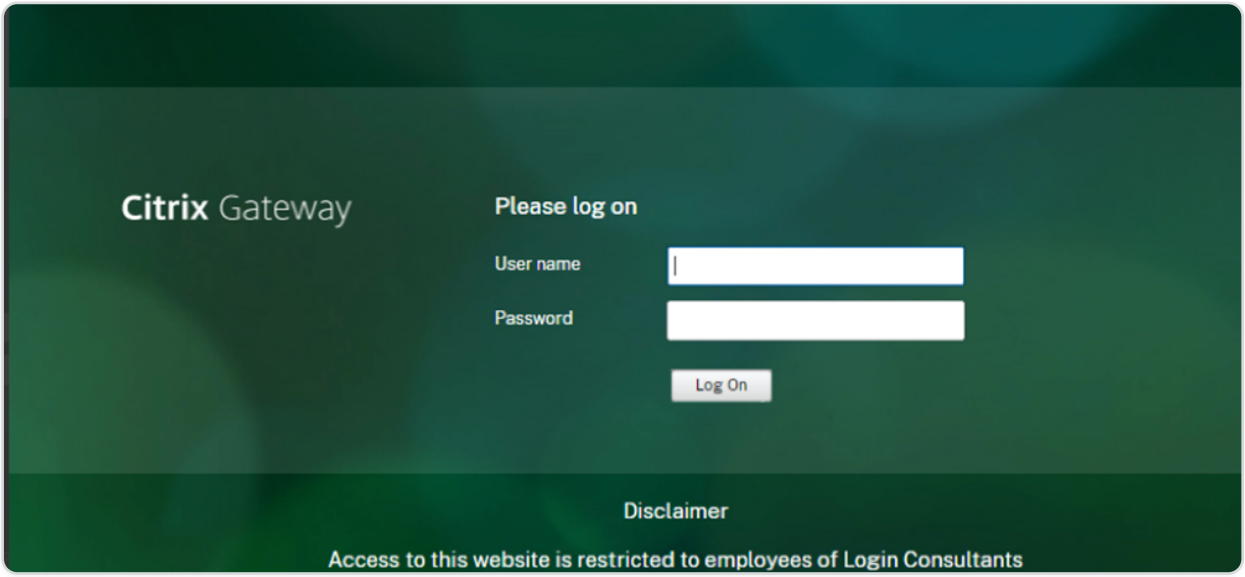
<plugin name="nsg-setclient" src="plugins/ns-gateway/nsg-
setclient.js" />

<plugin name="ns-nfactor" src="plugins/ns-gateway/ns-nfactor.js" />

<plugin name="ns-footer" src="plugins/ns-gateway/ns-footer.js" />

</plugins>
```

6. Configure el tema personalizado para el que se agrega el plug-in.
7. Vacíe la caché usando el comando `flush cache contentgroup loginstaticobjects`.
8. Vuelva a cargar la pantalla del portal. El pie de página se agrega a la página de inicio de sesión de NetScaler Gateway.




© 1997–2026 Citrix Systems, Inc. All rights reserved.

# Personalización del portal de Gateway mediante plug-ins personalizados

El marco RfWebUi de NetScaler Gateway proporciona la capacidad de agregar plug-ins personalizados para personalizar su portal de Gateway. Estos plug-ins personalizados se pueden usar para agregar una gran funcionalidad al Gateway, por ejemplo, si desea agregar una página completamente nueva en el flujo del Gateway. Para otros casos de uso, el código se puede agregar al archivo de script personalizado proporcionado para los temas del Gateway en la ubicación /`var/netscaler/logon/themes/<custom_theme>/script.js`.

**NOTA:**

NetScaler Gateway solo admite la creación y el uso de plug-ins personalizados para la personalización del portal. NetScaler Gateway no crea ni proporciona ningún plug-in personalizado basado en los requisitos del cliente.

1. Para agregar un plug-in personalizado, cree el archivo JavaScript en la ubicación `/var/netscaler/logon/LogonPoint/plugins/ns-gateway/`. Por ejemplo, puede encontrar los siguientes plug-ins en `/var/netscaler/logon/LogonPoint/plugins/ns-gateway/`.

   - ns-nfactor.js
   - nsg-epa.js
   - nsg-setclient.js

   Se recomienda introducir el nombre del plug-in en el formato `<plugin_name>`.js.

   Todos estos archivos de plug-in son obtenidos por el marco RfWebUI según lo requiera la funcionalidad.

2. Después de crear el archivo del plug-in, use el siguiente código como ejemplo para registrar el plug-in con el marco RfWebUI.

```
(function ($) {

            CTXS.ExtensionAPI.addPlugin( {

                        Name : “plugin name”,

                        initialize: function() {}
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
            });

    })(jQuery);
```

donde,

**name** es el nombre que se le da al plug-in. Se utiliza como identificador del plug-in.

**initialize** toma la función como parámetro que se utiliza para inicializar el plug-in.

3. Introduzca el nombre del plug-in y la función de inicialización en la función `CTXS.ExtensionAPI.addPlugin()` para registrar el plug-in. El nombre y la ubicación del plug-in agregado deben registrarse en el archivo plugins.xml en la ubicación `/var/netscaler/logon/themes/<custom_theme>/plugins.xml`.
4. Después de escribir el código del plug-in, el nombre y la ubicación del plug-in recién agregado deben registrarse con el archivo `plugins.xml` en la ubicación `/var/netscaler/logon/themes/<custom_theme>/plugins.xml`. El plug-in debe registrarse con la etiqueta `plug-in`.

```
<plugins>

<plugin name="nsg-epa" src="plugins/ns-gateway/nsg-epa.js"/>

<plugin name="nsg-setclient" src="plugins/ns-gateway/nsg-setclient.js"/
>

<plugin name="ns-nfactorn" src="plugins/ns-gateway/ns-nfactor.js"/>

</plugins>
```

5. Introduzca un nombre y un src para el plug-in para que RFWebUI pueda identificar y recuperar el plug-in.

## Ejemplo de configuración

Las siguientes configuraciones de ejemplo se pueden utilizar para agregar un plug-in personalizado para añadir un pie de página a la página de inicio de sesión de NetScaler Gateway.

1. Cree el archivo de plug-in de JavaScript en la ubicación, `/var/netscaler/logon/LogonPoint/plugins/ns-gateway/.`.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Asigne el nombre ns-footer.js al plug-in `/var/netscaler/logon/LogonPoint/plugins/ns-gateway/ns-footer.js`
3. Agregue el siguiente código al plug-in registrado en RfWebUI y, en la función de inicialización, agregue el pie de página a la puerta de enlace.

```
(function ($) {

CTXS.ExtensionAPI.addPlugin({

    name: "ns-footer", // Name of plugin - must match name sent in
configuration

    initialize: function () {



    // Add the footer for the login page

    $("#customExplicitAuthBottom").append("<div style='text-
align:center;color:white;font-size:15px;'><br />Disclaimer<br /><br /
>"+" Access to this website is restricted to employees of Login
Consultants<br/></div>");



    // To Add the footer to the login timeout page

    $("#customAuthBottom").append("<div style='text-
align:center;color:white;font-size:15px;'><br >Disclaimer<br /><br /
>"+" Access to this website is restricted to employees of Login
Consultants<br /></div>");



    callback();

    }

});

})(jQuery);
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. Guarde el archivo.
5. Agregue el nombre y el src en plugins.xml en la ubicación `var/netscaler/logon/themes/<custom_theme>/plugins.xml`.

```
<plugins>

<plugin name="nsg-epa" src="plugins/ns-gateway/nsg-epa.js" />

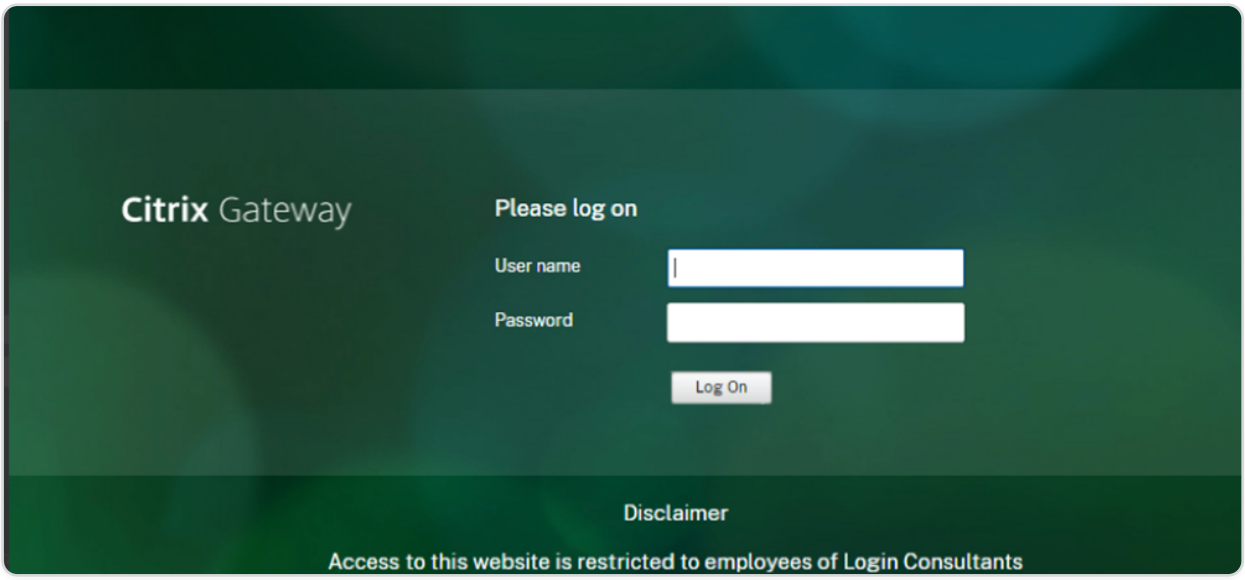
<plugin name="nsg-setclient" src="plugins/ns-gateway/nsg-
setclient.js" />

<plugin name="ns-nfactor" src="plugins/ns-gateway/ns-nfactor.js" />

<plugin name="ns-footer" src="plugins/ns-gateway/ns-footer.js" />

</plugins>
```

6. Configure el tema personalizado para el que se agrega el plug-in.
7. Vacíe la caché usando el comando `flush cache contentgroup loginstaticobjects`.
8. Vuelva a cargar la pantalla del portal. El pie de página se agrega a la página de inicio de sesión de NetScaler Gateway.




# Crear y personalizar el esquema de inicio de sesión

El esquema de inicio de sesión es el archivo XML que proporciona la estructura para la autenticación basada en formularios. Los usuarios pueden utilizar una amplia gama de formularios

© 1997–2026 Citrix Systems, Inc. All rights reserved.

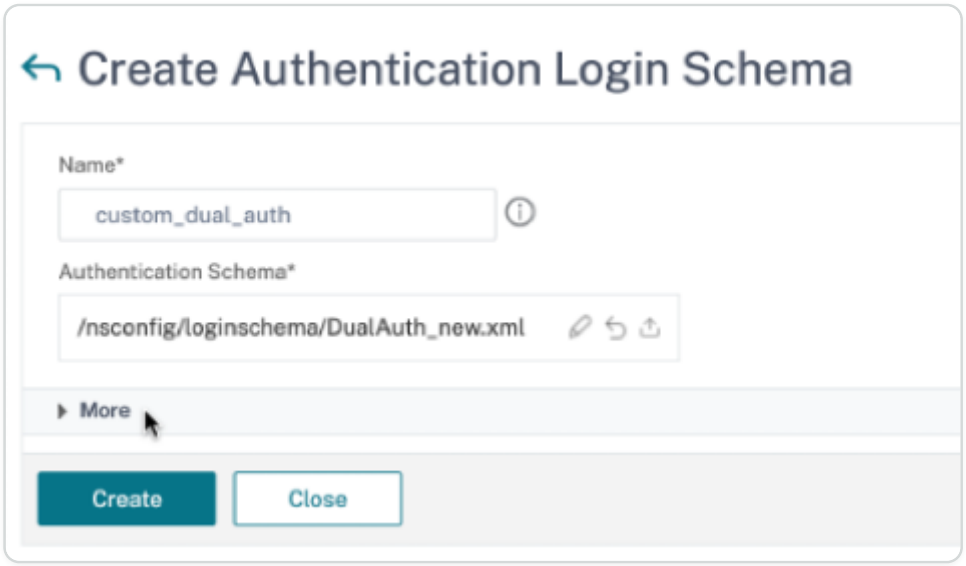
de autenticación mediante un conjunto de construcciones de interfaz de usuario similares a los formularios HTML básicos.

En las autenticaciones nFactor, los factores de autenticación se encadenan. Cada factor puede tener diferentes páginas o archivos de esquema de inicio de sesión. En algunos escenarios de autenticación, los usuarios pueden ver varias pantallas de inicio de sesión. También puede tener un esquema de inicio de sesión que recopile la información que se puede pasar a varios factores para que estos últimos no tengan que mostrar otro esquema de inicio de sesión.

Los archivos XML del esquema de inicio de sesión se incluyen con el dispositivo NetScaler en `/nsconfig/loginschema/LoginSchema`.

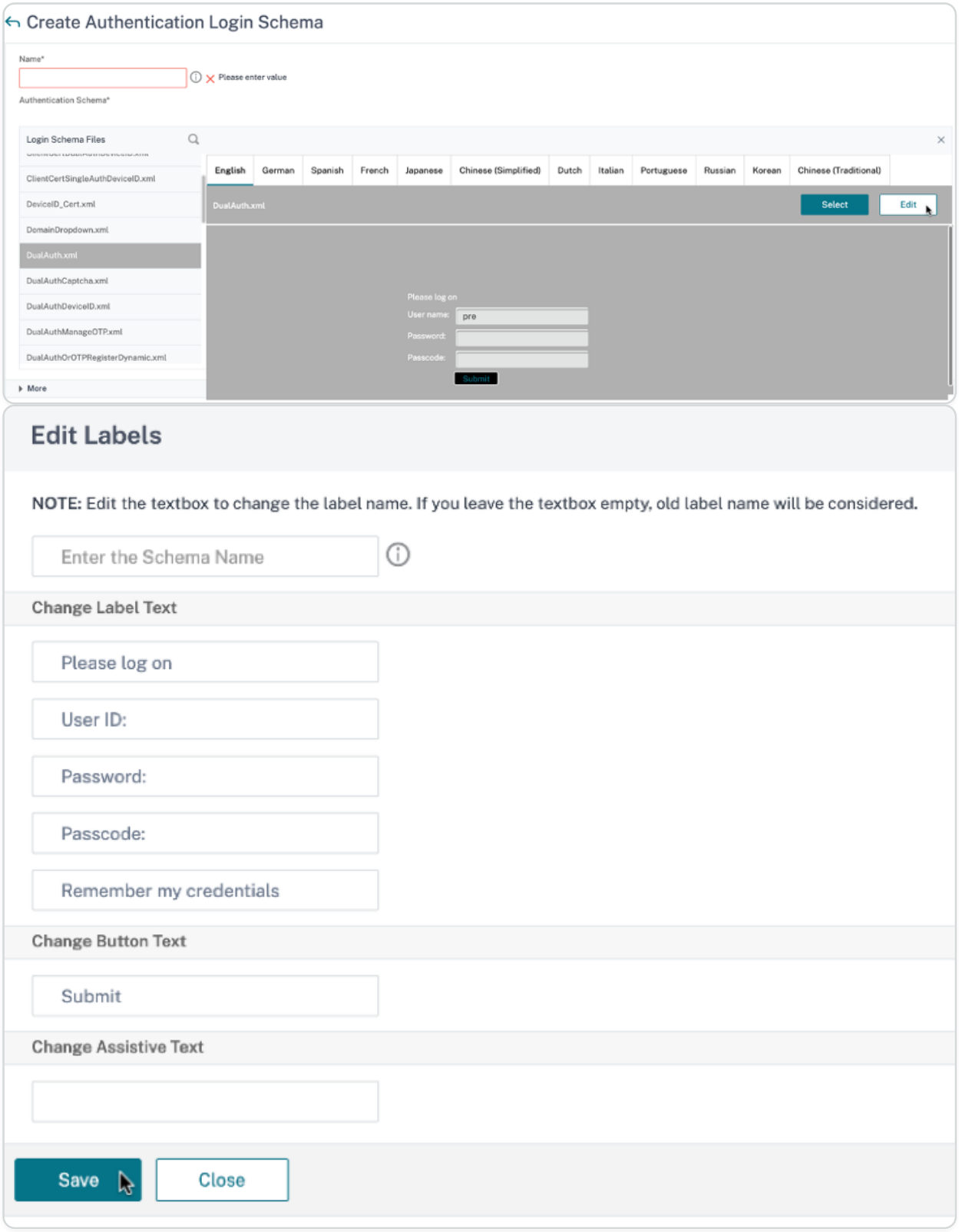
## Crear un perfil de esquema de inicio de sesión

1. Vaya a **Seguridad > AAA > Esquema de inicio de sesión**.
2. Haga clic en la pestaña **Perfiles** y, a continuación, en **Agregar**.
3. En **Esquema de autenticación**, haga clic en el icono del lápiz.




4. Haga clic en la carpeta **LoginSchema** para ver los archivos que contiene.
5. Seleccione uno de los archivos y realice los cambios según sea necesario.
    - Cambie las etiquetas haciendo clic en el botón Editar en la parte superior derecha.
    - Edite el esquema seleccionando el idioma.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

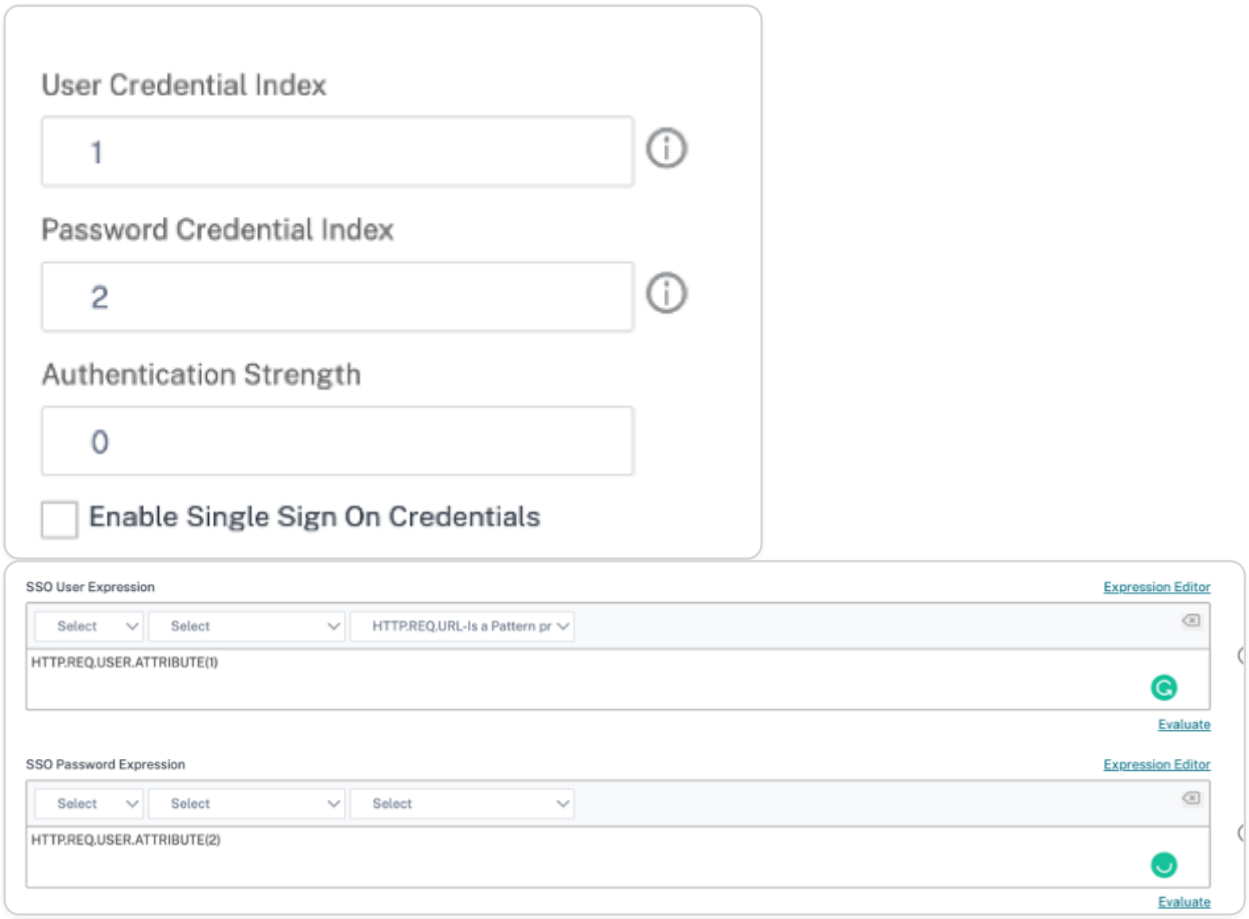



**Nota:** Cuando guarde los cambios después de la modificación, se creará un nuevo archivo XML de esquema con los cambios.

6. En la parte superior derecha, haga clic en **Seleccionar** para seleccionar el XML de esquema modificado.
7. Introduzca un nombre de esquema de inicio de sesión y haga clic en **Más**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**Nota:** Puede usar las credenciales ya introducidas en otro lugar. Por ejemplo, puede usar el nombre de usuario y una de las contraseñas para el inicio de sesión único en StoreFront. Puede hacer clic en **Más** e introducir valores únicos para los índices. Estos valores pueden estar entre 1 y 16. Puede hacer referencia a estos valores de índice en una directiva o perfil de tráfico mediante la expresión REQ.USER.ATTRIBUTE(#).




8. Haga clic en **Crear** para crear el perfil de esquema de inicio de sesión.

## Vincular un perfil de esquema de inicio de sesión a un servidor virtual de autenticación, autorización y auditoría

Para vincular un perfil de esquema de inicio de sesión a un servidor virtual de autenticación, autorización y auditoría, primero debe crear una directiva de esquema de inicio de sesión. Las directivas de esquema de inicio de sesión no son necesarias al vincular el perfil de esquema de inicio de sesión a una etiqueta de directiva de autenticación.

Para crear y vincular una directiva de esquema de inicio de sesión:

1. Vaya a **Seguridad > AAA > Esquema de inicio de sesión**.
2. Haga clic en la ficha **Directivas** y, a continuación, haga clic en **Agregar**.
3. En **Perfil**, seleccione el perfil de esquema de inicio de sesión creado anteriormente.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

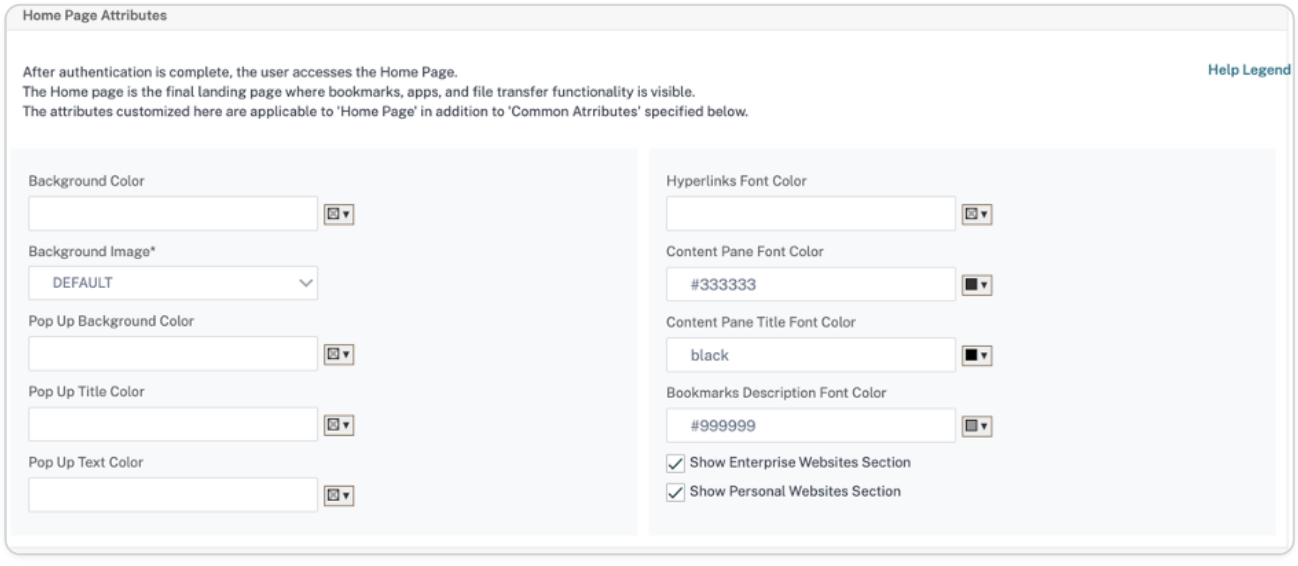
4. En **Regla**, introduzca la expresión de sintaxis predeterminada y haga clic en **Crear**.

# Personalizaciones del portal desde la interfaz de usuario de administración

Los administradores pueden personalizar los temas del portal creando temas personalizados para lograr una apariencia personalizada del portal de usuario. Los temas personalizados se pueden crear a partir de los temas RfWebUI, Default, X1 y GreenBubble.

**Para crear los temas personalizados:**

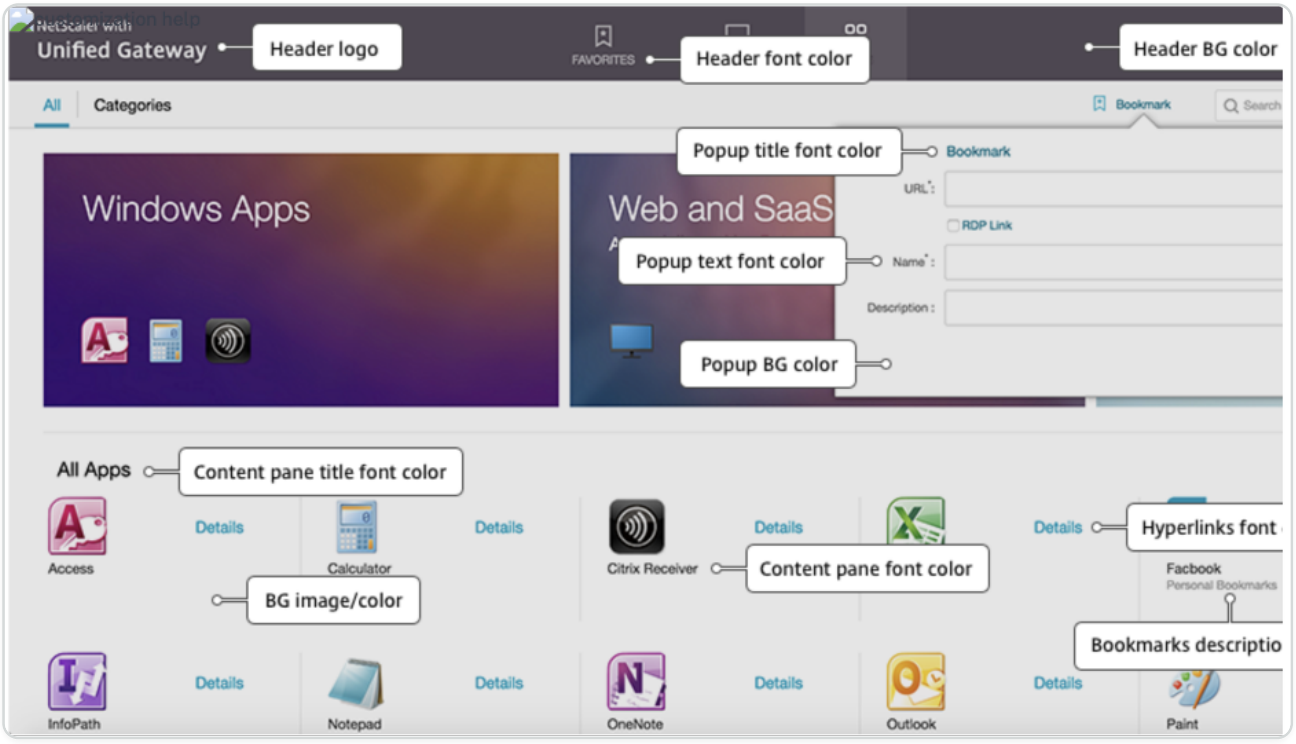
1. En la ficha Configuración, vaya a **NetScaler Gateway > Temas del portal** y haga clic en **Agregar**.
2. Introduzca un nombre para el tema personalizado.
3. En **Tema de plantilla**, seleccione el tema base, según sus requisitos. **RfWebUI** está seleccionado de forma predeterminada.
4. Haga clic en **Aceptar**.
5. En la sección **Aspecto**, modifique los atributos según sus requisitos para la página de inicio y haga clic en **Aceptar**.




La siguiente figura muestra el tema personalizado basado en RfWebUi.

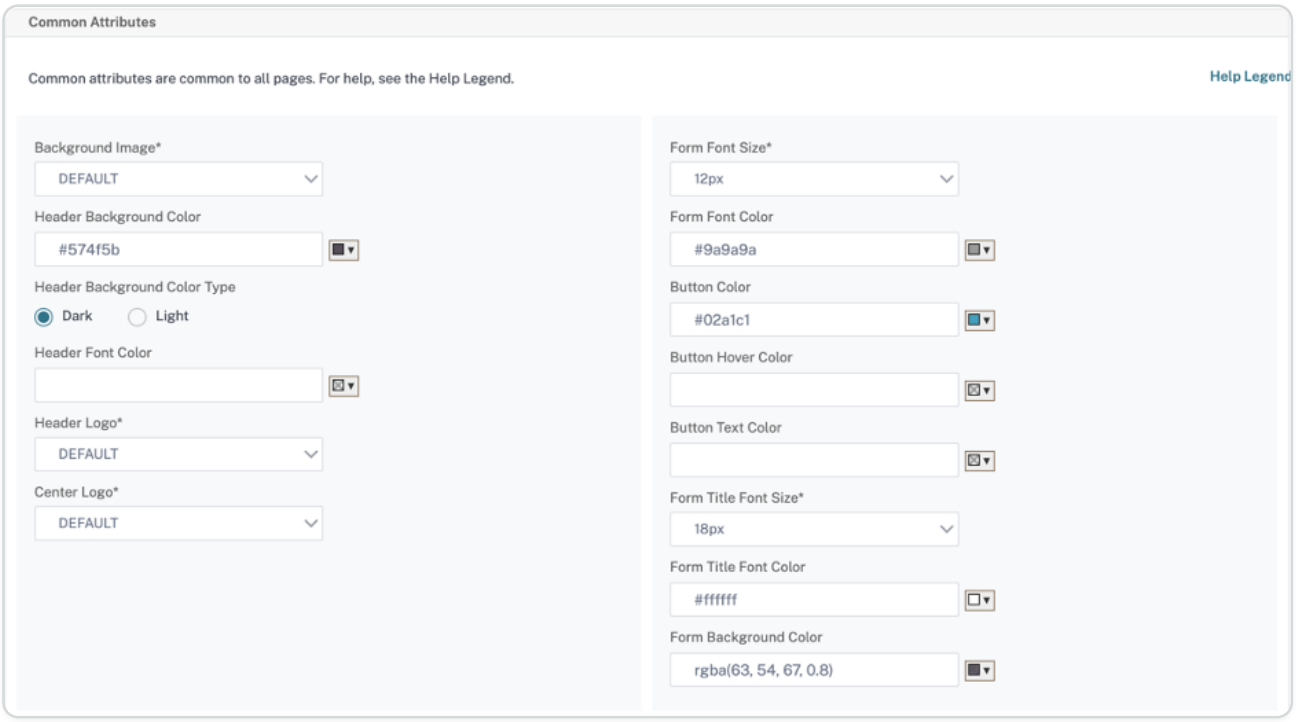
El enlace **Leyenda de ayuda** muestra la visualización gráfica de la página con los nombres de las secciones para ayudarle a elegir qué desea editar.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



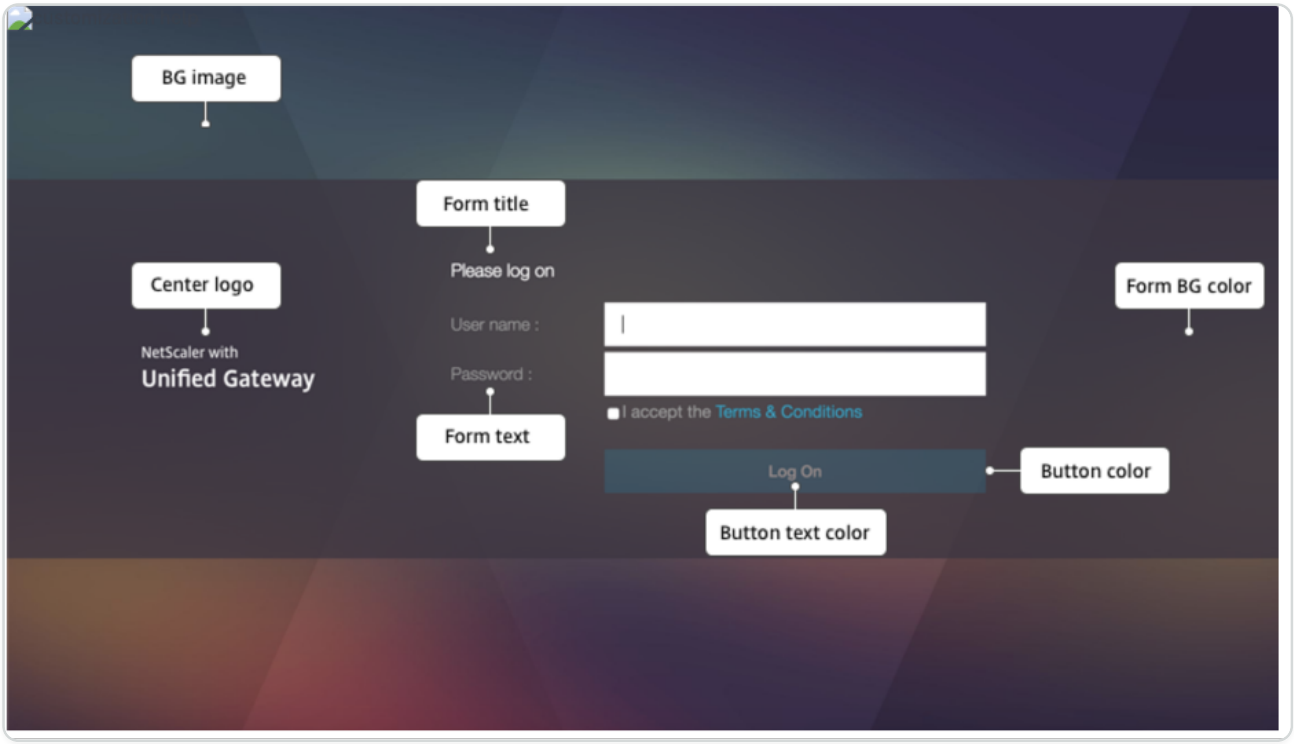

## Atributos comunes

La sección **Atributos comunes** proporciona la configuración configurable que es común a todas las páginas de inicio de sesión de NetScaler Gateway.

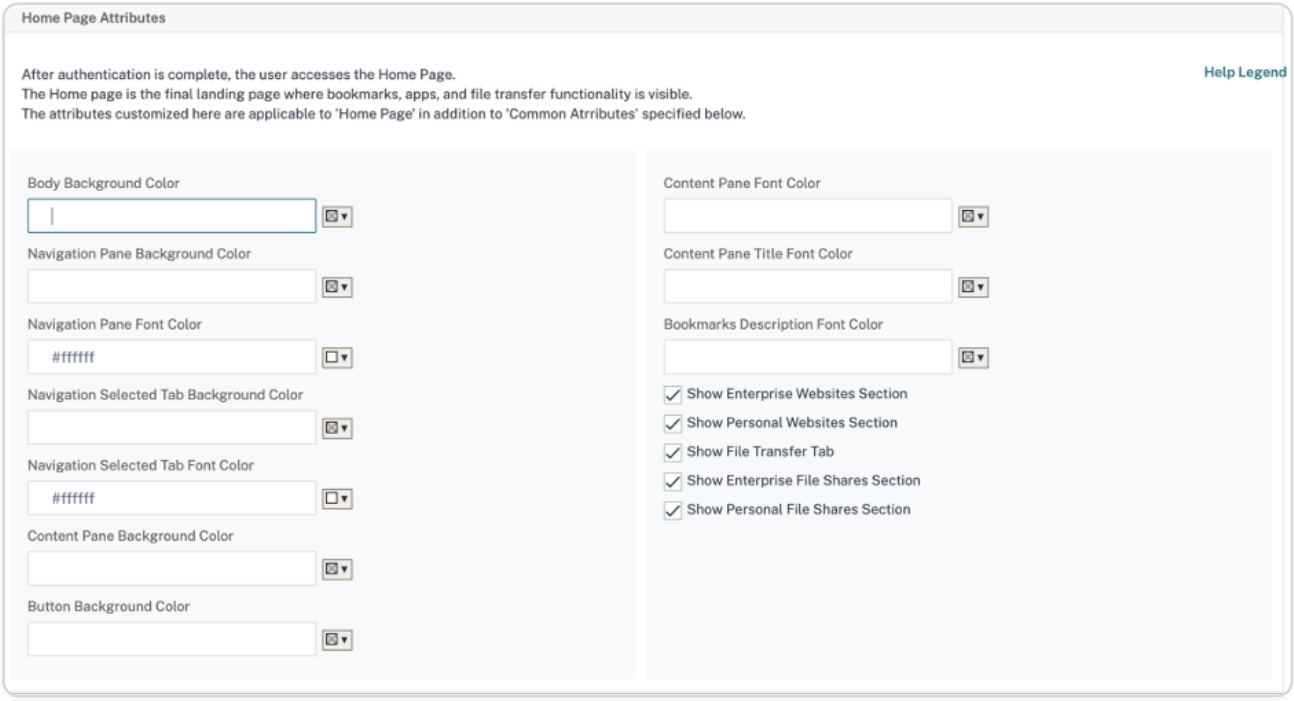



Haga clic en el enlace **Leyenda de ayuda** para ver cada parámetro configurable común.

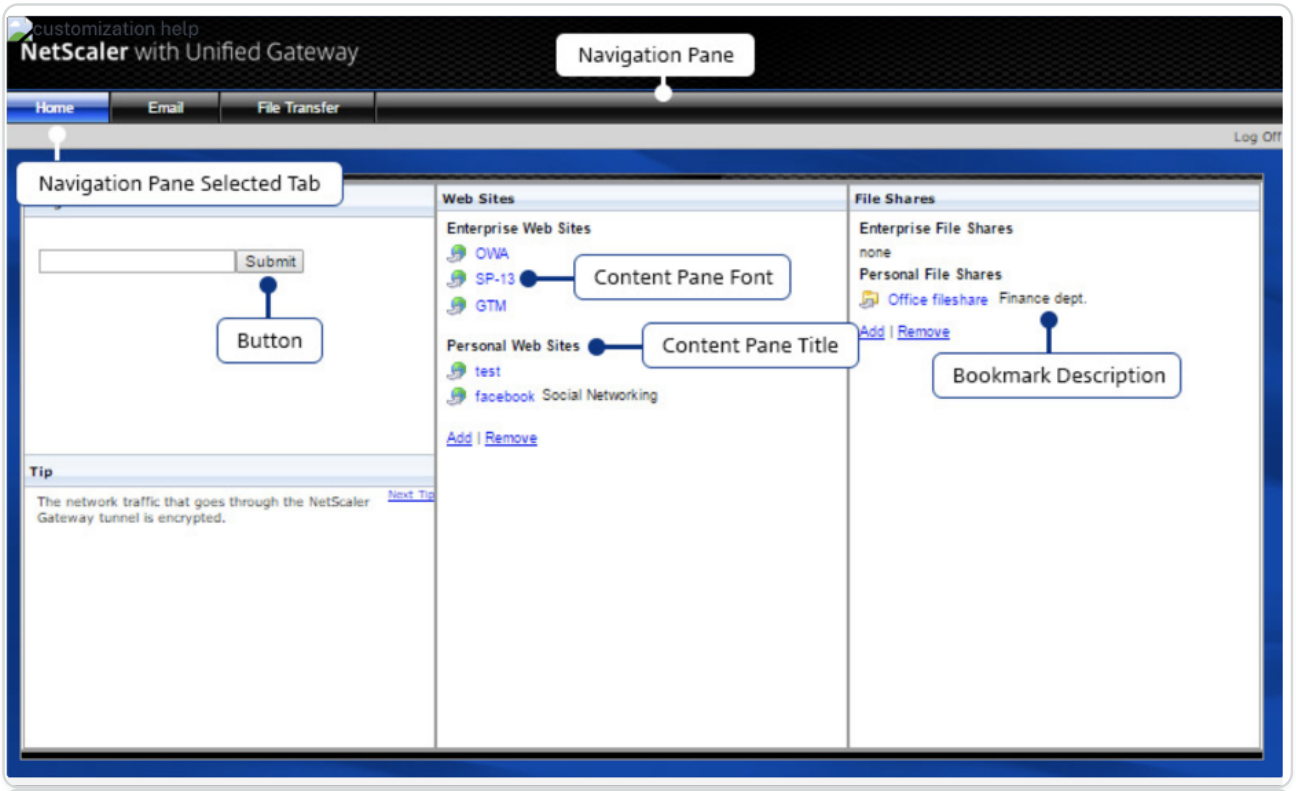
© 1997–2026 Citrix Systems, Inc. All rights reserved.

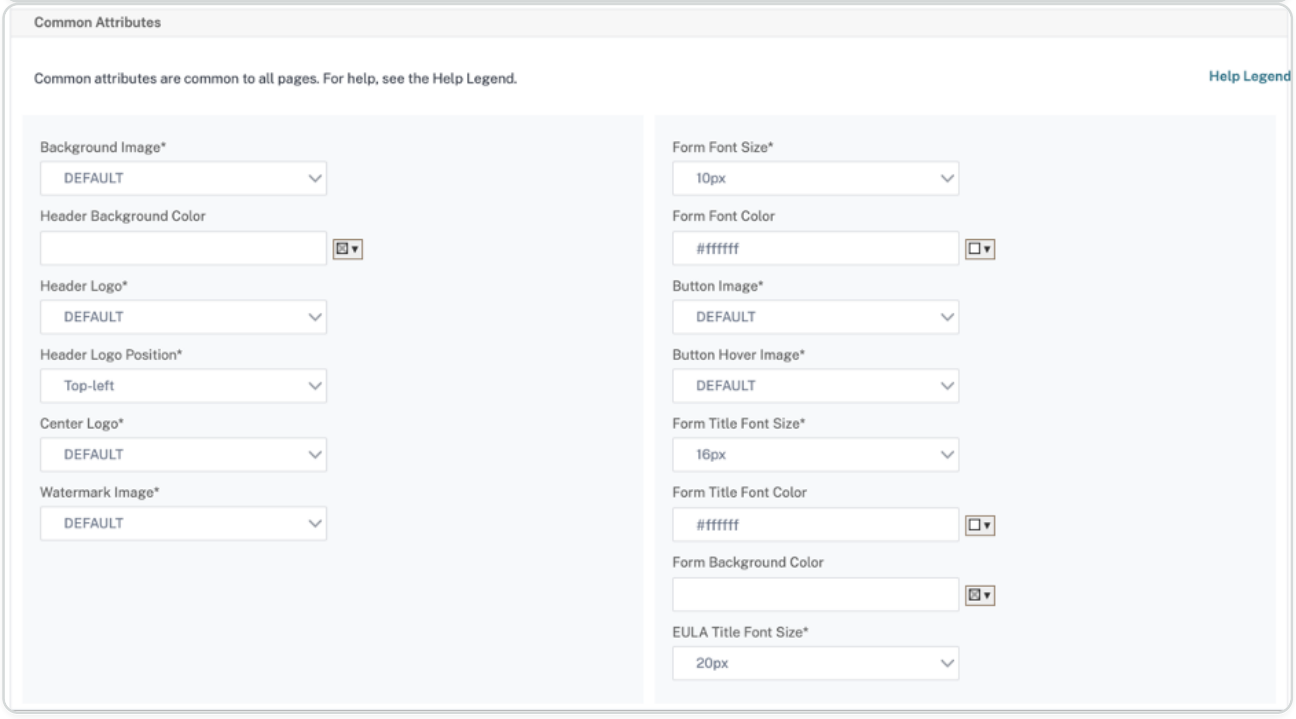



Del mismo modo, para el tema personalizado basado en **Default**, la siguiente figura muestra la configuración disponible para la página de inicio. **Nota:** Esta configuración es diferente para x1 y GreenBubble.

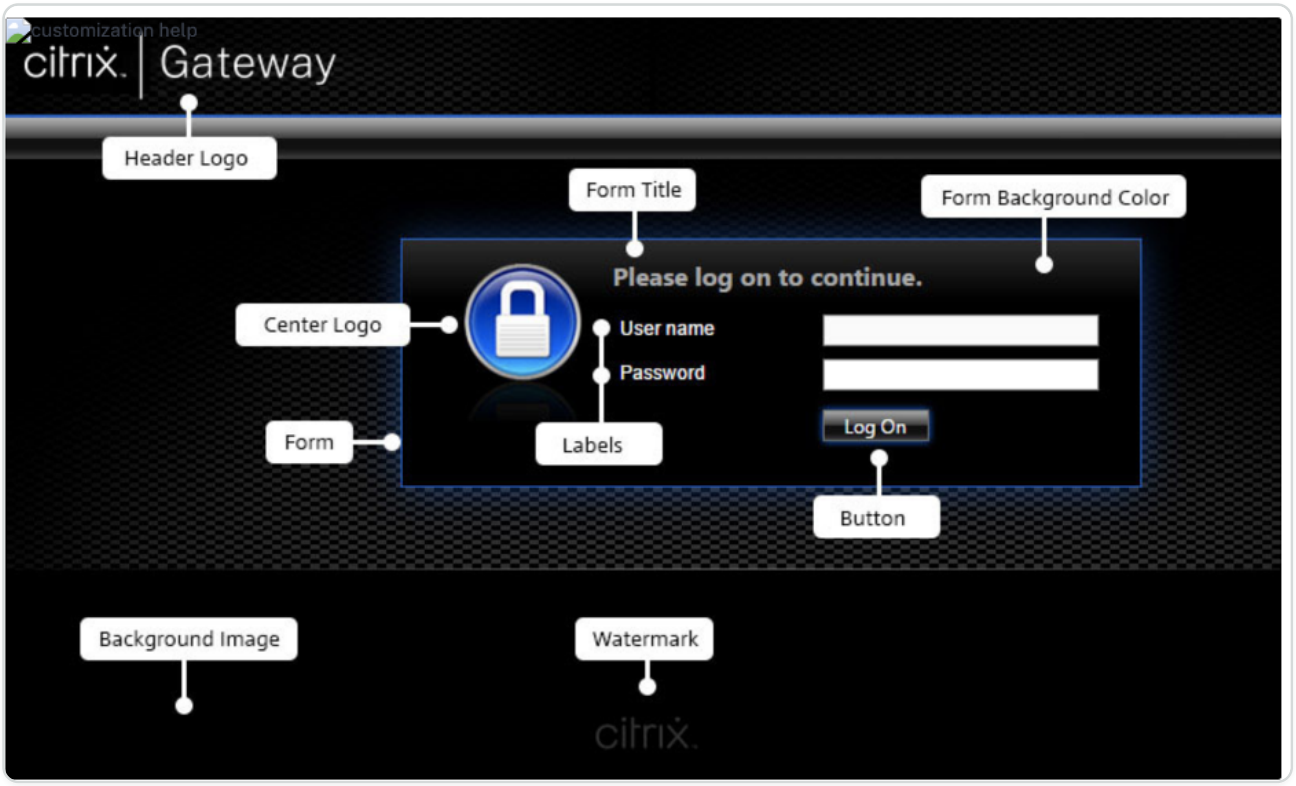



© 1997–2026 Citrix Systems, Inc. All rights reserved.




© 1997–2026 Citrix Systems, Inc. All rights reserved.

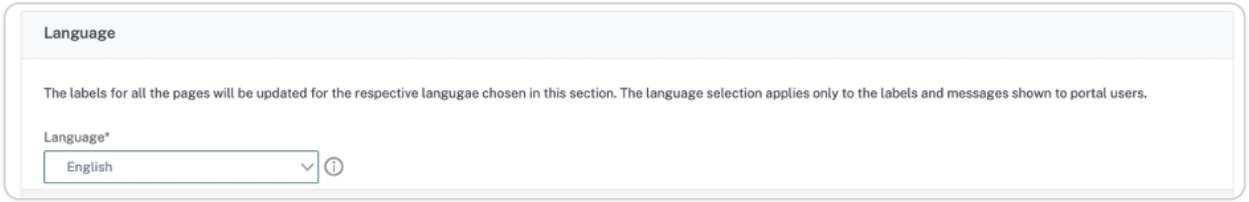



## Personalizaciones de cadenas

Además del aspecto de las páginas de inicio del portal de la puerta de enlace, la interfaz de usuario de administración también permite la personalización de cadenas en todas las páginas.

**Realice los siguientes pasos para personalizar las cadenas:**

1. Seleccione el idioma para el que desea editar la cadena. Las cadenas se muestran en el idioma seleccionado. El inglés está seleccionado de forma predeterminada.

   **Nota:** El idioma que seleccione no define el idioma del tema del portal. Es el idioma para el que se están personalizando las cadenas.

2. A la derecha, en **Configuración avanzada**, se enumeran las páginas disponibles para la personalización de cadenas.

   - Página de acceso
   - Página de EPA
   - Página de error de EPA
   - Página posterior a EPA

© 1997–2026 Citrix Systems, Inc. All rights reserved.

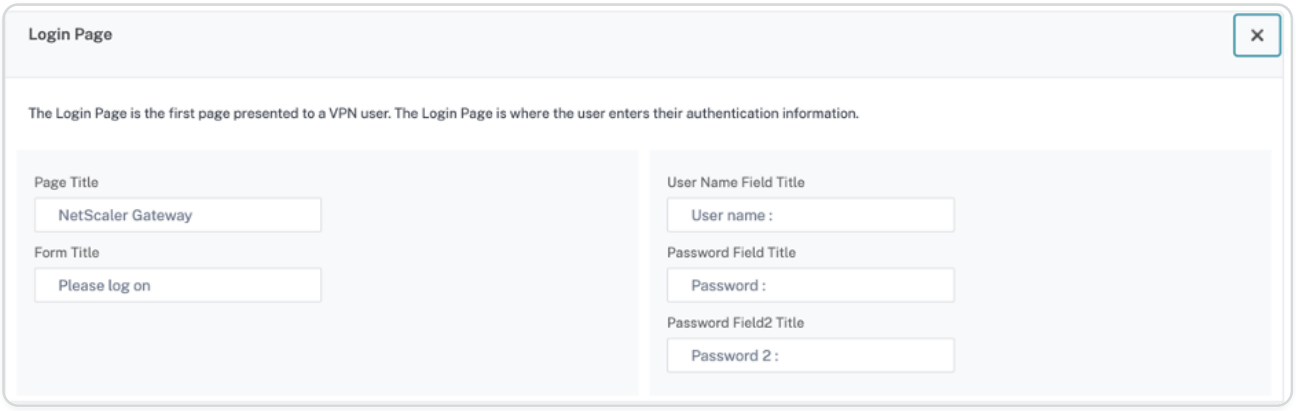
- Página de conexión VPN
- Página de inicio

3. Seleccione la página para la que desea personalizar las cadenas y haga clic en el icono de edición. Se muestra un formulario con personalizaciones de cadena precargadas.
4. Seleccione el campo y añada o edite la cadena según sus requisitos.
5. Haga clic en **Listo** para completar la creación del tema del portal personalizado. Puede editar los temas más tarde desde **NetScaler Gateway > Temas del portal**.

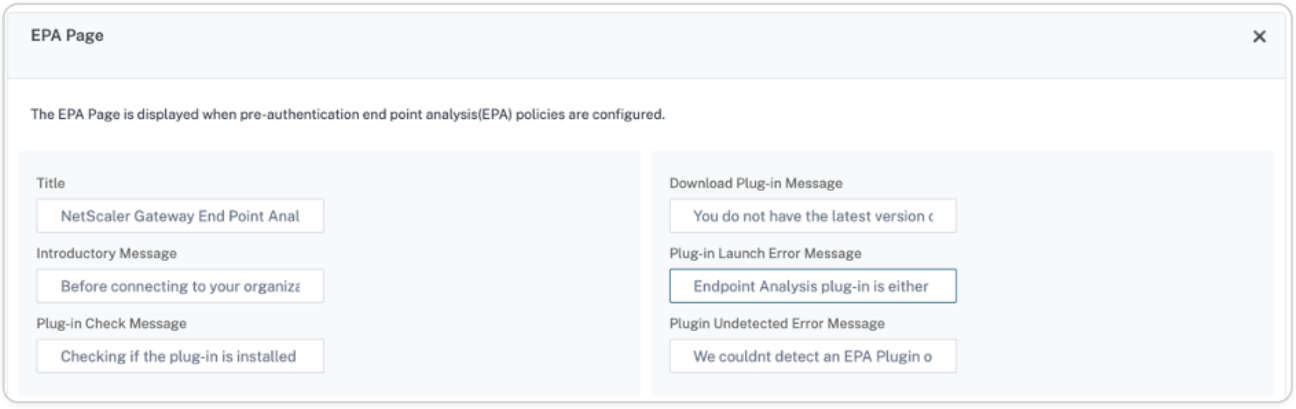
**Nota:** Si la sección sigue mostrando las cadenas en el idioma seleccionado anteriormente, es posible que la sección ya estuviera abierta cuando se cambió el idioma. En este caso, cierre la sección, seleccione el idioma y vuelva a abrir la página desde **Configuración avanzada**.

Las siguientes capturas de pantalla muestran el conjunto de cadenas personalizables disponibles para cada página.

**Página de inicio de sesión:**

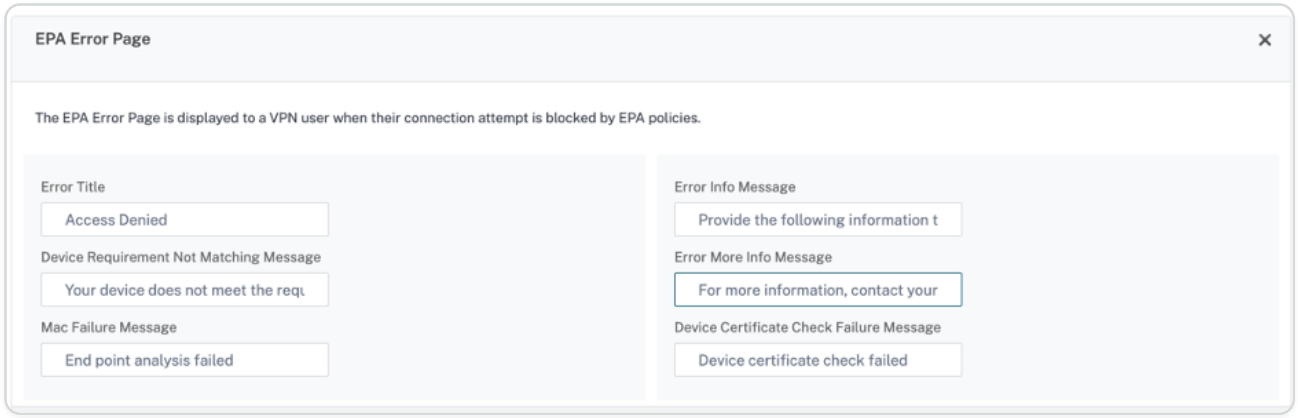



**Página de EPA:**

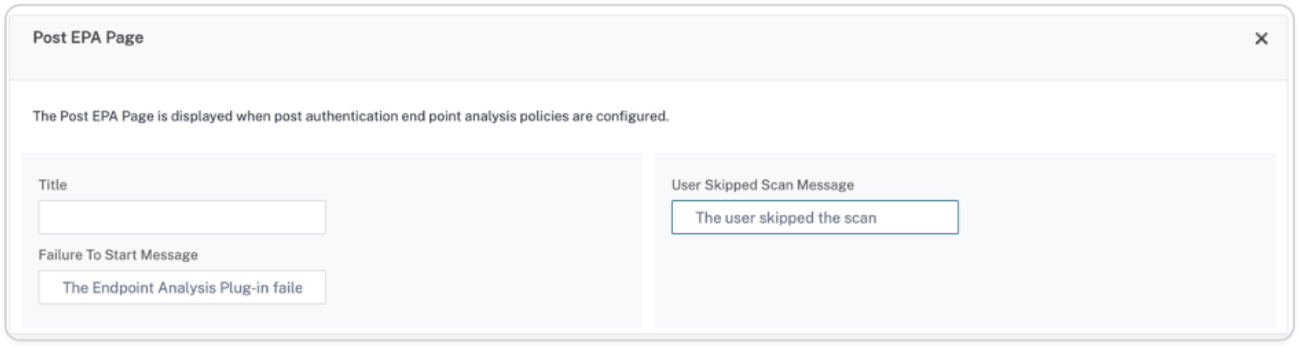



**Página de error de EPA:**

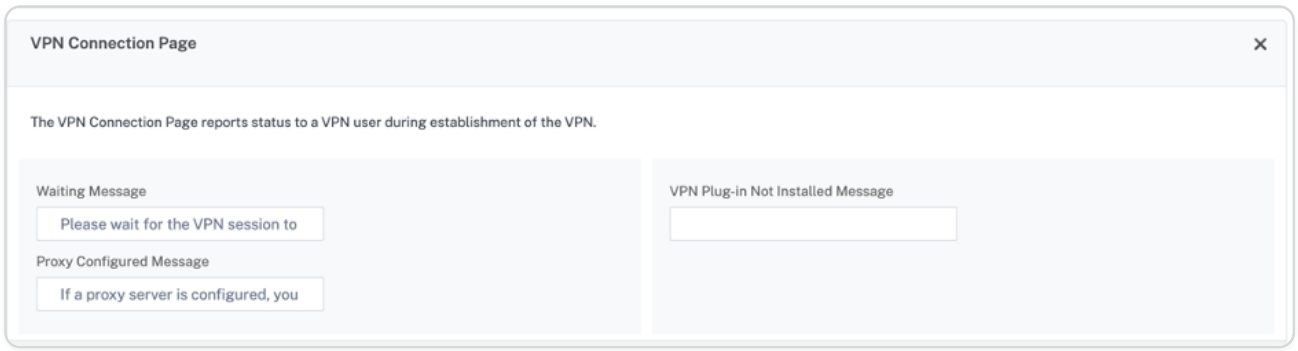
© 1997–2026 Citrix Systems, Inc. All rights reserved.



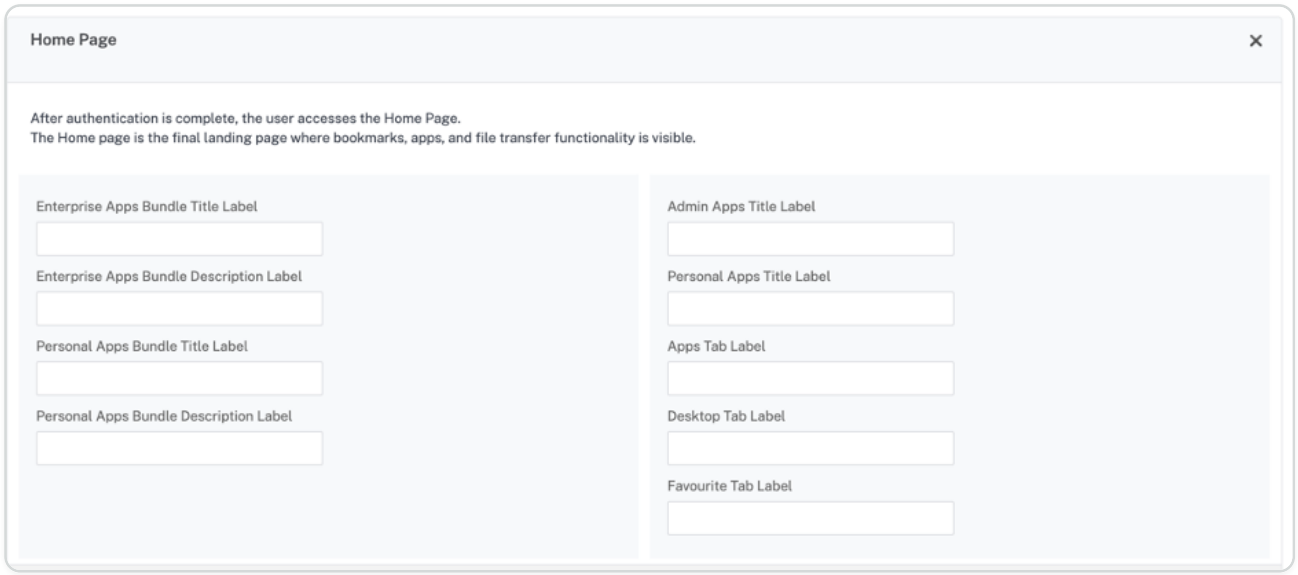

## Página posterior a EPA:




## Página de conexión VPN:




## Página de inicio:




© 1997–2026 Citrix Systems, Inc. All rights reserved.

# Optimización del túnel dividido VPN de NetScaler Gateway para Office365

A medida que las organizaciones se adaptan a las opciones de trabajo remoto más rápidamente que antes, la infraestructura de acceso remoto debe optimizarse para facilitar una conectividad fluida durante condiciones de carga de tráfico elevada.

**IMPORTANTE:**

Microsoft recomienda excluir el tráfico destinado a los servicios clave de Office 365 del ámbito de la conexión VPN configurando el túnel dividido mediante rangos de direcciones IPv4 e IPv6 publicados. Para obtener el mejor rendimiento y el uso más eficiente de la capacidad de la VPN, el tráfico a los rangos de direcciones IP dedicadas asociadas con las siguientes aplicaciones debe enrutarse directamente, fuera del túnel VPN:

- Office 365 Exchange Online
- SharePoint Online
- Microsoft Teams (denominado categoría Optimizar en la documentación de Microsoft)

Consulte la guía de Microsoft para obtener información más detallada sobre esta recomendación. La recomendación de Microsoft en NetScaler Gateway se logra enrutando la lista de direcciones IP proporcionada por Microsoft directamente a Internet para el tráfico de O365 mediante la configuración inversa del túnel dividido.

La configuración implica lo siguiente, que se puede realizar manualmente mediante la GUI o la CLI:

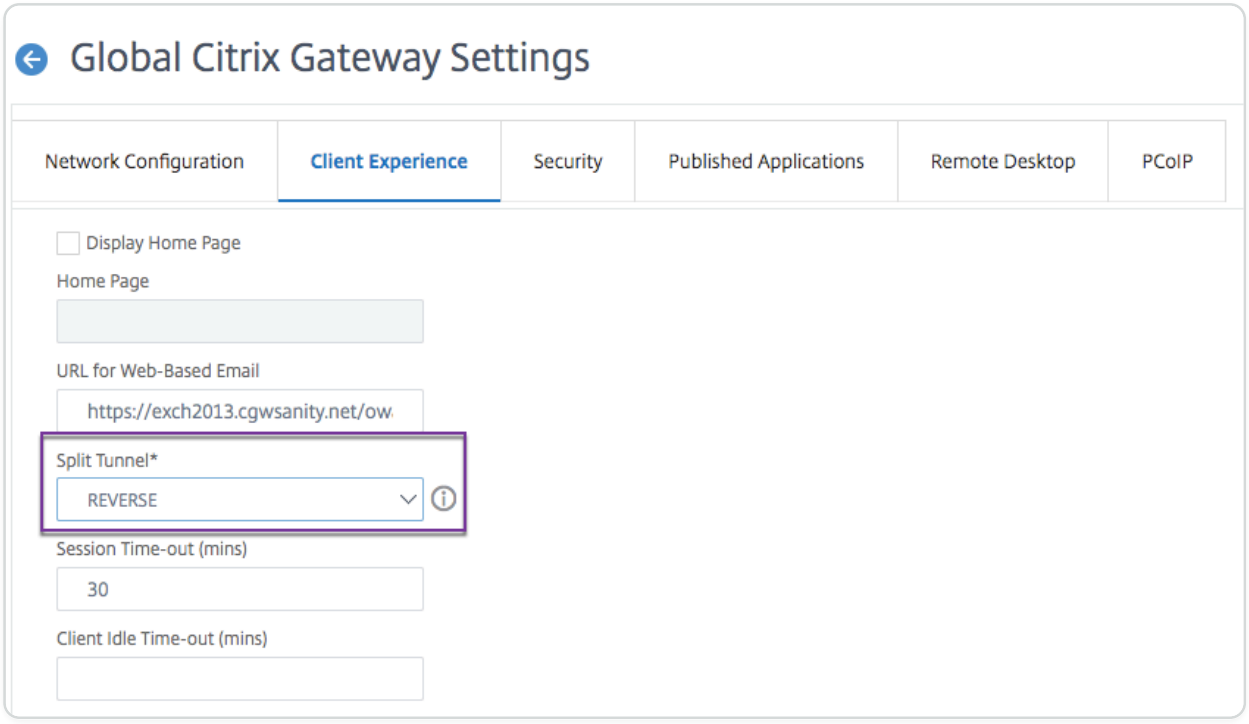
- Configure el túnel dividido para la configuración inversa. Para obtener más información, consulte Opciones de túnel dividido.
- Configure aplicaciones de intranet para el acceso de los usuarios a los recursos.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

# Configuración mediante la GUI

## Para configurar el túnel dividido mediante la GUI

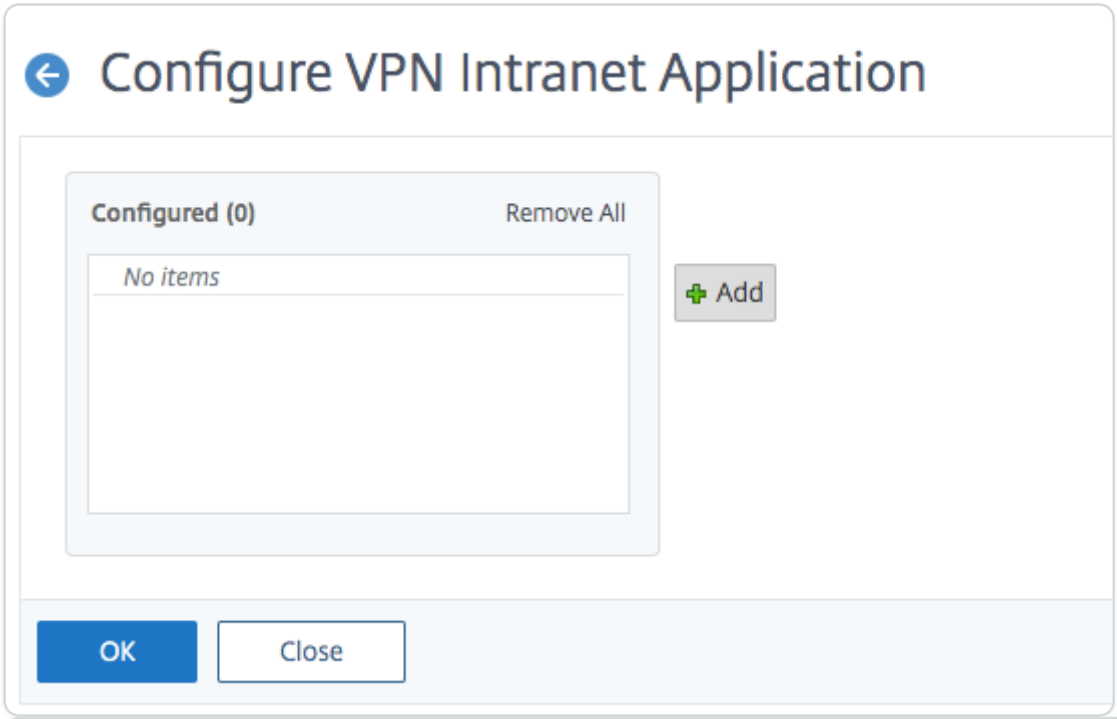
1. En la ficha Configuración, vaya a **NetScaler Gateway > Configuración global**.
2. En el panel de detalles, en **Configuración**, haga clic en **Cambiar configuración global**.
3. En la pestaña **Experiencia del cliente**, en **Túnel dividido**, seleccione **Inverso**.
4. Haga clic en **Aceptar**.

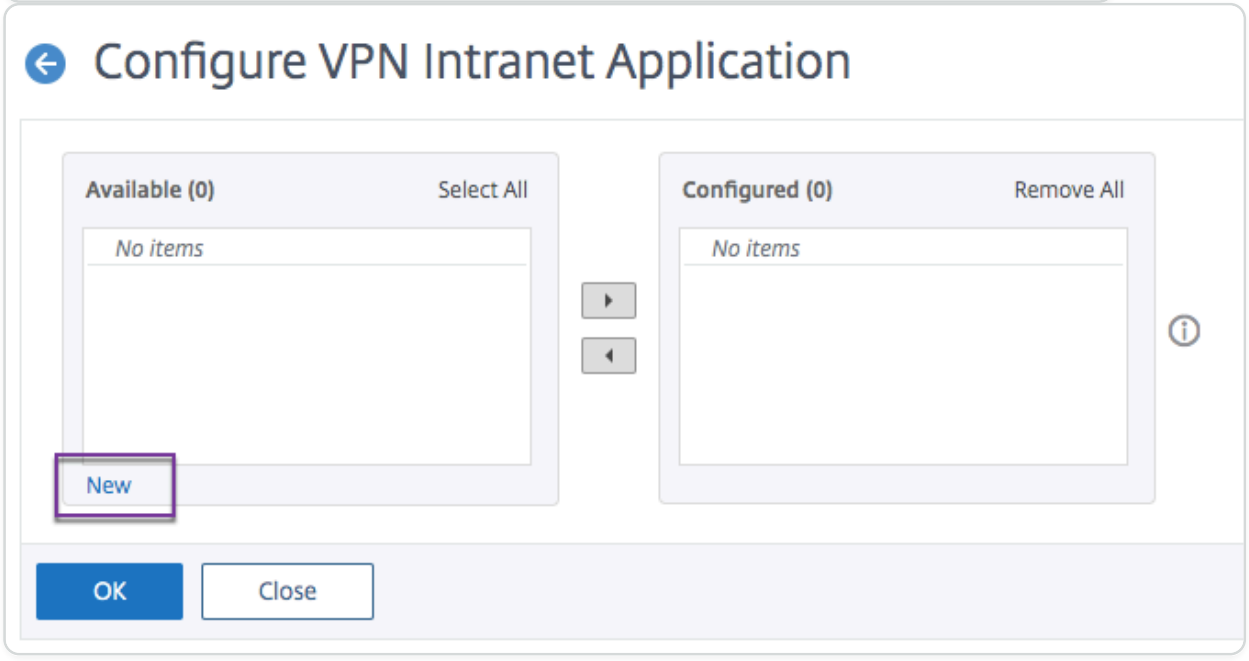



## Para crear una aplicación de intranet VPN mediante la GUI

1. En la pestaña Configuración, vaya a **Citrix Gateway > Configuración global**.
2. En el panel de detalles, en **Aplicaciones de intranet**, haga clic en el enlace.
3. En la página **Configurar aplicación de intranet VPN**, haga clic en **Agregar** y, a continuación, en **Nuevo**.

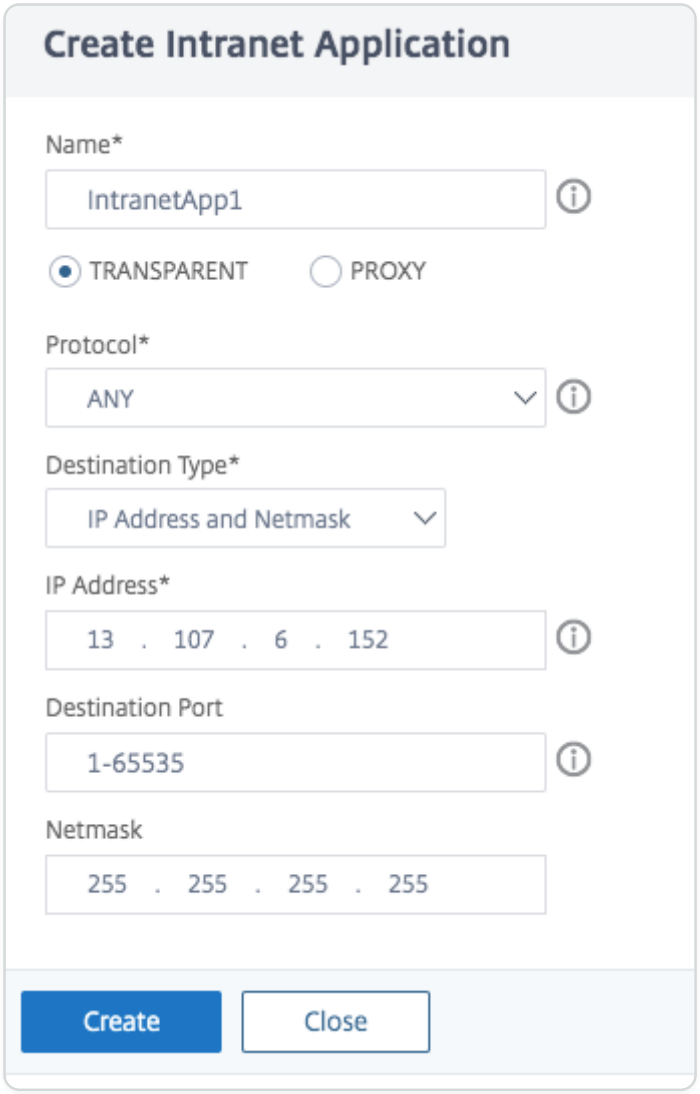
© 1997–2026 Citrix Systems, Inc. All rights reserved.




4. En **Nombre**, escriba un nombre para el perfil.
5. En **Protocolo**, seleccione el protocolo que se aplica al recurso de red.
6. En **Tipo de destino**, seleccione **Dirección IP y máscara de red**.
7. En **Dirección IP**, introduzca la dirección IP que debe enrutarse directamente a Internet para el tráfico de O365. Para ver la lista de direcciones IP, consulte Lista de direcciones IP.
8. En **Máscara de red**, introduzca la dirección IP de la máscara de red.

© 1997–2026 Citrix Systems, Inc. All rights reserved.




9. Haga clic en **Crear** y, a continuación, en **Cerrar**.

**Nota**: Repita este procedimiento para todas las direcciones IP.

# Configuración mediante la CLI

- Para establecer el túnel dividido en inverso, en el símbolo del sistema, escriba:

```
set vpn parameter -splitTunnel REVERSE
```

- Para agregar una aplicación de intranet VPN, en el símbolo del sistema, escriba:

```
add vpn intranetApplication intranetapp1 ANY 13.107.6.152 -netmask
255.255.255.254 -destPort 1-65535 -interception TRANSPARENT
```

**Nota**: Repita este procedimiento para todas las direcciones IP.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Para vincular la aplicación de intranet, en el símbolo del sistema, escriba:

```
bind vpn global -intranetApplication intranetapp1
```

# Lista de direcciones IP de los servicios de Office 365 (EXO, SPO y Microsoft Teams)

Referencia: `<https://docs.microsoft.com/es-es/office365/enterprise/urls-and-ip-address-ranges>`

**NOTA DE MICROSOFT:**

Como parte de la respuesta de Microsoft a la situación de la COVID-19, Microsoft ha declarado una moratoria temporal sobre algunos cambios planificados de URL y direcciones IP. Esta moratoria tiene como objetivo proporcionar a los equipos de TI de los clientes confianza y simplicidad en la implementación de optimizaciones de red recomendadas para escenarios de Office 365 de trabajo desde casa. Desde March 24, 2020 hasta June 30, 2020, esta moratoria detendrá los cambios para los servicios clave de Office 365 (Exchange Online, SharePoint Online y Microsoft Teams) en los rangos de IP y URL incluidos en la categoría Optimizar.

## Rango de direcciones IPv4

104.146.128.0/17

13.107.128.0/22 13.107.136.0/22

13.107.18.10/31 13.107.6.152/31

13.107.64.0/18 131.253.33.215/32

132.245.0.0/16 150.171.32.0/22

150.171.40.0/22 191.234.140.0/22

204.79.197.215/32 23.103.160.0/20

40.104.0.0/15 40.108.128.0/17

40.96.0.0/13 52.104.0.0/14

© 1997–2026 Citrix Systems, Inc. All rights reserved.

52.112.0.0/14 52.96.0.0/14

52.120.0.0/14|

## Rango de direcciones IPv6

2603:1006::/40

2603:1016::/36 2603:1026::/36

2603:1036::/36 2603:1046::/36

2603:1056::/36 2603:1096::/38

2603:1096:400::/40 2603:1096:600::/40

2603:1096:a00::/39 2603:1096:c00::/40

2603:10a6:200::/40 2603:10a6:400::/40

2603:10a6:600::/40 2603:10a6:800::/40

2603:10d6:200::/40 2620:1ec:4::152/128

2620:1ec:4::153/128 2620:1ec:c::10/128

2620:1ec:c::11/128 2620:1ec:d::10/128

2620:1ec:d::11/128 2620:1ec:8f0::/46

2620:1ec:900::/46 2620:1ec:a92::152/128

2620:1ec:a92::153/128 2a01:111:f400::/48

2620:1ec:8f8::/46 2620:1ec:908::/46

2a01:111:f402::/48

© 1997–2026 Citrix Systems, Inc. All rights reserved.

# Soporte de tipo de servicio para tráfico UDP

El soporte de Tipo de servicio (ToS) para UDP garantiza que una vez que un remitente configura un valor de ToS para un paquete UDP, NetScaler Gateway retiene el valor hasta que el paquete llega a su destino. Según el valor configurado y la configuración de la red de destino, la red de destino coloca el paquete UDP en una cola de salida priorizada.

**NOTA**

Mediante la información de ToS, puede asignar una precedencia a cada paquete IP y solicitar un tratamiento específico, como alto rendimiento, alta fiabilidad, baja latencia, etc.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

# Configuración de la extensión de indicación de nombre de servidor

Un dispositivo NetScaler Gateway ahora se puede configurar para incluir una extensión de indicación de nombre de servidor (SNI) en el paquete SSL «client hello» enviado al servidor back-end. La extensión SNI ayuda al servidor back-end a identificar el FQDN que se solicita durante el protocolo de enlace SSL y a responder con los certificados respectivos.

**NOTA**

Habilite la compatibilidad con SNI cuando se alojan varios dominios SSL en el mismo servidor.

**Para configurar NetScaler Gateway para que admita SNI mediante la GUI:**

1. En la GUI de NetScaler, vaya a **Configuration\> NetScaler\> Global Settings.**
2. Haga clic en el enlace **Change Global Settings** y en el menú **Backend Server SNI**, seleccione **Enabled**.

**Para configurar NetScaler Gateway para que admita SNI mediante la interfaz de línea de comandos, en el símbolo del sistema, escriba:**

```
set vpn parameter backendServerSni <ENABLED><DISABLED>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

# Validación del certificado del servidor durante un protocolo de enlace SSL

El dispositivo NetScaler Gateway ahora se puede configurar para validar el certificado del servidor proporcionado por el servidor back-end durante un protocolo de enlace SSL.

Para configurar los parámetros globales de NetScaler Gateway para admitir PAC para proxy saliente mediante la utilidad de configuración

Vincular el certificado de CA

1. Vaya a **Configuración** > **NetScaler Gateway** > **Administrador de directivas de NetScaler Gateway** > **Enlaces de certificados**.****
2. En la pantalla **Enlaces de certificados**, haga clic en el icono **+**.
3. En la pantalla **Enlace de certificado(s) de CA**, haga clic en **Agregar enlace** y, a continuación, en **Instalar**.
4. Seleccione el nombre del archivo de certificado en el campo **Nombre del archivo de certificado** y haga clic en **Instalar**.
5. En la pantalla **Enlace de certificado(s) de CA**, seleccione el certificado y haga clic en **Enlazar**.
6. Haga clic en **Listo**.

**Habilitar la validación del certificado:**

1. Vaya a **NetScaler Gateway\> Configuración global.**
2. Haga clic en **Cambiar configuración global**.****
3. Seleccione **Habilitado** en el menú desplegable **Validación de certificado de servidor back-end** y haga clic en **Aceptar**.

Para configurar los parámetros globales de NetScaler Gateway para admitir el certificado de servidor con la línea de comandos

En el símbolo del sistema, escriba los siguientes comandos:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
bind vpn global cacert DNPGCA1



set vpn parameter backendcertValidation ENABLED
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

# Configuración simplificada de aplicaciones SaaS mediante una plantilla

La configuración de aplicaciones SaaS con inicio de sesión único en NetScaler Gateway se simplifica al proporcionar un menú desplegable de plantillas para las aplicaciones SaaS populares. La aplicación SaaS que se va a configurar se puede seleccionar del menú. La plantilla rellena previamente gran parte de la información necesaria para configurar las aplicaciones. Sin embargo, la información específica del cliente aún debe proporcionarse.

**NOTA:**

Para configurar y publicar aplicaciones SaaS, configúrelas y publíquelas en NetScaler Gateway y, a continuación, en el servidor de aplicaciones.

Los pasos de la siguiente sección le ayudarán a configurar y publicar aplicaciones en NetScaler Gateway mediante una plantilla. Luego, pase a la sección que explica cómo configurar y publicar en el servidor de aplicaciones.

## Configuración y publicación de aplicaciones mediante plantilla - Configuración específica de NetScaler Gateway

La siguiente configuración utiliza la aplicación AWS Console como ejemplo de cómo configurar y publicar una aplicación mediante una plantilla.

Antes de empezar, necesita lo siguiente:

- Una cuenta de administrador para la consola de AWS
- Una cuenta de administrador para NetScaler Gateway

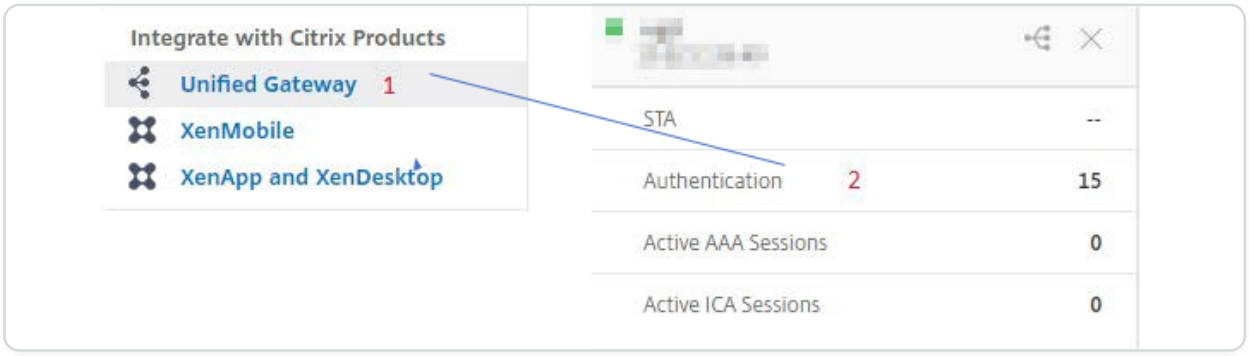
**Los pasos de configuración de la consola de AWS son los siguientes:**

1. Configure la consola de AWS con el catálogo de aplicaciones.
2. Exporte los metadatos de IdP de la consola de AWS desde NetScaler.
3. Configure IdP en la consola de AWS.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

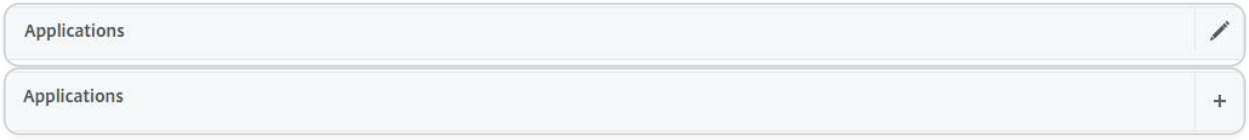
**PASO 1:** Configurar la consola de AWS con el catálogo de aplicaciones

1. Haga clic en **Unified Gateway > Authentication**.

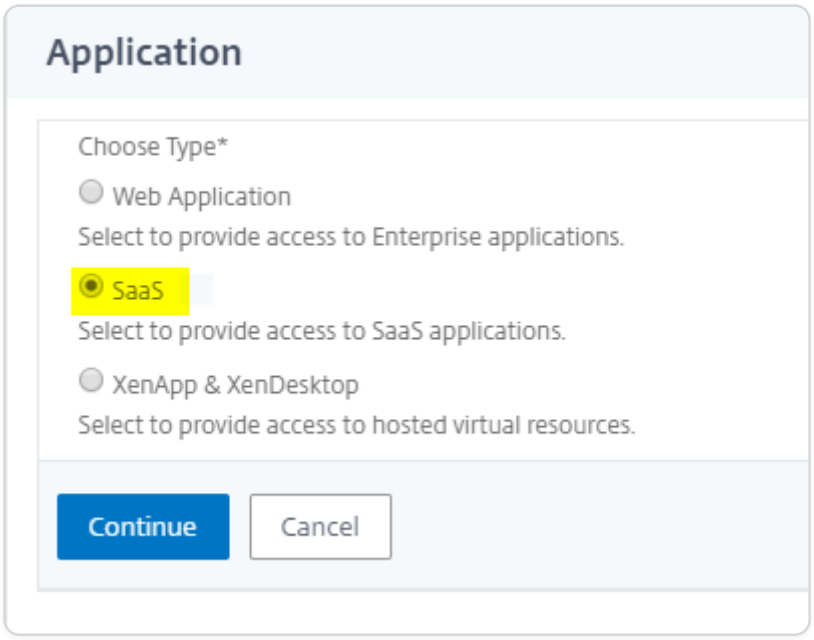



   Aparece la pantalla de configuración de Unified Gateway.

2. En la sección **Applications**, haga clic en el icono de edición. Ahora, haga clic en el icono de más. Aparece la ventana Aplicación.

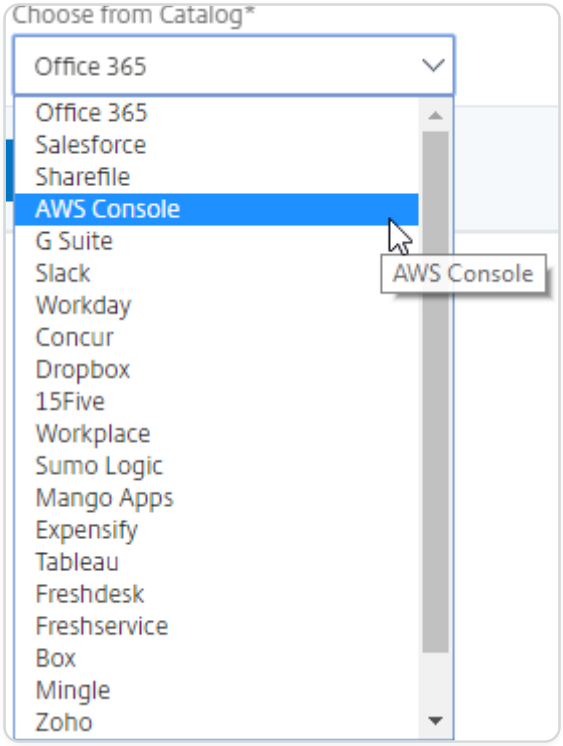



3. Seleccione **SaaS** en Tipo de aplicación.

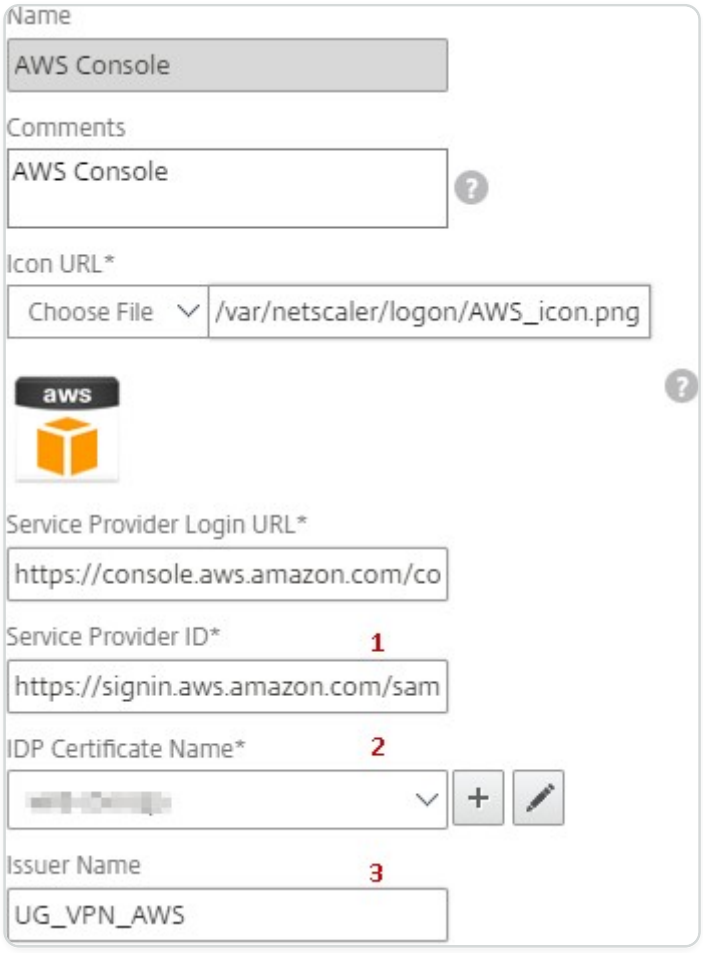



4. Seleccione **AWS Console** de la lista desplegable.

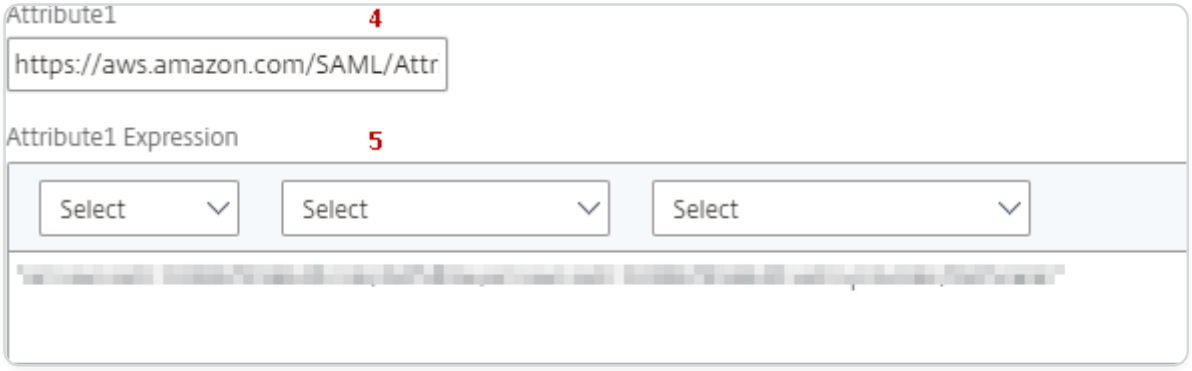
© 1997–2026 Citrix Systems, Inc. All rights reserved.




5. Rellene la plantilla de aplicación con los valores adecuados.




© 1997–2026 Citrix Systems, Inc. All rights reserved.




6. Introduzca los siguientes detalles de configuración de SAML y haga clic en **Continuar**.

   **ID de proveedor de servicios** – `<https://signin.aws.amazon.com/saml>`

   **Nombre del certificado de firma** – Se debe seleccionar el certificado IdP

   **Nombre del emisor** – El nombre del emisor se puede rellenar según su elección

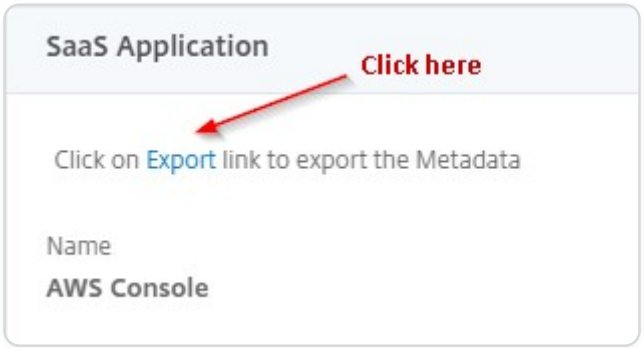
   **Atributo1** – `https://aws.amazon.com/SAML/Attributes/Role`

   **Expresión de Atributo1** `– Role ARN, IdP ARN`, como se muestra en el paso 3

7. Haga clic en **Listo**.

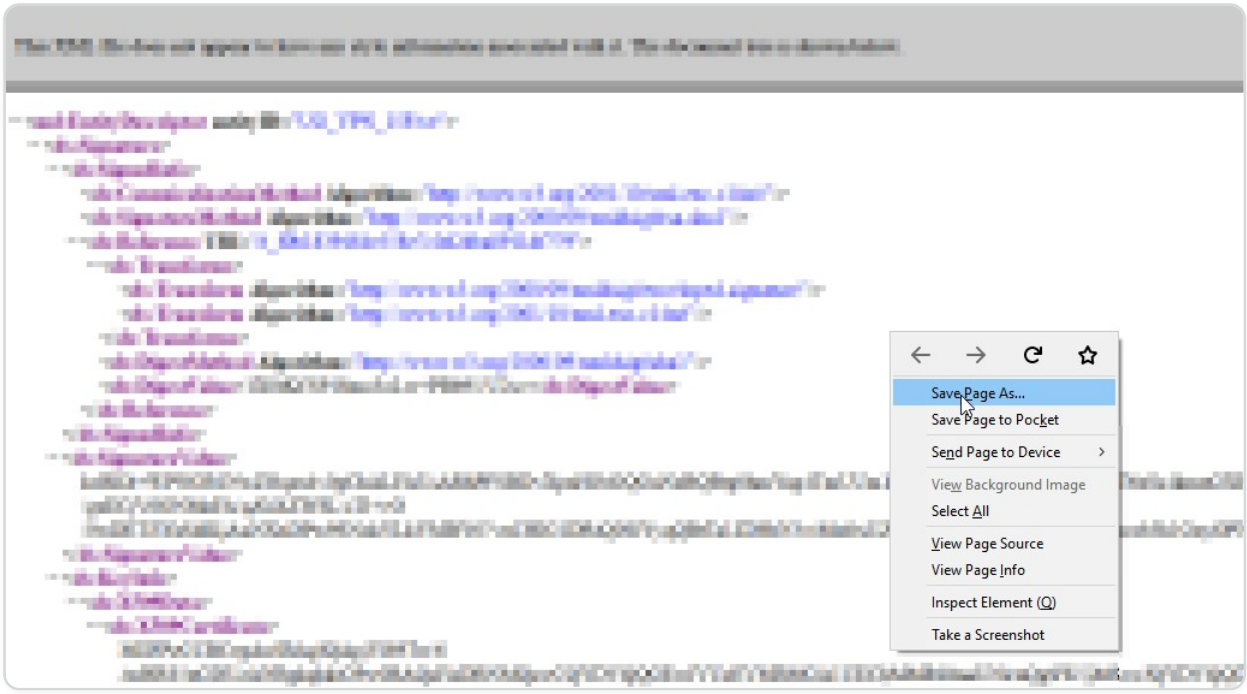
**PASO 2:** Exporte los metadatos de IdP de la consola de AWS desde NetScaler Gateway.

1. Haga clic en **Unified Gateway > Authentication**.
2. Desplácese hacia abajo y haga clic en la plantilla **AWS Console**. Aparece la ventana Aplicación SaaS. Haga clic en el enlace **Exportar**.




3. **Metadatos** se abre en una ventana diferente. Guarde el archivo de **metadatos de IdP**

© 1997–2026 Citrix Systems, Inc. All rights reserved.




**PASO 3:** Configurar IdP en la consola de AWS.

## Configuración y publicación de aplicaciones mediante plantilla - Configuración específica del servidor de aplicaciones

Los siguientes enlaces abren documentos PDF que proporcionan orientación específica para configurar y publicar aplicaciones SaaS populares mediante plantillas.

- 15Five
- Absorb
- Accompa
- Adobe Captivate Prime
- Adobe Creative Cloud
- Aha
- AlertOps
- Allocadia
- Ariba
- Assembla
- AWS Console
- BambooHR

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Base CRM
- BitaBIZ
- BlueJeans
- Blissbook
- Bonusly
- Box
- Bugsnag
- Buildkite
- CakeHR
- Cardboard
- Cedexis
- Celoxis
- Cisco Meraki
- ClearSlide
- CloudCheckr
- ConceptShare
- Concur
- Confluence
- Contactzilla
- Convo
- Circonus
- Dashlane
- Datadog
- Deskpro
- Deputy
- DigiCert
- DocuSign
- Domo
- Dropbox
- Duo

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- eFront
- Ekarda
- Envoy
- ERP
- Expensify
- EZOfficeInventory
- EZRentOut
- Favro
- Federated Directory
- Feedly
- Fivetran
- Flatter Files
- Flowdock
- Freshdesk
- Front
- G-Suite
- GitHub
- GlassFrog
- GotoMeeting
- HappyFox
- Helpjuice
- Help Scout
- Hoshinplan
- Humanity
- Igloo
- Illumio
- Image Relay
- iMeet Central
- InteractGo
- iQualify One

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Jira
- Kanban Tool
- Keeper Security
- Kentik
- Kentik
- Kissflow
- KnowBe4
- KnowledgeOwl
- Kudos
- LaunchDarkly
- Lifesize
- Litmos
- LiquidPlanner
- LogDNA
- Mango
- Manuscript
- Marketo
- Mingle
- Mixpanel
- MuleSoft
- MyWebTimesheets
- New Relic
- Nmbrs
- Nuclino
- Office365
- OneDesk
- OpsGenie
- Orginio
- PagerDuty
- Panorama9

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- ParkMyCloud
- Peakon
- People HR
- Pingboard
- Pipedrive
- PlanMyLeave
- PlayVox
- Podio
- ProdPad
- Proto.io
- Proxyclick
- PurelyHR
- Quandora
- Rackspace
- RealtimeBoard
- Remedyforce
- Robin
- Rollbar
- Salesforce
- Samanage
- Samepage
- Sentry
- ServiceDesk Plus
- ServiceNow
- Shufflrr
- Skeddly
- Skills Base
- Slack
- Slemma
- Sli.do

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Smartsheet
- Spoke
- Spotinst
- SproutVideo
- StatusCast
- Status Hero
- StatusHub
- Statuspage
- Sumo Logic
- Supermood
- Syncplicity
- Tableau
- Targetprocess
- Teamphoria
- Testable
- TestFairy
- TextExpander
- TextMagic
- ThousandEyes
- Thycotic Secret server
- Tinfoil Security
- Trisotech
- Trumba
- TwentyThree
- UniFi
- UserEcho
- UserVoice
- Velpic
- VictorOps
- VIDIZMO

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Visual Paradigm
- Weekdone
- Wepow
- When I Work
- Workday
- Workpath
- Workplace
- Workstars
- Workteam
- XaitPorter
- Ximble
- `XMatters`
- Yodeck
- Zendesk
- ZIVVER
- Zoho One
- ZIVVER
- Zoom

© 1997–2026 Citrix Systems, Inc. All rights reserved.