Clientes de NetScaler Gateway

Machine translated content

Disclaimer

Contents

Clientes VPN de NetScaler Gateway y funciones compatibles

March 27, 2024

> **Importante:**
>
> - Citrix SSO para iOS/Android ahora se llama Citrix Secure Access. Estamos actualizando nuestra documentación y las capturas de pantalla de la interfaz de usuario para reflejar este cambio de nombre.
> - El cliente VPN antiguo se creó con las API de VPN privadas de Apple que ahora están en desuso. La compatibilidad con VPN en el cliente Citrix Secure Access para macOS/iOS se reescribe mediante el marco de extensión de red pública de Apple. El complemento NetScaler Gateway y la VPN para iOS y macOS ya no son compatibles. Citrix Secure Access para iOS/macOS es el cliente VPN que se recomienda utilizar.
> - La disponibilidad general de la compatibilidad con la autenticación nFactor para dispositivos Android estará disponible en una de las próximas versiones.

En la tabla siguiente se enumeran algunas de las funciones de uso común compatibles con cada cliente VPN.

Función	Citrix Secure Access para Windows	Citrix Secure Access para Linux	Citrix Secure Access para macOS	Citrix Secure Access para iOS	Citrix Secure Access para Android
Siempre activado (modo usuario)	Sí (11.1 y posteriores)	No	No	No	Sí (a través de MDM) Android 7.0+
Archivo PAC	Sí (12.0 y posteriores)	No	Sí	Sí	No
Compatibilidad con proxy de cliente	Sí	Sí	No	No	Sí. *Ver nota 1*
Límite máximo de aplicaciones de intranet	512	128	Sin límite	Sin límite	Sin límite
Compatibilidad con IP de intranet (IIP)	Sí	Sí	Sí	Sí	Sí

Función	Citrix Secure Access para Windows	Citrix Secure Access para Linux	Citrix Secure Access para macOS	Citrix Secure Access para iOS	Citrix Secure Access para Android
Túnel dividido ENCENDIDO	Sí	Sí	Sí	Sí	Sí
Túnel dividido inverso	Sí	Sí	Sí	Sí	Sí. *Ver nota 5*
DNS REMOTE dividido	No	Sí	Sí	Sí	Sí. *Ver nota 6*
Split DNS BOTH	Sí	No	Sí	Sí	Sí. *Ver nota 6*
Túnel dividido basado en FQDN	Sí solo activado (13.0 y posteriores)	No	Sí	Sí	Sí. *Ver nota 5*
Tiempo de espera inactivo del cliente	Sí	Sí	Sí	No	No
Análisis de dispositivos de punto final	Sí	Sí	Sí	No	No
Certificado de dispositivo (clásico)	Sí	No	Sí	No	No
Autenticación nFactor	Sí (12.1 y posteriores)	No	Sí	Sí	Sí. *Ver nota 3*
EPA (nFactor)	Sí (12.1 y posteriores)	No	Sí	No	No
Certificado de dispositivo (nFactor)	Sí (12.1 y posteriores)	No	Sí	No	No
Notificación push	Sí (12.1 y posteriores)	No	No	Sí	Sí
Compatibilidad con el auto-completado de tokens OTP. *Ver nota 2*	No	No	No	Sí	Sí

Función	Citrix Secure Access para Windows	Citrix Secure Access para Linux	Citrix Secure Access para macOS	Citrix Secure Access para iOS	Citrix Secure Access para Android
Compatibilidad con TLS 1.3	Sí	Sí	Sí	Sí (desactivado, de forma predeterminada). Disponible bajo petición.)	Sí (desactivado, de forma predeterminada). Disponible bajo petición.)
Compatibilidad con DTLS. *Ver nota 4*	Sí (13.0 y posteriores)	No	Sí	Sí	No
Cookies de HTTPOnly	Sí	Sí	Sí	Sí	Sí
Equilibrio de carga de servidor global (GSLB)	Sí	Sí	Sí	Sí	Sí
Acceso a LAN local	Sí	No	Siempre habilitado	Siempre habilitado	No

Nota:

1. Se admite la configuración de un proxy en la configuración del cliente en el servidor virtual de VPN en la configuración de puerta de enlace para Android 10 y versiones posteriores. Solo se admite la configuración básica del proxy HTTP con dirección IP y puerto.
2. Solo los tokens escaneados con códigos QR son aptas para prerrellenarse automáticamente. El flujo de autenticación nFactor no admite el llenado automático.
3. La compatibilidad con la autenticación nFactor para dispositivos Android está en vista previa y la función está inhabilitada de forma predeterminada. Póngase en contacto con el soporte de NetScaler para habilitar esta función. Los clientes deben proporcionar el FQDN de NetScaler Gateway al equipo de soporte para habilitar la autenticación nFactor para dispositivos Android.
4. Para obtener más información, consulte Configurar el servidor virtual de VPN DTLS mediante el servidor virtual de VPN SSL.
5. La compatibilidad con túnel dividido basado en FQDN y túnel dividido inverso para dispositivos Android está en vista previa y la función está inhabilitada de forma predeterminada. Póngase en contacto con el soporte de NetScaler para habilitar esta función. Los clientes

deben proporcionar el FQDN de NetScaler Gateway al equipo de soporte para habilitarlo en dispositivos Android.

6. Para el modo Split DNS BOTH, los sufijos DNS deben configurarse en la puerta de enlace y solo las consultas de registro DNS A que terminen en esos sufijos se envían a la puerta de enlace. El resto de las consultas se resuelven localmente. Citrix Secure Access para Android también admite el modo local de DNS dividido.

Referencia

Documentación de ayuda para el usuario final

Citrix Secure Access para macOS/iOS

March 27, 2024

El cliente VPN antiguo se creó con las API de VPN privadas de Apple que ahora están en desuso. La compatibilidad con VPN en Citrix Secure Access para macOS e iOS se ha reescrito desde cero mediante el marco de extensión de red pública de Apple.

Nota

- Citrix SSO para iOS ahora se llama Citrix Secure Access. Estamos actualizando nuestra documentación y las capturas de pantalla de la interfaz de usuario para reflejar este cambio de nombre.
- Citrix Secure Access para macOS se admite en 10.15 (Catalina), 11.x (Big Sur) y 12.x (Monterey). Es compatible con dispositivos con chips Intel y chips M1.
- Los usuarios con hardware que no se puede actualizar a una de las versiones mencionadas anteriormente (macOS 10.15 y macOS 11.0) tienen acceso a la última versión compatible en la App Store, pero no hay más actualizaciones de las versiones anteriores.
- Si un usuario de macOS cambia entre la aplicación App Store y la versión preliminar de TestFlight o viceversa, los usuarios deben volver a crear el perfil de conexión realizando los siguientes pasos:

  1. Click the hamburger menu and then click **Configuration**.
  2. Delete the profile from the list and add the same profile again.

Características principales del cliente Citrix Secure Access para macOS/iOS

- **Tokens de contraseña:** un token de contraseña es un código de 6 dígitos que es una alternativa a los servicios de contraseñas secundarias como VIP, OKTA. Este código utiliza el protocolo Contraseña de un solo uso basada en tiempo (T-OTP) para generar el código OTP similar a servicios como Google Authenticator y Microsoft Authenticator. Se solicitan dos contraseñas a los usuarios durante la autenticación en NetScaler Gateway para un usuario de Active Directory determinado. El segundo factor es un código cambiante de seis dígitos que los usuarios copian de un servicio de terceros registrado como Google o Microsoft Authenticator en el explorador de escritorio. Los usuarios deben registrarse primero en T-OTP en el dispositivo NetScaler. Para conocer los pasos de registro, consulte https://support.citrix.com/article/CTX228454. En la aplicación, los usuarios pueden agregar la función OTP escaneando el código QR generado en NetScaler o introduciendo manualmente el secreto TOTP. Los tokens OTP, una vez agregados, aparecen en el segmento Tokens de contraseña de la interfaz de usuario.

Para mejorar la experiencia, la adición de una OTP solicita al usuario que cree un perfil VPN automáticamente. Los usuarios pueden aprovechar este perfil de VPN para conectarse a la VPN directamente desde sus dispositivos iOS.

El cliente Citrix Secure Access para macOS/iOS se puede usar para escanear el código QR mientras se registra para obtener soporte OTP nativo.
La función de notificación push de NetScaler Gateway solo está disponible para los usuarios de Citrix Secure Access para macOS/iOS.

- **Notificación push:** NetScaler Gateway envía notificaciones push en su dispositivo móvil registrado para ofrecer una experiencia de autenticación de dos factores simplificada. En lugar de iniciar el cliente Citrix Secure Access para macOS/iOS para proporcionar el segundo factor OTP en la página de inicio de sesión de NetScaler, puede validar su identidad proporcionando el PIN del dispositivo, Touch ID o Face ID para el dispositivo registrado.

Una vez que haya registrado el dispositivo para recibir notificaciones push, también puede usarlo para obtener compatibilidad nativa con OTP mediante Citrix Secure Access para macOS/iOS. El registro para las notificaciones push es transparente para el usuario. Cuando los usuarios registran TOTP, el dispositivo también se registra para notificaciones push si NetScaler lo admite.

Notas de la versión

March 27, 2024

> **Importante:**
>
> Citrix SSO para iOS ahora pasa a llamarse Citrix Secure Access. Estamos actualizando las capturas de pantalla de la interfaz de usuario de nuestra documentación para reflejar este cambio de nombre. Además, es posible que observe las referencias de Citrix SSO utilizadas en la documentación de iOS durante este período de transición.

Las notas de la versión describen las nuevas funciones, las mejoras de las funciones existentes, los problemas resueltos y los problemas conocidos disponibles en una versión de servicio. Las notas de la versión incluyen una o varias de las secciones siguientes:

Novedades: las nuevas funciones y mejoras disponibles en la versión actual.

Problemasresueltos : los problemas que se han corregido en la versión actual.

Problemasconocidos : los problemas que existen en la versión actual y sus soluciones alternativas, cuando proceda.

> **Notas importantes sobre los clientes de EPA:**
>
> - Los clientes EPA son compatibles con las versiones macOS 10.13, 10.14, 10.15, 11.x, 12.x y 13.x.
> - Los clientes EPA son compatibles con las versiones 12.1, 13.0, 13.1 y 14.1 de NetScaler.

V24.03.1 (14 de marzo de 2024)

Novedades

- Las bibliotecas de la EPA se actualizaron a 24.03.1.0 (biblioteca OPSWAT OESIS V 4.3.3460.0).
- **Inicio de sesión único (SSO) automático en Citrix Secure Access a través de la aplicación Citrix Workspace: versión preliminar**

  Citrix Secure Access para macOS ahora admite el inicio de sesión único (SSO) automático en Citrix Secure Access al iniciar sesión en la aplicación Citrix Workspace. Asegúrese de usar Citrix Secure Access para macOS 24.03.1 o la aplicación Citrix Workspace para Mac 2402 y versiones posteriores para aprovechar esta funcionalidad. Esta función solo se admite en las tiendas en la nube y no en las tiendas locales.

  Actualmente, esta capacidad está deshabilitada de forma predeterminada. Puede registrarte para la vista previa mediante https://podio.com/webforms/29383411/2410629.

  Para obtener más información, consulte las notas de la versión de la aplicación Citrix Workspace 2402 para Mac.

  [CSACLIENTS-6321]

- **Mejoras generales de rendimiento y estabilidad**

  El cliente Citrix Secure Access se ha mejorado con las siguientes funciones para mejorar el rendimiento y la estabilidad generales:

  - Un aumento en el número de conexiones simultáneas que se pueden canalizar a través de una VPN. Esto solo se aplica a los clientes de iOS.
  - Una resiliencia de conexión VPN mejorada con puertas de enlace IPv6. Esto se aplica tanto a los clientes de macOS como a los de iOS.

  [NSHELP-36903]

V24.02.1 (15 de febrero de 2024)

Novedades

- **Soporte para operadores de escaneo EPA en clientes Mac**

  El cliente Citrix Secure Access para macOS ahora es compatible con todos los operadores <, >, >=, <=, == y != en el editor EPA. Además, la opción **Mac OS** está disponible como una opción independiente en el editor de la EPA (**Mac > Mac OS**). Puedes escanear la versión del producto de tus dispositivos macOS con estos operadores.

  Para obtener más información, consulte la sección **Nota** de los escaneos de análisis avanzadosde puntos finales.

  [CSACLIENTS-6462]

- Las bibliotecas de la EPA se actualizaron a 24.1.2.1 (biblioteca OPSWAT OESIS V 4.3.3405.0).

  [CSACLIENTS-8520]

- Esta versión soluciona algunos problemas para mejorar el rendimiento y la estabilidad generales.

24.1.5 Cliente EPA para macOS (12 de febrero de 2024)

Novedades

- **Soporte de la EPA para dispositivos Mac con procesador de silicio de Apple**

  El cliente Citrix EPA ahora admite dispositivos Mac que utilizan el procesador de silicio de Apple. Los dispositivos Mac ya no requieren la instalación de Rosetta para ejecutar el cliente Citrix EPA.

  [CSACLIENTS-8731]

- **Soporte para operadores de escaneo EPA en clientes Mac**

  El cliente Citrix EPA para Mac ahora admite los operadores (<, >, >= y <=) en las expresiones EPA. Los administradores pueden configurar los escaneos de la EPA para permitir una amplia gama de versiones del sistema operativo.

  Por ejemplo, para permitir las versiones del sistema operativo de la 12.4 a la 13.0, excepto la 12.8, los administradores pueden configurar la expresión. `version >= 12.4 && version <= 13.0 && version != 12.8` Esto significa que la versión de macOS debe estar entre la 12.4 y la 13.0, pero no puede ser la 12.8.

  Para obtener más información, consulte Análisis avanzados de endpoints.

  [CSACLIENTS-6462]

V23.12.2 (20 de diciembre de 2023)

Novedades

Esta versión aborda problemas para mejorar el rendimiento y la estabilidad generales.

V23.12.1 (06 de diciembre de 2023)

Novedades

- Las bibliotecas de la EPA se actualizan a la versión 23.11.1.5 (biblioteca OPSWAT OESIS V 4.3.3318.0).

  [CSACLIENTS-8516]

- En esta versión se abordan otros problemas para mejorar el rendimiento y la estabilidad generales.

V23.11.2 (01 de noviembre de 2023)

Novedades

Las bibliotecas de la EPA se actualizan a la versión 23.11.1.1 (biblioteca OPSWAT OESIS V 4.3.3279.0).

[CSACLIENTS-8515]

V23.11.1 (27 de octubre de 2023)

Novedades

- Citrix SSO para iOS ahora pasa a llamarse Citrix Secure Access. Estamos actualizando las capturas de pantalla de la interfaz de usuario de nuestra documentación para reflejar este cambio de nombre.
- Las bibliotecas de la EPA se actualizan a la versión 23.10.1.1 (biblioteca OPSWAT OESIS V 4.3.3246.0).
- En esta versión se aborda lo siguiente:
  - Problemas de conexión con el entorno Citrix Secure Private Access.
  - Otros problemas para mejorar el rendimiento y la estabilidad generales.

V23.10.2 (17 de octubre de 2023)

Esta versión aborda los problemas de inicio de sesión de IPv6.

V23.10.1 (9 de octubre de 2023)

Novedades

- Las bibliotecas de la EPA se actualizaron a la versión 23.9.1.2 (biblioteca OPSWAT OESIS V4.3.3221.0).
- **Soporte para acceso LAN local**

  Citrix Secure Access para macOS y Citrix SSO para iOS ahora admiten la funcionalidad de acceso LAN local de NetScaler Gateway. Puede configurar el acceso a la LAN local de modo que, una vez establecida una conexión VPN, los usuarios finales puedan acceder a los recursos de la LAN local en sus dispositivos cliente o se les impida acceder a ellos. Para obtener más información, consulte lo siguiente:

  - Configuraciones de administración de NetScaler Gateway
  - Configuraciones de usuario final - macOS
  - Configuraciones de usuario final - iOS

V23.09.1 (7 de septiembre de 2023)

> **Importante:**
>
> Si utiliza las versiones más recientes de Apple OS, como macOS 14/iOS 17 y versiones posteriores, le recomendamos que actualice a Citrix Secure Access Client/Citrix SSO versión 23.09.1 o posterior. Para obtener más información sobre los requisitos de software cliente de NetScaler Gateway, consulte Requisitos del sistema cliente Citrix Secure Access.

Novedades

- Las bibliotecas de la EPA se actualizan a la versión 1.3.9.9 (OPSWAT OESIS v4.3.3160).

  [CSACLIENTS-6547]

- **Información sobre conexiones seguras en la interfaz de usuario**

  En la pantalla "Conexiones"de la interfaz de usuario del cliente Citrix Secure Access, puede ver los detalles de la conexión segura. Los detalles incluyen la dirección IP, el FQDN, el puerto de destino y la duración de la conexión. Para obtener más información, consulte Información sobre conexiones seguras.

  [SPA-2364]

- **Vuelva a autenticarse con NetScaler Gateway después de un error en la conexión VPN**

  El cliente Citrix Secure Access para macOS y Citrix SSO para iOS ahora le piden que se vuelva a autenticar con NetScaler Gateway cuando se pierde una conexión VPN. Se le notifica en la interfaz de usuario que indica que se ha perdido la conexión a NetScaler Gateway y que debe volver a autenticarse para reanudar la conexión. Para obtener más información, consulte:

  - Vuelva a conectarse a NetScaler Gateway desde macOS tras un error en la conexión VPN
  - Vuelva a conectarse a NetScaler Gateway desde iOS trasun error en la conexión VPN.

  [CSACLIENTS-6071]

V23.08.1 (24 de agosto de 2023)

Novedades

- En esta versión se han resuelto una serie de problemas para mejorar la estabilidad y el rendimiento generales.
- Las bibliotecas de EPA se actualizaron a la versión 1.3.9.9 (OPSWAT OESIS v4.3.3122).

Cliente de EPA 23.7.6 para macOS (10 de agosto de 2023)

En esta versión se han resuelto una serie de problemas para mejorar la estabilidad y el rendimiento generales.

V23.07.1 (17 de julio de 2023)

Novedades

- **Diversas opciones para compartir archivos de registros**

  La opción "Registros de correo electrónico"de Citrix SSO para iOS ahora se sustituye por la opción "Compartir registros". Los archivos de registros comprimidos ahora se pueden compartir a través de opciones como correo electrónico, chat, guardar en archivos, etc.

  Para obtener más información, consulte Enviar registros.

  [CSACLIENTS-3834]

- **Mejoras en la página de registros**

  La página de registros de Citrix Secure Access para macOS se ha mejorado con las siguientes opciones:

  - Cantidad máxima de archivos de registro: Especifique la cantidad máxima de archivos de registros que quiere agregar para la recopilación de registros.
  - Registros de correo electrónico: Envíe los registros por correo electrónico.

  Para obtener más información, consulte Enviar registros.

  [SPA-2365]

Problemas resueltos

Al conectarse a una VPN, si se le pide que seleccione un certificado para la autenticación, aparecerá la pantalla de inicio de sesión de autenticación detrás de la página de inicio del cliente Citrix Secure Access.

[CSACLIENTS-455]

V23.06.1 (07 de junio de 2023)

Novedades

- **Menú de ayuda en la barra de navegación**

Ahora se agrega un menú de ayuda a la barra de navegación del cliente Citrix Secure Access. Las opciones (Abrir registros, Exportar registros, Registros de correo electrónico y Borrar registros) del menú Ayuda se pueden usar para depurar los registros.

Se presenta una opción de registros de correo electrónico en el menú Ayuda. Se puede usar para compartir los registros por correo electrónico. Para obtener más información, consulte Enviar registros.

[SPA-2361]

Problemas resueltos

En algunos casos, la resolución de nombres abreviados de DNS falla en Citrix Secure Access para macOS y Citrix SSO para iOS.

[NSHELP-34568]

Problemas conocidos

En algunos casos, las rutas excluidas en la tunelización dividida inversa se tunelizan.

[CGOP-24575]

V23.05.2 (11 de mayo de 2023)

Problemas resueltos

Tras una actualización, los dispositivos cliente de Citrix SSO para iOS no pueden establecer conexiones VPN por aplicación.

[NSHELP-35224]

V23.05.1 (04 de mayo de 2023)

Novedades

- Las bibliotecas de EPA se actualizan a la versión 1.3.9.3 y las bibliotecas de OPSWAT se actualizan a la versión 4.3.2987.
- **Soporte para enviar eventos a Citrix Analytics**

  Citrix Secure Access para macOS ahora admite el envío de eventos como la creación, el cierre de sesiones y la conexión de aplicaciones al servicio Citrix Analytics. A continuación, estos eventos se registran en el panel de Secure Private Access Service.

[SPA-2197]

Problemas resueltos

- Cuando los usuarios están conectados a Citrix Secure Access o Citrix SSO, el campo "Duración de la conexión"no muestra la hora en el formato específico de la región.

  [CGOP-23587]

V23.04.1 (04 de abril de 2023)

Novedades

- Las bibliotecas de EPA se actualizan a la versión 1.3.9.1 y las bibliotecas de OPSWAT se actualizan a la versión 4.3.2923.

V22.12.2 (27 de febrero de 2023)

Novedades

- Las bibliotecas de EPA se han actualizado a la versión 1.3.8.9 (OPSWAT OESIS v4.3.2892.0).

V22.12.1 (7 de diciembre de 2022)

En esta versión se han resuelto una serie de problemas para mejorar la estabilidad y el rendimiento generales.

V22.11.1 (29 de noviembre de 2022)

Problemas resueltos

- El inicio de sesión por transferencia no funciona para la autenticación que no sea de nFactor con puertas de enlace locales.

  [CGOP-22729]

Plug-in 22.11.3 de EPA para macOS (28-nov-2022)

Problemas resueltos

- El plug-in de Citrix EPA para macOS se cierra de forma inesperada cuando la GSLB está habilitada en NetScaler.

  [CGOP-22722]

V22.10.1 (17 de noviembre de 2022)

Novedades

- El plug-in de Citrix Endpoint Analysis ahora admite una nueva expresión de validación de direcciones MAC en la que se pueden crear conjuntos de patrones para la lista de direcciones IP permitidas.

  [CGOP-22095]

Problemas resueltos

- A veces, la configuración de proxy vacía de las versiones 13.0 o 13.1 de NetScaler Gateway hace que Citrix SSO cree una configuración de proxy incorrecta.

  [NSHELP-31970]

- A veces, los clientes de VPN no se vuelven a conectar después de una interrupción de la red o después de que el dispositivo se despierte del modo de suspensión.

  [NSHELP-32483]

- A veces, las conexiones de puerta de enlace fallan cuando se utilizan literales de IPv6 como destino.

  [NSHELP-32876]

Plug-in de EPA 22.10.1 para macOS (27 de octubre de 2022)

Novedades

- El plug-in de Citrix Endpoint Analysis ahora admite una nueva expresión de validación de direcciones MAC en la que se pueden crear conjuntos de patrones para la lista de direcciones IP permitidas.

  [CGOP-22098]

- El plug-in de Citrix Endpoint Analysis envía alertas de consentimiento duplicadas mientras gestiona las solicitudes de acceso a redes privadas previas al vuelo de Google Chrome.

  [CGOP-21751]

V22.06.1 (20 de septiembre de 2022)

Novedades

- Las bibliotecas de EPA se actualizan a 4.3.2523.0 (1.3.7.5)

Problemas resueltos

- La autenticación nFactor con la detección EPA no funciona en los clientes de macOS.

  [NSHELP-32182 - macOS]

- En la página principal de Secure Access Agent para macOS, aparece un relleno adicional de color blanco o negro a la izquierda y la parte superior del menú de tres líneas, según el tema seleccionado (claro u oscuro).

  [CGOP-19353 - macOS]

- Al iniciar sesión en la VPN, la ventana WebView se minimiza en el primer intento si el certificado del dispositivo está configurado.

  [CGOP-19354 - macOS]

- Endpoint Analysis no funciona para la aplicación Citrix Secure Access en el cliente macOS cuando el GSLB está habilitado en el dispositivo NetScaler.

  [CGOP-21634 - macOS]

- Si hay un espacio en el nombre de la aplicación configurada e intenta acceder a la aplicación, la ventana emergente Enhanced Security Enabled no aparecerá en los clientes de macOS.

  [ACS-2632 - macOS]

- La autenticación de nFactor con un certificado de cliente opcional falla cuando no hay certificados de cliente apropiados en el dispositivo.

  [NSHELP-32127 - iOS]

- En un dispositivo Mac que usa Chrome, la extensión VPN se bloquea al acceder a dos FQDN.

  [NSHELP-32144]

- Citrix Secure Access se bloquea cuando se recibe un valor de ubicación incorrecto de la puerta de enlace. Esto puede suceder si el administrador define una directiva de respuesta para redirigir a otro host.

  [NSHELP-32312]

- Las conexiones directas a los recursos fuera del túnel establecido por Citrix Secure Access pueden fallar si se produce un retraso o una congestión significativos.

  [NSHELP-31598]

V3.2.4.9: Plug-in de EPA para macOS (01-ago-2022)

Problemas resueltos

- El plug-in de Citrix Endpoint Analysis no gestiona las solicitudes de verificación previa de acceso a redes privadas desde la versión 104 del explorador Google Chrome.

  [CGOP-20709]

- El plug-in de Citrix Endpoint Analysis para macOS no admite GSLB.

  [CGOP-21543]

Problemas conocidos

- El plug-in de Citrix Endpoint Analysis para macOS muestra un cuadro de diálogo de consentimiento duplicado cuando se inicie desde la versión 104 del explorador Google Chrome. Los usuarios tienen que aceptar ambas solicitudes.

  [CGOP-21751]

V22.03.1 (14 de junio de 2022)

Novedades

- Las bibliotecas de EPA se actualizan a 4.3.2393.0.

Problemas resueltos

- Se agrega un dominio DNS adicional a la lista de búsqueda. Esto se debe a que, cuando el túnel dividido se establece en "Dividir"o "Ambos", solo los dominios especificados y sus subdominios NO se tunelizan. Si el dominio especificado es A.B.C, B.C también coincide con A.B.C y *.A.B.C.

  [CGOP-21657]

- La configuración del proxy HTTP/HTTPS que no utiliza un archivo PAC no funciona.

  [CGOP-21660]

V22.02.3 (24 de marzo de 2022)

Novedades

- Citrix Secure Access para macOS resuelve el FQDN de un nodo de servicio en cada conexión de datos TCP del cliente para las conexiones del espacio de trabajo en la nube. La resolución del FQDN de un nodo de servicio en cada conexión de datos TCP no se aplica a las conexiones de puerta de enlace local.

  [ACS-1068]

Problemas resueltos

- A veces, Citrix Secure Access para macOS interrumpe las conexiones debido a problemas con algunos protocolos que no son de DNS que utilizan el puerto 53, como STUN.

  [NSHELP-31004]

- La aplicación Citrix Secure Access rompe algunos protocolos cuando el servidor envía datos antes que el cliente, inmediatamente después de establecer la conexión.

  [NSHELP-29374]

- Si el usuario cierra la ventana de autenticación del cliente Citrix Secure Access para macOS sin completar la autenticación, los intentos posteriores de conectarse al servidor fallarán hasta que se reinicie la aplicación.

  [ACS-2415]

- El cliente Citrix Secure Access para macOS ahora viene incluido con la versión 4.3.2367.0 de la biblioteca OPSWAT

  [NSHELP-30802]

- Citrix Secure Access para macOS tarda más de lo esperado en ejecutar la comprobación de EPA posterior a la autenticación.

  [NSHELP-29118]

Problemas conocidos

- La aplicación Citrix Secure Access para macOS cierra sesión un minuto después de que no se pueda acceder a la región del servicio Citrix Secure Private Access ya conectada. Sin embargo, esto no afecta a las conexiones de Gateway local.

  [ACS-2715]

V22.02.2 (15 de febrero de 2022)

Problemas resueltos

- Se muestran varias ventanas emergentes cuando un usuario intenta acceder a una aplicación web cancelada desde Citrix Secure Access para macOS.

  [ACS-2406]

V22.01.1 (08 de febrero de 2022)

Problemas resueltos

- Las conexiones VPN por aplicación con dispositivos Citrix SSO para iOS no se conectan a NetScaler Gateway en puertos que no sean 443.

  [NSHELP-30653]

V1.4.1 (28 de enero de 2022)

Novedades

- La aplicación Citrix SSO para macOS ahora pasa a llamarse Citrix Secure Access.

  [ACS-1092]

Problemas resueltos

- La autenticación de certificados de cliente falla si el servidor de autenticación solicita el certificado de cliente varias veces en la misma sesión de vista web.

  [CGOP-20388]

- Citrix SSO no puede establecer una conexión VPN si el certificado del servidor solo tiene una dirección IP para el nombre común debido a un proxy entre el cliente y el ADC.

  [CGOP-20390]

- La exploración de EPA para verificar el último análisis completo del sistema del antivirus falla en macOS.

  [NSHELP-29571]

- A veces, la aplicación Citrix SSO se bloquea mientras se gestionan paquetes DNS de gran tamaño.

  [NSHELP-29133]

V1.4.0 (17 de noviembre de 2021)

Problemas resueltos

- A veces, el código de validación del servidor falla cuando el certificado del servidor es de confianza. Como resultado, los usuarios finales no pueden acceder a la puerta de enlace.

  [NSHELP-28942]

- Citrix SSO no puede restablecer la conexión VPN después de una interrupción de la red.

  [CGOP-19988]

V1.3.13 (05 de noviembre de 2021)

Problemas resueltos

- Es posible que experimente errores al filtrar sesiones para VPN administradas y no administradas. A las solicitudes iniciales para establecer la sesión les falta la información de ‘‘ManagedVpn’’en el encabezado User-Agent.

  [CGOP-19561]

V1.3.12 (21 de octubre de 2021)

Problemas resueltos

- La autenticación de certificados de cliente falla para Citrix SSO para macOS si no hay certificados de cliente en el llavero de macOS.

  [NSHELP-28551]

- La aplicación Citrix SSO se bloquea de forma intermitente al recibir notificaciones.

  [CGOP-19363]

- La extensión VPN puede bloquearse cuando se llama al parámetro "isFeatureEnabled"para comprobar una marca de función.

  [CGOP-19360]

- La extensión VPN de puerta de enlace se bloquea si el protocolo DTLS tiene una carga útil vacía.

  [CGOP-19361]

- La aplicación SSO se bloquea de forma intermitente cuando el dispositivo se despierta del modo de suspensión y la VPN está conectada.

  [CGOP-19362]

V1.3.11 (17 de septiembre de 2021)

Problemas resueltos

- El análisis de EPA para comprobar el firewall falla en los dispositivos macOS que utilizan Citrix SSO.

  [CGOP-19271]

- El inicio de sesión Citrix SSO se bloquea en un dispositivo iOS 12 cuando se configura la autenticación heredada o el cumplimiento del acceso a la red de Intune (NAC).

  [CGOP-19261]

V1.3.10 (31 de agosto de 2021)

Novedades

- Citrix SSO para macOS se incluye ahora con la biblioteca OPSWAT versión 4.3.1977.0.

  [NSHELP-28467]

V1.3.9 (13 de agosto de 2021)

Problemas resueltos

- En algunos sistemas con software proxy HTTP instalado, la dirección IP de NetScaler Gateway aparece internamente como 127.0.0.1, lo que impide el establecimiento del túnel.

  [CGOP-18538]

- La configuración "Bloquear servidores que no son de confianza"no funciona en sistemas que admiten la localización de Citrix SSO para iOS en un idioma distinto al inglés.

  [CGOP-18539]

- Citrix SSO no puede conectarse a sistemas en los que el nombre DNS no coincide con el nombre común del certificado del servidor. Citrix SSO comprueba ahora los nombres alternativos del sujeto y se conecta correctamente.

  [NSHELP-28348]

V1.3.8 (07 de julio de 2021)

Novedades

- Citrix SSO para macOS solo es compatible con las versiones 10.15 (Catalina) y superiores.

  [CGOP-12555]

- A partir de la versión 1.3.8 de Citrix SSO para macOS, las bibliotecas EPA están integradas en la aplicación y no se descargan del servidor de NetScaler Gateway. La versión actual de la biblioteca EPA integrada es 1.3.5.1.

  [NSHELP-26838]

Configurar Citrix Secure Access para usuarios de iOS

March 27, 2024

> **Importante:**
>
> - Citrix SSO para iOS ahora pasa a llamarse Citrix Secure Access. Estamos actualizando nuestra documentación y las capturas de pantalla de la interfaz de usuario para reflejar este cambio de nombre. Es posible que observe las referencias de SSO de Citrix utilizadas en la documentación durante este período de transición.
> - La VPN no se puede usar en iOS 12 y versiones posteriores. Para continuar con la VPN, utilice Citrix Secure Access.

Para ver la lista de algunas de las funciones más utilizadas que admite Citrix Secure Access para iOS, consulte Clientes VPN de NetScaler Gateway y funciones compatibles.

Compatibilidad con productos MDM

Citrix Secure Access (macOS/iOS) es compatible con la mayoría de los proveedores de MDM, como Citrix Endpoint Management (anteriormente XenMobile), Microsoft Intune, etc.

Citrix Secure Access (macOS/iOS) también admite una función denominada Control de acceso a la red (NAC). Para obtener más información sobre NAC, consulte Configurar la comprobación del dispositivo de control de acceso a la red para el servidor virtual de NetScaler Gateway para el inicio de sesiónde Con NAC, los administradores de MDM pueden imponer el cumplimiento de los dispositivos del usuario final antes de conectarse al dispositivo NetScaler. NAC en Citrix Secure Access (macOS/iOS) requiere un servidor MDM como Citrix Endpoint Management o Intune y NetScaler.

> **Nota:**
>
> Para usar el cliente Citrix Secure Access en macOS/iOS con NetScaler Gateway VPN sin MDM, debe agregar una configuración de VPN. Puede agregar la configuración de VPN en iOS desde la página principal de Citrix Secure Access (macOS/iOS).

Configurar un perfil de VPN administrado por MDM para el cliente Citrix Secure Access (macOS/iOS)

En la siguiente sección se muestran instrucciones paso a paso para configurar perfiles de VPN para todo el dispositivo y por aplicación para el cliente Citrix Secure Access (macOS/iOS) mediante Citrix Endpoint Management (anteriormente XenMobile) como ejemplo. Otras soluciones de MDM pueden usar este documento como referencia cuando trabajen con Citrix Secure Access (macOS/iOS).

> **Nota:**
>
> En esta sección se explican los pasos de configuración de un perfil VPN básico para todo el dispositivo y por aplicación. También puede configurar Proxies bajo demanda siguiendo la documentación de Citrix Endpoint Management (anteriormente XenMobile) o la configuración de carga útil de VPN de MDM de Apple.

Perfiles VPN a nivel de dispositivo

Los perfiles VPN a nivel de dispositivo se utilizan para configurar una VPN para todo el sistema. El tráfico de todas las aplicaciones y servicios se dirige a NetScaler Gateway en función de las directivas de VPN (como túnel completo, túnel dividido, túnel dividido inverso) definidas en NetScaler.

Para configurar una VPN a nivel de dispositivo en Citrix Endpoint Management Realice los siguientes pasos para configurar una VPN a nivel de dispositivo en Citrix Endpoint Management.

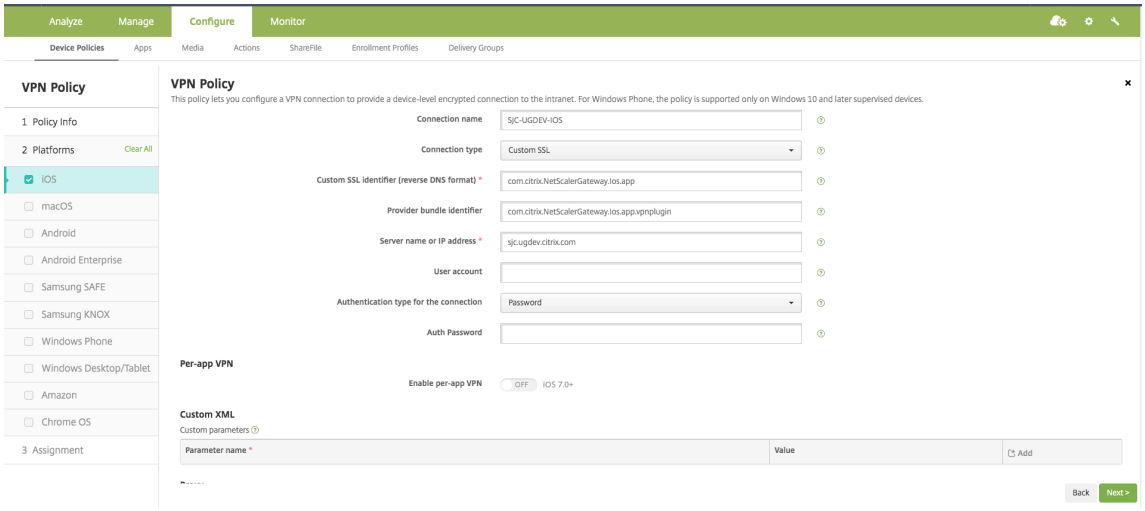
1. En la consola de Citrix Endpoint Management MDM, vaya a **Configurar** > **Directivas de dispositivo** > **Agregar nueva directiva**.
2. Seleccione **iOS** en el panel Plataforma de directivas izquierdo. Selecciona **VPN** en el panel derecho.
3. En la página **Información de directiva**, introduzca un nombre y una descripción de directiva válidos y haga clic en **Siguiente**.
4. En la página **Directiva de VPN** para iOS, escriba un nombre de conexión válido y elija **SSL personalizado** en **Tipo de conexión**.

   En la carga útil de VPN de MDM, el nombre de la conexión corresponde a la clave **UserDefinedName** y la **clave de tipo VPN** debe establecerse en **VPN**.
5. En **Identificador SSL personalizado (formato DNS inverso)**, escriba **com.citrix.NetscalerGateway.ios.ap**
   Este es el identificador de paquete de Citrix Secure Access en iOS.

   En la carga útil de VPN de MDM, el identificador SSL personalizado corresponde a la clave **VPNSubType**.
6. En el **identificador del paquete del proveedor**, escriba **com.citrix.NetScalerGateway.ios.app.vpnPlugin**
   Es el identificador del paquete de la extensión de red que se encuentra en el binario de la aplicación Citrix Secure Access para iOS.

   En la carga útil de VPN de MDM, el identificador del paquete de proveedores corresponde a la clave **ProviderBundleIdentifier**.
7. En **Nombre del servidor o dirección IP**, introduzca la dirección IP o FQDN (nombre de dominio completo) del NetScaler asociado a esta instancia de Citrix Endpoint Management.

   El resto de los campos de la página de configuración son opcionales. Las configuraciones de estos campos se encuentran en la documentación de Citrix Endpoint Management (anteriormente XenMobile).
8. Haga clic en **Siguiente**.



9. Haga clic en **Guardar**.

Perfiles VPN por aplicación

Los perfiles VPN por aplicación se utilizan para configurar la VPN para una aplicación específica. El tráfico de la aplicación específica se canalizará únicamente a NetScaler Gateway. La **carga útil de VPN por aplicación** admite todas las claves de la VPN en todo el dispositivo, además de algunas otras claves.

Para configurar una VPN por aplicación en Citrix Endpoint Management Realice los siguientes pasos para configurar una VPN por aplicación:

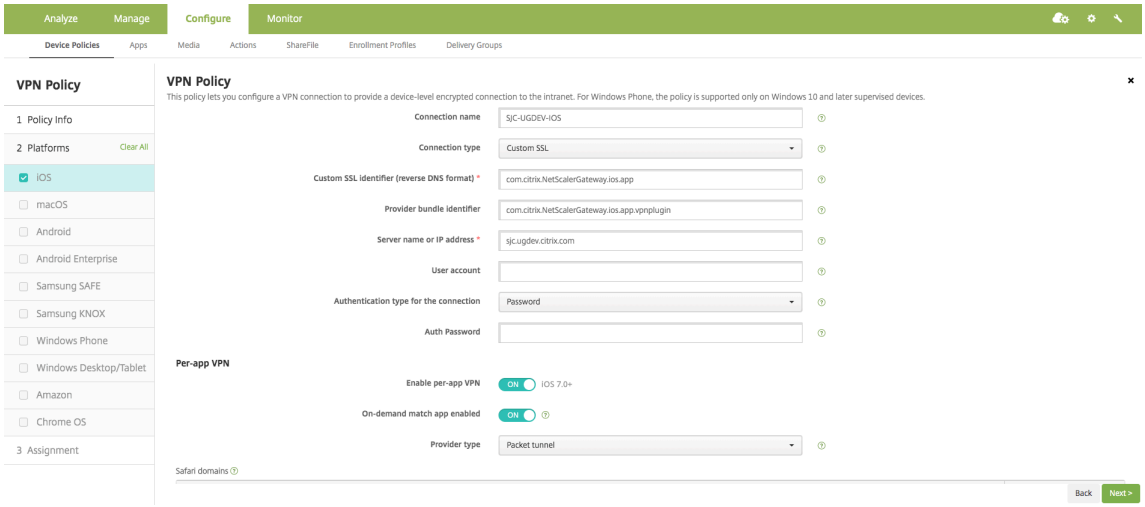
1. Complete la configuración VPN a nivel de dispositivo en Citrix Endpoint Management.
2. Active el interruptor **Habilitar VPN por aplicación** en la sección VPN por aplicación.
3. Encienda el **conmutador On-Demand Match App** si Citrix Secure Access (macOS/iOS) debe iniciarse automáticamente al iniciar la aplicación Match. Esto se recomienda para la mayoría de los casos por aplicación.

   En la carga útil de VPN de MDM, este campo corresponde a la clave **OnDemandMatchAppEnabled**.
4. En **Tipo de proveedor**, seleccione **Túnel de paquetes**.

   En la carga útil de VPN de MDM, este campo corresponde al **tipo de proveedor**clave.
5. La configuración de Safari Domain es opcional. Cuando se configura un dominio de Safari, Citrix Secure Access (macOS/iOS) se inicia automáticamente cuando los usuarios inician Safari y navegan hasta una URL que coincide con la del campo **Dominio**. Esto no es recomendable si quieres restringir la VPN para una aplicación específica.

En la carga útil de VPN de MDM, este campo corresponde a la clave **SafariDomains**.

El resto de los campos de la página de configuración son opcionales. Las configuraciones de estos campos se encuentran en la documentación de Citrix Endpoint Management (anteriormente XenMobile).



6. Haz clic en **Siguiente.**
7. Haga clic en **Guardar**.

Para asociar este perfil de VPN a una aplicación específica del dispositivo, debe crear una directiva de inventario de
aplicaciones y una directiva del proveedor de credenciales siguiendo esta guía - https://www.citrix.com/blogs/2016/04/19/per-app-vpn-with-xenmobile-and-citrix-vpn/.

Configuración de túnel dividido en VPN por aplicación

Los clientes de MDM pueden configurar el túnel dividido en una VPN por aplicación para Citrix Secure Access (macOS/iOS). El siguiente par clave/valor debe agregarse a la sección de configuración del proveedor del perfil VPN creado en el servidor MDM.

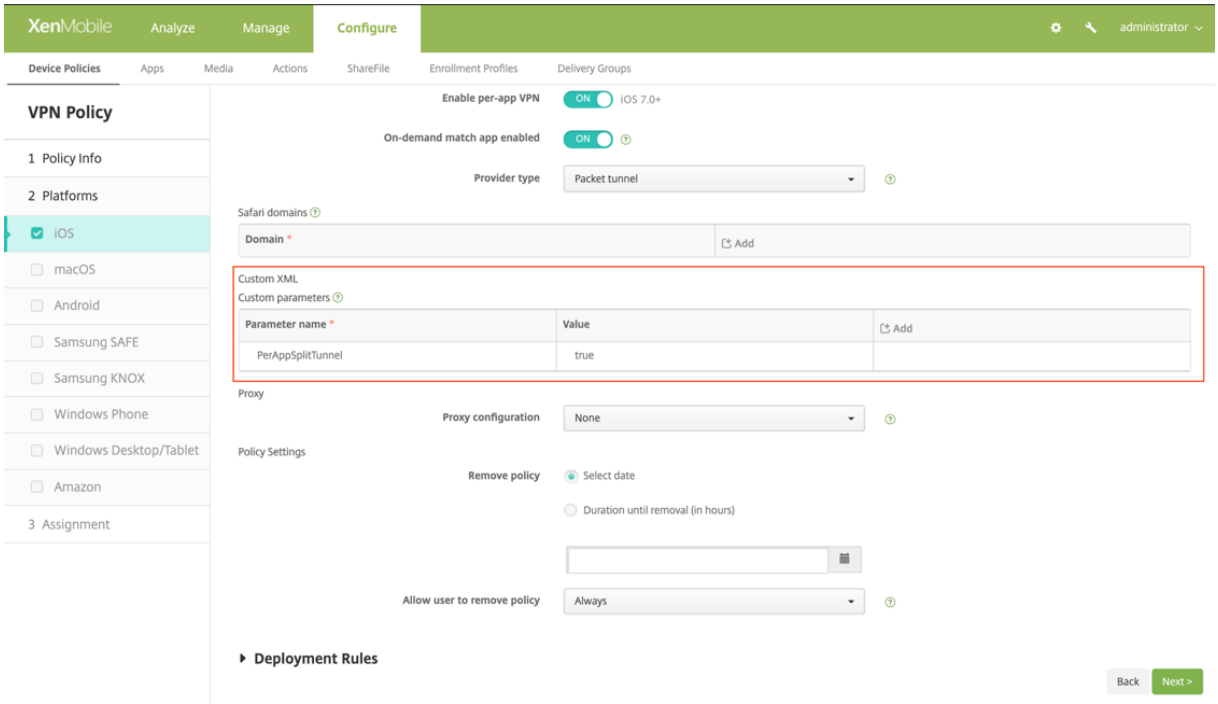
```
1  -  Key = "PerAppSplitTunnel"
2  -  Value = "true or 1 or yes"
3  <!--NeedCopy-->
```

La clave distingue entre mayúsculas y minúsculas y debe coincidir exactamente, mientras que el valor no distingue mayúsculas

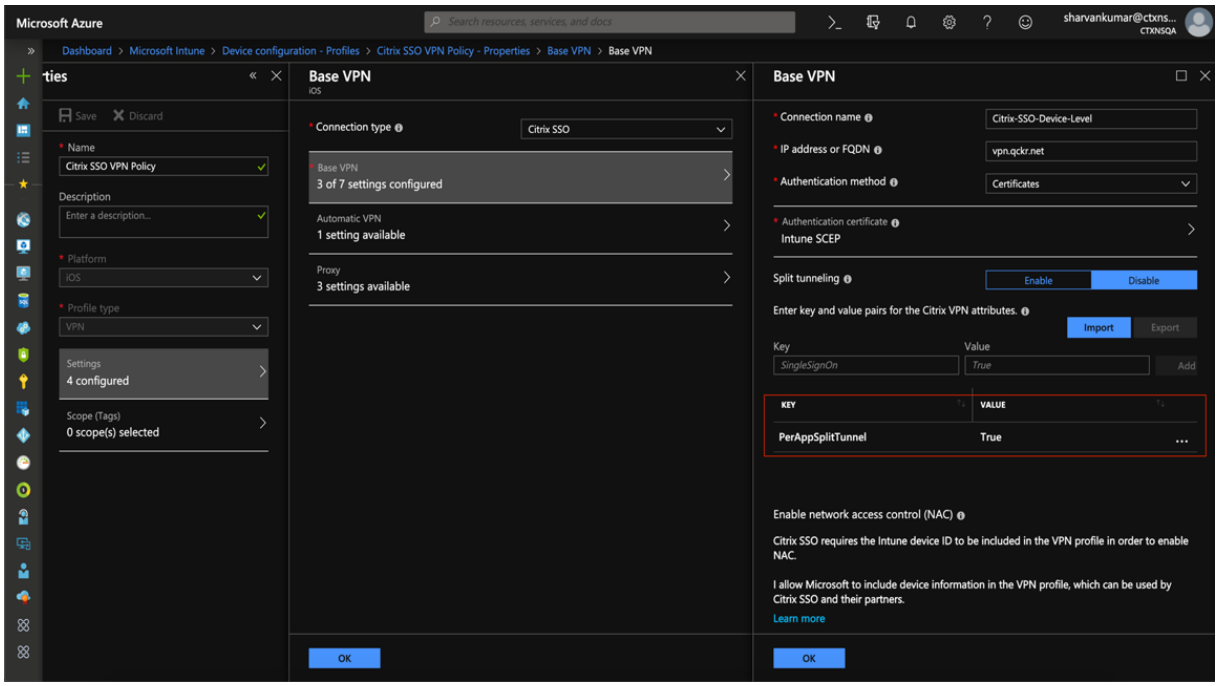
> **Nota:**
>
> La interfaz de usuario para configurar la configuración del proveedor no es estándar en todos los proveedores de MDM. Póngase en contacto con el proveedor de MDM para buscar la sección de

> configuración del proveedor en la consola de usuario de MDM.

A continuación se muestra una captura de pantalla de ejemplo de la configuración (configuración específica del proveedor) en Citrix Endpoint Management.



A continuación se muestra una captura de pantalla de ejemplo de la configuración (configuración específica del proveedor) en Microsoft Intune.



Inhabilitar los perfiles VPN creados por el usuario

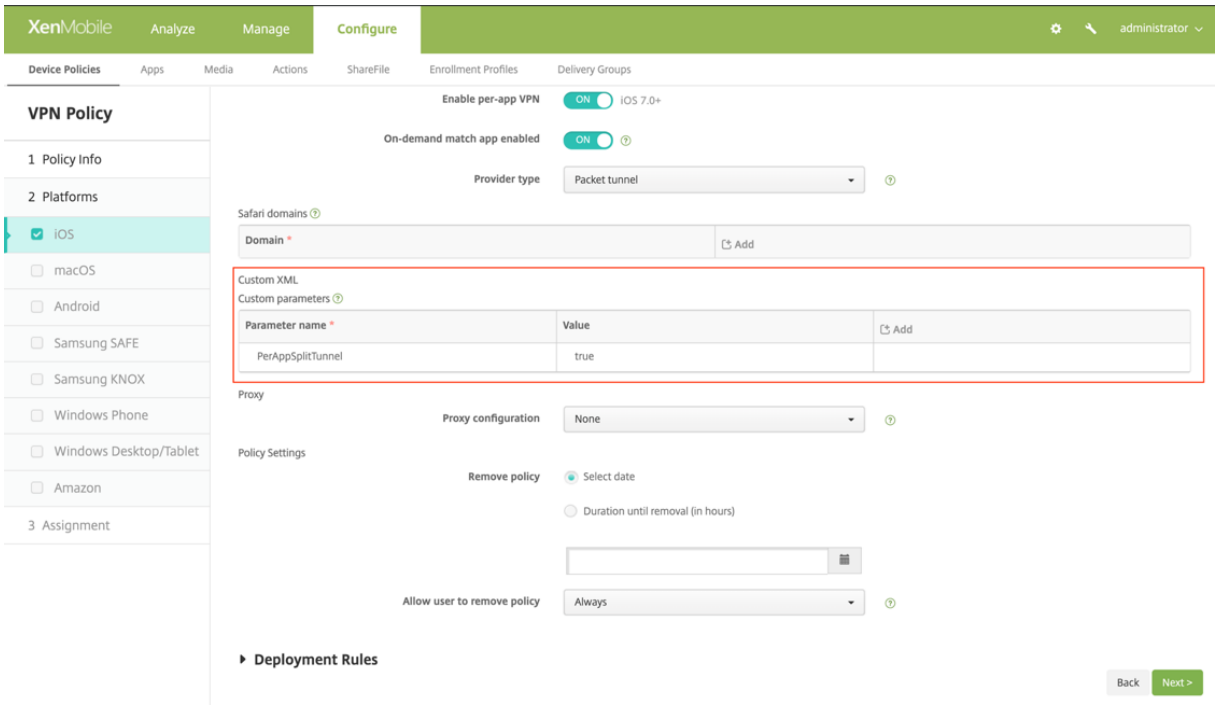
Los clientes de MDM pueden impedir que los usuarios creen manualmente perfiles de VPN desde Citrix Secure Access (macOS/iOS). Para ello, se debe agregar el siguiente par clave/valor a la sección de configuración del proveedor del perfil VPN creado en el servidor MDM.

```
1  -  Key = "disableUserProfiles"
2  -  Value = "true or 1 or yes"
3  <!--NeedCopy-->
```

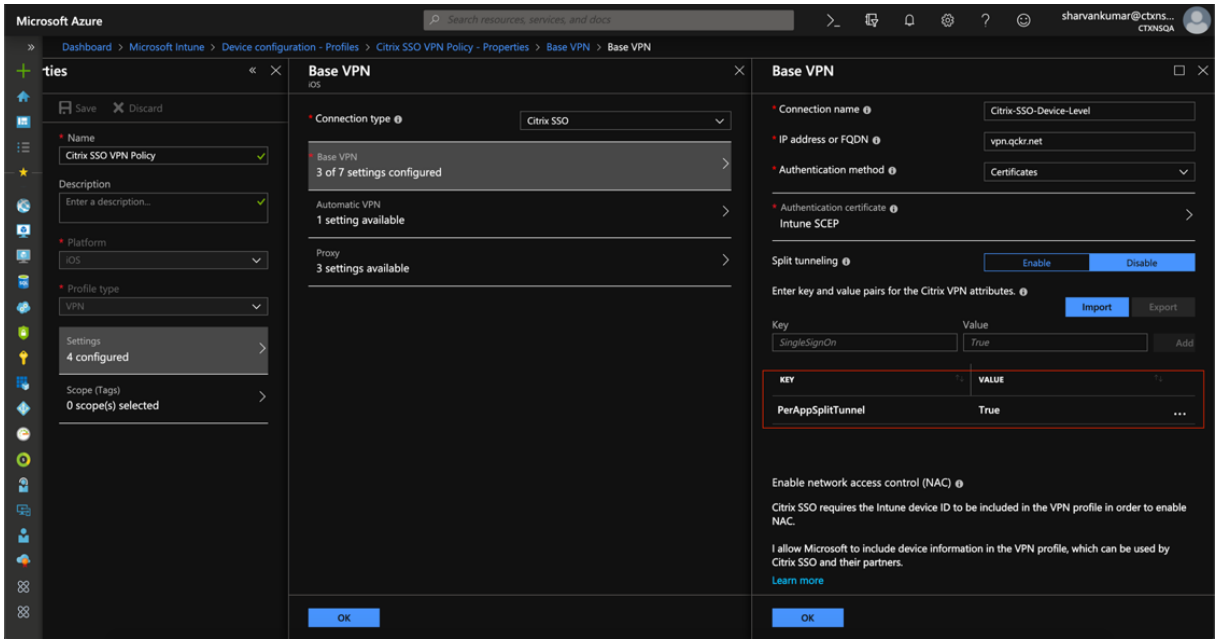
La clave distingue entre mayúsculas y minúsculas y debe coincidir exactamente, mientras que el valor no distingue mayúsculas

> **Nota:**
>
> La interfaz de usuario para configurar la configuración del proveedor no es estándar en todos los proveedores de MDM. Póngase en contacto con el proveedor de MDM para buscar la sección de configuración del proveedor en la consola de usuario de MDM.

A continuación se muestra una captura de pantalla de ejemplo de la configuración (configuración específica del proveedor) en Citrix Endpoint Management.



A continuación se muestra una captura de pantalla de ejemplo de la configuración (configuración específica del proveedor) en Microsoft Intune.



Manejo DNS

La configuración de DNS recomendada para el cliente Citrix Secure Access es la siguiente:

- **Dividir DNS > REMOTE** si el túnel dividido está en **OFF.**
- **DNS dividido > BOTH** si el túnel dividido está **activado**. En este caso, los administradores tienen que agregar sufijos DNS para los dominios de la intranet. Las consultas DNS de los FQDN pertenecientes a sufijos DNS se tunelizan al dispositivo NetScaler y las consultas restantes se dirigen al enrutador local.

> **Nota:**
>
> - Se recomienda que el indicador de **corrección de truncamiento de DNS** esté siempre **activado**. Para obtener más información detallada, consulte https://support.citrix.com/article/CTX200243.
> - Cuando el túnel dividido se establece **en ON** y DNS dividido en **REMOTE**, puede haber problemas para resolver las consultas DNS después de conectar la VPN. Esto se relaciona con que el marco de extensión de red no intercepta todas las consultas DNS.

Problemas conocidos

Descripción del problema: Túnel para direcciones FQDN que contienen un dominio “ `.local`” en configuraciones VPN por aplicación o VPN bajo demanda. Hay un error en el marco de extensiones de red de Apple que impide que las direcciones FQDN que contienen `.local` en la parte del dominio

(por ejemplo, http://wwww.abc.local) se envíen por túnel a través de la interfaz TUN del sistema. En su lugar, el tráfico de las direcciones FQDN se envía a través de la interfaz física del dispositivo cliente. El problema solo se observa con la configuración de VPN por aplicación o VPN bajo demanda y no se observa con las configuraciones de VPN de todo el sistema. Citrix ha presentado un informe de error de radar a Apple y Apple ha observado que, según el RFC-6762: https://tools.ietf.org/html/rfc6762, local es una consulta de DNS de multidifusión (mDNS) y, por lo tanto, no es un error. Sin embargo, Apple aún no ha cerrado el error y no está claro si el problema se solucionará en futuras versiones de iOS.

Solución alternativa: Asigne un nombre de dominio `non .local` para tales direcciones como solución alternativa.

Limitaciones

- El análisis de punto final (EPA) no es compatible con iOS.
- No se admite la tunelización dividida basada en puertos/protocolos.

Enviar identidad de certificado de usuario como archivo adjunto de correo electrónico a los usuarios de iOS

March 27, 2024

> **Importante:**
>
> Citrix SSO para iOS ahora se llama Citrix Secure Access. Estamos actualizando nuestra documentación y las capturas de pantalla de la interfaz de usuario para reflejar este cambio de nombre.

Citrix Secure Access para iOS admite la autenticación de certificados de cliente con NetScaler Gateway. En iOS, los certificados se pueden entregar a Citrix Secure Access de una de las siguientes maneras:

- Servidor MDM: este es el enfoque preferido por los clientes de MDM. Los certificados se configuran directamente en el perfil VPN administrado por MDM. Los perfiles VPN y los certificados se envían a continuación a los dispositivos inscritos cuando el dispositivo se inscribe en el servidor MDM. Siga los documentos específicos del proveedor de MDM para este enfoque.
- Correo electrónico: único enfoque para clientes que no sean MDM. En este enfoque, los administradores envían a los usuarios un correo electrónico con la identidad del certificado de usuario (certificado y clave privada) adjunta como archivo PCKS #12. Los usuarios deben tener configuradas sus cuentas de correo electrónico en su dispositivo iOS para recibir el correo electrónico

con datos adjuntos. A continuación, el archivo se puede importar a Citrix Secure Access en iOS. En la siguiente sección se explican los pasos de configuración de este enfoque.

Requisitos previos

- Certificado de usuario: archivo de identidad PKCS #12 con extensión.pfx o.p12 para un usuario determinado. Este archivo contiene tanto el certificado como la clave privada.
- Cuenta de correo electrónico configurada en el dispositivo iOS.
- Citrix Secure Access instalado en el dispositivo iOS.

Pasos de configuración

1. Cambie el nombre del tipo de extensión/MIME del certificado de usuario.

   Las extensiones de archivo más utilizadas para el certificado de usuario son ".pfx", ".p12", etc. Estas extensiones de archivo no son estándar para la plataforma iOS a diferencia de formatos como.pdf,.doc. Tanto «.pfx» como «.p12"son reclamados por el sistema iOS y no pueden ser reclamados por aplicaciones de terceros, como Citrix Secure Access. Por lo tanto, Citrix Secure Access ha definido un nuevo tipo de extensión/MIME denominado «.citrixsso-pfx» y «.citrixsso-p12". Los administradores deben cambiar el tipo de extensión o MIME del certificado de usuario, de ".pfx"estándar o ".p12"a ".citrixsso-pfx"o ".citrixsso-p12" respectivamente. Para cambiar el nombre de la extensión, los administradores pueden ejecutar el siguiente comando en el símbolo del sistema o en la terminal.

   Windows 10

   ```
   cd <DIRECTORY_PATH_TO_CERTIFICATE_FILE>
   rename <CERTIFICATE_FILE_NAME>.pfx <CERTIFICATE_FILE_NAME>.
      citrixsso-pfx
   <!--NeedCopy-->
   ```

   macOS

   ```
   cd <DIRECTORY_PATH_TO_CERTIFICATE_FILE>
   mv <CERTIFICATE_FILE_NAME>.pfx <CERTIFICATE_FILE_NAME>.citrixsso-
      pfx
   <!--NeedCopy-->
   ```

2. Envía el archivo como archivo adjunto de correo electrónico.

   El archivo de certificado de usuario con la nueva extensión se puede enviar como un archivo adjunto de correo electrónico al usuario.

   Al recibir el correo electrónico, los usuarios deben instalar el certificado en Citrix Secure Access.

Configure el archivo PAC proxy para la aplicación Citrix SSO para usuarios de iOS o el cliente Citrix Secure Access para usuarios de macOS

March 27, 2024

> **Importante:**
>
> Citrix SSO para iOS ahora se llama Citrix Secure Access. Estamos actualizando nuestra documentación y las capturas de pantalla de la interfaz de usuario para reflejar este cambio de nombre.

La aplicación Citrix Secure para iOS o el cliente Citrix Secure Access para macOS admiten la configuración automática de proxy (archivo PAC de proxy) una vez establecido el túnel VPN. Los administradores pueden usar el archivo PAC de proxy para permitir que todo el tráfico HTTP del cliente pase por un proxy, incluida la resolución de nombres de host.

Cómo configurar un archivo PAC proxy

Tener un equipo interno que pueda alojar un archivo proxy. Por ejemplo, considere que la IP del equipo es 172.16.111.43 y el nombre del archivo PAC es proxy.pac.

Si la dirección IP del servidor proxy real es 172.16.43.83 que escucha en el puerto 8080, entonces un ejemplo de proxy.pac es el siguiente:

```
function FindProxyForURL(url, host)
{
return “PROXY 172.16.43.83:8080”;
}
```

La URL del PAC proxy es http://172.16.111.43/proxy.pac. Suponiendo que el archivo está alojado en el puerto HTTP 80.

Para obtener más información, consulte https://support.citrix.com/article/CTX224235 o Configuración automática de proxy para compatibilidad con proxy saliente para NetScaler Gateway.

Nota:

- Si Split Tunnel está ACTIVADO, asegúrese de que la dirección IP del servidor que aloja el archivo PAC esté incluida en la lista de aplicaciones de la intranet para que sea accesible a través de VPN.
- Tras iniciar sesión desde Citrix Secure Access (macOS/iOS), los exploradores comienzan a utilizar las reglas del archivo PAC del proxy. Si solo se proporciona una regla de proxy como en el ejemplo anterior, todo el tráfico HTTP o HTTPS se enruta al servidor proxy interno.

Configurar Citrix Secure Access para usuarios de macOS

March 27, 2024

> **Importante:**
>
> Citrix SSO para iOS ahora se llama Citrix Secure Access. Estamos actualizando nuestra documentación y las capturas de pantalla de la interfaz de usuario para reflejar este cambio de nombre.

El cliente de Citrix Secure Access para macOS ofrece la mejor solución de acceso a las aplicaciones y protección de datos que ofrece NetScaler Gateway. Ahora puede acceder de forma segura a las aplicaciones críticas para el negocio, los escritorios virtuales y los datos corporativos en cualquier momento y desde cualquier lugar.
Citrix Secure Access es el cliente de VPN de próxima generación para que NetScaler Gateway cree y administre conexiones VPN desde dispositivos macOS. Citrix Secure Access se creó con el marco de extensión de red (NE) de Apple. NE framework de Apple es una biblioteca moderna que contiene API que se pueden usar para personalizar y ampliar las funciones de red principales de macOS. La extensión de red compatible con SSL VPN está disponible en dispositivos con macOS 10.11 o una versión posterior.

Citrix Secure Access proporciona compatibilidad completa con la administración de dispositivos móviles (MDM) en macOS. Con un servidor MDM, un administrador ahora puede configurar y administrar de forma remota perfiles VPN a nivel de dispositivo y por aplicación.
Citrix Secure Access para macOS se puede instalar desde una tienda de aplicaciones de Mac.

Para obtener una lista de algunas funciones de uso común que admite el cliente de Citrix Secure Access para macOS, consulte Clientes de VPN de NetScaler Gateway y funciones compatibles.

Compatibilidad con productos MDM

Citrix Secure Access para macOS es compatible con la mayoría de los proveedores de MDM, como Citrix XenMobile, Microsoft Intune, etc. Es compatible con una función denominada Control de acceso a la red (NAC) mediante la cual los administradores de MDM pueden imponer el cumplimiento de los dispositivos del usuario final antes de conectarse a NetScaler Gateway. El NAC en Citrix Secure Access requiere un servidor MDM como XenMobile y NetScaler Gateway. Para obtener más información sobre NAC, consulte Configurar la comprobación del dispositivo de control de acceso a la red para el servidor virtual de NetScaler Gateway para el inicio de sesiónde

> **Nota:**
>
> Para usar Citrix Secure Access con NetScaler Gateway VPN sin MDM, debe agregar una config-

> uración de VPN. Puede agregar la configuración de VPN en macOS desde la página de configuración de Citrix Secure Access.

Configurar un perfil de VPN administrada por MDM para Citrix Secure Access

En la siguiente sección se muestran instrucciones paso a paso para configurar perfiles de VPN para todo el dispositivo y por aplicación para Citrix Secure Access mediante Citrix Endpoint Management (anteriormente XenMobile) como ejemplo. Otras soluciones de MDM pueden usar este documento como referencia cuando trabajan con Citrix Secure Access.

> **Nota:**
>
> En esta sección se explican los pasos de configuración de un perfil VPN básico para todo el dispositivo y por aplicación. También puede configurar Proxies bajo demanda siguiendo la documentación de Citrix Endpoint Management (anteriormente XenMobile) o la configuración de carga útil de VPN de MDM de Apple.

Perfiles VPN a nivel de dispositivo

Los perfiles VPN a nivel de dispositivo se utilizan para configurar una VPN para todo el sistema. El tráfico de todas las aplicaciones y servicios se dirige a NetScaler Gateway en función de las directivas de VPN (como túnel completo, túnel dividido, túnel dividido inverso) definidas en NetScaler.

Para configurar una VPN a nivel de dispositivo en Citrix Endpoint Management Realice los siguientes pasos para configurar una VPN a nivel de dispositivo.

1. En la consola de Citrix Endpoint Management MDM, vaya a **Configurar** > **Directivas de dispositivo** > **Agregar nueva directiva**.
2. Seleccione **macOS** en el panel de la izquierda Plataforma de directivas. Seleccione **Directiva VPN** en el panel derecho.
3. En la página **Información de directiva**, introduzca un nombre y una descripción de directiva válidos y haga clic en **Siguiente**.
4. En la página de **detalles de directiva** para macOS, escriba un nombre de conexión válido y elija **SSL personalizado** en **Tipo de conexión**.

   En la carga útil de VPN de MDM, el nombre de la conexión corresponde a la clave **UserDefinedName** y la **clave de tipo VPN** debe establecerse en **VPN**.
5. En **Identificador SSL personalizado (formato DNS inverso)**, escriba **com.citrix.NetScalerGateway.macos**
   Este es el identificador del paquete de Citrix Secure Access en macOS.

En la carga útil de VPN de MDM, el identificador SSL personalizado corresponde a la clave **VPN-SubType**.

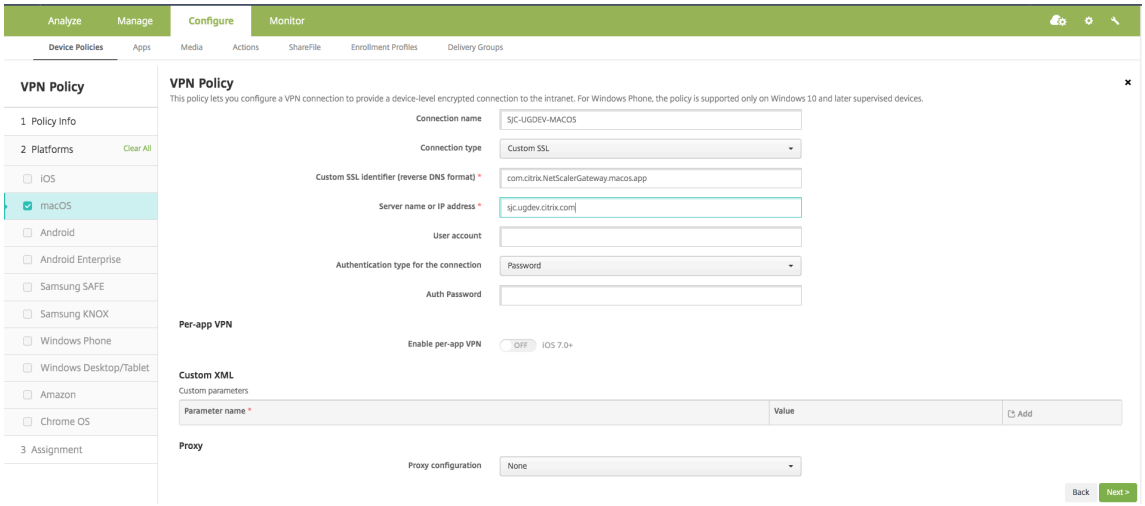
6. En el **identificador del paquete del proveedor**, escriba **com.citrix.NetScalerGateway.macos.app.vpnplu**
   Es el identificador del paquete de la extensión de red contenida en el binario del cliente Citrix Secure Access.

   En la carga útil de VPN de MDM, el identificador del paquete de proveedores corresponde a la clave **ProviderBundleIdentifier**.

7. En **Nombre del servidor o dirección IP**, introduzca la dirección IP o FQDN del NetScaler asociado a esta instancia de Citrix Endpoint Management.

   El resto de los campos de la página de configuración son opcionales. Las configuraciones de estos campos se encuentran en la documentación de Citrix Endpoint Management.

8. Haga clic en **Siguiente**.



9. Haga clic en **Guardar**.

Perfiles VPN por aplicación

Los perfiles VPN por aplicación se utilizan para configurar una VPN para una aplicación específica. El tráfico de la aplicación específica se canalizará únicamente a NetScaler Gateway. La **carga útil de VPN por aplicación admite todas** las claves de la VPN en todo el dispositivo, además de algunas otras claves.

Para configurar una VPN por aplicación en Citrix Endpoint Management Realice los siguientes pasos para configurar una VPN por aplicación en Citrix Endpoint Management:

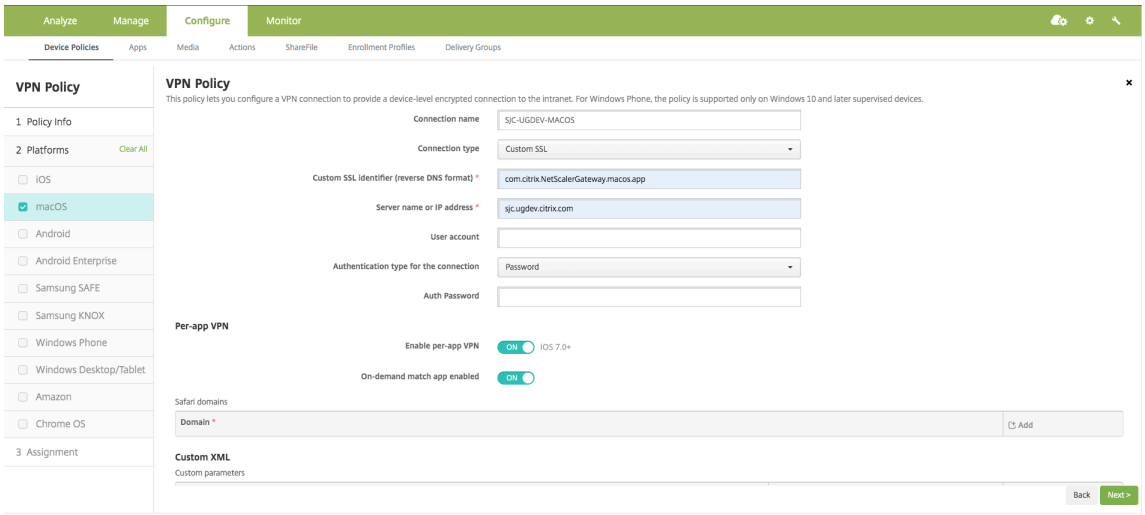
1. Complete la configuración VPN a nivel de dispositivo en Citrix Endpoint Management.

2. Active el interruptor **Habilitar VPN por aplicación** en la sección **VPN por aplicación** .
3. Active la opción **On-Demand Match App Enabled** si Citrix Secure Access debe iniciarse automáticamente cuando se inicia la aplicación Match. Esto se recomienda para la mayoría de los casos por aplicación.

   En la carga útil de VPN de MDM, este campo corresponde a la clave **OnDemandMatchAppEnabled**.
4. La configuración de Safari Domain es opcional. Cuando se configura un dominio de Safari, Citrix Secure Access se inicia automáticamente cuando los usuarios inician Safari y navegan hasta una URL que coincide con la del campo **Dominio** . Esto no es recomendable si quieres restringir la VPN para una aplicación específica.

   En la carga útil de VPN de MDM, este campo corresponde a la clave **SafariDomains**.

   El resto de los campos de la página de configuración son opcionales. Las configuraciones de estos campos se encuentran en la documentación de Citrix Endpoint Management (anteriormente XenMobile).



5. Haga clic en **Siguiente**.
6. Haga clic en **Guardar**.

   Para asociar el perfil VPN a una aplicación específica del dispositivo, debe crear una directiva de inventario de aplicaciones y una directiva del proveedor de credenciales siguiendo esta guía - https://www.citrix.com/blogs/2016/04/19/per-app-vpn-with-xenmobile-and-citrix-vpn/

Configuración de túnel dividido en VPN por aplicación

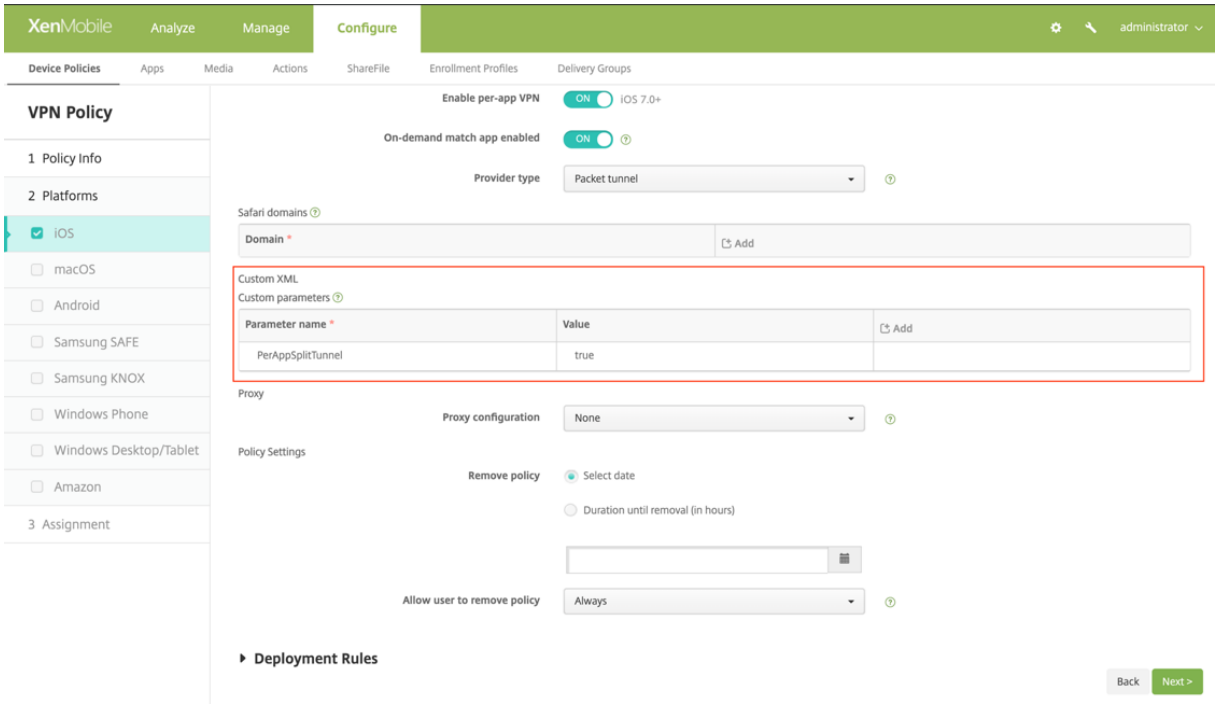
Los clientes de MDM pueden configurar el túnel dividido en VPN por aplicación para Citrix Secure Access. El siguiente par clave/valor debe agregarse a la sección de configuración del proveedor del perfil VPN creado en el servidor MDM.


```
- Key = "PerAppSplitTunnel"
- Value = "true or 1 or yes"
```

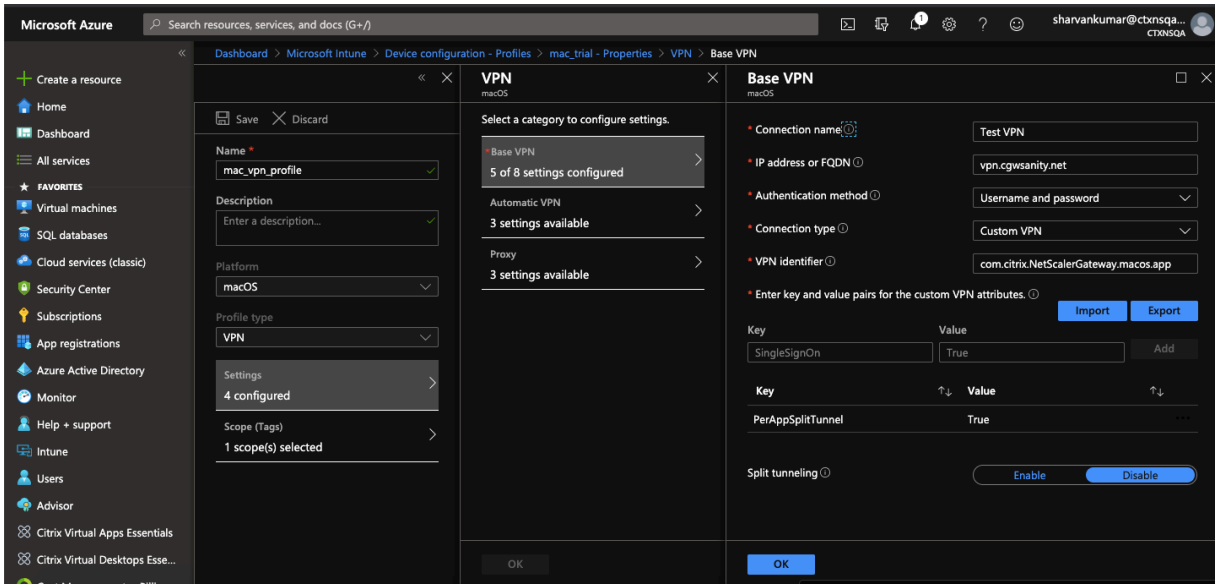
La clave distingue entre mayúsculas y minúsculas y debe coincidir exactamente, mientras que el valor no distingue mayúsculas

> **Nota:**
>
> La interfaz de usuario para configurar la configuración del proveedor no es estándar en todos los proveedores de MDM. Póngase en contacto con el proveedor de MDM para buscar la sección de configuración del proveedor en la consola de usuario de MDM.

A continuación se muestra una captura de pantalla de ejemplo de la configuración (configuración específica del proveedor) en Citrix Endpoint Management.



A continuación se muestra una captura de pantalla de ejemplo de la configuración (configuración específica del proveedor) en Microsoft Intune.



Inhabilitar los perfiles VPN creados por el usuario

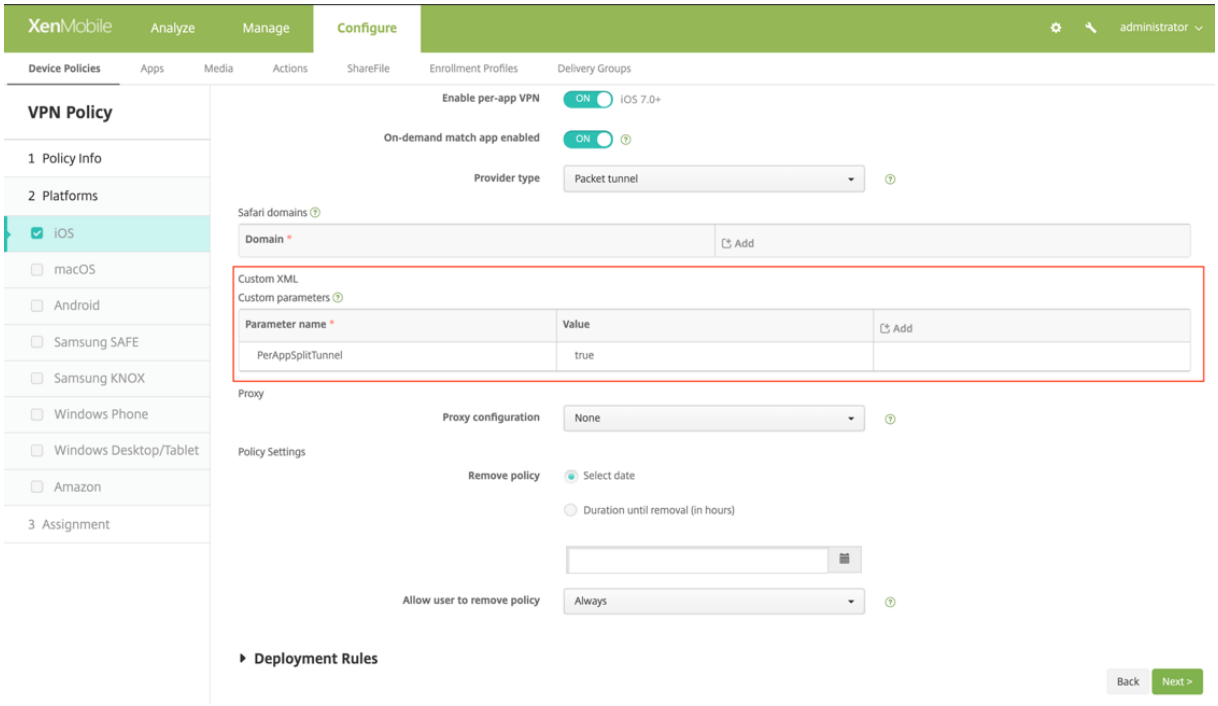
Los clientes de MDM pueden evitar que los usuarios creen perfiles de VPN manualmente desde Citrix Secure Access. Para ello, se debe agregar el siguiente par clave/valor a la sección de configuración del proveedor del perfil VPN creado en el servidor MDM.

```
- Key = "disableUserProfiles"
- Value = "true or 1 or yes"
```

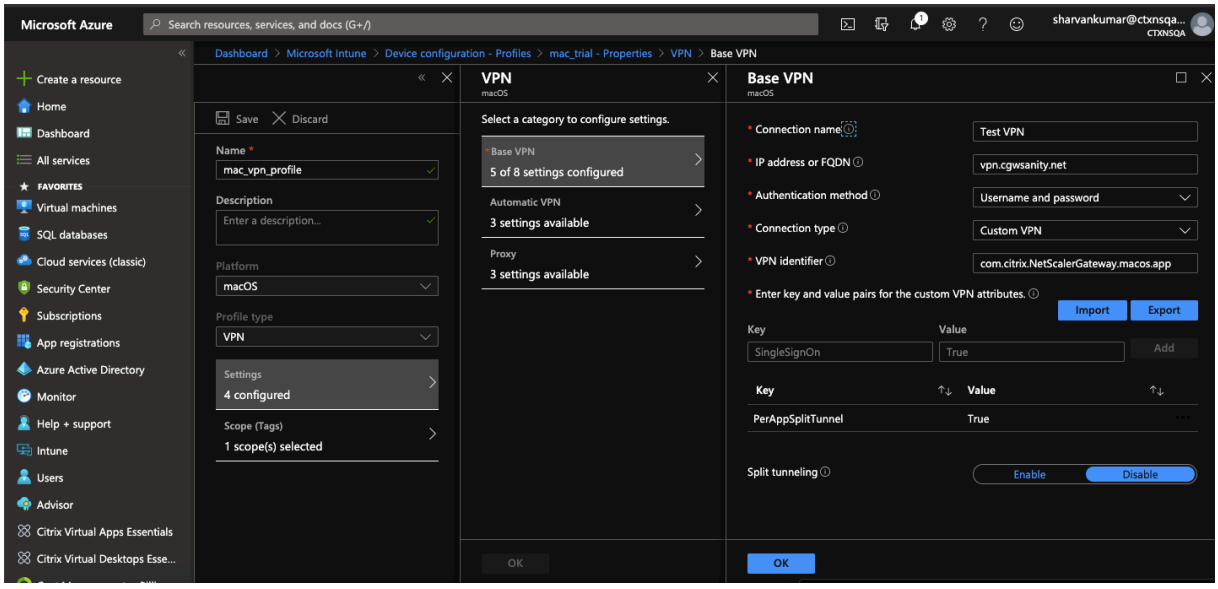
La clave distingue entre mayúsculas y minúsculas y debe coincidir exactamente, mientras que el valor no distingue mayúsculas

> **Nota:**
>
> La interfaz de usuario para configurar la configuración del proveedor no es estándar en todos los proveedores de MDM. Póngase en contacto con el proveedor de MDM para buscar la sección de configuración del proveedor en la consola de usuario de MDM.

A continuación se muestra una captura de pantalla de ejemplo de la configuración (configuración específica del proveedor) en Citrix Endpoint Management.



A continuación se muestra una captura de pantalla de ejemplo de la configuración (configuración específica del proveedor) en Microsoft Intune.



Manejo DNS

La configuración de DNS recomendada para Citrix Secure Access es la siguiente:

- **Dividir DNS > REMOTE** si el túnel dividido está en **OFF.**

- **DNS dividido > BOTH** si el túnel dividido está **activado**. En este caso, los administradores tienen que agregar sufijos DNS para los dominios de la intranet. Las consultas DNS de los FQDN pertenecientes a sufijos DNS se tunelizan al dispositivo NetScaler y las consultas restantes se dirigen al enrutador local.

> **Nota:**
>
> - Se recomienda que el indicador de **corrección de truncamiento de DNS** esté siempre **activado**. Para obtener más información detallada, consulte https://support.citrix.com/article/CTX200243.
> - Cuando el túnel dividido se establece **en ON** y DNS dividido en **REMOTE**, puede haber problemas para resolver las consultas DNS después de conectar la VPN. Esto se relaciona con que el marco de extensión de red no intercepta todas las consultas DNS.

Escaneos EPA compatibles

Para obtener una lista completa de las exploraciones admitidas, consulte Bibliotecas de la EPA

1. En la sección **Matriz de exploración admitida por OPSWAT v4**, haga clic en **Lista de aplicaciones compatibles** en la columna **Específico de MAC OS**.
2. En el archivo de Excel, haga clic en la ficha **Escaneos clásicos de la EPA** para ver los detalles.

Problemas conocidos

Los siguientes son los problemas conocidos actualmente.

- El inicio de sesión de la EPA falla si el usuario se coloca en el grupo de cuarentena.
- No se muestra el mensaje de advertencia de tiempo de espera forzado.
- Citrix Secure Access permite iniciar sesión si el túnel dividido está activado y no hay ninguna aplicación de intranet configurada.

Limitaciones

Las siguientes son las limitaciones actuales.

- Los siguientes escaneos de la EPA pueden fallar debido a la restricción del acceso a Secure Access debido al aislamiento.
  - "Tipo"y "ruta"de cifrado de disco duro
  - Explorador web "predeterminado"y "en ejecución"
  - Administración de parches "parches faltantes"

  - Desactivar la operación del proceso durante el EPA

- No se admite la tunelización dividida basada en puertos/protocolos.
- Asegúrese de que no tiene dos certificados con el mismo nombre y fecha de caducidad en el llavero, ya que esto hace que el cliente muestre solo uno de los certificados en lugar de ambos.

Solución de problemas

Si se muestra a los usuarios finales el botón **Descargar el complemento EPA en** la ventana de autenticación de Citrix Secure Access, significa que la política de seguridad del contenido del dispositivo NetScaler bloquea la invocación de la URL`com.citrix.agmacepa://`. Los administradores deben modificar la directiva de seguridad de contenido para que `com.citrix.agmacepa://` esté permitida.

Soporte de nFactor para el cliente Citrix Secure Access en macOS/iOS

March 27, 2024

> **Importante:**
>
> Citrix SSO para iOS ahora se llama Citrix Secure Access. Estamos actualizando nuestra documentación y las capturas de pantalla de la interfaz de usuario para reflejar este cambio de nombre.

La autenticación multifactor (nFactor) mejora la seguridad de una aplicación al exigir a los usuarios que proporcionen varias pruebas de identidad para obtener acceso. Los administradores pueden configurar distintos factores de autenticación que incluyen certificado de cliente, LDAP, RADIUS, OAuth, SAML, etc. Estos factores de autenticación se pueden configurar en cualquier orden según las necesidades de la organización.

El cliente Citrix Secure Access en macOS/iOS admite los siguientes protocolos de autenticación:

- **nFactor**: El protocolo nFactor se utiliza cuando un servidor virtual de autenticación está enlazado al servidor virtual VPN en la puerta de enlace. Como el orden de los factores de autenticación es dinámico, el cliente utiliza una instancia del explorador que se representa en el contexto de la aplicación para presentar la GUI de autenticación.
- **Clásico**: El protocolo clásico es el protocolo alternativo predeterminado que se utiliza si las directivas de autenticación clásicas están configuradas en el servidor virtual VPN de la puerta de enlace. El protocolo clásico es el protocolo de reserva si nFactor falla para métodos de autenticación específicos como NAC.

- **Plataforma de identidad Citrix** : el protocolo de plataforma de identidades de Citrix se utiliza al autenticarse en el servicio CloudGateway o Citrix Gateway y requiere la inscripción de MDM en Citrix Cloud.

En la tabla siguiente se resumen los distintos métodos de autenticación admitidos por cada protocolo.

Método de autenticación	nFactor	Clásico	IdP de Citrix
Certificado de cliente	Compatible	Compatible	No compatible
LDAP	Compatible	Compatible	No compatible
Locales	Compatible	Compatible	No compatible
RADIUS	Compatible	No compatible	No compatible
SAML	Compatible	No compatible	No compatible
OAuth	Compatible	No compatible	No compatible
TACACS	Compatible	No compatible	No compatible
WebAuth	Compatible	No compatible	No compatible
Negociar	Compatible	No compatible	No compatible
EPA	Compatible	Compatible	No compatible
NAC	No compatible	Compatible	No compatible
StoreFront	No compatible	No compatible	No compatible
ADAL	No compatible	No compatible	No compatible
DS-AUTH	No compatible	No compatible	Compatible

Configuración nFactor

Para obtener más información sobre la configuración de nFactor, consulte Configuración de la autenticación nFactor.

> **Importante:**
>
> Para usar el protocolo nFactor con el cliente Citrix Secure Access en macOS/iOS, la versión local recomendada de NetScaler Gateway es la 12.1.50.xx y posterior.

Limitaciones

- Las directivas de autenticación específicas para dispositivos móviles, como NAC (control de acceso a la red), requieren que el cliente envíe un identificador de dispositivo firmado como parte de la autenticación con NetScaler Gateway. El identificador de dispositivo firmado es una clave secreta giratoria que identifica de forma exclusiva un dispositivo móvil inscrito en un entorno MDM. Esta clave está incrustada en un perfil VPN administrado por un servidor MDM. Es posible que no sea posible introducir esta clave en el contexto de WebView. Si NAC está habilitado en un perfil de VPN de MDM, el cliente Citrix Secure Access en macOS/iOS recurre automáticamente al protocolo de autenticación clásico.
- No se puede configurar la comprobación de NAC con Intune para macOS, ya que Intune no proporciona una opción para habilitar NAC para macOS a diferencia de iOS.

Solución de problemas comunes de Citrix Secure Access para macOS/iOS

March 27, 2024

> **Importante:**
>
> Citrix SSO para iOS ahora se llama Citrix Secure Access. Estamos actualizando nuestra documentación y las capturas de pantalla de la interfaz de usuario para reflejar este cambio de nombre.

Problemas de resolución DNS

- Si el dispositivo se pone en reposo o permanece inactivo durante mucho tiempo, la VPN puede tardar entre 30 y 60 segundos en reanudarse. Durante este tiempo, es posible que los usuarios vean que algunas solicitudes DNS fallan. Las solicitudes DNS se resuelven automáticamente tras un breve periodo de tiempo.
  Si las consultas DNS no se resuelven, es posible que una directiva de autorización avanzada bloquee el tráfico DNS. Consulte https://support.citrix.com/article/CTX232237 para solucionar este problema.
- Compruebe siempre la resolución de DNS desde los exploradores. Es posible que las consultas DNS que utilizan el comando `nslookup` del terminal no sean precisas. Si tiene que usar el comando `nslookup`, debe incluir la dirección IP del cliente en el comando. Por ejemplo, `nslookup website_name 172.16.255.1.`

Problemas de la EPA

- Gatekeeper se considera un antivirus. Si hay un análisis que busca "cualquier antivirus"(MAC-ANTIVIR_0_0), el análisis siempre pasa aunque el usuario no haya instalado ningún antivirus de otros proveedores.

Nota:

- Habilite el registro de seguridad del cliente para obtener los registros de depuración de la EPA. Puede habilitar el registro de seguridad del cliente estableciendo el parámetro `clientsecurityLog` VPN en ON.
- El software de administración de parches integrado de Apple es "Actualización de software" . Corresponde a la aplicación "App Store"del dispositivo. La versión de la "Actualización de software"debe ser similar `"MAC-PATCH_100011_100076_VERSION_==_3.0[COMMENT : Software Update]"`
- Mantenga siempre actualizadas las bibliotecas EPA de NetScaler. Las bibliotecas más recientes se encuentran en https://www.citrix.com/downloads/citrix-gateway/epa-libraries/epa-libraries-for-netscaler-gateway.html

Problemas de nFactor

- Citrix Secure Access abre la ventana de autenticación de **Citrix SSO** para la autenticación nFactor. Es similar a un explorador. Si hay errores en esta página, se puede verificar de forma cruzada probando la autenticación en un explorador web.
- Si el inicio de sesión de transferencia falla cuando nFactor está habilitado, cambie el tema del portal a "rfWebUI".
- Si aparece el error "No se puede establecer una conexión segura con NetScaler Gateway porque la cadena de certificados no contiene ninguno de los certificados necesarios. Póngase en contacto con su administrador"o "Puerta de enlace no accesible"; a continuación, el certificado del servidor de puerta de enlace ha caducado o el certificado del servidor está vinculado con SNI habilitado. Citrix Secure Access aún no admite el SNI. Enlazar el certificado del servidor sin tener habilitado el SNI. El error también puede deberse a que la fijación de certificados configurada en el perfil VPN de MDM y el certificado presentado por NetScaler Gateway no coincide con el certificado anclado.
- Al intentar conectarse a la puerta de enlace, si la **ventana de autenticación de Citrix SSO** se abre pero está en blanco, compruebe si la curva ECC (ALL) está enlazada al grupo de cifrado predeterminado. La curva ECC (ALL) debe estar enlazada al grupo de cifrado predeterminado.

Comprobación del control de acceso a la red (NAC)

La directiva de autenticación de NAC solo se admite en la autenticación clásica. No se admite como parte de la autenticación nFactor.

Preguntas frecuentes

March 27, 2024

> **Importante:**
>
> Citrix SSO para iOS ahora se llama Citrix Secure Access. Estamos actualizando nuestra documentación y las capturas de pantalla de la interfaz de usuario para reflejar este cambio de nombre.

En esta sección se muestran las preguntas frecuentes sobre Citrix Secure Access para macOS/iOS.

¿En qué se diferencia el cliente Citrix Secure Access para macOS/iOS de la aplicación VPN?
Los clientes Citrix Secure Access para macOS y Citrix Secure Access para iOS (antes conocidos como Citrix SSO para iOS) son la próxima generación de clientes VPN SSL para NetScaler. La aplicación utiliza el marco de extensión de red de Apple para crear y administrar conexiones VPN en dispositivos iOS y macOS. Citrix VPN es el cliente VPN heredado que utiliza las API de VPN privadas de Apple, que ahora están en desuso. La compatibilidad con Citrix VPN ya no está disponible en la tienda de aplicaciones.

¿Qué es NE?
El marco de extensión de red (NE) de Apple es una biblioteca moderna que contiene API que se pueden utilizar para personalizar y ampliar las funciones principales de red de iOS y macOS. La extensión de red compatible con SSL VPN está disponible en dispositivos con iOS 9+ y macOS 10.11+.

¿Para qué versiones de NetScaler es compatible el cliente Citrix Secure Access para macOS/iOS?
Las funciones de VPN del cliente Citrix Secure Access para macOS/iOS son compatibles con las versiones 10.5 y posteriores de NetScaler. El TOTP está disponible en NetScaler versión 12.0 y superiores. La notificación push en NetScaler aún no se ha anunciado públicamente. La aplicación requiere las versiones iOS 9+ y macOS 10.11+.

¿Cómo funciona la autenticación basada en CERT para clientes que no son MDM?
Los clientes que anteriormente distribuían certificados por correo electrónico o explorador para realizar la autenticación de certificados de cliente en VPN deben tener en cuenta este cambio cuando utilicen el cliente Citrix Secure Access para macOS/iOS. Esto es especialmente cierto para los clientes que no son de MDM y que no utilizan un servidor de MDM para distribuir certificados de usuario.

¿Qué es el control de acceso a la red (NAC)? ¿Cómo configuro NAC con Citrix Secure Access para iOS y NetScaler Gateway?

Los clientes de MDM de Microsoft Intune y Citrix Endpoint Management (antes XenMobile) pueden aprovechar la función Network Access Control (NAC) de Citrix Secure Access para iOS. Con NAC, los administradores pueden proteger la red interna de su empresa añadiendo una capa adicional de autenticación para los dispositivos móviles gestionados por un servidor MDM. Los administradores pueden hacer cumplir una comprobación de la conformidad del dispositivo en el momento de la autenticación en Citrix Secure Access para iOS.

Para usar NAC con Citrix Secure Access para iOS, debe habilitarlo tanto en NetScaler Gateway como en el servidor MDM.

- Para habilitar NAC en NetScaler, consulte Configurar la comprobación de dispositivos de control de acceso a redes para el servidor virtual NetScaler Gateway para el inicio de sesión de un solo factor
- Si un proveedor de MDM es Intune, consulte Integración del control de acceso a la red (NAC) con Intune.
- Si un proveedor de MDM es Citrix Endpoint Management (anteriormente XenMobile), consulte Control de acceso a redes.

  > **Nota:**
  >
  > La versión mínima admitida del cliente Citrix Secure Access para macOS/iOS es la 1.1.6 y superior.

Citrix Secure Access para Android

March 27, 2024

Citrix Secure Access (anteriormente Citrix SSO) para Android ofrece la mejor solución de protección de datos y acceso a aplicaciones que ofrece NetScaler Gateway. Ahora puede acceder de forma segura a las aplicaciones críticas para el negocio, los escritorios virtuales y los datos corporativos en cualquier momento y desde cualquier lugar.

> **Importante:**
>
> - Citrix SSO para Android ahora se llama Citrix Secure Access. Estamos actualizando nuestra documentación y las capturas de pantalla de la interfaz de usuario para reflejar este cambio de nombre.
> - El cliente Citrix Secure Access para Android funciona dentro del subsistema Android inte-

> grado en ChromeOS. Funciona con ChromeOS si se instala como una aplicación de Android desde Play Store y puede canalizar cualquier aplicación dentro del subsistema de Android.

Notas de la versión

March 27, 2024

> **Importante:**
>
> - Citrix SSO para Android ahora pasa a llamarse Citrix Secure Access. Estamos actualizando nuestra documentación y las capturas de pantalla de la interfaz de usuario para reflejar este cambio de nombre. Es posible que observe las referencias de SSO de Citrix utilizadas en la documentación durante este período de transición.
> - Las funciones de túneles divididos basada en FQDN y autenticación nFactor se encuentran actualmente en Tech Preview.
> - Citrix Secure Access no es compatible con Android 6.x y versiones anteriores a partir de junio de 2020.

Las notas de la versión de Citrix Secure Access describen las nuevas funciones, las mejoras de las funciones existentes, los problemas resueltos y los problemas conocidos disponibles en una versión de servicio. Las notas de la versión incluyen una o varias de las secciones siguientes:

Novedades: las nuevas funciones y mejoras disponibles en la versión actual.

Problemasresueltos : los problemas que se han corregido en la versión actual.

Problemasconocidos : los problemas que existen en la versión actual y sus soluciones alternativas, cuando proceda.

V23.12.2 (15 de diciembre de 2023)

> **Nota:**
>
> La versión 23.12.2 de Citrix Secure Access para Android incluye la corrección para CSACLIENTS-8799 y reemplaza a la versión 23.12.1.

[CSACLIENTS-8799]

Novedades

- **Citrix SSO para Android pasa a llamarse Citrix Secure Access**

  Citrix SSO para Android ahora se llama Citrix Secure Access. Estamos actualizando nuestra documentación y las capturas de pantalla de la interfaz de usuario para reflejar este cambio de nombre.

  [CSACLIENTS-6337]

- **Recibir o bloquear notificaciones en dispositivos Android 13+**

  Al instalar o reinstalar el cliente Citrix Secure Access en un dispositivo Android 13, ahora se solicita a los usuarios finales que proporcionen permisos para recibir notificaciones del cliente Citrix Secure Access. Si los usuarios finales deniegan el permiso, no recibirán ningún estado de VPN ni notificaciones push del cliente Citrix Secure Access en sus dispositivos Android. Se recomienda a los administradores de MDM que concedan el permiso de notificación a Citrix Secure Access (ID del paquete: `com.citrix.CitrixVPN`) en su solución.

  Los usuarios finales pueden ir a **Configuración > Notificaciones** en el dispositivo Android para cambiar el permiso de
  notificación del cliente Citrix Secure Access. Para obtener más información, consulte Cómo utilizar Citrix Secure Access desde un dispositivo Android.

  [CSACLIENTS-8252]

- **Soporte para transferir el inicio de sesión en modo Always On VPN**

  Citrix Secure Access para Android ahora admite la función de transferencia de inicio de sesión en el modo VPN Always On. Para obtener más información sobre cómo configurar el inicio de sesión por transferencia, consulte Configurar la página por transferencia de inicio de sesión.

  [CSACLIENTS-8305]

Problemas resueltos

Citrix Secure Access se bloquea cuando los usuarios copian el token OTP basado en el tiempo (TOTP) en el dispositivo Android 13+.

[CSACLIENTS-8799]

V23.10.2 (19 de diciembre de 2023)

Novedades

> **Notas:**
>
> - La versión 23.10.2 de Citrix SSO para Android incluye la corrección para CSACLIENTS-8314 y reemplaza a la versión 23.10.1.
> - Citrix SSO para Android 23.10.1 funciona con Android 14.

- **Vuelva a autenticarse con NetScaler Gateway después de un error en la conexión VPN - Vista previa**

  Citrix SSO para Android ahora le pide que se vuelva a autenticar con NetScaler Gateway cuando se pierde una conexión VPN. En la interfaz de usuario de Citrix SSO y en el panel de notificaciones de su dispositivo Android se le notificará que se ha perdido la conexión a NetScaler Gateway y que debe volver a autenticarse para reanudar la conexión. Esta función se encuentra en Tech Preview.

  Para obtener más información, consulte Volver a conectarse a NetScaler Gateway despuésde un error en la conexión VPN.

Problemas resueltos

El SSO de Citrix se bloquea de forma intermitente al reiniciar el servicio VPN en determinados escenarios de Always On VPN.

[CSACLIENTS-8314]

V23.8.1 (31 de agosto de 2023)

Novedades

- **Reinicio automático de Always On VPN**

  La aplicación Citrix SSO reinicia automáticamente la VPN Always On cuando se instala una aplicación que forma parte de la lista de permitidos o bloqueados en un perfil de trabajo o de dispositivo. El tráfico de esta aplicación se canaliza automáticamente a través de una conexión VPN sin reiniciar el perfil de trabajo ni el dispositivo. Para habilitar el reinicio automático de Always On VPN, los usuarios finales deben conceder el consentimiento de Query all packages a la aplicación Citrix SSO. Para obtener más información, consulte Reinicio automático de Always On VPN.

  [CSACLIENTS-6158]

- **Habilitar el registro de depuración en un perfil VPN administrado**

Los administradores de MDM ahora pueden habilitar el registro de depuración como un parámetro personalizado en el perfil de VPN administrado de la consola de Endpoint Management. Para habilitar el registro de depuración, el valor de `EnableDebugLogging`debe estar establecido en True. Si alguna de las configuraciones de VPN administradas tiene habilitado el registro de depuración, la funcionalidad de registro de depuración surtirá efecto cuando se analice la configuración. Para obtener más información, consulte Parámetros personalizados para la configuración de Intune.

[CSACLIENTS-3746]

Problemas resueltos

- En ocasiones, la aplicación Citrix SSO puede no canalizar el tráfico a algunos recursos. Este problema se produce cuando la tunelización dividida está desactivada y algunos dominios o direcciones IP inaccesibles están bloqueados.

  [NSHELP-35555]

V22.11.1 (30 de noviembre de 2022)

Novedades

- **Citrix Secure Access se actualiza a Android 12.1 de destino (nivel de API 32)**

  Citrix Secure Access ahora está actualizado a Android 12.1 de destino (nivel de API 32). En el caso de una VPN por aplicación, es posible que el servicio VPN no se reinicie automáticamente si uno de los paquetes de la lista de paquetes de VPN por aplicación se instala después de configurar el túnel VPN. Esto se debe a las restricciones de visibilidad de la aplicación introducidas en Android 11. Para obtener información detallada, consulte https://developer.android.com/training/package-visibility.

  [CGOP-21409]

V22.10.1 (21 de octubre de 2022)

Novedades

- La visualización del número de versión de la aplicación se actualiza al formato YY.MM.Point-Release, donde YY es el año de 2 dígitos, MM es el mes de 2 dígitos y point-release es 1+, según el número de publicación dentro de un mes.
- La recopilación de datos de Google Analytics/Crashlytics de la región de la UE está inhabilitada para los clientes de Android.

Problemas resueltos

- Los mensajes de error que aparecen para una entrada no válida en las pantallas Agregar conexión y Modificar conexión no están traducidos.

  [CGOP-22060]

V2.5.3 (05 de mayo de 2022)

Novedades

- Citrix SSO actualizado al SDK de destino de Android 11 (API 30)

  La aplicación Citrix SSO ahora se ha actualizado al SDK de destino de Android 11 (API 30). Este cambio requiere que NetScaler Gateway utilice las API NAC v2 de Microsoft Intune para comprobar el cumplimiento de normativas de los dispositivos. Para obtener más información, consulte el artículo de la base de conocimientos.https://support.citrix.com/article/CTX331615

  [CGOP-19774]

Problemas resueltos

- A veces, es posible que Citrix SSO no utilice un servidor DNS alternativo para la resolución de nombres de host después de un cambio de red.

  [NSHELP-29378]

V2.5.2 (21 de octubre de 2021)

Problemas resueltos

- A veces, Citrix SSO se bloquea al controlar un error de incumplimiento en la comprobación de NAC.

  [CGOP-19198]

V2.5.1 (12 de agosto de 2021)

Problemas resueltos

- La aplicación Citrix SSO no resuelve el host cuando la cadena CNAME tiene más de 6 saltos.

  [CGOP-18475]

- Citrix SSO muestra un mensaje de autenticación cuando NetScaler Gateway solo requiere autenticación de comprobación de NAC.

  [CGOP-18348]

- Citrix SSO podría bloquearse al procesar paquetes ICMP inusualmente grandes.

  [CGOP-18286]

- El Citrix SSO puede bloquearse al agregar un perfil de VPN en algunos dispositivos Android 8.0.

  [CGOP-17607]

- Es posible que Citrix SSO se bloquee al reiniciar la VPN configurada para Always On.

  [CGOP-17580]

- Citrix SSO podría bloquearse al gestionar un error SSL en el flujo de autenticación de nFactor.

  [CGOP-17577]

V2.5.0 (8 de junio de 2021)

Novedades

- **Compatibilidad con túneles divididos basados en FQDN**

  Citrix SSO para Android ahora admite la tunelización dividida basada en FQDN.

  [CGOP-12079]

Problemas resueltos

- La versión Tech Preview de Citrix SSO 2.5.0 falla (110) al conectarse a las versiones 12.1 y anteriores de NetScaler Gateway.

  [CGOP-17735]

- La configuración "DisableUserProfiles"no se aplica después de reiniciar la aplicación SSO.

  [CGOP-17454]

V2.4.16 (31-Mar-2021)

Problemas resueltos

- La autenticación nFactor se anula si la navegación segura no está habilitada en algunos dispositivos.

  [CGOP-17514]

V2.4.15 (17-Mar-2021)

Problemas resueltos

- A veces, Citrix SSO no vuelve a conectar Always On VPN cuando se agota el tiempo de espera de la sesión en el dispositivo NetScaler Gateway.

  [CGOP-16800]

V2.4.14 (23-Feb-2021)

Problemas resueltos

- El inicio de sesión único de Citrix SSO requiere la interacción del usuario cuando se utiliza una VPN siempre activa con autenticación de solo certificado junto con la autenticación nFactor.

  [CGOP-16805]
- A veces, Citrix SSO puede bloquearse durante el reinicio o la transición del servicio VPN.

  [CGOP-16766]

V2.4.13 (04-Feb-2021)

Problemas resueltos

- En algunos casos, la solicitud de inicio de sesión de Citrix SSO se agotará antes de que NetScaler Gateway responda.

  [CGOP-16759]

V2.4.12 (15 de enero de 2021)

En esta versión se resolvieron varios problemas para mejorar la estabilidad y el rendimiento generales.

V2.4.11 (08-Jan-2021)

- La autenticación clásica falla porque Citrix SSO envía un encabezado HTTP (X-Citrix-Gateway) a NetScaler Gateway que se utiliza únicamente en la autenticación nFactor.

  [CGOP-16449]

V2.4.10 (09-Dec-2020)

Problemas resueltos

- A veces, la autenticación clásica puede fallar en los dispositivos Android.

  [CGOP-16219]

- El inicio de sesión Citrix SSO podría bloquearse al realizar la autenticación clásica.

  [CGOP-16012]

- La orientación de la aplicación Citrix SSO no cambia al girar el dispositivo.

  [CGOP-639]

V2.4.9 (20-Nov-2020)

Problemas resueltos

- La aplicación Citrix SSO se bloquea cuando un usuario toca el valor del token TOTP en el dispositivo.

  [CGOP-15886]

V2.4.8 (04-Nov-2020)

Problemas resueltos

- Citrix SSO podría bloquearse al desconectar la VPN después de agotar el tiempo de espera de la sesión en la puerta de enlace.

  [CGOP-15592]

V2.4.7 (12-Oct-2020)

En esta versión se resolvieron varios problemas para mejorar la estabilidad y el rendimiento generales.

V2.4.6 (28-Sep-2020)

En esta versión se resolvieron varios problemas para mejorar la estabilidad y el rendimiento generales.

V2.4.5 (16-Sep-2020)

Novedades

- Se presenta el nuevo logotipo de NetScaler.

  [CGOP-15327]

V2.4.4 (10-Sep-2020)

Problemas resueltos

- A veces, el Citrix SSO se bloquea al volver a conectar la sesión VPN.

  [CGOP-15215]

V2.4.3

Problemas conocidos

- Citrix SSO no establece una sesión VPN en NetScaler Gateway cuando el dispositivo Android tiene limitaciones de recursos.

  [NSHELP-24647]

V2.4.2

Problemas resueltos

- La aplicación Citrix SSO se bloquea al cargar datos de tokens corruptos guardados previamente. Con esta corrección, el valor del token se muestra como ‘‘Datos del token corruptos’’para los tokens corruptos en la lista de tokens. Elimina los tokens corruptos y agrégalos de nuevo.

  [CGOP-14546]

V2.4.1

Problemas resueltos

- La aplicación Citrix SSO no es compatible con Android 6.x y versiones posteriores a junio de 2020.

  [CGOP-13853]

V2.3.19

En esta versión se resolvieron varios problemas para mejorar la estabilidad y el rendimiento generales.

V2.3.18

Novedades

- La configuración de proxy ahora es compatible con la aplicación Citrix SSO para Android para dispositivos Android 10.

  [CGOP-12007]

V2.3.17

En esta versión se resolvieron varios problemas para mejorar la estabilidad y el rendimiento generales.

V2.3.16

En esta versión se resolvieron varios problemas para mejorar la estabilidad y el rendimiento generales.

V2.3.15

Novedades

- La aplicación Citrix SSO ahora admite la fijación de certificados de NetScaler Gateway para perfiles VPN administrados.

  [CGOP-12538]

- La aplicación Citrix SSO para Android 10 ahora detecta Always On VPN desde la configuración del sistema.

  [CGOP-12656]

Problemas resueltos

- La aplicación Citrix SSO se bloquea al desconectarse de la VPN si solo hay perfiles VPN de MDM definidos.

  [CGOP-13825]

V2.3.14

Novedades

- La aplicación Citrix SSO ahora puede realizar la autenticación de usuarios en nombre de la aplicación Citrix Workspace para el inicio de sesión único de la aplicación nativa.

  [CGOP-12083]

- El servicio VPN se reinicia si uno de los paquetes de la lista de paquetes VPN por aplicación se instala después de configurar el túnel VPN.

  [CGOP-11262]

Problemas resueltos

- Citrix SSO ahora gestiona correctamente el mensaje de establecimiento de la sesión VPN final.

  [CGOP-12488]

- La dirección IP de NetScaler Gateway se resuelve ahora solo una vez. Anteriormente, la dirección IP de NetScaler Gateway se resolvía varias veces, lo que ocasionaba errores de conexión en ocasiones.

  [CGOP-12101]

Problemas conocidos

- El estado de la VPN siempre activa no siempre se actualiza correctamente en la interfaz de usuario de la aplicación.

  [NSHELP-21709]

V2.3.13

Problemas resueltos

- La dirección IP de NetScaler Gateway se resuelve ahora solo una vez.

Anteriormente, la dirección IP de NetScaler Gateway se resolvía varias veces, lo que ocasionaba errores de conexión en ocasiones.

[CGOP-12101]

Problemas conocidos

- El estado de la VPN siempre activa no siempre se actualiza correctamente en la interfaz de usuario de la aplicación.

  [NSHELP-21709]

V2.3.12

Problemas resueltos

- Es posible que Citrix SSO se bloquee al guardar un perfil de VPN.

  [CGOP-12137]

V2.3.11

Problemas resueltos

- Es posible que Citrix SSO se bloquee al guardar un perfil de VPN.

  [CGOP-12137]

- La configuración disableUserProfile no se refleja correctamente en la interfaz de usuario cuando un nuevo perfil VPN o una actualización de un perfil existente dan como resultado el cambio del valor disableUserProfile.

  [CGOP-11899]

- Citrix SSO para Android no procesa los perfiles VPN en modo Propietario del dispositivo (DO).

  [CGOP-11981]

- La conexión VPN no se establece cuando solo hay servidores DNS locales IPv6.

  [CGOP-12053]

V2.3.10

Problemas resueltos

- La conexión VPN se pierde después de un tiempo de inactividad en el dispositivo.

  [CGOP-11381]

V2.3.8

Novedades

- **Configurar la aplicación Citrix SSO en un entorno Intune Android Enterprise**

  Ahora puede configurar la aplicación Citrix SSO en un entorno Intune Android Enterprise. Para obtener más información, consulte Configurar la aplicación Citrix SSO en un entorno Intune Android Enterprise.

  [CGOP-635]

- **Compatibilidad con el aprovisionamiento de perfiles VPN a través de Android Enterprise**

  Ahora se admite el aprovisionamiento de perfiles VPN a través de Android Enterprise.

  [CGOP-631]

Problemas resueltos

- Si guarda un token que ya está guardado y, a continuación, intenta abrirlo, aparecerán caracteres confusos en el nombre del token.

  [CGOP-11696]

- La aplicación Citrix SSO no establece una sesión VPN si no hay ningún dominio de búsqueda DNS configurado en NetScaler Gateway.

  [CGOP-11259]

V2.3.6

Novedades

- **Compatibilidad con Always On para Citrix SSO**

La función Always On de Citrix SSO garantiza que los usuarios estén siempre conectados a la red empresarial. Esta conectividad VPN persistente se consigue mediante el establecimiento automático de un túnel VPN.

[CGOP-10015]

- **Se muestra una notificación para volver a iniciar sesión si la caducidad del token de Athena provoca un cierre de sesión**

  Se muestra una notificación en la que se solicita a los usuarios que vuelvan a iniciar sesión en Citrix Workspace si se cumplen las siguientes condiciones.

  - La función Always On está habilitada en el perfil de VPN aprovisionada de Citrix Workspace
  - La autenticación Athena se utiliza para el inicio de sesión único
  - El usuario ha cerrado la sesión de la aplicación Citrix Workspace debido a la caducidad del token de Athena

  [CGOP-10016]

- **El registro para el servicio de notificaciones push se realiza mediante NetScaler Gateway**

  Ahora puede registrarse en el servicio de notificaciones push mediante el dispositivo NetScaler Gateway. Anteriormente, el registro se realizaba en el dispositivo cliente.

  [CGOP-10542]

Problemas resueltos

A veces, el Citrix SSO se bloquea cuando se analiza un nuevo token. Por ejemplo, Citrix SSO se bloquea cuando se elimina un token existente y se analiza otro con el mismo nombre de token.

[CGOP-10818]

V2.3.1

Novedades

- **Las configuraciones administradas se actualizan para incluir más ajustes de usuario**

  Las configuraciones administradas se actualizan para incluir los ajustes "BlockUntrusted-Servers", "DefaultProfileName"y "DisableUserProfiles"para entornos Android Enterprise.

  [CGOP-10033]

- **Compatibilidad mejorada con notificaciones push**

Al configurar NetScaler Gateway para notificaciones push con el tipo "OTP", no se solicita el PIN o la huella digital después de que el usuario selecciona "Permitir"en respuesta a la notificación push que solicita el consentimiento del usuario para permitir que la autenticación continúe.

[CGOP-9843]

- **Soporte de Firebase Analytics**

  Se agrega compatibilidad con Firebase Analytics básica para proporcionar información sobre el uso de la aplicación Citrix SSO. La mejora es aplicable a geolocalizaciones gruesas, uso de pantalla, diferentes versiones de Android en uso, etc.

  [CGOP-7523]

- **Compatibilidad con la configuración de perfiles VPN basada en configuraciones administradas de Android**

  La aplicación Citrix SSO se puede configurar en el entorno Android Enterprise mediante un proveedor de EMM/UEM como Citrix Endpoint Management. El asistente de configuraciones administradas de Android Enterprise de CEM se puede usar para implementar configuraciones de VPN administradas en la aplicación Citrix SSO. Para obtener información sobre cómo configurar la aplicación Citrix SSO mediante configuraciones administradas, consulte la directiva de dispositivos VPN.

V2.2.9

Novedades

- **Compatibilidad con notificaciones push**

  NetScaler Gateway envía una notificación push en su dispositivo móvil registrado para ofrecer una experiencia de autenticación de dos factores simplificada.

  [CGOP-9592]

Problemas resueltos

- Se permiten caracteres que no sean URL en el campo Servidor de la pantalla Agregar conexión.

  [CGOP-588]

Configurar Citrix Secure Access en un entorno de MDM

March 27, 2024

> **Importante:**
>
> Citrix SSO para Android ahora se llama Citrix Secure Access. Estamos actualizando nuestra documentación y las capturas de pantalla de la interfaz de usuario para reflejar este cambio de nombre.

Para configurar Citrix Secure Access en un entorno MDM, consulte Configurar el protocolo Citrix Secure Access para Android.

> **Notas:**
>
> - En un entorno que no es MDM, los usuarios crean perfiles VPN manualmente.
> - También puede crear una configuración administrada de Android Enterprise para Citrix Secure Access. Para obtener más información, consulte Configurar perfiles VPN para Android Enterprise.
> - Para los usuarios de Android 13+ que utilizan Citrix Secure Access 23.12.1 y versiones posteriores, se recomienda a los administradores de MDM que concedan el permiso de notificación a Citrix Secure Access (ID del paquete: `com.citrix.CitrixVPN`) en su solución.

Configurar Citrix Secure Access en un entorno de Intune Android Enterprise

March 27, 2024

> **Importante:**
>
> Citrix SSO para Android ahora se llama Citrix Secure Access. Estamos actualizando nuestra documentación y las capturas de pantalla de la interfaz de usuario para reflejar este cambio de nombre.

El tema captura detalles sobre la implementación y la configuración de Citrix Secure Access a través de Microsoft Intune. En este documento se supone que Intune ya está configurado para la compatibilidad con Android Enterprise y que la inscripción de dispositivos ya se ha realizado.

Requisitos previos

- Intune está configurado para la compatibilidad con Android Enterprise
- Se ha completado la inscripción de dispositivos

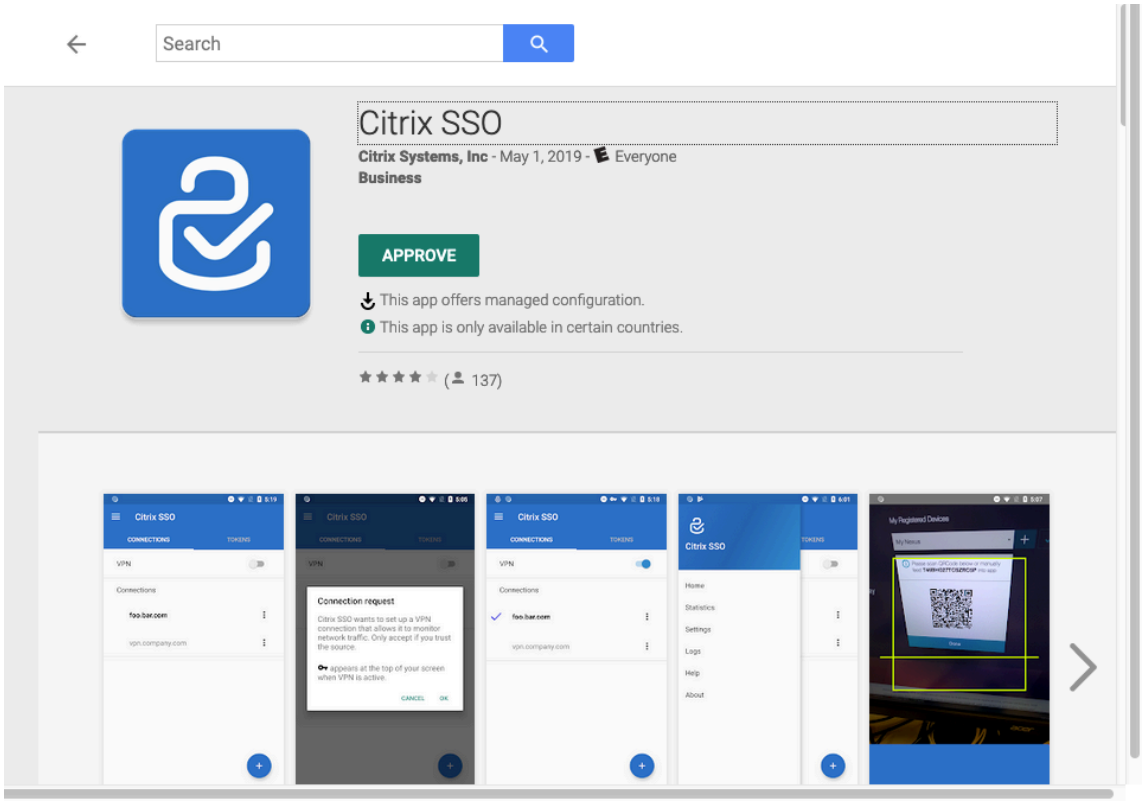
Para configurar Citrix Secure Access en un entorno Intune Android Enterprise

- Agregue Citrix Secure Access como aplicación administrada
- Configurar la directiva de aplicaciones administradas para Citrix Secure Access

Agregue Citrix Secure Access como aplicación administrada

1. Inicie sesión en el portal de Azure.
2. Haga clic en **Intune** en la hoja de navegación izquierda.
3. Haga clic en **Aplicaciones cliente** en el blade Microsoft Intune y, a continuación, haga clic en Aplicaciones en el blade Aplicaciones cliente.
4. Haga clic en **+Agregar enlace** en las opciones del menú superior derecho. Aparece el blade de configuración Agregar aplicación.
5. Selecciona **Google Play administrado** para el tipo de aplicación.

   Esto agrega Gestionar búsqueda en Google Play y aprobar blade si ha configurado Android Enterprise.
6. Busque Citrix Secure Access y selecciónelo en la lista de aplicaciones.



Nota: Si Citrix Secure Access no aparece en la lista, significa que la aplicación no está disponible en su país.

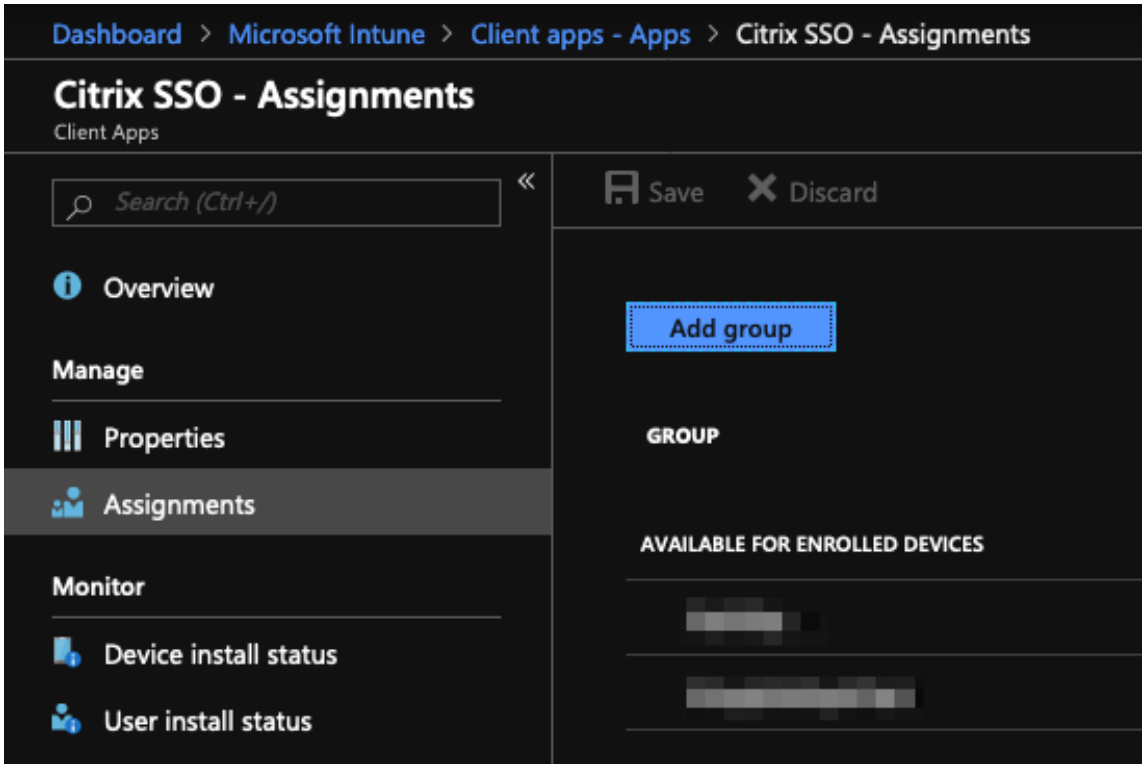
7. Haga clic en **APROBAR** para aprobar Citrix Secure Access para su implementación a través de la tienda gestionada de Google Play.

   Se enumeran los permisos que requiere Citrix Secure Access.

8. Haga clic en **APROBAR** para aprobar la aplicación para su implementación.
9. Haga clic en **Sincronizar** para sincronizar esta selección con Intune.

   Citrix Secure Access se agrega a la lista de aplicaciones cliente. Puede que tenga que buscar Citrix Secure Access si se han agregado muchas aplicaciones.

10. Haga clic en la aplicación **Citrix Secure Access** para abrir el módulo de detalles de la aplicación.
11. Haga clic en **Asignaciones** en la hoja de detalles. **Aparece el módulo Citrix Secure Access: Assignments.**



12. Haga clic en **Agregar grupo** para asignar los grupos de usuarios a los que quiere conceder permiso para instalar Citrix Secure Access y, a continuación, haga clic en **Guardar**.
13. Cierre el módulo de detalles de Citrix Secure Access.

Citrix Secure Access se agrega y habilita para su implementación entre los usuarios.

Configurar la directiva de aplicaciones administradas para Citrix Secure Access

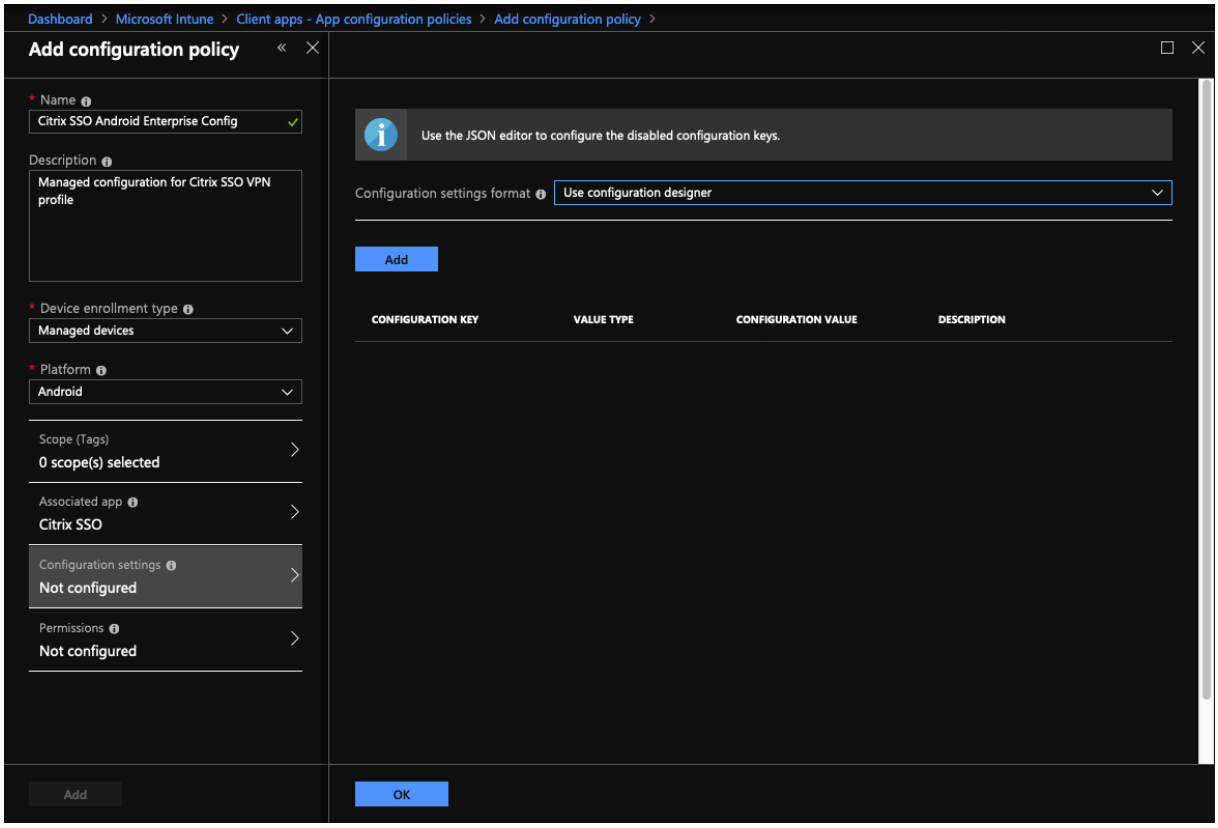
Una vez agregado Citrix Secure Access, debe crear una directiva de configuración administrada para Citrix Secure Access de modo que el perfil VPN se pueda implementar en Citrix Secure Access en el dispositivo.

1. Abra el blade de **Intune** en su portal de Azure.
2. Abra **el blade Client Apps** desde el blade de Intune.
3. Seleccione el elemento **Directivas de configuración de aplicaciones** en el blade Aplicaciones cliente y haga clic en **Agregar** para abrir el blade **Agregar directiva de configuración**.
4. Introduzca un nombre para la directiva y agregue una descripción.
5. En **Tipo de inscripción de dispositivos**, selecciona **Dispositivos administrados**.
6. En **Plataforma**, selecciona **Android**.

   Esto agrega otra opción de configuración para la aplicación asociada.
7. Haga clic en **Aplicación asociada** y seleccione la aplicación **Citrix Secure Access**.

   Es posible que tengas que buscarlo si tiene muchas aplicaciones.
8. Haga clic en **Aceptar**. Se agrega una opción de configuración en el blade Agregar directiva de configuración.
9. Haga clic en **Configuración**.

   Aparece un blade para configurar Citrix Secure Access.
10. En **Parámetros configuración**, seleccione **Usar el diseñador de configuración** o **Introducir datos JSON** para configurar Citrix Secure Access.



> **Nota:**
>
> Para configuraciones VPN sencillas, se recomienda utilizar el diseñador de configuración.

Configuración de VPN mediante el diseñador de configuración

1. En **Configuración**, seleccione **Usar diseñador de configuración** y haga clic en **Agregar**.

   Se le presenta una pantalla de introducción de valores clave para configurar varias propiedades compatibles con Citrix Secure Access. Como mínimo, debe configurar las propiedades Dirección del **servidor** y **Nombre del perfil de VPN**. Puede pasar el ratón por encima de la sección **DESCRIPCIÓN** para obtener más información sobre cada propiedad.

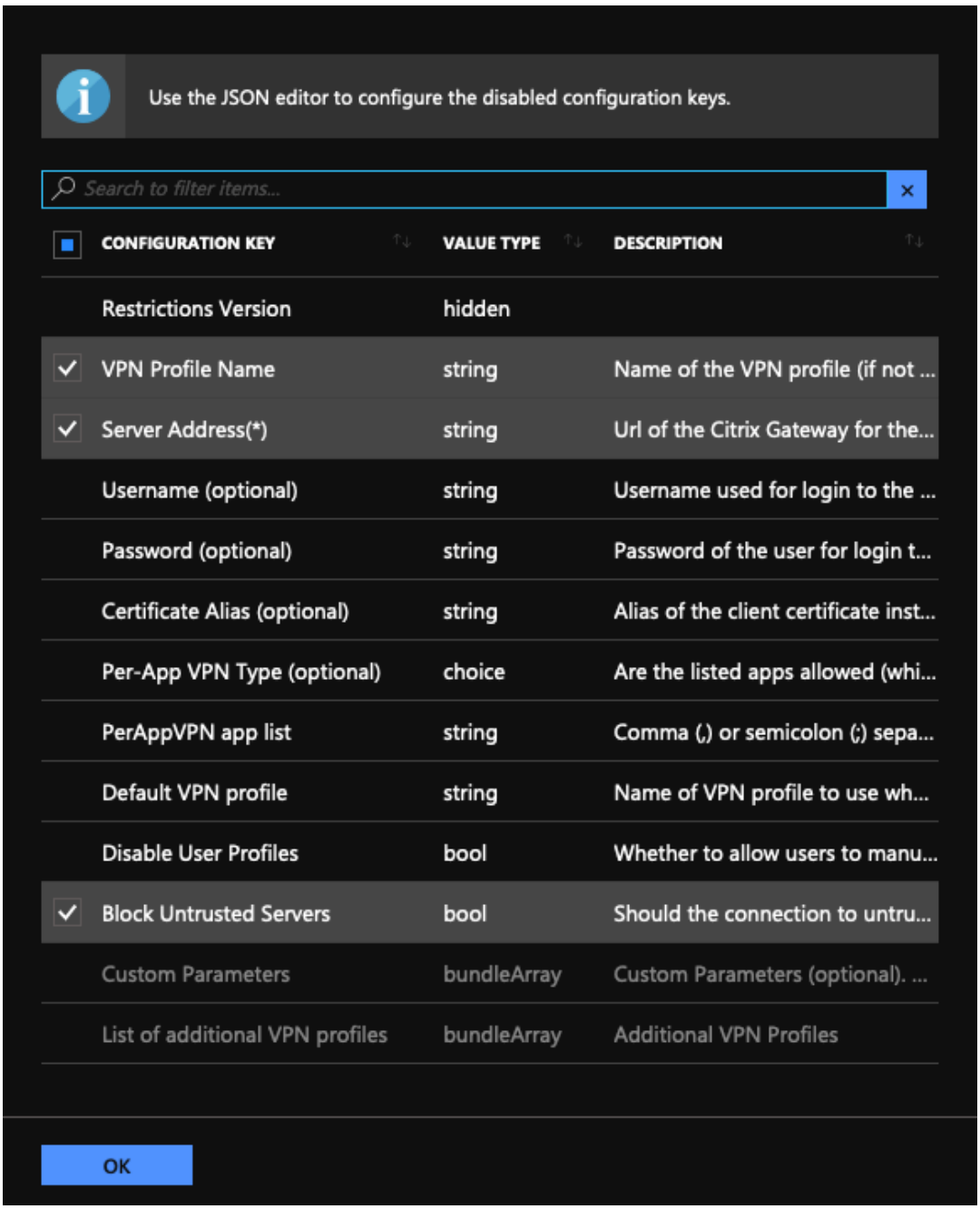
2. Por ejemplo, seleccione las propiedades **Nombre de perfil VPN** y **dirección del servidor (*)** y haga clic en **Aceptar**.

   Esto agrega las propiedades al diseñador de configuración. Puede configurar las siguientes propiedades.

   - **Nombre del perfil de VPN**. Escriba un nombre para el perfil VPN. Si va a crear más de un perfil de VPN, utilice un nombre único para cada perfil. Si no proporciona un nombre, la dirección que introduzca en el campo Dirección del servidor se utilizará como nombre del perfil de VPN.

- **Dirección del servidor(*)**. Escriba el FQDN base de NetScaler Gateway. Si el puerto de NetScaler Gateway no es 443, escriba también el puerto. Utilice un formato de URL. Por ejemplo: `https://vpn.mycompany.com:8443`.
- **Nombre de usuario (opcional)**. Introduzca el nombre de usuario que utilizan los usuarios finales para autenticarse en NetScaler Gateway. Puede usar el token de valor de configuración de Intune para este campo si la puerta de enlace está configurada para utilizarlo (consulte tokens de valor de configuración). Si no proporciona un nombre de usuario, se pide a los usuarios que proporcionen un nombre de usuario cuando se conectan a NetScaler Gateway.
- **Contraseña (opcional)**. Introduzca la contraseña que utilizan los usuarios finales para autenticarse en NetScaler Gateway. Si no proporciona una contraseña, se pedirá a los usuarios que proporcionen una contraseña cuando se conecten a NetScaler Gateway.
- **Alias de certificado (opcional)**. Proporcione un alias de certificado en el almacén de claves de Android para utilizarlo en la autenticación de certificados de cliente. Este certificado está preseleccionado para los usuarios si utiliza la autenticación basada en certificados.
- **Pins de certificados de Gateway (opcionales)**. Objeto JSON que describe los pines de certificado utilizados para NetScaler Gateway. Valor de ejemplo:.`{ "hash-alg": "sha256", "pinset": ["AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA=", "BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB="] }` Para obtener más información, consulte Fijación de certificados de NetScaler Gateway con Citrix Secure Access para Android.
- **Tipo de VPN por aplicación (opcional)**. Si usa una VPN por aplicación para restringir qué aplicaciones usan esta VPN, puede configurar esta configuración.
  - Si selecciona **Permitir**, el tráfico de red para los nombres de paquetes de aplicaciones que figuran en la lista de aplicaciones PerAppVPN se enruta a través de la VPN. El tráfico de red de todas las demás aplicaciones se redirige fuera de la VPN.
  - Si selecciona No **permitir**, el tráfico de red de los nombres de paquetes de aplicaciones que figuran en la lista de aplicaciones PerAppVPN se enruta fuera de la VPN. El tráfico de red de todas las demás aplicaciones se redirige a través de la VPN. El valor predeterminado es Permitir.
- **Lista de aplicaciones PerAppVPN**. Una lista de aplicaciones cuyo tráfico está permitido o no permitido en la VPN, en función del valor de Tipo de VPN por aplicación. Indique los nombres de los paquetes de aplicaciones separados por comas o puntos y comas. Los nombres de los paquetes de aplicaciones distinguen entre mayúsculas y minúsculas y deben estar escritos en esta lista tal y como lo están en la tienda de Google Play. Esta lista es opcional. Mantenga esta lista vacía para aprovisionar la VPN en todo el dispositivo.

- **Perfil VPN predeterminado**. El nombre del perfil de VPN que se utiliza cuando Always On VPN está configurado para Citrix Secure Access. Si este campo está vacío, se utiliza el perfil principal para la conexión. Si solo se configura un perfil, se marca como perfil VPN predeterminado.



Nota:

- Para convertir Citrix Secure Access en una aplicación VPN permanente en Intune, utilice el proveedor de VPN como personalizado y `com.citrix.CitrixVPN`como

> nombre del paquete de la aplicación.
>
> - Citrix Secure Access solo admite la autenticación de clientes basada en certificados para Always On VPN.
> - Los administradores deben seleccionar la **autenticación** de clientes y establecer el **certificado de cliente** como **obligatorio** en el **perfilSSL o las propiedades** SSL de NetScaler Gateway para que Citrix Secure Access funcione según lo previsto.

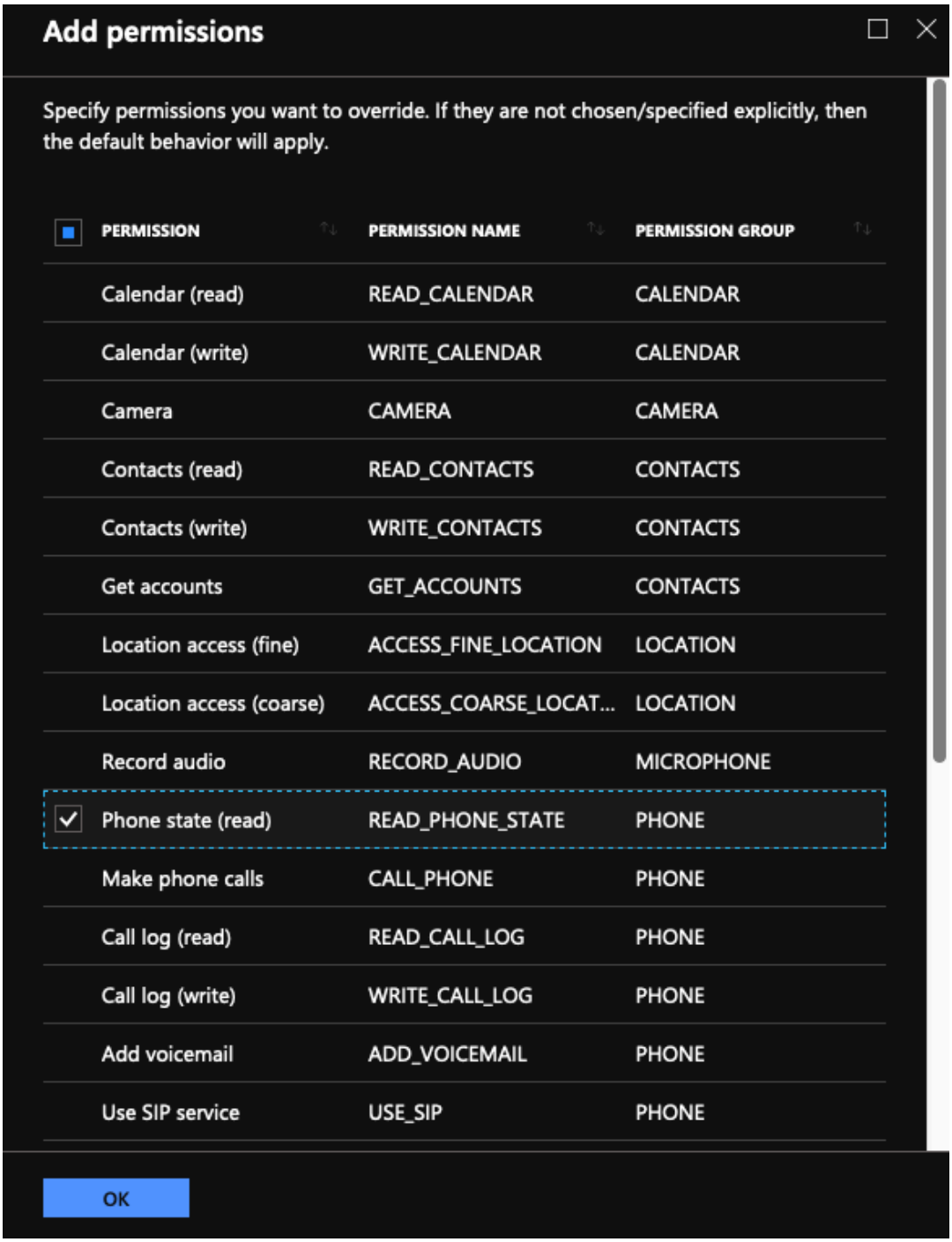
- **Inhabilitar perfiles de usuario**
  - Si establece este valor en true, los usuarios no pueden agregar nuevos perfiles VPN en sus dispositivos.
  - Si establece este valor en false, los usuarios pueden agregar sus propias VPN en sus dispositivos.

  El valor predeterminado es false.
- **Bloquear servidores no fiables**
  - Establezca este valor en false cuando utilice un certificado autofirmado para NetScaler Gateway o cuando el certificado raíz de la CA que emite el certificado de NetScaler Gateway no esté en la lista de CA del sistema.
  - Establezca este valor en true para permitir que el sistema operativo Android valide el certificado de NetScaler Gateway. Si se produce un error en la validación, no se permite la conexión.

  El valor predeterminado es true.

3. En la propiedad **Dirección del servidor (*)**, introduzca la URL base de la puerta de enlace VPN (por ejemplo, `https://vpn.mycompany.com`).
4. En **Nombre de perfil de VPN**, introduzca un nombre que esté visible para el usuario final en la pantalla principal del cliente Citrix Secure Access (por ejemplo, My Corporate VPN).
5. Puede agregar y configurar otras propiedades según corresponda a su implementación de NetScaler Gateway. Haga clic en **Aceptar** cuando haya terminado con la configuración.
6. Haga clic en la sección **Permisos**. Puede conceder los siguientes permisos requeridos por Citrix Secure Access:
   - Si utiliza la comprobación NAC de Intune, Citrix Secure Access requiere que conceda el permiso de **estado (lectura) del teléfono**. Haga clic en el botón **Agregar** para abrir la hoja de permisos. En la actualidad, Intune muestra una lista significativa de permisos disponibles para todas las aplicaciones.
   - Si utiliza la comprobación de NAC de Intune, seleccione Permiso de **estado del teléfono (lectura)** y haga clic en **Aceptar**. Esto lo agrega a la lista de permisos de la aplicación.

Seleccione **Solicitar** o **Concesión automática** para que la comprobación de NAC de Intune funcione y haga clic en **Aceptar**.



- Se recomienda conceder automáticamente permisos de notificación a Citrix Secure Access.

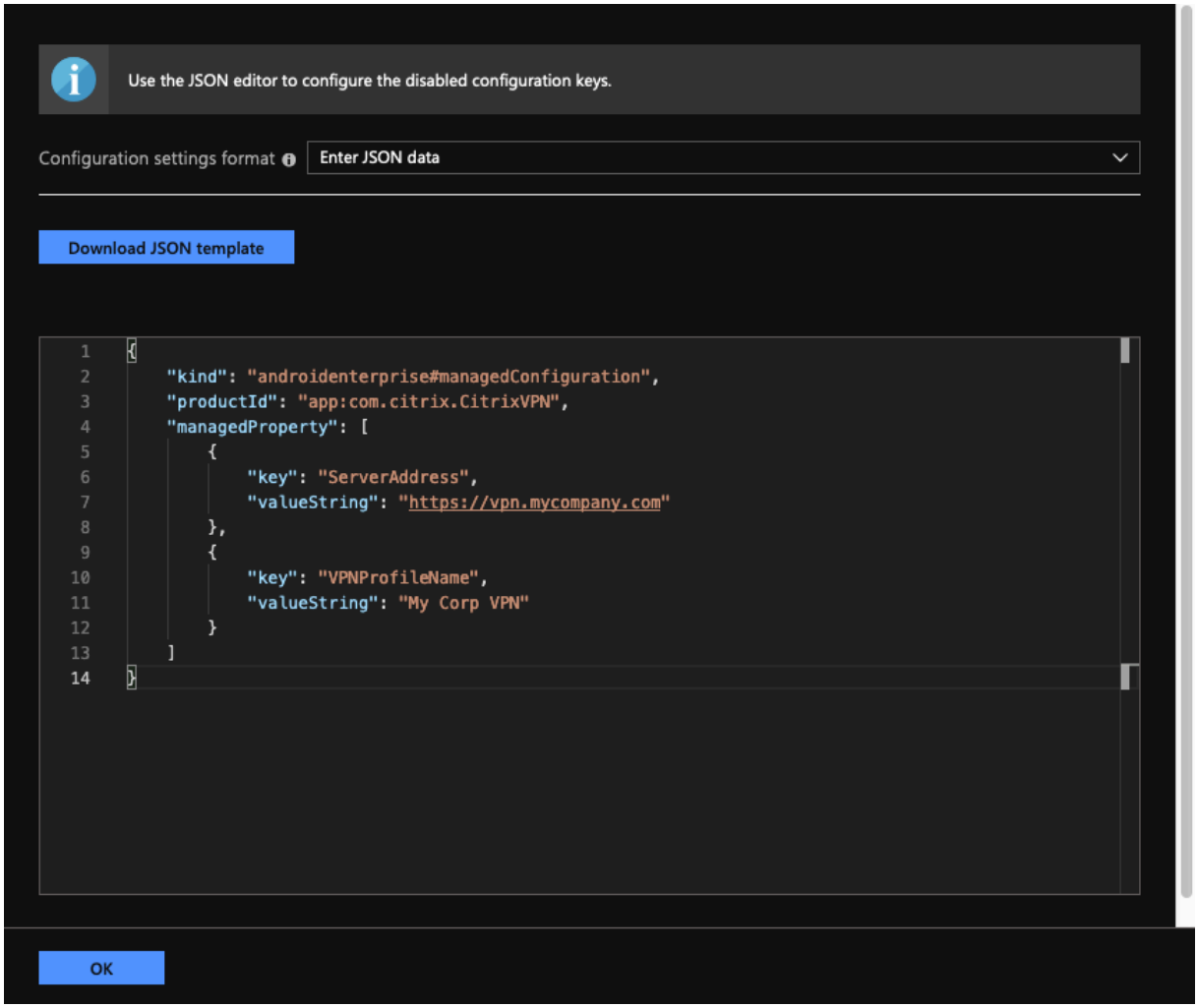
> **Nota:**
>
> Para los usuarios de Android 13+ que utilizan Citrix Secure Access 23.12.1 y versiones posteriores, se recomienda a los administradores de MDM que concedan el permiso de notificación a Citrix Secure Access (ID de paquete: `com.citrix.CitrixVPN`) en su solución.

7. Haga clic en **Agregar** en la parte inferior del módulo de directivas de configuración de aplicaciones para guardar la configuración administrada de Citrix Secure Access.
8. Haga clic en **Asignaciones** en el blade de directivas de configuración de aplicaciones para abrir el blade **Asignaciones**.
9. Seleccione los grupos de usuarios para los que quiere que se entregue y aplique esta configuración de Citrix Secure Access.

Configuración de VPN mediante la introducción de datos JSON

1. En **Parámetros de configuración**, seleccione **Introducir datos JSON** para configurar Citrix Secure Access.
2. Utilice el botón Descargar plantilla JSON para descargar una plantilla que permita proporcionar una configuración más detallada o compleja para Citrix Secure Access. Esta plantilla es un conjunto de pares clave-valor JSON para configurar todas las propiedades posibles que Citrix Secure Access entiende.

   Para obtener una lista de todas las propiedades disponibles que se pueden configurar, consulte Propiedades disponibles para configurar el perfil VPN en la aplicación Citrix Secure Access.
3. Una vez creado un archivo de configuración JSON, copie y pegue su contenido en el área de modificación. Por ejemplo, a continuación se muestra la plantilla JSON para la configuración básica creada previamente con la opción del diseñador de configuración.



Esto completa el procedimiento de configuración e implementación de perfiles VPN para Citrix Secure Access en el entorno Microsoft Intune Android Enterprise.

> **Importante:**
>
> El certificado utilizado para la autenticación basada en certificados de cliente se implementa mediante un perfil SCEP de Intune. El alias de este certificado debe configurarse en la propiedad **Certificate Alias** de la configuración administrada de Citrix Secure Access.

Propiedades disponibles para configurar el perfil VPN en Citrix Secure Access

Clave de configuración	Nombre de campo JSON	Tipo de valor	Descripción
Nombre del perfil VPN	VPNProfileName	Texto	Nombre del perfil VPN (si no se establece el valor predeterminado en la dirección del servidor).
Dirección del servidor (*)	ServerAddress	URL	URL base de NetScaler Gateway para la conexión (`https://host[:port]`). Este campo es obligatorio.
`Username` (optativo)	Nombre de usuario	Texto	Nombre de usuario utilizado para la autenticación con NetScaler Gateway (opcional).
Contraseña (opcional)	Contraseña	Texto	Contraseña del usuario para autenticarse con NetScaler Gateway (opcional).
Alias de certificado (opcional)	ClientCertAlias	Texto	Alias del certificado de cliente instalado en el almacén de credenciales de Android para su uso en la autenticación de clientes basada en certificados (opcional). El **alias del certificado** es un campo obligatorio cuando se utiliza la autenticación basada en certificados en NetScaler Gateway.

Clave de configuración	Nombre de campo JSON	Tipo de valor	Descripción
Pins de certificados de Gateway (opcionales)	ServerCertificatePins	Texto JSON	Objeto JSON incrustado que describe los pines de certificado utilizados en NetScaler Gateway. Valor de ejemplo:.{ "hash-alg": "sha256", "pinset": ["AAAAAAAAAAAAAAAAAAAAAAAAAA=", "BBBBBBBBBBBBBBBBBBBBBBBBBB="] } Asegúrese de escapar de estos datos JSON incrustados cuando utilice el configurador JSON.

Clave de configuración	Nombre de campo JSON	Tipo de valor	Descripción
Tipo de VPN por aplicación (opcional)	PerAppVPN_Allow_Disallow_Setting	Enum (Permitir, No permitir)	¿Se permite o no utilizar el túnel VPN a las aplicaciones de la lista (lista de permitidos) o no (lista de bloqueados)?Si se establece en **Permitir**, solo las aplicaciones de la lista (en la propiedad de lista de aplicaciones PerAppVPN) pueden realizar un túnel a través de la VPN. Si se establece en **No permitir**, todas las aplicaciones excepto las que aparecen en la lista pueden realizar un túnel a través de la VPN. Si no aparece ninguna aplicación en la lista, todas las aplicaciones pueden hacer túneles a través de la VPN.

Clave de configuración	Nombre de campo JSON	Tipo de valor	Descripción
Lista de aplicaciones PerAppVPN	PerAppName_Appnames	Texto	Lista de nombres de paquetes de aplicaciones separados por comas (,) o puntos y comas (;) para una VPN por aplicación. Los nombres de los paquetes deben ser los mismos que aparecen en la URL de la página de listado de aplicaciones de Google Play Store. Los nombres de los paquetes distinguen entre mayúsculas y minúsculas.
Perfil de VPN predeterminado	DefaultProfileName	Texto	Nombre del perfil de VPN que se utilizará cuando el sistema inicie el servicio de VPN. Esta configuración se usa para identificar el perfil de VPN que se utilizará cuando la VPN permanente esté configurada en el dispositivo.

Clave de configuración	Nombre de campo JSON	Tipo de valor	Descripción
Inhabilitar perfiles de usuario	DisableUserProfiles	Booleano	Propiedad que permite o no a los usuarios finales crear perfiles de VPN manualmente. Establezca este valor en **true** para impedir que los usuarios creen perfiles VPN. El valor predeterminado es **falso.**
Bloquear servidores no fiables	BlockUntrustedServers	Booleano	¿Propiedad para determinar si se bloquea la conexión a puertas de enlace que no son de confianza (por ejemplo, si se utilizan certificados autofirmados o cuando el sistema operativo Android no confía en la CA emisora)? El valor predeterminado es true (bloquea las conexiones a puertas de enlace que no son de confianza).

Clave de configuración	Nombre de campo JSON	Tipo de valor	Descripción
Parámetros personalizados (opcional)	CustomParameters	Lista	Lista de parámetros personalizados (opcionales) compatibles con Citrix Secure Access. Para obtener más información, consulte Parámetros personalizados. Consulte la **documentación del producto NetScaler Gateway** para ver las opciones disponibles.
Lista de otros perfiles de VPN	bundle_profiles	Lista	Lista de otros perfiles de VPN. Se admiten la mayoría de los valores mencionados anteriormente para cada perfil. Para obtener más información, consulte Propiedades compatibles para cada VPN en la lista de perfiles de VPN.

Parámetros personalizados Cada parámetro personalizado debe definirse con los siguientes nombres de clave-valor.

Clave	Tipo de valor	Valor
ParameterName	Texto	Nombre del parámetro personalizado.
ParameterValue	Texto	Valor del parámetro personalizado.

Parámetros personalizados para la configuración de Intune

Nombre del parámetro	Descripción	Valor
UserAgent	Citrix Secure Access agrega este valor de parámetro al encabezado HTTP del agente de usuario, cuando se comunica con NetScaler Gateway, para realizar una comprobación adicional en NetScaler Gateway.	Especifique el texto que debe adjuntar al encabezado HTTP del agente de usuario. El texto debe cumplir con las especificaciones del agente de usuario HTTP.
EnableDebugLogging	Habilite el registro de depuración en Citrix Secure Access para ayudar a solucionar problemas de conectividad VPN en caso de Always On VPN. Puede habilitarlos en cualquiera de las configuraciones de VPN administradas. Los registros de depuración surten efecto cuando se procesan las configuraciones administradas.	**True**: Habilita los registros de depuración. Valor predeterminado: **False**.

Para obtener más información sobre los parámetros personalizados, consulte Crear una configuración administrada de Android Enterprise para Citrix Secure Access.

Propiedades admitidas para cada VPN en la lista de perfiles de VPN Se admiten las siguientes propiedades para cada perfil de VPN al configurar varios perfiles VPN mediante la plantilla JSON.

Clave de configuración	Nombre de campo JSON	Tipo de valor
Nombre del perfil VPN	bundle_VPNProfileName	Texto
Dirección del servidor (*)	bundle_ServerAddress	URL
Nombre de usuario	bundle_username	Texto
Contraseña	bundle_password	Texto

Clave de configuración	Nombre de campo JSON	Tipo de valor
Alias de certificado de cliente	bundle_ClientCertAlias	Texto
Pins de certificados de Gateway	bundle_ServerCertificatePins	Texto
Tipo de VPN por aplicación	bundle_PerAppVPN_Allow_Disallow_Setting	En Set(Permitir, No permitir)
Lista de aplicaciones PerAppVPN	bundle_PerAppVPN_Appnames	Texto
Parámetros personalizados	bundle_CustomParameters	Lista

Configure Citrix Secure Access como proveedor de VPN siempre activo en Intune

En ausencia de una compatibilidad con VPN bajo demanda en un subsistema VPN de Android, la VPN Always On se puede utilizar como alternativa para ofrecer una opción de conectividad VPN perfecta junto con la autenticación de certificados de cliente con Citrix Secure Access. El sistema operativo inicia la VPN cuando se inicia o cuando se activa el perfil de trabajo.

Para convertir Citrix Secure Access en una aplicación VPN Always On en Intune, debe usar la siguiente configuración.

- Elija el tipo correcto de configuración administrada que quiere utilizar (propiedad personal con perfil de trabajo O perfil de trabajo totalmente administrado, dedicado y propiedad de la empresa).
- Cree un perfil de configuración de dispositivo y seleccione **Restricciones de dispositivos** y, a continuación, vaya a la sección **Conectividad**. Seleccione habilitar para la configuración VPN siempre activa.
- Elija **Citrix Secure Access** como cliente VPN. Si Citrix Secure Access no está disponible como opción, puede elegir **Personalizar**como cliente VPN e introducir **com.citrix.CitrixVPN** en el campo ID del paquete (el campo ID del paquete distingue entre mayúsculas y minúsculas)
- Deja las demás opciones tal cual. Se recomienda no habilitar el modo de bloqueo. Si está habilitado, el dispositivo podría perder la conectividad de red completa si la VPN no está disponible.
- Además de esta configuración, también puede establecer el **tipo de VPN por aplicación** y la **lista de aplicaciones PerAppVPN** en la página **Directivas de configuración de aplicaciones** para habilitar la VPN por aplicación para Android, tal y como se describe en las secciones anteriores.

> **Nota:**
>
> Always On VPN solo es compatible con la autenticación de certificados de cliente en Citrix Secure

> Access.

Referencias

Consulte los temas siguientes para obtener más información sobre cómo configurar las opciones de conectividad en Intune.

- Dispositivos corporativos dedicados totalmente administrados
- Dispositivos de propiedad personal

Reinicio automático de Always On VPN

A partir de Citrix SSO para Android 23.8.1, Citrix Secure Access reinicia automáticamente la VPN Always On cuando una aplicación que forma parte de la lista de permitidos o bloqueados se instala en un perfil de trabajo o de dispositivo. El tráfico de la aplicación recién instalada se canaliza automáticamente a través de una conexión VPN sin reiniciar el perfil de trabajo ni reiniciar el dispositivo.

Para habilitar el reinicio automático de Always On VPN, los usuarios finales deben conceder a la consulta todos los paquetes su consentimiento a Citrix Secure Access. Una vez otorgado el consentimiento, Citrix Secure Access:

- Recibe la notificación de instalación del paquete del sistema operativo.
- Reinicia la VPN Always On.

Cuando un usuario final se conecta a un perfil de VPN por aplicación por primera vez, se le pide que dé su consentimiento (exigido por las directivas de Google) para recopilar información del paquete instalado. Si el usuario final otorga el consentimiento, se inicie la conexión VPN. Si el usuario niega el consentimiento, se interrumpe la conexión VPN. La pantalla de consentimiento no vuelve a aparecer una vez que se ha otorgado el consentimiento. Para obtener más información sobre las instrucciones para el usuario final, consulte Cómo utilizar Citrix Secure Access desde un dispositivo Android.

Limitaciones

Estas limitaciones se aplican a las VPN por aplicación en dispositivos Android 11 o con una versión posterior en el entorno Android Enterprise debido a restricciones de visibilidad de los paquetes incorporadas en Android 11:

- Si una aplicación que forma parte de la lista de permitidos o denegados se implementa en un dispositivo después de que se haya iniciado la sesión de VPN, el usuario final debe reiniciar la sesión de VPN para que la aplicación pueda enrutar su tráfico a través de la sesión VPN.

- Si la VPN por aplicación se usa a través de una sesión de Always On VPN, después de instalar una nueva aplicación en el dispositivo, el usuario final debe reiniciar el perfil de trabajo o reiniciar el dispositivo para que el tráfico de la aplicación se enrute a través de la sesión de VPN.

> **Nota:**
>
> Estas limitaciones no se aplican si utiliza Citrix SSO para Android 23.8.1 o una versión posterior. Consulte Reinicio automático de Always On VPN para obtener más información.

Fijación de certificados de NetScaler Gateway con Citrix Secure Access para Android

January 26, 2024

> **Importante:**
>
> Citrix SSO para Android ahora se llama Citrix Secure Access. Estamos actualizando nuestra documentación y las capturas de pantalla de la interfaz de usuario para reflejar este cambio de nombre.

La fijación de certificados ayuda a prevenir los ataques de intermediarios. Citrix Secure Access solo admite la fijación de certificados para configuraciones de VPN administradas en el modo Android Enterprise y en el modo de administrador de dispositivos antiguos. No es compatible con los perfiles VPN agregados por el usuario final.

Configurar la anclaje de certificados de NetScaler Gateway con Citrix Secure Access para Android

Para obtener más información sobre la fijación de certificados en la configuración administrada (anteriormente restricciones de aplicaciones) para Citrix Secure Access, consulte Certificados y autenticación.

Se define un nuevo par clave-valor para llevar los hashes de certificados de NetScaler Gateway anclados de la siguiente manera.

```
Key: ServerCertificatePins
Value: {

  "hash-alg": "sha256",
  "pinset": [
    "cert1_base64_encoded_SHA-256_hash_of_the_X509_SubjectPublicKeyInfo
       (SPKI)",
```



```
      "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA=",
      "BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB="
      ...
    ]
  }

<!--NeedCopy-->
```

La clave para especificar los detalles de fijación de certificados en la configuración administrada es **ServerCertificatePins**. El valor es una carga útil JSON que lleva los hashes SHA-256 codificados en base64 del certificado de NetScaler Gateway anclado y el algoritmo hash utilizado. El certificado anclado puede ser cualquiera de los certificados de la cadena de confianza validados por el sistema operativo. En este caso, es Android.

La fijación de certificados solo se realiza después de que el sistema operativo haya validado la cadena de certificados durante el protocolo de enlace TLS. El pin del certificado se calcula mediante el hash de la información de clave pública del sujeto del certificado (SPKI). Ambos campos ("**hash-alg**" y **"pinset"**) deben especificarse en la carga útil de JSON.

El "**hash-alg**"especifica el algoritmo hash utilizado para calcular el hash SPKI.
El "**pinset**"especifica la matriz JSON que contiene el hash SHA-256 codificado en base64 de los datos SPKI del certificado de NetScaler Gateway.
Debe especificarse al menos un valor para el pin del certificado. Se pueden especificar más valores de pin para permitir la rotación o caducidad del certificado.

Puede calcular el valor del pin de un dominio (por ejemplo, gw.yourdomain.com) mediante el siguiente comando openssl.

```
openssl s_client -servername gw.yourdomain.com -connect gw.yourdomain.
    com:443 | openssl x509 -pubkey -noout | openssl pkey -pubin -outform
     der | openssl dgst -sha256 -binary | openssl enc -base64
<!--NeedCopy-->
```

El comando muestra el hash SHA-256 codificado en base64 del certificado hoja presentado por una puerta de enlace. Cualquier certificado de la cadena se puede utilizar para la fijación de certificados. Por ejemplo, si una empresa utiliza su propia entidad emisora de certificados intermedia para generar certificados para varias puertas de enlace, se puede utilizar el pin correspondiente al certificado de firma intermedio. Si ninguno de los pines coincide con los certificados de la cadena de certificados validada, el protocolo de enlace TLS se anula y la conexión a la puerta de enlace no continúa.

> **Nota:**
>
> En el modo de administrador de dispositivos, la fijación de certificados solo se admite con las soluciones Citrix Endpoint Management y Microsoft Endpoint Management. La fijación de certificados debe configurarse en los parámetros personalizados utilizados en el perfil VPN heredado (configuración no administrada) con el parámetro personalizado ServerCertificatePins con la

> misma carga útil JSON para la fijación.

Notas de la versión de Citrix Secure Access para Windows

March 27, 2024

El cliente de Citrix Secure Access para Windows ahora se publica de forma independiente y es compatible con todas las versiones de NetScaler. La versión del cliente de Citrix Secure Access sigue el formato YY.MM Release.Build.

Las notas de la versión describen las nuevas funciones, las mejoras de las funciones existentes y los problemas resueltos.

Novedades: Las nuevas funciones y mejoras disponibles en la versión actual.

Problemasresueltos : los problemas que se han corregido en la versión actual.

Para obtener información detallada sobre las funciones admitidas, consulte Documentación del producto NetScaler Gateway.

> **Nota:**
>
> - El cliente Citrix Secure Access para Windows, compilación 23.7.1.1 y versiones posteriores, contiene la solución para.https://support.citrix.com/article/CTX564833
> - El cliente de Citrix Secure Access (anteriormente conocido como plug-in de NetScaler Gateway para Windows), compilación 21.9.1.2 y posteriores, contiene la solución para.https://support.citrix.com/article/CTX341455

24.2.1.15 (4 de marzo de 2024)

Novedades

- **Soporte para SNI**

  En una implementación de Citrix Secure Private Access, el cliente Citrix Secure Access ahora admite la extensión de indicación del nombre del servidor (SNI) en todas las solicitudes previas a la autenticación.

  [SPAHELP-236]

- **Soporte para TLS 1.3**

  El cliente Citrix Secure Access ahora admite el protocolo TLS 1.3. TLS 1.3 es compatible con las siguientes plataformas:

- Windows 11 y versiones posteriores
- Windows Server 2022 y versiones posteriores

Para obtener más información sobre cómo configurar TLS 1.3 en NetScaler, consulte Compatibilidadcon el protocolo TLS 1.3.

[CSACLIENTS-6106]

- **Compatibilidad con los detalles del sistema operativo Windows en el encabezado HTTP**

  El cliente Citrix Secure Access ahora incluye detalles del sistema operativo Windows como parte de la cadena de encabezado HTTP (user-agent).

  [NSHELP-36732]

Problemas resueltos

La resolución de DNS falla de forma intermitente si IPv6 está habilitado en el adaptador de red del cliente.

[NHELP-35708]

Es posible que los usuarios no puedan iniciar sesión en el cliente Citrix Secure Access si hay intentos de inicio de sesión simultáneos mediante el inicio de sesión automático.

[NSHELP-35768]

La instalación de Citrix Secure Access falla cuando Smart App Control está habilitado en máquinas cliente que no están en inglés.

[NSHELP-36126], [NSHELP-36907]

Los usuarios no pueden acceder a algunas aplicaciones a través de VPN si el cliente Citrix Secure Access está configurado con el controlador WFP. Este problema se produce debido a modificaciones en las políticas del firewall.

[NSHELP-36254], [NSHELP-36312]

Aparece un cuadro de diálogo emergente durante un escaneo de la EPA. Sin embargo, cuando el usuario hace clic en Aceptar, el escaneo de la EPA funciona como de costumbre. Este problema se produce cuando se selecciona el idioma sueco (**Configuración > Idioma**) en la interfaz de usuario del cliente Citrix Secure Access.

[NHELP-36408]

En el modo Always On VPN, el túnel a nivel de máquina no puede transferir la sesión cuando la autenticación del certificado de usuario está configurada en NetScaler Gateway.

[NSHELP-36492]

El acceso a los recursos de la intranet falla de forma intermitente cuando el controlador de la Plataforma de filtrado de Windows (WFP) está habilitado en el cliente Citrix Secure Access.

[NSHELP-36568]

La página de la interfaz de usuario del cliente de Citrix Secure Access se bloquea de forma intermitente cuando los usuarios hacen clic en el botón Inicio.

[NSHELP-37046]

Los usuarios que no son administradores no pueden conectarse al túnel VPN completo si se cumplen las siguientes condiciones:

- El EPA está configurado como un factor en un flujo de nFactor.
- Edge WebView está activado.
- La configuración de actualización de controles del cliente Citrix EPA está establecida en **Always** on NetScaler Gateway y hay una discrepancia en las versiones del cliente Citrix EPA entre el dispositivo cliente y NetScaler.

[NHELP-37340]

El escaneo de certificados de dispositivos de la EPA falla si el almacén de certificados del sistema de la máquina cliente contiene solo un certificado de dispositivo.

[NSHELP-37371]

La página de inicio de sesión del cliente Citrix Secure Access se queda en blanco de forma intermitente al conectarse al servicio Citrix Secure Private Access.

[SPAHELP-202]

Es posible que los usuarios finales no puedan conectar las máquinas cliente al dominio a través de una VPN si se utilizan Windows Server 2019 o versiones posteriores.

[SPAHELP-219]

Cuando el servicio Citrix Device Posture está habilitado, aparecen entradas no deseadas en la lista desplegable **Conexión** de la interfaz de usuario del cliente Citrix Secure Access.

[SPAHELP-271]

Los usuarios finales no pueden acceder a los recursos de la intranet si la función de inicio de sesión único está habilitada en el cliente Citrix Secure Access.

[CSACLIENTS-9940]

23.10.1.7 (29 de noviembre de 2023)

Novedades

- **Configurar el rango de puertos privados para las conexiones iniciadas por el servidor**

  Ahora puede configurar un puerto privado que vaya del 49152 al 64535 para las conexiones iniciadas por el servidor. La configuración de puertos privados evita los conflictos que pueden surgir al utilizar los puertos para crear sockets entre el cliente Citrix Secure Access y las aplicaciones de terceros en las máquinas cliente. Puede configurar los puertos privados mediante el Registro de VPN de Windows "SicBeginPort". Como alternativa, puede configurar el rango de puertos privados mediante un archivo JSON de personalización del complemento VPN en NetScaler.

  Para obtener más información, consulte Configurar las conexiones iniciadas por el servidor y las claves de registro del cliente VPN de Windows de NetScaler Gateway.

  [NSHELP-36627]

- **Soporte de autenticación Kerberos para un inicio de sesión automático sin problemas**

  El cliente Citrix Secure Access ahora usa el método de autenticación Kerberos para el inicio de sesión automático. Como parte de este soporte, se introduce una clave de registro de clientes VPN "EnableKerberosAuth". Como requisito previo, los administradores deben configurar la autenticación Kerberos en NetScaler y en sus máquinas cliente. Los usuarios finales deben instalar Microsoft Edge WebView en sus máquinas para habilitar el método de autenticación Kerberos. Para obtener más información, consulte Inicio de sesión automático con autenticación Kerberos.

  [CSACLIENTS-3128]

- **Asignación automática de un rango de direcciones IP falsas**

  El cliente Citrix Secure Access ahora puede detectar y aplicar un nuevo rango de direcciones IP falsas si hay un conflicto entre el rango de direcciones IP falsas configurado por el administrador y las aplicaciones basadas en IP o la red del usuario final.

  [CSACLIENTS-6132]

- **Notificaciones de Microsoft**

  Las notificaciones del cliente Citrix Secure Access ahora aparecen como notificaciones de Microsoft en el panel de notificaciones de su máquina Windows.

  [CSACLIENTS-6136]

- **Recopilación de registros mejorada**

El nivel de registro de Verbose ahora se usa como el nivel de registro de depuración predeterminado para mejorar la recopilación de registros y la solución de problemas. Para obtener más información sobre el registro, consulte Configurar el registro mediante la interfaz de usuario del cliente.

[CSACLIENTS-8151]

Problemas resueltos

El cliente Citrix Secure Access permanece en estado "Conectado"si el túnel de máquinas del servicio Always On no detecta la ubicación del dispositivo cliente.

[CSACLIENTS-1174]

La función de transferencia de inicio de sesión no funciona cuando Microsoft Edge WebView está habilitado en el cliente Citrix Secure Access.

[CSACLIENTS-6655]

En el modo de servicio Always On, el cliente Citrix Secure Access no puede establecer un túnel a nivel de máquina con NetScaler Gateway si las directivas de autenticación clásica basadas en certificados del dispositivo están enlazadas a un servidor virtual VPN.

[NSHELP-33766]

Las llamadas entrantes y salientes de Webex fallan cuando los usuarios están conectados a la VPN. Este problema se produce cuando el controlador de la plataforma de filtrado de Windows (WFP) está habilitado en el cliente Citrix Secure Access en lugar del controlador Deterministic Network Enhancer (DNE).

[NSHELP-34651]

El cliente Citrix Secure Access se bloquea si se cumplen las siguientes condiciones:

- Las conexiones se cambian cuando las directivas SAML están enlazadas a un servidor virtual VPN.
- La compatibilidad con Internet Explorer WebView está habilitada.

[NSHELP-35366]

La interfaz de usuario del cliente Citrix Secure Access muestra el botón Conectar durante el inicio de sesión automático. Este problema se produce si se utiliza el método de autenticación UserCert para conectarse a la VPN.

[NSHELP-36134]

La función de acceso LAN local no funciona con el cliente Citrix Secure Access si se configura un túnel a nivel de máquina.

Con esta versión, la función de acceso LAN local se puede configurar con una configuración de túnel a nivel de máquina. Para lograrlo, debe configurar el parámetro de acceso a la LAN local en FORCED cuando utilice el modo de túnel de máquinas. Para obtener más información, consulte Exigir el acceso LAN local a los usuarios finales en función de la configuración del ADC.

[NSHELP-36214]

Cuando una máquina cliente se despierta del modo de suspensión varias veces, el cliente Citrix Secure Access no puede establecer una conexión VPN con las aplicaciones de la intranet.

[NSHELP-36221]

23.8.1.11 (19 de octubre de 2023)

Problemas resueltos

Es posible que el archivo epaPackage.exe no se descargue si la compatibilidad con proxy de reenvío está configurada en NetScaler Gateway.

[CSACLIENTS-6917]

La instalación del cliente Citrix EPA falla para los usuarios no administradores con acceso restringido a la unidad C.

[NSHELP-36590]

23.8.1.5 (09 de agosto de 2023)

Problemas resueltos

El SSO de Kerberos falla en las aplicaciones cuando se conectan a través del servicio Citrix Secure Private Access.

[CSACLIENTS-912]

El acceso a las aplicaciones con el servicio Citrix Secure Private Access falla de forma intermitente. Este problema se produce cuando el cliente Citrix Secure Access comparte una dirección IP de destino incorrecta para el tráfico TCP o UDP.

[CSACLIENTS-1151, CSACLIENTS-6326]

El cliente Citrix Secure Access no puede iniciar las aplicaciones de forma intermitente debido a un problema de almacenamiento en caché de DNS.

[CSACLIENTS-1170]

El cliente Citrix Secure Access no puede aplicar un sufijo DNS a Citrix Virtual Adapter. Este problema se produce cuando Citrix Virtual Adapter no se autentica con Active Directory.

[NSHELP-33817]

El cliente Citrix Secure Access se bloquea si se cumplen las siguientes condiciones:

- El servidor virtual de NetScaler Gateway contiene un certificado de cliente como factor de autenticación nFactor.
- La compatibilidad con Microsoft Edge WebView está habilitada.

[CSACLIENTS-6171]

Cuando se conecte a una VPN, es posible que no pueda acceder a los recursos de back-end después de aplicar Microsoft KB5028166.

[NSHELP-35909]

El cliente Citrix Secure Access no puede descargar las configuraciones de NetScaler Gateway de forma intermitente cuando la personalización del portal supera el límite permitido.

[NSHELP-35971]

Problemas conocidos

La función de transferencia de inicio de sesión no funciona con el cliente Citrix Secure Access. Este problema se produce cuando Microsoft Edge WebView está activado.

Solución alternativa: Inicie sesión con un explorador web para transferir la sesión.

23.7.1.1 (14-jul-2023)

Problemas resueltos

En algunos casos, tras una actualización a la versión 23.x.x.x, el tráfico no pasa por el túnel VPN, lo que provoca el bloqueo del acceso a la VPN cuando se configura un rango de IP de la intranet en NetScaler. Esto ocurre cuando la regla de firewall de perfil cruzado no se aplica a las aplicaciones VPN.

[NSHELP-35766]

23.5.1.3 (02-jun-2023)

Problemas resueltos

El servicio Always On se bloquea cuando se habilita la recopilación de registros mejorada mediante el registro “useNewLogger”en `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access`

`Client`.

[CGOP-24462]

23.4.1.5 (14 de abril de 2023)

Novedades

- **Compatibilidad con Microsoft Edge WebView**

  La compatibilidad con Microsoft Edge WebView en el cliente de Citrix Secure Access para Windows presenta una experiencia mejorada para el usuario final. Esta función está inhabilitada de forma predeterminada. Para obtener más información, consulte la compatibilidad con Microsoft Edge WebView para Windows Citrix Secure Access.

  [CGOP-22245]

- **Agregar sufijos DNS para resolver los FQDN en direcciones IP**

  Los administradores ahora pueden agregar sufijos a las aplicaciones a nivel del sistema operativo. Esto ayuda a los clientes de Citrix Secure Access a resolver un nombre de dominio que no esté totalmente cualificado durante la resolución de nombres.

  Los administradores también pueden configurar las aplicaciones mediante las direcciones IP (intervalo de IP/CIDR de IP) para que los usuarios finales puedan acceder a las aplicaciones mediante los FQDN correspondientes. Para obtener más información, consulte los sufijos DNS para resolver los FQDN en direcciones IP.

  [ACS-2490]

- **Recopilación de registros mejorada**

  La función de registro del cliente de Windows Secure Access ahora se ha mejorado para recopilar y depurar registros. Se han realizado los siguientes cambios en la función de registro.

  - Permita a los usuarios cambiar el tamaño máximo del archivo de registros a un valor inferior a 600 MB.
  - Permita a los usuarios actualizar el número de archivos de registros a menos de 5.
  - Aumente los niveles de registro a tres para la nueva función de registro.

  Con estos cambios, los administradores y los usuarios finales pueden recopilar registros de la sesión actual y de las sesiones pasadas. Anteriormente, la recopilación de registros se limitaba únicamente a las sesiones actuales. Para obtener más información, consulte Recopilación de registros mejorada para clientes de Windows.

> **Nota:**
>
> Para habilitar el registro de depuración, seleccione **Registros > Detallado** en la lista desplegable **Seleccionar nivel de registros**. Antes de la versión 23.4.1.5 del cliente Citrix Secure Access para Windows, el registro de depuración se podía habilitar mediante la casilla de verificación **Configuración > Habilitar registro de depuración**.

[CGOP-23537]

- **Soporte para enviar eventos al servicio Citrix Analytics**

  El cliente de Citrix Secure Access para Windows ahora admite el envío de eventos como la creación, el cierre de sesiones y la conexión de aplicaciones al servicio Citrix Analytics. A continuación, estos eventos se registran en el panel de control de Citrix Secure Private Access.

  [SPA-2197]

Problemas resueltos

- La autenticación de inicio de sesión único del cliente de Citrix Secure Access con la aplicación Citrix Workspace en el dispositivo de punto final de la nube no funciona para los usuarios de Unicode.

  [CGOP-22334]

- El acceso a los recursos falla cuando las aplicaciones basadas en nombres de host se configuran junto con el sufijo DNS en Citrix Secure Private Access.

  [SPA-4430]

- La conexión VPN siempre activa falla de forma intermitente al iniciarse debido a un problema de accesibilidad del servidor virtual de la puerta de enlace.

  [NSHELP-33500]

- No se puede acceder a los recursos de la intranet que se superpongan con un rango de direcciones IP falsificado si el túnel dividido está desactivado en el cliente de Citrix Secure Access.

  [NSHELP-34334]

- El cliente de Citrix Secure Access no carga el esquema de autenticación, lo que provoca un error de inicio de sesión en el servicio Citrix Secure Private Access.

  [SPAHELP-98]

23.1.1.11 (20 de febrero de 2023)

Esta versión aborda problemas que ayudan a mejorar el rendimiento y la estabilidad generales del servicio Citrix Secure Private Access.

23.1.1.8 (8 de febrero de 2023)

Problemas resueltos

- Los errores de resolución de DNS se producen cuando Citrix Secure Access no prioriza los paquetes IPv4 sobre los paquetes IPv6.

  [NSHELP-33617]

- Las reglas de filtrado del sistema operativo se capturan cuando el cliente de Citrix Secure Access se ejecuta en el modo Plataforma de filtrado de Windows (WFP).

  [NSHELP-33715]

- La dirección IP falsificada se utiliza para las aplicaciones de intranet basadas en IP cuando el cliente de Citrix Secure Access se ejecuta en el modo Citrix Deterministic Network Enhancer (DNE).

  [NSHELP-33722]

- Cuando se utiliza el controlador de la plataforma de filtrado de Windows (WFP), a veces el acceso a la intranet no funciona después de conectar la VPN de nuevo.

  [NSHELP-32978]

- El análisis de Endpoint Analysis (EPA) para comprobar la versión del sistema operativo no funciona en los escritorios multisesión de Windows 10 y Windows 11 Enterprise.

  [NSHELP-33534]

- El cliente de Windows admite un tamaño de archivo de configuración de 64 KB de forma predeterminada, y esto restringe a los usuarios agregar más entradas en el archivo de configuración. Este tamaño se puede aumentar estableciendo el valor de `ConfigSize`registro en HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Client. El tipo de clave del Registro `ConfigSize`es,`REG_DWORD` y los datos de la clave son.<`Bytes size`> Si el tamaño del archivo de configuración es mayor que el valor predeterminado (64 KB), el valor del Registro ConfigSize debe establecerse en 5 x 64 KB (después de convertirlo en bytes) por cada incorporación de 64 KB. Por ejemplo, si piensa agregar 64 KB más, debe establecer el valor del Registro en 64 x 1024 x 5 = 327680. Del mismo modo, si agrega 128 KB, debe establecer el valor del Registro en 64 x 1024 x (5+5) = 655360.

  [SPA-2865]

- Al cerrar sesión en la VPN, las entradas de la lista de sufijos DNS del Registro SearchList se vuelven a escribir en orden inverso, separadas por una o más comas.

  [NSHELP-33671]

- La autenticación del proxy falla cuando el dispositivo NetScaler completa un análisis de EPA en busca de antivirus.

  [NSHELP-30876]

- Si los valores del Registro relacionados con Citrix Secure Access superan los 1500 caracteres, el recopilador de registros no puede recopilar los registros de errores.

  [NSHELP-33457]

22.10.1.9 (08 de noviembre de 2022)

Novedades

- **Función EPA para la persistencia de sitios de tipo proxy de conexión en GSLB**

  El escaneo de EPA de Windows ahora admite la persistencia de sitios de tipo proxy de conexión en GSLB cuando el escaneo se inicie desde un explorador web. Anteriormente, el escaneo de EPA para Windows no admitía el tipo de persistencia del proxy de conexión para el escaneo EPA iniciado por el explorador web.

  [CGOP-21545]

- **Single Sign-On integrado para la URL de Workspace (solo en la nube)**

  El cliente de Citrix Secure Access ahora admite el inicio de sesión único para la URL de Workspace (solo en la nube) si el usuario ya ha iniciado sesión a través de la aplicación Citrix Workspace. Para obtener más información, consulte Compatibilidad con inicio de sesión único para la URL de Workspace para los usuarios que hayan iniciado sesión a través de la aplicación Citrix Workspace.

  [ACS-2427]

- **Administrar la versión del cliente de Citrix Secure Access o del plug-in de EPA mediante la aplicación Citrix Workspace (solo en la nube)**

  La aplicación Citrix Workspace ahora puede descargar e instalar la versión más reciente del plug-in de Citrix Secure Access o EPA a través del Global App Configuration Service. Para obtener más información, consulte Global App Configuration Service.

  [ACS-2426]

- **Mejora del control de registro de depuraciones**

El control del registro de depuraciones para el cliente de Citrix Secure Access ahora es independiente de NetScaler Gateway y se puede habilitar o inhabilitar desde la interfaz de usuario del complemento tanto para la máquina como para el túnel de usuario.

[NSHELP-31968]

- **Función para solicitudes preparatorias de acceso a redes privadas**

  El cliente de Citrix Secure Access para Windows ahora admite las solicitudes previas al acceso a redes privadas emitidas por el explorador web Chrome al acceder a recursos de redes privadas desde sitios web públicos.

  [CGOP-20544]

Problemas resueltos

- El cliente de Citrix Secure Access, versión 21.7.1.1 y posteriores, no puede actualizar a versiones posteriores para los usuarios sin privilegios administrativos.

  Esto solo se aplica si la actualización del cliente de Citrix Secure Access se realiza desde un dispositivo NetScaler. Para obtener más información, consulte Problema de actualización o reducción en el cliente de Citrix Secure Access.

  [NSHELP-32793]

- Los usuarios no pueden iniciar sesión en la VPN debido a fallas intermitentes de EPA.

  [NSHELP-32138]

- A veces, el cliente de Citrix Secure Access en modo solo túnel de máquinas no establece el túnel de máquina automáticamente después de que la máquina se active del modo de suspensión.

  [NSHELP-30110]

- En el modo Siempre en servicio, el túnel de usuario intenta iniciarse aunque solo esté configurado el túnel de la máquina.

  [NSHELP-31467]

- El enlace a la página de inicio de la interfaz de usuario de Citrix Secure Access no funciona si Microsoft Edge es el explorador web predeterminado.

  [NSHELP-31894]

- El mensaje personalizado de registro de errores de EPA no se muestra en el portal de NetScaler Gateway, sino que se muestra el mensaje "error interno".

  [NSHELP-31434]

- Cuando los usuarios hacen clic en la ficha Página principal de la pantalla de Citrix Secure Access para Windows, la página muestra el error de denegación de conexión.

  [NSHELP-32510]

- En algunos equipos cliente, el cliente de Citrix Secure Access no detecta la configuración del proxy y esto impide el inicio de sesión.

  [SPAHELP-73]

Problemas conocidos

- El escaneo de EPA basado en comprobaciones de Windows Update no funciona en la versión Windows 11 22H2. Para obtener más información, consulte Error de comprobación de EPA para Windows 11 22H2.

  [NSHELP-33068]

22.6.1.5 (17 de junio de 2022)

Novedades

- **Configuración de scripts de inicio y cierre de sesión**

  El cliente de Citrix Secure Access accede a la configuración del script de inicio y cierre de sesión desde los siguientes registros cuando el cliente de Citrix Secure Access se conecta al servicio en la nube de Citrix Secure Private Access.

  Ruta del Registro: **HKEY_LOCAL_MACHINE>SOFTWARE>Citrix > Secure Access Client**

  Valores del Registro:

  - SecureAccessLogInScript type REG_SZ: Ruta al script de inicio de sesión
  - SecureAccessLogOutScript type REG_SZ: Ruta al script de cierre de sesión

  [ACS-2776]

- **Cliente Citrix Secure Access para Windows que utiliza la plataforma de filtrado de Windows (WFP)**

  WFP es un conjunto de servicios de API y sistema que proporcionan una plataforma para crear aplicaciones de filtrado de red. WFP está diseñado para reemplazar las tecnologías de filtrado de paquetes anteriores, el filtro de especificación de interfaz de controlador de red (NDIS) que se utilizaba con el controlador DNE. Para obtener más información, consulte Cliente Citrix Secure Access para Windows mediante la plataforma de filtrado de Windows.

  [CGOP-19787]

- **Función de túnel dividido inverso basado en FQDN**

  El controlador de WFP ahora permite el uso de túneles divididos INVERSOS basados en FQDN. No se admite con el controlador DNE. Para obtener más información sobre el túnel dividido inverso, consulte Opciones de túnel dividido.

  [CGOP-16849]

Problemas resueltos

- A veces, el inicio de sesión automático de Windows no funciona cuando un usuario inicie sesión en la máquina de Windows en un modo de servicio Siempre activo. El túnel de máquina no pasa al túnel de usuario y se muestra el mensaje **Conectando** en la interfaz de usuario del plug-in VPN.

  [NSHELP-31357]

- Al cerrar la sesión de VPN, las entradas de la lista de sufijos DNS del registro SearchList (Equipo\HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Client) se escriben de nuevo en orden inverso, separadas por una o más comas.

  [NSHELP-31346]

- La dirección IP falsificada se utiliza incluso después de que la configuración de la aplicación de intranet de NetScaler cambie de una aplicación basada en FQDN a una basada en IP.

  [NSHELP-31236]

- La página principal de la puerta de enlace no se muestra inmediatamente después de que el plug-in de puerta de enlace establezca el túnel VPN correctamente.

  Con esta corrección, se introduce el siguiente valor del Registro.

  \HKLM\Software\Citrix\Secure Access Client\SecureChannelResetTimeoutSeconds

  Tipo: DWORD

  De forma predeterminada, este valor de Registro no se establece ni se agrega. Cuando el valor de “SecureChannelResetTimeoutSeconds”es 0 o no se agrega, la solución para gestionar la demora no funciona, que es el comportamiento predeterminado. El administrador debe configurar este Registro en el cliente para habilitar la corrección (es decir, mostrar la página de inicio inmediatamente después de que el plug-in de puerta de enlace establezca correctamente el túnel VPN).

  [NSHELP-30189]

- El Registro de la lista AlwaysOnAllow no funciona como se esperaba si el valor del registro es superior a 2000 bytes.

  [NSHELP-31836]

- El cliente Citrix Secure Access para Windows no canaliza las nuevas conexiones TCP al servidor TCP de fondo si la región del servicio Citrix Secure Private Access ya conectada deja de estar accesible. Sin embargo, esto no afecta a las conexiones de Gateway local.

  [ACS-2714]

22.3.1.5 (24 de marzo de 2022)

Problemas resueltos

- El nombre del plug-in EPA de Windows se revierte al plug-in EPA de NetScaler Gateway.

  [CGOP-21061]

Problemas conocidos

- El cliente Citrix Secure Access para Windows no canaliza las nuevas conexiones TCP al servidor TCP de fondo si la región del servicio Citrix Secure Private Access ya conectada deja de estar accesible. Sin embargo, esto no afecta a las conexiones de Gateway local.

  [ACS-2714]

22.3.1.4 (10-mar-2022)

Novedades

- **Aplique el acceso LAN local a los usuarios finales en función de la configuración de ADC**

  Los administradores pueden impedir que los usuarios finales inhabiliten la opción de acceso LAN local en sus máquinas cliente. Se agrega una nueva opción, FORCED a los valores de los parámetros de acceso LAN local existentes. Cuando el valor de acceso LAN local se establece en FORCED, el acceso LAN local siempre está habilitado para los usuarios finales en las máquinas cliente. Los usuarios finales no pueden inhabilitar la configuración de la LAN local mediante la interfaz de usuario del cliente de Citrix Secure Access. Si los administradores desean ofrecer una opción para habilitar o inhabilitar el acceso LAN local al usuario final, deben volver a configurar el parámetro Acceso LAN local en ON.

  Para habilitar la opción **FORZADO** mediante la interfaz gráfica de usuario:

  1. Vaya a **NetScaler Gateway > Configuración global > Cambiar configuración global**.
  2. Haga clic en la ficha **Experiencia del cliente** y, a continuación, en **Configuración avanzada**.
  3. En **Acceso LAN local**, seleccione **FORZADO**.

Para habilitar la opción **FORCED** mediante la CLI, ejecute el siguiente comando:

```
set vpn parameter -localLanAccess FORCED
<!--NeedCopy-->
```

[CGOP-19935]

- **Compatibilidad con Windows server 2019 y 2022 en el escaneo del sistema operativo de EPA**

  La exploración del SO de EPA ahora es compatible con Windows Server 2019 y 2022

  Puede seleccionar los nuevos servidores mediante la interfaz gráfica de usuario.

  1. Vaya a **NetScaler Gateway > Directivas > Autenticación previa**.
  2. Cree una directiva de autenticación previa o modifique una directiva existente.
  3. Haga clic en el enlace **Editor de EPA OPSWAT**.
  4. En el **Editor de expresiones**, seleccione **Windows > Windows Update** y haga clic en el icono **+**.
  5. En **Nombre del sistema operativo**, seleccione el servidor según sus requisitos.

  Puede actualizar a la versión 4.3.2744.0 de OPSWAT para usar el servidor Windows 2019 y 2022 en el análisis del sistema operativo de EPA.

  [CGOP-20061]

- **Nuevos tipos de clasificación de escaneo EPA para parches de seguridad faltantes**

  Los siguientes tipos de clasificación nuevos se agregan a la exploración de EPA para detectar parches de seguridad faltantes. La exploración de EPA falla si el cliente tiene alguno de los siguientes parches de seguridad faltantes.

  - Aplicación
  - Conectores
  - CriticalUpdates
  - DefinitionUpdates
  - DeveloperKits
  - FeaturePacks
  - Guidance
  - SecurityUpdates
  - ServicePacks
  - Herramientas
  - UpdateRollups
  - Actualizaciones

  Puede configurar los tipos de clasificación mediante la interfaz gráfica de usuario.

1. Vaya a **NetScaler Gateway > Directivas > Autenticación previa**.
2. Cree una directiva de autenticación previa o modifique una directiva 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 faltar un parche del siguiente tipo de clasificación de actualización de Windows**, seleccione el tipo de clasificación para los parches de seguridad que faltan
6. Haga clic en **Aceptar**.

Puede actualizar a la versión 4.3.2744.0 de OPSWAT para usar estas opciones.

- Para obtener información sobre los GUID de clasificación de los servicios de actualización del servidor de Windows, https://docs.microsoft.com/en-us/previous-versions/windows/desktop/ff357803(v=vs.85)
- Para obtener una descripción de la terminología de actualizaciones de software de Microsoft, consulte https://docs.microsoft.com/en-us/troubleshoot/windows-client/deployment/standard-terminology-software-updates

Anteriormente, las exploraciones de EPA para detectar parches de seguridad faltantes se realizaban en los niveles de gravedad; Crítico, Importante, Moderado y Bajo en el cliente Windows.

[CGOP-19465]

- **Soporte para certificados de dispositivos múltiples para escaneo de EPA**

  En la configuración Always on VPN, si se configuran varios certificados de dispositivo, se intenta el certificado con la fecha de caducidad más larga para la conexión VPN. Si este certificado permite el escaneo de EPA correctamente, se establece una conexión VPN. Si este certificado falla en el proceso de escaneo, se usa el siguiente certificado. Este proceso continúa hasta que se prueban todos los certificados.

  Anteriormente, si se configuraban varios certificados válidos, si la exploración de EPA fallaba para un certificado, la exploración no se intentaba en los demás certificados.

  [CGOP-19782]

Problemas resueltos

- Si el parámetro clientCert se establece en "Opcional"en el perfil SSL al configurar el servidor virtual de VPN, se les pide a los usuarios que seleccionen la tarjeta inteligente varias veces.

  [NSHELP-30070]

- Los usuarios no pueden conectarse al dispositivo NetScaler Gateway después de cambiar el parámetro "networkAccessOnVPNFailure"siempre en el perfil de "fullAccess"a "onlyToGateway".

[NSHELP-30236]

- Cuando se configura AlwaysOn, se produce un error en el túnel de usuario debido al número de versión incorrecto (1.1.1.1) en el archivo aoservice.exe.

  [NSHELP-30662]

- La resolución de DNS a recursos internos y externos deja de funcionar durante una sesión de VPN prolongada.

  [NSHELP-30458]

- El cliente VPN de Windows no respeta la alerta de "notificación de cierre SSL"del servidor y envía la solicitud de inicio de sesión de transferencia en la misma conexión.

  [NSHELP-29675]

- Comprobación de EPA del registro para "=="y "! ="falla en algunas entradas del registro.

  [NSHELP-29582]

22.2.1.103 (17-feb-2022)

Problemas resueltos

- Los usuarios no pueden iniciar el plug-in de EPA ni el plug-in de VPN después de actualizar a las versiones del explorador Chrome 98 o Edge 98. Para solucionar este problema, lleve a cabo lo siguiente:

  1. Para la actualización del plug-in de VPN, los usuarios finales deben conectarse mediante el cliente VPN por primera vez para obtener la solución en sus máquinas. En los intentos de inicio de sesión posteriores, los usuarios pueden elegir el explorador o el plug-in para conectarse.
  2. Para el caso de uso exclusivo de EPA, los usuarios finales no tendrán el cliente VPN para conectarse a la puerta de enlace. En este caso, lleve a cabo lo siguiente:

     a) Conéctese a la puerta de enlace mediante un explorador.
     b) Espere a que aparezca la página de descarga y descargue el archivo nsepa_setup.exe.
     c) Después de la descarga, cierre el explorador e instale el archivo nsepa_setup.exe.
     d) Reinicie el cliente.

  [NSHELP-30641]

21.12.1.4 (17-dic-2021)

Novedades

- **Cambios de cambio de marca**

  El plug-in de NetScaler Gateway para Windows pasa a llamarse cliente de Citrix Secure Access.

  [ACS-2044]

- **Compatibilidad con aplicaciones privadas TCP/HTTP (S)**

  El cliente de Citrix Secure Access ahora admite aplicaciones privadas TCP/HTTP(S) para usuarios remotos a través de Citrix Workspace Secure Access Service.

  [ACS-870]

- **Más idiomas disponibles**

  Los plug-ins de Windows VPN y EPA para NetScaler Gateway ahora admiten los siguientes idiomas:

  - Coreano
  - Ruso
  - Chino tradicional

  [CGOP-17721]

- **Soporte de Citrix Secure Access para Windows 11**

  El cliente de Citrix Secure Access ahora es compatible con Windows 11.

  [CGOP-18923]

- **Inicio de sesión de transferencia automática cuando el usuario inicie sesión desde la misma máquina y se configura Always on**

  La transferencia de inicio de sesión automática ahora se produce sin la intervención del usuario cuando Always on está configurado y el usuario inicie sesión desde el mismo equipo. Anteriormente, cuando el cliente (usuario) tenía que volver a iniciar sesión en casos como el reinicio del sistema o los problemas de conectividad de red, aparecía un mensaje emergente. El usuario tuvo que confirmar el inicio de sesión de la transferencia. Con esta mejora, la ventana emergente se desactiva.

  [CGOP-14616]

- **Derivación de la dirección IP de puerta de enlace predeterminada de Citrix Virtual Adapter a partir de la máscara de red de NetScaler**

  La dirección IP de la puerta de enlace predeterminada de Citrix Virtual Adapter ahora se deriva de la máscara de red proporcionada por NetScaler.

[CGOP-18487]

Problemas resueltos

- A veces, los usuarios pierden el acceso a Internet después de que se establece un túnel VPN en modo activado de túnel dividido. La ruta predeterminada errónea del adaptador Citrix Virtual provoca este problema de red.

  [NSHELP-26779]

- Cuando el túnel dividido se establece en "Invertir", se produce un error en la resolución de DNS para los dominios de intranet.

  [NSHELP-29371]

21.9.100.1 (30 dic-2021)

Novedades

- **Soporte de Citrix Secure Access para Windows 11**

  El cliente de Citrix Secure Access ahora es compatible con Windows 11.

  [CGOP-18923]

Problemas resueltos

- A veces, los usuarios pierden el acceso a Internet después de que se establece un túnel VPN en modo activado de túnel dividido. La ruta predeterminada errónea del adaptador Citrix Virtual provoca este problema de red.

  [NSHELP-26779]

- Cuando el túnel dividido se establece en "Invertir", se produce un error en la resolución de DNS para los dominios de intranet.

  [NSHELP-29371]

21.9.1.2 (04-oct-2021)

Problemas resueltos

- A veces, después de desconectar la VPN, el solucionador de DNS no resuelve los nombres de host porque los sufijos DNS se eliminan durante la desconexión de la VPN.

[NSHELP-28848]

- A veces, se desactiva la sesión de un usuario en NetScaler Gateway en unos segundos cuando se establece el tiempo de espera por inactividad del cliente.

  [NSHELP-28404]

- Es posible que el plug-in de Windows se bloquee durante la autenticación.

  [NSHELP-28394]

- En el modo de servicio Always On, el plug-in VPN para Windows no establece automáticamente el túnel de usuarios después de que los usuarios inicien sesión en sus equipos Windows.

  [NSHELP-27944]

- Tras el establecimiento del túnel, en lugar de agregar rutas del servidor DNS con la dirección IP de la puerta de enlace anterior, el plug-in de Windows agrega las rutas con la dirección de puerta de enlace predeterminada.

  [NSHELP-27850]

V21.7.1.1 (27 de agosto de 2021)

Novedades

- **Escaneo de nueva dirección MAC**

  Se agrega soporte para nuevos escaneos de direcciones MAC.

  [CGOP-16842]

- **Análisis de EPA para comprobar el sistema operativo Windows y su versión de compilación**

  Agregado análisis EPA para comprobar el sistema operativo Windows y su versión de compilación.

  [CGOP-15770]

- **Escaneo de EPA para comprobar la existencia de un valor determinado**

  Un nuevo método en el análisis EPA del registro comprueba ahora la existencia de un valor determinado.

  [CGOP-10123]

Problemas resueltos

- Si se produce un error de JavaScript durante el inicio de sesión debido a un error de red, los intentos de inicio de sesión posteriores fallan con el mismo error de JavaScript.

[NSHELP-27912]

- El análisis de EPA falla en la comprobación de la hora de la última actualización del antivirus McAfee.

  [NSHELP-26973]

- A veces, los usuarios pierden el acceso a Internet después de establecer un túnel VPN.

  [NSHELP-26779]

- Es posible que se muestre un error de script para el plug-in VPN durante la autenticación nFactor.

  [NSHELP-26775]

- Si se produce una interrupción de la red, el flujo de tráfico UDP que se inició antes de la interrupción de la red no disminuye hasta 5 minutos.

  [NSHELP-26577]

- Es posible que experimente un retraso en el inicio del túnel VPN si el registro de DNS tarda más de lo esperado.

  [NSHELP-26066]

V21.3.1.2 (31 de marzo de 2021)

Novedades

- **Bibliotecas EPA actualizadas**

  Las bibliotecas de EPA se actualizan para admitir la última versión de las aplicaciones de software utilizadas en los escaneos de EPA.

  [NSHELP-26274]

- **Compatibilidad con el adaptador virtual de NetScaler Gateway**

  El adaptador virtual NetScaler Gateway ahora es compatible con los adaptadores virtuales directos Hyper-V y Microsoft Wi-Fi (utilizados con impresoras).

  [NSHELP-26366]

Problemas resueltos

- El plug-in de puerta de enlace VPN de Windows bloquea el uso de “CTRL + P”y “CTRL + O”en el túnel VPN.

  [NSHELP-26602]

- El plug-in de NetScaler Gateway para Windows solo responde con una dirección IP de intranet registrada en Active Directory cuando se solicita una acción `"nslookup"` para el nombre de la máquina.

  [NSHELP-26563]

- El registro y cancelación de IIP fallan de forma intermitente si el DNS dividido se establece como "Local" o "Ambos".

  [NSHELP-26483]

- El inicio de sesión automático en el plug-in de puerta de enlace VPN de Windows falla si está configurado Always On.

  [NSHELP-26297]

- El plug-in de puerta de enlace VPN de Windows no descarta los paquetes DNS IPv6, lo que da lugar a problemas con la resolución de DNS.

  [NSHELP-25684]

- El plug-in de puerta de enlace de VPN de Windows mantiene la lista de excepciones de proxy existente incluso si la lista se desborda debido al límite del explorador en la lista de excepciones de proxy de Internet Explorer.

  [NSHELP-25578]

- El plug-in de puerta de enlace VPN de Windows no restaura la configuración del proxy cuando el cliente VPN se desconecta en modo Siempre activado.

  [NSHELP-25537]

- El plug-in VPN para Windows no establece el túnel después de iniciar sesión en Windows si se cumplen las siguientes condiciones:

  - El dispositivo NetScaler Gateway está configurado para la función Siempre activado.
  - El dispositivo está configurado para la autenticación basada en certificados con la autenticación de dos factores "desactivada".

  [NSHELP-23584]

Compatibilidad con Microsoft Edge WebView para Citrix Secure Access de Windows: Tech Preview

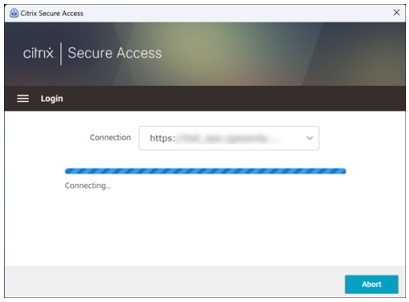
March 27, 2024

Microsoft Edge WebView es ahora el WebView recomendado por Microsoft porque Internet Explorer WebView está obsoleto. Le recomendamos que utilice el cliente Citrix Secure Access 23.8.1.5 o versiones posteriores para aprovechar las funcionalidades de Microsoft Edge WebView.

Actualmente, Microsoft Edge WebView está inhabilitado de forma predeterminada. Puede registrarte para la vista previa mediante https://podio.com/webforms/28291989/2245437.

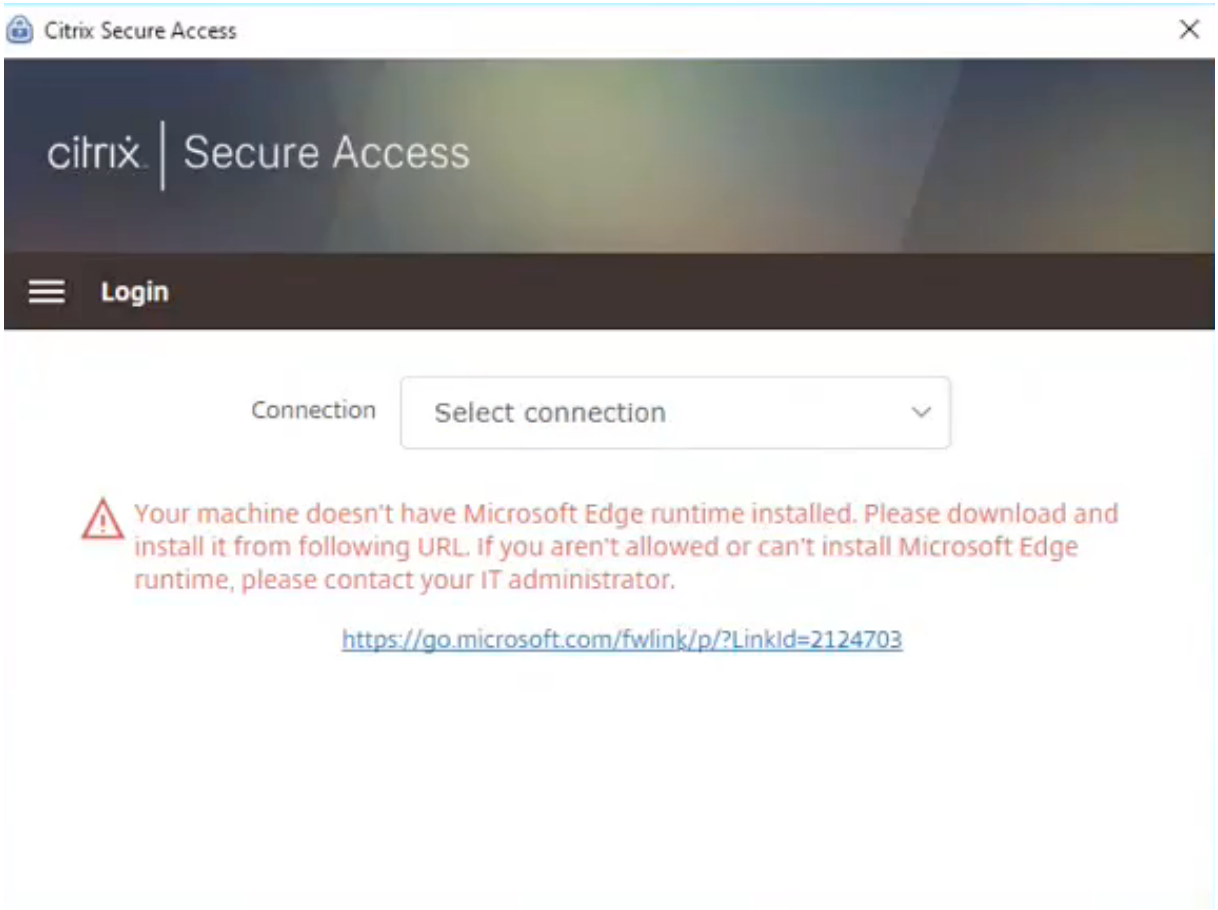
Cambios en el usuario final

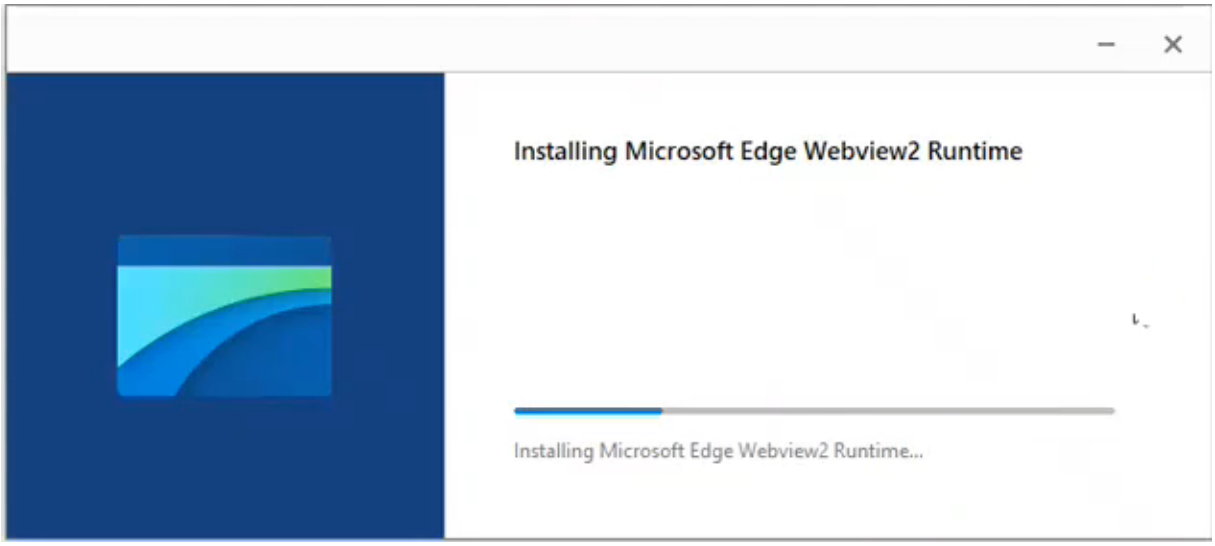
Las pantallas de autenticación de la interfaz de usuario del cliente Citrix Secure Access aparecen de la siguiente manera.



Una vez que los usuarios finales seleccionan la URL, el cliente Citrix Secure Access abre una nueva ventana en la que se les pide que inicien sesión en NetScaler Gateway con sus credenciales.

Si la máquina cliente de Windows no tiene instalado el tiempo de ejecución de Microsoft Edge WebView, los usuarios finales reciben un enlace en la interfaz de usuario del cliente de Citrix Secure Access para descargar e instalar el tiempo de ejecución de Microsoft Edge WebView. Los usuarios finales pueden descargar e instalar el motor de ejecución de Edge WebView sin problemas cuando están conectados a la VPN y la autenticación no se interrumpe durante este proceso.





Notas:

- La funcionalidad de Microsoft Edge WebView no afecta a ninguna configuración específica del administrador.
- Le recomendamos que habilite la función de cookies HttpOnly cuando utilice Edge Web-

> View en Citrix Secure Access. Esto mejora la duración del inicio de sesión de NetScaler Gateway cuando se usa EPA como factor en el flujo de nfactor.

Solución de problemas

- Si tiene algún problema con esta función, contacte con Citrix Support.
- Puede enviar sus comentarios sobre la función Edge WebView a través de citrixgatewaybetafeedback@cloud.com.

Recopilación de registros mejorada para el cliente de Windows

March 27, 2024

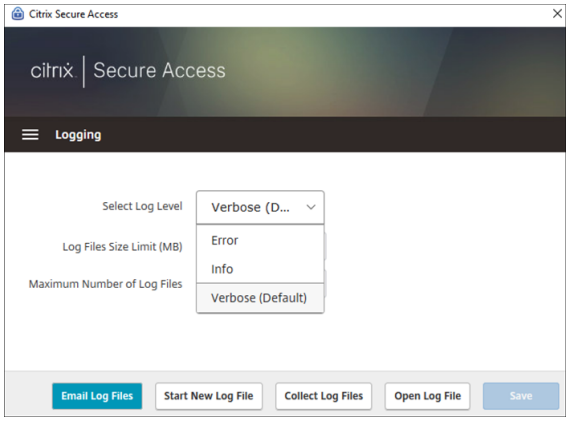
La función de registro del cliente Windows Secure Access se ha mejorado con una recopilación y depuración de registros mejoradas. Los nuevos archivos de registros llevan el prefijo "csa_".

A partir del cliente Citrix Secure Access para Windows 23.10.1.7, el nivel de registro predeterminado se establece en Verbose para mejorar la recopilación de registros y la solución de problemas.

Con estos cambios, los administradores y los usuarios finales pueden recopilar registros de la sesión actual y de las sesiones pasadas. Anteriormente, la recopilación de registros se limitaba únicamente a las sesiones actuales.

Configurar el registro mediante la interfaz de usuario del cliente Citrix Secure Access

1. Instale el cliente Secure Access para Windows.
2. En el menú, haga clic en **Registro**. Toda la configuración relacionada con los registros se puede realizar en la pantalla de registro.



- **Seleccione el nivel de registro:**

  Cuando se habilita el nuevo mecanismo de registro, están disponibles los tres niveles de registro siguientes.

  - Error: solo se registran las excepciones o los errores notificados por la aplicación.
  - Información: este nivel incluye mensajes informativos y eventos relacionados con la ejecución del programa. También incluye errores y excepciones.
  - Detalle (predeterminado): este nivel incluye todos los mensajes de registro informados por los niveles de registro de errores e información, así como los mensajes adicionales que pueden ayudar a solucionar problemas.

- **Límite de tamaño del archivo de registros:** (obligatorio) Introduzca el tamaño del archivo de registros de cada archivo de registros. El valor máximo es de 600 MB.
- **Número máximo de archivos de registros:** (Obligatorio) Introduzca el número de archivos que quiere agregar para la recopilación de registros. El valor máximo es 5.
- **Archivos de registro** de correo electrónico: envíe los archivos de registros por correo electrónico al ID de correo electrónico registrado.
- **Iniciar nuevo archivo**de registro: al seleccionar esta opción, se crea un nuevo archivo de registro.
- **Recopilar archivos de registros** : haga clic para crear un archivo zip con todos los archivos de registros de la aplicación. Este archivo zip se guarda en el escritorio del cliente.
- **Abrir archivos**de registro : al seleccionar esta opción, se abre el archivo más reciente`csa_nssslvpn*.txt`.

Cliente de Citrix Secure Access para Linux

March 27, 2024

El cliente Citrix Secure Access para Linux es un software de cliente VPN administrado por NetScaler Gateway que permite a los usuarios acceder a los datos y aplicaciones corporativos de forma remota. El cliente Citrix Secure Access protege las aplicaciones contra el acceso no autorizado, las amenazas al nivel de aplicación y los ataques por explorador web.

El cliente de Citrix End Point Analysis (EPA) es un software cliente administrado por NetScaler Gateway. Comprueba los criterios de los dispositivos de punto final antes de conceder el acceso a datos corporativos a través de NetScaler Gateway. El cliente de Citrix EPA y el cliente de Citrix Secure Access son independientes.

> **Nota:**
>
> Incluso si no usa EPA, le recomendamos que actualice los archivos binarios de los complementos de EPA y de la VPN juntos en caso de que decida utilizar la funcionalidad de EPA más adelante.

Versiones de Linux compatibles

El cliente Citrix Secure Access y el cliente Citrix EPA son compatibles con las versiones de Ubuntu 18.04, Ubuntu 20.04 y Ubuntu 22.04. Para obtener más información sobre los exploradores web compatibles, consulte Requisitos del software del cliente.

> **Nota:**
>
> Para que Ubuntu 22.04 funcione con el cliente Citrix Secure Access y el cliente Citrix EPA, establezca el parámetro SSL `denySSLReneg` en `NONSECURE` en la CLI de NetScaler.

Funcionalidades admitidas

El cliente Citrix Secure Access para Ubuntu admite las siguientes funciones:

- Tunelización dividida y tunelización dividida inversa
- Tunelización de aplicaciones TCP, UDP e ICMP
- Conexiones iniciadas por el servidor a través de IP de Intranet (IIP)
- DNS REMOTE dividido
- Proxy del lado del cliente
- Escaneos clásicos de EPA
- Autenticación avanzada (nFactor) que incluye escaneos avanzados de EPA (solo desde el explorador web)
- Cookies de HTTPOnly
- Equilibrio de carga de servidor global (GSLB)

> **Nota:**
>
> El cliente Citrix Secure Access para Ubuntu no admite la división de DNS BOTH.

Actualizar la versión de los clientes de Ubuntu en NetScaler Gateway

Puede descargar el cliente Citrix Secure Access y el cliente Citrix EPA para Ubuntu desde la página de descargas.

El cliente Citrix Secure Access y el cliente Citrix EPA se denominan "nsgclient18_64.deb"y "nsepa18.deb", respectivamente. Los clientes son compatibles con Ubuntu 18.04 y 20.04.

Los clientes Citrix Secure Access y Citrix EPA que admiten Ubuntu 22.04 se denominan “nsginstaller64.deb”y “nsepa.deb”, respectivamente.

Si desea actualizar a la versión más reciente del cliente Citrix Secure Access de la versión 1.0.0.x a la versión 23.6.1, por ejemplo:

1. Sustituya los archivos “nsgclient18_64.deb”y “nsginstaller64.deb”en la ubicación /var/netscaler/gui/vpn/scripts/linux/ mediante el indicador del shell.
2. Sustituya los archivos “nsepa18.deb”y “nsepa.deb”en la ubicación /var/netscaler/gui/epa/scripts/linux/ mediante el indicador del shell.
3. Abra el/var/netscaler/gui/vpn/scripts/linux/clientversions.xml archivo.

    a) Para el cliente Citrix EPA, sustituya la versión actual (1.0.0.x) de las siguientes etiquetas XML por la versión más reciente (23.6.1). Si las etiquetas XML no existen, agréguelas al archivo XML. Por ejemplo,

    replace

    ```
    <component pkgname="nsepa18"currentversion="1.0.0.x"minversion
    ="1.0.0.x"ostype="ubuntu64"minkernelversion="0"maxkernelversion
    ="100"updatetype="compatible"action="/epa/scripts/linux/
    nsepa18.deb"/>
    ```

    with

    ```
    <component pkgname="nsepa18"currentversion="23.6.1"minversion
    ="23.6.1"ostype="ubuntu64"minkernelversion="0"maxkernelversion
    ="100"updatetype="compatible"action="/epa/scripts/linux/
    nsepa18.deb"/>
    ```

    and replace

    ```
    <component pkgname="nsepa22"currentversion="1.0.0.x"minversion
    ="1.0.0.x"ostype="ubuntu64"minkernelversion="0"maxkernelversion
    ="100"updatetype="compatible"action="/epa/scripts/linux/nsepa
    .deb"/>
    ```

    with

    ```
    <component pkgname="nsepa22"currentversion="23.6.1"minversion
    ="23.6.1"ostype="ubuntu64"minkernelversion="0"maxkernelversion
    ="100"updatetype="compatible"action="/epa/scripts/linux/nsepa
    .deb"/>
    ```


b) Para el cliente Citrix Secure Access, sustituya la versión actual (1.0.0.x) de las siguientes etiquetas XML por la versión más reciente (23.6.1). Si las etiquetas XML no existen, agréguelas al archivo XML. Por ejemplo,

replace

```
<component pkgname="nsgclient18"currentversion="1.0.0.x"
minversion="1.0.0.x"ostype="ubuntu64"minkernelversion="3.0
"maxkernelversion="5.16"updatetype="compatible"action="/vpn/
scripts/linux/nsgclient18_64.deb"/>
```

to

```
<component pkgname="nsgclient18"currentversion="23.6.1"minversion
="23.6.1"ostype="ubuntu64"minkernelversion="3.0"maxkernelversion
="5.16"updatetype="compatible"action="/vpn/scripts/linux/
nsgclient18_64.deb"/>
```

y

```
<component pkgname="nsgclient22"currentversion="1.0.0.x"
minversion="1.0.0.x"ostype="ubuntu64"minkernelversion="3.0
"maxkernelversion="5.20"updatetype="compatible"action="/vpn/
scripts/linux/nsginstaller64.deb"/>
```

to

```
<component pkgname="nsgclient22"currentversion="23.6.1"minversion
="23.6.1"ostype="ubuntu64"minkernelversion="3.0"maxkernelversion
="5.20"updatetype="compatible"action="/vpn/scripts/linux/
nsginstaller64.deb"/>
```

4. En la línea de comandos del shell de NetScaler, ejecute los siguientes comandos:

```
rm -rf /netscaler/ns_gui
ln -s /var/netscaler/gui /netscaler/ns_gui
```

5. En la CLI de NetScaler, ejecute los siguientes comandos:

```
set vpn parameter -clientversions all
flush cache contentgroup loginstaticobjects
```

Referencias

- Clientes VPN de NetScaler Gateway y funciones compatibles
- Análisis de endpoint Analysis compatibles con Ubuntu
- Documentación de ayuda para el usuario final

Notas de la versión de Citrix Secure Access para Linux

March 27, 2024

Ahora, el cliente Citrix Secure Access y el cliente Citrix End Point Analysis (EPA) para Linux se inician de forma independiente y son compatibles con todas las versiones de NetScaler. La versión del cliente de Citrix Secure Access sigue el formato YY.MM Release.Build.

Las notas de la versión describen las nuevas funciones, las mejoras de las funciones existentes, los problemas resueltos y los problemas conocidos.

Novedades: Las nuevas funciones y mejoras disponibles en la versión actual.

Problemasresueltos : los problemas que se han corregido en la versión actual.

Problemasconocidos : los problemas que existen en la versión actual y sus soluciones alternativas, cuando proceda.

Para obtener información detallada sobre las funciones admitidas, consulte Documentación del producto NetScaler Gateway.

23.10.3 (16 de octubre de 2023)

Problemas resueltos

Para los usuarios franceses, la página Conexiones de la interfaz de usuario de Citrix Secure Access para Linux muestra la velocidad de transferencia de datos en KB y MB en lugar de en Ko y Mo, respectivamente.

[NSOSLX-177]

23.9.1 (08-Sep-2023)

Novedades

En esta versión se han resuelto una serie de problemas para mejorar la estabilidad y el rendimiento generales.

[CGOP-25231]

23.6.2 (20 de junio de 2023)

Novedades

- **Compatibilidad de Ubuntu 22.04 con el cliente Citrix Secure Access y el cliente Citrix EPA**

  Ubuntu 22.04 es la última versión de soporte a largo plazo de Ubuntu. Los clientes Citrix Secure Access y Citrix EPA son compatibles con Ubuntu 22.04. Para obtener más información, consulte Requisitos del software del cliente.

  [CGOP-24312]

- **Compatibilidad con GSLB para clientes de Citrix Secure Access y Citrix EPA**

  El cliente Citrix Secure Access y el cliente Citrix EPA para Ubuntu admiten la función de equilibrio de carga global de servidores (GSLB) de NetScaler Gateway. Al configurar GSLB para NetScaler Gateway, los administradores pueden garantizar que la red empresarial (recursos de intranet) esté siempre disponible para los usuarios finales desde cualquier ubicación geográfica. El GSLB también aborda situaciones de desastre o interrupciones de la red en las que los usuarios de un centro de datos pueden ser redirigidos a otro centro de datos. Para obtener más información, consulte Compatibilidad con implementaciones de GSLB activo-activo en NetScaler Gateway.

  [CGOP-23506]

- **Compatibilidad con HTTPOnly para clientes Citrix Secure Access y Citrix EPA**

  Los clientes Citrix Secure Access y Citrix EPA admiten el indicador HTTPOnly en las cookies de autenticación. Los administradores de NetScaler Gateway configuran la función HTTPOnly en las cookies de autenticación que generan las aplicaciones web. Esta función ayuda a prevenir el robo de cookies debido a la creación de scripts entre sitios. Para obtener más información, consulte Aplicar el indicador HttpOnly en las cookies de autenticación.

  [CGOP-23517]