NetScaler Gateway 14.1

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

Contents

NetScaler Gateway 发行说明 41
关于 NetScaler Gateway 42
NetScaler Gateway 体系结构 43
用户连接的工作方式 44
使用 Citrix Secure Access 客户端连接 44
使用 Citrix Workspace 应用程序连接 46
使用 iOS 和 Android 设备连接 46
常见的 NetScaler Gateway 部署 47
在 DMZ 中部署 NetScaler Gateway 47
DMZ 中的 NetScaler Gateway 连接 48
在安全网络中部署 NetScaler Gateway 48
客户端软件要求 50
Citrix Secure Access™ 客户端系统要求 50
端点分析要求 51
NetScaler Gateway 与 Citrix® 产品的兼容性 53
Citrix 产品和支持的版本 53
Citrix Workspace 应用程序、Citrix 移动生产力应用程序和插件 53
NetScaler Gateway 许可 55
NetScaler Gateway 许可证类型 55
平台许可证 56
通用许可证 56
获取通用许可证 57
安装通用许可证 57
验证通用许可证的安装 58
相关资源 58
在 NetScaler Gateway 上安装许可证 58

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

设置最大用户数 59
验证通用许可证安装 59
通过使用 GUI 验证通用许可证的安装 59
通过使用 CLI 验证通用许可证的安装 59
NetScaler Gateway 许可常见问题 60
如何获得试用或演示许可证的帮助? 60
如何安装许可证? 60
Gateway 许可证有哪些不同类型? 60
支持多少并发用户会话? 60
如何检查当前已许可的并发用户会话? 60
如何检查是否达到许可的吞吐量限制? 60
如何检查在达到许可吞吐量时是否丢弃了数据包? 61
如何查找 NetScaler 设备许可的吞吐量是多少? 61
如何向现有网关许可证添加更多用户? 61
开始之前 62
安装 NetScaler Gateway 的先决条件 63
安全规划 63
配置安全证书管理 63
身份验证支持 64
保护您的 NetScaler Gateway 部署 64
Gateway 预安装清单 65
用户设备 65
NetScaler Gateway 基本网络连接 65
可通过 NetScaler Gateway 访问的内部网络 66
高可用性 66
身份验证和授权 66
LDAP 身份验证 66
RADIUS 身份验证和授权 67

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

SAML 身份验证 67
通过防火墙打开端口（单跳 DMZ） 68
在非安全网络和 DMZ 之间的防火墙上 68
在安全网络之间的防火墙上 68
Citrix 虚拟桌面™、Citrix 虚拟应用或 StoreFront 68
Citrix 端点管理™ 69
采用 Citrix Virtual Apps™ 的双跳 DMZ 部署 69
第一个 DMZ 中的 NetScaler Gateway 69
第二个 DMZ 中的 NetScaler Gateway 69
安装和配置 NetScaler Gateway 设备 71
使用向导配置 NetScaler Gateway 设备 71
首次设置向导 71
使用首次设置向导配置 NetScaler Gateway 72
快速配置向导 72
使用快速配置向导配置设置 73
NetScaler Gateway 向导 77
使用 NetScaler Gateway 向导配置设置 77
安装向导 77
已发布应用程序向导 78
集成式 Citrix Endpoint Management 配置 78
配置 NetScaler Gateway 78
使用配置实用程序 79
登录配置实用程序 79
创建虚拟服务器 80
创建虚拟服务器 81
HTTP QUIC VPN 虚拟服务器 81
将网络配置文件绑定到 VPN 虚拟服务器时的注意事项 83
虚拟服务器上的当前用户和总连接用户 84

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

配置虚拟服务器上的连接类型 85

为通配符虚拟服务器配置侦听策略 85

在 NetScaler Gateway 上配置 IP 地址 87

NetScaler Gateway 如何使用 IP 地址 87

子网 IP 地址 88

为用户连接配置 IPv6 88

解析位于安全网络中的 DNS 服务器 89

配置 DNS 服务和 DNS 监视器 89

将 DNS 服务绑定到 DNS 虚拟服务器 90

配置 DNS 虚拟服务器 90

配置 DNS 虚拟服务器 90

配置名称服务提供程序 91

将 DNS 服务器添加到 NetScaler Gateway 91

将 WINS 服务器添加到 NetScaler Gateway 91

指定名称查找优先级 91

配置服务器发起的连接 92

配置服务器发起连接的私有端口范围 93

在 NetScaler Gateway 上配置路由 93

配置静态路由 94

配置自动协商 94

启用或禁用自动协商 95

在 NetScaler Gateway 上配置主机名和 FQDN 95

查看证书的 FQDN 95

NetScaler Gateway 上的策略和配置文件 95

策略的工作原理 95

条件策略 96

策略的优先级 97

在 NetScaler Gateway 上创建策略 97

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

配置系统表达式 97
配置客户端安全表达式 98
NetScaler Gateway 上的证书管理 98
创建证书签名请求 99
使用 NetScaler Gateway 向导创建 CSR 99
使用 NetScaler GUI 创建 CSR 99
在 NetScaler Gateway 上安装签名证书 100
配置中间证书 101
安装中间证书 103
将中间证书链接到服务器证书 103
使用设备证书进行身份验证 103
配置设备证书的步骤 104
为经典 EPA 策略在虚拟服务器上启用设备证书检查 105
在 Windows 计算机上验证设备证书 105
导入并安装现有证书 106
在 NetScaler Gateway 上安装证书和私钥 106
将证书从 PFX 格式转换为 PEM 格式 107
`OpenSSL utility` 109
证书吊销列表 110
CRL 刷新参数 111
使用 OCSP 监控证书状态 114
配置 OCSP 证书状态 114
NetScaler Gateway 上的证书管理 115
创建证书签名请求 116
使用 NetScaler Gateway 向导创建 CSR 117
使用 NetScaler GUI 创建 CSR 117
在 NetScaler Gateway 上安装签名证书 117
配置中间证书 118

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

安装中间证书 120
将中间证书链接到服务器证书 120
使用设备证书进行身份验证 121
配置设备证书的步骤 121
为经典 EPA 策略在虚拟服务器上启用设备证书检查 122
在 Windows 计算机上验证设备证书 123
导入并安装现有证书 123
在 NetScaler Gateway 上安装证书和私钥 123
证书吊销列表 124
CRL 刷新参数 126
使用 OCSP 监控证书状态 128
配置 OCSP 证书状态 129
管理 NetScaler Gateway 配置设置 130
保存 NetScaler Gateway 配置 130
在 NetScaler Gateway 上保存配置 130
在 NetScaler Gateway 上查看和保存配置文件 131
查看当前运行配置 131
比较已保存配置和运行配置 131
清除 NetScaler Gateway 配置 131
清除 NetScaler Gateway 配置设置 132
测试您的 NetScaler Gateway 配置 132
使用 GUI 创建用户帐户 133
升级 NetScaler Gateway 软件 134
检查软件更新 134
使用升级向导升级 NetScaler Gateway 134
使用命令提示符升级 NetScaler Gateway 135
在双跳 DMZ 中部署 NetScaler Gateway 136
双跳部署的工作原理 136

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

准备双跳 DMZ 部署 137
开始部署所需的组件 138
双跳 DMZ 部署中的通信流 138
连接过程 139
在双跳 DMZ 中安装和配置 NetScaler Gateway 141
在第一个 DMZ 中安装 NetScaler Gateway 142
在第一个 DMZ 中配置 NetScaler Gateway 142
在第二个 DMZ 中安装 NetScaler Gateway 142
在 NetScaler Gateway 代理上的虚拟服务器上配置设置 142
使用 GUI 在 NetScaler Gateway 代理上的虚拟服务器上启用双跳 143
使用 GUI 禁用 NetScaler Gateway 代理上的虚拟服务器上的身份验证 143
配置设备以与设备代理通信 144
配置 NetScaler Gateway 以与 NetScaler Gateway 代理通信 144
全局绑定 NetScaler Gateway 下一跳服务器 145
将 NetScaler Gateway 下一跳服务器绑定到虚拟服务器 145
配置 NetScaler Gateway 以处理 STA 和 ICA 流量 145
在防火墙上打开相应的端口 146
维护和监控系统 148
配置委派管理员 148
为委派管理员配置命令策略 149
在 NetScaler Gateway 上创建管理用户 149
创建管理组 149
为委派管理员配置自定义命令策略 150
创建简单自定义命令策略 150
创建高级自定义命令策略 150
将自定义命令策略绑定到用户或组 151
在 NetScaler Gateway 上配置审计 151
在 NetScaler Gateway 上配置日志 152

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

创建审计策略 152

全局绑定审计策略 153

修改审计策略 153

删除审计策略 154

配置 ACL 日志记录 154

使用配置实用程序配置ACL日志记录 155

在NetScaler Gateway上启用ACL或TCP日志记录 155

启用 Citrix Secure Access™ 日志记录 155

监控 ICA® 连接 156

ICA 会话日志 157

通过 Citrix 事务 ID 集成增强 ICA 会话监控 157

NetScaler Gateway 与 AoT 日志服务器的集成 157

限制 158

身份验证和授权 159

配置默认全局身份验证类型 159

全局配置身份验证 160

配置不带授权的身份验证 161

配置授权 161

配置授权策略 161

授权策略表达式示例 162

使用 GUI 配置授权策略 162

使用 GUI 将授权策略绑定到用户 163

使用 GUI 将授权策略绑定到组 163

设置默认全局授权 163

禁用身份验证 164

禁用身份验证 164

配置特定时间的身份验证 164

配置时间、日期或星期几的身份验证 164

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

身份验证策略的工作原理 165
配置身份验证配置文件 165
使用配置实用程序创建身份验证策略 166
使用配置实用程序修改身份验证策略 166
删除身份验证策略 166
绑定身份验证策略 167
使用 GUI 全局绑定身份验证策略 167
使用 GUI 解除绑定全局身份验证策略 167
设置身份验证策略的优先级 167
设置或更改全局身份验证策略的优先级 167
更改绑定到虚拟服务器的身份验证策略的优先级 168
配置本地用户 168
创建本地用户 168
更改用户密码 168
更改用户的身份验证方法 169
删除用户 169
配置组 169
创建组 170
删除组 170
将用户添加到组 170
使用组配置策略 170
配置 LDAP 身份验证 171
使用配置实用程序配置 LDAP 身份验证 173
确定 LDAP 目录中的属性 175
配置 LDAP 组提取 175
LDAP 组提取如何直接从用户对象进行工作 175
LDAP 组提取如何间接从组对象工作 176
LDAP 授权组属性字段 176

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

配置 LDAP 授权 176
配置 LDAP 嵌套组提取 177
配置多个域的 LDAP 组提取 178
为组提取创建会话策略 178
创建用于多个域的 LDAP 身份验证策略 179
为多个域创建组并绑定策略以进行 LDAP 组提取 180
LDAP 身份验证的 14 天密码过期通知 181
配置客户端证书身份验证 181
使用 GUI 将客户端证书配置为默认身份验证类型 182
从客户端证书中提取用户名 183
配置和绑定客户端证书身份验证策略 183
配置双因素客户端证书身份验证 184
配置智能卡身份验证 184
使用 Secure ICA® 连接配置智能卡身份验证 186
配置 RADIUS 身份验证 187
配置 Gemalto Protiva 系统 187
配置 SafeWord 187
配置 RADIUS 身份验证 188
选择 RADIUS 身份验证协议 188
配置 IP 地址提取 189
配置 RADIUS 组提取 189
在 Windows Server 2003 上配置 RADIUS 190
在 Windows Server 2008 上配置 RADIUS 身份验证 191
配置 RADIUS 授权 192
配置 RADIUS 用户记账 192
创建 RADIUS 策略 194
创建会话策略 194
全局绑定会话策略 194

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

将会话策略绑定到 NetScaler Gateway 虚拟服务器 195

配置 SAML 身份验证 195

配置 Active Directory 联合身份验证服务 2.0 196

配置 SAML 双因素身份验证 198

配置 SAML 身份验证 198

参考 201

SAML 身份验证的改进 201

解决方案 202

平台 202

配置 202

使用 SAML 身份验证登录到 NetScaler Gateway 203

支持的平台和应用程序 203

使用高级 SAML 策略配置 SAML 身份验证 204

配置 TACACS+ 身份验证 204

清除配置基本操作不得清除 TACACS 配置 205

新命令 205

CLI 配置 206

配置多重身份验证 206

配置级联身份验证 207

设置全局身份验证策略的优先级 207

更改绑定到虚拟服务器的身份验证策略的优先级 207

配置双因素身份验证 207

配置双因素身份验证 208

为单点登录选择身份验证类型 208

配置客户端证书和 LDAP 双因素身份验证 209

配置单点登录 212

配置 Windows 单点登录 212

全局配置 Windows 单点登录 212

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

使用会话策略配置 Windows 单点登录 212

配置 Web 应用程序的单点登录 213

全局配置 Web 应用程序的单点登录 213

使用会话策略配置 Web 应用程序的单点登录 213

定义 Web 应用程序单点登录的 HTTP 端口 214

使用 LDAP 配置 Web 应用程序的单点登录 214

配置到域的单点登录 215

配置到域的单点登录 215

配置 Microsoft Exchange 2010 的单点登录 215

使用 CLI 执行以下操作 216

使用 CLI 重写配置 216

配置一次性密码使用 217

配置 RSA SecurID 身份验证 217

配置 RADIUS 密码返回 218

配置 SafeWord 身份验证 220

配置 Gemalto Protiva 身份验证 220

网关身份验证的 nFactor 221

身份验证、授权和审计功能许可要求 221

用例 222

身份验证响应处理 223

客户端支持 223

WebView 凭据类型对身份验证机制的支持 224

命令行配置 224

互操作性挑战 225

端点分析 (EPA) 225

错误配置注意事项 225

定义客户端 225

限制网关的 nFactor 226

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

LoginSchema 226
参数说明 227
LoginSchema 和 nFactor 知识要求 227
不使用 LoginSchema 配置双因素身份验证 228
用户名和密码表达式 228
nFactor 配置中的高级步骤 228
GUI 配置 229
创建虚拟服务器 229
创建身份验证虚拟服务器 233
创建身份验证 CERT 配置文件 234
创建身份验证策略 234
添加 LDAP 身份验证服务器 235
添加 LDAP 身份验证策略 235
添加 RADIUS 身份验证服务器 236
添加 RADIUS 身份验证策略 236
创建身份验证登录架构 237
创建策略标签 238
用于 nFactor 身份验证的 re-Captcha 配置 239
re-Captcha 配置 240
在 NetScaler 标准许可证中为 nFactor 身份验证创建网关虚拟服务器 250
参考 253
统一网关可视化工具 253
配置统一网关 253
GUI 配置 256
VPN 虚拟服务器的详细信息 258
`The Pre Auth Block` 260
`The Auth Block` 261

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

添加 StoreFront™ 263

添加 SaaS 264

添加 Web 应用程序 265

配置 NetScaler Gateway 以将 RADIUS 和 LDAP 身份验证与移动/平板设备配合使用 266

限制一个 Active Directory 组的成员访问 NetScaler Gateway 274

LDAP 搜索过滤器方法 274

概述 274

先决条件 274

为单个 Active Directory 组成员配置 LDAP 搜索过滤器的步骤 274

NetScaler Gateway 会话策略方法 277

NetScaler® Gateway 上的设备姿态检查 278

先决条件 278

通过使用 GUI 启用设备姿态 279

在全局级别启用设备状态检查 279

在 VPN 虚拟服务器级别启用设备状态检查 280

在 nFactor 身份验证中将设备状态检查作为因素启用 280

使用 CLI 启用设备状态 281

参考资料 281

用于身份验证的原生 OTP 支持 282

原生 OTP 支持的优势 282

原生 OTP 工作流 282

先决条件 283

使用 GUI 配置本机 OTP 284

为第一因素创建登录架构 284

配置身份验证、授权和审计虚拟服务器 284

为第二因素 OTP 创建登录架构 286

配置用于管理 OTP 的内容切换策略 286

使用 CLI 配置本机 OTP 286

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

配置 OTP 设备注册和管理页面 287

创建 LDAP 登录操作 287

添加 LDAP 登录的身份验证策略 287

通过 LoginSchema 显示 UI 288

显示设备注册和管理页面 288

使用 CLI 配置用户登录页面 288

向 NetScaler 注册您的设备 290

使用 OTP 登录 NetScaler 292

使用高可用性 293

高可用性工作原理 294

配置高可用性的准则 294

配置高可用性设置 295

添加高可用性节点 296

启用或禁用辅助节点 296

配置高可用性设置 297

更改 RPC 节点密码 297

更改 RPC 节点密码并启用安全连接 297

使用 CLI 更改 RPC 节点密码 298

配置主备设备以实现高可用性 298

配置通信间隔 299

配置辅助 NetScaler Gateway 的通信间隔 299

同步 NetScaler Gateway 设备 299

启用或禁用高可用性同步 300

强制设备之间同步 300

在高可用性设置中同步配置文件 300

在高可用性设置中同步文件的参数 300

使用配置实用程序在高可用性设置中同步文件 301

配置命令传播 301

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

在主节点上启用或禁用传播 302
命令传播故障排除 302
配置故障安全模式 302
配置故障安全模式 304
配置虚拟 MAC 地址 304
配置 IPv4 虚拟 MAC 地址 304
创建或修改 IPv4 虚拟 MAC 地址 305
配置 IPv6 虚拟 MAC 地址 306
创建或修改 IPv6 虚拟 MAC 地址 306
在不同子网中配置高可用性对 307
独立网络配置的工作原理 307
添加远程节点 308
为独立网络计算模式添加远程节点 308
删除远程节点 309
配置路由监视器 309
添加或删除路由监视器 310
添加路由监视器 310
删除路由监视器 311
配置链路冗余 311
配置链路冗余 311
从故障转移接口集中删除接口 311
删除故障转移接口集 312
了解故障转移的原因 312
强制从节点进行故障转移 312
在主节点或辅助节点上强制故障转移 313
在主节点或辅助节点上强制故障转移 313
强制主节点保持主状态 313
强制主节点保持主状态 313

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

强制辅助节点保持辅助状态 314
强制辅助节点保持辅助状态 314
将 NetScaler Gateway 恢复为活动高可用性设备 314
使用群集 315
配置集群 315
使用配置实用程序创建 NetScaler Gateway 集群实例 316
将节点添加到 NetScaler Gateway 集群 316
创建群集节点组 317
将本地集群节点绑定到集群节点组 317
将 NetScaler Gateway 虚拟服务器绑定到集群节点组 318
统一网关 320
带统一网关的 NetScaler：一个 URL 320
统一网关配置向导 321
附加配置管理 322
内容交换虚拟服务器 322
VPN虚拟服务器 322
统一网关常见问题解答 323
什么是统一网关? 323
为什么要使用统一网关? 323
是否可以有多个统一网关虚拟服务器? 323
为什么统一网关需要内容切换? 323
在 11.0 之前的版本中，内容切换可用于接收多个虚拟服务器的流量。这种用法也称为统一网关? 324
统一网关中的内容切换策略发生了哪些变化? 324
统一网关目前不支持哪些 NetScaler Gateway 功能? 324
使用统一网关时，EPA 扫描的行为是什么? 324
统一网关的许可证要求是什么? 324
与统一网关一起使用的 NetScaler Gateway 虚拟服务器是否需要 IP/端口/SSL 配置? 325

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

我是否需要重新预配 NetScaler Gateway 虚拟服务器上的 SSL/TLS 证书以用于统一网关虚拟服务器? 325

单一 URL 部署和多主机部署之间有什么区别？我需要哪一个? 325

统一网关可以使用哪些身份验证机制? 325

什么是“SelfAuth”身份验证? 325

什么是“StepUp”身份验证? 326

NetScaler AAA TM 虚拟服务器是否支持 StepUp 身份验证? 326

什么是 `login once/logout once`? 326

可以在 Unified Gateway 级别指定通用身份验证策略，并且在负载平衡虚拟服务器级别绑定 NetScaler AAA TM 负载平衡虚拟服务器特定的身份验证吗？支持此用例的配置步骤是什么? 326

如何配置 Unified Gateway，以便绑定的 NetScaler AAA TM 虚拟服务器拥有自己的身份验证策略? 327

NetScaler AAA TM 认证虚拟服务器是否需要用于通过 Unified Gateway 虚拟服务器进行身份验证的用户? 327

您在哪里指定 NetScaler Gateway 身份验证策略——在 Unified Gateway 虚拟服务器上还是在 NetScaler Gateway 虚拟服务器上? 327

如何在 Unified Gateway 内容交换虚拟服务器后面的 NetScaler AAA TM 虚拟服务器上启用身份验证? 327

如何将 TM 虚拟服务器添加到内容交换后面（单个 URL 与多主机）? 327

如果将绑定到 NetScaler AAA TM 负载平衡虚拟服务器的身份验证策略移到 Unified Gateway 虚拟服务器后面，会发生什么? 327

如何为 NetScaler AAA TM 会话配置会话策略? 328

NetScaler 11.0 中 NetScaler Gateway 门户有哪些变化? 328

NetScaler 11.0 是否支持 NetScaler Gateway 门户自定义? 328

NetScaler 高可用性或群集部署是否支持门户主题? 328

我的自定义项是否会作为 NetScaler 11.0 升级过程的一部分进行迁移? 328

在 NetScaler 11.0 中使用门户主题之前，是否有任何需要遵循的预升级步骤? 329

如何将存储在 NetScaler 实例上并由 rc.conf 或 rc.netscaler 调用的自定义项迁移到门户主题? 329

如何在升级到 NetScaler 11.0 之前导出并保存当前自定义项，以及是否可将导出的文件移动到其他 NetScaler 设备? 329

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

NetScaler AAA TM 虚拟服务器是否支持门户主题? 329
NetScaler Gateway 11.0 的 RDP 代理功能有哪些变化? 329
许可变更 330
启用命令 330
其他 RDP 代理更改 330
如何将基于 NetScaler 10.5.e 的远程桌面协议 (RDP) 代理配置迁移到 NetScaler 11.0? 330
如何使用 NetScaler 11.0 版本设置 NetScaler Gateway 以进行 RDP 代理配置? 330
HDX™ Insight 是否与 Unified Gateway 兼容? 331
如何迁移我现有的 HDX Insight 配置? 331
NetScaler Gateway 设备上的 VPN 配置 332
用户如何使用 Citrix Secure Access™ 客户端连接 333
建立安全隧道 333
通过安全连接隧道传输专用网络流量 333
通过防火墙和代理连接 334
控制 Citrix Secure Access 客户端的升级 334
要求 334
插件行为 335
用于控制 VPN 插件升级的 CLI 参数 339
用于控制 EPA 插件升级的 CLI 参数 339
VPN 配置 340
EPA 配置 340
在 NetScaler Gateway 上设置完整 VPN 340
先决条件 341
在 NetScaler Gateway 设备上配置完整的 VPN 设置 341
配置拆分隧道 347
分流隧道选项 348
分流隧道关闭 349
分流隧道开启 349

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

反向拆分隧道 349

配置名称服务解析 351

参考 351

选择用户访问方法 351

部署 Citrix Secure Access™ 客户端供用户访问 353

通过使用 MSI 安装程序包部署 Citrix Secure Access 客户端 353

使用集中式部署工具的优势 353

确定要部署哪个软件插件 353

为用户选择 **Citrix Secure Access™ 客户端** 353

全局配置插件 354

在会话配置文件中配置适用于 Windows 或 macOS 的插件类型 354

适用于 Windows 的 Citrix Secure Access 客户端 354

安装适用于 Windows 的 Citrix Secure Access 客户端 355

配置适用于 Windows 的 Citrix Secure Access 客户端的登录对话框 356

为适用于 Windows 的 Citrix Secure Access 客户端设置拦截模式 356

适用于 Windows Citrix Secure Access 的 Microsoft Edge 网页视图支持 356

使用 Windows 筛选平台的 Windows Citrix Secure Access 客户端 357

适用于 macOS 的 Citrix Secure Access 客户端 362

根据 ADC 配置强制执行最终用户的本地 LAN 访问 362

通过 Active Directory 部署 Citrix Secure Access™ 客户端 365

要从配置实用程序下载 Citrix Secure Access 客户端 MSI 包 365

创建分发点 366

使用 Active Directory 管理 Citrix Secure Access™ 客户端 367

从用户设备中删除 Citrix Secure Access 客户端 367

使用 Active Directory 排除 Citrix Secure Access 客户端安装故障 367

将 Citrix Secure Access 客户端与 Citrix Workspace 应用程序集成 367

用户如何使用 Citrix Workspace 应用程序连接 368

解耦 Citrix Workspace 应用程序图标 369

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

使用 CLI 设置图标集成 369

使用 GUI 设置图标集成 369

配置 ICA® 连接的 IPv6 369

使用 CLI 配置 ICA 代理的 IPv6 370

在 NetScaler Gateway 上配置 Citrix Workspace 应用程序主页 371

全局配置 Citrix Workspace 应用程序主页 371

在会话配置文件中配置 Citrix Workspace 应用程序主页 371

将 Citrix Workspace 主题应用于 NetScaler Gateway 登录页面 372

切换到 Citrix Workspace 主题 372

创建自定义 Citrix Workspace 主题 372

为 NetScaler Gateway 登录页面创建自定义主题 374

使用 CLI 创建和部署自定义主题 374

NetScaler Gateway Windows VPN 客户端注册表项 374

在身份验证 Cookie 上强制执行 HttpOnly 标志 402

支持的场景 403

使用 CLI 配置 HttpOnly 功能 403

限制 404

为 VPN 用户自定义用户门户 404

应用门户主题 404

Caxton 主题 405

Green bubble 主题 406

X1 主题 406

将门户主题绑定到 VPN 虚拟服务器 406

使用 CLI 将门户主题绑定到 VPN 虚拟服务器 406

使用 GUI 将门户主题绑定到 VPN 虚拟服务器 406

将门户主题绑定到 VPN 全局 407

使用 CLI 将门户主题绑定到 VPN 全局 407

使用 GUI 将门户主题绑定到 VPN 全局 407

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

创建门户主题 408
使用库存门户主题作为自定义门户主题的模板 408
使用 CLI 创建门户主题 408
使用 GUI 创建门户主题 408
门户主题自定义 408
关于门户主题界面 408
可自定义页面属性的类型 409
创建 EULA 411
使用 CLI 创建 EULA 实体 411
使用 GUI 创建 EULA 实体 412
使用 CLI 将 EULA 绑定到 VPN 全局 412
使用 GUI 将 EULA 绑定到 VPN 全局 412
使用 CLI 将 EULA 绑定到 VPN 虚拟服务器 413
使用 GUI 将 EULA 绑定到 VPN 虚拟服务器 413
提示用户通过创建自定义页面升级旧版或不受支持的浏览器 413
如何创建自定义页面以提示用户根据 SSL 升级旧版不受支持的浏览器 413
使用 NetScaler Gateway 配置无客户端 VPN 访问 414
无客户端 VPN 访问策略的工作原理 414
启用无客户端 VPN 访问 416
全局启用无客户端访问 416
使用会话策略启用无客户端访问 416
编码 Web 地址 417
全局配置 Web 地址编码 417
通过创建会话策略配置 Web 地址编码 417
创建无客户端访问策略 418
使用默认设置创建无客户端访问策略 418
将无客户端访问策略绑定到虚拟服务器 418
创建和评估无客户端访问策略表达式 418

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

通过 NetScaler Gateway 进行高级无客户端 VPN 访问 419
先决条件 419
配置高级无客户端 VPN 访问 420
注意事项 421
为用户配置域访问 421
使用 NetScaler Gateway 向导配置域访问 421
使用配置实用程序配置域设置 421
SharePoint 2003、SharePoint 2007 和 SharePoint 2013 的无客户端 VPN 访问 422
使用 NetScaler GUI 配置 SharePoint 的无客户端访问 422
将 SharePoint 站点设置为主页 422
为 SharePoint 2007 服务器启用名称解析 423
配置 DNS 后缀 423
启用无客户端 VPN 访问持久性 Cookie 424
为 SharePoint 的无客户端 VPN 访问配置持久性 Cookie 424
Citrix® SSO 移动设备 VPN 客户端 425
参考 425
配置客户端选择页面 425
在登录时显示客户端选择页面 426
全局启用客户端选择选项 426
将会话策略的一部分启用客户端选择 427
配置客户端选择选项 427
创建授权组 427
为客户端选择创建会话配置文件 428
全局配置 STA 服务器 429
将 STA 绑定到虚拟服务器 429
配置访问场景回退 429
创建访问场景回退策略 430
创建隔离组 431

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

配置设置以隔离用户连接 431

为访问方案回退创建会话策略 431

将会话策略绑定到隔离组 432

创建全局客户端安全策略 432

配置 Citrix Secure Access™ 客户端的连接 432

配置用户会话数 433

设置全局用户限制 433

设置每个虚拟服务器的用户限制 433

配置超时设置 434

配置强制超时 435

配置会话或空闲超时 436

使用 GUI 全局配置会话或客户端空闲超时 436

使用 GUI 通过会话策略配置会话或客户端空闲超时设置 436

连接到内部网络资源 437

配置对内部网络资源的访问 437

配置拆分隧道 437

配置拆分隧道 438

配置拆分隧道和授权 438

配置客户端拦截 439

为 Citrix Secure Access™ 客户端配置内网应用程序 439

为一个 IP 地址创建内部网应用程序 440

配置 IP 地址范围 440

为主机名创建内网应用程序 441

从客户端拦截中排除特定域流量 441

配置名称服务解析 443

在会话配置文件中添加 DNS 或 WINS 服务器 443

启用用户连接的代理支持 444

代理设置 444

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

配置用户连接的代理支持 445

为 NetScaler Gateway 配置一个代理服务器以使用所有协议 446

将 NetScaler Gateway 配置为代理服务器 446

配置地址池 447

内部网 IP DNS 注册 448

使用 GUI 为用户、组或虚拟服务器配置地址池 449

使用 GUI 全局配置地址池 450

使用 CLI 配置地址池 450

定义地址池选项 451

定义地址池 451

配置传输登录页面 452

配置 DNS 后缀 452

支持 VoIP 电话 453

配置访问界面 454

更改访问界面 454

使用自定义主页替换访问界面 455

创建并应用网页链接 455

创建企业书签 456

创建个人书签 459

在书签中配置用户名令牌 460

配置 SmartAccess 460

流量策略 461

创建流量策略 461

流量策略表达式示例 462

使用 GUI 配置流量策略 462

配置基于表单的单点登录 463

配置基于表单的单点登录 463

配置 SAML 单点登录 464

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

配置 SAML 单点登录 464

绑定流量策略 464

使用 GUI 全局绑定流量策略 464

删除流量策略 465

使用 GUI 取消绑定流量策略 465

使用 GUI 移除流量策略 465

会话策略 465

创建会话策略 466

会话策略表达式示例 466

绑定会话策略 466

使用 GUI 将会话策略绑定到虚拟服务器 467

使用 GUI 将会话策略绑定到身份验证、授权和审计组 467

使用 GUI 将会话策略绑定到身份验证、授权和审计用户 467

创建会话配置文件 468

在会话配置文件中配置用户连接的网络设置 468

在会话配置文件中配置连接设置 468

在会话配置文件中配置安全设置 469

在会话配置文件中配置 Citrix Virtual Apps and Desktops 设置 470

企业书签的高级策略支持 471

将 VPN URL 配置为高级策略 471

在 GUI 上 471

在 CLI 上 475

端点分析 478

端点策略的工作原理 479

EPA 表达式示例 480

评估用户登录选项 480

跳过 EPA 扫描 481

Ubuntu 支持的端点分析扫描 481

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

预认证策略和配置文件 482
配置预身份验证配置文件 483
配置自定义表达式 484
配置复合表达式 485
绑定预身份验证策略 486
解除绑定并删除预身份验证策略 486
设置预身份验证策略的优先级 487
后身份验证策略 487
配置后身份验证策略 488
配置身份验证后扫描的频率 489
隔离组和授权组 489
用户设备的预身份验证设备检查表达式 492
配置防病毒、防火墙、互联网安全或反垃圾邮件表达式 492
配置服务策略 493
配置进程策略 494
配置操作系统策略 495
配置注册表策略 497
配置复合客户端设备检查表达式 499
使用 NOT (\!) 运算符配置策略 500
nFactor 中作为 EPA 组件的设备证书 500
在 nFactor 中将设备证书配置为 EPA 组件 501
参考 504
EPA 扫描作为 nFactor 身份验证的一个因素 504
EPA 因子互斥 506
EPA 执行 506
配置 EPA 扫描在身份验证后运行 507
参考 513
Windows 客户端上的 EPA 扫描分类类型 514

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

使用 GUI 配置 EPA 扫描分类类型 514

Windows 版 EPA 客户端的遥测数据扫描 515

参考 516

端点分析 v2 516

支持的平台和版本 516

支持和不支持的扫描 516

先决条件 517

在 NetScaler Gateway 上启用 EPA v2 517

升级 NetScaler 518

升级 NetScaler Gateway 上的客户端组件 519

升级最终用户计算机上的 Windows 和 macOS 版 EPA 客户端 520

EPA v2 故障排除 521

高级端点分析扫描 522

在 GUI 上 523

在 CLI 上 527

升级 EPA 库 528

高级端点分析扫描故障排除 528

Windows 上次更新扫描 529

MAC 地址的 EPA 扫描 530

使用 GUI 配置 MAC 地址的 EPA 扫描 531

使用 CLI 配置 MAC 地址的 EPA 扫描 532

注意事项 533

限制 534

参考 534

高级端点分析策略表达式参考 534

表达式格式 534

表达式字符串 534

应用程序扫描方法 536

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

管理用户会话 541
使用 GUI 管理用户会话 541
查看用户会话 541
刷新会话列表 542
结束用户或组会话或具有特定内网 IP 地址的会话 542
使用 CLI 管理用户会话 542
Windows 自动登录 542
使用 CLI 配置 Windows 自动登录 542
使用 Kerberos 身份验证进行自动登录 543
先决条件 543
使用 Citrix Secure Access™ 客户端配置 Kerberos 身份验证 543
参考 543
始终在线 543
何时使用 Always On 544
了解 Always On 框架 544
隧道的自动重新建立 544
无缝隧道建立支持的用户身份验证方法 545
Always On 的配置要求 545
启用 Always On 功能时的注意事项 545
配置 Always On 546
关于 IIP 的说明 547
管理员用户和非管理员用户的不同配置行为摘要 547
在“始终在线”关闭时允许选定的 URL 548
设置 AlwaysOnAllowlist 注册表 548
Windows 登录前始终开启 VPN（原 Always On 服务） 549
Windows 登录前始终开启 VPN 功能 549
了解 Windows 登录前始终开启 VPN 550
配置 Windows 登录前始终开启 VPN 后的 Windows 凭据管理器屏幕 551

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

配置 Windows 登录前始终开启 VPN 551
先决条件 552
主要配置步骤 552
计算机级隧道 552
用户级隧道 559
客户端配置 563
使用高级策略创建 VPN 策略 565
为何从经典策略迁移到高级策略? 565
使用高级 EPA 的预身份验证 EPA 566
使用高级 EPA 的身份验证后 EPA 566
使用高级策略的预身份验证和身份验证后 EPA 566
作为 nFactor 身份验证中一个因素的定期 EPA 扫描 566
NetScaler Gateway 上的 SSL 支持 568
在 NetScaler Gateway 上启用 TLS 1.3 协议 568
使用 GUI 启用 TLS 1.3 协议 569
使用 CLI 启用 TLS 1.3 协议 569
兼容性矩阵 570
对于后端连接 570
对于前端连接 570
限制 570
验证 TLS 1.3 加密状态 571
后端连接 571
前端连接 571
参考资料 572
在 NetScaler Gateway 上启用 DTLS 1.2 协议 572
使用 GUI 配置 DTLS 1.2 572
使用 CLI 配置 DTLS 1.2 573
验证 DTLS 1.2 加密状态 574

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

兼容性矩阵 574
限制 575
使用 SSL VPN 虚拟服务器配置 DTLS VPN 虚拟服务器 576
注意事项 576
使用 GUI 配置 DTLS VPN 虚拟服务器 577
使用 CLI 配置 DTLS VPN 虚拟服务器 577
支持的 DTLS VPN 虚拟服务器参数 578
不支持的 DTLS VPN 虚拟服务器参数 579
使用 XenApp 和 XenDesktop® 向导配置 DTLS 虚拟服务器 580
限制 580
与 Citrix® 产品集成 582
将 NetScaler Gateway 与 StoreFront 集成 582
配置 NetScaler Gateway 以与 StoreFront 配合使用 582
1. 为基于 Web 浏览器的访问创建会话策略 583
2. 为基于 Citrix Workspace™ 应用程序的访问创建会话策略 587
3. 创建身份验证配置文件 591
4. 创建 NetScaler® Gateway 虚拟服务器 591
5. 配置 StoreFront 594
仅将 NetScaler Gateway 与 StoreFront 或 StoreFront Cloud 集成以进行 HDX 路由 594
用例 594
StoreFront 594
店面云 594
先决条件 594
配置 NetScaler Gateway 以进行 HDX 路由 594
1. 创建会话配置文件和策略 595
2. 创建 NetScaler Gateway 虚拟服务器 595
3. 将 NetScaler Gateway 添加到 StoreFront 或 StoreFront Cloud 596
配置 SmartControl 596

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

ICA® 策略和配置文件 598
ICA 访问配置文件 598
ICA 延迟配置文件 599
ICA 操作 600
ICA 策略 600
SmartControl 对 Secure HDX™ 的支持 601
系统要求 601
主要增强功能 601
限制 601
Microsoft Intune 的集成 603
Citrix® 微型 VPN 与 Microsoft Endpoint Manager 的集成 603
何时使用集成的 Intune MDM 解决方案 604
了解 NetScaler Gateway 与 Intune 的 MDM 集成 604
Intune NAC v2 API 支持 605
配置 NetScaler Gateway 虚拟服务器的网络访问控制设备检查以进行单因素登录 605
许可 606
系统要求 606
先决条件 606
参考 607
添加具有 nFactor 的 NetScaler Gateway 虚拟服务器以进行网关部署 607
将身份验证登录方案绑定到身份验证虚拟服务器，以指示 VPN 插件发送设备 ID 作为 /cgi/login 请求的一部分 615
Intune NAC v2 API 支持 617
NetScaler Gateway 与 Intune NAC 集成中对强映射证书的支持 619
故障排除 619
常见问题 619
NetScaler Gateway 问题 619
NetScaler Gateway OAuth 状态和错误条件 620

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

Intune 配置检查 620
在 Azure 门户上配置 NetScaler Gateway 应用程序 620
先决条件 620
在 Azure 上创建 NetScaler Gateway 应用程序 621
理解 MSAL 令牌身份验证 630
配置 NetScaler Gateway 虚拟服务器以进行 MSAL 令牌身份验证 630
为将微 VPN 与 Microsoft Endpoint Manager 结合使用而设置 NetScaler Gateway 633
系统要求 634
先决条件 634
授予 Microsoft Entra ID 应用程序权限 634
配置 NetScaler Gateway 以用于 micro VPN 635
验证 NetScaler Gateway 与 Microsoft 服务的通信 636
配置 Microsoft Edge 浏览器 636
故障排除 638
常见问题 638
NetScaler Gateway 问题 639
NetScaler Gateway OAuth 状态和错误条件 639
最新的 OAuth 网络访问控制 (NAC) 服务终结点 640
Azure AD Graph 的扩展支持 641
HDX™ 智能数据传输支持 643
何时使用 Enlightened Data Transport 支持 643
配置 NetScaler 网关以支持智能数据传输 643
配置 NetScaler 网关以支持增强数据传输 645
使用 GUI 配置 NetScaler Gateway 以支持 EDT 645
使用 CLI 配置 NetScaler Gateway 以支持 EDT 645
配置音频的容损模式 645
使用 GUI 配置 NetScaler Gateway 以启用容损模式 646
使用 CLI 配置 NetScaler Gateway 以启用容损模式 647

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

配置 NetScaler Gateway 以支持 HDX Insight 647
使用 GUI 配置 NetScaler Gateway 以支持 HDX Insight 647
使用 CLI 配置 NetScaler Gateway 以支持 HDX Insight 653
增强型 HDX Insight 传输，无需 NetScaler Gateway 配置依赖项 653
要使用 GUI 禁用 HDX Insight 传输 653
要使用 CLI 禁用 HDX Insight 传输 654
禁用非 NetScaler® AppFlow (NSAP) HDX 会话的 HDX Insight 655
HDX Insight 对 Secure HDX 的支持 655
主要优势 655
系统要求 655
限制 656
使用 GUI 配置 DTLS 1.2 656
使用 CLI 配置 DTLS 1.2 656
PMTUD 和 DF 位传播，适用于通过 NetScaler Gateway 的 EDT 657
在 NetScaler Gateway 中启用 PMTUD 支持 657
在 NetScaler Gateway 中启用 PMTU 重新发现支持 659
在 NetScaler Gateway 中启用 DF 位持久性支持 660
L7 延迟阈值 661
L7 延迟与 L4 延迟有何不同 661
ICA RTT 与 L7 延迟计算之间的区别 662
使用 CLI 配置 L7 延迟阈值 662
参数 663
使用 GUI 配置 L7 延迟阈值 664
在 NetScaler ADM 中查看 L7 延迟参数 665
L7 延迟测量模型与 L7 延迟阈值报告模型 665
L7 延迟测量模型 665
L7 延迟阈值报告模型 666
HDX™ 压缩器 668

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

RDP 代理 670
通过无客户端 VPN 部署 671
通过 ICA 代理部署 671
强制执行详细信息 671
支持强制执行的 RDP 参数 672
连接流程 672
无状态（双）网关兼容性 672
单网关兼容性 673
支持单个侦听器 674
RDP 代理的许可证要求 674
书签 675
创建书签 675
RDP 代理要启用的功能和模式 676
RDP 代理高级配置步骤 676
配置客户端配置文件 676
配置服务器配置文件 678
使用 CLI 配置 RDP 代理 678
使用 GUI 配置 RDP 代理 679
禁用 SSO 的选项 685
无状态 RDP 代理 686
连接流程 686
先决条件 687
使用 CLI 配置无状态 RDP 代理 687
使用 GUI 配置无状态 RDP 代理 689
连接计数器 689
升级说明 690
RDP 连接重定向 690
先决条件 690

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

在连接代理存在的情况下部署 RDP 代理 690
使用 CLI 在存在连接代理的情况下配置 RDP 代理 691
使用 NetScaler GUI 配置 RDP 连接重定向 691
根据 LDAP 属性填充 RDP URL 691
使用 CLI 根据 LDAP 属性填充 RDP URL 691
LDAP 服务器配置 692
使用 GUI 根据 LDAP 属性填充 RDP URL 693
使用 RDP 代理随机化 RDP 文件名 693
配置使用 RDP 代理随机化 RDP 文件名的支持 693
配置 RDP 文件的名称 693
配置 RDP 文件的名称 694
出站 ICA® 代理支持 695
了解出站 ICA 代理支持 695
NetScaler LAN 代理上的 SSL 支持 696
配置出站 ICA® 代理 696
为 ICA 出站代理配置 NetScaler LAN 代理 696
NetScaler Gateway 支持 VMware Horizon View 的 PCoIP 代理 698
配置 NetScaler Gateway 启用的 VMware Horizon View PCoIP 代理 698
先决条件 698
启用 USB 重定向的步骤 701
更新统一网关的内容切换表达式 701
使用 PCoIP 网关 702
配置 VMware Horizon View 连接服务器 702
NetScaler Gateway 出站代理支持的代理自动配置 703
使用 CLI 配置 NetScaler Gateway 全局参数以支持出站代理的 PAC 703
使用 CLI 在会话配置文件中配置 NetScaler Gateway 以支持 PAC 703
使用 GUI 配置 NetScaler Gateway 全局参数以支持出站代理的 PAC 703
使用 GUI 配置 NetScaler Gateway 以支持会话配置文件上的 PAC 704

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

SameSite cookie 属性的配置支持 705
配置 `SameSite` cookie 属性 705
使用 CLI 设置 `SameSite` 属性 705
使用 CLI 将 Cookie 绑定到 `patset` 706
使用 GUI 设置 SameSite 属性 706
使用 Citrix SD-WAN™ WANOP 优化网络流量 709
创建流量策略 710
网关用户体验配置中的 RfWebUI 角色 711
何时使用 RfWebUI 角色 711
RfWebUI 角色提供的功能 711
GO 711
应用程序聚合 712
用户配置的 RDP 代理链接 712
常用应用程序 712
启用 RfWebUI Persona 时的注意事项 712
配置 RfWebUI 界面风格 712
RfWebUI 配置参数 713
使用自定义插件进行网关门户定制 717
示例配置 718
使用自定义插件进行网关门户定制 720
示例配置 722
创建和自定义登录方案 724
创建登录方案配置文件 724
将登录架构配置文件绑定到身份验证、授权和审计虚拟服务器 727
从管理 UI 进行门户自定义 728
通用属性 729
字符串自定义 732

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

优化 NetScaler Gateway VPN 拆分隧道以用于 Office365 735
使用 GUI 进行配置 735
使用 GUI 配置拆分隧道 735
使用 GUI 创建 VPN 内网应用程序 736
使用 CLI 进行配置 737
Office 365 服务（EXO、SPO 和 Microsoft Teams）的 IP 地址列表 738
IPv4 地址范围 738
IPv6 地址范围 739
UDP 流量的服务类型支持 740
配置服务器名称指示扩展 741
SSL握手期间服务器证书的验证 742
使用GUI配置服务器证书验证 742
绑定CA证书 742
启用证书验证 742
要使用 CLI 配置服务器证书验证 742
使用模板简化 SaaS 应用程序配置 744
使用模板配置和发布应用程序 - NetScaler Gateway 特定配置 744
使用模板配置和发布应用程序 — 应用程序服务器特定配置 748
__index__ 755
为您的 Citrix Endpoint Management Environment 配置设置 755
NetScaler 功能的许可要求 756
适用于 Citrix Endpoint Management 的 NetScaler 向导 756
使用 Web Interface 访问 Citrix Virtual Apps and Desktops 资源 758
将 Citrix Gateway 与 Citrix Virtual Apps and Desktops 集成 759
建立与服务器场的安全连接 759
进程概述：用户访问服务器场中的已发布资源 759
配置 Web Interface 故障切换 760
配置 Web Interface 故障切换 761

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

使用 Web Interface 配置智能卡访问 761
Web Interface 功能 762
设置 Web Interface 站点 762
配置 SmartAccess 763
SmartAccess 如何适用于 Citrix Virtual Apps and Desktops 763
配置 Citrix Virtual Apps 策略和筛选器 764
在 Citrix Virtual Desktops 5 中配置策略和筛选器 764
使用智能卡配置单点登录 Web Interface 765
使用智能卡为单点登录创建会话配置文件 766
与 Citrix Endpoint Management 或 StoreFront 集成 766
集成 NetScaler Gateway 和 Endpoint Management 767
集成 NetScaler Gateway 和 StoreFront 767
为 Endpoint Management 和 StoreFront 配置策略 769

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

NetScaler Gateway 发行说明

发行说明描述了软件在特定版本中的变化，以及该版本中已知存在的问题。

发行说明文档包含以下全部或部分章节：

- **新增功能**：该版本中发布的增强功能和其他更改。
- **已修复问题**：该版本中已修复的问题。
- **已知问题**：该版本中存在的问题。
- **注意事项**：使用该版本时需要牢记的重要方面。
- **限制**：该版本中存在的限制。

重要提示：

NetScaler Gateway 发行说明作为 ADC 发行说明的一部分。 有关 NetScaler Gateway 13.1 增强功能、已知问题和错误修复的详细信息，请参阅 发行说明 页面。

注意：

- 问题描述下方的 标签是 NetScaler 团队使用的内部跟踪 ID。
- 这些发行说明不包含安全相关的修复。有关安全相关修复和公告的列表，请参阅安全公告。

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

关于 NetScaler Gateway

NetScaler Gateway 易于部署且易于管理。最典型的部署配置是将 NetScaler Gateway 设备放置在 DMZ 中。您可以在网络中安装多个 NetScaler Gateway 设备以实现更复杂的部署。

首次启动 NetScaler Gateway 时，您可以使用串行控制台、配置实用程序中的设置向导或动态主机配置协议 (DHCP) 执行初始配置。在 MPX 设备上，您可以使用设备前面板上的 LCD 键盘执行初始配置。您可以配置特定于内部网络的基本设置，例如 IP 地址、子网掩码、默认网关 IP 地址和域名系统 (DNS) 地址。配置基本网络设置后，您将配置特定于 NetScaler Gateway 操作的设置，例如身份验证、授权、网络资源、虚拟服务器、会话策略和端点策略的选项。

在安装和配置 NetScaler Gateway 之前，请查阅本节中的主题，了解有关规划部署的信息。部署规划可能包括确定设备的安装位置、了解如何在 DMZ 中安装多个设备以及许可要求。您可以在任何网络基础结构中安装 NetScaler Gateway，而无需更改安全网络中运行的现有硬件或软件。NetScaler Gateway 支持其他网络产品，例如服务器负载均衡器、缓存引擎、防火墙、路由器和 IEEE 802.11 无线设备。

您可以在“安装前检查表”中写下您的设置，以便在配置 NetScaler Gateway 之前随时查阅。

NetScaler Gateway 设备	提供有关 NetScaler Gateway 设备和设备安装说明的信息。
安装前检查表	提供要查看的规划信息以及在网络中安装 NetScaler Gateway 之前要完成的任务列表。
常见部署	提供有关在网络 DMZ 中、在没有 DMZ 的安全网络中以及与其他设备一起部署 NetScaler Gateway 以支持负载平衡和故障转移的信息。还提供有关将 NetScaler Gateway 与 Citrix Virtual Apps and Desktops 结合部署的信息。
许可	提供有关在设备上安装许可证的信息。还提供有关在多个 NetScaler Gateway 设备上安装许可证的信息。

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

NetScaler Gateway 体系结构

NetScaler Gateway 的核心组件包括：

- **虚拟服务器**。NetScaler Gateway 虚拟服务器是一个内部实体，代表所有可供用户使用的已配置服务。虚拟服务器也是用户访问这些服务的接入点。您可以在单个设备上配置多个虚拟服务器，从而允许一个 NetScaler Gateway 设备为具有不同身份验证和资源访问要求的多个用户社区提供服务。
- **身份验证、授权和审计**。您可以配置身份验证、授权和记帐，以允许用户使用 NetScaler Gateway 或安全网络中（例如 LDAP 或 RADIUS）的身份验证服务器识别的凭据登录到 NetScaler Gateway。授权策略定义用户权限，确定给定用户有权访问哪些资源。有关身份验证和授权的更多信息，请参阅配置身份验证和授权。审计服务器维护有关 NetScaler Gateway 活动的数据，包括用户登录事件、资源访问实例和操作错误。此信息存储在 NetScaler Gateway 或外部服务器上。有关审计的更多信息，请参阅在 NetScaler Gateway 上配置审计。
- **用户连接**。用户可以使用以下访问方法登录到 NetScaler Gateway：
  - 适用于 Windows 的 Citrix Secure Access 客户端是安装在基于 Windows 的计算机上的软件。用户通过右键单击基于 Windows 的计算机通知区域中的图标来登录。如果用户使用的计算机未安装 Citrix Secure Access 客户端，他们可以通过使用 Web 浏览器下载并安装插件来登录。如果用户已安装 Citrix Workspace 应用程序，则用户可以通过 Citrix Workspace 应用程序使用 Citrix Secure Access 客户端登录。当用户设备上安装了 Citrix Workspace 应用程序和 Citrix Secure Access 客户端时，Citrix Workspace 应用程序会自动添加 Citrix Secure Access 客户端。
  - 适用于 macOS X 的 Citrix Secure Access 客户端允许运行 macOS X 的用户登录。它具有与适用于 Windows 的 Citrix Secure Access 客户端相同的功能。您可以通过安装 NetScaler Gateway 10.1, Build 120.1316.e 为此插件版本提供端点分析支持。
  - Citrix Workspace 应用程序，允许用户通过 Citrix StoreFront 连接到服务器场中的已发布应用程序和虚拟桌面。
  - Citrix Workspace 应用程序、Secure Hub、WorxMail 和 WorxWeb，允许用户访问 Web 和 SaaS 应用程序、iOS 和 Android 移动应用程序以及 Citrix Endpoint Management 中托管的 ShareFile 数据。
  - 用户可以从使用 NetScaler Gateway Web 地址的 Android 设备进行连接。当用户启动应用程序时，连接会使用 Micro VPN 将网络流量路由到内部网络。如果用户从 Android 设备进行连接，则必须在 NetScaler Gateway 上配置 DNS 设置。有关更多信息，请参阅通过使用 Android 设备的 DNS 后缀支持 DNS 查询。

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

  - 用户可以从使用 NetScaler Gateway Web 地址的 iOS 设备进行连接。您可以全局配置安全浏览，也可以在会话配置文件中配置。当用户在其 iOS 设备上启动应用程序时，VPN 连接会启动，并且连接会通过 NetScaler Gateway 路由。
  - 无客户端访问，无需在用户设备上安装软件即可为用户提供所需的访问权限。

  配置 NetScaler Gateway 时，您可以创建策略来配置用户如何登录。您还可以通过创建会话和端点分析策略来限制用户登录。

- **网络资源**。这些包括用户通过 NetScaler Gateway 访问的所有网络服务，例如文件服务器、应用程序和网站。
- **虚拟适配器**。NetScaler Gateway 虚拟适配器支持需要 IP 欺骗的应用程序。当安装 Citrix Secure Access 客户端时，虚拟适配器会安装在用户设备上。当用户连接到内部网络时，NetScaler Gateway 与内部服务器之间的出站连接使用内网 IP 地址作为源 IP 地址。Citrix Secure Access 客户端会从服务器接收此 IP 地址作为配置的一部分。

  如果在 NetScaler Gateway 上启用拆分隧道，所有内网流量都将通过虚拟适配器路由。在拦截内网绑定流量时，虚拟适配器将拦截 A 和 AAAA 记录类型的 DNS 查询，同时保持所有其他 DNS 查询不变。不绑定到内部网络的网络流量将通过安装在用户设备上的网络适配器路由。Internet 和专用局域网 (LAN) 连接保持打开和连接状态。如果禁用拆分隧道，所有连接都将通过虚拟适配器路由。任何现有连接都将断开，用户必须重新建立会话。

  如果配置了内网 IP 地址，则流向内部网络的流量将通过虚拟适配器使用内网 IP 地址进行欺骗。

用户连接的工作方式

用户可以从远程位置连接到其电子邮件、文件共享和其他网络资源。用户可以使用以下软件连接到内部网络资源：

- 思杰安全访问™ 客户端
- Citrix Workspace 应用程序
- WorxMail 和 WorxWeb
- Android 和 iOS 移动设备

使用 Citrix Secure Access 客户端连接

Citrix Secure Access 客户端允许用户通过以下步骤访问内部网络中的资源：

1. 用户首次通过在 Web 浏览器中键入 Web 地址连接到 NetScaler Gateway。此时将显示登录页面，并提示用户输入用户名和密码。如果配置了外部身份验证服务器，NetScaler Gateway 将联

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

系该服务器，并且身份验证服务器将验证用户的凭据。如果配置了本地身份验证，NetScaler Gateway 将执行用户身份验证。

2. 如果配置了预身份验证策略，当用户在基于 Windows 的计算机或 macOS X 计算机上的 Web 浏览器中键入 NetScaler Gateway Web 地址时，NetScaler Gateway 会在登录页面出现之前检查是否存在任何基于客户端的安全策略。安全检查会验证用户设备是否满足安全相关条件，例如操作系统更新、防病毒保护和正确配置的防火墙。如果用户设备未能通过安全检查，NetScaler Gateway 将阻止用户登录。无法登录的用户必须下载必要的更新或软件包并将其安装到用户设备上。当用户设备通过预身份验证策略时，将显示登录页面，用户可以输入登录凭据。如果安装了 NetScaler Gateway 10.1 Build 120.1316.e，则可以在 macOS X 计算机上使用高级端点分析。
3. 当 NetScaler Gateway 成功验证用户身份后，NetScaler Gateway 会启动 VPN 隧道。NetScaler Gateway 会提示用户下载并安装适用于 Windows 的 Citrix Secure Access 客户端或适用于 macOS X 的 Citrix Secure Access 客户端。
4. 如果配置了后身份验证扫描，则在用户成功登录后，NetScaler Gateway 会扫描用户设备以查找所需的客户端安全策略。您可以要求与预身份验证策略相同的安全相关条件。如果用户设备未能通过扫描，则策略将不适用，或者用户将被置于隔离组中，并且用户对网络资源的访问将受到限制。
5. 会话建立后，用户将被定向到 NetScaler Gateway 主页，用户可以在其中选择要访问的资源。NetScaler Gateway 附带的主页称为“访问界面”。如果用户使用适用于 Windows 的 Citrix Secure Access 客户端登录，Windows 桌面通知区域中的图标会显示用户设备已连接，并且用户会收到连接已建立的消息。用户还可以不使用访问界面访问网络中的资源，例如打开 Microsoft Outlook 并检索电子邮件。
6. 如果用户请求通过了预身份验证和后身份验证安全检查，NetScaler Gateway 随后会联系请求的资源，并在用户设备和该资源之间启动安全连接。
7. 用户可以通过右键单击基于 Windows 的计算机通知区域中的 NetScaler Gateway 图标，然后单击“注销”来关闭活动会话。会话也可能因不活动而超时。会话关闭后，隧道将关闭，用户将不再有权访问内部资源。用户还可以在浏览器中键入 NetScaler Gateway 网址。当用户按下 Enter 键时，将显示访问界面，用户可以从该界面注销。

注意： 如果您在内部网络中部署 Citrix Endpoint Management，则从内部网络外部连接的用户必须首先连接到 NetScaler Gateway。当用户建立连接后，他们可以访问 Citrix Endpoint Management 上托管的 Web 和 SaaS 应用程序、Android 和 iOS 移动应用程序以及 ShareFile 数据。用户可以通过无客户端访问方式使用 Citrix Secure Access 客户端连接，或者通过使用 Citrix Workspace 应用程序或 Secure Hub 连接。

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

使用 Citrix Workspace 应用程序连接

用户可以使用 Citrix Workspace 应用程序连接以访问其基于 Windows 的应用程序和虚拟桌面。用户还可以从 Endpoint Management 访问应用程序。要从远程位置连接，用户还需要在其设备上安装 Citrix Secure Access 客户端。Citrix Workspace 应用程序会自动将 Citrix Secure Access 客户端添加到其插件列表中。当用户登录 Citrix Workspace 应用程序时，他们也可以登录 Citrix Secure Access 客户端。您还可以配置 NetScaler Gateway，以便在用户登录 Citrix Workspace 应用程序时对 Citrix Secure Access 客户端执行单点登录。

使用 iOS 和 Android 设备连接

用户可以使用 Secure Hub 从 iOS 或 Android 设备连接。用户可以使用 Secure Mail 访问其电子邮件，并使用 WorxWeb 连接到网站。

当用户从移动设备连接时，连接会通过 NetScaler Gateway 路由以访问内部资源。如果用户使用 iOS 连接，您需要启用 Secure Browse 作为会话配置文件的一部分。如果用户使用 Android 连接，连接会自动使用 Micro VPN。此外， Secure Mail 和 WorxWeb 使用 Micro VPN 通过 NetScaler Gateway 建立连接。您无需在 NetScaler Gateway 上配置 Micro VPN。

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

常见的 NetScaler Gateway 部署

您可以将 NetScaler Gateway 部署在组织内部网络（或内网）的边界，以提供对内部网络中服务器、应用程序和其他网络资源的安全单点访问。所有远程用户必须先连接到 NetScaler Gateway，然后才能访问内部网络中的任何资源。

NetScaler Gateway 最常安装在网络中的以下位置：

- 在网络 DMZ 中
- 在没有 DMZ 的安全网络中

您还可以将 NetScaler Gateway 与 Citrix Virtual Apps、Citrix Virtual Desktops、StoreFront 和 Citrix Endpoint Management 结合部署，以允许用户访问其 Windows、Web、移动和 SaaS 应用程序。如果您的部署包含 Citrix Virtual Apps、StoreFront 和 Desktops 7，则可以将 NetScaler Gateway 部署为单跳或双跳 DMZ 配置。早期版本的 Citrix Virtual Desktops 或 Citrix Endpoint Management 不支持双跳部署。

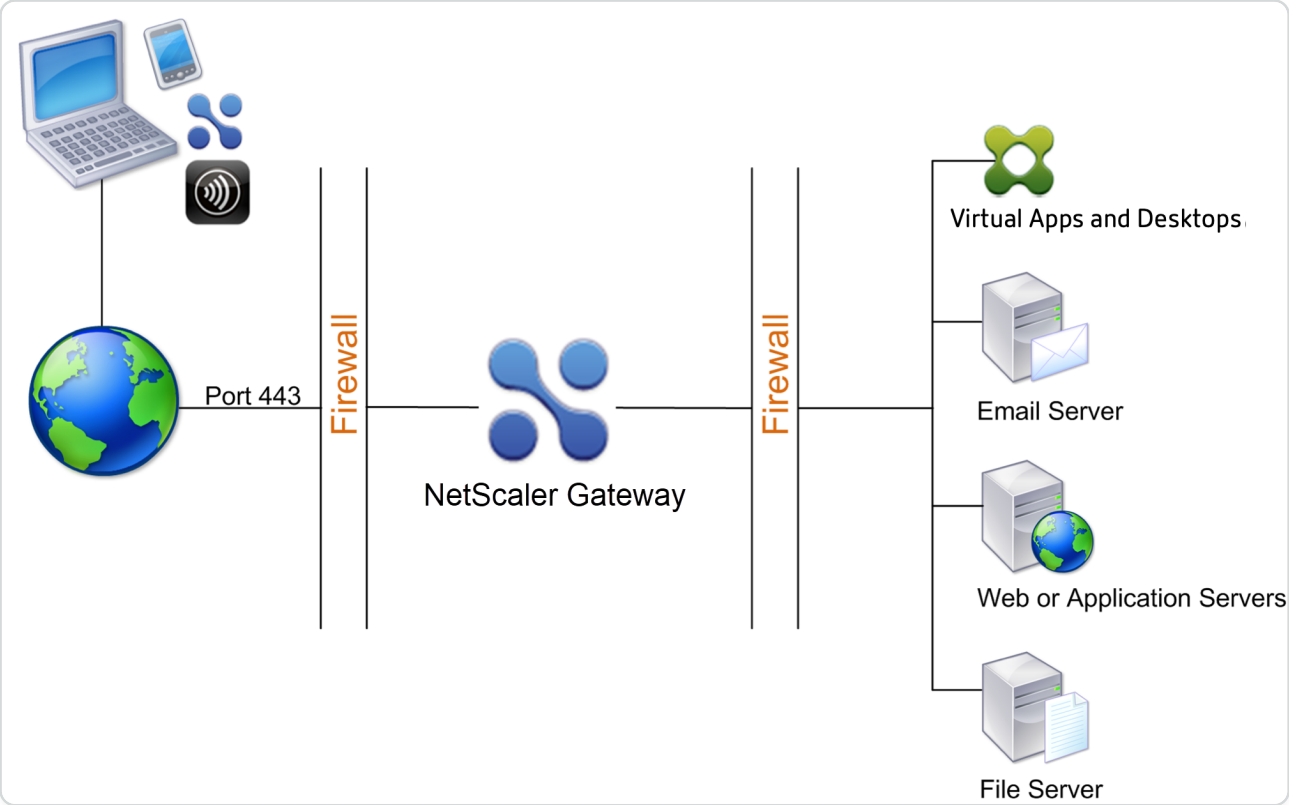
有关使用这些及其他受支持的 NetScaler 解决方案扩展 NetScaler Gateway 安装的更多信息，请参阅 与 NetScaler 产品集成 主题。

在 DMZ 中部署 NetScaler Gateway

许多组织使用 DMZ 保护其内部网络。DMZ 是位于组织安全内部网络与 Internet（或任何外部网络）之间的子网。当您在 DMZ 中部署 NetScaler Gateway 时，用户可以使用 Citrix Secure Access for Windows 或 Citrix Workspace 应用程序进行连接。

图 1. 在 DMZ 中部署的 NetScaler Gateway

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



在上一图中所示的配置中，您将 NetScaler Gateway 安装在 DMZ 中，并将其配置为同时连接到 Internet 和内部网络。

DMZ 中的 NetScaler Gateway 连接

当您在 DMZ 中部署 NetScaler Gateway 时，用户连接必须穿过第一个防火墙才能连接到 NetScaler Gateway。默认情况下，用户连接使用端口 443 上的 SSL 来建立此连接。为了允许用户连接到达内部网络，您必须允许 SSL 通过第一个防火墙上的端口 443。

NetScaler Gateway 解密来自用户设备的 SSL 连接，并代表用户与第二个防火墙后面的网络资源建立连接。必须通过第二个防火墙打开的端口取决于您授权外部用户访问的网络资源。

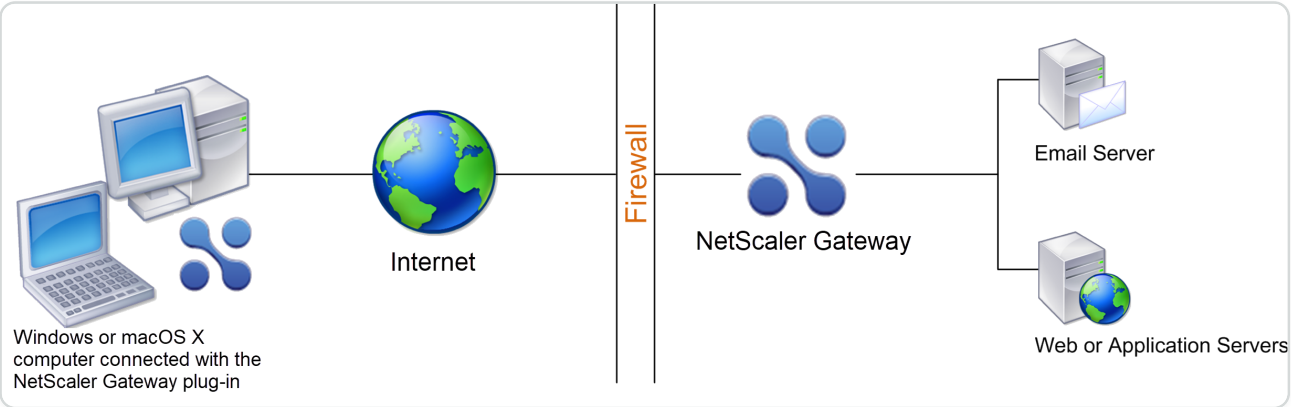
例如，如果您授权外部用户访问内部网络中的 Web 服务器，并且此服务器侦听端口 80 上的 HTTP 连接，则必须允许 HTTP 通过第二个防火墙在端口 80 上进行连接。NetScaler Gateway 代表外部用户设备，通过第二个防火墙与内部网络上的 HTTP 服务器建立连接。

在安全网络中部署 NetScaler Gateway

您可以在安全网络中安装 NetScaler Gateway。在这种情况下，一个防火墙位于 Internet 和安全网络之间。NetScaler Gateway 位于防火墙内部，用于控制对网络资源的访问。

图 1. 在安全网络中部署的 NetScaler Gateway

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



当您在安全网络中部署 NetScaler Gateway 时，请将 NetScaler Gateway 上的一个接口连接到 Internet，将另一个接口连接到安全网络中运行的服务器。将 NetScaler Gateway 放置在安全网络中可为本地和远程用户提供访问权限。由于此配置只有一个防火墙，因此对于从远程位置连接的用户而言，部署的安全性较低。尽管 NetScaler Gateway 会拦截来自 Internet 的流量，但流量会在用户通过身份验证之前进入安全网络。当 NetScaler Gateway 部署在 DMZ 中时，用户在网络流量到达安全网络之前会进行身份验证。

当 NetScaler Gateway 部署在安全网络中时，适用于 Windows 的 Citrix Secure Access 连接必须穿过防火墙才能连接到 NetScaler Gateway。默认情况下，用户连接使用端口 443 上的 SSL 协议建立此连接。为了支持此连接，您必须在防火墙上打开端口 443。

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

客户端软件要求

NetScaler Gateway 支持使用 Citrix Secure Access 客户端进行用户连接。当用户使用插件登录时，它会建立一个完整的 VPN 隧道。借助 Citrix Secure Access 客户端，用户可以连接到您允许访问的网络资源。

如果在 NetScaler Gateway 上配置了端点策略，则当用户登录时，NetScaler Gateway 会自动在用户设备上下载并安装 Citrix EPA 客户端。

Citrix Secure Access™ 客户端系统要求

Citrix Secure Access 客户端在客户端计算机和 NetScaler Gateway 设备之间建立安全连接。

该插件作为桌面应用程序分发，适用于 Microsoft Windows、macOS X 和 Linux 操作系统。使用 Web 浏览器对 NetScaler Gateway 设备的安全 URL 进行身份验证后，该插件将自动下载并安装到您的计算机上。

该插件作为移动应用程序提供，适用于 Android 和 iOS 设备。

注意：

- 要安装该插件，操作系统需要管理员/root 权限。
- 支持 Citrix Secure Access 客户端的浏览器也支持无客户端 VPN。

如果缺少所需的依赖包，命令会列出它们，并且插件安装会失败。这些依赖包必须手动安装。管理员可以使用 CLI 键入以下命令来安装缺少的包。

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

有关 Citrix Secure Access 客户端桌面应用程序和移动应用程序支持的操作系统的更多信息，请参阅系统要求。

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

端点分析要求

NetScaler Gateway 在用户设备上安装 Citrix EPA 客户端。Citrix EPA 客户端扫描用户设备，以检查您在 NetScaler Gateway 上配置的端点安全要求。这些要求包括操作系统、防病毒软件或 Web 浏览器版本等信息。

当用户首次使用浏览器连接到 NetScaler Gateway 时，门户会请求安装 Citrix EPA 客户端。在后续登录尝试中，Citrix EPA 客户端会验证升级控制配置，以确认是否需要升级 Citrix EPA 客户端。如果需要，用户会收到提示以下载并安装最新的 Citrix EPA 客户端。适用于 Windows 的 Citrix EPA 客户端作为 Windows 32 位应用程序安装。适用于 macOS 的 Citrix EPA 客户端作为 64 位应用程序安装。安装或使用 Citrix EPA 客户端不需要特殊权限，除非使用 EPA 访问设备证书。有关如何使用 EPA 进行设备证书身份验证的详细信息，请参阅使用设备证书进行身份验证。

从适用于 Windows 设备的 Device Posture 服务的 Citrix EPA 客户端版本 24.6.1.18 开始，该客户端现在支持自动升级到最新版本，无需用户干预。以前，当 Citrix EPA 客户端以管理员模式安装时，才支持自动更新功能。

管理 UI 控制台上的工具提示详细解释了扫描。有关 EPA 库的详细信息，请参阅 `<https://www.citrix.com/downloads/citrix-secure-access/epa-libraries/epa-libraries-for-netscaler-gateway.html>`。

重要提示：

- 支持 EPA 的浏览器也支持无客户端 VPN。
- 在预身份验证端点分析中，如果用户未安装端点分析插件或跳过扫描，则无法使用 Citrix Secure Access 客户端登录。
- 在后身份验证端点分析中，用户可以通过使用无客户端访问或使用 Citrix Workspace 应用程序来访问不需要扫描的资源。
- 对于 OPSWAT 相关扫描，您必须在客户端计算机上安装二进制软件包 `epaPackage.exe`。

用户设备上需要以下软件才能使用端点分析插件：

操作系统	支持的浏览器
macOS（10.9 及更高版本）	Safari 7.1 或更高版本；Google Chrome 30 或更高版本；Mozilla Firefox 30 或更高版本

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

操作系统	支持的浏览器
视窗 11	Google Chrome 30 或更高版本；Mozilla Firefox 24 或更高版本；Edge Chromium
视窗 10	Google Chrome 30 或更高版本；Mozilla Firefox 24 或更高版本；Edge Chromium
Linux；乌班图 18.04 LTS、20.04 LTS、22.04 LTS、24.04 LTS	Mozilla Firefox 44 及更高版本；Google Chrome 50 及更高版本

注意：

- 支持前面提到的所有操作系统版本。
- 不支持 S 模式下的 Windows 10 和 Windows 11。
- 对于 Windows 版本，必须安装所有服务包和关键更新。
- 对于 Mozilla Firefox 版本，必须启用端点分析插件。最低要求版本为 3.0。

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

NetScaler Gateway 与 Citrix® 产品的兼容性

下表提供了 NetScaler Gateway 兼容的产品和版本。

注意：

NetScaler Gateway 功能适用于 NetScaler VPX。

Citrix 产品和支持的版本

CITRIX 产品	发布版本
思杰 SD-WAN	10.2、11.0、11.1、11.2、11.3、11.4
NetScaler 平台	所有当前 MPX、BLX 和 VPX 型号，包括符合 FIPS 标准的设备。
StoreFront	所有当前支持的 StoreFront 版本。
思杰虚拟应用和桌面	所有当前支持的 Citrix Virtual Apps and Desktops 版本。
Citrix 端点管理	所有当前支持的 Citrix Endpoint Management 版本。

Citrix Workspace 应用程序、Citrix 移动生产力应用程序和插件

*下表列出了每个软件版本支持的第一个构建版本。除非另有说明，否则所有后续构建版本均受支持。有关发布生命周期的更多信息，请参阅产品矩阵。

CITRIX WORKSPACE 应用程序或插件	最低支持版本*
适用于 macOS X 的 Citrix Secure Access 客户端	3.1.8

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

CITRIX WORKSPACE 应用程序或插件	最低支持版本*
适用于 Windows 的 Citrix Secure Access 客户端	12.0
适用于 iOS 的 Citrix Secure Access 客户端	3.1.4
适用于 Android 的 Citrix Secure Access 客户端	2.0.14
适用于 Android 的 Citrix Workspace 应用程序	3.11
适用于 iOS 的 Citrix Workspace 应用程序	7.1.3
适用于 Mac 的 Citrix Workspace 应用程序	12.4
适用于 Windows 的 Citrix Workspace 应用程序	4.4
适用于 Linux 的 Citrix Workspace 应用程序	13.4
适用于 HTML5 的 Citrix Workspace 应用程序	2.3
适用于 Chrome 的 Citrix Workspace 应用程序	2.3
适用于 iOS 的 Secure Hub	10.5
适用于 Android 的 Secure Hub	10.5
适用于 iOS 的 Secure Mail	10.5
适用于 iOS 的 SecureWeb	10.5
适用于 Android 的 Secure Mail	10.5
适用于 Android 的 SecureWeb	10.5

注意：

- 有关每个 VPN 客户端支持的一些常用功能的详细信息，请参阅NetScaler Gateway VPN 客户端和支持的功能。

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

NetScaler Gateway 许可

安装 NetScaler Gateway 后，您可以从 Citrix 获取平台或通用许可证文件。您登录 Citrix 网站以访问可用许可证并生成许可证文件。生成许可证文件后，将其下载到计算机。当许可证文件在计算机上时，您可以将其上传到 NetScaler Gateway。有关 Citrix 许可的更多信息，请参阅 Citrix 许可系统。

在获取许可证文件之前，请务必使用安装向导配置设备的 hostname，然后重新启动设备。

要获取许可证，请访问 激活、升级和管理 NetScaler 许可证 网页。在此页面上，您可以获取新许可证并激活、升级和管理 NetScaler 许可证。

重要提示：

- 您必须在 NetScaler Gateway 上安装许可证。设备不会从 NetScaler 许可证服务器获取许可证。
- Citrix 建议您保留收到的所有许可证文件的本地副本。当您保存配置文件的备份副本时，所有已上传的许可证文件都将包含在备份中。如果您必须重新安装 NetScaler Gateway 设备软件且没有配置备份，则需要原始许可证文件。

在 NetScaler Gateway 上安装许可证之前，请设置设备的 hostname，然后重新启动 NetScaler Gateway。您可以使用安装向导配置 hostname。为 NetScaler Gateway 生成通用许可证时，许可证中会使用 hostname。

NetScaler Gateway 许可证类型

NetScaler Gateway 需要平台许可证。平台许可证允许通过 ICA 代理无限数量地连接到 Citrix Virtual Apps、Citrix Virtual Desktops 或 StoreFront。要允许 Citrix Secure Access 客户端、SmartAccess 登录点或 Secure Hub、WorxWeb 或 Secure Mail 的 VPN 连接到网络，您还必须添加通用许可证。NetScaler Gateway VPX 附带平台许可证。

以下 NetScaler Gateway 版本支持平台许可证：

- NetScaler 网关 12.1
- NetScaler 网关 12.0
- NetScaler 网关 11.1
- NetScaler 网关 11.0
- NetScaler 网关 10.5

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

- NetScaler 网关 10.1
- Access 网关 10
- NetScaler VPX

重要提示：

Citrix 建议您保留所有收到的许可证文件的本地副本。当您保存配置文件的备份副本时，所有上传的许可证文件都将包含在备份中。如果您需要重新安装 NetScaler Gateway 设备软件但没有配置备份，则需要原始许可证文件。

平台许可证

平台许可证允许用户无限次连接到 Citrix Virtual Apps 上的已发布应用程序或 Citrix Virtual Desktops 上的虚拟桌面。使用 Citrix Receiver 的连接不使用 NetScaler Gateway 通用许可证。这些连接只需要平台许可证。所有新的 NetScaler Gateway 订单（无论是物理设备还是虚拟设备）都将以电子方式交付平台许可证。如果您已拥有受保修或维护协议涵盖的设备，可以从 Citrix 网站 获取平台许可证。

通用许可证

NetScaler Gateway 通用许可证将并发用户会话数限制为所购买的许可证数量。如果您购买 100 个许可证，则可以随时拥有 100 个并发会话。如果您购买标准版许可证，则可以随时拥有 500 个并发会话。当用户结束会话时，该许可证将被释放以供下一个用户使用。从多台计算机登录到 NetScaler Gateway 的用户，每个会话都会占用一个许可证。

如果所有许可证都被占用，则在用户结束会话或管理员使用配置实用程序终止会话之前，无法打开其他连接。当连接关闭时，许可证将被释放并可供新用户使用。

当您收到 NetScaler Gateway 设备时，许可过程按以下顺序进行：

- 您将通过电子邮件收到许可证访问代码（许可证密钥）。
- 您使用安装向导配置带有主机名的 NetScaler Gateway。
- 您从 Citrix 网站分配 NetScaler Gateway 许可证。在分配过程中，使用主机名将许可证绑定到设备。
- 您在 NetScaler Gateway 上安装许可证文件。

通用许可证支持以下功能：

- 完整 VPN 隧道
- 微型 VPN
- 端点分析

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

- 基于策略的 SmartAccess
- 无客户端访问网站和文件共享

获取通用许可证

在访问 Citrix® 网站获取通用许可证之前，您需要以下信息。

您的 Citrix 帐户用户 ID 和密码。

> 在 Citrix 网站 (<https://www.citrix.com/welcome/create-account/>) 注册以获取您的用户 ID 和密码。
>
> 注意：如果您无法找到许可证代码或您的用户 ID 和密码，请联系 Citrix 客户服务。

NetScaler Gateway 的 主机名

> Citrix 网站上此名称的输入字段区分大小写，因此请确保您完全按照 NetScaler 设备上的配置复制主机名。

您希望在许可证文件中包含的许可证数量

> 您不必一次性下载所有您有权获得的许可证。例如，如果您的公司购买了 100 个许可证，您可以选择下载 50 个。您可以在以后在另一个许可证文件中分配其余的许可证。多个许可证文件可以安装在
>
> NetScaler Gateway 上。
>
> **注意：** 在获取许可证之前，请确保使用安装向导配置 NetScaler 设备的主机名，然后重新启动设备。

获取您的通用许可证

1. 使用您的 Citrix 凭据登录 Citrix 网站 (https://www.citrix.com/en-in/account/)。
2. 在 **Citrix Manage Licenses is here** 下，按照说明获取您的许可证文件。

安装通用许可证

要安装许可证，请参阅“安装许可证”(/zh-cn/citrix-adc/12-1/licensing/citrix-adc-licensing-overview.html)。安装后，请验证许可证是否已正确安装。

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

验证通用许可证的安装

在继续之前，请验证您的通用许可证是否已正确安装。

使用 CLI 验证通用许可证的安装

1. 使用 SSH 客户端（例如 PuTTY）打开与 NetScaler 设备的 SSH 连接。
2. 使用管理员凭据登录到 NetScaler 设备。
3. 使用 show license 命令验证“SSL VPN = YES”以及最大用户数已从 5 增加到预期的并发用户数。

使用 GUI 验证通用许可证的安装

1. 在 Web 浏览器中，键入 NetScaler 设备的 IP 地址，例如 `http://192.168.100.1`。
2. 在“用户名”和“密码”中，键入管理员凭据。
3. 在导航窗格中，展开“系统”，然后单击“许可证”。
4. 在“许可证”窗格中，您会看到 **Citrix Gateway** 旁边有一个绿色复选标记。“允许的最大 NetScaler Gateway 用户数”字段显示在 NetScaler 设备上获得许可的并发用户会话数量。

相关资源

- Citrix 许可系统
- NetScaler 数据表
- NetScaler 和 NetScaler Gateway 许可证类型

在 NetScaler Gateway 上安装许可证

成功将许可证文件下载到计算机后，即可在 NetScaler Gateway 上安装许可证。许可证安装在 /nsconfig/license 目录中。

如果您使用设置向导配置了 NetScaler Gateway 上的初始设置，则许可证文件会在您运行向导时安装。如果您分配了部分许可证，然后又分配了额外的数量，则无需使用设置向导即可安装许可证。

1. 在配置实用程序中，在“Configuration”（配置）选项卡上的导航窗格中，展开 **System**（系统），然后单击 **Licenses**（许可证）。
2. 在详细信息窗格中，单击 **Manage Licenses**（管理许可证）。
3. 单击 **Add New License**（添加新许可证），然后单击 **Browse**（浏览），导航到许可证文件，然后单击 **OK**（确定）。

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

配置实用程序中会显示一条消息，提示您必须重新启动 NetScaler Gateway。单击“Reboot”（重新启动）。

设置最大用户数

在设备上安装许可证后，您需要设置允许连接到设备的最大用户数。您可以在全局身份验证策略中设置最大用户数。

1. 在配置实用程序中，在“Configuration”（配置）选项卡上的导航窗格中，展开 **NetScaler Gateway**，然后单击 **Global Settings**（全局设置）。
2. 在详细信息窗格中，在“Settings”（设置）下，单击 **Change authentication AAA settings**（更改身份验证 AAA 设置）。
3. 在“Maximum Number of Users”（最大用户数）中，键入用户总数，然后单击 **OK**（确定）。

   此字段中的数字对应于许可证文件中包含的许可证数量。此数字必须小于或等于设备上安装的许可证总数。例如，您安装了一个包含 100 个用户许可证的许可证和第二个包含 400 个用户许可证的许可证。许可证总数等于 500。可以登录的最大用户数等于或小于 500。如果 500 个用户已登录，则任何尝试登录超出此数量的用户都将被拒绝访问，直到有用户注销或您终止会话。

验证通用许可证安装

在继续之前，请验证您的通用许可证是否已正确安装。

通过使用 GUI 验证通用许可证的安装

1. 在配置实用程序中，在“配置”选项卡上，在导航窗格中，展开“系统”，然后单击“许可证”。

   在“许可证”窗格中，您会看到 NetScaler Gateway 旁边有一个绿色复选标记。“允许的最大 NetScaler Gateway 用户数”字段显示设备上获得许可的并发用户会话数。

通过使用 CLI 验证通用许可证的安装

1. 使用 SSH 客户端（例如 PuTTY）打开与设备的 Secure Shell (SSH) 连接。
2. 使用管理员凭据登录到设备。
3. 在命令提示符下，键入；

```
show license
```

如果参数 SSL VPN 等于 Yes 且最大用户参数等于许可证数量，则表示许可证已正确安装。

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

NetScaler Gateway 许可常见问题

如何获得试用或演示许可证的帮助?

许多 NetScaler 产品现在以全面的、私密的、一对一的、专家主导的演示体验形式提供。我们的 Citrix 专家会根据您的需求、用例和正在进行的项目定制演示。无需下载、无需许可证或安装。您只需最少的设置即可观看即时演示。演示结束后，如需继续进行概念验证或试用适用于您服务的 Citrix 解决方案，请联系 Citrix 专家。如需演示，请点击 `<https://demo.citrix.com/>`。

如何安装许可证?

有关安装许可证的详细信息，请参阅 在 NetScaler Gateway 上安装许可证。

Gateway 许可证有哪些不同类型?

平台许可证允许通过 ICA 代理无限数量地连接到 Citrix Virtual Apps、Citrix Virtual Desktops™ 或 StoreFront。 通用许可证是 NetScaler 平台许可证之上的附加许可证。它允许从 Citrix Secure Access 客户端、SmartAccess 登录点或 Secure Hub、Secure Web 或 Secure Mail 连接到网络的 VPN。有关更多详细信息，请参阅 NetScaler Gateway 许可证类型。

支持多少并发用户会话?

支持的会话取决于网关许可证类型。有关详细信息，请参阅 NetScaler Gateway 许可证类型。

另一个需要考虑的因素是底层硬件本身的容量。有关性能注意事项，请参阅 NetScaler MPX/SDX 数据表 或 NetScaler VPX 数据表。

如何检查当前已许可的并发用户会话?

在配置实用程序中，在“配置”选项卡上，展开 **System**，然后单击 **Licenses**。 在 **Licenses** 窗格中，您会看到 NetScaler Gateway 旁边有一个绿色复选标记。**Maximum NetScaler Gateway Users Allowed** 字段显示设备上已许可的并发用户会话数。

如何检查是否达到许可的吞吐量限制?

您可以使用 `newnslog` 提取实时吞吐量。例如，如果许可吞吐量为 500 Mbps，则可以使用以下命令提取超过 500 的实时吞吐量。

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

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

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

如何检查在达到许可吞吐量时是否丢弃了数据包?

您可以使用以下命令检查数据包是否被丢弃。

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

许可吞吐量限制导致的数据包丢弃(/en-us/netscaler-gateway/media/licensed-throughput-packets-dropped.png)

如何查找 NetScaler 设备许可的吞吐量是多少?

从 CLI 运行 `show license` 命令，然后使用型号从 ADC 或网关 MPX、SDX 和 VPX 数据表中获取吞吐量。

显示许可证命令输出(/en-us/netscaler-gateway/media/show-license-command-output.png)

ADC 数据表(/en-us/netscaler-gateway/media/adc-datasheet.png)

如何向现有网关许可证添加更多用户?

您可以安装额外的通用许可证。例如，假设您已安装一个包含 100 个用户许可证的通用许可证。如果您安装第二个包含 400 个用户许可证的通用许可证，则用户许可证总数等于 500。

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

开始之前

在安装 NetScaler Gateway 之前，您必须评估您的基础架构并收集信息，以规划一个满足您组织特定需求的访问策略。在定义访问策略时，您需要考虑安全隐患并完成风险分析。您还需要确定允许用户连接的网络，并决定启用用户连接的策略。

除了规划可供用户使用的资源外，您还需要规划部署方案。NetScaler Gateway 与以下 NetScaler 产品兼容：

- 思杰端点管理™
- 思杰虚拟应用™
- 思杰虚拟桌面™
- StoreFront™
- 思杰SD-WAN™

有关部署 NetScaler Gateway 的更多信息，请参阅 常见部署 和 与 NetScaler 产品集成

在准备访问策略时，请执行以下初步步骤：

- 识别资源。列出您希望提供访问权限的网络资源，例如您在风险分析中定义的 Web、SaaS、移动或已发布的应用程序、虚拟桌面、服务和数据。
- 制定访问方案。创建描述用户如何访问网络资源的访问方案。访问方案由用于访问网络的虚拟服务器、端点分析扫描结果、身份验证类型或其组合定义。您还可以定义用户如何登录网络。
- 识别客户端软件。您可以使用 Citrix Secure Access 客户端提供完整的 VPN 访问，要求用户使用 Citrix Workspace 应用程序、Secure Hub 或通过无客户端访问登录。您还可以将电子邮件访问限制为 Outlook Web App 或 WorxMail。这些访问方案还决定了用户获得访问权限后可以执行的操作。例如，您可以指定用户是否可以通过使用已发布的应用程序或连接到文件共享来修改文档。
- 将策略与用户、组或虚拟服务器关联。您在 NetScaler Gateway 上创建的策略在个人或用户集满足指定条件时强制执行。您根据创建的访问方案确定条件。然后，您创建策略，通过控制用户可以访问的资源以及用户可以对这些资源执行的操作来扩展网络安全性。您将策略与适当的用户、组、虚拟服务器或全局关联。

本节包含以下主题，可帮助您规划访问策略：

- 安全规划包括有关身份验证和证书的信息。

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

- 定义您可能需要的网络硬件和软件的先决条件。
- 预安装清单，您可以在配置 NetScaler Gateway 之前使用它来记录您的设置。

安装 NetScaler Gateway 的先决条件

在配置 NetScaler Gateway 上的设置之前，请查看以下先决条件：

- NetScaler Gateway 已物理安装在您的网络中并可访问网络。NetScaler Gateway 部署在 DMZ 或防火墙后面的内部网络中。您还可以将 NetScaler Gateway 配置在双跳 DMZ 中，并配置与服务器场的连接。Citrix 建议将设备部署在 DMZ 中。
- 您可以使用默认网关或指向内部网络的静态路由配置 NetScaler Gateway，以便用户可以访问网络中的资源。NetScaler Gateway 默认配置为使用静态路由。
- 用于身份验证和授权的外部服务器已配置并正在运行。有关更多信息，请参阅身份验证和授权。
- 网络具有域名服务器 (DNS) 或 Windows Internet 命名服务 (WINS) 服务器，用于名称解析，以提供正确的 NetScaler Gateway 用户功能。
- 您已从 Citrix 网站下载了用于 Citrix Secure Access 客户端用户连接的通用许可证，并且这些许可证已准备好安装在 NetScaler Gateway 上。
- NetScaler Gateway 具有由受信任的证书颁发机构 (CA) 签名的证书。有关更多信息，请参阅安装和管理证书。

在安装 NetScaler Gateway 之前，请使用预安装清单记录您的设置。

安全规划

规划 NetScaler Gateway 部署时，您必须了解与证书以及身份验证和授权相关的基本安全问题。

配置安全证书管理

默认情况下，NetScaler Gateway 包含一个自签名安全套接字层 (SSL) 服务器证书，使设备能够完成 SSL 握手。自签名证书足以用于测试或示例部署，但 NetScaler 不建议将其用于生产环境。在生产环境中部署 NetScaler Gateway 之前，Citrix 建议您请求并接收来自已知证书颁发机构 (CA) 的已签名 SSL 服务器证书，并将其上传到 NetScaler Gateway。

如果您在任何环境中部署 NetScaler Gateway，并且 NetScaler Gateway 必须在 SSL 握手中充当客户端（与另一个服务器建立加密连接），则您还必须在 NetScaler Gateway 上安装受信任的根证书。例如，如果您将 NetScaler Gateway 与 Citrix Virtual Apps 和 StoreFront 一起部署，则可以使用 SSL 加密从 NetScaler Gateway 到 StoreFront 的连接。在此配置中，您必须在 NetScaler Gateway 上安装受信任的根证书。

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

身份验证支持

您可以将 NetScaler Gateway 配置为对用户进行身份验证，并控制用户对内部网络上网络资源的访问级别（或授权）。

在部署 NetScaler Gateway 之前，您的网络环境必须具备目录和身份验证服务器，以支持以下身份验证类型之一：

- LDAP
- RADIUS
- TACACS+
- 支持审计和智能卡的客户端证书
- 采用 RADIUS 配置的 RSA
- SAML 身份验证

如果您的环境不支持任何这些身份验证类型，或者您有少量远程用户，您可以在 NetScaler Gateway 上创建本地用户列表。然后，您可以将 NetScaler Gateway 配置为根据此本地列表对用户进行身份验证。通过此配置，您无需在单独的外部目录中维护用户帐户。

保护您的 NetScaler Gateway 部署

不同的部署可能需要不同的安全注意事项。NetScaler 安全部署指南提供了通用的安全指导，帮助您根据特定的安全要求决定适当的安全部署。

有关详细信息，请参阅 NetScaler 安全部署指南。

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

Gateway 预安装清单

此清单包含在安装 NetScaler Gateway 之前必须完成的任务列表和规划信息。

提供了空间，以便您可以在完成每项任务时进行勾选并做笔记。Citrix 建议您记下在安装过程和配置 NetScaler Gateway 时需要输入的配置值。

有关安装和配置 NetScaler Gateway 的步骤，请参阅安装 NetScaler Gateway。

用户设备

- 确保用户设备满足 Citrix Secure Access 系统要求 中所述的安装先决条件
- 识别用户连接所用的移动设备。**注意**：如果用户使用 iOS 设备连接，则必须在会话配置文件中启用安全浏览。

NetScaler Gateway 基本网络连接

Citrix® 建议您在开始配置设备之前获取许可证和已签名的服务器证书。

- 识别并记下 NetScaler Gateway 主机名。**注意**：这不是完全限定域名 (FQDN)。FQDN 包含在绑定到虚拟服务器的已签名服务器证书中。
- 从 Citrix 网站 获取通用许可证
- 生成证书签名请求 (CSR) 并将其发送给证书颁发机构 (CA)。输入您将 CSR 发送给证书颁发机构的日期。
- 记下系统 IP 地址和子网掩码。
- 记下子网 IP 地址和子网掩码。
- 记下管理员密码。NetScaler Gateway 附带的默认密码是 `nsroot`。
- 记下 NetScaler Gateway 侦听安全用户连接的端口号。默认值为 TCP 端口 443。此端口必须在非安全网络（Internet）和 DMZ 之间的防火墙上打开。
- 记下默认网关 IP 地址。
- 记下 DNS 服务器 IP 地址和端口号。默认端口号为 53。此外，如果您直接添加 DNS 服务器，则还必须在设备上配置 ICMP (ping)。
- 记下第一个虚拟服务器 IP 地址和主机名。
- 记下第二个虚拟服务器 IP 地址和主机名（如果适用）。

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

- 记下 WINS 服务器 IP 地址（如果适用）。

可通过 NetScaler Gateway 访问的内部网络

- 记下用户可通过 NetScaler Gateway 访问的内部网络。示例：10.10.0.0/24
- 输入用户在使用 Citrix Secure Access 客户端通过 NetScaler Gateway 连接时需要访问的所有内部网络和网络段。

高可用性

如果您有两台 NetScaler Gateway 设备，可以将其部署在高可用性配置中，其中一台 NetScaler Gateway 接受并管理连接，而第二台 NetScaler Gateway 监视第一台设备。如果第一台 NetScaler Gateway 因任何原因停止接受连接，第二台 NetScaler Gateway 将接管并开始主动接受连接。

- 记下 NetScaler Gateway 软件版本号。
- 两台 NetScaler Gateway 设备上的版本号必须相同。
- 记下管理员密码 (`nsroot`)。两台设备上的密码必须相同。
- 记下主 NetScaler Gateway IP 地址和 ID。最大 ID 号为 64。
- 记下辅助 NetScaler Gateway IP 地址和 ID。
- 获取并在两台设备上安装通用许可证。
- 在两台设备上安装相同的通用许可证。
- 记下 RPC 节点密码。

身份验证和授权

NetScaler Gateway 支持多种不同的身份验证和授权类型，这些类型可以以各种组合方式使用。有关身份验证和授权的详细信息，请参阅身份验证和授权。

LDAP 身份验证

如果您的环境包含 LDAP 服务器，则可以使用 LDAP 进行身份验证。

- 记下 LDAP 服务器 IP 地址和端口。

  如果允许与 LDAP 服务器进行不安全的连接，则默认端口为 389。如果使用 SSL 加密与 LDAP 服务器的连接，则默认端口为 636。

- 记下安全类型。

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

您可以配置带加密或不带加密的安全。

- 记下管理员绑定 DN。

  如果您的 LDAP 服务器需要身份验证，请输入 NetScaler Gateway 在查询 LDAP 目录时必须用于身份验证的管理员 DN。例如：cn=administrator,cn=Users,dc=ace, dc=com。

- 记下管理员密码。

  密码与管理员绑定 DN 相关联。

- 记下基本 DN。

  用户所在的 DN（或目录级别）；例如，ou=users,dc=ace,dc=com。

- 记下服务器登录名属性。

  输入指定用户登录名的 LDAP 目录人员对象属性。默认值为 sAMAccountName。如果您不使用 Active Directory，此设置的常见值为 cn 或 uid。 有关 LDAP 目录设置的更多信息，请参阅 配置 LDAP 身份验证

- 记下组属性。 输入指定用户所属组的 LDAP 目录人员对象属性。默认值为 memberOf。此属性使 NetScaler Gateway 能够识别用户所属的目录组。
- 记下子属性名称。

RADIUS 身份验证和授权

如果您的环境包含 RADIUS 服务器，则可以使用 RADIUS 进行身份验证。 RADIUS 身份验证包括 RSA SecurID、SafeWord 和 Gemalto Protiva 产品。

- 记下主 RADIUS 服务器 IP 地址和端口。默认端口为 1812。
- 记下主 RADIUS 服务器密钥（共享密钥）。
- 记下辅助 RADIUS 服务器 IP 地址和端口。默认端口为 1812。
- 记下辅助 RADIUS 服务器密钥（共享密钥）。
- 记下密码编码类型（PAP、CHAP、MS-CHAP v1、MSCHAP v2）。

SAML 身份验证

安全断言标记语言 (SAML) 是一种基于 XML 的标准，用于在身份提供商 (IdP) 和服务提供商之间交换身份验证和授权信息。

- 在 NetScaler Gateway 上获取并安装安全的 IdP 证书。
- 记下重定向 URL。

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

- 记下用户字段。
- 记下签名证书名称。
- 记下 SAML 颁发者名称。
- 记下默认身份验证组。

通过防火墙打开端口（单跳 DMZ）

如果您的组织使用单个 DMZ 保护内部网络，并且您在 DMZ 中部署 NetScaler Gateway，请通过防火墙打开以下端口。如果您在双跳 DMZ 部署中安装两台 NetScaler Gateway 设备，请参阅 在防火墙上打开相应的端口。

在非安全网络和 DMZ 之间的防火墙上

- 在 Internet 和 NetScaler Gateway 之间的防火墙上打开一个 TCP/SSL 端口（默认 443）。用户设备通过此端口连接到 NetScaler Gateway。

在安全网络之间的防火墙上

- 在 DMZ 和安全网络之间的防火墙上打开一个或多个适当的端口。NetScaler Gateway 通过这些端口连接到一个或多个身份验证服务器，或连接到安全网络中运行 Citrix Virtual Apps and Desktops 的计算机。
- 记下身份验证端口。

  仅打开适用于您的 NetScaler Gateway 配置的端口。

  - 对于 LDAP 连接，默认是 TCP 端口 389。
  - 对于 RADIUS 连接，默认是 UDP 端口 1812。记下 Citrix Virtual Apps and Desktops 端口。
- 如果您将 NetScaler Gateway 与 Citrix Virtual Apps and Desktops 结合使用，请打开 TCP 端口 1494。如果启用会话可靠性，请打开 TCP 端口 2598 而不是 1494。Citrix 建议保持这两个端口都打开。

Citrix 虚拟桌面™、Citrix 虚拟应用或 StoreFront

如果您正在部署 NetScaler Gateway 以通过 StoreFront 提供对 Citrix Virtual Apps and Desktops 的访问，请完成以下任务。此部署不需要 Citrix Secure Access 客户端。用户仅通过 Web 浏览器和 Citrix Receiver 即可通过 NetScaler Gateway 访问已发布的应用程序和桌面。

- 记下运行 StoreFront 的服务器的 FQDN 或 IP 地址。

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

Citrix 端点管理™

如果您在内部网络中部署 Citrix Endpoint Management，请完成以下任务。如果用户从外部网络（例如 Internet）连接到 Endpoint Management，则用户必须先连接到 NetScaler Gateway，然后才能访问移动、Web 和 SaaS 应用程序。

- 记下 Endpoint Management 的 FQDN 或 IP 地址。
- 确定用户可以访问的 Web、SaaS 和移动 iOS 或 Android 应用程序。

采用 Citrix Virtual Apps™ 的双跳 DMZ 部署

如果您正在双跳 DMZ 配置中部署两个 NetScaler Gateway 设备以支持访问运行 Citrix Virtual Apps 的服务器，请完成以下任务。

第一个 DMZ 中的 NetScaler Gateway

第一个 DMZ 是内部网络最外边缘的 DMZ（最靠近 Internet 或不安全网络）。客户端通过将 Internet 与 DMZ 分隔开的防火墙连接到第一个 DMZ 中的 NetScaler Gateway。在第一个 DMZ 中安装 NetScaler Gateway 之前，请收集此信息。

- 对于此 NetScaler Gateway，请完成此清单中“NetScaler Gateway 基本网络连接”部分中的项目。

  完成这些项目时，接口 0 将此 NetScaler Gateway 连接到 Internet，接口 1 将此 NetScaler Gateway 连接到第二个 DMZ 中的 NetScaler Gateway。
- 在主设备上配置第二个 DMZ 设备信息。

  要将 NetScaler Gateway 配置为双跳 DMZ 中的第一跳，您必须在第一个 DMZ 中的设备上指定第二个 DMZ 中 NetScaler Gateway 的主机名或 IP 地址。指定在第一跳设备上配置 NetScaler Gateway 代理后，将其全局绑定到 NetScaler Gateway 或绑定到虚拟服务器。
- 记下设备之间的连接协议和端口。

  要将 NetScaler Gateway 配置为双 DMZ 中的第一跳，您必须指定连接协议以及第二个 DMZ 中的 NetScaler Gateway 侦听连接的端口。连接协议和端口是带 SSL 的 SOCKS（默认端口 443）。协议和端口必须通过分隔第一个 DMZ 和第二个 DMZ 的防火墙打开。

第二个 DMZ 中的 NetScaler Gateway

第二个 DMZ 是最靠近您的内部安全网络的 DMZ。部署在第二个 DMZ 中的 NetScaler Gateway 充当 ICA 流量的代理，在外部用户设备和内部网络上的服务器之间穿越第二个 DMZ。

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

- 为此 NetScaler Gateway 完成此清单的“NetScaler Gateway 基本网络连接”部分中的任务。

  完成这些项目时，接口 0 将此 NetScaler Gateway 连接到第一个 DMZ 中的 NetScaler Gateway。接口 1 将此 NetScaler Gateway 连接到安全网络。

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

安装和配置 NetScaler Gateway 设备

收到 NetScaler Gateway 设备后，请拆开设备包装并准备场地和机架。在确定安装设备的位置符合环境标准且服务器机架已按照说明就位后，即可安装硬件。安装设备后，将其连接到网络、电源和用于初始配置的控制台终端。打开设备后，执行初始配置并分配管理和网络 IP 地址。请务必遵守安装说明中列出的注意事项和警告。

安装 NetScaler VPX 虚拟设备时，必须首先获取虚拟设备映像并将其安装在虚拟机管理程序或其他虚拟机监视器上。

Citrix 建议使用 NetScaler Gateway 预安装清单 主题，以便您在尝试配置 NetScaler Gateway 设备之前记下您的设置。该清单包含有关安装 NetScaler Gateway 和设备的信息。

使用向导配置 NetScaler Gateway 设备

NetScaler Gateway 具有以下六个向导，可用于配置设备上的设置：

- 首次登录 NetScaler Gateway 设备时，将显示首次设置向导。
- 快速配置向导可帮助您为连接到 Citrix Endpoint Management™ 和 StoreFront 配置正确的策略、表达式和设置。
- NetScaler Gateway 向导可帮助您配置 NetScaler Gateway 特定的设置。
- 设置向导可帮助您首次配置基本的 NetScaler Gateway 设置。
- Citrix Endpoint Management 集成配置可帮助您配置 NetScaler Gateway 和 Citrix Endpoint Management 环境。
- 已发布应用程序向导可帮助您使用 Citrix Workspace 应用程序配置用户连接的设置。

首次设置向导

在 NetScaler Gateway 设备上完成初始设置的安装和配置后，如果未满足以下条件，则首次登录配置实用程序时，将显示“首次设置”向导：

- 您未在设备上安装许可证。
- 您未配置子网或映射的 IP 地址。
- 如果设备的默认 IP 地址为 192.168.100.1。

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

使用首次设置向导配置 NetScaler Gateway

要首次配置 NetScaler Gateway（物理设备或 VPX 虚拟设备），您需要一台与设备配置在同一网络上的管理计算机。

将 NetScaler Gateway IP (NSIP) 地址指定为设备的管理 IP 地址，并将子网 IP (SNIP) 地址指定为服务器可以连接的地址。您将分配一个适用于 NetScaler Gateway 和 SNIP 地址的子网掩码。此外，还要配置时区。如果您分配了主机名，则可以通过指定其名称而不是 NSIP 地址来访问设备。

首次设置向导包含两个部分。在第一部分中，您将配置 NetScaler Gateway 设备的基本系统设置，包括：

NSIP 地址、SNIP 地址和子网掩码 设备主机名 DNS 服务器 时区 管理员密码 在第二部分中，您将安装许可证。如果您指定了 DNS 服务器的地址，则可以使用硬件序列号 (HSN) 或许可证密钥来分配许可证，而无需将许可证从本地计算机上传到设备。

注意：CitrixÂ® 建议将许可证保存到本地计算机。

完成这些设置的配置后，NetScaler Gateway 会提示您重新启动设备。再次登录设备后，您可以使用其他向导和配置实用程序来配置其他设置。

快速配置向导

快速配置向导允许您在 NetScaler Gateway 上配置多个虚拟服务器。您可以添加、编辑和删除虚拟服务器。

快速配置向导允许对以下部署进行无缝配置：

- StoreFront 连接到 Citrix Virtual Apps and Desktops，能够配置安全票证颁发机构 (STA) 的多个实例
- 仅限思杰端点管理
- 仅限 StoreFrontâ„¢
- Citrix Endpoint Management 和 StoreFront 协同使用

快速配置向导允许您在设备上配置以下设置：

- 虚拟服务器名称、IP 地址和端口
- 从不安全端口重定向到安全端口
- LDAP 服务器
- RADIUS 服务器
- 证书

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

- DNS 服务器
- Citrix 端点管理 和 Citrix 虚拟应用和桌面

  注意：要启用 SSO，您必须在会话操作的“**创建 NetScaler Gateway 会话配置文件 > 客户端体验**”选项卡中手动启用“**Web 应用程序单点登录**”选项。

NetScaler Gateway 支持用户直接连接到 Citrix Endpoint Management，这使用户能够访问其 Web、SaaS 和移动应用程序，以及访问 ShareFile。您还可以将设置配置到 StoreFront，这使用户能够访问其基于 Windows 的应用程序和虚拟桌面。

运行快速配置向导时，将根据您的 Citrix Endpoint Management 和 StoreFront 设置创建以下策略：

- 会话策略，包括适用于 Receiver、Receiver for Web、Citrix Secure Access™ 客户端和 Program Neighborhood Agent 的策略和配置文件
- 无客户端访问
- LDAP 和 RADIUS 身份验证

使用快速配置向导配置设置

您可以使用快速配置向导在 NetScaler Gateway 中配置设置，以启用与 Citrix Endpoint Management 或 StoreFront 的通信。完成配置后，向导会创建 NetScaler Gateway、Endpoint Management 和 StoreFront 之间通信的正确策略。这些策略包括身份验证、会话和无客户端访问策略。向导完成后，策略将绑定到虚拟服务器。

完成快速配置向导后，NetScaler Gateway 可以与 Endpoint Management 或 StoreFront 通信，用户可以访问其基于 Windows 的应用程序和虚拟桌面以及 Web、SaaS 和移动应用程序。然后，用户可以直接连接到 Endpoint Management。

在向导中，您将配置以下设置：

- 虚拟服务器名称、IP 地址和端口
- 从不安全端口重定向到安全端口
- 证书
- LDAP 服务器
- RADIUS 服务器
- 用于身份验证的客户端证书（仅适用于双因素身份验证）
- 端点管理 或 应用商店

快速配置向导支持 LDAP、RADIUS 和客户端证书身份验证。您可以通过遵循以下准则在向导中配置双因素身份验证：

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

- 如果您选择 LDAP 作为主要身份验证类型，则可以将 RADIUS 配置为辅助身份验证类型。
- 如果您选择 RADIUS 作为主要身份验证类型，则可以将 LDAP 配置为辅助身份验证类型。
- 如果您选择客户端证书作为主要身份验证类型，则可以将 LDAP 或 RADIUS 配置为辅助身份验证类型。

您不能使用快速配置向导创建多个 LDAP 身份验证策略。例如，您想要配置一个在 **Server Logon Name Attribute** 字段中使用 sAMAccountName 的策略，以及第二个在 **Server Logon Name Attribute** 字段中使用用户主体名称 (UPN) 的 LDAP 策略。要配置这些单独的策略，请使用 NetScaler Gateway 配置实用程序创建身份验证策略。有关更多信息，请参阅 配置 LDAP 身份验证。

您可以使用以下方法在快速配置向导中为 NetScaler Gateway 配置证书：

- 选择设备上已安装的证书。
- 安装证书和私钥。
- 选择测试证书。 **注意**：如果使用测试证书，则必须添加证书中的完全限定域名 (FQDN)。

您可以通过以下两种方式之一打开**快速配置向导**：

- 当您位于 NetScaler Gateway 登录页面并在**部署类型**中选择 **NetScaler Gateway** 时，将显示**主页**选项卡。如果您在**部署类型**中选择任何其他选项，则不会显示**主页**选项卡。
- 从 NetScaler Gateway 详细信息窗格中的链接**创建/监视 NetScaler Gateway**。如果您安装了启用 NetScaler 功能的许可证，则会显示该链接。如果您的设备仅获得 NetScaler Gateway 许可，则不会显示该链接。

首次运行向导后，您可以再次运行向导以创建更多虚拟服务器和设置。

重要提示：

如果使用快速配置向导配置额外的 NetScaler Gateway 虚拟服务器，则必须使用唯一的 IP 地址。您不能使用现有虚拟服务器上使用的相同 IP 地址。例如，您有一个 IP 地址为 192.168.10.5 且端口号为 80 的虚拟服务器。您运行快速配置向导以创建第二个 IP 地址为 192.168.10.5 且端口号为 443 的虚拟服务器。当您尝试保存配置时，会发生错误。

使用快速配置向导配置设置

1. 在配置实用程序中，执行以下操作之一：

   a. 如果设备仅获得 NetScaler Gateway 许可，请单击**主页**选项卡。

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

   b. 如果设备已获得包含 NetScaler 功能的许可，请在“Configuration”（配置）选项卡上的导航窗格中，单击 **NetScaler Gateway**，然后在详细信息窗格中的“**Getting Started**”（入门）下，单击“**Configure NetScaler Gateway for Enterprise Store**”（为企业商店配置 NetScaler Gateway）。

2. 在控制板中，单击**创建新的 NetScaler Gateway**。
3. 在 **NetScaler Gateway 设置**中，配置以下内容：
   a. 在**名称**中，键入虚拟服务器的名称。
   b. 在 **IP 地址**中，键入虚拟服务器的 IP 地址。
   c. 在**端口**中，键入端口号。默认端口号为 443。
   d. 选择“将来自端口 80 的请求重定向到安全端口”，以允许来自端口 80 的用户连接转到端口 443。
4. 单击**继续**。
5. 在“证书”页面上，执行以下操作之一：
   a. 单击**选择证书**，然后在“证书”中，选择证书。
   b. 单击**安装证书**，然后在**选择证书**和**选择密钥**中，单击**浏览**以导航到证书和私钥。
   c. 单击**使用测试证书**，然后在“证书 FQDN”中输入测试证书中包含的完全限定域名 (FQDN)。
6. 单击**继续**。
7. 在“身份验证设置”中，执行以下操作：
   a. 在**主身份验证**中，选择 LDAP、RADIUS 或证书。
   b. 选择身份验证服务器，或配置在上一步中选择的身份验证类型的设置。如果选择“证书”，则选择客户端证书或安装新的客户端证书。
   c. 在**辅助身份验证**中，选择身份验证类型，然后配置身份验证服务器设置。
8. 单击**继续**。

完成网络和身份验证设置配置后，即可配置 Citrix Endpoint Management 或 Citrix Virtual Apps and Desktops (StoreFront) 设置。

配置企业应用商店设置

NetScaler Gateway 仅通过 Endpoint Management 支持用户访问 Web、SaaS 和移动应用程序以及 ShareFile。如果您还部署 StoreFront，用户可以访问基于 Windows 的应用程序和虚拟桌面。您可以为以下选项配置设置：

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

- 端点管理 仅
- 仅 StoreFront
- Endpoint Management 和 StoreFront 协同使用

从上述过程单击“**继续**”后，您可以为部署方案配置设置。以下过程从“Citrix 集成设置”页面开始。

创建虚拟服务器后，在快速配置向导中编辑虚拟服务器不允许您更改 Citrix Endpoint Management 或 Citrix Virtual Apps and Desktops 设置。

例如，如果在配置“**Citrix Enterprise Store**”设置之前的任何阶段取消虚拟服务器的配置，向导将自动选择 StoreFront，而不配置任何设置。出现此情况时，您可以编辑虚拟服务器详细信息以配置 StoreFront，但无法切换到 Citrix Endpoint Management。要切换，您必须创建新的虚拟服务器，并且在配置过程中不得随时取消向导。如果您不需要 StoreFront 虚拟服务器，可以使用快速配置向导将其删除。

仅为 StoreFront 配置设置

1. 单击 **Citrix 虚拟应用和桌面**。
2. 在“**部署类型**”中，选择“**StoreFront**”。
3. 在“**StoreFront FQDN**”中，输入 StoreFront 服务器的完全限定域名 (FQDN)。
4. 在“**Receiver for Web 路径**”中，保留默认路径或输入您自己的路径。
5. 选择“**HTTPS**”以实现安全用户连接。
6. 在“**单点登录域**”中，输入 StoreFront 的域。
7. 在“**STA URL**”中，如果您部署 StoreFront 并提供对 Citrix Virtual Apps 中的已发布应用程序或 Citrix Virtual Desktops 中的虚拟桌面的访问，请输入运行安全票证颁发机构 (STA) 的服务器的完整 IP 地址或 FQDN。
8. 点击**完成**。

当用户通过 NetScaler Gateway 连接到 StoreFront 时，用户可以从 Receiver for Web 或 Receiver 启动其应用程序和桌面。

仅配置 Endpoint Management 的设置

1. 点击 **Citrix 端点管理**。
2. 在 **App Controller FQDN** 中，输入端点管理的 FQDN。
3. 点击**完成**。

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

NetScaler Gateway 向导

您可以使用 NetScaler Gateway 向导配置设备上的以下设置：

- 虚拟服务器
- 证书
- 名称服务提供程序
- 身份验证
- 授权
- 端口重定向
- 无客户端访问
- SharePoint 的无客户端访问

使用 NetScaler Gateway 向导配置设置

运行安装向导后，您可以运行 NetScaler Gateway 向导以配置 NetScaler Gateway 上的其他设置。您可以从配置实用程序运行 NetScaler Gateway 向导。

NetScaler Gateway 附带一个测试证书。如果您没有从证书颁发机构 (CA) 获取的签名证书，您可以在使用 NetScaler Gateway 向导时使用测试证书。当您收到签名证书时，您可以删除测试证书并安装签名证书。Citrix 建议在向用户公开 NetScaler Gateway 之前获取签名证书。

注意：您可以在 NetScaler Gateway 向导中创建证书签名请求 (CSR)。如果您使用 NetScaler Gateway 向导创建 CSR，您必须退出向导，然后在从证书颁发机构收到签名证书后再次启动向导。有关证书的更多信息，请参阅 安装和管理证书。

在 NetScaler Gateway 向导中配置虚拟服务器时，您可以配置 Internet 协议版本 6 (IPv6) 的用户连接。有关使用 IPv6 进行用户连接的更多信息，请参阅 配置 IPv6 以进行用户连接。

启动 NetScaler Gateway 向导

1. 在配置实用程序中，单击“配置”选项卡，然后在导航窗格中单击“NetScaler Gateway”。
2. 在详细信息窗格中，在“入门”下，单击“NetScaler Gateway 向导”。
3. 单击“下一步”，然后按照向导中的说明进行操作。

安装向导

您可以使用安装向导配置设备上的以下初始设置：

- 系统 IP 地址和子网掩码

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

- 映射的 IP 地址和子网掩码
- 主机名
- 默认网关
- 许可证

注意：在运行安装向导之前，请从 Citrix 网站下载您的许可证。有关详细信息，请参阅 许可 NetScaler Gateway

已发布应用程序向导

您可以使用已发布应用程序向导配置 NetScaler Gateway，以连接到内部网络中运行 Citrix Virtual Apps and Desktops 的服务器。使用已发布应用程序向导，您可以：

- 为连接到服务器场选择一个虚拟服务器。
- 配置 StoreFront、单点登录和安全票证颁发机构的用户连接设置。
- 为 SmartAccess 创建或选择会话策略。

在向导中，您还可以为用户连接创建会话策略表达式。有关配置 NetScaler Gateway 以连接到服务器场的详细信息，请参阅 将 NetScaler Gateway 与 StoreFront 集成。

集成式 Citrix Endpoint Management 配置

您可以使用 Citrix Endpoint Management MDM 部署 NetScaler Gateway，它提供扩展能力、确保应用程序的高可用性并维护安全性。要使用 Citrix Endpoint Management 配置，您需要安装版本 10.1，内部版本 120.1316.e。

集成式 Citrix Endpoint Management 配置会创建以下内容：

- 用于 Device Manager 的负载平衡服务器。
- 用于带电子邮件筛选的 Microsoft Exchange 的负载平衡服务器。
- 用于 ShareFile 的负载平衡服务器。

有关使用集成式 Citrix Endpoint Management 配置创建设置的更多信息，请参阅配置您的 Citrix Endpoint Management 环境的设置

配置 NetScaler Gateway

在 NetScaler Gateway 上配置基本网络设置后，您可以配置详细设置，以便用户可以连接到安全网络中的网络资源。这些设置包括：

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

- 虚拟服务器。您可以在 NetScaler Gateway 上配置多个虚拟服务器，这允许您根据需要实施的用户场景创建不同的策略。每个虚拟服务器都有自己的 IP 地址、证书和策略集。例如，您可以配置一个虚拟服务器，并根据用户在组中的成员身份以及您绑定到虚拟服务器的策略，将用户限制为内部网络中的网络资源。您可以使用以下方法创建虚拟服务器：
  - 快速配置向导
  - NetScaler Gateway 向导
  - 配置实用程序
- 高可用性。当您在网络中部署两台 NetScaler Gateway 设备时，可以配置高可用性。如果主设备发生故障，辅助设备可以接管，而不会影响用户会话。
- 证书。您可以使用证书来保护用户与 NetScaler Gateway 的连接。创建证书签名请求 (CSR) 时，您需要将完全限定域名添加到证书中。您可以将证书绑定到虚拟服务器。
- 身份验证。NetScaler Gateway 支持多种身份验证类型，包括本地 LDAP、RADIUS、SAML、客户端证书和 TACACS+。此外，您还可以配置级联和双因素身份验证。 注意：如果您使用 RSA、Safeword 或 Gemalto Protiva 进行身份验证，则通过 RADIUS 配置这些类型。
- 用户连接。您可以使用会话配置文件配置用户连接。在配置文件中，您可以确定用户可以登录的插件以及用户可能需要的任何限制。然后，您可以使用一个配置文件创建策略。您可以将会话策略绑定到用户、组和虚拟服务器。
- 主页。您可以使用默认的访问界面作为主页，也可以创建自定义主页。用户成功登录 NetScaler Gateway 后，主页将显示。
- 端点分析。您可以在 NetScaler Gateway 上配置策略，以便在用户登录时检查用户设备上的软件、文件、注册表项、进程和操作系统。端点分析通过要求用户设备具有所需的软件来提高网络安全性。

使用配置实用程序

配置实用程序允许您配置大多数 NetScaler Gateway 设置。您可以使用 Web 浏览器访问配置实用程序。

登录配置实用程序

1. 在 Web 浏览器中，键入 NetScaler Gateway 的系统 IP 地址，例如 `http://192.168.100.1`。 注意：NetScaler Gateway 预配置的默认 IP 地址为 192.168.100.1，子网掩码为 255.255.0.0。
2. 在“用户名”和“密码”中，键入 `nsroot.`.
3. 在“部署类型”中，选择 NetScaler Gateway，然后单击“登录”。

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

首次登录配置实用程序时，默认会在“**主页**”选项卡上打开“仪表板”。在“**主页**”选项卡上，您可以使用快速配置向导来配置虚拟服务器、身份验证、证书和 Citrix Endpoint Management 的设置。您还可以在快速配置向导中配置 StoreFront 设置。

有关配置 NetScaler Gateway 的更多信息，请参阅：

- 使用设置向导配置初始设置。
- 使用快速配置向导配置设置
- 使用 NetScaler Gateway 向导配置设置。

创建虚拟服务器

虚拟服务器是用户登录的访问点。每个虚拟服务器都有自己的 IP 地址、证书和策略集。虚拟服务器由接受传入流量的 IP 地址、端口和协议组合而成。虚拟服务器包含用户登录设备时的连接设置。您可以在虚拟服务器上配置以下设置：

- 证书
- 身份验证
- 策略
- 书签
- 地址池（也称为 IP 池或内网 IP）
- 使用 NetScaler Gateway 进行双跳 DMZ 部署
- 安全票证颁发机构
- SmartAccess ICA® 代理会话传输

如果运行 NetScaler Gateway 向导，可以在向导中创建虚拟服务器。您可以通过以下方式配置更多虚拟服务器：

- **通过虚拟服务器节点**。此节点位于配置实用程序的导航窗格中。您可以使用配置实用程序添加、编辑和删除虚拟服务器。
- **使用快速配置向导**。如果在您的环境中部署 Citrix Endpoint Management™ 或 StoreFront，可以使用快速配置向导创建虚拟服务器以及部署所需的所有策略。

如果您希望用户登录并使用特定的身份验证类型（例如 RADIUS），可以配置一个虚拟服务器并为其分配一个唯一的 IP 地址。当用户登录时，他们将被定向到虚拟服务器，然后系统会提示他们输入 RADIUS 凭据。

您还可以配置用户登录 NetScaler Gateway 的方式。您可以使用会话策略来配置用户软件类型、访问方法以及用户登录后看到的主页。

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

创建虚拟服务器

您可以使用 NetScaler Gateway GUI 或快速配置向导添加、修改、启用或禁用以及删除虚拟服务器。有关使用快速配置向导配置虚拟服务器的更多信息，请参阅 使用快速配置向导配置设置。

注意：

VPN 虚拟服务器默认支持 DTLS 1.0 版。要启用 DTLS 1.2 版，请参阅 使用 SSL VPN 虚拟服务器配置 DTLS VPN 虚拟服务器。

HTTP QUIC VPN 虚拟服务器

从版本 14.1 build 8.x 开始，NetScaler Gateway 支持在浏览器上使用 HTML5 通过 QUIC 发送 ICA 流量并启动 Citrix DaaS 会话。您可以创建服务类型为 HTTP QUIC 的 VPN 虚拟服务器，以便在 HTML5 客户端上通过 QUIC 启动 Citrix DaaS 应用程序，而无需客户端插件软件。以前，Citrix DaaS 应用程序必须通过浏览器使用 Citrix Workspace 应用程序客户端插件软件或使用 WebSockets（无客户端访问）的 HTML5 客户端应用程序启动。

HTML5 客户端支持 WebTransport 协议。WebTransport 协议使用基于 QUIC 的 HTTP3 在客户端和 Web 服务器之间建立通信。有关基于 QUIC 的 HTTP 的更多信息，请参阅 基于 QUIC 的 HTTP 协议。

使用 GUI 配置 HTTP QUIC VPN 虚拟服务器

1. 配置 HTTP QUIC VPN 虚拟服务器。
   a. 导航到 **配置 > NetScaler 网关 > 虚拟服务器**。
   b. 在 **NetScaler Gateway Virtual Servers** 页面上，单击 **Add**。
   c. 在 **Protocol** 中，选择 **HTTP_QUIC**。
   d. 根据需要更新其余字段，然后单击 **OK**。
2. 在 HTTP 配置文件上启用 HTTP/3 WebTransport。
   - 导航到 **System > Profiles > HTTP Profiles**。在 **HTTP/3** 部分中，启用 **HTTP/3 WebTransport** 复选框。有关 HTTP 配置文件的详细信息，请参阅 HTTP 配置。

使用 CLI 配置 HTTP QUIC VPN 虚拟服务器

1. 配置服务类型为 `HTTP QUIC` 的 VPN 虚拟服务器。

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

```
add vpn vserver <VPN server name> -service type <HTTP_QUIC> -dtls <off>
-Listenpolicy <NONE> -httpProfileName <name of the HTTP QUIC profile>
-deploymentType <ICA_STOREFRONT> -vserverFqdn <URL>
```

2. 在 HTTP 配置文件上启用 HTTP/3 WebTransport。

`set httpprofile nshttp_default_http_quic_profile -http3webTransport ENABLED`

以下 show 命令的输出显示参数 `HTTP/3 WebTransport: ENABLED`。此参数指示正在使用服务类型 `HTTP QUIC` 在客户端和 VPN 虚拟服务器之间发送 WebTransport 流量。

```
sh httpprofile <name>



HTTP/2 Strict Cipher: ENABLED

        HTTP/3: ENABLED

        HTTP/3 maximum header field section size: 24576

        HTTP/3 maximum header table size: 4096

        HTTP/3 maximum header blocked streams: 100

        HTTP/3 WebTransport: ENABLED

        gRPC Buffer Limit: 131072

        gRPC Buffer Timeout: 1000

        gRPC Length Delimited Message: ENABLED

        Apdex Client Response Threshold: 500

        HTTP pipeline req buffer size: 131072

        Reference count: 2
```

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

注意：

- SSL 和 HTTP QUIC VPN 虚拟服务器的 IP 地址和端口号必须相同。但是，必须在 SSL VPN 虚拟服务器上禁用 DTLS，因为不能在同一个 IP 地址和端口号上同时运行 DTLS 和 HTTP_QUIC。有关 DTLS VPN 虚拟服务器的详细信息，请参阅 使用 SSL VPN 虚拟服务器配置 DTLS VPN 虚拟服务器。
- 配置了替代服务值设置为 `Altsvc=h3=":port number"` 的 HTTP 配置文件必须绑定到 SSL VPN 虚拟服务器。有关替代服务参数的详细信息，请参阅 HTTP 负载平衡配置的 HTTP/2。

使用 GUI 创建虚拟服务器

1. 导航到 **NetScaler Gateway > 虚拟服务器**。
2. 在详细信息窗格中，单击 **添加**。
3. 根据您的要求配置设置。
4. 单击 **创建**，然后单击 **关闭**。

使用 CLI 创建虚拟服务器

在命令提示符下，键入：

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

示例：

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

将网络配置文件绑定到 VPN 虚拟服务器时的注意事项

您可以创建网络配置文件（net profile），以配置设备使用指定的源 IP 地址，并将网络配置文件绑定到 VPN 虚拟服务器。但是，在将网络配置文件绑定到 VPN 虚拟服务器时，请注意以下事项。

- 当您将网络配置文件绑定到 NetScaler Gateway 虚拟服务器时，它会为虚拟服务器选择一个特定的 SNIP，以便在向后端服务器发送流量时使用。
- 如果没有绑定网络配置文件，并且存在多个 SNIP，NetScaler Gateway 会使用循环法选择要使用的 SNIP。

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

- 网络配置文件不适用于动态生成的服务（STA、SF 监视器）。对于 STA 和其他动态生成的服务，您可以直接将网络配置文件绑定到这些监视器，并且这些监视器会在此时使用。但是，如果同一设备上有多个网关，则所有网关都将为配置的监视器使用相同的网络配置文件。

  有关网络配置文件的更多详细信息，请参阅 使用指定的源 IP 进行后端通信。

DTLS VPN 虚拟服务器配置中用于 UDP 启动的网络配置文件源 IP 地址

从版本 14.1 build 17.38 开始，配置了 DTLS 侦听器的 NetScaler Gateway 会从网络配置文件中选择源 IP 地址，以与虚拟投递代理 (VDA) 建立 UDP 连接。确保网络配置文件已绑定到 SSL VPN 虚拟服务器。

运行以下 CLI 命令以在 VPN 虚拟服务器中配置网络配置文件：

```
add ip <IPAddress><netmask> -type SNIP

add netprofile net1 -srcIP <IPAddress>

set vpn vserver <name> -netProfile net1
```

要验证是否使用了所选的源 IP 地址，请运行 `show connectiontable` CLI 命令。

虚拟服务器上的当前用户和总连接用户

当前用户： 登录到特定虚拟服务器的用户数量。建议您监视当前用户以跟踪 CCU。

总连接用户： 通过特定虚拟服务器建立一个或多个活动连接的用户数量。总连接用户数量主要用于 ICA 代理。

您可以在以下场景中使用总连接用户计数器：

- 假设已建立 ICA 连接，但未建立相应的身份验证、授权和审计会话。在这种情况下，用户启动应用程序或桌面并关闭浏览器，然后继续使用已启动的应用程序或桌面。身份验证、授权和审计会话超时，但连接仍然处于活动状态。连接用户总数可用于识别仍处于连接状态的用户。
- 在 HDX™ 优化路由中，身份验证网关和 ICA 网关可以位于不同的设备上。在这种情况下，连接用户总数可用于识别 ICA 网关上的连接用户数。

注意事项：

- 当存在活动会话（尚未超时）但这些会话上没有活动连接时，当前用户数会超过连接用户总数。例如，用户启动应用程序或桌面后立即将其关闭，但未从身份验证、授权和审计会话中注销。
- 如果身份验证、授权和审计会话超时但 ICA 连接仍处于活动状态，则连接用户总数会超过当前用户数。

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

- 在纯 VPN 设置中（不涉及 ICA），当前用户数和连接用户总数相等。

配置虚拟服务器上的连接类型

创建和配置虚拟服务器时，可以配置以下连接选项：

- 仅使用 Citrix Workspace 应用程序连接到 Citrix Virtual Apps and Desktops，不带 SmartAccess、端点分析或网络层隧道功能。
- 使用 Citrix Secure Access™ 客户端和 SmartAccess 进行连接，允许使用 SmartAccess、端点分析和网络层隧道功能。
- 使用 Secure Hub 进行连接，该连接可从移动设备建立到 NetScaler Gateway 的微型 VPN 连接。
- 用户从多个设备通过 ICA 会话协议建立的并行连接。这些连接将迁移到单个会话，以防止使用多个通用许可证。

如果您希望用户无需用户软件即可登录，可以配置无客户端访问策略并将其绑定到虚拟服务器。

在虚拟服务器上配置基本或 SmartAccess 连接

1. 导航到 **NetScaler Gateway**，然后单击 **Virtual Servers**。
2. 在详细信息窗格中，单击**添加**。
3. 在**名称**中，键入虚拟服务器的名称。
4. 在**IP 地址**和**端口**中，键入虚拟服务器的 IP 地址和端口号。
5. 执行以下操作之一：
   - 若要仅允许 ICA 连接，请单击**基本模式**。
   - 若要允许用户使用 Secure Hub、Citrix Secure Access 客户端和 SmartAccess 登录，请单击 **SmartAccess 模式**。
   - 若要允许 SmartAccess 管理多个用户连接的 ICA 代理会话，请单击**ICA 代理会话迁移**。
6. 配置虚拟服务器的其他设置，单击**创建**，然后单击**关闭**。

为通配符虚拟服务器配置侦听策略

您可以配置 NetScaler Gateway 虚拟服务器，以限制虚拟服务器在特定 VLAN 上侦听的能力。您可以创建具有侦听策略的通配符虚拟服务器，该策略将其限制为处理指定 VLAN 上的流量。

配置参数如下：

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

参数	描述
名称	虚拟服务器的名称。名称是必需的，创建虚拟服务器后无法更改。名称不能超过 127 个字符，并且第一个字符必须是数字或字母。您还可以使用以下字符：at 符号 (@)、下划线 (_)、破折号 (-)、句点 (.)、冒号 (:)、井号 (#) 和空格。
IP	虚拟服务器的 IP 地址。对于绑定到 VLAN 的通配符虚拟服务器，该值始终为 *。
类型	服务的行为。您的选择包括 HTTP、SSL、FTP、TCP、SSL_TCP、UDP、SSL_BRIDGE、NNTP、DNS、ANY、SIP-UDP、DNS-TCP 和 RTSP。
端口	虚拟服务器侦听用户连接的端口。端口号必须介于 0 到 65535 之间。对于绑定到 VLAN 的通配符虚拟服务器，该值通常为 *。
侦听优先级	分配给侦听策略的优先级。优先级按相反顺序评估；数字越小，分配给侦听策略的优先级越高。
侦听策略规则	策略规则用于标识虚拟服务器必须侦听的 VLAN。规则为 `CLIENT.VLAN.ID.EQ (<ipaddressat>)`。将 `<ipaddressat>` 替换为分配给 VLAN 的 ID。

创建具有侦听策略的通配符虚拟服务器

1. 在导航窗格中，展开 **NetScaler Gateway**，然后单击 **Virtual Servers**。
2. 在详细信息窗格中，单击 **Add**。
3. 在 **Name** 中，键入虚拟服务器的名称。
4. 在 **Protocol** 中，选择协议。
5. 在 **IP 地址**中，键入虚拟服务器的 IP 地址。
6. 在 **端口**中，键入虚拟服务器的端口。
7. 在 **高级** 选项卡上，在“侦听策略”下，在 **侦听优先级** 中，键入侦听策略的优先级。
8. 在“侦听策略规则”旁边，单击 **配置**。

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

9. 在 **创建表达式** 对话框中，单击 **添加**，配置表达式，然后单击 **确定**。
10. 单击 **创建**，然后单击 **关闭**。

在 NetScaler Gateway 上配置 IP 地址

您可以配置 IP 地址以登录配置实用程序和进行用户连接。NetScaler Gateway 配置了默认 IP 地址 192.168.100.1 和子网掩码 255.255.0.0 用于管理访问。当系统 IP (NSIP) 地址的用户配置值缺失时，将使用默认 IP 地址。

- NSIP 地址。用于 NetScaler Gateway 的管理 IP 地址，用于对设备进行所有管理相关的访问。NetScaler Gateway 也使用 NSIP 地址进行身份验证。
- **默认网关**。将安全网络外部的流量转发到 NetScaler Gateway 的路由器。
- **子网 IP (SNIP) 地址**。通过与辅助网络上的服务器通信来表示用户设备的 IP 地址。

SNIP 地址使用 1024 到 64000 端口。

NetScaler Gateway 如何使用 IP 地址

NetScaler Gateway 根据正在发生的功能从 IP 地址获取流量。以下列表描述了几个功能以及 NetScaler Gateway 如何为每个功能使用 IP 地址，作为一般指导原则：

- **身份验证。**NetScaler Gateway 使用的 IP 地址取决于身份验证服务器类型。
  - LDAP/RADIUS/TACACS 服务器。如果 AAAD 直接与身份验证虚拟服务器通信，则使用 NSIP 地址。
  - 如果使用负载均衡器作为代理，则负载均衡器使用 SNIP 地址进行身份验证。AAAD 使用 NSIP 地址与负载均衡器通信。NetScaler 使用的 IP 地址取决于与身份验证虚拟服务器通信的实体。
  - SAML/OAUTH/WEBAUTH 服务器：这些服务器使用 SNIP 地址进行通信。
- **从主页传输文件。**NetScaler Gateway 使用 SNIP 地址。
- **DNS 和 WINS 查询。**NetScaler Gateway 使用 SNIP 地址。
- **到安全网络中资源的网络流量。**NetScaler Gateway 使用 SNIP 地址或 IP 池，具体取决于 NetScaler Gateway 上的配置。
- **ICA 代理设置。** NetScaler Gateway 使用 SNIP 地址。

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

子网 IP 地址

子网 IP 地址允许用户从位于另一个子网上的外部主机连接到 NetScaler Gateway。添加子网 IP 地址时，路由表中会生成相应的路由条目。每个子网只生成一个条目。路由条目对应于子网中添加的第一个 IP 地址。

与系统 IP 地址和映射 IP 地址不同，在 NetScaler Gateway 的初始配置期间，不必强制指定子网 IP 地址。

映射的 IP 地址和子网 IP 地址使用端口 1024 到 64000。

添加子网 IP 地址

1. 在配置实用程序中，在“配置”选项卡上的导航窗格中，展开 **系统 \ > 网络**，然后单击 **IPs**。
2. 在详细信息窗格中，单击 **添加**。
3. 在“创建 IP”对话框中，在“IP 地址”中，键入 IP 地址。
4. 在“子网掩码”中，键入子网掩码。
5. 在“IP 类型”下，选择“子网 IP”，单击 **关闭**，然后单击 **创建**。

为用户连接配置 IPv6

您可以配置 NetScaler Gateway 以使用 Internet 协议版本 6 (IPv6) 侦听用户连接。配置以下设置之一时，您可以选中 IPv6 复选框，然后在对话框中输入 IPv6 地址：

- 全局设置 - 已发布的应用程序 - ICA® 代理
- 全局身份验证 - RADIUS
- 全局身份验证 - LDAP
- 全局身份验证 - TACACS
- 会话配置文件 - 已发布的应用程序 - ICA 代理
- NetScaler Gateway 虚拟服务器
- 创建身份验证服务器 - RADIUS
- 创建身份验证服务器 - LDAP
- 创建身份验证服务器 - TACACS
- 创建审计服务器
- 高可用性设置
- 绑定/解除绑定路由监视器以实现高可用性
- 虚拟服务器 (负载平衡)

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

当您将 NetScaler Gateway 虚拟服务器配置为侦听 IPv6 地址时，用户只能使用 Citrix Workspace 应用程序连接。使用 Citrix Secure Access 客户端的用户连接不支持 IPv6。

您可以使用以下准则在 NetScaler Gateway 上配置 IPv6：

- Citrix Virtual Apps 和 StoreFront。当您为用户连接配置 IPv6 并且如果存在使用 IPv6 的映射 IP 地址时，Citrix Virtual Apps 和 StoreFront 服务器也可以使用 IPv6。StoreFront 必须安装在 NetScaler Gateway 后面。当用户通过 NetScaler Gateway 连接时，IPv6 地址会转换为 IPv4。当连接返回时，IPv4 地址会转换为 IPv6。
- 虚拟服务器。当您运行 NetScaler Gateway 向导时，可以为虚拟服务器配置 IPv6。在 NetScaler Gateway 向导的“虚拟服务器”页面上，单击 IPv6 并输入 IP 地址。您只能通过使用 NetScaler Gateway 向导来为虚拟服务器配置 IPv6 地址。
- 其他。要为 ICA 代理、身份验证、审计和高可用性配置 IPv6，请在对话框中选择 IPv6 复选框，然后键入 IP 地址。

解析位于安全网络中的 DNS 服务器

如果您的 DNS 服务器位于防火墙后的安全网络中，并且防火墙正在阻止 ICMP 流量，则您无法测试与服务器的连接，因为防火墙正在阻止该请求。您可以通过执行以下步骤解决此问题：

- 创建具有自定义 DNS 监视器的 DNS 服务，该监视器解析为已知完全限定域名 (FQDN)。
- 在 NetScaler Gateway 上创建不可直接寻址的 DNS 虚拟服务器。
- 将服务绑定到虚拟服务器。

注意：

- 仅当您的 DNS 服务器位于防火墙后时，才配置 DNS 虚拟服务器和 DNS 服务。
- 如果您在设备上安装了 NetScaler 负载平衡许可证，则“虚拟服务器和服务”节点不会显示在导航窗格中。您可以通过展开“负载平衡”然后单击“虚拟服务器”来执行此过程。

配置 DNS 服务和 DNS 监视器

1. 在配置实用程序中，在“配置”选项卡上的导航窗格中，展开“虚拟服务器和服务”，然后单击“虚拟服务器”。
2. 在详细信息窗格中，单击“添加”。
3. 在“名称”中，键入服务的名称。
4. 在“协议”中，选择 DNS。
5. 在“IP 地址”中，键入 DNS 服务器的 IP 地址。
6. 在“端口”中，键入端口号。

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

7. 在“服务”选项卡上，单击“添加”。
8. 在“监视器”选项卡上，在“可用”下，选择“DNS”，单击“添加”，单击“创建”，然后单击“关闭”。
9. 在“创建虚拟服务器(负载平衡)”对话框中，单击“创建”，然后单击“关闭”。

接下来，使用过程配置 DNS 虚拟服务器创建 DNS 虚拟服务器，然后将 DNS 服务绑定到该虚拟服务器。

将 DNS 服务绑定到 DNS 虚拟服务器

1. 在“配置虚拟服务(负载平衡)”对话框中，在“服务”选项卡上，单击“添加”，选择 DNS 服务，单击“创建”，然后单击“关闭”。

配置 DNS 虚拟服务器

要配置 DNS 虚拟服务器，您需要指定名称和 IP 地址。与 NetScaler Gateway 虚拟服务器类似，您必须为 DNS 虚拟服务器分配一个 IP 地址。但是，此 IP 地址必须位于目标网络的内部侧，以便用户设备解析所有内部地址。此外，还要指定 DNS 端口。

注意：如果您在设备上安装了 NetScaler 负载平衡许可证，则 导航窗格中不会显示“虚拟服务器和服务”节点。您可以使用负载平衡虚拟服务器配置此功能。有关详细信息，请参阅 NetScaler 产品文档中的 NetScaler 文档。

配置 DNS 虚拟服务器

1. 在配置实用程序中，在“配置”选项卡上，在导航窗格中，展开“虚拟服务器和服务”，然后单击“虚拟服务器”。
2. 在详细信息窗格中，单击“添加”。
3. 在“名称”中，键入虚拟服务器的名称。
4. 在“IP 地址”中，键入 DNS 服务器的 IP 地址。
5. 在“端口”中，键入 DNS 服务器侦听的端口。
6. 在“协议”中，选择“DNS”，然后单击“创建”。

最后，根据您的部署需求，通过以下两种方法之一将 DNS 虚拟服务器与 NetScaler Gateway 关联：

- 将服务器全局绑定到 NetScaler Gateway。
- 按每个虚拟服务器绑定 DNS 虚拟服务器。

如果您全局部署 DNS 虚拟服务器，所有用户都可以访问它。然后，您可以通过将 DNS 虚拟服务器绑定到虚拟服务器来限制用户。

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

配置名称服务提供程序

NetScaler Gateway 使用名称服务提供程序将 Web 地址转换为 IP 地址。

运行 NetScaler Gateway 向导时，可以配置 DNS 服务器或 WINS 服务器。您还可以使用配置实用程序配置其他 DNS 或 WINS 服务器。

将 DNS 服务器添加到 NetScaler Gateway

1. 在配置实用程序中，在“配置”选项卡上的导航窗格中，展开 NetScaler Gateway，然后单击“全局设置”。
2. 在详细信息窗格中，在“设置”下，单击“更改全局设置”。
3. 在“网络配置”选项卡上，单击“添加”。
4. 在“插入名称服务器”对话框中，在“IP 地址”中，键入 DNS 服务器的 IP 地址，单击“创建”，然后单击“关闭”。
5. 在配置实用程序中单击“确定”。

将 WINS 服务器添加到 NetScaler Gateway

1. 在配置实用程序中，在“配置”选项卡上的导航窗格中，展开 NetScaler Gateway，然后单击“全局设置”。
2. 在详细信息窗格中，在“设置”下，单击“更改全局设置”。
3. 在“网络配置”选项卡上，在“WINS 服务器 IP”中，键入 WINS 服务器的 IP 地址，然后单击“确定”。

接下来，指定 DNS 虚拟服务器名称和 IP 地址。与 NetScaler Gateway 虚拟服务器一样，必须为虚拟服务器分配一个 IP 地址。但是，此 IP 地址必须位于目标网络的内部，以便用户设备正确解析所有内部地址。您还必须指定 DNS 端口。

如果您为名称解析配置了 DNS 服务器和 WINS 服务器，则可以使用 NetScaler Gateway 向导选择哪个服务器首先执行名称查找。

指定名称查找优先级

1. 在配置实用程序中，单击“配置”选项卡，然后在导航窗格中单击“NetScaler Gateway”。
2. 在详细信息窗格中，在“入门”下，单击“NetScaler Gateway 向导”。
3. 单击“下一步”接受当前设置，直到显示“名称服务提供商”页面。
4. 在“名称查找优先级”中，选择 WINS 或 DNS，然后继续完成向导。

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

配置服务器发起的连接

对于每个已登录到 NetScaler Gateway 且启用了 IP 地址的用户，DNS 后缀会附加到用户名，并且 DNS 地址记录会添加到设备的 DNS 缓存中。此技术有助于为用户提供 DNS 名称，而不是用户的 IP 地址。

当 IP 地址分配给用户会话时，可以从内部网络连接到用户的设备。例如，使用远程桌面或虚拟网络计算 (VNC) 客户端连接的用户可以访问用户设备以诊断问题应用程序。两个具有内部网络 IP 地址的 NetScaler Gateway 用户（远程登录）也可以通过 NetScaler Gateway 相互通信。允许在设备上发现已登录用户的内部网络 IP 地址有助于这种通信。

远程用户可以使用以下 ping 命令来发现已登录到 NetScaler Gateway 的用户的内部网络 IP 地址：

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

服务器可以通过以下不同方式启动与用户设备的连接：

- TCP 或 UDP 连接。连接可以源自内部网络中的外部系统，也可以源自登录到 NetScaler Gateway 的另一台计算机。分配给每个登录到 NetScaler Gateway 的用户设备的内部网络 IP 地址用于这些连接。本文介绍了 NetScaler Gateway 支持的不同类型的服务器发起连接。 对于 TCP 或 UDP 服务器发起连接，服务器预先知道用户设备的 IP 地址和端口，并与其建立连接。NetScaler Gateway 会拦截此连接。

  然后，用户设备与服务器建立初始连接，服务器通过已知端口或从第一个配置端口派生的端口连接到用户设备。

  在此场景中，用户设备与服务器建立初始连接，然后使用嵌入此信息的应用程序特定协议与服务器交换端口和 IP 地址。这使得 NetScaler Gateway 能够支持活动 FTP 连接等应用程序。
- 端口命令。这用于活动 FTP 和某些 IP 语音协议中。
- 插件之间的连接。NetScaler Gateway 支持使用内部网络 IP 地址在插件之间建立连接。

  通过此类连接，使用相同 NetScaler Gateway 的两个 NetScaler Gateway 用户设备可以相互发起连接。此类示例是使用即时消息应用程序，例如 Office Communicator 或 Yahoo\! Messenger。

如果用户从 NetScaler Gateway 注销，但注销请求未到达设备，则用户可以使用任何设备再次登录，并用新会话替换之前的会话。此功能在每个用户分配一个 IP 地址的部署中可能很有用。

当用户首次登录 NetScaler Gateway 时，会创建一个会话并为用户分配一个 IP 地址。如果用户注销但注销请求丢失，或者用户设备未能执行干净注销，则会话将保留在系统中。如果用户尝试从同一设备或另一设备再次登录，则在成功身份验证后，将出现一个传输登录对话框。如果用户选择传输

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

登录，则 NetScaler Gateway 上的先前会话将关闭并创建一个新会话。登录传输在注销后仅两分钟内有效，如果同时从多个设备尝试登录，则最后一次登录尝试将替换原会话。

配置服务器发起连接的私有端口范围

从 Citrix Secure Access 客户端版本 23.10.1.7 开始，您可以为服务器发起的连接 (SIC) 配置一个范围从 49152 到 64535 的私有端口。配置私有端口可避免在使用端口在 Citrix Secure Access 客户端和客户端计算机上的第三方应用程序之间创建套接字时可能出现的冲突。这仅在 WFP 驱动程序正在使用时适用。

您可以使用 `SicBeginPort` Windows VPN 注册表配置私有端口。或者，您可以使用 NetScaler 上的 VPN 插件自定义 JSON 文件配置私有端口范围。

如果服务器发起连接，Citrix Secure Access 客户端将使用从 `SicBeginPort` Windows VPN 注册表开始的前 1000 个端口来创建套接字。如果注册表在客户端计算机上配置，则注册表设置优先于 NetScaler JSON 设置。

以下是 NetScaler 上 VPN 插件 JSON 配置的示例：

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



{"SicBeginPort" : 51000}
```

有关注册表设置的详细信息，请参阅 NetScaler Gateway Windows VPN 客户端注册表项。

注意：

用于创建套接字的默认端口范围是 62500–63500。

在 NetScaler Gateway 上配置路由

为了提供对内部网络资源的访问，NetScaler Gateway 将数据路由到您的内部安全网络。默认情况下，NetScaler Gateway 使用静态路由。

NetScaler Gateway 可以路由数据的网络取决于您配置 NetScaler Gateway 路由表的方式以及为 NetScaler Gateway 指定的默认网关。

NetScaler Gateway 路由表必须包含将数据路由到用户可能需要访问的任何内部网络资源所需的路由。

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

NetScaler Gateway 支持以下路由协议：

- 路由信息协议 (RIP v1 和 v2)
- 开放最短路径优先 (OSPF)
- 边界网关协议 (BGF)

配置静态路由

如果未使用动态路由，则在设置与另一个主机或网络的通信时，需要从 NetScaler Gateway 配置到新目标的静态路由。

配置静态路由

1. 在配置实用程序中，在“Configuration”（配置）选项卡上的导航窗格中，展开 **System \> Network \> Advanced**（系统 \> 网络 \> 高级），然后单击 **Routes**（路由）。
2. 在详细信息窗格的“Basic”（基本）选项卡上，单击 **Add**（添加）。
3. 配置路由设置，然后单击 **Create**（创建）。

测试静态路由

1. 在配置实用程序中，在导航窗格中，展开 **系统**，然后单击 **诊断**。
2. 在详细信息窗格中，在“实用程序”下，单击 **Ping**。
3. 在“参数”下，在“主机名”中，键入设备的名称。
4. 在“高级”下，在“源 IP 地址”中，键入设备的 IP 地址，然后单击 **运行**。

   如果您成功地与另一台设备通信，消息会指示传输和接收的数据包数量相同，并且没有丢失任何数据包。

   如果您未与另一台设备通信，状态消息会指示接收到零个数据包，并且所有数据包都已丢失。要纠正这种通信中断，请重复添加静态路由的过程。

要停止测试，请在 **Ping** 对话框中，单击 **停止**，然后单击 **关闭**。

配置自动协商

默认情况下，设备配置为使用自动协商，其中 NetScaler Gateway 同时双向传输网络流量并确定适当的适配器速度。如果您将默认设置保留为 自动协商，NetScaler Gateway 将使用全双工操作，其中网络适配器能够同时双向发送数据。

如果您禁用自动协商，NetScaler Gateway 将使用半双工操作，其中适配器可以在两个节点之间双向发送数据，但适配器一次只能使用一个方向。

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

对于首次安装，Citrix 建议您将 NetScaler Gateway 配置为对连接到设备的端口使用自动协商。在您首次登录并配置 NetScaler Gateway 后，您可以禁用自动协商。您无法全局配置自动协商。您必须为每个接口启用或禁用该设置。

启用或禁用自动协商

1. 在配置实用程序中，在“配置”选项卡上，在导航窗格中，展开 **“系统”\ >“网络”**，然后单击 **“接口”**。
2. 在详细信息窗格中，选择接口，然后单击 **“打开”**。
3. 在 **“配置接口”** 对话框中执行以下操作之一：
   - 要启用自动协商，请单击“自动协商”旁边的 **“是”**，然后单击 **“确定”**。
   - 要禁用自动协商，请单击“自动协商”旁边的 **“否”**，然后单击 **“确定”**。

在 NetScaler Gateway 上配置主机名和 FQDN

主机名是与许可证文件关联的 NetScaler Gateway 设备名称。主机名对于设备是唯一的，并在您下载通用许可证时使用。首次运行安装向导配置 NetScaler Gateway 时，您需要定义主机名。

完全限定域名 (FQDN) 包含在绑定到虚拟服务器的签名证书中。您无需在 NetScaler Gateway 上配置 FQDN。一个设备可以通过使用证书，为在 NetScaler Gateway 上配置的每个虚拟服务器分配一个唯一的 FQDN。

您可以通过查看证书的详细信息来查找证书的 FQDN。FQDN 位于证书的主题字段中。

查看证书的 FQDN

1. 在配置实用程序中，在“配置”选项卡上的导航窗格中，展开 **SSL**，然后单击 **证书**。
2. 在详细信息窗格中，选择一个证书，单击 **操作**，然后单击 **详细信息**。
3. 在“证书详细信息”对话框中，单击 **主题**。证书的 FQDN 将显示在列表中。

NetScaler Gateway 上的策略和配置文件

NetScaler Gateway 上的策略和配置文件允许您在特定场景或条件下管理和实施配置设置。单个策略声明或定义了在满足特定条件集时生效的配置设置。每个策略都有一个唯一的名称，并且可以有一个绑定到该策略的配置文件。

策略的工作原理

策略由布尔条件和称为配置文件的设置集合组成。在运行时评估条件以确定是否必须应用策略。

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

配置文件是使用特定参数的设置集合。配置文件可以有任何名称，并且可以在多个策略中重复使用。您可以在配置文件中配置多个设置，但每个策略只能包含一个配置文件。

您可以将配置了条件和配置文件的策略绑定到虚拟服务器、组、用户或全局。策略根据其控制的配置设置类型来引用。例如，在会话策略中，您可以控制用户登录方式以及用户可以保持登录状态的时间。

如果您将 NetScaler Gateway 与 Citrix Virtual Apps 结合使用，NetScaler Gateway 策略名称将作为筛选器发送到 Citrix Virtual Apps。在配置 NetScaler Gateway 以兼容 Citrix Virtual Apps 和 SmartAccess 时，您需要在 Citrix Virtual Apps 中配置以下设置：

- 设备上配置的虚拟服务器的名称。该名称将作为 NetScaler Gateway 场名称发送到 Citrix Virtual Apps。
- 预身份验证或会话策略的名称将作为筛选器名称发送。

有关配置 NetScaler Gateway 以兼容 Citrix Endpoint Management 的更多信息，请参阅 配置 Citrix Endpoint Management 环境的设置。

有关配置 NetScaler Gateway 以兼容 Citrix Virtual Apps and Desktops 的更多信息，请参阅 将 NetScaler Gateway 与 StoreFront 集成。

有关预身份验证策略的更多信息，请参阅 配置端点策略。

条件策略

配置策略时，您可以使用任何布尔表达式来表示策略适用的条件。配置条件策略时，您可以使用任何可用的系统表达式，例如：

- 客户端安全字符串
- 网络信息
- HTTP 标头和 Cookie
- 一天中的时间
- 客户端证书值

您还可以创建仅在用户设备满足特定条件时才应用的策略，例如 SmartAccess 的会话策略。

配置条件策略的另一个示例是针对用户更改身份验证策略。例如，您可以要求从内部网络外部（例如从家用计算机或通过移动设备使用 Micro VPN）使用 Citrix Secure Access™ 客户端连接的用户通过 LDAP 进行身份验证，而通过 WAN 连接的用户则使用 RADIUS 进行身份验证。

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

注意：如果策略规则配置为会话配置文件中的安全设置的一部分，则不能使用基于端点分析结果的策略条件。

策略的优先级

策略按照绑定的顺序进行优先级排序和评估。

以下两种方法确定策略优先级：

- 策略绑定的级别：全局、虚拟服务器、组或用户。策略级别从高到低排名如下：
  - 用户（最高优先级）
  - 组
  - 虚拟服务器
  - 全局（最低优先级）
- 数值优先级优先，无论策略绑定到哪个级别。如果全局绑定的策略优先级为一，而绑定到用户的另一个策略优先级为二，则全局策略优先。较低的优先级数字赋予策略更高的优先级。

在 NetScaler Gateway 上创建策略

您可以使用配置实用程序创建策略。创建策略后，将其绑定到相应的级别：用户、组、虚拟服务器或全局。当您将策略绑定到其中一个级别时，如果满足策略条件，用户将收到配置文件中的设置。每个策略和配置文件都有一个唯一的名称。

如果您的部署中包含 Citrix Endpoint Management 或 StoreFront，则可以使用快速配置向导配置此部署的设置。有关向导的更多信息，请参阅 使用向导配置 NetScaler Gateway 设备。

配置系统表达式

系统表达式指定策略强制执行的条件。例如，预认证策略中的表达式在用户登录时强制执行。会话策略中的表达式在用户通过身份验证并登录到 NetScaler Gateway 后进行评估和强制执行。

NetScaler Gateway 上的表达式包括：

- 通用表达式，用于限制用户在建立与 NetScaler Gateway 的连接时可以使用的对象。例如，请参阅：
  - 会话策略
- 客户端安全表达式，用于定义必须安装并在用户设备上运行的软件、文件、进程或注册表值。例如，请参阅：

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

  - 端点策略

- 基于网络的表达式，用于根据网络设置限制访问。例如，请参阅：
  - 流量策略
  - 授权策略

NetScaler Gateway 也可以用作 NetScaler 设备。设备上的一些表达式更适用于 NetScaler。通用表达式和基于网络的表达式通常与 NetScaler 一起使用，而不常与 NetScaler Gateway 一起使用。客户端安全表达式用于 NetScaler Gateway，以确定用户设备上安装了正确的项目。

配置客户端安全表达式

表达式是策略的一个组成部分。表达式表示针对请求或响应进行评估的单个条件。您可以创建简单的表达式安全字符串来检查条件，例如：

- 用户设备操作系统，包括服务包
- 防病毒软件版本和病毒定义
- 文件
- 进程
- 注册表值
- 用户证书

NetScaler Gateway 上的证书管理

在 NetScaler Gateway 上，您可以使用证书创建安全连接并对用户进行身份验证。

为了建立安全连接，连接的一端需要服务器证书。连接的另一端需要颁发服务器证书的证书颁发机构 (CA) 的根证书。

- 服务器证书。服务器证书用于证明服务器的身份。NetScaler Gateway 需要这种类型的数字证书。
- 根证书。根证书用于标识签署服务器证书的 CA。根证书属于证书颁发机构。用户设备需要这种类型的数字证书来验证服务器证书。

当用户设备上的 Web 浏览器建立安全连接时，服务器会将其证书发送到设备。

当用户设备收到服务器证书时，Web 浏览器（例如 Internet Explorer）会检查是哪个 CA 颁发了该证书，以及该 CA 是否受用户设备信任。如果 CA 不受信任，或者它是一个测试证书，Web 浏览器会提示用户接受或拒绝该证书（实际上是接受或拒绝访问该站点的能力）。

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

NetScaler Gateway 支持以下三种类型的证书：

- 绑定到虚拟服务器的测试证书，也可用于连接到服务器场。NetScaler Gateway 附带预安装的测试证书。
- PEM 或 DER 格式的证书，由 CA 签名并与私钥配对。
- PKCS#12 格式的证书，用于存储或传输证书和私钥。PKCS#12 证书通常从现有 Windows 证书导出为 PFX 文件，然后安装在 NetScaler Gateway 上。

Citrix® 建议使用由受信任的 CA（例如 Thawte 或 Verisign）签名的证书。

创建证书签名请求

为了通过 SSL 或 TLS 提供安全通信，NetScaler Gateway 上需要服务器证书。在将证书上传到 NetScaler Gateway 之前，您需要生成证书签名请求 (CSR) 和私钥。您可以使用 NetScaler Gateway 向导或配置实用程序中包含的“创建证书请求”来创建 CSR。“创建证书请求”会创建一个 .csr 文件，该文件会通过电子邮件发送给证书颁发机构 (CA) 进行签名，并生成一个保留在设备上的私钥。CA 会对证书进行签名，并将其返回到您提供的电子邮件地址。收到签名证书后，您可以将其安装在 NetScaler Gateway 上。当您从 CA 收到证书后，您将证书与私钥配对。

重要提示：

当您使用 NetScaler Gateway 向导创建 CSR 时，您必须退出向导并等待 CA 向您发送签名证书。收到证书后，您可以再次运行 NetScaler Gateway 向导以创建设置并安装证书。有关 NetScaler Gateway 向导的更多信息，请参阅 使用 NetScaler Gateway 向导配置设置。

使用 NetScaler Gateway 向导创建 CSR

1. 在配置实用程序中，单击“配置”选项卡，然后在导航窗格中单击 **NetScaler Gateway**。
2. 在详细信息窗格的“入门”下，单击 **NetScaler Gateway** 向导。
3. 按照向导中的说明操作，直到出现“指定服务器证书”页面。
4. 单击“**创建证书签名请求**”并填写字段。 注意：完全限定域名 (FQDN) 不需要与 NetScaler Gateway 主机名相同。FQDN 用于用户登录。
5. 单击“**创建**”将证书保存到您的计算机，然后单击“**关闭**”。
6. 退出 NetScaler Gateway 向导，不保存您的设置。

使用 NetScaler GUI 创建 CSR

您也可以使用 NetScaler GUI 创建 CSR，而无需运行 NetScaler Gateway 向导。

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

1. 导航到“**流量管理**”>“**SSL**”>“**SSL 文件**”，然后选择“**创建证书签名请求 (CSR)**”。
2. 完成证书设置，然后单击“**创建**”。

创建证书和私钥后，将证书通过电子邮件发送给 CA，例如 Thawte 或 Verisign。

有关详细步骤，请参阅 创建证书签名请求。

在 NetScaler Gateway 上安装签名证书

从证书颁发机构 (CA) 收到签名证书后，将其与设备上的私钥配对，然后在 NetScaler Gateway 上安装证书。

使用 GUI 将签名证书与私钥配对

1. 使用 Secure Shell (SSH) 程序（例如 WinSCP）将证书复制到 NetScaler Gateway 的 nsconfig/ssl 文件夹。
2. 在配置实用程序中，在“配置”选项卡上的导航窗格中，展开 **SSL > 证书**。
3. 在 **SSL 证书** 页面中，单击 **开始**。
4. 在详细信息窗格中，单击 **安装**。
5. 在 **证书-密钥对名称** 中，键入证书的名称。
6. 在 **证书文件名** 中，单击 **设备**。
7. 导航到证书，单击 **选择**，然后单击 **打开**。
8. 在 **密钥文件名** 中，单击 **设备**。私钥的名称与证书签名请求 (CSR) 的名称相同。私钥位于 NetScaler Gateway 的 \\nsconfig\\ssl 目录中。
9. 选择私钥，然后单击 **打开**。
10. 如果证书是 PEM 格式，请在 **密码** 中键入私钥的密码。
11. 如果您想配置证书过期通知，请选择 **Notify When Expires**。
12. 在 **Notification Period** 中，键入天数，单击 **Create**，然后单击 **Close**。

使用 GUI 将证书和私钥绑定到虚拟服务器

创建并链接证书和私钥对后，将其绑定到虚拟服务器。

1. 在配置实用程序中，在“配置”选项卡上的导航窗格中，展开 **NetScaler Gateway > Virtual Servers**。
2. 在详细信息窗格中，单击一个虚拟服务器，然后单击 **Open**。
3. 在“证书”选项卡上，在 **Available** 下，选择一个证书，单击 **Add**，然后单击 **OK**。

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

使用 CLI 将证书和私钥绑定到虚拟服务器

在命令提示符下，键入：

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

示例：

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

注意： 如果设备证书不需要 OCSP 检查，则 oscpCheck 是可选的。

使用 GUI 从虚拟服务器解除绑定测试证书

安装签名证书后，解除绑定到虚拟服务器的任何测试证书。您可以使用配置实用程序解除绑定测试证书。

1. 在配置实用程序中，在“配置”选项卡上的导航窗格中，展开 **NetScaler Gateway > Virtual Servers**。
2. 在详细信息窗格中，单击一个虚拟服务器，然后单击 **Open**。
3. 在“证书”选项卡上，在“**已配置**”下，选择测试证书，然后单击“**删除**”。

配置中间证书

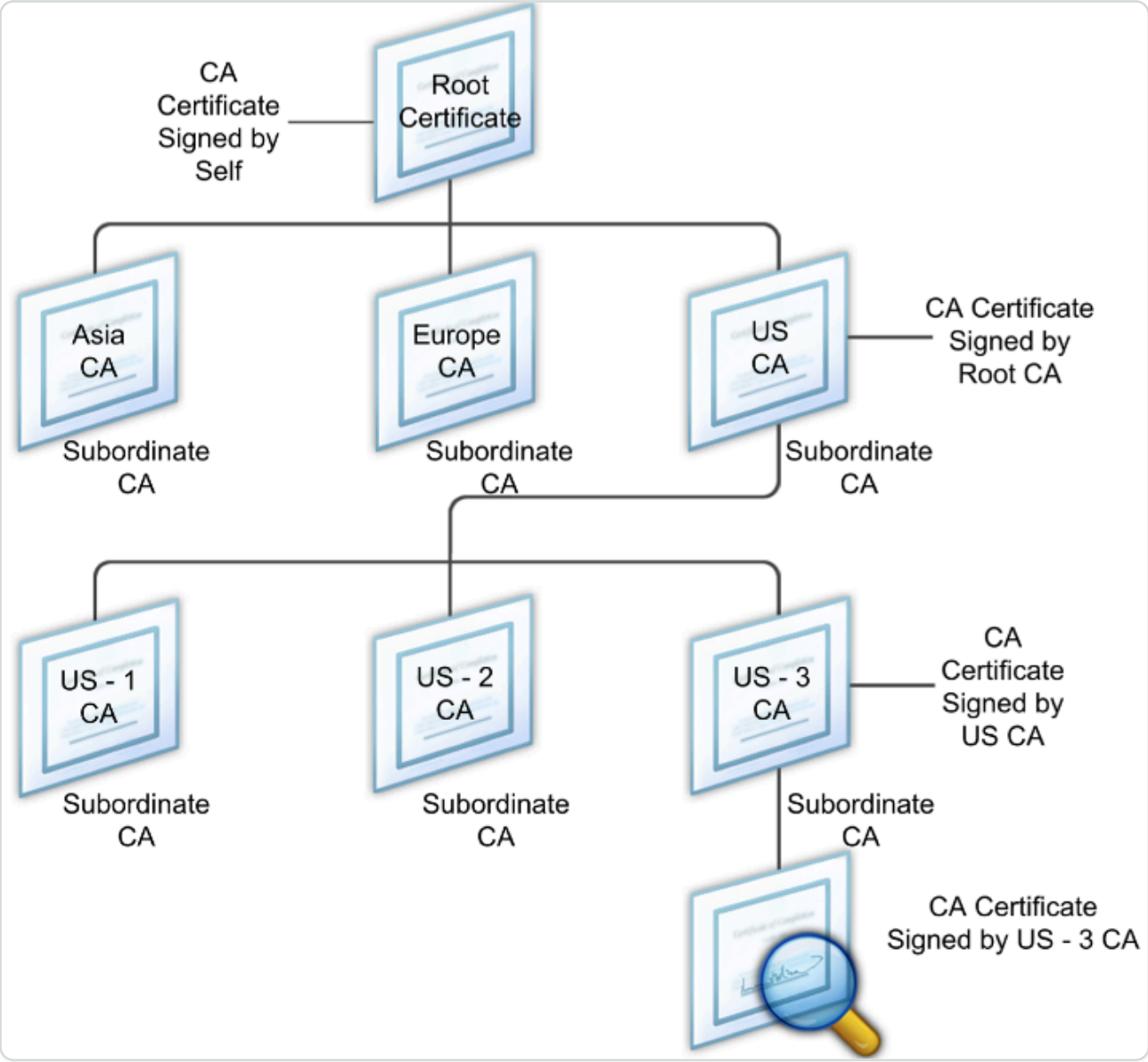
中间证书是一种介于 NetScaler Gateway（服务器证书）和根证书（安装在用户设备上）之间的证书。中间证书是证书链的一部分。

一些组织将颁发证书的职责委派出去，以解决组织单位之间的地理分离问题，或对组织的不同部门应用不同的颁发策略。

可以通过设置从属证书颁发机构 (CA) 来委派颁发证书的职责。CA 可以签署自己的证书（即它们是自签名的），也可以由另一个证书颁发机构签署。X.509 标准包含一个用于建立 CA 层次结构的模型。在此模型中，如下图所示，根 CA 位于层次结构的顶部，是由证书颁发机构自签名的证书。直接从属于根 CA 的 CA 具有由根证书颁发机构签署的 CA 证书。层次结构中从属 CA 下的 CA 具有由从属 CA 签署的 CA 证书。

图 1. 显示典型数字证书链层次结构的 X.509 模型

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



如果服务器证书由具有自签名证书的 CA 签署，则证书链由两个证书组成：最终实体证书和根证书颁发机构。如果用户或服务器证书由中间证书颁发机构签署，则证书链会更长。

下图显示，前两个元素是最终实体证书（在本例中为 gwy01.company.com）和中间证书颁发机构的证书，按此顺序排列。中间证书颁发机构的证书之后是其证书颁发机构的证书。此列表持续到列表中的最后一个证书是根证书颁发机构的证书。链中的每个证书都证明了前一个证书的身份。

图 2. 典型的数字证书链

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

安装中间证书

1. 在配置实用程序中，在“配置”选项卡上的导航窗格中，展开“SSL”，然后单击“证书”。
2. 在详细信息窗格中，单击“安装”。
3. 在“证书-密钥对名称”中，键入证书的名称。
4. 在“详细信息”下的“证书文件名”中，单击“浏览 (设备)”，然后在列表中选择“本地”或“设备”。
5. 导航到计算机（本地）或 NetScaler Gateway（设备）上的证书。
6. 在“证书格式”中，选择 PEM。
7. 单击“安装”，然后单击“关闭”。

在 NetScaler Gateway 上安装中间证书时，无需指定私钥或密码。

证书安装到设备上后，需要将其链接到服务器证书。

将中间证书链接到服务器证书

1. 在配置实用程序中，在“配置”选项卡上的导航窗格中，展开“SSL”，然后单击“证书”。
2. 在详细信息窗格中，选择服务器证书，然后在“操作”中单击“链接”。
3. 在“CA 证书名称”旁边，从列表中选择中间证书，然后单击“确定”。

使用设备证书进行身份验证

NetScaler Gateway 支持设备证书检查，使您能够将设备身份绑定到证书的私钥。设备证书检查可以配置为经典或高级端点分析 (EPA) 策略的一部分。在经典 EPA 策略中，设备证书只能为预身份验证 EPA 配置。

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

NetScaler Gateway 在运行端点分析扫描或显示登录页面之前验证设备证书。如果配置了端点分析，则会运行端点扫描以验证用户设备。当设备通过扫描并且 NetScaler Gateway 验证设备证书后，用户即可登录 NetScaler Gateway。

重要提示：

- 默认情况下，Windows 要求管理员权限才能访问设备证书。
- 要为非管理员用户添加设备证书检查，您必须安装 VPN 插件。VPN 插件版本必须与设备上的 EPA 插件版本相同。
- 您可以向网关添加多个 CA 证书并验证设备证书。
- 如果您在 NetScaler Gateway 上安装了两个或更多设备证书，用户在开始登录 NetScaler Gateway 或运行端点分析扫描之前必须选择正确的证书。
- 创建设备证书时，它必须是 X.509 证书。
- 如果您有由中间 CA 颁发的设备证书，则必须绑定中间 CA 证书和根 CA 证书。
- EPA 客户端需要用户具有本地管理员权限才能访问计算机证书存储。这种情况很少见，因此一种解决方法是安装完整的 NetScaler® Gateway 插件，该插件可以访问本地存储。

有关创建设备证书的更多信息，请参阅以下内容：

- Microsoft Learn Challenge 页面中的“什么是 Active Directory 证书服务的网络设备注册服务？”.
- Apple 支持网站上的“如何使用 DCE/RPC 和 Active Directory 证书配置文件负载从 Microsoft 证书颁发机构请求证书”。
- Ask the Directory Services Team Microsoft 支持博客上的“iPad / iPhone 证书颁发”。
- 在 Windows IT Pro 网站上，设置网络设备注册服务。
- 在 Microsoft System Center 网站上，Configuration Manager 的 PKI 证书分步示例部署：Windows Server 2008 证书颁发机构。

配置设备证书的步骤

要配置设备证书，您必须完成以下步骤：

- 在 NetScaler Gateway 上安装设备证书颁发者的证书颁发机构证书。有关详细信息，请参阅在 NetScaler Gateway 上安装已签名证书。
- 将设备证书颁发者的证书颁发机构证书绑定到 NetScaler Gateway 虚拟服务器并启用 OCSP 检查。有关详细信息，请参阅在 NetScaler Gateway 上安装已签名证书。

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

- 在设备证书颁发者的证书颁发机构证书上创建并绑定 OCSP（响应程序）。有关详细信息，请参阅使用 OCSP 监控证书状态。

在虚拟服务器上启用设备证书检查，并将设备证书颁发者的证书颁发机构证书添加到设备证书清单。有关详细信息，请参阅为经典 EPA 策略在虚拟服务器上启用设备证书检查。

在 Windows 计算机上完成设备证书的客户端配置和验证。有关详细信息，请参阅在 Windows 计算机上验证设备证书。

注意：

所有旨在利用设备证书 EPA 检查的客户端都必须在计算机的系统证书存储中安装设备证书。

为经典 EPA 策略在虚拟服务器上启用设备证书检查

创建设备证书后，您可以使用将现有证书导入并安装到 NetScaler Gateway 的过程在 NetScaler Gateway 上安装该证书。

1. 在“配置”选项卡上，导航到 **NetScaler Gateway > 虚拟服务器**。
2. 在“**NetScaler Gateway 虚拟服务器**”页面上，选择一个现有虚拟服务器，然后单击“**编辑**”。
3. 在 **VPN 虚拟服务器** 页面上，在 **基本设置** 部分下，单击 **编辑**。
4. 清除 **启用身份验证** 框以禁用身份验证。
5. 选中 **启用设备证书** 框以启用设备证书
6. 单击 **添加** 将可用设备证书颁发者的 CA 证书名称添加到列表中。
7. 要将 CA 证书绑定到虚拟服务器，请在 **设备证书的 CA** 部分下单击 **CA 证书**，然后单击 **添加**，选择证书，再单击 **+**。

注意：

有关在虚拟服务器上启用和绑定设备证书以实现高级 EPA 策略的信息，请参阅 nFactor 中作为 EPA 组件的设备证书。

在 Windows 计算机上验证设备证书

1. 打开浏览器并访问 NetScaler Gateway FQDN。
2. 允许 Citrix® 端点分析 (EPA) 客户端运行。如果尚未安装，请安装 EPA。

   Citrix EPA 运行并验证设备证书，如果设备证书 EPA 检查通过，则重定向到身份验证页面，否则重定向到 EPA 错误页面。如果您有其他 EPA 检查，则 EPA 扫描结果取决于配置的 EPA 检查。

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

要在客户端上进行进一步调试，请检查客户端上的以下 EPA 日志： C:\Users\<User name>\AppData\Local\Citrix\AGEE\nsepa.txt

注意：

不支持使用 CRL 进行设备证书验证。

导入并安装现有证书

您可以从运行 Internet Information Services (IIS) 的 Windows 计算机或运行 Secure Gateway 的计算机导入现有证书。

导出证书时，请确保也导出私钥。有时，您无法导出私钥，这意味着您无法在 NetScaler Gateway 上安装证书。如果发生这种情况，请使用证书签名请求 (CSR) 创建证书。有关详细信息，请参阅创建证书签名请求。

从 Windows 导出证书和私钥时，计算机将创建一个个人信息交换 (.pfx) 文件。然后，此文件将作为 PKCS#12 证书安装在 NetScaler Gateway 上。

如果您要用 NetScaler Gateway 替换 Secure Gateway，则可以从 Secure Gateway 导出证书和私钥。如果您正在从 Secure Gateway 到 NetScaler Gateway 进行就地迁移，则应用程序和设备上的完全限定域名 (FQDN) 必须相同。从 Secure Gateway 导出证书时，您会立即停用 Secure Gateway，在 NetScaler Gateway 上安装证书，然后测试配置。如果 Secure Gateway 和 NetScaler Gateway 具有相同的 FQDN，则它们不能同时在您的网络上运行。

如果您使用的是 Windows Server 2003 或 Windows Server 2008，则可以使用 Microsoft 管理控制台导出证书。有关详细信息，请参阅 Windows 联机帮助。

保留所有其他选项的默认值，定义密码，然后将 .pfx 文件保存到您的计算机。导出证书后，将其安装在 NetScaler Gateway 上。

在 NetScaler Gateway 上安装证书和私钥

1. 在配置实用程序中，单击“Configuration”选项卡，然后在导航窗格中单击 **NetScaler Gateway**。
2. 在详细信息窗格的“Getting Started”下，单击 **NetScaler Gateway wizard**。
3. 单击 **Next**，选择现有虚拟服务器，然后单击 **Next**。
4. 在 **证书选项** 中，选择 **安装 PKCS#12 (.pfx) 文件**。
5. 在 **PKCS#12 File Name** 中，单击 **Browse**，导航到证书，然后单击 **Select**。
6. 在 ((Password)) 中，键入私钥的密码。

   这是您将证书转换为 PEM 格式时使用的密码。

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

7. 单击“**下一步**”完成 NetScaler Gateway 向导，而不更改任何其他设置。

在 NetScaler Gateway 上安装证书后，证书将显示在配置实用程序中，位于“**SSL \ > 证书**”节点中。

创建私钥

1. 在配置实用程序中，在“配置”选项卡上的导航窗格中，单击“**SSL**”。
2. 在详细信息窗格中，在“**SSL 密钥**”下，单击“**创建 RSA 密钥**”。
3. 在“**密钥文件名**”中，键入私钥的名称，或单击“浏览”导航到现有文件。
4. 在“**密钥大小(位)**”中，键入私钥的大小。
5. 在“**公用指数值**”中，选择 F4 或 3。

   RSA 密钥的公用指数值。这是密码算法的一部分，是创建 RSA 密钥所必需的。值为 F4 (十六进制: 0x10001) 或 3 (十六进制: 0x3)。默认值为 F4。
6. 在“**密钥格式**”中，选择 PEM 或 DER。Citrix® 建议证书使用 PEM 格式。
7. 在“**PEM 编码算法**”中，选择 DES 或 DES3。
8. 在“**PEM 密码短语**”和“**验证密码短语**”中，键入密码，单击“**创建**”，然后单击“**关闭**”。

   注意：要分配密码短语，密钥格式必须为 PEM，并且必须选择编码算法。

要在配置实用程序中创建 DSA 私钥，请单击“**创建 DSA 密钥**”并按照创建 RSA 私钥的步骤操作。

将证书从 PFX 格式转换为 PEM 格式

SSL 证书用于 SSL 负载平衡虚拟服务器和 NetScaler Gateway 虚拟服务器。PEM 证书是 Base64 编码的 ASCII 文件。PEM 证书可以在文本编辑器/记事本中打开，你会发现它们包含“-----BEGIN CERTIFICATE-----”和“-----END CERTIFICATE-----”语句。

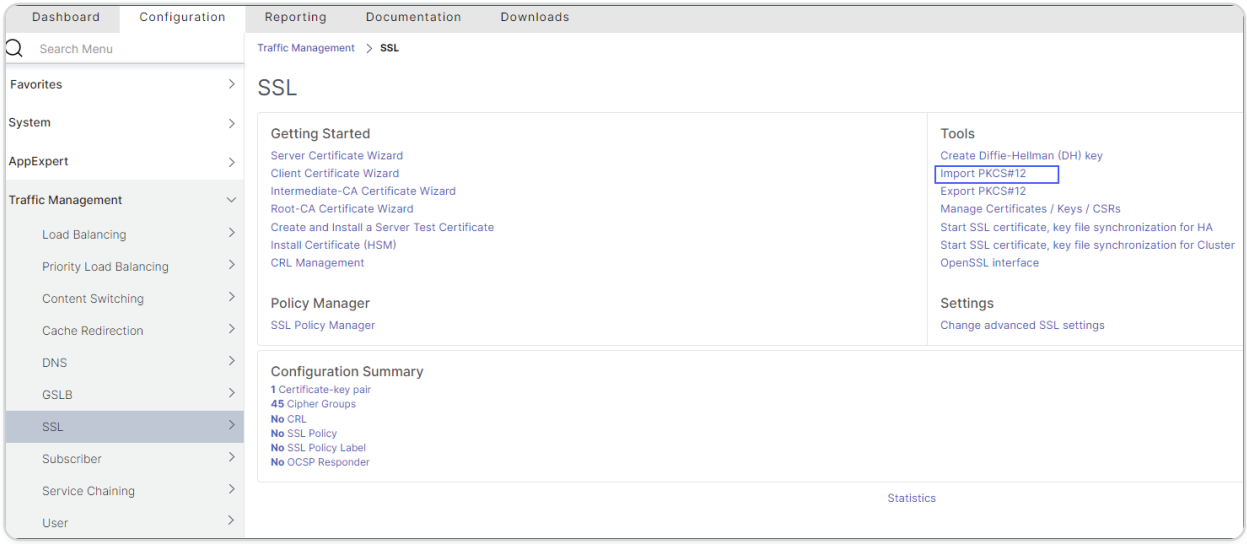
为了安全、受信任的访问，您必须在 NetScaler Gateway 服务器上安装 SSL 服务器证书。上传的证书文件必须具有以下特征：

- 最终用户信任的证书颁发机构 (CA) 必须颁发服务器证书。为获得最佳结果，请使用 Verisign、Thawte 或 GeoTrust 等商业 CA。
- 证书必须采用隐私增强邮件 (PEM) 格式，这是一种基于文本的格式，是二进制可分辨编码规则 (DER) 格式的 Base64 编码。
- 证书文件必须包含私钥，并且私钥不得加密。使用 PEM 文件时不得需要密码。
- 任何必要的中间证书都必须附加到 PEM 文件的末尾。

使用 NetScaler Gateway 向导将 PFX 证书转换为 PEM 格式，请完成以下步骤：

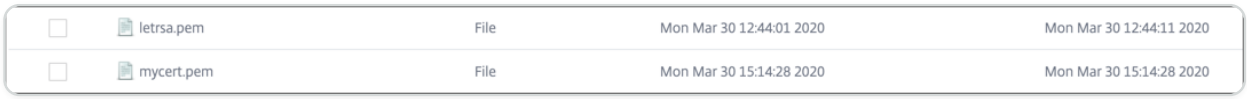
© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. 导航到 **流量管理**，选择 **SSL** 节点。
2. 单击 **导入 PKCS#12** 链接。



3. 在 **输出文件名** 字段中指定您希望用于 PEM 证书的文件名。
4. 单击 **浏览** 并选择要转换为 PEM 格式的 PFX 证书。有些用户更喜欢将证书上传到 /ncsonfig/SSL 目录并从那里使用。如果 PFX 证书存储在 NetScaler Gateway 上，则选择 **设备** 选项；如果存储在您的工作站上，则使用本地。

   ](/en-us/netscaler-gateway/media/2-convert-pfx-certificate-to-pem-format.png)
5. 指定导入密码。
6. 如果文件已编码，则选择 DES 或 3DES 作为编码格式：
7. 单击 **确定**。
8. 指定 PEM 密码和验证 PEM 密码。
9. 单击 **管理证书/密钥/CSR 链接** 以查看转换后的 PEM 证书文件。
10. 您可以查看已上传的 PFX 文件以及转换后的 PEM 文件。



11. 展开 **SSL** 节点。
12. 选择“证书”节点。
13. 单击 **安装**。
14. 在 **安装证书** 向导中指定证书-密钥对名称。
15. 浏览到 PEM 文件，用于证书文件名和私钥文件名。
16. 指定密码。

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

17. 单击 **安装**。

`OpenSSL utility`

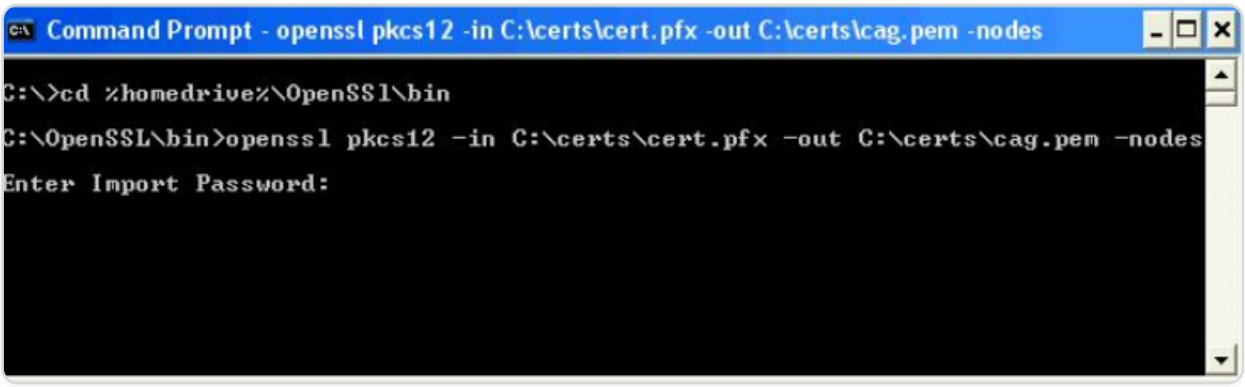
如果您已使用 Internet Information Service (IIS) 证书向导请求并将证书安装到 Windows 服务器上，则可以将该证书及其私钥导出到个人信息交换 (PFX) 文件。要将此证书导入到 NetScaler Gateway，您必须将 PFX 文件转换为未加密的 PEM 格式。

您可以使用开源实用程序 `OpenSSL` 将 PFX 转换为 PEM。从 Win32 `OpenSSL` 下载 `OpenSSL` 的 Win32 分发版。

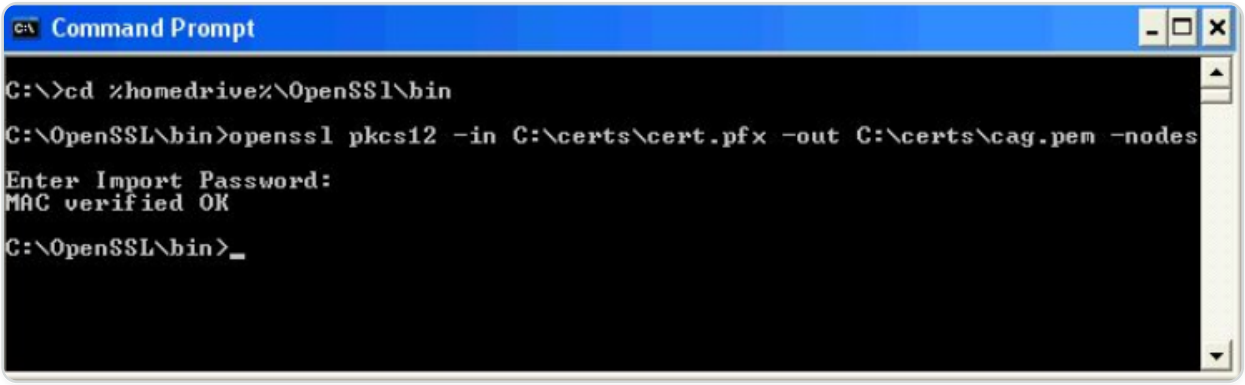
如果您想使用 `OpenSSL`，可能还需要 C++ 可再发行文件。请从 Microsoft Visual C++ 2008 Redistributable Package (x86) 下载此文件。

要在 Windows 计算机上将 PFX 文件转换为 PEM 文件，请完成以下步骤：

1. 从 Win32 `OpenSSL` 下载并安装 Win32 `OpenSSL` 软件包。
2. 创建文件夹 c:\certs 并将文件 yourcert.pfx 复制到 c:\certs 文件夹中。
3. 打开命令提示符并进入 `OpenSSL`\bin 目录：`cd %homedrive%\OpenSSL\bin`
4. 运行以下命令将 PFX 文件转换为未加密的 PEM 文件（全部在一行中）：`OpenSSL` pkcs12 -in c:\certs\yourcert.pfx -out c:\certs\cag.pem –nodes



5. 当系统提示输入导入密码时，请输入您在将证书导出到 PFX 文件时使用的密码。您必须收到一条消息，显示“MAC verified OK”。



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

6. 将浏览器指向 NetScaler Gateway 管理门户或 HTTPS 端口 9001：`https://netscaler-gateway-server:9001`。
7. 以 root 身份登录。默认密码是 `rootadmin`。
8. 单击页面顶部的“**维护**”链接。
9. 单击“**上传私钥+证书 (.pem)**”字段旁边的“**浏览**”按钮。浏览到 c:\certs\cag.pem 文件，然后单击“**上传**”。
10. 重新启动 NetScaler Gateway 以应用新的 SSL 证书。

证书吊销列表

证书颁发机构 (CA) 会不时颁发证书吊销列表 (CRL)。CRL 包含有关不再受信任的证书的信息。例如，假设 Ann 离开了 XYZ 公司。公司可以将 Ann 的证书放在 CRL 上，以防止她使用该密钥签署消息。

同样，如果私钥泄露或证书已过期并正在使用新证书，您可以吊销该证书。在信任公钥之前，请确保该证书未出现在 CRL 上。

NetScaler Gateway 支持以下两种 CRL 类型：

- 列出已吊销或不再有效的证书的 CRL
- 在线证书状态协议 (OSCP)，一种用于获取 X.509 证书吊销状态的互联网协议

添加 CRL：

在 NetScaler Gateway 设备上配置 CRL 之前，请确保 CRL 文件已本地存储在设备上。在高可用性设置中，CRL 文件必须同时存在于两台 NetScaler Gateway 设备上，并且文件的目录路径在两台设备上必须相同。

如果需要刷新 CRL，可以使用以下参数：

- CRL 名称：在 NetScaler 上添加的 CRL 的名称。最多 31 个字符。
- CRL 文件：在 NetScaler 上添加的 CRL 文件的名称。NetScaler 默认在 /var/netscaler/ssl 目录中查找 CRL 文件。最多 63 个字符。
- URL：最多 127 个字符
- 基本 DN：最多 127 个字符
- 绑定 DN：最多 127 个字符
- 密码：最多 31 个字符
- 天数：最大 31

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

1. 在配置实用程序中，在“配置”选项卡上，展开“SSL”，然后单击“CRL”。
2. 在详细信息窗格中，单击“添加”。
3. 在“添加 CRL”对话框中，指定以下值：
   - CRL 名称
   - CRL 文件
   - 格式 (可选)
   - CA 证书 (可选)
4. 单击“**创建**”，然后单击“**关闭**”。在 CRL 详细信息窗格中，选择您配置的 CRL 并验证屏幕底部显示的设置是否正确。

要在 GUI 中使用 LDAP 或 HTTP 配置 CRL 自动刷新：

CRL 由 CA 定期生成和发布，有时在特定证书被吊销后立即发布。Citrix 建议您定期更新 NetScaler Gateway 设备上的 CRL，以防止客户端尝试使用无效证书进行连接。

NetScaler Gateway 设备可以从 Web 位置或 LDAP 目录刷新 CRL。当您指定刷新参数以及 Web 位置或 LDAP 服务器时，在运行命令时，CRL 不必存在于本地硬盘驱动器上。首次刷新会将副本存储在本地硬盘驱动器上，路径由 CRL 文件参数指定。存储 CRL 的默认路径是 /var/netscaler/ssl。

CRL 刷新参数

CRL 名称

> 在 NetScaler Gateway 上刷新的 CRL 的名称。

启用 CRL 自动刷新

> 启用或禁用 CRL 自动刷新。

CA 证书

> 颁发 CRL 的 CA 证书。此 CA 证书必须安装在设备上。NetScaler 只能从已安装其证书的 CA 更新 CRL。

方法

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

> 用于从 Web 服务器 (HTTP) 或 LDAP 服务器获取 CRL 刷新的协议。可能的值：HTTP、LDAP。默认值：HTTP。

范围

> LDAP 服务器上搜索操作的范围。如果指定的范围是
>
> Base，则搜索与基本 DN 处于同一级别。如果指定的范围是
>
> One，则搜索扩展到基本 DN 下一级。

服务器 IP

> 从中检索 CRL 的 LDAP 服务器的 IP 地址。选择 IPv6 以使用 IPv6 IP 地址。

端口

> LDAP 或 HTTP 服务器进行通信的端口号。

URL

> 从中检索 CRL 的 Web 位置的 URL。

基本 DN

> LDAP 服务器用于搜索 CRL 属性的基本 DN。
>
> 注意：Citrix® 建议使用基本 DN 属性而不是 CA 证书中的颁发者名称 (Issuer-Name) 来搜索 LDAP 服务器中的 CRL。Issuer-Name 字段可能与 LDAP 目录结构的 DN 不完全匹配。

绑定 DN

> 绑定 DN 属性用于访问 LDAP 存储库中的 CRL 对象。绑定 DN 属性是 LDAP 服务器的管理员凭据。配置此参数以限制对 LDAP 服务器的未经授权的访问。

密码

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

> 用于访问 LDAP 存储库中 CRL 对象的管理员密码。如果对 LDAP 存储库的访问受限（即不允许匿名访问），则需要密码。

间隔

> 必须执行 CRL 刷新的间隔。对于即时 CRL 刷新，请将间隔指定为 NOW。可能的值：MONTHLY、DAILY、WEEKLY、NOW、NONE。

天数

> 必须执行 CRL 刷新的日期。如果间隔设置为 DAILY，则此选项不可用。

时间

> 必须执行 CRL 刷新的 24 小时制的确切时间。

二进制

> 将基于 LDAP 的 CRL 检索模式设置为二进制。可能的值：YES、NO。默认值：NO。

1. 在导航窗格中，展开 SSL，然后单击 CRL。
2. 选择要更新其刷新参数的已配置 CRL，然后单击“打开”。
3. 选择“启用 CRL 自动刷新”选项。
4. 在“CRL 自动刷新参数”组中，指定以下参数的值： 注意：星号 (*) 表示必填参数。
   - 方法
   - 二进制
   - 范围
   - 服务器 IP
   - 端口*
   - URL
   - 基本 DN*
   - 绑定 DN
   - 密码

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

- 间隔
- 天数
- 时间

5. 单击“创建”。在“CRL”窗格中，选择您配置的 CRL，并验证屏幕底部显示的设置是否正确。

使用 OCSP 监控证书状态

在线证书状态协议 (OCSP) 是一种互联网协议，用于确定客户端 SSL 证书的状态。NetScaler Gateway 支持 RFC 2560 中定义的 OCSP。在及时性方面，OCSP 比证书吊销列表 (CRL) 具有显著优势。客户端证书的最新吊销状态在涉及大笔资金和高价值股票交易的事务中特别有用。它还使用更少的系统和网络资源。NetScaler Gateway 的 OCSP 实现包括请求批处理和响应缓存。

NetScaler Gateway 的 OCSP 实现

NetScaler Gateway 设备上的 OCSP 验证在 NetScaler Gateway 在 SSL 握手期间收到客户端证书时开始。为了验证证书，NetScaler Gateway 会创建一个 OCSP 请求并将其转发给 OCSP 响应程序。为此，NetScaler Gateway 会从客户端证书中提取 OCSP 响应程序的 URL，或者使用本地配置的 URL。事务处于挂起状态，直到 NetScaler Gateway 评估来自服务器的响应并确定是允许还是拒绝该事务。如果服务器的响应延迟超过配置时间且未配置其他响应程序，NetScaler Gateway 将允许该事务或显示错误，具体取决于您将 OCSP 检查设置为可选还是强制。NetScaler Gateway 支持 OCSP 请求批处理和 OCSP 响应缓存，以减少 OCSP 响应程序的负载并提供更快的响应。

OCSP 请求批处理

每当 NetScaler Gateway 收到客户端证书时，它都会向 OCSP 响应程序发送请求。为避免 OCSP 响应程序过载，NetScaler Gateway 可以在同一请求中查询多个客户端证书的状态。为了使请求批处理高效工作，您需要定义一个超时时间，以便在等待形成批处理时不会延迟单个证书的处理。

OCSP 响应缓存

缓存从 OCSP 响应程序收到的响应可以加快对用户的响应速度，并减少 OCSP 响应程序的负载。从 OCSP 响应程序收到客户端证书的吊销状态后，NetScaler Gateway 会在本地缓存该响应一段预定义的时间。当在 SSL 握手期间收到客户端证书时，NetScaler Gateway 首先检查其本地缓存中是否存在此证书的条目。如果找到仍然有效（在缓存超时限制内）的条目，则评估该条目并接受或拒绝客户端证书。如果未找到证书，NetScaler Gateway 会向 OCSP 响应程序发送请求，并将响应存储在其本地缓存中一段配置的时间。

配置 OCSP 证书状态

配置在线证书状态协议 (OCSP) 涉及添加 OCSP 响应程序、将 OCSP 响应程序绑定到证书颁发机构 (CA) 颁发的签名证书，以及将证书和私钥绑定到安全套接字层 (SSL) 虚拟服务器。如果您需要将不

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

同的证书和私钥绑定到已配置的 OCSP 响应程序，则需要先解除绑定该响应程序，然后将其绑定到不同的证书。

配置 OCSP

1. 在“配置”选项卡上，在导航窗格中，展开“SSL”，然后单击“OCSP 响应程序”。
2. 在详细信息窗格中，单击“添加”。
3. 在“名称”中，键入配置文件的名称。
4. 在“URL”中，键入 OCSP 响应程序的 Web 地址。

   此字段为必填项。Web 地址不能超过 32 个字符。
5. 要缓存 OCSP 响应，请单击“缓存”，然后在“超时”中键入 NetScaler Gateway 保留响应的分钟数。
6. 在“请求批处理”下，单击“启用”。
7. 在“批处理延迟”中，指定允许批处理一组 OCSP 请求的时间（以毫秒为单位）。

   值范围为 0 到 10000。默认值为 1。
8. 在“生成时间偏差”中，键入设备必须检查或接受响应时 NetScaler Gateway 可以使用的时间量。
9. 在“响应验证”下，如果要禁用 OCSP 响应程序进行的签名检查，请选择“信任响应”。

   如果启用“信任响应”，请跳过步骤 8 和步骤 9。
10. 在“证书”中，选择用于签署 OCSP 响应的证书。

    如果未选择证书，则使用 OCSP 响应程序绑定的 CA 来验证响应。
11. 在“请求超时”中，键入等待 OCSP 响应的毫秒数。

    此时间包括“批处理延迟”时间。值范围为 0 到 120000。默认值为 2000。
12. 在“签名证书”中，选择用于签署 OCSP 请求的证书和私钥。如果未指定证书和私钥，则请求将不会签名。
13. 要启用一次性使用的数字 `(nonce) extension`，请选择“随机数”。
14. 要使用客户端证书，请单击“客户端证书插入”。
15. 点击“创建”，然后点击“关闭”。

NetScaler Gateway 上的证书管理

在 NetScaler Gateway 上，您可以使用证书创建安全连接并对用户进行身份验证。

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

为了建立安全连接，连接的一端需要服务器证书。连接的另一端需要颁发服务器证书的证书颁发机构 (CA) 的根证书。

- 服务器证书。服务器证书用于证明服务器的身份。NetScaler Gateway 需要这种类型的数字证书。
- 根证书。根证书用于标识签署服务器证书的 CA。根证书属于证书颁发机构。用户设备需要这种类型的数字证书来验证服务器证书。

当用户设备上的 Web 浏览器建立安全连接时，服务器会将其证书发送到设备。

当用户设备收到服务器证书时，Web 浏览器（例如 Internet Explorer）会检查是哪个 CA 颁发了该证书，以及该 CA 是否受用户设备信任。如果 CA 不受信任，或者它是一个测试证书，Web 浏览器会提示用户接受或拒绝该证书（实际上是接受或拒绝访问该站点的能力）。

NetScaler Gateway 支持以下三种类型的证书：

- 绑定到虚拟服务器的测试证书，也可用于连接到服务器场。NetScaler Gateway 附带预安装的测试证书。
- PEM 或 DER 格式的证书，由 CA 签名并与私钥配对。
- PKCS#12 格式的证书，用于存储或传输证书和私钥。PKCS#12 证书通常从现有 Windows 证书导出为 PFX 文件，然后安装在 NetScaler Gateway 上。

Citrix® 建议使用由受信任的 CA（例如 Thawte 或 Verisign）签名的证书。

创建证书签名请求

为了通过 SSL 或 TLS 提供安全通信，NetScaler Gateway 上需要服务器证书。在将证书上传到 NetScaler Gateway 之前，您需要生成证书签名请求 (CSR) 和私钥。您可以使用 NetScaler Gateway 向导或配置实用程序中包含的“创建证书请求”来创建 CSR。“创建证书请求”会创建一个 .csr 文件，该文件会通过电子邮件发送给证书颁发机构 (CA) 进行签名，并生成一个保留在设备上的私钥。CA 会对证书进行签名，并将其返回到您提供的电子邮件地址。收到签名证书后，您可以将其安装在 NetScaler Gateway 上。当您从 CA 收到证书后，您将证书与私钥配对。

重要提示：

当您使用 NetScaler Gateway 向导创建 CSR 时，您必须退出向导并等待 CA 向您发送签名证书。收到证书后，您可以再次运行 NetScaler Gateway 向导以创建设置并安装证书。有关 NetScaler Gateway 向导的更多信息，请参阅 使用 NetScaler Gateway 向导配置设置。

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

使用 NetScaler Gateway 向导创建 CSR

1. 在配置实用程序中，单击“配置”选项卡，然后在导航窗格中单击 **NetScaler Gateway**。
2. 在详细信息窗格的“入门”下，单击 **NetScaler Gateway** 向导。
3. 按照向导中的说明操作，直到出现“指定服务器证书”页面。
4. 单击“**创建证书签名请求**”并填写字段。 注意：完全限定域名 (FQDN) 不需要与 NetScaler Gateway 主机名相同。FQDN 用于用户登录。
5. 单击“**创建**”将证书保存到您的计算机，然后单击“**关闭**”。
6. 退出 NetScaler Gateway 向导，不保存您的设置。

使用 NetScaler GUI 创建 CSR

您也可以使用 NetScaler GUI 创建 CSR，而无需运行 NetScaler Gateway 向导。

1. 导航到“**流量管理**”>“**SSL**”>“**SSL 文件**”，然后选择“**创建证书签名请求 (CSR)**”。
2. 完成证书设置，然后单击“**创建**”。

创建证书和私钥后，将证书通过电子邮件发送给 CA，例如 Thawte 或 Verisign。

有关详细步骤，请参阅 创建证书签名请求。

在 NetScaler Gateway 上安装签名证书

从证书颁发机构 (CA) 收到签名证书后，将其与设备上的私钥配对，然后在 NetScaler Gateway 上安装证书。

使用 GUI 将签名证书与私钥配对

1. 使用 Secure Shell (SSH) 程序（例如 WinSCP）将证书复制到 NetScaler Gateway 的 nsconfig/ssl 文件夹。
2. 在配置实用程序中，在“配置”选项卡上的导航窗格中，展开 **SSL > 证书**。
3. 在 **SSL 证书** 页面中，单击 **开始**。
4. 在详细信息窗格中，单击 **安装**。
5. 在 **证书-密钥对名称** 中，键入证书的名称。
6. 在 **证书文件名** 中，单击 **设备**。
7. 导航到证书，单击 **选择**，然后单击 **打开**。
8. 在 **密钥文件名** 中，单击 **设备**。私钥的名称与证书签名请求 (CSR) 的名称相同。私钥位于 NetScaler Gateway 的 \\nsconfig\\ssl 目录中。
9. 选择私钥，然后单击 **打开**。

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

10. 如果证书是 PEM 格式，请在 **密码** 中键入私钥的密码。
11. 如果您想配置证书过期通知，请选择 **Notify When Expires**。
12. 在 **Notification Period** 中，键入天数，单击 **Create**，然后单击 **Close**。

使用 GUI 将证书和私钥绑定到虚拟服务器

创建并链接证书和私钥对后，将其绑定到虚拟服务器。

1. 在配置实用程序中，在“配置”选项卡上的导航窗格中，展开 **NetScaler Gateway > Virtual Servers**。
2. 在详细信息窗格中，单击一个虚拟服务器，然后单击 **Open**。
3. 在“证书”选项卡上，在 **Available** 下，选择一个证书，单击 **Add**，然后单击 **OK**。

使用 CLI 将证书和私钥绑定到虚拟服务器

在命令提示符下，键入：

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

示例：

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

注意： 如果设备证书不需要 OCSP 检查，则 oscpCheck 是可选的。

使用 GUI 从虚拟服务器解除绑定测试证书

安装签名证书后，解除绑定到虚拟服务器的任何测试证书。您可以使用配置实用程序解除绑定测试证书。

1. 在配置实用程序中，在“配置”选项卡上的导航窗格中，展开 **NetScaler Gateway > Virtual Servers**。
2. 在详细信息窗格中，单击一个虚拟服务器，然后单击 **Open**。
3. 在“证书”选项卡上，在“**已配置**”下，选择测试证书，然后单击“**删除**”。

配置中间证书

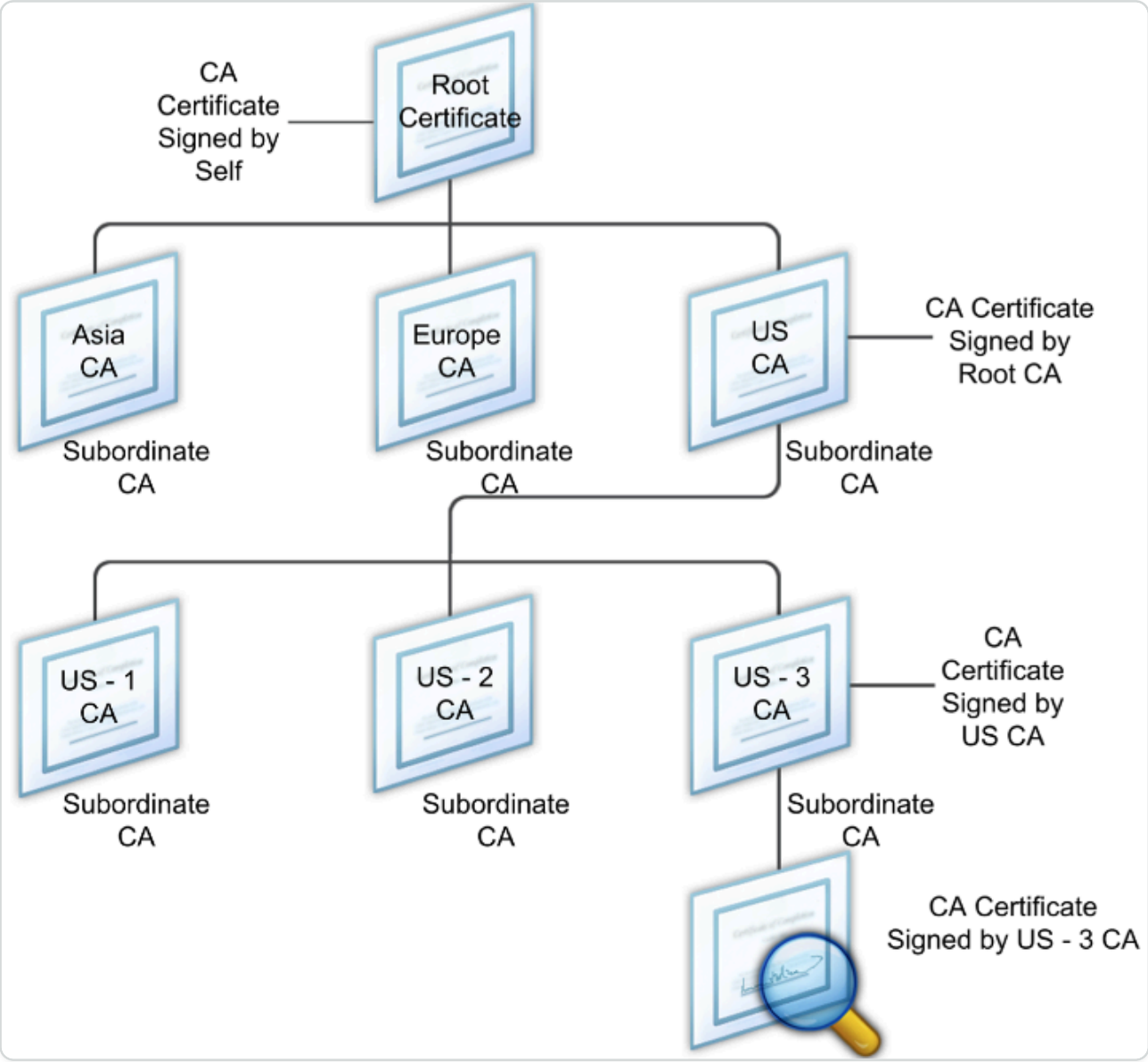
中间证书是一种介于 NetScaler Gateway（服务器证书）和根证书（安装在用户设备上）之间的证书。中间证书是证书链的一部分。

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

一些组织将颁发证书的职责委派出去，以解决组织单位之间的地理分离问题，或对组织的不同部门应用不同的颁发策略。

可以通过设置从属证书颁发机构 (CA) 来委派颁发证书的职责。CA 可以签署自己的证书（即它们是自签名的），也可以由另一个证书颁发机构签署。X.509 标准包含一个用于建立 CA 层次结构的模型。在此模型中，如下图所示，根 CA 位于层次结构的顶部，是由证书颁发机构自签名的证书。直接从属于根 CA 的 CA 具有由根证书颁发机构签署的 CA 证书。层次结构中从属 CA 下的 CA 具有由从属 CA 签署的 CA 证书。

图 1. 显示典型数字证书链层次结构的 X.509 模型



如果服务器证书由具有自签名证书的 CA 签署，则证书链由两个证书组成：最终实体证书和根证书颁发机构。如果用户或服务器证书由中间证书颁发机构签署，则证书链会更长。

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

下图显示，前两个元素是最终实体证书（在本例中为 gwy01.company.com）和中间证书颁发机构的证书，按此顺序排列。中间证书颁发机构的证书之后是其证书颁发机构的证书。此列表持续到列表中的最后一个证书是根证书颁发机构的证书。链中的每个证书都证明了前一个证书的身份。

图 2. 典型的数字证书链

安装中间证书

1. 在配置实用程序中，在“配置”选项卡上的导航窗格中，展开“SSL”，然后单击“证书”。
2. 在详细信息窗格中，单击“安装”。
3. 在“证书-密钥对名称”中，键入证书的名称。
4. 在“详细信息”下的“证书文件名”中，单击“浏览 (设备)”，然后在列表中选择“本地”或“设备”。
5. 导航到计算机（本地）或 NetScaler Gateway（设备）上的证书。
6. 在“证书格式”中，选择 PEM。
7. 单击“安装”，然后单击“关闭”。

在 NetScaler Gateway 上安装中间证书时，无需指定私钥或密码。

证书安装到设备上后，需要将其链接到服务器证书。

将中间证书链接到服务器证书

1. 在配置实用程序中，在“配置”选项卡上的导航窗格中，展开“SSL”，然后单击“证书”。
2. 在详细信息窗格中，选择服务器证书，然后在“操作”中单击“链接”。
3. 在“CA 证书名称”旁边，从列表中选择中间证书，然后单击“确定”。

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

使用设备证书进行身份验证

NetScaler Gateway 支持设备证书检查，使您能够将设备身份绑定到证书的私钥。设备证书检查可以配置为经典或高级端点分析 (EPA) 策略的一部分。在经典 EPA 策略中，设备证书只能为预身份验证 EPA 配置。

NetScaler Gateway 在运行端点分析扫描或显示登录页面之前验证设备证书。如果配置了端点分析，则会运行端点扫描以验证用户设备。当设备通过扫描并且 NetScaler Gateway 验证设备证书后，用户即可登录 NetScaler Gateway。

重要提示：

- 默认情况下，Windows 要求管理员权限才能访问设备证书。
- 要为非管理员用户添加设备证书检查，您必须安装 VPN 插件。VPN 插件版本必须与设备上的 EPA 插件版本相同。
- 您可以向网关添加多个 CA 证书并验证设备证书。
- 如果您在 NetScaler Gateway 上安装了两个或更多设备证书，用户在开始登录 NetScaler Gateway 或运行端点分析扫描之前必须选择正确的证书。
- 创建设备证书时，它必须是 X.509 证书。
- 如果您有由中间 CA 颁发的设备证书，则必须绑定中间 CA 证书和根 CA 证书。
- EPA 客户端需要用户具有本地管理员权限才能访问计算机证书存储。这种情况很少见，因此一种解决方法是安装完整的 NetScaler® Gateway 插件，该插件可以访问本地存储。

有关创建设备证书的更多信息，请参阅以下内容：

- Microsoft Learn Challenge 页面中的“什么是 Active Directory 证书服务的网络设备注册服务？”.
- Apple 支持网站上的“如何使用 DCE/RPC 和 Active Directory 证书配置文件负载从 Microsoft 证书颁发机构请求证书”。
- Ask the Directory Services Team Microsoft 支持博客上的“iPad / iPhone 证书颁发”。
- 在 Windows IT Pro 网站上，设置网络设备注册服务。
- 在 Microsoft System Center 网站上，Configuration Manager 的 PKI 证书分步示例部署：Windows Server 2008 证书颁发机构。

配置设备证书的步骤

要配置设备证书，您必须完成以下步骤：

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

- 在 NetScaler Gateway 上安装设备证书颁发者的证书颁发机构证书。有关详细信息，请参阅在 NetScaler Gateway 上安装已签名证书。
- 将设备证书颁发者的证书颁发机构证书绑定到 NetScaler Gateway 虚拟服务器并启用 OCSP 检查。有关详细信息，请参阅在 NetScaler Gateway 上安装已签名证书。
- 在设备证书颁发者的证书颁发机构证书上创建并绑定 OCSP（响应程序）。有关详细信息，请参阅使用 OCSP 监控证书状态。

在虚拟服务器上启用设备证书检查，并将设备证书颁发者的证书颁发机构证书添加到设备证书清单。有关详细信息，请参阅为经典 EPA 策略在虚拟服务器上启用设备证书检查。

在 Windows 计算机上完成设备证书的客户端配置和验证。有关详细信息，请参阅在 Windows 计算机上验证设备证书。

注意：

所有旨在利用设备证书 EPA 检查的客户端都必须在计算机的系统证书存储中安装设备证书。

为经典 EPA 策略在虚拟服务器上启用设备证书检查

创建设备证书后，您可以使用将现有证书导入并安装到 NetScaler Gateway 的过程在 NetScaler Gateway 上安装该证书。

1. 在“配置”选项卡上，导航到 **NetScaler Gateway > 虚拟服务器**。
2. 在“**NetScaler Gateway 虚拟服务器**”页面上，选择一个现有虚拟服务器，然后单击“**编辑**”。
3. 在 **VPN 虚拟服务器** 页面上，在 **基本设置** 部分下，单击 **编辑**。
4. 清除 **启用身份验证** 框以禁用身份验证。
5. 选中 **启用设备证书** 框以启用设备证书
6. 单击 **添加** 将可用设备证书颁发者的 CA 证书名称添加到列表中。
7. 要将 CA 证书绑定到虚拟服务器，请在 **设备证书的 CA** 部分下单击 **CA 证书**，然后单击 **添加**，选择证书，再单击 **+**。

注意：

有关在虚拟服务器上启用和绑定设备证书以实现高级 EPA 策略的信息，请参阅 nFactor 中作为 EPA 组件的设备证书。

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

在 Windows 计算机上验证设备证书

1. 打开浏览器并访问 NetScaler Gateway FQDN。
2. 允许 Citrix® 端点分析 (EPA) 客户端运行。如果尚未安装，请安装 EPA。

   Citrix EPA 运行并验证设备证书，如果设备证书 EPA 检查通过，则重定向到身份验证页面，否则重定向到 EPA 错误页面。如果您有其他 EPA 检查，则 EPA 扫描结果取决于配置的 EPA 检查。

要在客户端上进行进一步调试，请检查客户端上的以下 EPA 日志： C:\Users\<User name>\AppData\Local\Citrix\AGEE\nsepa.txt

注意：

不支持使用 CRL 进行设备证书验证。

导入并安装现有证书

您可以从运行 Internet Information Services (IIS) 的 Windows 计算机或运行 Secure Gateway 的计算机导入现有证书。

导出证书时，请确保也导出私钥。有时，您无法导出私钥，这意味着您无法在 NetScaler Gateway 上安装证书。如果发生这种情况，请使用证书签名请求 (CSR) 创建证书。有关详细信息，请参阅创建证书签名请求。

从 Windows 导出证书和私钥时，计算机将创建一个个人信息交换 (.pfx) 文件。然后，此文件将作为 PKCS#12 证书安装在 NetScaler Gateway 上。

如果您要用 NetScaler Gateway 替换 Secure Gateway，则可以从 Secure Gateway 导出证书和私钥。如果您正在从 Secure Gateway 到 NetScaler Gateway 进行就地迁移，则应用程序和设备上的完全限定域名 (FQDN) 必须相同。从 Secure Gateway 导出证书时，您会立即停用 Secure Gateway，在 NetScaler Gateway 上安装证书，然后测试配置。如果 Secure Gateway 和 NetScaler Gateway 具有相同的 FQDN，则它们不能同时在您的网络上运行。

如果您使用的是 Windows Server 2003 或 Windows Server 2008，则可以使用 Microsoft 管理控制台导出证书。有关详细信息，请参阅 Windows 联机帮助。

保留所有其他选项的默认值，定义密码，然后将 .pfx 文件保存到您的计算机。导出证书后，将其安装在 NetScaler Gateway 上。

在 NetScaler Gateway 上安装证书和私钥

1. 在配置实用程序中，单击“Configuration”选项卡，然后在导航窗格中单击 **NetScaler Gateway**。
2. 在详细信息窗格的“Getting Started”下，单击 **NetScaler Gateway wizard**。

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

3. 单击 **Next**，选择现有虚拟服务器，然后单击 **Next**。
4. 在 **证书选项** 中，选择 **安装 PKCS#12 (.pfx) 文件**。
5. 在 **PKCS#12 File Name** 中，单击 **Browse**，导航到证书，然后单击 **Select**。
6. 在 ((Password)) 中，键入私钥的密码。

   这是您将证书转换为 PEM 格式时使用的密码。
7. 单击“**下一步**”完成 NetScaler Gateway 向导，而不更改任何其他设置。

在 NetScaler Gateway 上安装证书后，证书将显示在配置实用程序中，位于“**SSL \ > 证书**”节点中。

创建私钥

1. 在配置实用程序中，在“配置”选项卡上的导航窗格中，单击“**SSL**”。
2. 在详细信息窗格中，在“**SSL 密钥**”下，单击“**创建 RSA 密钥**”。
3. 在“**密钥文件名**”中，键入私钥的名称，或单击“浏览”导航到现有文件。
4. 在“**密钥大小(位)**”中，键入私钥的大小。
5. 在“**公用指数值**”中，选择 F4 或 3。

   RSA 密钥的公用指数值。这是密码算法的一部分，是创建 RSA 密钥所必需的。值为 F4 (十六进制: 0x10001) 或 3 (十六进制: 0x3)。默认值为 F4。
6. 在“**密钥格式**”中，选择 PEM 或 DER。Citrix® 建议证书使用 PEM 格式。
7. 在“**PEM 编码算法**”中，选择 DES 或 DES3。
8. 在“**PEM 密码短语**”和“**验证密码短语**”中，键入密码，单击“**创建**”，然后单击“**关闭**”。

   注意：要分配密码短语，密钥格式必须为 PEM，并且必须选择编码算法。

要在配置实用程序中创建 DSA 私钥，请单击“**创建 DSA 密钥**”并按照创建 RSA 私钥的步骤操作。

证书吊销列表

证书颁发机构 (CA) 会不时颁发证书吊销列表 (CRL)。CRL 包含有关不再受信任的证书的信息。例如，假设 Ann 离开了 XYZ 公司。公司可以将 Ann 的证书放在 CRL 上，以防止她使用该密钥签署消息。

同样，如果私钥泄露或证书已过期并正在使用新证书，您可以吊销该证书。在信任公钥之前，请确保该证书未出现在 CRL 上。

NetScaler Gateway 支持以下两种 CRL 类型：

- 列出已吊销或不再有效的证书的 CRL

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

- 在线证书状态协议 (OSCP)，一种用于获取 X.509 证书吊销状态的互联网协议

添加 CRL：

在 NetScaler Gateway 设备上配置 CRL 之前，请确保 CRL 文件已本地存储在设备上。在高可用性设置中，CRL 文件必须同时存在于两台 NetScaler Gateway 设备上，并且文件的目录路径在两台设备上必须相同。

如果需要刷新 CRL，可以使用以下参数：

- CRL 名称：在 NetScaler 上添加的 CRL 的名称。最多 31 个字符。
- CRL 文件：在 NetScaler 上添加的 CRL 文件的名称。NetScaler 默认在 /var/netscaler/ssl 目录中查找 CRL 文件。最多 63 个字符。
- URL：最多 127 个字符
- 基本 DN：最多 127 个字符
- 绑定 DN：最多 127 个字符
- 密码：最多 31 个字符
- 天数：最大 31

1. 在配置实用程序中，在“配置”选项卡上，展开“SSL”，然后单击“CRL”。
2. 在详细信息窗格中，单击“添加”。
3. 在“添加 CRL”对话框中，指定以下值：
   - CRL 名称
   - CRL 文件
   - 格式 (可选)
   - CA 证书 (可选)
4. 单击“**创建**”，然后单击“**关闭**”。在 CRL 详细信息窗格中，选择您配置的 CRL 并验证屏幕底部显示的设置是否正确。

要在 GUI 中使用 LDAP 或 HTTP 配置 CRL 自动刷新：

CRL 由 CA 定期生成和发布，有时在特定证书被吊销后立即发布。Citrix 建议您定期更新 NetScaler Gateway 设备上的 CRL，以防止客户端尝试使用无效证书进行连接。

NetScaler Gateway 设备可以从 Web 位置或 LDAP 目录刷新 CRL。当您指定刷新参数以及 Web 位置或 LDAP 服务器时，在运行命令时，CRL 不必存在于本地硬盘驱动器上。首次刷新会将副本存储在本地硬盘驱动器上，路径由 CRL 文件参数指定。存储 CRL 的默认路径是 /var/netscaler/ssl。

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

CRL 刷新参数

CRL 名称

> 在 NetScaler Gateway 上刷新的 CRL 的名称。

启用 CRL 自动刷新

> 启用或禁用 CRL 自动刷新。

CA 证书

> 颁发 CRL 的 CA 证书。此 CA 证书必须安装在设备上。NetScaler 只能从已安装其证书的 CA 更新 CRL。

方法

> 用于从 Web 服务器 (HTTP) 或 LDAP 服务器获取 CRL 刷新的协议。可能的值：HTTP、LDAP。默认值：HTTP。

范围

> LDAP 服务器上搜索操作的范围。如果指定的范围是
>
> Base，则搜索与基本 DN 处于同一级别。如果指定的范围是
>
> One，则搜索扩展到基本 DN 下一级。

服务器 IP

> 从中检索 CRL 的 LDAP 服务器的 IP 地址。选择 IPv6 以使用 IPv6 IP 地址。

端口

> LDAP 或 HTTP 服务器进行通信的端口号。

URL

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

> 从中检索 CRL 的 Web 位置的 URL。

基本 DN

> LDAP 服务器用于搜索 CRL 属性的基本 DN。
>
> 注意：Citrix® 建议使用基本 DN 属性而不是 CA 证书中的颁发者名称 (Issuer-Name) 来搜索 LDAP 服务器中的 CRL。Issuer-Name 字段可能与 LDAP 目录结构的 DN 不完全匹配。

绑定 DN

> 绑定 DN 属性用于访问 LDAP 存储库中的 CRL 对象。绑定 DN 属性是 LDAP 服务器的管理员凭据。配置此参数以限制对 LDAP 服务器的未经授权的访问。

密码

> 用于访问 LDAP 存储库中 CRL 对象的管理员密码。如果对 LDAP 存储库的访问受限（即不允许匿名访问），则需要密码。

间隔

> 必须执行 CRL 刷新的间隔。对于即时 CRL 刷新，请将间隔指定为 NOW。可能的值：MONTHLY、DAILY、WEEKLY、NOW、NONE。

天数

> 必须执行 CRL 刷新的日期。如果间隔设置为 DAILY，则此选项不可用。

时间

> 必须执行 CRL 刷新的 24 小时制的确切时间。

二进制

> 将基于 LDAP 的 CRL 检索模式设置为二进制。可能的值：YES、NO。默认值：NO。

1. 在导航窗格中，展开 SSL，然后单击 CRL。

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

2. 选择要更新其刷新参数的已配置 CRL，然后单击“打开”。
3. 选择“启用 CRL 自动刷新”选项。
4. 在“CRL 自动刷新参数”组中，指定以下参数的值： 注意：星号 (*) 表示必填参数。
    - 方法
    - 二进制
    - 范围
    - 服务器 IP
    - 端口*
    - URL
    - 基本 DN*
    - 绑定 DN
    - 密码
    - 间隔
    - 天数
    - 时间
5. 单击“创建”。在“CRL”窗格中，选择您配置的 CRL，并验证屏幕底部显示的设置是否正确。

使用 OCSP 监控证书状态

在线证书状态协议 (OCSP) 是一种互联网协议，用于确定客户端 SSL 证书的状态。NetScaler Gateway 支持 RFC 2560 中定义的 OCSP。在及时性方面，OCSP 比证书吊销列表 (CRL) 具有显著优势。客户端证书的最新吊销状态在涉及大笔资金和高价值股票交易的事务中特别有用。它还使用更少的系统和网络资源。NetScaler Gateway 的 OCSP 实现包括请求批处理和响应缓存。

NetScaler Gateway 的 OCSP 实现

NetScaler Gateway 设备上的 OCSP 验证在 NetScaler Gateway 在 SSL 握手期间收到客户端证书时开始。为了验证证书，NetScaler Gateway 会创建一个 OCSP 请求并将其转发给 OCSP 响应程序。为此，NetScaler Gateway 会从客户端证书中提取 OCSP 响应程序的 URL，或者使用本地配置的 URL。事务处于挂起状态，直到 NetScaler Gateway 评估来自服务器的响应并确定是允许还是拒绝该事务。如果服务器的响应延迟超过配置时间且未配置其他响应程序，NetScaler Gateway 将允许该事务或显示错误，具体取决于您将 OCSP 检查设置为可选还是强制。NetScaler Gateway 支持 OCSP 请求批处理和 OCSP 响应缓存，以减少 OCSP 响应程序的负载并提供更快的响应。

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

OCSP 请求批处理

每当 NetScaler Gateway 收到客户端证书时，它都会向 OCSP 响应程序发送请求。为避免 OCSP 响应程序过载，NetScaler Gateway 可以在同一请求中查询多个客户端证书的状态。为了使请求批处理高效工作，您需要定义一个超时时间，以便在等待形成批处理时不会延迟单个证书的处理。

OCSP 响应缓存

缓存从 OCSP 响应程序收到的响应可以加快对用户的响应速度，并减少 OCSP 响应程序的负载。从 OCSP 响应程序收到客户端证书的吊销状态后，NetScaler Gateway 会在本地缓存该响应一段预定义的时间。当在 SSL 握手期间收到客户端证书时，NetScaler Gateway 首先检查其本地缓存中是否存在此证书的条目。如果找到仍然有效（在缓存超时限制内）的条目，则评估该条目并接受或拒绝客户端证书。如果未找到证书，NetScaler Gateway 会向 OCSP 响应程序发送请求，并将响应存储在其本地缓存中一段配置的时间。

配置 OCSP 证书状态

配置在线证书状态协议 (OCSP) 涉及添加 OCSP 响应程序、将 OCSP 响应程序绑定到证书颁发机构 (CA) 颁发的签名证书，以及将证书和私钥绑定到安全套接字层 (SSL) 虚拟服务器。如果您需要将不同的证书和私钥绑定到已配置的 OCSP 响应程序，则需要先解除绑定该响应程序，然后将其绑定到不同的证书。

配置 OCSP

1. 在“配置”选项卡上，在导航窗格中，展开“SSL”，然后单击“OCSP 响应程序”。
2. 在详细信息窗格中，单击“添加”。
3. 在“名称”中，键入配置文件的名称。
4. 在“URL”中，键入 OCSP 响应程序的 Web 地址。

   此字段为必填项。Web 地址不能超过 32 个字符。
5. 要缓存 OCSP 响应，请单击“缓存”，然后在“超时”中键入 NetScaler Gateway 保留响应的分钟数。
6. 在“请求批处理”下，单击“启用”。
7. 在“批处理延迟”中，指定允许批处理一组 OCSP 请求的时间（以毫秒为单位）。

   值范围为 0 到 10000。默认值为 1。
8. 在“生成时间偏差”中，键入设备必须检查或接受响应时 NetScaler Gateway 可以使用的时间量。
9. 在“响应验证”下，如果要禁用 OCSP 响应程序进行的签名检查，请选择“信任响应”。

   如果启用“信任响应”，请跳过步骤 8 和步骤 9。

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

10. 在“证书”中，选择用于签署 OCSP 响应的证书。

    如果未选择证书，则使用 OCSP 响应程序绑定的 CA 来验证响应。

11. 在“请求超时”中，键入等待 OCSP 响应的毫秒数。

    此时间包括“批处理延迟”时间。值范围为 0 到 120000。默认值为 2000。

12. 在“签名证书”中，选择用于签署 OCSP 请求的证书和私钥。如果未指定证书和私钥，则请求将不会签名。
13. 要启用一次性使用的数字 `(nonce) extension`，请选择“随机数”。
14. 要使用客户端证书，请单击“客户端证书插入”。
15. 点击“创建”，然后点击“关闭”。

管理 NetScaler Gateway 配置设置

当您对 NetScaler Gateway 进行配置更改时，这些更改会保存到日志文件中。您可以查看以下几种类型的配置设置：

- 已保存的配置。您可以查看已在 NetScaler Gateway 上保存的设置。
- 正在运行的配置。您可以查看已配置但尚未作为已保存配置保存到 NetScaler Gateway 的活动设置，例如虚拟服务器或身份验证策略。
- 正在运行的配置与已保存的配置。您可以并排比较 NetScaler Gateway 上正在运行的配置和已保存的配置。

您还可以清除 NetScaler Gateway 上的配置设置。

重要提示：

如果您选择清除 NetScaler Gateway 上的设置，则证书、虚拟服务器和策略将被删除。Citrix 建议您不要清除配置。

保存 NetScaler Gateway 配置

您可以将 NetScaler Gateway 上的当前配置保存到网络中的计算机，查看当前正在运行的配置，并比较已保存和正在运行的配置。

在 NetScaler Gateway 上保存配置

1. 在配置实用程序中，在详细信息窗格上方，单击“保存”图标，然后单击“是”。

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

在 NetScaler Gateway 上查看和保存配置文件

已保存的配置是保存在 NetScaler Gateway 日志文件中的设置，例如虚拟服务器、策略、IP 地址、用户、组和证书的设置。

在 NetScaler Gateway 上配置设置时，您可以将设置保存到计算机上的文件中。如果您需要重新安装 NetScaler Gateway 软件或不小心删除了某些设置，可以使用此文件来恢复配置。如果需要恢复设置，可以将文件复制到 NetScaler Gateway，然后使用命令行界面或 WinSCP 等程序将文件复制到 NetScaler Gateway，并重新启动设备。

1. 在配置实用程序中，在“配置”选项卡上，在导航窗格中，展开“系统”，然后单击“诊断”。
2. 在详细信息窗格中，在“查看配置”下，单击“已保存配置”。
3. 在“已保存配置”对话框中，单击“将输出文本保存到文件”，命名文件，然后单击“保存”。 注意：Citrix 建议使用文件名 ns.conf 保存文件。

查看当前运行配置

对 NetScaler Gateway 进行的任何未保存的更改都称为运行配置。这些设置在 NetScaler Gateway 上处于活动状态，但未保存在设备上。如果配置了其他设置，例如策略、虚拟服务器、用户或组，则可以在运行配置中查看这些设置。

1. 在配置实用程序中，在“配置”选项卡上，在导航窗格中，展开“系统”，然后单击“诊断”。
2. 在详细信息窗格中，在“查看配置”下，单击“运行配置”。

比较已保存配置和运行配置

您可以查看设备上保存了哪些设置，并将这些设置与运行配置进行比较。您可以选择保存运行配置或更改配置。

1. 在配置实用程序中，在“配置”选项卡上，在导航窗格中，展开“系统”，然后单击“诊断”。
2. 在详细信息窗格中，在“查看配置”下，单击“已保存与运行”。

清除 NetScaler Gateway 配置

您可以清除 NetScaler Gateway 上的配置设置。您可以从以下三个级别的设置中选择要清除的设置：

重要提示：

Citrix 建议您在清除 NetScaler Gateway 配置设置之前保存配置。

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

- 基本。清除设备上的所有设置，但系统 IP 地址、默认网关、映射的 IP 地址、子网 IP 地址、DNS 设置、网络设置、高可用性设置、管理密码以及功能和模式设置除外。
- 扩展。清除所有设置，但系统 IP 地址、映射的 IP 地址、子网 IP 地址、DNS 设置和高可用性定义除外。
- 完整。将配置恢复到原始出厂设置，不包括系统 IP (NSIP) 地址和默认路由，这些是维护设备网络连接所必需的。

当您清除部分或全部配置时，功能设置将恢复为出厂默认设置。

清除配置时，存储在 NetScaler Gateway 上的文件（例如证书和许可证）不会被删除。文件 ns.conf 不会被更改。如果您想在清除配置之前保存配置，请先将配置保存到您的计算机。如果您保存了配置，则可以在 NetScaler Gateway 上恢复 ns.conf 文件。将文件恢复到设备并重新启动 NetScaler Gateway 后，ns.conf 中的所有配置设置都将恢复。

对配置文件（例如 rc.conf）的修改不会被还原。

如果您有高可用性对，两个 NetScaler Gateway 设备都会以相同的方式进行修改。例如，如果您清除一个设备上的基本配置，则更改会传播到第二个设备。

清除 NetScaler Gateway 配置设置

1. 在配置实用程序中，在“配置”选项卡上，在导航窗格中，展开“系统”，然后单击“诊断”。
2. 在详细信息窗格中，在“维护”下，单击“清除配置”。
3. 在“配置级别”中，选择要清除的级别，然后单击“运行”。

测试您的 NetScaler Gateway 配置

在 NetScaler Gateway 上配置初始设置后，您可以通过连接到设备来测试您的设置。

要测试 NetScaler Gateway 设置，请创建一个本地用户帐户。然后，使用虚拟服务器 IP 地址或设备的完全限定域名 (FQDN)，打开 Web 浏览器并键入网址。例如，在地址栏中键入 `https://my.company.com` 或 `https://192.168.96.183`。

在登录屏幕上，输入您之前创建的用户帐户的用户名和密码。登录后，系统会提示您下载并安装 Citrix Secure Access™ 客户端。

安装并成功连接 Citrix Secure Access 客户端后，将显示访问界面。访问界面是 NetScaler Gateway 的默认主页。

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

使用 GUI 创建用户帐户

1. 在配置实用程序中，在“配置”选项卡上的导航窗格中，展开 **NetScaler Gateway \ > 用户管理**，然后单击 **AAA 用户**。
2. 在详细信息窗格中，单击“添加”。
3. 在“用户名”中，键入用户名。
4. 如果使用本地身份验证，请清除“外部身份验证”复选框。使用外部身份验证类型（例如 LDAP 或 RADIUS）对用户进行身份验证是默认设置。如果清除此复选框，NetScaler Gateway 将对用户进行身份验证。
5. 在“密码”和“确认密码”中，键入用户的密码，单击“创建”，然后单击“关闭”。

使用配置实用程序添加用户时，可以将以下策略绑定到用户：

- 授权
- 流量、会话和审计
- 书签
- 内网应用程序
- 内网 IP 地址

如果使用测试用户帐户登录时遇到问题，请检查以下内容：

- 如果您收到证书警告，则表示 NetScaler Gateway 上安装了测试证书或无效证书。如果设备上安装了由证书颁发机构 (CA) 签名的证书，请确保用户设备上存在相应的根证书。
- 如果您使用了 CA 签名的证书，请验证您是否使用签名的证书签名请求 (CSR) 正确生成了站点证书，以及在 CSR 中输入的专有名称 (DN) 数据是否准确。问题也可能是主机名与签名证书上的 IP 地址不匹配。请检查配置的证书的通用名称是否与配置的虚拟服务器 IP 地址信息相对应。
- 如果未显示登录屏幕或出现任何其他错误消息，请检查设置过程并确认您已正确执行所有步骤并准确输入所有参数。

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

升级 NetScaler Gateway 软件

当有新版本发布时，您可以升级 NetScaler Gateway 上的软件。您可以在 Citrix 网站上检查更新。只有当您的 NetScaler Gateway 许可证在更新发布时属于 Subscription Advantage 计划，您才能升级到新版本。您可以随时续订 Subscription Advantage。有关详细信息，请参阅 NetScaler 支持 网站。

升级路径和兼容产品信息也可在 Citrix 升级指南 中找到。

有关最新的 NetScaler Gateway 维护版本信息，请参阅 NetScaler 发行说明。

检查软件更新

1. 转到 Citrix 网站。
2. 单击 **“我的帐户”** 并登录。
3. 单击 **“下载”**。
4. 在“查找下载”下，选择 **NetScaler Gateway**。
5. 在 **“选择下载类型”** 中，选择 **“产品软件”**，然后单击 **“查找”**。 您也可以选择 **“虚拟设备”** 来下载 NetScaler VPX。当您选择此选项时，您会收到每个虚拟机管理程序的虚拟机软件列表。
6. 在 NetScaler Gateway 页面上，展开 **NetScaler Gateway 或 Access Gateway**。
7. 单击您要下载的设备软件版本。
8. 在您要下载的版本的设备软件页面上，选择虚拟设备，然后单击 **“下载”**。
9. 按照屏幕上的说明下载软件。

软件下载到您的计算机后，您可以使用升级向导或命令提示符安装软件。

使用升级向导升级 NetScaler Gateway

1. 在配置实用程序中，在导航窗格的“**配置**”选项卡上，单击“系统”。
2. 在详细信息窗格中，单击“**升级向导**”。
3. 单击“**下一步**”，然后按照向导中的说明进行操作。

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

使用命令提示符升级 NetScaler Gateway

1. 要将软件上传到 NetScaler Gateway，请使用安全的 FTP 客户端（例如 WinSCP）连接到设备。
2. 将软件从您的计算机复制到设备上的 /var/`nsinstall` 目录。
3. 使用 Secure Shell (SSH) 客户端（例如 PuTTY）打开与设备的 SSH 连接。
4. 登录到 NetScaler Gateway。
5. 在命令提示符下，键入：`shell`
6. 要更改到 `nsinstall` 目录，请在命令提示符下键入：`cd /var/nsinstall`
7. 要查看目录内容，请键入：`ls`
8. 要解压软件，请键入：tar –xvzf build_X_XX.tgz，其中 build_X_XX.tgz 是您要升级到的版本的名称。
9. 要开始安装，请在命令提示符下键入：`./installns`
10. 安装完成后，重新启动 NetScaler Gateway。

NetScaler Gateway 重启后，为验证安装成功，请启动配置实用程序。设备上的 NetScaler Gateway 版本将显示在右上角。

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

在双跳 DMZ 中部署 NetScaler Gateway

有些组织使用三个防火墙来保护其内部网络。这三个防火墙将 DMZ 分为两个阶段，为内部网络提供额外的安全层。这种网络配置称为双跳 DMZ。

图 1. 部署在双跳 DMZ 中的 NetScaler Gateway 设备

在双跳 DMZ 中部署 NetScaler Gateway(/en-us/netscaler-gateway/media/ng-doublehop-dmz-new-icons.png)

注意：

为便于说明，前面的示例描述了一个使用三个防火墙的双跳配置，其中包含 StoreFront、NetScaler Gateway 和 Citrix Virtual Apps。但是，您也可以拥有一个双跳 DMZ，其中一个设备位于 DMZ 中，另一个设备位于安全网络中。如果您配置了一个双跳配置，其中一个设备位于 DMZ 中，另一个设备位于安全网络中，则可以忽略在第三个防火墙上打开端口的说明。

您可以配置双跳 DMZ 以支持与 NetScaler Gateway 代理并行安装的 Citrix StoreFront。用户通过使用 Citrix Workspace 应用程序进行连接。

注意：

如果您在带有 StoreFront 的双跳 DMZ 中部署 NetScaler Gateway，Citrix Workspace 应用程序的基于电子邮件的自动发现功能将不起作用。

双跳部署的工作原理

您可以在双跳 DMZ 中部署 NetScaler Gateway 设备，以控制对运行 Citrix Virtual Apps 的服务器的访问。双跳部署中的连接按以下方式进行：

- 用户通过使用 Web 浏览器连接到第一个 DMZ 中的 NetScaler Gateway，并使用 Citrix Workspace 应用程序选择已发布的应用程序。
- Citrix Workspace 应用程序在用户设备上启动。用户连接到 NetScaler Gateway 以访问安全网络中服务器场中运行的已发布应用程序。

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

注意： 双跳 DMZ 部署不支持 Secure Hub 和适用于 Windows 的 Citrix Secure Access 客户端。仅使用 Citrix Workspace 应用程序进行用户连接。

- 第一个 DMZ 中的 NetScaler Gateway 处理用户连接并执行 SSL VPN 的安全功能。此 NetScaler Gateway 加密用户连接，确定用户如何进行身份验证，并控制对内部网络中服务器的访问。
- 第二个 DMZ 中的 NetScaler Gateway 用作 NetScaler Gateway 代理设备。此 NetScaler Gateway 使 ICA 流量能够穿过第二个 DMZ，以完成用户到服务器场的连接。第一个 DMZ 中的 NetScaler Gateway 与内部网络中的安全票证颁发机构 (STA) 之间的通信也通过第二个 DMZ 中的 NetScaler Gateway 进行代理。

NetScaler Gateway 支持 IPv4 和 IPv6 连接。您可以使用配置实用程序来配置 IPv6 地址。

下表显示了双跳部署对各种 ICA® 功能的支持：

ICA 功能	双跳支持
SmartAccess	是
SmartControl	是
智能数据传输 (EDT)	是
HDX 洞察	是
ICA 会话可靠性（端口 2598）	是
ICA 会话迁移	是
ICA 会话超时	是
多流 ICA	是（仅限 TCP）
弗雷姆霍克	否
UDP 音频	否

准备双跳 DMZ 部署

配置双跳 DMZ 部署时，您必须回答以下问题：

- 我是否要支持负载平衡？

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

- 我需要在防火墙上打开哪些端口？
- 我需要多少个 SSL 证书？
- 在开始部署之前，我需要哪些组件？

本节中的主题包含有助于您根据环境回答这些问题的信息。

开始部署所需的组件

在开始双跳 DMZ 部署之前，请确保您拥有以下组件：

- 至少需要两个 NetScaler Gateway 设备（每个 DMZ 一个）。
- 运行 Citrix Virtual Apps™ 的服务器必须安装并在内部网络中运行。
- StoreFront™ 必须安装在第二个 DMZ 中，并配置为与内部网络中的服务器场协同工作。
- 至少一个 SSL 服务器证书必须安装在第一个 DMZ 中的 NetScaler Gateway 上。此证书可确保 Web 浏览器和用户到 NetScaler Gateway 的连接是加密的。

  如果您希望加密双跳 DMZ 部署中其他组件之间的连接，则需要额外的证书。

双跳 DMZ 部署中的通信流

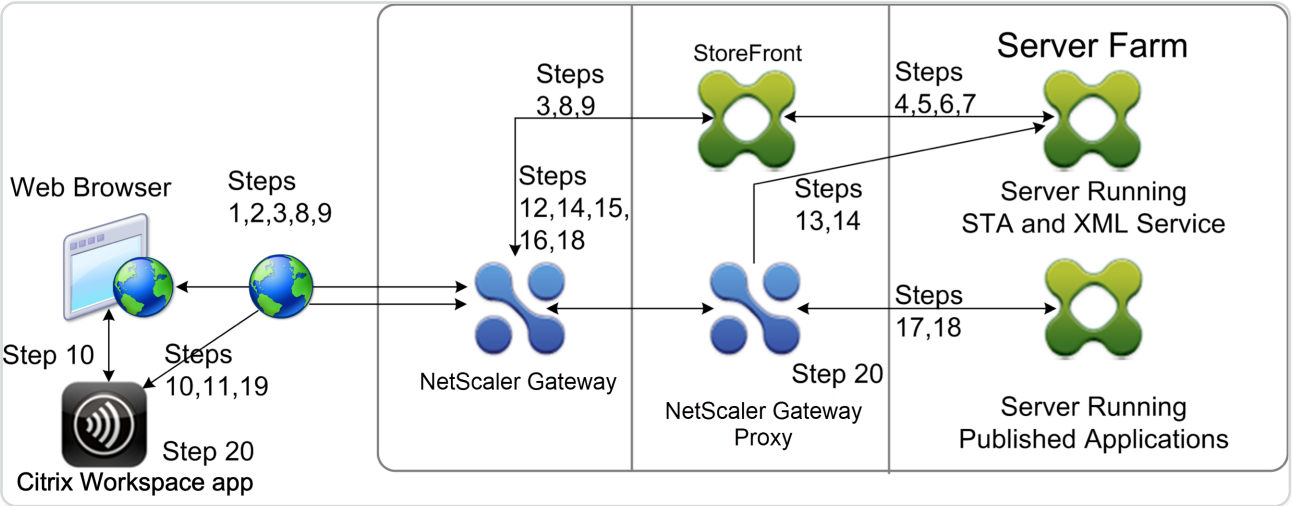
要了解双跳 DMZ 部署中涉及的配置问题，您必须对双跳 DMZ 部署中各种 NetScaler Gateway 和 Citrix Virtual Apps 组件如何通信以支持用户连接有基本的了解。

用户连接到 StoreFront™ 的过程以连续流的形式发生。此过程涉及以下高级步骤。

- 验证用户
- 创建会话票证
- 启动 Citrix Workspace 应用程序
- 完成连接

下图显示了用户连接到 StoreFront 过程中发生的步骤。在安全网络中，运行 Citrix Virtual Apps™ 的计算机也运行安全票证颁发机构 (STA)、XML 服务和已发布的应用程序。

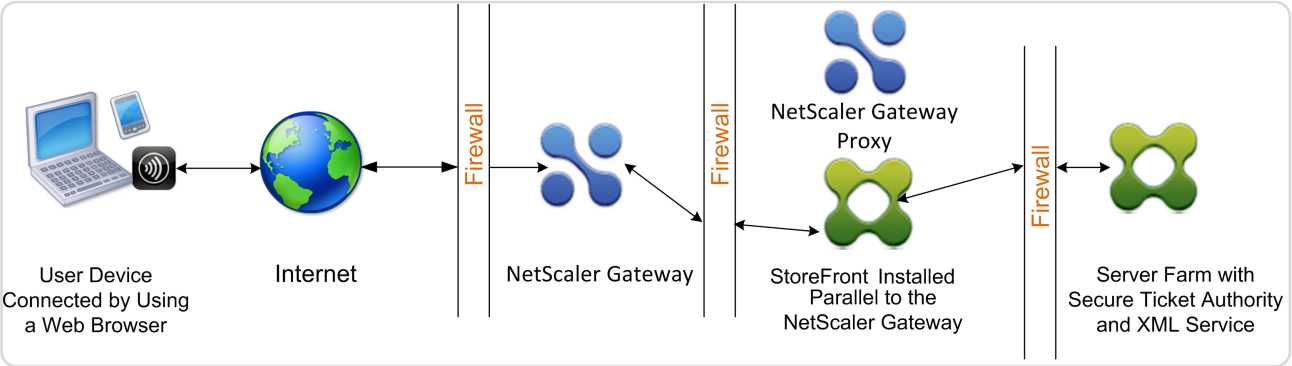
© 1997–2026 Citrix Systems, Inc. All rights reserved.



连接过程

验证用户是双跳 DMZ 部署中用户连接过程的第一步。

下图显示了此部署中的用户连接过程。



在用户身份验证阶段，会发生以下基本过程：

1. 用户在 Web 浏览器中键入 NetScaler Gateway 的地址（例如 `<https://www.ng.wxyco.com>` ）以连接到第一个 DMZ 中的 NetScaler Gateway。如果您在 NetScaler Gateway 上启用了登录页面身份验证，则 NetScaler Gateway 会对用户进行身份验证。
2. 第一层DMZ中的NetScaler Gateway接收请求。
3. NetScaler Gateway 将 Web 浏览器连接重定向到 StoreFront。
4. StoreFront 将用户凭据发送到内部网络中服务器场中运行的 Citrix® XML 服务。
5. Citrix XML 服务对用户进行身份验证。
6. XML 服务创建用户有权访问的已发布应用程序列表，并将此列表发送到 StoreFront。

   注意：

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

- 如果您在 NetScaler Gateway 上启用身份验证，设备会将 NetScaler Gateway 登录页面发送给用户。用户在登录页面上输入身份验证凭据，设备对用户进行身份验证。然后，NetScaler Gateway 将用户凭据返回到 StoreFront。
- 如果您未启用身份验证，NetScaler Gateway 不会执行身份验证。设备连接到 StoreFront，检索 StoreFront 登录页面，并将 StoreFront 登录页面发送给用户。用户在 StoreFront 登录页面上输入身份验证凭据，NetScaler Gateway 将用户凭据传回 StoreFront。

创建会话票证是双跳 DMZ 部署中用户连接过程的第二阶段。

在会话票证创建阶段，会发生以下基本过程：

7. StoreFront 与内部网络中的 XML 服务和安全票证颁发机构 (STA) 进行通信，为用户有权访问的每个已发布应用程序生成会话票证。会话票证包含运行托管已发布应用程序的 Citrix Virtual Apps 的计算机的别名地址。
8. STA 保存托管已发布应用程序的服务器的 IP 地址。然后，STA 将请求的会话票证发送到 StoreFront。每个会话票证都包含一个别名，该别名表示托管已发布应用程序的服务器的 IP 地址，但不是实际的 IP 地址。
9. StoreFront 为每个已发布应用程序生成一个 ICA® 文件。ICA 文件包含由 STA 颁发的票证。然后，StoreFront 创建一个网页，其中包含指向已发布应用程序的链接列表，并将此网页发送到用户设备上的 Web 浏览器。

启动 Citrix Workspace 应用程序是双跳 DMZ 部署中用户连接过程的第三阶段。基本过程如下：

10. 用户单击 StoreFront 中已发布应用程序的链接。StoreFront 将该已发布应用程序的 ICA 文件发送到用户设备的浏览器。

    ICA 文件包含指示 Web 浏览器启动 Receiver 的数据。

    ICA 文件还包含第一个 DMZ 中 NetScaler Gateway 的完全限定域名 (FQDN) 或域名系统 (DNS) 名称。
11. Web 浏览器启动 Receiver，用户使用 ICA 文件中的 NetScaler Gateway 名称连接到第一个 DMZ 中的 NetScaler Gateway。进行初始 SSL/TLS 握手以建立运行 NetScaler Gateway 的服务器的身份。

完成连接是双跳 DMZ 部署中用户连接过程的第四个也是最后一个阶段。

在连接完成阶段，会发生以下基本过程：

- 用户单击 StoreFront 中已发布应用程序的链接。
- Web 浏览器接收 StoreFront 生成的 ICA 文件并启动 Citrix Workspace 应用程序。 注意：ICA 文件包含指示 Web 浏览器启动 Citrix Workspace 应用程序的代码。

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

- Citrix Workspace 应用程序启动与第一个 DMZ 中 NetScaler Gateway 的 ICA 连接。
- 第一个 DMZ 中的 NetScaler Gateway 与内部网络中的安全票证颁发机构 (STA) 通信，以将会话票证中的别名地址解析为运行 Citrix Virtual Apps 或 StoreFront 的计算机的真实 IP 地址。此通信通过第二个 DMZ 由 NetScaler Gateway 代理进行代理。
- 第一个 DMZ 中的 NetScaler Gateway 完成与 Citrix Workspace 应用程序的 ICA 连接。
- Citrix Workspace 应用程序现在可以通过两个 NetScaler Gateway 设备与内部网络上运行 Citrix Virtual Apps 的计算机进行通信。

完成用户连接过程的详细步骤如下：

12. Citrix Workspace 应用程序将已发布应用程序的 STA 票证发送到第一个 DMZ 中的 NetScaler Gateway。
13. 第一个 DMZ 中的 NetScaler Gateway 联系内部网络中的 STA 进行票证验证。为了联系 STA，NetScaler Gateway 与第二个 DMZ 中的 NetScaler Gateway 代理建立 SOCKS 或带 SSL 的 SOCKS 连接。
14. 第二个 DMZ 中的 NetScaler Gateway 代理将票证验证请求传递给内部网络中的 STA。STA 验证票证并将其映射到托管已发布应用程序的运行 Citrix Virtual Apps 的计算机。
15. STA 将响应发送到第二层 DMZ 中的 NetScaler Gateway 代理，该响应随后传递到第一层 DMZ 中的 NetScaler Gateway。此响应完成票证验证，并包含托管已发布应用程序的计算机的 IP 地址。
16. 第一层 DMZ 中的 NetScaler Gateway 将 Citrix Virtual Apps 服务器的地址合并到用户连接数据包中，并将此数据包发送到第二层 DMZ 中的 NetScaler Gateway 代理。
17. 第二层 DMZ 中的 NetScaler Gateway 代理向连接数据包中指定的服务器发出连接请求。
18. 服务器响应第二层 DMZ 中的 NetScaler Gateway 代理。第二层 DMZ 中的 NetScaler Gateway 代理将此响应传递到第一层 DMZ 中的 NetScaler Gateway，以完成服务器与第一层 DMZ 中的 NetScaler Gateway 之间的连接。
19. 第一层 DMZ 中的 NetScaler Gateway 通过将最终连接数据包传递给用户设备，完成与用户设备的 SSL/TLS 握手。用户设备与服务器之间的连接已建立。
20. ICA 流量在用户设备和服务器之间流动，通过第一层 DMZ 中的 NetScaler Gateway 和第二层 DMZ 中的 NetScaler Gateway 代理。

在双跳 DMZ 中安装和配置 NetScaler Gateway

您需要完成几个步骤才能在双跳 DMZ 中部署 NetScaler Gateway。这些步骤包括在两个 DMZ 中安装设备以及配置设备以进行用户设备连接。

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

在第一个 DMZ 中安装 NetScaler Gateway

要在第一个 DMZ 中安装 NetScaler Gateway，请按照 安装硬件 中的说明进行操作。

如果您要在第一个 DMZ 中安装多个 NetScaler Gateway 设备，则可以将这些设备部署在负载均衡器后面。

在第一个 DMZ 中配置 NetScaler Gateway

在双跳 DMZ 部署中，必须将第一个 DMZ 中的每个 NetScaler Gateway 配置为将连接重定向到第二个 DMZ 中的 StoreFront。

重定向到 StoreFront 是在 NetScaler Gateway 全局或虚拟服务器级别执行的。要通过 NetScaler Gateway 连接到 StoreFront，用户必须与已启用重定向到 StoreFront 的 NetScaler Gateway 用户组相关联。

在第二个 DMZ 中安装 NetScaler Gateway

第二个 DMZ 中的 NetScaler Gateway 设备称为 NetScaler Gateway 代理，因为它代理跨第二个 DMZ 的 ICA 和安全票证颁发机构 (STA) 流量。 安装硬件 以在第二个 DMZ 中安装每个 NetScaler Gateway 设备。

您可以使用此安装过程在第二个 DMZ 中安装其他设备。

在第二个 DMZ 中安装 NetScaler Gateway 设备后，请配置以下设置：

- 在 NetScaler Gateway 代理上配置虚拟服务器。
- 配置第一个和第二个 DMZ 中的 NetScaler Gateway 设备以相互通信。
- 将第二个 DMZ 中的 NetScaler Gateway 全局绑定或绑定到虚拟服务器。
- 在第一个DMZ中的设备上配置STA。
- 打开分隔DMZ的防火墙中的端口。
- 在设备上安装证书。

在 NetScaler Gateway 代理上的虚拟服务器上配置设置

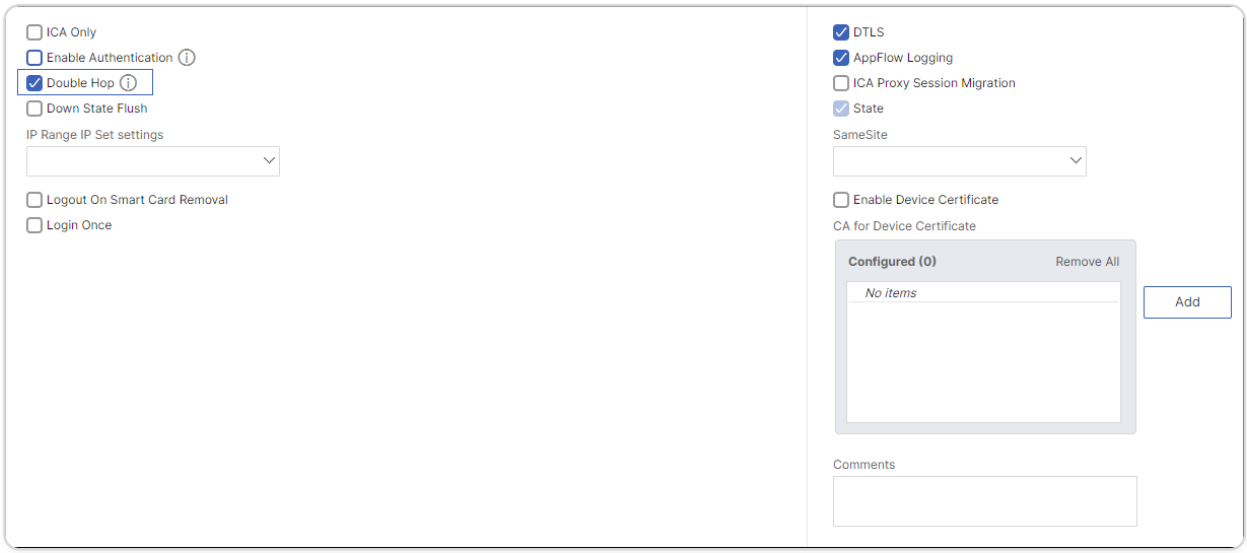
为了允许连接在 NetScaler Gateway 设备之间传递，您需要在 NetScaler Gateway 代理上的虚拟服务器中启用双跳。

当用户连接时，NetScaler Gateway 设备会验证用户，然后将连接代理到代理设备。在第一个 DMZ 中的 NetScaler Gateway 上，配置虚拟服务器以与第二个 DMZ 中的 NetScaler Gateway 进行通信。不要在 NetScaler Gateway 代理上配置身份验证或策略。Citrix 建议禁用虚拟服务器上的身份验证。

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

使用 GUI 在 NetScaler Gateway 代理上的虚拟服务器上启用双跳

1. 导航到 **配置 > NetScaler Gateway > 虚拟服务器**。
2. 选择一个虚拟服务器，然后单击 **Edit**。
3. 在 **Basic Settings** 部分中，单击编辑图标，然后单击 **More**。
4. 选择 **Double Hop**。



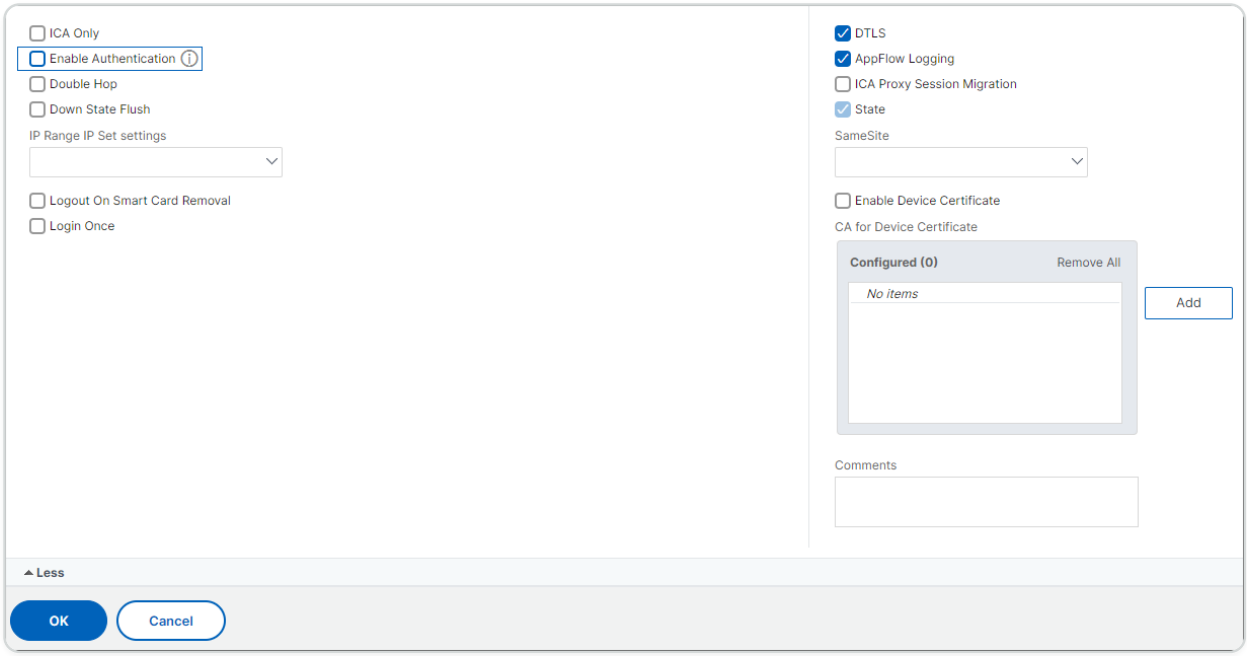
5. 单击 **OK**。

使用 GUI 禁用 NetScaler Gateway 代理上的虚拟服务器上的身份验证

1. 导航到 **配置 > NetScaler Gateway > 虚拟服务器**。
2. 选择一个虚拟服务器，然后单击 **Edit**。
3. 在 **Basic Settings** 部分中，单击编辑图标，然后单击 **More**。

4. 取消选中**启用身份验证**复选框。

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



5. 单击**确定**。

配置设备以与设备代理通信

当您在双跳 DMZ 中部署 NetScaler Gateway 时，您必须配置第一个 DMZ 中的 NetScaler Gateway 以与第二个 DMZ 中的 NetScaler Gateway 代理通信。

如果您在第二个 DMZ 中部署了多个设备，您需要配置第一个 DMZ 中的每个设备以与第二个 DMZ 中的每个代理设备通信。

注意：如果您想使用 IPv6，您可以使用配置实用程序配置下一跳服务器。为此，请展开 NetScaler Gateway \> Resources，然后单击 Next Hop Servers。按照以下步骤操作，然后选中 IPv6 复选框。

配置 NetScaler Gateway 以与 NetScaler Gateway 代理通信

1. 在配置实用程序中，在“配置”选项卡上，展开 NetScaler Gateway \> Resources，然后单击 Next Hop Servers。
2. 在详细信息窗格中，单击“添加”。
3. 在“名称”中，键入第一个 NetScaler Gateway 的名称。
4. 在“IP 地址”中，键入第二个 DMZ 中 NetScaler Gateway 代理的虚拟服务器 IP 地址。
5. 在“端口”中，键入端口号，单击“创建”，然后单击“关闭”。如果您使用的是安全端口（例如 443），请选择“安全”。

您必须配置安装在第一个 DMZ 中的每个 NetScaler Gateway，以与安装在第二个 DMZ 中的所有 NetScaler Gateway 代理设备通信。

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

配置 NetScaler Gateway 代理的设置后，将策略绑定到 NetScaler Gateway Global 中的下一跳服务器或虚拟服务器。

全局绑定 NetScaler Gateway 下一跳服务器

1. 在配置实用程序中，在“配置”选项卡上，展开 NetScaler Gateway \> Resources，然后单击 Next Hop Servers。
2. 在详细信息窗格中，选择一个下一跳服务器，然后在“操作”中，选择“全局绑定”。
3. 在“配置下一跳服务器全局绑定”对话框中，在“下一跳服务器名称”中，选择代理设备，然后单击“确定”。

将 NetScaler Gateway 下一跳服务器绑定到虚拟服务器

1. 在配置实用程序中，在“配置”选项卡上，展开 NetScaler Gateway，然后单击“虚拟服务器”。
2. 在详细信息窗格中，选择一个虚拟服务器，然后单击“打开”。
3. 在“已发布的应用程序”选项卡上，在“下一跳服务器”下，单击一个项目，然后单击“确定”。

您还可以从“已发布的应用程序”选项卡添加下一跳服务器。

配置 NetScaler Gateway 以处理 STA 和 ICA 流量

当您在双跳 DMZ 中部署 NetScaler Gateway 时，您必须在第一个 DMZ 中配置 NetScaler Gateway，以适当处理与安全票证颁发机构 (STA) 的通信和 ICA 流量。运行 STA 的服务器可以全局绑定，也可以绑定到虚拟服务器。

配置 STA 后，您可以将 STA 全局绑定，也可以绑定到虚拟服务器。

要全局配置和绑定 STA：

1. 在 GUI 中，在“配置”选项卡上，展开 **NetScaler Gateway**，然后单击 **全局设置**。
2. 在详细信息窗格中，在 **服务器** 下，单击 **绑定/取消绑定安全票证颁发机构使用的 STA 服务器**。
3. 在 **绑定/取消绑定 STA 服务器** 对话框中，单击 **添加**。
4. 在 **配置 STA 服务器** 对话框中，在 **URL** 中，键入运行 STA 的服务器路径，例如 `<http://mycompany.com>` 或 `<http://ipAddress>`，然后单击 **创建**。

要配置 STA 并将其绑定到虚拟服务器：

1. 在 GUI 中，在“配置”选项卡上，展开 **NetScaler Gateway**，然后单击 **虚拟服务器**。
2. 在详细信息窗格中，选择一个虚拟服务器，然后单击 **打开**。
3. 在 **已发布的应用程序** 选项卡上，在 **安全票证颁发机构** 下，单击 **添加**。

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

4. 在 **配置 STA 服务器** 对话框中，在 URL 中，键入运行 STA 的服务器路径，例如 `<http://mycompany.com>` 或 `<http://ipAddress>`，然后单击 **创建**。

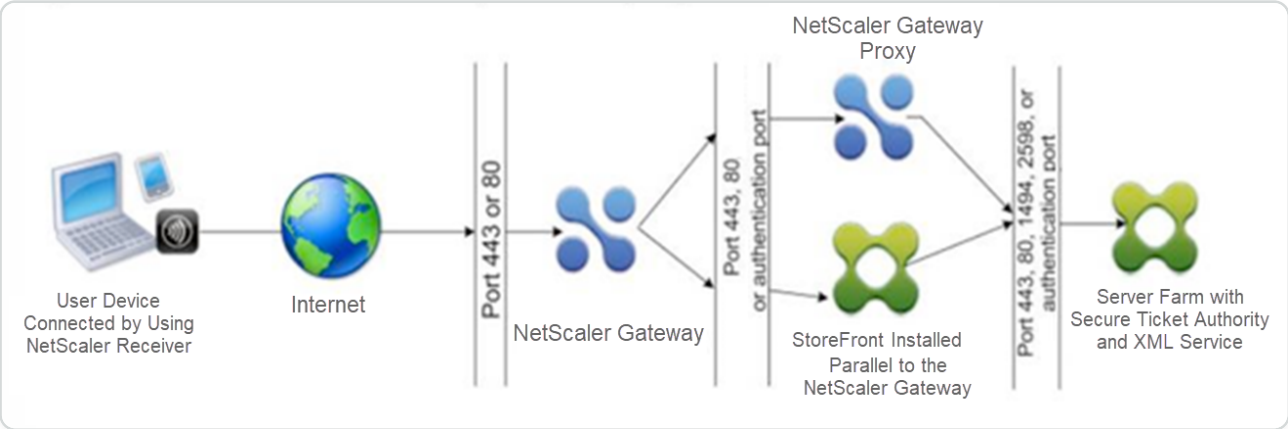
注意：

如果 VPN 虚拟服务器共享相同的下一跳虚拟服务器和 STA 服务器，则当公共 STA 服务器从共享相同下一跳虚拟服务器的虚拟服务器中解除绑定时，连接将重置。

在防火墙上打开相应的端口

您必须确保在防火墙上打开相应的端口，以支持双跳 DMZ 部署中涉及的各种组件之间发生的各种连接。有关连接和通信过程的更多信息，请参阅双跳 DMZ 部署中的通信流。

下图显示了双跳 DMZ 部署中可以使用的常用端口。



下表显示了通过第一个防火墙发生的连接以及必须打开以支持这些连接的端口。

通过第一个防火墙的连接	使用的端口
来自 Internet 的 Web 浏览器连接到第一个 DMZ 中的 NetScaler Gateway。**注意：** NetScaler Gateway 包含一个选项，可将端口 80 上的连接重定向到安全端口。如果在 NetScaler Gateway 上启用此选项，则可以通过第一个防火墙打开端口 80。当用户在端口 80 上与 NetScaler Gateway 建立未加密连接时，NetScaler Gateway 会自动将连接重定向到安全端口。	通过第一个防火墙打开 TCP 端口 443。
来自 Internet 的 Citrix Workspace 应用程序连接到第一个 DMZ 中的 NetScaler Gateway。	通过第一个防火墙打开 TCP 端口 443。

下表显示了通过第二个防火墙发生的连接以及必须打开以支持这些连接的端口。

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

通过第二个防火墙的连接	使用的端口
第一个 DMZ 中的 NetScaler Gateway 连接到第二个 DMZ 中的 StoreFront。	通过第二个防火墙，为不安全连接打开 TCP 端口 80，或为安全连接打开 TCP 端口 443。
第一个 DMZ 中的 NetScaler Gateway 连接到第二个 DMZ 中的 NetScaler Gateway。	通过第二个防火墙，为安全的 SOCKS 连接打开 TCP 端口 443。
如果您在第一个 DMZ 中的 NetScaler Gateway 上启用了身份验证，则此设备可能需要连接到内部网络中的身份验证服务器。	打开身份验证服务器侦听连接的 TCP 端口。例如，RADIUS 使用端口 1812，LDAP 使用端口 389。

下表显示了通过第三个防火墙发生的连接以及必须打开以支持这些连接的端口。

通过第三个防火墙的连接	使用的端口
第二个 DMZ 中的 StoreFront 连接到内部网络中服务器上托管的 XML 服务。	通过第三个防火墙，为不安全连接打开端口 80，或为安全连接打开端口 443。
第二个 DMZ 中的 StoreFront 连接到内部网络中服务器上托管的安全票证颁发机构 (STA)。	通过第三个防火墙，为不安全连接打开端口 80，或为安全连接打开端口 443。
第二个 DMZ 中的 NetScaler Gateway 连接到安全网络中的 STA。	通过第三个防火墙，为不安全连接打开端口 80，或为安全连接打开端口 443。
第二个 DMZ 中的 NetScaler Gateway 与内部网络中服务器上发布的应用程序或虚拟桌面建立 ICA 连接。	打开 TCP 端口 1494 以支持通过第三个防火墙的 ICA 连接。如果您在 Citrix Virtual Apps 上启用了会话可靠性，则打开 TCP 端口 2598 而不是 1494。
如果您在第一个 DMZ 中的 NetScaler Gateway 上启用了身份验证，则此设备可能需要连接到内部网络中的身份验证服务器。	打开身份验证服务器侦听连接的 TCP 端口。例如，RADIUS 使用端口 1812，LDAP 使用端口 389。

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

维护和监控系统

完成 NetScaler Gateway 配置后，您需要维护和监控设备。您可以通过以下方式进行操作：

- 您可以将 NetScaler Gateway 升级到最新版本的软件。登录 Citrix 网站后，您可以导航到 NetScaler Gateway 下载站点并下载软件。您可以在 Citrix 知识中心找到维护版本的自述文件。
- 您可以将 NetScaler Gateway 配置和管理任务分配给组中的不同成员。通过委派管理，您可以为个人分配访问级别，从而限制他们在 NetScaler Gateway 上执行特定任务。
- 您可以将 NetScaler Gateway 配置保存到设备或计算机上的文件中。您可以比较当前运行的配置和已保存的配置。您还可以从 NetScaler Gateway 中清除配置。
- 您可以在 NetScaler Gateway 配置实用程序中查看、刷新和结束用户会话。
- 您可以在 NetScaler Gateway 上配置日志记录。日志提供有关设备的重要信息，并在您遇到问题时非常有用。

配置委派管理员

NetScaler Gateway 具有默认的管理员用户名和密码。默认用户名和密码是 `nsroot`。首次运行安装向导时，您可以更改管理员密码。

您可以创建更多管理员帐户，并为每个帐户分配不同级别的 NetScaler Gateway 访问权限。这些附加帐户称为委派管理员。例如，您可以指派一个人负责监视 NetScaler Gateway 连接和日志，另一个人负责配置 NetScaler Gateway 上的特定设置。第一个管理员具有只读访问权限，第二个管理员对设备具有有限访问权限。

要配置委派管理员，您需要使用命令策略以及系统用户和组。

配置委派管理员时，配置过程如下：

- 添加系统用户。系统用户是具有指定权限的管理员。所有管理员都继承其所属组的策略。
- 添加系统组。系统组包含具有特定权限的系统用户。系统组的成员继承其所属组的策略。
- 创建命令策略。命令策略允许您定义用户或组可以访问和修改的 NetScaler Gateway 配置的哪些部分。您还可以规定管理员和组被允许配置哪些命令，例如命令组、虚拟服务器和其他元素。
- 通过设置优先级将命令策略绑定到用户或组。配置委派管理时，为管理员或组分配优先级，以便 NetScaler Gateway 可以确定哪个策略优先。

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

NetScaler Gateway 具有默认的拒绝系统命令策略。命令策略不能全局绑定。将策略直接绑定到系统管理员（用户）或组。如果用户和组没有关联的命令策略，则应用默认拒绝策略，用户将无法运行任何命令或配置 NetScaler Gateway。

您可以配置自定义命令策略，以更详细地定义用户权限分配。例如，您可以授予某人向 NetScaler Gateway 添加会话策略的权限，但不允许该用户执行任何其他配置。

为委派管理员配置命令策略

NetScaler Gateway 有四种内置命令策略，可用于委派管理：

- **只读** 允许只读访问，以显示除系统命令组和 `ns.conf show` 命令之外的所有命令。
- **操作员** 允许只读访问，并允许访问启用和禁用服务上的命令。此策略还允许访问将服务和服务器设置为“访问关闭”。
- **网络** 允许几乎完整的系统访问，但不包括系统命令和 shell 命令。
- **超级用户** 授予完整的系统权限，例如授予默认管理员 `nsroot` 的权限。

命令策略包含内置表达式。使用配置实用程序创建系统用户、系统组、命令策略并定义权限。

在 NetScaler Gateway 上创建管理用户

1. 在配置实用程序中，在导航窗格的“**配置**”选项卡上，展开“**系统**”>“**用户管理**”，然后单击“**系统用户**”。
2. 在详细信息窗格中，单击“**添加**”。
3. 在“**用户名**”中，键入用户名。
4. 在“**密码**”和“**确认密码**”字段中，键入密码。
5. 要将用户添加到组，请在“**所属成员**”中单击“**添加**”。
6. 在“**可用**”中，选择一个组，然后单击右箭头。
7. 单击“**命令策略 > 操作 > 插入**”。
8. 在“插入命令策略”对话框中，选择命令，然后单击 **确定 > 创建 > 关闭**。

创建管理组

管理组包含在 NetScaler Gateway 上具有管理权限的用户。您可以在配置实用程序中创建管理组。

使用配置实用程序配置管理组

1. 在配置实用程序中，在导航窗格的 **配置** 选项卡上，展开 **系统** > **用户管理**，然后单击 **系统组**。
2. 在详细信息窗格中，单击 **添加**。

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

3. 在 **组名** 中，键入组的名称。
4. 要将现有用户添加到组中，请在 **成员** 中单击 **添加**。
5. 在 **可用** 下，选择一个用户，然后单击右箭头。
6. 在 **命令策略** 下，在 **操作** 中，单击 **插入**，选择一个或多个策略，单击 **确定**，单击 **创建**，然后单击 **关闭**。

为委派管理员配置自定义命令策略

配置自定义命令策略时，您需要提供策略名称，然后配置策略组件以创建命令规范。通过命令规范，您可以限制管理员可以使用的命令。例如，您希望拒绝管理员使用 remove 命令。配置策略时，将操作设置为拒绝，然后配置参数。

您可以配置简单或高级命令策略。配置简单策略时，您可以在设备上配置一个组件，例如 NetScaler Gateway 和身份验证。配置高级策略时，您选择一个称为实体组的组件，然后选择管理员可以在该组中执行的命令。

创建简单自定义命令策略

1. 在配置实用程序中，在“**配置**”选项卡上的导航窗格中，展开“**系统**”>“**用户管理**”，然后单击“**命令策略**”。
2. 在详细信息窗格中，单击“**添加**”。
3. 在“**策略名称**”中，键入策略的名称。
4. 在“**操作**”中，选择“**允许**”或“**拒绝**”。
5. 在“**命令规范**”下，单击“**添加**”。
6. 在“**添加命令**”对话框中，在“**简单**”选项卡上的“操作”中，选择委派管理员可以执行的操作。
7. 在“**实体组**”下，选择一个或多个组。

   您可以按住 Ctrl 键选择多个组。
8. 单击“**创建**”，然后单击“**关闭**”。

创建高级自定义命令策略

1. 在配置实用程序中，在导航窗格的“**配置**”选项卡上，展开“**系统**”>“**用户管理**”，然后单击“**命令策略**”。
2. 在详细信息窗格中，单击 **添加**。
3. 在 **策略名称** 中，键入策略的名称。
4. 在 **操作** 中，选择 **允许** 或 **拒绝**。

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

5. 在 **命令规范** 下，单击 **添加**。
6. 在 **添加命令** 对话框中，单击 **高级** 选项卡。
7. 在 **实体组** 中，选择命令所属的组，例如身份验证或高可用性。
8. 在 **实体** 下，选择策略。

   您可以按 CTRL 键选择列表中的多个项目。
9. 在 **操作** 中，选择命令，单击 **创建**，然后单击 **关闭**。

   您可以按 CTRL 键选择列表中的多个项目。
10. 单击 **创建**，然后单击 **关闭**。
11. 在 **创建命令策略** 对话框中，单击 **创建**，然后单击 **关闭**。

单击 **创建** 后，表达式将显示在 **创建命令策略** 对话框中的“命令规范”下。

创建自定义命令策略后，可以将其绑定到用户或组。

注意： 您只能将自定义命令策略绑定到您创建的用户或组。您不能将自定义命令策略绑定到用户 `nsroot`。

将自定义命令策略绑定到用户或组

1. 在配置实用程序中，在“**配置**”选项卡上的导航窗格中，展开“**系统**”>“**用户管理**”，然后单击“**系统用户**”或单击“**系统组**”。
2. 在详细信息窗格中，从列表中选择一个用户或组，然后单击“**打开**”。
3. 在“**命令策略**”下，选择策略，然后单击“**确定**”。

在 NetScaler Gateway 上配置审计

NetScaler Gateway 允许您记录设备收集的状态和状态信息。您可以使用审计日志按时间顺序查看事件历史记录。日志中的消息包含有关生成消息的事件、时间戳、消息类型以及预定义的日志级别和消息信息。您可以配置设置来确定要记录的信息以及消息的存储位置。

NetScaler Gateway 当前支持两种日志格式：用于本地日志的专有日志格式，以及用于 syslog 服务器的 syslog 格式。您可以配置审计日志以提供以下信息：

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

级别	描述
紧急	仅记录主要错误。日志中的条目表示 NetScaler Gateway 正在经历导致其无法使用的严重问题。
警报	记录可能导致 NetScaler Gateway 无法正常运行但对其操作并非关键的问题。可以尽快采取纠正措施，以防止 NetScaler Gateway 出现严重问题。
严重	记录不限制 NetScaler Gateway 运行但可能升级为更大问题的严重情况。
错误	记录 NetScaler Gateway 上操作失败导致的条目。
警告	记录可能导致错误或严重错误的潜在问题。
通知	记录比信息级别日志更深入的问题，但其目的与通知相同。
信息	记录 NetScaler Gateway 执行的操作。此级别有助于排查问题。

如果您配置了 TCP 压缩，NetScaler Gateway 审计日志还会存储 NetScaler Gateway 的压缩统计信息。针对不同数据实现的压缩比存储在每个用户会话的日志文件中。

NetScaler Gateway 使用日志签名 SessionID。这允许您按会话而不是按用户跟踪日志。作为会话一部分生成的日志具有相同的 SessionID。如果用户从具有相同 IP 地址的同一用户设备建立两个会话，则每个会话都有一个唯一的 SessionID。

重要提示：

如果您编写了自定义日志解析脚本，则需要在自定义解析脚本中进行此签名更改。

在 NetScaler Gateway 上配置日志

在 NetScaler Gateway 上配置日志记录时，您可以选择将审计日志存储在 NetScaler Gateway 上，或将其发送到 syslog 服务器。您可以使用配置实用程序创建审计策略并配置设置以存储审计日志。

创建审计策略

1. 在配置实用程序中，在“配置”选项卡上，展开 **NetScaler Gateway** > **策略** > **审计**。

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

2. 在“**名称**”中，键入策略的名称。
3. 选择以下选项之一：
   - 如果要将日志发送到 Syslog 服务器，请选择 Syslog。
   - `Nslog` 将日志存储在 NetScaler Gateway 上。

     注意：
     如果选择此选项，日志将存储在设备的 /var/log 文件夹中。
4. 在详细信息窗格中，单击“**添加**”。
5. 键入以下服务器信息，其中存储日志：
   - 在“名称”中，键入服务器的名称。
   - 在“服务器”下，键入日志服务器的名称或 IP 地址。
6. 单击“创建”，然后单击“关闭”。

创建审计策略后，您可以将策略绑定到以下任意组合：

- 全局
- 虚拟服务器
- 组
- 用户

全局绑定审计策略

1. 在配置实用程序中，在“配置”选项卡上，展开 **NetScaler Gateway** > **策略** > **审计**。
2. 选择 `Syslog` 或 `Nslog`。
3. 在详细信息窗格中，单击“**操作**”，然后单击“**全局绑定**”。
4. 在“**绑定/取消绑定审计策略**”到“**全局**”对话框中，在“**详细信息**”下，单击“**插入策略**”。
5. 在“**策略名称**”下，选择一个策略，然后单击“**确定**”。

修改审计策略

您可以修改现有审计策略，以更改发送日志的服务器。

1. 在配置实用程序中，在“**配置**”选项卡上，展开 **NetScaler Gateway** > **策略** > **审计**
2. 选择 `Syslog` 或 `Nslog`。
3. 在详细信息窗格中，单击一个策略，然后单击“**打开**”。

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

4. 在服务器中，选择新服务器，然后单击“**确定**”。

删除审计策略

您可以从 NetScaler Gateway 中删除审计策略。删除审计策略后，该策略将自动解除绑定。

1. 在配置实用程序中，在“配置”选项卡上，展开“**NetScaler Gateway**”>“**策略**”>“**审计**”。
2. 选择“**Syslog**”或“`Nslog`”。
3. 在详细信息窗格中，单击一个策略，然后单击“**删除**”。

配置 ACL 日志记录

您可以将 NetScaler Gateway 配置为记录与扩展访问控制列表 (ACL) 匹配的数据包的详细信息。除了 ACL 名称之外，记录的详细信息还包括数据包特有的信息，例如源 IP 地址和目标 IP 地址。根据您启用的日志记录类型（syslog 或 `nslog`），信息存储在 syslog 或 `nslog` 文件中。

您可以在全局级别和 ACL 级别启用日志记录。但是，要在 ACL 级别启用日志记录，您还必须在全局级别启用它。全局设置优先。

为了优化日志记录，当来自同一流的多个数据包与 ACL 匹配时，仅记录第一个数据包的详细信息。对于属于同一流的每个其他数据包，计数器都会递增。流定义为一组具有以下参数相同值的数据包：

- 源 IP
- 目标 IP
- 源端口
- 目标端口
- 协议（TCP 或 UDP）

如果数据包不属于同一流，或者时间持续时间超出平均时间，则会创建一个新流。平均时间是指同一流的数据包不生成额外消息（尽管计数器会递增）的时间。

注意：在任何给定时间可以记录的不同流的总数限制为 10,000。

下表描述了可用于在规则级别为扩展 ACL 配置 ACL 日志记录的参数。

参数名称	描述
`Logstate`	ACL的日志记录功能的状体。可能的值：ENABLED和DISABLED。默认值：DISABLED。

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

参数名称	描述
`Ratelimit`	特定ACL可以生成的日志消息数量。默认值：100。

使用配置实用程序配置ACL日志记录

您可以为ACL配置日志记录，并指定该规则可以生成的日志消息数量。

1. 在配置实用程序中，在导航窗格中，展开 **系统** > **网络**，然后单击ACL。
2. 在详细信息窗格中，单击 **扩展ACL** 选项卡，然后单击添加。
3. 在 **创建扩展ACL** 对话框中，在名称中，键入策略的名称。
4. 选中 **日志状态** 复选框。
5. 在 **日志速率限制** 文本框中，键入要为规则指定的速率限制，然后单击 **创建**。

配置ACL日志记录后，您可以在NetScaler Gateway上启用它。创建审计策略，然后将其绑定到用户、组、虚拟服务器或全局。

在NetScaler Gateway上启用ACL或TCP日志记录

1. 在配置实用程序中，在导航窗格中，展开 **NetScaler Gateway** > **策略** > **审计**。
2. 选择syslog或 `nslog`。
3. 在 **服务器** 选项卡上，单击 **添加**。
4. 在“**创建审计服务器**”对话框中，在“**名称**”中，键入服务器的名称，然后配置服务器设置。
5. 单击“**ACL 日志记录**”或“**TCP 日志记录**”，然后单击“**创建**”。

启用 Citrix Secure Access™ 日志记录

您可以配置 Citrix Secure Access 客户端，将所有错误记录到存储在用户设备上的文本文件。用户可以配置 Citrix Secure Access 客户端，设置用户设备上的日志记录级别以记录特定的用户活动。当用户配置日志记录时，插件会在用户设备上创建以下两个文件：

- hooklog\<num\>.txt，它记录 Citrix Secure Access 客户端生成的拦截消息。
- nssslvpn.txt，它列出了插件的错误。

> **注意：**
> hooklog.txt 文件不会自动删除。Citrix 建议定期删除这些文件。

用户日志位于用户设备上的 Windows 中的以下目录中：

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

- Windows XP (所有用户): %SystemDrive%:\\Documents and Settings\\All Users\\Application Data\\Citrix\\AGEE
- Windows XP (用户特定): %SystemDrive%:\\Documents and Settings\\%username%\\Local Settings\\Application Data\\Citrix\\AGEE
- 视窗 Vista（所有用户）：%SystemDrive%:\ProgramData\Citrix\AGEE
- 视窗 Vista（特定用户）：%SystemDrive%:\Users\%username%\AppData\Local\Citrix\AGEE
- Windows 7（所有用户）: %SystemDrive%:\\ProgramData\\Citrix\\AGEE
- Windows 7（特定用户）: %SystemDrive%:\\Users\\%username%\\AppData\\Local\\Citrix\\AGEE
- Windows 8（所有用户）：%SystemDrive%:\\ProgramData\\Citrix\\AGEE
- Windows 8（特定用户）：%SystemDrive%:\\Users\\%username%\\AppData\\Local\\Citrix\\AGEE

您可以使用这些日志文件来排查 Citrix Secure Access 客户端的问题。用户可以将日志文件通过电子邮件发送给技术支持。

在“配置”对话框中，用户可以设置适用于 Citrix Secure Access 客户端的日志记录级别。日志记录级别包括：

- 记录错误消息
- 记录事件消息
- 记录 Citrix Secure Access 客户端统计信息
- 记录所有错误、事件消息和统计信息

有关适用于 Windows 的 Citrix Secure Access 客户端的日志记录功能的更多详细信息，请参阅 Improved log collection for Windows client。

监控 ICA® 连接

您可以使用“**ICA 连接**”对话框监控服务器场上的活动用户会话。此对话框提供以下信息：

- 连接到服务器场的人员的用户名
- 服务器场的域名
- 用户设备的 IP 地址
- 用户设备的端口号
- 运行 Citrix Virtual Apps and Desktops 的服务器的 IP 地址

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

- 运行 Citrix Virtual Apps and Desktops 的服务器的端口号

1. 导航到“**配置 > NetScaler Gateway**”。
2. 在“**监控连接**”部分中，单击“**ICA 连接**”。

ICA 会话日志

`ns.log` 文件以以下格式打印 ICA 会话日志：

```
May  2 09:29:02 <local0.info> 10.106.40.223  05/02/2023:09:29:02 GMT  0-
PPE-1 : default ICA Message 141327 0 :  "[Remote ip = 10.10.99.86:514]
[EDT] [CGP][ICAUUID=0006ab3454-d7de-1450-9678-c6333447a76] Received
response from STA server {sta-server=10.11.40.222:80,type=ResponseData}"
```

从版本 13.1 build 50.x 开始，ICA 日志进行了以下增强：

- 显示连接类型，例如 TCP、EDT、CGP 和 SOCKS。
- 显示 ICA 全局唯一标识符 (UUID)。
- 所有 STA 日志都显示为信息级别日志。

通过 Citrix 事务 ID 集成增强 ICA 会话监控

从 NetScaler Gateway 14.1 版本 build 60.x 开始，Citrix 事务 ID 直接集成到 NetScaler Gateway 的 ICA 进程中。此集成确保在 NetScaler Gateway、Citrix Workspace 应用程序和虚拟投递代理 (VDA) 的 ICA 日志中，使用一致的 ICA UUID。以前，NetScaler Gateway 上缺少事务 ID 会导致在 NetScaler Gateway、Citrix Workspace 应用程序和 VDA 环境中进行端到端 ICA 会话监控时出现关联问题。

将 Citrix 事务 ID 集成到 ICA 进程中具有以下优势：

- **简化监控**：实现 ICA 会话的全面、一致的端到端监控。
- **更快的问题解决**：通过提供一致的 ICA UUID，有助于更快地识别和解决问题。此增强功能可减少管理员和支持团队的故障排除时间。

NetScaler Gateway 与 AoT 日志服务器的集成

从 NetScaler Gateway 14.1 版本 build 60.x 开始，NetScaler Gateway 与 Always-on Tracing (AoT) 日志服务器已集成。这使得 NetScaler Gateway 能够将详细的日志流转发到 AoT 日志服务器，从而增强监控和故障排除能力。有关将 AoT 日志服务器部署并与本地 NetScaler Gateway 集成的更多信息，请参阅将审核日志导出到 HEC 端点。

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

限制

- NetScaler Gateway 将整个系统日志发送到 AoT 日志服务器，因为 `syslogAction` 是全局绑定的。

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

身份验证和授权

NetScaler Gateway 采用灵活的身份验证设计，允许对 NetScaler Gateway 的用户身份验证进行广泛自定义。您可以使用行业标准的身份验证服务器，并配置 NetScaler Gateway 以使用这些服务器对用户进行身份验证。NetScaler Gateway 还支持基于客户端证书中存在的属性进行身份验证。NetScaler Gateway 身份验证旨在适应使用单一来源进行用户身份验证的简单身份验证过程，以及依赖多种身份验证类型的更复杂的级联身份验证过程。

NetScaler Gateway 身份验证包含用于创建本地用户和组的本地身份验证。此设计以使用策略来控制您配置的身份验证过程为中心。您创建的策略可以应用于 NetScaler Gateway 全局或虚拟服务器级别，并可用于根据用户的源网络有条件地设置身份验证服务器参数。

由于策略是全局绑定或绑定到虚拟服务器的，因此您还可以为策略分配优先级，以创建多个身份验证服务器的级联作为身份验证的一部分。

NetScaler Gateway 支持以下身份验证类型。

- 本地
- 轻量级目录访问协议 (LDAP)
- RADIUS
- SAML
- TACACS+
- 客户端证书身份验证（包括智能卡身份验证）

NetScaler Gateway 还支持 RSA SecurID、Gemalto Protiva 和 SafeWord。您可以使用 RADIUS 服务器来配置这些类型的身份验证。

身份验证允许用户登录 NetScaler Gateway 并连接到内部网络，而授权则定义了用户可以访问的安全网络中的资源。您可以使用 LDAP 和 RADIUS 策略配置授权。

配置默认全局身份验证类型

当您安装 NetScaler Gateway 并运行 NetScaler Gateway 向导时，您在向导中配置了身份验证。此身份验证策略会自动绑定到 NetScaler Gateway 全局级别。您在 NetScaler Gateway 向导中配置的身份验证类型是默认身份验证类型。您可以通过再次运行 NetScaler Gateway 向导来更改默认授权类型，或者可以在配置实用程序中修改全局身份验证设置。

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

如果您需要添加其他身份验证类型，可以在 NetScaler Gateway 上配置身份验证策略，并使用配置实用程序将策略绑定到 NetScaler Gateway。当您全局配置身份验证时，您需要定义身份验证类型、配置设置并设置可进行身份验证的最大用户数。

配置并绑定策略后，您可以设置优先级以定义哪种身份验证类型优先。例如，您配置 LDAP 和 RADIUS 身份验证策略。如果 LDAP 策略的优先级为 10，RADIUS 策略的优先级为 15，则无论您将每个策略绑定到何处，LDAP 策略都将优先。这称为级联身份验证。

您可以选择从 NetScaler Gateway 内存缓存或从 NetScaler Gateway 上运行的 HTTP 服务器交付登录页面。如果您选择从内存缓存交付登录页面，则 NetScaler Gateway 交付登录页面的速度将比从 HTTP 服务器交付快得多。选择从内存缓存交付登录页面可以减少大量用户同时登录时的等待时间。您只能将从缓存交付登录页面配置为全局身份验证策略的一部分。

您还可以配置网络地址转换 (NAT) IP 地址，该地址是用于身份验证的特定 IP 地址。此 IP 地址对于身份验证是唯一的，而不是 NetScaler Gateway 子网、映射或虚拟 IP 地址。这是一个可选设置。

注意：您不能使用 NetScaler Gateway 向导来配置 SAML 身份验证。

您可以使用快速配置向导来配置 LDAP、RADIUS 和客户端证书身份验证。运行向导时，您可以从 NetScaler Gateway 上配置的现有 LDAP 或 RADIUS 服务器中进行选择。您还可以配置 LDAP 或 RADIUS 的设置。如果您使用双因素身份验证，Citrix 建议使用 LDAP 作为主要身份验证类型。

全局配置身份验证

1. 在配置实用程序中，在“配置”选项卡上的导航窗格中，展开 NetScaler Gateway，然后单击“全局设置”。
2. 在详细信息窗格中，在“设置”下，单击“更改身份验证设置”。
3. 在“最大用户数”中，键入可以使用此身份验证类型进行身份验证的用户数。
4. 在“NAT IP 地址”中，键入用于身份验证的唯一 IP 地址。
5. 选择“启用静态缓存”以更快地交付登录页面。
6. 选择“启用增强身份验证反馈”以在身份验证失败时向用户提供消息。用户收到的消息包括密码错误、帐户被禁用或锁定，或者找不到用户等。
7. 在“默认身份验证类型”中，选择身份验证类型。
8. 配置身份验证类型的设置，然后单击“确定”。

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

配置不带授权的身份验证

授权定义了用户可以通过 NetScaler Gateway 连接的资源。您可以通过使用表达式配置授权策略，然后将策略设置为允许或拒绝。您可以将 NetScaler Gateway 配置为仅使用身份验证，而不使用授权。

当您配置不带授权的身份验证时，NetScaler Gateway 不执行组授权检查。您为用户或组配置的策略将分配给该用户。

有关配置授权的更多信息，请参阅 配置授权。

配置授权

授权指定了用户登录到 NetScaler Gateway 时可以访问的网络资源。授权的默认设置是拒绝访问所有网络资源。Citrix 建议使用默认全局设置，然后创建授权策略来定义用户可以访问的网络资源。

您可以通过使用授权策略和表达式在 NetScaler Gateway 上配置授权。创建授权策略后，您可以将其绑定到您在设备上配置的用户或组。

配置授权策略

配置授权策略时，可以将其设置为允许或拒绝访问内部网络中的网络资源。例如，要允许用户访问 10.3.3.0 网络，请使用以下表达式：

CLIENT.IP.DST.IN_SUBNET(10.3.0.0/16)

授权策略应用于用户和组。用户通过身份验证后，NetScaler Gateway 通过从 RADIUS、LDAP 或 TACACS+ 服务器获取用户的组信息来执行组授权检查。如果用户有可用的组信息，NetScaler Gateway 会检查该组允许的网络资源。

要控制用户可以访问的资源，必须创建授权策略。如果不需要创建授权策略，可以配置默认的全局授权。

如果在授权策略中创建拒绝访问文件路径的表达式，则只能使用子目录路径，而不能使用根目录。例如，使用 fs.path contains "\\\\dir1\\\\dir2" 而不是 fs.path contains "\\\\rootdir\\\\dir1\\\\dir2"。如果在此示例中使用第二种版本，则策略将失败。

配置授权策略后，您可以将其绑定到用户或组，如下面的任务所示。

默认情况下，授权策略首先根据您绑定到虚拟服务器的策略进行验证，然后根据全局绑定的策略进行验证。如果您全局绑定策略，并希望全局策略优先于绑定到用户、组或虚拟服务器的策略，则可以更改策略的优先级编号。优先级编号从零开始。优先级编号越低，策略的优先级越高。

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

例如，如果全局策略的优先级编号为 1，用户的优先级为 2，则首先应用全局身份验证策略。

重要提示：

- 经典授权策略仅应用于 TCP 流量。
- 高级授权策略可应用于所有类型的流量（TCP/UDP/ICMP/DNS）。
  - 要将策略应用于 UDP/ICMP/DNS 流量，必须分别将策略绑定到 UDP_REQUEST、ICMP_REQUEST 和 DNS_REQUEST 类型。
  - 绑定时，如果未明确提及“type”或将“type”设置为 REQUEST，则行为与早期版本没有变化，即这些策略仅应用于 TCP 流量。
  - 绑定到 UDP_REQUEST 的策略不适用于 DNS 流量。对于 DNS，策略必须明确绑定到 DNS_REQUEST。TCP_DNS 类似于其他 TCP 请求。

有关高级授权策略的更多详细信息，请参阅文章 `<https://support.citrix.com/article/CTX232237>`。

授权策略表达式示例

以下是授权策略的表达式示例：

- `add authorization policy athzPol1 "HTTP.REQ.USER.IS_MEMBER_OF(\"allowedGroup\")" ALLOW`
- `add authorization policy athzPol2 "CLIENT.IP.DST.BETWEEN(192.0.2.10,192.0.2.20)" DENY`
- `add authorization policy athzPol3 "HTTP.REQ.HOSTNAME.CONTAINS(\"portal-srv") || CLIENT.IP.DST.IN_SUBNET(192.0.2.0/25)" ALLOW`

使用 GUI 配置授权策略

1. 导航到 **NetScaler Gateway > 策略 > 授权。**
2. 在详细信息窗格中，单击“**添加**”。
3. 在“**名称**”中，键入策略的名称。
4. 在“**操作**”中，选择“**允许**”或“**拒绝**”。
5. 在“**表达式**”中，单击“**表达式编辑器**”。
6. 要开始配置表达式，请单击“**选择**”并选择必要的元素。

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

7. 表达式完成后，单击“**完成**”。
8. 单击“**创建**”。

使用 GUI 将授权策略绑定到用户

1. 导航到 **NetScaler Gateway > 用户管理**。
2. 单击 **AAA 用户**。
3. 在详细信息窗格中，选择一个用户，然后单击 **编辑**。
4. 在 **高级设置** 中，单击 **授权策略**。
5. 在 **策略绑定** 页面中，选择一个策略或创建一个策略。
6. 在 **优先级** 中，设置优先级编号。
7. 在 **类型** 中，选择请求类型，然后单击 **确定**。

使用 GUI 将授权策略绑定到组

1. 导航到 **NetScaler Gateway > 用户管理**。
2. 单击 **AAA 组**。
3. 在详细信息窗格中，选择一个组，然后单击 **编辑**。
4. 在 **高级设置** 中，单击 **授权策略**。
5. 在 **策略绑定** 页面中，选择一个策略或创建一个策略。
6. 在 **优先级** 中，设置优先级编号。
7. 在 **类型** 中，选择请求类型，然后单击 **确定**。

设置默认全局授权

为了定义用户在内部网络上可以访问的资源，您可以配置默认全局授权。您可以通过允许或拒绝全局访问内部网络上的网络资源来配置全局授权。

您创建的任何全局授权操作都将应用于所有尚未直接或通过组关联授权策略的用户。用户或组授权策略始终会覆盖全局授权操作。如果默认授权操作设置为“拒绝”，则必须为所有用户或组应用授权策略，才能使这些用户或组能够访问网络资源。此要求有助于提高安全性。

要设置默认全局授权：

1. 在配置实用程序中，在“配置”选项卡上，在导航窗格中，展开 NetScaler Gateway，然后单击“全局设置”。
2. 在详细信息窗格中，在“设置”下，单击“更改全局设置”。

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

3. 在“安全”选项卡上，在“默认授权操作”旁边，选择“允许”或“拒绝”，然后单击“确定”。

禁用身份验证

如果您的部署不需要身份验证，则可以禁用它。您可以为每个不需要身份验证的虚拟服务器禁用身份验证。

重要提示：

Citrix 建议谨慎禁用身份验证。如果您不使用外部身份验证服务器，请创建本地用户和组以允许 NetScaler Gateway 验证用户。禁用身份验证会停止使用控制和监视 NetScaler Gateway 连接的身份验证、授权和记帐功能。当用户键入 Web 地址连接到 NetScaler Gateway 时，不会显示登录页面。

禁用身份验证

1. 在配置实用程序中，在导航窗格中，展开 NetScaler Gateway，然后单击“虚拟服务器”。
2. 在详细信息窗格中，单击一个虚拟服务器，然后单击“打开”。
3. 在“身份验证”选项卡上的“用户身份验证”下，单击以清除“启用身份验证”。

配置特定时间的身份验证

您可以配置身份验证策略，以便用户在特定时间（例如正常工作时间）访问内部网络。当用户在其他时间尝试登录时，登录将被拒绝。

要限制用户登录 NetScaler Gateway 的时间，请在身份验证策略中创建表达式，然后将其绑定到虚拟服务器或全局绑定。

配置时间、日期或星期几的身份验证

1. 在配置实用程序中，在“配置”选项卡上，展开 NetScaler Gateway \> 策略 \> 身份验证。
2. 在“身份验证”下，选择身份验证类型。
3. 在详细信息窗格中，单击“策略”选项卡，选择一个身份验证策略，然后单击“打开”。
4. 在“配置身份验证策略”对话框中，在“表达式”下，在“匹配任意表达式”旁边，单击“添加”。
5. 在“添加表达式”对话框中，在“表达式类型”中，选择“日期/时间”。
6. 在“限定符”中，选择以下选项之一：
   - TIME 用于配置用户无法登录的时间。

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

- DATE 用于配置用户无法登录的日期。
- DAYOFWEEK 用于配置用户无法登录的星期几。

示例：TIME: 2020-10-12-02:30:00GMT DATE: 2020-10-12 DAYOFWEEK: Monday

7. 在“运算符”中，选择值。
8. 在“值”中，单击文本框旁边的日历，然后选择星期几、日期或时间。
9. 单击两次“确定”，单击“关闭”，然后单击“确定”。

身份验证策略的工作原理

当用户登录到 NetScaler Gateway 时，他们会根据您创建的策略进行身份验证。该策略定义了身份验证类型。单个身份验证策略可用于简单的身份验证需求，并且通常绑定到全局级别。您还可以使用默认身份验证类型，即本地身份验证。如果您配置本地身份验证，则还必须在 NetScaler Gateway 上配置用户和组。

您可以配置多个身份验证策略并将其绑定，以创建详细的身份验证过程和虚拟服务器。例如，您可以通过配置多个策略来配置级联和双因素身份验证。您还可以设置身份验证策略的优先级，以确定 NetScaler Gateway 检查用户凭据的服务器以及顺序。身份验证策略包括表达式和操作。例如，如果您将表达式设置为 True 值，当用户登录时，操作会将用户登录评估为 true，然后用户就可以访问网络资源。

创建身份验证策略后，您可以将策略绑定到全局级别或虚拟服务器。当您将至少一个身份验证策略绑定到虚拟服务器时，用户登录到虚拟服务器时，您绑定到全局级别的任何身份验证策略都不会被使用，除非全局身份验证类型具有比绑定到虚拟服务器的策略更高的优先级。

当用户登录到 NetScaler Gateway 时，身份验证按以下顺序进行评估：

- 检查虚拟服务器是否有任何绑定的身份验证策略。
- 如果身份验证策略未绑定到虚拟服务器，NetScaler Gateway 将检查全局身份验证策略。
- 如果身份验证策略未绑定到虚拟服务器或全局，则用户通过默认身份验证类型进行身份验证。

如果您配置 LDAP 和 RADIUS 身份验证策略并希望将这些策略全局绑定以进行双因素身份验证，您可以在配置实用程序中选择该策略，然后选择该策略是主要还是次要身份验证类型。您还可以配置组提取策略。

配置身份验证配置文件

您可以使用 NetScaler Gateway 向导或配置实用程序创建身份验证配置文件。该配置文件包含身份验证策略的所有设置。您在创建身份验证策略时配置该配置文件。

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

使用 NetScaler Gateway 向导，您可以使用所选的身份验证类型来配置身份验证。如果您想在运行向导后配置其他身份验证策略，可以使用配置实用程序。有关 NetScaler Gateway 向导的更多信息，请参阅 使用 NetScaler Gateway 向导配置设置。

使用配置实用程序创建身份验证策略

1. 在配置实用程序中，在“Configuration”（配置）选项卡上，展开 NetScaler Gateway \> Policies \> Authentication（策略 \> 身份验证）。
2. 在导航窗格中，在“Authentication”（身份验证）下，选择一种身份验证类型。
3. 在详细信息窗格中，在“Policies”（策略）选项卡上，单击“Add”（添加）。
4. 如果您使用的是外部身份验证类型，请在“Server”（服务器）旁边，单击“New”（新建）。
5. 在“Create Authentication Server”（创建身份验证服务器）对话框中，配置您的身份验证类型的设置，单击“Create”（创建），然后单击“Close”（关闭）。
6. 在“Create Authentication Policy”（创建身份验证策略）对话框中，在“Named Expressions”（命名表达式）旁边，选择“True value”（真值），单击“Add Expression”（添加表达式），单击“Create”（创建），然后单击“Close”（关闭）。 注意：当您选择身份验证类型并保存身份验证配置文件后，您无法更改身份验证类型。要使用不同的身份验证类型，您必须创建新策略。

使用配置实用程序修改身份验证策略

您可以修改已配置的身份验证策略和配置文件，例如身份验证服务器的 IP 地址或表达式。

1. 在配置实用程序中，在“Configuration”（配置）选项卡上，展开 NetScaler Gateway \> Policies \> Authentication（策略 \> 身份验证）。
2. 在导航窗格中，在“Authentication”（身份验证）下，选择一种身份验证类型。
3. 在详细信息窗格中，在“Servers”（服务器）选项卡上，选择一个服务器，然后单击“Open”（打开）。

删除身份验证策略

如果您更改或从网络中删除了身份验证服务器，请从 NetScaler Gateway 中删除相应的身份验证策略。

1. 在配置实用程序中，在“配置”选项卡上，展开 NetScaler Gateway \> 策略 \> 身份验证。
2. 在导航窗格中，在“身份验证”下，选择身份验证类型。
3. 在详细信息窗格中，在“策略”选项卡上，选择一个策略，然后单击“删除”。

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

绑定身份验证策略

配置身份验证策略后，您可以将策略全局绑定或绑定到虚拟服务器。您可以使用配置实用程序来绑定身份验证策略。

使用 GUI 全局绑定身份验证策略

1. 在配置实用程序中，在“配置”选项卡上，展开 **NetScaler Gateway > 策略 > 身份验证**。
2. 单击身份验证类型。
3. 在详细信息窗格中，在“**策略**”选项卡上，单击服务器，然后在“**操作**”中，单击“**全局绑定**”。
4. 在“**主或辅助**”选项卡上，在“**详细信息**”下，单击“**插入策略**”。
5. 在“**策略名称**”下，选择策略，然后单击“**确定**”。

   注意： 选择策略后，NetScaler Gateway 会自动将表达式设置为 True 值。

使用 GUI 解除绑定全局身份验证策略

1. 在配置实用程序中，在“配置”选项卡上，展开 **NetScaler Gateway > 策略 > 身份验证**。
2. 在“**策略**”选项卡上，在“**操作**”中，单击“**全局绑定**”。
3. 在“**将身份验证策略绑定/解除绑定到全局**”对话框中，在“**主或辅助**”选项卡上，在“**策略名称**”中，选择策略，单击“**解除绑定策略**”，然后单击“**确定**”。

设置身份验证策略的优先级

默认情况下，身份验证策略首先根据您绑定到虚拟服务器的策略进行验证，然后根据全局绑定的策略进行验证。如果您全局绑定了一个身份验证策略，并希望该全局策略优先于您绑定到虚拟服务器的策略，您可以更改该策略的优先级编号。优先级编号从零开始。较低的优先级编号赋予身份验证策略更高的优先级。

例如，如果全局策略的优先级编号为一，而虚拟服务器的优先级为二，则全局身份验证策略将首先应用。

设置或更改全局身份验证策略的优先级

1. 在配置实用程序中，在“配置”选项卡上，展开 NetScaler Gateway \> 策略 \> 身份验证。
2. 在“策略”选项卡上的“操作”中，单击“全局绑定”。
3. 在“绑定/解除绑定身份验证全局策略”对话框中，在“主要”或“次要”选项卡上，在“优先级”下，键入数字，然后单击“确定”。

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

更改绑定到虚拟服务器的身份验证策略的优先级

您还可以修改绑定到虚拟服务器的身份验证策略。

1. 在配置实用程序中，在“配置”选项卡上的导航窗格中，展开 NetScaler Gateway，然后单击“虚拟服务器”。
2. 选择一个虚拟服务器，然后单击“打开”。
3. 单击“身份验证”选项卡，然后选择“主要”或“次要”。
4. 选择策略，然后在“优先级”中，键入优先级编号，然后单击“确定”。

配置本地用户

您可以在 NetScaler Gateway 上本地创建用户帐户，以补充身份验证服务器上的用户。例如，您可能希望为临时用户（如顾问或访客）创建本地用户帐户，而无需在身份验证服务器上为这些用户创建条目。

如果您正在使用本地身份验证，请创建用户，然后将其添加到您在 NetScaler Gateway 上创建的组中。配置用户和组后，您可以应用授权和会话策略、创建书签、指定应用程序，并指定用户有权访问的文件共享和服务器的 IP 地址。

创建本地用户

1. 在配置实用程序中，单击“**配置**”选项卡，然后在导航窗格中展开“**NetScaler Gateway > 用户管理**”，然后单击“**AAA 用户**”。
2. 在详细信息窗格中，单击“**添加**”。
3. 在“**用户名**”中，键入用户名。
4. 如果您正在使用本地身份验证，请清除“**外部身份验证**”。 **注意**：选择“**外部身份验证**”以让用户针对外部身份验证服务器（如 LDAP 或 RADIUS）进行身份验证。清除此复选框以让 NetScaler Gateway 针对本地用户数据库进行身份验证。
5. 在“**密码**”和“**确认密码**”中，键入用户的密码，单击“**创建**”，然后单击“**关闭**”。

更改用户密码

创建本地用户后，您可以更改用户的密码或将用户帐户配置为针对外部身份验证服务器进行身份验证。

1. 在配置实用程序中，单击“**配置**”选项卡，然后在导航窗格中展开“**NetScaler Gateway > 用户管理**”，然后单击“**AAA 用户**”。
2. 在详细信息窗格中，选择一个用户，然后单击“**打开**”。

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

3. 在“**密码**”和“**确认密码**”中，键入用户的新密码，然后单击“**确定**”。

更改用户的身份验证方法

如果您有配置为本地身份验证的用户，您可以将身份验证更改为外部身份验证服务器。为此，请启用外部身份验证。

1. 在配置实用程序中，单击“**配置**”选项卡，然后在导航窗格中展开“**NetScaler Gateway > 用户管理**”，然后单击“**AAA 用户**”。
2. 在详细信息窗格中，选择一个用户，然后单击“**打开**”。
3. 选择“**外部身份验证**”，然后单击“**确定**”。

删除用户

您还可以从 NetScaler Gateway 中删除用户。

1. 在配置实用程序中，单击“**配置**”选项卡，然后在导航窗格中展开“**NetScaler Gateway > 用户管理**”，然后单击“**AAA 用户**”。
2. 在详细信息窗格中，选择一个用户，然后单击“**删除**”。

当您从 NetScaler Gateway 中删除用户时，所有关联的策略也会从用户配置文件中删除。

配置组

您可以在 NetScaler Gateway 上拥有本地组，并可以使用本地身份验证对用户进行身份验证。如果您使用外部服务器进行身份验证，则 NetScaler Gateway 上的组将配置为与内部网络中身份验证服务器上配置的组匹配。当用户登录并进行身份验证时，如果组名与身份验证服务器上的组匹配，则用户将继承 NetScaler Gateway 上该组的设置。

配置组后，您可以应用授权和会话策略、创建书签、指定应用程序以及指定用户有权访问的文件共享和服务器的 IP 地址。

如果您使用本地身份验证，请创建用户并将其添加到 NetScaler Gateway 上配置的组中。然后，用户将继承该组的设置。

重要提示：

如果用户是 Active Directory 组的成员，则 NetScaler Gateway 上的组名必须与 Active Directory 组的名称相同。

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

创建组

1. 在配置实用程序中，单击“**配置**”选项卡，然后在导航窗格中展开“**NetScaler Gateway > 用户管理**”，然后单击“**AAA 组**”。
2. 在详细信息窗格中，单击“**添加**”。
3. 在“**组名**”中，键入组的名称，单击“**创建**”，然后单击“**关闭**”。

删除组

您还可以从 NetScaler Gateway 中删除用户组。

1. 在配置实用程序中，单击“**配置**”选项卡，然后在导航窗格中展开“**NetScaler Gateway > 用户管理**”，然后单击“**AAA 组**”。
2. 在详细信息窗格中，选择组，然后单击“**删除**”。

将用户添加到组

您可以在创建组时或之后将用户添加到组。您可以将用户添加到多个组，以便用户可以继承绑定到这些组的策略和设置。

要将用户添加到组，请执行以下操作：

1. 在配置实用程序中，单击“Configuration”（配置）选项卡，然后在导航窗格中展开 **NetScaler Gateway > User Administration**（NetScaler Gateway > 用户管理），然后单击 **AAA Users**（AAA 用户）。
2. 在详细信息窗格中，选择一个组，然后单击 **Open**（打开）。
3. 在 **Users**（用户）选项卡上的 **Available Users**（可用用户）下，选择用户，单击 **Add**（添加），然后单击 **OK**（确定）。

使用组配置策略

配置组后，您可以使用“组”对话框应用指定用户访问权限的策略和设置。如果您使用本地身份验证，则可以创建用户并将其添加到在 NetScaler Gateway 上配置的组中。然后，用户将继承该组的设置。

您可以在“组”对话框中为用户组配置以下策略或设置：

- 用户
- 授权策略
- 审计策略

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

- 会话策略
- 流量策略
- 书签
- 内网应用程序
- 内网 IP 地址

在您的配置中，用户可能属于多个组。此外，每个组可能有一个或多个绑定的会话策略，并配置了不同的参数。属于多个组的用户将继承分配给用户所属所有组的会话策略。为了确保哪个会话策略评估优先于其他策略，您必须设置会话策略的优先级。

例如，您有一个 group1，它绑定了一个配置了主页 www.homepage1.com 的会话策略。Group2 绑定了一个配置了主页 www.homepage2.com 的会话策略。当这些策略在没有优先级编号或具有相同优先级编号的情况下绑定到各自的组时，属于这两个组的用户显示的主页取决于哪个策略首先处理。通过为配置了主页 www.homepage1.com 的会话策略设置较低的优先级编号（这会赋予更高的优先级），您可以确保属于这两个组的用户收到主页 www.homepage1.com。

如果会话策略没有分配优先级编号或具有相同的优先级编号，则按以下顺序评估优先级：

- 用户
- 组
- 虚拟服务器
- 全局

如果策略绑定到同一级别，没有优先级编号，或者如果策略具有相同的优先级编号，则评估顺序按照策略绑定顺序进行。首先绑定到某个级别的策略优先于稍后绑定的策略。

如果一个用户绑定到多个组，并且每个组都绑定了 IIP，则用户可以从任何绑定的组中获取空闲 IP。

配置 LDAP 身份验证

您可以配置 NetScaler Gateway 以使用一个或多个 LDAP 服务器对用户访问进行身份验证。

LDAP 授权要求 Active Directory、LDAP 服务器和 NetScaler Gateway 上的组名相同。字符和大小写也必须匹配。

默认情况下，LDAP 身份验证通过使用安全套接字层 (SSL) 或传输层安全 (TLS) 来确保安全。有两种类型的安全 LDAP 连接。其中一种类型是，LDAP 服务器在与 LDAP 服务器用于接受明文 LDAP 连接的端口不同的端口上接受 SSL 或 TLS 连接。用户建立 SSL 或 TLS 连接后，LDAP 流量可以通过该连接发送。

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

LDAP 连接的端口号为：

- 389 用于不安全的 LDAP 连接
- 636 用于安全的 LDAP 连接
- 3268 用于 Microsoft 不安全的 LDAP 连接
- 3269 用于 Microsoft 安全的 LDAP 连接

第二种类型的安全 LDAP 连接使用 StartTLS 命令并使用端口号 389。如果您在 NetScaler Gateway 上配置端口号 389 或 3268，服务器会尝试使用 StartTLS 建立连接。如果您使用任何其他端口号，服务器会尝试使用 SSL 或 TLS 建立连接。如果服务器无法使用 StartTLS、SSL 或 TLS，连接将失败。

如果您指定 LDAP 服务器的根目录，NetScaler Gateway 会搜索所有子目录以查找用户属性。在大型目录中，这种方法可能会影响性能。因此，Citrix 建议您使用特定的组织单位 (OU)。

下表包含适用于 LDAP 服务器的用户属性字段的示例：

LDAP 服务器	用户属性	区分大小写
微软活动目录服务器	sAMAccountName	否
诺维尔 e目录	ou	是
IBM 目录服务器	用户 ID	是
莲花 Domino	CN	是
Sun ONE 目录（原 iPlanet）	uid 或 cn	是

此表包含基本 DN 的示例：

LDAP 服务器	基本 DN
微软活动目录服务器	DC=`citrix`,DC=本地
诺维尔 eDirectory	ou=用户,ou=开发
IBM Directory 服务器	cn=用户
莲花 多米诺	OU=城市,O=`Citrix`, C=US
Sun ONE 目录（前身为 iPlanet）	ou=人员,dc=`citrix`,dc=com

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

下表包含绑定 DN 的示例：

LDAP 服务器	绑定 DN
微软活动目录服务器	CN=管理员, CN=用户, DC=`citrix`, DC=local
诺维尔电子目录	cn=管理员, o=`citrix`
IBM 目录服务器	LDAP_dn
莲花 Domino	CN=Notes 管理员, O=`Citrix`, C=US
Sun ONE 目录（原 iPlanet）	uid=admin,ou=管理员, ou=拓扑管理,o=NetscapeRoot

注意：有关 LDAP 服务器设置的更多信息，请参阅 确定 LDAP 目录中的属性。

使用配置实用程序配置 LDAP 身份验证

1. 导航到 **NetScaler Gateway** >**策略** > **身份验证**。
2. 单击 **LDAP**。
3. 在详细信息窗格的“**策略**”选项卡上，单击“**添加**”。
4. 在“**名称**”中，键入策略的名称。
5. 在“**服务器**”旁边，单击“**新建**”。
6. 在“**名称**”中，键入服务器的名称。
7. 在“**服务器**”下，在“**IP 地址和端口**”中，键入 LDAP 服务器的 IP 地址和端口号。
8. 在“**类型**”中，选择 **AD**（表示 Active Directory）或 **NDS**（表示 Novell Directory Services）。
9. 在“**连接设置**”下，完成以下操作：

   a. 在“**基本 DN（用户位置）**”中，键入用户所在的基本 DN。基本 DN 搜索所选目录（AD 或 NDS）下的用户。

   基本 DN 是通过删除用户名并指定用户所在的组从绑定 DN 派生的。基本 DN 语法的示例如下：

   ```
   ou=users,dc=ace,dc=com

   cn=Users,dc=ace,dc=com
   ```

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

b. 在“**管理员绑定 DN**”中，键入用于查询 LDAP 目录的管理员绑定 DN。绑定 DN 语法的示例如下：

```
domain/user name

ou=administrator,dc=ace,dc=com

user@domain.name (for Active Directory)

cn=Administrator,cn=Users,dc=ace,dc=com
```

对于 Active Directory，需要指定为 cn=groupname 的组名。您在 NetScaler Gateway 中定义的组名和 LDAP 服务器上的组名必须相同。

对于其他 LDAP 目录，组名不是必需的，或者如果需要，则指定为 ou=groupname。

NetScaler Gateway 使用管理员凭据绑定到 LDAP 服务器，然后搜索用户。找到用户后，NetScaler Gateway 解除管理员凭据绑定，并使用用户凭据重新绑定。

c. 在 **管理员密码和确认管理员密码** 中，键入 LDAP 服务器的管理员密码。

10. 要自动检索更多 LDAP 设置，请单击 **检索属性**。

    单击 **检索属性** 后，“其他设置”下的字段将自动填充。如果要忽略此步骤，请继续执行步骤 12 和 13。否则，请跳到步骤 14。

11. 在 **其他设置** 下的“服务器登录名属性”中，键入 NetScaler Gateway 必须查找您正在配置的 LDAP 服务器的用户登录名的属性。默认值为 `samAccountName`。

12. 在 **搜索筛选器** 中，键入用于搜索与单个或多个 Active Directory 组关联的用户的值。

    例如，“memberOf=CN=GatewayAccess,OU=Groups,DC=Users,DC=lab”。

    注意

    您可以使用上述示例将 NetScaler Gateway 访问权限限制为仅特定 AD 组的成员。

13. 在 **组属性** 中，保留 Active Directory 的默认 memberOf，或者将属性更改为您正在使用的 LDAP 服务器类型的属性。此属性使 NetScaler Gateway 能够在授权期间获取与用户关联的组。

14. 在 **安全** 类型中，选择安全类型，然后单击 **创建**。

15. 要允许用户更改其 LDAP 密码，请选择 **允许更改密码**。

    注意：

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

- 如果选择 **PLAINTEXT** 作为安全类型，则不支持允许用户更改其密码。
- 如果为安全性选择 **PLAINTEXT** 或 **TLS**，请使用端口号 389。如果选择 **SSL**，请使用端口号 636。

确定 LDAP 目录中的属性

如果您在确定 LDAP 目录属性方面需要帮助，以便在 NetScaler® Gateway 上配置身份验证设置，您可以使用 Softerra 提供的免费 LDAP 浏览器轻松查找它们。

您可以从 Softerra LDAP Administrator 网站 下载 LDAP 浏览器。安装浏览器后，请设置以下属性：

- 您的 LDAP 服务器的主机名或 IP 地址。
- 您的 LDAP 服务器的端口。默认值为 389。
- 基本 DN 字段，您可以将其留空。LDAP 浏览器提供的信息可以帮助您确定需要在 NetScaler Gateway 上配置的基本 DN。
- 匿名绑定检查用于确定 LDAP 服务器是否需要用户凭据才能连接。如果 LDAP 服务器需要凭据，请取消选中该复选框。

完成设置后，LDAP 浏览器会在左侧窗格中显示配置文件名称，并连接到 LDAP 服务器。

配置 LDAP 组提取

如果您正在使用双因素身份验证，从主要和辅助身份验证源提取的组将被连接。授权策略可以应用于从主要或辅助身份验证服务器提取的组。

从 LDAP 服务器获取的组名将与在 NetScaler Gateway 上本地创建的组名进行比较。如果两个组名匹配，则本地组的属性将应用于从 LDAP 服务器获取的组。

如果用户属于多个 LDAP 组，NetScaler Gateway 会从用户所属的所有组中提取用户信息。如果用户是 NetScaler Gateway 上两个组的成员，并且每个组都有一个绑定的会话策略，则用户将继承这两个组的会话策略。为确保用户收到正确的会话策略，请设置会话策略的优先级。

有关 LDAP 组成员属性的更多信息，请参阅以下内容：

- LDAP 组提取如何直接从用户对象工作
- LDAP 组提取如何间接从组对象工作

LDAP 组提取如何直接从用户对象进行工作

从组对象评估组成员资格的 LDAP 服务器支持 NetScaler Gateway 授权。

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

某些 LDAP 服务器允许用户对象包含有关其所属组的信息，例如 Active Directory（通过使用 memberOf 属性）或 IBM eDirectory（通过使用 groupMembership 属性）。用户的组成员资格可以是来自用户对象的属性，例如 IBM Directory Server（通过使用 ibm-allGroups）或 Sun ONE 目录服务器（通过使用 nsRole）。这两种类型的 LDAP 服务器都支持 NetScaler Gateway 组提取。

例如，在 IBM Directory Server 中，所有组成员资格（包括静态、动态和嵌套组）都可以通过使用 ibm-allGroups 属性返回。在 Sun ONE 中，所有角色（包括托管、过滤和嵌套）都通过使用 nsRole 属性计算。

LDAP 组提取如何间接从组对象工作

间接从组对象评估组成员资格的 LDAP 服务器与 NetScaler Gateway 授权不兼容。

某些 LDAP 服务器（例如 Lotus Domino）仅允许组对象包含有关用户的信息。这些 LDAP 服务器不允许用户对象包含有关组的信息，因此与 NetScaler Gateway 组提取不兼容。对于此类 LDAP 服务器，组成员资格搜索是通过在组的成员列表中查找用户来执行的。

LDAP 授权组属性字段

下表包含 LDAP 组属性字段的示例：

LDAP 服务器	LDAP 属性
微软活动目录服务器	memberOf
诺维尔电子目录	groupMembership
IBM 目录服务器	ibm-allGroups
Sun ONE 目录（以前称为 iPlanet）	nsRole

配置 LDAP 授权

您可以通过设置组属性名称和子属性在身份验证策略中配置 LDAP 授权。

1. 在配置实用程序中，在“配置”选项卡上，展开 NetScaler Gateway \> 策略 \> 身份验证。
2. 在“身份验证”下，单击身份验证类型。
3. 在详细信息窗格中，单击“添加”。
4. 在“名称”中，键入策略的名称。
5. 在“服务器”旁边，单击“新建”。
6. 在“名称”中，键入服务器的名称。

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

7. 在“服务器”下，键入 LDAP 服务器的 IP 地址和端口。
8. 在“组属性”中，键入 memberOf。
9. 在“子属性名称”中，键入 CN，然后单击“创建”。
10. 在“创建身份验证策略”对话框中，在“命名表达式”旁边，选择表达式，单击“添加表达式”，单击“创建”，然后单击“关闭”。

配置 LDAP 嵌套组提取

NetScaler Gateway 可以查询 LDAP 组并从您在身份验证服务器上配置的祖先组中提取组和用户信息。例如，您创建了 group1，并在该组中创建了 group2 和 group3。如果用户属于 group3，NetScaler Gateway 将从所有嵌套的祖先组（group2、group1）中提取信息，直到指定的级别。

您可以使用身份验证策略来配置 LDAP 嵌套组提取。运行查询时，NetScaler Gateway 会搜索组，直到达到最大嵌套级别或直到搜索所有可用组。

配置 LDAP 嵌套组提取

1. 在配置实用程序中，在导航窗格中，展开 **NetScaler Gateway > 策略 > 身份验证/授权 > 身份验证 > 身份验证**，然后单击 **LDAP**。
2. 在详细信息窗格中，在“策略”选项卡上，单击 **添加**。
3. 在“名称”中，键入策略的名称。
4. 在“服务器”旁边，单击 **新建**。
5. 在“名称”中，键入服务器的名称。
6. 配置 LDAP 服务器的设置。
7. 展开 **嵌套组提取**，然后单击 **启用**。
8. 在“**最大嵌套级别**”中，键入 NetScaler Gateway 检查的级别数。
9. 在“**组名称标识符**”中，键入在 LDAP 服务器上唯一标识组名称的 LDAP 属性名称，例如 `sAMAccountName`。
10. 在“**组搜索属性**”中，键入要在搜索响应中获取的 LDAP 属性名称，以确定任何组的父组。例如，`memberOf`。
11. 在“**组搜索子属性**”中，键入要作为组搜索属性的一部分进行搜索的 LDAP 子属性名称，以确定任何组的父组。例如，键入 CN。
12. 在 **组搜索筛选器** 中，键入查询字符串。例如，筛选器可以是 `&(samaccountname=test)(objectClass=*)`。
13. 单击 **创建**，然后单击 **关闭**。

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

14. 在“创建身份验证策略”对话框中，在“命名表达式”旁边，选择表达式，单击 **添加表达式**，单击 **创建**，然后单击 **关闭**。

配置多个域的 LDAP 组提取

如果您有多个用于身份验证的域并正在使用 StoreFront，则可以配置 NetScaler Gateway 以使用组提取功能将正确的域名发送到 StoreFront。

在 Active Directory 中，您需要为网络中的每个域创建一个组。创建组后，添加属于该组和指定域的用户。在 Active Directory 中配置组后，您可以在 NetScaler Gateway 上为多个域配置 LDAP 组提取。

要为多个域配置 NetScaler Gateway 的组提取，您需要创建与网络中域数量相同的会话策略和身份验证策略。例如，如果您有两个域，名为 `Sampa` 和 Child。每个域都会收到一个会话策略和一个身份验证策略。

创建策略后，您可以在 NetScaler Gateway 上创建组，并将会话策略绑定到该组。然后，将身份验证策略绑定到虚拟服务器。

如果您在多个域中部署 StoreFront™，则域之间必须存在信任关系。

如果您在多个域中部署 Citrix Endpoint Management™ 或 StoreFront，则域之间无需相互信任。

为组提取创建会话策略

为组提取创建会话策略的第一步是创建两个会话配置文件并设置以下参数：

- 启用 ICA® 代理。
- 添加 StoreFront™ 网址。
- 添加 Windows 域。
- 将配置文件添加到会话策略并将表达式设置为 true。

为组提取创建会话配置文件

1. 在配置实用程序中，在“配置”选项卡上的导航窗格中，展开 **NetScaler Gateway > 策略**，然后单击 **会话**。
2. 在详细信息窗格中，单击“**配置文件**”选项卡，然后单击“**添加**”。
3. 在“**名称**”中，键入配置文件的名称。例如，键入 `Sampa`。
4. 在“**已发布的应用程序**”选项卡上，执行以下操作：

   a. 在“**ICA 代理**”旁边，单击“**覆盖全局**”，然后选择“**开**”。

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

   b. 在“**Web 界面地址**”旁边，单击“**覆盖全局**”，然后键入 StoreFront 的 Web 地址。
   c. 在“**单点登录域**”旁边，单击“**覆盖全局**”，键入 Windows 域的名称，然后单击“**创建**”。

5. 在“**名称**”中，清除第一个域的名称，然后键入第二个域的名称，例如 Child。
6. 在 **单点登录域** 旁边，清除第一个 Windows 域的名称，然后键入第二个域的名称，单击 **创建**，然后单击 **关闭**。

创建会话配置文件后，您将创建两个会话策略。每个会话策略使用其中一个配置文件。

创建会话策略

1. 在配置实用程序中，在“配置”选项卡上，在导航窗格中，展开 **NetScaler Gateway > 策略**，然后单击 **会话**。
2. 在详细信息窗格中，在 **策略** 选项卡上，单击 **添加**。
3. 在 **名称** 中，键入策略的名称。
4. 在 **请求配置文件** 中，选择第一个域的配置文件。
5. 在 **命名表达式** 旁边，单击 **常规**，选择 **True 值**，单击 **添加表达式**，然后单击 **创建**。
6. 在 **名称** 中，将名称更改为第二个域。
7. 在 **请求配置文件** 中，选择第二个域的配置文件，单击 **创建**，然后单击 **关闭**。

创建用于多个域的 LDAP 身份验证策略

在 NetScaler Gateway 上创建会话策略后，您将创建几乎相同的 LDAP 身份验证策略。配置身份验证策略时，重要的字段是 搜索筛选器。在此字段中，您必须键入在 Active Directory 中创建的组的名称。

首先创建身份验证配置文件，然后创建身份验证策略。

创建用于多个域组提取的身份验证配置文件

1. 在配置实用程序中，在“配置”选项卡上，展开 Citrix® **Gateway > 策略 > 身份验证**。
2. 在导航窗格中，单击 **LDAP**。
3. 在详细信息窗格中，单击“**服务器**”选项卡，然后单击“**添加**”。
4. 在“**名称**”中，键入第一个域的名称，例如 `Sampa`。
5. 配置 LDAP 服务器的设置，然后单击“**创建**”。
6. 重复步骤 3、4 和 5 以配置第二个域的身份验证配置文件，然后单击“**关闭**”。

创建并保存配置文件后，创建身份验证策略。

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

创建用于多个域组提取的身份验证策略

1. 在配置实用程序中，在“配置”选项卡上，展开 **NetScaler Gateway > 策略 > 身份验证**。
2. 在详细信息窗格中，单击“**策略**”选项卡，然后单击“**添加**”。
3. 在“**名称**”中，键入第一个域的名称。
4. 在“**身份验证类型**”中，选择“**LDAP**”。
5. 在“**服务器**”中，选择第一个域的身份验证配置文件。
6. 在“**命名表达式**”旁边，单击“**常规**”，选择“**真值**”，单击“**添加表达式**”，然后单击“**创建**”。
7. 在 Name 中，键入第二个域的名称。
8. 在“**服务器**”中，选择第二个域的身份验证配置文件，单击“**创建**”，然后单击“**关闭**”。

为多个域创建组并绑定策略以进行 LDAP 组提取

创建身份验证策略后，在 NetScaler Gateway 上创建组。创建组后，将身份验证策略绑定到虚拟服务器。

在 NetScaler Gateway 上创建组

1. 在配置实用程序中，在“**配置**”选项卡上的导航窗格中，展开“**NetScaler Gateway > 用户管理**”，然后单击“**AAA 组**”。
2. 在详细信息窗格中，单击“**添加**”。
3. 在“**组名**”中，键入第一个 Active Directory 组的名称。

> **重要提示：**
>
> 在 NetScaler Gateway 上为从多个域提取组而创建组时，组名必须与您在 Active Directory 中定义的组相同。组名也区分大小写，并且大小写必须与您在 Active Directory 中输入的大小写匹配。

4. 在“**策略**”选项卡上，单击“**会话**”，然后单击“**插入策略**”。
5. 在“**策略名称**”下，双击策略，然后单击“**创建**”。

将身份验证策略绑定到虚拟服务器

1. 在配置实用程序中，在“**配置**”选项卡上的导航窗格中，展开“**NetScaler Gateway**”，然后单击“**虚拟服务器**”。
2. 在详细信息窗格中，单击虚拟服务器，然后单击“**打开**”。

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

3. 在“身份验证”选项卡上，单击“**主要**”，在“**策略名称**”下，双击“**插入策略**”，然后选择第一个身份验证策略。
4. 在“**策略名称**”下，单击“**插入策略**”，双击第二个身份验证策略，然后单击“**确定**”。

LDAP 身份验证的 14 天密码过期通知

NetScaler Gateway 设备支持基于 LDAP 的身份验证的 14 天密码过期通知。通过使用此功能，管理员可以通知最终用户密码过期阈值时间（以天为单位）。有关更多详细信息，请参阅LDAP 身份验证的密码过期通知。

配置客户端证书身份验证

登录到 NetScaler Gateway 虚拟服务器的用户也可以根据提供给虚拟服务器的客户端证书属性进行身份验证。客户端证书身份验证还可以与其他身份验证类型（例如 LDAP 或 RADIUS）结合使用，以提供双因素身份验证。

要根据客户端证书属性对用户进行身份验证，必须在虚拟服务器上启用客户端身份验证并请求客户端证书。您必须将根证书绑定到 NetScaler Gateway 上的虚拟服务器。

当用户登录到 NetScaler Gateway 虚拟服务器时，身份验证后，将从证书的指定字段中提取用户名信息。通常，此字段是 Subject:CN。如果成功提取用户名，则用户将进行身份验证。在以下情况下，身份验证会失败。

- 如果用户在安全套接字层 (SSL) 握手期间未提供有效证书。
- 用户名提取失败，身份验证失败。

您可以通过将默认身份验证类型设置为使用客户端证书来根据客户端证书对用户进行身份验证。您还可以创建证书操作，该操作定义在基于客户端 SSL 证书的身份验证期间要执行的操作。

从适用于 Windows 的 Citrix Secure Access 客户端版本 24.8.1.15 和适用于 macOS 的版本 25.11.1.1 开始，在客户端证书身份验证期间，Citrix Secure Access 会根据 NetScaler Gateway 上配置的 CA 证书自动选择客户端证书。在以前的版本中，当存在来自不同证书颁发机构的多个证书时，用户必须通过试错过程来选择正确的证书进行身份验证。

注意：

- 请联系 Citrix 支持 以在 macOS 设备中启用客户端证书的自动选择。
- App Store 版本的 Citrix Secure Access for macOS 不支持客户端证书的自动选择。

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

下表说明了不同的客户端证书身份验证场景：

CA 证书配置	客户端证书选项	CITRIX SECURE ACCESS™ 的预期行为
CA1 配置在 NetScaler Gateway 上	来自 CA1 的客户端证书 1	Citrix Secure Access 自动选择客户端证书，无需用户交互即可进行身份验证。
	来自 CA 1 的客户端证书 1 和客户端证书 2	Citrix Secure Access 根据最长有效期选择客户端证书，无需用户交互即可进行身份验证。
CA1 和 CA2 配置在 NetScaler Gateway 上	来自 CA 1 或 CA 2 的客户端证书 1 和客户端证书 2	Citrix Secure Access 根据最长有效期选择客户端证书，无需用户交互即可进行身份验证。
	仅来自 CA1 或 CA2 的 1 个客户端证书	Citrix Secure Access 自动选择客户端证书，无需用户交互即可进行身份验证。
	来自 CA1 的客户端证书 1 和来自 CA 2 的客户端证书 2	Citrix Secure Access 会向用户提示两个客户端证书，用户应根据其要求选择客户端证书。

使用 GUI 将客户端证书配置为默认身份验证类型

1. 转到 **Configuration > NetScaler Gateway**，然后单击 **Global Settings**。
2. 在详细信息窗格中，在 **Authentication Settings** 下，单击 **Change authentication CERT settings**。
3. 根据您的要求，选择 **ON** 以启用使用证书的双因素身份验证。
4. 在 **User Name Field** 中，选择包含用户名的证书字段类型。
5. 在 **Group Name Field** 中，选择包含组名的证书字段类型。
6. 在 **Default Authorization Group** 中，键入默认组的名称，然后单击 **OK**。

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

从客户端证书中提取用户名

如果在 NetScaler Gateway 上启用了客户端证书身份验证，则用户将根据客户端证书的某些属性进行身份验证。身份验证成功后，将从证书中提取用户的用户名或用户和组名。此外，还会应用为该用户指定的策略。

配置和绑定客户端证书身份验证策略

您可以创建客户端证书身份验证策略并将其绑定到虚拟服务器。您可以使用该策略限制对特定组或用户的访问。此策略优先于全局策略。

配置客户端证书身份验证策略：

1. 在配置实用程序中，在“配置”选项卡上，展开 **NetScaler Gateway > 策略 > 身份验证**。
2. 在导航窗格中，在 **身份验证** 下，单击 **CERT**。
3. 在详细信息窗格中，单击 **添加**。
4. 在 **名称** 字段中，键入策略的名称。
5. 在 **服务器** 旁边，单击 **新建**。
6. 在 **名称** 中，键入配置文件的名称。
7. 在 **双因素** 旁边，选择 **关闭**。
8. 在 **用户名** 字段和 **组名** 字段中，选择值，然后单击 &**创建**。 注意：如果您之前将客户端证书配置为默认身份验证类型，请使用您用于策略的相同名称。 如果您填写了 用户名字段和组名字段对于默认身份验证类型，请为配置文件使用相同的值。
9. 在 **创建身份验证策略** 对话框中，在 **命名表达式** 旁边，选择表达式，单击 **添加表达式**，单击 **创建**，然后单击 **关闭**。

将客户端证书策略绑定到虚拟服务器：

配置客户端证书身份验证策略后，您可以将其绑定到虚拟服务器。

1. 在配置实用程序中，在“配置”选项卡上的导航窗格中，展开 **NetScaler Gateway**，然后单击 **虚拟服务器**。
2. 在详细信息窗格中，单击虚拟服务器，然后单击“**打开**”。
3. 在配置“**NetScaler Gateway 虚拟服务器**”对话框中，单击“**身份验证**”选项卡。
4. 单击“**主要**”或“**辅助**”。
5. 在“**详细信息**”下，单击“**插入策略**”。
6. 在“**策略名称**”中，选择策略，然后单击“**确定**”。

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

要将虚拟服务器配置为请求客户端证书：

当您要使用客户端证书进行身份验证时，必须配置虚拟服务器，以便在 SSL 握手期间请求客户端证书。

1. 在配置实用程序中，在“配置”选项卡上的导航窗格中，展开“**NetScaler Gateway**”，然后单击“**虚拟服务器**”。
2. 在详细信息窗格中，单击“**虚拟服务器**”，然后单击“**打开**”。
3. 在“**证书**”选项卡上，单击“**SSL 参数**”。
4. 在“**其他**”下，单击“**客户端身份验证**”。
5. 在“**客户端证书**”中，选择“**可选**”或“**强制**”，然后单击两次“确定”。如果您希望在同一虚拟服务器上允许其他身份验证类型且不需要使用客户端证书，请选择“**可选**”。

注意

- 有关回调 URL 的更多信息，请参阅导入 NetScaler Gateway。
- 有关证书的更多信息，请参阅安装、链接和更新证书。

配置双因素客户端证书身份验证

您可以配置客户端证书以首先对用户进行身份验证，然后要求用户使用辅助身份验证类型（例如 LDAP 或 RADIUS）登录。在此场景中，客户端证书首先对用户进行身份验证。然后，会出现一个登录页面，用户可以在其中输入其用户名和密码。当安全套接字层 (SSL) 握手完成后，登录序列可以采用以下两种路径之一：

- 既不从证书中提取用户名，也不提取组。登录页面会向用户显示，提示输入有效的登录凭据。NetScaler Gateway 会像正常密码身份验证一样对用户凭据进行身份验证。
- 用户名和组名从客户端证书中提取。如果只提取了用户名，则会向用户显示一个登录页面，其中包含登录名，并且用户无法修改该名称。只有密码字段为空。

NetScaler Gateway 在第二轮身份验证期间提取的组信息将附加到 NetScaler Gateway 从证书中提取的任何组信息（如果有）中。

配置智能卡身份验证

您可以将 NetScaler Gateway 配置为使用加密智能卡对用户进行身份验证。

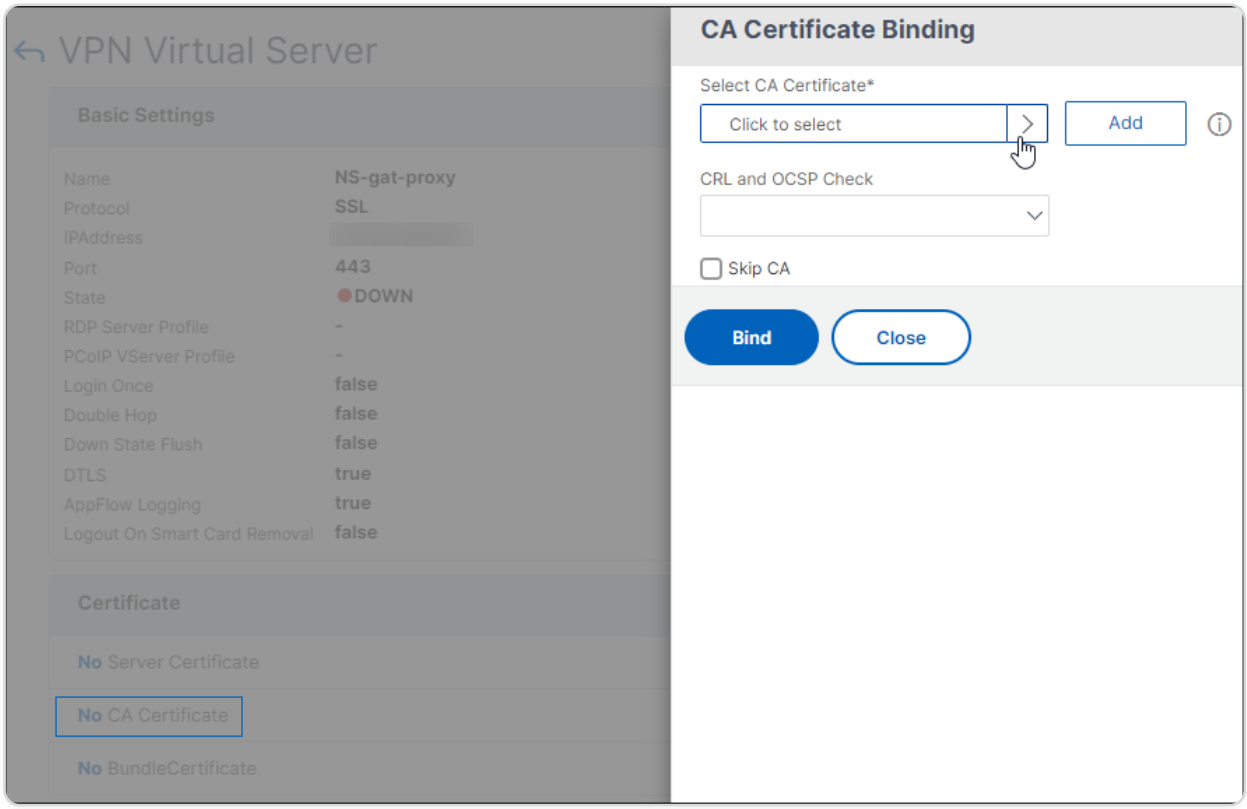
要使用 NetScaler Gateway 配置智能卡，您需要执行以下操作：

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

- 创建证书身份验证策略。有关详细信息，请参阅配置客户端证书身份验证。
- 将身份验证策略绑定到虚拟服务器。
- 将颁发客户端证书的证书颁发机构 (CA) 的根证书添加到 NetScaler Gateway。有关详细信息，请参阅在 NetScaler Gateway 上安装根证书。

重要提示：

当您将根证书添加到虚拟服务器以进行智能卡身份验证时，您必须从 **选择 CA 证书** 列表中选择证书。



创建客户端证书后，您可以将该证书（称为闪存）写入智能卡。完成该步骤后，即可测试智能卡。

如果您为 StoreFront™ 配置了智能卡直通身份验证，并且存在以下任一情况，则 StoreFront 的单点登录将失败：

- 如果您在“**已发布的应用程序**”选项卡上将域设置为 `mydomain`.com 而不是 `mydomain`。
- 如果您未在“**已发布的应用程序**”选项卡上设置域名，并且运行命令 `wi-sso-split-upn` 将值设置为 1。在此情况下，UserPrincipalName 包含域名“`mydomain`.com。”

您可以使用智能卡身份验证来简化用户的登录过程，同时增强用户访问基础架构的安全性。通过使用公钥基础架构的基于证书的双因素身份验证来保护对内部公司网络的访问。私钥受硬件控制保

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

护，并且永远不会离开智能卡。您的用户可以通过智能卡和 PIN 码方便地从各种公司设备访问其桌面和应用程序。

您可以使用智能卡通过 StoreFront 对 Citrix Virtual Apps and Desktops 提供的桌面和应用程序进行用户身份验证。登录 StoreFront 的智能卡用户还可以访问 NetScaler Endpoint Management 提供的应用程序。但是，用户必须再次进行身份验证才能访问使用客户端证书身份验证的 Endpoint Management Web 应用程序。

有关详细信息，请参阅 StoreFront 文档中的 配置智能卡身份验证。

使用 Secure ICA® 连接配置智能卡身份验证

使用智能卡在 NetScaler Gateway 上配置了单点登录并登录和建立安全 ICA 连接的用户，可能会收到两次个人识别码 (PIN) 提示。

- 登录时以及尝试启动已发布的资源时。如果 Web 浏览器和 Citrix Workspace 应用程序使用配置为使用客户端证书的同一虚拟服务器，则会出现此情况。
- Citrix Workspace 应用程序不与 Web 浏览器共享进程或安全套接字层 (SSL) 连接。因此，当 ICA 连接完成与 NetScaler Gateway 的 SSL 握手时，需要再次提供客户端证书。

为防止用户收到第二次 PIN 提示，您必须更改两个设置：

- 必须禁用 VPN 虚拟服务器上的客户端身份验证。
- 必须启用 SSL 重新协商。

配置虚拟服务器后，按照 配置 NetScaler Gateway 以处理 STA 和 ICA 流量 中所述，将一个或多个 STA 服务器绑定到虚拟服务器。

您可能还需要测试智能卡身份验证。

要禁用客户端身份验证：

1. 在配置实用程序中，在“配置”选项卡上的导航窗格中，展开 NetScaler Gateway，然后单击“虚拟服务器”。
2. 在主详细信息窗格中选择相关的虚拟服务器，然后单击“编辑”。
3. 在“高级选项”窗格中，单击“SSL 参数”。
4. 清除“客户端身份验证”复选框。
5. 点击完成。

要启用 SSL 重新协商：

1. 使用配置实用程序，从“配置”选项卡导航到“流量管理”，然后点击“SSL”。

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

2. 在主面板中，点击“更改高级 SSL 设置”。
3. 从“拒绝 SSL 重新协商”菜单中，选择“否”。

要测试智能卡身份验证：

1. 将智能卡连接到用户设备。
2. 打开您的 Web 浏览器并登录到 NetScaler Gateway。

配置 RADIUS 身份验证

您可以将 NetScaler Gateway 配置为使用一个或多个 RADIUS 服务器对用户访问进行身份验证。如果您使用的是 RSA SecurID、SafeWord 或 Gemalto Protiva 产品，则每个产品都通过 RADIUS 服务器进行配置。

您的配置可能需要使用网络访问服务器 IP 地址 (NAS IP) 或网络访问服务器标识符 (NAS ID)。将 NetScaler Gateway 配置为使用 RADIUS 身份验证服务器时，请遵循以下准则：

- 如果您启用 NAS IP 的使用，设备会将其配置的 IP 地址发送到 RADIUS 服务器，而不是用于建立 RADIUS 连接的源 IP 地址。
- 如果您配置了 NAS ID，设备会将该标识符发送到 RADIUS 服务器。如果您未配置 NAS ID，设备会将其主机名发送到 RADIUS 服务器。
- 启用 NAS IP 后，设备会忽略使用 NAS IP 配置的任何 NAS ID，以与 RADIUS 服务器通信。

配置 Gemalto Protiva 系统

Protiva 是 Gemalto 开发的一个强大的身份验证平台，旨在利用 Gemalto 智能卡身份验证的优势。使用 Protiva，用户通过用户名、密码和 Protiva 设备生成的一次性密码登录。与 RSA SecurID 类似，身份验证请求会发送到 Protiva 身份验证服务器，服务器会验证或拒绝密码。要配置 Gemalto Protiva 以兼容 NetScaler Gateway，请遵循以下准则：

- 安装 Protiva 服务器。
- 在 Microsoft IAS RADIUS 服务器上安装 Protiva SAS 代理软件，该软件扩展了 Internet 身份验证服务器 (IAS)。请务必记下 IAS 服务器的 IP 地址和端口号。
- 在 NetScaler Gateway 上配置 RADIUS 身份验证配置文件，并输入 Protiva 服务器的设置。

配置 SafeWord

SafeWord 产品系列使用基于令牌的密码提供安全身份验证。用户输入密码后，SafeWord 会立即使该密码失效，并且不能再次使用。配置 SafeWord 服务器时，您需要以下信息：

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

- NetScaler Gateway 的 IP 地址。该 IP 地址必须与您在 RADIUS 服务器客户端配置中配置的 IP 地址相同。NetScaler Gateway 使用内部 IP 地址与 RADIUS 服务器通信。配置共享密钥时，请使用内部 IP 地址。如果您为高可用性配置了两台设备，请使用虚拟内部 IP 地址。
- 共享密钥。
- SafeWord 服务器的 IP 地址和端口。默认端口号是 1812。

配置 RADIUS 身份验证

1. 在配置实用程序中，在“配置”选项卡上，展开 NetScaler Gateway \> 策略 \> 身份验证。
2. 单击 RADIUS，然后，在详细信息窗格中，在“策略”选项卡上，单击“添加”。
3. 在“创建身份验证策略”对话框中，在“名称”中，键入策略的名称。
4. 在“名称”中，键入策略的名称。
5. 在“服务器”旁边，单击“新建”。
6. 在“创建身份验证策略”对话框中，在“名称”中，键入服务器的名称。
7. 在“服务器”下，在“IP 地址”中，键入 RADIUS 服务器的 IP 地址。
8. 在“端口”中，键入端口。默认值为 1812。
9. 在“详细信息”下，在“密钥”和“确认密钥”中，键入 RADIUS 服务器密钥。
10. 在“NAS ID”中，键入标识符编号，然后单击“创建”。
11. 在“创建身份验证策略”对话框中，在“命名表达式”旁边，选择表达式，单击“添加表达式”，单击“创建”，然后单击“关闭”。

选择 RADIUS 身份验证协议

NetScaler Gateway 支持配置为使用多种协议进行用户身份验证的 RADIUS 实现，包括：

- 密码身份验证协议 (PAP)
- 质询握手身份验证协议 (CHAP)
- Microsoft 质询握手身份验证协议 (MS-CHAP 版本 1 和版本 2)

如果您的 NetScaler Gateway 部署配置为使用 RADIUS 身份验证，并且您的 RADIUS 服务器配置为使用 PAP，您可以通过为 RADIUS 服务器分配一个强共享密钥来增强用户身份验证。强 RADIUS 共享密钥由大小写字母、数字和标点符号的随机序列组成，长度至少为 22 个字符。如果可能，请使用随机字符生成程序来确定 RADIUS 共享密钥。

为了进一步保护 RADIUS 流量，请为每个 NetScaler Gateway 设备或虚拟服务器分配不同的共享密钥。在 RADIUS 服务器上定义客户端时，您还可以为每个客户端分配单独的共享密钥。如果这样做，您必须单独配置每个使用 RADIUS 身份验证的 NetScaler Gateway 策略。

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

创建 RADIUS 策略时，您将在 NetScaler Gateway 上配置共享密钥作为策略的一部分。

配置 IP 地址提取

您可以配置 NetScaler Gateway 以从 RADIUS 服务器提取 IP 地址。当用户使用 RADIUS 服务器进行身份验证时，服务器会返回分配给用户的帧 IP 地址。帧 IP 地址在访问请求中也称为 RADIUS 属性 8 Framed-IP-Address。

以下是 IP 地址提取的组件：

- 允许远程 RADIUS 服务器为登录到 NetScaler Gateway 的用户提供内部网络的 IP 地址。
- 允许使用类型 **ipaddress** 配置任何 RADIUS 属性，包括供应商编码的属性。

为 IP 地址提取配置 RADIUS 服务器时，您需要配置供应商标识符和属性类型。供应商 ID 和属性用于在 RADIUS 客户端和 RADIUS 服务器之间建立关联。

- 供应商标识符 (ID) 使 RADIUS 服务器能够从 RADIUS 服务器上配置的 IP 地址池中为客户端分配 IP 地址。供应商 ID 是 RADIUS 响应中提供内部网络 IP 地址的属性。值为零表示该属性未进行供应商编码。
- 属性类型是 RADIUS 响应中的远程 IP 地址属性。最小值为 1，最大值为 255。

常见的配置是提取 RADIUS 属性 **framed IP address**。供应商 ID 设置为 0 或未指定。属性类型设置为 8。

使用 GUI 从 RADIUS 服务器配置 IP 地址提取：

1. 导航到 **NetScaler Gateway \> 策略 \> 身份验证**，然后单击 **RADIUS**。
2. 在**详细信息**窗格的**策略**选项卡上，选择一个 RADIUS 策略，然后单击**打开**。
3. 在**配置身份验证策略**对话框中，在“服务器”旁边，单击**修改**。
4. 在**详细信息**下的**组供应商标识符**中，键入值。
5. 在**组属性类型**中，键入值，然后单击两次**确定**。

配置 RADIUS 组提取

您可以使用一种称为组提取的方法来配置 RADIUS 授权。配置组提取允许您在 RADIUS 服务器上管理用户，而无需将他们添加到 NetScaler Gateway。

您可以通过使用身份验证策略并配置组供应商标识符 (ID)、组属性类型、组前缀和组分隔符来配置 RADIUS 授权。配置策略时，您需要添加一个表达式，然后将策略全局绑定或绑定到虚拟服务器。

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

在 Windows Server 2003 上配置 RADIUS

如果您在 Windows Server 2003 上使用 Microsoft Internet 身份验证服务 (IAS) 进行 RADIUS 授权，则在配置 NetScaler Gateway 期间，您需要提供以下信息：

- 供应商 ID 是您在 IAS 中输入的供应商特定代码。
- 类型是供应商分配的属性编号。
- 属性名称是您在 IAS 中定义的属性名称类型。默认名称为 CTXSUserGroups=

如果 RADIUS 服务器上未安装 IAS，您可以从“控制面板”中的“添加或删除程序”安装它。有关详细信息，请参阅 Windows 在线帮助。

要配置 IAS，请使用 Microsoft 管理控制台 (MMC) 并安装 IAS 的管理单元。按照向导操作，确保选择以下设置：

- 选择本地计算机。
- 选择“远程访问策略”并创建自定义策略。
- 为策略选择 Windows-Groups。
- 选择以下协议之一：
  - Microsoft 质询握手身份验证协议版本 2 (MS-CHAP v2)
  - Microsoft 质询握手身份验证协议 (MS-CHAP)
  - 质询握手身份验证协议 (CHAP)
  - 未加密身份验证 (PAP, SPAP)
- 选择供应商特定属性。

  供应商特定属性需要与您在服务器上定义的组中的用户与 NetScaler Gateway 上的用户匹配。为满足此要求，您将供应商特定属性发送到 NetScaler Gateway。请确保选择 RADIUS=Standard。
- RADIUS 默认值为 0。将此数字用于供应商代码。
- 供应商分配的属性编号为 0。

  这是用户组属性的分配编号。该属性为字符串格式。
- 属性格式选择“字符串”。

  属性值需要属性名称和组。

  对于 Access Gateway，属性值为 CTXSUserGroups=groupname。如果定义了两个组，例如 sales 和 finance，则属性值为 CTXSUserGroups=sales;finance。使用分号分隔每个组。

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

- 删除“编辑拨入配置文件”对话框中的所有其他条目，只保留“供应商特定”条目。

在 IAS 中配置远程访问策略后，您将在 NetScaler Gateway 上配置 RADIUS 身份验证和授权。

配置 RADIUS 身份验证时，请使用您在 IAS 服务器上配置的设置。

在 Windows Server 2008 上配置 RADIUS 身份验证

在 Windows Server 2008 上，您可以使用网络策略服务器 (NPS) 配置 RADIUS 身份验证和授权，NPS 取代了 Internet 身份验证服务 (IAS)。您可以使用服务器管理器并将 NPS 添加为角色来安装 NPS。

安装 NPS 时，请选择“网络策略服务”。安装后，您可以通过从“开始”菜单中的“管理工具”启动 NPS 来配置网络的 RADIUS 设置。打开 NPS 后，将 NetScaler Gateway 添加为 RADIUS 客户端，然后配置服务器组。

配置 RADIUS 客户端时，请确保选择以下设置：

- 对于供应商名称，选择“RADIUS Standard”。
- 记下共享密钥，因为您需要在 NetScaler Gateway 上配置相同的共享密钥。

对于 RADIUS 组，您需要 RADIUS 服务器的 IP 地址或主机名。请勿更改默认设置。

配置 RADIUS 客户端和组后，您需要在以下两个策略中配置设置：

- 连接请求策略，您可以在其中配置 NetScaler Gateway 连接的设置，包括网络服务器类型、网络策略的条件以及策略的设置。
- 网络策略，您可以在其中配置可扩展身份验证协议 (EAP) 身份验证和供应商特定属性。

配置连接请求策略时，请为网络服务器类型选择“未指定”。然后，通过选择“NAS 端口类型”作为条件，“虚拟 (VPN)”作为值来配置您的条件。

配置网络策略时，您需要配置以下设置：

- 选择“远程访问服务器 (VPN 拨号)”作为网络访问服务器类型。
- 为 EAP 选择“加密身份验证 (CHAP)”和“未加密身份验证 (PAP 和 SPAP)”。
- 为供应商特定属性选择“RADIUS Standard”。

  默认属性编号为 26。此属性用于 RADIUS 授权。

  NetScaler Gateway 需要供应商特定属性来将服务器上组中定义的用户与 NetScaler Gateway 上的用户进行匹配。这通过将供应商特定属性发送到 NetScaler Gateway 来完成。
- 为属性格式选择“字符串”。

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

属性值需要属性名称和组。

对于 NetScaler Gateway，属性值为 CTXSUserGroups= groupname。如果定义了两个组，例如 sales 和 finance，则属性值为 CTXSUserGroups=sales;finance。使用分号分隔每个组。

- 分隔符是您在 NPS 上用于分隔组的字符，例如分号、冒号、空格或句点。

在 IAS 中完成远程访问策略配置后，您可以在 NetScaler Gateway 上配置 RADIUS 身份验证和授权。

配置 RADIUS 授权

1. 在配置实用程序中，在“配置”选项卡上，展开 NetScaler Gateway \> 策略 \> 身份验证。
2. 单击“RADIUS”。
3. 在“策略”选项卡中，单击“添加”。
4. 在“名称”中，键入策略的名称。
5. 在 Server* 下方点击 +
6. 在“名称”中，键入 RADIUS 服务器的名称。
7. 在“服务器”下，键入 RADIUS 服务器的 IP 地址和端口。
8. 在“详细信息”下，输入“组供应商标识符”和“组属性类型”的值。
9. 在“密码编码”中，选择身份验证协议，然后单击“创建”。
10. 在“创建身份验证策略”对话框中，在“命名表达式”旁边，选择表达式，单击“添加表达式”，单击“创建”，然后单击“关闭”。

配置 RADIUS 用户记账

NetScaler Gateway 可以向您的 RADIUS 记账服务器发送用户会话启动和停止消息。这些消息针对每个用户会话发送，包含 RFC2866 中定义的属性子集。表 1 列出了支持的属性以及发送它们的 RADIUS 记账消息类型（RAD_START 和 RAD_STOP）。表 2 列出了可以分配给 `Acct-Terminate-Cause` 属性的预定义值以及相应的 NetScaler Gateway 事件。

表 1. 支持的 RADIUS 属性

属性	含义	RAD_START	RAD_STOP
用户名	与会话关联的用户名称。	X	X
会话 ID	NetScaler 会话 ID。	X	X

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

属性	含义	RAD_START	RAD_STOP
计费会话时间	会话持续时间（秒）。	X	
计费终止原因	账户终止原因。	X	

表 2. RADIUS 终止原因

NETSCALER 注销方法	RADIUS 终止原因
LOGOUT_SESSN_TIMEDOUT	RAD_TERM_SESSION_TIMEOUT
LOGOUT_SESSN_INITIATEDBYUSER	RAD_TERM_USER_REQUEST
LOGOUT_SESSN_KILLEDBYADMIN	RAD_TERM_ADMIN_RESET
LOGOUT_SESSN_TLOGIN	RAD_TERM_NAS_REQUEST
LOGOUT_SESSN_MAXLICRCHD	RAD_TERM_NAS_REQUEST
LOGOUT_SESSN_CLISECCHK_FAILED	RAD_TERM_NAS_REQUEST
LOGOUT_SESSN_PREAUTH_CHANGED	RAD_TERM_NAS_REQUEST
LOGOUT_SESSN_COOKIE_MISMATCH	RAD_TERM_NAS_REQUEST
LOGOUT_SESSS_DHT	RAD_TERM_NAS_REQUEST
LOGOUT_SESSS_2FACTOR_FAIL	RAD_TERM_NAS_REQUEST
LOGOUT_SESSN_ICALIC	RAD_TERM_NAS_REQUEST
LOGOUT_SESSN_INTERNALERR	RAD_TERM_NAS_ERROR

RADIUS 用户记账的配置需要创建一对策略。第一个策略是 RADIUS 身份验证策略，用于指定发送记账消息的 RADIUS 服务器。第二个是会话策略，它使用 RADIUS 记账策略作为其操作。

要配置 RADIUS 用户记账，您必须：

1. 创建 RADIUS 策略以定义 RADIUS 记账服务器。记账服务器可以与您用于 RADIUS 身份验证的服务器相同。
2. 创建会话策略，使用 RADIUS 策略作为指定 RADIUS 用户记账服务器的操作。

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

3. 将会话策略全局绑定，使其适用于所有流量；或者绑定到 NetScaler Gateway 虚拟服务器，使其仅适用于流经该虚拟服务器的流量。

创建 RADIUS 策略

1. 在配置实用程序中，在导航窗格中，展开 NetScaler Gateway 节点，然后展开“策略”。
2. 展开“身份验证”并选择“RADIUS”。
3. 在详细信息窗格中，在“策略”选项卡上，单击“添加”。
4. 输入策略名称。
5. 从“服务器”菜单中选择一个服务器，或单击 + 图标并按照提示添加新的 RADIUS 服务器。
6. 在“表达式”窗格中，从“已保存的策略表达式”菜单中选择 ns_true。
7. 单击“创建”。

创建会话策略

配置指定 RADIUS 记账服务器的 RADIUS 策略后，创建一个会话策略，通过操作应用此记账服务器，如下所示：

1. 在配置实用程序中，在导航窗格中，展开 NetScaler Gateway 节点，然后选择“策略”。
2. 选择“会话”。
3. 在主详细信息窗格中，选择“添加”。
4. 输入策略名称。
5. 在“操作”菜单中，单击 + 图标以添加新的会话操作。
6. 输入会话操作的名称。
7. 单击“客户端体验”选项卡。
8. 在“记账策略”菜单中，选择您之前创建的 RADIUS 策略。
9. 单击“创建”。
10. 在“表达式”窗格中，从“已保存的策略表达式”菜单中选择 ns_true。
11. 单击“创建”。

全局绑定会话策略

1. 在配置实用程序中，在导航窗格中，展开 NetScaler Gateway 节点，然后展开“策略”。
2. 选择“会话”。
3. 在主详细信息窗格的“操作”菜单中，选择“全局绑定”。
4. 单击“绑定”。

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

5. 在“策略”窗格中，选择您之前创建的会话策略，然后单击“插入”。
6. 在“策略”列表中，单击会话策略的“优先级”条目，然后输入一个介于 0 到 64000 之间的值。
7. 单击“确定”。

将会话策略绑定到 NetScaler Gateway 虚拟服务器

1. 在配置实用程序中，在导航窗格中，展开 NetScaler Gateway 节点，然后选择“虚拟服务器”。
2. 在主详细信息窗格中，选择一个虚拟服务器，然后单击“编辑”。
3. 在“策略”窗格中，单击“+”图标以选择策略。
4. 从“选择策略”菜单中，选择“会话”，并确保在“选择类型”菜单中选择了“请求”。
5. 单击“继续”。
6. 点击绑定。
7. 在“策略”窗格中，选择之前创建的会话策略，然后单击“插入”。
8. 点击确定。

配置 SAML 身份验证

安全断言标记语言 (SAML) 是一种基于 XML 的标准，用于在身份提供者 (IdP) 和服务提供者之间交换身份验证和授权信息。NetScaler Gateway 支持 SAML 身份验证。

配置 SAML 身份验证时，您需要创建以下设置：

- IdP 证书名称。这是与 IdP 上的私钥对应的公钥。
- 重定向 URL。这是身份验证 IdP 的 URL。未通过身份验证的用户将被重定向到此 URL。
- 用户字段。如果 IdP 以不同于 Subject 标签的 NameIdentifier 标签的格式发送用户名，您可以使用此字段提取用户名。这是一个可选设置。
- 签名证书名称。这是 NetScaler Gateway 服务器的私钥，用于对发送到 IdP 的身份验证请求进行签名。如果未配置证书名称，则断言将未签名发送，或者身份验证请求将被拒绝。
- SAML 颁发者名称。此值在发送身份验证请求时使用。颁发者字段中必须有一个唯一名称，以表示发送断言的机构。这是一个可选字段。
- 默认身份验证组。这是身份验证服务器上用户从中进行身份验证的组。
- 双因素。此设置启用或禁用双因素身份验证。
- 拒绝未签名断言。如果启用，当未配置签名证书名称时，NetScaler Gateway 将拒绝用户身份验证。

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

NetScaler Gateway 支持 HTTP POST 绑定。在此绑定中，发送方以包含所需信息的表单自动提交（form-auto post）的 200 OK 响应用户。具体来说，默认表单必须包含两个名为 `SAMLRequest` 和 `SAMLResponse` 的隐藏字段，具体取决于表单是请求还是响应。表单还包括 RelayState，它是发送方用于发送任意信息的状态或信息，这些信息不会由依赖方处理。依赖方将信息发送回去，以便当发送方收到断言以及 RelayState 时，发送方就知道下一步该怎么做。建议您加密或混淆 RelayState。

注意

- 当 NetScaler Gateway 用作 Citrix Cloud 的 IdP 时，您无需在 NetScaler Gateway 上配置 **RelayState** 规则。
- 在 IdP 链式连接的情况下，只需在第一个 SAML 策略上配置 **RelayState** 规则即可。在此上下文中，IdP 链式连接是指配置的 SAML 操作引用包含另一个 SAML 操作的身份验证虚拟服务器 IdP 的场景。

配置 Active Directory 联合身份验证服务 2.0

您可以在任何用作联合服务器角色的 Windows Server 2008 或 Windows Server 2012 计算机上配置 Active Directory 联合身份验证服务 (AD FS) 2.0。将 ADFS 服务器配置为与 NetScaler Gateway 兼容时，需要使用 Windows Server 2008 或 Windows Server 2012 中的依赖方信任向导配置以下参数。

Windows Server 2008 配置参数：

- 依赖方信任。您提供 NetScaler Gateway 元数据文件位置，例如 `https://vserver.fqdn.com/ns.metadata.xml`，其中 vserver.fqdn.com 是 NetScaler Gateway 虚拟服务器的完全限定域名 (FQDN)。您可以在绑定到虚拟服务器的服务器证书上找到 FQDN。
- 授权规则。您可以允许或拒绝用户访问依赖方。

Windows Server 2012 配置参数：

- 依赖方信任。您提供 NetScaler Gateway 元数据文件位置，例如 `https://vserver.fqdn.com/ns.metadata.xml`，其中 vserver.fqdn.com 是 NetScaler Gateway 虚拟服务器的完全限定域名 (FQDN)。您可以在绑定到虚拟服务器的服务器证书上找到 FQDN。
- AD FS 配置文件。选择 AD FS 配置文件。
- 证书。NetScaler Gateway 不支持加密。您无需选择证书。

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

- 启用对 SAML 2.0 WebSSO 协议的支持。这将启用对 SAML 2.0 SSO 的支持。您提供 NetScaler Gateway 虚拟服务器 URL，例如 `https:netScaler.virtualServerName.com/cgi/samlauth`。

  此 URL 是 NetScaler Gateway 设备上的断言使用者服务 URL。这是一个常量参数，NetScaler Gateway 期望在此 URL 上收到 SAML 响应。
- 依赖方信任标识符。输入名称 NetScaler Gateway。这是一个用于标识依赖方的 URL，例如 `https://netscalerGateway.virtualServerName.com/adfs/services/trust`。
- 授权规则。您可以允许或拒绝用户访问依赖方。
- 配置声明规则。您可以使用“颁发转换规则”配置 LDAP 属性的值，并使用模板“将 LDAP 属性作为声明发送”。然后配置 LDAP 设置，其中包括：
  - 电子邮件地址
  - sAMAccountName
  - 用户主体名称 (UPN)
  - MemberOf
- 证书签名。您可以通过选择信赖方属性并添加证书来指定签名验证证书。

  如果签名证书小于 2048 位，将显示警告消息。您可以忽略该警告以继续。如果您正在配置测试部署，请在信赖方上禁用证书吊销列表 (CRL)。如果您不禁用此检查，AD FS 将尝试使用 CRL 来验证证书。

  您可以通过运行以下命令禁用 CRL：Set-ADFWRelayingPartyTrust - SigningCertficateRevocatonCheck None-TargetName NetScaler®

配置设置后，在完成信赖方信任向导之前验证信赖方数据。您可以使用端点 URL（例如 `https://vserver.fqdn.com/cgi/samlauth`）检查 NetScaler Gateway 虚拟服务器证书。

完成信赖方信任向导中的设置配置后，选择已配置的信任，然后编辑属性。执行以下操作：

- 将安全哈希算法设置为 SHA-1。

  注意：NetScaler 仅支持 SHA-1。
- 删除加密证书。不支持加密断言。
- 编辑声明规则，包括以下内容：
  - 选择转换规则
  - 添加声明规则

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

  - 选择声明规则模板：将 LDAP 属性作为声明发送
  - 命名
  - 选择属性存储：Active Directory
  - 选择 LDAP 属性：\<Active Directory 参数\>
  - 选择传出声明规则为“名称 ID”

  注意：不支持属性名称 XML 标签。

- 配置单点注销的注销 URL。声明规则为“发送注销 URL”。自定义规则必须如下：

```
=> issue(Type = "logoutURL", Value = "https://<adfs.fqdn.com>/adfs/
ls/", Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/
claimproperties/attributename"] =
"urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified");
```

配置 AD FS 设置后，下载 AD FS 签名证书，然后在 NetScaler Gateway 上创建证书密钥。然后，您可以使用该证书和密钥在 NetScaler Gateway 上配置 SAML 身份验证。

配置 SAML 双因素身份验证

您可以配置 SAML 双因素身份验证。将 SAML 身份验证与 LDAP 身份验证结合使用时，请遵循以下准则：

- 如果 SAML 是主要身份验证类型，请在 LDAP 策略中禁用身份验证并配置组提取。然后，将 LDAP 策略绑定为辅助身份验证类型。
- SAML 身份验证不使用密码，只使用用户名。此外，SAML 身份验证只在身份验证成功时通知用户。如果 SAML 身份验证失败，用户不会收到通知。由于不发送失败响应，SAML 必须是级联中的最后一个策略或唯一的策略。
- 建议您配置实际用户名而不是不透明字符串。
- SAML 不能绑定为辅助身份验证类型。

配置 SAML 身份验证

1. 在配置实用程序中，在“配置”选项卡上，展开 **NetScaler Gateway > Policies > Authentication**。
2. 在导航窗格中，单击 **SAML**。
3. 在详细信息窗格中，单击 **添加**。
4. 在“创建身份验证策略”对话框中，在“**名称**”中，键入策略的名称。

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

Create Authentication SAML Server

Name*

saml-pol1-server

Export SAML Metadata

☐ Import Metadata

Redirect URL*

https://test.com/saml/saml.aspx

Single Logout URL

SAML Binding*

POST

Logout Binding

POST

IDP Certificate Name*

ns-server-certificate | Add

Authentication Type

SAML

User Field

user1

Signing Certificate Name

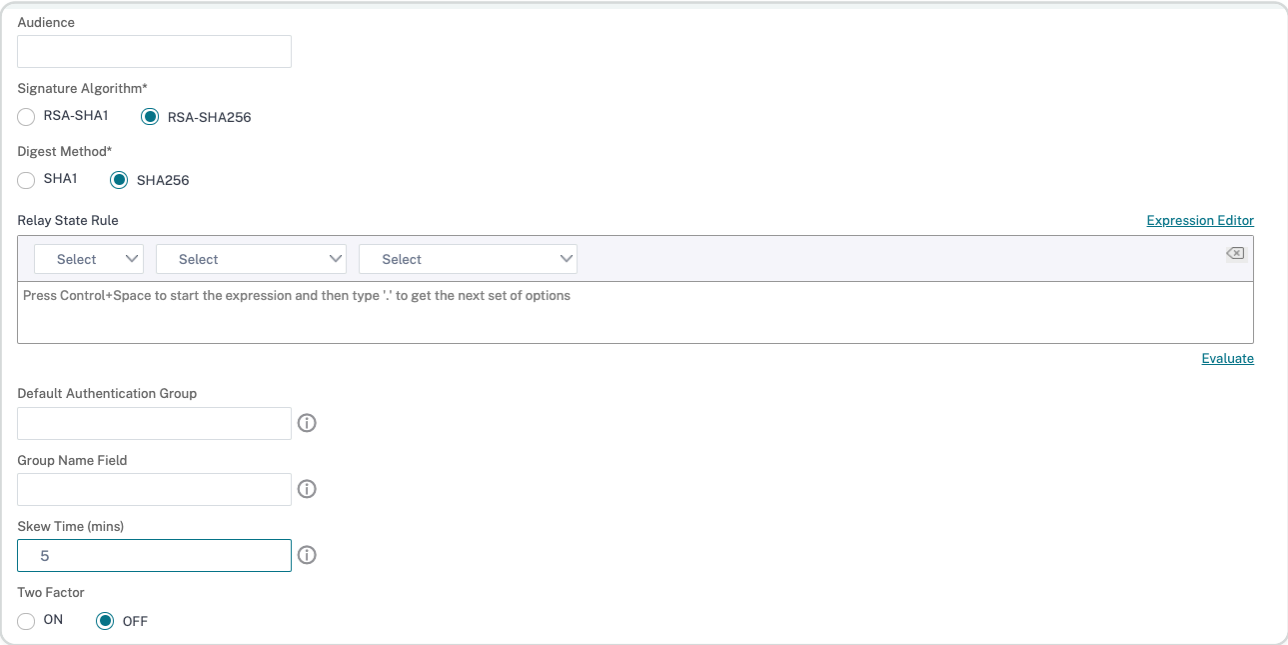
ns-server-certificate

Issuer Name

Reject Unsigned Assertion*

ON

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



1. 在“服务器”旁边，单击 **添加**。
2. 在“**名称**”中，键入服务器配置文件的名称。
3. 在“IdP 证书名称”中，选择证书或单击 **安装**。这是安装在 SAML 或 IdP 服务器上的证书。

   如果单击“安装”，请添加证书和私钥。有关详细信息，请参阅安装和管理证书。
4. 在“**重定向 URL**”中，输入身份验证身份提供程序 (IdP) 的 URL。

   这是用户登录 SAML 服务器的 URL。这是 NetScaler Gateway 将初始请求重定向到的服务器。
5. 在“**单一注销 URL**”中，指定 URL，以便设备可以识别何时将客户端发送回 IdP 以完成注销过程。
6. 在“**SAML 绑定**”中，选择用于将客户端从 SP 移动到 IdP 的方法。这需要在 IdP 上保持一致，以便 IdP 了解客户端如何连接到它。当设备充当 SP 时，它支持 POST、REDIRECT 和 ARTIFACT 绑定。
7. 在 **注销绑定** 中，选择 **重定向**。
8. 在 **IDP 证书名称** 中，选择 SAML 签名证书下的 IdPCert 证书 (Base64)。

   注意：

   您还可以单击 **导入元数据** 并选择存储元数据配置的 URL。

9. 在 **用户字段** 中，输入要提取的用户名。

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

10. 在 **签名证书名称** 中，选择设备用于向 IdP 签署身份验证请求的 SAML SP 证书（带私钥）。必须将相同的证书（不带私钥）导入到 IdP，以便 IdP 可以验证身份验证请求签名。大多数 IdP 不需要此字段。

    这是绑定到 NetScaler Gateway 虚拟 IP 地址的证书。SAML 颁发者名称是用户登录的完全限定域名 (FQDN)，例如 lb.example.com 或 ng.example.com。
11. 在 **颁发者名称** 中，输入设备发送初始身份验证 (GET) 请求的负载平衡或 NetScaler Gateway 虚拟 IP 地址的 FQDN。
12. 在 **拒绝未签名断言** 中，指定是否要求 IdP 的断言必须签名。您可以确保只有断言必须签名 (ON)，或者断言和 IdP 的响应都必须签名 (STRICT)。
13. 在 **受众** 中，输入 IdP 发送的断言适用的受众。这通常是代表服务提供商的实体名称或 URL。
14. 在 **签名算法** 中，选择 RSA-SHA256。
15. 在 **摘要方法** 中，选择 SHA256。
16. 在 **默认身份验证组** 中，输入除提取的组之外，身份验证成功时选择的默认组。
17. 在 **组名称** 中，输入断言中包含用户组的标签名称。
18. 在 **偏差时间（分钟）** 中，指定服务提供商允许传入断言的时钟偏差（以分钟为单位）。
19. 单击**创建**，然后单击**关闭**。
20. 在“创建身份验证策略”对话框中，在“命名表达式”旁边，选择“常规”，选择“真值”，单击**添加表达式**，单击**创建**，然后单击**关闭**。

参考

- 将 NetScaler 用作 SAML SP
- 将 NetScaler 用作 SAML IdP
- SAML 支持的其他功能

SAML 身份验证的改进

此功能需要 SAML 知识、基本的身份验证能力和对 FIPS 的理解才能使用此信息。

您可以将以下 NetScaler 功能与兼容 SAML 2.0 规范的第三方应用程序和服务器配合使用：

- SAML 服务提供商 (SP)
- SAML 身份提供商 (IdP)

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

SP 和 IdP 允许云服务之间进行单点登录 (SSO)。SAML SP 功能提供了一种从 IdP 处理用户声明的方式。IdP 可以是第三方服务或另一个 NetScaler 设备。SAML IdP 功能用于断言用户登录并提供由 SP 消费的声明。

作为 SAML 支持的一部分，IdP 和 SP 模块都会对发送给对等方的数据进行数字签名。数字签名包括来自 SP 的身份验证请求、来自 IdP 的断言以及这两个实体之间的注销消息。数字签名验证消息的真实性。

SAML SP 和 IdP 的当前实现是在数据包引擎中执行签名计算的。这些模块使用 SSL 证书对数据进行签名。在符合 FIPS 标准的 NetScaler 中，SSL 证书的私钥在数据包引擎或用户空间中不可用，因此当前的 SAML 模块尚未为 FIPS 硬件做好准备。

本文档描述了将签名计算卸载到 FIPS 卡的机制。签名验证在软件中完成，因为公钥是可用的。

解决方案

SAML 功能集已增强，可使用 SSL API 进行签名卸载。有关这些受影响的 SAML 子功能的详细信息，请参阅 NetScaler® 产品文档：

1. SAML SP Post 绑定 – AuthnRequest 的签名
2. SAML IdP Post 绑定 – 断言/响应/两者的签名
3. SAML SP 单点注销场景 – SP 发起的模型中 LogoutRequest 的签名以及 IdP 发起的模型中 LogoutResponse 的签名
4. SAML SP Artifact 绑定 – ArtifactResolve 请求的签名
5. SAML SP 重定向绑定 – AuthnRequest 签名
6. SAML IdP 重定向绑定 – Response/Assertion/两者签名
7. SAML SP 加密支持 – Assertion 解密

平台

API 只能卸载到 FIPS 平台。

配置

卸载配置在 FIPS 平台上自动执行。

但是，由于 SSL 私钥在 FIPS 硬件的用户空间中不可用，因此在 FIPS 硬件上创建 SSL 证书时，配置会略有不同。

以下是配置信息：

- `add ssl fipsKey fips-key`

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

创建一个 CSR 并在 CA 服务器上使用它来生成证书。然后，您可以将该证书复制到 `/nsconfig/ssl` 中。假设文件名为 fips3cert.cer。

- `add ssl certKey fips-cert -cert fips3cert.cer -fipsKey fips-key`

  然后在 SAML SP 模块的 SAML 操作中指定此证书。

- `set samlAction <name> -samlSigningCertName fips-cert`

  同样，您可以在 SAML IdP 模块的 `samlIdpProfile` 中使用此证书。

- `set samlidpprofile fipstest –samlIdpCertName fips-cert`

FIPS 密钥首次不可用。如果没有 FIPS 密钥，请按照 创建 FIPS 密钥 中所述创建一个。

```
create ssl fipskey <fipsKeyName> -modulus <positive_integer> [-exponent (3
| F4)]



create certreq <reqFileName> -fipskeyName <string>
```

使用 SAML 身份验证登录到 NetScaler Gateway

您可以使用 SAML 身份验证通过 VPN 客户端和 Workspace 应用程序登录到 NetScaler Gateway。该插件仅支持通过绑定到身份验证虚拟服务器的高级 SAML 策略（即 nFactor 身份验证）进行 SAML 身份验证。

重要提示：

当 SAML 策略直接绑定到 VPN 虚拟服务器（即非 nFactor 身份验证）时，该插件不支持 SAML 身份验证。

支持的平台和应用程序

下表列出了支持 SAML 身份验证以登录到 NetScaler Gateway 的平台和应用程序。

产品	版本
NetScaler 网关	12.0 版本 build 41.16 及更高版本

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

产品	版本
VPN 客户端	12.1 版本 build 49.37 及更高版本。**支持的平台**：Windows 7、Windows 8、Windows 8.1、Windows 10
Workspace 应用程序版本	Windows 系统：1808；Mac 系统：1808

使用高级 SAML 策略配置 SAML 身份验证

有关使用高级 SAML 策略配置 SAML 身份验证的详细信息，请参阅：NetScaler 作为 SAML IdP。

配置 TACACS+ 身份验证

您可以配置 TACACS+ 服务器进行身份验证。与 RADIUS 身份验证类似，TACACS+ 使用密钥、IP 地址和端口号。默认端口号为 49。

要将 NetScaler Gateway 配置为使用 TACACS+ 服务器，请提供服务器 IP 地址和 TACACS+ 密钥。仅当使用的服务器端口号不是默认端口号 49 时，才需要指定端口。

要使用用户界面配置 TACACS+ 身份验证，请执行以下步骤。

1. 在配置实用程序中，在“配置”选项卡上，展开 **NetScaler Gateway > 策略 > 身份验证**。
2. 单击 **TACACS**。
3. 在详细信息窗格中，单击 **添加**。
4. 在“**名称**”字段中，键入策略的名称。
5. 在“**服务器**”字段旁边，单击 **添加** 以创建新的 TACACS 服务器，或单击 **编辑** 以更改现有 TACACS 服务器。
6. 在“**名称**”字段中，键入服务器的名称。
7. 在“**IP 地址**”下，键入 IP 地址。
8. 在“**端口**”下，使用默认端口号 49。
9. 在“**TACACS 密钥**”字段中，键入密钥。在“**确认 TACACS 密钥**”字段中，键入相同的密钥进行确认。
10. 单击 **更多**。
11. 在“**授权**”中，选择 **ON**，然后单击 **创建**。
12. 在**创建身份验证TACACS策略**对话框中，选择表达式，单击“创建”，然后单击“关闭”。

要使用命令行界面配置TACACS+身份验证，请键入以下命令。

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

```
add authentication tacacsAction <name> [-serverIP <ip_addr|ipv6_addr|*>][-
serverPort <port>] [-authTimeout <positive_integer>] {-tacacsSecret }

[-authorization ( ON | OFF )] [-accounting ( ON | OFF )][-auditFailedCmds
( ON | OFF )] [-groupAttrName <string>][-defaultAuthenticationGroup
<string>] [-Attribute1 <string>] [-Attribute2 <string>] [-Attribute3
<string>] [-Attribute4 <string>]

[-Attribute5 <string>] [-Attribute6 <string>] [-Attribute7 <string>] [-
Attribute8 <string>] [-Attribute9 <string>] [-Attribute10 <string>]

[-Attribute11 <string>] [-Attribute12 <string>] [-Attribute13 <string>] [-
Attribute14 <string>] [-Attribute15 <string>] [-Attribute16 <string>]
```

在NetScaler Gateway中配置TACACS+服务器设置后，绑定策略以使其处于活动状态。您可以在全局或虚拟服务器级别绑定策略。有关绑定身份验证策略的更多信息，请参阅绑定身份验证策略。

清除配置基本操作不得清除 TACACS 配置

本主题重点介绍在运行清除配置命令时，不清除所有 RBA（基于角色的访问）相关配置。

当前的清除配置命令在以下三个级别之一执行：

- 基本
- 扩展
- 完整

根据级别，NetScaler 配置将被清除并重置为出厂默认设置。

使用的命令是；

```
clear ns config [-force] <level>
```

新命令添加了一个开关，用于允许/拒绝删除所有 RBA 相关配置。

新命令

以下是清除 RBA 配置功能的描述：

1. 带默认值 YES 的 YES/NO 开关。

   管理员决定是否保留 RBA 配置。

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

2. 仅支持清除配置的基本级别。
3. 以下配置未清除：
   - 添加/绑定系统用户/组。
   - 添加命令策略。
   - TACACS 命令（添加 TACACS 动作/策略）。
   - 绑定系统全局

   注意： 如果策略绑定到系统全局，则保留 TACACS 相关配置（动作/策略），否则将清除。

CLI 配置

使用的命令是；

```
clear config [-force] <level> [-RBAconfig]
```

默认情况下，它设置为 YES，并根据级别清除配置。

如果 –`RBAconfig` 设置为 NO，则保留 RBA 相关配置。其中包括：

- 添加/绑定系统用户/组
- 绑定系统全局
- TACACS 相关命令（添加 TACACS 动作/策略）
- 添加命令策略

配置多重身份验证

您可以在 NetScaler Gateway 中配置两种类型的多重身份验证：

- 级联身份验证，用于设置身份验证优先级级别
- 双因素身份验证，要求用户使用两种类型的身份验证登录

如果您有多个身份验证服务器，可以设置身份验证策略的优先级。您设置的优先级级别决定了身份验证服务器验证用户凭据的顺序。优先级数字较低的策略优先于优先级数字较高的策略。

您可以让用户针对两个不同的身份验证服务器进行身份验证。例如，您可以配置 LDAP 身份验证策略和 RSA 身份验证策略。当用户登录时，他们首先使用用户名和密码进行身份验证。然后，他们使用个人识别码 (PIN) 和 RSA 令牌中的代码进行身份验证。

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

配置级联身份验证

身份验证允许您使用策略优先级创建多个身份验证服务器的级联。配置级联时，系统会按照级联策略的定义遍历每个身份验证服务器，以验证用户的凭据。优先的身份验证策略按升序级联，优先级值范围为 1-9999。您可以在全局或虚拟服务器级别绑定策略时定义这些优先级。

在身份验证期间，当用户登录时，首先检查虚拟服务器，然后检查全局身份验证策略。如果用户同时属于虚拟服务器和全局的身份验证策略，则首先应用虚拟服务器的策略，然后应用全局身份验证策略。如果您希望用户接收全局绑定的身份验证策略，请更改该策略的优先级。当全局身份验证策略的优先级为 1，而绑定到虚拟服务器的身份验证策略的优先级为 2 时，全局身份验证策略优先。例如，您可以将三个身份验证策略绑定到虚拟服务器，并可以设置每个策略的优先级。

如果用户未能通过主级联中的策略进行身份验证，或者该用户成功通过主级联中的策略进行身份验证但未能通过辅助级联中的策略进行身份验证，则身份验证过程将停止，用户将被重定向到错误页面。

注意：Citrix® 建议，当您将多个策略绑定到虚拟服务器或全局时，为所有身份验证策略定义唯一的优先级。

设置全局身份验证策略的优先级

1. 在配置实用程序中，在“配置”选项卡上，展开 **NetScaler Gateway > 策略 > 身份验证**。
2. 选择全局绑定的策略，然后在“**操作**”中，单击“**全局绑定**”。
3. 在“**绑定/取消绑定全局身份验证策略**”对话框中，在“优先级”下，键入数字，然后单击“**确定**”。

更改绑定到虚拟服务器的身份验证策略的优先级

您还可以修改绑定到虚拟服务器的身份验证策略。

1. 在配置实用程序中，在“配置”选项卡上的导航窗格中，展开 **NetScaler Gateway**，然后单击“**虚拟服务器**”。
2. 在详细信息窗格中，选择一个虚拟服务器，然后单击“**打开**”。
3. 单击“**身份验证**”选项卡，然后单击“**主**”或“**辅助**”。
4. 在身份验证策略旁边，在“**优先级**”下，键入数字，然后单击“**确定**”。

配置双因素身份验证

NetScaler Gateway 支持双因素身份验证。通常，在对用户进行身份验证时，NetScaler Gateway 会在通过任何一个配置的身份验证方法成功验证用户后立即停止身份验证过程。在某些情况下，您可能需要对用户在一个服务器上进行身份验证，但从另一个服务器中提取组。例如，如果您的网络通

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

过 RADIUS 服务器对用户进行身份验证，但您也使用 RSA SecurID 令牌身份验证，并且用户组存储在该服务器上，则您可能需要对用户在该服务器上进行身份验证，以便提取组。

如果用户通过两种身份验证类型进行身份验证，并且其中一种类型是客户端证书身份验证，则可以将证书身份验证策略配置为第二种身份验证方法。例如，您使用 LDAP 作为主要身份验证类型，并使用客户端证书作为辅助身份验证。当用户使用其用户名和密码登录时，他们就可以访问网络资源。

配置双因素身份验证时，您可以选择身份验证类型是主要类型还是辅助类型。

配置双因素身份验证

1. 在配置实用程序中，在“配置”选项卡上，展开 NetScaler Gateway \> 策略 \> 身份验证。
2. 在“策略”选项卡上，单击“全局绑定”。
3. 在“绑定/取消绑定身份验证策略到全局”对话框中，单击“主要”。
4. 单击“插入策略”。
5. 在“策略名称”下，选择身份验证策略。
6. 单击“辅助”，重复步骤 4 和 5，然后单击“确定”。

为单点登录选择身份验证类型

如果在 NetScaler Gateway 上配置了单点登录和双因素身份验证，则可以选择用于单点登录的密码。例如，您将 LDAP 配置为主要身份验证类型，将 RADIUS 配置为辅助身份验证类型。当用户访问需要单点登录的资源时，默认发送用户名和主要密码。您可以在会话配置文件中设置用于 Web 应用程序单点登录的密码。

配置单点登录的身份验证

1. 在配置实用程序中，在“配置”选项卡上的导航窗格中，展开 **NetScaler Gateway > 策略 > 会话**。
2. 在详细信息窗格中，单击“**配置文件**”选项卡，然后执行以下操作之一：
   - 要创建新配置文件，请单击“**添加**”。
   - 要修改现有配置文件，请单击“**打开**”。
3. 在“客户端体验”选项卡上，在“凭据索引”旁边，单击“**覆盖全局**”，然后选择“**主要**”或“**辅助**”。
4. 如果这是新配置文件，请单击“**创建**”，然后单击“**关闭**”。
5. 如果要修改现有配置文件，请单击“**确定**”。

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

配置客户端证书和 LDAP 双因素身份验证

您可以使用安全的客户端证书进行 LDAP 身份验证和授权，例如使用智能卡身份验证与 LDAP。用户登录后，用户名将从客户端证书中提取。客户端证书是主要的身份验证形式，LDAP 是次要形式。客户端证书身份验证必须优先于 LDAP 身份验证策略。设置策略优先级时，请为客户端证书身份验证策略分配一个低于 LDAP 身份验证策略的数字。

要使用客户端证书，您必须拥有企业证书颁发机构 (CA)，例如 Windows Server 2008 中的证书服务，它运行在与 Active Directory 相同的计算机上。您可以使用 CA 创建客户端证书。

要将客户端证书与 LDAP 身份验证和授权结合使用，它必须是使用安全套接字层 (SSL) 的安全证书。要将安全的客户端证书用于 LDAP，请在用户设备上安装客户端证书，并在 NetScaler Gateway 上安装相应的根证书。

在配置客户端证书之前，请执行以下操作：

- 创建虚拟服务器。
- 为 LDAP 服务器创建 LDAP 身份验证策略。
- 将 LDAP 策略的表达式设置为 True 值。

配置使用 LDAP 的客户端证书身份验证

1. 在配置实用程序中，在“配置”选项卡上，展开 **NetScaler Gateway \> 策略 \ > 身份验证**。
2. 在导航窗格中，在“身份验证”下，单击“证书”。
3. 在详细信息窗格中，单击“添加”。
4. 在“名称”中，键入策略的名称。
5. 在“身份验证类型”中，选择“证书”。
6. 在“服务器”旁边，单击“新建”。
7. 在“名称”中，键入服务器的名称，然后单击“创建”。
8. 在“创建身份验证服务器”对话框的“名称”中，键入服务器的名称。
9. 在“双因素”旁边，选择“开”。
10. 在“用户名”字段中，选择“主题:CN”，然后单击“创建”。
11. 在“创建身份验证策略”对话框中，在“命名表达式”旁边，选择“True 值”，单击“添加表达式”，单击“创建”，然后单击“关闭”。

创建证书身份验证策略后，将策略绑定到虚拟服务器。绑定证书身份验证策略后，将 LDAP 身份验证策略绑定到虚拟服务器。

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

重要提示：

必须先将证书身份验证策略绑定到虚拟服务器，然后才能将 LDAP 身份验证策略绑定到虚拟服务器。

在 NetScaler Gateway 上安装根证书

创建证书身份验证策略后，您将从 CA 下载并安装 Base64 格式的根证书，并将其保存到计算机上。然后，您可以将根证书上传到 NetScaler Gateway。

1. 在配置实用程序中，在“配置”选项卡上的导航窗格中，展开“SSL”，然后单击“证书”。
2. 在详细信息窗格中，单击“安装”。
3. 在“证书 - 密钥对名称”中，键入证书的名称。
4. 在“证书文件名”中，单击“浏览”，然后在列表中选择“设备”或“本地”。
5. 导航到根证书，单击“打开”，然后单击“安装”。

将根证书添加到虚拟服务器

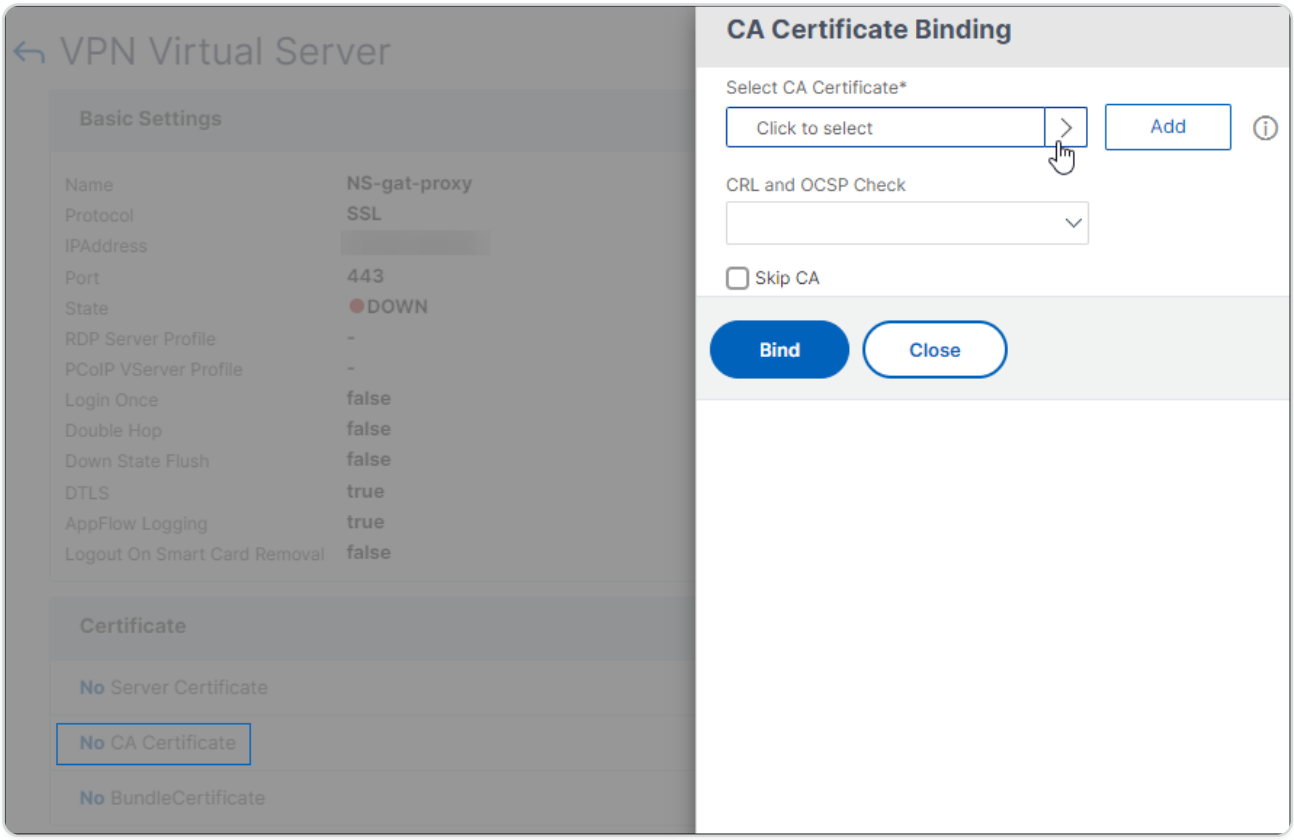
在 NetScaler Gateway 上安装根证书后，将该证书添加到虚拟服务器的证书存储中。

重要提示：

当您将根证书添加到虚拟服务器以进行智能卡身份验证时，您必须从 **选择 CA 证书** 列表框中选择证书，如下图所示。

图 1. 将根证书添加为 CA

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



1. 在配置实用程序中，在“配置”选项卡上的导航窗格中，展开“NetScaler Gateway”，然后单击“虚拟服务器”。
2. 在详细信息窗格中，选择一个虚拟服务器，然后单击“打开”。
3. 在“证书”选项卡上，在“可用”下，选择证书，在“添加”旁边，在列表中单击“CA”，然后单击“确定”。
4. 重复步骤 2。
5. 在“证书”选项卡上，单击“SSL 参数”。
6. 在“其他”下，选择“客户端身份验证”。
7. 在“其他”下，在“客户端证书”旁边，选择“可选”，然后单击“确定”两次。
8. 配置客户端证书后，使用 Citrix Secure Access 客户端登录 NetScaler Gateway 以测试身份验证。如果安装了多个证书，系统会提示您选择正确的证书。选择证书后，将显示登录屏幕，其中用户名已填充从证书获取的信息。键入密码，然后单击“登录”。

如果您在登录屏幕的“用户名”字段中没有看到正确的用户名，请检查 LDAP 目录中的用户帐户和组。在 NetScaler Gateway 上定义的组必须与 LDAP 目录中的组相同。在 Active Directory 中，在域根级别配置组。如果您创建的 Active Directory 组不在域根级别，则可能导致客户端证书读取不正确。

如果用户和组不在域根级别，NetScaler Gateway 登录页面会显示在 Active Directory 中配置的用户名。例如，在 Active Directory 中，您有一个名为 Users 的文件夹，并且证书显示 CN=Users。在登录页面中，“用户名”字段会显示“Users”一词。

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

如果您不想将组和用户帐户移动到根域级别，在 NetScaler Gateway 上配置证书身份验证服务器时，请将“用户名”字段和“组名”字段留空。

配置单点登录

您可以将 NetScaler Gateway 配置为支持 Windows、Web 应用程序（例如 SharePoint）、文件共享以及 StoreFront 的单点登录。单点登录也适用于用户可以通过访问界面中的文件传输实用程序或通知区域中的 NetScaler Gateway 图标菜单访问的文件共享。

如果您在用户登录时配置单点登录，他们将自动再次登录，而无需第二次输入其凭据。

配置 Windows 单点登录

用户通过从桌面启动 Citrix Secure Access 客户端来建立连接。您可以通过启用单点登录来指定 Citrix Secure Access 客户端在用户登录 Windows 时自动启动。配置单点登录后，用户的 Windows 登录凭据将传递给 NetScaler Gateway 进行身份验证。为 Citrix Secure Access 客户端启用单点登录有助于用户设备上的操作，例如安装脚本和自动驱动器映射。

仅当用户设备登录到您组织的域时才启用单点登录。如果启用了单点登录，并且用户从不在您域中的设备进行连接，则会提示用户登录。

您可以全局配置 Windows 单点登录，也可以使用附加到会话策略的会话配置文件来配置。

全局配置 Windows 单点登录

1. 在配置实用程序中，在“**Configuration**”选项卡上的导航窗格中，展开“**NetScaler Gateway**”，然后单击“**Global Settings**”。
2. 在详细信息窗格中，在“**Settings**”下，单击“**Change global settings**”。
3. 在“**Client Experience**”选项卡上，单击“**Single Sign-on with Windows**”，然后单击“**OK**”。

使用会话策略配置 Windows 单点登录

1. 在配置实用程序中，在“**Configuration**”选项卡上的导航窗格中，展开“**NetScaler Gateway > Policies**”，然后单击“**Session**”。
2. 在详细信息窗格中，单击“**Add**”。
3. 在“**Name**”中，键入策略的名称。
4. 在“**Request Profile**”旁边，单击“**New**”。
5. 在“**Name**”中，键入配置文件的名称。
6. 在“**Client Experience**”选项卡上，在“**Single Sign-On with Windows**”旁边，单击“**Override Global**”，单击“**Single Sign-on with Windows**”，然后单击“**OK**”。

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

7. 在“**创建会话策略**”对话框中，在“**命名表达式**”旁边，选择“**常规**”，选择“真值”，单击“**添加表达式**”，单击“**创建**”，然后单击“**关闭**”。

配置 Web 应用程序的单点登录

您可以将 NetScaler Gateway 配置为向使用基于 Web 的身份验证的内部网络中的服务器提供单点登录。通过单点登录，您可以将用户重定向到自定义主页，例如 SharePoint 站点或 StoreFront。您还可以通过 Citrix Secure Access 客户端，从主页上配置的书签或用户在 Web 浏览器中键入的 Web 地址，配置对资源的单点登录。

如果您要将主页重定向到 SharePoint 站点或 StoreFront，请提供该站点的 Web 地址。当用户通过 NetScaler Gateway 或外部身份验证服务器进行身份验证后，用户将被重定向到指定的主页。用户凭据会透明地传递给 Web 服务器。如果 Web 服务器接受凭据，用户将自动登录。如果 Web 服务器拒绝凭据，用户将收到身份验证提示，要求输入其用户名和密码。

您可以全局配置 Web 应用程序的单点登录，也可以使用会话策略进行配置。

全局配置 Web 应用程序的单点登录

1. 在配置实用程序中，在“Configuration”（配置）选项卡上的导航窗格中，展开 NetScaler Gateway，然后单击“Global Settings”（全局设置）。
2. 在详细信息窗格的“Settings”（设置）下，单击“Change global settings”（更改全局设置）。
3. 在“Client Experience”（客户端体验）选项卡上，单击“Single sign-on to Web Applications”（Web 应用程序的单点登录），然后单击“OK”（确定）。

使用会话策略配置 Web 应用程序的单点登录

1. 在配置实用程序中，在“Configuration”（配置）选项卡上的导航窗格中，展开 NetScaler Gateway \> Policies（策略），然后单击“Session”（会话）。
2. 在详细信息窗格的“Policies”（策略）选项卡上，选择一个会话策略，然后单击“Open”（打开）。
3. 在“Configure Session Policy”（配置会话策略）对话框中，在“Request Profile”（请求配置文件）旁边，单击“Modify”（修改）。
4. 在“Client Experience”（客户端体验）选项卡上，在“Single Sign-On to Web Applications”（Web 应用程序的单点登录）旁边，单击“Global Override”（全局覆盖），单击“Single Sign-On to Web Applications”（Web 应用程序的单点登录），然后单击“OK”（确定）。

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

定义 Web 应用程序单点登录的 HTTP 端口

仅当目标端口被视为 HTTP 端口时，才尝试进行单点登录。要允许对使用端口 80 以外的端口进行 HTTP 流量的应用程序进行单点登录，请在 NetScaler Gateway 上添加一个或多个端口号。您可以启用多个端口。这些端口是全局配置的。

1. 在配置实用程序中，在“配置”选项卡上的导航窗格中，展开 NetScaler Gateway，然后单击“全局设置”。
2. 在详细信息窗格中，在“设置”下，单击“更改全局设置”。
3. 在“网络配置”选项卡上，单击“高级设置”。
4. 在“HTTP 端口”下，键入端口号，单击“添加”，然后单击两次“确定”。

   您可以对要添加的每个端口重复步骤 4。

注意：如果内部网络中的 Web 应用程序使用公共 IP 地址，则单点登录将无法运行。要启用单点登录，必须将拆分隧道作为全局策略设置的一部分启用，无论用户设备连接是使用无客户端访问还是 Citrix Secure Access™ 客户端。如果无法在全局级别启用拆分隧道，请创建一个使用专用地址范围的虚拟服务器。

使用 LDAP 配置 Web 应用程序的单点登录

当您配置单点登录，并且用户使用以下格式的用户主体名称 (UPN) 登录时：username@domain.com，默认情况下单点登录会失败，用户必须进行两次身份验证。如果您需要使用此格式进行用户登录，请修改 LDAP 身份验证策略以接受此形式的用户名。

配置 Web 应用程序的单点登录

1. 在配置实用程序中，在“**配置**”选项卡上，展开“**NetScaler Gateway > 策略 > 身份验证**”。
2. 在详细信息窗格中，在“**策略**”选项卡上，选择一个 LDAP 策略，然后单击“**打开**”。
3. 在“**配置身份验证策略**”对话框中，在“**服务器**”旁边，单击“**修改**”。
4. 在“**连接设置**”下，在“基本 DN”（用户位置）中，键入 DC=domainname,DC=com。
5. 在“**管理员绑定 DN**”中，键入 LDAPaccount@domainname.com，其中 domainname.com 是您的域名。
6. 在“**管理员密码**”和“**确认管理员密码**”中，键入密码。
7. 在“**其他设置**”下，在“**服务器登录名属性**”中，键入 UserPrincipalName。
8. 在“**组属性**”中，键入 memberOf。
9. 在“**子属性名称**”中，键入 CN。

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

10. 在“**SSO 名称属性**”中，键入用户登录的格式，然后单击两次“**确定**”。此值可以是 `SamAccountName` 或 `UserPrincipalName`。

配置到域的单点登录

如果用户连接到运行 Citrix Virtual Apps™ 的服务器并使用 SmartAccess，您可以为连接到服务器场的用户配置单点登录。当您使用会话策略和配置文件配置对已发布应用程序的访问时，请使用服务器场的域名。

您还可以配置到网络中文件共享的单点登录。

配置到域的单点登录

1. 在配置实用程序中，在“配置”选项卡上，在导航窗格中，展开 NetScaler Gateway \> 策略，然后单击“会话”。
2. 在详细信息窗格中，在“策略”选项卡上，选择一个会话策略，然后单击“打开”。
3. 在“配置会话策略”对话框中，在“请求配置文件”旁边，单击“修改”。
4. 在“配置会话配置文件”对话框中，在“已发布应用程序”选项卡上，在“单点登录域”中，单击“覆盖全局”，键入域名，然后单击两次“确定”。

有关使用 Citrix Virtual Apps 配置 NetScaler Gateway 的更多信息，请参阅将 NetScaler Gateway 与 StoreFront 集成。

配置 Microsoft Exchange 2010 的单点登录

以下部分描述了在 NetScaler Gateway 上为 Microsoft Exchange 2010 配置单点登录 (SSO)。Outlook Web Access (OWA) 2010 的 SSO 在以下情况下不起作用：

- 在 Microsoft Exchange 2010 上使用基于表单的身份验证。
- 具有身份验证、授权和审计流量管理策略的负载平衡虚拟服务器。

注意：

此配置仅适用于具有身份验证、授权和审计流量管理策略的负载平衡虚拟服务器。它不适用于 OWA 2010 中使用无客户端 VPN 的 SSO。

以下步骤是在 NetScaler Gateway 上为 Microsoft Exchange 2010 配置 SSO 之前必须考虑的先决条件。

- OWA 2010 中 SSO 表单的 Action URL 不同。请相应地修改流量管理策略。
- 您需要一个重写策略来在 logon.aspx 请求中设置 `PBack` cookie。在正常情况下，您在客户端设置 `PBack` cookie 并点击“提交”。

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

- 当您使用 SSO 时，logon.aspx 的响应会被消耗，NetScaler Gateway 会生成表单请求。cookie 不会附加到表单提交请求中。
- OWA 服务器期望在表单提交请求中包含 `PBack` cookie。需要重写策略才能在表单提交请求中附加 `PBack` cookie。

使用 CLI 执行以下操作

1. 配置身份验证、授权和审计流量管理

   ```
   add tm formSSOAction OWA_Form_SSO_SSOPro -actionURL "/owa/auth.owa"
   -userField username -passwdField password -ssoSuccessRule
   "http.RES.SET_COOKIE.COOKIE(\"cadata\").VALUE(\"cadata\").LENGTH.GT(70"
   -responsesize 15000 -submitMethod POST
   ```

2. 配置流量管理策略并绑定策略

   - `add tm trafficAction OWA_2010_Prof -appTimeout 1 -SSO ON -formSSO Action OWA_Form_SSO_SSOPro`
   - `add tm trafficPolicy owa2k10_pol "HTTP.REQ.URL.CONTAINS(\"owa/auth/logon.aspx\")" OWA_2010_Prof`
   - `bind tm global -policyName owa2k10_pol -priority 100`

使用 CLI 重写配置

在命令提示符下，键入：

- `add rewrite action set_pback_cookie insert_after "http.REQ.COOKIE.VALUE(\"OutlookSession\")" "\";PBack=0\"" -bypassSafetyCheck YES`
- `add rewrite policy set_pback_cookie "http.REQ.URL.CONTAINS(\"logon.aspx\")" set_pback_cookie`
- `bind rewrite global set_pback_cookie 100 END -type REQ_DEFAULT`

备用重写配置

在极少数情况下，Microsoft Outlook 可能不会发出 OWA 会话 Cookie，并且 `Pback` Cookie 也可能不会被插入。在您运行了上述命令以实施重写配置后，可能会出现此问题。

为了克服此类情况并作为一种变通方法，您可以配置以下命令，而不是重写配置。

在命令提示符下，键入：

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

- `add rewrite action set_pback_cookie insert_http_header "Cookie" '"PBack=0"'`
- `add rewrite policy set_pback_cookie "http.REQ.URL.CONTAINS(\"logon.aspx\")" set_pback_cookie`
- `set rewrite policy set_pback_cookie -action set_pback_cookie`
- `bind rewrite global set_pback_cookie 100 END -type REQ_DEFAULT`

配置一次性密码使用

您可以将 NetScaler Gateway 配置为使用一次性密码，例如令牌个人识别码 (PIN) 或密码。用户输入密码或 PIN 后，身份验证服务器会立即使该一次性密码失效，用户无法再次输入相同的 PIN 或密码。

使用一次性密码的产品包括：

- RSA SecurID
- 易普瑞瓦塔 欧耐信
- SafeWord
- 金雅拓 普罗蒂瓦
- 北欧 短信通行码

要使用这些产品中的每一个，请将内部网络中的身份验证服务器配置为使用 RADIUS。有关详细信息，请参阅配置 RADIUS 身份验证。

如果您在 NetScaler Gateway 上配置身份验证以使用 RADIUS 的一次性密码（例如，由 RSA SecurID 令牌提供），NetScaler Gateway 会尝试使用缓存的密码重新验证用户身份。当您对 NetScaler Gateway 进行更改，或者 Citrix Secure Access 客户端与 NetScaler Gateway 之间的连接中断后又恢复时，会发生此重新验证。

当连接配置为使用 Citrix Workspace 应用程序且用户通过 RADIUS 或 LDAP 连接到 StoreFront 时，也可能发生重新验证尝试。当用户启动并使用某个应用程序，然后返回 Receiver 启动另一个应用程序时，NetScaler Gateway 会使用缓存的信息来验证用户身份。

配置 RSA SecurID 身份验证

配置 RSA/ACE 服务器以进行 RSA SecureID 身份验证时，您需要完成以下步骤：

配置 RADIUS 客户端并提供以下信息：

- 提供 NetScaler Gateway 设备名称。

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

- 提供描述（非强制）。
- 提供系统 IP 地址。
- 提供 NetScaler Gateway 和 RADIUS 服务器之间的共享密钥。
- 将制造商/型号配置为标准 RADIUS。

在代理主机配置中，您需要以下信息：

- 提供 NetScaler Gateway 的完全限定域名 (FQDN)（与绑定到虚拟服务器的证书上显示的一致）。提供 FQDN 后，单击 Tab 键，“网络地址”窗口将自动填充。

  输入 FQDN 后，网络地址会自动显示。如果未显示，请输入系统 IP 地址。
- 使用通信服务器提供代理类型。
- 配置导入所有用户或一组允许通过 NetScaler Gateway 进行身份验证的用户。

如果尚未配置，请为 RADIUS 服务器创建代理主机条目，包括以下信息：

- 提供 RSA 服务器的 FQDN。

  输入 FQDN 后，网络地址会自动出现。如果未出现，请提供 RSA 服务器的 IP 地址。
- 提供代理类型，即 RADIUS 服务器。

有关配置 RSA RADIUS 服务器的更多信息，请参阅制造商文档。

要配置 RSA SecurID，请创建身份验证配置文件和策略，然后将策略全局绑定或绑定到虚拟服务器。要创建使用 RSA SecurID 的 RADIUS 策略，请参阅配置 RADIUS 身份验证。

创建身份验证策略后，将其绑定到虚拟服务器或全局。有关更多信息，请参阅绑定身份验证策略。

配置 RADIUS 密码返回

您可以使用令牌从 RADIUS 服务器生成的一次性密码来替换域密码。当用户登录到 NetScaler Gateway 时，他们会输入个人识别码 (PIN) 和令牌中的密码。NetScaler Gateway 验证其凭据后，RADIUS 服务器会将用户的 Windows 密码返回给 NetScaler Gateway。NetScaler Gateway 接受来自服务器的响应，然后使用返回的密码进行单点登录，而不是使用用户在登录时输入的密码。此 RADIUS 密码返回功能允许您配置单点登录，而无需用户记住其 Windows 密码。

当用户使用密码返回登录时，他们可以访问内部网络中的所有允许的网络资源，包括 Citrix Endpoint Management™ 和 StoreFront。

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

要使用返回的密码启用单点登录，您可以通过使用“密码供应商标识符”和“密码属性类型”参数在 NetScaler Gateway 上配置 RADIUS 身份验证策略。这两个参数会将用户的 Windows 密码返回给 NetScaler Gateway。

NetScaler Gateway 支持 Imprivata OneSign。Imprivata OneSign 的最低要求版本是 4.0 Service Pack 3。Imprivata OneSign 的默认密码供应商标识符为 398。Imprivata OneSign 的默认密码属性类型代码为 5。

您可以使用其他 RADIUS 服务器进行密码返回，例如 RSA、Cisco 或 Microsoft。配置 RADIUS 服务器以供应商特定的属性值对形式返回用户单点登录密码。在 NetScaler Gateway 身份验证策略中，您必须为这些服务器添加“**密码供应商标识符和密码**”属性类型参数。

您可以在 Internet Assigned Numbers Authority (IANA) 网站 上找到完整的供应商标识符列表。例如，RSA Security 的供应商标识符是 2197，Microsoft 的是 311，Cisco Systems 的是 9。供应商支持的特定于供应商的属性必须与供应商确认。例如，Microsoft 已在 Microsoft 供应商特定 RADIUS 属性 发布了特定于供应商的属性列表。

您可以选择任何特定于供应商的属性，以在供应商的 RADIUS 服务器上存储用户的单点登录密码。如果您使用供应商标识符和用户密码存储在 RADIUS 服务器上的属性配置 NetScaler Gateway，则 NetScaler Gateway 会在发送到 RADIUS 服务器的访问请求数据包中请求该属性的值。如果 RADIUS 服务器在访问接受数据包中响应相应的属性-值对，则无论您使用哪个 RADIUS 服务器，密码返回都将起作用。

要使用返回的密码配置单点登录：

1. 在配置实用程序中，在“配置”选项卡上，展开“**NetScaler Gateway \> 策略 \ > 身份验证**”。
2. 在导航窗格中，单击“**RADIUS**”。
3. 在详细信息窗格中，单击“**添加**”。
4. 在“**创建身份验证策略**”对话框中，在“名称”中，键入策略的名称。
5. 在“**服务器**”旁边，单击“**新建**”。
6. 在“**名称**”中，键入服务器的名称。
7. 配置 RADIUS 服务器的设置。
8. 在 **密码供应商标识符** 中，键入 RADIUS 服务器返回的供应商标识符。此标识符的最小值必须为 1。
9. 在 **密码属性类型** 中，键入 RADIUS 服务器在供应商特定的 AVP 代码中返回的属性类型。该值的范围为 1 到 255。
10. 在 **创建身份验证策略** 对话框中，在 **命名表达式** 旁边，选择表达式，单击 **添加表达式**，单击 **创建**，然后单击 **关闭**。

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

配置 SafeWord 身份验证

SafeWord 产品系列通过使用基于令牌的密码，有助于提供安全的身份验证。用户输入密码后，该密码会被 SafeWord 禁用，并且不能再次使用。

如果 NetScaler Gateway 正在 Secure Gateway 和 StoreFront 部署中替换 Secure Gateway，您可以选择不在 NetScaler Gateway 上配置身份验证，并继续允许 StoreFront 为传入的 HTTP 流量提供 SafeWord 身份验证。

NetScaler Gateway 支持以下产品的 SafeWord 身份验证：

- SafeWord 2008
- SafeWord PremierAccess
- SafeWord 适用于 Citrix®
- SafeWord RemoteAccess

您可以通过以下方式配置 NetScaler Gateway 以使用 SafeWord 产品进行身份验证：

- 配置身份验证以使用作为 SafeWord PremierAccess 一部分安装的 PremierAccess RADIUS 服务器，并允许其处理身份验证。
- 配置身份验证以使用 SafeWord IAS 代理，它是 SafeWord RemoteAccess、SafeWord for Citrix 和 SafeWord PremierAccess 4.0 的一个组件。
- 安装 SafeWord Web Interface 代理以支持 StoreFront。您无需在 NetScaler Gateway 上配置身份验证，StoreFront 可以处理此问题。此配置不使用 PremierAccess RADIUS 服务器或 SafeWord IAS 代理。

配置 SafeWord RADIUS 服务器时，您需要以下信息：

- NetScaler Gateway 的 IP 地址。在 RADIUS 服务器上配置客户端设置时，请使用 NetScaler Gateway 的 IP 地址。
- 共享密钥。
- SafeWord 服务器的 IP 地址和端口。

配置 Gemalto Protiva 身份验证

Protiva 是一个强大的身份验证平台，旨在利用 Gemalto 智能卡身份验证的优势而开发。通过 Protiva，用户可以使用用户名、密码以及由 Protiva 设备生成的一次性密码登录。与 RSA SecurID 类似，身份验证请求会发送到 Protiva 身份验证服务器，密码会经过验证或被拒绝。

要配置 Gemalto Protiva 以支持 NetScaler Gateway，请遵循以下准则：

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

- 安装 Protiva 服务器。
- 在 Microsoft IAS RADIUS 服务器上安装 Protiva Internet 身份验证服务器 (IAS) 代理插件。请务必记下 IAS 服务器的 IP 地址和端口号。

网关身份验证的 nFactor

nFactor 身份验证为身份验证带来了全新的可能性。使用 nFactor 的管理员在为虚拟服务器配置身份验证因子时，可享有身份验证、授权和审计的灵活性。

两个策略库或两个因子不再限制管理员。策略库的数量可以扩展以适应不同的需求。nFactor 根据先前的因子确定身份验证方法。通过使用 nFactor，可以实现动态登录表单和故障时操作。

重要提示：

- 从版本 13.0 build 67.x 开始，nFactor 身份验证仅在 Standard 许可证下支持网关/VPN 虚拟服务器，而不支持身份验证虚拟服务器。在 Standard 许可证中，nFactor 可视化工具 GUI 无法用于在 nFactor 流程中创建 EPA。此外，您不能编辑登录架构，而必须按原样使用开箱即用的登录架构。
- NetScaler 要支持 nFactor 身份验证，需要 Advanced 许可证或 Premium 许可证。有关 NetScaler nFactor 身份验证的更多信息，请参阅 nFactor 身份验证。

身份验证、授权和审计功能许可要求

下表列出了可用身份验证、授权和审计功能的许可要求。

	STANDARD 许可证	ADVANCED 许可证	PREMIUM 许可证
本地身份验证	是	是	是
LDAP 身份验证	是	是	是
RADIUS 身份验证	是	是	是
TACACS 身份验证	是	是	是
Web 身份验证	是	是	是
客户端证书身份验证	是	是	是

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

	STANDARD 许可证	ADVANCED 许可证	PREMIUM 许可证
协商身份验证	是	是	是
SAML 身份验证	是	是	是
OAuth 身份验证	否	是	是
本机 OTP	否	是	是
电子邮件 OTP	否	是	是
OTP 推送通知	否	否	是
基于知识的问题和答案（KBA 身份验证）	否	是	是
自助服务密码重置 (SSPR)	否	是	是
nFactor 可视化工具	是	是	是

注意

- 有关为 NetScaler Standard 许可证配置 nFactor 的步骤，请参阅 创建虚拟服务器 部分。
- 在 NetScaler Standard 许可证中，只有不可寻址的身份验证、授权和审计虚拟服务器才能绑定到 Gateway/VPN 虚拟服务器。
- NetScaler Standard 许可证不允许自定义 LoginSchema。nFactor 支持是基本的，仅包含设备附带的默认和已添加的登录架构。管理员可以在其配置中使用它们，但不能添加登录架构。因此，GUI 选项被禁用。

用例

nFactor 身份验证可根据用户配置文件启用动态身份验证流。有时，这些流程对用户来说可能简单直观。在其他情况下，它们可以与保护 Active Directory 或其他身份验证服务器结合使用。以下是 Gateway 的一些特定要求：

1. **动态用户名和密码选择。** 传统上，客户端（包括浏览器和接收器）使用 Active Directory (AD) 密码作为第一个密码字段。第二个密码保留用于一次性密码 (OTP)。但是，为了保护 AD 服务器，需要首先验证 OTP。nFactor 无需客户端修改即可完成此操作。

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

2. **多租户身份验证端点。** 一些组织对证书用户和非证书用户使用不同的 Gateway 服务器。随着用户使用自己的设备登录，用户在 NetScaler 设备上的访问级别会因所使用的设备而异。Gateway 可以满足不同的身份验证需求。
3. **基于组成员身份的身份验证。** 一些组织从 AD 服务器获取用户属性以确定身份验证要求。身份验证要求可能因个人用户而异。
4. **身份验证协同因素。** 有时，不同的身份验证策略对用于对不同的用户集进行身份验证。提供配对策略可提高有效身份验证。可以从一个流中创建依赖策略。通过这种方式，独立的策略集成为自己的流，从而提高效率并降低复杂性。

身份验证响应处理

NetScaler Gateway 回调注册处理身份验证响应。AAAD（身份验证守护程序）响应以及成功/失败/错误/对话代码被馈送到回调句柄。成功/失败/错误/对话代码指示 Gateway 采取适当的操作。

客户端支持

下表详细介绍了配置详细信息。

客户端	NFACTOR 支持	身份验证策略绑定点	EPA
浏览器	是	身份验证	是
Citrix Workspace 应用程序	是	VPN	是
Gateway 插件	是	VPN	是

注意：

- Citrix Workspace 应用程序支持以下列出的版本中受支持操作系统的 nFactor 身份验证。
  - Windows 4.12 版本
  - Linux 13.10 版本
  - Mac 1808
  - iOS 2007
  - 安卓 1808
  - HTML5: 通过 Store Web 支持
  - Chrome: 通过 Store Web 支持

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

WebView 凭据类型对身份验证机制的支持

注意：

阻止表达式（例如 ns 变量）在支持 WebView 的 VPN 会话策略中不受支持。有关阻止表达式的更多信息，请联系 Citrix 支持。

NetScaler 身份验证支持 AUTHv3 协议。AUTHv3 协议中的 WebView 凭据类型支持所有类型的身份验证机制（包括 SAML 和 OAuth）。WebView 凭据类型是 AUTHv3 的一部分，由 Citrix Workspace 应用程序和 Web 应用程序中的浏览器实现。

以下示例解释了 WebView 事件通过 NetScaler Gateway 和 Citrix Workspace 应用程序的流程：

1. Citrix Workspace 应用程序与 NetScaler Gateway 协商以支持 AUTHv3 协议。
2. NetScaler 做出积极响应并建议一个特定的起始 URL。
3. Citrix Workspace 应用程序然后连接到特定的端点 (URL)。
4. NetScaler Gateway 向客户端发送响应以启动 WebView。
5. Citrix Workspace 应用程序启动 WebView 并向 NetScaler 发送初始请求。
6. NetScaler 将 URI 重定向到浏览器登录端点。
7. 身份验证完成后，NetScaler 会向 WebView 发送完成响应。
8. WebView 现在退出，并将控制权交还给 Citrix Workspace 应用程序，以继续 AUTHv3 协议进行会话建立。

命令行配置

Gateway 虚拟服务器需要一个名为属性的身份验证虚拟服务器。作为属性的虚拟服务器名称是此模型所需的唯一配置。

```
add authnProfile <name-of-profile> -authnVsName <name-of-auth-vserver>
```

authnVsName 是身份验证虚拟服务器的名称。authnVsName 虚拟服务器必须配置高级身份验证策略，并用于 nFactor 身份验证。

```
add vpn vserver <name> <serviceType> <IP> <PORT> -authnProfile <name-of-profile>
```

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

```
set vpn vserver <name> -authnProfile <name-of-profile>
```

其中 authnProfile 是之前创建的身份验证配置文件。

互操作性挑战

大多数旧版 Gateway 客户端，除了 rfWeb 客户端之外，都是根据 Gateway 发送的响应建模的。例如，许多客户端都期望收到对 /vpn/index.html 的 302 响应。这些客户端还依赖于各种网关 Cookie，例如“`pwcount`”、“NSC_CERT。”

端点分析 (EPA)

nFactor 中的 EPA 不支持 NetScaler 身份验证、授权和审计模块。因此，NetScaler Gateway 虚拟服务器执行 EPA。EPA 后，登录凭据使用前面提到的 API 发送到身份验证虚拟服务器。身份验证完成后，Gateway 继续执行身份验证后过程并建立用户会话。

错误配置注意事项

Gateway 客户端仅发送一次用户凭据。Gateway 从客户端的登录请求中获取一个或两个凭据。在旧版模式下，最多有两个因素。获取的密码用于这些因素。然而，使用 nFactor，可以配置的因素数量实际上是无限的。从 Gateway 客户端获取的密码会根据配置重复用于已配置的因素。必须注意，一次性密码 (OTP) 不得重复使用多次。同样，管理员必须确保在某个因素处重复使用的密码确实适用于该因素。

定义客户端

提供此配置选项是为了帮助 NetScaler 区分浏览器客户端和 Receiver 等厚客户端。

提供了一个模式集 ns_vpn_client_useragents，供管理员配置所有客户端的模式。

同样，将“Citrix Receiver”字符串绑定到上述 `patset`，以忽略用户代理中包含“Citrix Receiver”的所有客户端。

重要提示：

从适用于 Android 24.08.1 的 Citrix Secure Access 开始，用于 nFactor 身份验证的 webview 中的 User-Agent 字符串格式更改如下：

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

`CitrixSecureAccess/CitrixVPN <version> (Linux; Android 14; Build/AP31.240426.023; wv) VpnCapable AuthV3Capable NAC/1.0 [ManagedVpn] [custom-user-agent]`

- 包含 `CitrixSecureAccess/CitrixVPN` 是为了向后兼容，用于识别 NetScaler Gateway 上的 Citrix Secure Access 客户端以筛选策略。
- `<version>` 字符串将替换为适用的应用程序/操作系统版本号。
- `ManagedVpn` 和 `custom-user-agent` 字符串是可选的。`ManagedVpn` 字符串仅包含在 MDM 部署的 VPN 中。`custom-user-agent` 字符串由 MDM 管理员在托管 VPN 配置中配置。

在以前的版本中，webview 中的 User-Agent 字符串包含旧版 Mozilla 或 WebKit 兼容性信息。

限制网关的 nFactor

如果存在以下条件，则不会发生网关身份验证的 nFactor。

1. authnProfile 未设置为 NetScaler Gateway。
2. 高级身份验证策略未绑定到身份验证虚拟服务器，并且在 `authnProfile` 中提到了相同的身份验证虚拟服务器。
3. HTTP 请求中的 User-Agent 字符串与 `patset` ns_vpn_client_useragents 中配置的 User-Agent 匹配。

如果这些条件不满足，则使用绑定到网关的经典身份验证策略。

如果用户代理或其一部分绑定到前面提到的 `patset`，则来自这些用户代理的请求不参与 nFactor 流程。例如，以下命令限制所有浏览器（假设所有浏览器在用户代理字符串中都包含“Mozilla”）的配置：

```
bind patset ns_vpn_client_useragents Mozilla
```

LoginSchema

LoginSchema 是登录表单的逻辑表示。它由 XML 语言定义。登录架构的语法符合 Citrix 的通用表单协议规范。

LoginSchema 定义了产品的“视图”。管理员可以提供表单的自定义描述、辅助文本等。登录架构包括表单本身的标签。客户可以提供描述在给定点呈现的表单的成功或失败消息。

使用以下命令配置登录架构。

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

```
add authentication loginSchema <name> -authenticationSchema <string> [-
userExpression <string>] [-passwdExpression <string>] [-
userCredentialIndex <positive_integer>]

[-passwordCredentialIndex <positive_integer>] [-authenticationStrength
<positive_integer>] [-SSOCredentials ( YES | NO )]
```

参数说明

- name - 新登录架构的名称。这是一个必填参数。最大长度：127
- authenticationSchema - 用于读取要发送到登录页面 UI 的身份验证架构的文件名。此文件包含根据 Citrix 表单身份验证协议定义的元素 XML 定义，以便能够呈现登录表单。如果管理员不想提示用户输入其他凭据，而是继续使用之前获得的凭据，则可以将 `noschema` 作为参数。这仅适用于与用户定义因素一起使用的 loginSchemas，而不适用于虚拟服务器因素。

这是一个必填参数。最大长度：255

- userExpression - 登录期间用于提取用户名的表达式。这可以是任何相关的高级策略表达式。最大长度：127
- passwdExpression - 登录期间用于提取密码的表达式。这可以是任何相关的先进策略表达式。最大长度：127
- userCredentialIndex - 用户输入的用户名必须存储在会话中的索引。最小值：1，最大值：16
- passwordCredentialIndex - 用户输入的密码必须存储在会话中的索引。最小值：1，最大值：16
- authenticationStrength - 当前身份验证的权重。最小值：0，最大值：65535
- `SSOCredentials` - 此选项指示当前因素凭据是否为默认 SSO（单点登录）凭据。可能的值：YES、NO。默认值：NO

LoginSchema 和 nFactor 知识要求

预构建的 loginSchema 文件位于以下 NetScaler 位置 **/nsconfig/loginschema/LoginSchema/**。这些预构建的 loginSchema 文件适用于常见用例，如有必要，可对其进行修改以适应细微变化。

此外，大多数具有少量自定义的单因素用例不需要登录架构配置。

建议管理员查阅文档，了解其他配置选项，这些选项使 NetScaler 能够发现因素。用户提交凭据后，管理员可以配置多个因素，以灵活选择和处理身份验证因素。

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

不使用 LoginSchema 配置双因素身份验证

NetScaler 根据配置自动确定双因素要求。用户提交这些凭据后，管理员可以在虚拟服务器上配置第一组策略。每个策略都可以配置一个“nextFactor”作为“passthrough”。“passthrough”意味着 NetScaler 必须使用现有凭据集处理登录，而无需用户干预。通过使用“passthrough”因素，管理员可以编程方式驱动身份验证流程。建议管理员阅读 nFactor 规范或部署指南以获取更多详细信息。请参阅 多因素 (nFactor) 身份验证。

用户名和密码表达式

为了处理登录凭据，管理员必须配置 loginSchema。具有少量 loginSchema 自定义的单因素或双因素用例不需要指定的 XML 定义。LoginSchema 还有其他属性，例如 userExpression 和 passwdExpression，可用于更改用户提供的用户名或密码。

登录架构是高级策略表达式，也可用于覆盖用户输入。这可以通过在 **-authenticationSchema** 的参数中附加字符串来实现，如以下示例所示。

以下是分别修改用户名和密码用户输入的示例。

- 将用户名的用户输入从 `username@citrix.com` 更改为 `username@xyz.com`

  ```
  add authentication loginSchema user_schema -authenticationSchema
  LoginSchema/DualAuth.xml -userExpression
  "AAA.LOGIN.USERNAME.BEFORE_STR(\"@\").APPEND(\"@xyz.com\")"
  ```

- 考虑这样一种情况：用户在第一个因素中提供了密码和通行码，作为已配置登录架构的一部分。要使用用户在第一个因素中提供的 **通行码** 和在第二个因素中提供的 **密码**，您可以使用以下命令修改现有登录架构。

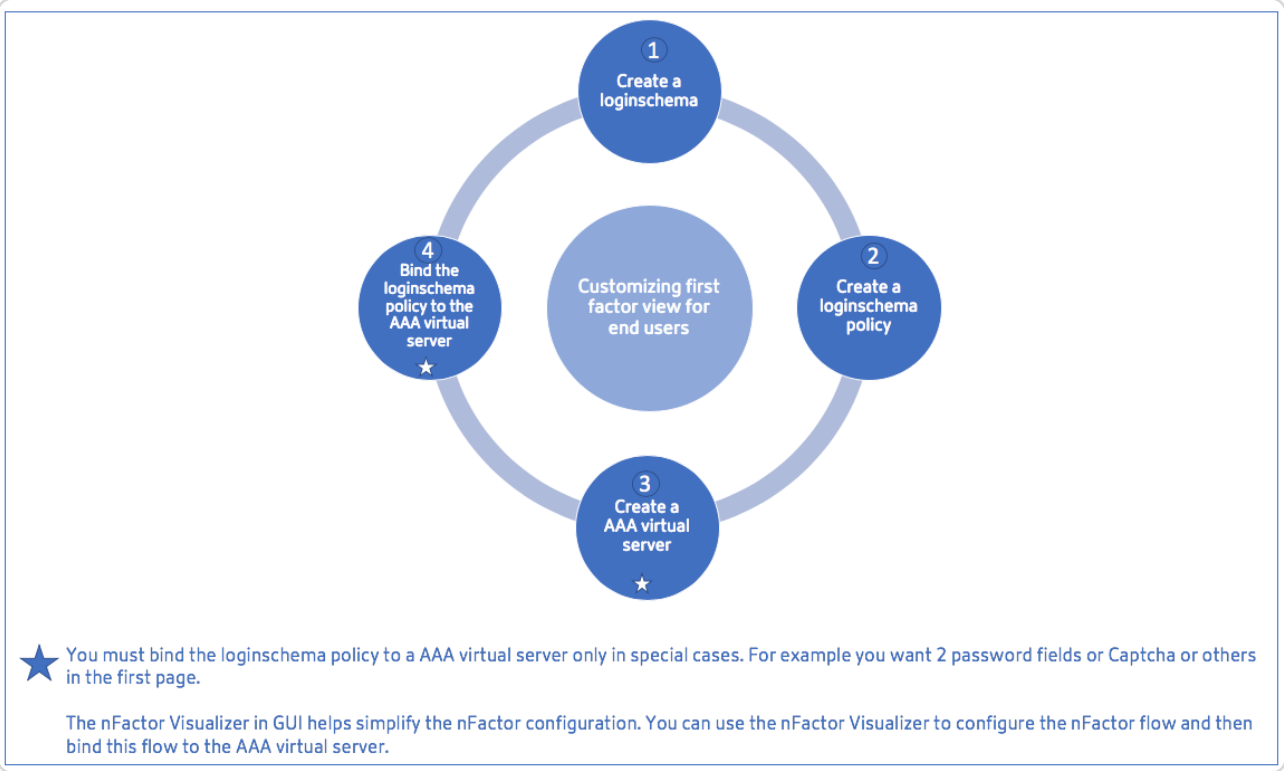
  ```
  add authentication loginSchema user_schema -authenticationSchema
  LoginSchema/DualAuth.xml -passwdExpression "AAA.LOGIN.PASSWORD2"
  ```

  ```
  add authentication loginSchema user_schema_second -authenticationSchema
  noschema  -passwdExpression "AAA.LOGIN.PASSWORD"
  ```

nFactor 配置中的高级步骤

下图说明了 nFactor 配置中涉及的高级步骤。

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



GUI 配置

本节介绍以下主题：

- 创建虚拟服务器
- 创建身份验证虚拟服务器
- 创建身份验证 CERT 配置文件
- 创建身份验证策略
- 添加 LDAP 身份验证服务器
- 添加 LDAP 身份验证策略
- 添加 RADIUS 身份验证服务器
- 添加 RADIUS 身份验证策略
- 创建身份验证登录架构
- 创建策略标签

创建虚拟服务器

1. 导航到 **NetScaler Gateway > 虚拟服务器**。
2. 单击 **添加**按钮以创建网关虚拟服务器。
3. 输入以下信息，然后单击 **确定**。

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

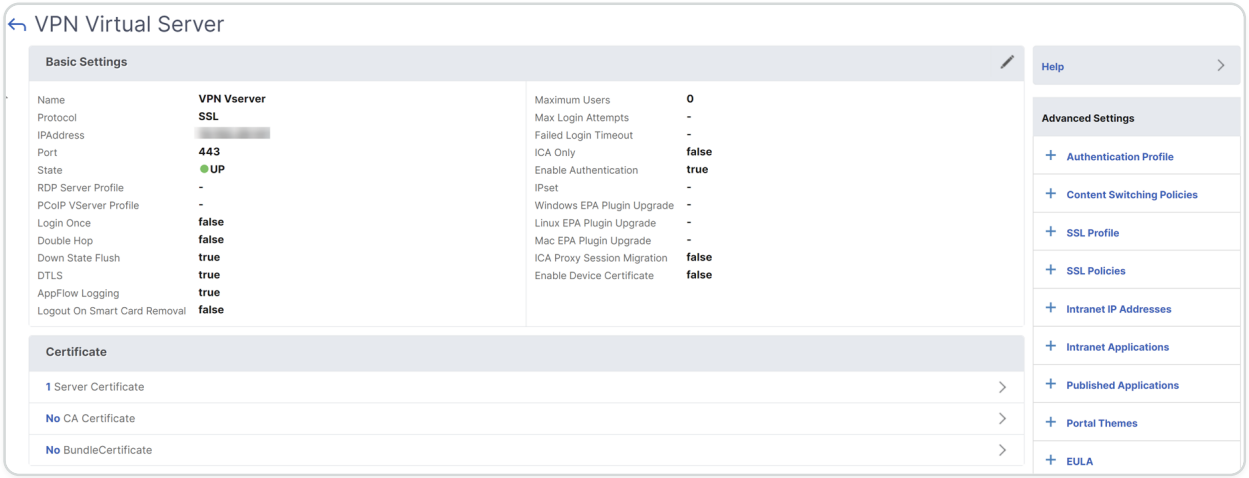
参数名称	参数说明
名称	NetScaler Gateway 虚拟服务器的名称。必须以 ASCII 字母或下划线 (_) 字符开头，并且只能包含 ASCII 字母数字、下划线、哈希 (#)、句点 (.)、空格、冒号 (:)、at (@)、等号 (=) 和连字符 (-) 字符。创建虚拟服务器后可以更改。以下要求仅适用于 NetScaler CLI：如果名称包含一个或多个空格，请将名称用双引号或单引号括起来（例如，“my server”或“my server”）。
IP 地址类型	从下拉菜单中选择 **IP 地址** 或 **不可寻址** 选项。
IP 地址	Internet 协议地址 (IP 地址) 是分配给参与计算机网络的每个设备的数字标签，该网络使用 Internet 协议进行通信。
端口	输入虚拟服务器的端口号。
RDP 服务器配置文件	与虚拟服务器关联的 RDP 服务器配置文件的名称。
PCoIP 虚拟服务器配置文件	与虚拟服务器关联的 PCoIP 虚拟服务器配置文件的名称。
最大用户数	此虚拟服务器上允许的最大并发用户会话数。允许登录此虚拟服务器的实际用户数取决于用户许可证总数。
最大登录尝试次数	最大登录尝试次数。
登录失败超时	如果用户超出最大允许尝试次数，帐户将被锁定的分钟数。
Windows EPA 插件升级	用于设置 Windows 客户端插件升级行为的选项。
Linux EPA 插件升级	用于设置 Linux 客户端插件升级行为的选项。
	>注意：

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

参数名称	参数说明
	>- 对于 eLux 和 IGEL OS，此参数必须始终设置为 **从不**。
	>- Citrix Secure Access 客户端 for Linux 不支持 **Essential** 选项。
Mac EPA 插件升级	用于设置 macOS 客户端插件升级行为的选项。
一次登录	此选项用于为此虚拟服务器启用或禁用无缝 SSO。
仅限 ICA	- 当设置为 **ON** 时，表示基本模式，用户可以使用 Citrix Workspace 应用程序或浏览器登录，并访问 `Wihome` 参数指向的 Citrix Virtual Apps and Desktops 环境中配置的已发布应用程序。用户不允许使用 Citrix Secure Access 客户端连接，并且无法配置端点扫描。在此模式下，可以登录和访问应用程序的用户数量不受许可证限制。
	- 当设置为 **OFF** 时，表示 SmartAccess 模式，用户可以使用 Citrix Workspace 应用程序、浏览器或 Citrix Secure Access 客户端登录。管理员可以配置在客户端系统上运行端点扫描，然后使用结果来控制对已发布应用程序的访问。在此模式下，客户端可以以其他客户端模式（即 VPN 和无客户端 VPN）连接到网关。在此模式下，可以登录和访问资源的用户数量受 CCU 许可证限制。
启用身份验证	要求连接到 NetScaler Gateway 的用户进行身份验证。
双跳	在双跳配置中使用 NetScaler Gateway。双跳部署通过使用三个防火墙将 DMZ 分为两个阶段，为内部网络提供了额外的安全层。此类部署可以在 DMZ 中部署一个设备，在安全网络中部署一个设备。

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

参数名称	参数说明
关闭状态刷新	当虚拟服务器被标记为 DOWN 时（这意味着服务器可能已超时），关闭现有连接。断开现有连接可以释放资源，在某些情况下可以加快过载负载平衡设置的恢复。在连接可以安全关闭的服务器上启用此设置。不要在必须完成其事务的服务器上启用 DOWN 状态刷新。
DTLS	此选项启动或停止虚拟服务器上的 turn 服务
AppFlow 日志记录	记录包含标准 NetFlow 或 IPFIX 信息的 AppFlow 记录，例如流的开始和结束时间戳、数据包计数和字节计数。还记录包含应用程序级别信息的记录，例如 HTTP 网址、HTTP 请求方法和响应状态码、服务器响应时间以及延迟。
ICA 代理会话迁移	此选项确定当用户从另一台设备登录时，是否传输现有 ICA 代理会话。
状态	虚拟服务器的当前状态，例如 UP、DOWN、BUSY 等。
启用设备证书	指示作为 EPA 的一部分的设备证书检查是启用还是禁用。



4. 选择页面中的**无服务器证书**部分。
5. 在**选择服务器证书**下单击 **>** 以选择服务器证书。
6. 选择 SSL 证书，然后单击**选择**按钮。

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

7. 单击**绑定**。
8. 如果您看到关于 **无可用密码** 的警告，请单击 **确定**
9. 单击 **继续** 按钮。
10. 在“身份验证”部分，单击右上角的 **+** 图标。

创建身份验证虚拟服务器

1. 导航到 **安全 > AAA – 应用程序流量 > 虚拟服务器。**
2. 单击 **添加** 按钮。
3. 完成以下基本设置以创建身份验证虚拟服务器。

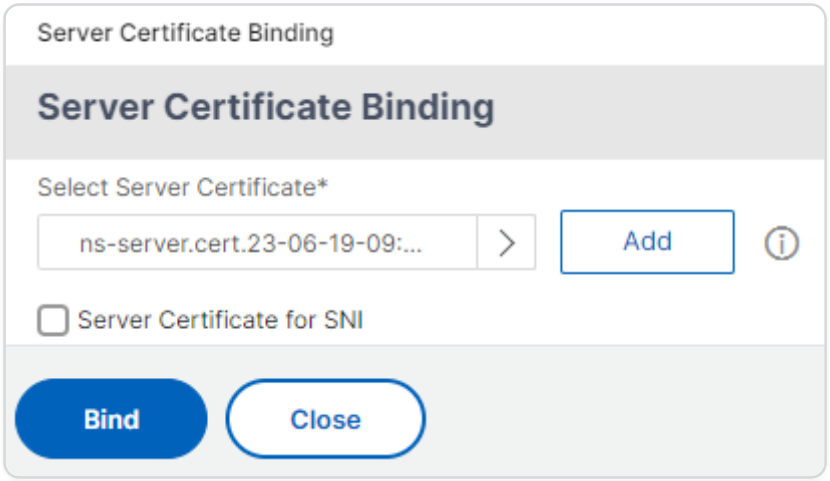
   注意： 设置名称右侧的 * 符号表示必填字段。

   - 输入新身份验证虚拟服务器的 **名称**。
   - 输入 **IP 地址类型**。IP 地址类型可以配置为不可寻址。
   - 输入 **IP 地址**。IP 地址可以为零。
   - 输入身份验证虚拟服务器的 **协议** 类型。
   - 输入虚拟服务器接受连接的 **TCP 端口**。
   - 输入身份验证虚拟服务器设置的身份验证 Cookie 的 **域**。
4. 单击 **确定**。
5. 单击“**无服务器证书**”部分。
6. 在“**选择服务器证书**”下单击“**>**”。
7. 选择所需的 SSL 证书，然后单击“**选择**”按钮。

   注意：身份验证虚拟服务器不需要绑定证书。
8. 配置“**服务器证书绑定**”。

   - 选中“**用于 SNI 的服务器证书**”复选框，以绑定用于 SNI 处理的一个或多个证书密钥。
   - 单击“**绑定**”按钮。

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



创建身份验证 CERT 配置文件

1. 导航到“**安全 > AAA – 应用程序流量 > 策略 > 身份验证 > 基本策略 > CERT。**”.
2. 选择“配置文件”选项卡，然后选择“**添加**”。
3. 填写以下字段以创建身份验证 CERT 配置文件。设置名称右侧的 * 符号表示必填字段。
   - **名称** - 客户端证书身份验证服务器配置文件（操作）的名称。
   - **双因素** – 在此实例中，双因素身份验证选项为 NOOP。
   - **用户名字段** – 输入从中提取用户名的客户端证书字段。必须设置为“"Subject"”或“"Issuer"”（包括两组双引号）。
   - **组名字段** - 输入从中提取组的客户端证书字段。必须设置为“"Subject"”或“"Issuer"”（包括两组双引号）。
   - **默认身份验证组** - 这是除了提取的组之外，身份验证成功时选择的默认组。
4. 单击**创建**。

创建身份验证策略

注意

如果使用 AAA.login 配置具有策略规则的第一因子策略，则必须为 Citrix Workspace 应用程序配置以下带有 OR 条件的表达式，以支持 nFactor 部署。

```
|| HTTP.REQ.URL.CONTAINS("/cgi/authenticate")
```

1. 导航到**安全 > AAA – 应用程序流量 > 策略 > 身份验证 > 高级策略 > 策略**。
2. 选择**添加**按钮

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

3. 填写以下信息以创建身份验证策略。设置名称右侧的 * 号表示必填字段。

   a) **名称** – 输入高级身份验证策略的名称。必须以字母、数字或下划线字符 (_) 开头，并且只能包含字母、数字、连字符 (-)、句点 (.)、井号 (#)、空格 ()、at (@)、等号 (=)、冒号 (:) 和下划线字符。身份验证策略创建后无法更改。

   以下要求仅适用于 NetScaler CLI：如果名称包含一个或多个空格，请将名称用双引号或单引号括起来（例如，“my authentication policy”或 'my authentication policy'）。

   b) **操作类型** - 输入身份验证操作的类型。

   c) **操作** - 输入如果策略匹配要执行的身份验证操作的名称。

   d) **日志操作** - 输入当请求与此策略匹配时要使用的消息日志操作的名称。

   e) **表达式** - 输入 NetScaler 命名规则的名称，或默认语法表达式，策略使用该规则来确定是否尝试使用身份验证服务器对用户进行身份验证。

   f) **注释** – 输入任何注释以保留有关此策略的信息。

4. 单击**创建**

添加 LDAP 身份验证服务器

1. 导航到 **安全 > AAA – 应用程序流量 > 策略 > 身份验证 > 基本策略 > LDAP。**
2. 通过选择**服务器**选项卡并选择**添加**按钮来添加 LDAP 服务器。

添加 LDAP 身份验证策略

1. 转到 **安全 > AAA – 应用程序流量 > 策略 > 身份验证 > 高级策略 > 策略**。
2. 单击**添加**以添加身份验证策略。
3. 填写以下信息以创建身份验证策略。设置名称右侧的 * 号表示必填字段。

   a) **名称** - 高级身份验证策略的名称。 必须以字母、数字或下划线字符 (_) 开头，并且只能包含字母、数字、连字符 (-)、句点 (.)、井号 (#)、空格 ()、at (@)、等号 (=)、冒号 (:) 和下划线字符。身份验证策略创建后无法更改。

   以下要求仅适用于 NetScaler CLI：如果名称包含一个或多个空格，请将名称用双引号或单引号括起来（例如，“my authentication policy”或 'my authentication policy'）。

   b) **操作类型** - 身份验证操作的类型。

   c) **操作** - 如果策略匹配，要执行的身份验证操作的名称。

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

d) **日志操作** - 当请求与此策略匹配时要使用的消息日志操作的名称。

e) **表达式** - NetScaler 命名规则的名称，或默认语法表达式，策略使用它来确定是否尝试使用身份验证服务器对用户进行身份验证。

f) **注释** - 用于保留有关此策略信息的任何注释。

4. 单击 **创建。**

添加 RADIUS 身份验证服务器

1. 导航到 **安全 > AAA – 应用程序流量 > 策略身份验证 > 基本策略 > RADIUS**。
2. 要添加服务器，请选择 **服务器** 选项卡，然后选择 **添加** 按钮。
3. 输入以下内容以创建身份验证 RADIUS 服务器。设置名称右侧的 * 符号表示必填字段。

   a. 输入 RADIUS 操作的 **名称**。

   b. 输入分配给 RADIUS 服务器的 **服务器名称** 或 **服务器 IP** 地址。

   c. 输入 RADIUS 服务器侦听连接的 **端口** 号。

   d. 输入 **超时** 值（秒）。NetScaler 设备会等待 RADIUS 服务器的响应，直到配置的超时值过期。

   e. 输入 RADIUS 服务器和 NetScaler 设备之间共享的 **密钥**。需要密钥才能允许 NetScaler 设备与 RADIUS 服务器通信。

   f. **确认密钥**。

4. 单击 **创建。**

添加 RADIUS 身份验证策略

1. 导航到 **安全 > AAA – 应用程序流量 > 策略 > 身份验证 > 高级策略 > 策略。**
2. 单击 **添加** 以创建身份验证策略。
3. 填写以下信息以创建身份验证策略。设置名称右侧的 * 符号表示必填字段。

   a. **名称** - 高级身份验证策略的名称。 必须以字母、数字或下划线字符 (_) 开头，并且只能包含字母、数字、连字符 (-)、句点 (.)、井号 (#)、空格 ()、at (@)、等号 (=)、冒号 (:) 和下划线字符。身份验证策略创建后无法更改。

   以下要求仅适用于 NetScaler CLI：如果名称包含一个或多个空格，请将名称用双引号或单引号括起来（例如，“my authentication policy”或 'my authentication policy'）。

   a. **操作类型** - 身份验证操作的类型。

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

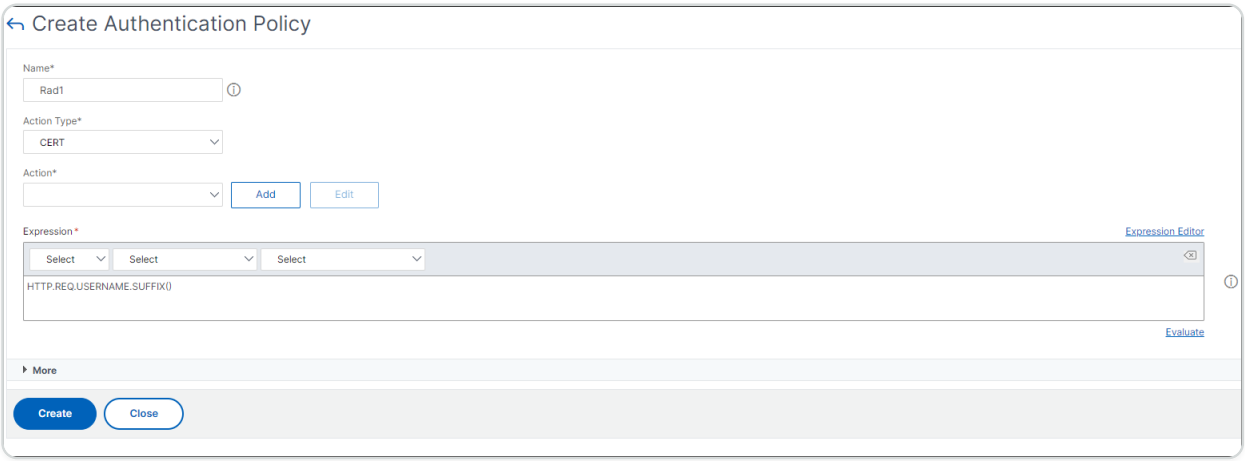
b. **操作** - 如果策略匹配，则执行的身份验证操作的名称。

c. **日志操作** - 当请求与此策略匹配时要使用的消息日志操作的名称。

d. **表达式** - NetScaler 命名规则的名称，或策略用于确定是否尝试使用身份验证服务器对用户进行身份验证的默认语法表达式。

e. **注释** - 用于保留有关此策略信息的任何注释。

4. 单击 **确定**。您创建的身份验证策略将列在策略列表中。



创建身份验证登录架构

1. 导航到 **安全 > AAA – 应用程序流量 > 登录架构。**
2. 选择“配置文件”选项卡，然后单击 **添加** 按钮。
3. 填写以下字段以创建身份验证登录方案：

   a. 输入 **名称** – 新登录方案的名称。

   b. 输入 **身份验证方案** - 用于读取要发送到登录页面 UI 的身份验证方案的文件名。此文件必须包含根据 Citrix 表单身份验证协议的元素 XML 定义，才能呈现登录表单。如果管理员不想提示用户输入更多凭据，而是继续使用之前获得的凭据，则可以将“`noschema`”作为参数。这仅适用于与用户定义因素一起使用的登录方案，而不适用于虚拟服务器因素

   c. 输入 **用户表达式** - 登录期间用于提取用户名的表达式

   d. 输入 **密码表达式** - 登录期间用于提取密码的表达式

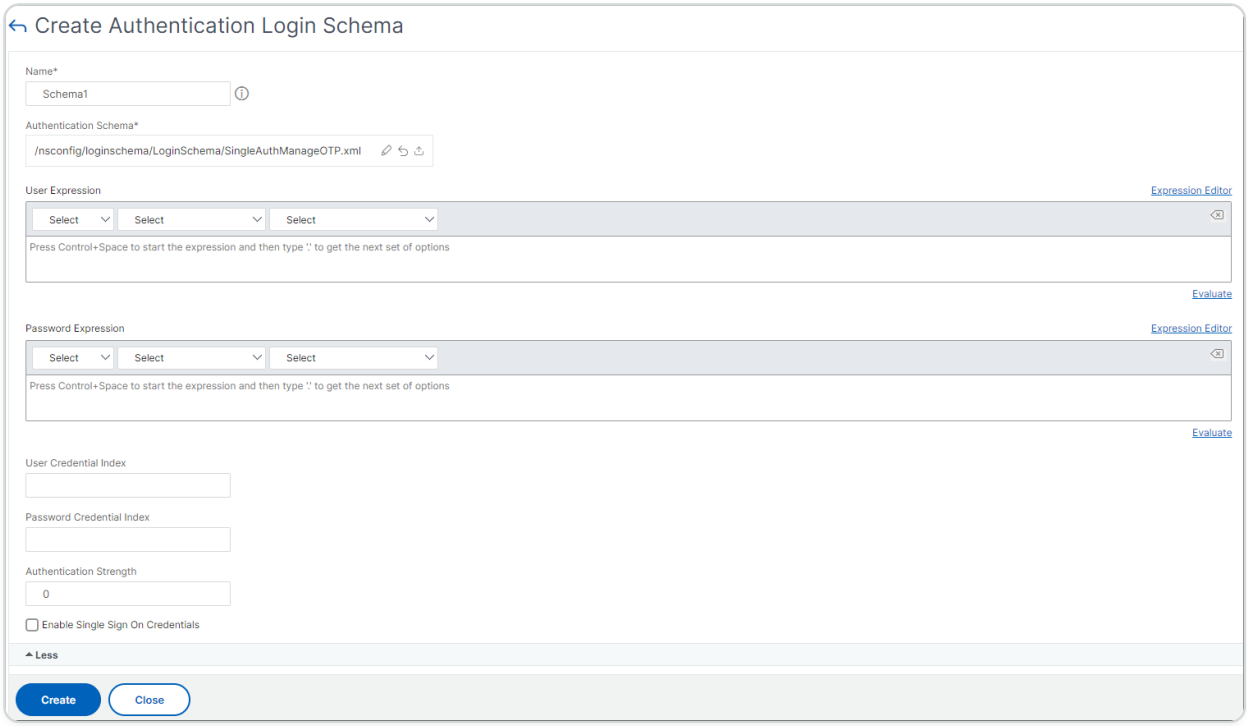
   e. 输入 **用户凭据索引** - 用户输入的用户名在会话中存储的索引。

   f. 输入 **密码凭据索引** - 用户输入的密码必须在会话中存储的索引。

   g. 输入 **身份验证强度** - 当前身份验证的权重。

4. 单击 **创建**。您创建的登录方案配置文件必须显示在登录方案配置文件列表中。

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

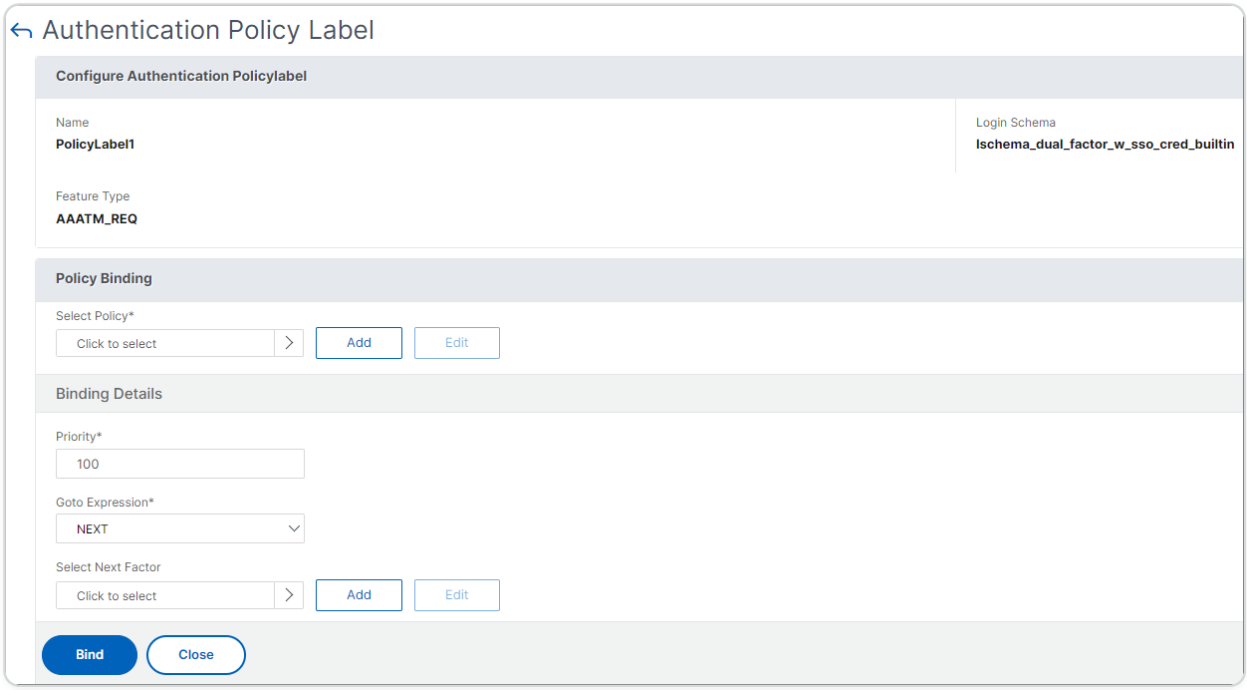


创建策略标签

策略标签指定特定因素的身份验证策略。每个策略标签对应一个因素。策略标签指定必须向用户呈现的登录表单。策略标签必须绑定为身份验证策略或另一个身份验证策略标签的下一个因素。通常，策略标签包含特定身份验证机制的身份验证策略。但是，您也可以拥有包含不同身份验证机制的身份验证策略的策略标签。

1. 导航到 **安全 > AAA – 应用程序流量 > 策略 > 身份验证 > 高级策略 > 策略标签。**
2. 单击 **添加** 按钮。
3. 填写以下字段以创建身份验证策略标签：
   a. 输入新的身份验证策略标签的**名称**。
   b. 输入与身份验证策略标签关联的**登录架构**。
   c. 单击**继续**。
4. 从下拉菜单中**选择策略**。
5. 选择所需的**身份验证策略**，然后单击**选择**按钮。
6. 填写以下字段：
   a. 输入策略绑定的**优先级**。
   b. 输入**Goto 表达式**——该表达式指定了如果当前策略规则评估为 TRUE，则将评估的下一个策略的优先级。

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



7. 选择所需的身份验证策略，然后单击**选择**按钮。
8. 单击**绑定**按钮。
9. 单击**完成**。
10. 查看身份验证策略标签。

用于 nFactor 身份验证的 re-Captcha 配置

从 NetScaler 12.1 版本 build 50.x 开始，NetScaler Gateway 支持一个新的第一类操作 'captchaAction'，它简化了 Captcha 配置。由于 Captcha 是一种第一类操作，它可以成为一个独立的因素。您可以在 nFactor 流程中的任何位置注入 Captcha。

以前，您必须编写自定义的 WebAuth 策略，并同时更改 RfWebUI。随着 captchaACtion 的引入，您无需修改 JavaScript。

从 NetScaler 14.1 版本 build 47.46 开始，nFactor 身份验证除了支持 re-Captcha v2 外，还支持 Google re-Captcha v3。Google re-Captcha v3 提供了一种高级身份验证方法，该方法无需用户交互即可评估登录请求。它为每个请求分配一个介于 0.0 和 1.0 之间的分数，分数越高表示请求越安全。NetScaler 随后可以使用此分数来确定是否对用户进行身份验证。

从 14.1 版本 build 51.x 开始，NetScaler 支持 Google re-Captcha v3 Enterprise 控制台。以前，re-Captcha v3 支持仅限于 Admin 控制台，该控制台对可处理的请求数量有固定限制。相比之下，Enterprise 控制台允许根据订阅计划增加请求限制。

NetScaler 目前支持以下 re-Captcha 配置：

- 用于 Admin 控制台的 re-Captcha v2

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

- 用于 Admin 控制台的 re-Captcha v3
- 用于 Enterprise 控制台的 re-Captcha v3

重要提示：

如果 re-Captcha 与架构中的用户名或密码字段一起使用，则在满足 re-Captcha 要求之前，**登录**按钮将处于禁用状态。

re-Captcha 配置

re-Captcha 配置包括两个部分。

1. 在 Google 上注册 re-Captcha 的配置。
2. 在 NetScaler 上使用 re-Captcha 作为登录流程一部分的配置。

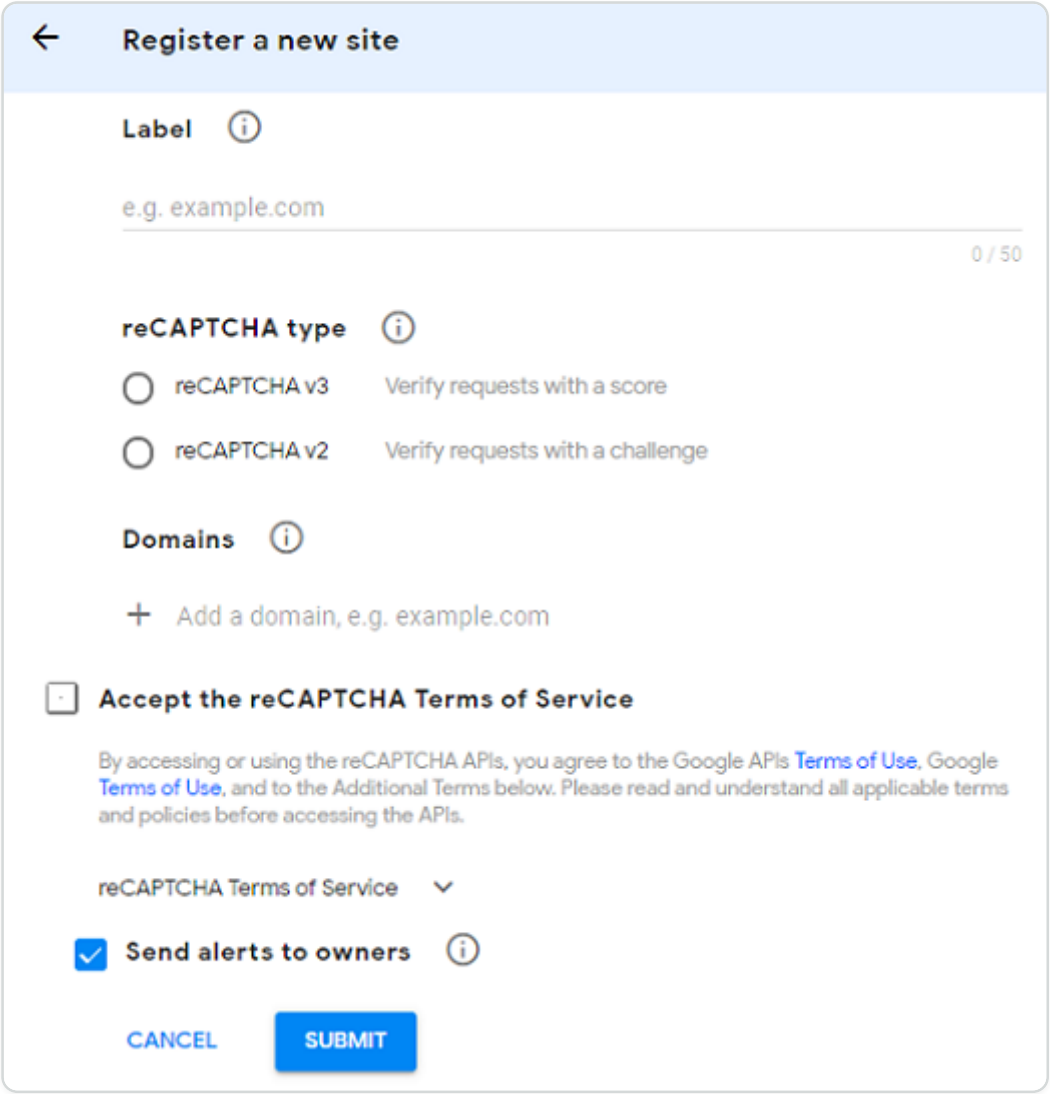
Google 上的 re-Captcha 配置

ADMIN 控制台的 RE-CAPTCHA 配置（RE-CAPTCHA V2 和 V3）

在 `<https://www.google.com/recaptcha/admin#llist>` 注册 re-Captcha 域。

1. 当您导航到此页面时，将显示以下屏幕。

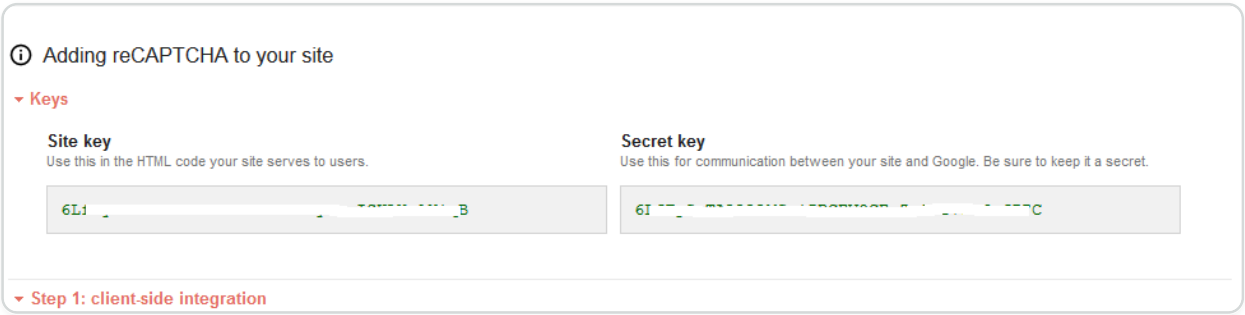
© 1997–2026 Citrix Systems, Inc. All rights reserved.



注意

对于 NetScaler 14.1 版本 build 47.46 及更高版本，请根据需要选择 **reCAPTCHA v2** 或 **reCAPTCHA v3**。以前的版本仅支持 **reCAPTCHA v2**。

2. 注册域后，将显示“SiteKey”和“SecretKey”。记下显示的“SiteKey”和“SecretKey”。



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

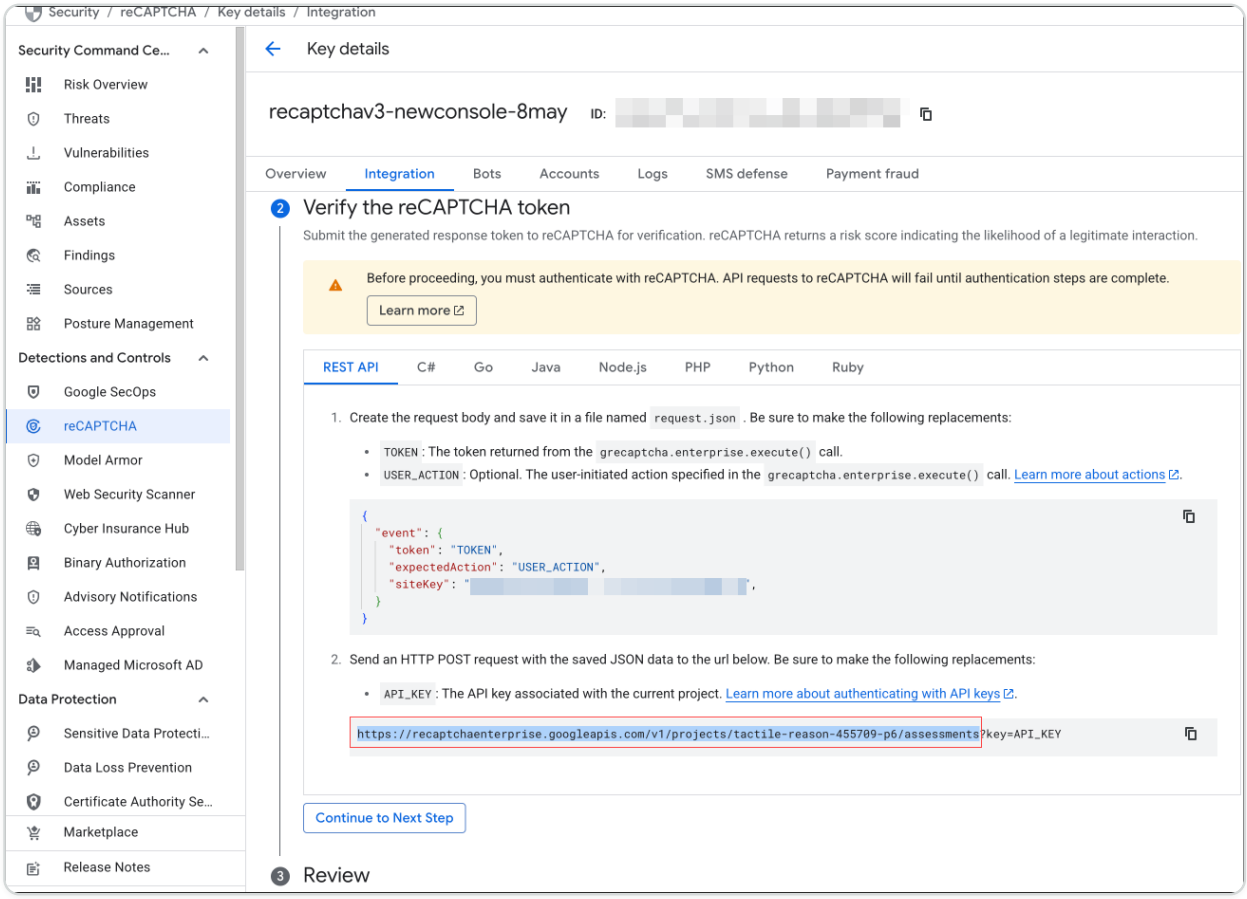
注意

出于安全原因，“SiteKey”和“SecretKey”显示为灰色。“SecretKey”必须妥善保管。

企业控制台的 RE-CAPTCHA 配置 (RE-CAPTCHA V3)

1. 使用 Gmail 帐户登录 `<https://console.cloud.google.com/>` 并创建一个项目。
2. 转到 `<https://console.cloud.google.com/security/recaptcha>` 并创建站点密钥。记下创建的站点密钥。有关更多信息，请参阅 Google re-Captcha 文档。
3. 转到 `<https://console.cloud.google.com/apis/>` 并创建 API 密钥。记下创建的 API 密钥。有关更多信息，请参阅 Google re-Captcha 文档。
4. 转到 `<https://console.cloud.google.com/security/recaptcha>` 并从评估 API 复制服务器 URL（复制到“assessments”一词）。保存复制的服务器 URL。

   例如，如果评估 API 是“`<https://recaptchaenterprise.googleapis.com/v1/projects/tactile-reason-455709-p6/assessments?key=API_KEY>`”，则必须复制到“assessments”的部分，即“`<https://recaptchaenterprise.googleapis.com/v1/projects/tactile-reason-455709-p6/assessments>`”。此提取的 URL 用作 `captchaAction` 命令中的服务器 URL。



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

NetScaler 上的 re-Captcha 配置

NetScaler 上的 re-Captcha 配置可分为三个部分：

- 显示 re-Captcha 屏幕
- 将 re-Captcha 响应发布到 Google 服务器
- 将 LDAP 配置为用户登录的第二个因素

显示 RE-CAPTCHA 屏幕

登录表单自定义通过以下登录架构完成：

- `SingleAuthCaptcha.xml` 用于管理员控制台的 re-Captcha v2
- `SingleAuthCaptchav3.xml` 用于管理员控制台的 re-Captcha v3
- `SingleAuthReCaptchav3Enterprise.xml` 用于企业控制台的 re-Captcha v3

自定义在身份验证虚拟服务器中指定，并发送到 UI 以呈现登录表单。内置登录架构位于 NetScaler 上的 `/nsconfig/loginSchema/LoginSchema` 目录中。

重要提示：

- 当 LDAP 配置为第二个因素时，可以使用登录架构。
- 您可以根据您的用例自定义现有架构。例如，您可以修改它以仅包含 re-Captcha 因素（不含用户名或密码）或使用 re-Captcha 进行双重身份验证。
- 如果进行了任何自定义修改或文件被重命名，我们建议将所有 loginSchemas 从 `/nsconfig/loginschema/LoginSchema` 目录复制到父目录 `/nsconfig/loginschema`。

使用 CLI 配置 RE-CAPTCHA 的显示

验证码 第二版：

```
add authentication loginSchema singleauthcaptcha -authenticationSchema /
nsconfig/loginschema/SingleAuthCaptcha.xml



add authentication loginSchemaPolicy singleauthcaptcha -rule true -action
singleauthcaptcha
```

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

```
add authentication vserver auth SSL <IP> <Port>


add ssl certkey vserver-cert -cert <path-to-cert-file> -key <path-to-key-
file>


bind ssl vserver auth -certkey vserver-cert


bind authentication vserver auth -policy singleauthcaptcha -priority 5
-gotoPriorityExpression END
```

re-Captcha v3 版本：

```
add authentication loginSchema singleauthcaptcha -authenticationSchema /
nsconfig/loginschema/SingleAuthCaptchav3.xml


add authentication loginSchemaPolicy singleauthcaptcha -rule true -action
singleauthcaptcha


add authentication vserver auth SSL <IP> <Port>


add ssl certkey vserver-cert -cert <path-to-cert-file> -key <path-to-key-
file>


bind ssl vserver auth -certkey vserver-cert
```

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

```
bind authentication vserver auth -policy singleauthcaptcha -priority 5
-gotoPriorityExpression END
```

在上述命令中，对 `<login_schema>` 参数使用以下登录架构：

- 用于管理员控制台的 re-Captcha v2 的 `SingleAuthCaptcha.xml`
- 用于管理员控制台的 re-Captcha v3 的 `SingleAuthCaptchav3.xml`
- 用于企业控制台的 re-Captcha v3 的 `SingleAuthReCaptchav3Enterprise.xml`

将 RE-CAPTCHA 响应发布到 GOOGLE 服务器

配置好必须向用户显示的 re-Captcha 后，管理员会将配置添加到 Google 服务器，以验证来自浏览器的 re-Captcha 响应。

先决条件：

NetScaler 联系 `<https://www.google.com/recaptcha/api/siteverify>` 以验证 Captcha 信息。因此，请确保 NetScaler 可以访问该站点。

要验证 Google 站点是否可访问，请运行以下脚本：

`curl -vvv https://www.google.com/recaptcha/api/siteverify`

NetScaler 联系 `<https://www.google.com/recaptcha/api/siteverify>` 以验证 Captcha 信息。
验证来自浏览器的 re-Captcha 响应以用于管理控制台
在 Google 服务器中注册域时生成的“SiteKey”和“SecretKey”必须用于以下 CLI 命令中。

re-Captcha v2 版本：

```
add authentication captchaAction myrecaptcha -sitekey <sitekey-copied-
from-google> -secretkey <secretkey-from-google>



add authentication policy myrecaptcha -rule true -action myrecaptcha



bind authentication vserver auth -policy myrecaptcha -priority 1
```

re-Captcha 版本 3：

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

```
add authentication captchaAction -siteKey <sitekey> -secretKey <secretKey>
-scoreThreshold <0 to 10>



add authentication policy myrecaptcha -rule true -action myrecaptcha



bind authentication vserver auth -policy myrecaptcha -priority 1
```

`scoreThreshold` 的默认值为 5。

验证来自浏览器的 re-Captcha 响应以用于企业控制台

在 Google 服务器中注册域时生成的“站点密钥”、“API 密钥”和“服务器 URL”必须用于以下 CLI 命令中：

```
add authentication captchaAction -siteKey <sitekey> -secretKey <APIkey>
-scoreThreshold<0 - 10> -serverurl <serverURL>



add authentication policy myrecaptcha -rule true -action myrecaptcha



bind authentication vserver auth -policy myrecaptcha -priority 1
```

`scoreThreshold` 的默认值为 5。

将 LDAP 配置为用户登录的第二个因素

注意：

如果不需要 LDAP 身份验证，请自定义以下登录架构以删除用户名和密码标签：

- 用于管理控制台的 re-Captcha v2 的 `SingleAuthCaptcha.xml`
- 用于管理控制台的 re-Captcha v3 的 `SingleAuthCaptchav3.xml`
- 用于企业控制台的 re-Captcha v3 的 `SingleAuthReCaptchav3Enterprise.xml`

如果您将 LDAP 身份验证添加为第二个因素，它将在 re-Captcha 之后发生。

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

```
add authentication ldapAction ldap-new -serverIP x.x.x.x -serverPort 636
-ldapBase "cn=users,dc=aaatm,dc=com" -ldapBindDn adminuser@aaatm.com
-ldapBindDnPassword <password> -encrypted -encryptmethod ENCMTHD_3
-ldapLoginName sAMAccountName -groupAttrName memberof -subAttributeName CN
-secType SSL -passwdChange ENABLED -defaultAuthenticationGroup ldapGroup



add authenticationpolicy ldap-new -rule true -action ldap-new



add authentication policylabel second-factor



bind authentication policylabel second-factor -policy ldap-new -priority
10



bind authentication vserver auth -policy myrecaptcha -priority 1
-nextFactor second-factor
```

管理员必须根据是使用负载平衡虚拟服务器还是 NetScaler Gateway 进行访问来添加适当的虚拟服务器。如果需要负载平衡虚拟服务器，管理员必须配置以下命令：

```
add lb vserver lbtest HTTP <IP> <Port> -authentication ON
-authenticationHost nssp.aaatm.com
```

`**nssp.aaatm.com**` â€“ 解析为身份验证虚拟服务器。

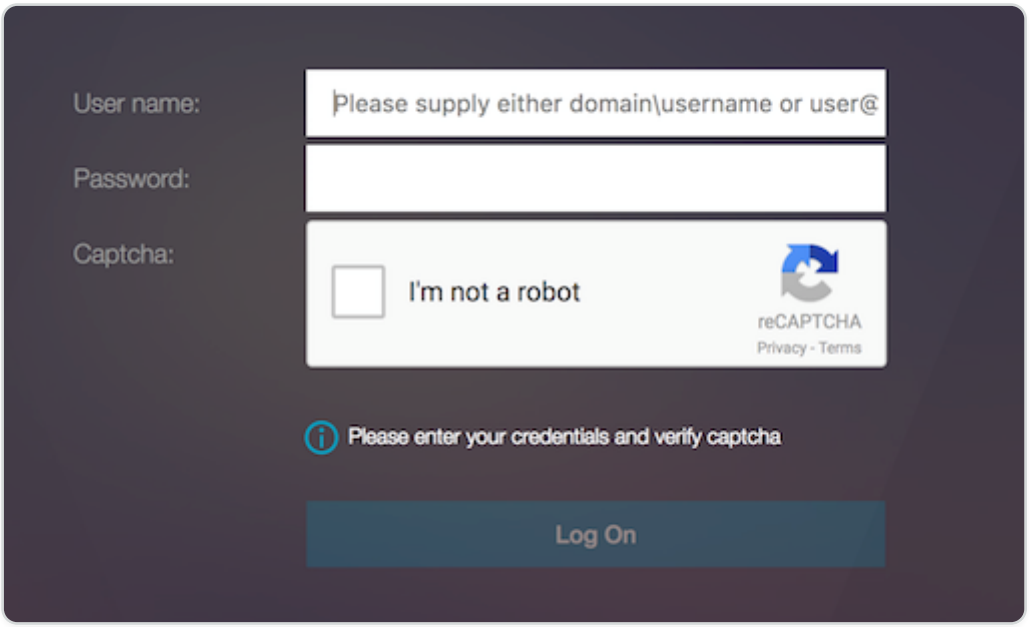
RE-CAPTCHA 的用户验证

re-Captcha 第二版：

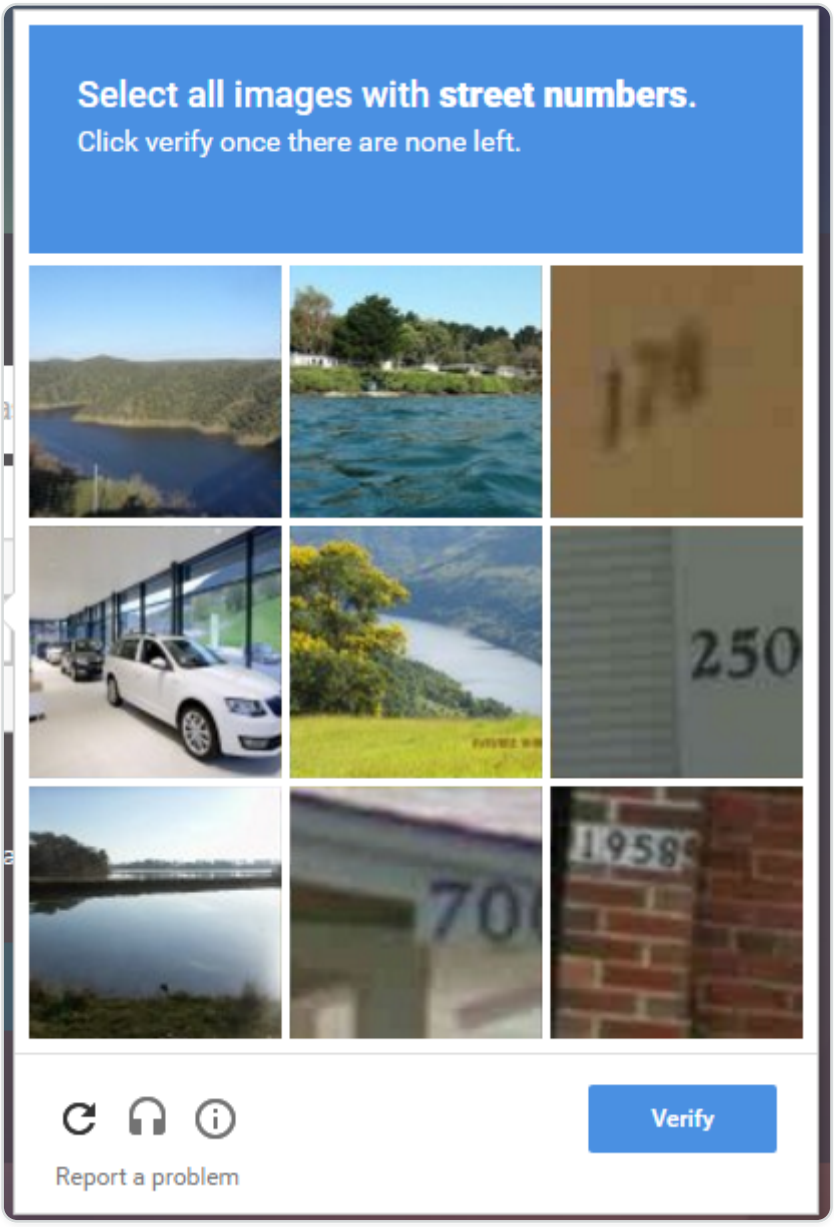
配置 re-Captcha 后，您将看到以下 UI。

1. 身份验证虚拟服务器加载登录页面后，将显示登录屏幕。在 re-Captcha 完成之前，**登录**按钮处于禁用状态。

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

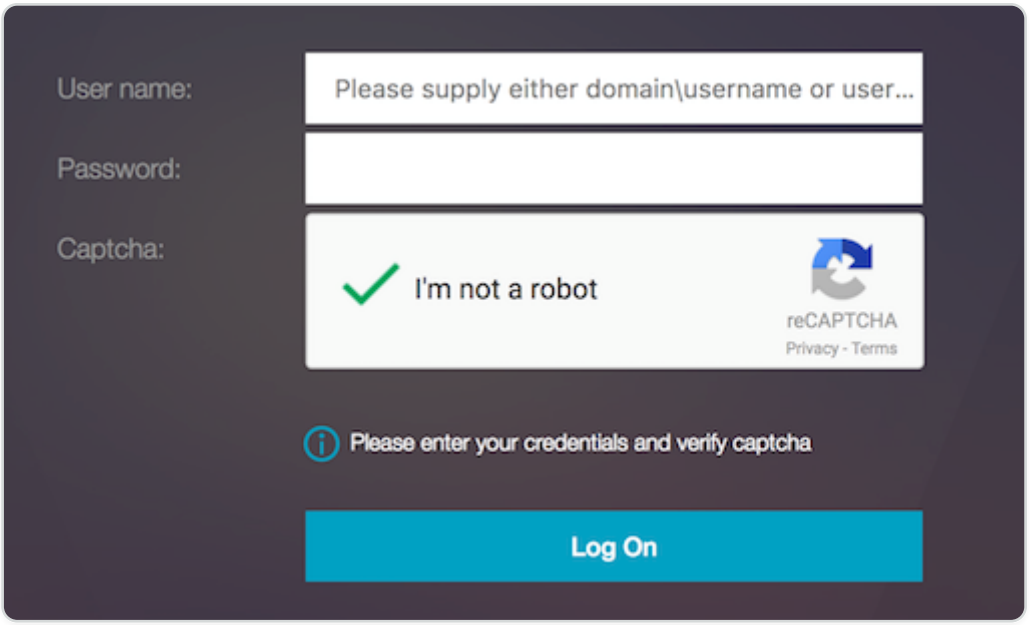


2. 选择**我不是机器人**。re-Captcha 小部件将显示。



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

3. 在显示完成页面之前，您将浏览一系列 re-Captcha 图像。
4. 输入 AD 凭据，选择**我不是机器人**，然后单击**登录**。如果身份验证成功，您将被重定向到所需资源。



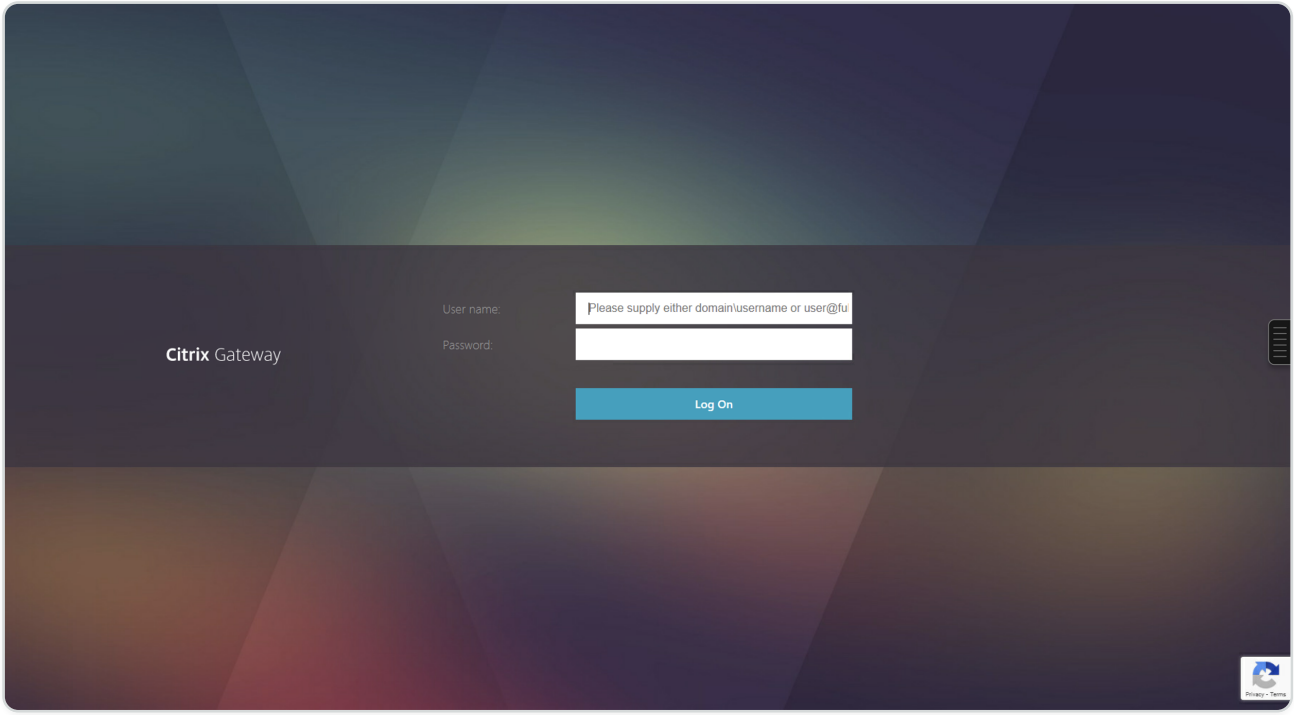
注意：

- 如果 re-Captcha 与 AD 身份验证一起使用，则凭据的**提交**按钮在 re-Captcha 完成之前处于禁用状态。
- re-Captcha 发生在它自己的因素中。因此，任何后续验证（例如 AD）都必须发生在 re-Captcha 的 `nextfactor` 中。

re-Captcha v3（管理控制台和企业控制台）：

配置 re-Captcha v3 后，您会看到以下 UI。

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



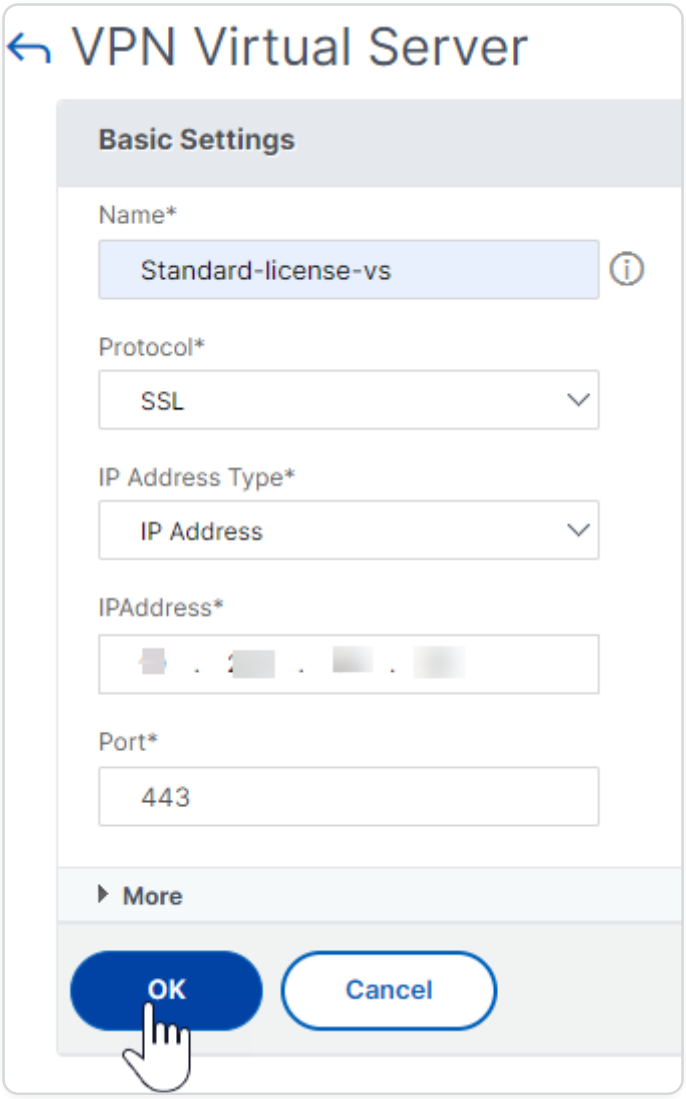
注意：

如果配置了 re-Captcha v3，则当从 Google 服务器收到验证码响应时，**登录**按钮将启用。当用户单击**登录**按钮时，仅当 re-Captcha 服务生成的评分在配置的 scoreThreshold 参数范围内时，身份验证才成功。

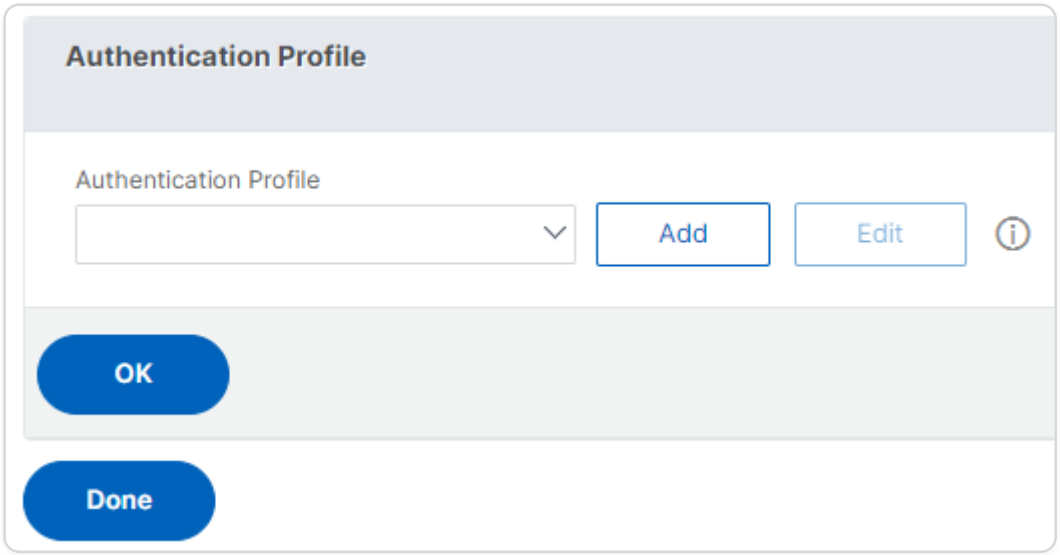
在 NetScaler 标准许可证中为 nFactor 身份验证创建网关虚拟服务器

1. 导航到 **NetScaler Gateway > 虚拟服务器**。
2. 在 **NetScaler Gateway 虚拟服务器**页面上，单击**添加**。
3. 在**VPN 虚拟服务器**页面上输入以下详细信息，单击**确定**，然后单击**继续**。
   - 名称 - NetScaler Gateway 虚拟服务器的名称
   - 协议 - 选择**SSL**
   - IP 地址 - NetScaler Gateway 虚拟服务器的 IP 地址
   - 端口 - 输入 443

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

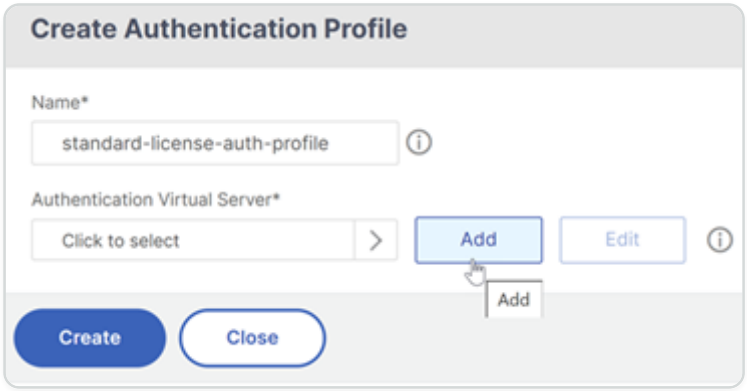


1. 在**VPN 虚拟服务器**页面上，单击**身份验证配置文件**旁边的加号图标。
2. 单击 **添加** 以配置身份验证配置文件。



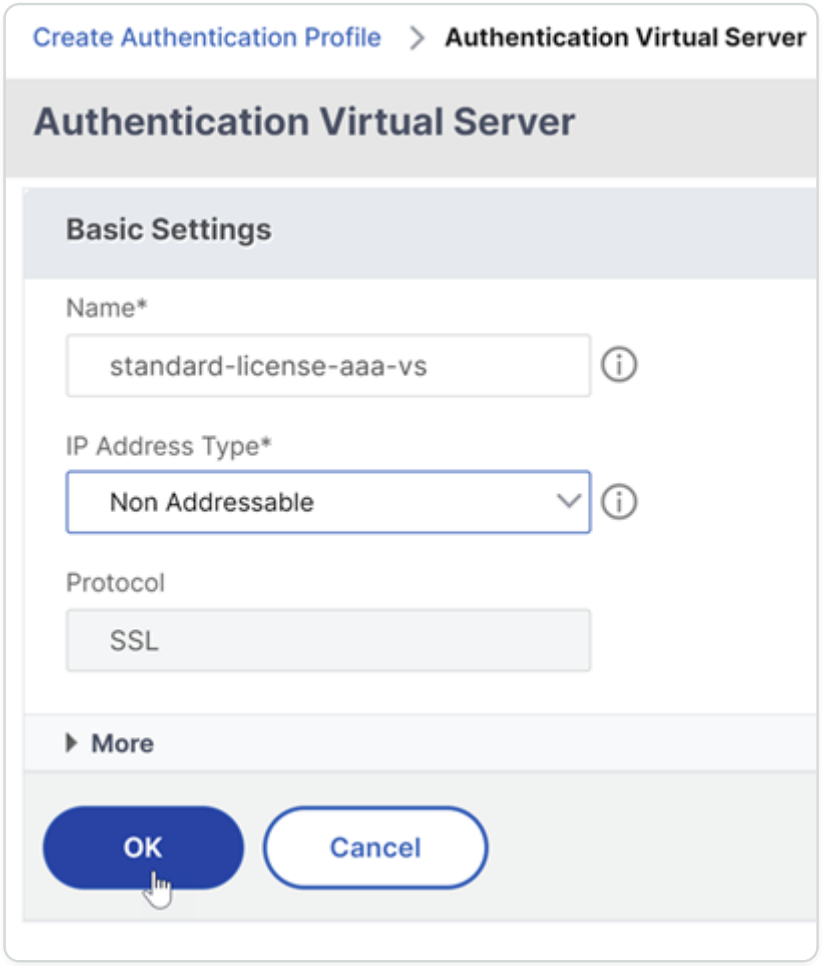
3. 输入身份验证配置文件的名称，然后单击 **添加**。

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



4. 在 **VPN 虚拟服务器** 页面上输入以下详细信息，单击 **确定**，然后单击 **继续**。

   - 名称 - 身份验证、授权和审计虚拟服务器的名称
   - 协议 - 选择 **不可寻址**。在 NetScaler Standard 许可证中，只有不可寻址的身份验证、授权和审计虚拟服务器才能绑定到 Gateway/VPN 虚拟服务器。



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

注意：

- 在 NetScaler Standard 许可证中，创建策略的步骤与 Premium 许可证支持的策略类型相同。
- NetScaler Standard 许可证不支持在 nFactor 配置中添加新的登录架构。

参考

有关端到端 nFactor 配置示例，请参阅 配置 nFactor 身份验证。

统一网关可视化工具

统一网关可视化工具使用统一网关向导提供配置的可视化表示。统一网关可视化工具用于添加和编辑配置，以及诊断后端问题。

统一网关可视化工具显示以下内容：

配置	配置
预认证策略	认证策略
CS 虚拟服务器	VPN 虚拟服务器
LB 虚拟服务器	XA/XD 应用程序
Web 应用程序	SaaS 应用程序

统一网关部署通过一个 URL 为您的企业或 SaaS 应用程序、无客户端访问应用程序、Citrix Virtual Apps™ 和桌面资源提供安全的远程访问。

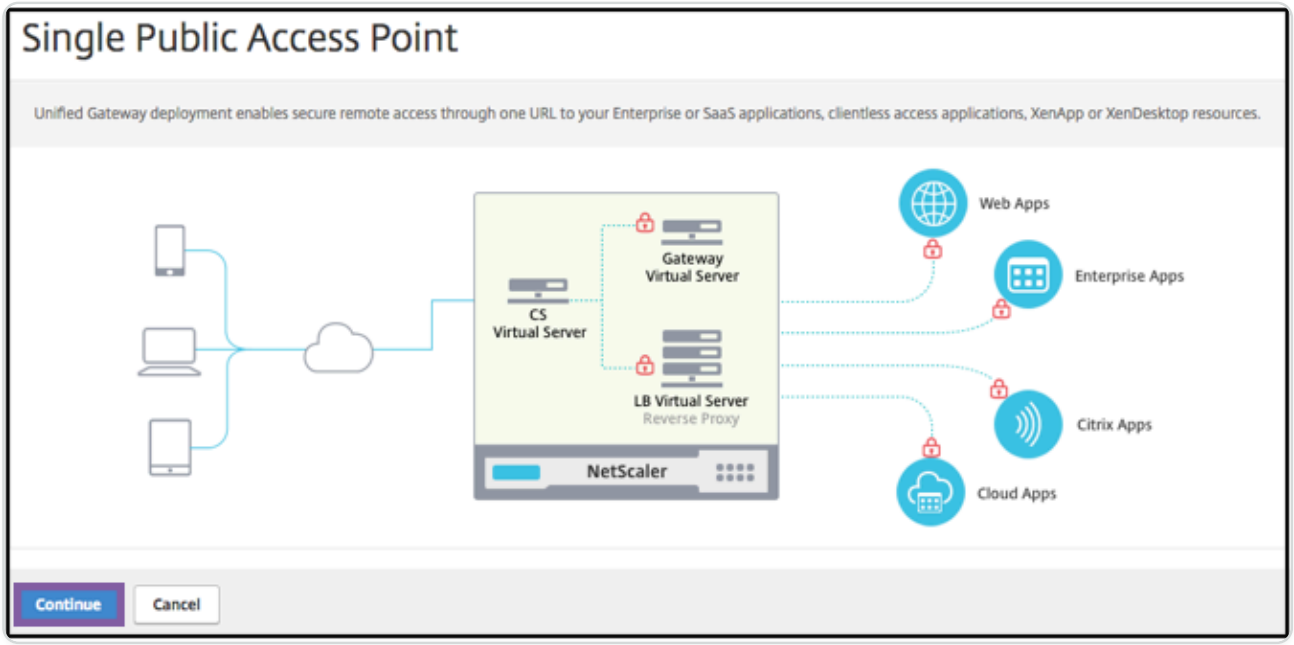
配置统一网关

1. 从菜单中选择 Unified Gateway。
2. 在下一个屏幕上，验证您是否拥有以下信息，然后单击 **Get Started**：
   - Unified Gateway 的公共 IP 地址。
   - 服务器证书链（.PFX 或 .PEM），可选择包含根 CA 证书。
   - 基于 LDAP/RADIUS/客户端证书的身份验证详细信息。

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

- 应用程序详细信息（SaaS 应用程序的 URL 或 Citrix Virtual Apps and Desktops 服务器详细信息）。

3. 单击 **Continue** 按钮。



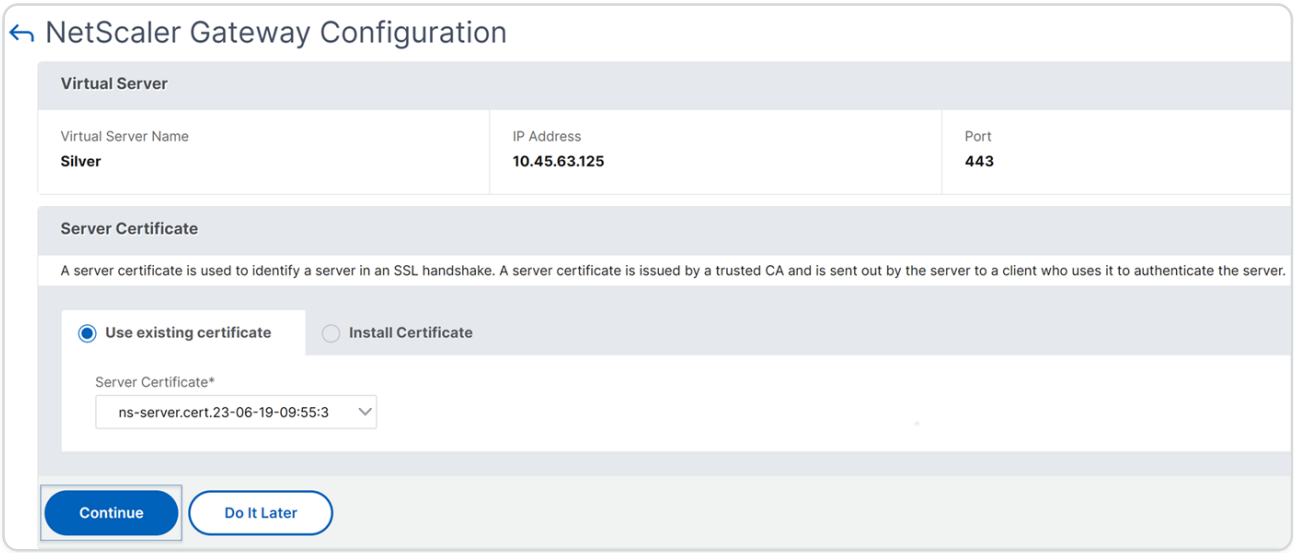
创建 Unified Gateway 配置虚拟服务器。

1. 输入虚拟服务器的配置 **Name**。
2. 输入 Unified Gateway 部署的面向公众的 **Unified Gateway IP address**。
3. 输入 Unified Gateway 部署的完全限定域名 (**FQDN**)。
4. 输入 **Port** 号。端口号范围是 1–65535。
5. 单击 **Continue**。

填写以下信息以指定服务器证书。

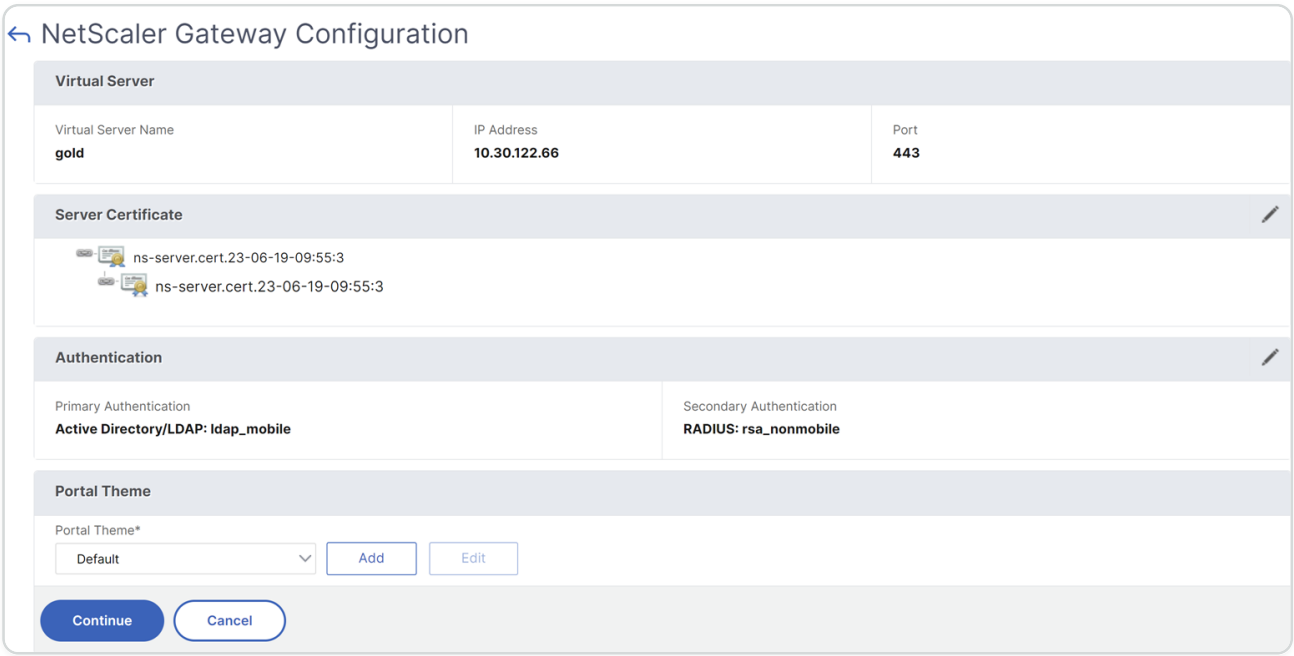
1. 选择“**使用现有证书**”或“**安装证书**”单选按钮。
2. 从菜单中选择一个“**服务器证书**”。
3. 单击“**继续**”按钮。

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



填写以下信息以指定身份验证。

1. 从菜单中选择一个“**主要身份验证方法**”。
2. 选择“**使用现有服务器**”或“**添加新服务器**”单选按钮以指定主要身份验证服务器详细信息。
3. 从菜单中选择一个“**辅助身份验证方法**”。
4. 选择“**使用现有服务器**”或“**添加新服务器**”单选按钮以指定辅助身份验证服务器详细信息。
5. 单击“**继续**”按钮。
6. 从菜单中选择“**门户主题**”。
7. 单击“**继续**”。
8. 选择“**Web 应用程序**”或“**Citrix Virtual Apps Desktops**”单选按钮。
9. 单击“**继续**”。



选择应用程序(/en-us/netscaler-gateway/media/fig8_-webapplication1.png)

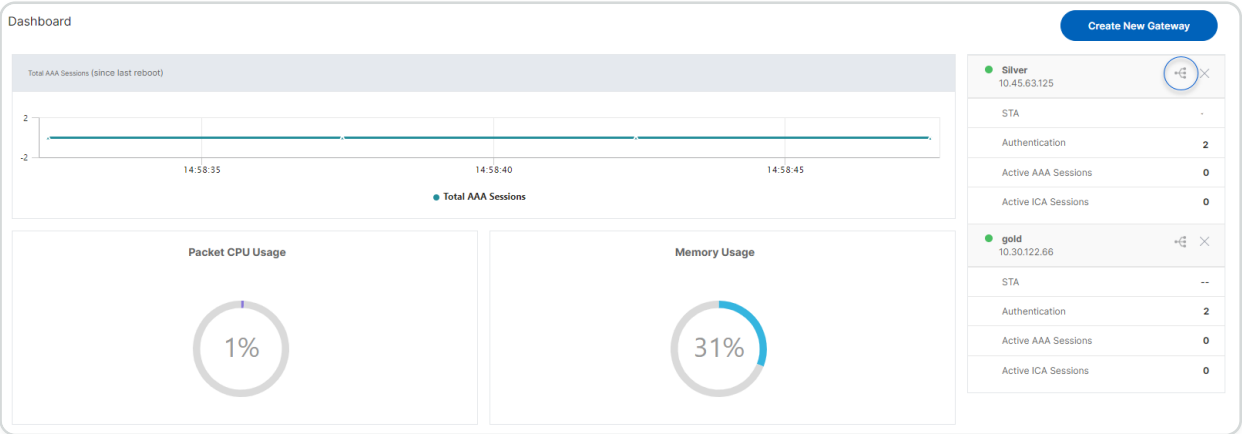
© 1997–2026 Citrix Systems, Inc. All rights reserved.

填写以下信息以指定 Web 应用程序。

1. 输入书签链接的名称。
2. 选择 VPN URL 所代表的应用程序类型。可能的值为：
   - 内网应用程序
   - 无客户端访问
   - SaaS
   - 此 NetScaler 上的预配置应用程序
3. 勾选此框以通过统一网关 URL 访问此应用程序。
4. 输入书签链接的 URL。
5. 从图标 URL 中选择一个文件以获取图标文件。最大长度 = 255
6. 单击“**继续**”按钮。
7. 单击“**完成**”。
8. 单击“**继续**”。
9. 单击“**完成**”。

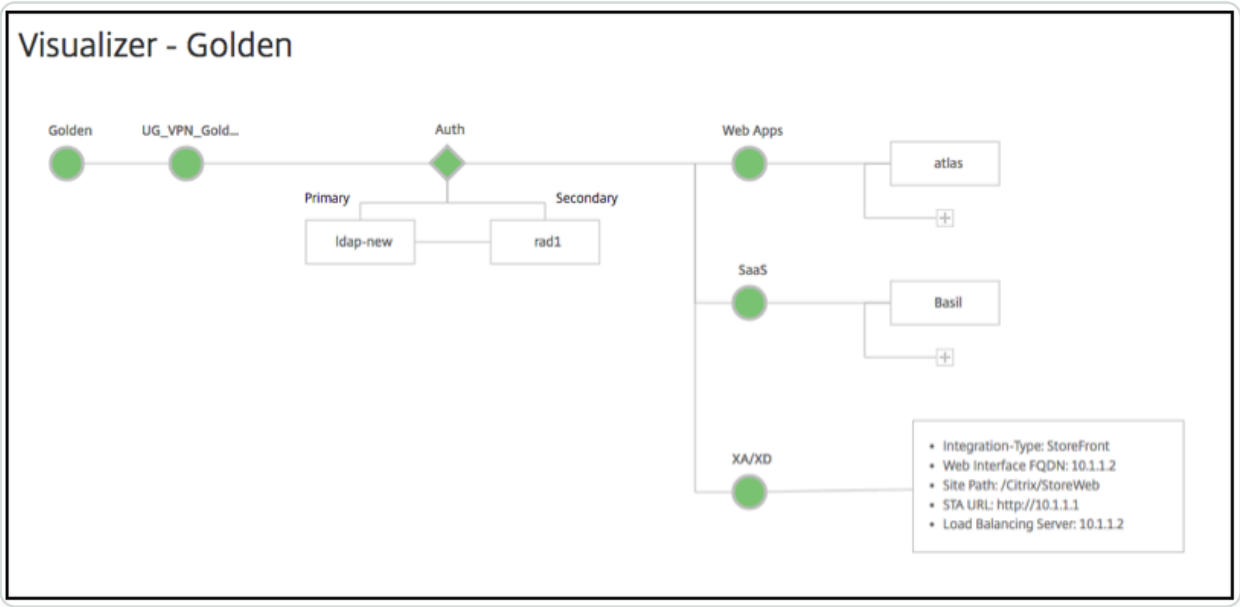
GUI 配置

1. 从菜单中选择 Unified Gateway。
2. 单击**Unified Gateway Visualizer**图标以访问已配置的网关实例。

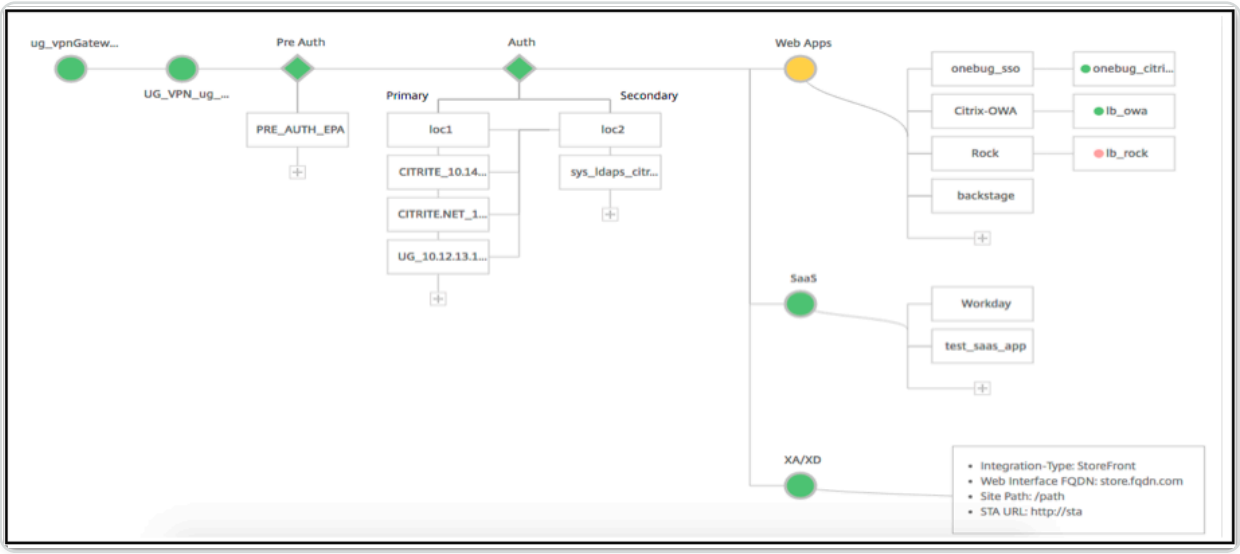


Unified Gateway Visualizer 看起来像一个流程图，如下图所示：

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



Unified Gateway Visualizer 具有预认证、 `Auth` 和应用程序部分。如果 VPN 虚拟服务器具有预认证策略，则只有此时， `pre-auth` 才会在 Unified Gateway Visualizer 中显示。



Unified Gateway Visualizer 使用颜色编码方案来指示负载均衡和 VPN 虚拟服务器的状态。

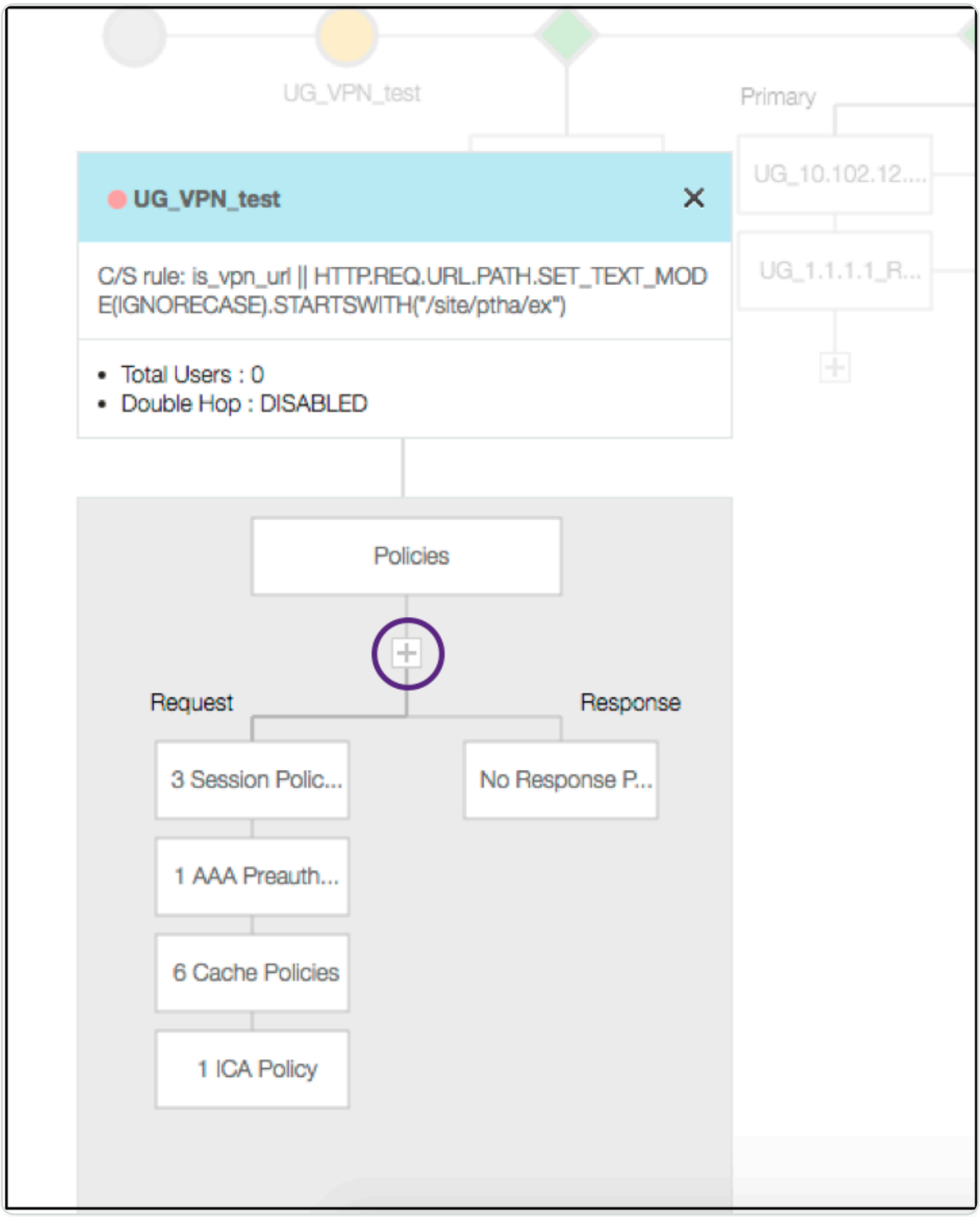
颜色	描述
红色	表示服务器已关闭。
灰色	表示未配置 webapps/Citrix Virtual Apps。
绿色	表示虚拟服务器一切正常。
橙色	表示负载平衡虚拟服务器服务之一已关闭，但仍能正常运行。

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

VPN 虚拟服务器的详细信息

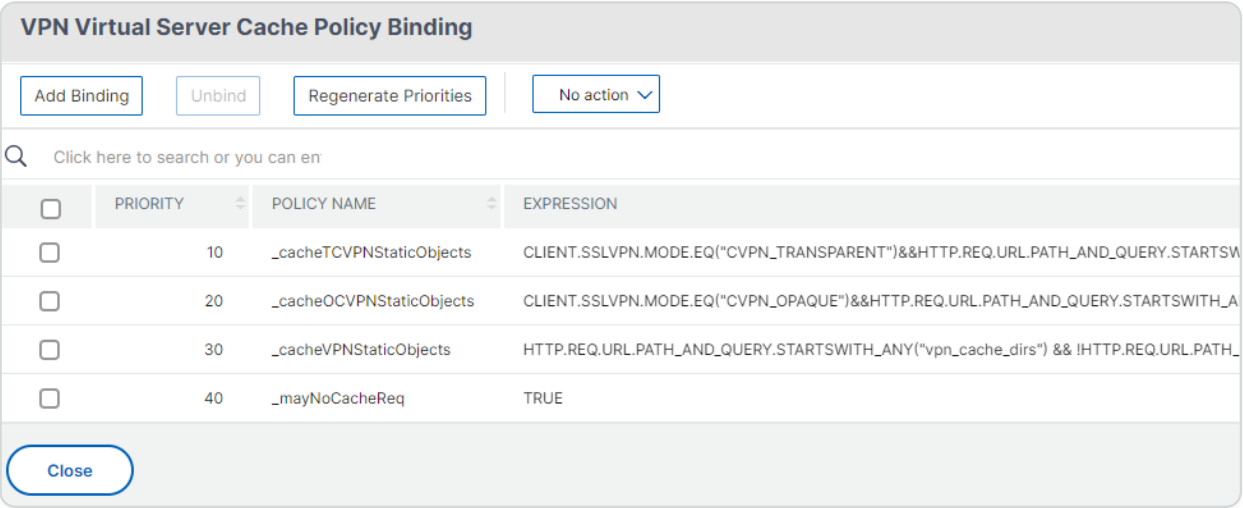
要获取 VPN 虚拟服务器的详细信息，请单击 **VPN 虚拟服务器节点**。弹出窗口会显示 C/S 规则和所有策略等详细信息。

1. 通过单击 (+) 图标将策略添加到 VPN 实体。

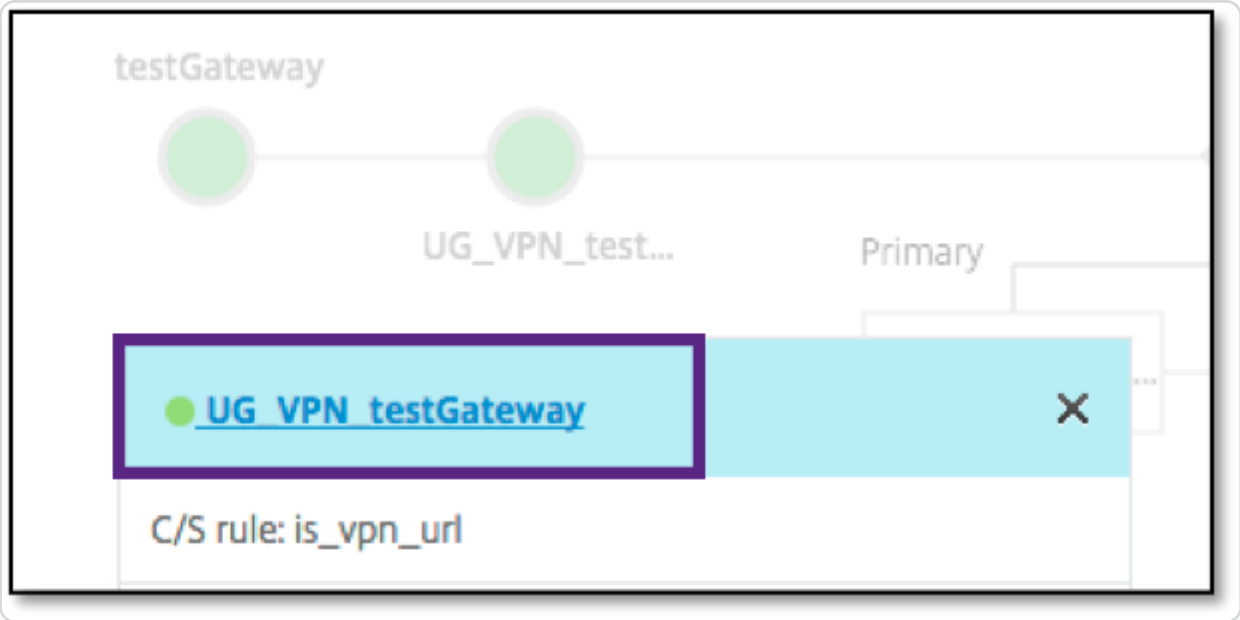


2. 单击所需的节点以查看已配置策略的详细信息。

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

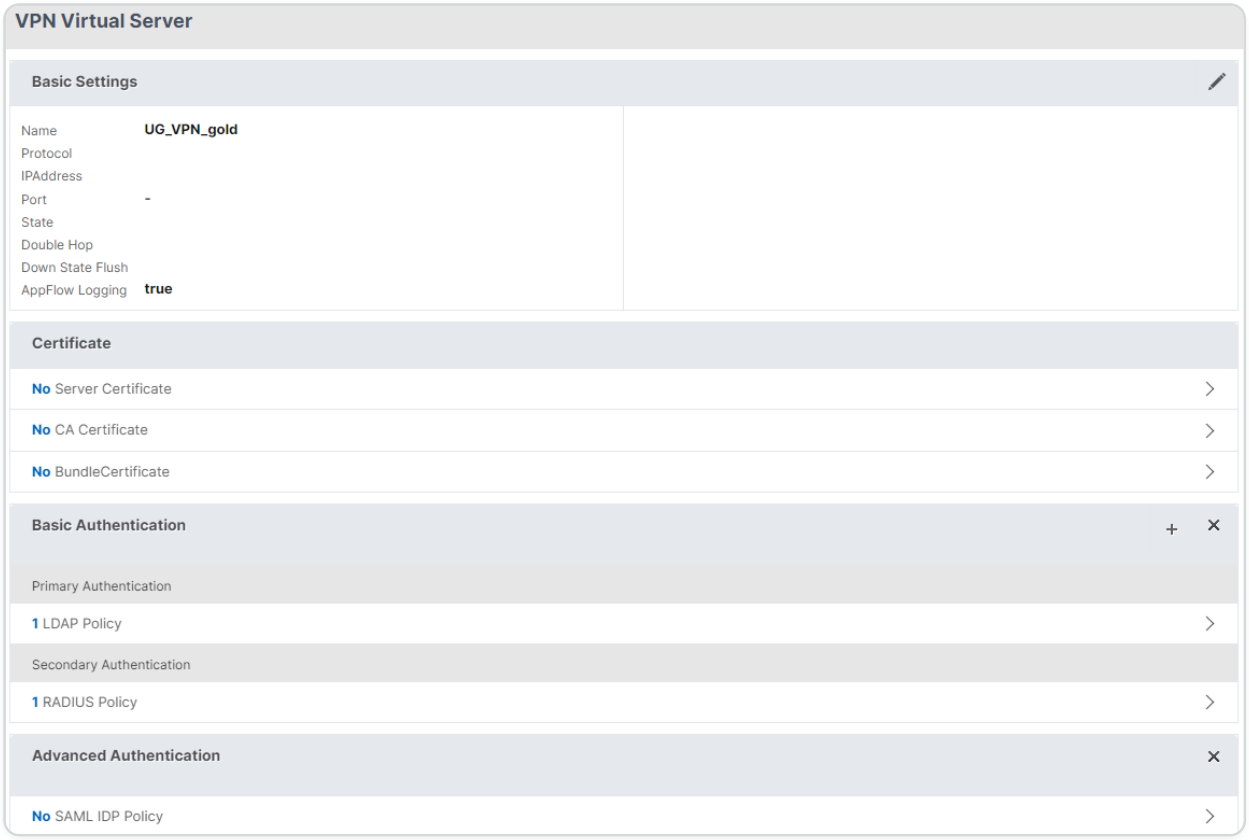


对于 VPN 虚拟服务器信息，弹出窗口中的 VPN 标题是一个可点击的实体，可转到显示 VPN 虚拟服务器详细信息的滑块。



此处显示 VPN 服务器的详细信息。

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

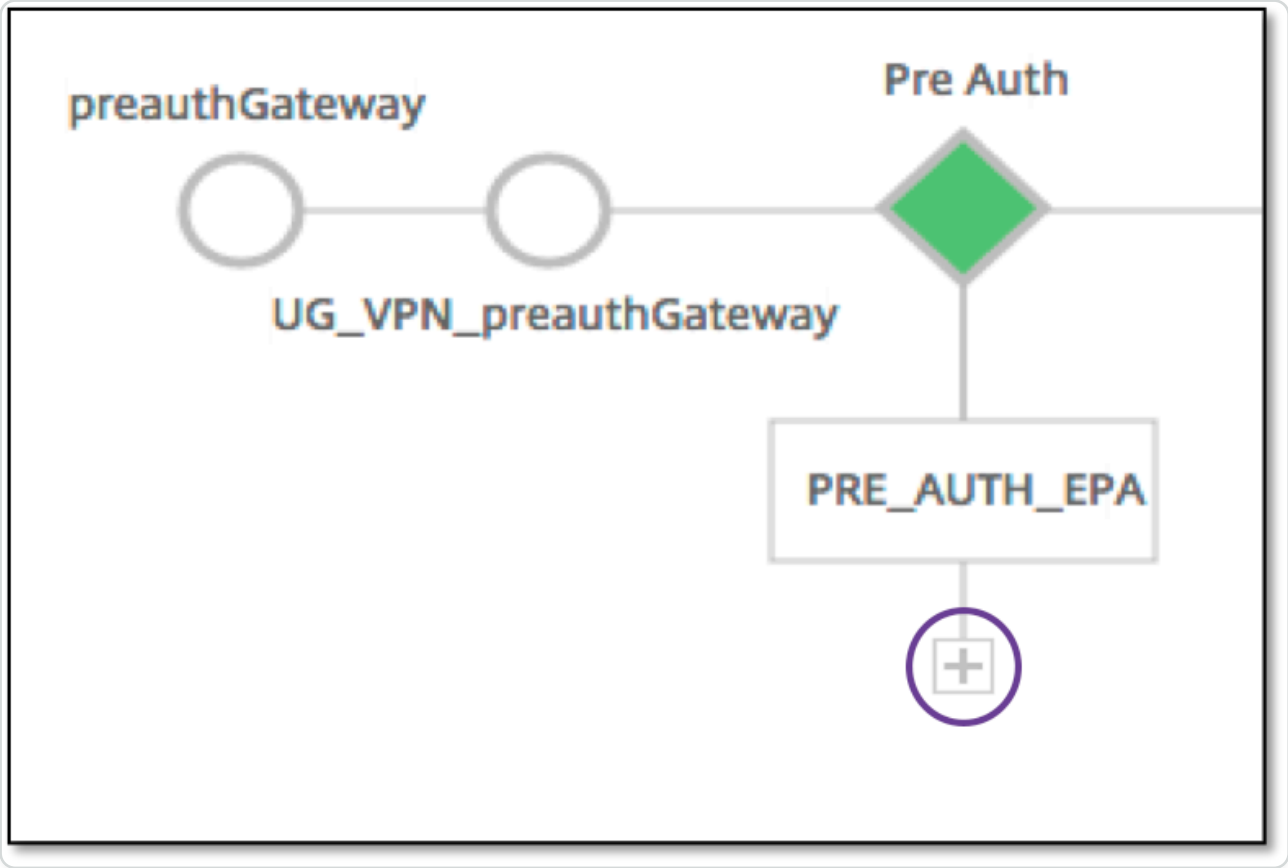


The Pre Auth Block

如果 VPN 虚拟服务器关联了预认证策略，Unified Gateway Visualizer 会显示一个 `Pre Auth` 块。`Pre Auth` 块显示了这些策略，并提供了向 VPN 添加预认证策略的选项。

1. 单击 **+** 以添加 `preauth` 策略。

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



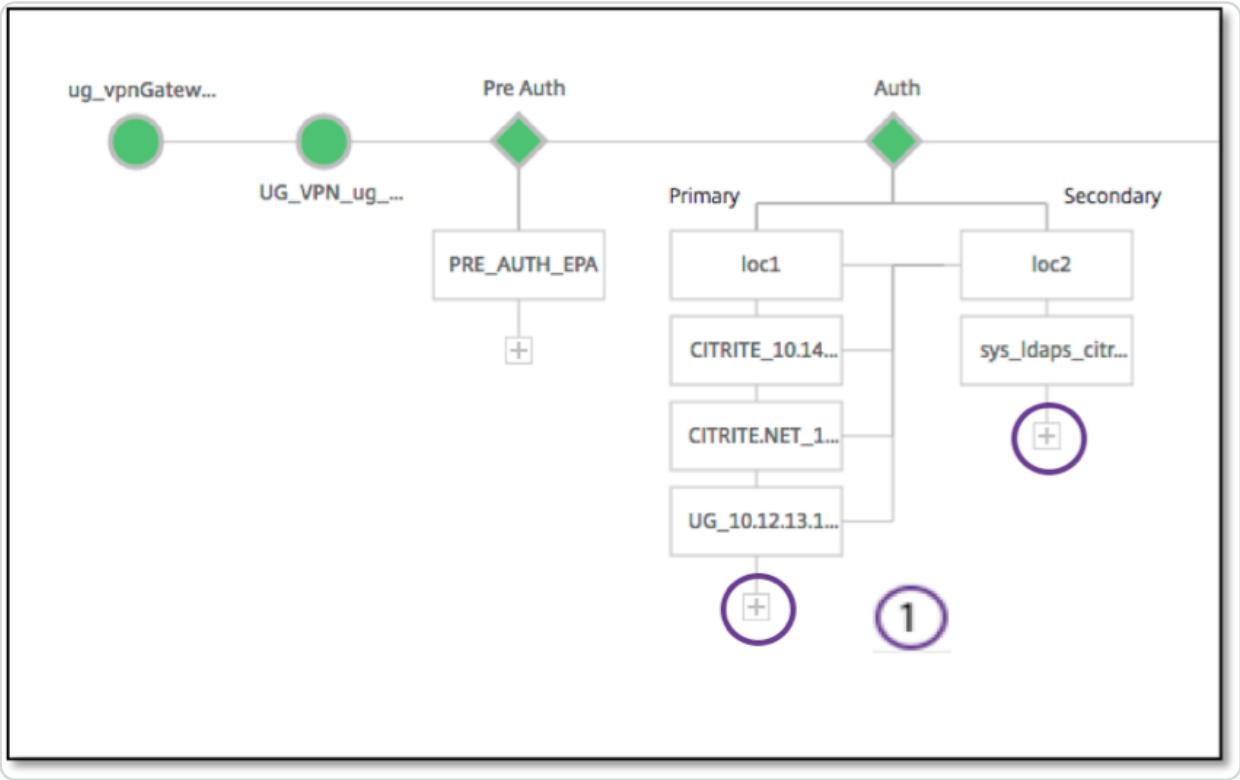
如果没有关联预认证策略，此块将从视图中隐藏。

The Auth Block

`Auth` 块列出了主策略和辅助策略。`Auth` 块提供了添加策略的选项。

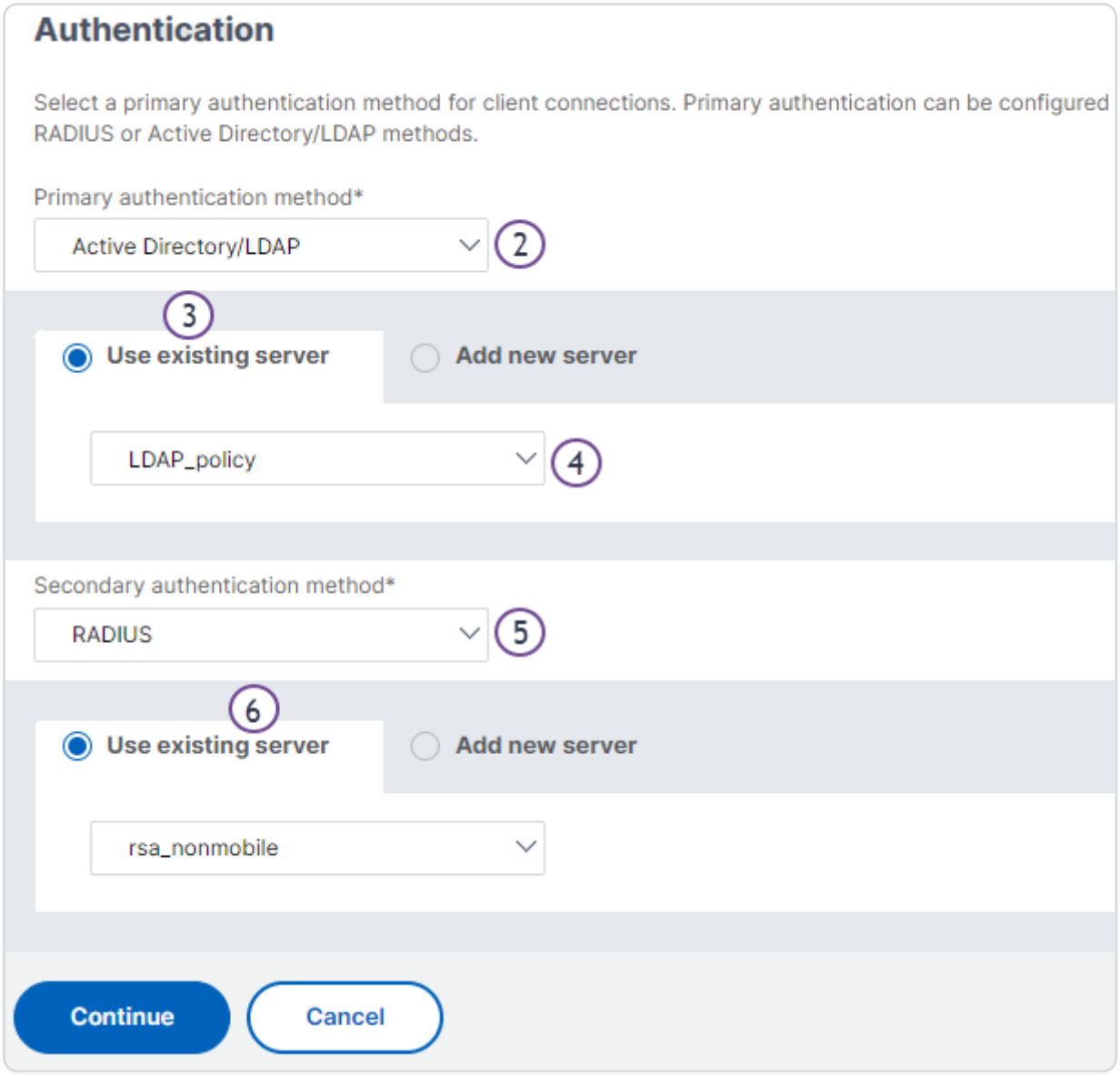
1. 在主列表中单击 **+** 以添加主身份验证绑定，或在辅助列表中单击 + 以添加辅助身份验证绑定。

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



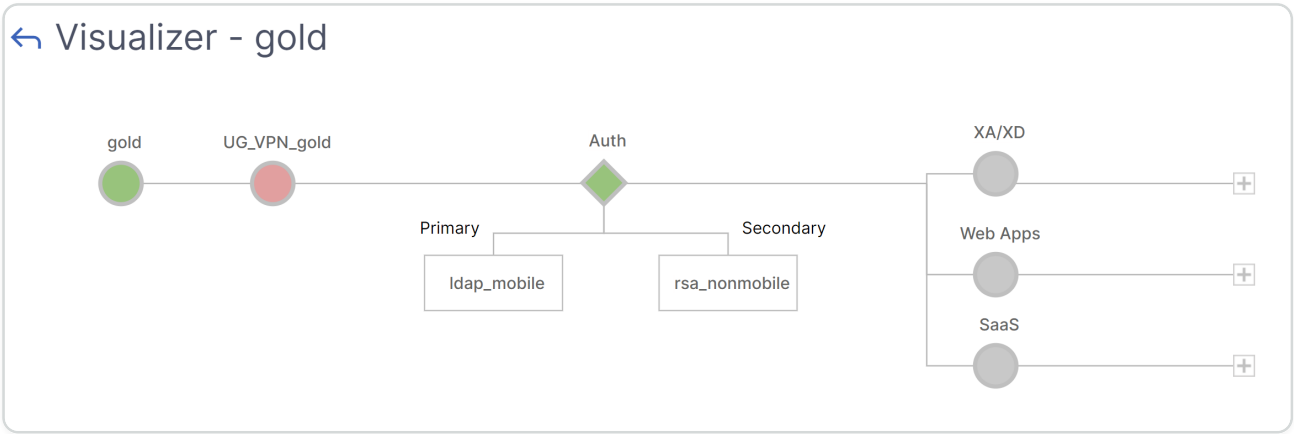
2. 从“**主身份验证方法**”菜单中选择一个选项。
3. 通过选择单选按钮指定是**现有服务器**还是**添加新服务器**。
4. 从“**LDAP 策略名称**”菜单中选择一个选项。
5. 从“**辅助身份验证方法**”菜单中选择 **RADIUS**。
6. 通过选择单选按钮指定是要**使用现有服务器**还是**添加新服务器**。
7. 单击“**继续**”。

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



添加 StoreFront™

1. 单击 XA/XD 旁边的 **+**，它将带您添加“XA/XD”应用程序。



您可以选择集成点。选项包括 StoreFront、WI 或 WionNS。单击**继续**。

1. 填写以下字段以配置 StoreFront。带 * 的字段为必填信息。

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

字段	描述
StoreFront FQDN*	输入 StoreFront 服务器的 FQDN。最大长度：255 个字符。示例：// storefront.xendt.net
站点路径*	输入 StoreFront 上已配置的网站的 Receiver 路径。
`Single Sign-on Domain` *	输入用户身份验证的默认域
应用商店名称*	输入 StoreFront 监视器的名称。STORENAME 是一个参数，用于定义 StoreFront 服务应用商店名称，以探测 StoreFront 服务器的运行状况。适用于 StoreFront 监视器。最大长度：31
安全票证颁发机构服务器*	输入安全票证颁发机构 URL，通常位于交付控制器上。示例：`http://sta`
StoreFront 服务器*	输入 StoreFront 服务器的 IP 地址
协议*	输入服务器使用的协议。
端口*	输入服务器使用的端口。
负载平衡	输入 StoreFront 服务器的负载平衡配置。
虚拟服务器*	输入 Unified Gateway 部署的面向公众的 IP 地址。

2. 单击 **继续**。

添加 SaaS

1. 单击 **+** 添加 SaaS 应用程序，这将带您进入“添加 SaaS”页面。填写以下字段以配置 SaaS。必填字段标有 *。

字段	描述
名称*	输入书签链接的名称。

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

字段	描述
应用程序类型	输入此 VPN URL 所代表的应用程序类型。可能的值包括：内网应用程序/无客户端访问/SaaS/此 NetScaler 上的预配置应用程序
输入 URL*	输入内网应用程序的 URL。
选择 **文件**	输入用于获取此资源显示图标文件的 URL。最大长度 = 255

添加 Web 应用程序

1. 单击 **+** 添加 Web 应用程序，这将带您进入“添加 Web 应用程序”页面。填写以下字段以配置 Web 应用程序。必填字段标有 *。

字段	描述
名称*	输入书签链接的名称。
应用程序类型	输入此 VPN URL 所代表的应用程序类型。可能的值包括：内部网应用程序/无客户端访问/SaaS/此 NetScaler 上的预配置应用程序
输入 URL*	输入内部网应用程序的 URL。
选择 **文件**	输入用于显示此资源的图标文件的 URL。最大长度 = 255

如果应用程序可通过统一网关 URL 访问，则可以通过单击该应用程序来访问负载平衡服务器的详细信息：

可视化工具中的负载平衡服务器(/en-us/netscaler-gateway/media/fig30_-loadbalancingserver.png)

可以通过单击 (+) 添加新策略，并通过单击显示策略信息的节点来查看所有已绑定的策略。

还会显示绑定到负载平衡器的服务数量以及总体状态信息。进一步单击会列出所有服务。可以将新服务添加到负载平衡器。

有关负载平衡器的更多详细信息，可以单击弹出窗口的标题，这将跳转到负载平衡虚拟服务器详细信息页面。

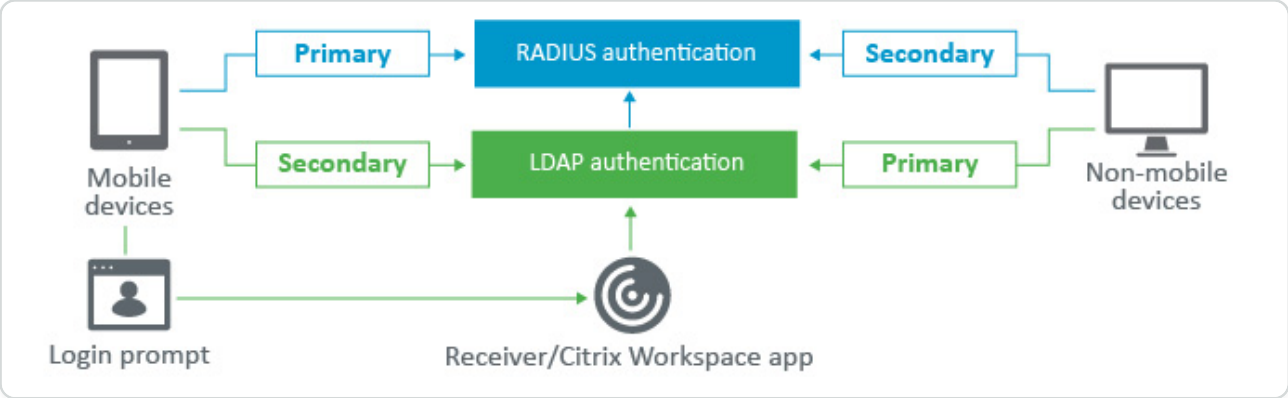
© 1997–2026 Citrix Systems, Inc. All rights reserved.

配置 NetScaler Gateway 以将 RADIUS 和 LDAP 身份验证与移动/平板设备配合使用

本节介绍如何配置 NetScaler Gateway 设备，以将 RADIUS 身份验证用作主要身份验证，将 LDAP 身份验证用作辅助身份验证，并与移动/平板设备配合使用。

本节中演示的配置仍然允许所有其他连接先使用 LDAP，后使用 RADIUS。

当您在 Citrix Workspace 应用程序上配置双因素身份验证以与移动/平板设备配合使用时，您必须将 RSA SecureID (RADIUS 身份验证) 添加为主要身份验证。但是，当用户在 Receiver 上收到用户名和密码、通行码提示时，他们会先输入 LDAP，然后输入 RADIUS 作为辅助凭据。从管理员的角度来看，这与非移动配置是不同的配置。



完成以下步骤，以配置 NetScaler Gateway 设备，使其将 RADIUS 身份验证用作主要身份验证，将 LDAP 身份验证用作辅助身份验证，并与移动/平板设备配合使用。

1. 在配置实用程序中，选择 **NetScaler Gateway > 策略 > 身份验证**，并为移动设备和非移动设备创建 LDAP 和 RSA 身份验证策略。这对于避免可能允许用户绕过 RADIUS 身份验证的逻辑条件是必要的。
2. 在 LDAP 的“**服务器**”选项卡下单击“**添加**”选项后，输入 LDAP 服务器详细信息。
3. 通过选择所需的 LDAP 服务器，为移动设备创建 LDAP 策略。

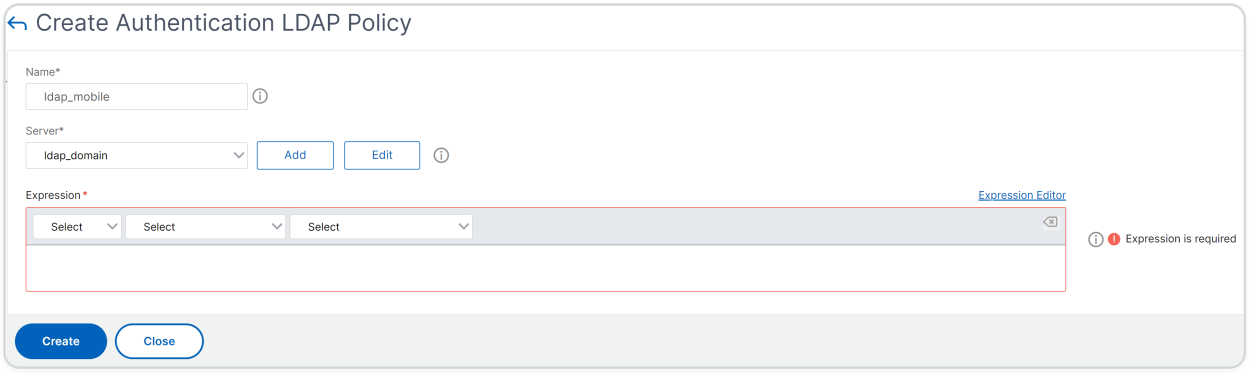
   要将此策略仅绑定到移动设备，请使用以下表达式：

   ```
   REQ.HTTP.HEADER User-Agent CONTAINS CitrixReceiver
   ```

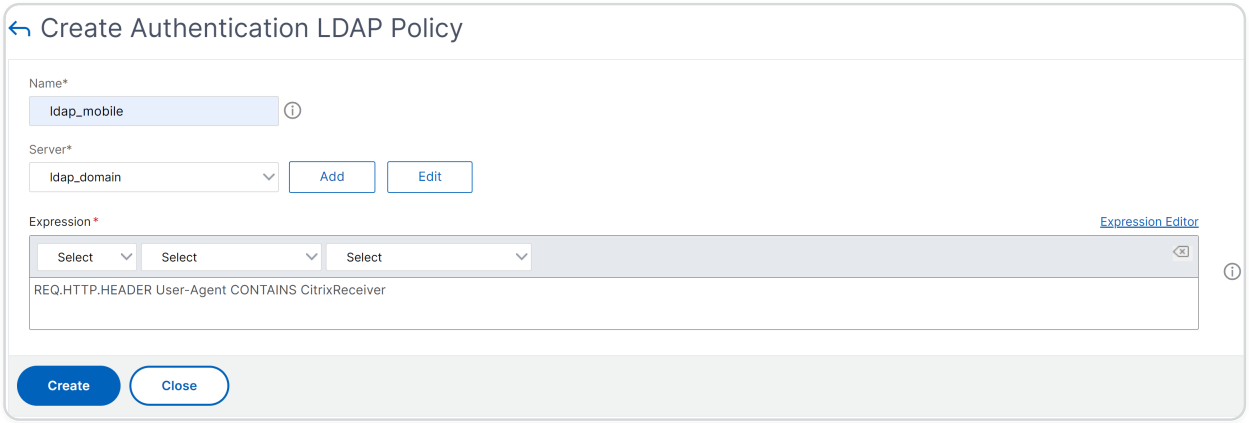
   相应的表达式为：

   ```
   HTTP.REQ.HEADER("User-Agent").CONTAINS("CitrixReceiver")
   ```

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



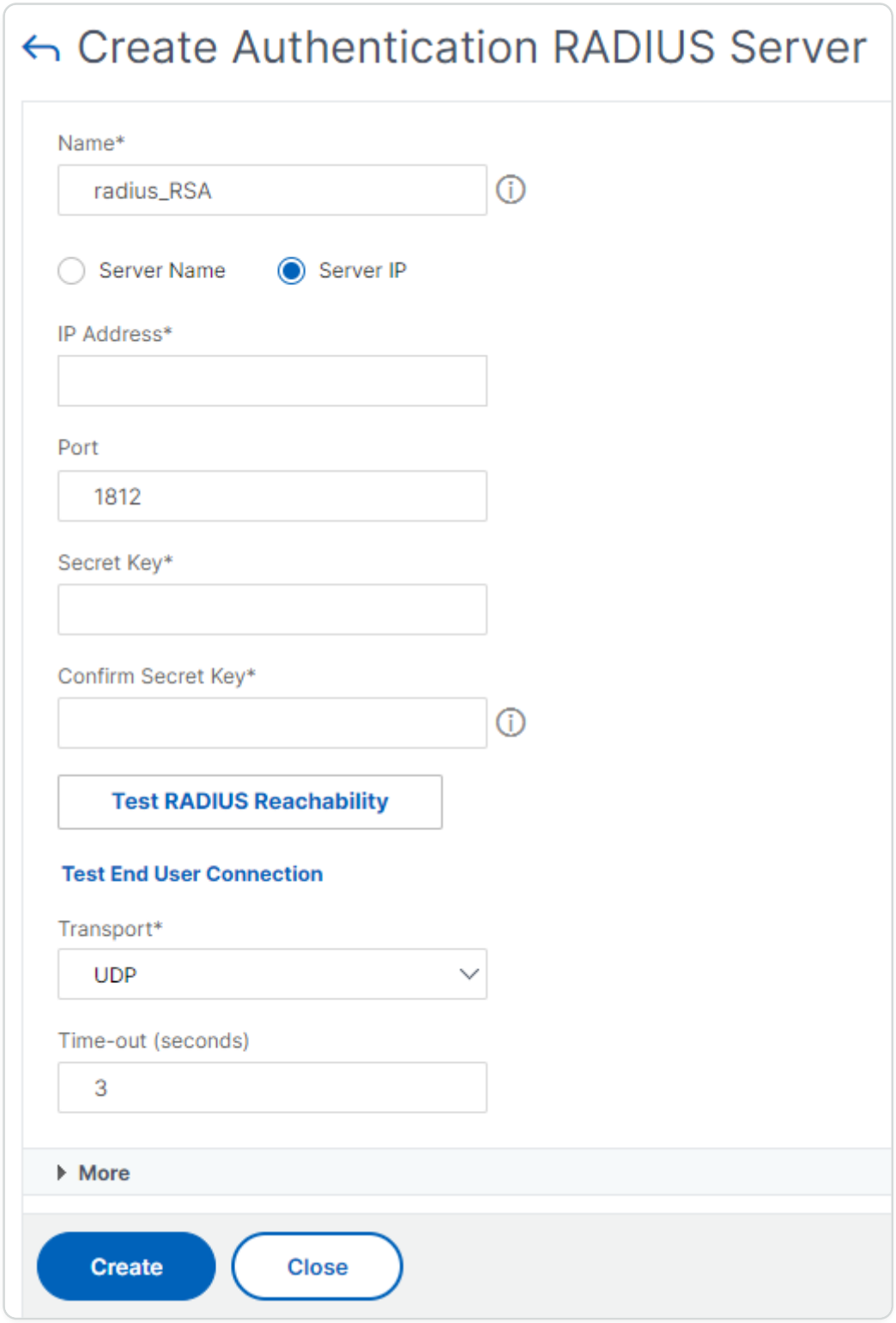
4. 单击“**表达式编辑器**”以创建策略：



5. 为移动设备创建 RADIUS 策略和 RADIUS 服务器。

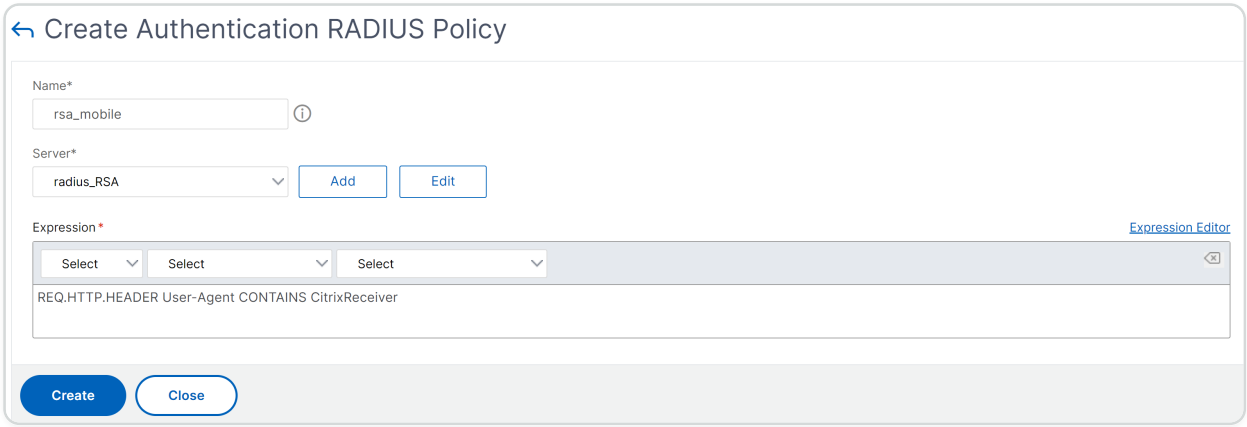
   - 从 **NetScaler Gateway > 策略 > 身份验证 > RADIUS** 导航到 RADIUS 选项。在“服务器”选项卡下单击“**添加**”。
   - 添加所需详细信息。RADIUS 身份验证的默认端口是 1812。

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



- 要将此策略仅绑定到移动设备，请使用以下表达式：

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



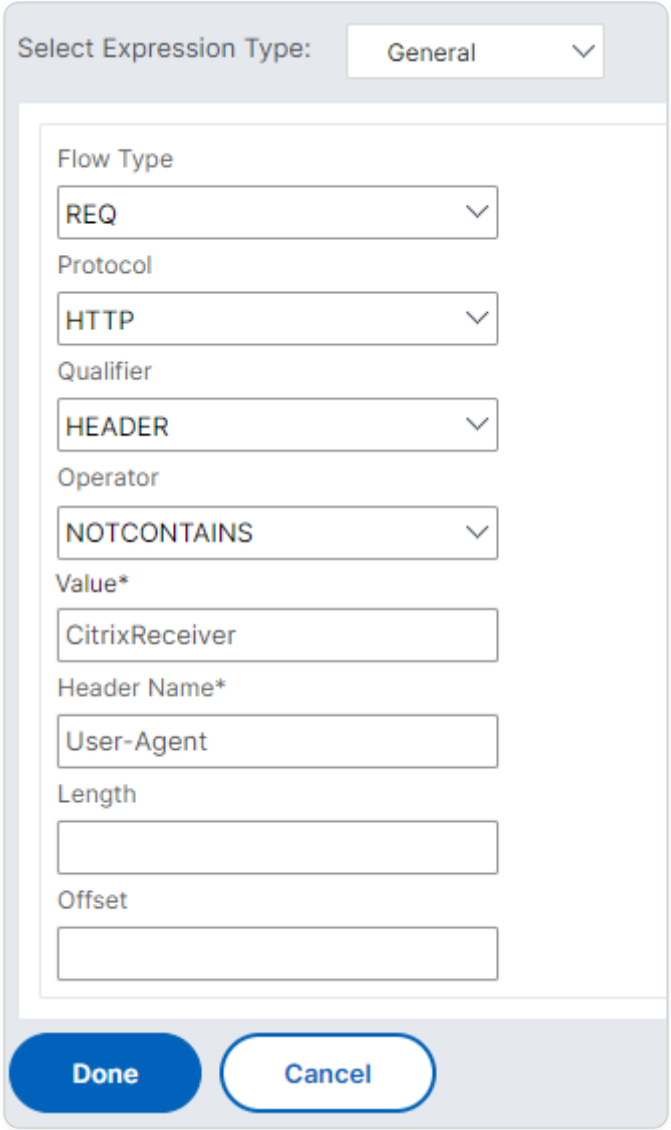
6. 按照相同的步骤为非移动设备创建 LDAP 策略。要将此策略仅绑定到非移动设备，请使用以下表达式：

```
REQ.HTTP.HEADER User-Agent NOTCONTAINS CitrixReceiver
```

相应的“高级表达式”为：

```
HTTP.REQ.HEADER("User-Agent").CONTAINS("CitrixReceiver").NOT
```

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



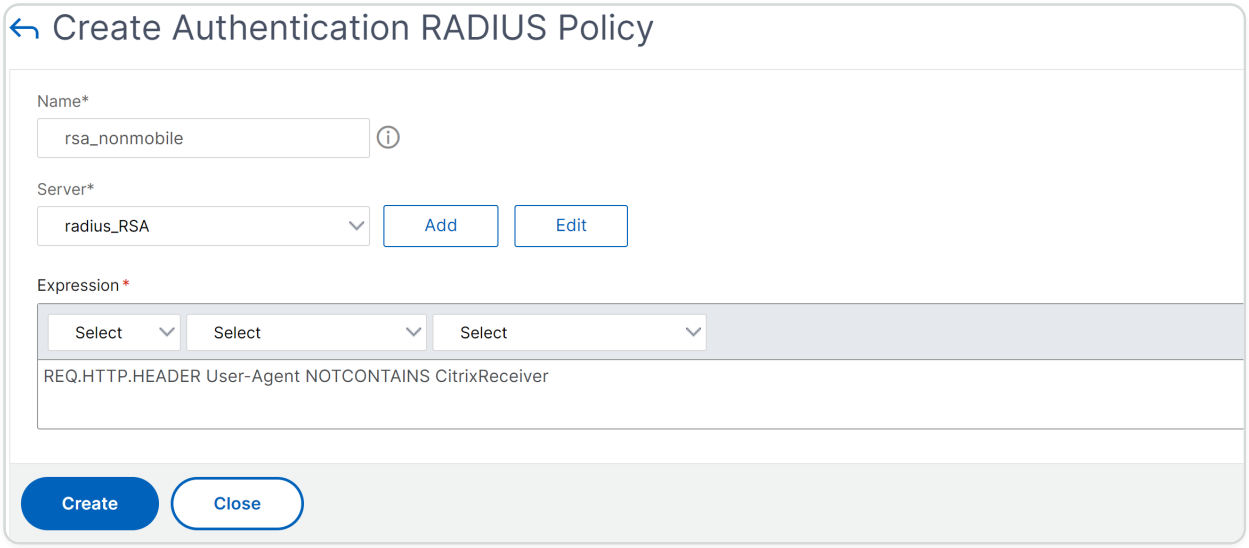
7. 为非移动设备创建 RADIUS 策略。要将此策略仅绑定到非移动设备，请使用以下表达式：

```
REQ.HTTP.HEADER User-Agent NOTCONTAINS CitrixReceiver
```

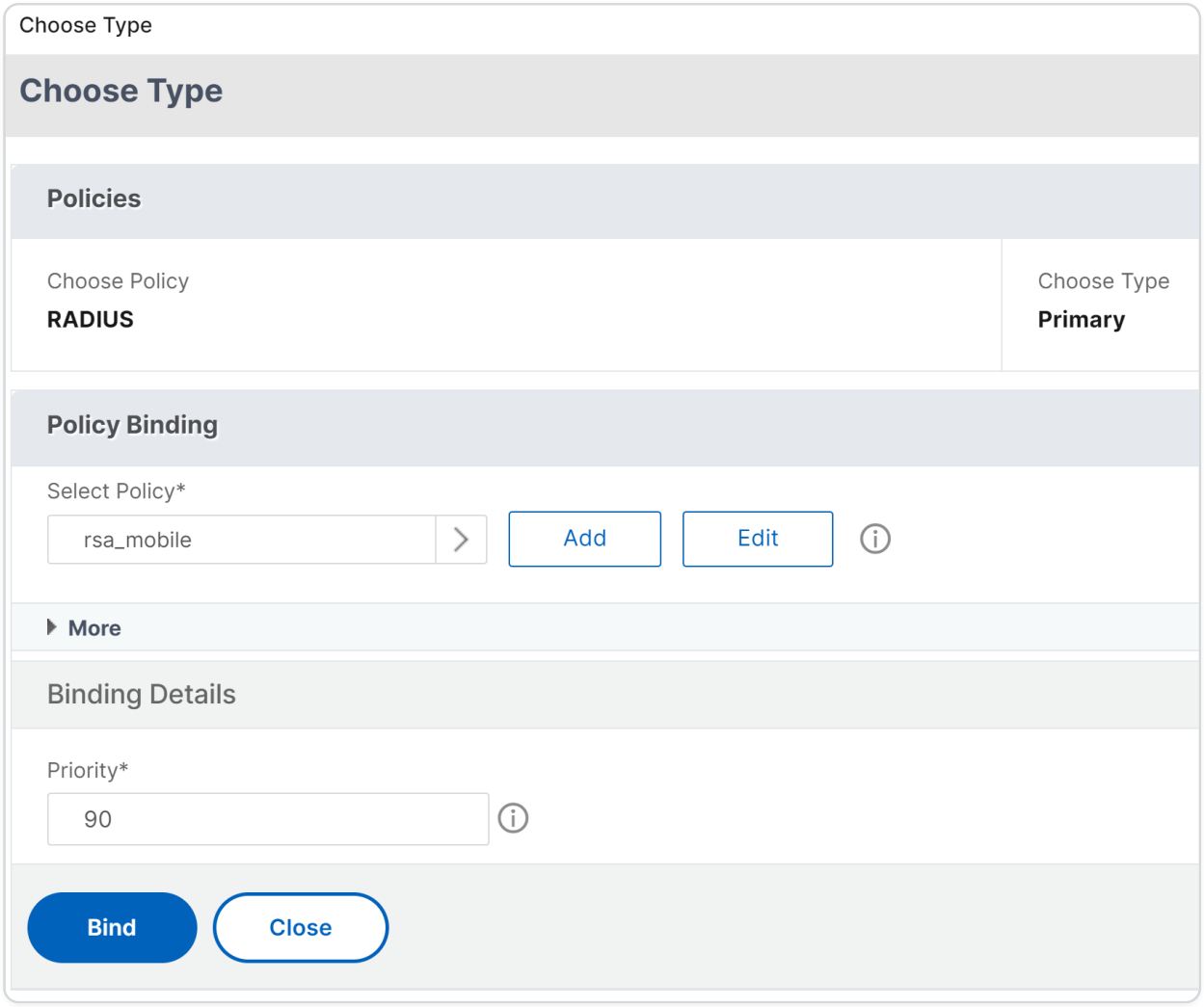
相应的“高级表达式”为：

```
HTTP.REQ.HEADER("User-Agent").CONTAINS("CitrixReceiver").NOT
```

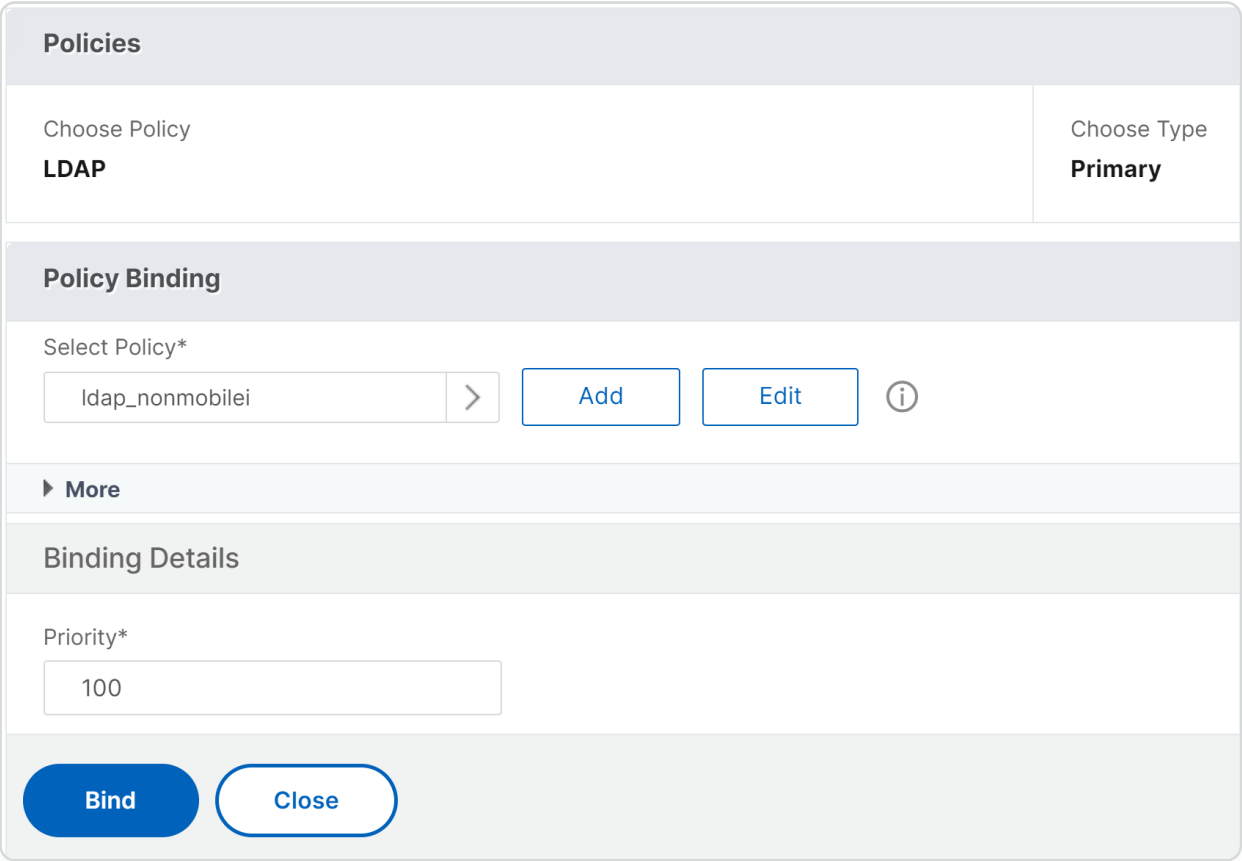
© 1997–2026 Citrix Systems, Inc. All rights reserved.



8. 转到 NetScaler Gateway 虚拟服务器的“属性”，然后单击“**身份验证**”选项卡。在“主身份验证策略”中，将 RSA_Mobile 策略添加为最高优先级，将 LDAP_NonMobile 策略添加为次要优先级：



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



9. 在“辅助身份验证策略”中，将 LDAP_Mobile 策略添加为最高优先级，然后将 RSA_NonMobile 策略添加为次要优先级：

   辅助身份验证策略(/en-us/netscaler-gateway/media/12-radius-ldap-authentication-mobile.png)

   会话策略必须具有正确的单点登录凭据索引，即必须是 LDAP 凭据。对于移动设备，**会话配置文件 > 客户端体验**下的**凭据索引**必须设置为**辅助**，即 LDAP。

   因此，您需要两个会话策略，一个用于移动设备，另一个用于非移动设备。

   - 对于移动设备，会话策略和会话配置文件显示在以下屏幕截图中。 要创建会话策略，请导航到所需的虚拟服务器，然后单击**编辑**，转到策略部分，然后单击 + 号：

   编辑虚拟服务器(/en-us/netscaler-gateway/media/13-radius-ldap-authentication-mobile.png)

   - 从菜单中选择**会话**选项。

   选择会话作为策略(/en-us/netscaler-gateway/media/14-radius-ldap-authentication-mobile.png)

   - 输入所需的会话策略名称，然后单击 + 创建配置文件。对于移动设备，**会话配置文件 > 客户端体验**下的**凭据索引**必须设置为**辅助**，即 LDAP。

   客户端体验选项卡(/en-us/netscaler-gateway/media/15-radius-ldap-authentication-mobile.png)

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

- 对于非移动设备，请遵循相同的步骤。**会话配置文件 > 客户端体验**下的**凭据索引**必须设置为**主要**，即 LDAP。

表达式必须更改为：

```
REQ.HTTP.HEADER User-Agent NOTCONTAINS CitrixReceiver
```

相应的表达式是：

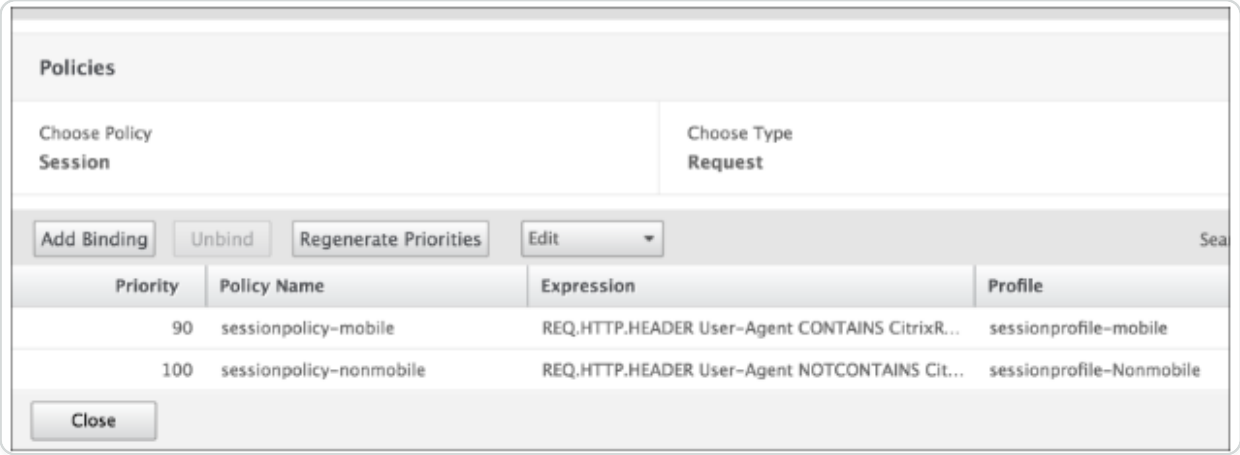
```
HTTP.REQ.HEADER("User-Agent").CONTAINS("CitrixReceiver").NOT
```

表达式(/en-us/netscaler-gateway/media/16-radius-ldap-authentication-mobile.png)

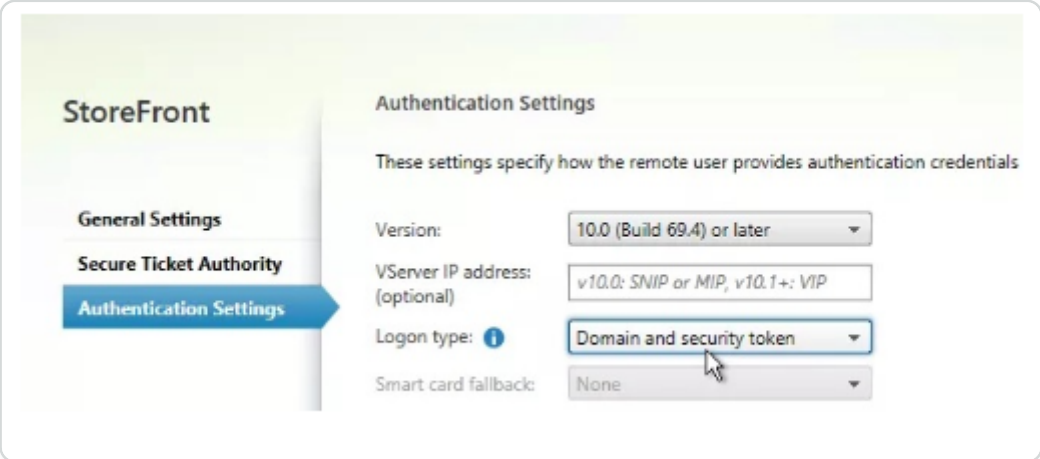
- 要为非移动用户创建配置文件，请单击 + 号。

创建配置文件(/en-us/netscaler-gateway/media/17-radius-ldap-authentication-mobile.png)

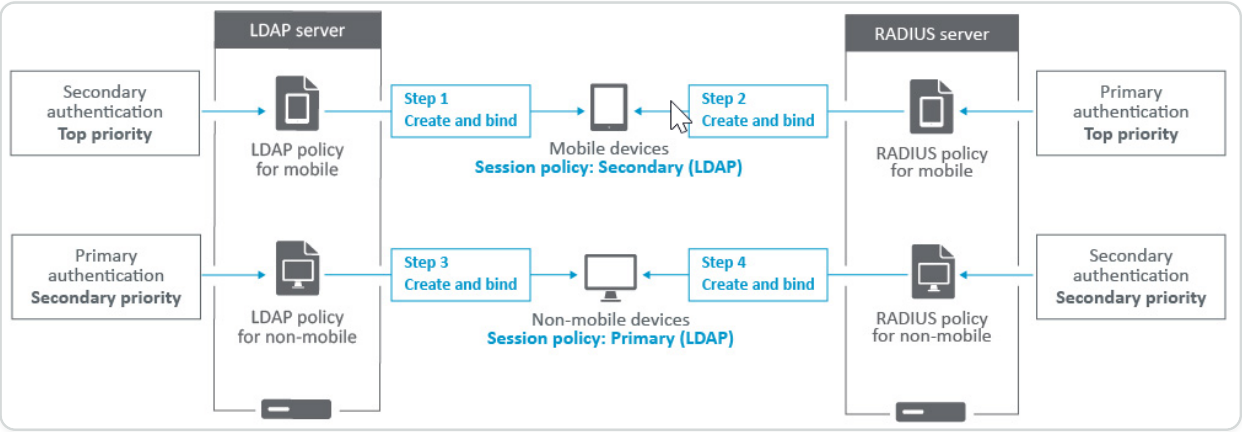
10. 下图显示了所需虚拟服务器下的策略和配置文件。



11. 同样在 StoreFront 上，在 NetScaler Gateway 配置下，设置为使用“登录类型”=“域和安全令牌”



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



限制一个 Active Directory 组的成员访问 NetScaler Gateway

NetScaler Gateway 支持两种限制登录访问的方法。

- **LDAP 搜索过滤器：** 仅将登录访问限制为与 LDAP 搜索过滤器匹配的用户名（例如，Active Directory 组成员身份）。
- **NetScaler Gateway 会话策略：** 仅将登录访问限制为会话策略或配置文件中包含的组中的用户。此方法支持多个 Active Directory 组。

LDAP 搜索过滤器方法

概述

当用户在 NetScaler Gateway 虚拟服务器的登录页面上输入凭据并按 Enter 键时，设备首先在 Active Directory (LDAP) 中搜索用户名。如果在 LDAP 策略或服务器中未定义 LDAP 搜索过滤器，则设备会搜索所有 Active Directory 用户名以查找匹配项。找到匹配项后，设备会提取用户的完整专有名称 (DN)，并使用用户的 DN 和密码向 Active Directory 进行身份验证。

如果定义了 LDAP 搜索过滤器，则仅搜索与 LDAP 搜索过滤器匹配的用户名以查找用户名匹配项。例如，如果 LDAP 搜索过滤器旨在仅搜索 Active Directory 组的成员，则用户输入的用户名必须与该组的成员匹配。

先决条件

必须为 NetScaler Gateway 虚拟服务器配置 LDAP 身份验证。

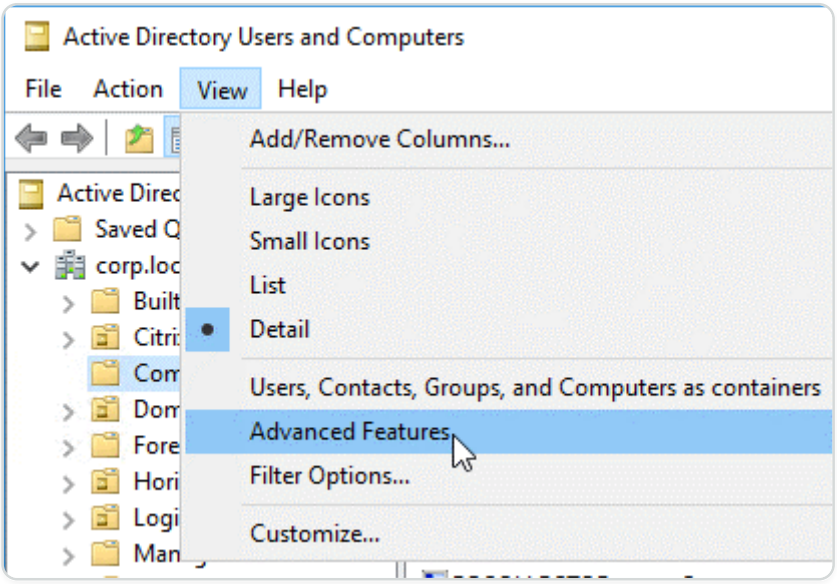
为单个 Active Directory 组成员配置 LDAP 搜索过滤器的步骤

1. 确定具有访问权限的 Active Directory 组，并获取其完整专有名称。

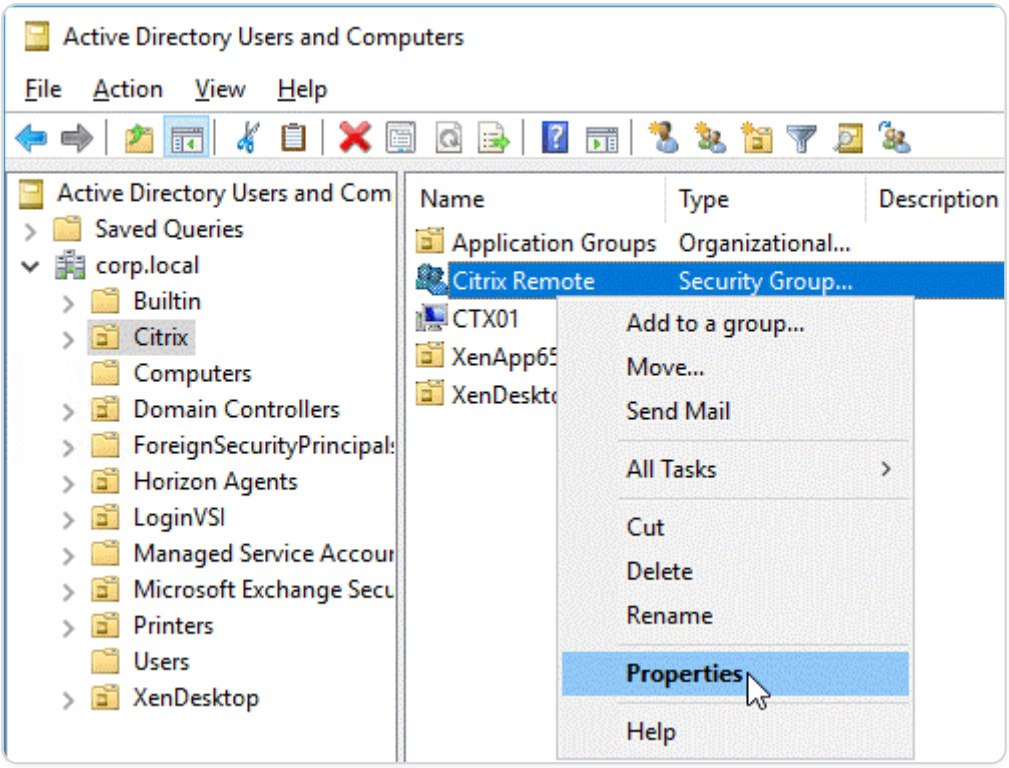
   获取组的完整专有名称的一种简单方法是通过 Active Directory 用户和计算机。

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

2. 在 Active Directory 用户和计算机中，从“**视图**”菜单中启用“**高级功能**”。

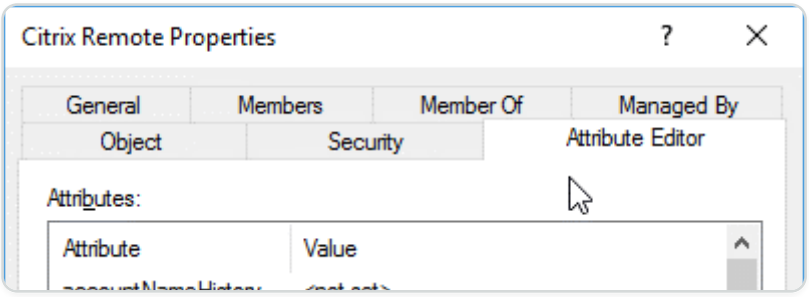


3. 浏览树到组对象，右键单击，然后点击 **属性**。 **注意：** 您不能使用 **查找**。相反，您必须通过导航树来查找对象。



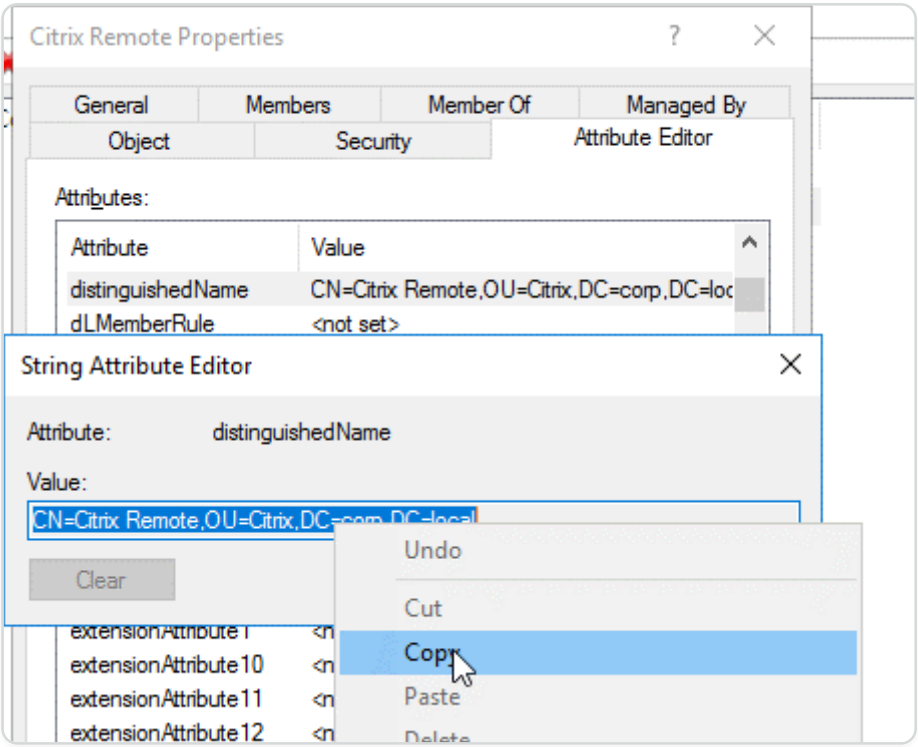
4. 在右侧，切换到 **属性编辑器** 选项卡。

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



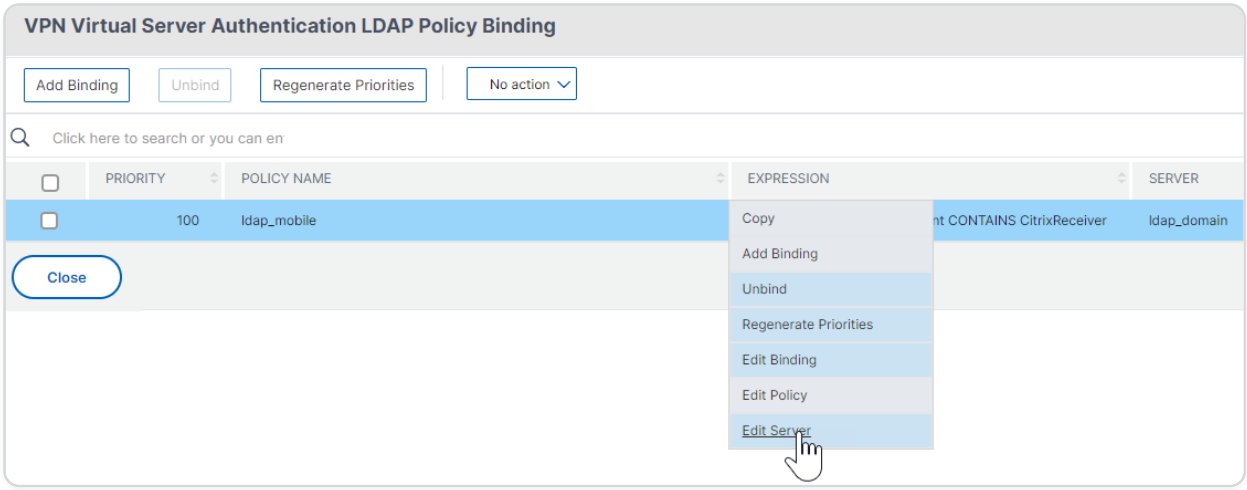
仅当启用了 **高级功能** 且您未使用 **查找** 功能时，此选项卡才可见。

5. 向下滚动到 **distinguishedName**，双击它，然后将其复制到剪贴板。

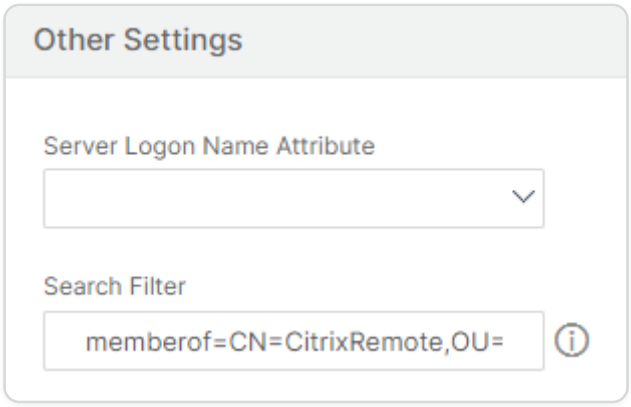


6. 在 NetScaler Gateway GUI 中，导航到 **NetScaler Gateway > 虚拟服务器**。
7. 选择一个现有的 NetScaler Gateway 虚拟服务器，然后点击 **编辑**。
8. 在“基本身份验证”部分中，点击 **LDAP 策略**。
9. 右键单击现有 LDAP 策略，然后点击 **编辑服务器**。

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



10. 在 **其他设置** 部分的 **搜索筛选器** 字段中，键入 **memberOf=**，然后将 Active Directory 组的可分辨名称粘贴到等号 (=) 后面。



搜索筛选器示例如下： memberOf=CN=Citrix® Remote,OU=Citrix,DC=corp,DC=local **注意：** 默认情况下，NetScaler® 仅搜索作为 Active Directory 组直接成员的用户名。如果要搜索嵌套组，请将 Microsoft OID:: 添加到 LDAP 搜索筛选器。OID 插入在 memberOf 和 = 之间。

示例： memberOf:1.2.840.113556.1.4.1941:=CN=Citrix Remote,OU=Citrix,DC=corp,DC=local

11. 单击 **确定**。

NetScaler Gateway 会话策略方法

NetScaler Gateway 允许管理员指定哪些 Active Directory 组的用户可以通过会话策略或配置文件登录。有关创建 Active Directory 组并将用户添加到其中的信息，请参阅 在 NetScaler Gateway 上创建组。

使用 CLI：

运行以下命令以限制特定组的用户对 NetScaler Gateway 的访问：

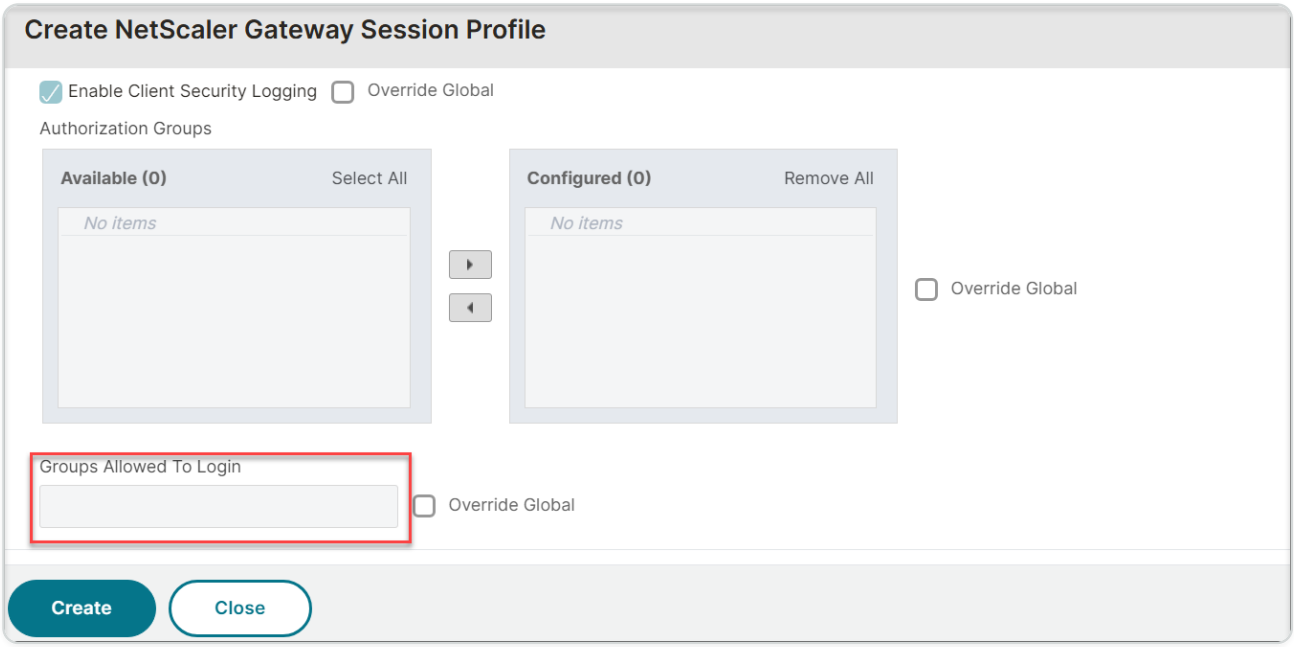
```
set vpn sessionAction sessionActionName -allowedLoginGroups groupName
```

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

使用 GUI：

1. 导航到 **NetScaler Gateway** > **策略** > **会话**。
2. 在详细信息窗格中，单击 **添加**。
3. 在 **名称** 中，键入策略的名称。
4. 在 **配置文件** 旁边，单击 **添加**。
5. 在 **名称** 中，键入配置文件的名称。
6. 单击 **安全** 选项卡并选择 **高级设置**。
7. 在 **允许登录的组** 旁边，选择 **覆盖全局**，然后输入允许登录 NetScaler Gateway 的 **Active Directory** 组。
8. 单击 **创建**。

创建并关闭会话配置文件后，在“**创建 NetScaler Gateway 会话策略**”对话框中创建会话策略的表达式。



NetScaler® Gateway 上的设备姿态检查

从 NetScaler Gateway 14.1 build 43.x 版本开始，Citrix Device Posture 服务已与 NetScaler Gateway 集成。您可以在 NetScaler Gateway 上配置设备姿态检查。此集成仅支持 Citrix Secure Private Access 混合部署。

先决条件

在 NetScaler Gateway 上配置设备姿态检查时，请确保满足以下先决条件：

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

- 客户 ID 已通过 GUI 或 CLI 在 NetScaler Gateway 上设置：
  - CLI 命令：`set dps parameter -CustomerID <CCID>`
  - GUI：**NetScaler Gateway > 全局设置 > 更改 DPS 参数**设置。
- 虚拟服务器 FQDN 已在 VPN 虚拟服务器配置中设置。
- 虚拟服务器 FQDN 已添加到 **Device Posture > 设置**页面中。有关详细信息，请参阅 配置允许的域列表。
- NetScaler SNIP 必须能够访问 Citrix Cloud 服务端点 FQDN `device-posture-controller.cloud.com`。

注意：

- 对于 14.1-56.x 之前的 NetScaler Gateway 版本，请使用 set cloud parameter -CustomerID `<CCID>` -Deployment `<DeploymentType>` 命令配置客户 ID。例如，set cloud parameter -CustomerID krfnzimofi6b -Deployment Production。
- 在用于混合部署的 Secure Private Access 中，set dps parameter -customerID 和 VPN 虚拟服务器 FQDN 会在入职期间自动配置。

通过使用 GUI 启用设备姿态

NetScaler Gateway 上的设备姿态检查可以在全局范围内、VPN 虚拟服务器级别或作为 nFactor 身份验证的一部分启用。

- **全局** - 设备状态检查在任何其他身份验证之前执行。
- **VPN 虚拟服务器级别** - 设备状态扫描仅应用于连接到特定 VPN 虚拟服务器的用户，从而实现精细控制。
- **nFactor 身份验证中的一个因素** - 设备状态扫描可以配置为身份验证过程中的一个步骤。设备状态可以配置为 nFactor 身份验证流程中的第一步、第二步或任何步骤。有关详细信息，请参阅配置 nFactor 身份验证。

在全局级别启用设备状态检查

执行以下步骤以全局启用设备状态：

1. 导航到 **NetScaler Gateway -> 全局设置 -> 更改全局设置**。
2. 单击“**安全**”选项卡。
3. 在“**设备状态**”中，选择“**已启用**”，然后单击“**确定**”。

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

在 VPN 虚拟服务器级别启用设备状态检查

执行以下步骤以针对特定 VPN 虚拟服务器启用设备状态：

1. 导航到 **NetScaler Gateway -> 虚拟服务器**。
2. 在“**NetScaler Gateway 虚拟服务器**”页面上，选择要启用设备状态检查的 VPN 虚拟服务器，然后单击“**编辑**”。
3. 在“**基本设置**”中，单击编辑图标，然后单击“**更多**”。
4. 在“**设备状态**”中，选择“**已启用**”，然后单击“**确定**”。

在 nFactor 身份验证中将设备状态检查作为因素启用

您必须创建一个执行设备姿态扫描的 EPA 操作，然后将此操作作为 nFactor 身份验证流程中的一个因素添加。执行以下步骤将设备姿态作为 nFactor 身份验证流程中的一个因素添加：

注意：

您可以将 EPA 或设备姿态配置为 nFactor 流程中的一个因素。它们可以作为不同的因素存在。但是，如果出现故障，它们之间没有回退机制。

1. 导航到 **安全 -> AAA - 应用程序流量 -> 策略 -> 身份验证 -> 高级策略 -> 操作 -> EPA**。
2. 在“**身份验证 EPA 操作**”页面上，单击“**添加**”。
3. 在“**创建身份验证 EPA 操作**”页面上，更新以下信息，然后单击“**创建**”。
   - **名称：** EPA 操作的名称。
   - **默认组：** 设备姿态检查成功时选择的默认组。
   - **隔离组：** 设备姿态检查失败时选择的隔离组。
   - **设备姿态：** 选择 ENABLED 以启用设备姿态检查。

   注意：

   - **设备姿态**选项默认禁用。现有用户可以继续使用现有 EPA 表达式。
   - 启用**设备姿态**选项后，您无需配置表达式，因为姿态扫描是在设备姿态服务门户中配置的。**终止进程**、**删除文件**和**表达式**字段在 EPA 表达式中变为不可编辑。

4. 将 EPA 操作绑定到策略。有关详细信息，请参阅 配置 nFactor 身份验证 和 将 EPA 扫描作为 nFactor 身份验证的一个因素。

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

- 导航到 **安全 -> AAA - 应用程序流量 > 虚拟服务器**。
- 选择虚拟服务器，然后点击**编辑**。
- 在**高级身份验证策略**中，点击**身份验证策略**，然后点击**添加绑定**。
- 选择之前创建的 EPA 操作。
- 分配优先级并选择下一个因素。
- 点击**绑定**。

使用 CLI 启用设备状态

您可以在以下级别启用设备状态：

- 全局级别

  `set vpn parameter -devicePosture ENABLED`

- VPN 虚拟服务器级别

  `set vpn vserver <vserver-name> -devicePosture ENABLED`

- 作为 nFactor 流程中的一个因素

  将设备状态配置为第一个因素的示例：

  `add authentication epaAction dps_act -devicePosture ENABLED`

  `add authentication Policy dps_pol -rule true -action dps_act`

  `bind authentication vserver dpsspa -policy dps_pol`

  `show authentication vserver dpsspa`

  对于 nFactor 流程，您必须创建一个 EPA 操作和一个身份验证策略，然后将该策略绑定到身份验证虚拟服务器。

参考资料

- 配置设备姿态扫描
- 配置允许的域列表

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

用于身份验证的原生 OTP 支持

NetScaler Gateway 支持一次性密码 (OTP)，无需使用第三方服务器。一次性密码是向安全服务器进行身份验证的高度安全选项，因为生成的数字或密码是随机的。以前，像 RSA 这样的专业公司提供 OTP，它们使用生成随机数的特定设备。该系统必须与客户端保持持续通信，以生成服务器期望的数字。

除了降低资本和运营支出外，此功能还通过将整个配置保留在 NetScaler 设备上，增强了管理员的控制。

注意：

由于不再需要第三方服务器，NetScaler 管理员必须配置一个接口来管理和验证用户设备。

用户必须在 NetScaler Gateway 虚拟服务器上注册才能使用 OTP 解决方案。每个唯一设备只需注册一次，并且可以限制在特定环境中。配置和验证注册用户类似于配置额外的身份验证策略。

原生 OTP 支持的优势

- 通过消除除了 Active Directory 之外，在身份验证服务器上额外基础设施的需求，从而降低运营成本。
- 将配置仅整合到 NetScaler 设备上，从而为管理员提供强大的控制。
- 消除了客户端对额外身份验证服务器的依赖，以生成客户端期望的数字。

原生 OTP 工作流

原生 OTP 解决方案是一个双重过程，其工作流分类如下：

- 设备注册
- 最终用户登录

重要提示： 如果您正在使用第三方解决方案或管理 NetScaler 设备之外的其他设备，则可以跳过注册过程。您添加的最终字符串必须采用 NetScaler 指定的格式。

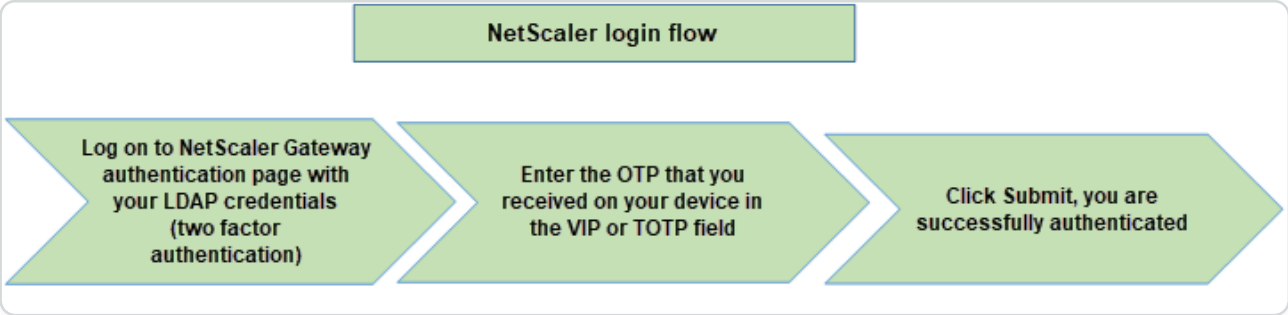
下图描述了注册新设备以接收 OTP 的设备注册流程。

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

注意：

设备注册可以使用任意数量的因素完成。单因素（如上图所示）用作解释设备注册过程的示例。

下图描述了通过已注册设备验证 OTP 的过程。



先决条件

要使用本机 OTP 功能，请确保满足以下先决条件。

- NetScaler 功能版本为 12.0 build 51.24 及更高版本。
- NetScaler Gateway 上已安装 Advanced 或 Premium 版许可证。
- NetScaler Gateway 配置了管理 IP，并且管理控制台可以通过浏览器和命令行访问。
- NetScaler 配置了身份验证、授权和审计虚拟服务器以对用户进行身份验证。
- NetScaler 设备配置了统一网关，并且身份验证、授权和审计配置文件已分配给网关虚拟服务器。
- 本机 OTP 解决方案仅限于 nFactor 身份验证流程。需要高级策略来配置该解决方案。有关更多详细信息，请参阅文章 CTX222713。

此外，请确保 Active Directory 满足以下条件：

- 属性的最小长度为 256 个字符。
- 属性类型必须是“DirectoryString”，例如 UserParameters。这些属性可以保存字符串值。

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

- 如果设备名称包含非英文字符，则属性字符串类型必须为 Unicode。
- NetScaler LDAP 管理员必须对选定的 AD 属性具有写入权限。
- NetScaler 设备和客户端计算机必须与公共网络时间服务器同步。

使用 GUI 配置本机 OTP

本机 OTP 注册不仅仅是单因素身份验证。以下部分将帮助您配置单因素和第二因素身份验证。

为第一因素创建登录架构

1. 导航到 **安全 AAA > 应用程序流量 > 登录架构**。
2. 转到 **Profiles**，然后单击 **Add**。
3. 在 **Create Authentication Login Schema** 页面上，在 **Name** 字段下输入 *lschema_single_auth_manage_otp*，然后单击 **noschema** 旁边的 **Edit**。
4. 单击 **LoginSchema** 文件夹。
5. 向下滚动以选择 **SingleAuth.xml**，然后单击 **Select**。
6. 单击 **Create**。
7. 单击 **Policies**，然后单击 **Add**。
8. 在“**创建身份验证登录架构策略**”屏幕上，输入以下值。

   名称： `lpol_single_auth_manage_otp_by_url` **配置文件：** 从列表中选择 l`pol_single_auth_manage_otp_by_url`。 **规则：** `HTTP.REQ.COOKIE.VALUE("NSC_TASS").EQ("`manageotp`")`

配置身份验证、授权和审计虚拟服务器

1. 导航到“**安全 > AAA – 应用程序流量 > 身份验证虚拟服务器**”。单击以编辑现有虚拟服务器。
2. 单击右侧窗格中“**高级设置**”下的“**登录架构**”旁边的“**+**”图标。
3. 选择“**无登录架构**”。
4. 单击箭头并选择 **lpol_single_auth_manage_otp_by_url** 策略。
5. 选择 **lpol_single_auth_manage_otp_by_url** 策略，然后单击“**选择**”。
6. 单击“**绑定**”。
7. 向上滚动并在“**高级身份验证策略**”下选择“**1 身份验证策略**”。
8. 右键单击“**nFactor 策略**”并选择“**编辑绑定**”。
9. 单击“**选择下一个因子**”下的“**+**”图标，创建一个下一个因子，然后单击“**绑定**”。

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

10. 在“**创建身份验证** `PolicyLabel` ”屏幕上，输入以下内容，然后单击“**继续**”：

    名称：manage_otp_flow_label

    登录架构：Lschema_Int

11. 在 **Authentication PolicyLabel** 屏幕上，单击 **+** 图标以创建策略。
12. 在 **Create Authentication Policy** 屏幕上，输入以下内容：

    名称：auth_pol_ldap_otp_action

13. 使用 **Action Type** 列表选择操作类型。
14. 在 **Action** 字段中，单击 **+** 图标以创建操作。
15. 在 **Create Authentication LDAP server** 页面中，选择 **Server IP** 单选按钮，取消选中 **Authentication** 旁边的复选框，输入以下值，然后选择 **Test Connection**。

    名称：ldap_otp_action

    IP 地址：192.168.10.11

    基本可分辨名称：DC=training, DC=lab

    管理员：Administrator@training.lab

    密码： `xxxxx`

16. 向下滚动到 **Other Settings** 部分。使用下拉菜单选择以下选项。 将 **Server Logon Name Attribute** 设为 **New** 并键入 **userprincipalname**。
17. 使用下拉菜单将 **SSO Name Attribute** 设为 **New** 并键入 **userprincipalname**。
18. 在 **OTP Secret** 字段中输入“UserParameters”，然后单击 **More**。
19. 输入以下属性。

    属性 1 = mail **属性 2** = objectGUID **属性 3** = immutableID

20. 点击**确定**。
21. 在**创建身份验证策略**页面上，将表达式设置为 **true**，然后点击**创建**。
22. 在**创建身份验证策略标签**页面上，点击**绑定**，然后点击**完成**。
23. 在**策略绑定**页面上，点击**绑定**。
24. 在**身份验证策略**页面上，点击**关闭**，然后点击**完成**。

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

注意：

身份验证虚拟服务器必须绑定到 RFWebUI 门户主题。将服务器证书绑定到服务器。服务器 IP ‘1.2.3.5’ 必须具有相应的 FQDN，即 otpauth.server.com，以备后用。

为第二因素 OTP 创建登录架构

1. 导航到**安全 > AAA - 应用程序流量 > 虚拟服务器**。选择要编辑的虚拟服务器。
2. 向下滚动并选择**1 登录架构**。
3. 点击**添加绑定**。
4. 在**策略绑定**部分下，点击**+**图标以添加策略。
5. 在**创建身份验证登录架构策略**页面上，将名称输入为 OTP，然后点击**+**图标以创建配置文件。
6. 在**创建身份验证登录架构**页面上，将名称输入为 OTP，然后点击**noschema**旁边的图标。
7. 单击 **LoginSchema** 文件夹，选择 **DualAuthManageOTP.xml**，然后单击 **Select**。
8. 单击 **Create**。
9. 在 **Rule** 部分中，输入 **True**。单击 **Create**。
10. 单击 **Bind**。
11. 请注意身份验证的两个因素。单击 **Close**，然后单击 **Done**。

配置用于管理 OTP 的内容切换策略

如果您正在使用 Unified Gateway，则需要以下配置。

1. 导航到 **Traffic Management > Content Switching > Policies**。选择内容切换策略，右键单击并选择 **Edit**。
2. 编辑表达式以评估以下 OR 语句，然后单击 **OK**：

is_vpn_url||HTTP.REQ.URL.CONTAINS(“`manageotp`”)

使用 CLI 配置本机 OTP

您必须具备以下信息才能配置 OTP 设备管理页面：

- 分配给身份验证虚拟服务器的 IP
- 与分配的 IP 对应的 FQDN
- 用于身份验证虚拟服务器的服务器证书

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

注意：

原生 OTP 仅是基于 Web 的解决方案。

配置 OTP 设备注册和管理页面

创建身份验证虚拟服务器

```
add authentication vserver authvs SSL 1.2.3.5 443

bind authentication vserver authvs -portaltheme RFWebUI

bind ssl vserver authvs -certkeyname otpauthcert
```

注意：

身份验证虚拟服务器必须绑定到 RFWebUI 门户主题。将服务器证书绑定到服务器。服务器 IP ‘1.2.3.5’ 必须具有相应的 FQDN，即 otpauth.server.com，以供后续使用。

创建 LDAP 登录操作

```
add authentication ldapAction <LDAP ACTION NAME> -serverIP <SERVER IP> -
 serverPort <SERVER PORT> -ldapBase <BASE> -ldapBindDn <AD USER>
-ldapBindDnPassword <PASSWO> -ldapLoginName <USER FORMAT>
```

示例：

```
add authentication ldapAction ldap_logon_action -serverIP 1.2.3.4
-serverPort 636 -ldapBase "OU=Users,DC=server,DC=com" -ldapBindDn
administrator@ctxnsdev.com -ldapBindDnPassword PASSWORD -ldapLoginName
userprincipalname
```

添加 LDAP 登录的身份验证策略

```
add authentication Policy auth_pol_ldap_logon -rule true -action
ldap_logon_action
```

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

通过 LoginSchema 显示 UI

登录时向用户显示用户名和密码字段

```
add authentication loginSchema lschema_single_auth_manage_otp
-authenticationSchema "/nsconfig/loginschema/LoginSchema/
SingleAuthManageOTP.xml"
```

显示设备注册和管理页面

Citrix® 建议通过两种方式显示设备注册和管理屏幕：URL 或主机名。

- **使用 URL**

  当 URL 包含 ‘/manageotp’ 时

  - `add authentication loginSchemaPolicy lpol_single_auth_manage_otp_by_url -rule 'http.req.cookie.value("NSC_TASS").contains("manageotp")' -action lschema_single_auth_manage_otp`
  - `bind authentication vserver authvs -policy lpol_single_auth_manage_otp_by_url -priority 10 -gotoPriorityExpression END`

- **使用主机名**

  当主机名为“alt.server.com”时

  - `add authentication loginSchemaPolicy lpol_single_auth_manage_otp_by_host -rule 'http.req.header("host").eq("alt.server.com")' -action lschema_single_auth_manage_otp`
  - `bind authentication vserver authvs -policy lpol_single_auth_manage_otp_by_host -priority 20 -gotoPriorityExpression END`

使用 CLI 配置用户登录页面

您必须具备以下信息才能配置用户登录页面：

- 负载平衡虚拟服务器的 IP
- 负载平衡虚拟服务器对应的 FQDN
- 负载平衡虚拟服务器的服务器证书

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

```
bind ssl vserver lbvs_https -certkeyname lbvs_server_cert
```

负载平衡中的后端服务表示如下：

```
add service iis_backendsso_server_com 1.2.3.210 HTTP 80

bind lb vserver lbvs_https iis_backendsso_server_com
```

创建 OTP 密码验证操作

```
add authentication ldapAction <LDAP ACTION NAME> -serverIP <SERVER IP>
-serverPort <SERVER PORT> -ldapBase <BASE> -ldapBindDn <AD USER>
-ldapBindDnPassword <PASSWORD> -ldapLoginName <USER FORMAT>
-authentication DISABLED -OTPSecret <LDAP ATTRIBUTE>
```

示例：

```
add authentication ldapAction ldap_otp_action -serverIP 1.2.3.4
-serverPort 636 -ldapBase "OU=Users,DC=server,DC=com" -ldapBindDn
administrator@ctxnsdev.com -ldapBindDnPassword PASSWORD -ldapLoginName
userprincipalname -authentication DISABLED -OTPSecret userParameters
```

重要提示：

LDAP 登录和 OTP 操作之间的区别在于需要禁用身份验证并引入新参数 `OTPSecret`。请勿使用 AD 属性值。

添加用于 OTP 密码验证的身份验证策略

```
add authentication Policy auth_pol_otp_validation -rule true -action
ldap_otp_action
```

通过 LoginSchema 呈现双因素身份验证

添加双因素身份验证的用户界面。

```
add authentication loginSchema lscheme_dual_factor -authenticationSchema
"/nsconfig/loginschema/LoginSchema/DualAuth.xml"
```

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

```
add authentication loginSchemaPolicy lpol_dual_factor -rule true -action
lscheme_dual_factor
```

通过策略标签创建密码验证因子

为下一个因子创建管理 OTP 流程策略标签（第一个因子是 LDAP 登录）

```
add authentication loginSchema lschema_noschema -authenticationSchema
noschema

add authentication policylabel manage_otp_flow_label -loginSchema
lschema_noschema
```

将 OTP 策略绑定到策略标签

```
bind authentication policylabel manage_otp_flow_label -policyName
 auth_pol_otp_validation -priority 10 -gotoPriorityExpression NEXT
```

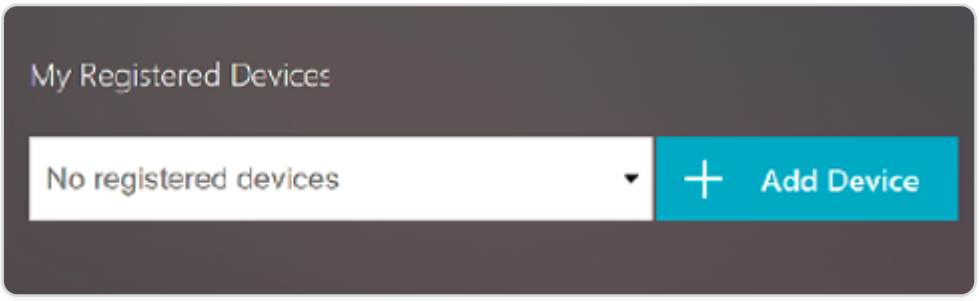
绑定 UI 流程

将 LDAP 登录和 OTP 验证绑定到身份验证虚拟服务器。

```
bind authentication vserver authvs -policy auth_pol_ldap_logon -priority
10 -nextFactor  manage_otp_flow_label -gotoPriorityExpression NEXT

bind authentication vserver authvs -policy lpol_dual_factor -priority 30
-gotoPriorityExpression END
```

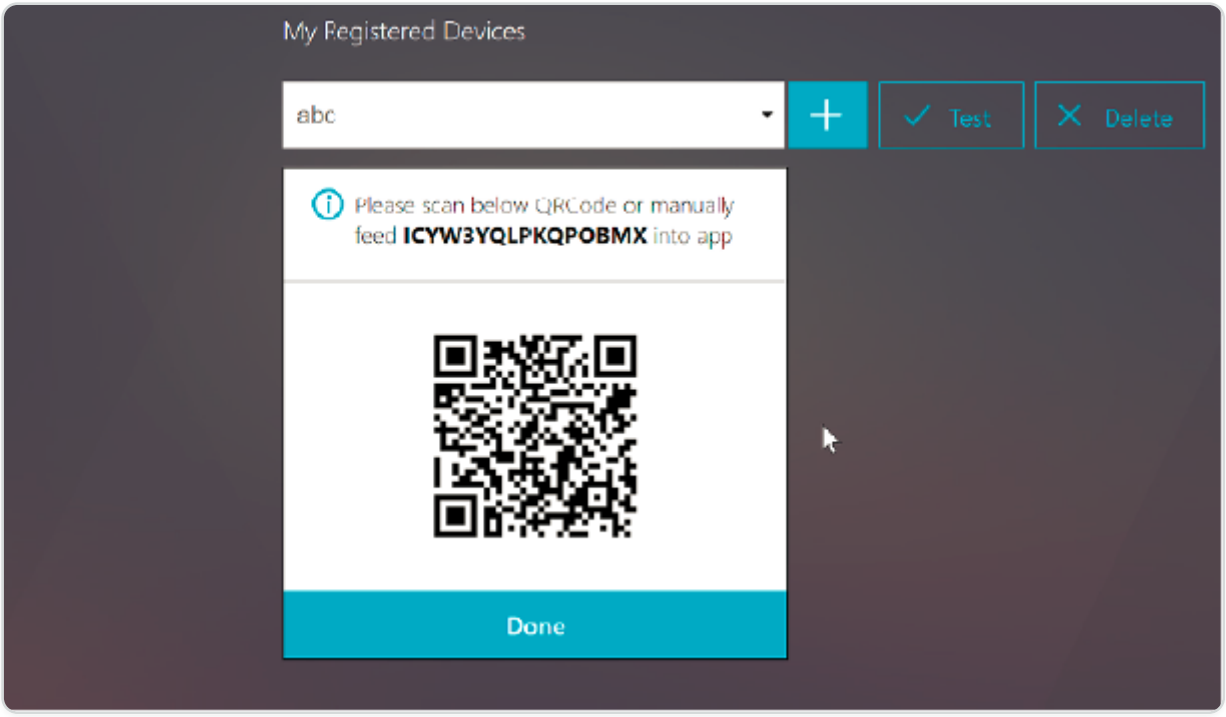
向 NetScaler 注册您的设备

1. 导航到您的 NetScaler FQDN（第一个面向公众的 IP），并带有 /manageotp 后缀。例如，`<https://otpauth.server.com/manageotp>` 使用用户凭据登录。
2. 单击 **+** 图标以添加设备。



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

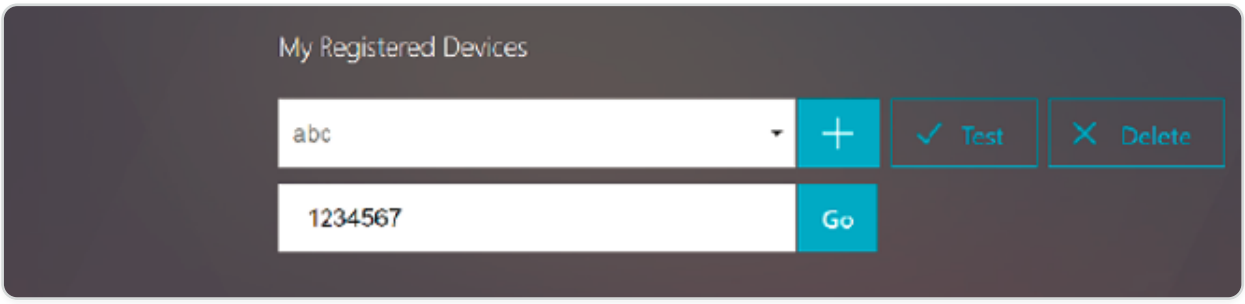
3. 输入设备名称，然后按 **Go**。屏幕上会出现一个条形码。
4. 单击 **Begin Setup**，然后单击 **Scan Barcode**。
5. 将设备摄像头悬停在二维码上方。您可以选择输入代码。



注意：

显示的二维码有效期为 3 分钟。

6. 成功扫描后，您将看到一个 6 位数的有时效性的代码，可用于登录。

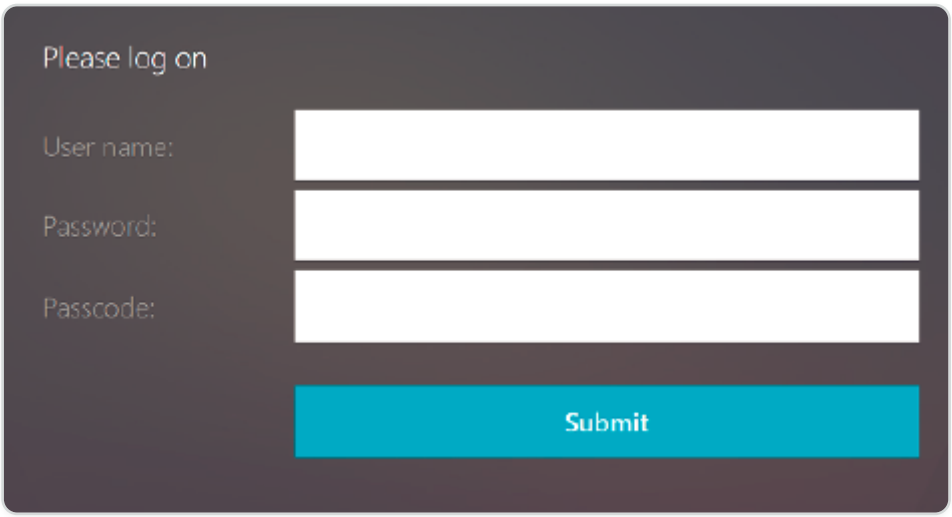


7. 要测试，请在二维码屏幕上单击**完成**，然后单击右侧的绿色复选标记。
8. 从下拉菜单中选择您的设备，然后输入 Google Authenticator 中的代码（必须是蓝色，而不是红色），然后单击**Go**。
9. 请务必使用页面右上角的下拉菜单注销。

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

使用 OTP 登录 NetScaler

1. 导航到您的第一个面向公众的 URL，然后输入 Google Authenticator 中的 OTP 进行登录。
2. 对 NetScaler 启动页进行身份验证。



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

使用高可用性

高可用性部署的两个 NetScaler Gateway 设备可以在任何事务中提供不间断的操作。当您将一个设备配置为主节点，另一个配置为辅助节点时，主节点接受连接并管理服务器，而辅助节点则监视主节点。如果由于任何原因主节点无法接受连接，辅助节点将接管。

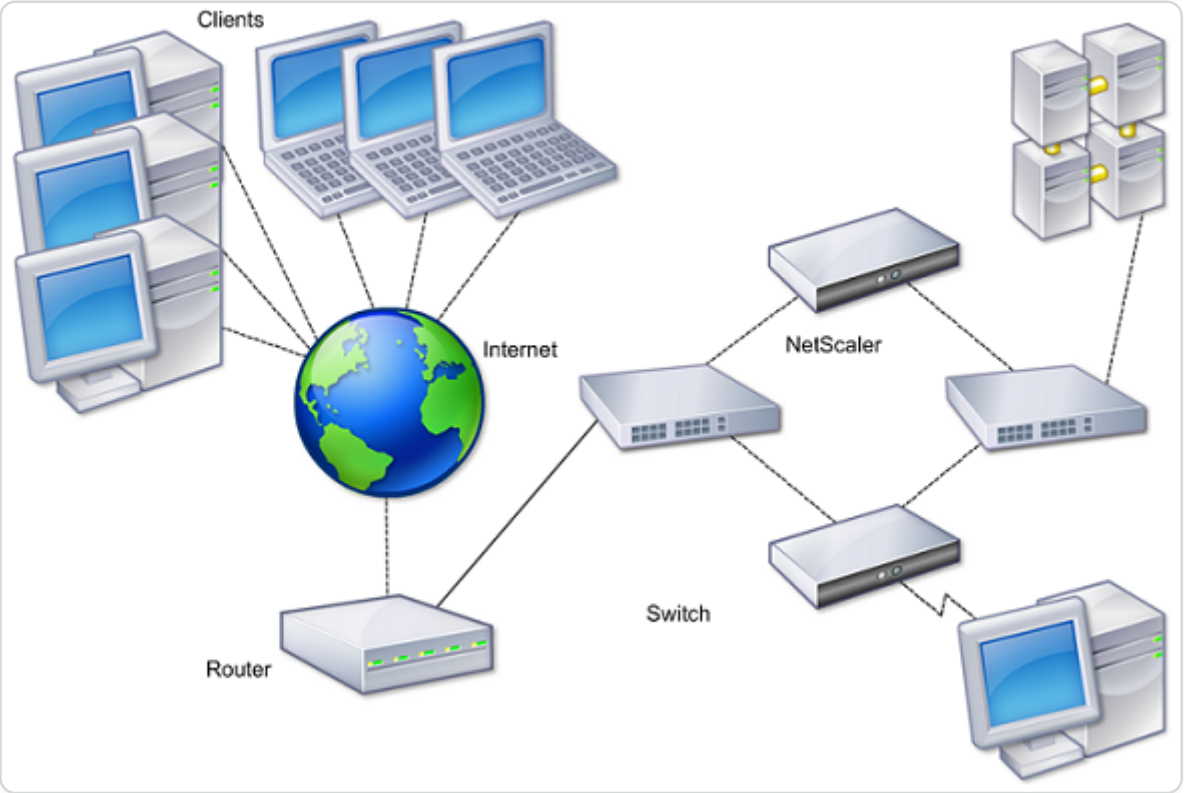
辅助节点通过发送周期性消息（通常称为心跳消息或健康检查）来监视主节点，以确定主节点是否正在接受连接。如果健康检查失败，辅助节点会在指定的时间段内重试连接，之后它会确定主节点未正常运行。然后，辅助节点会接管主节点（此过程称为故障转移）。

故障转移后，所有客户端都必须重新建立与托管服务器的连接，但会话持久性规则将保持不变，与故障转移之前相同。

启用 Web 服务器日志记录持久性后，不会因故障转移而丢失任何日志数据。要启用日志记录持久性，日志服务器配置必须在 log.conf 文件中包含两个系统的条目。

下图显示了具有高可用性对的网络配置。

图 1. 高可用性配置中的 NetScaler Gateway 设备



配置高可用性的基本步骤如下：

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

1. 创建基本设置，使两个节点位于同一子网中。
2. 自定义节点通信健康检查信息的间隔。
3. 自定义节点保持同步的过程。
4. 自定义命令从主节点传播到辅助节点的方式。
5. （可选）配置故障安全模式，以防止出现两个节点都不是主节点的情况。
6. 如果您的环境包含不接受 NetScaler Gateway 无偿 ARP 消息的设备，请配置虚拟 MAC 地址。

当您准备好进行更复杂的配置时，您可以在不同的子网中配置高可用性节点。

为了提高高可用性设置的可靠性，您可以配置路由监视器并创建冗余链接。在某些情况下，例如在故障排除或执行维护任务时，您可能希望强制一个节点进行故障转移（将主状态分配给另一个节点），或者您可能希望强制辅助节点保持辅助状态，或强制主节点保持主状态。

高可用性工作原理

当您将 NetScaler Gateway 配置为高可用性对时，辅助 NetScaler Gateway 通过发送周期性消息（也称为心跳消息或健康检查）来监视第一个设备，以确定第一个设备是否正在接受连接。如果健康检查失败，辅助 NetScaler Gateway 会在指定时间内再次尝试连接，直到确定主设备不工作为止。如果辅助设备确认健康检查失败，辅助 NetScaler Gateway 将接管主 NetScaler Gateway 的工作。这称为故障转移。

以下端口用于在 NetScaler Gateway 设备之间交换与高可用性相关的信息：

- UDP 端口 3003 用于交换 hello 数据包，以在间隔时间内通信状态。
- TCP 端口 3010 用于高可用性配置同步。
- TCP 端口 3011 用于同步配置设置。

配置高可用性的准则

在配置高可用性对之前，您必须查看以下准则：

- 每个 NetScaler Gateway 设备必须运行相同版本的 NetScaler Gateway 软件。您可以在配置实用程序的页面顶部找到版本号。
- NetScaler Gateway 不会自动在两个设备之间同步密码。您可以选择为每个 NetScaler Gateway 配置对中另一个设备的用户名和密码。
- 主 NetScaler Gateway 和辅助 NetScaler Gateway 上的配置文件 ns.conf 中的条目必须匹配，但有以下例外：

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

- 主 NetScaler Gateway 和辅助 NetScaler Gateway 设备必须各自配置其唯一的系统 IP 地址。使用安装向导在任一 NetScaler Gateway 上配置或修改系统 IP 地址。
- 在高可用性对中，NetScaler Gateway ID 和关联的 IP 地址必须指向另一个 NetScaler Gateway。

  例如，如果您有两个设备，名为 AG1 和 AG2，您必须使用 AG2 的唯一 NetScaler Gateway ID 和 IP 地址配置 AG1。您必须使用 AG1 的唯一 NetScaler Gateway ID 和 IP 地址配置 AG2。

  注意：每个 NetScaler Gateway 设备始终被标识为节点 0。为每个设备配置唯一的节点 ID。

- 高可用性对中的每个设备都必须具有相同的许可证。有关许可的更多信息，请参阅 许可。
- 如果您在任一节点上创建配置文件时使用的方法未直接通过配置实用程序或命令行界面（例如，导入 SSL 证书或更改启动脚本），则必须将配置文件复制到另一个节点，或在该节点上创建相同的文件。
- 配置高可用性对时，请确保主设备和辅助设备的映射 IP 地址和默认网关地址相同。如有必要，您可以随时通过运行安装向导来更改映射的 IP 地址。

您可以使用预安装清单来查看在高可用性部署中需要配置的特定设置列表。有关详细信息，请参阅 预安装清单。

配置高可用性设置

要设置高可用性配置，您需要创建两个节点，每个节点都将另一个节点的 NetScaler Gateway IP 地址定义为远程节点。您可以首先登录到要配置高可用性的两台 NetScaler 设备之一，然后添加一个节点。将另一台设备的 NetScaler Gateway IP 地址指定为新节点的地址。然后，登录到另一台设备，添加一个具有第一台设备的 NetScaler Gateway IP 地址的节点。算法将决定哪个节点成为主节点，哪个节点成为辅助节点。

在配置设备之前，请添加一个高可用性节点。此节点表示高可用性对中的第一个或第二个 NetScaler Gateway。要配置高可用性，您首先创建节点，然后配置高可用性设置。

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

重要提示：

- 为确保无缝高可用性和不间断的 HDX™ insight 功能，两个节点在同一软件版本上运行至关重要。升级期间的版本不匹配可能会中断基本会话数据的收集，从而导致潜在的服务中断并在故障转移后生成“跳过代码 143”错误。因此，在升级期间或升级后，不会为现有 ICA 连接填充 HDX insight 数据。
- 当主节点和辅助节点之间的数据同步不完整时，辅助节点可能缺乏足够的信息来无缝恢复连接。这可能导致 NetScaler Gateway 无法检索必要的 HDX insight 数据，从而导致“跳过代码 169”错误。因此，在故障转移场景中，HDX insight 支持可能会暂时中断。

添加高可用性节点

1. 在配置实用程序中，在“配置”选项卡上，在导航窗格中，展开 **系统 > 高可用性**。
2. 在详细信息窗格中，在“节点”选项卡上，单击 **添加**。
3. 在“**创建 HA 节点**”页面中，在“**远程节点 IP 地址**”文本框中，键入要添加为远程节点的 NetScaler 的 NSIP 地址。如果 NetScaler Gateway IP 地址是 IPv6 地址，请在输入地址之前选中“**IPv6**”复选框。
4. 如果要自动将本地节点添加到远程节点，请选择“配置远程系统以参与高可用性设置”。如果不选择此选项，您必须登录到远程节点所代表的设备，并添加当前正在配置的节点。
5. 单击以启用 **关闭 HA 监视器中已关闭的接口/通道**。
6. 如果远程设备具有不同的用户名和密码，请在“远程系统登录凭据”中，单击“远程系统的登录凭据与自节点不同”。
7. 在“**用户名**”中，键入远程设备的用户名。
8. 在“**密码**”中，键入远程设备的密码。
9. 单击 **OK**。

启用或禁用辅助节点

您只能禁用或启用辅助节点。禁用辅助节点时，它会停止向主节点发送心跳消息，因此主节点无法再检查辅助节点的状态。启用节点后，该节点将参与高可用性配置。

1. 在配置实用程序中，在“配置”选项卡上，在导航窗格中，展开“系统”，然后单击“高可用性”。
2. 在详细信息窗格中，在“节点”选项卡上，选择本地节点，然后单击“打开”。
3. 在“HA 配置节点”对话框中，在“高可用性状态”中，选择“已启用(不参与 HA)”。
4. 单击“确定”。状态栏中显示一条消息，指示节点已成功配置。

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

配置高可用性设置

1. 在配置实用程序中，在“配置”选项卡上，在导航窗格中，展开 **系统 > 高可用性**。
2. 在详细信息窗格中，在“节点”选项卡上，选择一个节点，然后单击 **编辑**。
3. 在 **HA 配置节点** 对话框中，在“ID”中，键入节点标识符的编号。ID 指定其他设备的唯一节点编号。
4. 在 **IP 地址** 中，键入系统 IP 地址，然后单击“确定”。IP 地址指定其他设备的 IP 地址。

注意：高可用性对中节点的 ID 最大值为 64。

更改 RPC 节点密码

为了与其他 NetScaler Gateway 设备通信，每个设备都需要了解其他设备，包括如何在 NetScaler Gateway 上进行身份验证。RPC 节点是内部系统实体，用于系统间配置和会话信息的通信。每个 NetScaler Gateway 上都存在一个 RPC 节点，并存储信息，例如其他 NetScaler Gateway 设备的 IP 地址以及用于身份验证的密码。与另一个 NetScaler Gateway 建立联系的 NetScaler Gateway 会检查 RPC 节点中的密码。

NetScaler Gateway 要求高可用性对中的两个设备都具有 RPC 节点密码。两个设备上的密码必须相同。主设备必须知道辅助 RPC 节点密码，辅助设备必须知道主 RPC 节点密码。最初，每个 NetScaler Gateway 都配置了相同的 RPC 节点密码。为了增强安全性，您必须更改默认的 RPC 节点密码。您可以使用配置实用程序来配置和更改 RPC 节点。

RPC 节点是在添加节点或添加全局服务器负载平衡 (GSLB) 站点时隐式创建的。您无法手动创建或删除 RPC 节点。

重要：

您还必须保护设备之间的网络连接。您可以在配置 RPC 节点密码时，通过选择“**安全**”复选框来配置安全性。

更改 RPC 节点密码并启用安全连接

1. 导航到 **系统 > 网络 > RPC**。
2. 在详细信息窗格中，选择节点，然后单击“**编辑**”。
3. 在“**密码**”和“**确认密码**”中，键入新密码。
4. 在“**源 IP 地址**”中，键入其他 NetScaler Gateway 设备的系统 IP 地址。
5. 单击“**安全**”，然后单击“**确定**”。

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

注意：

启用“**安全**”选项后，设备会加密从该节点发送到其他 RPC 节点的所有通信，从而保护 RPC 通信。

使用 CLI 更改 RPC 节点密码

在命令提示符下，键入：

```
set ns rpcNode <IPAddress> {-password} [-secure ( YES | NO )]



show ns rpcNode
```

示例：

```
> set ns rpcNode 192.0.2.4 -password mypassword -secure YES

 Done

> show rpcNode

.

.

.

 IPAddress:  192.0.2.4 Password:  d336004164d4352ce39e

     SrcIP:  *           Secure:  ON

Done

>
```

配置主备设备以实现高可用性

更改 RPC 节点密码并启用安全通信后，使用配置实用程序配置主备 NetScaler Gateway 高可用性节点。

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

1. 在配置实用程序中，在“配置”选项卡上的导航窗格中，展开“系统”，然后单击“高可用性”。
2. 在详细信息窗格中，在“节点”选项卡上，选择一个节点，然后单击“编辑”。
3. 在“高可用性状态”下，单击“已启用(主动参与 HA)”，然后单击“确定”。

配置通信间隔

当您将 NetScaler Gateway 配置为高可用性对时，您可以将辅助 NetScaler Gateway 配置为以特定间隔（以毫秒 (msec) 为单位）进行侦听。这些间隔称为 hello 间隔和 dead 间隔。

hello 间隔是向对等节点发送心跳消息的间隔。dead 间隔是如果未收到心跳数据包，对等节点被标记为 DOWN 的时间间隔。心跳消息是发送到高可用性对中另一个节点的端口 3003 的 UDP 数据包。

配置 hello 间隔时，可以使用 200 到 1000 之间的值。默认值为 200。dead 间隔值为 3 到 60。默认值为 3。

注意

dead 间隔必须设置为 hello 间隔的倍数。

配置辅助 NetScaler Gateway 的通信间隔

1. 在配置实用程序中，在“配置”选项卡上，在导航窗格中，展开“系统”，然后单击“高可用性”。
2. 在详细信息窗格中，在“节点”选项卡上，选择一个节点，然后单击“编辑”。
3. 在“间隔”下，执行以下一项或两项操作：
   - 在“Hello 间隔 (msec)”中，键入值，然后单击“确定”。默认值为 200 毫秒。
   - 在“Dead 间隔 (secs)”中，键入值，然后单击“确定”。默认设置为三秒。

同步 NetScaler Gateway 设备

高可用性对中的 NetScaler Gateway 设备自动同步默认启用。通过自动同步，您可以对一台设备进行更改，并使更改自动传播到第二台设备。同步使用端口 3010。

同步在以下情况发生时开始：

- 辅助节点重新启动。
- 主节点在故障转移后成为辅助节点。

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

您可以禁用同步，这会阻止辅助 NetScaler Gateway 在主设备发生更改时将其配置与主 NetScaler Gateway 同步。您还可以强制同步。

您可以在对中的辅助节点上启用或禁用高可用性同步。

启用或禁用高可用性同步

1. 在配置实用程序中，在“配置”选项卡上，在导航窗格中，展开“系统”，然后单击“高可用性”。
2. 在详细信息窗格中，在“节点”选项卡上，选择一个节点，然后单击“编辑”。
3. 在“配置节点”对话框中，在“HA 同步”下，执行以下操作之一：
   - 要禁用同步，请清除“辅助节点将从主节点获取配置”复选框。
   - 要启用同步，请选择“辅助节点将从主节点获取配置”复选框。
4. 单击“确定”。状态栏中会出现一条消息，指示节点配置成功。

强制设备之间同步

除了自动同步之外，NetScaler Gateway 还支持高可用性对中两个节点之间的强制同步。

您可以在主 NetScaler Gateway 设备和辅助 NetScaler Gateway 设备上强制同步。但是，如果同步已在进行中，则命令将失败，并且 NetScaler Gateway 会显示警告。在以下情况下，强制同步也会失败：

- 您在独立系统上强制同步。
- 辅助节点已禁用。
- 您在辅助节点上禁用高可用性同步。

1. 在配置实用程序中，在“配置”选项卡上的导航窗格中，展开“系统”，然后单击“高可用性”。
2. 在“节点”选项卡上，单击“强制同步”。

在高可用性设置中同步配置文件

在高可用性设置中，您可以将各种配置文件从主节点同步到辅助节点。

在高可用性设置中同步文件的参数

模式

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

```
要执行的同步类型。以下描述在括号中包含指定该选项的命令行参数。

-  **除许可证和 rc.conf 之外的所有内容** (all)。同步与系统配置、NetScaler Gateway
书签、SSL 证书、SSL CRL 列表、HTML 注入脚本和应用程序防火墙 XML 对象相关的文件。

-  **书签** (bookmarks)。同步所有 NetScaler Gateway 书签。

-  **SSL 证书和密钥** (`ssl`)。同步 SSL 功能的所有证书、密钥和 CRL。

-  **许可证和 rc.conf** (misc)。同步所有许可证文件和 rc.conf 文件。

-  **包括许可证和 rc.conf 在内的所有内容** (all\_plus\_misc)。同步与系统配置、
NetScaler Gateway 书签、SSL 证书、SSL CRL 列表、HTML 注入脚本、应用程序防火墙 XML
对象、许可证和 rc.conf 文件相关的文件。
```

注意：如果您在设备上安装了 NetScaler 许可证，则有更多选项可用。

使用配置实用程序在高可用性设置中同步文件

1. 在导航窗格中，展开**系统**，然后单击**诊断**。
2. 在详细信息窗格中，在**实用程序**下，单击**启动 HA 文件同步**。
3. 在**启动文件同步**对话框中，在**模式**菜单中，选择适当的同步类型（例如，除许可证和 rc.conf 之外的所有内容），然后单击**确定**。

配置命令传播

在高可用性设置中，主节点上发出的任何命令都会在命令在主节点上运行之前自动传播到辅助节点并在其上运行。如果命令传播失败，或者命令在辅助节点上执行失败，主节点将运行该命令并记录错误。命令传播使用端口 3011。

在高可用性对配置中，命令传播在主节点和辅助节点上默认启用。您可以在高可用性对中的任一节点上启用或禁用命令传播。如果在主节点上禁用命令传播，则命令不会传播到辅助节点。如果在辅助节点上禁用命令传播，则从主节点传播的命令不会在辅助节点上运行。

注意：重新启用传播后，请记住强制同步。

注意：如果在禁用传播时发生同步，则在禁用传播生效之前所做的任何与配置相关的更改都将与辅助节点同步。对于在同步进行时禁用传播的情况，此规则同样适用。

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

在主节点上启用或禁用传播

1. 在配置实用程序中，在“Configuration”（配置）选项卡上的导航窗格中，展开 **“System”**（系统），然后单击 **“High Availability”**（高可用性）。
2. 在详细信息窗格的 **“Nodes”**（节点）选项卡上，选择一个节点，然后单击 **“Edit”**（编辑）。
3. 在 **HA 传播** 下，执行以下操作之一：
   - 要禁用高可用性传播，请清除 **“Primary node propagates configuration to the Secondary”**（主节点将配置传播到辅助节点）复选框。
   - 要启用高可用性传播，请选择 **“Primary node propagates configuration to the Secondary”**（主节点将配置传播到辅助节点）复选框。
4. 单击 **“OK”**（确定）。

命令传播故障排除

以下列表描述了命令传播可能失败的原因，以及恢复设置的解决方案：

- 网络连接不正常。如果命令传播失败，请检查主 NetScaler Gateway 设备和辅助 NetScaler Gateway 设备之间的网络连接。
- 辅助 NetScaler Gateway 上缺少资源。如果命令在主 NetScaler Gateway 上执行成功但未能传播到辅助 NetScaler Gateway，请直接在辅助 NetScaler Gateway 上运行该命令以查看错误消息。错误可能发生的原因是命令所需的资源存在于主 NetScaler Gateway 上，但在辅助 NetScaler Gateway 上不可用。此外，请验证每个设备上的许可证文件是否匹配。

  例如，验证所有 Secure Sockets Layer (SSL) 证书是否存在于每个 NetScaler Gateway 上。验证任何初始化脚本自定义是否存在于两个 NetScaler Gateway 设备上。
- 身份验证失败。如果您收到身份验证失败错误消息，请验证每个设备上的 RPC 节点设置。

配置故障安全模式

在高可用性配置中，故障安全模式可确保当两个节点都未能通过健康检查时，始终有一个节点是主节点。故障安全模式可确保当节点仅部分可用时，备份方法可以激活并处理流量。

您可以在每个节点上独立配置高可用性故障安全模式。

下表显示了一些故障安全情况。NOT_UP 状态表示节点未能通过健康检查，但节点仍部分可用。UP 状态表示节点通过了健康检查。

表 1. 故障安全模式情况

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

节点 A（主）健康状态	节点 B（辅助）健康状态	默认高可用性行为	启用故障安全的高可用性行为	描述
NOT_UP (最后失败)	NOT_UP (首先失败)	A（辅助），B（辅助）	A（主），B（辅助）	如果两个节点相继发生故障，则最后一个主节点仍保持主节点状态。
NOT_UP (首先失败)	NOT_UP (最后失败)	A (辅助), B (辅助)	A (辅助), B (主)	如果两个节点相继发生故障，则最后一个主节点仍保持主节点状态。
正常	正常	A (主), B (辅助)	A (主), B (辅助)	如果两个节点都通过了运行状况检查，则在启用故障安全模式的情况下行为没有变化。
正常	NOT_UP	A (主), B(辅助)	A (主), B (辅助)	如果只有辅助节点发生故障，则在启用故障安全模式的情况下行为没有变化。
NOT_UP	UP	A (辅助), B (主)	A (辅助), B (主)	如果只有主节点发生故障，在启用故障安全模式的情况下，行为没有变化。
NOT_UP	UP (STAYSECONDARY)	A (辅助), B (辅助)	A (主), B (辅助)	如果辅助节点配置为 STAYSECONDARY，即使主节点发生故障，它仍保持为主节点。

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

配置故障安全模式

1. 在配置实用程序中，在“配置”选项卡上，在导航窗格中，展开“系统”，然后单击“高可用性”。
2. 在详细信息窗格中，在“节点”选项卡上，选择一个节点，然后单击“编辑”。
3. 在“配置节点”对话框中，在“故障安全模式”下，选择“即使两个节点都不正常，也保持一个主节点”，然后单击“确定”。

配置虚拟 MAC 地址

虚拟 MAC 地址由高可用性设置中的主 NetScaler Gateway 设备和辅助 NetScaler Gateway 设备共享。

在高可用性设置中，主 NetScaler Gateway 拥有所有浮动 IP 地址，例如映射的 IP 地址或虚拟 IP 地址。它使用自己的 MAC 地址响应这些 IP 地址的地址解析协议 (ARP) 请求。因此，外部设备（例如路由器）的 ARP 表会使用浮动 IP 地址和主 NetScaler Gateway MAC 地址进行更新。发生故障转移时，辅助 NetScaler Gateway 将接管成为新的主 NetScaler Gateway。然后，它使用免费地址解析协议 (GARP) 来通告它从主设备获取的浮动 IP 地址。新主设备通告的 MAC 地址是其自身接口的 MAC 地址。

某些设备不接受 NetScaler Gateway 生成的 GARP 消息。因此，一些外部设备会保留旧主 NetScaler Gateway 通告的旧 IP 到 MAC 映射。这种情况可能导致站点不可用。为了解决此问题，您需要在高可用性对的两个 NetScaler Gateway 设备上配置虚拟 MAC 地址。此配置意味着两个 NetScaler Gateway 设备具有相同的 MAC 地址。因此，当发生故障转移时，辅助 NetScaler Gateway 的 MAC 地址保持不变，并且外部设备上的 ARP 表无需更新。

要创建虚拟 MAC 地址，请创建虚拟路由器标识符 (ID) 并将其绑定到接口。在高可用性设置中，用户需要将 ID 绑定到两个设备上的接口。

当虚拟路由器 ID 绑定到接口时，系统会生成一个虚拟 MAC 地址，其中虚拟路由器 ID 作为最后一个八位字节。通用虚拟 MAC 地址的一个示例是 00:00:5e:00:01:\<VRID\>。例如，如果您创建了一个值为 60 的虚拟路由器 ID 并将其绑定到接口，则生成的虚拟 MAC 地址为 00:00:5e:00:01:3c，其中 3c 是虚拟路由器 ID 的十六进制表示。您可以创建 255 个虚拟路由器 ID，范围从 1 到 254。

您可以为 IPv4 和 IPv6 配置虚拟 MAC 地址。

配置 IPv4 虚拟 MAC 地址

当您创建 IPv4 虚拟 MAC 地址并将其绑定到接口时，从该接口发送的任何 IPv4 数据包都将使用绑定到该接口的虚拟 MAC 地址。如果没有 IPv4 虚拟 MAC 地址绑定到接口，则使用该接口的物理 MAC 地址。

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

通用虚拟 MAC 地址的形式为 00:00:5e:00:01:\<VRID\>。例如，如果您创建值为 60 的 VRID 并将其绑定到接口，则生成的虚拟 MAC 地址为 00:00:5e:00:01:3c，其中 3c 是 VRID 的十六进制表示。您可以创建 255 个 VRID，其值范围为 1 到 255。

创建或修改 IPv4 虚拟 MAC 地址

您可以通过为其分配虚拟路由器 ID 来创建 IPv4 虚拟 MAC 地址。然后，您可以将虚拟 MAC 地址绑定到接口。您不能将多个虚拟路由器 ID 绑定到同一接口。要验证虚拟 MAC 地址配置，您必须显示并检查虚拟 MAC 地址以及绑定到虚拟 MAC 地址的接口。

配置虚拟 MAC 地址的参数

- VRID

> 标识虚拟 MAC 地址的虚拟路由器 ID。可能的值：1–255。

- `ifnum`

> 要绑定到虚拟 MAC 地址的接口编号（插槽/端口表示法）。

配置虚拟 MAC 地址

1. 导航到 **System > Network**，然后单击 **VMAC**。
2. 在详细信息窗格中，在 **VMAC** 选项卡上，单击 **Add**。
3. 在 **Create VMAC** 对话框中，在 **Virtual Router ID** 中，键入值。
4. 在 **Associated Interfaces** 下，在 **Available Interfaces** 中，选择一个网络接口，单击 **Add**，单击 **Create**，然后单击 **Close**。

创建虚拟 MAC 地址后，它会显示在配置实用程序中。如果您选择了网络接口，则虚拟路由器 ID 将绑定到该接口。

删除虚拟 MAC 地址

要删除虚拟 MAC 地址，您需要删除相应的虚拟路由器 ID。

1. 导航到 **系统 > 网络**，然后单击 **VMAC**。
2. 在详细信息窗格中，选择一个项目，然后单击 **删除**。

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

绑定和解除绑定虚拟 MAC 地址

创建虚拟路由器 ID 时，您在 NetScaler Gateway 上选择了一个网络接口，然后将虚拟路由器 ID 绑定到该网络接口。您还可以从网络接口解除绑定虚拟 MAC 地址，但将 MAC 地址保留在 NetScaler Gateway 上。

1. 导航到 **系统 > 网络**，然后单击 **VMAC**。
2. 在详细信息窗格中，选择一个项目，然后单击 **打开**。
3. 在 **已配置接口** 下，选择一个网络接口，单击 **删除**，单击 **确定**，然后单击 **关闭**。

配置 IPv6 虚拟 MAC 地址

NetScaler Gateway 支持 IPv6 数据包的虚拟 MAC 地址。您可以将任何接口绑定到 IPv6 的虚拟 MAC 地址，即使该接口已绑定 IPv4 虚拟 MAC 地址。从该接口发送的任何 IPv6 数据包都将使用绑定到该接口的虚拟 MAC 地址。如果没有虚拟 MAC 地址绑定到接口，则 IPv6 数据包将使用物理 MAC 地址。

创建或修改 IPv6 虚拟 MAC 地址

通过为其分配 IPv6 虚拟路由器 ID 来创建 IPv6 虚拟 MAC 地址。然后将虚拟 MAC 地址绑定到接口。您不能将多个 IPv6 虚拟路由器 ID 绑定到同一个接口。要验证虚拟 MAC 地址配置，请显示并检查虚拟 MAC 地址以及绑定到虚拟 MAC 地址的接口。

配置 IPv6 虚拟 MAC 地址的参数

- `Virtual Router ID`

  标识虚拟 MAC 地址的虚拟路由器 ID。可能的值：1–255。

- `ifnum`

  要绑定到虚拟 MAC 地址的接口编号（插槽/端口表示法）。

配置 IPv6 虚拟 MAC 地址

1. 在配置实用程序中，在“配置”选项卡上，展开 **系统 > 网络**，然后单击“VMAC”。
2. 在详细信息窗格中，在“VMAC6”选项卡上，执行以下操作之一：
   - 要创建新的虚拟 MAC 地址，请单击“添加”。
   - 要修改现有虚拟 MAC 地址，请单击“打开”。
3. 在“创建 VMAC6”或“配置 VMAC6”对话框中，在“虚拟路由器 ID”中输入值，例如 vrID6。
4. 在“关联接口”中，单击 **添加 > 创建 > 关闭**。状态栏中将显示一条消息，指示虚拟 MAC 地址已配置。

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

删除 IPv6 虚拟 MAC 地址

1. 在配置实用程序中，在“配置”选项卡上，展开 **系统 > 网络**，然后单击“VMAC”。
2. 在详细信息窗格中，在“VMAC6”选项卡上，选择要删除的虚拟路由器 ID，然后单击“删除”。状态栏中会显示一条消息，指示虚拟 MAC 地址已删除。

在不同子网中配置高可用性对

典型的高可用性部署是高可用性对中的两个设备都位于同一子网中。高可用性部署也可以由两个 NetScaler Gateway 设备组成，其中每个设备位于不同的网络中。本主题描述了后一种配置，并包括示例配置以及同一网络内和跨网络的高可用性配置之间的差异列表。

您还可以配置链路冗余和路由监视器。这些 NetScaler Gateway 功能在跨网络高可用性配置中很有用。这些功能还涵盖了每个 NetScaler Gateway 用于确保伙伴设备处于活动状态的运行状况检查过程。

独立网络配置的工作原理

NetScaler Gateway 设备连接到两个不同网络上的不同路由器（称为 R3 和 R4）。设备通过这些路由器交换心跳数据包。心跳数据包是定期发生的信号，用于确保连接仍然处于活动状态。您可以扩展此配置以适应涉及任意数量接口的部署。

注意：如果您在网络上使用静态路由，则必须在所有系统之间添加静态路由，以确保心跳数据包成功发送和接收。（如果您在系统上使用动态路由，则不需要静态路由。）

当高可用性对中的设备位于两个不同的网络上时，辅助 NetScaler Gateway 必须具有独立的网络配置。这意味着不同网络上的 NetScaler Gateway 设备不能共享映射的 IP 地址、虚拟 LAN 或网络路由。这种配置类型，即高可用性对中的 NetScaler Gateway 设备具有不同的可配置参数，称为独立网络配置或对称网络配置。

下表总结了独立网络配置的可配置参数，并显示了您必须如何在每个 NetScaler Gateway 上设置它们：

可配置参数	行为
IP 地址	NetScaler Gateway 特有。仅在该设备上处于活动状态。
虚拟 IP 地址	浮动。
虚拟 LAN	NetScaler Gateway 特有。仅在该设备上处于活动状态。

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

可配置参数	行为
路由	NetScaler Gateway 特有。仅在该设备上处于活动状态。链路负载平衡 (LLB) 路由是浮动的。
访问控制列表 (ACL)	浮动（通用）。在两台设备上均处于活动状态。
动态路由	NetScaler Gateway 特有。仅在该设备上处于活动状态。辅助 NetScaler Gateway 也必须运行路由协议并与上游路由器对等。
L2 模式	浮动（通用）。在两台设备上均处于活动状态。
L3 模式	浮动（通用）。在两台设备上均处于活动状态。
反向网络地址转换 (NAT)	NetScaler Gateway 特有。使用虚拟 IP 地址进行反向 NAT，因为 NAT IP 地址是浮动的。

注意：

INC 模式下的 IPSET 支持公共 IP 地址。有关详细信息，请参阅 使用 Azure ILB 通过 NetScaler 高可用性模板配置 HA-INC 节点。

添加远程节点

当高可用性对的两个节点位于不同的子网时，每个节点必须具有不同的网络配置。因此，要将两个独立的系统配置为高可用性对，您必须在配置过程中指定独立网络计算模式。

添加高可用性节点时，必须禁用未连接或未用于流量的每个接口的高可用性监视器。

为独立网络计算模式添加远程节点

1. 在配置实用程序中，在“配置”选项卡上的导航窗格中，展开“**系统 > 高可用性**”。
2. 在详细信息窗格中，单击“**节点**”选项卡，然后单击“**添加**”。
3. 在“高可用性设置”对话框中，在“**远程节点 IP 地址**”文本框中，键入作为远程节点的设备的 NetScaler Gateway IP 地址。

   要使用 IPv6 地址，请在输入 IP 地址之前单击“**IPv6**”复选框。

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

4. 如果要自动将本地节点添加到远程节点，请选择“配置远程系统以参与高可用性设置”。如果未选择此选项，则必须登录到远程节点所代表的设备并添加当前正在配置的节点。
5. 单击以启用对已关闭的接口/通道的清除 HA 监视器。
6. 单击以在自模式下启用 INC（独立网络配置）模式。
7. 单击“**确定**”。“**节点**”页面将显示高可用性配置中的本地节点和远程节点。

删除远程节点

1. 在配置实用程序中，在“配置”选项卡上的导航窗格中，展开“**系统 > 高可用性**”。
2. 在详细信息窗格中，单击“**节点**”选项卡。
3. 选择要移除的节点，单击 **Remove**，然后单击 **Yes**。

配置路由监视器

您可以使用路由监视器使高可用性状态依赖于内部路由表，无论该表包含任何动态学习的路由还是静态路由。在高可用性配置中，每个节点上的路由监视器都会检查内部路由表，以确保始终存在用于访问特定网络的路由条目。如果路由条目不存在，路由监视器的状态将变为 DOWN。

当 NetScaler Gateway 设备仅具有用于访问网络的静态路由，并且您希望为该网络创建路由监视器时，您必须为静态路由启用受监视的静态路由。受监视的静态路由会从内部路由表中删除不可达的静态路由。如果您在静态路由上禁用受监视的静态路由，则不可达的静态路由可能会保留在内部路由表中，从而使路由监视器的目的失效。

路由监视器支持启用或禁用独立网络配置设置。下表显示了在高可用性设置中以及启用或禁用独立网络配置时路由监视器的情况。

禁用独立网络配置模式下高可用性中的路由监视器	启用独立网络配置模式下高可用性中的路由监视器
路由监视器由节点传播并在同步期间交换。	路由监视器既不由节点传播，也不在同步期间交换。
路由监视器仅在当前主节点中处于活动状态。	路由监视器在主节点和辅助节点上都处于活动状态。
无论内部路由表中是否存在路由条目，NetScaler Gateway 设备始终将路由监视器的状态显示为 UP。	如果内部路由表中不存在相应的路由条目，NetScaler Gateway 设备会将路由监视器的状态显示为 DOWN。
在以下情况下，路由监视器开始监视其路由，以允许 NetScaler Gateway 学习动态路由（这	不适用。

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

禁用独立网络配置模式下高可用性中的路由监视器	启用独立网络配置模式下高可用性中的路由监视器
可能需要长达 180 秒）：重新启动、故障转移、用于 v6 路由的 set route6 命令、用于 v4 路由的 set route `msr` enable/disable 命令、添加新的路由监视器。	

当您禁用独立网络配置模式，并且希望将主节点中的网关不可达作为高可用性故障转移的条件之一时，路由监视器非常有用。

例如，您在双臂拓扑的高可用性设置中禁用独立网络配置，该拓扑中 NetScaler Gateway 设备 NS1 和 NS2 位于同一子网中，并带有路由器 R1 和交换机 SW1、SW2 和 SW3，如下图所示。由于 R1 是此设置中唯一的路由器，因此您希望高可用性设置在 R1 无法从当前主节点访问时进行故障转移。您可以在每个节点上配置一个路由监视器（例如，分别为 RM1 和 RM2），以监视该节点到 R1 的可达性。

网络流(/en-us/netscaler-gateway/media/ha-rm-ha-non-inc.png)

当 NS1 作为当前主节点时，网络流如下所示：

1. NS1 上的路由监视器 RM1 监视 NS1 的内部路由表，以检查是否存在路由器 R1 的路由条目。NS1 和 NS2 通过交换机 SW1 或 SW3 定期交换心跳消息。
2. 如果交换机 SW1 发生故障，NS1 上的路由协议会检测到 R1 不可达，因此会从内部路由表中删除 R1 的路由条目。NS1 和 NS2 通过交换机 SW3 定期交换心跳消息。
3. 检测到 R1 的路由条目不在内部路由表中，RM1 启动故障转移。如果从 NS1 和 NS2 到 R1 的路由都已中断，则每 180 秒发生一次故障转移，直到其中一个设备能够访问 R1 并恢复连接。

添加或删除路由监视器

当高可用性对的设备位于不同网络时，NetScaler Gateway 的高可用性状态取决于设备是否可达。在跨网络高可用性配置中，每个 NetScaler Gateway 上的路由监视器会扫描内部路由表，以确保始终存在另一个 NetScaler Gateway 的条目。

添加路由监视器

1. 在配置实用程序中，在“配置”选项卡上，在导航窗格中，展开“系统”，然后单击“高可用性”。
2. 在“绑定/取消绑定路由监视器”对话框中，在“路由监视器”选项卡上，单击“操作”，然后单击“配置”。
3. 在“指定路由监视器”下，在“网络”中，键入其他 NetScaler Gateway 设备网络的 IP 地址。

   要配置 IPv6 地址，请单击“IPv6”，然后键入 IP 地址。

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

4. 在“网络掩码”中，键入其他网络的子网掩码，单击“添加”，然后单击“确定”。

此过程完成后，路由监视器将绑定到 NetScaler Gateway。

注意：当路由监视器未绑定到 NetScaler Gateway 时，任一设备的高可用性状态由接口状态决定。

删除路由监视器

1. 在配置实用程序中，在“配置”选项卡上，在导航窗格中，展开“系统”，然后单击“高可用性”。
2. 在“路由监视器”选项卡上，单击“操作”，然后单击“配置”。
3. 在“已配置的路由监视器”下，选择监视器，单击“删除”，然后单击“确定”。

配置链路冗余

链路冗余将网络接口组合在一起，以防止由于 NetScaler Gateway 的一个网络接口发生故障而导致故障转移，即使该 NetScaler Gateway 还有其他正常运行的接口。主 NetScaler Gateway 上第一个接口的故障会触发故障转移，尽管第一个接口仍然可以使用其第二个链路来处理用户请求。配置链路冗余时，可以将两个接口分组到一个故障转移接口集中，从而防止单个链路故障导致故障转移到辅助 NetScaler Gateway，除非主 NetScaler Gateway 上的所有接口都无法正常工作。

故障转移接口集中的每个接口都维护独立的桥接条目。在 NetScaler Gateway 上启用且高可用性但未绑定到故障接口集的监视接口称为关键接口，因为如果其中任何一个接口发生故障，就会触发故障转移。

配置链路冗余

1. 在配置实用程序中，在“配置”选项卡上的导航窗格中，展开“系统”，然后单击“高可用性”。
2. 在“故障转移接口集”选项卡上，单击“添加”。
3. 在“名称”中，键入集的名称。
4. 在“接口”中，单击“添加”。
5. 在“可用接口”下，选择一个接口，然后单击箭头将该接口移动到“已配置”。
6. 对第二个接口重复步骤 4 和 5，然后单击“创建”。

您可以根据需要在接口之间添加任意数量的接口以进行故障转移。

从故障转移接口集中删除接口

1. 在配置实用程序中，在“配置”选项卡上的导航窗格中，展开“系统”，然后单击“高可用性”。
2. 在“故障转移接口集”选项卡上，选择一个集，然后单击“删除”。

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

删除故障转移接口集

如果您不再需要故障转移接口集，可以将其从 NetScaler Gateway 中删除。

1. 在配置实用程序中，在“配置”选项卡上，在导航窗格中，展开“系统”，然后单击“高可用性”。
2. 在“故障转移接口集”选项卡上，选择一个集，然后单击“删除”。

了解故障转移的原因

以下事件可能导致高可用性配置中发生故障转移：

1. 如果辅助节点在超过辅助节点上设置的死亡间隔的时间段内未从主节点接收到心跳包。有关设置死亡间隔的更多信息，请参阅配置通信间隔。节点未从对等节点接收心跳包的可能原因包括：
   - 网络配置问题阻止心跳在高可用性节点之间遍历网络。
   - 对等节点发生硬件或软件故障，导致其冻结（挂起）、重新启动或以其他方式停止处理和转发心跳包。
2. 主节点的 SSL 卡发生硬件故障。
3. 主节点在三秒内未在其网络接口上接收到任何心跳包。
4. 在主节点上，不属于故障转移接口集 (FIS) 或链路聚合 (LA) 通道且已启用高可用性监视器 (HAMON) 的网络接口发生故障。接口已启用，但进入 DOWN 状态。
5. 在主节点上，FIS 中的所有接口都发生故障。接口已启用，但进入 DOWN 状态。
6. 在主节点上，启用了 HAMON 的 LA 通道发生故障。接口已启用，但进入 DOWN 状态。
7. 在主节点上，所有接口都发生故障。在这种情况下，无论 HAMON 配置如何，都会发生故障转移。
8. 在主节点上，所有接口都已手动禁用。在这种情况下，无论 HAMON 配置如何，都会发生故障转移。
9. 通过在任一节点上发出强制故障转移命令来强制进行故障转移。
10. 绑定到主节点的路由监视器变为 DOWN。

强制从节点进行故障转移

例如，如果您需要更换或升级主节点，您可能希望强制进行故障转移。您可以从主节点或辅助节点强制进行故障转移。强制故障转移不会传播或同步。要查看强制故障转移后的同步状态，您可以查看节点的状态。

在以下任何情况下，强制故障转移都会失败：

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

- 您在独立系统上强制进行故障转移。
- 辅助节点已禁用。
- 辅助节点配置为保持辅助状态。

当您运行强制故障转移命令时，如果 NetScaler Gateway 设备检测到潜在问题，它会显示一条警告消息。该消息包含触发警告的信息，并在继续之前请求确认。

在主节点或辅助节点上强制故障转移

如果您在主节点上强制故障转移，主节点将变为辅助节点，辅助节点将变为主节点。只有当主节点能够确定辅助节点处于“UP”状态时，才可能进行强制故障转移。

如果辅助节点处于“DOWN”状态，强制故障转移命令将返回以下错误消息：“由于对等节点状态无效，操作无法执行。请纠正并重试。”

如果辅助系统处于声明状态或非活动状态，该命令将返回以下错误消息：`"Operation not possible now. Please wait for system to stabilize before retrying."`

如果您从辅助节点运行强制故障转移命令，辅助节点将变为主节点，主节点将变为辅助节点。只有在辅助节点运行状况良好且未配置为保持辅助状态的情况下才能发生强制故障转移。

如果辅助节点无法变为主节点，或者辅助节点配置为保持辅助状态（使用 STAYSECONDARY 选项），节点将显示以下错误消息：“由于我的状态无效，操作无法执行。请查看节点以获取更多信息。”

在主节点或辅助节点上强制故障转移

1. 在配置实用程序中，在“配置”选项卡上，在导航窗格中，展开“系统”，然后单击“高可用性”。
2. 在详细信息窗格中，在“节点”选项卡上，选择主节点，然后在“操作”中，单击“强制故障转移”。
3. 在“警告”对话框中，单击“是”。

强制主节点保持主状态

在高可用性配置中，即使设备故障转移后，您也可以强制主 NetScaler Gateway 保持主状态。您只能在独立 NetScaler Gateway 设备以及高可用性对中的主 NetScaler Gateway 设备上配置此设置。

强制主节点保持主状态

1. 在配置实用程序中，在“配置”选项卡上，在导航窗格中，展开“系统”，然后单击“高可用性”。
2. 在详细信息窗格中，在“节点”选项卡上，选择一个节点，然后单击“编辑”。
3. 在“高可用性状态”下，单击“保持主状态”，然后单击“确定”。

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

您只能使用以下命令清除此配置：

`clear configuration full`

以下命令不会更改 NetScaler Gateway 高可用性配置：

`clear configuration basic`

`clear configuration extended`

强制辅助节点保持辅助状态

在高可用性设置中，您可以强制辅助 NetScaler Gateway 保持辅助状态，而与主 NetScaler Gateway 的状态无关。当您将 NetScaler Gateway 配置为保持辅助状态时，即使主 NetScaler Gateway 发生故障，它也会保持辅助状态。

例如，在现有高可用性设置中，假设您需要升级主 NetScaler Gateway，并且此过程需要一定的时间。在升级期间，主 NetScaler Gateway 可能会变得不可用，但您不希望辅助 NetScaler Gateway 接管。您希望它保持辅助 NetScaler Gateway，即使它检测到主 NetScaler Gateway 发生故障。

如果高可用性对中 NetScaler Gateway 的状态配置为保持辅助状态，则它不参与高可用性状态机转换。您可以在配置实用程序中的“**节点**”选项卡上检查 NetScaler Gateway 的状态。

此设置适用于独立 NetScaler Gateway 和辅助 NetScaler Gateway。

当您设置高可用性节点时，它不会传播或同步，并且仅影响配置了该设置的 NetScaler Gateway。

强制辅助节点保持辅助状态

1. 在配置实用程序中，在“配置”选项卡上的导航窗格中，展开“系统”，然后单击“高可用性”。
2. 在详细信息窗格的“节点”选项卡上，选择一个节点，然后单击“编辑”。
3. 在“高可用性状态”下，单击“保持辅助”（保持侦听模式），然后单击“确定”。

将 NetScaler Gateway 恢复为活动高可用性设备

1. 在配置实用程序中，在“配置”选项卡上的导航窗格中，展开“系统”，然后单击“高可用性”。
2. 在详细信息窗格的“节点”选项卡上，选择将保持主节点状态的设备，然后单击“打开”。
3. 在“高可用性状态”下，单击“已启用”（主动参与 HA），然后单击“确定”。

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

使用群集

NetScaler Gateway 可以部署在群集配置中，为 VPN 客户端流量提供高吞吐量、高可用性和可扩展性。在群集中，一组 NetScaler Gateway 设备或虚拟机作为一个单一系统映像运行，以协调用户会话并管理到网络资源的流量。NetScaler Gateway 群集可以由最少两台、最多 32 台配置为群集节点的 NetScaler Gateway 设备或虚拟机构建。

阅读 NetScaler 群集 文档，然后再开始配置 NetScaler Gateway 群集。请特别注意该文档中的以下主题。

- 请参阅 (/zh-cn/citrix-adc/current-release/clustering.html)，以验证您计划使用的系统是否符合要求。
- 请参阅 (/zh-cn/citrix-adc/current-release/clustering/cluster-overview.html)，了解群集概念的描述。
- 请参阅 (/zh-cn/citrix-adc/current-release/clustering/cluster-overview/cluster-node-states.html)，以规划部署并确定可能与您的环境相关的任何注意事项。

NetScaler Gateway 群集作为斑点 VIP 配置类型 NetScaler 群集运行。

重要提示：

XenApp and XenDesktop® 向导不支持群集，因此您在 **GUI > 导航窗格 > 与 NetScaler 产品集成**部分中找不到 **XenApp and XenDesktop** 向导。

配置集群

设置 NetScaler Gateway 集群的主要任务是：

1. 决定哪个 NetScaler Gateway 设备或虚拟机是配置协调器，并在该系统上创建集群实例（如果尚未存在）。
2. 将 NetScaler Gateway 系统作为节点加入集群。
3. 在集群实例上创建节点组，并设置 STICKY 选项。
4. 将单个集群节点绑定到集群节点组。
5. 在配置协调器上配置 NetScaler Gateway 虚拟服务器，并将其绑定到集群节点组。

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

有多种方法可用于配置 NetScaler 集群。以下任务集使用配置实用程序中最直接的方法。

使用配置实用程序创建 NetScaler Gateway 集群实例

部署详细信息就绪后，在作为配置协调器的 NetScaler Gateway 上开始配置。

注意：创建集群实例会清除配置。如果需要保存现有系统配置以供参考，请在继续进行集群配置之前存档副本。集群建立后，任何要在集群中使用的现有设置都可以在配置协调器上重新应用。

1. 使用 NSIP 地址登录到 NetScaler 配置实用程序。
2. 展开“系统”节点，然后展开“集群”子节点。
3. 在详细信息窗格中，单击“管理集群”。
4. 在“集群配置”对话框中，设置创建集群所需的参数。
   a. 输入集群实例 ID。集群实例 ID 是集群实例的数字标识符。默认值为 1，但您可以将其设置为 1 到 16 之间的任何数字。
   b. 输入集群 IP 地址。集群 IP 地址是集群的配置协调器 IP 地址，也是集群的管理 IP 地址。
   c. 选择首选的背板接口。这是用于集群节点之间通信的 NetScaler Gateway 接口。
5. 单击“创建”。
6. 在确认系统重启的提示符下，单击“是”。
7. 节点启动并成功同步后，从集群 IP 地址更改节点和集群 IP 地址的 RPC 凭据。有关更改 RPC 节点密码的更多信息，请参阅更改 RPC 节点密码。
8. 等待系统重启。可用后，使用在步骤 4(2) 中配置的集群 IP 地址登录配置实用程序。

注意： 在**系统信息详细信息**窗格中，NSIP 地址处的本地节点被报告为配置协调器。这确认基本集群实例现在正在运行。

配置协调器的本地节点会自动添加到集群中。可以在以下任务中添加更多节点。

将节点添加到 NetScaler Gateway 集群

集群实例建立后，您可以开始将其他 NetScaler Gateway 节点添加到集群中。

要将更多 NetScaler Gateway 系统添加到集群，您可以使用配置实用程序远程发出集群节点创建和加入集群设置。

注意：在配置 NetScaler Gateway 设置之前，必须完成向集群添加节点的操作。这样，如果集群配置出现问题并且您想删除集群并重新开始，则无需重复 NetScaler Gateway 配置。

1. 使用集群 IP 地址登录 NetScaler 配置实用程序。

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

2. 展开 **System** 节点，然后展开 Cluster 子节点。
3. 在详细信息窗格中，单击“**管理群集**”。
4. 在群集节点详细信息窗格中，单击“**添加**”。
5. 在“**创建群集节点**”窗格中，为此节点输入唯一的节点 ID。
6. 输入要添加为群集节点的系统的 NetScaler IP 地址。
7. 在“**群集节点凭据**”窗格中，输入远程 NetScaler Gateway 系统的 NetScaler Gateway 用户名和密码。
8. 在“配置协调器凭据”窗格中，输入本地授权用户的密码。
9. 单击“**创建**”。
10. 出现提示时，单击“**是**”以允许保存系统配置并对远程 NetScaler Gateway 执行热重启。
11. 节点启动并成功同步后，从群集 IP 地址更改节点和群集 IP 地址的 RPC 凭据。有关更改 RPC 节点密码的更多信息，请参阅更改 RPC 节点密码。

对于要配置为群集节点的每个其他远程 NetScaler Gateway 系统，重复步骤 4 到 11。

验证群集节点是否包含在“群集节点”详细信息窗格中的“活动节点列表”中。如果缺少任何节点，请重复步骤 4 到 10，直到列出所有必需的节点。

创建群集节点组

添加群集节点后，可以创建群集节点组。

1. 使用群集 IP 地址登录到 NetScaler 配置实用程序。
2. 展开“**系统**”节点，然后展开“群集”子节点。
3. 单击 **节点组**。
4. 在详细信息窗格中，单击 **添加**。
5. 输入集群节点组的名称。
6. 选择 **Sticky** 选项以支持 NetScaler Gateway 虚拟服务器类型。
7. 单击 **继续**。

集群节点组现已建立。在离开配置实用程序的此区域之前，您可以将本地 NetScaler Gateway 节点绑定到新的集群节点组。这是绑定到集群组的唯一节点。

将本地集群节点绑定到集群节点组

由于 NetScaler Gateway 集群配置是斑点类型，因此只有一个节点可以绑定到节点组。以下过程将配置协调器上的本地节点绑定到节点组，但集群中的任何节点都可用于此绑定。

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

1. 在高级窗格中，展开集群节点。
2. 在中间的“集群节点”窗格中，选择“无集群节点”。
3. 在“集群节点”配置屏幕上，单击“绑定”。
4. 选择由此 NetScaler Gateway 系统的 NSIP 地址表示的本地节点。
5. 单击“插入”。
6. 单击“确定”。
7. 单击“完成”。

集群现已填充完毕，可以按照以下任务配置共享 NetScaler Gateway 虚拟服务器。

将 NetScaler Gateway 虚拟服务器绑定到集群节点组

建立集群后，您可以继续构建集群部署旨在服务的 NetScaler Gateway 配置。要将配置与集群关联，您需要创建 NetScaler Gateway 虚拟服务器并将其绑定到设置为“Sticky”类型的集群节点组。虚拟服务器绑定到集群节点组后，您可以继续配置 NetScaler Gateway。

如果配置了多个 NetScaler Gateway 虚拟服务器，则这些虚拟服务器也必须绑定到集群节点组。

注意： 如果尚未配置 NetScaler Gateway 虚拟服务器，您可能需要首先在 **系统 > 设置 > 配置基本功能** 下启用 NetScaler Gateway 以及身份验证、授权和审计功能。

1. 使用集群 IP 地址登录 NetScaler 配置实用程序。
2. 展开 **系统** 节点，然后展开集群子节点。
3. 单击 **节点组**。
4. 在 **节点组** 窗格中，选择所需的节点组名称，然后单击 **编辑**。
5. 在右侧的 **高级** 窗格中，展开 **虚拟服务器** 选项，然后单击 + 图标以添加虚拟服务器。
6. 选择 VPN 虚拟服务器类型，然后单击 **继续**。
7. 单击 **绑定**。
8. 如果列出了所需的虚拟服务器，请选择它，然后单击 **插入**，再单击 **确定**。
9. 如果必须创建新的虚拟服务器，请单击 **添加**。继续执行 NetScaler 虚拟服务器配置。最少只需创建虚拟服务器，以便将其绑定到集群节点组。
10. 虚拟服务器在 NetScaler Gateway 虚拟服务器列表中可用后，选择它，然后单击 **插入**。
11. 单击 **确定**。
12. 单击 **完成**。

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

注意：如果配置了多个 NetScaler Gateway 虚拟服务器，则必须使用相同的方法将它们绑定到集群节点组。

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

统一网关

带统一网关的 NetScaler：一个 URL

带统一网关的 NetScaler 使桌面和移动用户能够通过单个 URL 简化对任何应用程序的安全访问。在此单个 URL 背后，管理员拥有一个用于配置、安全和控制对应用程序的远程访问的单一入口点。远程用户通过无缝单点登录到他们所需的所有应用程序，以及一次登录/注销的便捷性，获得了更好的体验。

为此，带网关的 NetScaler，以及 NetScaler 的内容交换功能和广泛的身份验证基础架构，通过此单个 URL 提供对组织站点和应用程序的访问。此外，远程用户可以使用 iOS 或 Android 移动设备以及带有 Citrix Secure Access 客户端的 Linux、PC 或 Mac 系统，无论他们身在何处，都可以统一访问统一网关 URL。

统一网关部署允许通过单个 URL 访问以下类别的应用程序：

- 内部网应用程序。
- 无客户端应用程序
- 软件即服务应用程序
- NetScaler 提供的预配置应用程序
- Citrix Virtual Apps and Desktops 发布应用程序

内部网应用程序可能是位于安全企业网络内的任何基于 Web 的应用程序。这些是内部资源，例如组织内部网站点、错误跟踪应用程序或 Wiki。

通常也位于安全企业网络内部，统一网关提供单个 URL 访问的**无客户端应用程序**是 Outlook Web Access 和 SharePoint。这些应用程序提供对 Exchange 电子邮件和团队资源的访问，而无需专用客户端软件，这些资源需要供远程用户使用。

SaaS 应用程序，也常被称为云应用程序，是组织所依赖的外部、基于云的应用程序，例如 ShareFile、Salesforce 或 NetSuite。支持提供基于 SAML 的单点登录的 SaaS 应用程序。

一些组织可能在 NetScaler 负载均衡配置中部署了**预配置的 NetScaler 提供的应用程序**。这通常也称为“反向代理”应用程序。当部署的虚拟服务器位于同一 NetScaler 统一网关实例或设备上时，统一网关支持这些应用程序。这些应用程序可能拥有自己的身份验证配置，该配置独立于统一网关配置。

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

任何已发布的 **Citrix Virtual Apps and Desktops 发布应用程序**都可以通过统一网关 URL 提供。SmartAccess 和 SmartControl 策略可以选择性地应用于这些资源的细粒度策略和访问控制。

统一网关配置向导

配置带有统一网关部署的 NetScaler 的推荐方法是使用统一网关配置向导。该向导会引导您完成配置，并创建所有必要的虚拟服务器、策略和表达式，然后根据提供的详细信息应用设置。初始设置完成后，该向导可用于管理您的部署并监控其运行情况。

注意：

统一网关配置向导不执行初始系统配置。在配置统一网关之前，您的 NetScaler Gateway 设备或 VPX 实例必须已完成基本安装。请参阅 (/zh-cn/netscaler-gateway/current-release/install-citrix-gateway/configure-gateway-using-wizards.html#setup-wizard) 中的安装说明以完成基本配置。

向导配置的统一网关元素包括：

- 统一网关主虚拟服务器
- 统一网关虚拟服务器的 SSL 服务器证书
- 主身份验证配置和任何可选的辅助身份验证配置
- 门户主题选择和可选自定义
- 将通过统一网关门户访问的用户应用程序

对于这些元素中的每一个，您都需要提供配置信息。对于基本的统一网关部署，需要以下信息。

- 对于主统一网关虚拟服务器，部署的公共 IP 地址和 IP 端口号。这是在 DNS 中解析为统一网关 URL 主机名的 IP 地址。例如，如果您的统一网关部署的 URL 是 `https://mycompany.com/`，则 IP 地址必须解析为 mycompany.com。
- 部署的签名 SSL 服务器证书。NetScaler Gateway 支持 PEM 或 PFX 格式的证书。
- 主身份验证服务器信息。此身份验证配置支持的身份验证系统包括 LDAP/Active Directory、RADIUS 和基于证书的身份验证。还可以创建辅助 LDAP 或 RADIUS 身份验证配置。必须提供身份验证服务器 IP 地址以及任何相关的管理员凭据或目录属性。对于证书身份验证，必须提供设备证书属性和 CA 证书。
- 可以选择门户主题。如果需要自定义或品牌化的门户设计，可以使用向导将自定义图形上传到系统。

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

- 对于基于Web的用户应用程序，必须指定各个应用程序的URL。对于将利用SAML单点登录身份验证的Web应用程序，该实用程序会收集断言消费者服务URL以及其他可选的SAML参数。请提前收集使用SAML身份验证系统的应用程序的配置详细信息。
- 要通过统一网关部署提供Citrix Virtual Apps and Desktops发布的资源，您必须指定集成点(StoreFront)。该实用程序需要集成点的完全限定域名、站点路径、单点登录域、安全票证颁发机构 (STA) 服务器URL以及其他取决于集成点类型的参数。

附加配置管理

对于统一网关配置实用程序中不可用的特定站点设置，例如备用SSL设置或会话策略，您可以在NetScaler Gateway配置实用程序中管理所需的设置。一旦这些设置由统一网关配置实用程序创建，您就可以在内容交换或VPN虚拟服务器上修改它们。

内容交换虚拟服务器

这是部署主IP地址和URL背后的NetScaler配置实体。SSL服务器证书和参数在此虚拟服务器上进行管理。由于此虚拟服务器是部署的响应网络主机，因此如有必要，可以在此虚拟服务器上修改ICMP服务器响应和RHI状态。内容交换虚拟服务器可以在“**配置**”选项卡下的“**流量管理**”>“**内容交换**”>“**虚拟服务器**”中找到。

重要提示：

当您将统一网关环境升级到版本13.0 build 58.x或更高版本时，在网关或VPN虚拟服务器之前配置的内容交换虚拟服务器中，DTLS旋钮将被禁用。升级后，请在内容交换虚拟服务器中手动启用DTLS旋钮。如果您使用向导进行配置，请勿启用DTLS旋钮。

VPN虚拟服务器

统一网关配置的所有其他VPN参数、配置文件和策略绑定都在此虚拟服务器上进行管理，包括主身份验证配置。此实体在“**配置**”选项卡下的“**NetScaler Gateway**”>“**虚拟服务器**”中进行管理。相关VPN虚拟服务器的名称包含在初始统一网关配置期间赋予内容交换虚拟服务器的名称。

注意：

为统一网关部署创建的VPN虚拟服务器是不可寻址的，并分配有0.0.0.0 IP地址。

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

统一网关常见问题解答

什么是统一网关？

统一网关是 NetScaler 11.0 版本中的一项新功能，它能够在一个虚拟服务器（称为统一网关虚拟服务器）上接收流量，然后根据需要，在内部将该流量定向到绑定到统一网关虚拟服务器的虚拟服务器。

统一网关功能允许最终用户通过使用单个 IP 地址或 URL（与统一网关虚拟服务器关联）访问多个服务。管理员可以释放 IP 地址并简化 NetScaler Gateway 部署的配置。

每个统一网关虚拟服务器都可以作为前端连接一个 NetScaler Gateway 虚拟服务器以及零个或多个负载平衡虚拟服务器，作为编组的一部分。统一网关通过使用 NetScaler 设备的内容切换功能来工作。

统一网关部署的一些示例：

- 统一网关虚拟服务器 ->
- 统一网关虚拟服务器 ->
- 统一网关虚拟服务器 ->
- 统一网关虚拟服务器 ->

每个负载平衡虚拟服务器都可以是托管后端服务的任何标准负载平衡服务器，例如 Microsoft Exchange 或 Citrix® ShareFile。

为什么要使用统一网关？

统一网关功能使最终用户能够通过使用单个 IP 地址或 URL（与统一网关虚拟服务器关联）访问多个服务。对于管理员而言，其优势在于他们可以释放 IP 地址并简化 NetScaler Gateway 部署的配置。

是否可以有多个统一网关虚拟服务器?

是的。您可以根据需要设置任意数量的统一网关虚拟服务器。

为什么统一网关需要内容切换?

内容切换功能是必需的，因为内容切换虚拟服务器是接收流量并在内部将其定向到适当虚拟服务器的服务器。内容切换虚拟服务器是统一网关功能的主要组件。

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

在 11.0 之前的版本中，内容切换可用于接收多个虚拟服务器的流量。这种用法也称为统一网关？

在 11.0 之前的版本中，支持使用内容切换虚拟服务器接收多个虚拟服务器的流量。但是，内容切换无法将流量定向到 NetScaler Gateway 虚拟服务器。

11.0 中的增强功能使内容切换虚拟服务器能够将流量定向到任何虚拟服务器，包括 NetScaler Gateway 虚拟服务器。

统一网关中的内容切换策略发生了哪些变化?

1. 已为内容切换操作添加了一个新的命令行参数 "-targetVserver"。此新参数用于指定目标 NetScaler Gateway 虚拟服务器。示例：

   添加内容切换操作 UG_CSACT_MyUG -targetVserver UG_VPN_MyUG

   在 NetScaler Gateway 配置实用程序中，内容切换操作有一个新选项“目标虚拟服务器”，它可以引用 NetScaler Gateway 虚拟服务器。
2. 一个新的高级策略表达式 is_vpn_url 可用于匹配 NetScaler Gateway 和特定于身份验证的请求。

统一网关目前不支持哪些 NetScaler Gateway 功能?

统一网关支持所有功能。但是，已通过 VPN 插件报告了一个小问题 (issue ID 544325)，即本机登录。在这种情况下，无缝单点登录 (SSO) 不起作用。

使用统一网关时，EPA 扫描的行为是什么?

使用统一网关时，端点分析仅针对 NetScaler Gateway 访问方法触发，而不是针对 NetScaler AAA TM 访问。如果用户尝试访问 NetScaler AAA TM 虚拟服务器，即使身份验证是在 NetScaler Gateway 虚拟服务器上完成的，也不会触发 EPA 扫描。但是，如果用户尝试获取无客户端 VPN/完整 VPN 访问权限，则会触发配置的 EPA 扫描。在这种情况下，将完成身份验证或无缝 SSO。

统一网关的许可证要求是什么?

统一网关仅支持 Advanced 和 Premium 许可证。它不适用于仅限 NetScaler Gateway 或 Standard 许可证版本。

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

与统一网关一起使用的 NetScaler Gateway 虚拟服务器是否需要 IP/端口/SSL 配置?

对于与统一网关虚拟服务器一起使用的 NetScaler Gateway 虚拟服务器，NetScaler Gateway 虚拟服务器上不需要 IP/端口/SSL 配置。但是，对于 RDP 代理功能，您可以将相同的 SSL/TLS 服务器证书绑定到 NetScaler Gateway 虚拟服务器。

我是否需要重新预配 NetScaler Gateway 虚拟服务器上的 SSL/TLS 证书以用于统一网关虚拟服务器?

您无需重新预配当前绑定到 NetScaler Gateway 虚拟服务器的证书。您可以自由重用任何现有 SSL 证书并将其绑定到统一网关虚拟服务器。

单一 URL 部署和多主机部署之间有什么区别？我需要哪一个?

单一 URL 是指统一网关虚拟服务器处理一个完全限定域名 (FQDN) 流量的能力。当统一网关使用其证书主题填充了 FQDN 的 SSL/TLS 服务器证书时，存在此限制。例如：ug.citrix.com

如果统一网关使用通配符服务器证书，则它可以处理多个子域的流量。例如：*.citrix.com

另一个选项是使用服务器名称指示 (SNI) 功能的 SSL/TLS 配置，以允许绑定多个 SSL/TLS 服务器证书。示例：auth.citrix.com、auth.citrix.de、auth.citrix.co.uk、auth.citrix.co.jp

单主机与多主机类似于网站通常在 Web 服务器（例如 Apache HTTP 服务器或 Microsoft Internet Information Services (IIS)）上托管的方式。如果是单主机，您可以使用站点路径切换流量，就像在 Apache 中使用别名或“虚拟目录”一样。如果是多主机，您可以使用主机头切换流量，类似于在 Apache 中使用虚拟主机的方式。

统一网关可以使用哪些身份验证机制?

所有与 NetScaler Gateway 兼容的现有身份验证机制也与统一网关兼容。

其中包括 LDAP、RADIUS、SAML、Kerberos、基于证书的身份验证等。

升级前在 NetScaler Gateway 虚拟服务器上配置的任何身份验证机制，在 NetScaler Gateway 虚拟服务器放置在统一网关虚拟服务器后面时都会自动使用。除了为 NetScaler Gateway 虚拟服务器分配一个不可寻址的 IP 地址 (0.0.0.0) 之外，没有其他配置步骤。

什么是“SelfAuth”身份验证?

SelfAuth 本身不是一种身份验证类型。SelfAuth 描述了 URL 的创建方式。一个新的命令行参数 `ssotype` 可用于 VPN URL 配置。示例：

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

`> add vpn url RGB RGB "http://blue.citrix.lab/" -vServerName Blue -ssotype selfauth`

SelfAuth 是 `ssotype` 参数的值之一。这种类型的 URL 可用于访问与 Unified Gateway 虚拟服务器不在同一域中的资源。配置书签时，可以在配置实用程序中看到此设置。

什么是“StepUp”身份验证?

当需要额外、更安全的身份验证级别才能访问 NetScaler AAA TM 资源时，您可以使用 StepUp 身份验证。在命令行中，使用 authnProfile 命令设置 authenticationLevel 参数。示例：

```
add authentication authnProfile AuthProfile -authnVsName AAATMVserver
-AuthenticationHost auth.citrix.lab -AuthenticationDomain citrix.lab **-
**AuthenticationLevel 100
```

此身份验证配置文件绑定到负载平衡虚拟服务器。

NetScaler AAA TM 虚拟服务器是否支持 StepUp 身份验证?

是的，支持。

什么是 `login once/logout once`?

`Login Once`：VPN 用户只需登录一次 NetScaler AAA TM 或 NetScaler Gateway 虚拟服务器。从那时起，VPN 用户可以无缝访问所有企业/云/Web 应用程序。用户无需重新进行身份验证。但是，在特殊情况下（例如 NetScaler AAA TM StepUp），会进行重新身份验证。

`Logout Once`：在创建第一个 NetScaler AAA TM 或 NetScaler Gateway 会话后，它将用于为该用户创建后续的 NetScaler AAA TM 或 NetScaler Gateway 会话。如果其中任何会话注销，NetScaler 设备也会注销用户的其他应用程序或会话。

可以在 Unified Gateway 级别指定通用身份验证策略，并且在负载平衡虚拟服务器级别绑定 NetScaler AAA TM 负载平衡虚拟服务器特定的身份验证吗？支持此用例的配置步骤是什么?

如果您需要为 Unified Gateway 后面的 NetScaler AAA TM 虚拟服务器指定单独的身份验证策略，则需要有一个单独的、可独立寻址的身份验证虚拟服务器（类似于普通的 NetScaler AAA TM 配置）。负载平衡虚拟服务器上的身份验证主机设置必须指向此身份验证虚拟服务器。

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

如何配置 Unified Gateway，以便绑定的 NetScaler AAA TM 虚拟服务器拥有自己的身份验证策略?

在此场景中，负载平衡服务器必须将身份验证 FQDN 选项设置为指向 NetScaler AAA TM 虚拟服务器。NetScaler AAA TM 虚拟服务器必须具有独立的 IP 地址，并且可从 NetScaler 和客户端访问。

NetScaler AAA TM 认证虚拟服务器是否需要用于通过 Unified Gateway 虚拟服务器进行身份验证的用户?

不需要。NetScaler Gateway 虚拟服务器甚至可以对 NetScaler AAA TM 用户进行身份验证。

您在哪里指定 NetScaler Gateway 身份验证策略——在 Unified Gateway 虚拟服务器上还是在 NetScaler Gateway 虚拟服务器上?

身份验证策略应绑定到 NetScaler Gateway 虚拟服务器。

如何在 Unified Gateway 内容交换虚拟服务器后面的 NetScaler AAA TM 虚拟服务器上启用身份验证?

在 NetScaler AAA TM 上启用身份验证，并将身份验证主机指向 Unified Gateway 内容交换 FQDN。

如何将 TM 虚拟服务器添加到内容交换后面（单个 URL 与多主机）?

为单个 URL 添加 NetScaler AAA TM 虚拟服务器与为多个主机添加它之间没有区别。在任何一种情况下，虚拟服务器都作为目标添加到内容交换操作中。单个 URL 与多主机之间的区别通过内容交换策略规则实现。

如果将绑定到 NetScaler AAA TM 负载平衡虚拟服务器的身份验证策略移到 Unified Gateway 虚拟服务器后面，会发生什么?

身份验证策略绑定到身份验证虚拟服务器，身份验证虚拟服务器绑定到负载平衡虚拟服务器。对于 Unified Gateway 虚拟服务器，Citrix 建议将 NetScaler Gateway 虚拟服务器作为单一身份验证点，这消除了在身份验证虚拟服务器上执行身份验证的需要（甚至不需要特定的身份验证虚拟服务器）。将身份验证主机指向 Unified Gateway 虚拟服务器 FQDN 可确保由 NetScaler Gateway 虚拟服务器执行身份验证。如果将身份验证主机指向 Unified Gateway 的内容交换，并且仍然绑定了身份验证虚拟服务器，则绑定到身份验证虚拟服务器的身份验证策略将被忽略。但是，如果将身份验证主机指向独立的、可寻址的身份验证虚拟服务器，则绑定的身份验证策略将生效。

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

如何为 NetScaler AAA TM 会话配置会话策略?

如果在 Unified Gateway 中，未为 NetScaler AAA TM 虚拟服务器指定身份验证虚拟服务器，则 NetScaler AAA TM 会话将继承 NetScaler Gateway 会话策略。如果指定了身份验证虚拟服务器，则将应用绑定到该虚拟服务器的 NetScaler AAA TM 会话策略。

NetScaler 11.0 中 NetScaler Gateway 门户有哪些变化?

在 NetScaler 11.0 之前的版本中，可以在全局级别设置单个门户自定义。给定 NetScaler 设备中的每个网关虚拟服务器都使用全局门户自定义。

在 NetScaler 11.0 中，借助门户主题功能，您可以设置多个门户主题。主题可以全局绑定，也可以绑定到特定的虚拟服务器。

NetScaler 11.0 是否支持 NetScaler Gateway 门户自定义?

使用配置实用程序，您可以使用新的门户主题功能完全自定义和创建门户主题。您可以上传不同的图像、设置配色方案、更改文本标签等。

可自定义的门户页面包括：

- 登录页面
- 端点分析页面
- 端点分析错误页面
- 后端点分析页面
- VPN 连接页面
- 门户主页

通过此版本，您可以使用独特的门户设计自定义 NetScaler Gateway 虚拟服务器。

NetScaler 高可用性或群集部署是否支持门户主题?

是的。NetScaler 高可用性部署和群集部署支持门户主题。

我的自定义项是否会作为 NetScaler 11.0 升级过程的一部分进行迁移?

否。通过修改 rc.conf/rc.netscaler 文件或使用 10.1/10.5 中的自定义主题功能对 NetScaler Gateway 门户页面进行的现有自定义项，在升级到 NetScaler 11.0 后不会自动迁移。

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

在 NetScaler 11.0 中使用门户主题之前，是否有任何需要遵循的预升级步骤?

必须从 rc.conf 或 rc.netscaler 文件中删除任何现有自定义项。

另一种选择是，如果使用自定义主题，则必须将其分配为“默认”设置：

1. 导航到 **配置 > NetScaler Gateway > 全局设置**
2. 单击 **更改全局设置**。
3. 单击 **Client Experience**，然后从 **UI Theme** 列表中选择 **Default**。

如何将存储在 NetScaler 实例上并由 rc.conf 或 rc.netscaler 调用的自定义项迁移到门户主题?

为 NetScaler Gateway 登录页面创建自定义主题 详细介绍了 NetScaler 9.3 和 10.0 版本（最高 10.0 build 73.5001.e）的此类配置。自 NetScaler 10.0 build 10.0 73.5002.e（包括 10.1 和 10.5）以来，UITHEME CUSTOM 参数已可用，可帮助客户在重新启动后保留其自定义项。如果自定义项存储在 NetScaler 硬盘上，并且您希望继续使用这些自定义项，请备份 11.0 GUI 文件并将其插入到现有自定义主题文件中。如果要迁移到门户主题，则必须首先在“全局设置”或“会话配置文件”中的 **Client Experience** 下取消设置 UITHEME 参数。或者，您可以将其设置为 DEFAULT 或 GREENBUBBLE。然后，您就可以开始创建和绑定门户主题了。

如何在升级到 NetScaler 11.0 之前导出并保存当前自定义项，以及是否可将导出的文件移动到其他 NetScaler 设备?

上传到 **ns_gui_custom** 文件夹的自定义文件位于磁盘上，并在升级后仍然存在。但是，这些文件可能与新的 NetScaler 11.0 内核以及作为内核一部分的其他 GUI 文件不完全兼容。因此，Citrix 建议备份 11.0 GUI 文件并自定义备份。

此外，配置实用程序中没有用于将 **ns_custom_gui** 文件夹导出到另一个 NetScaler 设备的功能。请使用 SSH 或 WinSCP 等文件传输实用程序将文件从 NetScaler 实例中取出。

NetScaler AAA TM 虚拟服务器是否支持门户主题?

是的。NetScaler AAA TM 虚拟服务器支持门户主题。

NetScaler Gateway 11.0 的 RDP 代理功能有哪些变化?

自 NetScaler 10.5.e 增强版发布以来，RDP 代理已进行了许多增强。在 NetScaler 11.0 中，此功能从第一个发布的版本开始即可用。

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

许可变更

NetScaler 11.0 中的 RDP 代理功能只能与 Premium 和 Advanced 版本一起使用。每个用户都必须获取 Citrix 并发用户 (CCU) 许可证。

启用命令

在 NetScaler 10.5.e 中，没有用于启用 RDP 代理的命令。在 NetScaler 11.0 中，已添加启用命令：

```
enable feature rdpproxy
```

必须获得此功能的许可才能运行此命令。

其他 RDP 代理更改

服务器配置文件上的预共享密钥 (PSK) 属性已成为强制性要求。

要将现有的 NetScaler 10.5.e RDP 代理配置迁移到 NetScaler 11.0，必须理解并解决以下详细信息。

如果管理员希望将现有的 RDP 代理配置添加到所选的统一网关部署中：

- 必须编辑 NetScaler Gateway 虚拟服务器的 IP 地址，并将其设置为不可寻址的 IP 地址 (0.0.0.0)。
- 任何 SSL/TLS 服务器证书、身份验证策略都必须绑定到作为所选统一网关组成部分的 NetScaler Gateway 虚拟服务器。

如何将基于 NetScaler 10.5.e 的远程桌面协议 (RDP) 代理配置迁移到 NetScaler 11.0?

选项 1：保持现有的 NetScaler Gateway 虚拟服务器及其 RDP 代理配置不变，并使用 Premium 或 Advanced 许可证。

选项 2：移动现有的 NetScaler Gateway 虚拟服务器及其 RDP 代理配置，并将其放置在统一网关虚拟服务器之后。

选项 3：将带有 RDP 代理配置的独立 NetScaler Gateway 虚拟服务器添加到现有的 Standard Edition 设备中。

如何使用 NetScaler 11.0 版本设置 NetScaler Gateway 以进行 RDP 代理配置?

使用 NS 11.0 版本部署 RDP 代理有两种选项：

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

1. 使用外部面向的 NetScaler Gateway 虚拟服务器。这需要为 NetScaler Gateway 虚拟服务器提供一个外部可见的 IP 地址/FQDN。此选项在 NetScaler 10.5.e 中可用。
2. 使用作为 NetScaler Gateway 虚拟服务器前端的 Unified Gateway 虚拟服务器。

对于选项 2，NetScaler Gateway 虚拟服务器不需要自己的 IP 地址/FQDN，因为它使用不可寻址的 IP 地址 (0.0.0.0)。

HDX™ Insight 是否与 Unified Gateway 兼容?

当 NetScaler Gateway 与 Unified Gateway 一起部署时，必须满足以下条件：

- NetScaler Gateway 虚拟服务器必须绑定有效的 SSL 证书。
- NetScaler Gateway 虚拟服务器必须处于 UP 状态，才能在 NetScaler ADM 上生成 AppFlow 记录，用于 HDX Insight 报告。

如何迁移我现有的 HDX Insight 配置?

无需迁移。如果 NetScaler Gateway 虚拟服务器置于 Unified Gateway 虚拟服务器之后，则绑定到 NetScaler Gateway 虚拟服务器的 AppFlow 策略会继承。

对于 NetScaler ADM 上 NetScaler Gateway 虚拟服务器的现有数据，有两种可能性：

- 如果 NetScaler Gateway 虚拟服务器的 IP 地址在迁移到 Unified Gateway 过程中分配给 Unified Gateway 虚拟服务器，则数据仍与 NetScaler Gateway 虚拟服务器关联
- 如果 Unified Gateway 虚拟服务器分配了单独的 IP 地址，则来自 NetScaler Gateway 虚拟服务器的 AppFlow 数据将链接到该新 IP 地址。因此，现有数据不属于新数据。

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

NetScaler Gateway 设备上的 VPN 配置

重要提示：

本节中的屏幕截图采用灰度方案，原因如下：

- 帮助视障读者，特别是那些色盲或色弱的读者。
- 使用灰度图像以通用形式表示图像，不显示用户浏览器或操作系统中可能已完成的颜色编码自定义的影响。

用户可以通过以下方法通过 NetScaler Gateway 连接到您组织的网络资源：

- Citrix Workspace 应用程序，其中包含用户设备上安装的所有 Citrix 插件。
- 适用于 Web 的 Citrix Workspace 应用程序，允许用户通过 Web 浏览器连接到应用程序、桌面和 ShareFile。
- Secure Hub，允许用户从其 iOS 和 Android 设备访问 Secure Mail、WorxWeb 和移动应用程序。
- 适用于 Windows、macOS X 或 Linux 的 Citrix Secure Access™ 客户端。
- 适用于 iOS 和 Android 的 NetScaler Gateway 应用程序。
- 无客户端访问，无需安装用户软件即可为用户提供所需的访问权限。
- 与 Citrix SD-WAN™ 插件的互操作性。

如果用户安装 Citrix Secure Access 客户端，然后从适用于 Windows Server 2008 的 Citrix Virtual Apps 6.5（包括功能包和功能包 2）、Citrix Virtual Desktops 7.0 或更高版本安装 Citrix Workspace 应用程序，Citrix Workspace 应用程序会自动添加 Citrix Secure Access 客户端。用户可以通过 Web 浏览器或 Citrix Workspace 应用程序连接到 Citrix Secure Access 客户端。

SmartAccess 根据端点分析扫描的结果自动确定允许用户设备访问的方法。有关 SmartAccess 的更多信息，请参阅配置 SmartAccess。

NetScaler Gateway 支持适用于 iOS 和 Android 移动设备的 Citrix Endpoint Management 移动生产力应用程序。NetScaler Gateway 包含 Secure Browse，它允许 iOS 移动设备连接到 NetScaler Gateway 并建立微型 VPN 隧道。连接到 Secure Hub 的 Android 设备也会自动建立微型 VPN 隧道，从而提供对内部网络资源的 Web 和移动应用程序级别的安全访问。如果用户通过 Android 设备

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

使用移动生产力应用程序进行连接，则必须在 NetScaler Gateway 上配置 DNS 设置。有关详细信息，请参阅 通过使用 Android 设备的 DNS 后缀支持 DNS 查询。

用户如何使用 Citrix Secure Access™ 客户端连接

NetScaler Gateway 的运行方式如下：

- 当用户尝试通过 VPN 隧道访问网络资源时，Citrix Secure Access 客户端会加密所有目标为组织内部网络的网络流量，并将数据包转发到 NetScaler Gateway。
- NetScaler Gateway 终止 SSL 隧道，接受所有目标为专用网络的传入流量，并将流量转发到专用网络。NetScaler Gateway 通过安全隧道将流量发送回远程计算机。

当用户输入网址时，他们会收到一个登录页面，可以在其中输入凭据并登录。如果凭据正确，NetScaler Gateway 会完成与用户设备的握手。

如果用户位于代理服务器后面，则可以指定代理服务器和身份验证凭据。有关详细信息，请参阅 为用户连接启用代理支持。

Citrix Secure Access 客户端安装在用户设备上。首次连接后，如果用户使用基于 Windows 的计算机登录，他们可以使用通知区域中的图标建立连接。

建立安全隧道

当用户使用 Citrix Secure Access 客户端、Secure Hub 或 Citrix Workspace 应用程序连接时，客户端软件会通过端口 443（或 NetScaler Gateway 上的任何已配置端口）建立安全隧道并发送身份验证信息。隧道建立后，NetScaler Gateway 会向 Citrix Secure Access 客户端、Secure Hub 或 Citrix Workspace 应用程序发送配置信息，描述要保护的网络，如果启用了地址池，则包含一个 IP 地址。

通过安全连接隧道传输专用网络流量

当 Citrix Secure Access 客户端启动且用户通过身份验证后，所有目标为指定专用网络的网络流量都会被捕获并通过安全隧道重定向到 NetScaler Gateway。Citrix Workspace 应用程序必须支持 Citrix Secure Access 客户端，以便用户登录时通过安全隧道建立连接。

Secure Hub、Secure Mail 和 WorxWeb 使用 Micro VPN 为 iOS 和 Android 移动设备建立安全隧道。

NetScaler Gateway 拦截用户设备发出的所有网络连接，并通过安全套接字层 (SSL) 将它们多路复用到 NetScaler Gateway，在那里流量被解复用，并将连接转发到正确的主机和端口组合。

这些连接受制于适用于单个应用程序、部分应用程序或整个内部网的管理安全策略。您可以指定远程用户可以通过 VPN 连接访问的资源（IP 地址/子网对的范围）。

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

Citrix Secure Access 客户端为已定义的内部网应用程序拦截并隧道传输以下协议：

- TCP （所有端口）
- UDP （所有端口）
- ICMP （类型 8 和 0 - 回显请求/回复）

用户设备上的本地应用程序连接会安全地通过隧道传输到 NetScaler Gateway，NetScaler Gateway 会重新建立与目标服务器的连接。目标服务器将连接视为源自专用网络上的本地 NetScaler Gateway，从而隐藏了用户设备。这也被称为反向网络地址转换 (NAT)。隐藏 IP 地址可增加源位置的安全性。

在用户设备本地，所有与连接相关的流量（例如 SYN-ACK、PUSH、ACK 和 FIN 数据包）都由 Citrix Secure Access 客户端重新创建，使其看起来像是来自专用服务器。

通过防火墙和代理连接

Citrix Secure Access 客户端的用户有时位于其他组织的防火墙内部，如下图所示：

用户通过两个内部防火墙连接(/en-us/netscaler-gateway/media/ng-nat-firewall.png)

NAT 防火墙维护一个表，该表允许它们将来自 NetScaler Gateway 的安全数据包路由回用户设备。对于面向电路的连接，NetScaler Gateway 维护一个端口映射的反向 NAT 转换表。反向 NAT 转换表使 NetScaler Gateway 能够匹配连接，并通过隧道将数据包以正确的端口号发送回用户设备，从而使数据包返回到正确的应用程序。

控制 Citrix Secure Access 客户端的升级

系统管理员控制当 NetScaler 插件版本与 NetScaler Gateway 修订版不匹配时其行为方式。新选项控制 Mac 和 Windows 或其他操作系统的插件升级行为。

对于 VPN 插件，可以在 NetScaler 设备用户界面中的两个位置设置升级选项：

- 在全局设置中
- 在会话配置文件级别

要求

- Windows EPA 和 VPN 插件版本必须高于 11.0.0.0
- Mac EPA 插件版本必须高于 3.0.0.31
- Mac VPN 插件版本必须高于 3.1.4 (357)

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

注意：

如果 NetScaler 设备升级到 11.0 版本，所有以前的 VPN（和 EPA）插件都会升级到最新版本，无论升级控制配置如何。对于后续升级，它们将遵循以前的升级控制配置。

插件行为

注意：

从适用于 Windows 版本 25.2.x.x 的 EPA 客户端开始，当在最终用户设备上检测到更高版本的 EPA 客户端时，EPA 客户端会阻止降级到较低版本的提示。此功能适用于 NetScaler Gateway 中 **Windows EPA 插件升级** 配置（**始终**、**必要** 或 **从不**）的任何情况。此增强功能可确保最终用户设备始终运行最新版本的 EPA 客户端，从而维护安全性和稳定性。

对于每种客户端类型，NetScaler Gateway 允许以下三个选项来控制插件升级行为：

- **始终**

  当最终用户的插件版本与 NetScaler 附带的插件不匹配时，插件总是会升级。这是默认行为。如果您不希望企业中运行多个插件版本，请选择此选项。

- **必要**

  插件仅在必要时升级。在以下两种情况下，升级被认为是必要的：

  - 已安装的插件与当前的 NetScaler 版本不兼容。
  - 必须更新已安装的插件以获取必要的安全修复。

  如果您想最大限度地减少插件升级次数，但又不想错过任何插件安全更新，请选择此选项。

  注意：

  适用于 Linux 的 Citrix Secure Access 客户端不支持插件升级选项 **Essential**。

  为确保 **Windows 插件升级** 参数的 **Essential** 选项功能正常，请按照以下步骤操作：

  a. 从 Citrix 下载 页面下载所需版本的 `win-vpn.tgz`。

  b. 提取 `win-vpn.tgz` 文件。此提取包含三个文件：`AGEE-setup.exe`、`nsepa_setup.exe` 和 `package.json`。

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

c. 编辑 `package.json` 文件以添加 `compatibleFrom` 和 `compatibleTill` 参数。您可以从“https://<vserv_url>/vpn/pluginList.xml”处的 `pluginList.xml` 文件中获取 `compatibleFrom` 值。

以下是修改后的 `package.json` 文件的示例：

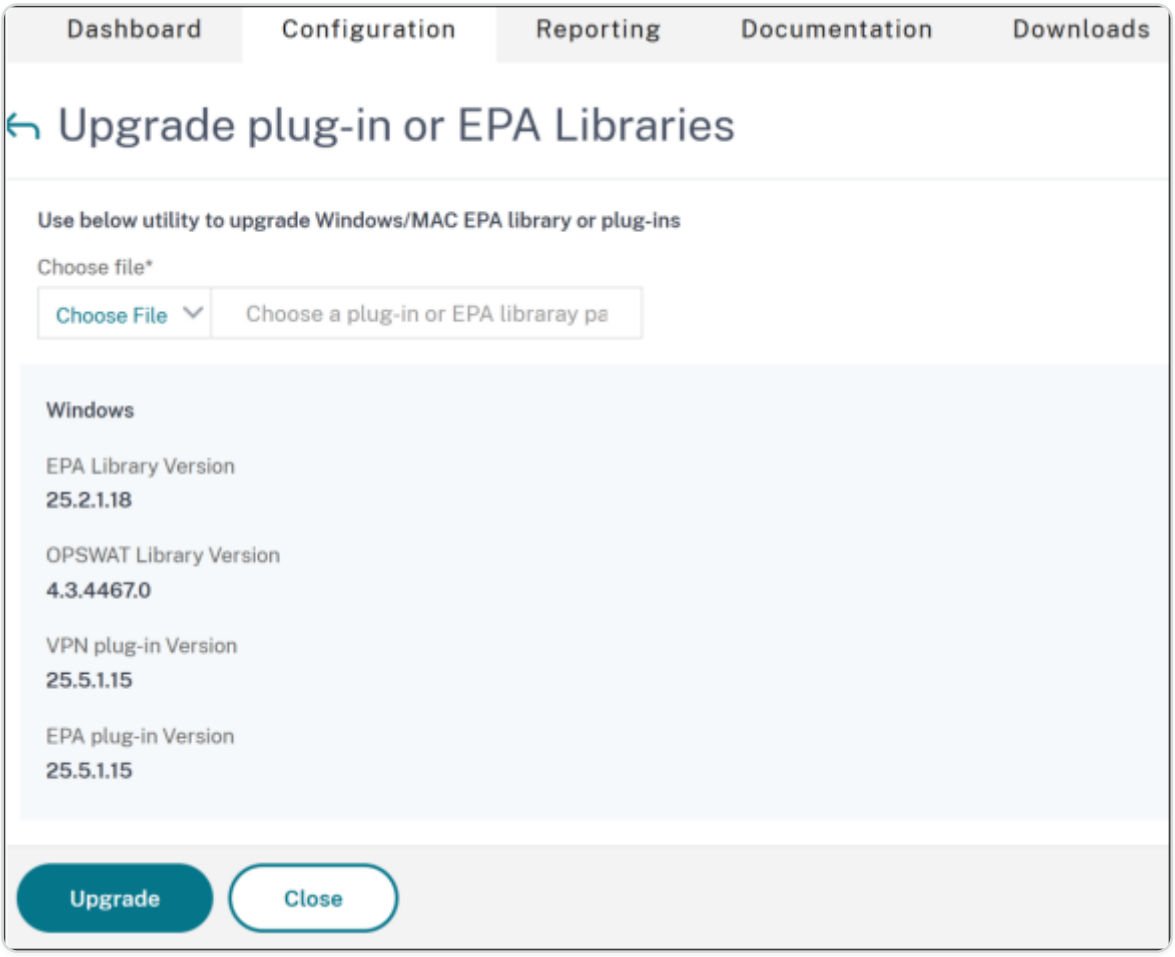
```
{

"Description": "This zip file contains VPN and EPA Plugins for
Windows",

"packages": [

    {

    "metadata": {

        "version": "25.5.1.15"

            "compatibleFrom": "25.5.1.15",

            "compatibleTill": ""

    },

    "type": "WIN-VPN"

    },

    {

    "metadata": {

        "version": "25.5.1.15"

            "compatibleFrom": "25.5.1.15",

            "compatibleTill": ""

    },

    "type": "WIN-EPA"
```

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

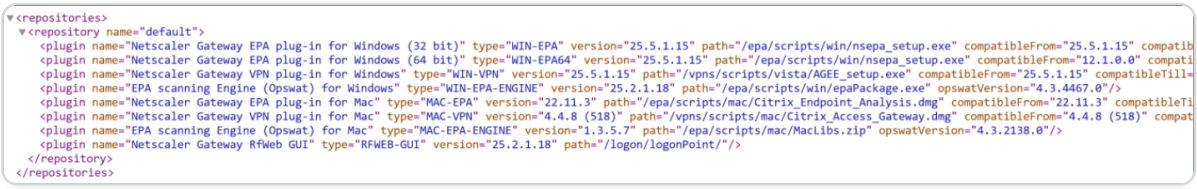
```
    },
    {
    "metadata": {
        "version": "25.5.1.15"
            "compatibleFrom": "25.5.1.15",
            "compatibleTill": ""
    },
    "type": "WIN-EPA64"
    }
]
}
```

d. 将所有三个文件重新压缩为 .tgz 格式，然后将此新的 .tgz 文件上传到 NetScaler。有关更多信息，请参阅 在 NetScaler Gateway 上升级适用于 Windows 的 Citrix Secure Access 客户端和 EPA 客户端。

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



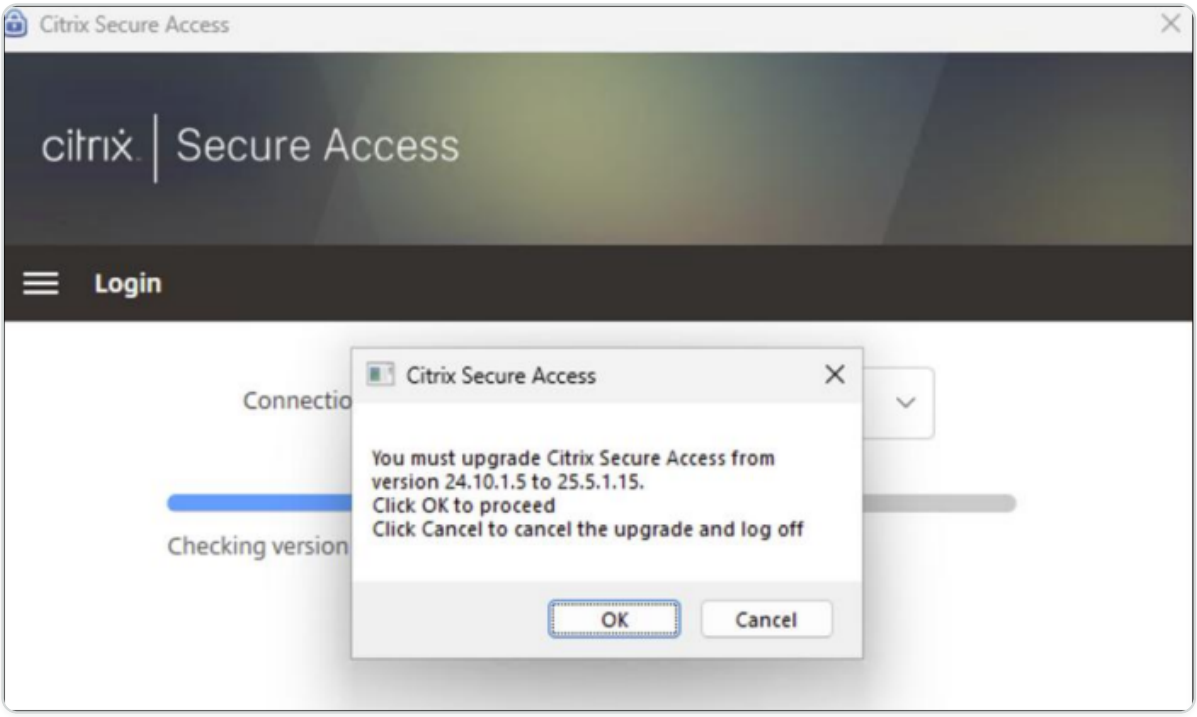
e. 上传后，验证 NetScaler 上的 `pluginList.xml` 文件是否已使用正确的 `compatibleFrom` 值进行更新。



```
▼<repositories>
 ▼<repository name="default">
    <plugin name="Netscaler Gateway EPA plug-in for Windows (32 bit)" type="WIN-EPA" version="25.5.1.15" path="/epa/scripts/win/nsepa_setup.exe" compatibleFrom="25.5.1.15" compatib
    <plugin name="Netscaler Gateway EPA plug-in for Windows (64 bit)" type="WIN-EPA64" version="25.5.1.15" path="/epa/scripts/win/nsepa_setup.exe" compatibleFrom="12.1.0.0" compati
    <plugin name="Netscaler Gateway VPN plug-in for Windows" type="WIN-VPN" version="25.5.1.15" path="/vpns/scripts/vista/AGEE_setup.exe" compatibleFrom="25.5.1.15" compatibleTill=
    <plugin name="EPA scanning Engine (Opswat) for Windows" type="WIN-EPA-ENGINE" version="25.2.1.18" path="/epa/scripts/win/epaPackage.exe" opswatVersion="4.3.4467.0"/>
    <plugin name="Netscaler Gateway EPA plug-in for Mac" type="MAC-EPA" version="22.11.3" path="/epa/scripts/mac/Citrix_Endpoint_Analysis.dmg" compatibleFrom="22.11.3" compatibleTi
    <plugin name="Netscaler Gateway VPN plug-in for Mac" type="MAC-VPN" version="4.4.8 (518)" path="/vpns/scripts/mac/Citrix_Access_Gateway.dmg" compatibleFrom="4.4.8 (518)" compat
    <plugin name="EPA scanning Engine (Opswat) for Mac" type="MAC-EPA-ENGINE" version="1.3.5.7" path="/epa/scripts/mac/MacLibs.zip" opswatVersion="4.3.2138.0"/>
    <plugin name="Netscaler Gateway RfWeb GUI" type="RFWEB-GUI" version="25.2.1.18" path="/logon/logonPoint/"/>
  </repository>
</repositories>
```

f. 从适用于 Windows 的 Citrix Secure Access 客户端连接到虚拟服务器 URL。系统会提示用户继续进行插件升级。

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



- **从不**

  插件不会升级。

> **注意：**
>
> 对于 eLux® 和 IGEL OS，**客户端体验**选项卡中的**Linux 插件升级**选项必须始终设置为**从不**。

用于控制 VPN 插件升级的 CLI 参数

NetScaler Gateway 支持 Windows 和 Mac 操作系统上的两种插件（EPA 和 VPN）。为了在会话级别支持 VPN 插件升级控制，NetScaler Gateway 支持两个名为 WindowsinPluginUpgrade 和 MacPluginUpgrade 的会话配置文件参数。

这些参数可在全局、虚拟服务器、组和用户级别使用。每个参数可以具有 Always、Essential 或 Never 值。有关这些参数的说明，请参阅插件行为。

用于控制 EPA 插件升级的 CLI 参数

NetScaler Gateway 支持 Windows 和 Mac 操作系统上的 EPA 插件。为了在虚拟服务器级别支持 EPA 插件升级控制，NetScaler Gateway 支持两个名为 windowsEPAPluginUpgrade 和 macEPAPluginUpgrade 的虚拟服务器参数。

这些参数可在虚拟服务器级别使用。每个参数可以具有 Always、Essential 或 Never 值。有关这些参数的说明，请参阅插件行为

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

VPN 配置

请按照以下步骤进行 Windows、Linux 和 Mac 插件的 **VPN 配置**。

1. 转到 **NetScaler > 策略 > 会话**。
2. 选择所需的会话策略，然后单击**编辑**。
3. 选择**客户端体验**选项卡。
4. 这些对话框选项会影响升级行为。

   - 始终
   - 必要
   - 从不

   默认值为“始终”。
5. 选中每个选项右侧的复选框。选择应用升级行为的频率。

   升级选项(/en-us/netscaler-gateway/media/figure6-expandedpluginview.png)

EPA 配置

请按照以下步骤配置 Windows、Linux 和 Apple 插件的 EPA。

1. 转到 **NetScaler Gateway > 虚拟服务器**。
2. 选择一个服务器，然后单击“**编辑**”按钮。
3. 单击“**铅笔**”图标。

   单击铅笔图标(/en-us/netscaler-gateway/media/figa_vpnserver.png)
4. 单击“**更多**”
5. 出现的对话框会影响升级行为。可用选项包括：

   - 始终
   - 必需
   - 从不

在 NetScaler Gateway 上设置完整 VPN

本节介绍如何在 NetScaler Gateway 设备上配置完整 VPN 设置。它包含网络注意事项以及从网络角度解决问题的理想方法。

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

先决条件

- 安装 SSL 证书并将其绑定到 VPN 虚拟服务器。
  - CTX109260 - 如何在 NetScaler 设备上生成和安装公共 SSL 证书
  - CTX122521 - 如何使用与设备主机名匹配的可信 CA 证书替换 NetScaler 设备的默认证书
  - NetScaler 文档 - 将证书密钥对绑定到基于 SSL 的虚拟服务器
- 为 NetScaler Gateway 创建身份验证配置文件。
  - 有关其他信息，请参阅 NetScaler 文档 - 配置外部用户身份验证
  - 有关其他信息，请参阅清单：使用 AD FS 实施和管理单点登录
- 下载 VPN 客户端。
- 创建允许完整 VPN 连接的会话策略。

当用户使用 Citrix Secure Access 客户端、Secure Hub 或 Citrix Workspace 应用程序连接时，客户端软件会通过端口 443（或 NetScaler Gateway 上配置的任何端口）建立安全隧道并发送身份验证信息。隧道建立后，NetScaler Gateway 会向 Citrix Secure Access 客户端、Citrix Secure Hub 或 Citrix Workspace 应用程序发送配置信息，描述要保护的网络。如果您启用内网 IP，该信息还包含一个 IP 地址。

您可以通过定义用户可以在内部网络中访问的资源来配置用户设备连接。配置用户设备连接包括以下内容：

- 拆分隧道
- 用户的 IP 地址，包括地址池（内部网 IP）
- 通过代理服务器的连接
- 定义允许用户访问的域
- 超时设置
- 单点登录
- 通过 NetScaler Gateway 连接的用户软件
- 移动设备访问

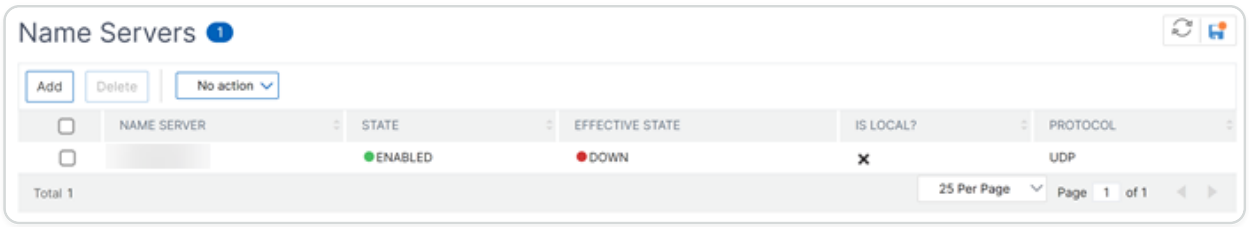
您可以通过会话策略中的配置文件来配置大多数用户设备连接。您还可以使用每个身份验证、流量和授权策略来定义用户设备连接设置。它们也可以使用内部网应用程序进行配置。

在 NetScaler Gateway 设备上配置完整的 VPN 设置

若要在 NetScaler Gateway 设备上配置 VPN 设置，请完成以下步骤：

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

1. 导航到 **流量管理 > DNS**。
2. 选择“名称服务器”节点，如以下屏幕截图所示。确保列出了 DNS 名称服务器。如果不可用，请添加一个 DNS 名称服务器。



3. 展开 **NetScaler Gateway > 策略**。
4. 选择“**会话**”节点。
5. 在 NetScaler Gateway 会话策略和配置文件页面中，单击“**配置文件**”选项卡，然后单击“**添加**”。对于在“配置 NetScaler Gateway 会话配置文件”对话框中配置的每个组件，请确保为相应组件选择“**覆盖全局**”选项。
6. 单击“**客户端体验**”选项卡。
7. 如果希望在用户登录 VPN 时显示任何 URL，请在“主页”字段中键入内网门户 URL。如果主页参数设置为“nohomepage.html”，则不显示主页。当插件启动时，浏览器实例会自动启动并终止。
8. 确保从“拆分隧道”列表中选择所需设置。
9. 如果需要 FullVPN，请从“**无客户端访问**”列表中选择“**关闭**”。
10. 确保从“**插件类型**”列表中选择“**Windows/Mac OS X**”。
11. 如果需要，请选择“**Web 应用程序单点登录**”选项。
12. 如果需要，请确保选中“**客户端清理提示**”选项，如下图所示：

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

Home Page

none ☑ Override Global

URL for Web-Based Email

https://exch2013.cgwsanity.net ☑ Override Global ⓘ

Split Tunnel*

OFF ☐ Override Global

Session Time-out (mins)

30 ☐ Override Global

Client Idle Time-out (mins)

☐ Override Global

Clientless Access*

Off ☑ Override Global ⓘ

Clientless Access URL Encoding*

Obscure ☐ Override Global

Clientless Access Persistent Cookie*

DENY ☐ Override Global ⓘ

Advanced Clientless VPN Mode*

DISABLED ☐ Override Global ⓘ

Plug-in Type*

Windows/MAC OS X ☑ Override Global ⓘ

Windows Plugin Upgrade

Always ☐ Override Global

Linux Plugin Upgrade

Always ☐ Override Global

MAC Plugin Upgrade

Always ☐ Override Global

AlwaysON Profile Name

Add Edit ☐ Override Global

The SSO setting does not honor the following authentication types. BASIC, DIGEST, and NTLM (without Negotiat

☑ Single Sign-on to Web Applications ☑ Override Global ⓘ

Credential Index*

PRIMARY ☐ Override Global

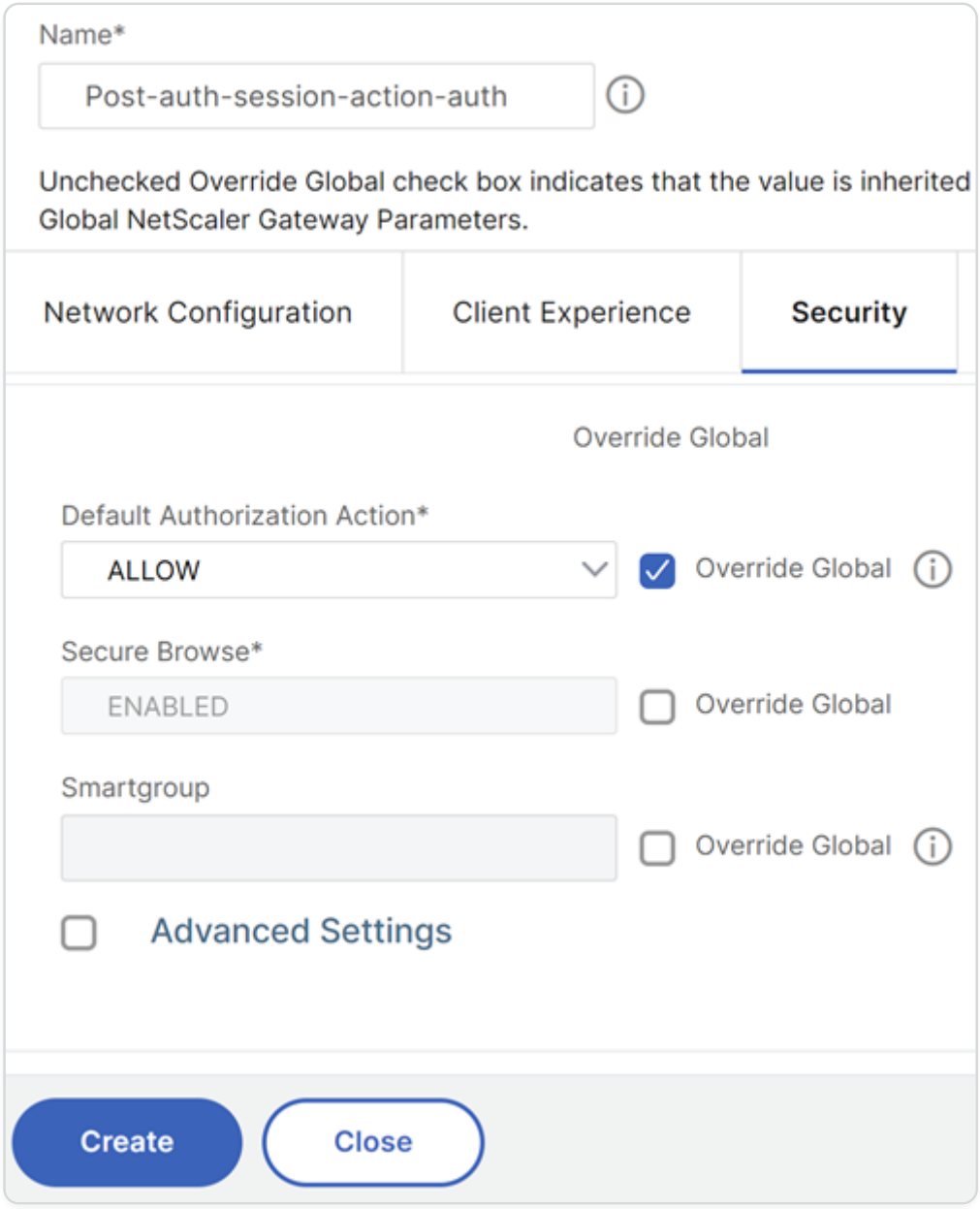
KCD Account

Add Edit ☐ Override Global

Single Sign-on with Windows*

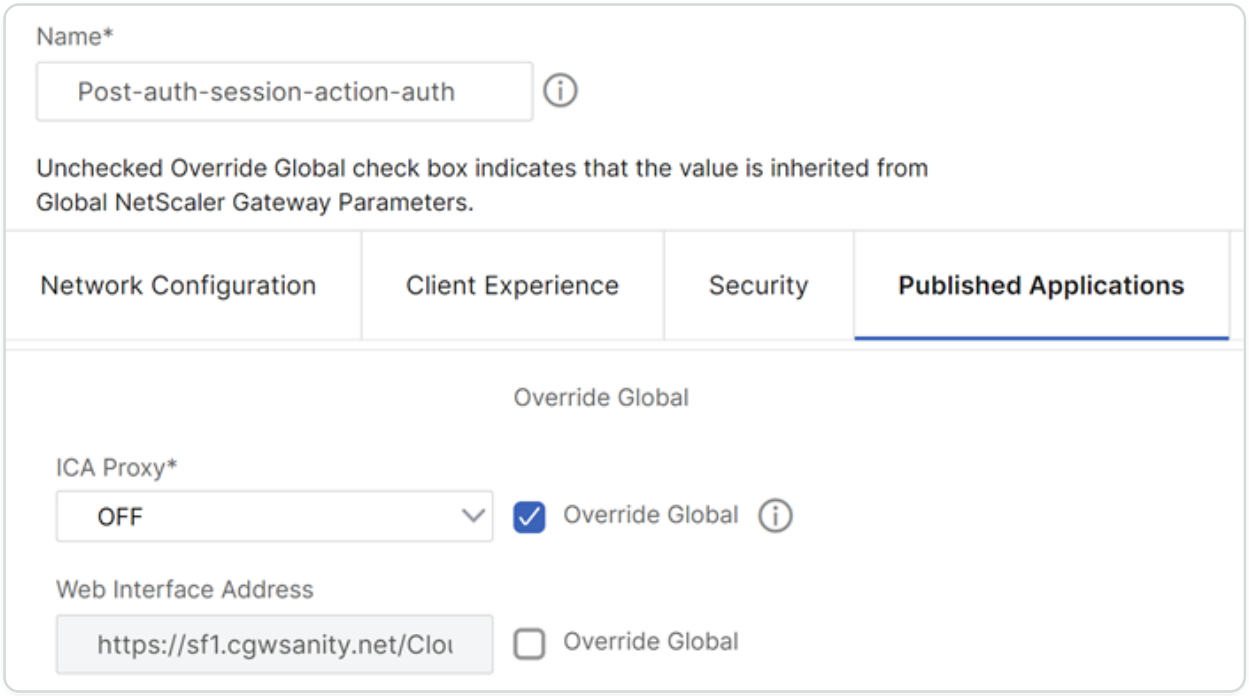
OFF ☐ Override Global

13. 单击“**安全**”选项卡。
14. 确保从“**默认授权操作**”列表中选择“**允许**”。

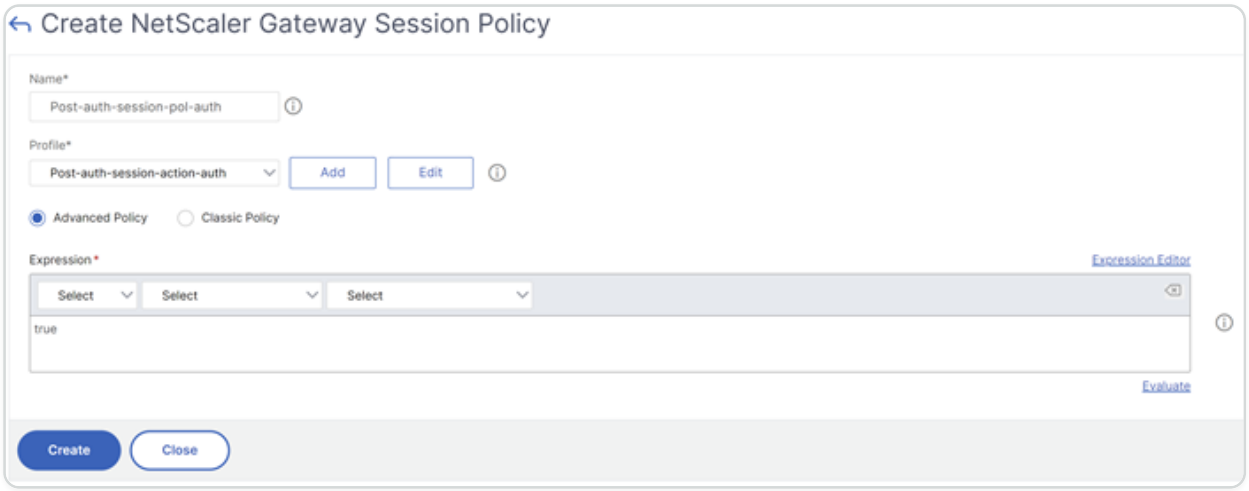


15. 单击“**已发布应用程序**”选项卡。
16. 确保在“**已发布应用程序**”选项下，从“**ICA® 代理**”列表中选择“**关闭**”。

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



17. 单击“**创建**”。
18. 单击“**关闭**”。
19. 在虚拟服务器中，单击 NetScaler Gateway 会话策略和配置文件页面的“**策略**”选项卡，或根据需要激活 GROUP/USER 级别的会话策略。
20. 使用所需表达式或 true 创建会话策略，如以下屏幕截图所示：

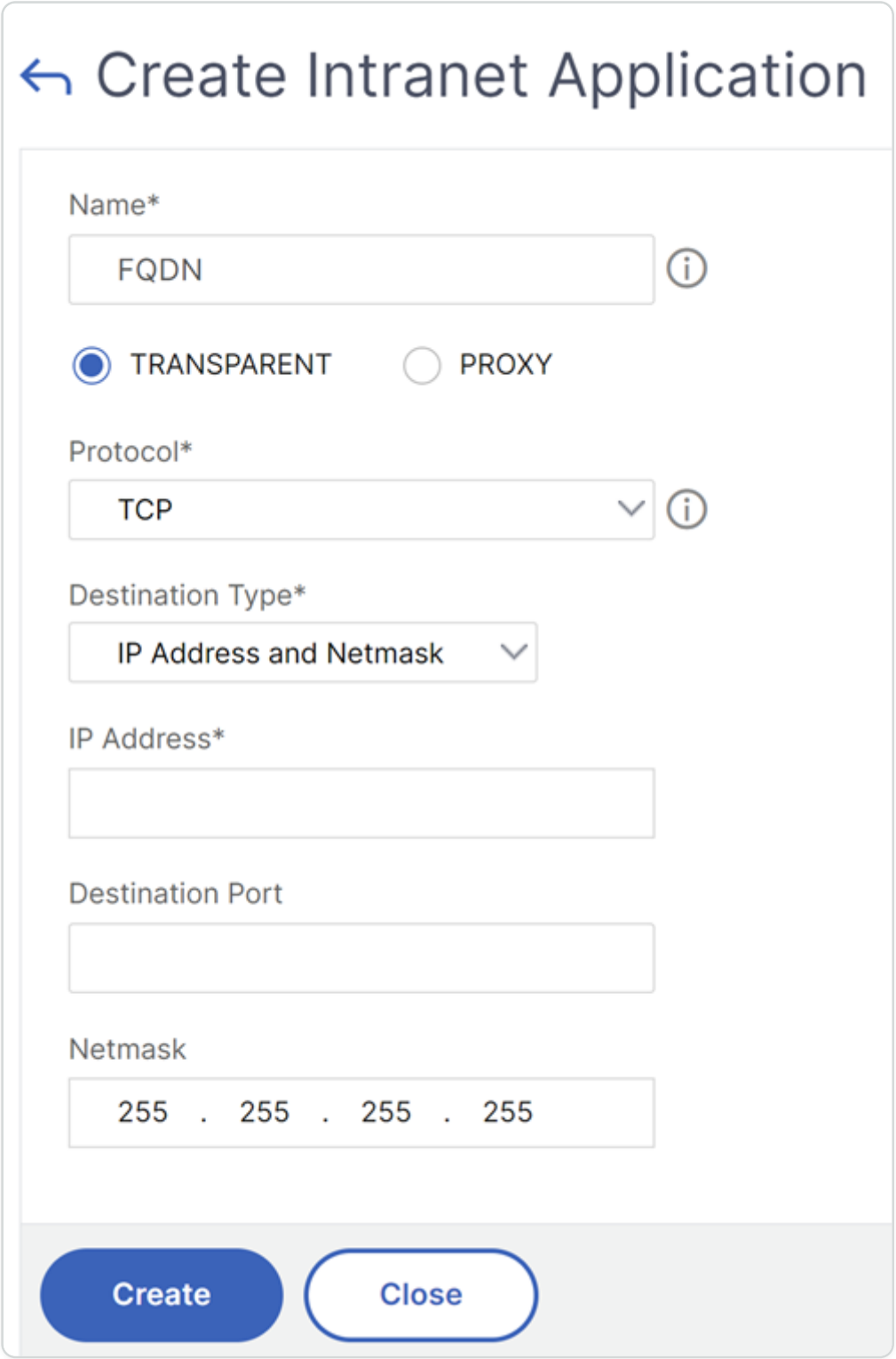


21. 将会话策略绑定到 VPN 虚拟服务器。有关详细信息，请参阅绑定会话策略。

    如果分流隧道配置为“开”，则必须配置用户连接到 VPN 时希望访问的内网应用程序。有关内网应用程序的详细信息，请参阅为 Citrix Secure Access 客户端配置内网应用程序。

    a. 转到 **NetScaler Gateway > 资源 > 内网应用程序**。
    b. 创建内网应用程序。对于使用 Windows 客户端的 FullVPN，选择“透明”。选择您希望允许的协议（TCP、UDP 或 ANY）、目标类型（IP 地址和掩码、IP 地址范围或主机名）。

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



c. 如有必要，使用以下表达式为 iOS 和 Android 上的 VPN 设置新策略：

```
HTTP.REQ.HEADER("User-Agent").CONTAINS("CitrixVPN")&&HTTP.REQ.HEADER("User-Agent").CONTAINS("NSGiOSplugin")&&HTTP.REQ.HEADER("User-Agent").CONTAINS("Android")
```

d. 根据需要将创建的内网应用程序绑定到 USER/GROUP/VSERVER 级别。

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

注意：

即使访问策略明确允许，发布在端口 80 (HTTP) 上的 Web 应用程序也会自动被阻止。要解决此问题，请在 NetScaler Gateway shell 中运行以下命令：

```
nsapimgr -y -s vpn_http_port80=0
```

为了在重新启动后保持持久性，请将此命令添加到 `/nsconfig/rc.netscaler`。

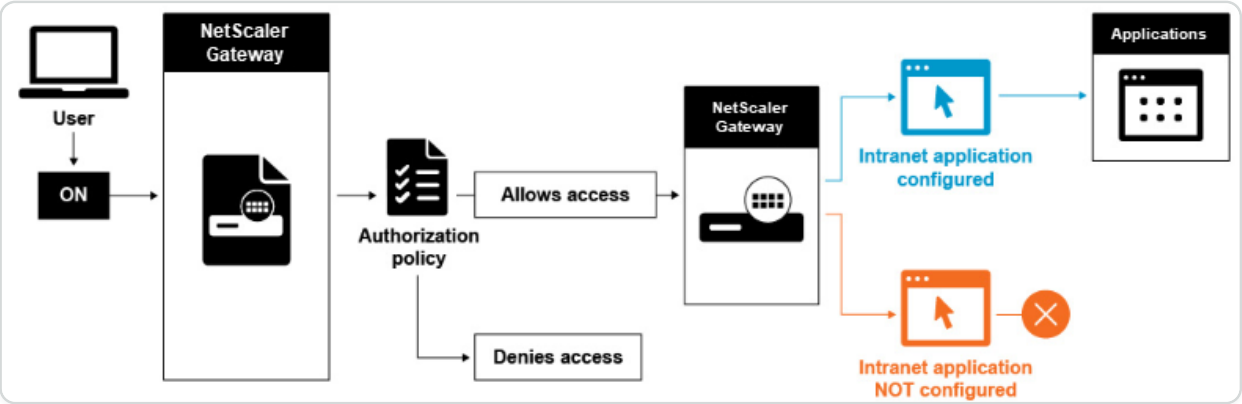
配置拆分隧道

1. 导航到 **配置** > **NetScaler Gateway > 策略 > 会话**。
2. 在详细信息窗格中，在“配置文件”选项卡上，选择一个配置文件，然后单击“**编辑**”。
3. 在“**客户端体验**”选项卡上，在“**拆分隧道**”旁边，选择“**全局覆盖**”，选择一个选项，然后单击“**确定**”。

   配置拆分隧道和授权

   规划 NetScaler Gateway 部署时，务必考虑拆分隧道以及默认授权操作和授权策略。

   例如，您有一个授权策略，允许访问网络资源。您已将拆分隧道设置为“开”，并且未配置内部网应用程序通过 NetScaler Gateway 发送网络流量。当 NetScaler Gateway 具有此类配置时，允许访问资源，但用户无法访问该资源。



如果授权策略拒绝访问网络资源，Citrix Secure Access 客户端会将流量发送到 NetScaler Gateway，但在以下情况下，对资源的访问将被拒绝。

- 您已将拆分隧道设置为“开”。
- 内部网应用程序配置为通过 NetScaler Gateway 路由网络流量

有关授权策略的更多信息，请查看以下内容：

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

- 配置授权
- 配置授权策略
- 设置默认全局授权

配置对内部网络资源的访问

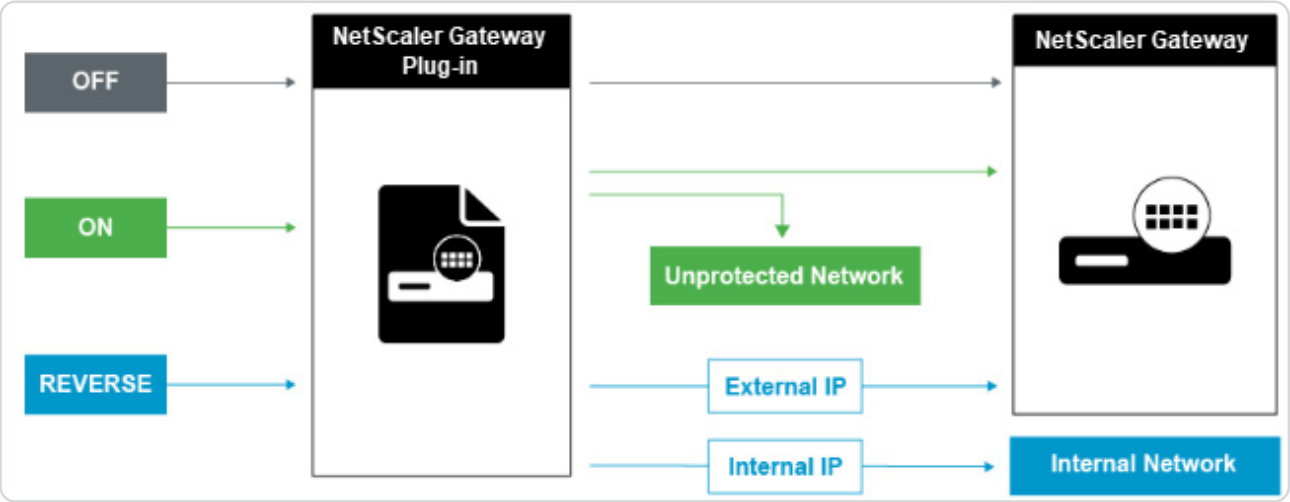
1. 导航到 **配置** > **NetScaler Gateway > 资源 > 内网应用程序**。
2. 在详细信息窗格中，单击 **Add**。
3. 完成允许网络访问的参数，单击 **Create**，然后单击 **Close**。

当我们不为 VPN 用户设置内网 IP 时，用户会将流量发送到 NetScaler Gateway VIP，然后 NetScaler 设备会从那里构建一个新数据包，发送到内部 LAN 上的内网应用程序资源。这个新数据包将从 SNIP 发送到内网应用程序。从这里，内网应用程序接收数据包，处理它，然后尝试回复该数据包的源（在这种情况下是 SNIP）。SNIP 接收数据包并将回复发送给发出请求的客户端。

当使用内网 IP 地址时，用户会将流量发送到 NetScaler Gateway VIP，然后 NetScaler 设备会将客户端 IP 映射到池中配置的其中一个内网 IP。请注意，NetScaler 设备将拥有内网 IP 池，因此这些范围不得在内部网络中使用。NetScaler 设备会像 DHCP 服务器一样为传入的 VPN 连接分配一个内网 IP。NetScaler 设备会构建一个新数据包，发送到用户将访问的 LAN 上的内网应用程序。这个新数据包将从其中一个内网 IP 发送到内网应用程序。从这里，内网应用程序接收数据包，处理它，然后尝试回复该数据包的源（内网 IP）。在这种情况下，回复数据包需要路由回 NetScaler 设备，即内网 IP 所在的位置（请记住，NetScaler 设备拥有内网 IP 子网）。为了完成此任务，网络管理员必须有一个指向其中一个 SNIP 的内网 IP 路由。建议将流量指向首次数据包离开 NetScaler 设备时所使用的 SNIP，以避免任何非对称流量。

分流隧道选项

以下是各种分流隧道选项。



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

分流隧道关闭

当分流隧道设置为关闭时，Citrix Secure Access 客户端会捕获来自用户设备的所有网络流量，并通过 VPN 隧道将流量发送到 NetScaler Gateway。换句话说，VPN 客户端会从客户端 PC 建立一个指向 NetScaler Gateway VIP 的默认路由，这意味着所有流量都需要通过隧道发送才能到达目的地。由于所有流量都将通过隧道发送，因此授权策略必须确定流量是否允许通过到内部网络资源，或者被拒绝。

当设置为“关闭”时，所有流量（包括到网站的标准 Web 流量）都将通过隧道。如果目标是监控和控制这些 Web 流量，则必须使用 NetScaler 设备将这些请求转发到外部代理。用户设备也可以通过代理服务器连接以访问内部网络。

NetScaler Gateway 支持 HTTP、SSL、FTP 和 SOCKS 协议。要为用户连接启用代理支持，您必须在 NetScaler Gateway 上指定这些设置。您可以在 NetScaler Gateway 上指定代理服务器使用的 IP 地址和端口。代理服务器用作所有后续内部网络连接的正向代理。

有关更多信息，请查看以下链接：

- 启用用户连接的代理支持

分流隧道开启

您可以启用拆分隧道，以防止 Citrix Secure Access 客户端向 NetScaler Gateway 发送不必要的网络流量。如果启用了拆分隧道，Citrix Secure Access 客户端将仅通过 VPN 隧道发送目标为受 NetScaler Gateway 保护的网络（内部网应用程序）的流量。Citrix Secure Access 客户端不会将目标为未受保护网络的网络流量发送到 NetScaler Gateway。当 Citrix Secure Access 客户端启动时，它会从 NetScaler Gateway 获取内部网应用程序列表，并为客户端 PC 上内部网应用程序选项卡中定义的每个子网建立路由。Citrix Secure Access 客户端会检查从用户设备传输的所有数据包，并将数据包中的地址与内部网应用程序列表（VPN 连接启动时创建的路由表）进行比较。如果数据包中的目标地址在某个内部网应用程序范围内，Citrix Secure Access 客户端会将数据包通过 VPN 隧道发送到 NetScaler Gateway。如果目标地址不在定义的内部网应用程序中，则数据包不会加密，然后用户设备会使用客户端 PC 上最初定义的默认路由适当地路由数据包。“当您启用拆分隧道时，内部网应用程序会定义被拦截并通过隧道发送的网络流量。”.

反向拆分隧道

NetScaler Gateway 还支持反向拆分隧道，它定义了 NetScaler Gateway 不会拦截的网络流量。如果将拆分隧道设置为反向，则内部网应用程序会定义 NetScaler Gateway 不会拦截的网络流量。启用反向拆分隧道后，所有指向内部 IP 地址的网络流量都会绕过 VPN 隧道，而其他流量则通过 NetScaler Gateway。反向拆分隧道可用于记录所有非本地 LAN 流量。例如，如果用户拥有家庭无

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

线网络并使用 Citrix Secure Access 客户端登录，NetScaler Gateway 不会拦截目标为无线网络中打印机或其他设备的网络流量。

注意：

适用于 Windows、macOS、iOS 和 Android 的 Citrix Secure Access 客户端支持基于 FQDN 的反向拆分隧道。对于 Windows 客户端，从 Citrix Secure Access 22.6.1.5 开始，此功能仅在启用 WFP 驱动程序时才有效。

注意事项

基于 IP 的反向拆分隧道：

- 基于 IP 地址的规则数量限制为 1024 条。
- DNE 和 WFP 驱动程序均支持。

基于主机名的反向拆分隧道：

- VPN 会话期间可访问的主机名数量受 FQDN 欺骗范围中指定的可用 IP 地址数量的限制。这是因为每个主机名都会占用 FQDN 欺骗范围中的一个 IP 地址。一旦 IP 范围耗尽，最近最少分配的 IP 地址将重新用于下一个新主机名。
- 必须配置 DNS 后缀。

  注意：

  - 适用于 Windows、macOS、iOS 和 Android 的 Citrix Secure Access™ 客户端支持基于主机名的反向拆分隧道。
  - 对于 Windows 客户端，仅 WFP 驱动程序支持基于主机名的反向拆分隧道。通过将 `EnableWFP` 注册表值设置为 `1` 来启用 WFP 驱动程序模式。有关详细信息，请参阅使用 Windows 筛选平台的 Windows Citrix Secure Access 客户端。
  - 对于 Android 客户端，基于主机名的反向分流隧道处于预览阶段。请联系 NetScaler® 支持以启用此功能。

基于 IP 和基于主机名的反向分流隧道：

- 仅支持 WFP 驱动程序。基于 IP 的反向分流隧道和基于主机名的反向分流隧道中提及的所有其他指南均适用。

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

配置名称服务解析

在安装 NetScaler Gateway 期间，您可以使用 NetScaler Gateway 向导配置其他设置，包括名称服务提供程序。名称服务提供程序将完全限定域名 (FQDN) 转换为 IP 地址。在 NetScaler Gateway 向导中，您还可以执行以下操作：

- 配置 DNS 或 WINS 服务器
- 设置 DNS 查找的优先级
- 设置重试连接到服务器的次数。

运行 NetScaler Gateway 向导时，您可以添加一个 DNS 服务器。您可以使用会话配置文件向 NetScaler Gateway 添加其他 DNS 服务器和 WINS 服务器。然后，您可以将用户和组定向到连接到与您最初使用向导配置的服务器不同的名称解析服务器。

在 NetScaler Gateway 上配置另一个 DNS 服务器之前，请创建一个充当名称解析 DNS 服务器的虚拟服务器。

在会话配置文件中添加 DNS 或 WINS 服务器

1. 在配置实用程序中，配置选项卡 > **NetScaler Gateway > 策略 > 会话**。
2. 在详细信息窗格中，在“配置文件”选项卡上，选择一个配置文件，然后单击“打开”。
3. 在“网络配置”选项卡上，执行以下操作之一：
   - 要配置 DNS 服务器，请在 **DNS 虚拟服务器**旁边，单击 **覆盖全局**，选择服务器，然后单击 **确定**。
   - 要配置 WINS 服务器，在 **WINS Server IP** 旁边，单击 **Override Global**，键入 IP 地址，然后单击 **OK**。

参考

- 拆分隧道
- 用户如何使用 Citrix Secure Access 客户端连接
- 关于 NetScaler Gateway
- 选择用户访问方法

选择用户访问方法

您可以将 NetScaler Gateway 配置为通过以下方案提供用户连接：

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

- 通过使用 Citrix Workspace 应用程序的用户连接。Citrix Workspace 应用程序与 StoreFront 兼容，可为用户提供对服务器场中已发布的应用程序或虚拟桌面的访问。Citrix Workspace 应用程序是使用 ICA 网络协议建立用户连接的软件。用户在用户设备上安装 Citrix Workspace 应用程序。当用户在其基于 Windows 或 Mac 的计算机上安装 Citrix Workspace 应用程序时，Citrix Workspace 应用程序会包含所有插件，包括用于用户连接的 Citrix Secure Access 客户端。NetScaler Gateway 还支持来自适用于 Android 的 Citrix Workspace 应用程序和适用于 iOS 的 Citrix Workspace 应用程序的连接。用户可以通过 Citrix Endpoint Management 或 StoreFront 连接到其虚拟桌面以及基于 Windows、Web、移动和 SaaS 应用程序。
- 通过 Secure Hub 的用户连接。用户可以连接到在 Endpoint Management 中配置的移动、Web 和 SaaS 应用程序。用户在其移动设备（Android 或 iOS）上安装 Secure Hub。当用户登录 Secure Hub 时，他们可以安装 WorxMail 和 WorxWeb，以及您在 Endpoint Management 中安装的任何其他移动应用程序。Secure Hub、Secure Mail 和 WorxWeb 使用 Micro VPN 技术通过 NetScaler Gateway 建立连接。
- 通过使用 Citrix Secure Access™ 客户端作为独立应用程序的用户连接。Citrix Secure Access 客户端是用户可以在用户设备上下载和安装的软件。当用户使用插件登录时，他们可以访问安全网络中的资源，就像在办公室一样。资源包括电子邮件服务器、文件共享和内部网网站。
- 通过使用无客户端访问的用户连接。无客户端访问为用户提供所需的访问权限，而无需在用户设备上安装软件，例如 Citrix Secure Access 客户端或 Citrix Workspace 应用程序。无客户端访问允许连接到有限的 Web 资源集，例如 Outlook Web Access 或 SharePoint、在 Citrix Virtual Apps 上发布的应用程序、来自 Citrix Virtual Apps and Desktops 的虚拟桌面，以及通过访问接口访问安全网络中的文件共享。用户通过在 Web 浏览器中输入 NetScaler Gateway Web 地址，然后从选择页面中选择无客户端访问来连接。
- 如果预身份验证或后身份验证扫描失败，则进行用户连接。此方案称为访问方案回退。如果用户设备未通过初始端点分析扫描，访问方案回退允许用户设备通过使用 Citrix Workspace 应用程序从 Citrix Secure Access 客户端回退到 StoreFront。

  如果用户通过 Citrix Workspace 应用程序登录 NetScaler Gateway，则预身份验证扫描不起作用。当 NetScaler Gateway 建立 VPN 隧道时，后身份验证扫描确实起作用。

用户可以通过以下方法下载和安装 Citrix Secure Access 客户端：

- 通过使用 Web 浏览器连接到 NetScaler Gateway。
- 连接到配置为接受 NetScaler Gateway 连接的 StoreFront。
- 通过使用组策略对象 (GPO) 安装插件。
- 将 NetScaler 插件上传到 Merchandising Server。

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

部署 Citrix Secure Access™ 客户端供用户访问

NetScaler Gateway 附带以下插件供用户访问：

- 适用于 Windows 的 Citrix Secure Access 客户端
- 适用于 Mac 的 Citrix Secure Access 客户端

当用户首次登录 NetScaler Gateway 时，他们会从网页下载并安装 Citrix Secure Access 客户端。用户可以通过单击 Windows 计算机通知区域中的 NetScaler Gateway 图标登录。在 macOS X 计算机上，用户可以从 **Dock 或应用程序**菜单登录。如果您将 NetScaler Gateway 升级到新的软件版本，Citrix Secure Access 客户端会在用户设备上自动更新。

通过使用 MSI 安装程序包部署 Citrix Secure Access 客户端

您可以使用 Microsoft Active Directory 基础结构部署 Citrix Secure Access 客户端，或使用标准第三方 MSI 部署工具（例如 Windows Server Update Services）进行部署。如果您使用的工具支持 Windows Installer 软件包，则可以使用任何支持 MSI 文件的工具部署这些软件包。然后，您可以使用部署工具在相应的用户设备上部署和安装软件。

使用集中式部署工具的优势

- 能够遵守安全要求。例如，您可以在不为非管理用户启用软件安装权限的情况下安装用户软件。
- 控制软件版本。您可以同时向所有用户部署软件的更新版本。
- 可扩展性。集中式部署策略可轻松扩展以支持更多用户。
- 积极的用户体验。您可以在不让用户参与此过程的情况下部署、测试和排查与安装相关的问题。

当需要对用户软件的安装进行管理控制并且可以轻松访问用户设备时，Citrix® 建议使用此选项。

有关详细信息，请参阅 从 Active Directory 部署 Citrix Secure Access 客户端。

确定要部署哪个软件插件

如果您的 NetScaler Gateway 部署不需要在用户设备上安装任何软件插件，则您的部署被视为提供无客户端访问。在这种情况下，用户只需一个 Web 浏览器即可访问网络资源。但是，某些功能需要在用户设备上安装插件软件。

为用户选择 Citrix Secure Access™ 客户端

配置 NetScaler Gateway 时，您可以选择用户登录方式。用户可以使用以下插件之一登录：

- 适用于 Windows 的 Citrix Secure Access 客户端

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

- 适用于 macOS 的 Citrix Secure Access 客户端

您可以通过创建会话策略，然后将策略绑定到用户、组或虚拟服务器来完成配置。您还可以通过配置全局设置来启用插件。在全局或会话配置文件中，您可以选择 Windows 或 macOS X 作为插件类型。用户登录时，他们会收到全局或会话配置文件和策略中定义的插件。为插件类型创建单独的配置文件。

全局配置插件

1. 导航到 **NetScaler Gateway > 全局设置**。
2. 在详细信息窗格中，在 **设置** 下，单击 **更改全局设置**。
3. 在 **客户端体验** 选项卡上，在 **插件类型** 旁边，选择 **Windows/MAC OS X**，然后单击 **确定**。

在会话配置文件中配置适用于 Windows 或 macOS 的插件类型

1. 导航到 **NetScaler Gateway > 策略 > 会话**。
2. 执行以下操作之一：
   - 如果要创建会话策略，请在详细信息窗格中单击 **添加**。
   - 如果要更改现有策略，请选择一个策略，然后单击 **打开**。
3. 创建配置文件或修改现有配置文件。为此，请执行以下操作之一：
   - 在 **配置文件** 旁边，点击 **添加**。
   - 在 **配置文件** 旁边，点击 **编辑**。
4. 在 **客户端体验** 选项卡中，在 **插件类型** 旁边，点击 **覆盖全局**，然后选择 **Windows/MAC OS X**。
5. 执行以下操作之一：
   - 如果您正在创建配置文件，点击 **创建**，在策略对话框中设置表达式，点击 **创建**，然后点击 **关闭**。
   - 如果您正在修改现有配置文件，在做出选择后，点击两次 **确定**。

适用于 Windows 的 Citrix Secure Access 客户端

当用户登录到 NetScaler Gateway 时，他们会在用户设备上下载并安装 Citrix Secure Access 客户端。

要安装插件，用户必须是本地管理员或 Administrators 组的成员。此限制仅适用于首次安装。插件升级不需要管理员级别的访问权限。

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

要使用户能够连接和使用 NetScaler Gateway，您需要向他们提供以下信息：

- NetScaler Gateway 网址，例如 `<https://NetScalerGatewayFQDN/>`
- 如果您配置了端点资源和策略，则运行 Citrix Secure Access 客户端的任何系统要求

根据用户设备的配置，您可能还需要提供以下信息：

- 如果用户在其计算机上运行防火墙，他们必须更改防火墙设置，以使防火墙不会阻止与您授予访问权限的资源对应的 IP 地址之间的流量。Citrix Secure Access 客户端会自动处理 Windows XP 中的 Internet 连接防火墙以及 Windows XP Service Pack 2、Windows Vista、Windows 7、Windows 8 或 Windows 8.1 中的 Windows 防火墙。
- 希望通过 NetScaler Gateway 连接将流量发送到 FTP 的用户必须将其 FTP 应用程序设置为执行被动传输。被动传输意味着远程计算机建立与您的 FTP 服务器的数据连接，而不是由 FTP 服务器建立与远程计算机的数据连接。
- 希望通过连接运行 X 客户端应用程序的用户必须在其计算机上运行 X 服务器，例如 `XManager`。
- 安装适用于 Windows 的 Receiver 或适用于 Mac 的 Receiver 的用户可以从 Receiver 或通过使用 Web 浏览器启动 Citrix Secure Access 客户端。向用户提供有关如何通过 Receiver 或 Web 浏览器使用 Citrix Secure Access 客户端登录的说明。

由于用户处理文件和应用程序时就像它们在组织的本地网络中一样，因此您无需重新培训用户或配置应用程序。

首次建立安全连接时，请使用 Web 登录页面登录 NetScaler Gateway。Web 地址的典型格式为 `<https://companyname.com>`。用户登录后，可以在其计算机上下载并安装 Citrix Secure Access 客户端。

安装适用于 Windows 的 Citrix Secure Access 客户端

1. 在 Web 浏览器中，键入 NetScaler Gateway 的 Web 地址。
2. 键入用户名和密码，然后单击“登录”。
3. 选择“网络访问”，然后单击“下载”。
4. 按照说明安装插件。

下载完成后，Citrix Secure Access 客户端将连接并在基于 Windows 的计算机的通知区域中显示一条消息。

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

如果您希望用户在不使用 Web 浏览器的情况下连接 Citrix Secure Access 客户端，则可以配置插件，使其在用户右键单击基于 Windows 的计算机通知区域中的 **NetScaler Gateway** 图标或从“开始”菜单启动插件时显示登录对话框。

配置适用于 Windows 的 Citrix Secure Access 客户端的登录对话框

要将 Citrix Secure Access 客户端配置为使用登录对话框，用户必须登录才能完成此过程。

1. 在基于 Windows 的计算机上，在通知区域中，右键单击 NetScaler Gateway 图标，然后单击“**配置 NetScaler Gateway**”。
2. 单击“**配置文件**”选项卡，然后单击“**更改配置文件**”。
3. 在“**选项**”选项卡上，单击“**使用 Citrix Secure Access 客户端进行登录**”。

> **注意：**
>
> 如果用户从 Receiver 中打开“**配置 NetScaler Gateway**”对话框，则“**选项**”选项卡不可用。

为适用于 Windows 的 Citrix Secure Access 客户端设置拦截模式

如果您正在配置适用于 Windows 的 Citrix Secure Access 客户端，则还需要配置拦截模式并将其设置为透明。

1. 在配置实用程序中，单击“配置”选项卡，展开“**NetScaler Gateway > 资源**”，然后单击“**内部网应用程序**”。
2. 在详细信息窗格中，单击“**添加**”。
3. 在“**名称**”中，键入策略的名称。
4. 单击“**透明**”。
5. 在“**协议**”中，选择“**任意**”。
6. 在“**目标类型**”中，选择“**IP 地址和网络掩码**”。
7. 在“**IP 地址**”中，键入 IP 地址。
8. 在“**网络掩码**”中，键入子网掩码，单击“**创建**”，然后单击“**关闭**”。

适用于 Windows Citrix Secure Access 的 Microsoft Edge 网页视图支持

适用于 Windows Citrix Secure Access 的 Microsoft Edge WebView 支持可提供增强的最终用户体验。有关详细信息，请参阅 适用于 Windows Citrix Secure Access 的 Microsoft Edge WebView 支持

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

使用 Windows 筛选平台的 Windows Citrix Secure Access 客户端

Windows 筛选平台 (WFP) 是一组 API 和系统服务，提供了一个用于创建网络筛选应用程序的平台。WFP 旨在取代以前的数据包筛选技术，即与 DNE 驱动程序一起使用的网络驱动程序接口规范 (NDIS) 筛选器。Windows Citrix Secure Access 客户端的 22.6.1.5 版本支持 WFP 模式。

安装 WFP 版本

您可以使用以下方法之一安装 WFP 版本。

- 安装同时包含 DNE 和 WFP 驱动程序的 VPN 插件（默认方法）

  当插件同时安装了 DNE 和 WFP 驱动程序时，管理员可以通过注册表项选择使用 WFP 或 DNE 驱动程序进行隧道连接。默认情况下，DNE 驱动程序用于隧道连接。

- 仅安装 WFP 驱动程序的 VPN 插件（跳过 DNE 驱动程序安装）

  即使不使用，某些第三方应用程序也不支持 DNE 驱动程序。对于这些部署，管理员可以使用此安装类型。由于未安装 DNE 驱动程序，因此仅使用 WFP 驱动程序进行隧道连接。

选择 WFP 驱动程序而不是 DNE 驱动程序

执行以下步骤以选择 WFP 驱动程序而不是 DNE 驱动程序。

注意：

这仅适用于默认安装方法。

1. 下载支持 WFP 的 VPN 插件版本并安装新的 VPN 插件。
2. 默认情况下，DNE 驱动程序用于隧道传输流量。要使用 WFP 驱动程序进行隧道连接，管理员必须创建以下注册表项：
   - 注册表路径 - HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Client
     - REG_TYPE - REG_DWORD
     - REG_NAME - EnableWFP
     - REG_VALUE – 将值设置为 1 以使用 WFP，设置为 0 以使用 DNE（如果此注册表值不存在或设置为 0，则默认启用 DNE）

注意：

在将隧道模式从 DNE 切换到 WFP 或反向切换后，系统必须重新启动以使更改正确生效。

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

完全跳过 DNE 安装

执行以下步骤以跳过 DNE 安装。

1. 执行 VPN 插件的干净卸载。

   a. 卸载计算机上当前存在的 VPN 插件并重新启动计算机。

   b. 使用以下任一选项检查 DNE 驱动程序是否已卸载。

      - 打开提升的命令提示符（或 PowerShell）。运行以下命令（示例输出显示基于 DNE 的驱动程序已安装在系统上）

```
PS C:\Users\Administrator> sc qc cag

[SC] QueryServiceConfig SUCCESS

SERVICE_NAME: cag

TYPE               : 1  KERNEL_DRIVER

START_TYPE         : 2   AUTO_START

ERROR_CONTROL      : 1   NORMAL

BINARY_PATH_NAME   : \??\C:\Program Files\Common Files\Deterministic
Networks\Common Files\cag.sys

LOAD_ORDER_GROUP   :

TAG                : 0

DISPLAY_NAME       : Citrix cag plugin for Access Gateway

DEPENDENCIES       :

SERVICE_START_NAME :

PS C:\Users\Administrator> sc qc dne

[SC] QueryServiceConfig SUCCESS



SERVICE_NAME: dne
```

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

```
TYPE               : 1  KERNEL_DRIVER

START_TYPE         : 1   SYSTEM_START

ERROR_CONTROL      : 1   NORMAL

BINARY_PATH_NAME   : \SystemRoot\system32\DRIVERS\dnelwf64.sys

LOAD_ORDER_GROUP   : NDIS

TAG                : 38

DISPLAY_NAME       : DNE LightWeight Filter

DEPENDENCIES       :

SERVICE_START_NAME :
```

如果驱动程序未安装，将显示以下输出：

`The specified service does not exist as an installed service.`.

由于 DNE 驱动程序 (dnelwf64.sys) 也被其他供应商使用，因此即使系统上未安装 Citrix Secure Access 客户端，它也可能存在。另一方面，CAG 插件仅由 Citrix Secure Access 客户端使用。

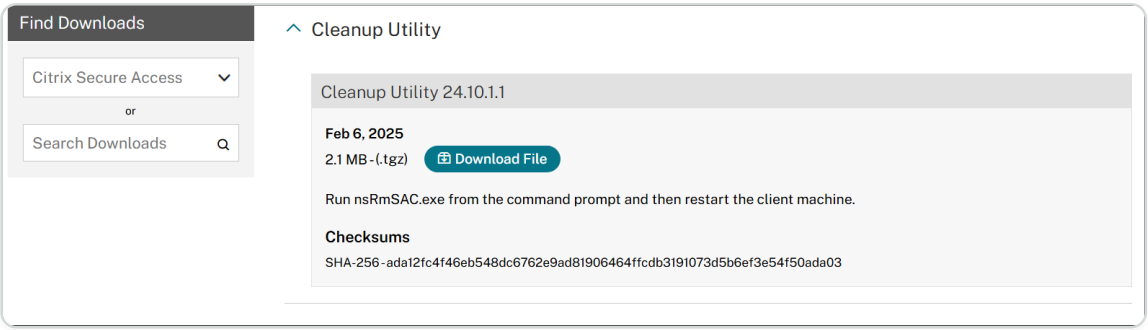
- 还可以通过尝试启动 CAG 和 DNE 驱动程序来检查 DNE 是否存在。使用管理员权限打开命令提示符并运行以下命令：

```
net start cag

net start dne
```

  - 如果输出消息指示无法找到服务（服务名称无效），则插件和驱动程序组件已成功卸载。在这种情况下，请转到步骤 2。
  - 如果插件和驱动程序组件未成功卸载，请按照以下说明在客户端计算机上运行清理实用程序 nsRmSac.exe：
    - 解压清理实用程序并将其复制到文件夹中。
    - 以管理员权限从命令提示符运行 nsRmSAC.exe。
    - 重启客户端计算机。

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

清理实用程序 nsRmSac.exe 可在 思杰下载 页面上的“**清理实用程序**”部分下找到。



注意：

从适用于 Windows 版本 24.10.1.5 的 Citrix Secure Access 客户端开始，清理实用程序 nsRmSac.exe 支持命令行参数 `/quiet` 和 `/autoreboot`。nsRmSac.exe `/quiet /autoreboot` 命令使清理实用程序无需手动干预即可运行。

- `/quiet` 选项会删除 Citrix Secure Access 应用程序和关联的驱动程序。
- `/autoreboot` 选项会在 nsRmSac.exe 实用程序完成清理功能后重新启动系统。`/autoreboot` 参数仅适用于 `/quiet` 选项。

2. 创建以下注册表项。

- 注册表路径 - HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Client
  - 注册表类型 - REG_DWORD
  - 注册表名称 - SkipDNE
  - REG_VALUE - 设置为 1 以确保 DNE 未安装在计算机上
- 注册表路径 - HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Client
  - REG_TYPE - REG_DWORD
  - REG_NAME - EnableWFP
  - REG_VALUE - 设置为 1 以启用 WFP（如果跳过 DNE 安装，则必须创建此条目）

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

注意：

- 如果在安装前未创建注册表项，则默认安装 DNE。此外，您可以检查 VPN 日志文件以验证是使用 WFP 还是 DNE。
- 如果跳过 DNE 安装，则必须将 EnableWFP 设置为 1。在这种情况下，如果不重新安装 Citrix Secure Access 客户端，则无法切换到基于 DNE 的插件。

3. 安装新的 VPN 插件。
4. 确认 WFP 驱动程序是否已安装在系统上。打开提升的命令提示符并运行以下命令。示例输出显示 WFP 驱动程序已安装在系统上。

```
PS C:\Users\Administrator> sc qc ctxsgwcallout

[SC] QueryServiceConfig SUCCESS



SERVICE_NAME: ctxsgwcallout

    TYPE               : 1  KERNEL_DRIVER

    START_TYPE         : 1   SYSTEM_START

    ERROR_CONTROL      : 0   IGNORE

    BINARY_PATH_NAME   : \??\C:\Program Files\Citrix\Secure Access
Client\ctxsgwcallout.sys

    LOAD_ORDER_GROUP   :

    TAG                : 0

    DISPLAY_NAME       : Citrix Secure Access Callout Driver

    DEPENDENCIES       :

    SERVICE_START_NAME :
```

如果未安装驱动程序，则显示以下输出：

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

`The specified service does not exist as an installed service.`.

5. 重新启动客户端计算机。

WFP 的优势

如果客户端上进行了独立的 WFP 驱动程序安装，以下是 WFP 的一些优势。

- **基于 FQDN 的反向拆分隧道支持：** WFP 驱动程序支持基于 FQDN 的反向拆分隧道。DNE 驱动程序不支持此功能。有关更多详细信息，请参阅拆分隧道选项。
- **Wireshark 支持：** DNE 不允许在客户端计算机上捕获双向流量，因为它与以太网/Wi-Fi 适配器相关联。新 WFP 驱动程序不存在此问题。任何流量捕获（单向或双向）都经过加密，需要 SSL 密钥才能解密。
- **NMAP 支持：** 新的 WFP 驱动程序支持在 VPN 插件用于隧道传输流量时进行 NMAP 扫描，而 DNE 不允许在 VPN 插件用于隧道传输流量时进行 NMAP 扫描。
- **网络速度：** 在某些情况下，如果在客户端计算机上安装了 DNE，下载和上传速度会受到影响，而 WFP 则不会出现这种情况。
- **改进的 nslookup 性能：** 有时使用 DNE 时，`nslookup` 尝试次数较少时无法响应，而 WFP 则未观察到相同情况。
- **改进的 UDP iperf 性能：** 使用 DNE 时，在使用 iperf 进行 UDP 可扩展性测试期间观察到一些数据包丢失。使用 WFP 时未观察到数据包丢失。

适用于 macOS 的 Citrix Secure Access 客户端

1. 从 App Store 下载适用于 macOS/iOS 的 Citrix Secure Access 应用程序。
2. 下载完成后，单击“**打开**”。

有关如何使用适用于 macOS 的 Citrix Secure Access 的详细信息，请参阅如何从 macOS 设备使用 Citrix Secure Access 应用程序。

根据 ADC 配置强制执行最终用户的本地 LAN 访问

管理员可以限制最终用户在其客户端计算机上禁用本地 LAN 访问选项。现有本地 LAN 访问参数值中添加了一个新选项“FORCED”。当本地 LAN 访问值设置为 FORCED 时，客户端计算机上的最终用户始终启用本地 LAN 访问。最终用户无法使用 Citrix Secure Access 客户端 UI 禁用本地 LAN 设置。

管理员可以通过将本地 LAN 访问参数设置为 ON 来使最终用户能够访问其客户端计算机上的本地 LAN 资源。要阻止最终用户访问其客户端计算机上的本地 LAN 资源，管理员可以将本地 LAN 访问

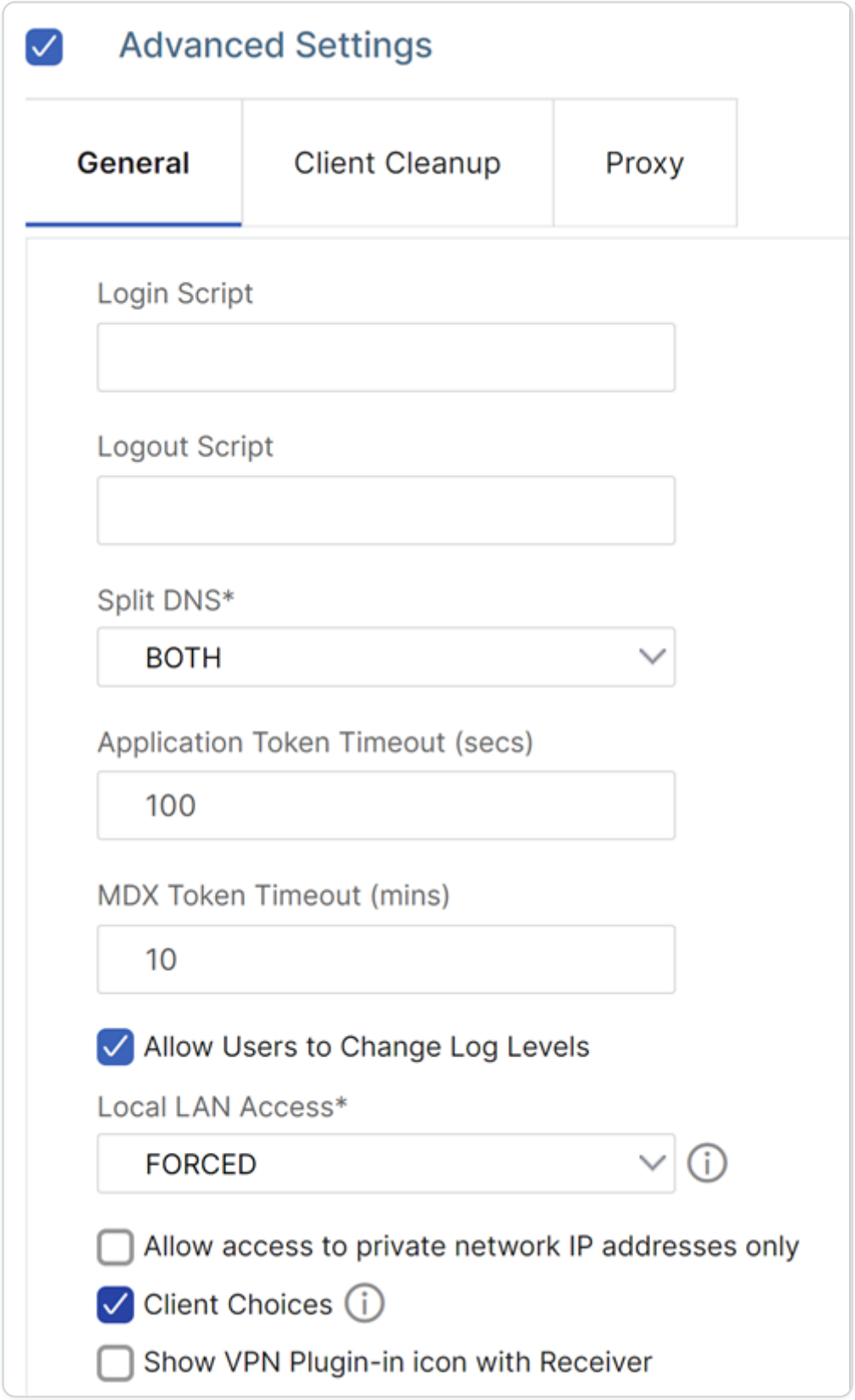
© 1997–2026 Citrix Systems, Inc. All rights reserved.

参数设置为 OFF。有关最终用户配置的详细信息，请参阅适用于 macOS 的本地 LAN 访问 和适用于 iOS 的本地 LAN 访问。

要使用 GUI 启用强制选项：

1. 导航到 **NetScaler Gateway > 全局设置 > 更改全局设置**。
2. 点击“**客户端体验**”选项卡，然后点击“**高级设置**”。
3. 在“**本地 LAN 访问**”中，选择“**强制**”。

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



要使用 CLI 启用强制选项，请运行以下命令：

```
set vpn parameter -localLanAccess FORCED
```

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

注意：

- 适用于 macOS/iOS 的 Citrix Secure Access 客户端及更高版本支持 NetScaler Gateway 的本地 LAN 访问功能。
- 从适用于 Windows 23.10.1.7 的 Citrix Secure Access 客户端开始，如果 NetScaler Gateway 上的“本地 LAN 访问”参数设置为“**强制**”，则在计算机级隧道上支持本地 LAN 访问。

通过 Active Directory 部署 Citrix Secure Access™ 客户端

如果用户没有管理员权限在用户设备上安装 Citrix Secure Access 客户端，您可以从 Active Directory 为用户部署插件。当您使用此方法部署 Citrix Secure Access 客户端时，您可以提取安装程序，然后使用组策略部署该程序。此类部署的一般步骤包括：

- 提取 MSI 包。
- 通过使用组策略分发插件。
- 创建分发点。
- 通过使用组策略对象分配 Citrix Secure Access 客户端包。

  注意： 从 Active Directory 分发 Citrix Secure Access 客户端仅在 Windows 7、Windows 8 和 Windows 10 上受支持。

您可以从配置实用程序或从 Citrix® 网站下载 MSI 包。

要从配置实用程序下载 Citrix Secure Access 客户端 MSI 包

1. 在配置实用程序中，单击“**下载**”。
2. 在 Citrix Secure Access 客户端下，单击“**下载适用于 Windows 的 NetScaler Gateway 插件**”，然后将文件 **nsvpnc_setup.exe** 保存到您的 Windows 服务器。

   注意：

   - 对于 64 位计算机，您必须将文件 Agee_setup.exe 保存到您的 Windows 服务器。
   - 如果未显示“**文件下载**”对话框，请在单击链接“**下载适用于 Windows 的 Citrix Secure Access 客户端**”时按 CTRL 键。
3. 在命令提示符下，导航到保存 **nsvpnc_setup.exe** 的文件夹，然后键入：

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

```
nsvpnc_setup /c
```

这将提取文件 agee.msi。

注意： 对于 64 位计算机，请导航到保存 **Agee_setup.exe** 的文件夹，然后键入：

```
Agee_setup.exe /c
```

这将提取文件 agee64.msi。

4. 将提取的文件保存到 Windows 服务器上的一个文件夹中。

提取文件后，使用 Windows Server 上的组策略分发该文件。

在开始分发之前，请在 Windows Server 2003、Windows Server 2008 或 Windows Server 2012 上安装组策略管理控制台。有关详细信息，请参阅 Windows 在线帮助。

注意： 当您使用组策略发布 Citrix Secure Access 客户端时，Citrix 建议将软件包分配给用户设备。MSI 软件包是按设备安装的。

在分发软件之前，请在发布服务器（例如 Microsoft Internet Security and Acceleration (ISA) Server）的网络共享上创建分发点。

创建分发点

1. 以管理员身份登录到发布服务器。
2. 创建一个文件夹并在网络上共享，为所有需要访问分发包的帐户授予读取权限。
3. 在命令提示符下，导航到保存提取文件的文件夹，然后键入：msiexec -a agee.msi
4. 在“**网络位置**”屏幕上，单击“**更改**”，然后导航到您要创建 Citrix Secure Access 客户端管理安装的共享文件夹。
5. 单击“**确定**”，然后单击“**安装**”。

将提取的软件包放到网络共享上后，将其分配给 Windows 中的组策略对象。

成功将 Citrix Secure Access 客户端配置为托管软件包后，插件将在用户设备下次启动时自动安装。

注意：
当安装包分配给计算机时，用户必须重新启动计算机。

安装开始时，用户会收到一条消息，提示 Citrix Secure Access 客户端正在安装。

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

使用 Active Directory 管理 Citrix Secure Access™ 客户端

Citrix Secure Access 客户端的每个版本都打包为完整产品安装，而不是修补程序。当用户登录且 Citrix Secure Access 客户端检测到新版本的插件时，插件会自动升级。您还可以使用 Active Directory 部署 Citrix Secure Access 客户端进行升级。

为此，请为 Citrix Secure Access 客户端创建分发点。创建组策略对象并将新版本的插件分配给它。然后，在新包和现有包之间创建链接。创建链接后，Citrix Secure Access 客户端将更新。

从用户设备中删除 Citrix Secure Access 客户端

要从用户设备中删除 Citrix Secure Access 客户端，请从组策略对象编辑器中删除分配的包。

当插件从用户设备中删除时，用户会收到一条消息，提示插件正在卸载。

使用 Active Directory 排除 Citrix Secure Access 客户端安装故障

如果用户设备启动时分配的包未能安装，您可能会在应用程序事件日志中看到以下警告：

未能应用软件安装设置的更改。软件安装策略应用程序已延迟到下次登录，因为管理员已为组策略启用了登录优化。错误是：组策略框架必须在同步前台策略刷新中调用扩展。

此错误是由 Windows XP 中的快速登录优化引起的，在该优化中，用户可以在操作系统初始化所有网络组件（包括组策略对象处理）之前登录。某些策略可能需要多次重新启动才能生效。要解决此问题，请在 Active Directory 中禁用快速登录优化。

要排除托管软件的其他安装问题，Citrix® 建议使用组策略启用 Windows Installer 日志记录。

将 Citrix Secure Access 客户端与 Citrix Workspace 应用程序集成

NetScaler Gateway 支持 Citrix Workspace 应用程序。编排系统包含以下组件：

- 适用于 Windows 3.4 或更高版本的 Citrix Workspace 应用程序
- 适用于 Mac 的 Citrix Workspace 应用程序
- 适用于 Android 的 Citrix Workspace 应用程序
- 适用于 iOS 的 Citrix Workspace 应用程序
- StoreFront 2.1 或更高版本
- Endpoint Management 2.8 版本及更新版本或 Citrix Endpoint Management 10
- 托管在 Citrix 网站 上的 Citrix 更新服务

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

有关 NetScaler Gateway 与 Citrix 产品兼容性的更多信息，请参阅 (/zh-cn/netscaler-gateway/current-release/citrix-prod-compatibility.html)。

您可以配置 NetScaler Gateway，以便当用户登录设备时，Citrix Secure Access 客户端会打开一个 Web 浏览器，允许单点登录到 Citrix Workspace 应用程序主页。用户可以从主页下载 Citrix Workspace 应用程序。

当用户使用 Citrix Workspace 应用程序登录时，用户连接可以通过 NetScaler Gateway 以以下方式路由：

- 直接连接到 Endpoint Management
- 直接连接到 StoreFront™
- 如果您未在 Endpoint Management 中配置 MDX 移动应用程序，则连接到 StoreFront，然后连接到 Endpoint Management
- 如果您在 Endpoint Management 中配置了 MDX 移动应用程序，则路由到 Endpoint Management，然后到 StoreFront

注意：

直接路由到 Endpoint Management 的连接仅在 Endpoint Management 2.0、Endpoint Management 2.5、Endpoint Management 2.6、Endpoint Management 2.8 和 Endpoint Management 2.9 中受支持。如果您的网络中部署了 Endpoint Management 1.1，则用户连接必须通过 StoreFront 路由。

用户如何使用 Citrix Workspace 应用程序连接

用户可以通过 Citrix Workspace 应用程序连接到以下应用程序、桌面和数据：

- 在 StoreFront™ 中发布的基于 Windows 的应用程序和虚拟桌面
- 通过 Citrix Endpoint Management™ 访问的 ShareFile 数据

用户可以使用以下任一 Citrix Workspace 应用程序登录：

- 适用于 Web 的 Citrix Workspace 应用程序
- 适用于 Windows 的 Citrix Workspace 应用程序
- 适用于 Mac 的 Citrix Workspace 应用程序
- 适用于 iOS 的 Citrix Workspace 应用程序
- 适用于 Android 的 Citrix Workspace 应用程序

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

用户可以通过 Web 浏览器或用户设备上的 Citrix Workspace 应用程序图标，使用适用于 Web 的 Citrix Workspace 应用程序登录。

当用户使用任何版本的 Citrix Workspace 应用程序登录时，应用程序、ShareFile 数据和桌面将显示在浏览器或 Citrix Workspace 应用程序窗口中。

解耦 Citrix Workspace 应用程序图标

当 Citrix Virtual Apps and Desktops 部署配置为将 Citrix Secure Access 客户端与 Citrix Workspace 应用程序集成时，连接到 VPN 的用户将看不到插件图标。**Citrix Secure Access** 图标通常位于 Windows 系统托盘或 macOS X Finder 的菜单栏中。此图标是插件设置和控件的界面。对于 Windows 用户，当 Citrix Workspace 应用程序和 Citrix Secure Access 客户端集成时，Citrix Workspace 应用程序中的“**关于**”对话框会显示 Citrix Secure Access 客户端的控件。对于 macOS X 用户，集成后没有可用的 Citrix Secure Access 客户端控件。

某些集成部署可能需要在保留底层功能集成的同时公开插件控件。为此，请使用以下 CLI 命令或 NetScaler 配置实用程序任务来切换 VPN 客户端的图标集成。

使用 CLI 设置图标集成

在命令提示符下，键入；

```
set vpn parameter [-iconWithReceiver (ON/OFF)]
```

使用 GUI 设置图标集成

1. 在“配置”选项卡上，导航到 **NetScaler Gateway > 全局设置**。
2. 单击“**更改全局设置**”，然后选择“**客户端体验**”选项卡。
3. 单击“**高级设置**”。
4. 选择“**与 Citrix Workspace 应用程序一起显示 VPN 插件图标**”。

配置 ICA® 连接的 IPv6

NetScaler Gateway 支持 ICA 连接的 IPv6 地址。使用 IPv6 连接到 StoreFront 的方式与 IPv4 连接相同。当用户使用 NetScaler Gateway Web 地址连接时，NetScaler Gateway 会将连接代理到 StoreFront。

您可以为部署在单个 DMZ 或双跳 DMZ 中的 NetScaler Gateway 配置 IPv6。

您可以使用命令行在 NetScaler Gateway 上启用 IPv6。您可以使用以下准则：

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

- 在设备上启用 IPv6。
- 配置子网 IP 地址。
- 设置 DNS 解析顺序。
- 设置 StoreFront™ Web 地址。
- 将安全票证颁发机构 (STA) 绑定到 NetScaler Gateway。

默认情况下，映射的 IP 地址不支持 IPv6 地址。要将用户通信路由到内部网络，您需要创建子网 IP 地址，然后配置 NetScaler Gateway 以使用这些子网 IP 地址。

如果您在网络中部署了多个 IPv6 子网，请在 NetScaler Gateway 上为网络中的每个子网创建多个 IPv6 子网 IP 地址。网络路由使用子网 IP 地址将 IPv6 数据包发送到相应的子网。

使用 CLI 配置 ICA 代理的 IPv6

1. 使用 Secure Shell (SSH) 连接（例如 PuTTY）登录到 NetScaler Gateway。在命令提示符下，键入：

```
enable ns feature IPv6PT. This enables IPv6.



enable ns mode USNIP.



set dns parameter –resolutionOrder AAAAThenAQuery AThenAAAAQuery
OnlyAAAAQuery OnlyAQuery



set vpn parameter -wihome `http://XD_domain/Citrix/StoreWeb`
```

其中 <XD_domain> 是 StoreFront 的域名或 IP 地址。

示例：

```
set vpn parameter -wihome `http://storefront.domain.com/Citrix/StoreWeb`.
```

或者

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

```
set vpn parameter -wihome `http://[1000:2000::3000]/Citrix/StoreWeb`
```

注意：

如果您使用 IPv6 地址配置此参数，则 IP 地址必须包含在方括号中。

在 NetScaler Gateway 上配置 Citrix Workspace 应用程序主页

您可以全局配置 Citrix Workspace 应用程序主页，也可以将其作为会话配置文件的一部分进行配置。如果要为 Web 版 Citrix Workspace 应用程序和不通过 NetScaler Gateway 识别 StoreFront 的早期 Citrix Workspace 应用程序版本进行配置，则需要创建两个单独的会话配置文件。Citrix Workspace 应用程序主页字段需要为每个配置文件设置正确的网址，以便用户可以成功登录。

对于通过 NetScaler Gateway 识别 StoreFront 的 Citrix Workspace 应用程序，您可以让 Web 版 Citrix Workspace 应用程序和 Citrix Workspace 应用程序共享一个配置文件。但是，Citrix 建议您为 Web 版 Citrix Workspace 应用程序配置一个会话配置文件，并为所有其他 Citrix Workspace 应用程序配置一个单独的会话配置文件。

全局配置 Citrix Workspace 应用程序主页

要全局配置 Citrix Workspace 应用程序主页，请执行以下操作：

1. 在配置实用程序中，在“Configuration”（配置）选项卡上的导航窗格中，展开 NetScaler Gateway，然后单击“Global Settings”（全局设置）。
2. 在详细信息窗格的“Settings”（设置）下，单击“Change global settings”（更改全局设置）。
3. 在“Global NetScaler Gateway Settings”（全局 NetScaler Gateway 设置）对话框中，单击“Published Applications”（已发布的应用程序）选项卡。
4. 在“Citrix Workspace app Home Page”（Citrix Workspace 应用程序主页）中，键入 Citrix Workspace 应用程序或 Web 版 Citrix Workspace 应用程序主页的网址，然后单击“OK”（确定）。

在会话配置文件中配置 Citrix Workspace 应用程序主页

要在会话配置文件中配置 Citrix Workspace 应用程序主页，请执行以下操作：

1. 在配置实用程序中，在“Configuration”（配置）选项卡上的导航窗格中，展开 **NetScaler Gateway > Policies**，然后单击 **Session**。
2. 在详细信息窗格的“**Profiles**”（配置文件）选项卡上，单击“**Add**”（添加）。

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

3. 在“**Create NetScaler Gateway Session Profile**”（创建 NetScaler Gateway 会话配置文件）对话框中，在“**Published Application**”（已发布的应用程序）选项卡上，在“**Citrix Receiver Home** Page”（Citrix Receiver 主页）旁边，单击“**Override Global**”（覆盖全局）。
4. 在 Citrix Workspace 应用程序主页中，键入 Citrix Workspace 应用程序或 Web 版 Citrix Workspace 应用程序主页的网址，然后单击“**Create**”（创建）。

将 Citrix Workspace 主题应用于 NetScaler Gateway 登录页面

默认情况下，NetScaler Gateway 使用 RfWebUI 门户主题，该主题与 StoreFront 2311 CR 及更高版本使用的经典（统一 UI）主题匹配。在 2311 CR 版本之前，StoreFront 只有一个 UI 主题，该主题默认与 RfWebUI 视觉主题匹配。 NetScaler Gateway 14.1 build 43.50 版本引入了一个新的门户主题，该主题与 Citrix Workspace UI 非常相似。您可以切换到 Citrix Workspace 主题，或者创建自定义主题以匹配 Citrix Workspace 和 StoreFront 下一代 UI 的外观和风格。

切换到 Citrix Workspace 主题

使用 GUI：

您可以使用 使用 GUI 将门户主题绑定到 VPN 虚拟服务器 中的说明切换到 Citrix Workspace 主题。

使用 CLI：

在命令提示符下，键入：

```
bind vpn vserver <vserver_name> -portaltheme WStheme
```

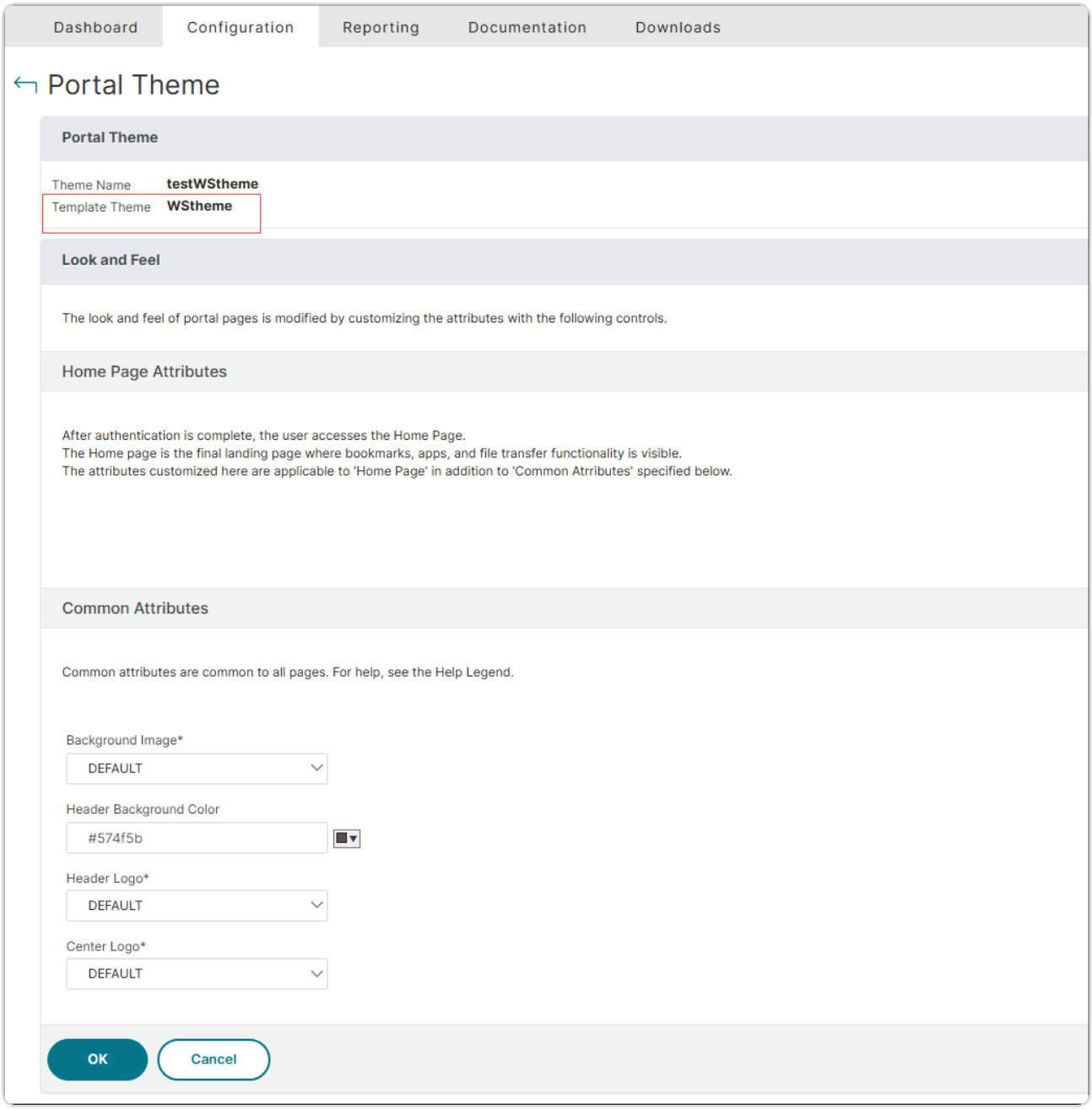
创建自定义 Citrix Workspace 主题

使用 GUI：

请按照以下说明创建自定义主题以匹配 Citrix Workspace 的外观和风格：

1. 导航到 **配置** - > **NetScaler Gateway** - > **门户主题**。
2. 在 **Portal Theme** 页面上，单击左上角的“**Add**”。
3. 输入主题名称，并选择 **WStheme** 作为模板主题。
4. 单击“**OK**”。
5. 通过修改背景图像、标题背景颜色、标题徽标、中心徽标来自定义主题，然后单击“**OK**”。
6. 将自定义主题绑定到 VPN 虚拟服务器。有关详细信息，请参阅使用 GUI 将门户主题绑定到 VPN 虚拟服务器。

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



使用 CLI：

创建自定义 Citrix Workspace 主题：

```
add vpn portaltheme <custom_WStheme_name> -basetheme WStheme
```

将自定义主题绑定到 VPN 虚拟服务器：

```
bind vpn vserver <vserver_name> -portaltheme <custom_WStheme_name>
```

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

为 NetScaler Gateway 登录页面创建自定义主题

您可以使用 GUI 为 NetScaler Gateway 登录页面创建自定义主题。您也可以保留默认主题或使用 Citrix Workspace 应用程序主题。当您选择将自定义主题应用于登录页面时，您需要使用 NetScaler Gateway 命令行来创建和部署该主题。然后，您可以使用 GUI 设置自定义主题页面。

您可以通过使用 NetScaler Gateway 全局设置来配置自定义主题页面。

您可以将此功能与以下版本的 NetScaler Gateway 结合使用：

- NetScaler 网关 10.1
- Access Gateway 10，版本 73.5002.e（您必须在版本 71.6104.e 之后安装此版本，才能将此功能与 Endpoint Management 2.5、2.6 或 2.8 版结合使用）
- Access 网关 10，版本 71.6104.e

使用 CLI 创建和部署自定义主题

要使用命令行创建和部署自定义主题：

1. 登录到 NetScaler Gateway 命令行。
2. 在命令提示符下，键入 shell。
3. 在命令提示符下，键入 `mkdir /var/ns_gui_custom; cd /netscaler; tar -cvzf /var/ns_gui_custom/customtheme.tar.gz ns_gui/*` 。
4. 使用配置实用程序切换到自定义主题，然后在 /var/ns_gui_custom/ns_gui/vpn 下进行自定义更改。您可以：
   - 编辑 css/ctx.authentication.css 文件。
   - 将自定义徽标复制到 /var/ns_gui_custom/ns_gui/vpn/media 文件夹。**注意：** 您可以使用 WinSCP 传输文件。
5. 如果您有多个 NetScaler Gateway 设备，请对所有设备重复步骤 3 和 4。

NetScaler Gateway Windows VPN 客户端注册表项

VPN 客户端注册表项位于 **HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Client** 下。下表列出了 NetScaler Gateway Windows VPN 客户端注册表项、值以及每个值的简要说明。

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

注册表项	注册表类型	注册表控制	值和说明	默认值
addedRoutes/ modifiedRoutes	REG_SZ	由 Citrix Secure Access 客户端管理。	为内部插件通信而创建。用户不得修改此项。	此注册表项没有默认值。
AlwaysOnService	REG_DWORD	管理员可以通过组策略对象 (GPO) 使用组策略管理控制台 (GPMC) 或 System Center Configuration Manager (SCCM) 推送来部署此注册表项。	• 1 => 建立机器级隧道，但不建立用户级隧道。 • 2 => 在任何给定时间建立机器级隧道或用户级隧道。 • 3 => 建立机器级隧道和用户级隧道，以便在 Citrix Secure Private Access 中为已加入域的计算	此注册表没有默认值。

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

注册表项	注册表类型	注册表控制	值和说明	默认值
			机启用多会话操作系统。 **注意：**多会话操作系统功能支持处于预览阶段。	
AlwaysOnURL	REG_SZ	您可以通过以下两种方式之一控制此注册表。 • 管理员可以通过 GPO 使用 GPMC 或 SCCM 推送部署此注册表（或） • 使用 CLI。有关详细信息，请参阅注释*。	用户希望连接的 NetScaler Gateway 虚拟服务器的 URL。示例：`https://xyz.companyDomain.com`	此注册表没有默认值，因为它配置用于自定义解决方案。

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

注册表项	注册表类型	注册表控制	值和说明	默认值
AlwaysOn	REG_DWORD	使用 CLI。有关详细信息，请参阅注释*。	• 1 => 允许在 VPN 故障时进行网络访问。 • 2=> 在 VPN 故障时阻止网络访问。	此注册表没有默认值。
AlwaysOnAllowlist	REG_SZ	管理员可以使用 GPMC 或 SCCM 推送通过 GPO 部署此注册表。	由分号分隔的 FQDN、IP 地址范围或 IP 地址列表，在 Always On 严格模式下由驱动程序允许。示例：`example.citrix.com;192.0.2.0;192.0.2.100-192.0.2.255`	空或 NULL
ClientControl	REG_DWORD	使用 CLI。有关详细信息，请参阅注释*。	• 1 => 允许用户注销或连接到其他网关。	1

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

注册表项	注册表类型	注册表控制	值和说明	默认值	
			• 0 => 阻止用户注销或连接到其他网关。		
ConfigSize	REG_DWORD	管理员可以使用 GPMC 或 SCCM 推送通过 GPO 部署此注册表。此注册表仅用于 Citrix Secure Private Access。	Windows 客户端默认支持 64 KB 的配置文件大小。使用此注册表可增加配置文件大小。 如果配置文件大小超过 64 KB 的默认值，则对于每个额外的 64 KB，将 `ConfigSize` 注册表值设置为 5 倍 64 KB（以字节为单位）。 例如，如果您要额外增加 64 KB，则必须将注册表值设置为 64 x 1024 x 5 = 327680。同	64 KB	

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

注册表项	注册表类型	注册表控制	值和说明	默认值
			样，如果您要增加 128 KB，则必须将注册表值设置为 64 x 1024 x (5+5) = 655360。	
已连接	REG_DWORD	由 Citrix Secure Access™ 客户端管理。	连接成功时，此键设置为 1，否则设置为 0。此键供内部使用。用户不得修改此键。	此注册表没有默认值。
DisableCredProv	REG_DWORD	管理员可以使用 GPMC 或 SCCM 推送通过 GPO 部署此注册表。	启用 **AlwaysOn VPN before Windows Logon** 后，Windows VPN 插件会添加凭据提供程序以在登录屏幕上显示隧道状态。如果不需要此附加功能，请创建此注册表并将其设置为 1。	0
DisableIconHide	REG_DWORD	使用 CLI：`set vpn parameter`	• 1 => Citrix Worksp	0

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

注册表项	注册表类型	注册表控制	值和说明	默认值
		`iconWithReceiver ON`	ace 应用程序和 NetScaler Gateway 插件显示在任务栏上。	
			0 => NetScaler Gateway 插件图标已与适用于 Windows 的 Citrix Workspace 应用程序集成。当完整的 VPN 会话运行时，NetScaler Gateway 插件在任务栏上不可见。	
DisableDNSRoutes	REG_DWORD	管理员可以使用 GPMC 或 SCCM 推送通过 GPO 部署此注册表。	• 0 => 默认值。如果 DNS 服务器与物理接口的默认网关不同，	0

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

注册表项	注册表类型	注册表控制	值和说明	默认值
			VPN 插件会为 DNS 服务器添加路由。但是，根据 Windows 客户端计算机的网络拓扑，DNS 服务器路由可能并非总是必需的。	
			1 => VPN 插件不为 DNS 服务器添加显式路由。	
DisallowCaptivePortals	REG_DWORD	管理员可以使用 GPMC 或 SCCM 推送通过 GPO 部署此注册表。	• 1 => VPN 插件在启动 VPN 会话之前，通过尝试连接到 Microso	0

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

注册表项	注册表类型	注册表控制	值和说明	默认值	
			ft Connect test 页面来检查强制门户。 • 0 => VPN 插件跳过强制门户检查。		
DisableIntuneDeviceEnrollment	REG_DWORD	管理员可以使用 GPMC 或 SCCM 推送通过 GPO 部署此注册表。	如果设置为 1，则不执行 Intune 设备注册。	0	
DisableWebViewForAutoLogon	REG_DWORD	管理员可以使用 GPMC 或 SCCM 推送或通过功能标志通过 GPO 部署此注册表。	• 1 => 在“始终开启”模式下运行时，隐藏设备状态或身份验证屏幕。 • 0 => 在“始终开启”模式下运行时，	0	

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

注册表项	注册表类型	注册表控制	值和说明	默认值	
			显示设备状态或身份验证屏幕。		
EnableAdminConfigFetch	REG_DWORD	管理员可以使用 GPMC 或 SCCM 推送通过 GPO 部署此注册表。	在客户端启用客户端应用程序管理设置。 • 0 => 禁用客户端应用程序管理功能。 • 1 => 启用客户端应用程序管理功能。	0	
EnableAntiDllProtection	REG_DWORD	管理员可以使用 GPMC 或 SCCM 推送通过 GPO 部署此注册表。	• 1 => 启用反 DLL 注入安全增强功能。 • 0 => 禁用反 DLL注入安全	0	

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

注册表项	注册表类型	注册表控制	值和说明	默认值	
			增强功能。		
EnableAutoUpdate	REG_DWORD	管理员可以通过GPMC或SCCM推送，通过GPO部署此注册表。	用于从客户端控制插件更新功能。 • 0 => 禁用自动更新功能。 • 1 => 启用自动更新功能。 **注意：** 此注册表项位于 **HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SecureAccessClient\AutoUpdate** 下。	0	

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

注册表项	注册表类型	注册表控制	值和说明	默认值	
EnableContextualAccess	REG_DWORD	管理员可以通过 GPO 使用 GPMC 或 SCCM 推送或通过功能标志部署此注册表。	• 0 => 禁用 Secure Private Access 中的上下文访问 • 1 => 启用 Secure Private Access 中的上下文访问	0	
EnableEdgeWebview	REG_DWORD	管理员可以通过 GPO 使用 GPMC 或 SCCM 推送部署此注册表。	• 0 => 禁用 微软 Edge WebView。 • 1 => 启用 微软 Edge WebView。	1	
EnableKerberosAuth	REG_DWORD	管理员可以通过 GPO 使用 GPMC 或 SCCM 推送部署此注册表。	• 0 => 默认值。 • 1 => VPN 客户端使	0	

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

注册表项	注册表类型	注册表控制	值和说明	默认值	
			用 Kerberos 身份验证方法进行自动登录。		
EnableMonitorDuringSleep	REG_DWORD	管理员可以通过 GPO 使用 GPMC 或 SCCM 推送部署此注册表。	• 0 => 当最终用户计算机中的电源事件被修改时，禁用对睡眠和唤醒事件的监控。 • 1 => 即使最终用户计算机中的电源事件被修改，也启用对睡眠和唤醒事件的监控。	0	

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

注册表项	注册表类型	注册表控制	值和说明	默认值	
EnableMultiSessionFlow	REG_DWORD	管理员可以使用 GPMC 或 SCCM 推送通过 GPO 部署此注册表。	• 0 => 在 Citrix Secure Private Access 中禁用对多会话操作系统的访问 • 1 => 在 Citrix Secure Private Access 中启用对多会话操作系统的访问	此注册表没有默认值，因为它配置用于自定义解决方案。	
EnableTCPDNS	REG_DWORD	管理员可以使用 GPMC 或 SCCM 推送通过 GPO 部署此注册表。	• 0 => 禁用对基于 TCP 的 DNS 请求的拆分 DNS 支持。 • 1 => 启用对基于 TCP 的 DNS	1	

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

注册表项	注册表类型	注册表控制	值和说明	默认值	
			请求的拆分 DNS 支持。		
EnableVA	REG_DWORD	由 Citrix Secure Access 客户端管理。	此键在内部使用，如果存在 IIP 时必须启用 Citrix 虚拟适配器。用户不得修改此键。	1	
EnableWebModuleUI	REG_DWORD	管理员可以通过 GPMC 或 SCCM 推送或通过功能标志，使用 GPO 部署此注册表。	• 1 => 启用带有 **通知中心** 和集成 WebView 的增强型 UI。 • 0 => 禁用增强型 UI。	0	
EnableWFP	REG_DWORD	管理员可以通过 GPMC 或 SCCM 推送或通过功能标志，使用 GPO 部署此注册表。	• 1 => VPN 插件使用 WFP。从适用于 Windows 的	1	

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

注册表项	注册表类型	注册表控制	值和说明	默认值	
			Citrix Secure Access 客户端 25.1.1.27 版本开始，WFP 默认启用。 • 0 => VPN 插件使用 DNE。		
ExcludeDomainsFromRemoteDns	REG_SZ	管理员可以使用 GPMC 或 SCCM 推送通过 GPO 部署此注册表。	排除 Citrix Secure Access 客户端通过远程 DNS 服务器执行的 DNS 解析。 如果 `example.com` 是一个内部网域，并且您想排除 `sshhost.example.com`、`rdphost.example.com` 或 `*.ftphost.example.`	此注册表没有默认值，因为它配置用于自定义解决方案。	

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

注册表项	注册表类型	注册表控制	值和说明	默认值	
			`com` 等特定应用程序，请使用此注册表。`*.ftphost.example.com` 是一个通配符模式，匹配 `ftphost.example.com` 下的任何子域。 请务必根据您的要求调整域名和模式。完成更改后，请重新启动 Citrix Secure Access 或系统以使设置生效。		
ExcludeDomainsFromTunnel (预览)	REG_SZ	管理员可以通过使用 GPMC 或 SCCM 推送的 GPO 部署此注册表。	排除特定域的流量通过 Citrix Secure Access 客户端进行隧道传输。如果 `example.com` 是一个内部网域，并且您想排除	此注册表没有默认值，因为它配置用于自定义解决方案。	

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

注册表项	注册表类型	注册表控制	值和说明	默认值
			`sshhost.example.com`、`rdphost.example.com` 或 `*.ftphost.example.com` 等特定应用程序，请使用此注册表。请务必将注册表值设置为逗号分隔的域名或模式列表。	
HideLoginLogoutScripts Prompt	REG_DWORD	管理员可以通过使用 GPMC 或 SCCM 推送的 GPO 或通过功能标志部署此注册表。	• 1 => 隐藏登录/注销脚本执行。 • 0 => 登录/注销脚本执行在 Citrix 安全访问隧道建立或终止期间可见。	0
HttpTimeout	REG_DWORD	管理员可以使用 GPMC 或 SCCM 推送通过 GPO	HTTP 超时以秒为单位配置。如果未配置超	100 秒

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

注册表项	注册表类型	注册表控制	值和说明	默认值
		部署此注册表。	时，则使用默认超时。默认超时值为 100 秒，基于 Windows 标准。	
InstallDir	REG_SZ	由 Citrix Secure Access 客户端管理。	Citrix Secure Access 客户端的安装位置。	"C:\程序文件\Citrix\安全访问客户端\"
IsAutoUpdateControlledViaAdmin	REG_DWORD	管理员可以使用 GPMC 或 SCCM 推送通过 GPO 部署此注册表。	用于选择哪些计算机必须自动获取适用于 Windows 的 Citrix Secure Access 客户端的 Beta 版本或生产版本的更新。 • 0 => 最终用户可以选择更新到 Beta 版或最新生产版本。	默认禁用。
			最终用户无法控制选择	

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

注册表项	注册表类型	注册表控制	值和说明	默认值
			测试版和生产版。 **注意：** 如果管理员使用 `EnableAutoUpdate` 注册表禁用自动更新功能，则 `IsAutoUpdateControlledViaAdmin` 注册表无效。 • `IsAutoUpdateControlledViaAdmin` 注册表位于 **HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SecureAccessClient\AutoUp**	

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

注册表项	注册表类型	注册表控制	值和说明	默认值	
			date 下。		
locationDetection	REG_DWORD	使用 CLI。有关详细信息，请参阅注释*。	• 1 => 启用位置检测。 • 0 => 禁用位置检测。	此注册表没有默认值，并且仅在启用“始终开启”模式时才进行配置。	
NoDHCPRoute	REG_DWORD	1. 在 NetScaler 设备上，创建一个名为 `plugin Customization.json` 的新文件，其值为 `\{ "NoDHCPRoute" : true }`。 2. 将 `plugin Customization.json`	如果设置为 1，则不添加 DHCP 服务器路由。	此注册表没有默认值，因为它根据网络拓扑进行自定义。	

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

注册表项	注册表类型	注册表控制	值和说明	默认值	
		文件放置在 **/netscaler/ns_gui/vpn** 和 **/var/netscaler/gui/vpn** 文件夹中。			
overrideIPV6DnsDrop	REG_DWORD	管理员可以使用 GPMC 或 SCCM 推送通过 GPO 部署此注册表。	• 1 => 允许 IPv6 DNS 流量通过 VPN。 • 0 => 限制 IPv6 DNS 流量。	此注册表没有默认值，因为它根据网络拓扑进行自定义。	
ProductVersion	REG_SZ	由 Citrix Secure Access 客户端管理。	当前安装的 Citrix Secure Access 客户端版本。	产品版本信息	
ProductCode	REG_SZ	由 Citrix Secure Access 客户端管理。	此密钥供内部使用。用户不得修改此密钥。	{B04137FF-B5C9-4058-ACEB-04118790118D}	

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

注册表项	注册表类型	注册表控制	值和说明	默认值
secureDNSUpdate	REG_DWORD	管理员可以通过 GPO 使用 GPMC 或 SCCM 推送部署此注册表。	• 0 => VPN 插件只尝试不安全的 DNS 更新。 • 1 => VPN 插件首先尝试不安全的 DNS 更新。如果不安全的 DNS 更新失败，VPN 插件会尝试安全的 DNS 更新。这是从 21.3.1.2 Windows 插件版本开始的默认行为。	1

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

注册表项	注册表类型	注册表控制	值和说明	默认值
			• 2 => VPN 插件只尝试安全的 DNS 更新。	
SecureChannelResetTimeoutSeconds	REG_DWORD	管理员可以使用 GPMC 或 SCCM 推送通过 GPO 部署此注册表。	默认情况下，此注册表值未设置或添加。当 `SecureChannelResetTimeoutSeconds` 的值为 `0xFFFFFFFF` 或注册表中不存在时，VPN 插件会等待 `SecureChannelReset()` API 调用完成，然后才开始隧道传输数据流量。这是默认行为。管理员必须在客户端上设置此注册表，以便 VPN 插件在等待 API 调用完成指定时间后开始隧道传输数据流量。	此注册表没有默认值，因为它配置用于自定义解决方案。

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

注册表项	注册表类型	注册表控制	值和说明	默认值
SecureAccessLogInScript	REG_SZ	管理员可以使用 GPMC 或 SCCM 推送通过 GPO 部署此注册表。	Citrix Secure Access 服务在连接到 Citrix Secure Private Access 服务时，使用此注册表项访问登录脚本配置。有关详细信息，请参阅 登录和注销脚本配置注册表。	此注册表没有默认值，因为它配置用于自定义解决方案。
SecureAccessLogOutScript	REG_SZ	管理员可以使用 GPMC 或 SCCM 推送通过 GPO 部署此注册表。	Citrix Secure Access 服务在连接到 Citrix Secure Private Access 服务时，使用此注册表项访问注销脚本配置。有关详细信息，请参阅 登录和注销脚本配置注册表。	此注册表没有默认值，因为它配置用于自定义解决方案。
suffixList	REG_SZ	使用 CLI: `add dns suffix`	内网域名的分号分隔列表。在启用	从服务器上配置的 DNS 后缀中检索值。

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

注册表项	注册表类型	注册表控制	值和说明	默认值
			位置检测时使用。	
SicBeginPort	REG_DWORD	1. 在 NetScaler 设备上，创建一个名为 `plugin Customization.json` 的新文件，其值为 `\{"SicBeginPort" : 51000}` 。 2. 将 `plugin Customization.json` 文件放置在 **/netscaler/ns_gui/vpn** 和 **/var/netscaler/gui/**	避免在使用端口在 Citrix Secure Access 客户端和客户端计算机上的第三方应用程序之间创建套接字时可能出现的冲突。允许的范围是 49152–64535（十六进制格式为 C000 到 FC17）。VPN 客户端仅在 `EnableWFP` 也设置为 `1` 时，才使用从 `SicBeginPort` 开始的最多 1000 个端口。	此注册表没有默认值，因为它配置用于自定义解决方案。

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

注册表项	注册表类型	注册表控制	值和说明	默认值	
		vpn 文件夹中。			
userCertCAList	REG_SZ	管理员可以使用 GPMC 或 SCCM 推送通过 GPO 部署此注册表。	在Always On服务中使用，客户可以在其中指定选择客户端证书的CA列表。	此注册表没有默认值，因为它配置用于自定义解决方案。	
UserTunnelFallbackEnabled	REG_DWORD	管理员可以通过GPMC或SCCM推送，通过GPO部署此注册表。	当机器隧道无法建立时，Always On VPN的备用机制。如果UserTunnelFallbackEnabled注册表项已启用，即使机器隧道无法建立，Citrix Secure Access客户端也会自动尝试形成用户隧道。如果设置为1，则启用UserTunnelFallbackEnabled参数。	此注册表没有默认值，因为它配置用于自定义解决方案。	

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

注册表项	注册表类型	注册表控制	值和说明	默认值
smartCardProviders	REG_SZ	管理员可以通过GPMC或SCCM推送，通过GPO部署此注册表。	分号分隔的智能卡提供商列表。	空或 NULL

注意：

*使用以下命令通过 CLI 应用 `AlwaysOnURL`、`AlwaysOn`、`ClientControl` 和 `locationDetection` 注册表项：

`add alwaysONProfile <alwaysONProfileName>-clientControl ( ALLOW | DENY )-locationBasedVPN ( Remote | Everywhere )-networkAccessOnVPNFailure ( onlyToGateway | fullAccess )`

重要：

- 您可以根据部署应用注册表项。例如，`AlwaysOnService` 注册表项仅适用于 Always on 服务，而 `ClientControl` 注册表项不适用于 Always on 服务。有关更多详细信息，请参阅各个部署文档。
- `secureDNSUpdate` 仅适用于已加入域的客户端设备。
- 对于适用于 Windows 23.1.1.8 及更高版本的 Citrix Secure Access 客户端，注册表项名称为 `overrideIPV6DnsDrop`。对于适用于 Windows 22.10.1.9 及更早版本的 Citrix Secure Access 客户端，注册表项名称为 `overrideIP6DnsDrop`。
- 从适用于 Windows 24.8.1.15 的 Citrix Secure Access 客户端开始，注册表项 `DisableGA`、`ForcedLogging` 和 `OverrideSpoofIPRange` 已弃用。
- 从适用于 Windows 24.8.1.19 的 Citrix Secure Access 客户端开始，管理员可以使用 `EnableMultiSessionFlow` 注册表在 Citrix Secure Private Access 中启用云托管多会话 VDI，以便根据其位置、设备和其他因素对资源进行上下文访问。对于已加入域的计算机，请同时使用 `EnableMultiSessionFlow` 和 `AlwaysOnService` 注册表。
- 从适用于 Windows 24.11.1.17 的 Citrix Secure Access 客户端开始，管理员可以使用注册表 `EnableAutoUpdate` 和 `IsAutoUpdateControlledViaAdmin` 启用自动更新功能，并选择哪些计算机必须自动获取早期访问版本或生产版本的更新。由于自动更新功能是在适用于

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

Windows 24.11.1.17 的 Citrix Secure Access 客户端中引入的，因此管理员可以在后续版本中使用此功能。

- 从适用于 Windows 24.11.1.17 的 Citrix Secure Access 客户端开始，管理员可以使用 `EnableContextualAccess` 注册表在 Secure Private Access 中启用上下文访问功能。上下文访问功能使管理员能够根据用户上下文（例如网络位置、地理位置和设备状态）动态实施 ZTNA 策略。
- 对于适用于 Windows 24.8.1.19 之前的 Citrix Secure Access 客户端版本，管理员可以使用 `EnableEdgeWebview` 注册表启用 Microsoft Edge WebView。
- 从适用于 Windows 25.11.1.12 的 Citrix Secure Access 客户端版本开始，管理员可以使用 `EnableWebModuleUI` 注册表启用增强型 UI，其中包含**通知中心**、集成 WebView 和强制门户支持。
- 从 Citrix Secure Access 客户端版本 25.11.1.12 开始，管理员可以使用 `EnableAntiDllProtection` 注册表启用反 DLL 注入安全增强功能。启用后，它可保护 Citrix Secure Access 客户端免受某些未经授权的动态链接库 (DLL) 或不受信任的模块的侵害。如果注入了此类不受信任的模块，Citrix Secure Access 客户端会检测到这些干预并阻止模块加载。此外，如果在 Citrix Secure Access 启动期间检测到任何不受信任或恶意 DLL，它会生成通知并终止应用程序启动。
- 从 Citrix Secure Access 客户端版本 25.11.1.12 开始，管理员可以配置 `HideLoginLogoutScriptsPrompt` 注册表，以确保在 Citrix Secure Access 隧道建立或终止期间执行登录或注销脚本时，命令提示符不会闪烁。
- 从 Citrix Secure Access 客户端版本 25.11.1.12 开始，管理员可以配置 `DisableWebViewForAutoLogon` 注册表，以确保 Citrix Secure Access 客户端在“始终开启”模式下运行时隐藏设备状态或身份验证屏幕。此功能仅在新 UI 中受支持，新 UI 是使用 `EnableWebModuleUI` 注册表启用的。
- 从适用于 Windows 的 Citrix Secure Access 客户端版本 25.11.1.12 开始，管理员必须配置 `EnableAdminConfigFetch` 注册表以在客户端启用客户端应用程序管理设置，或联系 Citrix 支持。有关详细信息，请参阅 Citrix Secure Access - 客户端应用程序管理。
- `UserTunnelFallbackEnabled` 注册表从适用于 Windows 的 Citrix Secure Access 客户端版本 26.1.1.9 开始提供。

在身份验证 Cookie 上强制执行 HttpOnly 标志

从 NetScaler Gateway 13.1-37.x 及更高版本开始，HttpOnly 标志可用于 VPN 场景的身份验证 Cookie，即 NSC_AAAC 和 NSC_TMAS Cookie。NSC_TMAS 身份验证 Cookie 在 nFactor 身份验

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

证期间使用，NSC_AAAC Cookie 用于已验证的会话。Cookie 上的 HttpOnly 标志限制了使用 JavaScript 文档 Cookie 选项访问 Cookie。这有助于防止因跨站点脚本攻击而导致的 Cookie 窃取。

从适用于 Windows 的 Citrix Secure Access 24.8.1.x 和 NetScaler Gateway 14.1-34.x 开始，Citrix Secure Access 客户端的主页在 NetScaler Gateway 上启用 HttpOnly Cookie 后可成功启动。在以前的版本中，当启用 HttpOnly 功能时，Citrix Secure Access 客户端 UI 上的**主页**链接无法正常工作。

支持的场景

nFactor 身份验证支持 HTTPOnly 标志。

当 NetScaler AAA 参数的 HttpOnlyCookie 旋钮与流量管理 (TM) 会话的 HttpOnlyCookie 旋钮一起使用时的行为：

- 当为身份验证、授权和审计启用 httpOnlyCookie 旋钮时，它会在 nFactor 身份验证期间覆盖流量管理会话的 HttpOnlyCookie 旋钮。此外，无论会话类型如何，NSC_TMAS 和 NSC_AAAC 都被标记为 HttpOnly。这适用于 VPN 会话、TM 会话或 nFactor 身份验证。
- 如果 HttpOnlyCookie 旋钮被禁用，则不会为 VPN 会话设置 HttpOnly 标志。对于身份验证、授权和审计场景，HttpOnly 标志根据 TM 会话旋钮值设置。

使用 CLI 配置 HttpOnly 功能

- 启用 HttpOnly 标志。

  ```
  set aaa parameter -httpOnlyCookie ENABLED
  ```

  注意：

  - 默认情况下，在以下 NetScaler Gateway 版本中启用 HttpOnly 标志：
    - 14.1-43.56 及更高版本
    - 13.1-59.19 及更高版本
  - 要禁用 HttpOnly 标志，请运行以下命令：

    ```
    set aaa parameter -httpOnlyCookie DISABLED
    ```

- 检查 HttpOnly 功能的状态。

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

```
show aaa parameter
```

限制

- HttpOnly 标志未在任何经典身份验证中设置。

为 VPN 用户自定义用户门户

NetScaler Gateway 允许管理员自定义 VPN 用户访问的用户门户的外观。您可以从一组预设主题中进行选择，或使用其中一个作为模板来创建完全自定义或品牌化的门户。

使用配置实用程序，您可以通过添加新徽标、背景图像、自定义输入框标签以及基于 CSS 的门户设计的各种其他属性来定制主题。内置门户主题包含五种语言的内容：英语、法语、西班牙语、德语和日语。呈现给用户的语言会根据其 Web 浏览器的区域设置自动确定。

您可以创建自定义 EULA，在 VPN 用户登录之前向其显示。EULA 功能支持特定于区域设置的 EULA 版本，这些版本会根据用户的 Web 浏览器报告的区域设置向用户显示。

门户主题和 EULA 配置都可以在 VPN 虚拟服务器和 VPN 全局级别独立绑定。

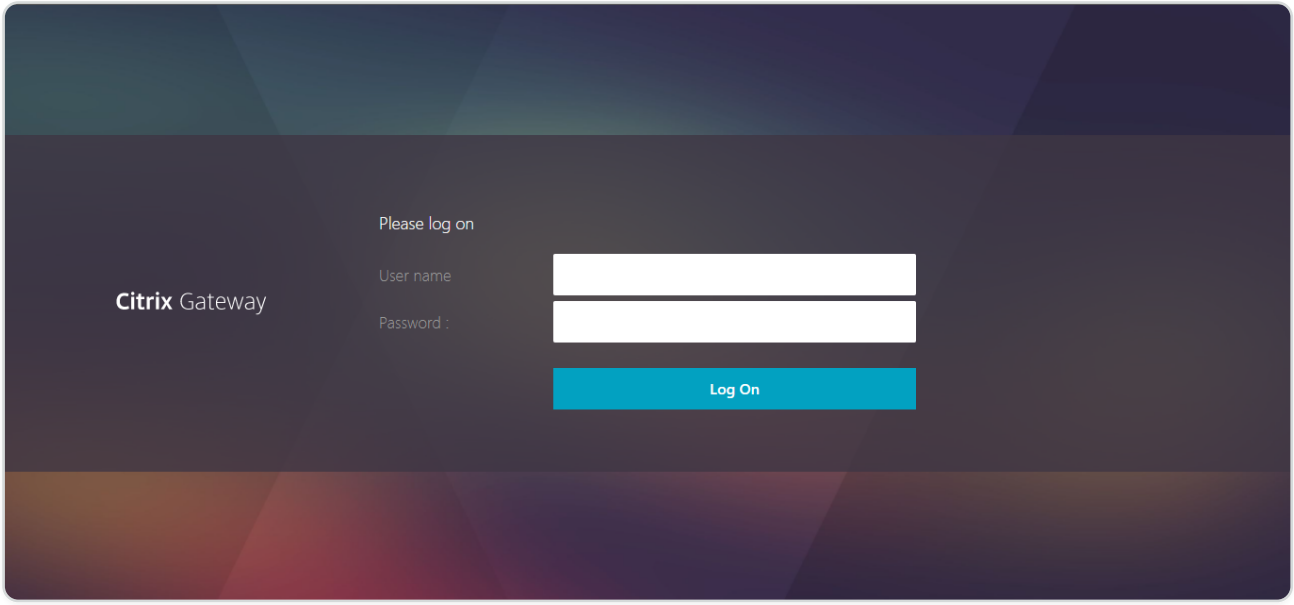
重要提示：

NetScalerÂ® 不支持需要代码修改的自定义，并且不提供超出恢复到默认主题范围的问题解决方案支持。

应用门户主题

从版本 13.0 build 67.43 开始，VPN 门户默认配置为使用 RfWebUI 主题。以前，`Caxton theme` 是默认主题。您还可以应用 Green bubble 和 X1 主题。

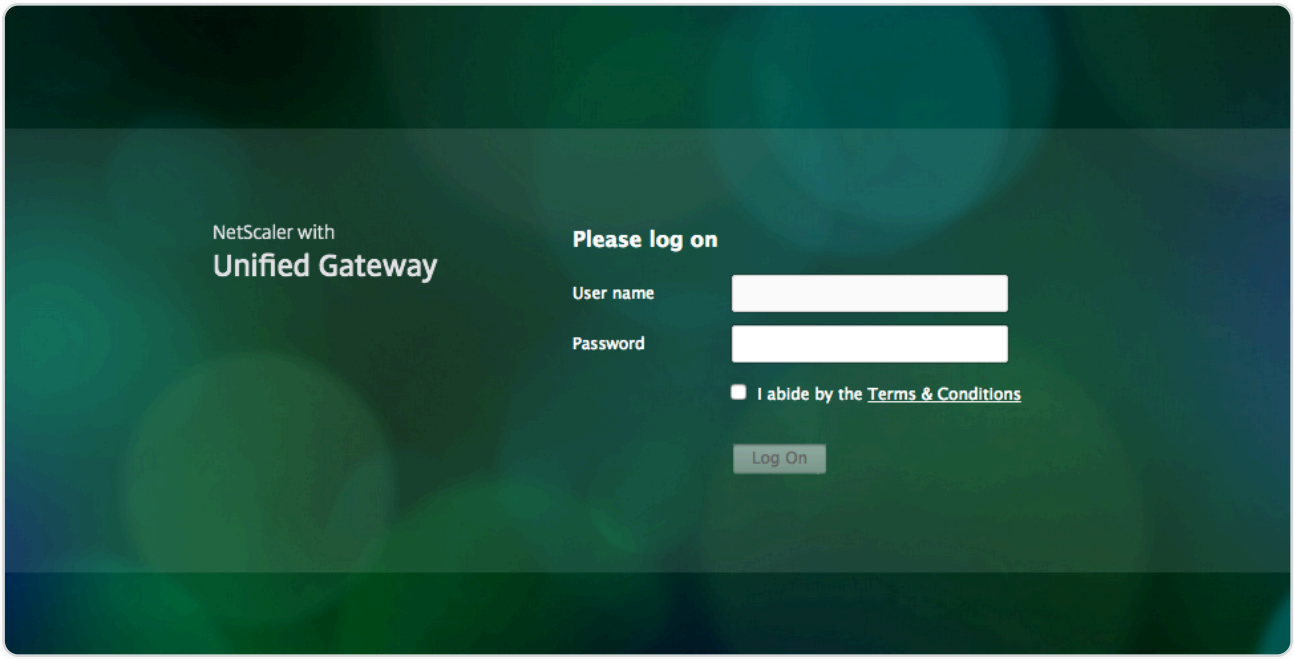
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Caxton 主题

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

Green bubble 主题



X1 主题

X1 主题(/en-us/netscaler-gateway/media/x1-theme.png)

您可以将任何提供的主题直接应用于 VPN 虚拟服务器，或作为全局 VPN 绑定。

将门户主题绑定到 VPN 虚拟服务器

您可以在现有虚拟服务器上或创建新虚拟服务器时绑定门户主题。

使用 CLI 将门户主题绑定到 VPN 虚拟服务器

在命令提示符下，键入：

```
bind vpn vserver <name> - portaltheme <name>
```

使用 GUI 将门户主题绑定到 VPN 虚拟服务器

1. 在“**配置**”选项卡上，导航到“**NetScaler Gateway**”，然后单击“**虚拟服务器**”。
2. 选择一个虚拟服务器，然后单击“**编辑**”。
3. 如果尚未将门户主题绑定到虚拟服务器，请在详细信息窗格的“**高级设置**”下单击“**门户主题**”。否则，“**门户主题**”Â 选项已在详细信息窗格中展开。
4. 在详细信息窗格中，在“**门户主题**”下，单击“**无门户主题**”Â 以展开“门户主题”绑定窗口。
5. `Click` **单击以选择。**

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

6. 在“**门户主题**”窗口中，单击一个主题名称，然后单击“**选择**”。
7. 单击“**绑定**”。
8. 单击“**完成**”。

如果您正在创建 VPN 虚拟服务器，则可以在 **VPN 虚拟服务器编辑** 窗格中，从步骤 3 开始，按照上一个过程中的步骤绑定门户主题。

将门户主题绑定到 VPN 全局

使用 CLI 将门户主题绑定到 VPN 全局

在命令提示符下，键入；

```
bind vpn global portaltheme <name>
```

使用 GUI 将门户主题绑定到 VPN 全局

1. 在 **Configuration**（配置）选项卡上，导航到 **NetScaler Gateway**。
2. 在主详细信息窗格中，单击 **NetScaler Gateway Policy Manager**。
3. 单击“**+**”图标。
4. 在 **Bind Point**（绑定点）列表中，选择 **Resources**（资源）。
5. 在 **Connection Type**（连接类型）列表中，选择 **Portal Theme**（门户主题）。
6. 单击 **Continue**（继续）。
7. 在 **Bind Point**（绑定点）屏幕中，单击 **Add Binding**（添加绑定）。
8. 单击 **Click to select**（单击以选择）。
9. 在 **Portal Themes**（门户主题）窗口中，单击主题名称，然后单击 **Select**（选择）。
10. 单击 **Bind**（绑定）。
11. 点击 **关闭**。
12. 点击 **完成**。

注意：

进行更改后，请在命令行上使用“save ns config”命令，或单击配置实用程序中的保存图标，以确保您的更改已保存到 NetScaler 配置文件中。

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

创建门户主题

要创建自定义门户设计，请使用提供的门户主题之一作为模板。系统会使用您指定的名称复制所选的模板主题。

使用库存门户主题作为自定义门户主题的模板

要创建门户主题，您可以使用配置实用程序或命令行来创建主题实体。但是，详细的自定义控件仅在配置实用程序中可用。

使用 CLI 创建门户主题

在命令提示符下，键入；

```
add portaltheme <name> basetheme <name>
```

使用 GUI 创建门户主题

1. 在“**配置**”选项卡上，导航到“**NetScaler Gateway**”，然后单击“**门户主题**”。
2. 在主详细信息窗格中，单击“**添加**”。
3. 输入主题名称，从模板列表中选择一个模板，然后单击“**确定**”。
4. 此时，您将看到门户主题编辑窗口的首次视图。单击“**确定**”退出。

您可以继续使用首次视图自定义新的门户主题。

创建新主题后，您可以将其绑定到 VPN 虚拟服务器或 VPN 全局。您可以在创建后立即绑定新主题，也可以在完成自定义后绑定。

门户主题自定义

要自定义门户主题，请在配置实用程序中使用门户主题界面。为获得最佳结果，您必须在使用此界面之前了解其各种元素。

关于门户主题界面

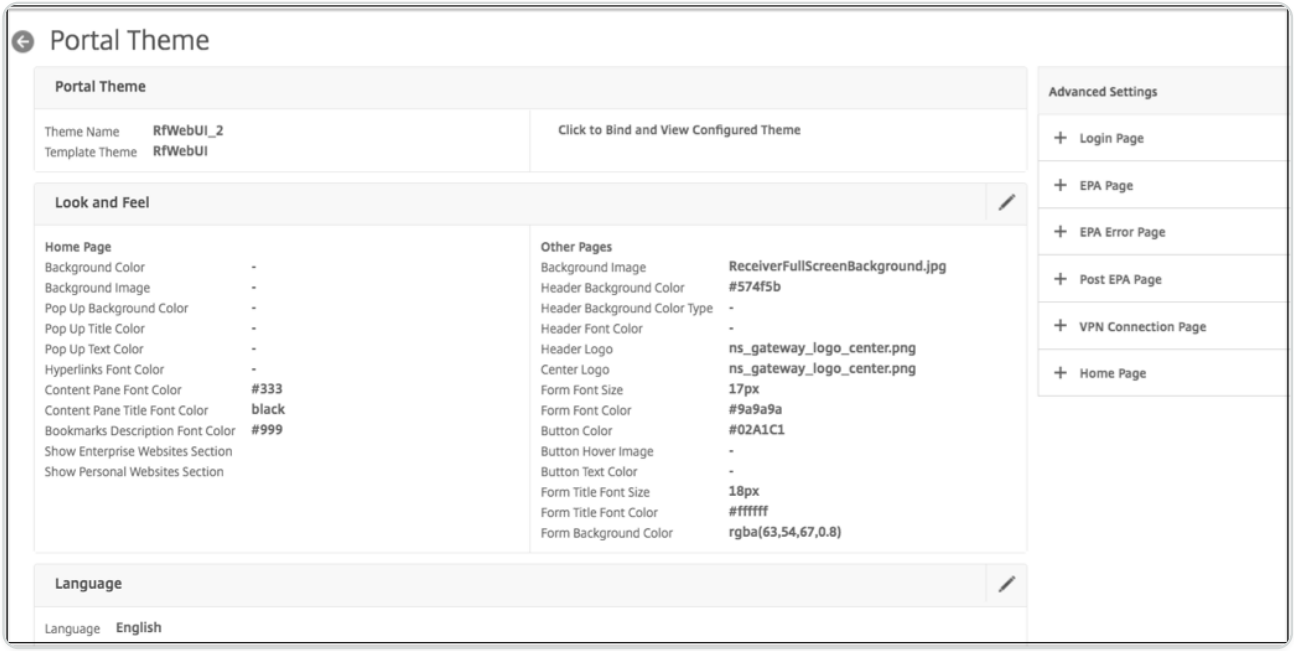
要在 NetScaler Gateway 配置实用程序中打开 **门户主题界面**，请在 **配置** 选项卡上，导航到 **NetScaler Gateway** 并单击 **门户主题**。您可以按照 *创建门户主题* 中所述创建主题，也可以在主详细信息窗格中选择现有主题并单击 **编辑**。

门户主题自定义页面有四个主要组件窗格，用于修改门户设计：

- 门户主题窗格

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

- 外观和感觉窗格
- 高级设置窗格
- 语言窗格



页面顶部的 **门户主题** 窗格报告了正在加载进行编辑的主题以及它所基于的模板主题。此处的查看选项允许您在不通过用户连接访问 VPN 的情况下查看您的自定义。使用查看选项需要将主题绑定到 VPN 虚拟服务器，并且在查看窗口关闭后绑定仍然有效。

通过页面中心的 **外观和感觉** 窗格，您可以配置主题的常规属性，例如页眉、背景颜色和图像、字体属性以及徽标。当此窗格处于编辑模式时，将提供属性图例，以指导门户页面上外观和感觉属性的使用位置。

高级设置 窗格包含各个门户页面的屏幕内容控件。要加载页面内容进行编辑，请单击列出的页面之一。然后，页面控件将在其他中心窗格下方打开。只要页面未修改，页面在门户主题编辑过程中在 **高级设置** 窗格中保持折叠状态。

在**语言**窗格中，您可以选择从**高级设置**窗格中选择页面进行编辑时加载哪种语言。默认加载英文页面。

可自定义页面属性的类型

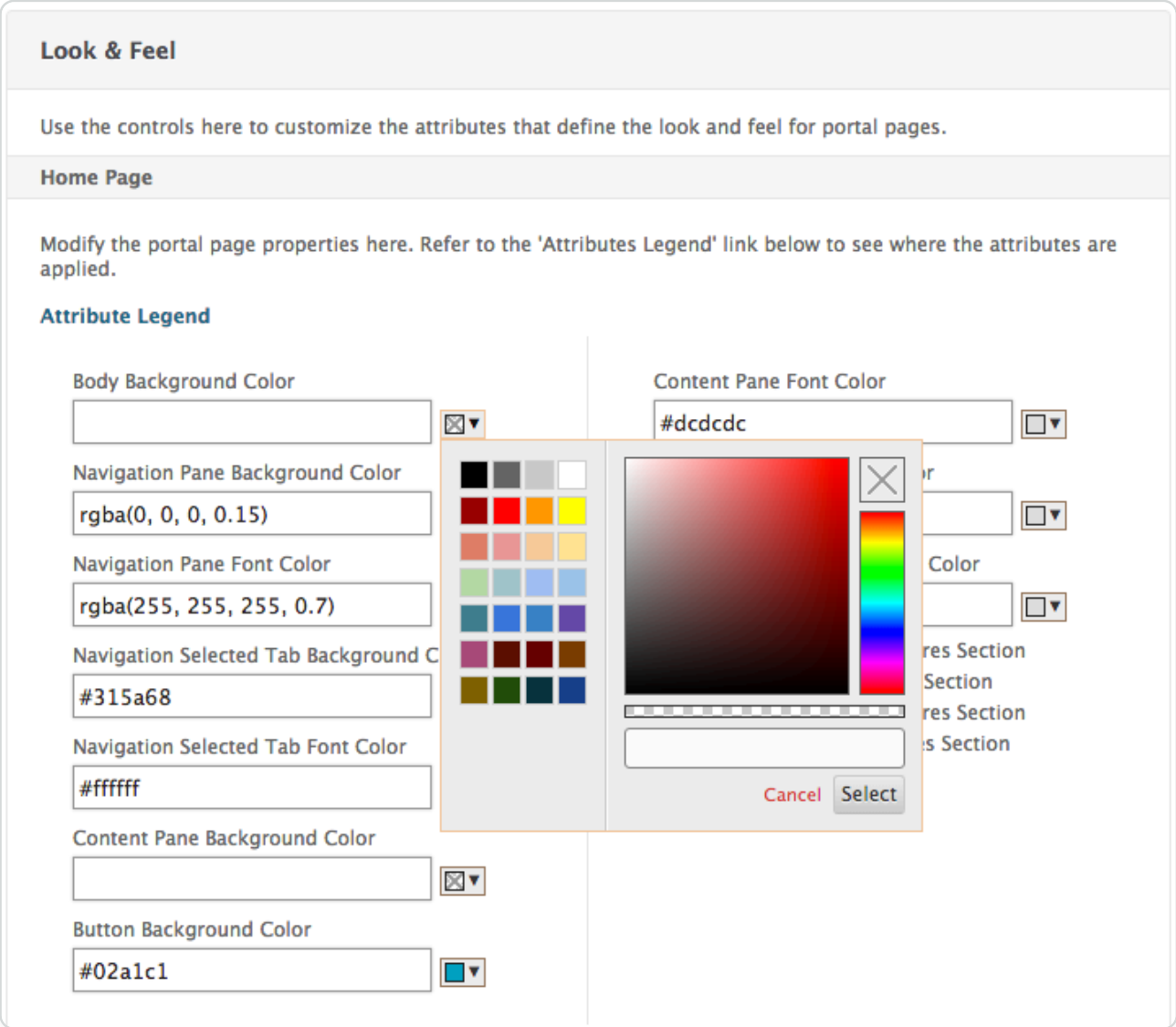
自定义门户主题时，您可以在门户主题界面中修改一系列属性。除了可以编辑的文本和支持的语言外，门户布局的图形元素也可以根据您的需求进行定制。每种页面元素类型都有在修改前需要考虑的参数或建议。

颜色

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

门户设计指定了页面背景、高亮显示、标题和正文内容文本、按钮控件以及悬停响应等属性的颜色。

要自定义颜色属性，您可以直接为选定项目输入颜色值，也可以使用提供的颜色选择器生成颜色值。该界面支持输入 RGBA 格式、HTML 十六进制三元组格式和 X11 颜色名称的有效 HTML 颜色值。通过单击属性输入字段旁边的颜色框，可以访问任何适用颜色属性的颜色选择器。



字体

除了字体颜色，您还可以修改某些页面属性的字体大小。对于每个这些属性，菜单会提供门户设计确定的每个属性的可用大小。

图像

对于图像，每个控件都有一个弹出式描述，提供大小建议和其他要求。描述根据属性在页面上的位置及其功能而异。您可以使用 PNG 或 JPEG 图像文件格式。您可以通过选择项目文件名下方的复选框，然后浏览到图像在本地计算机驱动器上的位置来选择要上传的图像。

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

标签

在**高级设置**部分，您可以选择特定门户页面的文本进行修改。如果您修改页面的默认英文文本，其他语言的文本不会重新翻译。其他语言的页面内容是为了方便而提供的，但任何自定义都需要手动更新。

要编辑页面的其他语言版本，如果窗口已打开，请首先单击打开的门户页面的 **X** 图标将其折叠。然后，在**语言**窗格中选择语言并单击**确定**。从**高级设置**窗格打开的所有门户页面都将使用该语言，直到您选择其他语言。

重要：

在高可用性或集群部署中，门户主题仅在主 NetScaler 实体或配置协调器 NetScaler 实体上进行门户主题设置时，才会跨共享配置分发。

创建 EULA

VPN 门户系统提供了将 EULA 应用于门户配置的选项。一旦 EULA 绑定到 NetScaler Gateway 配置（无论是在 VPN 全局范围还是绑定到相关的 VPN 虚拟服务器），VPN 用户必须先同意 EULA 作为条款和条件，然后才能通过身份验证登录 VPN。

与门户主题一样，系统会根据用户 Web 浏览器报告的区域设置向用户提供特定语言的 EULA。如果区域设置与任何受支持的语言不匹配，则默认提供的语言是英语。

对于每个 EULA，您可以在支持的语言中输入自定义消息。EULA 配置不提供预翻译内容，而门户主题则提供。如果用户报告的区域设置与未输入 EULA 内容的语言匹配，则当用户单击 VPN 登录页面上的“条款和条件”链接时，将返回空白页面。

要创建 EULA，您可以使用配置实用程序中“**配置**”选项卡下的任一控件，路径为“**NetScaler Gateway > 全局设置 > EULA**”或“**NetScaler Gateway > 资源 > EULA**”。“**全局设置**”窗格中的控件用于管理 VPN 全局 EULA 绑定，而“**资源 > EULA**”节点上的控件用于 EULA 配置的常规操作。

您可以通过编辑“**NetScaler Gateway > 虚拟服务器**”下的 VPN 虚拟服务器来管理 VPN 虚拟服务器 EULA 绑定。命令行也提供了一些用于管理 EULA 实体的命令。但是，完整的 EULA 管理控件仅在配置实用程序中可用。

使用 CLI 创建 EULA 实体

在命令提示符下，键入；

```
add vpn eula <name>
```

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

使用 GUI 创建 EULA 实体

1. 导航到“**NetScaler Gateway > 资源 > EULA**”。
2. 单击“**添加**”以创建实体。
3. 输入实体的名称。
4. 对于每种语言，将内容粘贴到相应的选项卡下。
5. 单击“**创建**”。

从版本 14.1 build 17.38 开始，以下 HTML 标签在 EULA 文本中重新启用。这些标签必须在不带 HTML 属性的情况下使用。

```
- <html></html>

- <b></b>

- <p></p>

- <i></i>

- <ol></ol>

- <ul></ul>

- <li></li>

- <br></br><br/>
```

创建 EULA 实体后，可以将其全局绑定到 VPN 配置，也可以绑定到 VPN 虚拟服务器。

使用 CLI 将 EULA 绑定到 VPN 全局

在命令提示符下，键入：

```
bind vpn global eula <name>
```

使用 GUI 将 EULA 绑定到 VPN 全局

1. 在“**配置**”选项卡上，导航到“**NetScaler Gateway > 全局设置**”。
2. 在主详细信息窗格中，单击“**配置最终用户许可协议**”。
3. 单击“**添加绑定**”。

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

4. 单击“**单击以选择**”。
5. 选择一个 EULA 实体，然后单击“**选择**”。
6. 单击“**绑定**”。
7. 单击“**关闭**”。

使用 CLI 将 EULA 绑定到 VPN 虚拟服务器

在命令提示符下，键入：

```
bind vpn vserver <name> eula <name>
```

使用 GUI 将 EULA 绑定到 VPN 虚拟服务器

1. 在“**配置**”选项卡上，导航到“**NetScaler Gateway > 虚拟服务器**”。
2. 在主详细信息窗格中，选择一个 VPN 虚拟服务器，然后单击“**编辑**”。
3. 在页面右侧的“**高级设置**”窗格中，单击“**EULA**”。
4. 在新添加的 EULA 窗格中，单击“**无 EULA**”。
5. `Click` “**单击以选择**”。
6. 选择一个 EULA 实体，然后单击“**选择**”。
7. 单击“**绑定**”。
8. 单击“**完成**”。

提示用户通过创建自定义页面升级旧版或不受支持的浏览器

如果客户端使用不安全的密码（例如 SSLv3）连接到 NetScaler® VIP 地址，则可以将其重定向到自定义页面，提示他们升级到最新版本的 Internet Explorer、Firefox、Chrome 或 Safari。

注意：根据互联网工程任务组 (ITEF) 的 RFC6176，TLS 服务器不得支持 SSLv2。因此，NetScaler 设备从 12.1 版本及更高版本不支持 SSLv2。

如何创建自定义页面以提示用户根据 SSL 升级旧版不受支持的浏览器

- 使用规则 `client.ssl.version.eq()` 创建 NetScaler 响应程序策略。该版本返回 SSL 协议版本。
  - 如果事务不是基于 SSL 的，则返回 0。
  - 如果事务是 SSLv2，则返回 0x002。
  - 如果事务是 SSLv3，则返回 0x300。

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

  - 如果事务是 TLSv1，则返回 0x301。

- 您必须启用 SSLv3（或其他早期版本）才能触发响应程序策略。

  例如，如果 NetScaler 设备上禁用了 SSLv3，并且使用 SSLv3 的旧版浏览器客户端尝试连接，则访问将被拒绝。

- 如果您的部署在指定时期（一两个月）内需要 SSLv3 或更早版本，请配置以下内容：

  - 启用 SSLv3 协议。
  - 更新自定义页面，以包含在指定时期后浏览器无法连接到设备的信息。

使用 NetScaler Gateway 配置无客户端 VPN 访问

无客户端访问允许用户获得所需的访问权限，而无需安装用户软件，例如 Citrix Secure Access™ 客户端或 Receiver。用户可以使用其 Web 浏览器连接到 Web 应用程序，例如 Outlook Web Access。

您可以使用以下步骤配置无客户端访问：

- 全局启用无客户端访问，或通过使用绑定到用户、组或虚拟服务器的会话策略启用。
- 选择 Web 地址编码方法。

要仅为特定虚拟服务器启用无客户端访问，请全局禁用无客户端访问，然后创建会话策略以启用它。

如果您使用 NetScaler Gateway 向导配置设备，则可以选择在向导中配置无客户端访问。向导中的设置将全局应用。在 NetScaler Gateway 向导中，您可以配置以下客户端连接方法：

- Citrix Secure Access 客户端。用户只能使用 Citrix Secure Access 客户端登录。
- 使用 Citrix Secure Access 客户端并允许访问场景回退。用户使用 Citrix Secure Access 客户端登录到 NetScaler Gateway。如果用户设备未能通过端点分析扫描，则允许用户使用无客户端访问登录。发生这种情况时，用户对网络资源的访问权限将受到限制。
- 允许用户使用 Web 浏览器和无客户端访问登录。用户只能通过无客户端访问登录，并且对网络资源的访问权限受到限制。

无客户端 VPN 访问策略的工作原理

您可以通过创建策略来配置对 Web 应用程序的无客户端访问。您可以在配置实用程序中配置无客户端访问策略的设置。无客户端访问策略由规则和配置文件组成。您可以使用 NetScaler Gateway 附带的预配置无客户端访问策略。您还可以创建自己的自定义无客户端访问策略。

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

NetScaler Gateway 为以下各项提供预配置策略：

- Outlook 网页访问 和 Outlook 网页应用
- SharePoint 2007
- 所有其他 Web 应用程序

注意：

OWA 2016 和 SharePoint 2016 仅支持使用高级无客户端访问。

请记住预配置的无客户端访问策略的以下特点：

- 它们是自动配置的，无法更改。
- 每个策略都在全局级别绑定。
- 除非您在全局启用无客户端访问或通过创建会话策略启用无客户端访问，否则不会强制执行每个策略。
- 即使您未启用无客户端访问，也无法删除或修改全局绑定。

对其他 Web 应用程序的支持取决于您在 NetScaler Gateway 上配置的重写策略。Citrix 建议测试您创建的任何自定义策略，以确保应用程序的所有组件都成功重写。

如果您允许来自 Receiver for Android、Receiver for iOS 或 Citrix Secure Hub™ 的连接，则必须启用无客户端访问。对于在 iOS 设备上运行的 Citrix Secure Hub，您还必须在会话配置文件中启用安全浏览。安全浏览和无客户端访问协同工作，以允许来自 iOS 设备的连接。如果用户不使用 iOS 设备连接，则无需启用安全浏览。

快速配置向导为移动设备配置正确的无客户端访问策略和设置。Citrix® 建议运行快速配置向导，为连接到 StoreFront 和 Citrix Endpoint Management 配置正确的策略。

您可以在全局或绑定到虚拟服务器自定义无客户端访问策略。如果要将无客户端访问策略绑定到虚拟服务器，则需要创建自定义策略并将其绑定。要在全局或针对虚拟服务器强制执行不同的无客户端访问策略，请更改自定义策略的优先级编号，使其低于预配置策略的编号，从而使自定义策略具有更高的优先级。如果没有其他无客户端访问策略绑定到虚拟服务器，则预配置的全局策略将优先。

注意：

您无法更改预配置的无客户端访问策略的优先级编号。

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

启用无客户端 VPN 访问

当您在全球级别启用无客户端访问时，所有用户都会收到无客户端访问的设置。您可以使用 NetScaler Gateway 向导、全局策略或会话策略来启用无客户端访问。

在全局设置或会话配置文件中，无客户端访问具有以下设置：

- **开**。启用无客户端访问。如果您禁用客户端选择并且未配置或禁用 StoreFront™，用户将通过无客户端访问登录。
- **关**。无客户端访问默认不启用。用户使用 Citrix Secure Access 客户端登录后，无客户端访问才启用。如果您禁用客户端选择并且未配置或禁用 StoreFront，用户将使用 Citrix Secure Access 客户端登录。如果用户登录时端点分析失败，用户将收到选择页面，其中包含可用的无客户端访问选项。
- **已禁用**。无客户端访问已禁用。当您选择**已禁用**时，用户无法通过无客户端访问登录，并且无客户端访问的图标不会显示在选择页面上。

如果您不使用 NetScaler Gateway 向导启用无客户端访问，则可以使用配置实用程序在全球范围或会话策略中启用它。

全局启用无客户端访问

1. 在配置实用程序中，在“配置”选项卡上，在导航窗格中，展开 NetScaler Gateway，然后单击**全局设置**。
2. 在详细信息窗格中，在**设置**下，单击**更改全局设置**。
3. 在**客户端体验**选项卡上，在**无客户端访问**旁边，选择**开**，然后单击**确定**。

使用会话策略启用无客户端访问

如果您只想让选定的用户组、组或虚拟服务器使用无客户端访问，请全局禁用或清除无客户端访问。然后，使用会话策略启用无客户端访问并将其绑定到用户、组或虚拟服务器。

1. 在配置实用程序中，在“配置”选项卡上，在导航窗格中，展开 **NetScaler Gateway > 策略 > 会话**。
2. 在详细信息窗格中，在“策略”选项卡上，单击**添加**。
3. 在**名称**中，键入策略的名称。
4. 在 **请求配置文件** 旁边，点击 **新建**。
5. 在 **名称** 中，输入配置文件的名称。
6. 在 **客户端体验** 选项卡上，在“无客户端访问”旁边，点击 **覆盖全局**，选择 **开**，然后点击 **创建**。

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

7. 在 **创建会话策略** 对话框中，在 **命名表达式** 旁边，选择“常规”，选择“真值”，点击“添加表达式”，点击 **创建**，然后点击 **关闭**。
8. 点击 **创建**，然后点击 **关闭**。

创建启用无客户端访问的会话策略后，将其绑定到用户、组或虚拟服务器。

编码 Web 地址

启用无客户端访问时，可以选择编码内部 Web 应用程序的地址，或将地址保留为明文。设置包括：

- 模糊处理。这使用标准编码机制来模糊处理资源的域和协议部分。
- 明文。Web 地址未编码，对用户可见。
- 加密。域和协议使用会话密钥加密。当 Web 地址加密时，同一 Web 资源的 URL 对于每个用户会话都不同。如果用户将编码的 Web 地址添加书签，将其保存在 Web 浏览器中然后注销，当用户再次登录并尝试使用书签连接到该 Web 地址时，他们将无法连接到该 Web 地址。 注意：如果用户在会话期间将加密的书签保存在访问界面中，则每次用户登录时该书签都有效。

您可以全局配置此设置，也可以将其作为会话策略的一部分进行配置。如果将编码配置为会话策略的一部分，则可以将其绑定到用户、组或虚拟服务器。

全局配置 Web 地址编码

1. 在配置实用程序中，在“配置”选项卡上的导航窗格中，展开 NetScaler Gateway，然后点击“全局设置”。
2. 在详细信息窗格中，在“设置”下，点击“更改全局设置”。
3. 在“客户端体验”选项卡上，在“无客户端访问 URL 编码”旁边，选择编码级别，然后单击“确定”。

通过创建会话策略配置 Web 地址编码

1. 在配置实用程序中，在“配置”选项卡上的导航窗格中，展开 **NetScaler Gateway > 策略**，然后单击“会话”。
2. 在详细信息窗格中，在“策略”选项卡上，单击“添加”。
3. 在“名称”中，键入策略的名称。
4. 在“请求配置文件”旁边，单击“新建”。
5. 在“名称”中，键入配置文件的名称。
6. 在“客户端体验”选项卡上，在“无客户端访问 URL 编码”旁边，单击“覆盖全局”，选择编码级别，然后单击“确定”。

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

7. 在“创建会话策略”对话框中，在“命名表达式”旁边，选择“常规”，选择“True 值”，单击“添加表达式”，单击“创建”，然后单击“关闭”。

创建无客户端访问策略

如果您想使用与默认无客户端访问策略相同的设置，但又想将策略绑定到虚拟服务器，则可以复制默认策略，并为该策略提供一个新名称。您可以使用配置实用程序复制默认策略。

将新策略绑定到虚拟服务器后，您可以设置策略的优先级，以便在用户登录时首先运行它。

使用默认设置创建无客户端访问策略

1. 在配置实用程序中，在导航窗格中，展开 **NetScaler Gateway > 策略**，然后单击“无客户端访问”。
2. 在详细信息窗格中，在“策略”选项卡上，单击一个默认策略，然后单击“添加”。
3. 在“名称”中，键入策略的新名称，单击“创建”，然后单击“关闭”。

将无客户端访问策略绑定到虚拟服务器

创建策略后，将其绑定到虚拟服务器。

1. 在配置实用程序中，在“配置”选项卡上的导航窗格中，展开 NetScaler Gateway，然后单击“虚拟服务器”。
2. 在详细信息窗格中，选择一个虚拟服务器，然后单击“打开”。
3. 在“配置 NetScaler Gateway 虚拟服务器”对话框中，单击“策略”选项卡，然后单击“无客户端”。
4. 单击“插入策略”，从列表中选择一个策略，然后单击“确定”。

创建和评估无客户端访问策略表达式

为无客户端访问创建策略时，可以为该策略创建自己的表达式。完成表达式创建后，可以评估表达式的准确性。

1. 在配置实用程序中，在导航窗格中，展开 **NetScaler Gateway > 策略**，然后单击“无客户端访问”。
2. 在详细信息窗格中，在“策略”选项卡上，单击一个默认策略，然后单击“添加”。
3. 在“名称”中，键入策略的名称。
4. 在“配置文件”旁边，单击“新建”。
5. 在“名称”中，键入配置文件的名称。
6. 配置重写设置，然后单击“创建”。

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

7. 在“创建无客户端访问策略”对话框中，在“表达式”下，单击“添加”。
8. 在“添加表达式”对话框中，创建表达式，然后单击“确定”。
9. 在“创建无客户端访问策略”对话框中，单击“评估”，如果表达式测试正确，则单击“创建”。

通过 NetScaler Gateway 进行高级无客户端 VPN 访问

无客户端 VPN 是一种通过 NetScaler Gateway 为企业内网资源提供远程访问的方式，无需在客户端计算机上安装 VPN 客户端应用程序。无客户端 VPN 允许客户端使用 Web 浏览器远程访问企业 Web 应用程序、门户和其他资源。 高级无客户端 VPN 解决方案消除了与无客户端 VPN 相关的以下限制：

- 相对 URL 有时无法识别。
- 动态生成的相对 URL 无法识别。

高级无客户端 VPN 识别绝对 URL 和主机名，并以一种新的、独特的方式重写它们，而不是尝试重写 HTTP 响应/网页中存在的相对 URL。SharePoint 不再需要使用默认文件夹来重写 URL，并且支持自定义 SharePoint 访问。

先决条件

以下是配置高级无客户端 VPN 的先决条件。

- **通配符服务器证书** - 高级无客户端 VPN 以独特的方式重写 URL。每个用户的每个 URL 都保持这种独特性。例如，如果 Web 应用程序托管在 `https://webapp.customer.com` 上，并且 VPN 虚拟服务器托管在 `https://vpn.customer.com` 上，则高级无客户端 VPN 会将其重写为 `https://cvpneqwerty.vpn.customer.com`。这意味着，每个 URL 都被重写为 VPN 虚拟服务器的子域。在这个新 URL 中， `cvpneqwerty` 可以解密回 `https://webapp.customer.com`。字符串 `cvpneqwerty` 是动态的，因此对于 SSL，您必须将 VPN 虚拟服务器绑定到通配符证书。

  如果服务器托管在 `https://vpn.customer.com` 上，则服务器证书现在必须包含 (vpn.customer.com 和 .vpn.customer.com) 作为证书 CN 或 SAN 的一部分（其中 CN=通用名，SAN=主题备用名称）。在 NetScaler Gateway 上绑定此证书的过程保持不变。 **注意：** 通配符证书仅支持一级（即不允许 ..customer.com）。如果您已经在使用通配符证书（用于 *.customer.com）并托管 `https://vpn.customer.com`，则这不适用于高级无客户端 VPN。您必须获取一个包含 `*.vpn.customer.com` 的新证书。

- **通配符 DNS 条目** - 客户端（Web 浏览器）必须解析高级无客户端 VPN 应用程序的 FQDN。在设置 NetScaler Gateway 服务器时，您必须已配置 DNS 条目以解析 vpn.customer.com。这允许浏览器将 vpn.customer.com 解析为您的 VPN 虚拟服务器的 IP 地址。要将 `https://cvpnqwerty.vpn.customer.com` 等 URL 解析到相同的 IP（VPN 虚拟服务器的 IP 地址），您

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

必须为 `vpn.customer.com` 的域添加一个新记录。在您的 DNS 服务器中找到域设置，并为“*”添加一个与之前相同的 IP 地址的新主机记录。添加主机记录后，您应该会看到 `https://cpvnanything.vpn.customer.com` 的成功 ping 响应。

配置高级无客户端 VPN 访问

要使用命令行界面配置高级无客户端 VPN 访问，请在命令提示符下键入：

```
set vpn parameter -clientlessVpnMode ON

set vpn parameter -advancedClientlessVpnMode ENABLED
```

如果会话操作绑定到虚拟服务器，则还必须为该会话操作启用高级无客户端 VPN 模式选项。

示例：

```
set vpn sessionaction SessionActionName -advancedclientlessvpn ENABLED
```

要使用 NetScaler GUI 配置高级无客户端 VPN 访问：

1. 在 NetScaler® GUI 中，导航到 **配置 > NetScaler > 全局设置**。
2. 在 **全局设置页面** 上，单击 **更改全局设置**，然后选择 **客户端体验** 选项卡。
3. 在 **客户端体验** 选项卡上，从 **无客户端访问** 列表中，单击 **开**。
4. 在 **客户端体验** 选项卡上，从 **高级无客户端 VPN 模式** 列表中，单击 **已启用**。 如果您从 **高级无客户端 VPN 模式** 列表中选择 **严格**，NetScaler 设备将仅响应经典无客户端 VPN 形式的 StoreFront URL，并阻止所有其他经典无客户端 VPN 请求。此选项为设备提供更安全的配置，用于交付内部 Web 资源。

注意：

- 如果会话操作绑定到虚拟服务器，您还必须在 **配置 NetScaler Gateway 会话配置文件** 页面中的 **客户端体验** 选项卡上为该会话操作启用 **高级无客户端 VPN 模式** 选项。
- 您可以选择 **覆盖全局** 选项来覆盖全局设置。
- 您还可以在会话级别配置高级无客户端 VPN 功能。

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

注意事项

高级无客户端 VPN 旨在提供对企业 Web 应用程序的访问。此类应用程序对于它们所需的每种资源（JavaScript、CSS、图像等）只有一个 FQDN。由于我们将内部应用程序的完整 FQDN 编码为单八位字节（无客户端 VPN），因此我们失去了子域关系。因此，每当企业 Web 应用程序配置了 CORS 时，有时您可能会在通过高级无客户端 VPN 访问它时遇到问题。

为用户配置域访问

如果用户通过无客户端访问连接，您可以限制用户被允许访问的网络资源、域和网站。您可以使用 NetScaler Gateway 向导或全局设置来创建包含或排除域访问的列表。

您可以允许访问所有网络资源、域和网站，然后创建一个排除列表。排除列表列出了用户不允许访问的特定资源集。用户无法访问排除列表中的任何域。

您也可以拒绝访问所有网络资源、域和网站，然后创建一个特定的包含列表。包含列表列出了用户可以访问的资源。用户无法访问列表中未出现的任何域。

注意：如果您为 Citrix Endpoint Management 或 StoreFront 配置无客户端访问策略，并且用户使用 Receiver for Web 连接，则需要允许 Receiver for Web 可以访问的域。这是必需的，以便 NetScaler Gateway 可以为 StoreFront 和 Endpoint Management 重写网络流量。

使用 NetScaler Gateway 向导配置域访问

1. 在配置实用程序中，单击“配置”选项卡，然后在导航窗格中单击“NetScaler Gateway”。
2. 在详细信息窗格中，在“入门”下，单击“NetScaler Gateway 向导”。
3. 单击“下一步”，然后按照向导中的说明操作，直到到达“配置无客户端访问”页面。
4. 单击“配置无客户端访问域”，然后执行以下操作之一：
   - 要创建排除域列表，请单击“排除域”。
   - 要创建包含域列表，请单击“允许域”。
5. 在“域名”下，键入域名，然后单击“添加”。
6. 对要添加到列表中的每个域重复步骤 5，完成后单击“确定”。
7. 继续使用 NetScaler Gateway 向导配置设备。

使用配置实用程序配置域设置

您还可以使用配置实用程序中的全局设置创建或修改域列表。

1. 在配置实用程序中，在“配置”选项卡上的导航窗格中，展开 NetScaler Gateway，然后单击“全局设置”。

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

2. 在详细信息窗格中，在“无客户端访问”下，单击“配置无客户端访问域”。
3. 执行以下操作之一：
   - 要创建排除域列表，请单击“排除域”。
   - 要创建包含域列表，请单击“允许域”。
4. 在“域名”下，键入域名，然后单击“添加”。
5. 对要添加到列表中的每个域重复步骤 4，完成后单击“确定”。

SharePoint 2003、SharePoint 2007 和 SharePoint 2013 的无客户端 VPN 访问

NetScaler Gateway 可以重写一个或多个 SharePoint 2003、SharePoint 2007 或 SharePoint 2013 站点中的内容，以便用户无需 Citrix Secure Access 客户端即可访问这些内容。为了成功完成重写过程，您必须为网络中的每个 SharePoint 服务器配置 NetScaler Gateway 的主机名。

您可以使用 NetScaler Gateway 向导或配置实用程序来配置 SharePoint 站点的主机名。

在 NetScaler Gateway 向导中，导航通过向导以配置您的设置。当您到达“配置无客户端访问”页面时，键入 SharePoint 站点的网址，然后单击“**添加**”。

要添加更多网站或在运行 NetScaler Gateway 向导后首次配置 SharePoint，请使用配置实用程序。

重要提示：

经典无客户端访问支持 SharePoint 2013 和 OWA 2013 及更早版本。高级无客户端访问支持 SharePoint 2016 和 OWA 2016 及更高版本。

使用 NetScaler GUI 配置 SharePoint 的无客户端访问

1. 导航到“**NetScaler Gateway**”>“**全局设置**”。
2. 在详细信息窗格中，在“无客户端访问”下，单击“**配置 SharePoint 的无客户端访问**”。
3. 在“SharePoint 的无客户端访问”下，在“SharePoint 服务器的主机名”中，键入 SharePoint 站点的主机名，然后单击“**添加**”。
4. 对要添加到列表中的每个 SharePoint 站点重复步骤 3，完成后单击“**确定**”。

将 SharePoint 站点设置为主页

如果要将 SharePoint 站点设置为主页，请配置会话配置文件并输入 SharePoint 站点的主机名。

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

配置 SharePoint 站点作为主页

1. 导航到 **NetScaler Gateway > 策略**，然后单击 **会话**。
2. 在详细信息窗格中，单击 **添加**。
3. 在 **名称** 中，键入策略的名称。
4. 在 **请求配置文件** 旁边，单击 **新建**。
5. 在名称中，键入配置文件的名称。
6. 在“客户端体验”选项卡上，“主页”旁边，单击 **覆盖全局**，然后键入 SharePoint 站点的名称。
7. 在“无客户端访问”旁边，单击 **覆盖全局**，选择 **开**，然后单击 **创建**。
8. 在“创建会话策略”对话框中，“命名表达式”旁边，选择 **常规**，选择 **真值**，单击 **添加表达式**，单击 **创建**，然后单击 **关闭**。

完成会话策略后，将其绑定到用户、组、虚拟服务器或全局。用户登录时，他们会看到 SharePoint 网站作为其主页。

为 SharePoint 2007 服务器启用名称解析

SharePoint 2007 服务器在响应中将配置的服务器名称作为各种 URL 中的主机名发送。如果配置的 SharePoint 服务器名称不是完全限定域名 (FQDN)，NetScaler Gateway 将无法使用 SharePoint 服务器名称解析 IP 地址，并且某些用户功能会因错误消息“HTTP:1.1 Gateway Time-out”而超时。这些功能可能包括用户使用无客户端访问登录时签入和签出文件、查看工作区以及上传多个文件。

要解决此问题，您可以尝试以下方法之一：

- 在 NetScaler Gateway 上配置 DNS 后缀，以便在名称解析之前将 SharePoint 主机名转换为 FQDN。
- 为每个 SharePoint 服务器名称在 NetScaler Gateway 上配置本地 DNS 条目。
- 将所有 SharePoint 服务器名称更改为使用 FQDN，例如 SharePoint.intranetdomain 而不是 SharePoint，

配置 DNS 后缀

1. 在配置实用程序中，在“配置”选项卡上的导航窗格中，展开 **DNS**，然后单击 **DNS 后缀**。
2. 在详细信息窗格中，单击 **添加**。
3. 在 **DNS 后缀** 中，键入内部网域名作为后缀，单击 **创建**，然后单击 **关闭**。

您可以对要添加的每个域重复步骤 3。

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

配置 NetScaler Gateway 上每个 SharePoint 服务器名称的本地 DNS 记录

1. 在配置实用程序中，在导航窗格中，展开 **DNS > 记录**，然后单击 **地址记录**。
2. 在详细信息窗格中，单击 **添加**。
3. 在 **主机名** 中，键入用于 DNS 地址记录的 SharePoint 主机名。
4. 在 **IP 地址** 中，键入 SharePoint 服务器的 IP 地址，单击 **添加**，单击 **创建**，然后单击 **关闭**。

添加 A 记录的主机名不得具有 CNAME 记录。此外，设备上不能有重复的 A 记录。

启用无客户端 VPN 访问持久性 Cookie

访问 SharePoint 的某些功能（例如打开和编辑 SharePoint 服务器上托管的 Microsoft Word、Excel 和 PowerPoint 文档）需要持久性 Cookie。

持久性 Cookie 留在用户设备上，并随每个 HTTP 请求发送。NetScaler Gateway 在将持久性 Cookie 发送到用户设备上的插件之前对其进行加密，并在会话存在期间定期刷新该 Cookie。如果会话结束，该 Cookie 将失效。

在 NetScaler Gateway 向导中，管理员可以全局启用持久性 Cookie。您还可以创建会话策略，为每个用户、组或虚拟服务器启用持久性 Cookie。

持久性 Cookie 有以下选项：

- 允许 启用持久性 Cookie，用户可以打开和编辑存储在 SharePoint 中的 Microsoft 文档。
- 拒绝 禁用持久性 Cookie，用户无法打开和编辑存储在 SharePoint 中的 Microsoft 文档。
- 提示 在会话期间提示用户允许或拒绝持久性 Cookie。

如果用户不连接到 SharePoint，则无客户端访问不需要持久性 Cookie。

为 SharePoint 的无客户端 VPN 访问配置持久性 Cookie

您可以全局配置 SharePoint 的无客户端访问持久性 Cookie，也可以将其作为会话策略的一部分进行配置。

全局配置持久性 Cookie

1. 在配置实用程序中，在“配置”选项卡上，在导航窗格中，展开 NetScaler Gateway，然后单击“全局设置”。
2. 在详细信息窗格中，在“设置”下，单击“更改全局设置”。
3. 在“客户端体验”选项卡上，在“无客户端访问持久性 Cookie”旁边，选择一个选项，然后单击“确定”。

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

将持久性 Cookie 配置为会话策略的一部分

1. 在配置实用程序中，在“配置”选项卡上，在导航窗格中，展开 **NetScaler Gateway > 策略**，然后单击“会话”。
2. 在详细信息窗格中，在“策略”选项卡上，单击“添加”。
3. 在“名称”中，键入策略的名称。
4. 在“请求配置文件”旁边，单击“新建”。
5. 在“名称”中，键入配置文件的名称。
6. 在“客户端体验”选项卡上，在“无客户端访问持久性 Cookie”旁边，单击“覆盖全局”，选择一个选项，然后单击“创建”。
7. 在“创建身份验证策略”对话框中，在“命名表达式”旁边，选择“常规”，选择“真值”，单击“添加表达式”，单击“创建”，然后单击“关闭”。

Citrix® SSO 移动设备 VPN 客户端

Citrix SSO 是适用于移动设备（macOS、iOS 和 iOS）的 VPN 客户端。Citrix SSO 在 macOS、iOS 和 Android 上提供完整的移动设备管理 (MDM) 支持。借助 MDM 服务器，管理员可以远程配置和管理设备级 VPN 配置文件和按应用程序 VPN 配置文件。 Citrix SSO 还支持大多数常用功能。

参考

- Citrix 安全访问客户端
- NetScaler Gateway VPN 客户端和支持的功能

配置客户端选择页面

您可以配置 NetScaler Gateway，为用户提供多种登录选项。通过配置客户端选择页面，用户可以选择从一个位置登录，并具有以下选项：

- 适用于 Windows 的 Citrix Secure Access™ 客户端
- 适用于 macOS X 的 Citrix Secure Access 客户端
- StoreFront™
- 无客户端访问

用户通过使用绑定到 NetScaler Gateway 或虚拟服务器的证书中的 Web 地址登录 NetScaler Gateway。通过创建会话策略和配置文件，您可以确定用户收到的登录选项。根据您配置 NetScaler Gateway 的方式，客户端选择页面最多显示三个图标，代表以下登录选项：

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

- 网络访问。当用户首次使用 Web 浏览器登录 NetScaler Gateway 并选择“网络访问”时，将显示下载页面。当用户单击“下载”时，插件将下载并安装到用户设备上。下载和安装完成后，将显示访问界面。如果您安装了更新版本或恢复到旧版 NetScaler Gateway，适用于 Windows 的 Citrix Secure Access 客户端将静默升级或降级到设备上的版本。如果用户使用适用于 Mac 的 Citrix Secure Access 客户端连接，并且在用户登录时检测到新的设备版本，则插件将静默升级。此版本的插件不会静默降级。
- StoreFront。如果用户选择 StoreFront 登录，则 Receiver 将打开，用户可以访问应用程序和桌面。

  注意：

  如果您将 StoreFront 配置为客户端选择，应用程序和桌面不会显示在访问界面的左侧窗格中。

- 无客户端访问。如果用户选择无客户端访问登录，则会显示访问界面或您的自定义主页。在访问界面中，用户可以导航到文件共享、网站并使用 Outlook Web Access。

Secure Browse 允许用户通过 NetScaler Gateway 从 iOS 设备进行连接。如果您启用 Secure Browse，当用户使用 Secure Hub 登录时，Secure Browse 会禁用客户端选择页面。

在登录时显示客户端选择页面

当您启用客户端选择选项时，用户在成功通过 NetScaler Gateway 身份验证后，可以从一个网页使用 Citrix Secure Access 客户端、Receiver 或无客户端访问进行登录。登录成功后，网页中会显示图标，用户可以从中选择建立连接的方法。

您可以在不使用端点分析或不实施访问场景回退的情况下启用客户端选择。如果您未定义客户端安全表达式，用户将收到 NetScaler Gateway 上配置的设置的连接选项。如果用户会话存在客户端安全表达式，并且用户设备未能通过端点分析扫描，则选择页面仅提供无客户端访问以供登录。

您可以全局配置客户端选择，也可以通过使用会话配置文件和策略进行配置。

重要提示：

配置客户端选择时，请勿配置隔离组。未能通过端点分析扫描并被隔离的用户设备与通过端点扫描的用户设备受到相同对待。

全局启用客户端选择选项

1. 在 GUI 中，在“配置”选项卡上的导航窗格中，展开 **NetScaler Gateway**，然后单击 **全局设置**。

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

2. 在详细信息窗格中，在“设置”下，单击 **更改全局设置**。
3. 在“客户端体验”选项卡上，单击 **高级设置**。
4. 在“常规”选项卡上，单击 **客户端选择，** 然后单击 **确定**。

将会话策略的一部分启用客户端选择

您还可以将会话策略的一部分配置为客户端选择，然后将其绑定到用户、组和虚拟服务器。

1. 在 GUI 中，在“配置”选项卡上的导航窗格中，展开 **NetScaler Gateway > 策略，** 然后单击 **会话**。
2. 在详细信息窗格中，在“策略”选项卡上，单击 **添加**。
3. 在“名称”中，键入策略的名称。
4. 在“请求配置文件”旁边，单击 **新建**。
5. 在“名称”中，键入配置文件的名称。
6. 在“客户端体验”选项卡上，单击“**高级**”。
7. 在“常规”选项卡上，在“客户端选择”旁边，单击“**覆盖全局**”，单击“**客户端选择**”，单击“**确定**”，然后单击“**创建**”。
8. 在“创建会话策略”对话框中，在“命名表达式”旁边，选择“**常规**”，选择“**True value**”，单击“**添加表达式**”，单击“**创建**”，然后单击“**关闭**”。

配置客户端选择选项

除了使用会话配置文件和策略启用客户端选择之外，您还需要配置用户软件的设置。例如，您希望用户使用 Citrix Secure Access 客户端、StoreFront 或无客户端访问登录。您创建一个会话配置文件，该配置文件启用所有这三个选项和客户端选择。然后，您创建一个会话策略，其中表达式设置为 True value 并附加了配置文件。接下来，您将该会话策略绑定到虚拟服务器。

在创建会话策略和配置文件之前，您需要为用户创建一个授权组。

创建授权组

1. 在配置实用程序中，在导航窗格的“配置”选项卡上，选择“**NetScaler Gateway > 用户管理**”，然后单击“**AAA 组**”。
2. 在详细信息窗格中，单击“**添加**”。
3. 在“**组名**”中，键入组的名称。
4. 在“**用户**”选项卡上，选择用户，为每个用户单击“**添加**”，单击“**创建**”，然后单击“**关闭**”。

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

以下过程是使用 Citrix Secure Access 客户端、StoreFront 和无客户端访问的客户端选择的会话配置文件示例。

为客户端选择创建会话配置文件

1. 在配置实用程序中，在“配置”选项卡上的导航窗格中，展开“**NetScaler Gateway > 策略 > 会话**”。
2. 在详细信息窗格中，单击“**配置文件**”选项卡，然后单击“**添加**”。
3. 在“**名称**”中，键入配置文件的名称。
4. 在“**客户端体验**”选项卡上，执行以下操作：
   a. 在“主页”旁边，单击“**覆盖全局**”，然后清除“**显示主页**”。这将禁用访问界面。
   b. 在“**无客户端访问**”旁边，单击“**覆盖全局**”，然后选择“**关闭**”。
   c. 在“**插件类型**”旁边，单击“**覆盖全局**”，然后选择 Windows/Mac OS X。
   d. 单击“**高级设置**”，然后在“**客户端选择**”旁边，单击“**覆盖全局**”，再单击“**客户端选择**”。
5. 在“**安全**”选项卡上“**默认授权操作**”旁边，单击“**覆盖全局**”，然后选择“**允许**”。
6. 在“**安全**”选项卡上，单击“**高级设置**”。
7. 在“**授权组**”下，单击“**覆盖全局**”，单击“**添加**”，然后选择组。
8. 在“**已发布的应用程序**”选项卡上，执行以下操作：
   a. 在“**ICA® 代理**”旁边，单击“**覆盖全局**”，然后选择“**关闭**”。
   b. 在“**Web 界面地址**”旁边，单击“**覆盖全局**”，然后键入 StoreFront 的 Web 地址，例如 `<http://ipAddress/Citrix/>`。
   c. 在“**Web 界面门户模式**”旁边，单击“**覆盖全局**”，然后选择“**紧凑**”。
   d. 在“**单点登录域**”旁边，单击“**覆盖全局**”，然后键入域的名称。
9. 点击 **创建**，然后点击 **关闭**。

如果您想使用适用于 Java 的 Citrix Secure Access 客户端作为客户端选择，请在插件类型中的“**客户端体验**”选项卡上选择 **Java**。如果您选择此选项，则必须配置一个内部网应用程序并将拦截模式设置为代理。

创建会话配置文件后，创建一个会话策略。在策略中，选择配置文件，并将表达式设置为 True 值。

要将 StoreFront 用作客户端选择，您还必须在 NetScaler Gateway 上配置安全票证颁发机构 (STA)。STA 绑定到虚拟服务器。

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

注意：

如果运行 StoreFront 的服务器不可用，Citrix Virtual Apps™ 选项不会显示在选择页面上。

全局配置 STA 服务器

1. 在配置实用程序中，在“配置”选项卡上的导航窗格中，展开 **NetScaler Gateway**，然后点击 **全局设置**。
2. 在详细信息窗格中，在“服务器”下，点击 **绑定/取消绑定 STA 服务器**，供安全票证颁发机构使用。
3. 在“**绑定/取消绑定 STA 服务器**”对话框中，点击 **添加**。
4. 在“**配置 STA 服务器**”对话框中，在 URL 中键入 STA 服务器的网址，然后点击 **创建**。
5. 重复步骤 3 和 4 以添加更多 STA 服务器，然后点击 **确定**。

将 STA 绑定到虚拟服务器

1. 在配置实用程序中，在“配置”选项卡上的导航窗格中，展开 **NetScaler Gateway**，然后点击 **虚拟服务器**。
2. 在详细信息窗格中，点击一个虚拟服务器，然后点击 **打开**。
3. 在 **已发布的应用程序** 选项卡上，在 **安全票证颁发机构** 下，在 **活动** 下，选择 STA 服务器，然后单击 **确定**。

您还可以在 **已发布的应用程序** 选项卡上添加 STA 服务器。

配置访问场景回退

SmartAccess 允许 NetScaler Gateway 根据端点分析扫描结果自动确定用户设备允许的访问方法。访问场景回退通过允许用户设备在未通过初始端点分析扫描时，使用 Citrix Workspace 应用程序从 Citrix Secure Access 客户端回退到 StoreFront，从而进一步扩展了此功能。

要启用访问场景回退，您需要配置一个身份验证后策略，该策略决定用户登录 NetScaler Gateway 时是否获得替代访问方法。此身份验证后策略定义为客户端安全表达式，您可以将其配置为全局设置或作为会话配置文件的一部分。如果您配置会话配置文件，则该配置文件将与会话策略关联，然后您将该策略绑定到用户、组或虚拟服务器。启用访问场景回退后，NetScaler Gateway 会在用户身份验证后启动端点分析扫描。对于不符合回退身份验证后扫描要求的用户设备，结果如下：

- 如果启用了客户端选择，用户只能使用 Citrix Workspace 应用程序登录 StoreFront。

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

- 如果禁用了无客户端访问和客户端选择，用户可以被隔离到一个仅提供 StoreFront 访问的组中。
- 如果在 NetScaler Gateway 上启用了无客户端访问和 StoreFront 并且禁用了 ICA 代理，用户将回退到无客户端访问。
- 如果未配置 StoreFront 并且无客户端访问设置为允许，用户将回退到无客户端访问。

当无客户端访问被禁用时，必须为访问场景回退配置以下设置组合：

- 定义用于回退身份验证后扫描的客户端安全参数。
- 定义 Web Interface 主页。
- 禁用客户端选择。
- 如果用户设备未能通过客户端安全检查，用户将被置于一个隔离组中，该组仅允许访问 StoreFront 和已发布的应用程序。

创建访问场景回退策略

要为访问场景回退配置 NetScaler Gateway，您需要通过以下方式创建策略和组：

- 创建一个隔离组，如果端点分析扫描失败，用户将被置于其中。
- 创建一个全局 StoreFront 设置，该设置在端点分析扫描失败时使用。
- 创建一个会话策略，该策略覆盖全局设置，然后将会话策略绑定到组。
- 创建一个全局客户端安全策略，该策略在端点分析失败时应用。

配置访问场景回退时，请遵循以下准则：

- 使用客户端选择或访问场景回退需要所有用户都安装端点分析插件。如果端点分析无法运行，或者用户在扫描期间选择“跳过扫描”，则用户将被拒绝访问。 注意：在 NetScaler Gateway 10.1 Build 120.1316.e 中已删除跳过扫描的选项。
- 启用客户端选择后，如果用户设备未能通过端点分析扫描，用户将被置于隔离组中。用户可以使用 Citrix Secure Access 客户端或 Citrix Workspace 应用程序继续登录 StoreFront。 注意：CitrixÂ® 建议您在启用客户端选择时不要创建隔离组。未能通过端点分析扫描的用户设备被隔离后，其处理方式与通过端点扫描的用户设备相同。
- 如果端点分析扫描失败且用户被置于隔离组中，则只有在没有直接绑定到用户的策略且其优先级编号不高于绑定到隔离组的策略时，绑定到隔离组的策略才有效。
- 您可以为访问接口和 StoreFront 使用不同的 Web 地址。配置主页时，访问接口主页对于 Citrix Secure Access 客户端具有优先权，而 Citrix Workspace 应用程序主页对于 StoreFront 具有优先权。

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

创建隔离组

1. 在配置实用程序中，在“配置”选项卡上的导航窗格中，展开 **NetScaler Gateway > 用户管理**，然后单击 **AAA 组**。
2. 在详细信息窗格中，单击“**添加**”。
3. 在“**组名称**”中，键入组的名称，单击“**创建**”，然后单击“**关闭**”。

> **重要提示：**
>
> 隔离组的名称不得与用户可能所属的任何域组的名称匹配。如果隔离组与 Active Directory 组名称匹配，即使用户设备通过了端点分析安全扫描，用户也会被隔离。

创建组后，如果用户设备未能通过端点分析扫描，请将 NetScaler Gateway 配置为回退到访问接口。

配置设置以隔离用户连接

1. 在配置实用程序中，在“配置”选项卡上的导航窗格中，展开 NetScaler Gateway，然后单击“**全局设置**”。
2. 在详细信息窗格中，在“**设置**”下，单击“**更改全局设置**”。
3. 在“**全局 NetScaler Gateway 设置**”对话框中，在“**已发布的应用程序**”选项卡上，在“**ICA 代理**”旁边，选择“**关闭**”。
4. 在“**Web 界面地址**”旁边，键入 StoreFront 的 Web 地址。
5. 在“**单点登录域**”旁边，键入 Active Directory 域的名称，然后单击“**确定**”。

配置全局设置后，创建会话策略以覆盖全局 ICA® 代理设置，然后将会话策略绑定到隔离组。

为访问方案回退创建会话策略

1. 在配置实用程序中，在“配置”选项卡上的导航窗格中，展开“**NetScaler Gateway > 策略**”，然后单击“**会话**”。
2. 在详细信息窗格中，单击“**添加**”。
3. 在“**名称**”中，键入策略的名称。
4. 在“**请求配置文件**”旁边，单击“**新建**”。
5. 在“**已发布的应用程序**”选项卡上，在“**ICA 代理**”旁边，单击“**覆盖全局**”，选择“**开**”，然后单击“**创建**”。

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

6. 在“**创建会话策略**”对话框中，在“**命名表达式**”旁边，选择“**常规**”，选择“**真值**”，单击“**添加表达式**”，单击“**创建**”，然后单击“**关闭**”。

创建会话策略后，将策略绑定到隔离组。

将会话策略绑定到隔离组

1. 在配置实用程序中，在“配置”选项卡上，在导航窗格中，展开 **NetScaler Gateway > 用户管理**，然后单击 **AAA 组**。
2. 在详细信息窗格中，选择一个组，然后单击 **打开**。
3. 单击“会话”。
4. 在“**策略**”选项卡上，选择“**会话**”，然后单击“**插入策略**”。
5. 在“**策略名称**”下，选择策略，然后单击“**确定**”。

在创建了会话策略和配置文件以在 NetScaler Gateway 上启用 StoreFront 后，创建全局客户端安全策略。

创建全局客户端安全策略

1. 在配置实用程序中，在“配置”选项卡上，在导航窗格中，展开 NetScaler Gateway，然后单击“**全局设置**”。
2. 在详细信息窗格中，在“**设置**”下，单击“**更改全局设置**。
3. 在“**安全**”选项卡上，单击“**高级设置**”。
4. 在“**客户端安全**”中，输入表达式。有关配置系统表达式的更多信息，请参阅配置系统表达式 和配置复合客户端安全表达式。
5. 在“**隔离组**”中，选择您在组过程中配置的组，然后单击“**确定**”。

配置 Citrix Secure Access™ 客户端的连接

您可以通过定义用户可在内部网络中访问的资源来配置用户设备连接。配置用户设备连接包括：

- 定义允许用户访问的域。
- 配置用户的 IP 地址，包括地址池（内网 IP）。
- 配置超时设置。
- 配置单点登录。
- 配置客户端拦截。
- 配置拆分隧道。

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

- 配置通过代理服务器的连接。
- 配置用户软件以通过 NetScaler Gateway 连接。
- 配置移动设备的访问。

您可以通过使用会话策略中的配置文件来配置大多数用户设备连接。您还可以通过使用内网应用程序、预身份验证和流量策略来定义用户设备连接设置。

注意：

Windows VPN 插件和 EPA 插件会收集其各种操作的遥测数据。要禁用此功能，请在客户端计算机上执行以下操作。

将注册表项“HKLM\Software\Citrix\Secure Access Client\DisableGA”（类型为 REG_DWORD）设置为 1。

配置用户会话数

您可以配置在特定时间点允许连接到 NetScaler Gateway 的最大用户数，可以在全局级别或每个虚拟服务器级别进行配置。当连接到设备的 NetScaler Gateway 用户数超过您配置的值时，NetScaler Gateway 上不会创建会话。如果用户数超过您允许的数量，用户将收到错误消息。

设置全局用户限制

当您全局配置用户限制时，此限制适用于所有在系统上与不同虚拟服务器建立会话的用户。当用户会话数达到您设置的值时，NetScaler Gateway 上存在的任何虚拟服务器都无法建立新会话。

当您为 NetScaler Gateway 设置默认身份验证类型时，可以在全局级别设置最大用户数。

1. 在配置实用程序中，在“配置”选项卡上，在导航窗格中，展开 NetScaler Gateway，然后单击“全局设置”。
2. 在详细信息窗格中，在“设置”下，单击“更改身份验证设置”。
3. 在“全局身份验证设置”对话框中，在“最大用户数”中，键入用户数，然后单击“确定”。

设置每个虚拟服务器的用户限制

您还可以将用户限制应用于系统上的每个虚拟服务器。当您配置每个虚拟服务器的用户限制时，此限制仅适用于与特定虚拟服务器建立会话的用户。与其它虚拟服务器建立会话的用户不受此限制的影响。

1. 在配置实用程序中，在“配置”选项卡上，在导航窗格中，展开 NetScaler Gateway，然后单击“虚拟服务器”。

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

2. 在详细信息窗格中，单击一个虚拟服务器，然后单击“打开”。
3. 在“最大用户数”中，键入用户数，然后单击“确定”。

配置超时设置

您可以将 NetScaler Gateway 配置为在连接在指定分钟数内没有活动时强制断开连接。会话超时（断开连接）前一分钟，用户会收到一条警报，指示会话即将关闭。如果会话关闭，用户必须重新登录。

提供以下超时选项。

- **强制超时：** 如果启用此设置，NetScaler Gateway 将在超时间隔（以分钟为单位）过去后断开会话，无论用户正在做什么。当超时间隔过去时，用户无法采取任何措施来阻止断开连接。此设置适用于通过 Citrix Secure Access 客户端、Citrix Workspace 应用程序、Secure Hub 或通过 Web 浏览器连接的用户。最小值为 1，最大值为 65535。
- **会话超时：** 如果启用此设置，NetScaler Gateway 将在指定间隔（以分钟为单位）内未检测到网络活动时断开会话。此设置适用于通过 Citrix Secure Access 客户端、Citrix Workspace 应用程序、Citrix Secure Hub 或通过 Web 浏览器连接的用户。默认超时设置为 30 分钟。最小值为 1，最大值为 65535。
- **空闲会话超时：** 如果在指定间隔内没有用户活动（例如鼠标、键盘或触摸），Citrix Secure Access™ 客户端终止空闲会话的持续时间（以分钟为单位）。此设置仅适用于通过 Citrix Secure Access 客户端连接的用户。最小值为 1，最大值为 9999。

您可以通过输入 1 到 65536 之间的值来启用任何超时设置，以指定超时间隔的分钟数。如果您启用多个这些设置，则第一个到期的超时间隔将关闭用户设备连接。

您可以通过配置全局设置或使用会话配置文件来配置超时设置。当您将会话配置文件添加到会话策略时，该策略将绑定到用户、组或虚拟服务器。当您全局配置超时设置时，这些设置将应用于所有用户会话。

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

注意：

- 在 Always On（服务模式或用户模式）中，VPN 客户端会忽略所有超时。强制超时和会话超时决策发生在 NetScaler 设备上，因此这些超时按预期工作。如果发生此类超时，VPN 插件会尝试执行自动身份验证。

  在 Always On 中，由于用户设备必须始终通过 VPN 隧道连接，因此请勿配置强制超时或客户端空闲超时。但是，可以配置会话超时以清除陈旧会话。
- 某些应用程序（例如 Microsoft Outlook）会自动向电子邮件服务器发送网络流量探测，无需任何用户干预。Citrix® 建议您将空闲会话超时与会话超时一起配置，以确保用户设备上无人看管的会话在合理的时间内超时。

配置强制超时

强制超时会在指定分钟数后自动断开 Citrix Secure Access 客户端的连接。您可以全局配置强制超时，也可以将其作为会话策略的一部分进行配置。

配置全局强制超时

1. 在配置实用程序中，在“**配置**”选项卡上，在导航窗格中，展开 NetScaler Gateway，然后单击“**全局设置**”。
2. 在详细信息窗格中，在“**设置**”下，单击“**更改全局设置**”。
3. 在“**网络配置**”选项卡上，单击“**高级设置**”。
4. 在“强制超时（分钟）”中，键入用户可以保持连接的分钟数。
5. 在“强制超时警告（分钟）”中，键入在连接即将断开之前警告用户的分钟数，然后单击“**确定**”。

在会话策略中配置强制超时

如果您想进一步控制谁接收强制超时，请创建会话策略，然后将策略应用于用户或组。

1. 在配置实用程序中，在“**配置**”选项卡上，在导航窗格中，展开“**NetScaler Gateway**”>“**策略**”，然后单击“**会话**”。
2. 在详细信息窗格中，单击“**添加**”。
3. 在“名称”中，键入策略的名称。
4. 在“请求配置文件”旁边，单击“**新建**”。
5. 在“名称”中，键入配置文件的名称。
6. 在“**网络配置**”选项卡上，单击“**高级**”。

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

7. 在“超时”下，单击“**覆盖全局**”，并在“强制超时（分钟）”中键入用户可以保持连接的分钟数。
8. 在“**强制超时警告（分钟）**”旁边，单击“**覆盖全局**”，并键入在连接即将断开之前警告用户的分钟数。单击两次“**确定**”。
9. 在 **创建会话策略** 对话框中，在 **命名表达式** 旁边，选择“常规”，选择 **True 值**，单击 **添加表达式**，单击 **创建**，然后单击 **关闭**。

配置会话或空闲超时

您可以使用 NetScaler GUI 全局配置会话和客户端超时设置，或创建会话策略。创建会话策略和配置文件时，将表达式设置为 True。

注意：

如果您未明确覆盖全局设置并在 **客户端体验 > 会话超时（分钟）** 中设置会话超时，这可能会导致需要重新登录的身份验证循环。即使默认会话超时为 30 分钟，也会发生这种情况。

使用 GUI 全局配置会话或客户端空闲超时

1. 在 **配置** 选项卡上的导航窗格中，展开 **NetScaler Gateway**，然后单击 **全局设置**。
2. 在详细信息窗格中，在 **设置** 下，单击 **更改全局设置**。
3. 在 **客户端体验** 选项卡上，执行以下一项或两项操作：
   - 在 **会话超时（分钟）** 中，键入分钟数。
   - 在 **客户端空闲超时（分钟）** 中，键入分钟数，然后单击 **确定**。

使用 GUI 通过会话策略配置会话或客户端空闲超时设置

1. 在 **配置** 选项卡上的导航窗格中，展开 **NetScaler Gateway** > **策略**，然后单击 **会话**
2. 在 **NetScaler Gateway 会话策略和配置文件** 页面中，单击 **会话配置文件**，然后单击 **添加**。
3. 在“名称”中，键入配置文件的名称。
4. 在“**客户端体验**”选项卡上，执行以下一项或两项操作：
   - 在“**会话超时（分钟）**”旁边，单击“**覆盖全局**”，然后键入分钟数，再单击“**创建**”。
   - 在“**客户端空闲超时（分钟）**”旁边，单击“**覆盖全局**”，键入分钟数，然后单击“**创建**”。
5. a. 在“**NetScaler Gateway 会话策略和配置文件**”页面中，单击“**会话策略**”，然后单击“**添加**”。
6. 在“**创建 NetScaler Gateway 会话策略**”中，
   - 在“**名称**”中，输入策略的名称。

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

- 在“**配置文件**”中，选择一个配置文件，该配置文件指定如果满足规则条件，新会话策略将应用的操作。
- 选择“**高级策略**”。
- 在“**表达式**”字段中，添加您的表达式或命名表达式的名称，指定与策略匹配的流量。
- 单击“**创建**”，然后单击“**关闭**”。

连接到内部网络资源

您可以配置 NetScaler Gateway 以允许用户访问内部网络中的资源。如果禁用拆分隧道，则来自用户设备的所有网络流量都将发送到 NetScaler Gateway，并且授权策略将确定是否允许流量通过到内部网络资源。启用拆分隧道后，只有目标为内部网络的流量才会被用户设备拦截并发送到 NetScaler Gateway。您可以使用内网应用程序配置 NetScaler Gateway 拦截的 IP 地址。

如果您使用的是 Citrix Secure Access™ 客户端 for Windows，请将拦截模式设置为透明。如果您使用的是 Citrix Secure Access 客户端 for Java，请将拦截模式设置为代理。当您将拦截模式设置为透明时，您可以使用以下方式允许访问网络资源：

- 单个 IP 地址和子网掩码
- IP 地址范围

如果将拦截模式设置为代理，则可以配置目标和源 IP 地址以及端口号。

配置对内部网络资源的访问

1. 在配置实用程序中，在**配置**选项卡上的导航窗格中，展开 NetScaler Gateway，展开“资源”，然后单击**内网应用程序**。
2. 在详细信息窗格中，单击**添加**。
3. 完成允许网络访问的参数，单击**创建**，然后单击**关闭**。

配置拆分隧道

您可以启用拆分隧道，以防止 Citrix Secure Access 客户端向 NetScaler Gateway 发送不必要的网络流量。

如果不启用拆分隧道，Citrix Secure Access 客户端会捕获源自用户设备的所有网络流量，并通过 VPN 隧道将流量发送到 NetScaler Gateway。

如果启用拆分隧道，Citrix Secure Access 客户端将仅通过 VPN 隧道发送目标为受 NetScaler Gateway 保护的网络流量。Citrix Secure Access 客户端不会将目标为未受保护网络的网络流量发送到 NetScaler Gateway。

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

Citrix Secure Access 客户端启动时，它会从 NetScaler Gateway 获取内部网应用程序列表。Citrix Secure Access 客户端会检查从用户设备在网络上传输的所有数据包，并将数据包中的地址与内部网应用程序列表进行比较。如果数据包中的目标地址在某个内部网应用程序中，Citrix Secure Access 客户端会通过 VPN 隧道将数据包发送到 NetScaler Gateway。如果目标地址不在定义的内部网应用程序中，则数据包不会加密，用户设备会适当地路由数据包。启用拆分隧道时，内部网应用程序定义了要拦截的网络流量。

注意：

如果用户使用 Citrix Workspace 应用程序连接到服务器场中已发布的应用程序，则无需配置拆分隧道。

NetScaler Gateway 还支持反向拆分隧道，它定义了 NetScaler Gateway 不拦截的网络流量。如果将拆分隧道设置为反向，则内部网应用程序定义了 NetScaler Gateway 不拦截的网络流量。启用反向拆分隧道时，所有指向内部 IP 地址的网络流量都将绕过 VPN 隧道，而其他流量则通过 NetScaler Gateway。反向拆分隧道可用于记录所有非本地 LAN 流量。例如，如果用户拥有家庭无线网络并使用 Citrix Secure Access 客户端登录，NetScaler Gateway 不会拦截目标为无线网络中打印机或其他设备的网络流量。

有关内部网应用程序的更多信息，请参阅配置客户端拦截。

您可以将拆分隧道配置为会话策略的一部分。

配置拆分隧道

1. 在配置实用程序中，在“配置”选项卡上的导航窗格中，展开 **NetScaler Gateway 策略**，然后单击**会话**。
2. 在详细信息窗格中，在**配置文件**选项卡上，选择一个配置文件，然后单击**打开**。
3. 在**客户端体验**选项卡上，在**拆分隧道**旁边，选择**全局覆盖**，选择一个选项，然后单击两次**确定**。

配置拆分隧道和授权

在规划 NetScaler Gateway 部署时，务必考虑分流隧道、默认授权操作和授权策略。

例如，您有一个允许访问网络资源的授权策略。您将分流隧道设置为“开”，并且未配置内部网应用程序通过 NetScaler Gateway 发送网络流量。当 NetScaler Gateway 具有此类配置时，允许访问资源，但用户无法访问该资源。

如果授权策略拒绝访问网络资源，并且您将分流隧道设置为“开”，同时内部网应用程序配置为通过 NetScaler Gateway 路由网络流量，则 Citrix Secure Access 客户端会将流量发送到 NetScaler Gateway，但对资源的访问将被拒绝。

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

有关分流隧道选项的更多信息，请参阅 分流隧道选项。

配置客户端拦截

您可以使用内网应用程序在 NetScaler Gateway 上为用户连接配置拦截规则。默认情况下，当您在设备上配置系统 IP 地址、映射 IP 地址或子网 IP 地址时，会根据这些 IP 地址创建子网路由。内网应用程序会根据这些路由自动创建，并可以绑定到虚拟服务器。如果启用分流隧道，则必须定义内网应用程序才能进行客户端拦截。

您可以使用 GUI 配置内网应用程序。您可以将内网应用程序绑定到用户、组或虚拟服务器。

如果启用分流隧道并且用户使用 WorxWeb 或 WorxMail 进行连接，则在配置客户端拦截时，必须添加 Citrix Endpoint Management™ 和 Exchange 服务器的 IP 地址。如果您未启用分流隧道，则无需在内网应用程序中配置 Endpoint Management 和 Exchange IP 地址。

有关分流隧道配置的信息，请参阅 (/zh-cn/netscaler-gateway/current-release/vpn-user-config/configure-full-vpn-setup.html#configure-split-tunneling)。

为 Citrix Secure Access™ 客户端配置内网应用程序

您可以通过定义以下内容来创建用于用户访问资源的内网应用程序：

- 一个 IP 地址
- 一个 IP 地址范围
- 一个主机名

当您在 NetScaler Gateway 上定义内网应用程序时，适用于 Windows 的 Citrix Secure Access 客户端会拦截目标为该资源的用户流量，并通过 NetScaler Gateway 发送该流量。

配置内网应用程序时，请考虑以下事项：

- 当分流隧道开启时，
  - 配置内网应用程序。
  - 将内网应用程序分配给每个身份验证、授权和审计组。
- 当分流隧道为“关闭”时，
  - 所有流量都通过 VPN 隧道进行拦截。
  - 无需配置内部网应用程序。
- 当分流隧道为“反向”时，

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

- 配置内部网应用程序。未由内部网应用程序指定的流量将通过 VPN 隧道。
- 将要从 VPN 中排除的内部网应用程序分配给每个身份验证、授权和审计组。

重要提示：

无论分流隧道配置如何，拦截都必须设置为 **TRANSPARENT**。

注意：

- 配置内部网应用程序时，必须选择与用于建立连接的插件软件类型相对应的拦截模式。
- 您不能为代理拦截和透明拦截同时配置内部网应用程序。

为一个 IP 地址创建内部网应用程序

1. 在“配置”选项卡上的导航窗格中，展开 **NetScaler Gateway Resources**，然后单击 **Intranet Applications**。
2. 在详细信息窗格中，单击 **Add**。
3. 在“名称”中，键入配置文件的名称。
4. 在**创建内网应用程序**对话框中，选择**透明**。
5. 在**目标类型**中，选择**IP 地址**和**子网掩码**。
6. 在“协议”中，选择适用于网络资源的协议。
7. 在**IP 地址**中，键入 IP 地址。
8. 在**子网掩码**中，键入子网掩码，单击**创建**，然后单击**关闭**。

配置 IP 地址范围

如果您的网络中有多个服务器，例如 Web、电子邮件和文件共享服务器，您可以配置一个网络资源，其中包含网络资源的 IP 范围。此设置允许用户访问 IP 地址范围中包含的网络资源。

1. 在**配置**选项卡上的导航窗格中，展开**NetScaler Gateway 资源**，然后单击**内网应用程序**。
2. 在详细信息窗格中，单击**添加**。
3. 在**名称**中，键入配置文件的名称。
4. 在“协议”中，选择适用于网络资源的协议。
5. 在**创建内网应用程序**对话框中，选择**透明**。
6. 在**目标类型**中，选择**IP 地址范围**。
7. 在**起始 IP**中，键入起始 IP 地址；在 IP 结束中，键入结束 IP 地址，单击**创建**，然后单击**关闭**。

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

为主机名创建内网应用程序

1. 在“配置”选项卡上，在导航窗格中，展开“**NetScaler Gateway 资源**”，然后单击“**内网应用程序**”。
2. 在详细信息窗格中，单击“**添加**”。
3. 在“**名称**”中，键入配置文件的名称。
4. 在“**创建内网应用程序**”对话框中，选择“**透明**”。
5. 在“**目标类型**”中，选择“**主机名**”。
6. 在“协议”中，选择“**任意**”，单击“**创建**”，然后单击“**关闭**”。

重要提示：

- 从版本 13.0 build 36.27 及更高版本开始，Windows VPN 插件支持基于主机名 (FQDN) 的拆分隧道规则。您必须将 NetScaler 设备和 Windows VPN 插件都升级到版本 13.0 build 36.27 或更高版本。
- 还支持通配符主机名。例如，如果配置了主机名为“*.example.com”的内网应用程序，则 `a1.example.com`、`b2.example.com` 等将通过隧道传输。
- 仅当您将拆分隧道设置为“开”或“反向”时，基于主机名的内网应用程序才有效。

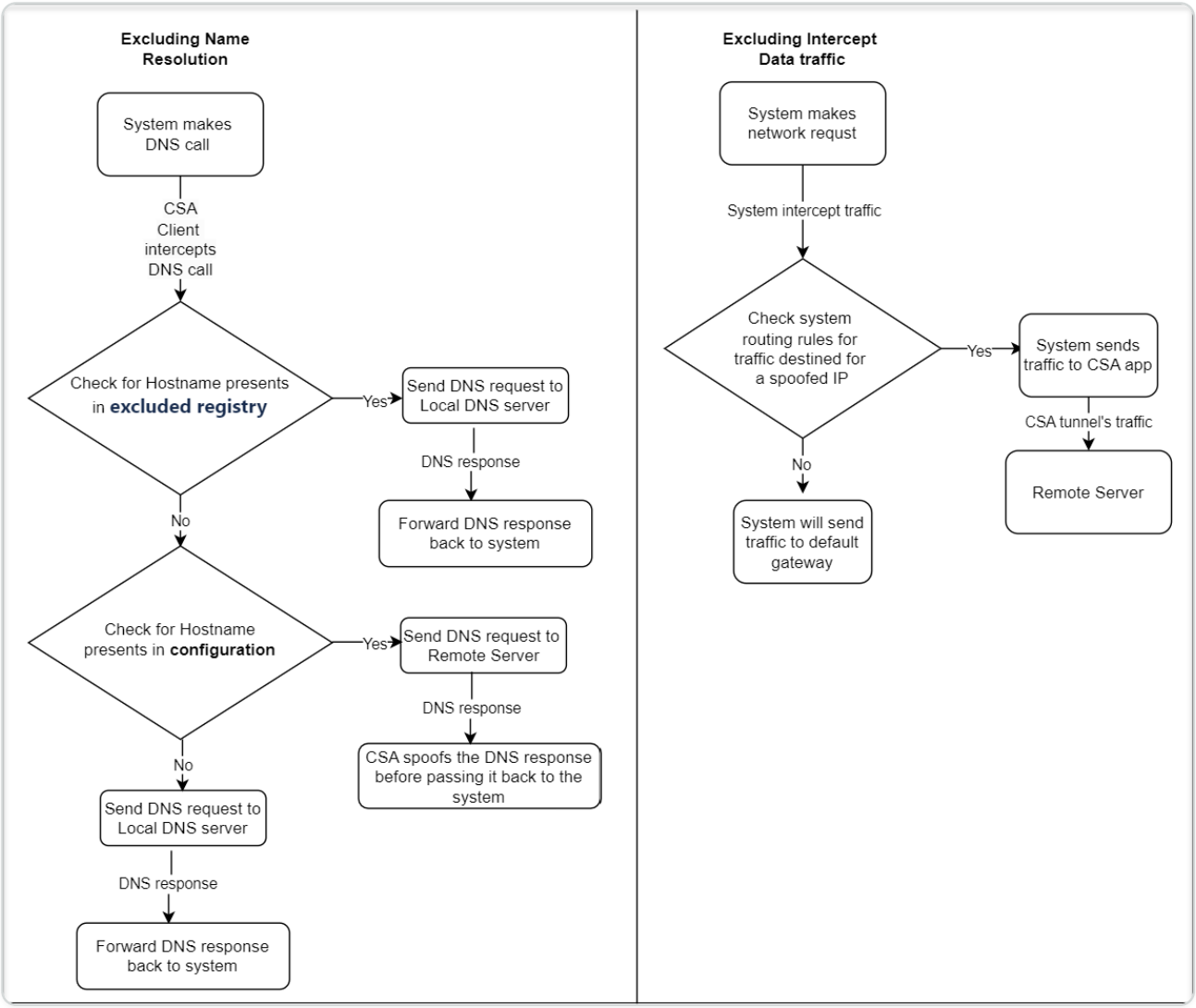
从客户端拦截中排除特定域流量

Citrix Secure Access 客户端拦截并隧道传输基于主机名的应用程序。例如，如果为基于主机名的应用程序 `*.example.com` 配置了客户端拦截，则 Citrix Secure Access 客户端会拦截所有以 `example.com` 结尾的基于主机名的应用程序访问。

从适用于 Windows 的 Citrix Secure Access 客户端版本 24.8.1.15 和适用于 macOS/iOS 的版本 24.10.1 开始，您可以从客户端拦截和隧道传输中排除某些子域。例如，要排除 `rdp.example.com` 和 `ftp.example.com`，请在排除参数中定义这些域。Citrix Secure Access 客户端会绕过这些域的 DNS 调用，并将其发送到本地 DNS 服务器，而不是远程 DNS 服务器。它不会拦截或隧道传输这些子域的流量。

下图说明了 Citrix Secure Access 客户端排除 DNS 解析和客户端拦截的过程。

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



重要：

- 对于适用于 Windows 的 Citrix Secure Access 客户端，您只能通过 NetScaler® Gateway 中的注册表来配置客户端拦截排除项，而在 Secure Private Access 中，则可以使用注册表和 UI 两种方式。
- 对于适用于 macOS/iOS 的 Citrix Secure Access 客户端，您只能使用 Secure Private Access UI 来配置客户端拦截排除项。

使用注册表配置客户端拦截排除项

1. 在最终用户设备上配置 `ExcludeDomainsFromRemoteDns` 注册表，以排除 Citrix Secure Access 客户端通过远程 DNS 服务器执行 DNS 解析。有关详细信息，请参阅 NetScaler Gateway Windows VPN 客户端注册表项。

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

2. 在最终用户设备上配置 `ExcludeDomainsFromTunnel` 注册表，以排除 Citrix Secure Access 客户端对流量进行隧道传输。有关详细信息，请参阅 NetScaler Gateway Windows VPN 客户端注册表项。

在 Secure Private Access 管理控制台中配置客户端拦截排除项

有关在 Secure Private Access 服务控制台中配置 TCP/UDP 应用程序的详细信息，请参阅 支持 TCP/UDP 应用程序。

> **注意：**
>
> 对于客户端拦截排除项，路由类型必须为 **External**。

配置名称服务解析

在安装 NetScaler Gateway 期间，您可以使用 NetScaler Gateway 向导配置其他设置，包括名称服务提供程序。名称服务提供程序将完全限定域名 (FQDN) 转换为 IP 地址。在 NetScaler Gateway 向导中，您可以配置 DNS 或 WINS 服务器，设置 DNS 查找的优先级，以及重试连接到服务器的次数。

运行 NetScaler Gateway 向导时，您可以添加 DNS 服务器。您可以使用会话配置文件向 NetScaler Gateway 添加更多 DNS 服务器和 WINS 服务器。然后，您可以引导用户和组连接到与您最初使用向导配置的名称解析服务器不同的服务器。

在 NetScaler Gateway 上配置额外的 DNS 服务器之前，请创建一个充当 DNS 服务器的虚拟服务器以进行名称解析。

在会话配置文件中添加 DNS 或 WINS 服务器

1. 在配置实用程序中，在“**配置**”选项卡上的导航窗格中，展开“**NetScaler Gateway 策略**”，然后单击“**会话**”。
2. 在详细信息窗格中，在“配置文件”选项卡上，选择一个配置文件，然后单击“打开”。
3. 在“网络配置”选项卡上，执行以下操作之一：
   - 要配置 DNS 服务器，请在“DNS 虚拟服务器”旁边，单击“**覆盖全局**”，选择服务器，然后单击“**确定**”。
   - 要配置 WINS 服务器，请在“WINS 服务器 IP”旁边，单击“**覆盖全局**”，键入 IP 地址，然后单击“**确定**”。

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

重要提示：

对于附加到 VPN 会话配置文件的不可寻址 DNS 虚拟服务器，不会评估响应程序策略。

启用用户连接的代理支持

用户设备可以通过代理服务器连接以访问内部网络。NetScaler Gateway 支持 HTTP、SSL、FTP 和 SOCKS 协议。要启用用户连接的代理支持，您需要在 NetScaler Gateway 上指定设置。您可以在 NetScaler Gateway 上指定代理服务器使用的 IP 地址和端口。代理服务器用作所有后续内部网络连接的正向代理。

代理设置

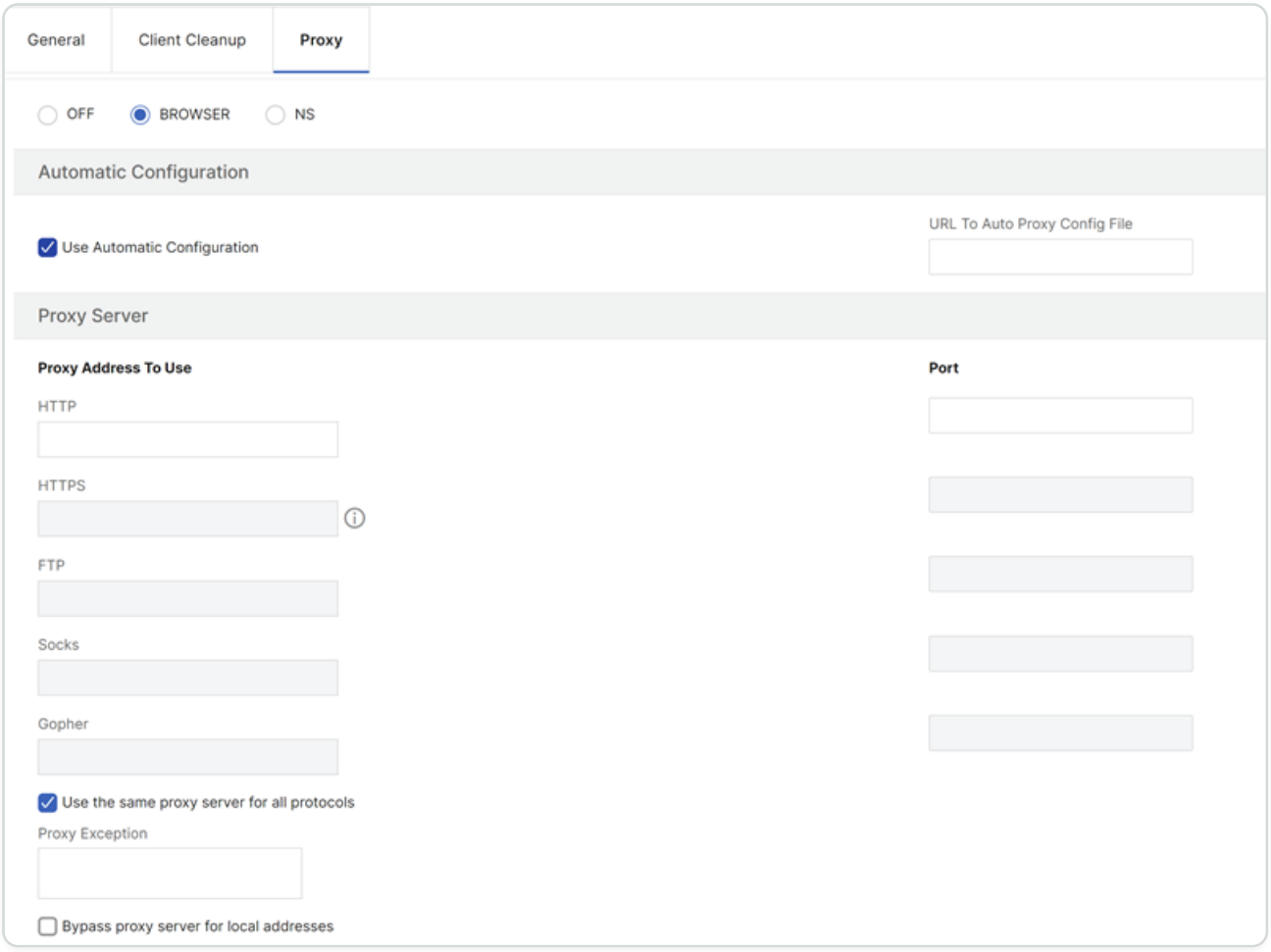
您可以在浏览器或 NetScaler 设备上配置代理设置。要在浏览器或设备上配置代理设置，请导航到 **NetScaler Gateway > 全局设置 > 更改全局 NetScaler Gateway 设置 > 客户端体验选项卡 > 高级设置 > 代理**，然后根据需要选择 **浏览器** 或 **NS**。

- **浏览器**：当您选择在浏览器上配置代理设置时，可以通过提供自动代理配置文件链接来使用自动配置选项。自动配置可能会覆盖手动设置。

  此外，当您选择 **浏览器** 时，可以通过选择代理例外选项来绕过以前配置的代理。

  注意：不同类型的客户端在 **浏览器** 代理配置方面具有不同的功能。有关详细信息，请参阅 NetScaler Gateway VPN 客户端和支持的功能。
- **NS**：如果您在 NetScaler 设备上配置代理设置，则无法使用自动配置选项。在设备上配置代理设置时，您无法绕过以前配置的代理。
- **关闭**：选择此选项后，NetScaler Gateway 将禁用 VPN 插件中的代理设置。

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



配置用户连接的代理支持

1. 在导航窗格中，展开 **NetScaler Gateway**，然后单击 **全局设置**。
2. 在详细信息窗格中，在 **设置** 下，单击“更改全局设置”。
3. 在“客户端体验”选项卡上，单击 **高级设置**。
4. 在 **代理** 选项卡上，在 **代理设置** 下，选择 **浏览器**。
5. 对于协议，输入 IP 地址和端口号，然后点击 **确定**。

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

注意：

- 如果您选择 **NS**，则只能配置支持安全和不安全 HTTP 连接的代理服务器。
- 在 NetScaler Gateway 上启用代理支持后，您需要在用户设备上为与协议对应的代理服务器指定配置详细信息。

  启用代理支持后，NetScaler Gateway 会将代理服务器详细信息发送到客户端 Web 浏览器，并更改浏览器上的代理配置。

  - 当用户设备连接到 NetScaler Gateway 时，用户设备可以直接与代理服务器通信，以连接到用户网络。
  - 当用户设备与 NetScaler Gateway 断开连接时，代理设置将恢复到连接 VPN 插件之前的默认设置。

为 NetScaler Gateway 配置一个代理服务器以使用所有协议

您可以配置一个代理服务器来支持 NetScaler Gateway 使用的所有协议。此设置提供一个 IP 地址和端口组合，适用于所有协议。

1. 在导航窗格中，展开 **NetScaler Gateway**，然后点击 **全局设置**。
2. 在详细信息窗格中，在 **设置** 下，点击“更改全局设置”。
3. 在 **客户端体验** 选项卡上，点击 **高级设置**。
4. 在 **代理** 选项卡上，在 **代理设置** 下，选择 **浏览器**。
5. 对于协议，输入 IP 地址和端口号。
6. 点击“对所有协议使用相同的代理服务器”，然后点击 **确定**。

当您禁用拆分隧道并将所有代理设置设为“开”时，代理设置会传播到用户设备。如果代理设置设为“设备”，这些设置不会传播到用户设备。

NetScaler Gateway 代表用户设备连接到代理服务器。代理设置不会传播到用户的浏览器，因此用户设备与代理服务器之间无法直接通信。

将 NetScaler Gateway 配置为代理服务器

当您将 NetScaler Gateway 配置为代理服务器时，仅支持不安全的 HTTP 和安全的 HTTP 协议。

1. 在导航窗格中，展开 **NetScaler Gateway**，然后单击 **全局设置**。
2. 在详细信息窗格中，在 **设置** 下，单击“更改全局设置”。

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

3. 在 **客户端体验** 选项卡上，单击 **高级设置**。
4. 在 **代理** 选项卡上，在 **代理设置** 下，选择 **NS**。
5. 对于协议，键入 IP 地址和端口号，然后单击 **确定**。

配置地址池

在某些情况下，使用 Citrix Secure Access 客户端连接的用户需要一个唯一的 IP 地址才能访问 NetScaler Gateway。例如，在 Samba 环境中，每个连接到映射网络驱动器的用户都需要看起来源自不同的 IP 地址。当您为某个组启用地址池（也称为 IP 池）时，NetScaler Gateway 可以为每个用户分配一个唯一的 IP 地址别名。

您可以使用内网 IP 地址配置地址池。以下类型的应用程序可能需要使用从 IP 池中获取的唯一 IP 地址：

- IP 语音 (VoIP)
- 主动 FTP
- 即时消息
- 安全外壳 (SSH)
- 虚拟网络计算 (VNC) 连接到计算机桌面
- 远程桌面 (RDP) 连接到客户端桌面

您可以配置 NetScaler Gateway，为连接到 NetScaler Gateway 的用户分配内部 IP 地址。静态 IP 地址可以分配给用户，或者可以将一系列 IP 地址分配给组、虚拟服务器或全局系统。

NetScaler Gateway 允许您将内部网络中的 IP 地址分配给远程用户。内部网络上的 IP 地址可以寻址远程用户。如果您选择使用一系列 IP 地址，系统会根据需要动态地从该范围内为远程用户分配一个 IP 地址。

配置地址池时，请注意以下事项：

- 分配的 IP 地址必须正确路由。为确保正确路由，请考虑以下事项：
  - 如果未启用拆分隧道，请确保 IP 地址可以通过网络地址转换 (NAT) 设备进行路由。
  - 通过使用内网 IP 地址的用户连接访问的任何服务器都必须配置正确的网关才能访问这些网络。
  - 在 NetScaler Gateway 上配置网关或静态路由，以便将来自用户软件的网络流量路由到内部网络。

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

- 分配 IP 地址范围时，只能使用连续的子网掩码。范围的子集可以分配给较低级别的实体。例如，如果 IP 地址范围绑定到虚拟服务器，则将该范围的子集绑定到组。
- IP 地址范围不能在绑定级别内绑定到多个实体。例如，绑定到组的地址范围的子集不能绑定到第二个组。
- NetScaler Gateway 不允许您在 IP 地址被用户会话主动使用时将其删除或解除绑定。
- 内部网络 IP 地址通过以下层次结构分配给用户：
  - 用户的直接绑定
  - 组分配的地址池
  - 虚拟服务器分配的地址池
  - 全局地址范围
- 分配地址范围时只能使用连续的子网掩码。但是，已分配范围的子集可以进一步分配给较低级别的实体。 绑定的全局地址范围可以绑定到以下各项：
  - 虚拟服务器
  - 组
  - 用户
- 绑定的虚拟服务器地址范围可以有子集绑定到以下各项：
  - 组
  - 用户

绑定的组地址范围可以有一个子集绑定到用户。

当 IP 地址分配给用户时，该地址会为用户的下次登录保留，直到地址池范围耗尽。当地址耗尽时，NetScaler Gateway 会从离开 NetScaler Gateway 时间最长的用户那里收回 IP 地址。

如果无法收回地址且所有地址都在活动使用中，NetScaler Gateway 将不允许用户登录。您可以通过允许 NetScaler Gateway 在所有其他 IP 地址不可用时使用映射的 IP 地址作为内部网 IP 地址来防止这种情况发生。

内部网 IP DNS 注册

如果为客户端计算机分配了内部网 IP，并且在 VIP 隧道建立后，VPN 插件会检查该客户端计算机是否已加入域。如果客户端计算机是已加入域的计算机，VPN 插件会启动 DNS 注册过程，将计算机的主机名内部网与分配的内部网 IP 地址关联起来。此注册会在隧道解除建立之前恢复。

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

为了成功进行 DNS 注册，请确保设置了以下 `nsapimgr` 旋钮。此外，请确保将权威 DNS 服务器设置为允许“非安全”DNS 更新。

- **`nsapimgr` -ys enable_vpn_dns_override=1**：此标志与其它配置参数一起发送到 NetScaler Gateway VPN 客户端。如果此标志未设置，并且当 VPN 客户端拦截到 DNS/WINS 请求时，它会通过隧道向 NetScaler Gateway 虚拟服务器发送相应的“GET /DNS”HTTP 请求以获取解析的 IP 地址。但是，如果设置了 'enable_vpn_dnstruncate_fix' 标志，VPN 客户端会将 DNS/WINS 请求透明地转发到 NetScaler Gateway 虚拟服务器。在这种情况下，DNS 数据包会原样通过 VPN 隧道发送到 NetScaler Gateway 虚拟服务器。这有助于解决从 NetScaler Gateway 中配置的名称服务器返回的 DNS 记录过大而无法容纳在 UPD 响应数据包中的情况。在这种情况下，当客户端回退到使用 TCP-DNS 时，此 TCP-DNS 数据包会原样到达 NetScaler Gateway 服务器，因此 NetScaler Gateway 服务器会向 DNS 服务器发出 TCP-DNS 查询。
- **nsapimgr -ys enable_vpn_dnstruncate_fix=1**：此标志由 NetScaler Gateway 服务器本身使用。如果设置了此标志，NetScaler Gateway 会将“DNS 端口上的 TCP 连接”的目标覆盖为 NetScaler Gateway 上配置的 DNS 服务器（而不是尝试将它们发送到传入 TCP-DNS 数据包中最初存在的 DNS 服务器 IP）。对于 UDP DNS 请求，默认是使用配置的 DNS 服务器进行 DNS 解析。适用于 Windows 的 NetScaler Gateway 插件支持安全和非安全 DNS 更新。安全 DNS 更新支持在 21.7.1.1 或更高版本中默认存在。

  Windows 插件上的安全 DNS 更新默认禁用。要启用它，请在 `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access` 中创建一个 REG_DWORD 类型的值并将其设置为 1。

  - 当您将值设置为 1 时，VPN 插件会首先尝试不安全的 DNS 更新。如果不安全的 DNS 更新失败，VPN 插件会尝试安全的 DNS 更新。
  - 要仅尝试安全的 DNS 更新，您可以将值设置为 2。

有关设置这些旋钮的更多信息，请参阅 `<https://support.citrix.com/article/CTX200243>` 。

使用 GUI 为用户、组或虚拟服务器配置地址池

1. 导航到 **Configuration** > **NetScaler® Gateway**，然后执行以下操作之一：
   - 导航到 **NetScaler Gateway** > **用户管理**，然后单击 **AAA 用户**。
   - 导航到 **NetScaler Gateway** > **用户管理**，然后单击 **AAA 组**。
   - 展开 **NetScaler Gateway**，然后单击 **虚拟服务器**。
2. 在详细信息窗格中，单击用户、组或虚拟服务器，然后单击 **打开**。

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

3. 在 **内网 IP** 选项卡上的 **IP 地址** 和 **子网掩码** 文本框中，键入 IP 地址和子网掩码，然后单击 **添加**。
4. 对要添加到池中的每个 IP 地址重复步骤 3，然后单击 **确定**。

使用 GUI 全局配置地址池

1. 导航到 **配置** > **NetScaler Gateway** > **全局设置**。
2. 在详细信息窗格中，在 **内网 IP** 下，单击 **要为所有客户端 NetScaler Gateway 会话分配唯一、静态的 IP 地址或 IP 地址池，请配置内网 IP**。
3. 在 **绑定内网 IP** 对话框中，单击 **操作**，然后单击 **插入**。
4. 在 **IP 地址** 和 **子网掩码** 文本框中，键入 IP 地址和子网掩码，然后单击 **添加**。
5. 对要添加到池中的每个 IP 地址重复步骤 3 和 4，然后单击 **确定**。

使用 CLI 配置地址池

1. 运行以下命令之一来配置地址池：
   - **对于 AAA 用户：** `bind aaa user <username> -intranetIP <ip_address> <netmask>`
   - **对于 AAA 组：** `bind aaa group <groupname> -intranetIP <ip_address> <netmask>`
   - **对于 VPN 虚拟服务器：** `bind vpn vserver <vservername> -intranetIP <ip_address> -netmask <netmask>`
   - **对于 VPN 全局：** `bind vpn global -intranetIP <ip_address> -netmask <netmask>`
2. 运行以下命令以设置可分配给用户的内部网 IP 地址的最大数量限制：

   `set vpn parameter -maxIIPperUser <number>`

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

注意：

- `maxIIPperUser` 的最小值为 1，最大值为 10。
- 如果未设置 `maxIIPperUser` 参数，则默认情况下分配给用户的内部网 IP 地址数量为 1。
- `maxIIPperUser` 配置仅适用于在 AAA 组、VPN 虚拟服务器或 VPN 全局级别配置的内部网 IP 地址。在 AAA 用户级别配置的内部网 IP 地址不受此配置的影响。
- 增加或减少 `maxIIPPerUser` 限制不会影响现有会话或已分配的内部网 IP 地址数量。现有会话将保持活动状态，直到会话/空闲超时或管理员干预。但是，此配置会立即对新会话生效。

定义地址池选项

您可以使用会话策略或全局 NetScaler Gateway 设置来控制在用户会话期间是否分配内部网 IP 地址。定义地址池选项允许您将内部网 IP 地址分配给 NetScaler Gateway，同时禁用特定用户组使用内部网 IP 地址。

您可以通过以下三种方式之一使用会话策略配置地址池：

- **`Nospillover`** - 当您为内部网 IP 地址配置地址池时，您将获得一个会话，其中包含池中可用的 IP。对于已用完所有可用内部网 IP 地址的用户，将显示“传输登录”页面。
- **溢出** - 当您配置地址池并将映射的 IP 用作内部网 IP 地址时，映射的 IP 地址将用于已用完所有可用内部网 IP 地址的用户。
- **关闭** - 地址池未配置。

注意：

如果未配置映射的 IP 地址，则使用 SNIP。

定义地址池

1. 在配置实用程序中，在“**配置**”选项卡上，在导航窗格中，展开“**NetScaler Gateway > 策略**”，然后单击“**会话**”。
2. 在详细信息窗格中，在“**策略**”选项卡上，单击“**添加**”。
3. 在“**名称**”中，键入策略的名称。
4. 在“**请求配置文件**”旁边，单击“**新建**”。

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

5. 在“名称”中，键入配置文件的名称。
6. 在“**网络配置**”选项卡上，单击“**高级**”。
7. 在“内网 IP”旁边，单击“**覆盖全局**”，然后选择一个选项。
8. 如果在步骤 9 中选择“**溢出**”，请在“映射的 IP”旁边，单击“**覆盖全局**”，选择设备的主机名，单击“**确定**”，然后单击“**创建**”。
9. 在“**创建会话策略**”对话框中，创建表达式。单击“**创建**”，然后单击“**关闭**”。

配置传输登录页面

如果用户没有可用的内网 IP 地址，然后尝试与 NetScaler Gateway 建立另一个会话，则会出现“传输登录”页面。传输登录页面允许用户将其现有的 NetScaler Gateway 会话替换为新会话。

如果注销请求丢失或用户未执行干净注销，也可以使用传输登录页面。例如：

- 如果用户被分配了一个静态内网 IP 地址并拥有一个现有的 NetScaler Gateway 会话。如果用户尝试从不同的设备建立第二个会话，则会出现传输登录页面，用户可以将该会话传输到新设备。
- 如果用户被分配了五个内网 IP 地址并通过 NetScaler Gateway 拥有五个会话。如果用户尝试建立第六个会话，则会出现传输登录页面，用户可以选择用新会话替换现有会话。

注意：

- 如果用户没有可用的已分配 IP 地址，导致无法建立新会话，则会出现错误消息。
- Citrix Secure Access for Android 23.12.1 及更高版本在 Always On VPN 模式下支持 NetScaler Gateway 的传输登录功能。

传输登录页面仅在您配置地址池并禁用溢出时才会出现。

配置 DNS 后缀

当用户登录 NetScaler Gateway 并被分配 IP 地址时，用户名称和 IP 地址组合的 DNS 记录会添加到 NetScaler Gateway DNS 缓存中。您可以配置一个 DNS 后缀，以便在 DNS 记录添加到缓存时附加到用户名称。这允许用户通过 DNS 名称进行引用，这比 IP 地址更容易记住。当用户从 NetScaler Gateway 注销时，该记录将从 DNS 缓存中删除。

配置 DNS 后缀

1. 在配置实用程序中，在**配置**选项卡上的导航窗格中，展开 **NetScaler Gateway > 策略**，然后单击**会话**。
2. 在详细信息窗格中，在**策略**选项卡上，选择一个会话策略，然后单击**打开**。

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

3. 在“请求配置文件”旁边，单击**修改**。
4. 在**网络配置**选项卡上，单击**高级**。
5. 在“内网 IP DNS 后缀”旁边，单击**覆盖全局**，键入 DNS 后缀，然后单击三次**确定**。

支持 VoIP 电话

当您将 NetScaler Gateway 作为独立设备安装并且用户使用 Citrix Secure Access 客户端连接时，NetScaler Gateway 支持与 IP 语音 (VoIP) 软电话进行双向通信。

以下是 Citrix Secure Access™ 支持的一些 VoIP 软电话：

- Cisco 软电话
- Avaya IP 软电话

IP PBX 与用户设备上运行的软电话软件之间支持安全隧道。要使 VoIP 流量通过安全隧道，您必须在同一用户设备上安装 Citrix Secure Access 客户端和其中一个受支持的软电话。

当 VoIP 流量通过安全隧道发送时，Citrix Secure Access 支持以下软电话功能：

- 从 IP 软电话拨打的呼出电话
- 拨打到 IP 软电话的呼入电话
- 双向语音流量
- 与 VoIP 应用程序的 TCP 和 UDP 控制流

注意：

对于使用 DNE 的 UDP 控制流，如果非活动持续时间为 30 秒或更长，VoIP 应用程序将断开连接。因此，如果 VoIP 应用程序支持 UDP 控制消息传递并且您遇到任何问题，我们建议您在 WFP 模式下使用 Citrix Secure Access。

VoIP 软电话的支持通过使用内网 IP 地址进行配置。您必须为每个用户配置一个内网 IP 地址。如果您使用的是 Cisco 软电话通信，在配置内网 IP 地址并将其绑定到用户后，无需进行额外配置。有关配置内网 IP 地址的更多信息，请参阅 配置地址池。

如果启用拆分隧道，请创建一个内网应用程序并指定 Avaya 软电话应用程序。此外，您必须启用透明拦截。

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

配置访问界面

NetScaler Gateway 包含一个默认主页，用户登录后会显示该主页。此默认主页称为访问界面。您可以将访问界面用作主页，或将 StoreFront 配置为主页，或自定义主页。

访问界面包含三个面板。如果您的部署中包含 StoreFront™，用户可以登录到访问界面的左侧面板中的 Receiver。如果您的部署中包含 StoreFront，用户无法从左侧面板登录到 Receiver。

访问界面用于提供网站链接（包括内部和外部网站）以及内部网络中文件共享的链接。您可以通过以下方式自定义访问界面：

- 更改访问界面。
- 创建访问界面链接。

用户也可以通过添加自己的网站和文件共享链接来自定义访问界面。用户还可以使用主页将文件从内部网络传输到其设备。

注意：

当用户登录并尝试从访问界面打开文件共享时，文件共享无法打开，用户会收到错误消息“无法建立到服务器的 TCP 连接。”要解决此问题，请配置防火墙，以允许来自 NetScaler Gateway 系统 IP 地址的流量通过 TCP 端口 445 和 139 到达文件服务器 IP 地址。

更改访问界面

您可能希望将用户定向到自定义主页，而不是依赖访问界面。为此，请在 NetScaler Gateway 上安装主页，然后配置会话策略以使用新主页。

安装自定义主页

1. 在配置实用程序中，单击“**配置**”选项卡，然后在导航窗格中，单击“**NetScaler Gateway**”。
2. 在详细信息窗格中，在“**自定义访问界面**”下，单击“**上载**”**访问界面**。
3. 要从网络中计算机上的文件安装主页，请在“本地文件”中，单击“**浏览**”，导航到该文件，然后单击“**选择**”。
4. 要使用安装在 NetScaler Gateway 上的主页，请在“远程路径”中单击“**浏览**”，选择文件，然后单击“**选择**”。
5. 单击“**上传**”，然后单击“**关闭**”。

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

使用自定义主页替换访问界面

您可以使用全局设置或会话策略和配置文件来配置自定义主页以替换默认主页（即访问界面）。配置策略后，您可以将策略绑定到用户、组、虚拟服务器或全局。配置自定义主页后，用户登录时不会显示访问界面。

全局配置自定义主页

1. 在配置实用程序中，在“**配置**”选项卡上，在导航窗格中，展开“**NetScaler Gateway**”，然后单击“**全局设置**”。
2. 在详细信息窗格中，在“**设置**”下，单击“更改全局设置”。
3. 在“**客户端体验**”选项卡上，在“**主页**”中，单击“**显示主页**”，然后输入自定义主页的网址。
4. 单击“**确定**”，然后单击“**关闭**”。

在会话配置文件中配置自定义主页

1. 在配置实用程序中，在“**配置**”选项卡上，在导航窗格中，展开“**NetScaler Gateway 策略**”，然后单击“**会话**”。
2. 在详细信息窗格中，在“**策略**”选项卡上，单击“**添加**”。
3. 在“名称”中，键入策略的名称。
4. 在“**请求配置文件**”旁边，单击“**新建**”。
5. 在“**名称**”中，键入配置文件的名称。
6. 在“**客户端体验**”选项卡上，在“**主页**”旁边，单击“**覆盖全局**”，单击“**显示主页**”，然后键入主页的网址。
7. 在“**创建会话策略**”对话框中，在“**命名表达式**”旁边，选择“**常规**”，选择“True”值，单击“**添加表达式**”，单击“**创建**”，然后单击“**关闭**”。

创建并应用网页链接

您可以配置访问界面以显示一组可供用户使用的内部资源链接。创建这些链接需要您首先将链接定义为资源。然后，将它们绑定到用户、组、虚拟服务器或全局，以使其在访问界面中处于活动状态。您创建的链接将显示在**企业网站**下的**网站**窗格中。

重要提示：

从 NetScaler 13.0 版本 64.xx 及更高版本开始，不再支持通过 NetScaler Gateway 进行文件共享。

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

创建企业书签

在会话策略中创建访问界面链接

1. 在配置实用程序中，在“**配置**”选项卡上的导航窗格中，展开“**NetScaler Gateway > 资源**”，然后单击“**门户书签**”。
2. 在详细信息窗格中，单击“**添加**”。

3. 在“**名称**”中，键入书签的名称。
4. 在“**要显示的文本**”中，键入链接的描述。该描述将显示在“**访问界面**”中。
5. 在“**书签**”中，键入应用程序的网址。
6. 在“**虚拟服务器**”中，键入关联的负载平衡/内容交换虚拟服务器的名称。此字段是可选的。

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

7. 在“**图标 URL**”中，上传的图标支持除默认主题之外的所有主题。建议的最大大小为 70x70 像素。建议使用透明图像。此字段是可选的。
8. 在“**应用程序类型**”中，选择 URL 所代表的应用程序类型（VPN、无客户端 VPN 或 SaaS）。此字段是可选的。
9. 在“**SSO 类型**”中，选择要为书签配置的 SSO 类型。配置 SSO 后，用户无需在后续登录中输入凭据即可访问应用程序。支持以下 SSO 类型：
   - 统一网关：此 SSO 配置允许通过单个 URL 安全地远程访问应用程序的多个资源。
   - 自认证：在此 SSO 配置中，系统会提示 NetScaler Gateway 用户提供登录凭据以访问应用程序。
   - 基于 SAML 的身份验证：在此 SSO 配置中，NetScaler Gateway 使用 IdP 验证用户详细信息，生成 SAML 断言，并将其发送到 SP。如果验证通过，则 SSO 成功。

   注意：

   如果启用无客户端访问，可以确保对网站的请求通过 NetScaler Gateway。例如，您为 Google 添加了书签。选中“**将 NetScaler Gateway 用作反向代理**”复选框。选中此复选框后，网站请求将从用户设备发送到 NetScaler Gateway，然后再发送到网站。清除此复选框后，请求将从用户设备直接发送到网站。此复选框仅在启用无客户端访问时可用。

10. 单击“**创建**”，然后单击“**关闭**”。

绑定访问接口链接

可以将访问接口链接绑定到以下位置：

- 用户
- 组
- 虚拟服务器

保存配置后，链接将在访问接口的“**主页**”选项卡中对用户可用，这是用户成功登录后看到的第一个页面。

1. 在配置实用程序中，在导航窗格中执行以下操作之一：
   - 展开“**NetScaler Gateway 用户管理**”，然后单击“**AAA 用户**”。
   - 展开“**NetScaler Gateway 用户管理**”，然后单击“**AAA 组**”。
   - 展开“**NetScaler Gateway**”，然后单击“**虚拟服务器**”。

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

2. 在详细信息窗格中，执行以下操作之一：
   - 选择一个用户，然后单击“打开”。
   - 选择一个组，然后单击“打开”。
   - 选择一个虚拟服务器，然后单击“打开”。
3. 在对话框中，单击“**书签**”选项卡。
4. 在“**可用书签**”下，选择一个或多个书签，单击右箭头将书签移动到“已配置书签”下，然后单击“**确定**”。

通过 GUI 全局绑定书签

1. 在“**配置**”选项卡上的导航窗格中，展开“**NetScaler Gateway**”，然后单击“**全局设置**”。
2. 在详细信息窗格的“**书签**”下，单击“**创建指向您希望在 NetScaler Gateway 门户页面上可访问的 HTTP 和 Windows 文件共享应用程序的链接**”。

3. 在 **配置 VPN 全局绑定*** 对话框中，单击 **添加。**
4. 在“**可用**”下，选择一个或多个书签，单击右箭头将书签移动到“已配置”下，然后单击“**确定**”。

通过 CLI 添加企业书签

在命令提示符下，键入：

```
add vpn url <urlName> <linkName> <actualURL>  [-ssotype <ssotype>]
```

示例：

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

Web 书签

```
add vpn url google google "https://www.google.com"
```

使用 CLI 绑定企业书签

您可以将企业书签绑定到用户、组、虚拟服务器和全局级别。

```
bind aaa user <userName> -urlName <string>

bind aaa group <groupName> -urlName <string>

bind vpn vserver <vserverName> -urlName <string>

bind vpn global –urlName <string>
```

示例：

```
bind vpn global -urlName google
```

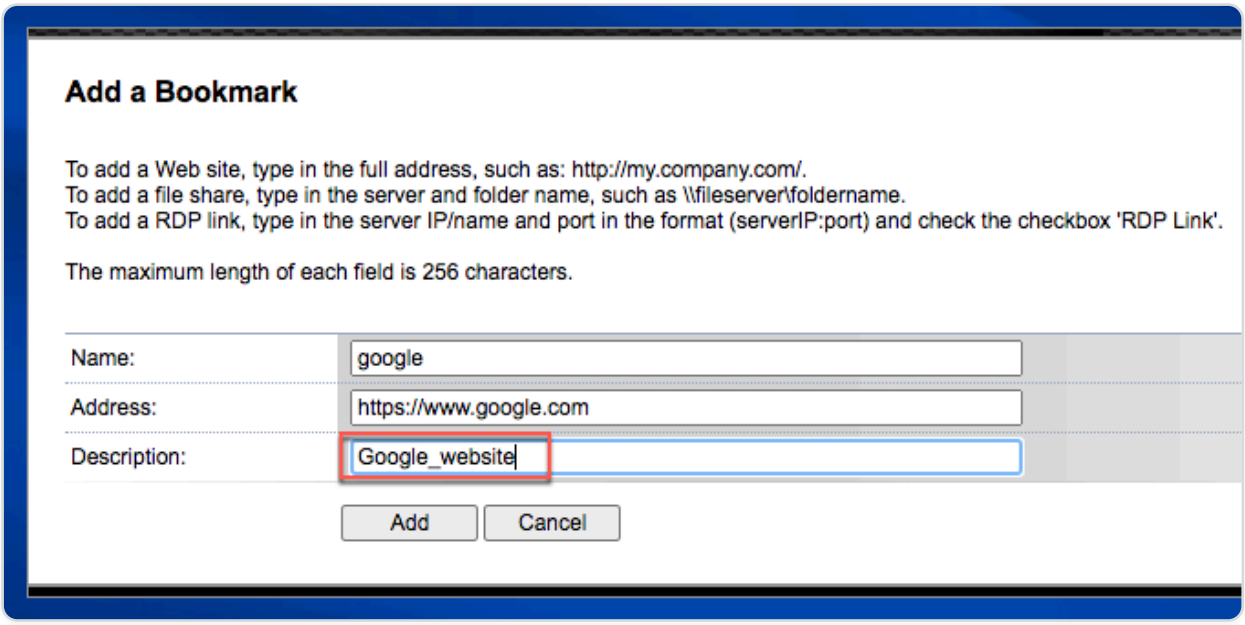
创建个人书签

您只能从 VPN 虚拟服务器创建个人网站。NetScaler Gateway 管理 GUI 中没有用于添加个人书签的选项。

1. 登录到 VPN 虚拟服务器。
2. 单击“**网络访问**”或“**无客户端访问**”以添加书签。
3. 单击“**添加**”。

4. 输入书签详细信息，例如网站名称、地址和描述。

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



5. 单击“**添加**”。

您添加的网站会显示在相应的选项卡下。

VPN 中的个人书签(/en-us/netscaler-gateway/media/vpn-server-after-adding-personal-bookmark-new.png)

在书签中配置用户名令牌

You can configure bookmark and file share URLs using a special token, %`username`%. When users log on, the token is replaced with each users' logon name. For example, you create a bookmark for an employee named Jack for a folder as \\\\EmployeeServer\\%`username`%\\. When Jack logs on, the file share URL is mapped to \\\\EmployeeServer\\Jack\\. When you configure user name tokens in bookmarks, keep the following situations in mind:

- 如果您使用一种身份验证类型，则用户名将替换令牌 %`username`%。
- 如果您使用双因素身份验证，则主身份验证类型中的用户名将用于替换 %`username`% 令牌。
- 如果您使用客户端证书身份验证，则客户端证书身份验证配置文件中的用户名字段将用于替换 %`username`% 令牌。

配置 SmartAccess

您可以将 SmartAccess 与 Citrix Virtual Apps and Desktops 结合使用，以智能地向用户交付已发布的应用程序和虚拟桌面。

SmartAccess 允许您通过使用 NetScaler Gateway 会话策略来控制对服务器上已发布的应用程序和桌面的访问。您可以使用预身份验证和后身份验证检查作为条件，以及其他条件，来访问已发布的

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

资源。其他条件包括您可以通过 Citrix Virtual Apps and Desktops 策略控制的任何内容，例如打印机带宽限制、用户设备驱动器映射、剪贴板、音频和打印机映射。您可以根据用户是否通过 NetScaler Gateway 检查来应用 Citrix Virtual Apps and Desktops 策略。

NetScaler Gateway 可以通过使用与 StoreFront、ICA 代理访问、无客户端访问和 NetScaler Gateway 访问相同的选项来交付 Citrix Virtual Desktops。

此功能通过将 NetScaler Gateway 组件与 StoreFront 和 Citrix Virtual Apps and Desktops 集成来实现。此集成向 StoreFront 提供了高级身份验证和访问控制选项。有关更多信息，请参阅 NetScaler 产品文档中“技术”节点下的 StoreFront 文档。

远程连接到服务器场不需要 Citrix Secure Access 客户端。用户可以使用 Citrix Workspace 应用程序进行连接。用户可以使用 Citrix Secure Access 客户端登录并通过访问界面（NetScaler Gateway 的默认主页）接收其已发布的应用程序和虚拟桌面。

流量策略

流量策略允许您为用户连接配置以下设置：

- 对从不受信任网络访问的敏感应用程序强制执行更短的超时时间。
- 将网络流量切换为对某些应用程序使用 TCP。如果选择 TCP，则必须为某些应用程序启用或禁用单点登录。
- 识别您希望对 Citrix Secure Access™ 客户端流量使用其他 HTTP 功能的情况。
- 定义与文件类型关联一起使用的文件扩展名。

创建流量策略

要配置流量策略，您需要创建一个配置文件并配置以下参数：

- 协议（HTTP 或 TCP）
- 应用程序超时
- Web 应用程序的单点登录
- 表单单点登录
- 文件类型关联
- 中继器插件
- Kerberos 约束委派 (KCD) 帐户

创建流量策略后，您可以将该策略绑定到虚拟服务器、用户、组或全局。

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

例如，您在内部网络中的服务器上安装了 Web 应用程序 PeopleSoft Human Resources。您可以为此应用程序创建流量策略，该策略定义目标 IP 地址、目标端口，并且您可以设置用户可以保持登录到应用程序的时间量，例如 15 分钟。

如果要配置其他功能（例如对应用程序进行 HTTP 压缩），可以使用流量策略来配置设置。创建策略时，请对操作使用 HTTP 参数。在表达式中，创建运行该应用程序的服务器的目标地址。

流量策略表达式示例

以下是流量策略的表达式示例：

- `add vpn trafficPolicy trafPol1 "HTTP.REQ.URL.CONTAINS(\"/Citrix/\") || HTTP.REQ.URL.CONTAINS(\"10.102.\")")" trafAct1`
- `add vpn trafficPolicy trafPol2 "HTTP.REQ.HOSTNAME.CONTAINS(\"portal-srv\") || HTTP.REQ.URL.CONTAINS(\"homePage\"))" trafAct2`
- `add vpn trafficPolicy trafPol3 true trafAct3`

使用 GUI 配置流量策略

1. 展开 **NetScaler Gateway > 策略**，然后单击 **流量**。
2. 在详细信息窗格中，在**策略**选项卡上，单击**添加**。
3. 在**创建流量策略**对话框中，在**名称**中，键入策略的名称。
4. 在**请求配置文件**旁边，单击**新建**。
5. 在**名称**中，键入配置文件的名称。
6. 在**协议**中，选择 **HTTP** 或 **TCP**。

   注意： 如果选择 TCP 作为协议，则无法配置单点登录，并且配置文件对话框中的设置将被禁用。
7. 在 **AppTimeout (分钟)** 中，键入分钟数。此设置限制了用户可以登录到 Web 应用程序的时间。
8. 要为 Web 应用程序启用单点登录，请在 **Single Sign-On** 中选择 **ON**。

   注意： 要使用基于表单的单点登录，可以在流量配置文件中配置设置。有关详细信息，请参阅配置基于表单的单点登录。

   注意： SSO 设置仅适用于不使用 Citrix Secure Access 客户端的连接。
9. 要指定文件类型关联，请在 **File Type Association** 中选择 **ON**。
10. 要使用中继器插件优化网络流量，请在 Citrix SD-WAN™ 中选择 **ON**，单击 **Create**，然后单击 **Close**。

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

11. 如果在设备上配置 KCD，请在 KCD Account 中选择帐户。

    有关在设备上配置 KCD 的详细信息，请参阅 如何为 Kerberos 约束委派配置 NetScaler Gateway。

12. 在“创建流量策略”对话框中，创建或添加表达式，单击 **Create**，然后单击 **Close**。

配置基于表单的单点登录

基于表单的单点登录允许用户一次登录到网络中的所有受保护应用程序。在 NetScaler Gateway 中配置基于表单的单点登录后，用户可以访问需要基于 HTML 表单登录的 Web 应用程序，而无需再次键入密码。如果没有单点登录，用户需要单独登录才能访问每个应用程序。

创建表单单点登录配置文件后，您将创建一个包含该表单单点登录配置文件的流量配置文件和策略。有关详细信息，请参阅 创建流量策略。

配置基于表单的单点登录

1. 展开 **NetScaler Gateway > Policies**，然后单击 **Traffic**。
2. 在详细信息窗格中，单击“**表单 SSO 配置文件**”选项卡，然后单击“**添加**”。
3. 在“**名称**”中，键入配置文件的名称。
4. 在“**操作 URL**”中，键入提交已完成表单的 URL。

   注意： URL 是根相对 URL。

5. 在“**用户名**”中，键入用户名字段的属性名称。
6. 在“**密码**”中，键入密码字段的属性名称。
7. 在“**SSO 成功规则**”中，创建描述此配置文件在策略调用时所执行操作的表达式。您还可以使用此字段下的“前缀”、“添加”和“运算符”按钮来创建表达式。

   此规则检查单点登录是否成功。

8. 在“**名称值对**”中，键入用户名字段值，后跟一个与号 (&)，然后是密码字段值。

   值名称用与号 (&) 分隔，例如 name1=value1&name2=value2。

9. 在“**响应大小**”中，键入允许的完整响应大小的字节数。键入响应中要解析以提取表单的字节数。
10. 在“**提取**”中，选择名称/值对是静态还是动态。默认设置为“动态”。
11. 在“**提交方法**”中，选择单点登录表单用于将登录凭据发送到登录服务器的 HTTP 方法。默认值为 Get。
12. 单击“**创建**”，然后单击“**关闭**”。

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

配置 SAML 单点登录

您可以为单点登录 (SSO) 创建 SAML 1.1 或 SAML 2.0 配置文件。用户可以连接到支持 SAML 协议的 Web 应用程序以进行单点登录。NetScaler Gateway 支持 SAML Web 应用程序的身份提供程序 (IdP) 单点登录。

配置 SAML 单点登录

1. 在配置实用程序中，在“配置”选项卡上的导航窗格中，展开 **NetScaler Gateway \ > 策略**，然后单击“流量”。
2. 在详细信息窗格中，单击“SAML SSO 配置文件”选项卡。
3. 在详细信息窗格中，单击“添加”。
4. 在“名称”中，键入配置文件的名称。
5. 在“签名证书名称”中，输入 X.509 证书的名称。
6. 在“ACS URL”中，输入身份提供程序或服务提供程序的断言消费者服务。AssertionConsumerServiceURL (ACS URL) 为用户提供 SSO 功能。
7. 在“中继状态规则”中，从“已保存的策略表达式”和“常用表达式”构建策略表达式。从“运算符”列表中选择以定义如何评估表达式。要测试表达式，请单击“评估”。
8. 在“发送密码”中选择“开”或“关”。
9. 在“颁发者名称”中输入 SAML 应用程序的身份。
10. 单击“创建”，然后单击“关闭”。

绑定流量策略

您可以将流量策略绑定到虚拟服务器、组、用户以及 NetScaler Gateway 全局。您可以使用配置实用程序绑定流量策略。

使用 GUI 全局绑定流量策略

1. 在配置实用程序中，在“配置”选项卡上，在导航窗格中，展开 **NetScaler Gateway > 策略**，然后单击“流量”。
2. 在详细信息窗格中，选择一个策略，然后在“操作”中，单击“全局绑定”。
3. 在“绑定/取消绑定流量策略”对话框中，在“详细信息”下，单击“插入策略”。
4. 在“策略名称”下，选择策略，然后单击“确定”。

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

删除流量策略

您可以使用配置实用程序从 NetScaler Gateway 中删除流量策略。如果您使用配置实用程序删除流量策略，并且该策略已绑定到用户、组或虚拟服务器级别，则必须首先取消绑定该策略。然后，您可以删除该策略。

使用 GUI 取消绑定流量策略

1. 展开 **NetScaler Gateway**，然后单击 **虚拟服务器**。
   - 展开 **NetScaler Gateway > 用户管理**，然后单击 **AAA 组**。
   - 展开 **NetScaler Gateway > 用户管理**，然后单击 **AAA 用户**。
2. 在详细信息窗格中，选择一个虚拟服务器、组或用户，然后单击 **打开**。
3. 在“**配置 NetScaler Gateway 虚拟服务器、配置 AAA 组**”或“**配置 AAA 用户**”对话框中，单击“**策略**”选项卡。
4. 单击 **流量**，选择策略，然后单击 **取消绑定策略**。
5. 单击 **确定**，然后单击 **关闭**。

流量策略取消绑定后，您可以删除该策略。

使用 GUI 移除流量策略

1. 展开 **NetScaler Gateway > 策略**，然后单击**流量**。
2. 在详细信息窗格的“策略”选项卡上，选择流量策略，然后单击**删除**。

会话策略

会话策略是应用于用户、组、虚拟服务器和全局的表达式和设置的集合。

您可以使用会话策略来配置用户连接的设置。您可以定义设置来配置用户登录所用的软件，例如适用于 Windows 的 Citrix Secure Access 客户端或适用于 Mac 的 Citrix Secure Access 客户端。您还可以配置设置以要求用户使用 Citrix Workspace 应用程序或 Secure Hub 登录。会话策略在用户通过身份验证后进行评估和应用。

会话策略根据以下规则应用：

- 会话策略始终覆盖配置中的全局设置。
- 任何未使用会话策略设置的属性或参数都将在为虚拟服务器建立的策略上设置。
- 任何未由会话策略或虚拟服务器设置的其他属性都将由全局配置设置。

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

重要提示：

以下说明是创建会话策略的一般准则。对于不同配置（例如无客户端访问或访问已发布的应用程序）的会话策略配置，有特定的说明。这些说明可能包含配置特定设置的指导。但是，该设置可以是会话配置文件和策略中包含的众多设置之一。这些说明指导您在会话配置文件中创建设置，然后将该配置文件应用于会话策略。您可以在不创建会话策略的情况下更改配置文件和策略中的设置。此外，您可以在全局级别创建所有设置，然后创建会话策略来覆盖全局设置。

如果您在网络中部署 Citrix Endpoint Management 或 StoreFront，Citrix 建议使用快速配置向导来配置会话策略和配置文件。运行向导时，您将定义部署的设置。NetScaler Gateway 然后创建所需的身份验证、会话和无客户端访问策略。

创建会话策略

1. 在配置实用程序中，在“Configuration”（配置）选项卡上的导航窗格中，展开“NetScaler Gateway”>“Policies”（策略），然后单击“Session”（会话）。
2. 在详细信息窗格的“Policies”（策略）选项卡上，单击“Add”（添加）。
3. 在“Name”（名称）中，键入策略的名称。
4. 在“Request Profile”（请求配置文件）旁边，单击“New”（新建）。
5. 在“名称”中，键入配置文件的名称。
6. 完成会话配置文件的设置，然后单击“创建”。
7. 在“创建会话配置文件”对话框中，为策略添加表达式，单击“创建”，然后单击“关闭”。 注意：在表达式中，选择 True 值，以便策略始终应用于其绑定的级别。

会话策略表达式示例

以下是会话策略的表达式示例：

- `add vpn sessionPolicy sessPol1 "HTTP.REQ.HEADER(\"User-Agent\").CONTAINS(\"CitrixReceiver\") || HTTP.REQ.HEADER(\"User-Agent\").CONTAINS(\"CitrixWorkspace\")" sessAct1`
- `add vpn sessionPolicy sessPol2 "HTTP.REQ.HEADER(\"User-Agent\").CONTAINS(\"CitrixReceiver\").NOT" sessAct2`
- `add vpn sessionPolicy sessPol3 true sessAct3`

绑定会话策略

创建会话策略后，将其绑定到用户、组、虚拟服务器或全局。会话策略按以下顺序分层应用：

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

- 用户
- 组
- 虚拟服务器
- 全局

使用 GUI 将会话策略绑定到虚拟服务器

1. 导航到 **NetScaler Gateway > 虚拟服务器**。
2. 选择一个虚拟服务器，然后点击**编辑**。您也可以创建一个新的虚拟服务器。
3. 向下滚动到**策略**部分，然后点击**+**图标。
4. 在**选择策略**中，选择**会话**。
5. 在**选择类型**中，选择**请求**，然后点击**继续**。
6. 在**选择策略**中，选择要绑定到此虚拟服务器的策略。
7. 在**优先级**中，输入策略的优先级编号。
8. 点击**绑定**。

使用 GUI 将会话策略绑定到身份验证、授权和审计组

1. 导航到 **NetScaler Gateway > 用户管理 > AAA 组**。
2. 选择一个现有的身份验证、授权和审计组，然后点击**编辑**。您也可以创建一个身份验证、授权和审计组。
3. 在**高级设置**中，点击**策略**，然后点击**+**图标。
4. 在**选择策略**中，选择**会话**，然后点击**继续**。
5. 在**选择策略**中，选择要绑定到此身份验证、授权和审计组的策略。
6. 在**优先级**中，输入策略的优先级编号。
7. 点击**绑定**。

使用 GUI 将会话策略绑定到身份验证、授权和审计用户

1. 导航到 **NetScaler Gateway > 用户管理 > AAA 用户**。
2. 选择一个现有的 NetScaler 用户，然后点击**编辑**。您还可以创建身份验证、授权和审计用户。
3. 在**高级设置**中，点击**策略**，然后点击**+**图标。
4. 在**选择策略**中，选择**会话**，然后点击**继续**。
5. 在**选择策略**中，选择要绑定到此身份验证、授权和审计用户的策略。
6. 在**优先级**中，输入策略的优先级编号。

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

7. 点击**绑定**。

注意：有关优先级的详细信息，请参阅 `<https://support.citrix.com/article/CTX214588>`。

创建会话配置文件

会话配置文件包含用户连接的设置。

如果用户设备满足策略表达式条件，会话配置文件会指定应用于用户会话的操作。配置文件与会话策略一起使用。您可以使用配置实用程序独立于会话策略创建会话配置文件，然后将该配置文件用于多个策略。一个策略只能使用一个配置文件。

在会话配置文件中配置用户连接的网络设置

您可以使用会话配置文件中的**网络配置**选项卡配置用户连接的以下网络设置：

- DNS 服务器
- WINS 服务器 IP 地址
- 可用作内网 IP 地址的映射 IP 地址
- 地址池（内网 IP 地址）的溢出设置
- 内网 IP DNS 后缀
- HTTP 端口
- 强制超时设置

在会话配置文件中配置连接设置

您可以使用会话配置文件中的“**客户端体验**”选项卡来配置以下连接设置：

- 访问界面或自定义主页
- 基于 Web 的电子邮件的 Web 地址，例如 Outlook Web Access
- 插件类型（适用于 Windows 的 Citrix Secure Access™ 客户端，或适用于 macOS X 的 Citrix Secure Access 客户端）
- 拆分隧道
- 会话和空闲超时设置
- 无客户端访问
- 无客户端访问 URL 编码
- 插件类型（Windows 或 Mac）

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

- Web 应用程序的单点登录
- 用于身份验证的凭据索引
- Windows 单点登录
- 客户端清理行为
- 登录脚本
- 客户端调试设置
- 分割 DNS
- 访问专用网络 IP 地址和本地 LAN 访问
- 客户端选择
- 代理设置

注意：

- Citrix Secure Access 客户端支持基于 TCP 和 UDP 的 DNS 请求的分割 DNS 解析。DNS 解析根据分割 DNS 设置工作，如下所示：
  - **远程：** 所有 DNS 请求都在远程 DNS 服务器上解析。
  - **本地：** 匹配 DNS 后缀或隧道应用程序的主机名的 DNS 请求将发送到远程 DNS 服务器。其他主机名的 DNS 请求将发送到本地 DNS 服务器。
  - **两者：** 所有匹配 DNS 后缀或隧道应用程序的 DNS 请求都将发送到远程 DNS 服务器。其他主机名的 DNS 请求将发送到本地和远程服务器，并接受第一个成功的响应。
- 从适用于 Windows 版本 24.8.1.15 的 Citrix Secure Access 客户端开始，拆分 DNS 功能除了适用于基于 UDP 的请求外，还适用于基于 TCP 的 DNS 请求。
- 从适用于 Linux 版本 25.2.2 的 Citrix Secure Access 开始，拆分 DNS 功能（**远程**、**本地**和**两者**）适用于基于 TCP 和 UDP 的 DNS 请求。拆分 DNS 设置**两者**的功能与拆分 DNS 设置**本地**相同。

有关配置用户连接设置的更多信息，请参阅配置 Citrix Secure Access 客户端的连接。

在会话配置文件中配置安全设置

您可以使用会话配置文件中的“**安全**”选项卡来配置以下安全设置：

- 默认授权操作（允许或拒绝）
- 适用于 iOS 设备连接的安全浏览
- 隔离组

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

- 授权组

有关在 NetScaler Gateway 上配置授权的更多信息，请参阅配置授权。

在会话配置文件中配置 Citrix Virtual Apps and Desktops 设置

您可以使用会话配置文件中的“**已发布的应用程序**”选项卡来配置连接到运行 Citrix Virtual Apps and Desktops 的服务器的以下设置：

- ICA 代理，即使用 Citrix Workspace 应用程序的客户端连接
- Web 界面地址
- Web Interface 门户模式
- 单点登录到服务器场域
- Citrix Workspace 应用程序主页
- 帐户服务地址

有关配置连接到服务器场中已发布应用程序的设置的更多信息，请参阅 将 NetScaler Gateway 与 StoreFront 集成。

您可以独立于会话策略创建会话配置文件。创建策略时，可以选择要附加到策略的配置文件。

使用 GUI 创建会话配置文件

1. 在配置实用程序中，在“配置”选项卡上的导航窗格中，展开 **NetScaler Gateway > 策略**，然后单击 **会话**。
2. 在详细信息窗格中，单击“**配置文件**”选项卡，然后单击“**添加**”。
3. 配置配置文件的设置，单击“**创建**”，然后单击“**关闭**”。

创建配置文件后，可以将其包含在会话策略中。

使用 GUI 将配置文件添加到会话策略

1. 在配置实用程序中，在导航窗格中，展开 **Access Gateway > 策略**，然后单击 **会话**。
2. 在“**策略**”选项卡上，执行以下操作之一：
   - 点击 **添加** 以创建会话策略。
   - 选择一个策略，然后点击 **打开**。
3. 在 **请求配置文件** 中，从列表中选择一个配置文件。
4. 完成会话策略的配置，然后执行以下操作之一：

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

a. 点击 **创建**，然后点击 **关闭** 以创建策略。

b. 点击 **确定**，然后点击 **关闭** 以修改策略。

企业书签的高级策略支持

企业书签 (VPN URL) 可以配置为高级策略。

注意：

- NetScaler Gateway 支持企业书签的 HTTP、HTTPS 和 RDP 协议。
- NetScaler Gateway 仅支持企业书签的绝对 URL。

将 VPN URL 配置为高级策略

在 GUI 上

1. 创建 VPN URL 配置文件。

   - 导航到 **配置 > NetScaler Gateway > 策略 > VPN URL**。
   - 在**VPN URL 策略和配置文件**页面上，选择**VPN URL 配置文件**选项卡，然后单击**添加**。
   - 更新所需字段，然后单击**创建**。

     - 名称：VPN URL 配置文件的名称。
     - 要显示的文本：链接的简要说明。该说明显示在访问界面上。
     - 书签：应用程序的 Web 地址。
     - 虚拟服务器：已配置的关联负载平衡或内容交换虚拟服务器的名称。此字段是可选的。
     - 图标 URL：此字段中上传的图标支持所有主题，但默认主题除外。建议最大尺寸为 70x70 像素。我们建议您使用透明图像。此字段是可选的。
     - 应用程序类型：选择 URL 所代表的应用程序类型（VPN、无客户端 VPN 或 SaaS）。此字段是可选的。
     - SSO 类型：您要为书签配置的 SSO 类型。配置 SSO 后，用户无需在后续登录中输入凭据即可访问应用程序。支持以下 SSO 类型：

       - 统一网关：此 SSO 配置允许通过单个 URL 安全地远程访问应用程序的多个资源。
       - 自我身份验证：在此 SSO 配置中，NetScaler Gateway 用户需要提供登录凭据才能访问应用程序。

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

- 基于 SAML 的身份验证：在此 SSO 配置中，NetScaler Gateway 使用 IdP 验证用户详细信息，生成 SAML 断言，并将其发送到 SP。如果验证通过，则 SSO 成功。

注意：

如果启用无客户端访问，可以确保对网站的请求通过 NetScaler Gateway。例如，您为 Google 添加了书签。选中“将 NetScaler Gateway 用作反向代理”复选框。选中此复选框后，网站请求将从用户设备发送到 NetScaler Gateway，然后再发送到网站。取消选中此复选框后，请求将从用户设备直接发送到网站。仅当启用无客户端访问时，此复选框才可用。

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

Create VPN URL Profiles

Name*

vpnurlact

Text to display*

Google

Bookmark*

https://google.com

Virtual Server

Icon URL

Choose File

Application Type

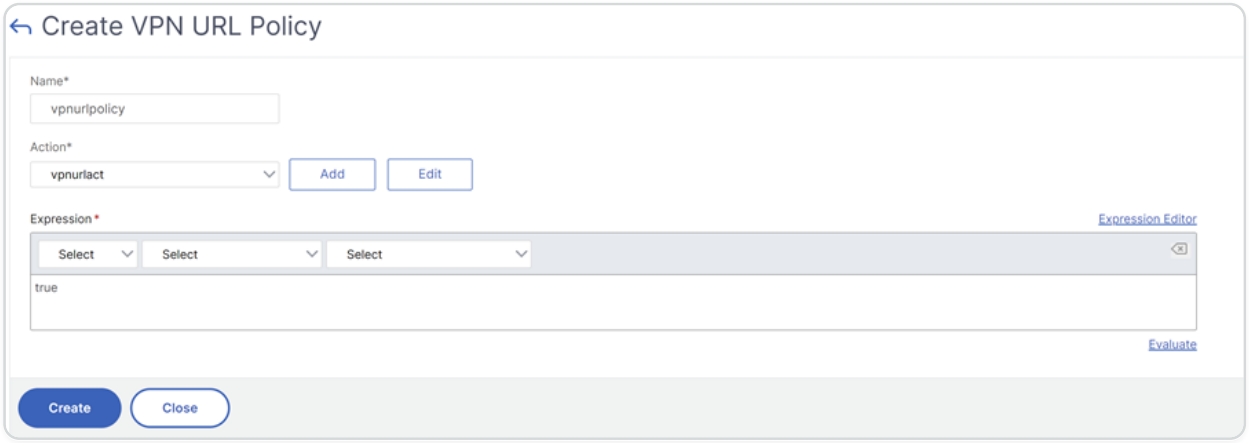
SSO Type

☑ Use NetScaler Gateway as a Reverse Proxy

Comments

2. 创建 VPN URL 策略。

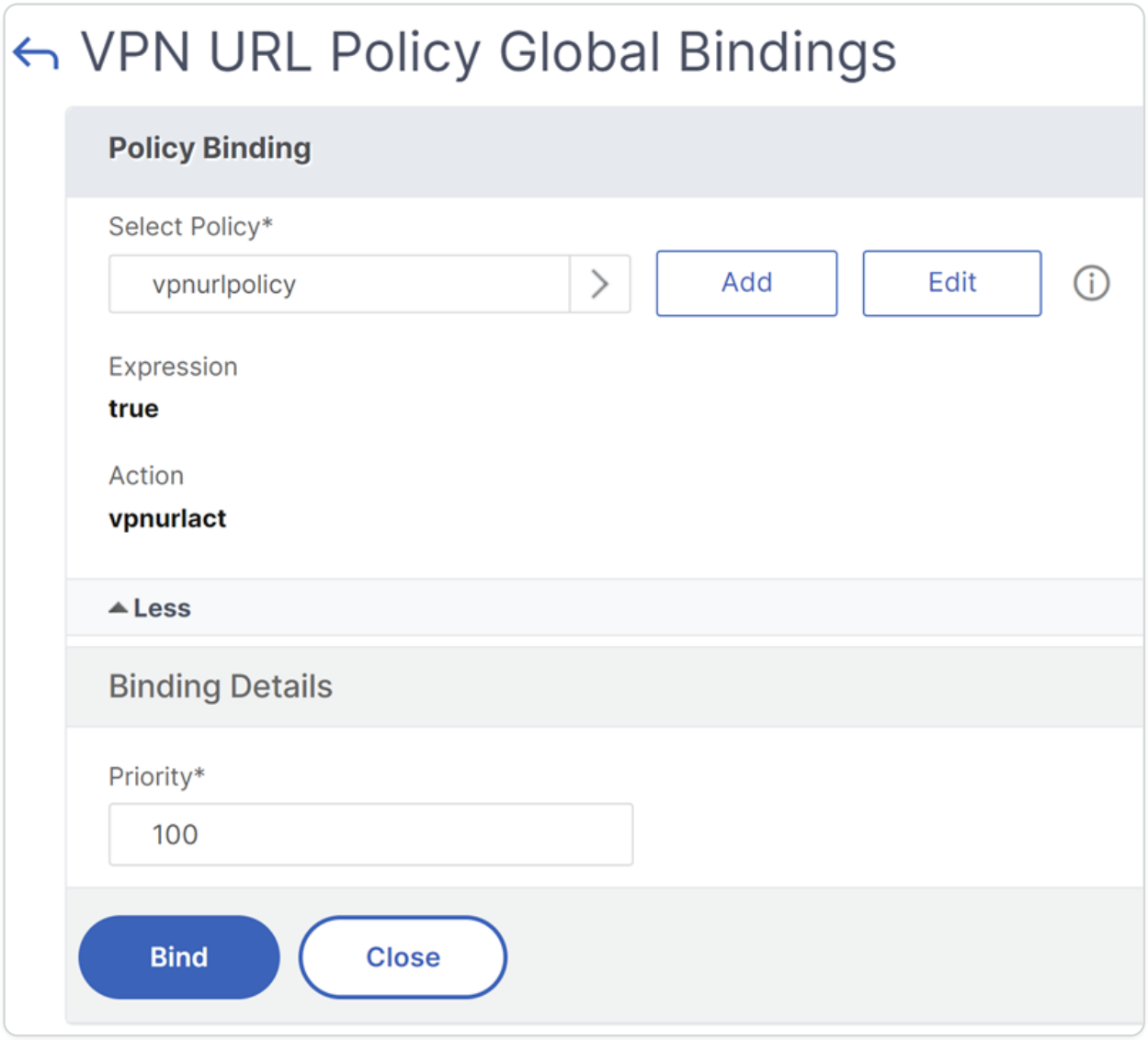
   - 导航到 **配置 > NetScaler Gateway > 策略 > VPN URL**。
   - 在“**VPN URL 策略和配置文件**”页面上，选择“**VPN URL 策略**”选项卡，然后单击“**添加**”。
   - 更新所需字段，然后单击“**创建**”。
     - 名称：VPN URL 策略的名称。
     - 操作：选择已配置的 VPN URL 配置文件。如果下拉列表中没有配置文件，请单击“添加”并重复步骤 1。
     - 表达式：有关高级策略表达式的信息，请参阅策略和表达式。



3. 将 VPN URL 策略绑定到绑定点。

   - 导航到 **配置 > NetScaler Gateway > 策略 > VPN URL**。
   - 在 **VPN URL 策略和配置文件** 页面上，选择 **VPN URL 策略** 选项卡。
   - 从 **选择操作** 下拉列表中选择 **全局绑定**。
   - 选择 VPN URL 策略。如果没有列出策略，请单击 **添加** 并重复步骤 2。
   - 在 **绑定详细信息** 部分中，为 VPN URL 策略分配优先级。

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



在 CLI 上

创建 VPN URL 操作：

在命令提示符下，键入以下内容：

```
add vpn urlAction &lt;name> -linkName &lt;string> -actualURL &lt;string>
[-vServerName &lt;string>] [-clientlessAccess ( ON | OFF )] [-comment
&lt;string>] [-iconURL &lt;URL>] [-ssotype &lt;ssotype>] [-applicationtype
&lt;applicationtype>] [-samlSSOProfile &lt;string>]
```

NetScaler Gateway 支持以下 VPN URL 操作：

- **添加**

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

```
add vpn urlAction &lt;name> -linkName &lt;string> -actualURL
&lt;string> [-vServerName &lt;string>] [-clientlessAccess ( ON | OFF )]
[-comment &lt;string>] [-iconURL &lt;URL>] [-ssotype &lt;ssotype>] [-
applicationtype &lt;applicationtype>] [-samlSSOProfile &lt;string>]
```

- **设置**

```
set vpn urlAction &lt;name> [-vServerName &lt;string>] [-
clientlessAccess ( ON | OFF )] [-comment &lt;string>] [-iconURL
&lt;URL>] [-ssotype &lt;ssotype>] [-applicationtype
&lt;applicationtype>] [-samlSSOProfile &lt;string>]
```

- **取消设置**

```
unset vpn urlAction &lt;name> [-vServerName] [-clientlessAccess] [-
comment] [-iconURL] [-ssotype] [-applicationtype] [-samlSSOProfile]
```

注意：

如果您将无客户端访问设置为开启，您可以确保对网站的请求从用户设备发送到 NetScaler Gateway，然后再发送到网站。

- **显示**

```
show vpn urlAction [&lt;name>]
```

- **删除**

```
remove vpn urlAction &lt;name>
```

- **重命名**

```
rename vpn urlAction &lt;name>@ &lt;newName>@
```

创建 VPN URL 策略：

NetScaler Gateway 支持用于 VPN URL 策略的以下操作：

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

- **添加**

```
add vpn urlPolicy &lt;name> -rule &lt;expression> -action &lt;string>
[-comment &lt;string>] [-logAction &lt;string>]
```

- **设置**

```
set vpn urlPolicy &lt;name> [-rule &lt;expression>] [-action
&lt;string>] [-comment &lt;string>] [-logAction &lt;string>]
```

- **取消设置**

```
unset vpn urlPolicy &lt;name> [-comment] [-logAction]
```

- **显示**

```
show vpn urlPolicy [&lt;name>]
```

- **删除**

```
remove vpn urlPolicy &lt;name>
```

- **重命名**

```
rename vpn urlpolicy &lt;name>@ &lt;newName>@
```

- **统计**

```
stat vpn urlpolicy [&lt;name>] [-detail] [-fullValues] [-ntimes
&lt;positive_integer>] [-logFile &lt;input_filename>] [-clearstats
( basic | full )]
```

将策略绑定到绑定点：

NetScaler Gateway 支持以下 VPN URL 策略绑定操作：

- **绑定**

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

```
bind vpn vserver &lt;vserver name> -policy &lt;string> -priority
&lt;positive_integer> [-gotoPriorityExpression &lt;expression>]

bind vpn global -policyName &lt;string> -priority &lt;positive_integer>
[-gotoPriorityExpression &lt;expression>]

bind aaa user &lt;userName> -policy &lt;string> [-priority
&lt;positive_integer>] [-type &lt;type>] [-gotoPriorityExpression
&lt;expression>]

bind aaa group &lt;groupName> -policy &lt;string> [-priority
&lt;positive_integer>] [-type &lt;type>] [-gotoPriorityExpression
&lt;expression>]
```

- **解除绑定**

```
unbind vpn vserver &lt;name> -policy &lt;string>

unbind vpn global -policyName &lt;string>

unbind aaa user &lt;name> -policy &lt;string>

unbind aaa group &lt;name> -policy &lt;string>
```

注意：

绑定点包括 `aaauser`、`aaagroup`、`vpnvserver` 和 `vpnglobal`。

端点分析

端点分析 (EPA) 是一种扫描用户设备并检测信息（例如操作系统更新、防病毒、防火墙和网络浏览器软件的存在和版本级别）的过程。端点分析允许您在用户设备连接到您的网络之前，确定其是否符合您的要求。它还可以配置为在用户保持连接时定期检查任何更改。您可以在用户会话期间检查用户设备上的文件、进程和注册表项，以确保设备持续满足要求。

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

重要提示：

- 端点分析旨在根据预定的合规性标准分析用户设备，不强制执行或验证最终用户设备的安全性。建议使用端点安全系统来保护设备免受本地管理员攻击。
- EPA 客户端可作为独立客户端使用，也可与 Citrix Secure Access™ 客户端捆绑使用。Citrix® EPA 客户端和 Citrix Secure Access 客户端彼此独立。

端点策略的工作原理

您可以配置 NetScaler Gateway，以在用户登录前检查用户设备是否满足特定要求。这称为预身份验证策略。您可以配置 NetScaler Gateway，以检查用户设备是否具有您在策略中指定的防病毒、防火墙、反垃圾邮件、进程、文件、注册表项、互联网安全或操作系统。如果用户设备未能通过预身份验证扫描，则不允许用户登录。

要验证预身份验证策略中未使用的其他要求，您可以配置会话策略并将其绑定到用户或组。这种类型的策略称为后身份验证策略，它在用户会话期间运行，以确保所需的标准（例如防病毒软件或进程）保持合规。

当您配置预身份验证或后身份验证策略时，NetScaler Gateway 会下载端点分析插件，然后在用户设备上运行扫描。每次用户登录时，端点分析插件都会自动运行。

您可以使用以下三种类型的策略来配置端点策略：

- 使用“是”或“否”参数的预身份验证策略。扫描确定用户设备是否满足指定要求。如果扫描失败，用户无法在登录页面上输入凭据。
- 有条件且可用于 SmartAccess 的会话策略。
- 会话策略中的客户端设备检查表达式。如果用户设备未能满足客户端设备检查表达式的要求，您可以配置将用户置于隔离组中。如果用户设备通过扫描，用户可以被置于可能需要其他检查的不同组中。

您可以将检测到的信息纳入策略中，从而根据用户设备授予不同级别的访问权限。例如，您可以向从满足当前防病毒和防火墙软件要求的用户设备远程连接的用户提供具有下载权限的完全访问权限。对于从不合规设备连接的用户，您可以提供更受限制的访问级别，允许用户在远程服务器上编辑文档而无需下载。所有运行 EPA 的设备都被视为不合规设备。

端点分析执行以下基本步骤：

- 检查用户设备的初始信息集，以确定要应用哪些扫描。

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

- 运行所有适用的扫描。当用户尝试连接时，端点分析插件会检查用户设备是否符合预身份验证或会话策略中指定的要求。如果用户设备通过扫描，则允许用户登录。如果用户设备未能通过扫描，则不允许用户登录。

  注意： 端点分析扫描在用户会话使用许可证之前完成。

- 将用户设备上检测到的属性值与配置扫描中列出的所需属性值进行比较。
- 生成输出，验证是否找到了所需的属性值。

注意：

创建端点分析策略的说明是通用指南。一个会话策略中可以包含许多设置。配置会话策略的具体说明可能包含配置特定设置的指导。但是，该设置可以是会话配置文件和策略中包含的众多设置之一。

EPA 表达式示例

以下是一些 EPA 组件的表达式示例，例如终止进程、删除文件和设备证书：

- 视窗:
  - 终止进程：`sys.client_expr(\“proc_0_perl\“) -killProcess processToKill.exe`
  - 设备证书：`sys.client_expr(“device-cert_0_0”)`
  - 删除文件：`sys.client_expr(\“proc_0_perl\“) -deletefiles “C:/removefile.txt”`
- Mac
  - 终止进程：`sys.client_expr(\“proc_0_perl\“) -killProcess processToKill.exe`
  - 设备证书:`sys.client_expr(“device-cert_0_0”)`
  - 删除文件:`sys.client_expr(\“proc_0_perl\“) -deletefiles “C:/removefile.txt”`

评估用户登录选项

用户登录时，可以选择跳过端点分析扫描。如果用户跳过扫描，NetScaler Gateway 会将此操作视为端点分析失败。如果用户扫描失败，他们只能通过无客户端访问获取访问权限。

例如，您希望通过使用 Citrix Secure Access 客户端为用户提供访问权限。要使用插件登录到 NetScaler Gateway，用户必须运行防病毒应用程序，例如 Norton Antivirus。如果用户设备未运行

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

该应用程序，用户只能使用 Receiver 登录并使用已发布的应用程序。您还可以配置无客户端访问，它将访问权限限制为指定的应用程序，例如 Outlook Web Access。

要配置 NetScaler Gateway 以实现此登录场景，您需要将限制性会话策略指定为默认策略。然后，当用户设备通过端点分析扫描时，您配置设置以将用户升级到特权会话策略。此时，用户拥有网络层访问权限，并且可以使用 Citrix Secure Access 客户端登录。

要配置 NetScaler Gateway 以首先强制执行限制性会话策略，请执行以下步骤：

- 配置全局设置，启用 ICA® Proxy 和所有其他必要的设置，如果指定应用程序未在用户设备上运行。
- 创建启用 Citrix Secure Access 客户端的会话策略和配置文件。
- 在会话策略的规则部分中创建表达式以指定应用程序，例如 `(client.application.process(symantec.exe) exists)`

  用户登录时，会话策略会首先应用。如果端点分析失败或用户跳过扫描，NetScaler Gateway 会忽略会话策略中的设置（会话策略中的表达式被视为 false）。因此，用户通过无客户端访问获得受限访问权限。如果端点分析通过，NetScaler Gateway 会应用会话策略，用户将通过 Citrix Secure Access 客户端获得完全访问权限。

跳过 EPA 扫描

您只能跳过后身份验证和高级身份验证的 EPA 扫描。所有受支持操作系统的浏览器都提供跳过 EPA 功能。用户必须单击访问网关时出现的“**跳过 EPA**”按钮。如果用户跳过扫描，NetScaler Gateway 会将此操作视为端点分析失败。如果用户扫描失败，他们只能通过无客户端访问获取访问权限。

另请参阅 `<https://support.citrix.com/article/CTX200748>`。

Ubuntu 支持的端点分析扫描

以下端点分析 (EPA) 扫描支持为 Ubuntu 操作系统安装的 EPA 插件。每个扫描的配置示例表达式与 EPA 扫描一起列出。您可以在身份验证策略中配置这些表达式。

- **文件**
  - **存在性**：sys.client_expr("file_0_/home/user/test.txt")
  - **MD5 校验和**: sys.client_expr("file_0_/home/user/test.txt_md5_ce780e271debcc29f551546e8db3368f")
  - **文件中的文本（支持正则表达式）**：sys.client_expr("file_0_/home/user/test.txt_search_cloud”)

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

- **进程**
  - **存在性**：sys.client_expr("proc_0_perl")
  - **MD5 校验和**: sys.client_expr("proc_0_perl_md5_ c060d3a5f97e27066cef8c116785567a")
  - **路径**：sys.client_expr("proc_0_perl_path_/usr/bin/perl")
- **文件系统设备或挂载点名称**：sys.client_expr("mountpoint_0_/sys”)

如果您正在使用高级策略，则可以从 GUI 生成每个扫描的表达式（**安全 > AAA > 策略 > 身份验证 > 高级策略 > EPA**）。

注意：

- 在表达式编辑器页面中，对于 Linux 客户端，您可以选择 **通用**，然后选择 **进程**、**文件** 或 **挂载点**。
- Linux 客户端不支持 MAC 地址的 EPA 扫描。

预认证策略和配置文件

重要：

端点分析旨在根据预定义的合规性标准分析用户设备，不强制执行或验证最终用户设备的安全性。建议使用端点安全系统来保护设备免受本地管理员攻击。

您可以将 NetScaler Gateway 配置为在用户通过 NetScaler Gateway 进行身份验证之前检查其设备。如果用户设备不符合您组织的要求，这可用于限制访问。设备检查可以通过特定于虚拟服务器的单独策略或全局策略来实现，如下面两个过程所述。

预认证策略由配置文件和表达式组成。您可以配置配置文件以使用表达式来允许或拒绝进程在用户设备上运行。例如，文本文件 clienttext.txt 正在用户设备上运行。当用户登录到 NetScaler Gateway 时，您可以根据文本文件是否正在运行来允许或拒绝访问。如果您不希望在进程运行时允许用户登录，则可以配置预认证配置文件以在用户登录之前停止该进程。

您可以为预认证策略配置以下设置：

- 表达式。包括以下设置以帮助您创建表达式：
  - 表达式。显示所有表达式。

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

- 匹配任意表达式。配置策略以匹配所选表达式列表中存在的任意表达式。
- 匹配所有表达式。配置策略以匹配所选表达式列表中存在的所有表达式。
- 表格表达式。使用 `OR (||) or AND (&&)` 运算符创建包含现有表达式的复合表达式。
- 高级自由格式。使用表达式名称和 `OR (||) and AND (&&)` 运算符创建自定义复合表达式。仅选择您需要的表达式，并从所选表达式列表中省略其他表达式。
- 添加。创建表达式。
- 修改。修改现有表达式。
- 删除。从复合表达式列表中删除所选表达式。
- 命名表达式。选择一个已配置的命名表达式。您可以从 NetScaler Gateway 上已有的表达式菜单中选择命名表达式。
- 添加表达式。将选定的命名表达式添加到策略。
- 替换表达式。将选定的命名表达式替换到策略。
- 预览表达式。当您选择命名表达式时，显示在 NetScaler Gateway 上配置的详细字符串。

配置预身份验证配置文件

使用 GUI 全局配置预身份验证配置文件

1. 在“配置”选项卡上，单击 **NetScaler Gateway**，然后单击 **全局设置**。
2. 在详细信息窗格中，在 **设置** 下，单击 **更改预身份验证设置**。
3. 在 **全局预身份验证设置** 对话框中，配置以下设置：

   a. 在 **操作** 中，选择 **允许或拒绝**。

   在端点分析发生后，拒绝或允许用户登录。

   b. 在 **要取消的进程** 中，输入进程。

   这指定了端点分析插件必须停止的进程。

   c. 在 **要删除的文件** 中，输入文件名。

   这指定了端点分析插件必须删除的文件。当您删除或取消进程时，会向最终用户显示通知。

   已删除进程(/en-us/netscaler-gateway/media/epa-scan-cancel-delete.png)

4. 在“表达式”中，您可以保留表达式 ns_true，或者为特定应用程序（例如防病毒或安全软件）构建表达式，然后单击 **确定**。

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

使用 GUI 配置预身份验证配置文件

1. 导航到 **NetScaler Gateway > 策略 > 身份验证/授权**，然后单击 **预身份验证 EPA**。
2. 在详细信息窗格的“**配置文件**”选项卡上，单击“**添加**”。
3. 在“**名称**”中，键入要检查的应用程序的名称。
4. 在“**操作**”中，选择“**允许**”或“**拒绝**”。
5. 在“**要取消的进程**”中，键入要停止的进程的名称。
6. 在“**要删除的文件**”中，键入要删除的文件的名称，例如 c:\clientext.txt，单击“**创建**”，然后单击“**关闭**”。

   这指定了端点分析插件必须删除的文件。当您删除或取消进程时，将向最终用户显示通知。

   已删除进程(/en-us/netscaler-gateway/media/epa-scan-cancel-delete.png)

如果您使用 GUI 配置预身份验证配置文件，则可以通过单击“**策略**”选项卡上的“**添加**”来创建预身份验证策略。在“**创建预身份验证策略**”对话框中，从“**请求配置文件**”菜单中选择配置文件。

将预配置表达式添加到预身份验证策略

NetScaler Gateway 附带预配置表达式，称为命名表达式。配置策略时，可以使用命名表达式。例如，您希望预身份验证策略检查具有更新病毒定义的赛门铁克防病毒 10。创建预身份验证策略并按照以下过程添加表达式。

创建预身份验证或会话策略时，可以在创建策略时创建表达式。然后，您可以将带有表达式的策略应用于虚拟服务器或全局。

以下步骤介绍了如何使用配置实用程序将预配置的防病毒表达式添加到策略。

将命名表达式添加到预身份验证策略

1. 导航到 **NetScaler Gateway > 策略 > 身份验证/授权**，然后单击 **预身份验证 EPA**。
2. 在详细信息窗格中，选择一个策略，然后单击 **打开**。
3. 在 **命名表达式** 旁边，选择 **防病毒**，然后从列表中选择防病毒产品。
4. 单击 **添加表达式**，单击 **创建**，然后单击 **关闭**。

配置自定义表达式

自定义表达式是您在策略中创建的表达式。创建表达式时，您需要配置表达式的参数。

您还可以创建自定义表达式来引用常用字符串。这简化了配置预身份验证策略的过程，也有助于维护已配置的表达式。

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

例如，您想为 Symantec 防病毒 10 创建一个自定义表达式，并确保病毒定义不超过三天。创建一个策略，然后配置表达式以指定病毒定义。

以下步骤展示了如何在预身份验证策略中创建表达式。您可以在会话策略中使用相同的步骤。

创建预身份验证策略和自定义表达式

1. 导航到 **NetScaler Gateway > 策略 > 身份验证/授权**，然后单击 **预身份验证 EPA**。
2. 在详细信息窗格中，单击 **添加**。
3. 在 **名称** 中，键入策略的名称。
4. 在“**请求配置文件**”旁边，单击“**新建**”。
5. 在“创建身份验证配置文件”对话框中，在“**名称**”中，键入配置文件的名称，在“**操作**”中，选择“**允许**”，然后单击“**创建**”。
6. 在“创建预身份验证策略”对话框中，在“**匹配任意表达式**”旁边，单击“**添加**”。
7. 在“**表达式类型**”中，选择“**客户端安全**”。
8. 配置以下内容：
   a. 在“**组件**”中，选择“**防病毒**”。
   b. 在“**名称**”中，键入应用程序的名称。
   c. 在“**限定符**”中，选择“**版本**”。
   d. 在“**运算符**”中，选择“**==**”。
   e. 在“**值**”中，键入值。
   f. 在“**新鲜度**”中，键入 3，然后单击“**确定**”。
9. 在“创建预身份验证策略”对话框中，单击“**创建**”，然后单击“**关闭**”。

配置自定义表达式后，它将添加到策略对话框中的“**表达式**”框中。

配置复合表达式

预身份验证策略可以有一个配置文件和多个表达式。如果配置复合表达式，则使用运算符来指定表达式的条件。例如，您可以配置复合表达式以要求用户设备运行以下防病毒应用程序之一：

- 赛门铁克防病毒 10
- 迈克菲防病毒 11
- Sophos 防病毒 4

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

您可以使用 OR 运算符配置表达式，以检查上述三个应用程序。如果 NetScaler Gateway 在用户设备上检测到任何应用程序的正确版本，则允许用户登录。策略对话框中的表达式如下所示：

```
av_5_Symantec_10 || av_5_McAfeevirusscan_11 || av_5_sophos_4
```

有关复合表达式的更多信息，请参阅配置复合表达式。

绑定预身份验证策略

创建预身份验证策略后，将其绑定到适用的级别。您可以将预身份验证策略绑定到虚拟服务器或全局。

全局创建并绑定预身份验证策略

1. 在“配置”选项卡上，单击 **NetScaler Gateway**，然后单击 **全局设置**。
2. 在详细信息窗格中，单击 **更改预身份验证设置**。
3. 在“全局预身份验证设置”对话框中，在 **操作** 中，选择 **允许** 或 **拒绝**。
4. 在 **名称** 中，键入策略的名称。
5. 在“**全局预身份验证设置**”对话框中，在 **命名表达式** 旁边，选择 **常规**，选择 **True** 值，单击 **添加表达式**，单击 **创建**，然后单击 **关闭**。

将预身份验证策略绑定到虚拟服务器

1. 在“配置”选项卡上，单击“**NetScaler Gateway**”，然后单击“**虚拟服务器**”。
2. 在详细信息窗格中，选择一个虚拟服务器，然后单击“**打开**”。
3. 在“配置 NetScaler Gateway 虚拟服务器”对话框中，单击“**策略**”选项卡，然后单击“**预身份验证**”。
4. 在“详细信息”下，单击“**插入策略**”，然后在“策略名称”下，选择预身份验证策略。
5. 单击“**确定**”。

解除绑定并删除预身份验证策略

如有必要，您可以从 NetScaler Gateway 中删除预身份验证策略。在删除预身份验证策略之前，请将其从虚拟服务器或全局解除绑定。

解除绑定全局预身份验证策略

1. 导航到“**NetScaler Gateway > 策略 > 身份验证/授权**”，然后单击“**预身份验证 EPA**”。
2. 在详细信息窗格中，选择一个策略，然后在“**操作**”中，单击“**全局绑定**”。
3. 在“**将预身份验证策略绑定/解除绑定到全局**”对话框中，选择一个策略，单击“**解除绑定策略**”，然后单击“**确定**”。

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

从虚拟服务器解除绑定预身份验证策略

1. 在“配置”选项卡上，单击“**NetScaler Gateway**”，然后单击“**虚拟服务器**”。
2. 在“**配置 NetScaler Gateway 虚拟服务器**”对话框中，单击“**策略**”选项卡，然后单击“**预身份验证**”。
3. 选择策略，然后单击“**解除绑定策略**”。

当预身份验证策略解除绑定时，您可以从 NetScaler Gateway 中删除该策略。

删除预身份验证策略

1. 导航到 **NetScaler Gateway > 策略 > 身份验证/授权**，然后单击 **预身份验证 EPA**。
2. 在详细信息窗格中，选择一个策略，然后单击 **删除**。

设置预身份验证策略的优先级

您可以有多个绑定到不同级别的预身份验证策略。例如，您有一个全局绑定的策略，用于检查特定的防病毒应用程序，以及一个绑定到虚拟服务器的防火墙策略。当用户登录时，绑定到虚拟服务器的策略首先应用。全局绑定的策略其次应用。

您可以更改预身份验证扫描的发生顺序。要使 NetScaler Gateway 首先应用全局策略，请更改绑定到虚拟服务器的策略的优先级编号，使其优先级高于全局绑定的策略。例如，将全局策略的优先级编号设置为一，将虚拟服务器策略的优先级编号设置为二。当用户登录时，NetScaler Gateway 首先运行全局策略扫描，然后运行虚拟服务器策略扫描。

更改预身份验证策略的优先级

1. 在“配置”选项卡上，单击 **NetScaler Gateway**，然后单击 **虚拟服务器**。
2. 在详细信息窗格中，选择一个虚拟服务器，然后单击 **打开**。
3. 在“策略”选项卡上，单击 **预身份验证**。
4. 在“优先级”下，键入策略的优先级编号，然后单击 **确定**。

后身份验证策略

重要提示：

端点分析旨在根据预定的合规性标准分析用户设备，而不是强制执行或验证最终用户设备的安全性。建议使用端点安全系统来保护设备免受本地管理员攻击。

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

后身份验证策略是一组通用规则，用户设备必须满足这些规则才能保持会话处于活动状态。如果策略失败，与 NetScaler Gateway 的连接将终止。配置后身份验证策略时，可以为可设置为条件的用户连接配置任何设置。

您可以使用会话策略来配置后身份验证策略。首先，创建策略适用的用户。然后，将用户添加到组中。接下来，将会话、流量策略和内部网应用程序绑定到该组。

您还可以指定组作为授权组。此类组允许您根据会话策略中的客户端设备检查表达式将用户分配到组。

如果用户设备不符合策略要求，您还可以配置后身份验证策略以将用户置于隔离组中。一个简单的策略包括客户端设备检查表达式和一条消息。当用户处于隔离组中时，用户可以登录 NetScaler Gateway；但是，他们对网络资源的访问权限受到限制。

您不能使用相同的会话配置文件和策略创建授权组和隔离组。创建后身份验证策略的步骤是相同的。创建会话策略时，您可以选择授权组或隔离组。您可以创建两个会话策略并将每个策略绑定到该组。

后身份验证策略也与 SmartAccess 结合使用。有关 SmartAccess 的更多信息，请参阅配置 SmartAccess。

注意：

此功能仅适用于 Citrix Secure Access 客户端。如果用户使用 Citrix Workspace 应用程序登录，则端点分析扫描仅在登录时运行。

配置后身份验证策略

您可以使用会话策略来配置后身份验证策略。一个简单的策略包括客户端设备检查表达式和一条消息。

使用 GUI 配置后身份验证策略

1. 展开 **NetScaler Gateway > 策略**，然后单击 **会话**。
2. 在详细信息窗格中，在“**策略**”选项卡上，单击“**添加**”。
3. 在“**名称**”中，键入策略的名称。
4. 在“**请求配置文件**”旁边，单击“**新建**”。
5. 在“**名称**”中，键入配置文件的名称。
6. 在“安全”选项卡上，单击“**高级设置**”。
7. 在“**客户端安全**”下，单击“**覆盖全局**”，然后单击“**新建**”。

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

8. 配置客户端设备检查表达式，然后单击“**创建**”。
9. 在“**客户端安全**”下，在“隔离组”中，选择一个组。
10. 在“**错误消息**”中，键入当身份验证后扫描失败时您希望用户收到的消息。
11. 在“授权组”下，单击“**覆盖全局**”，选择一个组，单击“**添加**”，单击“**确定**”，然后单击“**创建**”。
12. 在“**创建会话策略**”对话框中，在“命名表达式”旁边，选择“**常规**”，选择“**真值**”，单击“**添加表达式**”，单击“**创建**”，然后单击“**关闭**”。

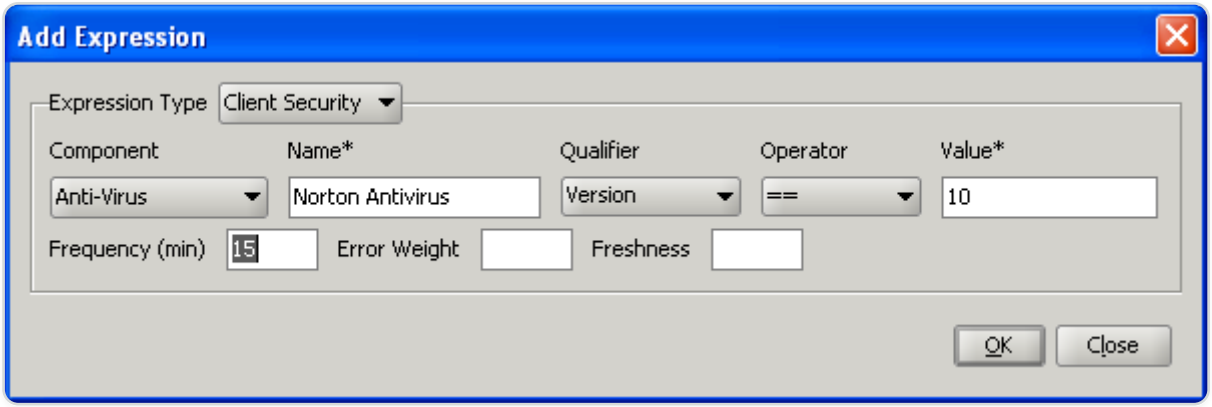
配置身份验证后扫描的频率

您可以将 NetScaler Gateway 配置为按指定间隔运行身份验证后策略。例如，您配置了一个客户端设备检查策略，并希望它每 10 分钟在用户设备上运行一次。您可以通过在策略中创建自定义表达式来配置此频率。

注意：

身份验证后策略的频率检查功能仅适用于 Citrix Secure Access 客户端。如果用户使用 Citrix Workspace 应用程序登录，则端点分析扫描仅在登录时运行。

配置客户端设备检查策略时，可以设置频率（以分钟为单位）。下图显示了可在“**添加表达式**”对话框中输入频率值的位置。



隔离组和授权组

当用户登录到 NetScaler Gateway 时，您可以将他们分配到在 NetScaler Gateway 或安全网络中的身份验证服务器上配置的组。如果用户未能通过身份验证后扫描，您可以将该用户分配到一个受限组（称为隔离组），该组限制对网络资源的访问。

您还可以使用授权组来限制用户对网络资源的访问。例如，您可能有一个合同人员组，他们只能访问您的电子邮件服务器和文件共享。当用户设备通过您在 NetScaler Gateway 上定义的设备检查要求时，用户可以动态地成为组的成员。

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

您可以使用全局设置或会话策略来配置绑定到用户、组或虚拟服务器的隔离组和授权组。您可以根据会话策略中的客户端设备检查表达式将用户分配到组。当用户是组的成员时，NetScaler Gateway 会根据组成员身份应用会话策略。

配置授权组

配置 Endpoint Analysis 扫描时，当用户设备通过扫描后，您可以将用户动态添加到授权组。例如，您可以创建一个 Endpoint Analysis 扫描来检查用户设备的域成员身份。在 NetScaler Gateway 上，创建一个名为 Domain-Joined Computers 的本地组，并将其添加为通过扫描的任何人的授权组。当用户加入该组时，用户将继承与该组关联的策略。

您无法全局绑定授权策略或将其绑定到虚拟服务器。当用户未配置为 NetScaler Gateway 上其他组的成员时，您可以使用授权组提供一组默认授权策略。

使用会话策略配置授权组

1. 导航到“**NetScaler Gateway > 策略**”，然后单击“**会话**”。
2. 在详细信息窗格的“策略”选项卡上，单击“**添加**”。
3. 在“**名称**”中，键入策略的名称。
4. 在“**请求配置文件**”旁边，单击“**新建**”。
5. 在“**名称**”中，键入配置文件的名称。
6. 在“安全”选项卡上，单击“**高级设置**”。
7. 在“授权组”下，单击“**覆盖全局**”，并从下拉列表中选择一个组。
8. 单击“**添加**”，单击“**确定**”，然后单击“**创建**”。
9. 在“**创建会话策略**”对话框中，在“命名表达式”旁边，选择“**常规**”，选择“**真值**”，单击“**添加表达式**”，单击“**创建**”，然后单击“**关闭**”。

创建会话策略后，您可以将其绑定到用户、组或虚拟服务器。

配置全局授权组

1. 展开“**NetScaler Gateway**”，然后单击“**全局设置**”。
2. 在详细信息窗格中，在“设置”下，单击“**更改全局设置**”。
3. 在“安全”选项卡上，单击“**高级设置**”。
4. 在“授权组”下，从下拉列表中选择一个组。
5. 单击“**添加**”，然后单击“**确定**”。

如果要从全局或会话策略中删除授权组，请在“安全设置 - 高级”对话框中，从列表中选择授权组，然后单击“**删除**”。

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

配置隔离组

配置隔离组时，您可以在会话配置文件中使用“安全设置 - 高级设置”对话框来配置客户端设备检查表达式。

配置隔离组的客户端设备检查表达式

1. 导航到 **NetScaler Gateway > Policies**，然后单击 **Session**。
2. 在详细信息窗格的“策略”选项卡上，单击 **Add**。
3. 在 **Name** 中，键入策略的名称。
4. 在 **Request Profile** 旁边，单击 **New**。
5. 在 **Name** 中，键入配置文件的名称。
6. 在“安全”选项卡上，单击 **Advanced Settings**。
7. 在 **Client Security** 下，单击 **Override Global**，然后单击 **New**。
8. 在 **Client Expression** 对话框中，配置客户端设备检查表达式，然后单击 **Create**。
9. 在 **Quarantine Group** 中，选择组。
10. 在“错误消息”中，键入描述用户问题的消息，然后单击 **Create**。
11. 在 **Create Session Policy** 对话框中，在“命名表达式”旁边，选择 **General**，选择 **True value**，单击 **Add Expression**。
12. 单击 **Create**，然后单击 **Close**。

创建会话策略后，将其绑定到用户、组或虚拟服务器。

注意：

如果端点分析扫描失败且用户被置于隔离组中，则只有在没有直接绑定到用户的策略且其优先级编号不高于或低于绑定到隔离组的策略时，绑定到隔离组的策略才有效。

配置全局隔离组

1. 展开 **NetScaler Gateway**，然后单击 **全局设置**。
2. 在详细信息窗格中，在“设置”下，单击 **更改全局设置**。
3. 在 **安全** 选项卡上，单击 **高级设置**。
4. 在 **客户端安全** 中，配置客户端设备检查表达式。
5. 在 **隔离组** 中，选择该组。
6. 在 **错误消息** 中，键入描述用户问题的消息，然后单击 **确定**。

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

用户设备的预身份验证设备检查表达式

重要提示：

端点分析旨在根据预设的合规性标准分析用户设备，但它不强制执行或验证最终用户设备的安全性。建议使用端点安全系统来保护设备免受本地管理员攻击。

NetScaler Gateway 在用户登录期间或会话期间的其他配置时间提供各种端点合规性检查，以帮助验证用户设备。只有通过这些检查的用户设备才允许建立 NetScaler Gateway 会话。

以下是您可以在 NetScaler Gateway 上配置的用户设备检查类型：

- 反垃圾邮件
- 防病毒
- 文件策略
- 互联网安全
- 操作系统
- 个人防火墙
- 进程策略
- 注册表策略
- 服务策略

如果用户设备上的设备检查失败，则在后续检查通过之前（对于定期检查），不会建立新连接；但是，通过现有连接流动的流量会继续通过 NetScaler Gateway 进行隧道传输。

您可以使用配置实用程序来配置预身份验证策略或会话策略中的设备检查表达式，这些策略旨在对用户设备执行检查。

配置防病毒、防火墙、互联网安全或反垃圾邮件表达式

您可以在**添加表达式**对话框中配置防病毒、防火墙、互联网安全和反垃圾邮件策略的设置。每个策略的设置都相同：不同之处在于您选择的值。例如，如果您想检查用户设备是否安装了 Norton 防病毒软件版本 10 和 ZoneAlarm Pro，您可以在会话或预身份验证策略中创建两个表达式，分别指定每个应用程序的名称和版本号。

当您选择客户端安全作为表达式类型时，您可以配置以下内容：

- 组件：客户端安全类型，例如防病毒、防火墙或注册表项。
- 名称：应用程序、进程、文件、注册表项或操作系统的名称。

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

- 限定符：表达式检查的组件版本或值。
- 运算符：检查值是否存在或是否等于该值。
- 值：用户设备上防病毒、防火墙、互联网安全或反垃圾邮件软件的应用程序版本。
- 频率：运行身份验证后扫描的频率（以分钟为单位）。
- 错误权重：当多个表达式具有不同的错误字符串时，分配给嵌套表达式中包含的每个错误消息的权重。该权重决定显示哪个错误消息。
- 新鲜度：定义病毒定义的有效期。例如，您可以配置表达式，使病毒定义不超过三天。

将客户端设备检查策略添加到预身份验证或会话策略

1. 在配置实用程序中，在导航窗格中，执行以下操作之一：
   a. 在配置实用程序中，在“配置”选项卡上，在导航窗格中，展开 **NetScaler Gateway > 策略**，然后单击 **会话**。
   b. 在配置实用程序中，在“配置”选项卡上的导航窗格中，展开 **NetScaler Gateway > 策略 > 身份验证/授权**，然后单击 **预身份验证 EPA**。
2. 在详细信息窗格的“策略”选项卡上，单击 **添加**。
3. 在“名称”中，键入策略的名称。
4. 在“匹配任意表达式”旁边，单击“添加”。
5. 在“添加表达式”对话框的“表达式类型”中，选择 **客户端安全**。
6. 配置以下设置：
   a. 在“组件”中，选择要扫描的项目。
   b. 在“名称”中，键入应用程序的名称。
   c. 在“限定符”中，选择 **版本**。
   d. 在“运算符”中，选择值。
   e. 在“值”中，键入客户端设备检查字符串，单击 **确定**，单击 **创建**，然后单击 **关闭**。

配置服务策略

服务是在用户设备上静默运行的程序。创建会话或预身份验证策略时，可以创建一个表达式，以确保在建立会话时用户设备正在运行特定服务。

配置服务策略

1. 在配置实用程序中，在导航窗格中，执行以下操作之一：

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

   a. 在配置实用程序中，在“配置”选项卡上的导航窗格中，展开 **NetScaler Gateway > 策略**，然后单击“会话”。
   b. 在配置实用程序中，在“配置”选项卡上的导航窗格中，展开 **NetScaler Gateway > 策略 > 身份验证/授权**，然后单击“预身份验证 EPA”。
2. 在详细信息窗格的“策略”选项卡上，单击“添加”。
3. 在“名称”中，键入策略的名称。
4. 在“匹配任意表达式”旁边，单击“添加”。
5. 在“添加表达式”对话框中，在“表达式类型”中，选择“客户端安全”。
6. 配置以下设置：
   a. 在“组件”中，选择“服务”。
   b. 在“名称”中，键入服务的名称。
   c. 在“限定符”中，留空或选择“版本”。
   d. 根据您在“限定符”中的选择，执行以下操作之一：
      - 如果留空，请在“运算符”中选择 == 或 \!=
      - 如果您选择了“版本”，请在“运算符”中，在“值”中键入值，单击“确定”，然后单击“关闭”。

您可以在基于 Windows 的计算机上的以下位置查看所有可用服务及其状态的列表：

控制面板 > 管理 工具 > 服务

> **注意：**
>
> 每个服务的服务名称与其列出的名称不同。通过查看 “属性”对话框来检查服务名称。

配置进程策略

创建会话或预身份验证策略时，您可以定义一个规则，要求所有用户设备在用户登录时运行特定进程。该进程可以是任何应用程序，包括自定义应用程序。

注意：Windows 计算机上运行的所有进程列表显示在 Windows 任务管理器的“**进程**”选项卡上。

配置进程策略

1. 在配置实用程序中，在导航窗格中，执行以下操作之一：
   a. 在配置实用程序中，在“配置”选项卡上，在导航窗格中，展开 **NetScaler Gateway \ > 策略**，然后单击“会话”。

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

   b. 在配置实用程序中，在“配置”选项卡上，在导航窗格中，展开 **NetScaler Gateway \> 策略 \> 身份验证/授权**，然后单击“预身份验证 EPA”。

2. 在详细信息窗格中，在“策略”选项卡上，单击“添加”。
3. 在“名称”中，键入策略的名称。
4. 在“匹配任意表达式”旁边，单击“添加”。
5. 在“添加表达式”对话框中，在“表达式类型”中，选择“客户端安全”。
6. 配置以下设置：

   a. 在“组件”中，选择“进程”。
   b. 在“名称”中，键入应用程序的名称。
   c. 在“运算符”中，选择 EXISTS 或 NOTEXISTS，单击“确定”，然后单击“关闭”。

当您配置端点分析策略（预身份验证或后身份验证）以检查进程时，可以配置 MD5 校验和。

创建策略表达式时，可以将 MD5 校验和添加到要检查的进程中。例如，如果您正在检查 notepad.exe 是否在用户设备上运行，则表达式为：
CLIENT.APPLICATION.PROCESS(notepad.exe_md5_388b8fbc36a8558587afc90fb23a3b00) EXISTS

配置操作系统策略

创建会话或预身份验证策略时，可以配置客户端设备检查字符串，以确定用户登录时用户设备是否正在运行特定的操作系统。您还可以配置表达式以检查特定的 Service Pack 或修补程序。

Windows 和 Macintosh 的值如下：

操作系统	值
macOS X	macOS
Windows 8.1 系统	win8.1
Windows 8 系统	win8
视窗 7	win7
视窗 维斯塔	维斯塔
视窗 XP	`winxp`

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

操作系统	值
视窗服务器 2008	win2008
视窗服务器 2003	win2003
视窗 2000 服务器	win2000
Windows 64 位平台	win64

使用 GUI 配置操作系统策略

1. 在导航窗格中，执行以下操作之一：
   a. 导航到 **NetScaler Gateway > 策略**，然后单击 **会话**。
   b. 导航到 **NetScaler Gateway > 策略 > 预身份验证**。
2. 在详细信息窗格中，在 **策略** 选项卡上，单击 **添加**。
3. 在 **名称** 中，键入策略的名称。
4. 在 **请求操作** 中，选择现有操作或创建一个新操作。
5. 单击 **表达式编辑器**。
6. 在 **选择表达式类型** 中，选择 **客户端安全**。
7. 配置以下设置：
   a. 在 **组件** 中，选择 **操作系统**。
   b. 在 **名称** 中，键入操作系统的名称。
   c. 在限定符中，执行以下操作之一：
      - 将字段留空
      - 选择 **Service Pack**
      - 选择 **Hotfix**
      - 选择 **版本** (仅适用于 macOS)
   d. 根据您在步骤 7 中的选择，在“运算符”中，执行以下操作之一：
      - 如果“限定符”为空，在“运算符”中，选择 EQUAL (= =)、NOTEQUAL (\!=)、EXISTS 或 NOTEXISTS。
      - 如果您选择了 Service Pack 或 Hotfix，请选择运算符并在“值”中键入值。

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

8. 单击 **完成**，然后单击 **关闭**。

如果您正在配置服务包，例如 client.os `(winxp).sp`，如果 **值** 字段中没有数字，NetScaler Gateway 将返回错误消息，因为表达式无效。

如果操作系统存在服务包，例如 Service Pack 3 和 Service Pack 4，您可以仅为 Service Pack 4 配置检查，因为 Service Pack 4 的存在自动表明以前的服务包也存在。

配置注册表策略

当您创建会话或预身份验证策略时，您可以检查用户设备上注册表项的存在和值。只有当特定条目存在或具有配置值或更高值时，才会建立会话。

配置注册表表达式时，请遵循以下准则：

- 使用四个反斜杠分隔键和子键，例如

  HKEY_LOCAL_MACHINE\\\\\\\\SOFTWARE

- 使用下划线分隔子键和关联的值名称，例如

  HKEY_LOCAL_MACHINE\\\\\\\\SOFTWARE\\\\\\\\VirusSoftware_Version

- 反斜杠 (\\) 用于表示空格，例如以下两个示例：

  HKEY_LOCAL_MACHINE\\\\\\\\SOFTWARE\\\\Citrix\\\\\\\\Secure\\ Access\\ Client_ProductVersion

  CLIENT.REG(HKEY_LOCAL_MACHINE\\\\\\\\Software\\\\\\\\Symantec\\\\Norton\\ 防病毒_版本).VALUE == 12.8.0.4 -频率 5

以下是一个注册表表达式，用于在用户登录时查找 Citrix Secure Access™ 客户端注册表项：

CLIENT.REG(`secureaccess`).VALUE==HKEY_LOCAL_MACHINE\\\\\\\\SOFTWARE\\\\\\\\CITRIX\\\\\\\\Secure\\Access\\Client_ProductVersion

注意：

如果您正在扫描注册表项和值，并在“表达式”对话框中选择“高级自由格式”，则表达式必须以 CLIENT.REG 开头。

注册表检查支持以下五种最常见的类型：

- HKEY_CLASSES_ROOT

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

- HKEY_CURRENT_USER
- HKEY_LOCAL_MACHINE
- HKEY_USERS
- HKEY_CURRENT_CONFIG

要检查的注册表值使用以下类型：

- 字符串

  对于字符串值类型，会检查大小写敏感性。

- DWORD

  对于 DWORD 类型，会比较值并且必须相等。

- 扩展字符串

  其他类型（例如二进制和多字符串）不受支持。

- 仅支持“==”比较运算符。
- 其他比较运算符（例如 \<、\> 和区分大小写的比较）不受支持。
- 注册表字符串总长度必须小于 256 字节。

您可以向表达式添加值。该值可以是软件版本、Service Pack 版本或注册表中出现的任何其他值。如果注册表中的数据值与您正在测试的值不匹配，则用户将被拒绝登录。

注意：

您无法扫描子项中的值。扫描必须与命名值和关联的数据值匹配。

配置注册表策略

1. 在配置实用程序中，在导航窗格中，执行以下操作之一：

   a. 在配置实用程序中，在“配置”选项卡上的导航窗格中，展开 **NetScaler Gateway \ > 策略**，然后单击“会话”。

   b. 在配置实用程序中，在“配置”选项卡上的导航窗格中，展开 **NetScaler Gateway \> 策略 \ > 身份验证/授权**，然后单击“预身份验证 EPA”。

2. 在详细信息窗格中，在“策略”选项卡上，单击“添加”。
3. 在“名称”中，键入策略的名称。
4. 在“匹配任意表达式”旁边，单击“添加”。

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

5. 在“添加表达式”对话框中，在“表达式类型”中，选择“客户端安全”。
6. 配置以下设置：
   a. 在“组件”中，选择“注册表”。
   b. 在“名称”中，键入注册表项的名称。
   c. 在“限定符”中，留空或选择“值”。
   d. 在“运算符”中，执行以下操作之一：
      - 如果“限定符”留空，请选择“EXISTS”或“NOTEXISTS”。
      - 如果您在“限定符”中选择了“值”，请选择“==”或“\!=”。
   e. 在“值”中，键入注册表编辑器中显示的值，单击“确定”，然后单击“关闭”。

配置复合客户端设备检查表达式

您可以组合客户端设备检查字符串以形成复合客户端设备检查表达式。

NetScaler Gateway 中支持的布尔运算符包括：

- 与 (&&)
- 或 (||)
- 非 (\!)

为了提高精确度，您可以使用括号将字符串组合在一起。

注意：

如果您使用命令行配置表达式，请使用括号将设备检查表达式组合在一起以形成复合表达式。使用括号可以提高对客户端表达式的理解和调试效率。

使用 AND (&&) 运算符配置策略

AND (&&) 运算符通过组合两个客户端设备检查字符串来工作，这样只有当两个检查都为真时，复合检查才通过。表达式从左到右进行评估，如果第一个检查失败，则不执行第二个检查。

您可以使用关键字“AND”或符号“&&”来配置 AND (&&) 运算符。

示例：

以下是一个客户端设备检查，用于确定用户设备是否安装并运行了 Sophos 防病毒软件的 7.0 版本。它还会检查同一台计算机上是否正在运行 Net Logon 服务。

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

`CLIENT.APPLICATION.AV(sophos).version==7.0 AND CLIENT.SVC(netlogon) EXISTS`

此字符串也可以配置为：

`CLIENT.APPLICATION.AV(sophos).version==7.0 && CLIENT.SVC(netlogon) EXISTS`

使用 OR (||) 运算符配置策略

OR `(||)` 运算符通过组合两个设备检查字符串来工作。当任一检查为真时，复合检查通过。表达式从左到右进行评估，如果第一个检查通过，则不执行第二个检查。如果第一个检查未通过，则执行第二个检查。

您可以使用关键字 `OR` 或符号 `||` 来配置 OR `(||)` 运算符。

示例：

以下是一个客户端设备检查，用于确定用户设备上是否存在文件 `c:\\file.txt` 或是否正在运行 `putty.exe` 进程。

`client.file(c:\\\\\\\\file.txt) EXISTS) OR (client.proc(putty.exe) EXISTS`

此字符串也可以配置为

`client.file(c:\\\\\\\\file.txt) EXISTS) || (client.proc(putty.exe) EXISTS`

使用 NOT (\!) 运算符配置策略

NOT (\!) 或非运算符用于否定客户端设备检查字符串。

示例：

如果文件 c:\\sophos_virus_defs.dat 的创建时间不超过两天，则以下客户端设备检查通过：

`\!(client.file(c:\\\\\\\\sophos\_virus\_defs.dat).timestamp==2dy)`

nFactor 中作为 EPA 组件的设备证书

重要提示：

端点分析旨在根据预定的合规性标准分析用户设备，而不是强制执行或验证最终用户设备的安全性。建议使用端点安全系统来保护设备免受本地管理员攻击。

设备证书可以在 nFactor 中配置为 EPA 组件。设备证书可以作为 EPA 的一部分以任何因素出现。

在 nFactor 中将设备证书配置为 EPA 组件的优势如下。

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

- 设备证书验证失败不会导致登录失败。根据配置，登录可以继续，并且用户可以被置于具有有限访问权限的组中。
- 由于设备证书检查是策略驱动的，因此您可以根据设备证书身份验证选择性地允许或阻止对公司内部网资源的访问。例如，设备证书身份验证可用于仅在公司管理的笔记本电脑上提供对 Office 365 应用程序的条件访问。

设备证书验证不能作为定期 EPA 扫描的一部分。

重要提示：

- 默认情况下，Windows 要求管理员权限才能访问设备证书。要为非管理员用户添加设备证书检查，您必须在设备上安装与 EPA 插件版本相同的 VPN 插件。
- 您可以向网关添加多个 CA 证书并验证设备证书。
- 如果您在客户端计算机上安装了两个或更多设备证书，用户在登录 NetScaler Gateway 或端点分析扫描运行之前必须选择正确的证书。
- 创建设备证书时，它必须是 X.509 证书。
- 您必须将 CA 证书绑定到 VPN 虚拟服务器。如果设备证书由中间 CA 颁发，则中间 CA 证书和根 CA 证书都必须绑定到 VPN 虚拟服务器。

在 nFactor 中将设备证书配置为 EPA 组件

使用 CLI 将 nFactor 中的设备证书配置为 EPA 组件：

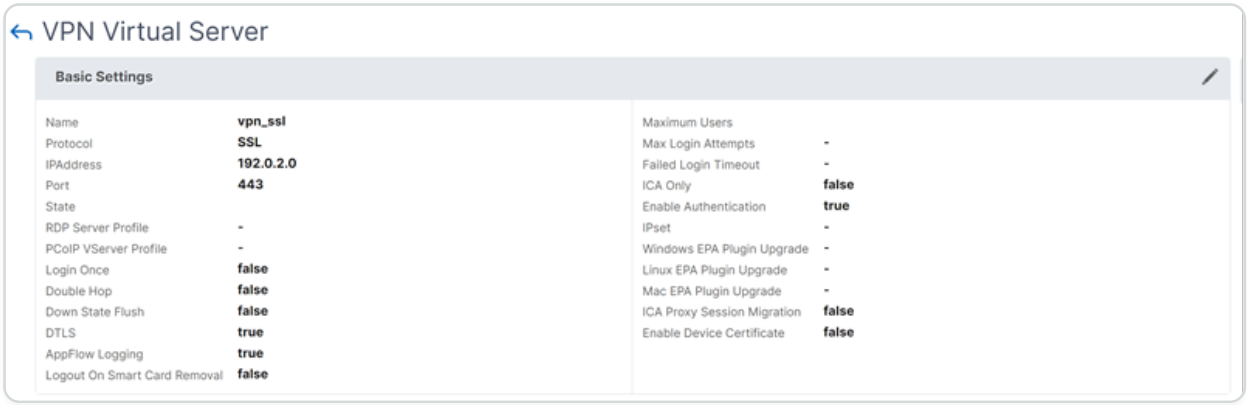
在命令提示符下，键入；

```
add authentication epaAction epa-act -csecexpr sys.client_expr("device-cert_0_0") -defaultgroup epa_pass -quarantine_group epa_fail
```

使用 GUI 将 nFactor 中的设备证书配置为 VPN 虚拟服务器的 EPA 组件：

1. 在 NetScaler GUI 中，导航到 **配置 > NetScaler Gateway > 虚拟服务器**。
2. 在 **NetScaler Gateway Virtual Servers** 页面上，选择要修改的虚拟服务器，然后单击 **Edit**。
3. 在 **VPN Virtual Server** 页面上，单击“编辑”图标。

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

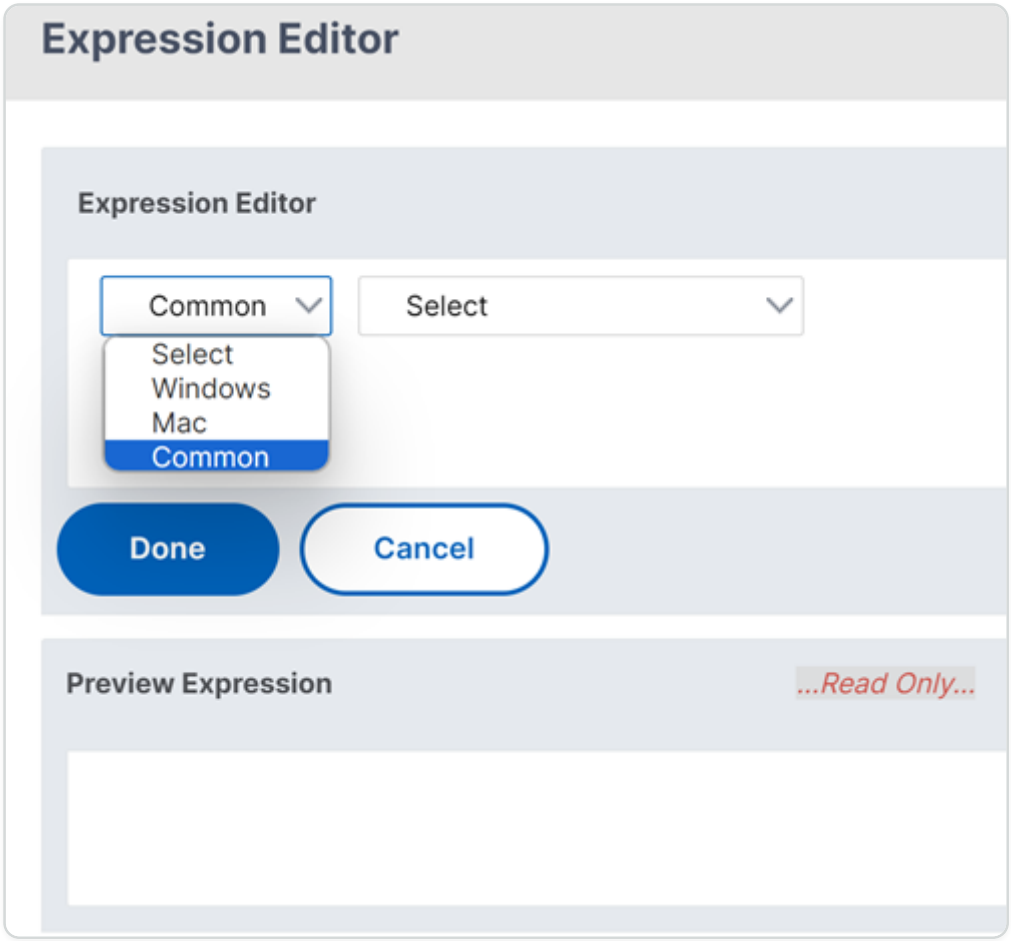


4. 单击 **More**。
5. 在“CA for Device Certificate”部分中单击 **+**，然后单击“确定”。

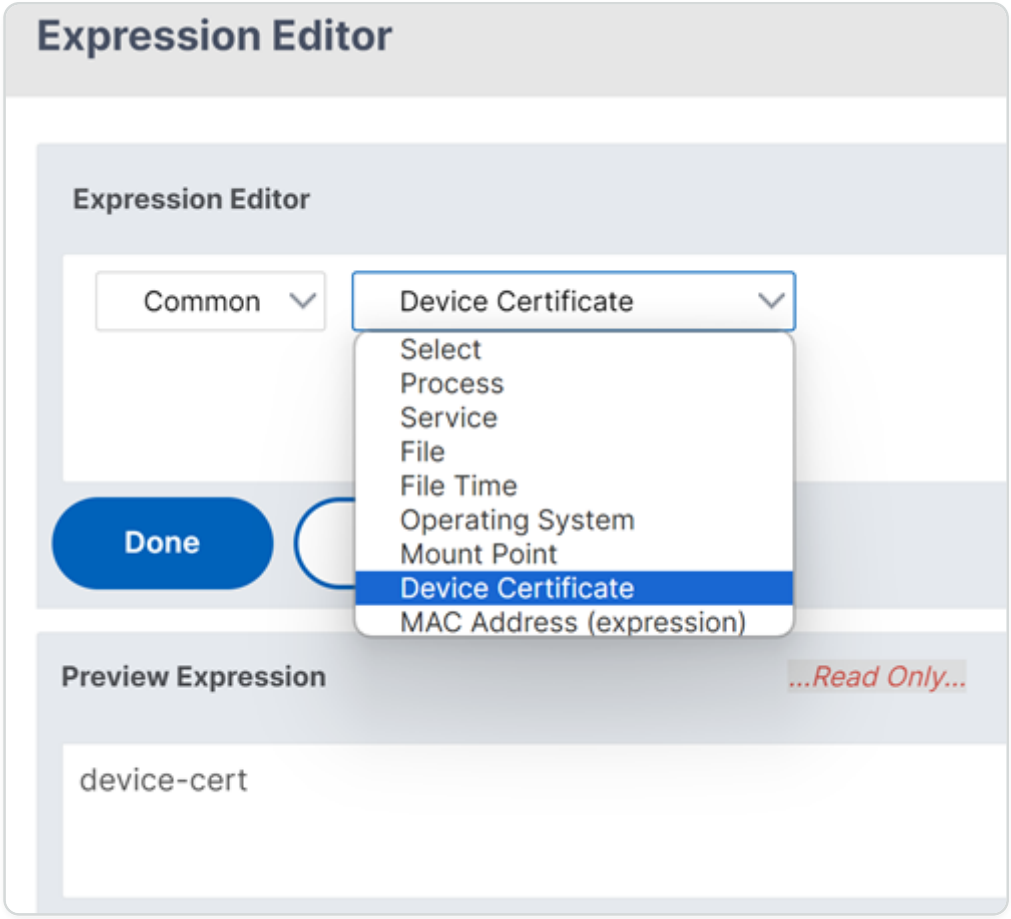
> **注意：**
>
> 不要选中 **Enable Device Certificate** 复选框。启用它会在经典 EPA 中启用设备证书验证。

6. 在 NetScaler GUI 中，导航到 **配置 > 安全 > AAA – 应用程序流量 > 策略 > 身份验证 > 高级策略 > 操作 > EPA**。
7. 在 **Authentication EPA Action** 页面上，单击 **Add**。您可以单击 **Edit** 以编辑现有 EPA 操作。
8. 在 **Create Authentication EPA Action** 页面上，为必填字段提供值以创建身份验证 EPA 操作，然后单击 **EPA Editor** 链接。
9. 从 **Expression Editor** 菜单中选择 **Common**。

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



10. 从出现的后续菜单中选择**设备证书**，然后单击**完成**以完成配置。



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

通过使用 GUI 将 nFactor 中的设备证书配置为身份验证虚拟服务器的 EPA 组件：

1. 在 NetScaler 图形用户界面中，导航到 **安全 > AAA-应用程序流量 > 虚拟服务器**。
2. 在**NetScaler Gateway 虚拟服务器**页面上，选择要修改的虚拟服务器，然后单击“编辑”。
3. 在**身份验证虚拟服务器**页面上，单击“编辑”图标。
4. 单击**更多**。
5. 在**设备证书的 CA** 部分旁边单击**添加**。
6. 选择要添加的证书，然后单击**确定**以完成配置。
7. 重复 **步骤 6 到步骤 10** 以完成配置。

参考

- 配置预身份验证配置文件
- 绑定预身份验证策略
- 设置预身份验证策略的优先级
- 配置身份验证后策略
- 配置身份验证后扫描的频率

EPA 扫描作为 nFactor 身份验证的一个因素

重要提示：

端点分析旨在根据预定的合规性标准分析用户设备，而不是强制执行或验证最终用户设备的安全性。建议使用端点安全系统来保护设备免受本地管理员攻击。

以下是 nFactor EPA 的一些基本实体。

EPA 操作： EPA 操作是为 nFactor EPA 引入的一种操作类型。它包含以下内容：

- 客户端设备检查表达式：此表达式将发送到网关 EPA 插件进行评估。
- 成功组：如果配置了此组，并且 EPA 结果为 true，则此组将继承到网关会话。
- 隔离组：如果配置了此组，并且 EPA 结果为 false，则此组将继承到网关会话。
- killProcess：这表示 EPA 进程必须终止的进程名称。
- deleteFiles：指定 EPA 进程必须删除的文件的逗号分隔路径。

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

组可以在会话生命周期内用于确定客户端是否满足特定的 EPA 条件。 如果在给定因素下，EPA 失败且上次操作不包含“隔离组”，则该用户的身份验证将终止。 如果存在“隔离组”，则身份验证将继续，管理员可以检查该组以授予有限访问权限。有关更多详细信息，请参阅EPA 执行。

要使用 GUI 配置身份验证 EPA 操作：

- 导航到 **安全 > AAA - 应用程序流量 > 策略 > 身份验证 > 高级策略 > 操作 > 身份验证 EPA 操作**。
- 配置以下参数：
  - 名称：EPA 操作的名称。
  - 默认组：当 EPA 检查成功时选择的默认组。
  - 隔离组：当 EPA 检查失败时选择的隔离组。
  - 终止进程：一个字符串，指定要由 EPA 工具终止的进程名称。多个进程之间用逗号分隔。
  - 删除文件：一个字符串，指定要由 EPA 工具删除的文件的路径和名称。多个文件之间用逗号分隔。
  - 表达式：要发送到客户端的客户端安全表达式。

要使用 CLI 配置身份验证 EPA 操作：

```
add authentication epaAction CWA version check scan -csecexpr
sys.client_expr("sys_0_MAC-CWA_version_>=_23.9.0.99")
```

前面的 CLI 示例表示一个 EPA 扫描，用于验证 macOS 计算机上的 Citrix Workspace™ 应用程序版本。

EPA 策略： 在 nFactor 中，所有策略都使用相同的语法“add authentication policy”添加。但是，操作类型将策略限定为 EPA 策略。

EPA 因子： EPA 因子是一个常规策略标签。没有名为 EPA 因子 的实体。一旦 EPA 策略绑定到某个因子，它就会继承某些属性，使其成为 EPA 因子。

注意：

本文档中，“EPA 因子”一词通常用于指代具有 EPA 策略的因子。

EPA – 隔离： 当设备未能通过端点分析 (EPA) 扫描时，配置的隔离组会授予有限访问权限，而不是立即拒绝访问。

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

如果 EPA 检查失败且上次 EPA 操作包含隔离组，则用户将被添加到隔离组，并且不会评估下一个因子。将隔离组配置为独立的受限访问级别。

隔离用户的访问权限由绑定到隔离组的策略控制。这些策略可以限制应用程序或资源访问，强制执行仅修复工作流，或与合规用户相比降低权限。

如果 EPA 检查失败，并且在上次操作中未配置隔离组，则身份验证将失败，并且访问将被拒绝。

nFactor 中的 EPA 还使用以下实体：

- **LoginSchema：** 登录表单的 XML 表示。它定义了登录表单的“视图”，并且还具有“因子”的属性。
- **策略标签或策略因子：** 它是在身份验证的给定阶段尝试的一组策略。
- **虚拟服务器标签：** 虚拟服务器也是一个策略标签，可以将策略绑定到虚拟服务器。但是，虚拟服务器是各种策略标签的集合，因为它是用户访问的入口点。
- **下一个因子：** 它用于指定在给定身份验证策略成功后要采用的策略标签/因子。
- **NO_AUTHN 策略：** 其操作始终成功的特殊策略。
- **直通因子：** 是一种登录架构不包含视图的策略标签/因子。它指示 NetScaler 设备在给定因子处继续身份验证，无需用户干预。

有关更多信息，请参阅 nFactor 概念、实体和术语。

EPA 因子互斥

EPA 因子包含一个或多个 EPA 策略。一旦 EPA 策略绑定到某个因子，该因子上就不允许使用常规身份验证策略。此限制旨在提供最佳用户体验和端点分析的清晰分离。此规则的唯一例外是 NO_AUTHN 策略。由于 NO_AUTHN 策略是用于模拟“失败跳转”的特殊策略，因此它在 EPA 因子中是允许的。

EPA 执行

在任何给定因子（包括虚拟服务器因子）中，在提供登录表单之前，NetScaler 设备会检查该因子是否配置了 EPA。如果是，它会向客户端 (UI) 发送特定响应，从而触发 EPA 序列。此序列包括客户端请求客户端设备检查表达式并发送结果。 因子中所有策略的客户端设备检查表达式会一次性发送给客户端。一旦 NetScaler 设备获得结果，所有操作中的每个表达式都会按顺序进行评估。第一个导致 EPA 成功的操作会终止该因子，并且如果配置了 DefaultGroup，则会将其继承到会话中。如果遇到 NO_AUTHN 策略，则视为自动成功。如果指定了 nextFactor，设备将继续使用该因子。否则，身份验证终止。 此条件也适用于第一个因子。如果在虚拟服务器上的 EPA 之后没有身份验证策略因子，则身份验证终止。这与经典策略行为不同，在经典策略行为中，用户在 EPA 后总是会看到登录页面。 但是，如果没有成功的 EPA 策略，则 NetScaler Gateway 会查看为该因子或级联中的最

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

后一个 EPA 策略配置的隔离组。如果最后一个策略配置了隔离组，则该组将添加到会话中并检查 nextFactor。如果存在 nextFactor，则身份验证将继续到该因子。否则，身份验证完成。

配置 EPA 扫描在身份验证后运行

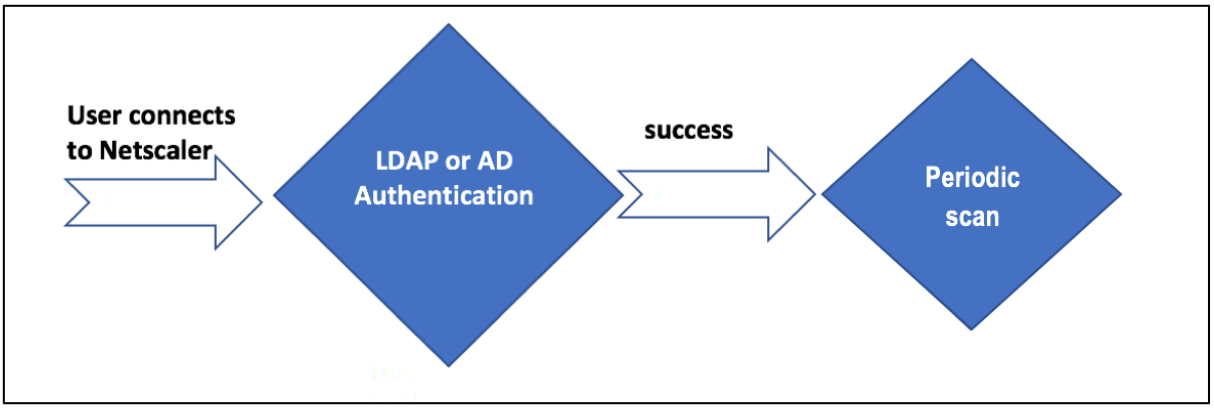
您可以配置 EPA 扫描在身份验证后运行。在以下示例中，EPA 扫描用作 nFactor 或多因素身份验证中的最终检查。在此设置中，如果 EPA 扫描在此类检查期间失败，则会话将终止。

注意：

在配置具有多个 EPA 策略的 nFactor 身份验证时，建议不要将它们顺序放置，因为这可能会导致用户多次提示启动 EPA 插件。相反，建议将 EPA 策略与其他身份验证方法交替使用。

示例：

- **推荐：** EPA 因素 1 > LDAP > EPA 因素 2
- **不推荐：** LDAP > EPA 因素 1 > EPA 因素 2



- 用户尝试连接到 NetScaler® Gateway 虚拟 IP。
- 系统会向用户呈现一个包含用户名和密码字段的登录页面，供用户提供登录凭据。使用这些凭据，将在后端执行 LDAP 或基于 AD 的身份验证。如果成功，系统会向用户显示一个弹出窗口，以授权 EPA 扫描。
- 用户授权后，将执行 EPA 扫描，并根据用户客户端设置的成功或失败情况提供访问权限。
- 如果扫描成功，将定期执行 EPA 扫描，以确认配置的设备检查要求仍然满足。
- 如果在任何此类检查期间 EPA 扫描失败，会话将被终止。

先决条件

假定已完成以下配置：

- VPN 虚拟服务器、网关和身份验证虚拟服务器配置

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

- LDAP 服务器配置和相关策略。

以下部分介绍了所需的策略和策略标签配置，以及策略和策略标签到身份验证配置文件的映射。

nFactor 策略和策略标签映射中的 EPA(/en-us/netscaler-gateway/media/epa-in-nfactor-policy-labels.png)

在 CLI 上

1. 创建操作以在 LDAP 身份验证之前执行 EPA 扫描，并将其与 EPA 扫描策略关联。

   ```
   add authentication epaAction pre-ldap-epa-action -csecexpr
   "sys.client_expr (\"proc_2_firefox\")"



   add authentication Policy pre-ldap-epa-pol -rule true -action pre-ldap-
   epa-action
   ```

   上述表达式扫描进程“Firefox”是否正在运行。EPA 客户端每 2 分钟检查一次进程是否存在，这由扫描表达式中的数字“2”表示。

2. 配置策略标签 `pre-ldap-epa-label`，该标签承载 EPA 扫描策略。

   ```
   add authentication policylabel pre-ldap-epa-label -loginSchema
   LSCHEMA_INT
   ```

   注意：

   LSCHEMA_INT 是一个内置的无架构（noschema）架构，这意味着在此步骤中不会向用户显示额外的网页。

3. 将步骤 1 中配置的策略与步骤 2 中配置的策略标签关联。这完成了身份验证机制。

   ```
   bind authentication policylabel pre-ldap-epa-label -policyName pre-
   ldap-epa-pol -priority 100 -gotoPriorityExpression END
   ```

4. 配置 LDAP 操作和策略。

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

```
add authentication ldapAction ldap-act -serverIP 192.0.2.0 -ldapBase
"dc=example,dc=net" -ldapBindDn user1@example.net -ldapBindDnPassword
1.cloud -ldapLoginName samAccountName -groupAttrName memberOf
-subAttributeName CN -passwdChange ENABLED



add authentication Policy ldap-pol -rule true -action ldap-act
```

5. 创建启用 SSO 的登录架构。

```
add authentication loginSchema ldap-schema -authenticationSchema "/
nsconfig/loginschema/LoginSchema/SingleAuth.xml" -SSOCredentials Yes
```

6. 配置策略标签 `ldap-pol-label`，该标签承载 LDAP 身份验证策略。

```
add authentication policylabel ldap-pol-label -loginSchema ldap-schema
```

7. 将步骤 5 中配置的登录架构绑定到步骤 6 中配置的策略标签。

```
bind authentication policylabel ldap-pol-label -policyName ldap-pol
-priority 100 -gotoPriorityExpression NEXT
```

8. 创建操作以在 LDAP 身份验证后执行 EPA 扫描，并将其与 EPA 扫描策略关联。

```
add authentication epaAction post-ldap-epa-action -csecexpr
"sys.client_expr (\"proc_2_chrome\")"



add authentication Policy post-ldap-epa-pol -rule true -action post-
ldap-epa-action



add authentication policylabel post-ldap-epa-label -loginSchema
LSCHEMA_INT
```

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

```
bind authentication policylabel post-ldap-epa-label -policyName post-
ldap-epa-pol -priority 100 -gotoPriorityExpression
```

9. 总而言之，将策略 `pre-ldap-epa-pol` 与身份验证虚拟服务器关联，下一步指向策略标签 `ldap-pol-label` 以执行 EPA 扫描。

```
bind authentication vserver user.auth.test -policy pre-ldap-epa-pol
-priority 100 -nextFactor ldap-pol-label -gotoPriorityExpression NEXT



bind authentication policylabel ldap-pol-label -policyName ldap-pol
-priority 100 -gotoPriorityExpression NEXT -nextFactor post-ldap-epa-
label
```

注意：

- 在配置为多个因素的周期性 EPA 中，将考虑具有周期性 EPA 配置的最新因素。
- 周期性扫描只能使用 EPA 插件运行，而不能在浏览器上运行。
- 在第一个示例中，EPA 是第一个因素，扫描会查找进程“Firefox”。
- 如果 EPA 扫描成功，它将导致 LDAP 身份验证，然后是下一个 EPA 扫描，该扫描会查找进程“Chrome”。
- 当多个周期性扫描配置为不同因素时，最新的扫描优先。在这种情况下，EPA 插件会在登录成功后每 2 分钟扫描一次进程“Chrome”。

在 GUI 上（使用 nFactor Visualizer）

您可以使用 GUI 上的 nFactor visualizer 将高级 EPA 扫描配置为一个因素。在以下示例中，我们使用 LDAP 作为第一个因素，EPA 作为下一个因素。

1. 为 nFactor 流创建第一个因素。

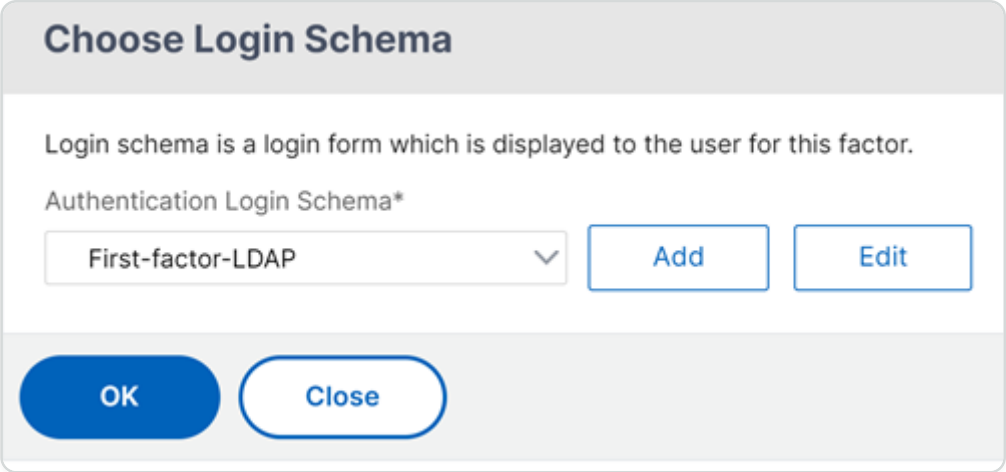
   - 导航到“**安全 > AAA - 应用程序流量 > nFactor Visualizer > nFactor 流**”，然后单击“**添加**”。
   - 单击“**+**”以添加 nFactor 流。
   - 添加一个因素，然后单击“**创建**”。

   nFactor 流序列中的 EPA(/en-us/netscaler-gateway/media/nfactor-add-factor.png)

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

2. 为第一个因素创建登录架构和策略。

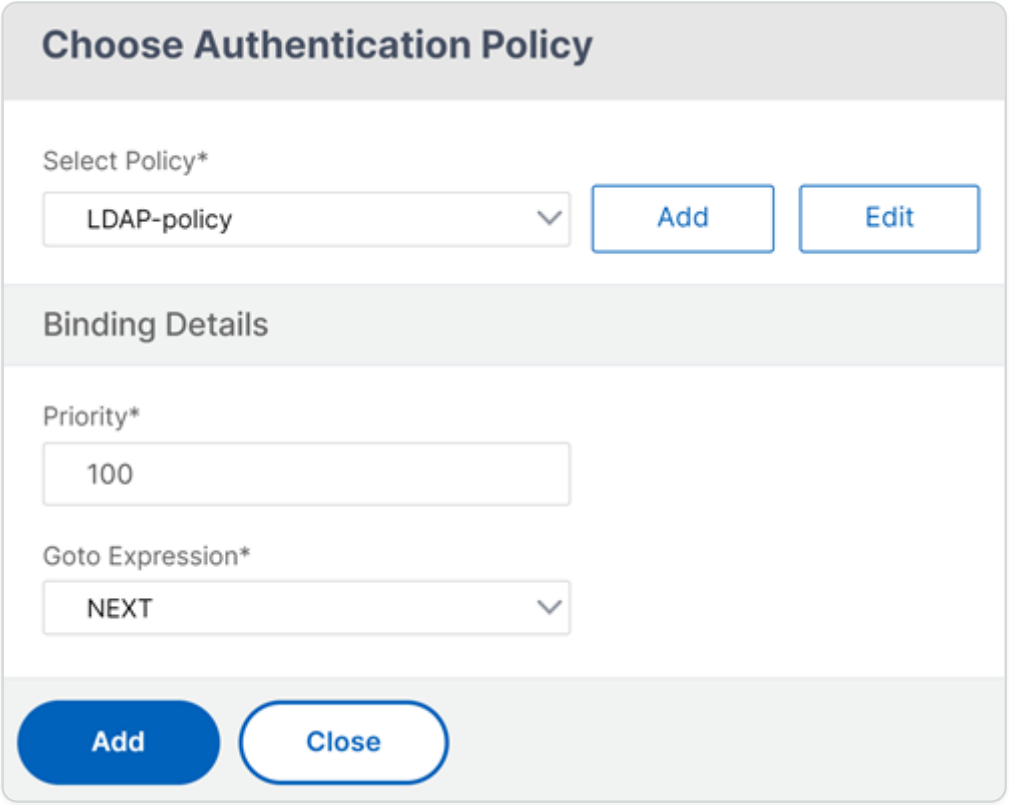
   - 在第一个因素磁贴上，单击“**添加架构**”以添加登录架构。您可以从下拉列表中选择现有身份验证登录架构，或创建登录架构。
   - 要创建身份验证登录方案，请单击 **添加**。有关身份验证登录方案的详细信息，请参阅 配置 nFactor 身份验证。



   - 单击 **添加策略** 以添加 LDAP 策略。如果 LDAP 策略已创建，您可以选择该策略。单击 **添加**。

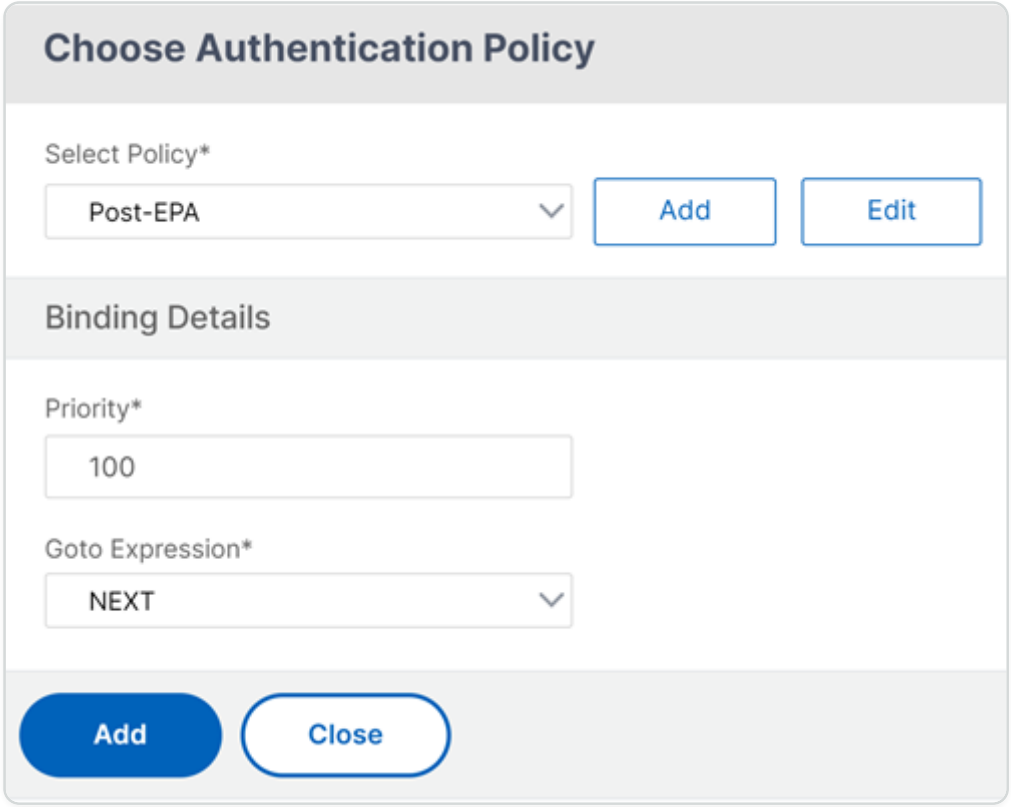
> **注意：**
>
> 如果未创建 LDAP 策略，您可以创建一个。单击 **选择策略** 下拉列表旁边的 **添加** 按钮。在 **操作** 字段中，选择 LDAP。有关添加身份验证 LDAP 服务器的详细信息，请参阅 `https://support.citrix.com/article/CTX123782`。

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

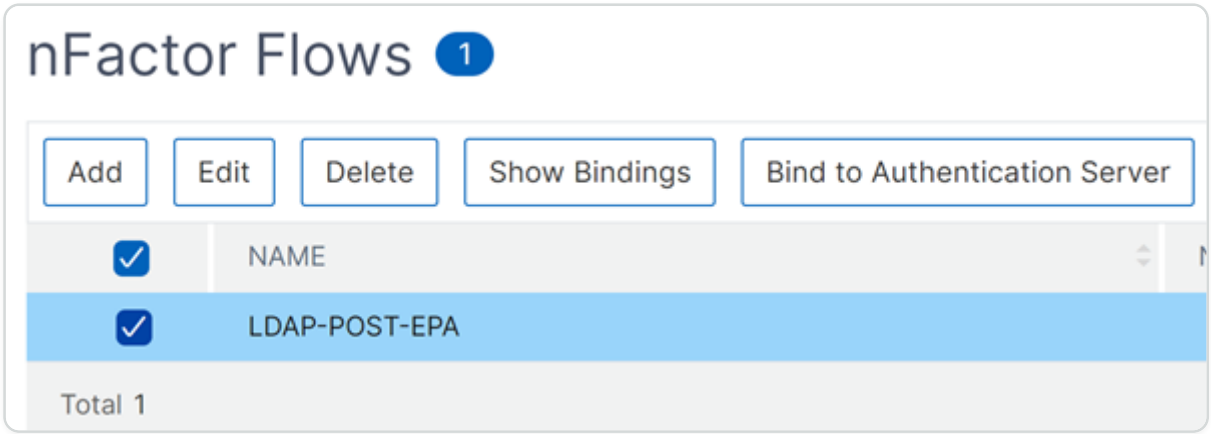


3. 创建下一个因子并将其连接到第一个因子。
   - 单击绿色或红色的 **+** 图标，将 EPA 添加为下一个因子。
   - 在 **要连接的下一个因子** 页面上创建下一个因子。
   - 将 **添加方案** 部分留空，以便此因子应用默认的无方案。
4. 为下一个因子添加策略。
   - 单击 **添加策略** 以添加身份验证后 EPA 策略和操作。
   - 您可以从现有策略列表中选择，也可以创建策略。要从现有策略中选择，请从 **选择策略** 下拉列表中选择一个策略，提供绑定详细信息，然后单击 **添加**。
   - 要创建策略，请单击 **选择策略** 下拉列表旁边的 **添加** 按钮。

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



5. nFactor 流程完成后，单击 **Done**。
6. 将 nFactor 流程绑定到身份验证服务器。
   - 导航到 **安全 AAA - 应用程序流量 > nFactor 可视化工具 > nFactor 流程**。
   - 选择 nFactor，然后单击 **Bind to Authentication Server**。



参考

- nFactor 概念、实体和术语
- 如何在 NetScaler Gateway 上配置 LDAP 身份验证
- LDAP 身份验证
- 高级端点分析扫描

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

Windows 客户端上的 EPA 扫描分类类型

重要提示：

端点分析旨在根据预定的合规性标准分析用户设备，但不强制执行或验证最终用户设备的安全性。建议使用端点安全系统来保护设备免受本地管理员攻击。

以下新的分类类型已添加到 EPA 扫描中，用于查找缺失的补丁。如果客户端缺少以下任何补丁，EPA 扫描将失败。

- 应用程序
- 连接器
- 关键更新
- 定义更新
- 开发工具包
- 功能包
- 指南
- 安全更新
- 服务包
- 工具
- 更新汇总
- 更新

注意：

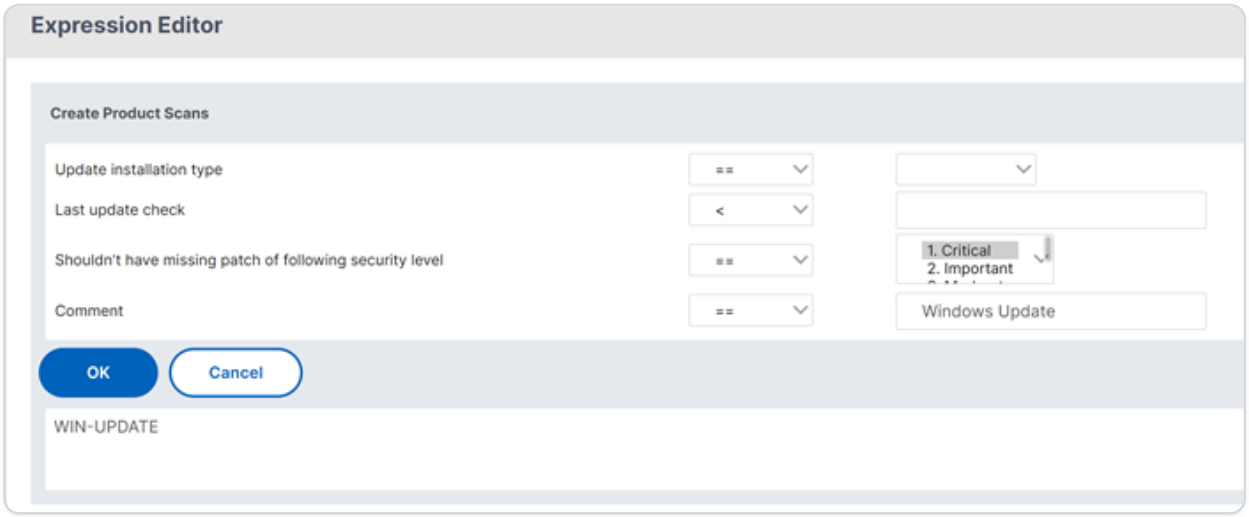
- 此前，Windows 客户端上针对缺失补丁的 EPA 扫描是根据严重性级别进行的：严重、重要、中等和低。
- 如果您使用的是 Citrix Secure Access for Windows 23.8.1.1 及更高版本，则扫描 `CLIENT.SYSTEM('WIN-UPDATE_SCAN-TIME')` 仅限于已启用自动更新的客户端计算机。如果禁用了自动更新，则此扫描会返回不同的结果。

使用 GUI 配置 EPA 扫描分类类型

1. 导航到 **NetScaler Gateway > 策略 > 预身份验证**。

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

2. 创建预身份验证策略或编辑现有策略。
3. 单击 **OPSWAT EPA 编辑器** 链接。
4. 在表达式编辑器中，选择 **Windows > Windows Update**。
5. 在 **不应缺少以下 Windows 更新分类类型的补丁** 中，选择缺失补丁的分类类型。
6. 单击 **确定**。



客户可以升级到 OPSWAT 4.3.2744.0s 版本以使用这些选项。

Windows 版 EPA 客户端的遥测数据扫描

从 Windows 版 EPA 客户端 24.8.1.19 版本开始，EPA 客户端会将应用程序事件和指标发送到 TAP 服务器。

注意事项：

- EPA 客户端发送的遥测数据仅发送给 TAP，而不发送给任何第三方供应商。此外，EPA 客户端不会与 TAP 共享用户的任何个人信息。
- 要禁用遥测功能，管理员必须联系 Citrix 支持。
- EPA 客户端收集产品配置和使用数据，以增强客户端体验。

数据收集

每当执行 EPA 扫描时，TAP 都会收集以下元数据和遥测日志：

- 每个客户的唯一终端设备数量，根据地理位置（国家和大陆）划分
- 终端设备的平台 (Windows)
- EPA 客户端版本

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

- 客户端安装类型（本地或管理员）
- 身份验证类型（预身份验证或后身份验证 EPA）
- 扫描状态（成功或失败的扫描以及扫描期间的错误）
- 使用不同类型扫描的客户数量（设备证书扫描、OPSWAT 扫描、操作系统版本检查扫描）
- 使用 EPA 客户端与本地 NetScaler Gateway 的客户数量

参考

- 有关 Windows 服务器更新服务分类 GUID 的详细信息，请参阅 `<https://docs.microsoft.com/zh-cn/previous-versions/windows/desktop/ff357803(v=vs.85)>`。
- 有关 Microsoft 软件更新术语的说明，请参阅 `<https://docs.microsoft.com/zh-cn/troubleshoot/windows-client/deployment/standard-terminology-software-updates>`。

端点分析 v2

端点分析 (EPA) 对于零信任网络访问 (ZTNA) 至关重要，它在授予访问权限之前评估端点设备上下文和姿态。从版本 14.1 build 25.56 开始，EPA v2 提供了更强大、更可靠的策略评估，具有增强的功能，可提供更强的保障和更高的安全性，使其成为推荐选项。

支持的平台和版本

下表列出了支持 EPA v2 的 EPA 客户端平台和版本：

EPA 客户端平台	版本
视窗	25.8.1.6 及更高版本
macOS	25.11.19 及更高版本
琳纳克斯	26.2.3 及更高版本

支持和不支持的扫描

EPA v2 支持大多数基于浏览器和 Citrix Workspace 应用程序启动的会话扫描，这些扫描也受 EPA v1 支持。有关详细信息，请参阅 端点分析。

EPA v2 不支持以下扫描：

- Windows EPA 扫描缺失的补丁

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

- Windows 上次更新扫描
- 在“**表达式编辑器**”中的“**Windows**”和“**Mac**”下拉菜单下扫描“**MAC 地址**”
- 使用运算符（<、>、==、!=、<=、>=）进行版本比较的注册表扫描。此限制仅适用于版本比较，而标准整数比较按预期工作。

先决条件

- 在 NetScaler Gateway 中配置 nFactor 身份验证（高级身份验证）。
- 使用 CLI 或 GUI 启用 `HttpOnlyCookie` 参数。
  - 要使用 CLI 启用 `HttpOnlyCookie` 参数，请在命令提示符下键入以下命令：

    ```
    set aaa parameter -httpOnlyCookie ENABLED
    ```

  - 要使用 GUI 启用 `HttpOnlyCookie` 参数，请导航到“**NetScaler Gateway > 全局设置 > 更改身份验证 AAA 设置**”。在“**配置 AAA 参数**”页面上，将“**HttpOnly Cookie**”设置为“**已启用**”。

在 NetScaler Gateway 上启用 EPA v2

使用 CLI 启用 EPA v2

在命令提示符下，键入：

```
set aaa parameter -enhancedEPA ENABLED
```

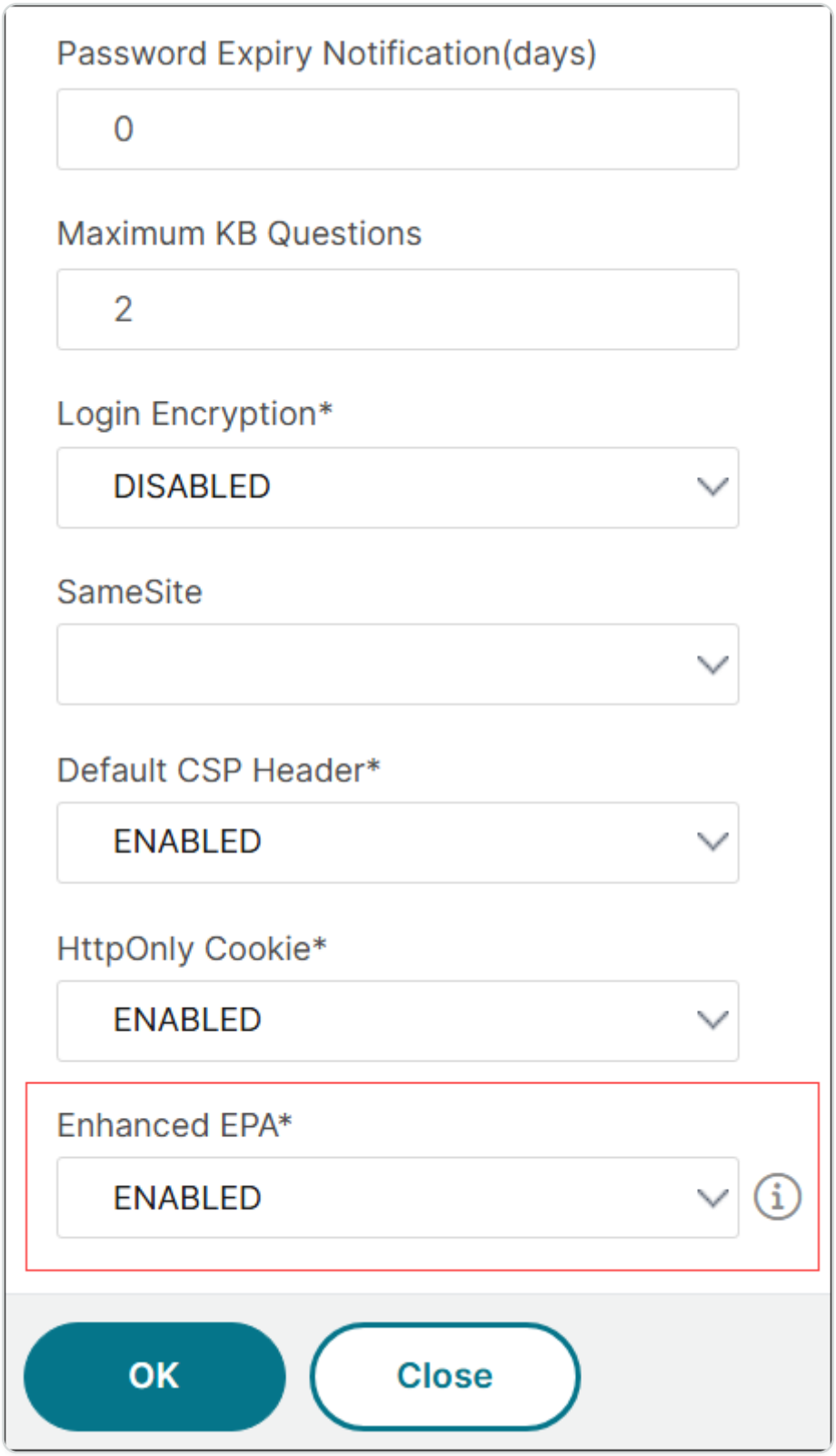
使用 GUI 启用 EPA v2

1. 导航到“**NetScaler Gateway > 全局设置 > 更改身份验证 AAA 设置**”。
2. 在“**配置 AAA 参数**”页面上，将“**增强型 EPA**”设置为“**已启用**”。
3. 点击 **确定**。
4. 重启主节点（之前是辅助节点），以确保 HA 设置中的两个节点具有相同的配置。

注意：

对于新的 NetScaler 配置，不需要重启。

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



升级 NetScaler

从 Citrix 下载 页面下载，将您的 NetScaler 升级到相应的版本。有关如何升级 HA 对的详细说明，请参阅 升级高可用性对。

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

升级 NetScaler Gateway 上的客户端组件

在 NetScaler shell 中运行以下命令，检查与您的 NetScaler 关联的客户端版本：

```
cat /var/netscaler/gui/vpn/pluginlist.xml
```

如果关联的客户端版本不符合 支持的平台和版本，请按照以下部分所述更新客户端。

升级适用于 Windows 的 Citrix Secure Access™ 客户端和 EPA 客户端

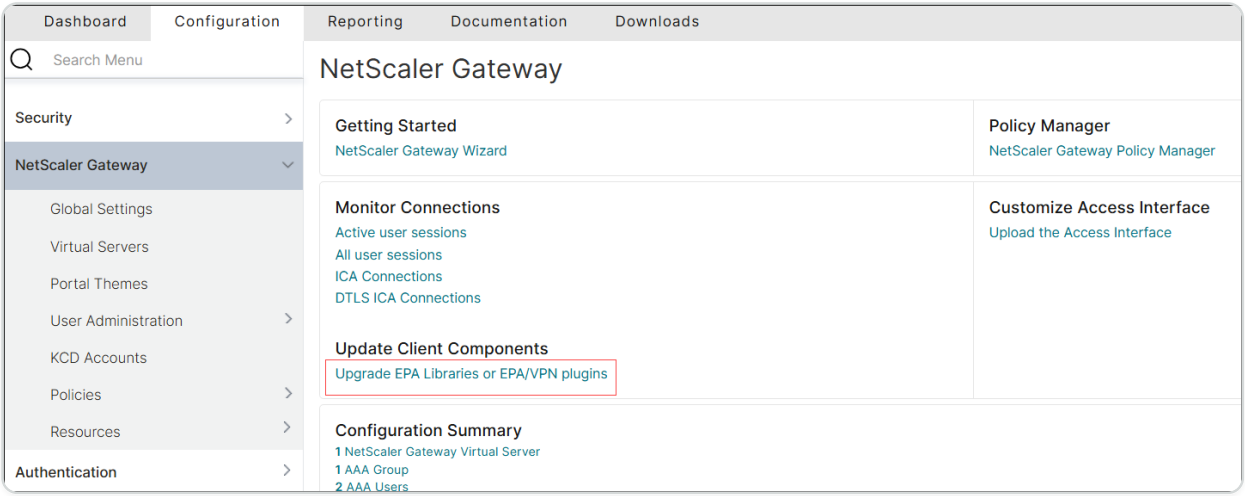
按照 在 NetScaler Gateway 上升级适用于 Windows 的 Citrix Secure Access 客户端和 EPA 客户端中所述的步骤，升级适用于 Windows 的 Citrix Secure Access 客户端和 EPA 客户端。

升级适用于 macOS 的 Citrix Secure Access 客户端和 EPA 客户端

从 App Store 将适用于 macOS 的 Citrix Secure Access 客户端升级到最新版本。

在 NetScaler Gateway 上执行以下步骤，以升级适用于 macOS 的 EPA 客户端：

1. 从 `<https://www.citrix.com/downloads/citrix-secure-access/plug-ins/citrix-secure-access-client-for-macOS.html>` 下载适用于 macOS 的最新 EPA 客户端
2. 导航到 **NetScaler Gateway** > **更新客户端组件**。
3. 在 **更新客户端组件** 下，单击 **升级 EPA 库或 EPA/VPN 插件** 链接。



4. 单击 **选择文件** 并选择已下载的 EPA 客户端文件。
5. 单击 **升级**。
6. 如下所示更新 `pluginlist.xml` 以反映新版本详细信息：

   a. 将下载的 `Citrix_Endpoint_Analysis.dmg` 复制到 NetScaler Gateway 上的 `/var/netscaler/gui/epa/scripts/mac/directory`。

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

b. 将 `/var/netscaler/gui/vpn/pluginlist.xml` 中名称为 `NetScaler Gateway EPA plug-in for Mac` 的 `plugin` 标签的 `version` 和 `compatibleFrom` 属性修改为相应的值。

```
version=“<version>”

compatibleFrom=”<version>”
```

新的 `plugin` 标签显示如下：

```
<plugin

    name="NetScaler Gateway EPA plug-in for Mac" type="MAC-EPA"

    version="23.7.6" path="/epa/scripts/mac/
Citrix_Endpoint_Analysis.dmg"

    compatibleFrom="23.7.6" compatibleTill=""

/>
```

c. 要使更改生效，请在主节点和辅助节点上运行以下命令：

```
rm -rf /netscaler/ns_gui

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

升级最终用户计算机上的 Windows 和 macOS 版 EPA 客户端

将 NetScaler Gateway 中的 EPA 升级到 EPA v2 后，如果最终用户计算机上安装的 EPA 客户端版本不受 EPA v2 支持，则 EPA 客户端将无法启动。20 秒超时后，系统会提示用户下载新的 EPA 客户端。

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

使用以下步骤更新最终用户计算机上的 EPA 客户端：

1. 点击“**下载**”按钮以下载之前已上传到 NetScaler Gateway 的新 EPA 客户端。
2. 安装新 EPA 客户端后，单击同一页面上的“**重试 EPA 启动**”按钮以重新启动 EPA 客户端。

升级 EPA 客户端(/en-us/netscaler-gateway/media/epa-v2-launch.png)

EPA v2 故障排除

MAC 地址扫描

EPA v2 不支持“**表达式编辑器**”中“**Windows**”和“**Mac**”下拉菜单下的 **MAC 地址**扫描。以下是扫描配置示例：

Windows 操作系统： `sys.client_expr("sys_0_MAC_1A2B3C4D5E6F,1D2B3E4D5F6E[COMMENT: MAC Address]")`

macOS： `sys.client_expr("sys_0_MAC-MAC_1A2B3C4D5E6F,1D2B3E4D5F6E[COMMENT: MAC Address]")`

解决方法：

配置 EPA 扫描以允许特定的 MAC 地址。有关详细信息，请参阅MAC 地址的 EPA 扫描。

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

EPA 客户端下载失败

在最终用户计算机上升级 EPA 客户端期间，从 NetScaler Gateway 下载 EPA 客户端可能会失败。

解决方法：

使用 `NOCACHE` 参数可避免此问题：

```
add cache policy bypass_epa_plugin_cache -rule
"HTTP.REQ.URL.ENDSWITH(\".dmg\") || HTTP.REQ.URL.ENDSWITH(\".exe\") ||
HTTP.REQ.URL.ENDSWITH(\".deb\")" -action NOCACHE



bind vpn vserver <vpn-vserver-name> -policy bypass_epa_plugin_cache
-priority 5 -gotoPriorityExpression END -type REQUEST



bind authentication vserver <authvs-name> -policy bypass_epa_plugin_cache
-priority 5 -gotoPriorityExpression END -type REQUEST
```

高级端点分析扫描

高级端点分析 (EPA) 用于扫描用户设备，以满足在 NetScaler Gateway 上配置的端点安全要求。如果用户设备尝试访问 NetScaler Gateway，则在管理员授予访问权限之前，会扫描该设备以获取安全信息，例如操作系统、防病毒软件、Web 浏览器版本等。

高级 EPA 扫描是一种基于策略的扫描，您可以在 NetScaler Gateway 上为身份验证会话配置它。该策略对用户设备执行注册表检查，并根据评估结果，允许或拒绝访问 NetScaler 网络。有关 Citrix EPA 客户端系统要求的更多信息，请参阅 端点分析要求。

重要提示：

Citrix EPA 客户端不支持 Windows 和 macOS 上需要管理员权限的 OPSWAT 扫描。要验证支持的 OPSWAT 扫描，请参阅 Citrix 下载 页面上提供的“Supported application list.xlsx”，以了解所使用的 OPSWAT 库的特定版本。

如果“Supported application list.xlsx”中的扫描限定符标记为“FALSE”，则表示不支持相应的 OPSWAT 扫描限定符。在这种情况下，建议调整您的扫描以使用受支持的配置。
您可以使用 GUI 或 CLI 配置高级 EPA 扫描。

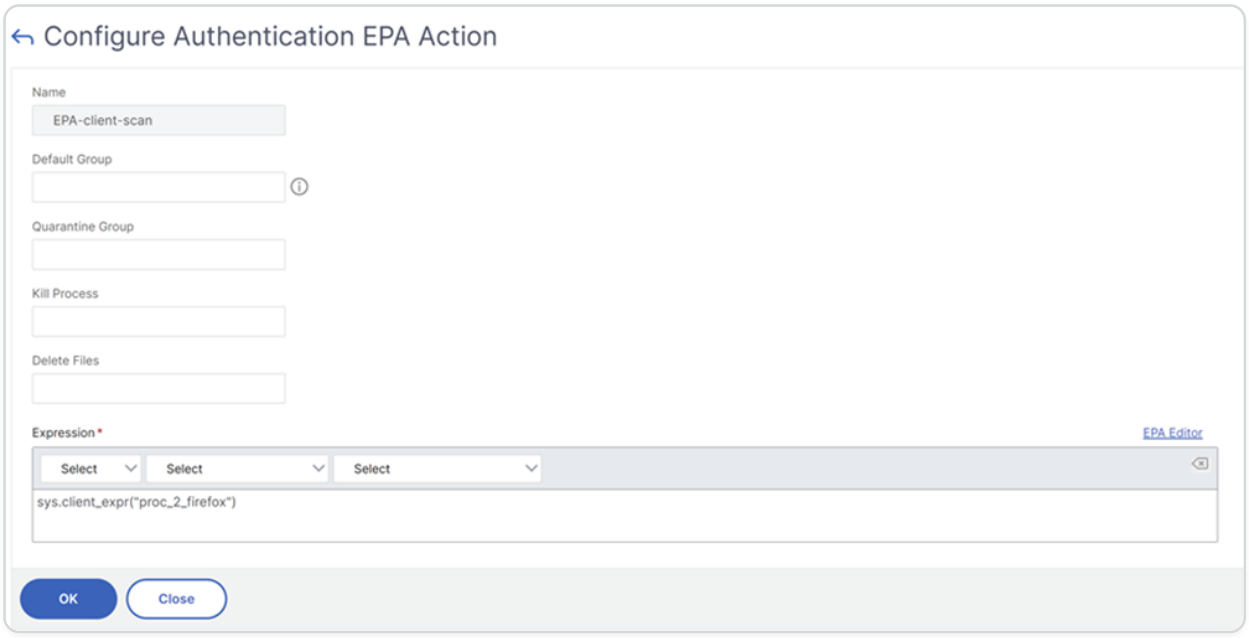
© 1997–2026 Citrix Systems, Inc. All rights reserved.

在 GUI 上

1. 创建 EPA 操作。

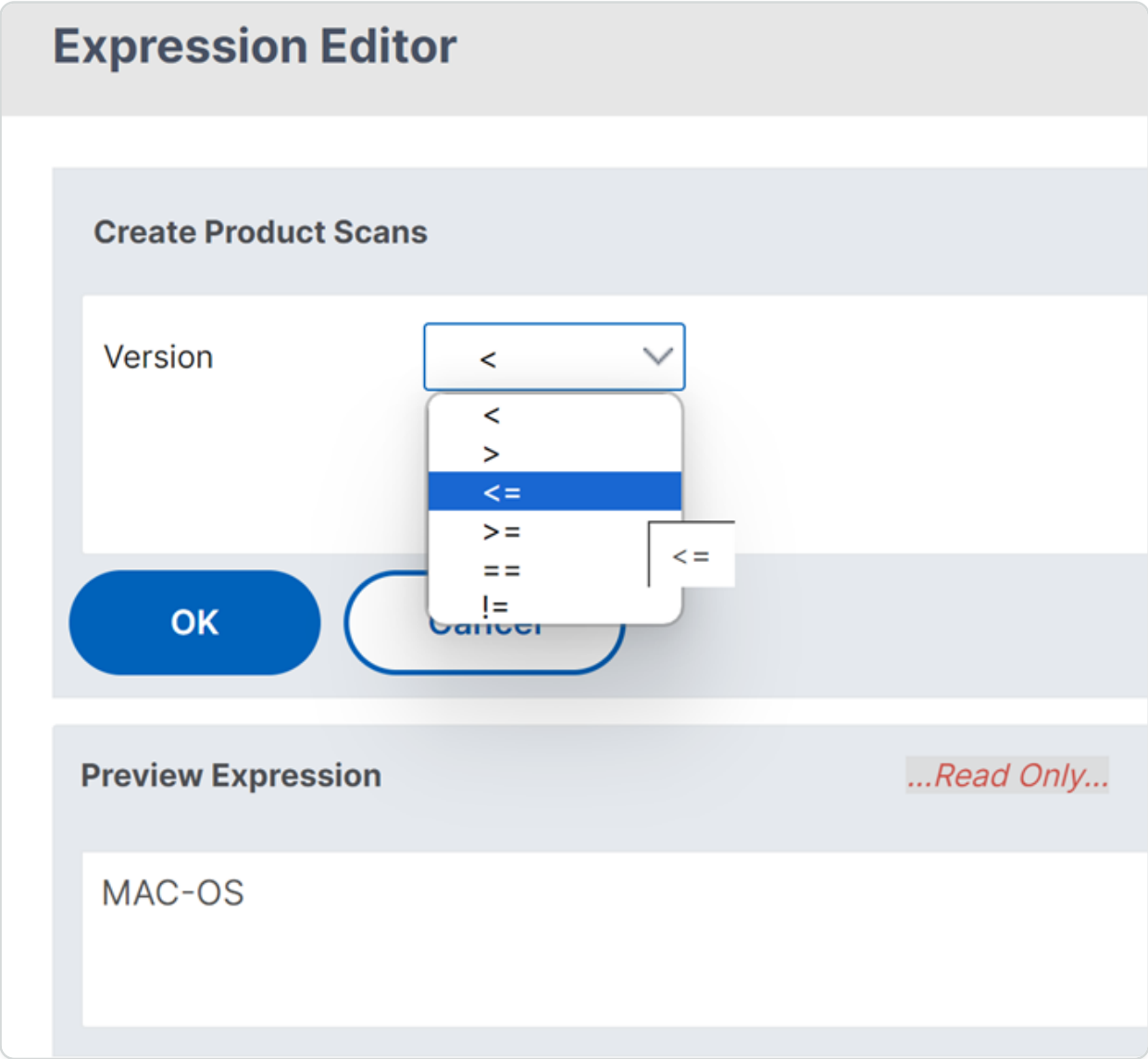
   导航到 **Security > AAA - Application Traffic > Policies > Authentication > Advanced Policies > Actions > EPA**，然后单击 **Add**。在 **Create Authentication EPA Action** 页面上，更新以下信息，然后单击 **Create**。

   - Name: EPA 操作的名称。
   - Default Group: EPA 检查成功时选择的默认组。
   - Quarantine Group: EPA 检查失败时选择的隔离组。
   - Kill Process: 一个字符串，指定要由 EPA 插件终止的进程名称。多个进程必须用逗号分隔。
   - Delete Files: 一个字符串，指定要由 EPA 插件删除的文件的路径和名称。多个文件必须用逗号分隔。
   - 表达式：有关 EPA 表达式格式，请参阅高级端点分析策略表达式参考。



   - EPA 编辑器：选择用于产品版本扫描的运算符。

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



注意：

适用于 macOS 24.2.1.5 的 Citrix EPA 客户端/适用于 macOS 24.02.1 及更高版本的 Citrix Secure Access 客户端支持 EPA 编辑器上的 EPA 运算符 `>`、`<`、`>=`、`<=`、`==` 和 `!=`。此外，**Mac OS** 选项现在作为 EPA 编辑器上的一个单独选项提供（**Mac > Mac OS**）。以前，macOS 产品版本扫描必须在 **Common > Operating System > MacOS** 下执行，并且只能使用 `==` 和 `!=` 运算符。请确保您使用的是 NetScaler Gateway 14.1-12.x 或更高版本才能使用此功能。

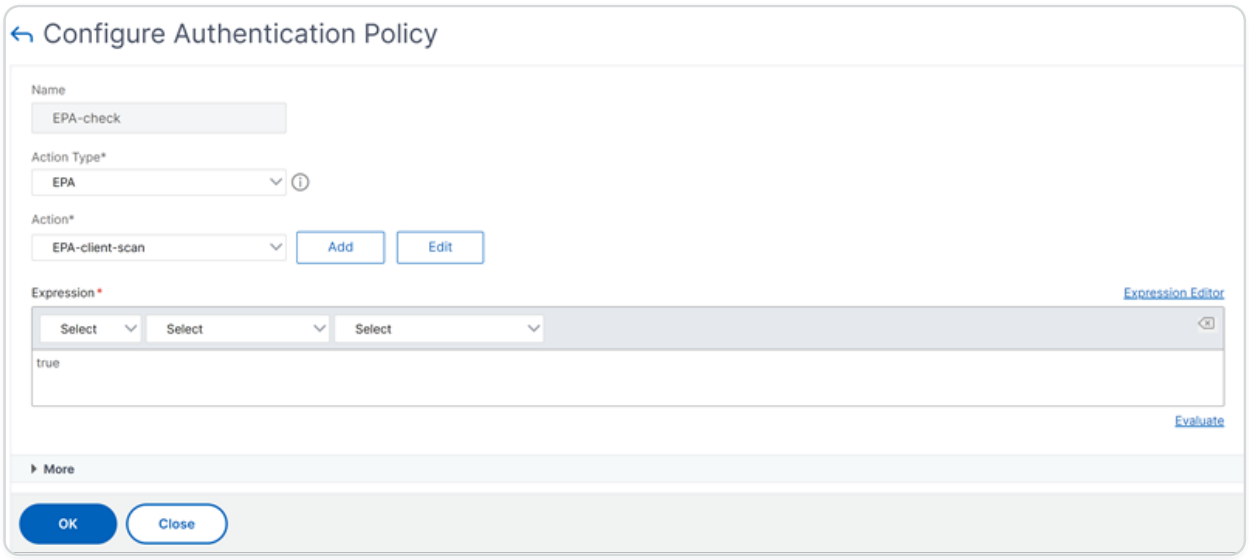
您可以使用这些运算符在 **Mac > Mac OS** 下对 macOS 设备执行产品版本扫描。例如，要允许 12.4 到 13.0（不包括 12.8）的操作系统版本，请在 EPA 编辑器上配置表达式 `sys.client_expr("sys_0_MAC-OS_version_>=_12.4")&&sys.client_expr("sys_0_MAC-OS_version_<=_13.0")&&sys.client_expr("sys_0_MAC-OS_version_!=_12.8")`。

2. 创建相应的 EPA 策略。

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

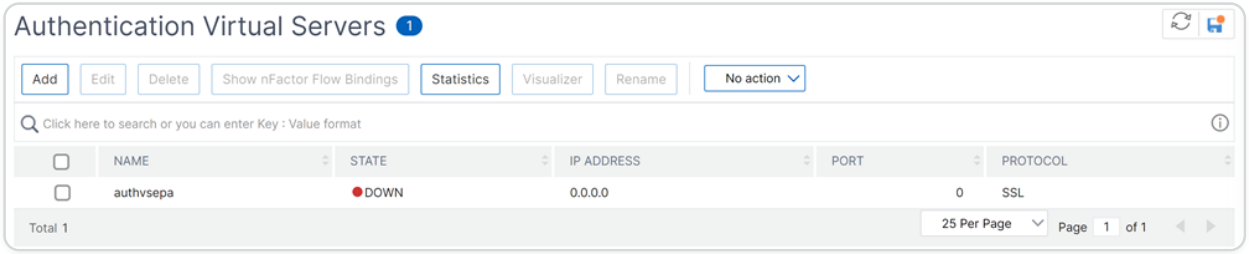
导航到 **Security > AAA - Application Traffic > Policies > Authentication > Advanced Policies > Policies**，然后单击 **Add**。在 **Create Authentication Policy** 页面上，更新以下信息，然后单击 **Create**。

- 名称：高级 EPA 策略的名称。
- 操作类型：身份验证操作的类型。
- 操作：如果策略匹配，则执行的身份验证操作的名称。
- 表达式：有关 EPA 表达式格式，请参阅高级端点分析策略表达式参考。
- 日志操作：当请求与此策略匹配时要使用的消息日志操作的名称。允许的最大长度为 127 个字符。



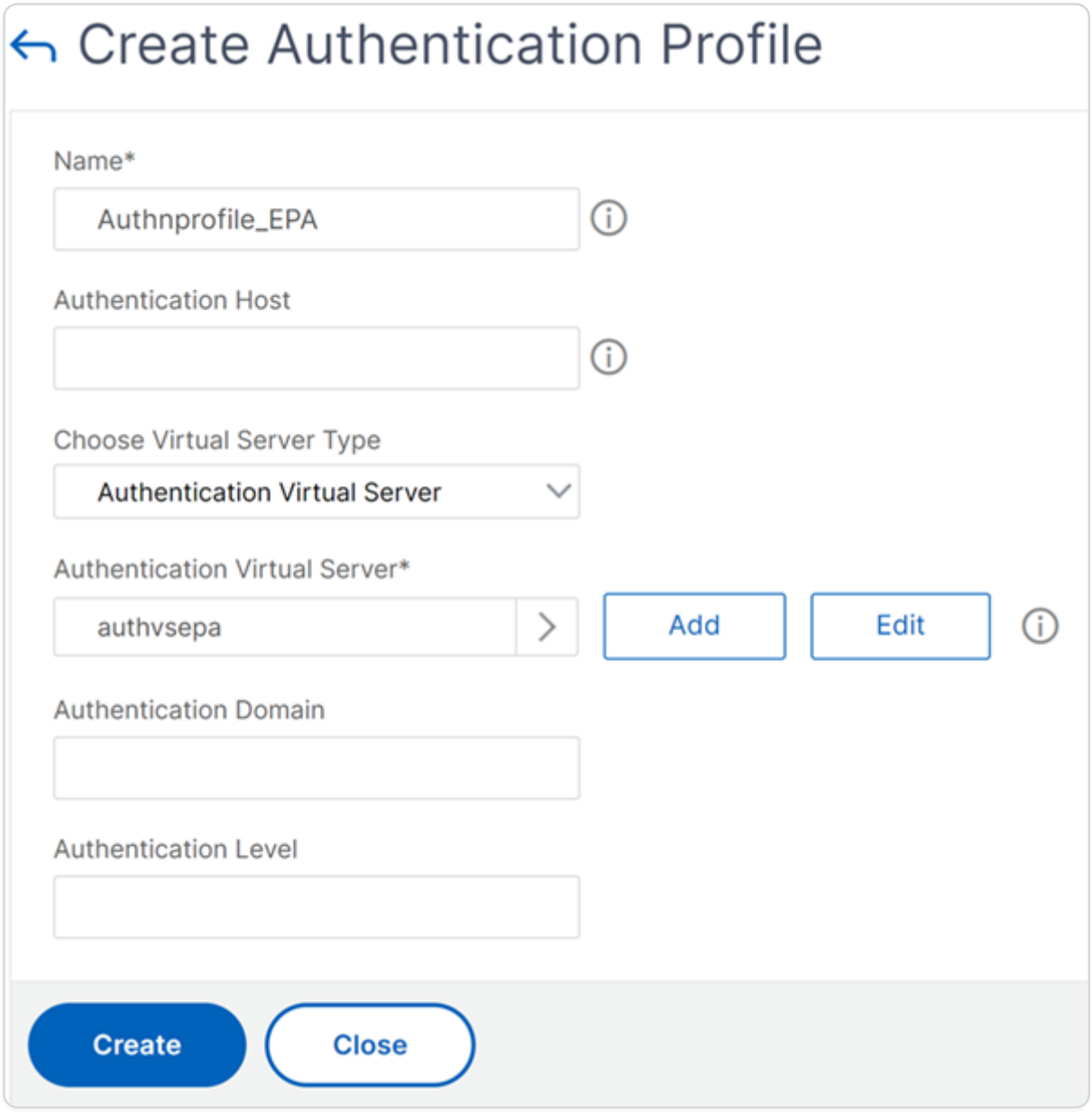
3. 配置一个身份验证虚拟服务器和一个身份验证配置文件。

   - 导航到 **安全 > AAA - 应用程序流量 > 身份验证虚拟服务器**，然后点击 **添加**。



   - 导航到 **Security > AAA - Application Traffic > Authentication Profile**，然后单击 **创建**。

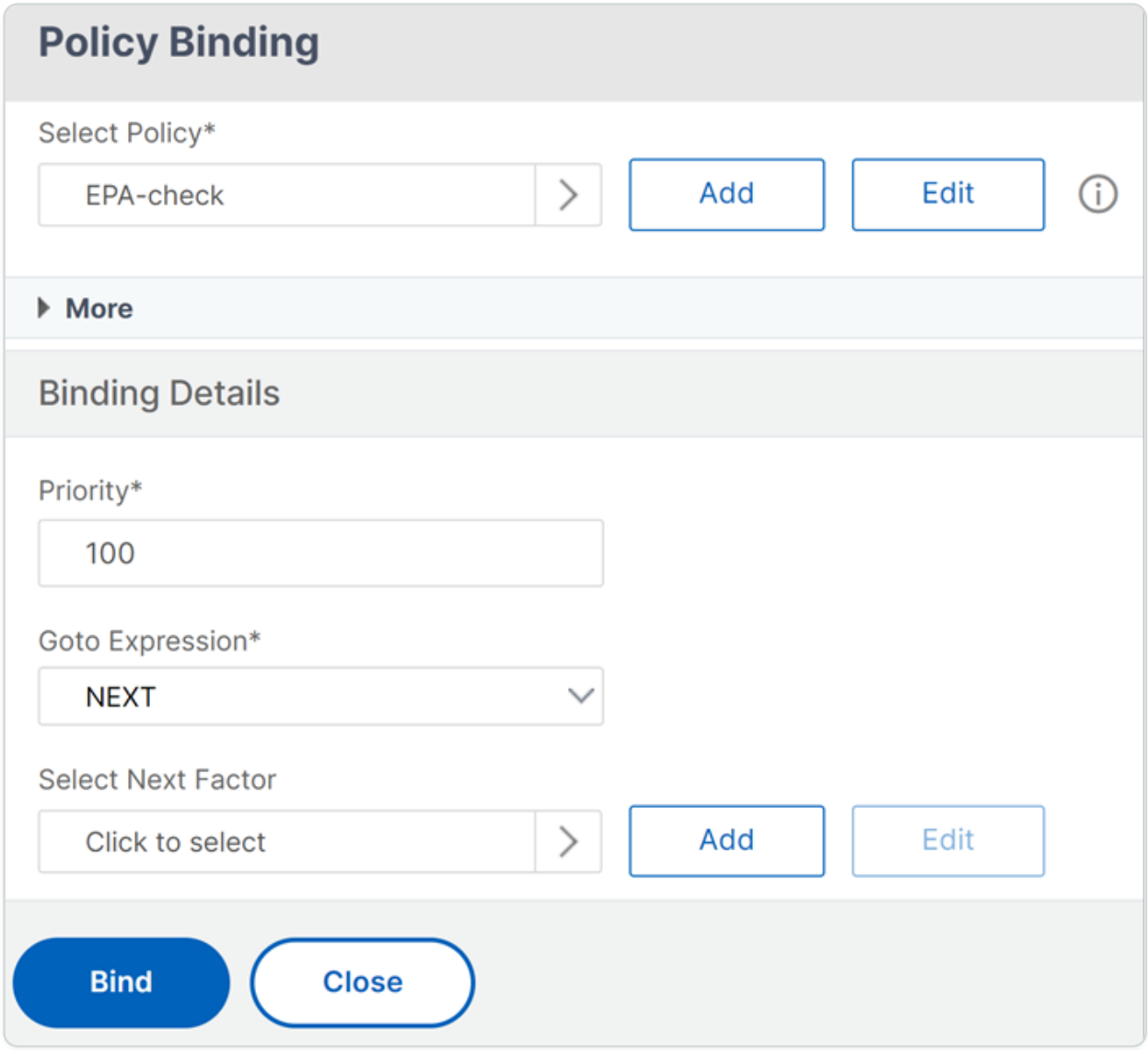
© 1997–2026 Citrix Systems, Inc. All rights reserved.



4. 将高级 EPA 策略绑定到身份验证虚拟服务器。

   - 导航到 **Security > AAA – Application Traffic > Authentication Virtual Servers**，然后选择身份验证虚拟服务器。
   - 在 **Advanced Authentication Policies** 部分中选择策略。
   - 在 **Policy Binding** 部分中单击 **Bind**。

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



5. 将 EPA 策略绑定到 nFactor 流程。

   有关如何将高级 EPA 策略作为因子添加到 nFactor 流程的详细信息，请参阅 nFactor 身份验证中的 EPA 扫描作为因子。

在 CLI 上

1. 创建一个执行 EPA 扫描的操作。

```
add authentication epaAction EPA-client-scan -csecexpr "sys.client_expr
(\"proc_2_firefox\")"
```

   上述表达式扫描进程“Firefox”是否正在运行。EPA 插件每 2 分钟检查一次进程是否存在，这由扫描表达式中的数字“2”表示。

2. 将 EPA 操作与高级 EPA 策略关联。

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

```
add authentication Policy EPA-check -rule true -action EPA-client-scan
```

3. 配置身份验证虚拟服务器和身份验证配置文件。

```
add authentication vserver authnvsepa ssl -ip address 192.0.2.0 -port
443
```

```
add Authnprofile_EPA -authnVsName authnvsepa
```

4. 将高级 EPA 策略绑定到身份验证虚拟服务器。

```
bind authentication vs authnvsepa -policy EPA-check -pr 1
```

升级 EPA 库

要使用 NetScaler GUI 升级 EPA 库：

1. 导航到 **配置 > NetScaler Gateway > 更新客户端组件**。
2. 在 **更新客户端组件** 下，单击 **升级 EPA 库** 链接。
3. 选择所需文件，然后单击 **Upgrade**。

重要提示：

- 在 NetScaler Gateway 高可用性中，必须在主节点和辅助节点上升级 EPA 库。
- 在 NetScaler Gateway 群集设置中，必须在所有群集节点上升级 EPA 库。
- 如果您在升级 EPA 库后遇到问题，则无法降级到较低版本。请联系 Citrix Support 寻求帮助。

有关 OPSWAT 支持的用于 NetScaler 扫描的 Windows 和 MAC 应用程序列表，请参阅 `<https://support.citrix.com/article/CTX234466>`。

高级端点分析扫描故障排除

为了帮助排查高级端点分析扫描问题，客户端插件会将日志信息写入客户端端点系统上的文件。这些日志文件可以在以下目录中找到，具体取决于用户的操作系统。

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

Windows Vista、Windows 7、Windows 8、Windows 8.1 和 Windows 10：

C:\\Users\\\<username\>\\AppData\\Local\\Citrix\\AGEE\\nsepa.txt

视窗 XP：

C:\\文档和设置\\所有用户\\应用程序数据\\Citrix\\AGEE\\nsepa.txt

Mac OS X 系统：

~/Library/Application Support/Citrix/EPAPlugin/epaplugin.log

(其中 ~ 符号表示相关 macOS 用户的家目录路径。) (其中 ~ 符号表示相关 macOS 用户的家目录路径。)

乌班图：

- ~/.citrix/nsepa.txt
- ~/.citrix/nsgcepa.txt

Windows 上次更新扫描

注意：

要更新 EPA 库，请从 `<https://www.citrix.com/downloads/citrix-secure-access/epa-libraries/epa-libraries-for-netscaler-gateway.html>` 下载。

Windows 上次更新扫描增强功能适用于 EPA 库版本 24.9.1.1 及更高版本。从版本 24.9.1.1 开始，除了通过 Windows 自动升级服务安装的更新外，此扫描还包括通过 BigFix、Intune 和其他第三方工具安装的更新。Windows 上次更新扫描不适用于用户手动下载和安装更新补丁的更新。

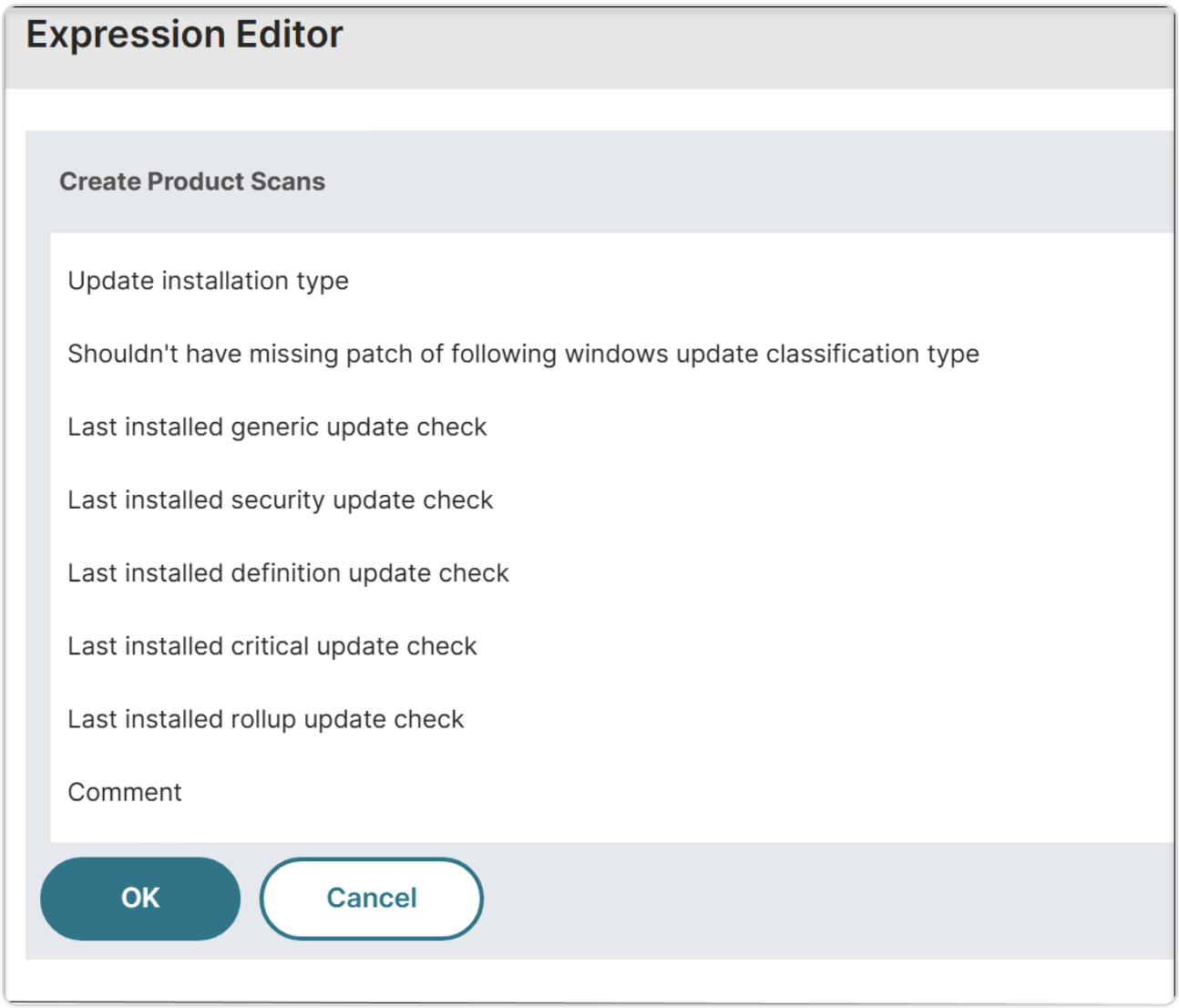
从 EPA 库版本 24.11.1.1 开始，Windows 上次更新扫描将 Windows 更新列为以下类别：

- **通用更新：** 此类别包括使用 Windows 更新、Microsoft 更新或自动更新功能安装的更新。
- **安全更新：** 此类别包括针对安全相关漏洞的补丁。安全更新在每个月的第二个星期二发布。
- **关键更新：** 此类别包括针对关键和非安全相关错误的补丁。关键更新会根据需要发布。
- **定义更新：** 此类别包括包含产品定义数据库新增内容的更新。发布定义更新时，只会下载最新更新与当前已安装更新之间的差异并将其应用到设备。
- **更新汇总：** 此类别包括经过测试的累积性修补程序、安全更新、关键更新和更新集，它们打包在一起以便于部署。更新汇总在每个月的第二个星期二发布。

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

注意：

配置 Windows 上次更新扫描时，请确保在每个类别的配置期限内安排更新。如果未在此时间范围内安装更新，则扫描将失败。



MAC 地址的 EPA 扫描

从 NetScaler 13.0-88.x 版本开始，您可以配置用于允许的或特定 MAC 地址的 EPA 扫描配置。NetScaler 使用策略表达式和模式集来指定 MAC 地址列表。

在 NetScaler 13.0-88.x 版本之前，允许的 MAC 地址列表必须在 EPA 表达式中定义。对于拥有大量允许 MAC 地址的客户来说，将所有 MAC 地址包含在一个表达式中非常麻烦。此外，单个表达式中可添加的 MAC 地址数量也有限制。

例如，

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

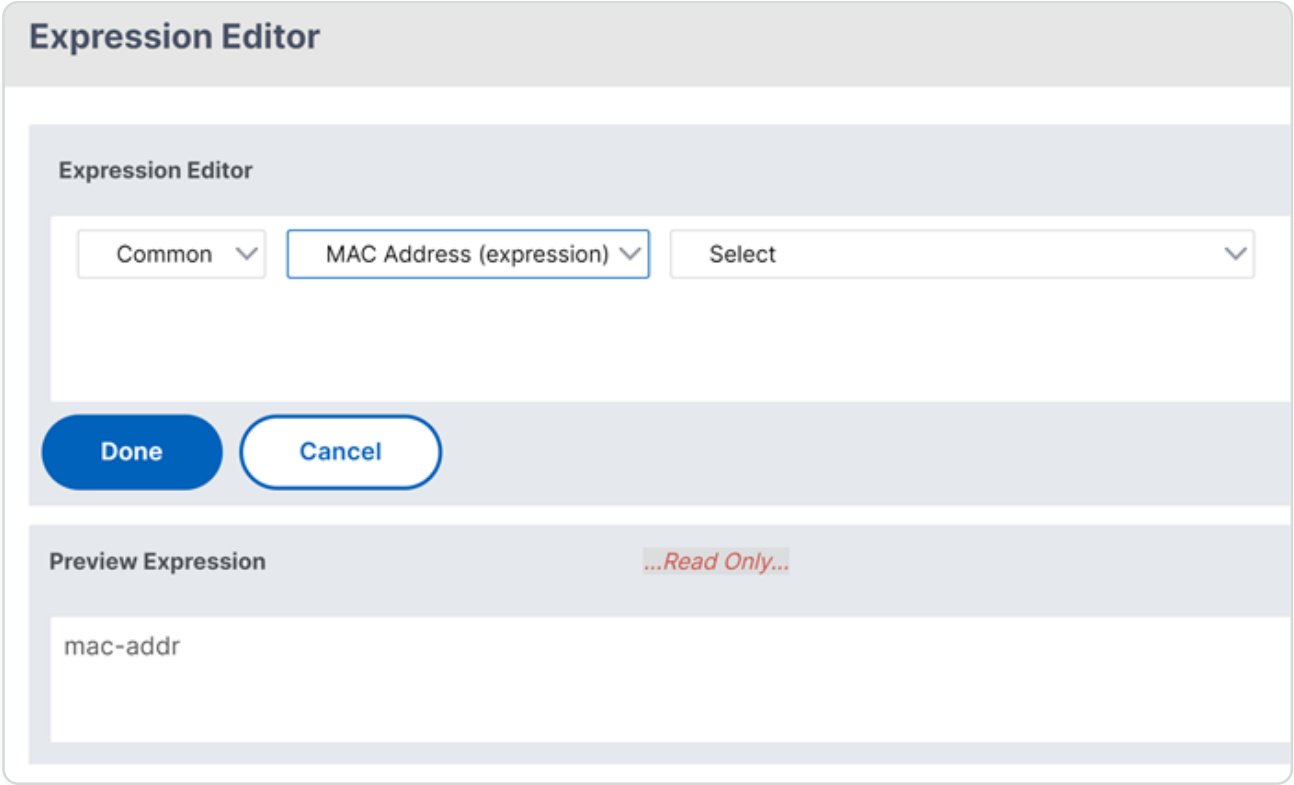
```
add authentication epaAction epa -csecexpr q/
sys.client_expr("proc_0_notepad.exe") || sys.client_expr("proc_0_chrome")
|| sys.client_expr("proc_0_firefox") &&
sys.client_expr("sys_0_MAC_ADDR_anyof_1AC89C83BOF7,0250F20A777C[COMMENT:
MAC Address]")/
```

使用 GUI 配置 MAC 地址的 EPA 扫描

以前在 **Windows** 扫描类别中可用的 **MAC 地址（表达式）** 选项现在在 NetScaler GUI 的 **通用** 扫描类别中可用。此选项使用户能够配置用于允许的或特定 MAC 地址列表的 EPA 扫描。

注意：

Citrix Secure Access 客户端 22.10.1 及更高版本支持 NetScaler 在 GUI 上处理 EPA 扫描配置的这种方法。



1. 配置模式集。有关详细信息，请参阅 配置模式集。
2. 为每个模式集创建相应的策略表达式。

   配置表达式时，在表达式编辑器中，选择 **AAA > LOGIN > CLIENT_MAC_ADDR > EQUAL_ANY(string) > Pattern Set**。

   有关配置高级表达式的详细信息，请参阅 在策略中配置高级策略表达式。

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

3. 为前面步骤中配置的表达式创建 EPA 扫描。有关详细信息，请参阅 高级端点分析扫描。

使用 CLI 配置 MAC 地址的 EPA 扫描

1. 将 MAC 地址存储在模式集中。

   在命令提示符下，键入；

   ```
   add policy patset <name> [-comment <string>]
   ```

   示例：

   ```
   add policy patset patset1

   bind policy patset patset1 1A-C8-9C-83-BO-F7

   bind policy patset patset1 02-50-F2-0A-77-7C … and so on up to 3K
   entries.

   add policy patset patset2

   bind policy patset patset2 1A-2B-3C-4D-5E-6A

   bind policy patset patset2 1A-2B-3C-4D-5E-6B … and so on up to 3K
   entries.
   ```

2. 使用 AAA.LOGIN.CLIENT_MAC_ADDR.equals_any() 为每个模式集创建相应的策略表达式。

   在命令提示符下，键入；

   ```
   Add policy expression <name> <value> [-comment <string>] [-
   clientSecurityMessage <string>]
   ```

   示例：

   ```
   add policy expression exp1
   AAA.LOGIN.CLIENT_MAC_ADDR.equals_any("patset1")

   add policy expression exp2
   AAA.LOGIN.CLIENT_MAC_ADDR.equals_any("patset2")
   ```

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

3. 使用配置的策略表达式创建 EPA 扫描。

   在命令提示符下，键入；

   ```
   add authentication epaAction <name>  -csecexpr <expression>
   ```

   示例：

   ```
   add authentication epaAction epa -csecexpr q/
   sys.client_expr("proc_0_notepad.exe") ||
   sys.client_expr("proc_0_chrome")  || sys.client_expr("mac-addr_0_exp1")
   || sys.client_expr("mac-addr_0_exp2") ||
   sys.client_expr("proc_0_firefox")/
   ```

   配置预身份验证策略，

   ```
   add authentication Policy epapol -rule true -action epa
   ```

   绑定预身份验证策略，

   ```
   bind authentication vserver <name> -policy epapol -priority 10
   -gotoPriorityExpression NEXT
   ```

注意事项

- 为允许的 MAC 地址列表配置 EPA 扫描仅适用于 nFactor 身份验证流。
- 建议在模式集中存储不超过 3000 个条目。
- MAC 地址必须配置为 1A-2B-3C-4D-5E-6F 格式。
- EPA 扫描的格式是 `mac-addr_0_<policy-expression-name>`。在此格式中，`mac-addr_0_` 是一个静态值，您必须在 `mac-addr_0_` 之后输入策略表达式名称。
- EPA 扫描可以使用符号 `( ||, &&)` 进行适当分隔。
- 要将多个 MAC 地址添加到模式集，您可以使用基于文件的模式集导入。建议每个模式集最多存储 3000 个条目以获得最佳性能。
- 如果 MAC 地址存在于文件中，您可以通过使用基于文件的模式集导入并在导入期间指定适当的分隔符来创建模式集。

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

限制

- Linux 计算机不支持 MAC 地址的 EPA 扫描。

参考

- 配置模式集。
- 使用基于文件的导入创建模式集。

高级端点分析策略表达式参考

本主题介绍高级端点分析表达式的格式和构造。NetScaler Gateway 配置实用程序会自动构建此处包含的表达式元素，无需手动配置。

表达式格式

高级端点分析表达式具有以下格式：

`CLIENT.APPLICATION (SCAN-type_ Product-id_ Method-name _ Method-comparator_ Method-param _…)`

其中：

SCAN-type 是正在分析的应用程序类型。

Product-id 是所分析应用程序的产品标识。

Method-name 是正在分析的产品或系统属性。

Method-comparator 是为分析选择的比较器。

Method-param 是正在分析的属性值。

示例：

client.application(ANTIVIR_2600_RTP_==_TRUE)

注意：

对于非应用程序扫描类型，表达式前缀是 CLIENT.SYSTEM 而不是 CLIENT.APPLICATION。

表达式字符串

高级端点分析中每种支持的扫描类型在表达式中使用唯一的标识符。下表列出了每种扫描类型的字符串。

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

扫描类型	扫描类型表达式字符串
反网络钓鱼	ANTIPHI
防病毒	ANTIVIR
备份客户端	BACKUP
Citrix Workspace 应用程序 (macOS)	MAC-CWA
Citrix Workspace 应用程序 (Windows)	WIN-CWA
数据丢失防护	DATA-PREV
防火墙	FIREWALL
健康代理	HEALTH
硬盘加密	HD-ENC
即时通讯工具	IM
网页浏览器	BROWSER
P2P	P2P
补丁管理	PATCH
MAC 地址 (表达式)	MAC
域检查	DOMAIN
注册表扫描	REG
Windows 更新扫描	WIN-UPDATE

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

注意：

- 对于 macOS 特定扫描，表达式在方法类型前包含前缀 `MAC-`。因此，对于防病毒和反网络钓鱼扫描，方法分别为 MAC-ANTIVIR 和 MAC-ANTIPHI。例如：`client.application(MAC-ANTIVIR_2600_RTP_==_TRUE)`。
- 从 Windows EPA 库版本 24.8.1.4 开始支持 WIN-CWA 扫描，该版本可在 `<https://www.citrix.com/downloads/citrix-secure-access/epa-libraries/epa-libraries-for-netscaler-gateway.html>` 获取。
- 从适用于 macOS 的 EPA 客户端版本 24.9.26（可在 `<https://www.citrix.com/downloads/citrix-secure-access/plug-ins/EPA-clients-for-macOS.html>` 获取）以及 OPSWAT 版本 4.3.3762 的 mac_epa.tgz（可在 `<https://www.citrix.com/downloads/citrix-secure-access/epa-libraries/epa-libraries-for-netscaler-gateway.html>` 获取）开始支持 MAC-CWA 扫描。

应用程序扫描方法

在配置高级端点分析表达式时，方法用于定义端点扫描的参数。这些方法包括方法名称、比较器和值。下表列出了可在表达式中使用的所有方法。

常用扫描方法：

以下方法用于多种类型的应用程序扫描。

方法	描述	比较器	可能的值
VERSION*	指定应用程序的版本。	<, <=, >, >=, !=, ==	版本字符串
AUTHENTIC**	检查应用程序是否为正版。	\==	TRUE
ENABLED	检查应用程序是否已启用。	\==	真
运行中	检查应用程序是否正在运行。	\==	真

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

方法	描述	比较器	可能的值
注释	注释字段（扫描时忽略）。在表达式中用 [] 分隔。	\==	任何文本

* VERSION 字符串可以指定最多四个值的十进制字符串，例如 1.2.3.4。

** AUTHENTIC 检查用于验证应用程序二进制文件的真实性。

注意：

您可以为应用程序扫描类型选择通用版本。选择通用扫描时，产品 ID 为 0。

Gateway 提供了一个选项，可以为每种软件类型配置通用扫描。使用通用扫描，管理员可以扫描客户端计算机，而无需将扫描检查限制为任何特定产品。

对于通用扫描，扫描方法仅在用户系统上安装的产品支持该扫描方法时才有效。要了解哪些产品支持特定的扫描方法，请联系 NetScaler® 支持。

独特的扫描方法：

以下方法是指定扫描类型所特有的。

方法	描述	比较器	可能的值
ENABLED-FOR	检查所选应用程序是否启用了反网络钓鱼软件。	`allof`, `anyof`,`noneof`	**对于 Windows**：IE 浏览器、火狐浏览器、谷歌浏览器、Opera 浏览器、Safari 浏览器。**对于 Mac**：Safari 浏览器、火狐浏览器、谷歌、Chrome 浏览器、Opera 浏览器。

表 2. 防病毒

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

方法	描述	比较器	可能的值
RTP	检查实时保护是否开启。	\==	TRUE
SCAN-TIME	自上次执行完整系统扫描以来经过了多少**分钟**。	<, <=, >, >=, !=, ==	任何正数
VIRDEF-FILE-TIME	自病毒定义文件更新以来经过了多少**分钟**（即，病毒定义文件时间戳与当前时间戳之间的分钟数）。	<, <=, >, >=, !=, ==	任何正数
VIRDEF-FILE-VERSION	定义文件的版本。	<, <=, >, >=, !=, ==	版本字符串
ENGINE-VERSION	引擎版本。	<, <=, >, >=, !=, ==	版本字符串

表 3. 备份客户端

方法	描述	比较器	可能的值
LAST-BK-ACTIVITY	自上次备份活动完成以来经过了多少**分钟**。	<, <=, >, >=, !=, ==	任何正数

表 4. 数据丢失防护

方法	描述	比较器	可能的值
ENABLED	检查应用程序是否已启用以及时间保护是否已开启。	\==	TRUE

表 5. 健康检查代理

方法	描述	比较器	可能的值
SYSTEM-COMPL	检查系统是否合规。	\==	TRUE

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

表 6. 硬盘加密

方法	描述	比较器	可能的值
ENC-PATH	用于检查加密状态的路径。	NO OPERATOR	任何文本
ENC-TYPE	检查指定路径的加密类型。	`allof, anyof, noneof`	**列表包含以下选项：** UNENCRYPTED, PARTIAL, ENCRYPTED, VIRTUAL, SUSPENDED, PENDING

表 7. Web 浏览器

方法	描述	比较器	可能的值
DEFAULT	检查是否设置为默认浏览器。	\==	TRUE

表 8. 补丁管理

方法	描述	比较器	可能的值
SCAN-TIME	自上次执行补丁扫描以来经过了多少分钟。	<, <=, >, >=, !=, ==	任何正数
MISSED-PATCH	客户端系统未缺少这些类型的补丁。	`anyof, noneof`	任何预选（补丁管理器服务器上预选的补丁）

表 9. MAC 地址（表达式）

方法	描述	比较器	可能的值
ADDR	检查客户端机器的 MAC 地址是否在给定列表中。	`anyof, noneof`	可编辑列表

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

表 10. 域成员资格

方法	描述	比较器	可能的值
SUFFIX	检查客户端计算机是否存在于给定列表中。	`anyof, noneof`	可编辑列表

表 11. 数字注册表项

方法	描述	比较器	可能的值
路径	注册表检查的路径。格式为：HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Client\EnableAutoUpdate。无需转义特殊字符。所有注册表根键：HKEY_LOCAL_MACHINE、HKEY_CURRENT_USER、HKEY_USERS、HKEY_CLASSES_ROOT、HKEY_CURRENT_CONFIG	无运算符	任何文本
REDIR-64	遵循 64 位重定向。如果设置为 TRUE，则遵循 WOW 重定向（即，在 32 位系统上检查注册表路径，但在 64 位系统上检查 WOW 重定向路径）。如果未设置，则不遵循 WOW 重定向（即，在 32 位和 64 位系统上检查相同的注册表路径）。对	==	TRUE

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

方法	描述	比较器	可能的值
	于未重定向的注册表项，此设置无效。有关在 64 位系统上重定向的注册表项列表，请参阅以下文章：`http://msdn.microsoft.com/zh-cn/library/aa384253%28v=vs.85%29.aspx`		
值	上述路径的预期值。此扫描仅适用于 REG_DWORD 和 REG_QWORD 注册表类型。	<, <=, >, >=, !=, ==	任何数字

管理用户会话

您可以在 NetScaler GUI 中通过“**活动用户会话**”对话框管理用户会话。此对话框显示 NetScaler Gateway 上的活动用户会话列表。您可以使用用户名、组名或 IP 地址查看最终用户或组会话。您还可以在此对话框中查看活动会话。会话信息包括：

- 用户名
- 用户设备的 IP 地址
- 用户设备的端口号
- 虚拟服务器的 IP 地址
- 虚拟服务器的端口号
- 分配给用户的内网 IP 地址

使用 GUI 管理用户会话

查看用户会话

1. 在 NetScaler GUI 导航窗格中，单击“**NetScaler Gateway**”。
2. 在详细信息窗格的“监视连接”下，单击“**活动用户会话**”。
3. 在“**活动用户会话**”中，从以下类型中选择。

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

- **“活动用户”**
- **“活动组”**
- **内网 IP** - 当您选择内网 IP 时，您必须输入内网 IP 地址和子网掩码。

4. 单击 **继续**。

刷新会话列表

您可以检索有关 NetScaler Gateway 会话的更新信息。

1. 在 NetScaler GUI 导航窗格中，单击 **NetScaler Gateway**。
2. 在详细信息窗格中，在“监视连接”下，单击 **活动用户会话**。
3. 单击 **刷新**。

结束用户或组会话或具有特定内网 IP 地址的会话

您可以终止用户和组会话。您还可以结束具有特定内网 IP 地址和子网掩码的会话。

1. 在 NetScaler GUI 导航窗格中，单击 **NetScaler Gateway**。
2. 在详细信息窗格中，在“监视连接”下，单击 **活动用户会话**。
3. 在“会话”下，选择用户、组或具有特定内网 IP 地址的会话，然后单击 **结束**。

使用 CLI 管理用户会话

您可以使用以下 CLI 命令查看用户会话、结束用户或组会话。

- `show aaa session` - 显示绑定到指定用户、组、IP 地址或 IP 范围的所有 NetScaler 身份验证、授权和审计或 VPN 连接。
- `show vpn icaConnection` - 显示所有使用 ICA 代理的活动连接。
- `show system session` - 显示所有当前系统会话或指定会话的信息。

Windows 自动登录

Windows 自动登录功能使 Citrix Secure Access 客户端能够在用户登录 Windows 计算机后自动与 NetScaler 建立隧道。支持 Windows 自动登录功能的身份验证方法是 LDAP 和 Kerberos。

使用 CLI 配置 Windows 自动登录

您可以使用以下 CLI 命令配置 Windows 自动登录：

```
set vpn parameter -windowsAutoLogon ON
```

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

使用 Kerberos 身份验证进行自动登录

从适用于 Windows 23.10.1.7 及更高版本的 Citrix Secure Access 客户端开始，您可以使用 Kerberos 身份验证方法进行自动登录。

使用此身份验证方法，后端 Kerberos SSO 无缝运行，管理员无需向客户端计算机推送任何额外的后端 URL 配置。 此外，网关 URL 会自动添加到客户端计算机上的 **Internet 属性 > 受信任的站点** 部分。

先决条件

- **管理员配置**：如果在 NetScaler 上配置了 Kerberos 身份验证并将 `windowsAutoLogon` 设置为 ON，则 Kerberos 身份验证方法将自动在 NetScaler 上启用。有关详细信息，请参阅 在 NetScaler 设备上配置 Kerberos 身份验证。

  管理员还必须在其客户端计算机上配置 Kerberos 身份验证。有关详细信息，请参阅 在客户端上配置 Kerberos 身份验证。
- **最终用户配置**：最终用户必须在 Citrix Secure Access 客户端上启用 Microsoft Edge WebView。有关详细信息，请参阅 适用于 Windows Citrix Secure Access 的 Microsoft Edge WebView 支持。

使用 Citrix Secure Access™ 客户端配置 Kerberos 身份验证

要使用 Citrix Secure Access 客户端配置 Kerberos 身份验证，管理员必须设置 `EnableKerberosAuth` VPN 客户端注册表项。有关 VPN 注册表项的详细信息，请参阅 NetScaler Gateway Windows VPN 客户端注册表项。

参考

- 使用本地 Citrix Gateway 作为身份提供程序，将域直通到 Citrix Workspace
- 如何为 Kerberos 约束委派配置 NetScaler

始终在线

NetScaler Gateway 的 Always On 功能可确保用户始终连接到企业网络。这种持久的 VPN 连接是通过自动建立 VPN 隧道来实现的。

注意

Always On 功能支持 NetScaler 12.0 Build 51.24 及更高版本的强制门户。

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

何时使用 Always On

当您需要根据用户位置提供无缝 VPN 连接并阻止未连接到 VPN 的用户访问网络时，请使用 Always On。

以下场景说明了 Always On 的使用。

- 员工在企业网络外部启动笔记本电脑，需要帮助建立 VPN 连接。

  解决方案： 当笔记本电脑在企业网络外部启动时，Always On 会无缝建立隧道并提供 VPN 连接。

- 使用 VPN 连接的员工进入企业网络。员工已切换到企业网络，但仍连接到 VPN 隧道，这不是理想状态。

  解决方案： 当员工进入企业网络时，Always On 会拆除 VPN 隧道，并将员工无缝切换到企业网络。

- 员工移出企业网络并合上笔记本电脑（未关机）。员工在恢复使用笔记本电脑时需要帮助建立 VPN 连接。

  解决方案： 当员工移出企业网络时，Always On 会无缝建立隧道并提供 VPN 连接。

- 企业希望在其用户未连接到 VPN 隧道时规范其网络访问。

  解决方案： 根据配置，Always On 会限制访问，允许用户仅访问网关网络。

了解 Always On 框架

Always On 自动将用户连接到客户端之前已建立的 VPN 隧道。用户首次需要 VPN 隧道时，必须连接到 NetScaler Gateway URL 并建立隧道。Always On 配置下载到客户端后，此配置将驱动后续隧道的建立。

Citrix Secure Access™ 客户端可执行文件始终在客户端计算机上运行。当用户登录或网络发生变化时，Citrix Secure Access 客户端会确定用户笔记本电脑是否在企业网络上。根据位置和配置，Citrix Secure Access 客户端会建立隧道或拆除现有隧道。

只有在用户登录计算机后才启动隧道建立。Citrix Secure Access 客户端使用客户端计算机的凭据向网关服务器进行身份验证并尝试建立隧道。

隧道的自动重新建立

当 NetScaler Gateway 拆除 VPN 隧道时，将触发隧道的自动重新建立。

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

注意

当端点分析失败时，NetScaler Gateway 客户端不会重新尝试建立隧道，但会显示错误消息。如果出现身份验证失败，NetScaler Gateway 客户端会提示用户输入凭据。

无缝隧道建立支持的用户身份验证方法

支持的用户身份验证方法如下：

- 用户名 + AD 密码：如果使用 Windows 用户名和密码进行身份验证，Citrix Secure Access 客户端将使用这些凭据无缝建立隧道。
- 用户证书：如果使用用户证书进行身份验证，并且客户端计算机上只有一个证书，Citrix Secure Access 客户端将使用此证书无缝建立隧道。如果安装了多个客户端证书，则在用户选择首选证书后建立隧道。Citrix Secure Access 客户端将使用此首选证书用于后续隧道。

  如果智能卡共享用户证书，则如果证书是动态安装在存储中的，而不是存储中已有的证书，则无法实现自动登录。
- 用户证书和用户名 + AD 密码：此身份验证方法是前面描述的身份验证方法的组合。

注意

支持所有其他身份验证机制，但对于任何其他身份验证方法，隧道建立都不是无缝的。

Always On 的配置要求

企业管理员必须对托管设备强制执行以下操作：

- 用户不得终止特定配置的进程/服务
- 用户不得卸载特定配置的软件包
- 用户不得更改特定的注册表项

注意

如果用户具有管理权限（例如在非托管设备的情况下），该功能可能无法按预期工作。

启用 Always On 功能时的注意事项

在启用 Always On 功能之前，请查看以下部分。

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

主要网络访问：隧道建立后，到企业网络的流量根据分流隧道配置决定。未提供其他配置来覆盖此行为。

客户端计算机的代理设置：连接到网关服务器时，客户端计算机的代理设置将被忽略。

注意

NetScaler 设备代理配置不会被忽略。只有客户端计算机的代理设置会被忽略。系统上配置了代理的用户会收到通知，告知 VPN 插件已忽略其代理设置。

配置 Always On

要配置 Always On，请在 NetScaler Gateway 设备上创建 Always On 配置文件并应用该配置文件。

要创建 Always On 配置文件：

1. 在 NetScaler GUI 中，导航到 **Configuration > NetScaler Gateway > Policies > AlwaysON。**
2. 在 **AlwaysON Profiles** 页面上，单击 **Add**。
3. 在 **创建 AlwaysON 配置文件** 页面上，输入以下详细信息：
   - **名称** – 配置文件的名称。
   - **Location Based VPN (client-side registry name: LocationDetection) – Select one of the following settings:
     - **远程**：使客户端能够检测其是否在企业网络中，如果不在企业网络中则建立隧道。远程是默认设置。
     - **随处**：让客户端跳过位置检测，无论客户端位置如何都建立隧道。
   - **客户端控制** – 选择以下设置之一：
     - **拒绝**：阻止用户注销并连接到另一个网关。拒绝是默认设置。
     - **允许**：使用户能够注销并连接到另一个网关。
   - **VPN 故障时的网络访问 (客户端注册表名称: AlwaysOn)** – 选择以下设置之一：
     - **完全访问**：允许在隧道未建立时网络流量流向客户端和从客户端流出。完全访问是默认设置。
     - **仅限网关**：阻止在隧道未建立时网络流量流向客户端或从客户端流出。但是，允许流向或流出网关 IP 地址的流量。

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

注意： 在 **仅限网关** 模式下，只有虚拟服务器、DNS 和 DHCP 流量未被阻止。要解除阻止其他网站、IP 地址范围或 IP 地址，您必须使用以分号分隔的 FQDN、IP 地址范围或 IP 地址列表来设置 **AlwaysOnAllowlist** 注册表。 例如：mycompany.com,mycdn.com,10.120.67.0-10.120.67.255,67.67.67.67

4. 单击 **创建** 完成配置文件创建。

要应用 Always On 配置文件：

1. 在 NetScaler 界面中，选择 **配置 > NetScaler Gateway > 全局设置**。
2. 在“全局设置”页面上，单击“**更改全局设置**”链接，然后选择“**客户端体验**”选项卡。
3. 从“**AlwaysON 配置文件名称**”下拉菜单中，选择新创建的配置文件，然后单击“**确定**”。

注意： 可以在会话配置文件中进行类似配置，以在组级别、服务器级别或用户级别应用策略。

关于 IIP 的说明

机器级隧道使用基于证书的身份验证，并且创建的会话将证书的通用名称作为用户名。因此，如果设备证书具有唯一的通用名称，则不同机器的会话将具有不同的用户名，从而具有不同的 IIP。请确保生成具有唯一名称的设备证书。理想情况下，您必须使用机器名称作为设备证书的通用名称。

管理员用户和非管理员用户的不同配置行为摘要

下表总结了不同配置的行为。它还详细说明了某些用户操作的可能性，这些操作可能会影响 Always On 功能。

NETWORKACCESS ONVPNFAILURE	客户端控制	非管理员用户	管理员用户
`fullaccess`	允许	隧道自动建立。用户可以注销并保持脱离网络。用户还可以指向另一个 NetScaler Gateway。	隧道自动建立。用户可以注销并保持脱离企业网络。用户还可以指向另一个 NetScaler Gateway。
`fullaccess`	拒绝	隧道会自动建立。用户无法注销或指向其他 NetScaler Gateway。	隧道会自动建立。用户可以卸载 Citrix Secure Access 客户端或移动到其他 NetScaler Gateway。

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

NETWORKACCESS ONVPNFAILURE	客户端控制	非管理员用户	管理员用户
onlyToGateway	允许	隧道会自动建立。用户可以注销（无网络访问）。用户还可以指向另一个 NetScaler Gateway，在这种情况下，访问权限仅授予新指向的 NetScaler Gateway。	隧道会自动建立。用户可以卸载 Citrix Secure Access 客户端或移动到其他 NetScaler Gateway。
onlyToGateway	拒绝	隧道会自动建立。用户无法注销或指向其他 NetScaler Gateway。	隧道会自动建立。用户可以卸载 Citrix Secure Access 客户端或移动到其他 NetScaler Gateway。

在“始终在线”关闭时允许选定的 URL

即使在“始终在线”关闭且网络被锁定时，用户也可以访问一些网站。管理员可以使用 **AlwaysOnAllowlist** 注册表添加在“始终在线”关闭时要启用访问的网站。

注意：

- **AlwaysOnAllowlist** 注册表从 13.0 build 47.x 及更高版本开始支持。
- **AlwaysOnAllowlist** 注册表位置是 Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Client。
- 通配符 URL/FQDN 在 **AlwaysOnAllowlist** 注册表中不受支持。

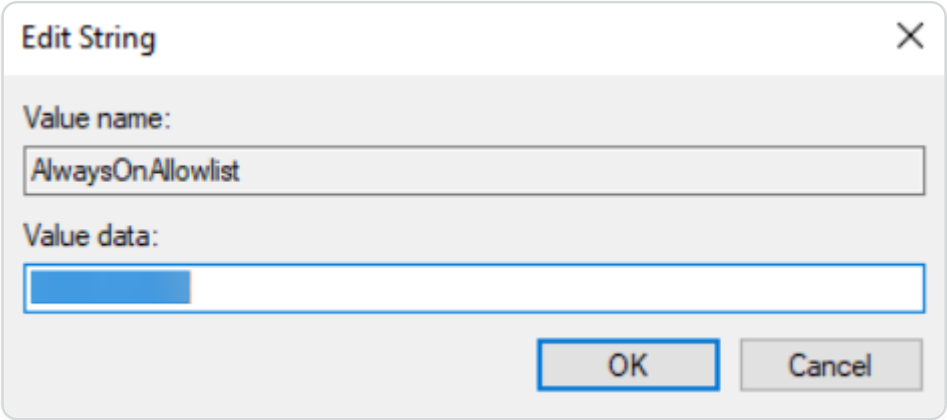
设置 AlwaysOnAllowlist 注册表

将 **AlwaysOnAllowlist** 注册表设置为以分号分隔的 FQDN、IP 地址范围或您希望允许访问的 IP 地址列表。

示例： example.citrix.com;192.0.2.0;192.0.2.100-192.0.2.255

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

下图显示了一个 **AlwaysOnAllowlist** 注册表示例。



Windows 登录前始终开启 VPN（原 Always On 服务）

此 **Windows 登录前始终开启 VPN**（原 Always On 服务）功能使用户能够在用户登录 Windows 系统之前建立机器级 VPN 隧道。该隧道在机器关闭之前一直保持活动状态。用户登录后，机器级 VPN 隧道将由用户级 VPN 隧道接管。用户注销后，用户级隧道将被断开，并建立机器级隧道。**Windows 登录前始终开启 VPN** 只能通过使用高级身份验证策略进行配置。有关详细信息，请参阅配置 Windows 登录前始终开启 VPN。

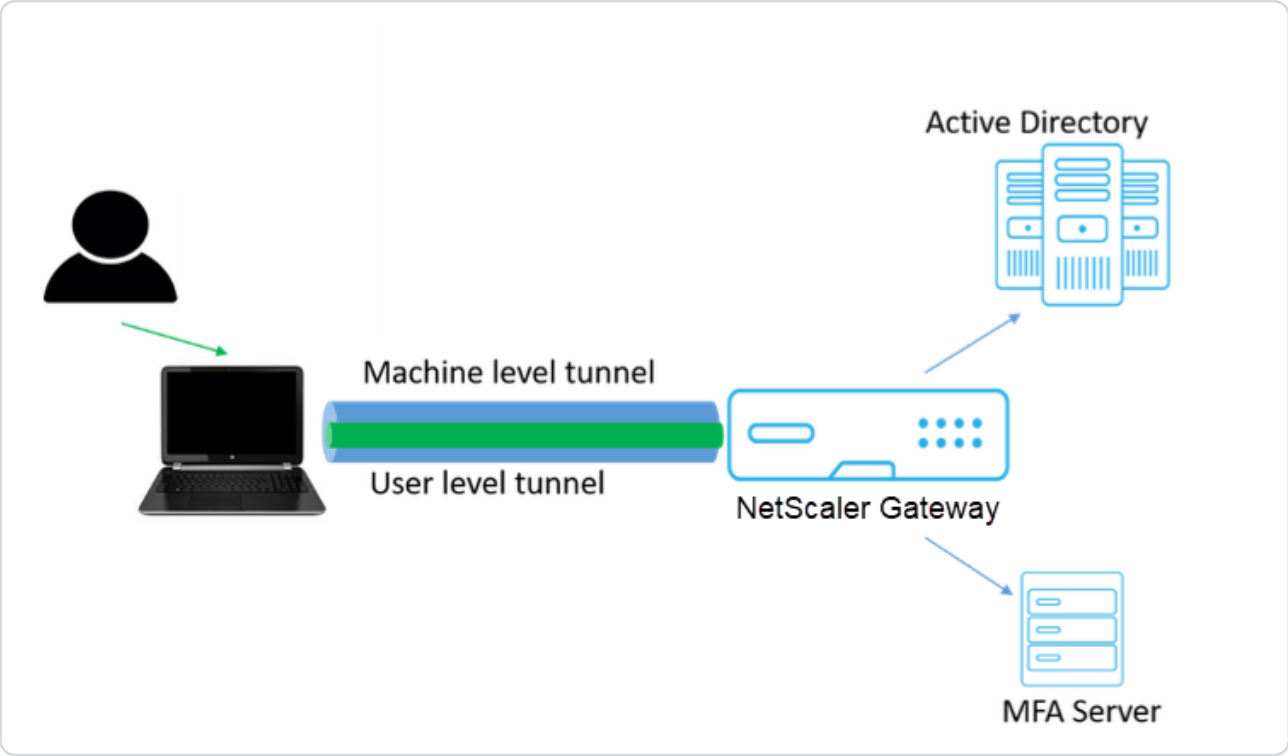
Windows 登录前始终开启 VPN 功能

- 管理员可以向远程工作的首次用户提供一次性密码，用户可以使用该密码连接到域控制器以更改其密码。
- 管理员可以在用户登录之前远程管理/强制执行设备的 AD 策略。
- 用户登录后，管理员可以根据用户组向用户提供精细的控制级别。例如，使用用户级隧道，您可以限制或向特定用户组提供对资源的访问权限。
- 用户隧道可以根据用户要求配置 MFA。
- 多个用户可以使用同一台机器。对选择性资源的访问权限是根据用户配置文件提供的。例如，多个用户可以在自助服务终端中轻松使用一台机器。
- 远程工作的用户连接到域控制器以更改其密码。
- Windows 机器可以使用企业活动目录 (AD) 验证用户的登录凭据，并且机器上的 Windows 凭据不会被缓存。此外，新的企业 AD 用户能够无缝登录到机器。
- 即使在用户登录之前，Windows 机器也成为企业内部网的一部分，允许 IT 管理员从企业网络访问客户端机器以进行调试。
- 即使不同的用户登录或注销机器，Windows 机器的 VPN 隧道也保持连接。

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

了解 Windows 登录前始终开启 VPN

以下是 **Windows 登录前始终开启 VPN** 功能的事件流程。



- 用户打开笔记本电脑。使用设备证书作为身份，建立到 NetScaler Gateway 的机器级隧道。
- 用户使用 AD 凭据登录笔记本电脑。
- 登录后，用户需要进行 MFA 挑战。
- 成功认证后，机器级隧道将替换为用户级隧道。
- 用户注销后，用户级隧道将替换为机器级隧道。

注意事项：

- NetScaler Gateway 和 VPN 插件必须是 13.0.41.20 或更高版本。
- 如果客户端计算机没有互联网连接，**Windows 登录前始终开启 VPN** 会等待互联网连接可用后才建立 VPN 隧道。
- 如果客户端计算机连接到强制门户网络，**Windows 登录前始终开启 VPN** 会等待用户向强制门户进行身份验证。用户登录并启用互联网访问后，**Windows 登录前始终开启 VPN** 会建立 VPN 隧道。
- Windows 登录前始终开启 VPN 功能支持 NetScaler 的强制门户。
- 如果未为 Windows 启用缓存登录凭据选项，则用户在以下情况下无法登录：
  - 计算机没有互联网连接

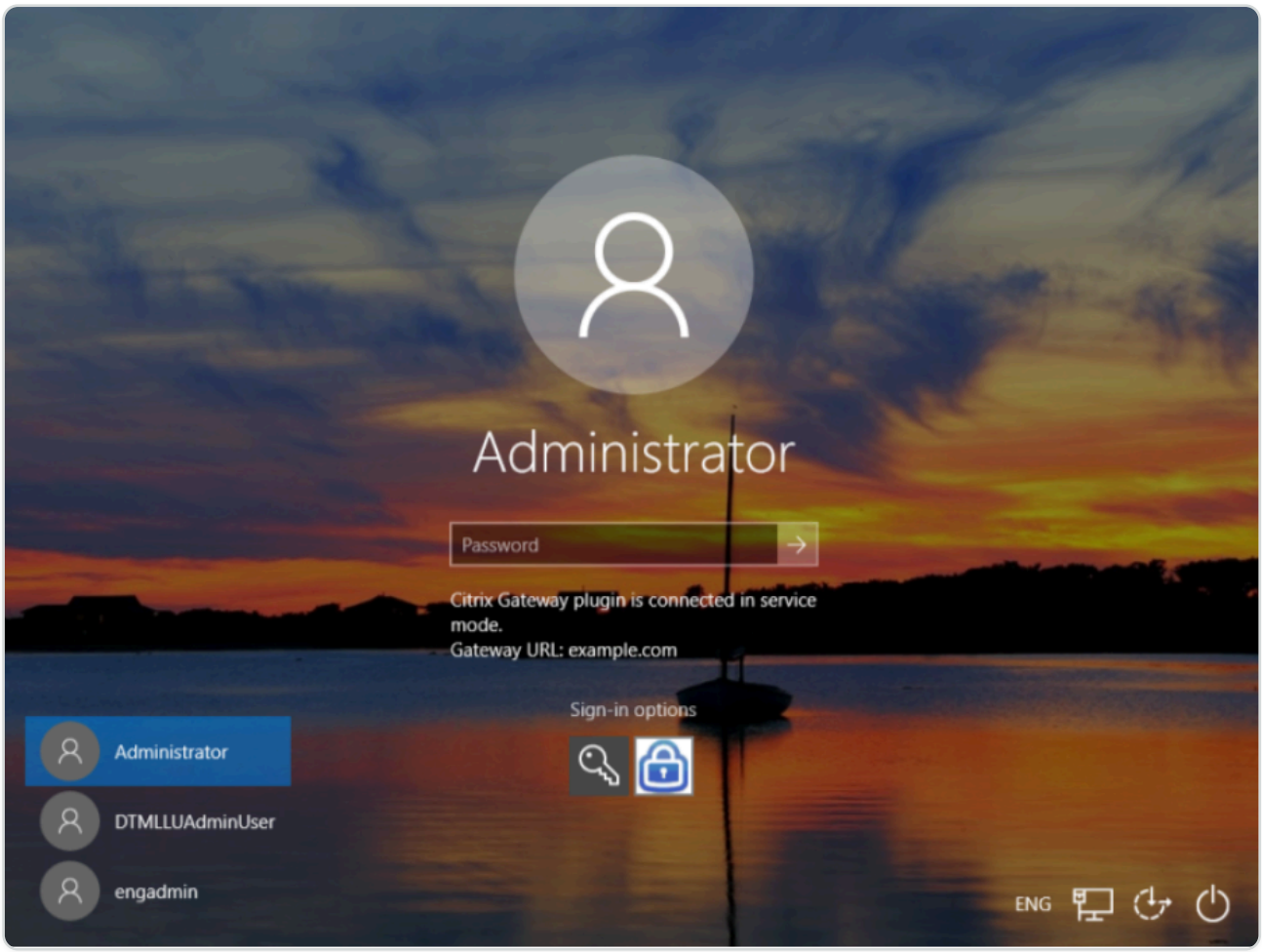
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 计算机连接到强制门户网络

- 管理员必须在向最终用户显示登录页面之前检查设备证书吊销状态。

配置 Windows 登录前始终开启 VPN 后的 Windows 凭据管理器屏幕

在配置了 **Windows 登录前始终在线 VPN** 功能后，**Windows 凭据管理器** 屏幕会按如下方式修改。



当您在登录屏幕上单击“**登录选项**”时，将显示以下信息：

- NetScaler Gateway 图标指示计算机是否已连接到 NetScaler Gateway。
- 根据用户配置模式，登录屏幕上会显示以下语句之一。
  - NetScaler Gateway 以服务模式连接
  - NetScaler Gateway 以用户模式连接

配置 Windows 登录前始终开启 VPN

本节详细说明了如何通过使用高级策略配置 **Windows 登录前始终开启 VPN**。

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

先决条件

- NetScaler Gateway 和 VPN 插件必须是 13.0.41.20 或更高版本。
- NetScaler Advanced Edition 及更高版本是此解决方案正常工作所必需的。
- 您只能通过使用高级策略来配置此功能。
- VPN 虚拟服务器必须已启动并正在运行。

主要配置步骤

Windows 登录前始终开启 VPN 配置涉及以下主要步骤：

1. 设置机器级隧道
2. 设置用户级隧道（可选）
3. 启用用户身份验证
   a. 配置 VPN 虚拟服务器，安装 CA 证书，并将证书密钥绑定到虚拟服务器。
   b. 创建身份验证配置文件
   c. 创建身份验证虚拟服务器
   d. 创建身份验证策略
   e. 将策略绑定到身份验证配置文件

计算机级隧道

计算机级隧道使用设备证书作为身份建立到 NetScaler Gateway。设备证书必须安装在客户端计算机的计算机存储中。这仅适用于 Windows 登录前始终开启服务。

有关设备证书的更多详细信息，请参阅使用设备证书进行身份验证。

重要提示：

如果 NetScaler Gateway 设备上的 VPN 虚拟服务器配置在非标准端口（443 以外的端口）上，则计算机级隧道将无法按预期工作。

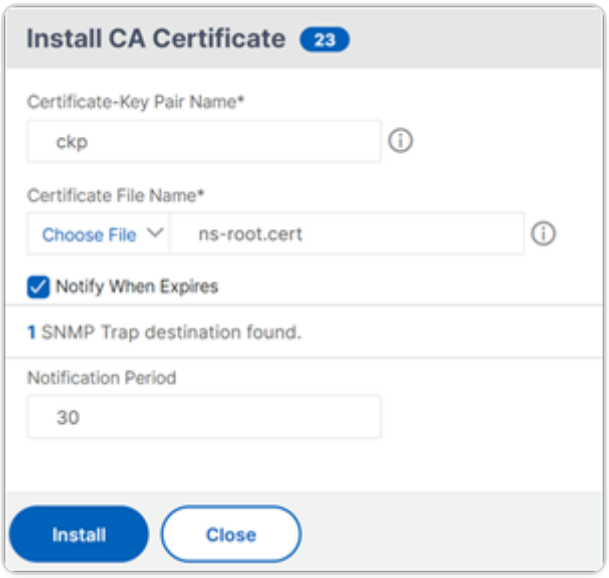
使用设备证书设置计算机级隧道

使用 GUI 进行基于设备证书的身份验证配置

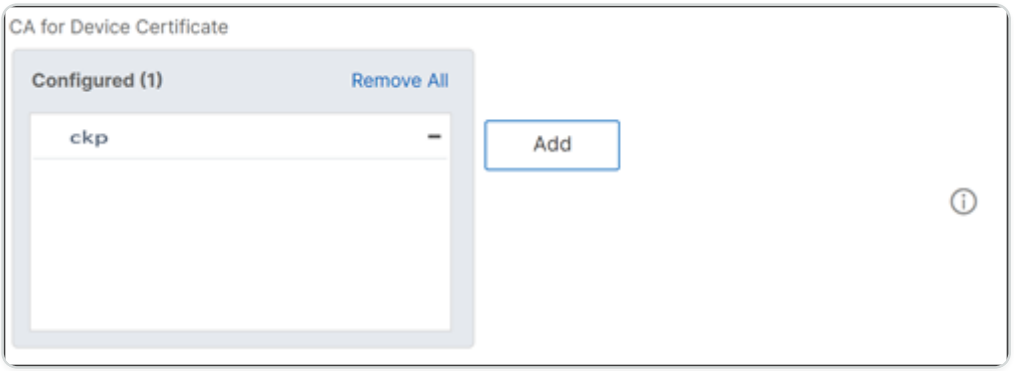
1. 在“**配置**”选项卡上，导航到“**NetScaler Gateway > 虚拟服务器**”。
2. 在 NetScaler Gateway 虚拟服务器页面上，选择一个现有虚拟服务器，然后单击“**编辑**”。
3. 在“**证书**”下，单击“**CA 证书**”。

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

4. 在“**CA 证书绑定**”页面上，单击“**选择 CA 证书**”字段旁边的“**添加**”，更新所需信息，然后单击“**安装**”。



5. 在“**VPN 虚拟服务器**”页面上，单击编辑图标。
6. 在**基本设置**部分中，单击**更多**。
7. 在**设备证书的 CA** 部分旁边单击**添加**，然后单击**确定**。



注意： 不要选中**启用设备证书**复选框。

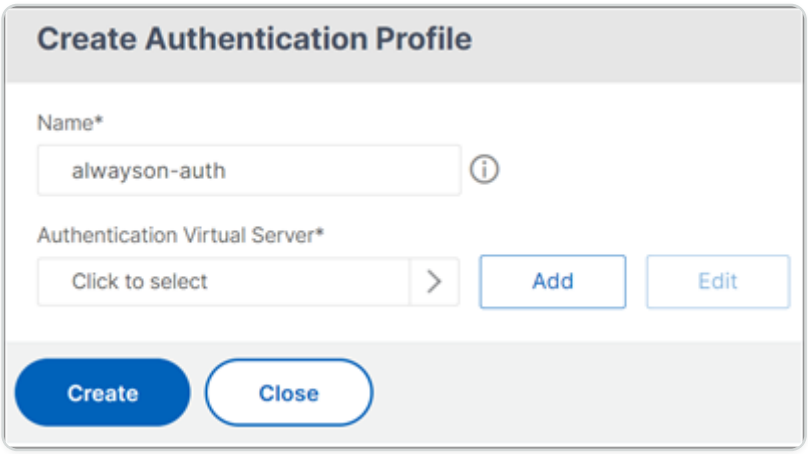
8. 要将 CA 证书绑定到虚拟服务器，请在**证书**部分下单击**CA 证书**。在**SSL 虚拟服务器 CA 证书绑定**页面下单击**添加绑定**。

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

注意：

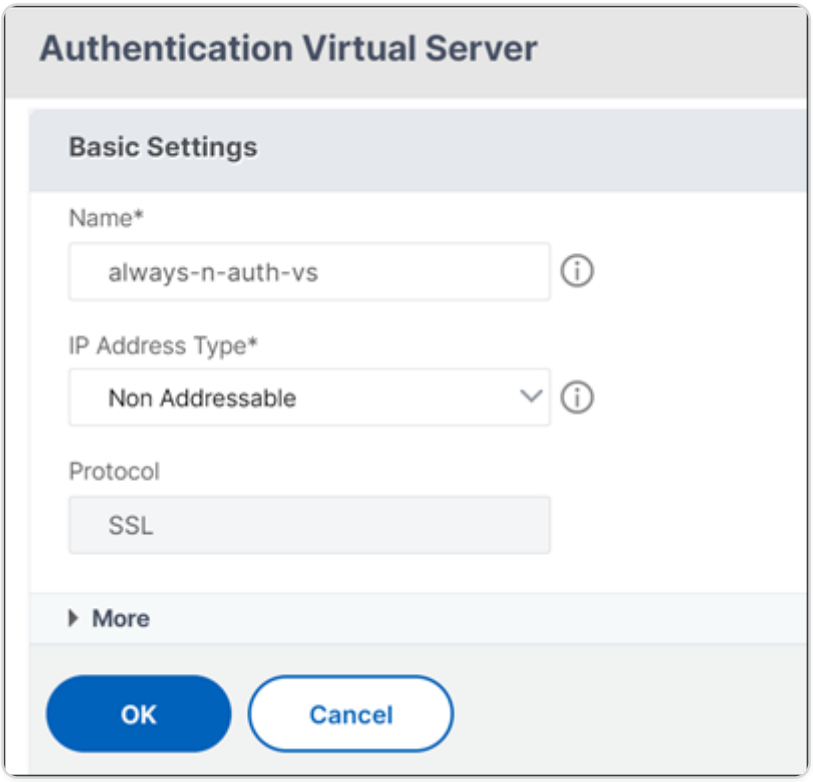
- 设备证书的主题公用名 (CN) 字段不能为空。如果设备尝试使用空的 CN 设备证书登录，则其 VPN 会话将以“anonymous”作为用户名创建。在 IIP 中，如果多个会话具有相同的用户名，则以前的会话将被断开连接。因此，当启用 IIP 时，您会注意到由于公用名为空而导致的功能影响。
- 所有可能签署颁发给客户端的设备证书的 CA 证书（根证书和中间证书）都必须绑定在**设备证书的 CA** 部分以及步骤 4 和 5 中虚拟服务器的**CA 证书绑定**部分下。有关将 CA 证书与中间/从属证书链接的更多信息，请参阅安装、链接和更新证书。
- 如果配置了多个设备证书，则会尝试使用有效期最长的证书进行 VPN 连接。如果此证书成功通过 EPA 扫描，则建立 VPN 连接。如果此证书在扫描过程中失败，则使用下一个证书。此过程将持续到所有证书都尝试完毕。

9. 在**CA 证书绑定**页面上，选择证书。
10. 单击**绑定**。
11. 创建身份验证虚拟服务器。
    a. 在**VPN 虚拟服务器**页面上，导航到**高级设置 > 身份验证配置文件**，然后单击**添加**。
    b. 在**创建身份验证配置文件**页面上，为身份验证配置文件分配一个名称，然后单击**创建**。



    c. 在**身份验证虚拟服务器**页面上，为身份验证虚拟服务器分配一个名称。将 IP 地址类型选择为**不可寻址**，然后单击**确定**。

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



注意：

身份验证虚拟服务器始终处于 DOWN 状态。

12. 创建身份验证策略。

    a. 在“**Security > AAA-Application Traffic > Authentication Virtual Servers**”页面的“**Advanced Authentication Policies**”部分中，选择身份验证策略，然后单击“**Add Binding**”。

    b. 在“**Policy Binding**”页面上，单击“**Select Policy**”字段旁边的“**Add**”。

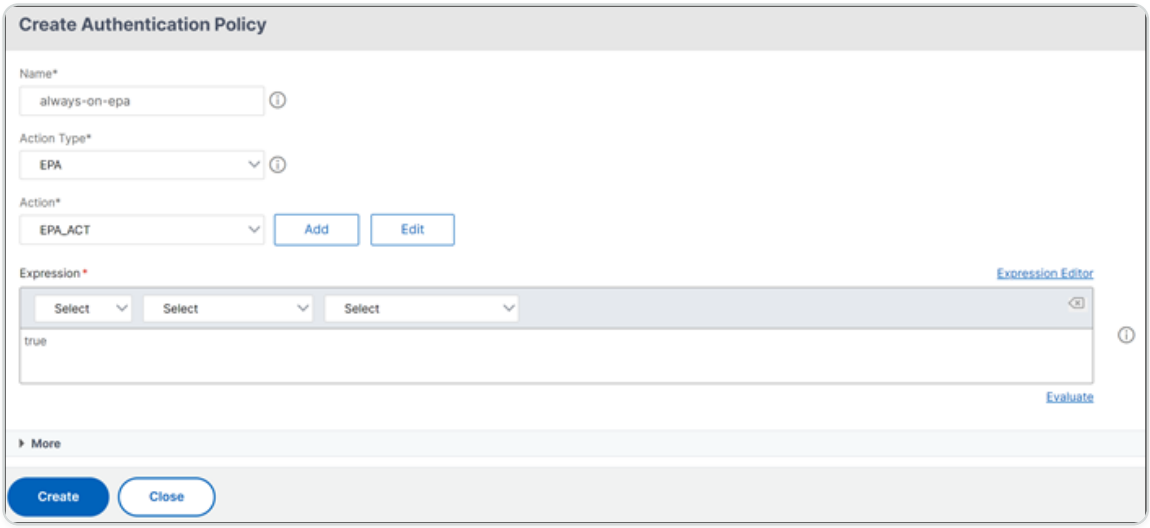
    c. 在“创建身份验证策略”页面上；

        i. 为高级身份验证策略分配一个名称。

        ii. 从“**Action Type**”列表中选择“**EPA**”。

        iii. 单击“**Action**”旁边的“**Add**”。

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

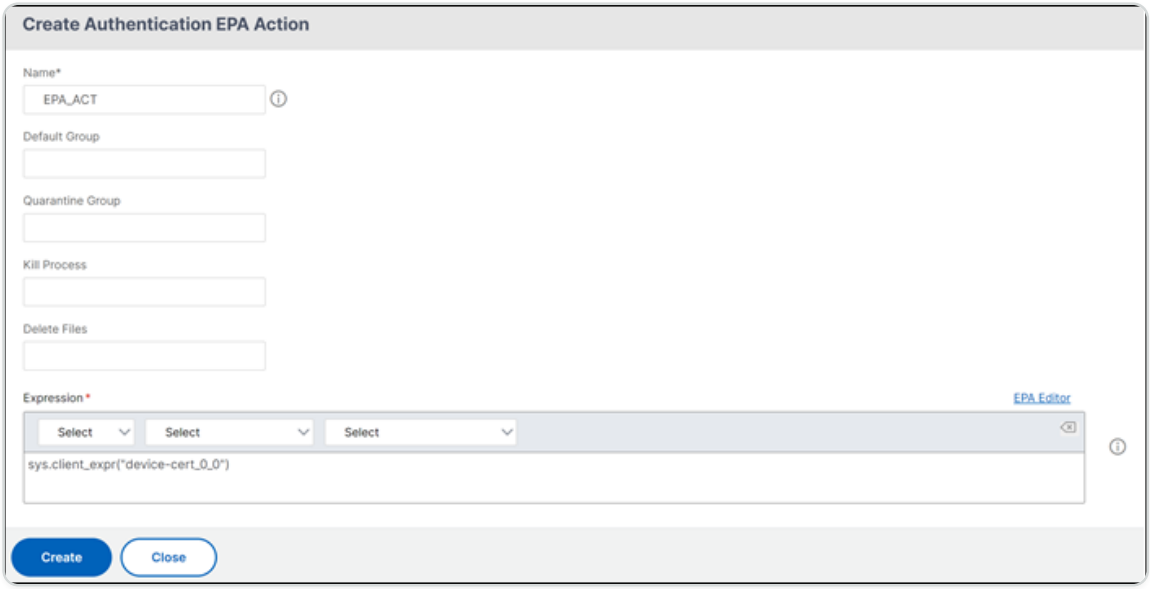


d. 在“创建身份验证 EPA 操作”页面上；

   i. 为 EPA 操作分配一个名称。

   ii. 在“**Expression**”字段中输入 `sys.client_expr("device-cert_0_0")`。

   iii. 单击“**Create**”。



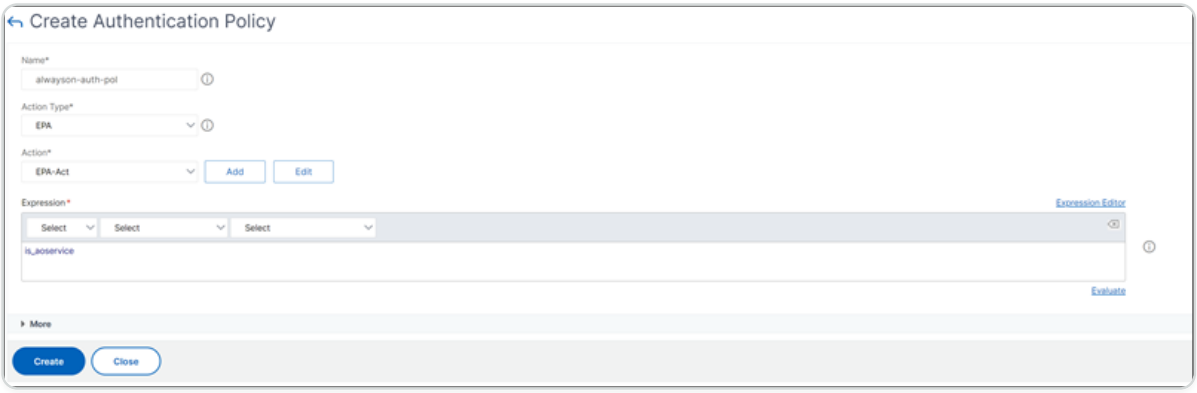
13. 在“**创建认证策略**”页面上；

   a. 为身份验证策略分配一个名称。

   b. 在“**表达式**”字段中输入 **is_aoservice**。

   c. 单击“**创建**”。

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



14. 在“策略绑定”页面上，在“**优先级**”中输入 **100**，然后单击“**绑定**”。

使用 CLI 进行基于设备证书的身份验证配置

1. 在 VPN 虚拟服务器上安装 CA 证书。

```
add ssl certkey ckp -cert t_CA.cer
```

2. 将 CA 证书绑定到 VPN 虚拟服务器。

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

示例

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

3. 将服务器证书及其对应的私钥设置为 VPN 虚拟服务器。

```
set vpn vserver <vServerName> -certkeyNames <string>
```

示例

```
set vpn vserver TestClient -certkeyNames ag51.xm.nsi.test.com
```

4. 添加身份验证虚拟服务器。

```
add authentication authnProfile <name>  {-authnVsName <string>}
```

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

示例

```
add authentication authnProfile always_on -authnVsName
always_on_auth_server
```

5. 创建身份验证 EPA 操作。

```
add authentication epaAction <name> -csecexpr <expression>
```

示例

```
add authentication epaAction epa-act -csecexpr
 `sys.client_expr("device-cert_0_0")`
```

6. 创建身份验证策略

```
add authentication Policy <name> -rule <expression> -action <string>
```

示例：

```
add authentication Policy always_on_epa_auth -rule is_aoservice -action
epa_auth
```

重要提示：

- 机器级隧道配置现已完成。要在 Windows 登录后设置用户级隧道，请参阅“**用户级隧道**”部分。
- 在客户端计算机上，设备证书采用 .pfx 格式。.pfx 证书安装在 Windows 计算机上，因为 Windows 能够识别 .pfx 格式。此文件包含证书和密钥文件。此证书必须与绑定到虚拟服务器的域相同。可以使用客户端证书向导生成 .pfx 和服务器证书以及密钥。这些证书可与证书颁发机构一起使用，以生成带有服务器证书和域的相应 .pfx。.pfx 证书安装在计算机帐户的个人文件夹中。`show aaa session` 命令在 NetScaler 设备上显示设备隧道。

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

用户级隧道

使用 GUI 将机器级隧道替换为用户级隧道

注意： 表达式 `is_aoservice.not` 适用于 NetScaler Gateway 13.0.41.20 及更高版本。

1. 配置用户身份验证策略。

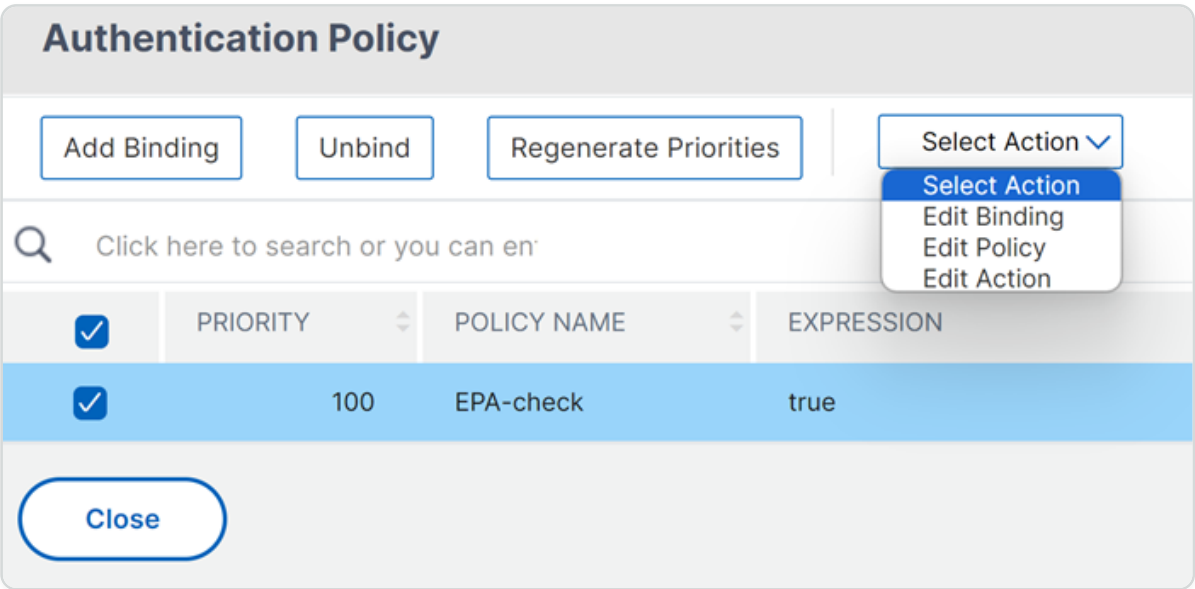
   a. 导航到 **NetScaler Gateway > 虚拟服务器**，然后选择一个虚拟服务器。

   b. 在**高级设置**中，单击**身份验证配置文件**。

   c. 配置身份验证配置文件。

   d. 在 **Configuration > Security > AAA-Application Traffic > Authentication Virtual Servers** 页面上，选择身份验证策略。

   e. 在**选择操作**中，单击**编辑绑定**并将已绑定策略的**转到表达式**更改为 **NEXT** 而不是 **END**。

   绑定策略(/en-us/netscaler-gateway/media/always-on-goto-next.png)

   f. 点击 **绑定**，然后在 **身份验证策略** 页面中，选择身份验证策略并点击 **添加绑定**。

   绑定策略2(/en-us/netscaler-gateway/media/alwayson-edit-binding.png)

   g. 在策略绑定页面上，点击 **选择策略** 旁边的 **添加**。

   在创建身份验证策略页面上；

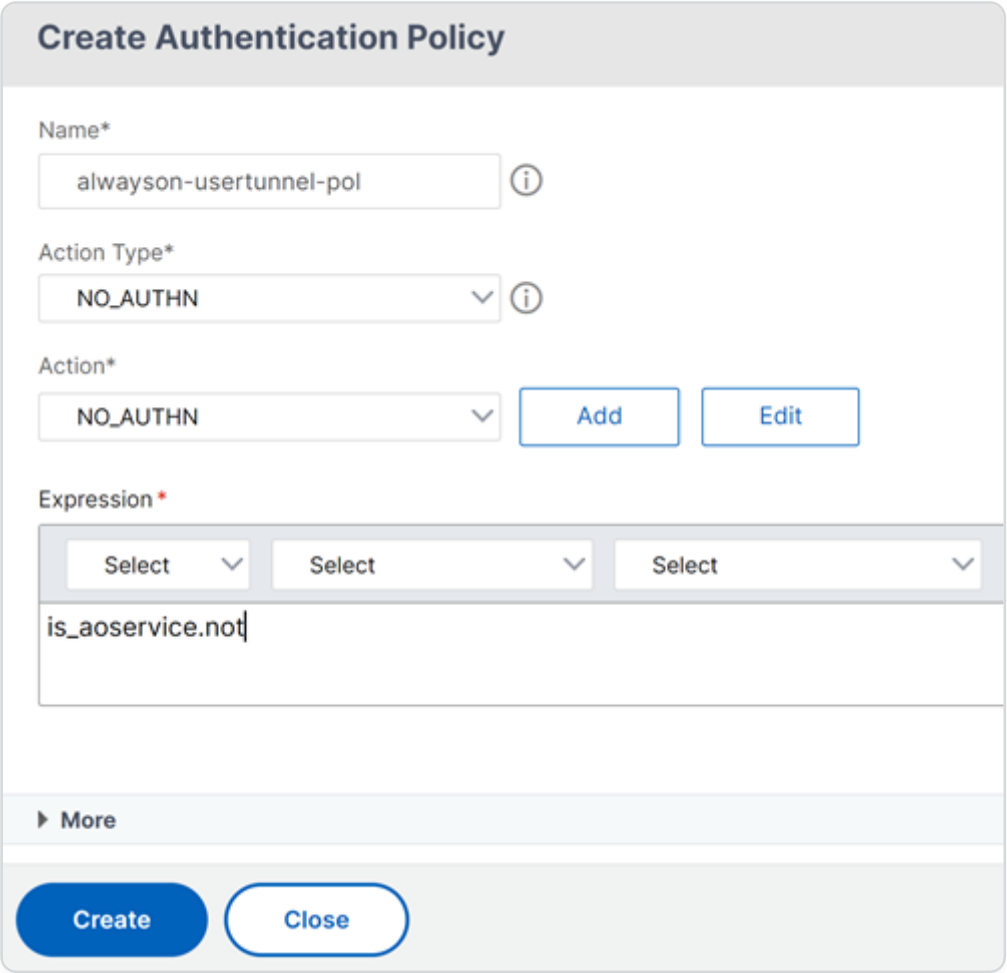
      i. 输入要创建的“无身份验证”策略的名称。

      ii. 选择操作类型为 **No_AUTHN**。

      iii. 在 **表达式** 字段中输入 **is_aoservice.not**。

      iv. 点击 **创建**。

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



2. 在 **选择操作** 中，点击 **编辑绑定**。

   编辑绑定用户隧道(/en-us/netscaler-gateway/media/aoswup-7cc.png)

3. 在策略绑定页面上，在 **优先级** 中输入 **110**。点击 **选择下一个因素** 旁边的 **添加**。

   a. 在身份验证策略标签页面上，为策略标签输入一个描述性名称，选择登录方案，然后点击 **继续**。

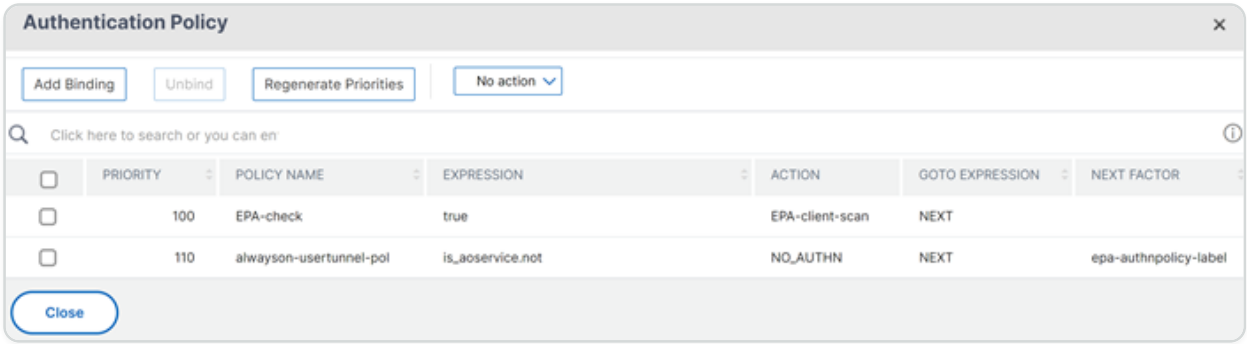
   b. 在 **选择策略** 中，点击 **添加** 并创建 LDAP 身份验证策略。

   c. 点击 **创建**，然后点击 **绑定**。

   d. 点击“**完成**”，然后点击“**绑定**”。

   在“身份验证策略”页面中，“**下一个因素**”列显示已配置的下一个因素策略。

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



4. 您可以将 LDAP 策略配置为身份验证策略的下一个因素。

   a. 在“创建身份验证策略”页面上，输入 LDAP 策略的名称。

   b. 将“**操作类型**”选择为“**LDAP**”。

   c. 将“**操作**”输入为已配置的 LDAP 操作。

注意：

- 有关创建登录架构 XML 文件，请参阅登录架构 XML 文件。
- 有关创建策略标签，请参阅验证策略标签。
- 有关创建 LDAP 身份验证策略，请参阅使用配置实用程序配置 LDAP 身份验证。

使用 CLI 将计算机级隧道替换为用户级隧道

1. 将策略绑定到身份验证虚拟服务器

```
bind authentication vserver <name> -policy <name> -priority
 <positive_integer> -gotoPriorityExpression <expression>
```

   示例

```
bind authentication vserver alwayson-auth-vserver -policy alwayson-
auth-pol -priority 100 -gotoPriorityExpression NEXT
```

2. 添加一个身份验证策略，其操作为 `NO_AUTH`，表达式为 `is_aoservice.not,`，并将其绑定到该策略。

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

```
add authentication Policy <name> -rule <expression> -action <string>



bind authentication vserver <name> -policy <name> -priority
<positive_integer> -gotoPriorityExpression <expression>
```

示例

```
add authentication Policy alwayson-usertunnel-pol -rule
is_aoservice.not -action NO_AUTHN



bind authentication vserver alwayson-auth-vserver -policy alwayson-
usertunnel-pol -priority 110
```

3. 添加下一个因子并将策略标签绑定到下一个因子。

```
add authentication policylabel <labelName> -loginSchema <string>



bind authentication  policylabel <string>  -policyName <string>  -
priority <positive_integer> -gotoPriorityExpression <expression>
-nextFactor <string>
```

示例

```
add authentication policylabel user-tunnel-auth-label -loginSchema
singleauth_alwayson



bind authentication policylabel user -policyName alwayson-usertunnel-
pol -priority 100
```

4. 配置 LDAP 策略并将其绑定到用户隧道策略标签。

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

```
add authentication policy <name>  -rule <expression>  -action <string>


bind authentication vserver <vserver_name> -policy <string>  -priorit <
positive integer>  gotoPriorityExpression <string>
```

示例

```
add authentication Policy LDAP_new -rule true -action LDAP_new


bind authentication policylabel user-tunnel-auth-label -policyName
LDAP_new -priority 100 -gotoPriorityExpression NEXT
```

客户端配置

如果需要位置检测功能，`AlwaysOn, locationDetection, and suffixList registries` 是可选的。

要访问注册表项，请导航到以下路径：

Computer>HKEY_LOCAL_MACHINE>SOFTWARE>Citrix®>Secure Access Client

注册表项	注册表类型	值和描述
AlwaysOnService	REG_DWORD	1 => 建立机器级隧道，但不建立用户级隧道；2 => 建立机器级隧道和用户级隧道
AlwaysOnURL	REG SZ	用户希望连接的 NetScaler Gateway 虚拟服务器的 URL。**示例：** `https://xyz.companyDomain.com` **重要提示：** 只有一个 URL 负责机器级隧道和用户级隧道。AlwaysOnURL 注册表有助于服务和用户级组件协同工作，

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

注册表项	注册表类型	值和描述
		并根据设计连接单独的隧道，即机器级隧道和用户级隧道。
AlwaysOn	REG_DWORD	1 => VPN 故障时允许网络访问；2 => VPN 故障时阻止网络访问
AlwaysOnAllowlist	REG_SZ	在机器以严格模式运行时必须列入白名单的 IP 地址或 FQDN 的分号分隔列表。**示例：** `8.8.8.8;linkedin.com`
UserCertCAList	REG_SZ	根 CA 名称的逗号或分号分隔列表，即证书的颁发者名称。在 Always On 服务的上下文中，客户可以指定 CA 列表以从中选择客户端证书。**示例：** `example.net;xyz.gov.in`
locationDetection	REG_DWORD	1 => 启用位置检测；0 => 禁用位置检测
suffixList	REG SZ	分号分隔的域列表，负责在启用位置检测时，随时检查机器是否在内网中。**示例：** `citrite.net,example.net`

有关这些注册表项的更多信息，请参阅 Always On。

注意：

- 配置 Always On 服务时，在客户端上，NetScaler Gateway 虚拟服务器或 NetScaler 上配置的 Always On 配置文件将被忽略。因此，在配置 Always On 服务时，请确保同时启用 `locationDetection` 和 `AlwaysOn` VPN 注册表。
- `ClientControl` 注册表配置仅在 Always On 模式下受支持，而在 Always On 服务模式下不受支持。因此，当启用 Always On 服务模式时，不支持**注销**选项。

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

使用高级策略创建 VPN 策略

经典策略引擎 (PE) 和高级策略基础架构 (PI) 是 NetScaler 当前支持的两种不同的策略配置和评估框架。

高级策略基础架构包含强大的表达式语言。表达式语言可用于定义策略中的规则、定义操作的各个部分以及其他受支持的实体。表达式语言可以解析请求或响应的任何部分，还可以让您深入查看标头和有效负载。相同的表达式语言可扩展并适用于 NetScaler 支持的每个逻辑模块。

注意：

建议您使用高级策略来创建策略。

为何从经典策略迁移到高级策略?

高级策略具有丰富的表达式集，并且比经典策略提供了更大的灵活性。随着 NetScaler 的扩展并满足各种客户端的需求，支持远远超出高级策略的表达式势在必行。有关详细信息，请参阅策略和表达式。

以下是高级策略新增的功能。

- 能够访问消息正文。
- 支持许多其他协议。
- 访问系统的许多其他功能。
- 具有更多基本函数、运算符和数据类型。
- 支持解析 HTML、JSON 和 XML 文件。
- 支持快速并行多字符串匹配 (`patsets` 等)。

现在可以使用高级策略配置以下 VPN 策略。

- 会话策略
- 授权策略
- 流量策略
- 隧道策略
- 审计策略

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

此外，可以将端点分析 (EPA) 配置为身份验证功能的 nFactor。EPA 用作尝试连接到 Gateway 设备的端点设备的看门人。在 Gateway 登录页面显示在端点设备上之前，会根据 Gateway 管理员配置的资格标准检查设备是否满足最低硬件和软件要求。根据执行检查的结果授予对 Gateway 的访问权限。以前，EPA 是作为会话策略的一部分进行配置的。现在，它可以链接到 nFactor，从而在执行时间上提供更大的灵活性。有关 EPA 的更多信息，请参阅 端点策略的工作原理 主题。有关 nFactor 的更多信息，请参阅 nFactor 身份验证 主题。

用例：

使用高级 EPA 的预身份验证 EPA

预身份验证 EPA 扫描在用户提供登录凭据之前进行。

使用高级 EPA 的身份验证后 EPA

身份验证后 EPA 扫描在用户凭据验证后进行。在经典策略基础架构下，身份验证后 EPA 是作为会话策略或会话操作的一部分进行配置的。在高级策略基础架构下，EPA 扫描将配置为 nFactor 身份验证中的 EPA 因素。有关更多信息，请参阅 将 EPA 扫描作为 nFactor 身份验证中的一个因素。

使用高级策略的预身份验证和身份验证后 EPA

EPA 可以在身份验证之前和身份验证之后执行。

作为 nFactor 身份验证中一个因素的定期 EPA 扫描

在经典策略基础架构下，定期 EPA 扫描是作为会话策略操作的一部分进行配置的。在高级策略基础架构下，它可以配置为 nFactor 身份验证中 EPA 因素的一部分。

有关将定期 EPA 扫描配置为 nFactor 身份验证中的一个因素的更多信息，请参阅 将定期端点分析扫描配置为 nFactor 身份验证中的一个因素。

故障排除：

故障排除时应牢记以下几点。

- 相同类型的经典策略和高级策略（例如，会话策略）不能绑定到同一实体/绑定点。
- 对于所有 PI 策略，优先级是强制性的。
- VPN 的高级策略可以绑定到所有绑定点。
- 具有相同优先级的高级策略可以绑定到单个绑定点。
- 如果没有选择任何已配置的授权策略，则应用在 VPN 参数中配置的全局授权操作。

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

- 在授权策略中，如果授权规则失败，授权操作不会被撤销。

常用高级策略等效表达式（用于经典策略）：

经典策略表达式	高级策略表达式
ns_true	是
ns_false	否
REQ.HTTP	HTTP.REQ
RES.HTTP	HTTP.RES
标头 "foo"	HEADER("foo")
CONTAINS "bar"	.CONTAINS("bar") [Note use of “..”]
REQ.IP	CLIENT.IP
RES.IP	SERVER.IP
SOURCEIP	SRC
DESTIP	目标
请求.TCP	客户端.TCP
响应.TCP	服务器.TCP
源端口	源端口
目标端口	目标端口
状态码	状态
请求.SSL.客户端.证书	客户端.SSL.客户端_证书

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

NetScaler Gateway 上的 SSL 支持

SSL 加密是 NetScaler Gateway 中的一项关键安全功能，可确保客户端与公司网络之间的安全通信。NetScaler Gateway 上的 SSL 支持提供以下优势：

- **数据隐私：** SSL 加密客户端与 NetScaler Gateway 之间传输的数据，使其对任何拦截者都不可读。此加密可确保登录凭据、个人详细信息和财务数据等敏感信息保持机密。
- **数据完整性：** SSL 确保发送和接收的数据在传输过程中不会被更改。这可以防止数据篡改，并确保客户端收到的信息与服务器发送的信息完全一致。
- **身份验证：** SSL 证书验证 NetScaler Gateway 的身份，确保用户正在与合法的网关通信，而不是冒名顶替者。这有助于防止网络钓鱼攻击并建立用户信任。
- **合规性：** 许多监管框架和标准（例如 GDPR、PCI DSS 和 HIPAA）都要求使用 SSL 加密来保护敏感数据。在 NetScaler Gateway 中实施 SSL 有助于组织遵守这些法规。

在 NetScaler Gateway 上启用 TLS 1.3 协议

NetScaler Gateway 14.1 build 43.50 及更高版本引入了对最新安全标准 TLS 1.3 协议的支持，以保护 NetScaler Gateway 和 VDA 之间的连接。

注意：

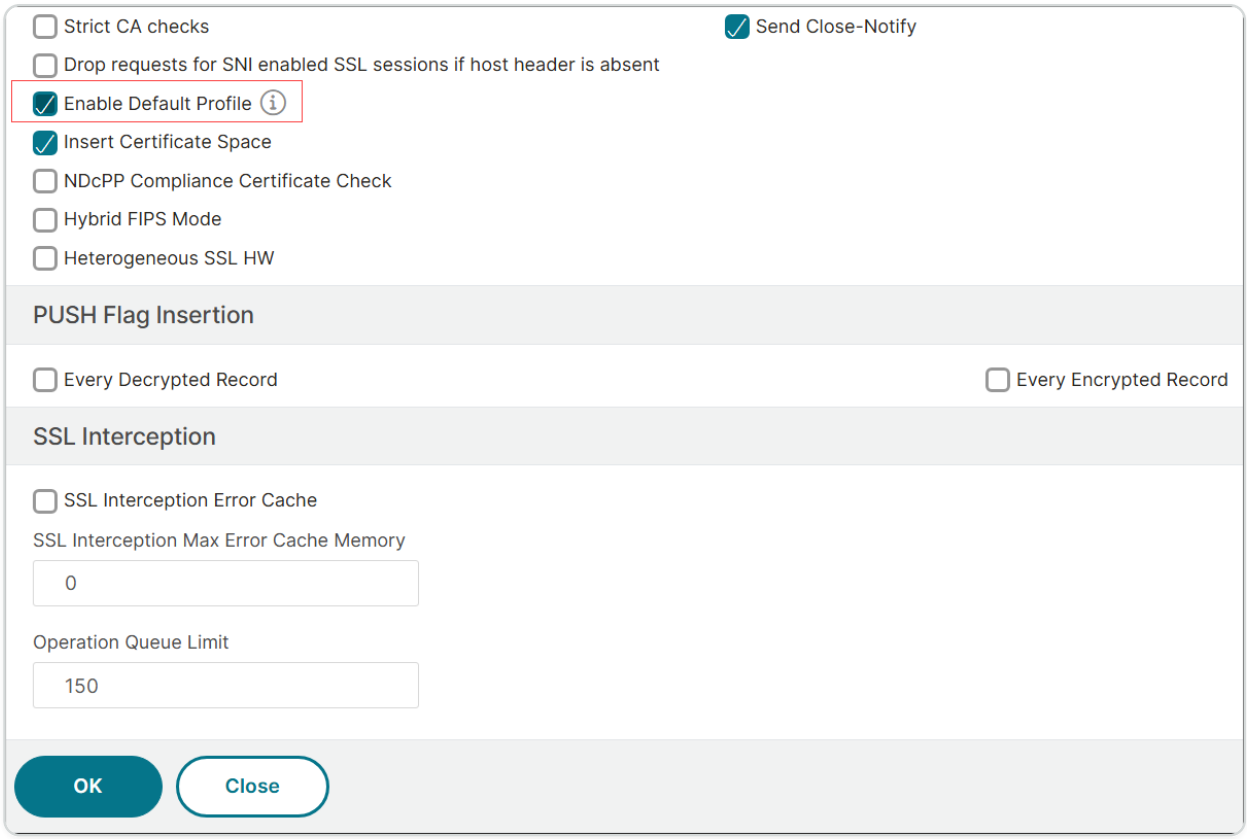
- 如果 TLS 1.3 协议失败，NetScaler Gateway 会尝试使用下一个可用的最高版本。
- TLS 1.3 可以独立用于保护 NetScaler Gateway 和 VDA 之间的后端连接。我们建议您也将 TLS 1.3 用于前端连接。
- 使用默认后端配置文件 (ns_default_ssl_profile_backend) 在后端连接上启用 TLS 1.3。使用默认前端配置文件 (ns_default_ssl_profile_frontend) 或自定义配置文件在前端连接上启用 TLS 1.3。有关更多信息，请参阅使用 GUI 设置 SSL 配置文件参数。
- 默认前端和默认后端 SSL 配置文件包含所有默认密码和 ECC 曲线，以及旧配置文件中的设置。启用默认配置文件操作会自动将默认前端配置文件绑定到所有前端实体，并将默认后端配置文件绑定到所有后端实体。您可以修改默认配置文件以适应您的部署。您还可以创建自定义配置文件并将其绑定到 SSL 实体。在启用默认配置文件之前，请参阅启用默认配置文件 以了解此操作的影响。

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

使用 GUI 启用 TLS 1.3 协议

执行以下步骤，使用 GUI 在 NetScaler Gateway 上启用 TLS 1.3 协议。

1. 导航到 **流量管理** > **SSL** > **设置** > **更改高级 SSL 设置**，选择 **启用默认配置文件**，然后单击 **确定**。



2. 导航到 **系统** > **配置文件** > **SSL 配置文件**。
3. 选择 **ns_default_ssl_profile_backend**，然后单击编辑图标以编辑后端配置文件。
4. 在 **协议** 下，选择 **TLSv13**，然后单击 **确定**。
5. 要为前端连接启用 TLS 1.3 协议，请修改默认配置文件 **ns_default_ssl_profile_frontend** 或编辑现有 SSL 配置文件。
6. 在“**协议**”下，选择“**TLSv13**”，然后单击“**确定**”。

   启用 TLS 1.3(/en-us/netscaler-gateway/media/nsg-tls-1-3.png)

使用 CLI 启用 TLS 1.3 协议

要在默认前端和后端配置文件上启用 TLS 1.3 协议，请在命令提示符下键入：

```
set ssl parameter -defaultProfile enaBLED

set ssl profile ns_default_ssl_profile_frontend -tls13 enaBLED
```

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

```
set ssl profile ns_default_ssl_profile_backend -tls13 enaBLED
```

要创建新的前端配置文件并启用 TLS 1.3 协议，请在命令提示符下键入：

```
add ssl profile <new SSL profile> -sslProfileType FrontEnd

set ssl profile <name> -tls13 ENABLED
```

兼容性矩阵

对于后端连接

下表提供了支持 TLS 1.3 以及支持 HDX Insight 的 TLS 1.3 的 VDA 平台的兼容性矩阵，确保 NetScaler Gateway 和 VDA 之间安全的端到端连接。

支持的平台	TLS 1.3	带有 HDX INSIGHT 的 TLS 1.3
视窗	2407 及更高版本	2503 及更高版本
利努克斯	2411 及更高版本	2411 及更高版本
macOS	2507 及更高版本	2507 及更高版本

从 NetScaler Gateway 14.1 版本 build 56.x 开始，适用于 macOS 的 VDA 支持 TLS 1.3 以及带有 HDX Insight 的 TLS 1.3，前提是已在 Delivery Controller 或 Citrix Studio 上配置了 Secure HDX。有关配置 Secure HDX 的详细信息，请参阅 Secure HDX™。

对于前端连接

有关支持 TLS 1.3 的 Citrix Workspace 应用程序版本，请参阅 Citrix Workspace 应用程序功能矩阵 - 安全性。TLS 1.3 加密可确保 NetScaler Gateway 和 Citrix Workspace 应用程序之间安全的端到端连接。

限制

- 在 NetScaler Gateway 13.1 及更早版本中，NetScaler Gateway 到 VDA 的后端连接不支持 TLS 1.3 协议。
- TLS 1.3 协议仅在 VDA 2503 及更高版本的 Windows 和 Linux 平台上受支持。
- NetScaler FIPS 设备不支持 TLS 1.3。

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

- TLS 1.3 握手仅支持具有 1024 位及更大密钥的 RSA 证书。

验证 TLS 1.3 加密状态

后端连接

对于后端连接，使用以下命令检查 TLS 1.3 加密状态：

```
ctxsession -v
```

排除后端连接故障(/en-us/netscaler-gateway/media/tls-1-3-backend.png)

前端连接

对于前端连接，请在连接中心（适用于 Windows 和 Linux）或 Citrix Viewer（适用于 macOS）中验证 TLS 1.3 加密状态。

排除前端连接故障(/en-us/netscaler-gateway/media/tls-1-3-frontend.png)

适用于 Windows 的 Citrix Workspace™ 应用程序

1. 右键单击通知区域中的 Citrix Workspace 应用程序图标。
2. 导航到 **连接中心** > **首选项**。
3. 在出现的 **客户端连接状态** 屏幕中验证加密状态。

CWA Windows 中的连接中心(/en-us/netscaler-gateway/media/connection-center-windows.png)

适用于 Linux 的 Citrix Workspace 应用程序

1. 在 Citrix Workspace 应用程序中导航到 **菜单 > 连接中心**。活动会话将列在 **连接中心** 中。
2. 选择所需的会话并在出现的 **服务器属性** 屏幕中验证加密状态。

CWA Linux 中的连接中心(/en-us/netscaler-gateway/media/connection-center-linux.png)

适用于 macOS 的 Citrix Workspace 应用程序

1. 导航到 **Citrix Viewer > 关于 Citrix Viewer**。
2. 验证出现的 **Citrix Viewer** 屏幕中的加密状态。

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

参考资料

有关 TLS 1.3 协议的更多信息，请参阅 支持 TLS 1.3 协议。

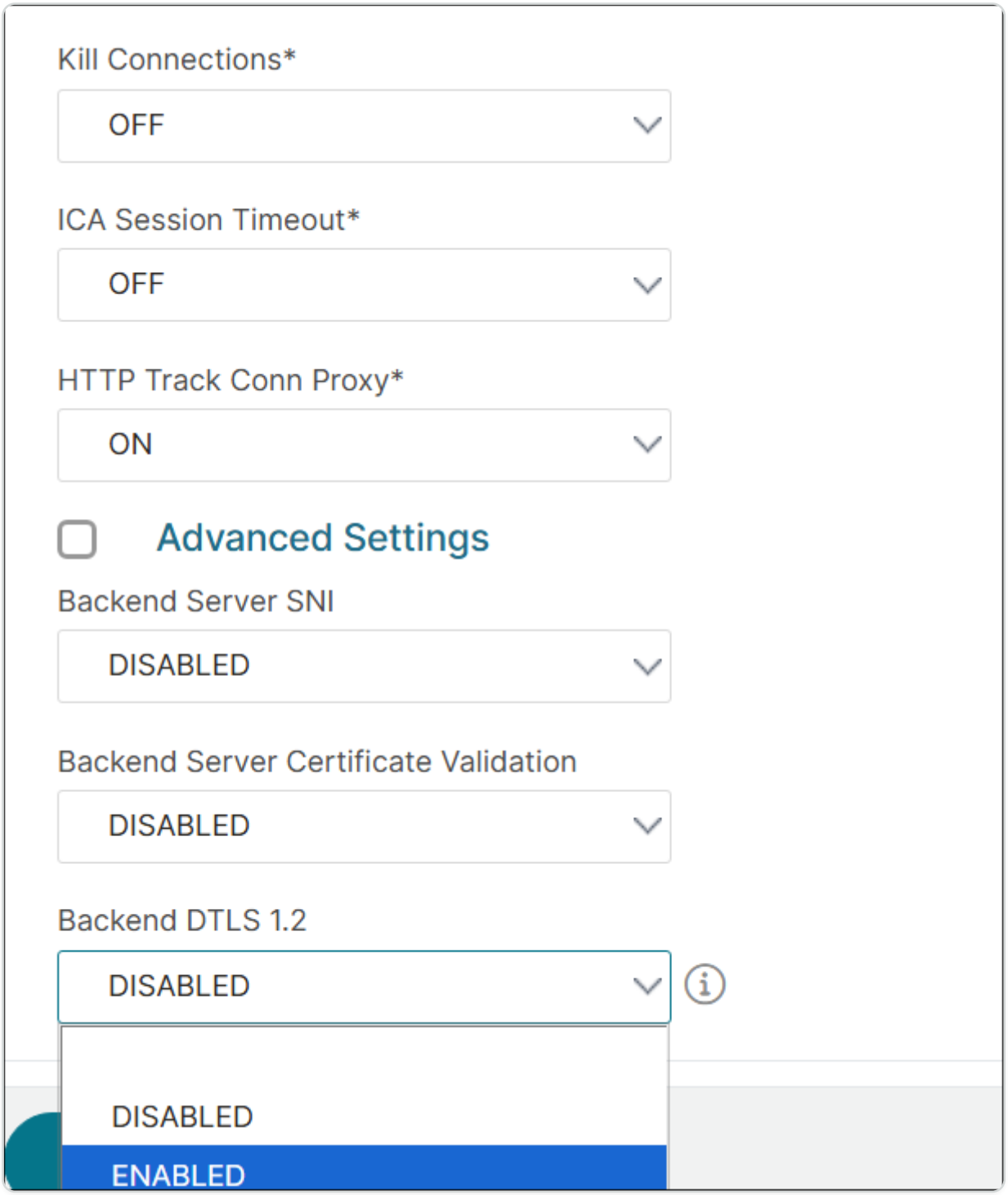
在 NetScaler Gateway 上启用 DTLS 1.2 协议

NetScaler Gateway 现在支持最新的安全标准 DTLS 1.2 协议，以提高后端连接的安全性和保护。从版本 14.1 build 47.46 开始，您可以配置 NetScaler Gateway 使用 DTLS 1.2 来保护 NetScaler Gateway 和 VDA 之间的连接。

使用 GUI 配置 DTLS 1.2

1. 导航到 **NetScaler Gateway** -> **全局设置** -> **更改全局设置**。
2. 在“**全局 NetScaler Gateway 设置**”页面上，在“**后端 DTLS 1.2**”菜单中选择“**已启用**”，然后单击“**确定**”。

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



使用 CLI 配置 DTLS 1.2

要为后端连接启用 DTLS 1.2，请在命令提示符下键入：

```
set vpn parameter -backenddtls12 ENABLED
```

要为后端连接禁用 DTLS 1.2，请在命令提示符下键入：

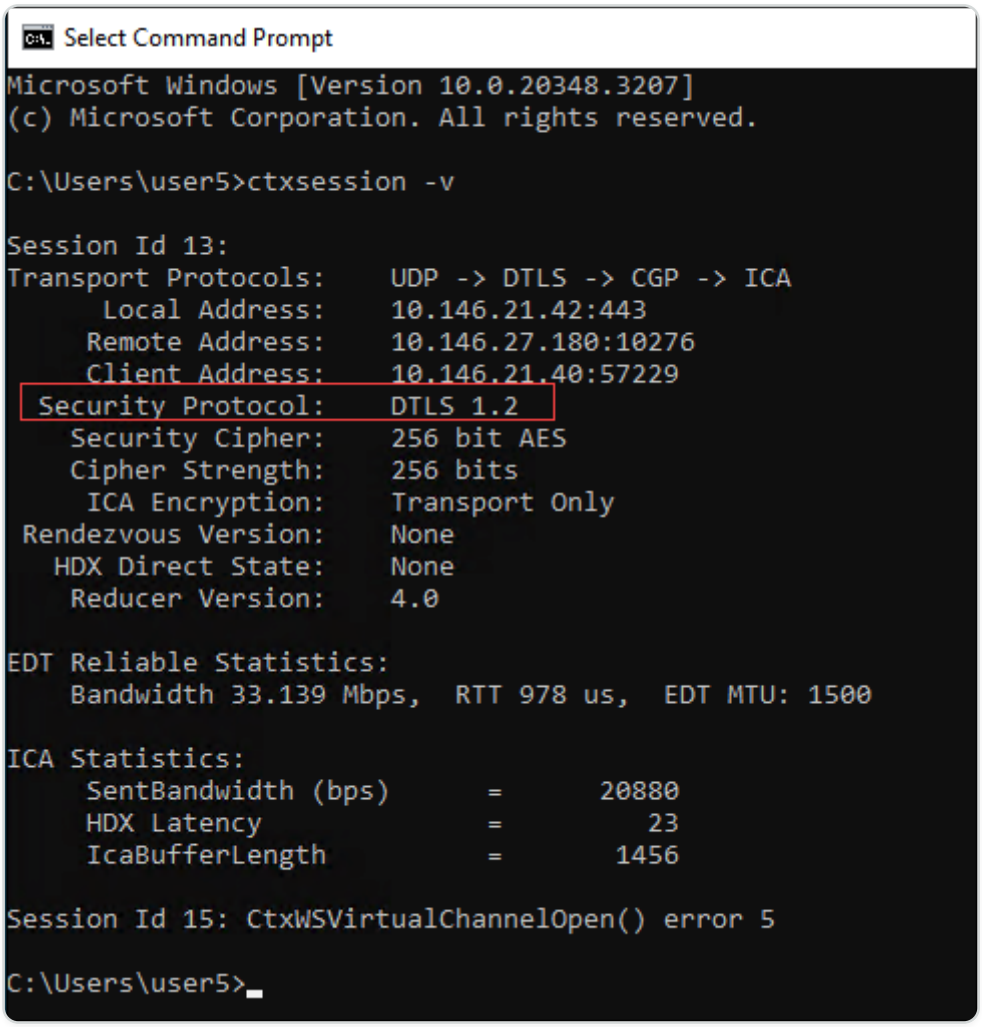
© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
set vpn parameter -backenddtls12 DISABLED

unset vpn parameter -backendDtls12
```

验证 DTLS 1.2 加密状态

使用以下命令检查 DTLS 1.2 加密的状态：

```
sh vpn parameter - Backend DTLS 1.2: DISABLED
```



兼容性矩阵

下表提供了支持 DTLS 1.2 以及支持 DTLS 1.2 和 HDX Insight 的 VDA 平台的兼容性矩阵，可确保 NetScaler Gateway 和 VDA 之间安全的端到端连接。

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

支持的平台	DTLS 1.2	带 HDX INSIGHT 的 DTLS 1.2
视窗	2407 及更高版本	2503 及更高版本
琳琅克斯	2411 及更高版本	2411 及更高版本
macOS	2507 及更高版本	2507 及更高版本

从 NetScaler Gateway 14.1 版本 build 56.x 开始，适用于 macOS 的 VDA 支持 DTLS 1.2 和带 HDX Insight 的 DTLS 1.2，前提是在 Delivery Controller 或 Citrix Studio 上配置了 Secure HDX。有关配置 Secure HDX 的详细信息，请参阅 Secure HDX™。

限制

双跳拓扑不支持 DTLS 1.2。

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

使用 SSL VPN 虚拟服务器配置 DTLS VPN 虚拟服务器

您可以为 NetScaler Gateway 配置 DTLS VPN 虚拟服务器，使用已配置的 SSL VPN 虚拟服务器的相同 IP 地址和端口号。配置 DTLS VPN 虚拟服务器使您能够将高级 DTLS 密码和证书绑定到 DTLS 流量，以增强安全性。

重要提示：

- 默认情况下，现有 SSL VPN 虚拟服务器的 DTLS 功能已设置为“开”。在创建 DTLS VPN 虚拟服务器之前，请禁用该服务器的功能。
- NetScaler Gateway 13.0 版本 64.x 及更高版本支持 DTLS 网关虚拟服务器的 SNI。
- 从 NetScaler 13.0 版本 79.x 开始，`helloverifyrequest` 参数默认启用。在 DTLS 配置文件上启用 `helloverifyrequest` 参数有助于降低攻击者或机器人使网络吞吐量过载的风险，这可能导致出站带宽耗尽。也就是说，它有助于缓解 DTLS DDoS 放大攻击。有关 `helloverifyrequest` 参数的详细信息，请参阅 DTLS 配置文件。
- 处理 UDP 流量时，如果后端服务器推送大量流量，NetScaler 设备内存消耗会增加。因此，由于客户端的 TCP MUX 连接，NetScaler 设备无法将此流量推送到客户端。在这种情况下，Citrix 建议您使用 DTLS 协议。

注意事项

- NetScaler Gateway 设备上的 DTLS VPN 虚拟服务器可从 13.0 版本 58.x 开始配置。
- 在 NetScaler Gateway 设备上配置 DTLS VPN 虚拟服务器之前，您必须已在该设备上配置 SSL VPN 虚拟服务器。
- DTLS VPN 虚拟服务器使用已配置的 SSL VPN 虚拟服务器的 IP 地址和端口号。
- 如果 DTLS 握手失败，连接将回退到 TLS。
- 若要仅使用 DTLS，您可以通过仅将 DTLS 密码绑定到 DTLS 流量来禁用 TLS。
- 当 TCP 流量通过 VPN 隧道传输时，DTLS 多路复用不受支持。

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

使用 GUI 配置 DTLS VPN 虚拟服务器

1. 在“配置”选项卡上，导航到 **NetScaler Gateway > 虚拟服务器**。
2. 在“**NetScaler Gateway 虚拟服务器**”页面上，选择现有的 SSL VPN 虚拟服务器，然后单击“**编辑**”。
3. 在“**VPN 虚拟服务器**”页面上，单击编辑图标，清除“**DTLS**”复选框，然后单击“**确定**”。
4. 导航回 **NetScaler Gateway > 虚拟服务器**，然后单击“**添加**”。
5. 在“**基本设置**”下，输入以下字段的值，然后单击“**确定**”。
   - 名称 - DTLS VPN 虚拟服务器的名称
   - 协议 - 选择 DTLS
   - IP 地址 – 输入 SSL VPN 虚拟服务器 IP 地址
   - 端口 – 输入 SSL VPN 虚拟服务器端口号
6. 在“**NetScaler® Gateway 虚拟服务器**”页面上，选择您之前添加的虚拟服务器，然后单击“**编辑**”。
7. 在“**证书**”下，单击箭头图标以选择所需的证书密钥。
8. 在“**服务器证书绑定 > 选择服务器证书**”中，选择现有 SSL 证书密钥或创建一个。
9. 在“**服务器证书绑定**”页面上，单击“**绑定**”。

注意：

- 要使用 DTLS 1.2，请单击“SSL 参数”下的编辑图标，并选择“**DTLS 1.2**”复选框。
- DTLS 类型的 VPN 虚拟服务器支持服务器名称指示 (SNI)。

使用 CLI 配置 DTLS VPN 虚拟服务器

在命令提示符下，键入以下命令集：

```
set vpn vserver <ssl vpnvserver name> -dtls off

add vpn vserver <dtls vpnvserver name> dtls <ssl vpn vserver IP> <ssl vpn
vserver port>
```

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

```
bind ssl vservser <dtls vpnvserver name> -certkeyName <existing ssl cert
key or newly created cert key>
```

DTLS 1.0 照常工作，要使用 DTLS 1.2，请键入以下命令：

```
set ssl vserver < dtls vpnvserver name > -dtls12 ENABLED
```

示例

```
set vpn vserver vpnvserver  -dtls off

add vpn vserver vpnvserver_dtls dtls 10.108.45.220 443

bind ssl vservser vpnvserver_dtls -certkeyName sslcertkey

set ssl vserver vpnvserver_dtls -dtls12 ENABLED
```

要为 DTLS 类型 VPN 虚拟服务器启用 SNI，请键入以下命令：

```
set ssl vserver <vServerName>@ [-SNIEnable ( ENABLED | DISABLED )

bind ssl vservser <dtls vpnvserver name> -certkeyName <existing ssl cert
key or newly created cert key> <-SNICert>
```

示例

```
set ssl vserver _XD_10.106.40.225_443_DTLS -sniEnable eNABLED

bind ssl vserver _XD_10.106.40.225_443_DTLS -certkeyName "Insight/
*.insight.net.cer_CERT_" -snICert
```

支持的 DTLS VPN 虚拟服务器参数

DTLS 类型的 VPN 虚拟服务器仅支持以下参数。

- IP 地址
- 端口

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

- 状态
- 双跳
- 下行状态清除
- 注释
- Appflow日志
- ICMP VSR响应

不支持的 DTLS VPN 虚拟服务器参数

类型为 DTLS 的 VPN 虚拟服务器不支持以下参数。

- LinuxEPAPluginUpgrade
- WindowsEPAPluginUpgrade
- maxAAAUsers
- icaProxySessionMigration
- loginOnce
- cginfraHomePageRedirect
- logoutOnSmartcardRemoval
- L2连接
- MacEPAPluginUpgradeRHIstate
- icaOnly
- maxLoginAttempts
- 登录失败超时
- 虚拟服务器完全限定域名
- 设备证书
- RDP服务器配置文件名
- PCoIP虚拟服务器配置文件名
- TCP配置文件名
- 网络配置文件
- 身份验证配置文件
- 侦听优先级
- 侦听策略

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

- IP集
- 证书密钥名称

使用 XenApp 和 XenDesktop® 向导配置 DTLS 虚拟服务器

1. 在**与 Citrix® 产品集成**下，单击**XenApp® 和 XenDesktop**。
2. 在 XenApp 和 XenDesktop 设置向导上，选择**StoreFront™**，然后单击**继续**。
3. 在 **NetScaler Gateway 设置** 页面上，启用 **为此 VPN 虚拟服务器配置 DTLS 侦听器** 复选框，然后单击 **继续**。

   DTLS 侦听器现已配置。
4. 在服务器证书中，单击 **选择文件** 以选择服务器证书，然后单击 **继续**。
5. 指定证书文件和密钥文件名，然后单击 **继续**。
6. 在 **StoreFront** 部分下，按照以下说明提供所需参数的值，然后单击 **继续**。
7. 在 **身份验证** 部分下，按照以下说明提供所需参数的值，然后单击 **测试连接**。

   确保服务器可访问，提供超时值和服务器登录名属性，然后单击 **继续**。

   指定配置值(/en-us/netscaler-gateway/media/dtls-xaxd-server-state.png)
8. 单击 **完成** 以完成配置。

   配置完成(/en-us/netscaler-gateway/media/dtls-xaxd-done.png)

限制

- DTLS 1.2 仅在 Windows、macOS 和 iOS 客户端上受支持。
- 带有 DTLS 的 VPN 虚拟服务器不支持 IPv6 地址。
- DTLS VPN 虚拟服务器不支持 SSL 策略和 SSL 配置文件。此外，也不支持 VPN 虚拟服务器策略的绑定。
- NetScaler Gateway DTLS VPN 虚拟服务器不支持以下功能。但是，NetScaler Gateway SSL VPN 虚拟服务器支持这些功能：
  - 带内容交换虚拟服务器的统一网关
  - UDP MUX
  - UDP 视频
  - UDP 音频

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

  - PCOIP

- 与 DTLS VPN 虚拟服务器统计信息相关的 `stat vpn vserver` 命令不受支持。
- DTLS 虚拟服务器不支持 HSM 密钥。
- 不支持集群配置。

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

与 Citrix® 产品集成

如果您是负责安装和配置 NetScaler Gateway 的系统管理员，您可以将设备配置为与 StoreFront 和 StoreFront Cloud 集成。本节包含以下主题：

- 将 NetScaler Gateway 与 StoreFront 集成：配置 NetScaler Gateway 以代理 StoreFront 商店 UI 并对用户进行身份验证，以便用户可以通过 Web 浏览器或 Citrix Workspace 应用程序访问已发布的应用程序和虚拟桌面。
- 仅将 NetScaler Gateway 与 StoreFront 和 StoreFront Cloud 集成用于 HDX 路由：配置 NetScaler Gateway 以仅代理虚拟应用程序和桌面的 HDX (ICA) 连接。这可用于 StoreFront 或 StoreFront Cloud，在这些情况下无需代理商店 UI 或对用户进行身份验证。
- 配置 SmartControl：配置策略以控制用户在 Citrix Virtual Apps and Desktops 会话期间对剪贴板访问、打印和文件传输等功能的访问。

将 NetScaler Gateway 与 StoreFront 集成

本文介绍如何为使用 Citrix Workspace 应用程序或 Web 浏览器的用户创建 NetScaler Gateway 虚拟服务器，以便远程访问 StoreFront。

StoreFront 设置(/en-us/netscaler-gateway/media/1-configure-gateway-session-policies-for-storefront.png)

用户通过 Web 浏览器或 Citrix Workspace 应用程序连接到 NetScaler Gateway。NetScaler Gateway 根据配置的策略对用户进行身份验证。如果身份验证成功，NetScaler Gateway 将使用户能够单点登录到商店，并将 StoreFront 商店代理给用户。

重要提示：

建议您不要使用 Citrix Virtual Apps and Desktops 向导将 NetScaler Gateway 与 StoreFront 集成，因为它会使用经典身份验证策略（已弃用）创建无效配置。

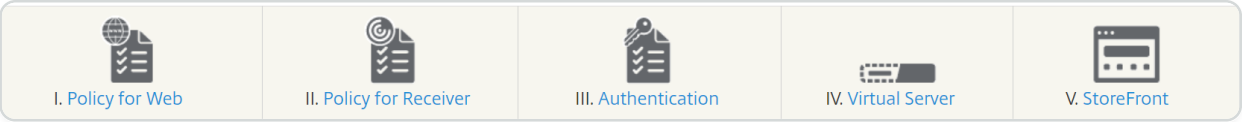
配置 NetScaler Gateway 以与 StoreFront 配合使用

要将 NetScaler Gateway 与 StoreFront 集成，请完成以下步骤：

1. 为基于 Web 浏览器的访问创建会话策略

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

2. 为基于 Citrix Workspace 应用程序的访问创建会话策略
3. 创建身份验证配置文件
4. 创建 NetScaler Gateway 虚拟服务器
5. 在 StoreFront 上添加 NetScaler Gateway 实例

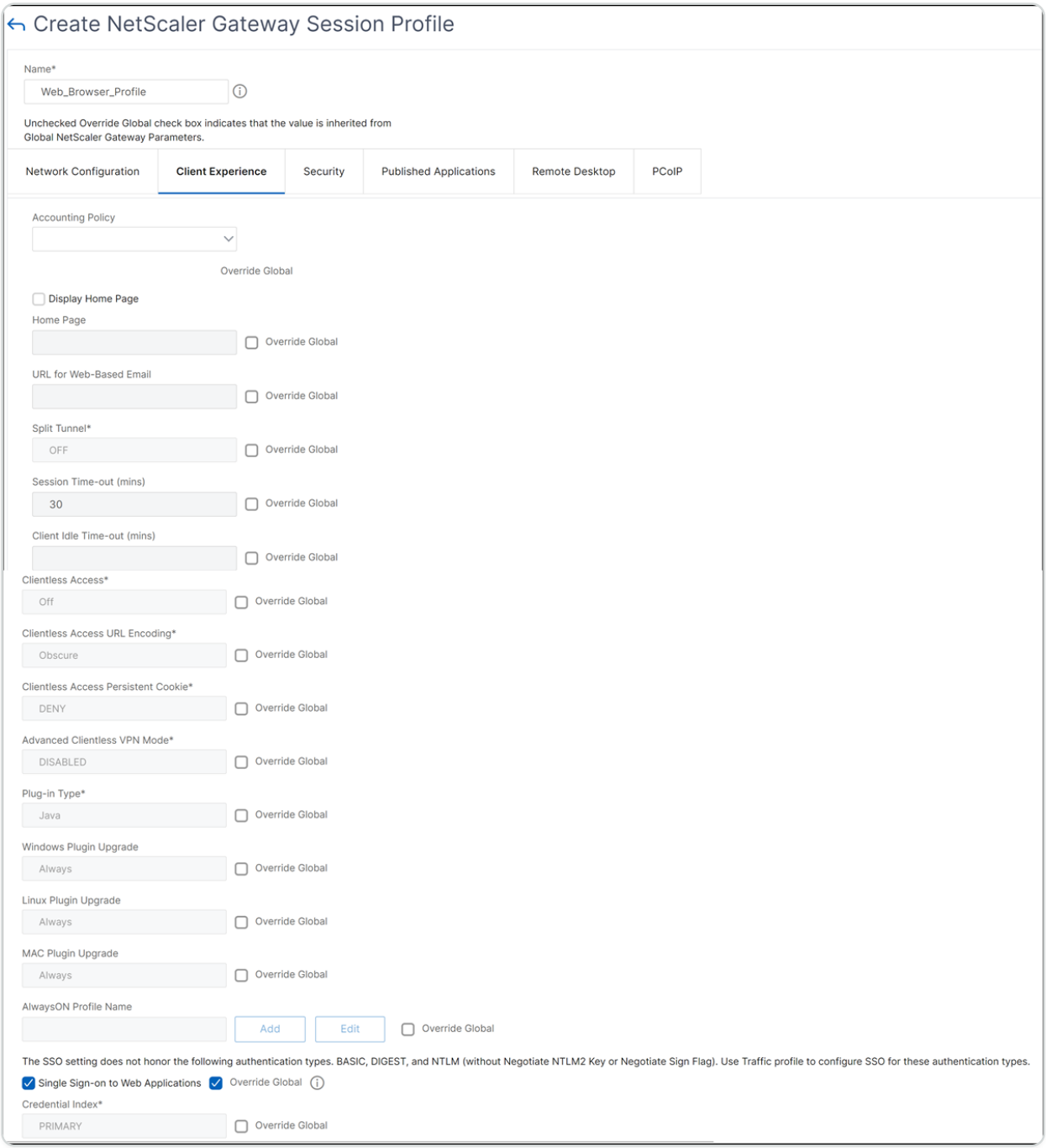


1. 为基于 Web 浏览器的访问创建会话策略

1. 导航到 **配置 > NetScaler Gateway > 策略 > 会话**。
2. 在 **会话配置文件** 选项卡中，单击 **添加**。
3. 为会话配置文件分配一个名称。
4. 在 **客户端体验** 选项卡中，配置以下设置：

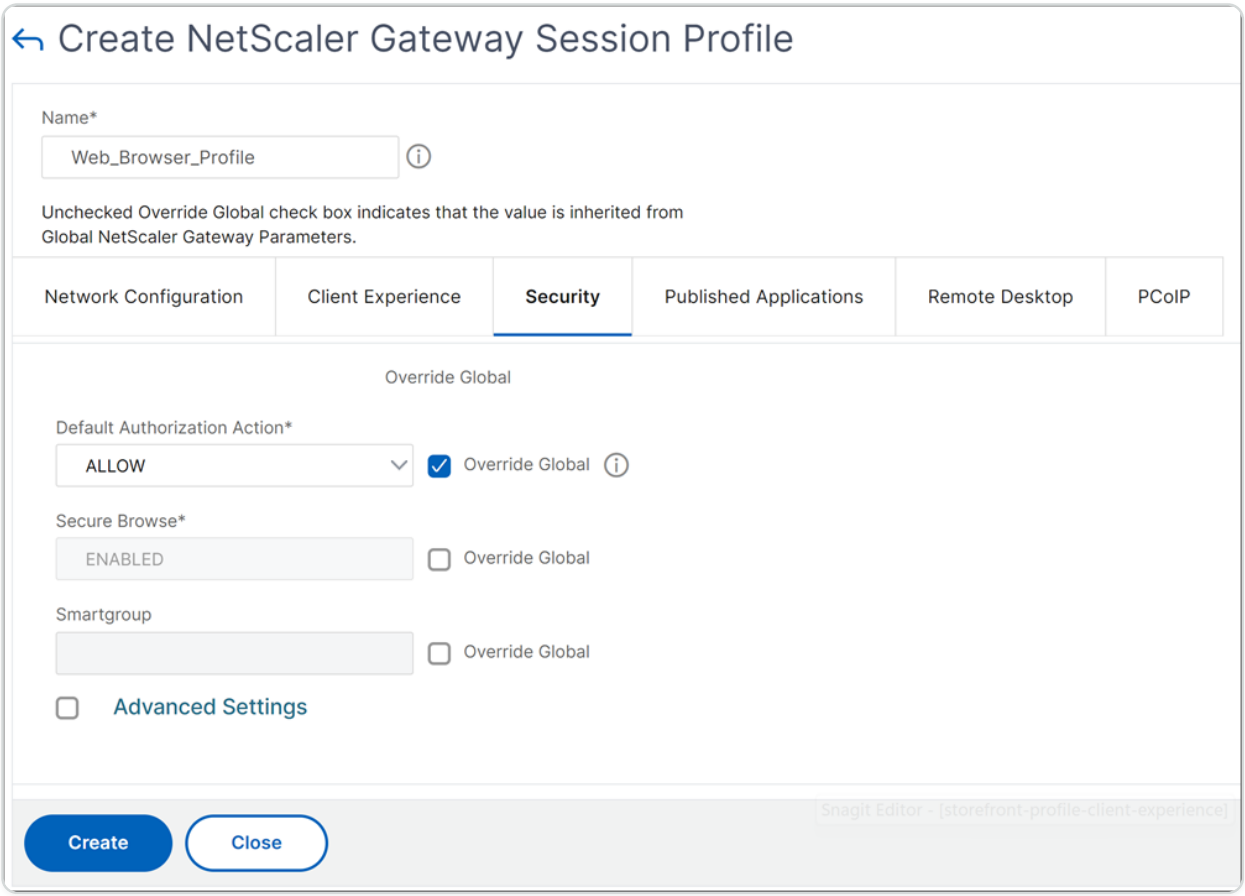
   - **会话超时（分钟）**：将其设置为所需的非活动超时。此设置应与 StoreFront 中为应用商店网站配置的 Web 非活动超时相同或更低。建议您选择 **覆盖全局**，即使您打算使用全局会话超时设置。未能明确覆盖此设置，即使使用默认的 30 分钟超时，也可能导致身份验证循环并强制用户重新登录。
   - **插件类型**：要禁用 Secure Access 客户端（建立完整 VPN 所必需）的使用，请将其设置为 **Java**。如果要允许完整 VPN，请参阅 在 NetScaler Gateway 上设置完整 VPN。
   - **Web 应用程序单点登录**：选择此选项后，当用户登录 NetScaler Gateway 时，它会将凭据转发到 StoreFront 网站。此设置可避免用户两次输入其凭据。但是，您还必须在 StoreFront 上启用 从 NetScaler Gateway 直通 身份验证方法。如果您要求用户使用不同的凭据登录 NetScaler Gateway 和 StoreFront 应用商店，请禁用此选项。

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



5. 在 **安全** 选项卡中，启用 **默认授权操作** 并将其设置为 **允许**。

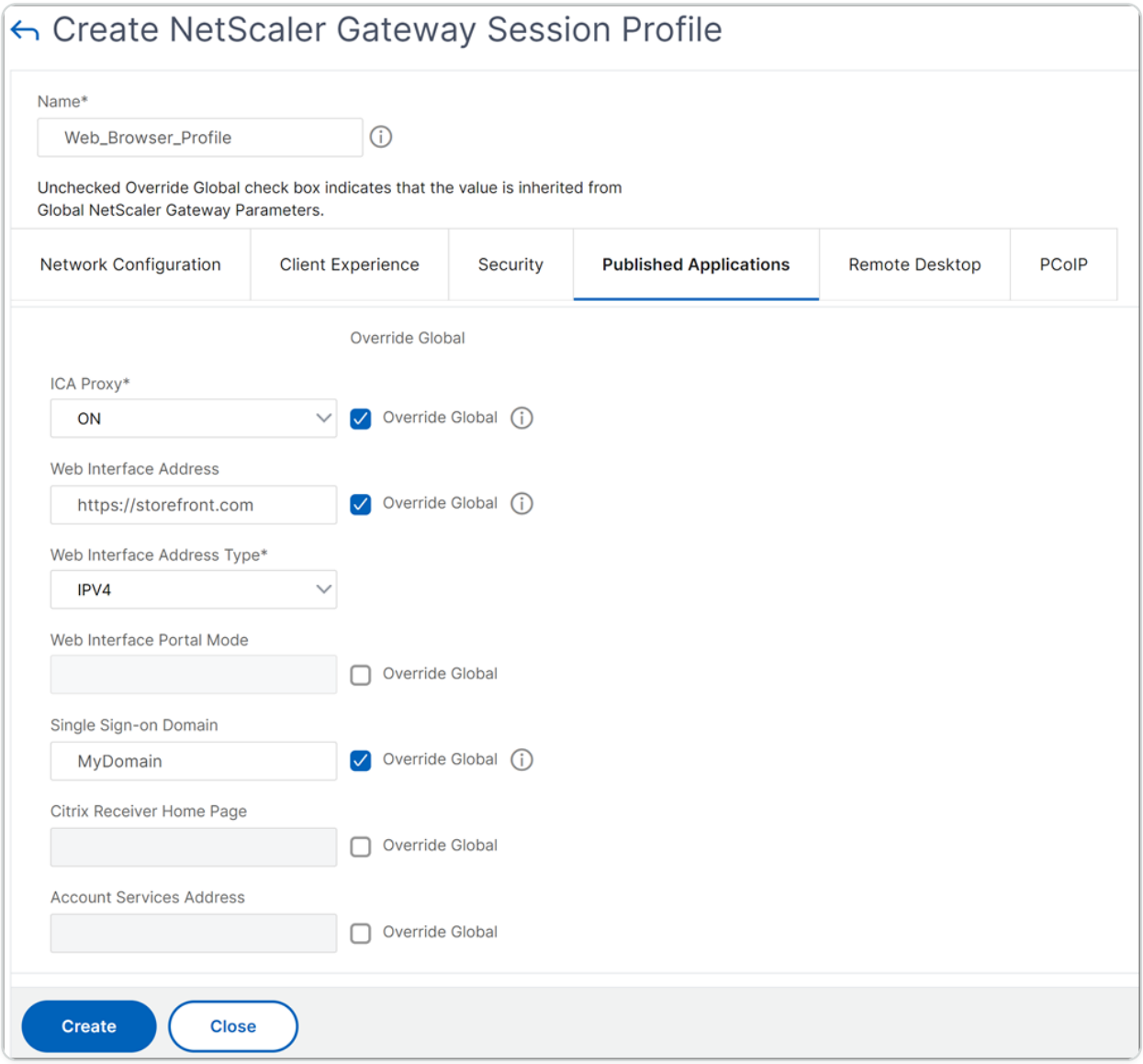
© 1997–2026 Citrix Systems, Inc. All rights reserved.



6. 在 **已发布的应用程序** 选项卡中，配置以下设置：

   - **ICA 代理**：设置为 ON。
   - **Web 界面地址**：StoreFront™ 服务器的 FQDN，后跟应用商店网站的路径。
   - **单点登录域**：如果您只使用一个域，可以选择输入该域的 NetBIOS 名称。

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

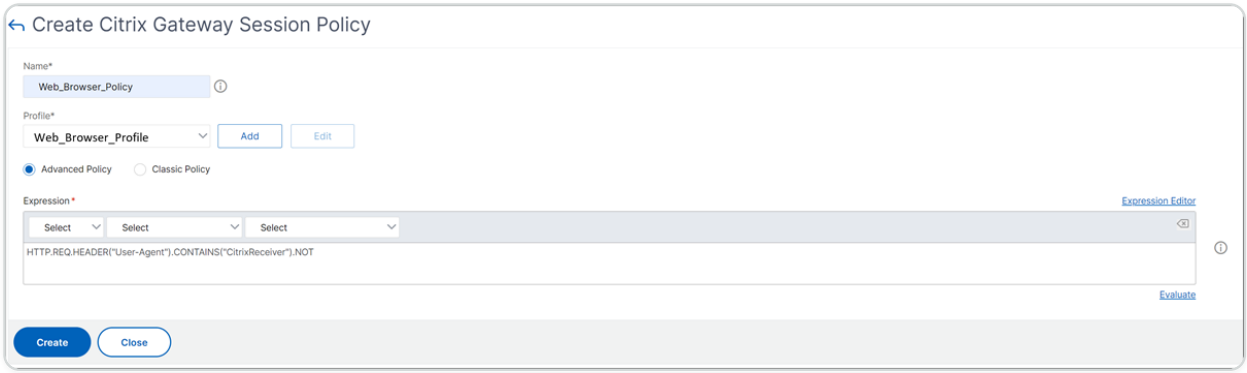


7. 点击**创建**。
8. 在**会话策略**选项卡中，点击**添加**。NetScaler 需要会话策略来区分基于 Web 浏览器和基于 Citrix Workspace 应用程序的连接。此策略应用于基于 Web 浏览器的连接。
9. 在**名称**中，为会话策略分配一个名称。
10. 在**配置文件**中，选择您创建的会话配置文件。
11. 点击**高级策略**选项，并在**表达式**下输入以下语法：

    `HTTP.REQ.HEADER("User-Agent").CONTAINS("CitrixReceiver").NOT`

12. 点击**创建**。

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



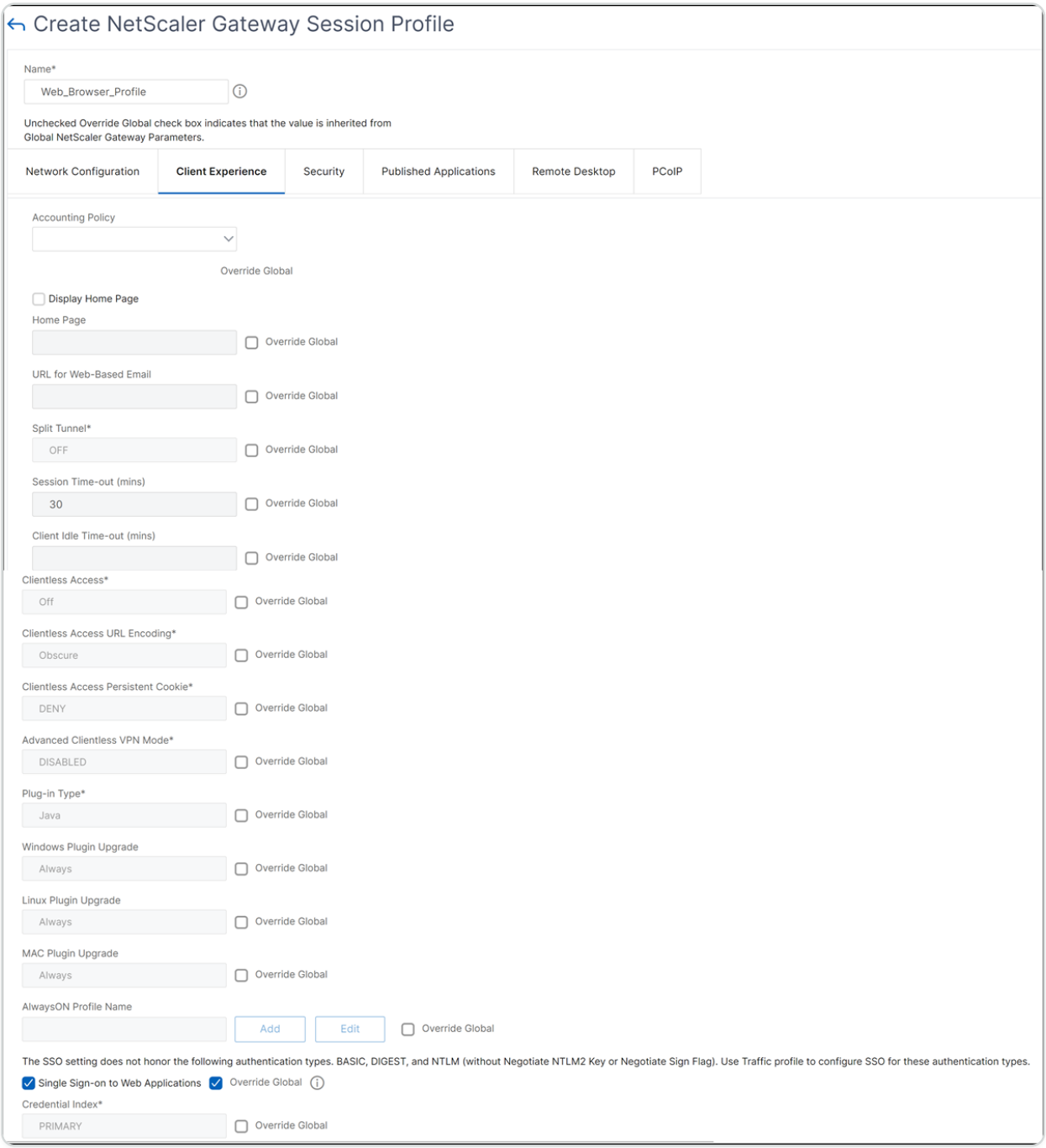
有关 NetScaler Gateway 会话策略的更多详细信息，请参阅会话策略。

2. 为基于 Citrix Workspace™ 应用程序的访问创建会话策略

1. 导航到**配置 > NetScaler Gateway > 策略 > 会话**。
2. 在**会话配置文件**选项卡中，点击**添加**。
3. 为 Citrix Workspace 应用程序的会话配置文件分配一个名称。
4. 在**客户端体验**选项卡中，启用以下设置：

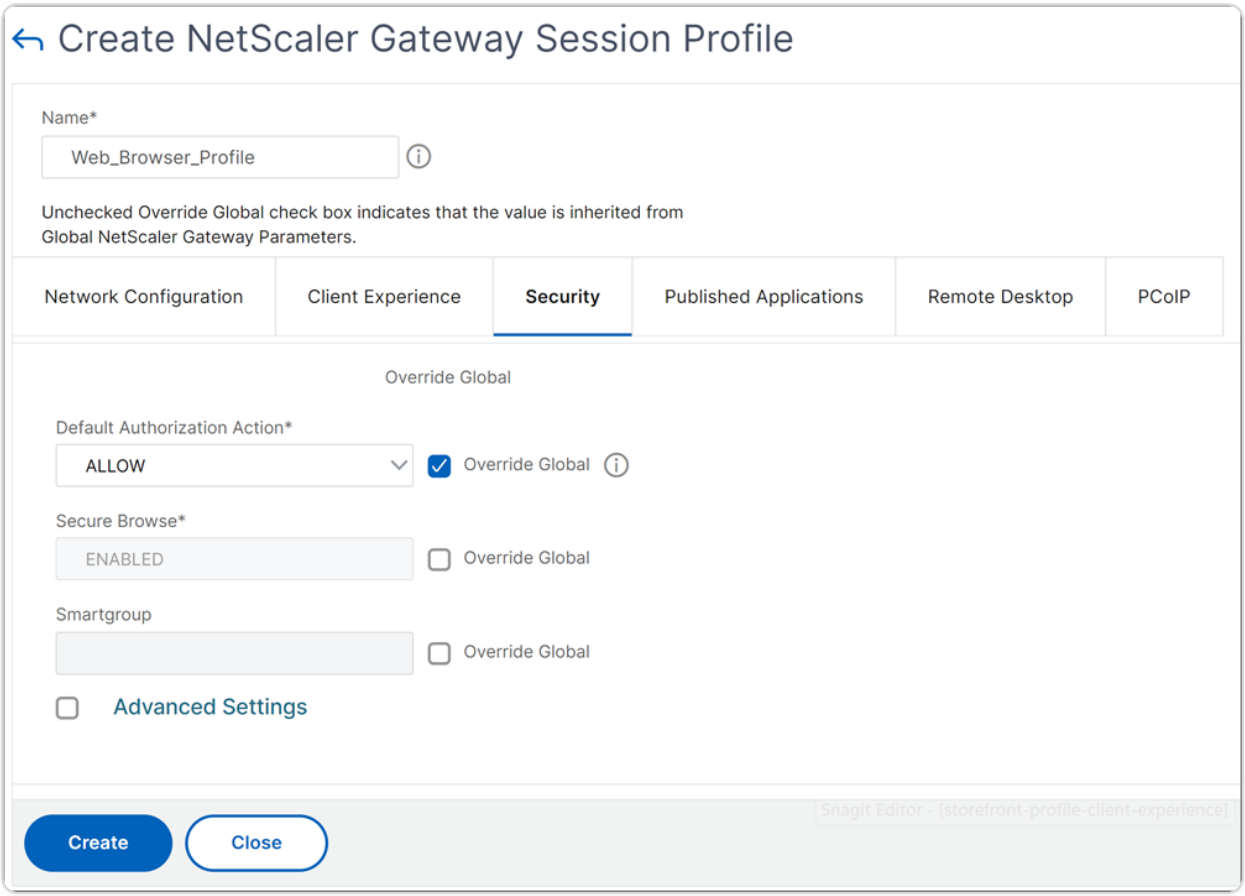
   - **会话超时（分钟）**：将此设置为所需的非活动超时。建议您选择**覆盖全局**，即使您打算使用全局会话超时设置。未能明确覆盖此设置（即使使用默认的 30 分钟超时）也可能导致身份验证循环并强制用户重新登录。
   - **插件类型**：要禁用安全访问客户端（建立完整 VPN 所必需），请将其设置为 **Java**。如果要允许完整 VPN，请参阅 NetScaler Gateway 上的完整 VPN 设置。
   - **Web 应用程序单点登录**：选中此选项后，当用户登录到 NetScaler Gateway 时，它会将凭据转发到 StoreFront 应用商店。如果在 StoreFront 上启用了 NetScaler Gateway 直通 身份验证，则允许单点登录到 StoreFront 应用商店，从而避免用户两次输入凭据。如果您要求用户使用不同的凭据登录到 NetScaler Gateway 和 StoreFront 应用商店，请禁用此选项。

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



5. 在“**安全**”选项卡中，启用“**默认授权操作**”并将其设置为“**允许**”。

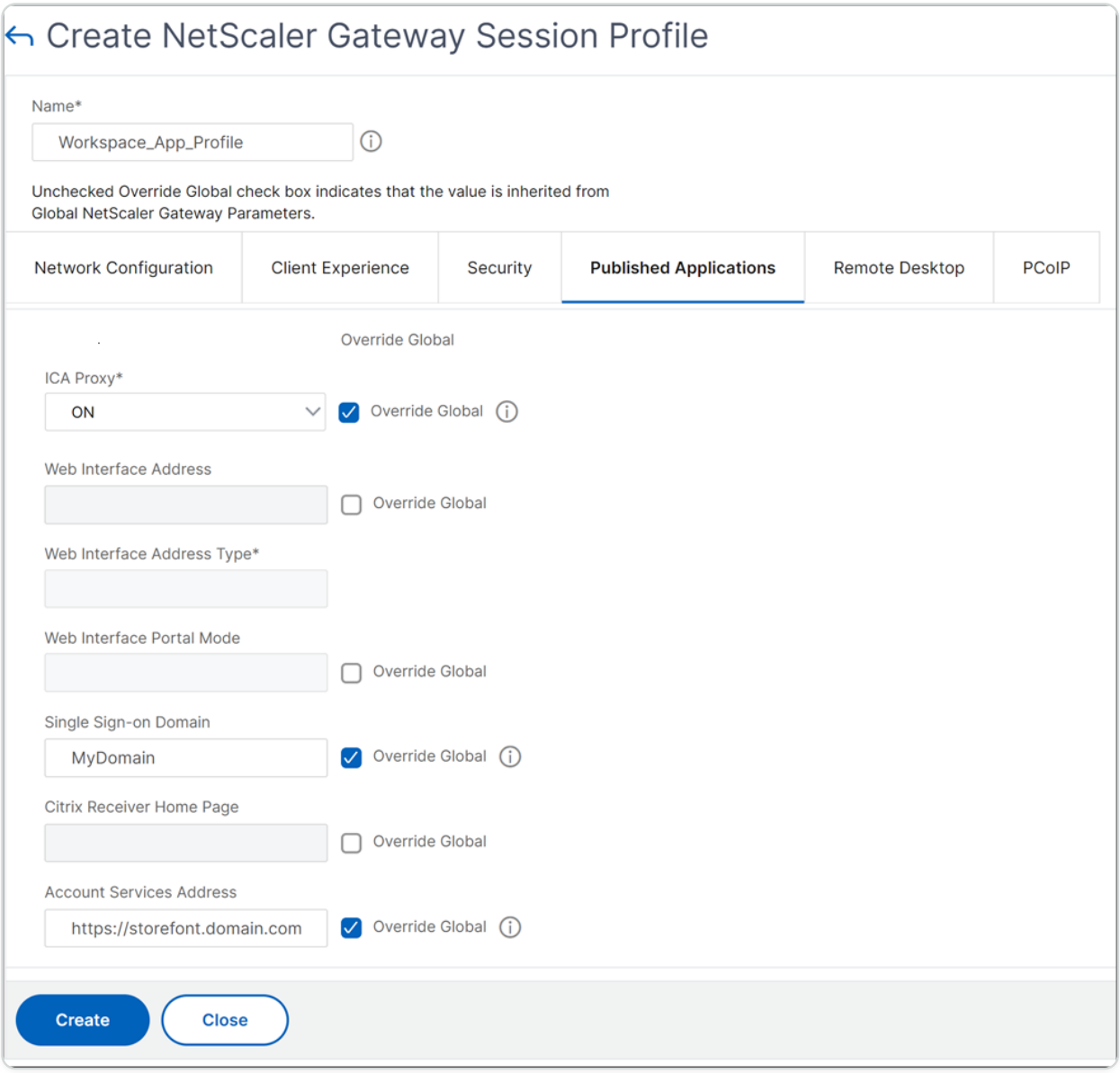
© 1997–2026 Citrix Systems, Inc. All rights reserved.



6. 在“**已发布的应用程序**”选项卡中，启用以下设置：

   - **ICA 代理**：设置为“**开**”。
   - **帐户服务地址**：StoreFront™ 服务器或 StoreFront 服务器组的基本 URL。Citrix Workspace 应用程序使用此地址来发现服务器上可用的应用商店。
   - **单点登录域**：如果您只使用一个域，可以选择输入该域的 NetBIOS 名称。

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

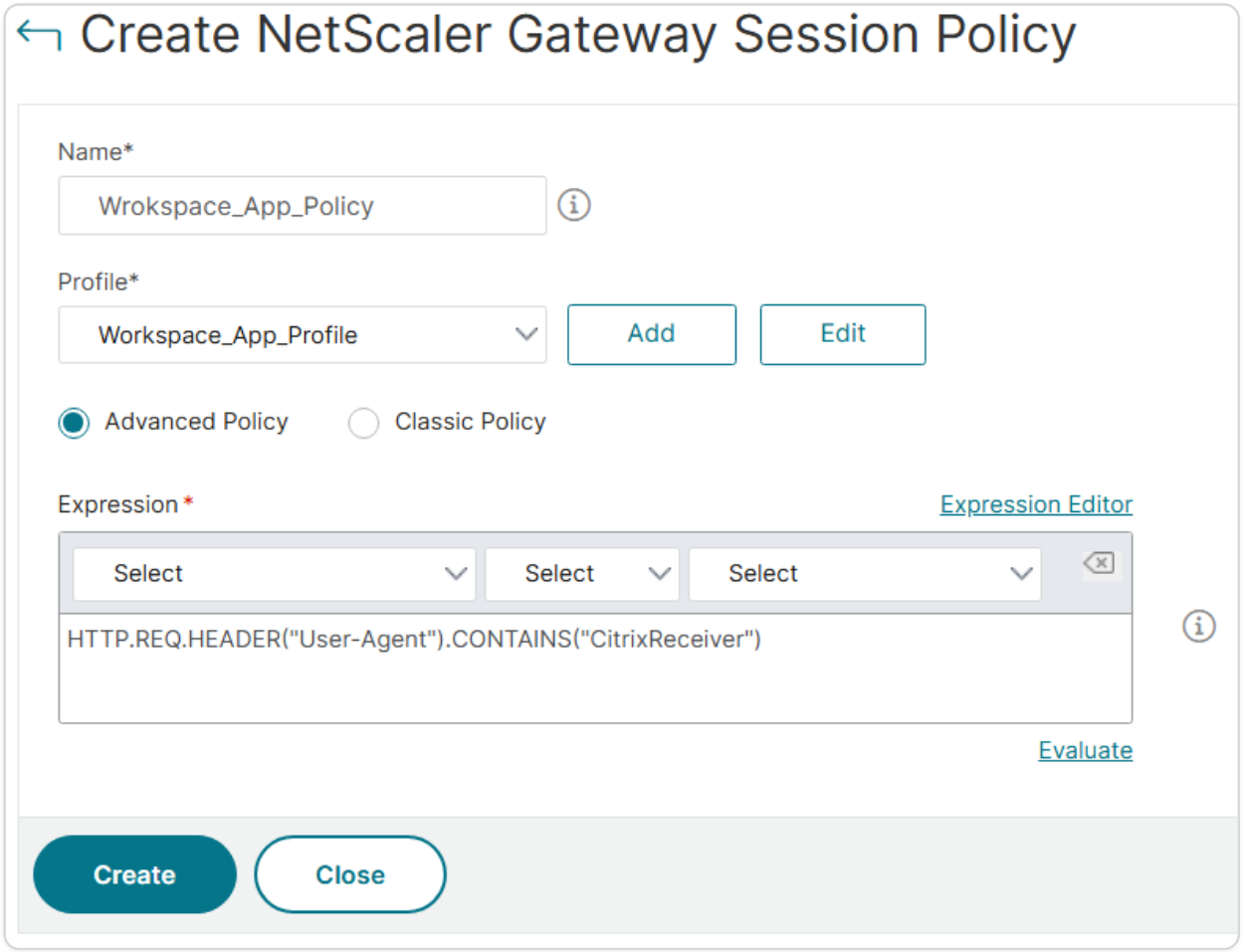


7. 单击“**创建**”。
8. 在“**会话策略**”选项卡中，单击“**添加**”。NetScaler 需要会话策略来区分基于 Web 浏览器和基于 Citrix Workspace 应用程序的连接。此策略应用于基于 Web 浏览器的连接。
9. 在“**名称**”中，为会话策略分配一个名称。
10. 在“**配置文件**”中，选择您创建的会话配置文件。
11. 单击“**高级策略**”选项，并在“**表达式**”下输入以下语法：

    ```
    HTTP.REQ.HEADER("User-Agent").CONTAINS("CitrixReceiver")
    ```

12. 单击 **创建**。

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



3. 创建身份验证配置文件

根据您需要配置的身份验证方法的类型，在 NetScaler 上创建身份验证配置文件。

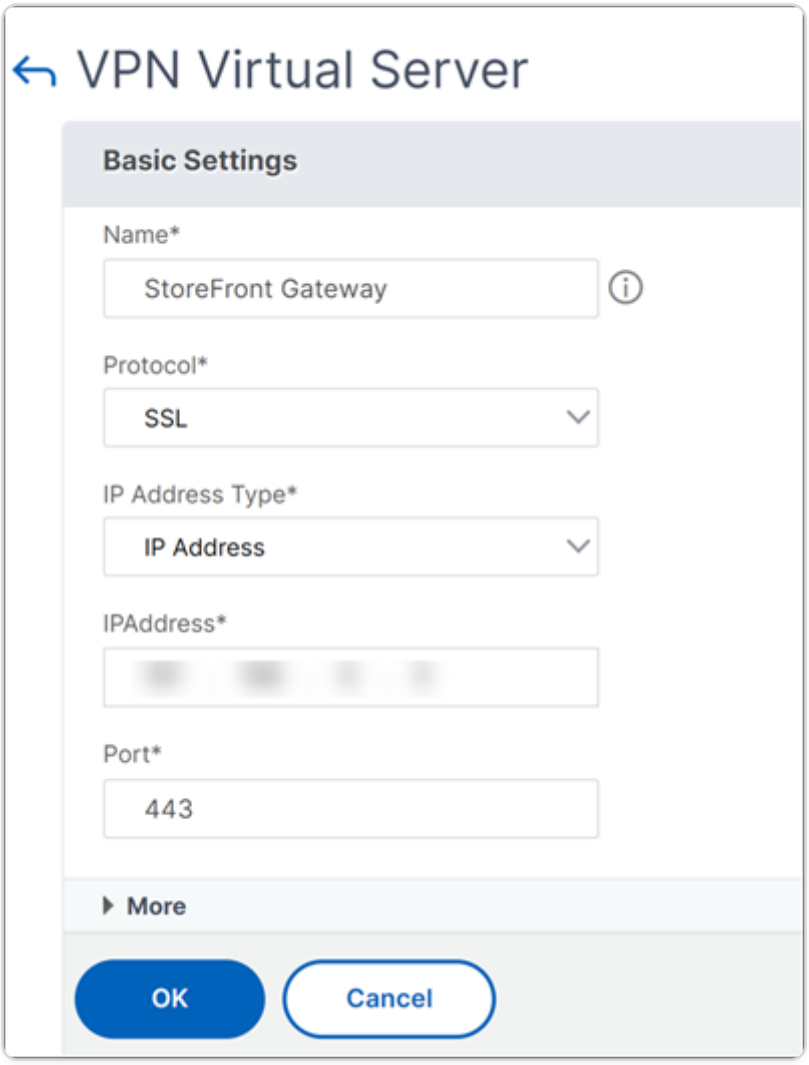
尽管此步骤是可选的，但我们建议将其作为一种良好实践，即在授予对 StoreFront 的访问权限之前，使用 NetScaler Gateway 验证用户的身份。

有关更多详细信息，请参阅身份验证和授权。

4. 创建 NetScaler® Gateway 虚拟服务器

1. 导航到 **NetScaler Gateway > 虚拟服务器**。
2. 单击 **添加** 以添加 NetScaler Gateway 虚拟服务器。
3. 为虚拟服务器分配名称和 IP 地址。

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



注意：

如果您选择不使用 NetScaler Gateway 验证用户，请单击 **更多** 并清除 **启用身份验证** 复选框。

4. 选择 **确定**。
5. 添加证书。
   a. 在“**证书**”下，选择“**服务器证书**”。
   b. 上传服务器证书
   c. 选择“**绑定**”。
6. 选择“**继续**”。
7. 添加会话策略：
   a. 在“**策略**”下，单击“**+**”。

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

b. 从“**选择策略**”下拉列表中，选择“**会话**”。从“**类型**”下拉列表中，选择“**请求**”，然后单击“**继续**”。

c. 在“**策略绑定**”下，单击“**选择策略**”，然后选择您之前创建的基于 Web 浏览器的会话策略和基于 Citrix Workspace 应用程序的会话策略，然后单击“**绑定**”将会话策略绑定到虚拟服务器。

8. 添加 STA 服务器。

a. 如果未显示“**已发布的应用程序**”部分，请从“**高级设置**”中添加。

b. 在“**已发布的应用程序**”部分中，选择“**无 STA 服务器**”。

c. 在“**STA 服务器绑定**”屏幕中，输入第一个 STA 服务器 URL。如果您使用的是 Citrix Virtual Apps and Desktops，请输入 Desktop Delivery Controllers 的 URL。如果您使用的是 Citrix DaaS，请输入 Citrix Cloud Connectors 的 URL。

d. 选择“**绑定**”。

e. 选择“**1 个 STA 服务器**”。在“**VPN 虚拟服务器 STA 服务器绑定**”屏幕上，绑定更多 STA 服务器。

重要提示：

请包含您在 StoreFront 中配置的所有 STA 服务器，否则用户可能会遇到启动失败。

9. 设置身份验证配置文件。

a. 如果未显示“**身份验证配置文件**”部分，请从“**高级设置**”中添加。

b. 在“**身份验证配置文件**”中，选择您之前创建的身份验证配置文件。

c. 选择“**确定**”。

注意：

您必须选择身份验证配置文件，而不是将策略添加到“**基本身份验证**”。基本身份验证使用不再受支持的经典策略，这可能会导致登录失败。

10. 设置适当的 UI 主题。

a. 如果未显示“**门户主题**”部分，请从“**高级设置**”中添加。

b. 如果 StoreFront 网站配置为“**经典体验**”，则选择 **RfWebUI**。如果 StoreFront 网站配置为“**现代体验**”，则选择 **WStheme**。

c. 选择“**确定**”。

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

您可以选择基于 **RfWebUI** 或 **WStheme** 创建自己的自定义主题。

11. 选择“**完成**”。

5. 配置 StoreFront

有关如何将 NetScaler Gateway 添加到 StoreFront 的说明，请参阅配置 NetScaler Gateway。

仅将 NetScaler Gateway 与 StoreFront 或 StoreFront Cloud 集成以进行 HDX 路由

本文介绍如何配置仅用于 HDX 路由的 NetScaler Gateway 虚拟服务器。在此配置中，NetScaler Gateway 不提供任何身份验证或对 StoreFront 的远程访问。相反，您仅使用 NetScaler Gateway 在用户端点与资源位置中的虚拟应用程序和桌面之间代理 HDX (ICA) 连接。

用例

此配置可用于以下场景。

StoreFront

默认情况下，使用 StoreFront 时，同一个 NetScaler Gateway 既用于向 StoreFront 提供远程访问，也用于向虚拟应用程序和桌面提供远程访问。但是，如果您的资源位于与 StoreFront 服务器不同的位置，则可以仅为 HDX 路由在该位置部署 NetScaler Gateway。使用 StoreFront 的**最佳网关路由**功能告知 StoreFront 使用该网关访问特定站点或区域中的资源。

店面云

与本地 StoreFront 部署不同，StoreFront Cloud 托管应用商店 UI 并自行执行用户身份验证。因此，您应将 NetScaler Gateway 配置为仅用于 HDX 路由。

先决条件

- 可从 Internet 访问的 NetScaler Gateway 实例，并具有可绑定到虚拟服务器的有效 SSL 证书。
- 已添加到 Citrix Cloud 并安装了 Cloud Connector 的资源位置。

配置 NetScaler Gateway 以进行 HDX 路由

要配置 NetScaler Gateway 以通过 StoreFront Cloud 进行 HDX 路由，请完成以下步骤：

1. 创建会话配置文件和策略
2. 创建 NetScaler Gateway 虚拟服务器
3. 将 NetScaler Gateway 添加到 StoreFront 或 StoreFront Cloud

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

1. 创建会话配置文件和策略

1. 导航到 **配置 > NetScaler Gateway > 策略 > 会话**。
2. 在 **Session Profiles** 选项卡中，单击 **Add**。
3. 为会话配置文件分配一个名称。
4. 在 **Client Experience** 选项卡中，将 **Session Time-out (mins)** 设置为 **Override Global** 并指定一个值。这是一个非活动超时：它会被网络流量重置，并且不会断开活动的 HDX 连接，因为 ICA 流量会阻止会话进入空闲状态。它仅在连接在配置的持续时间内真正空闲时才结束会话。
5. 在 **Security** 选项卡中，启用 **Default Authorization Action** 并将其设置为 **ALLOW**。
6. 在 **Published Applications** 选项卡中，将 **ICA Proxy** 设置为 **ON**。
7. 单击 **Create**。
8. 在 **Session Policies** 选项卡中，单击 **Add**。
9. 在 **Name** 中，为会话策略分配一个名称。
10. 在 **Profile** 中，选择您创建的会话配置文件。
11. 在 **Expression** 中，输入 `true`，以便策略应用于此虚拟服务器的所有连接。
12. 单击 **Create**。

2. 创建 NetScaler Gateway 虚拟服务器

1. 导航到 **Configuration > NetScaler Gateway > Virtual Servers**，然后单击 **Add**。
2. 分配名称和 IP 地址，然后单击 **Continue**。
3. 在 **Basic Settings** 中，清除 **Enable Authentication** 并选择 **ICA Only**。
4. 绑定证书。
   a. 在 **Certificate** 部分中，单击 **No Server Certificate**。
   b. 在 **Select Server Certificate** 下，选择此虚拟服务器的公共 FQDN 的 SSL 证书，或者如果尚未提供，请单击 **Add** 进行安装。
   c. 单击 **Bind**。
5. 单击 **Continue**。
6. 绑定策略。
   a. 在 **Policies** 部分中，单击 **+**。
   b. 将 **Choose Policy** 保留为 **Session**，将 **Choose Type** 保留为 **Request**，然后选择 **Continue**。

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

c. 在 **策略绑定** 下，单击 **单击以选择**。

d. 选择您在上一步中创建的会话策略，然后单击 **Select**。

e. 单击 **Bind**。

7. 添加 STA 服务器。

a. 在“**高级设置**”列中，单击“**已发布的应用程序**”以将该部分添加到虚拟服务器。

b. 在“**已发布的应用程序**”部分中，单击“**无 STA 服务器**”。

c. 输入资源位置中 Cloud Connector 的地址，然后单击“**绑定**”。

d. 对资源位置中的每个 Cloud Connector 重复此操作。

8. 单击“**完成**”。

3. 将 NetScaler Gateway 添加到 StoreFront 或 StoreFront Cloud

如果您使用的是 StoreFront Cloud，请参阅 连接到 DaaS 资源。

如果您使用的是本地 StoreFront，请参阅 配置 Citrix Gateway。将“**用法或角色**”设置为“**仅 HDX 路由**”。

配置 SmartControl

SmartControl 允许管理员定义精细策略，以配置和强制执行 NetScaler Gateway 上的 Citrix Virtual Apps and Desktops 的用户环境属性。SmartControl 允许管理员从单个位置管理这些策略，而不是在这些服务器类型的每个实例上进行管理。

SmartControl 通过 NetScaler Gateway 上的 ICA 策略实现。每个 ICA 策略都是表达式和访问配置文件组合，可以应用于用户、组、虚拟服务器和全局。ICA 策略在用户会话建立时进行身份验证后进行评估。要启用 SmartControl，您必须将 ICA 策略与 VPN 虚拟服务器关联。

注意：

启用客户端检测功能时，避免使用包含身份验证、授权和审计表达式（例如 AAA.USER、AAA.GROUP）的 ICA 策略。

下表列出了 SmartControl 可以强制执行的用户环境属性：

属性	描述
ConnectClientDrives	指定用户登录时与客户端驱动器的默认连接。

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

属性	描述
ConnectClientLPTPorts	指定用户登录时从客户端自动连接 LPT 端口。LPT 端口是本地打印机端口。
ClientAudioRedirection	指定服务器上托管的应用程序通过安装在客户端计算机上的声音设备传输音频。
ClientClipboardRedirection	指定并配置客户端设备上的剪贴板访问，并将剪贴板映射到服务器。
客户端COM端口重定向	指定客户端的COM端口重定向。COM端口是通信端口。COM端口是串行端口。
客户端驱动器重定向	指定客户端的驱动器重定向。
多流	为指定用户指定多流功能。
客户端USB设备重定向	指定USB设备与客户端之间的重定向（仅限工作站主机）。
`Localremotedata`	指定Citrix Workspace应用程序的HTML5文件上传下载功能。
客户端打印机重定向	指定用户登录会话时要映射到服务器的客户端打印机。
客户端TWAIN设备重定向	允许从已发布的图像处理应用程序默认访问或禁用客户端设备上的TWAIN设备，例如数码相机或扫描仪。
WIA重定向	允许默认访问或禁用 WIA 扫描仪重定向。
拖放	允许默认访问或禁用客户端与远程应用程序和桌面之间的拖放。
智能卡重定向	允许默认访问或禁用智能卡重定向。智能卡虚拟通道在 CVAD 中始终允许。
FIDO2重定向	允许默认访问或禁用 FIDO2 重定向。

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

ICA® 策略和配置文件

ICA 访问配置文件

ICA 配置文件定义了用户连接的设置。如果用户设备满足策略表达式条件，访问配置文件会指定应用于用户 Citrix Virtual Apps and Desktops™ 环境 ICA 的操作。您可以使用 GUI 独立于 ICA 策略创建 ICA 配置文件，然后将该配置文件用于多个策略。一个策略只能使用一个配置文件。

您可以独立于 ICA 策略创建访问配置文件。创建策略时，您可以选择要附加到策略的访问配置文件。访问配置文件指定了用户可用的资源。

从版本 14.1-8.x 开始，NetScaler Gateway 将 SmartControl 功能扩展到 Citrix Virtual Apps and Desktops 的更多 ICA 虚拟通道。此扩展改进了 NetScaler Gateway 与 ICA 虚拟通道之间的交互。

为了利用扩展的 SmartControl 功能，您可以在 ICA 访问配置文件上配置以下设置。

- 客户端 TWAIN 设备重定向
- WIA重定向
- 拖放
- 智能卡重定向
- FIDO2重定向

使用 GUI 配置 ICA 访问配置文件

1. 导航到 **NetScaler Gateway > 策略 > NetScaler Gateway ICA 策略和配置文件 > 访问配置文件**，然后单击“**添加**”。此时将显示“**创建 ICA 访问配置文件**”页面。
2. 为 ICA 访问配置文件提供名称，配置以下参数，然后单击“**创建**”。
    - 连接客户端 LPT 端口：允许或阻止用户登录时从客户端自动连接线路打印终端 (LPT) 端口。
    - 客户端音频重定向：允许或阻止服务器上托管的应用程序通过客户端计算机上安装的声音设备播放声音。此设置还允许或阻止用户录制音频输入。
    - 本地远程数据共享：允许或阻止通过适用于 HTML5 的 Citrix Workspace™ 应用程序进行文件或数据共享。
    - 客户端剪贴板重定向：允许或阻止将客户端设备上的剪贴板映射到服务器上的剪贴板。
    - 客户端 COM 端口重定向：允许或阻止与客户端之间的通信 (COM) 端口重定向。
    - 客户端驱动器重定向：允许或阻止与客户端之间的驱动器重定向。
    - 客户端打印机重定向：允许或阻止用户登录会话时将打印机映射到服务器。
    - 多流：允许或阻止为指定用户启用多流功能。

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

- 客户端 USB 驱动器重定向：允许或阻止 USB 设备重定向到客户端或从客户端重定向。
- 客户端 TWAIN 设备重定向：允许或阻止已发布的图像处理应用程序在客户端设备上使用 TWAIN 设备（例如数码相机或扫描仪）。
- WIA 重定向：允许或阻止 Windows 图像采集 (WIA) 扫描仪重定向。
- 拖放：允许或阻止客户端与远程应用程序和桌面之间的拖放操作。
- 智能卡重定向：允许或阻止智能卡重定向。在 Citrix Virtual Apps and Desktops 中，智能卡虚拟通道始终允许。
- FIDO2 重定向：允许或阻止快速身份在线 2 (FIDO 2) 重定向。

使用 CLI 配置 ICA 访问配置文件

```
add ica accessprofile <name> [-ConnectClientLPTPorts ( DEFAULT |
DISABLED )] [-ClientAudioRedirection ( DEFAULT | DISABLED )][-
LocalRemoteDataSharing ( DEFAULT | DISABLED )][-ClientClipboardRedirection
( DEFAULT | DISABLED )][-ClientCOMPortRedirection ( DEFAULT | DISABLED )]
[-ClientDriveRedirection ( DEFAULT | DISABLED )][-ClientPrinterRedirection
( DEFAULT | DISABLED )] [-Multistream (DEFAULT | DISABLED )][-
ClientUSBDriveRedirection ( DEFAULT | DISABLED)] [-
ClientTWAINDeviceRedirection ( DEFAULT | DISABLED )][-WIARedirection
( DEFAULT | DISABLED )] [-DragAndDrop ( DEFAULT | DISABLED )] [-
SmartCardRedirection ( DEFAULT | DISABLED )]

[-FIDO2Redirection ( DEFAULT | DISABLED )]
```

ICA 延迟配置文件

使用 GUI 配置 ICA 延迟配置文件

1. 导航到 **NetScaler Gateway > 策略 > NetScaler Gateway ICA 策略和配置文件 > ICA 延迟配置文件**。
2. 更新所需字段，然后单击“**创建**”。

使用 CLI 配置 ICA 延迟配置文件

`add ica latencyprofile [-l7LatencyMonitoring ( ENABLED | DISABLED )] [-l7LatencyThresholdFactor ] [-l7LatencyWaitTime ] [-l7LatencyNotifyInterval ] [-l7LatencyMaxNotifyCount ]`

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

ICA 操作

使用 GUI 配置 ICA 操作

1. 导航到 **NetScaler Gateway > Policies**，然后单击 **ICA**。
2. 在 **ICA Actions** 选项卡中，单击 **Add**。将显示 **Create ICA Action** 页面。
3. 在 **Name** 字段中，为 ICA 策略指定一个名称。
4. 在 **ICA Access Profile** 字段旁边，执行以下操作之一：
   - 单击 **>** 图标以选择现有 ICA 访问配置文件。
   - 单击 **Add** 以创建 ICA 访问配置文件。
5. 创建一个 ICA 延迟配置文件，并将其关联到 ICA 操作。
6. 单击 **Create**。

ICA 策略

ICA 策略指定操作、访问配置文件、表达式以及可选的日志操作。您可以执行以下 ICA 策略配置：

使用 GUI 配置 ICA 策略

1. 导航到 **NetScaler Gateway > Policies**，然后单击 **ICA**。
2. 在 **ICA Policies** 部分中，单击 **Add**。将显示 **Create ICA Policy** 页面。
3. 在 **Name** 字段中，为 ICA 策略指定一个名称。
4. 在 **Action** 字段旁边，执行以下操作之一：
   - 单击 **>** 图标以选择现有操作。
   - 单击 **添加** 以创建操作。
5. 添加表达式。
6. 创建日志操作。
7. 根据需要配置其余参数，然后单击 **确定**。

使用 CLI 配置 ICA 策略

```
add ica policy smartaccess_policy -rule TRUE -action smartaccess_action
```

使用 GUI 将 ICA 策略绑定到绑定点

1. 导航到 **NetScaler Gateway > 策略 > NetScaler Gateway > ICA 策略和配置文件 > ICA 策略**。单击 **策略管理器**。

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

2. 选择绑定点和虚拟服务器，然后单击 **继续**。
3. 在 **策略绑定** 部分中，选择需要与绑定点关联的 ICA 策略。
4. 单击 **绑定**，然后单击 **完成**。

要验证绑定，请在 **ICA 策略** 部分中单击 **显示绑定**。您可以查看与 ICA 策略关联的绑定点列表。

使用 CLI 将 ICA 策略绑定到 VPN 虚拟服务器

```
bind vpn vserver vpnvserver -policy smartaccess_policy -type ICA_REQUEST
-priority 10
```

使用 CLI 配置 ICA 操作

```
add ica action smartaccess_action -accessProfileName smartaccess_profile
```

SmartControl 对 Secure HDX™ 的支持

Secure HDX 是一种应用层加密 (ALE) 解决方案，可防止流量路径中的任何网络元素检查 HDX 流量。从版本 14.1 build 47.46 开始，在启用 Secure HDX 时可以配置 SmartControl。有关在 NetScaler Gateway 上配置 Secure HDX 的更多信息，请参阅 Secure HDX（预览版）。

从版本 14.1 build 60.x 开始，NetScaler Gateway 支持在适用于 Linux 的 VDA 中启用 Secure HDX 的 SmartControl。

系统要求

目前，仅在以下平台上支持启用 Secure HDX 的 SmartControl：

- 适用于 Windows 的 Citrix Workspace 应用程序 - 2503 版及更高版本。
- 适用于 Windows 的 VDA - 2503 版及更高版本。
- 适用于 Linux 的 VDA - 2507 版及更高版本

有关在启用 Secure HDX 时配置 SmartControl 的系统要求的更多信息，请参阅 系统要求。

主要增强功能

- **数据安全：** 通过 TLS 在 NetScaler Gateway 和 VDA 之间建立安全的端到端连接。

限制

在以下场景中不支持启用 Secure HDX 的 SmartControl：

- EDT 连接
- HDX 多流 ICA (MSI) 连接

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

- IPv6 协议
- 透明模式和 LAN 代理模式拓扑
- SOCKS 协议

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

Microsoft Intune 的集成

Microsoft Intune 与 NetScaler Gateway 的集成提供了由 NetScaler Gateway 和 Intune 提供的同类最佳的应用程序访问和数据保护解决方案。

您将获得最完整的安全生产力应用程序套件，包括电子邮件、日历、联系人、笔记、文档编辑和远程访问——所有这些都可以在不同平台上进行集中管理。Intune 和 NetScaler Gateway 集成提供了世界一流的移动设备管理 (MDM) 功能，而 Citrix Secure Access 客户端技术则使这些 Intune 增强型应用程序能够通过 NetScaler Gateway 安全地访问企业数据和应用程序。

此集成允许 NetScaler Gateway 从 Intune 拉取合规性数据，从而启用条件访问策略。条件访问策略使 NetScaler Gateway 能够根据设备功能等对访问进行更精细的控制。例如，管理员可以创建一项策略，规定只有禁用“摄像头”的设备才能获得访问权限。

NetScaler Gateway 虚拟服务器配置完成后，NetScaler Gateway 支持 Microsoft 身份验证库 (MSAL) 令牌身份验证。配置后，使用 Citrix 仅网络包装器或 SDK 封装的移动应用程序通过使用可直接从 Microsoft Entra ID 获取的 MSAL 令牌访问 NetScaler Gateway。

Citrix® 微型 VPN 与 Microsoft Endpoint Manager 的集成

NetScaler Gateway 客户可以将微型 VPN 与 Microsoft Endpoint Manager (Intune) 结合使用。Citrix 微型 VPN 与 Microsoft Endpoint Management 的集成使您的应用程序能够访问本地资源。

Citrix 微型 VPN 技术提供按需 VPN，可降低数据传输成本并简化安全性，因为 VPN 隧道并非始终处于活动状态。相反，它仅在需要时才处于活动状态，这降低了风险并优化了设备的性能，从而提供更好的用户体验。这还有助于延长移动设备的电池续航时间。NetScaler® 的微型 VPN 技术为移动用户提供对内部业务资源的安全访问，同时为他们提供最佳用户体验。

微型 VPN 仅支持以下用例：

- 仅限 Intune 移动应用程序管理 (MAM)
- Intune 移动设备管理 (MDM) 和移动应用程序管理 (MAM)

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

重要提示：

对于 SSL VPN 功能，微型 VPN 需要 NetScaler Gateway Advanced 或 Premium 版本（VPX 3000 或更高版本）以及 Citrix Endpoint Management 授权。Citrix Endpoint Management 授权可确保在 Microsoft Edge 移动浏览器（iOS 和 Android）上持续支持微型 VPN SDK。有关更多信息，请联系您的销售、客户或合作伙伴代表。

有关设置 Citrix 微型 VPN 与 Microsoft Endpoint Manager 集成的详细信息，请参阅 设置 NetScaler Gateway 以将微型 VPN 与 Microsoft Endpoint Manager 结合使用。

何时使用集成的 Intune MDM 解决方案

以下场景说明了集成的 Intune MDM 解决方案的使用：

- 新客户决定引入 Intune 并部署本地 NetScaler Gateway
- 现有 NetScaler Gateway 用户希望添加使用 Intune 进行移动设备管理
- 现有 Intune 用户希望允许移动设备或应用程序通过公司 DMZ 中的 NetScaler Gateway 物理或虚拟设备访问公司网络内部的数据

注意

仅支持 iOS 和 Android 客户端。

了解 NetScaler Gateway 与 Intune 的 MDM 集成

以下是 NetScaler Gateway 与 Intune 的典型 MDM 集成中的事件流示例：

1. 使用 Intune 注册移动设备。
2. 企业批准的应用程序和设备策略被推送到设备。
3. 从设备浏览 SharePoint（本地应用程序）。
4. 浏览器请求发送到 NetScaler Gateway。
5. NetScaler Gateway 设备向 Intune 检查设备的注册状态。
6. 如果合规设备成功注册，则授予 SharePoint 访问权限。

Intune 和 NetScaler 集成(/en-us/netscaler-gateway/media/intune_diagram.jpg)

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

当设备不符合条件访问策略时，NetScaler Gateway VPN 客户端会显示一条错误消息。该消息提供了一个从设备到 Intune 托管页面的链接，该页面为用户提供了注册或修复设备合规性状态的选项。

注意：

管理员在将证书推送到 Intune 时必须确保以下事项，以便用户可以区分其设备上的各种证书。

- 证书必须具有主题摘要。
- 不同证书的主题摘要必须是唯一的。

Intune NAC v2 API 支持

作为 Intune NAC v2 API 支持的一部分，您必须绑定一个证书颁发机构文件（CA 证书），以确保 NetScaler 设备从移动设备获取有效证书。在 Intune NAC v2 中，移动设备将设备 ID 作为 CA 证书的一部分发送。此处绑定的 CA 证书必须是用于向最终用户 iOS 和 Android 设备颁发客户端证书的证书。如果存在中间证书，也必须在此处绑定。

有关更多详细信息，请参阅 Intune NAC v2 API 支持

配置 NetScaler Gateway 虚拟服务器的网络访问控制设备检查以进行单因素登录

本主题提供有关配置 NetScaler Gateway 的信息，以便通过 Microsoft Intune 提供的网络访问合规性 (NAC) 安全功能，从移动设备（iOS 和 Android）连接到内部网络。当用户尝试从 iOS 或 Android VPN 客户端连接到 NetScaler Gateway 时，网关首先会向 Intune 服务检查设备是否为受管设备和合规设备。

- 受管：设备已使用 Intune 公司门户客户端注册。
- 合规：已应用从 Intune MDM 服务器推送的所需策略。

仅当设备既受管又合规时，才会建立 VPN 会话，并向用户提供对内部资源的访问权限。

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

注意：

- 在此设置中，后端 NetScaler Gateway 与 Intune 服务通信。SSL 配置文件处理到 NetScaler Gateway 的传入连接。NetScaler Gateway 后端通信处理后端云服务 (Intune) 的任何 SNI 要求。
- NetScaler Gateway 13.0 build 64.x 及更高版本支持 DTLS 网关虚拟服务器的 SNI。
- Intune NAC 检查（无论是针对每应用 VPN 还是设备范围 VPN）仅在 VPN 配置文件由 Intune 管理门户（现称为 Microsoft Endpoint Manager）预配时才受支持。这些功能不支持最终用户添加的 VPN 配置文件。最终用户设备必须由其 Intune 管理员通过 Microsoft Endpoint Manager 将 VPN 配置文件部署到其设备上，才能使用 NAC 检查。

许可

此功能需要 Citrix Enterprise Edition 许可证。

系统要求

- NetScaler Gateway 11.1 build 51.21 或更高版本
- iOS VPN – 10.6 或更高版本
- Android VPN – 2.0.13 或更高版本
- 微软
  - Microsoft Entra ID 访问权限（拥有租户和管理员权限）
  - 启用 Intune 的租户
- 防火墙 启用防火墙规则，允许所有 DNS 和 SSL 流量从子网 IP 地址流向 `https://login.microsoftonline.com` 和 `https://graph.microsoft.com`（端口 53 和端口 443）

先决条件

- 所有现有身份验证策略都必须从经典策略转换为高级策略。有关如何从经典策略转换为高级策略的信息，请参阅 `<https://support.citrix.com/article/CTX131024>`。
- 在 Azure 门户上创建 NetScaler Gateway 应用程序。有关详细信息，请参阅 在 Azure 门户上配置 NetScaler Gateway 应用程序。
- 使用以下应用程序特定信息，在您创建的 NetScaler Gateway 应用程序上配置 OAuth 策略。
  - 客户端 ID / 应用程序 ID

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

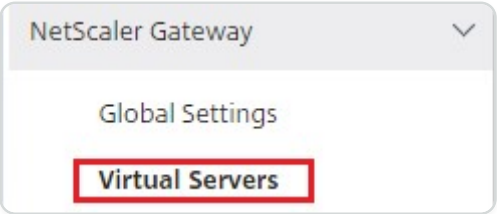
- 客户端密钥 / 应用程序密钥
- 微软 Entra 租户 ID

参考

- 本文档介绍了 NetScaler Gateway 的设置配置。大部分 Citrix SSO 客户端 (iOS/Android) 配置是在 Intune 端完成的。有关 NAC 的 Intune VPN 配置的详细信息，请参阅 `<https://docs.microsoft.com/zh-cn/mem/intune/protect/network-access-control-integrate>`。
- 要为 iOS 应用程序配置 VPN 配置文件，请参阅 `<https://docs.microsoft.com/zh-cn/mem/intune/configuration/vpn-settings-ios>`。
- 要在 Azure 门户上设置 NetScaler Gateway 应用程序，请参阅 在 Azure 门户上配置 NetScaler Gateway 应用程序。

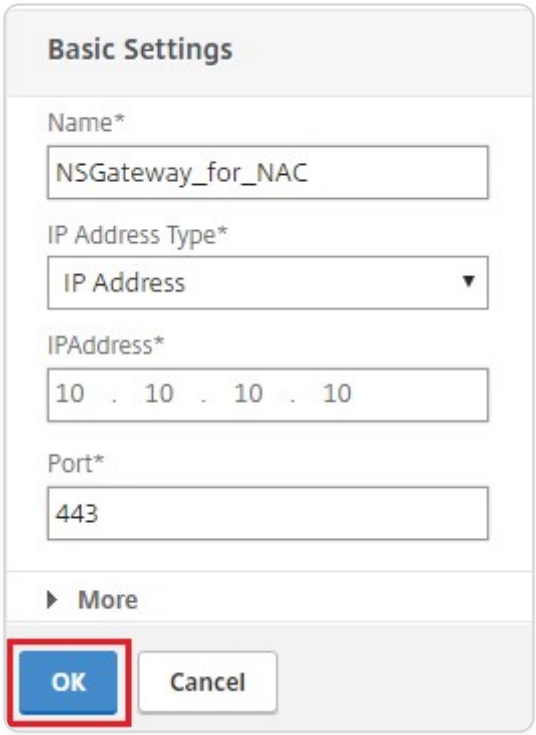
添加具有 nFactor 的 NetScaler Gateway 虚拟服务器以进行网关部署

1. 导航到 **NetScaler Gateway > 虚拟服务器**。



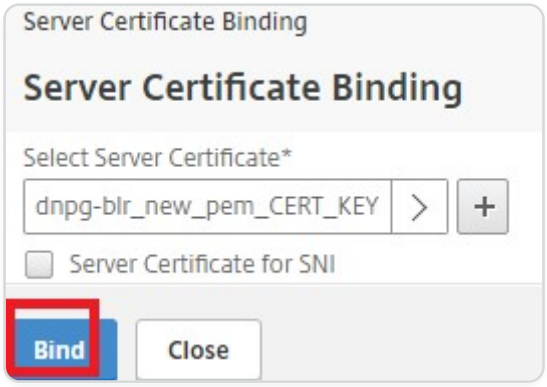
2. 单击 **添加**。
3. 在 **基本设置** 区域中提供所需信息，然后单击 **确定**。

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



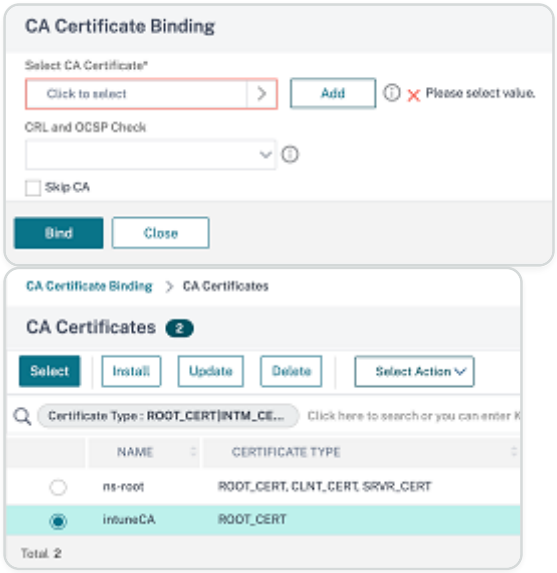
4. 选择 **服务器证书**。

5. 选择所需的服务器证书，然后单击 **绑定**。



6. 作为 Intune NAC v2 API 支持的一部分，您必须绑定证书颁发机构文件（CA 证书），以确保 NetScaler 设备从移动设备获取有效证书。在 Intune NAC v2 中，移动设备将设备 ID 作为客户端证书的一部分发送。此处绑定的 CA 证书必须是用于向最终用户 iOS 和 Android 设备颁发客户端证书的证书。如果存在中间证书，也必须在此处绑定。有关 Intune 配置的更多信息，请参阅在 Azure 门户上配置 NetScaler Gateway 应用程序。对于 Intune NAC v2 API 支持，请选择所需的 CA 证书，然后单击 **绑定**。

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



7. 单击 **继续**。
8. 单击 **继续**。
9. 点击**继续**。
10. 点击**策略**旁边的加号图标 ，并从**选择策略**列表中选择**会话**，再从**选择类型**列表中选择**请求**，然后点击**继续**。
11. 点击**选择策略**旁边的加号图标 。
12. 在**创建 NetScaler Gateway 会话策略**页面上，为会话策略提供一个名称。
13. 点击**配置文件**旁边的加号图标 ，并在**创建 NetScaler Gateway 会话配置文件**页面上，为会话配置文件提供一个名称。
14. 在**客户端体验**选项卡上，点击**无客户端访问**旁边的复选框，并从列表中选择**关闭**。
15. 点击**插件类型**旁边的复选框，并从列表中选择 Windows/Mac OS X。
16. 点击**高级设置**，并选中**客户端选择**旁边的复选框，然后将其值设置为**开**。
17. 在**安全**选项卡上，点击**默认授权操作**旁边的复选框，并从列表中选择**允许**。
18. 在**已发布的应用程序**选项卡上，点击**ICA 代理**旁边的复选框，并从列表中选择**关闭**。
19. 点击**创建**。
20. 在**创建 NetScaler Gateway 会话策略**页面上，在**表达式**区域中，配置限定表达式。
21. 点击**创建**。
22. 点击**绑定**。
23. 在**高级设置**中选择**身份验证配置文件**。

    选择身份验证配置文件(/en-us/netscaler-gateway/media/intune_6.jpg)
24. 单击加号图标 ，并为身份验证配置文件提供一个名称。

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

身份验证配置文件名称(/en-us/netscaler-gateway/media/intune_7.jpg)

25. 单击加号图标 以创建身份验证虚拟服务器。

    添加身份验证虚拟服务器(/en-us/netscaler-gateway/media/intune_8.jpg)

26. 在“**基本设置**”区域下指定身份验证虚拟服务器的名称和 IP 地址类型，然后单击“**确定**”。IP 地址类型也可以是“**不可寻址**”。

    设置基本设置(/en-us/netscaler-gateway/media/intune_9.jpg)

27. 单击“**身份验证策略**”。

    身份验证策略(/en-us/netscaler-gateway/media/intune_10.jpg)

28. 在“策略绑定”视图下，单击加号图标 以创建身份验证策略。

    创建身份验证策略(/en-us/netscaler-gateway/media/intune_11.jpg)

29. 选择 **OAUTH** 作为“**操作类型**”，然后单击加号图标 以为 NAC 创建 OAuth 操作。

    选择 OAuth 操作类型(/en-us/netscaler-gateway/media/intune_12.jpg)

30. 使用“**客户端 ID**”、“**客户端密钥**”和“**租户 ID**”创建 OAuth 操作。

    注意：

    - 在 Azure 门户上配置 NetScaler Gateway 应用程序后，会生成 **客户端 ID**、**客户端密钥** 和 **租户 ID**。
    - 记下客户端 ID/应用程序 ID、客户端密钥/应用程序密钥和 Microsoft Entra 租户 ID 信息，因为稍后在 NetScaler Gateway 上创建 OAuth 操作时需要它们。

    确保您的设备上已配置适当的 DNS 名称服务器，以便解析和访问；

    ```
    -  `https://login.microsoftonline.com/,`

    -  `https://graph.microsoft.com/`,

    -  *.manage.microsoft.com.
    ```

    Azure 门户的 ID 和密钥(/en-us/netscaler-gateway/media/intune_13.jpg)

31. 为 **OAuth 操作**创建身份验证策略。

    规则：

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

```
http.req.header("User-Agent").contains("NAC/1.0")&&
((http.req.header("User-Agent").contains("iOS") &&
http.req.header("User-Agent").contains("NSGiOSplugin")) ||
(http.req.header("User-Agent").contains("Android") &&
http.req.header("User-Agent").contains("CitrixVPN")))
```

身份验证策略规则(/en-us/netscaler-gateway/media/intune_14.jpg)

32. 单击加号图标 以创建 nextFactor 策略标签。

    创建 next factor 策略标签(/en-us/netscaler-gateway/media/intune_15.jpg)

33. 单击加号图标 以创建登录架构。

    创建登录架构(/en-us/netscaler-gateway/media/intune_16.jpg)

34. 选择 `noschema` 作为身份验证架构，然后单击**创建**。

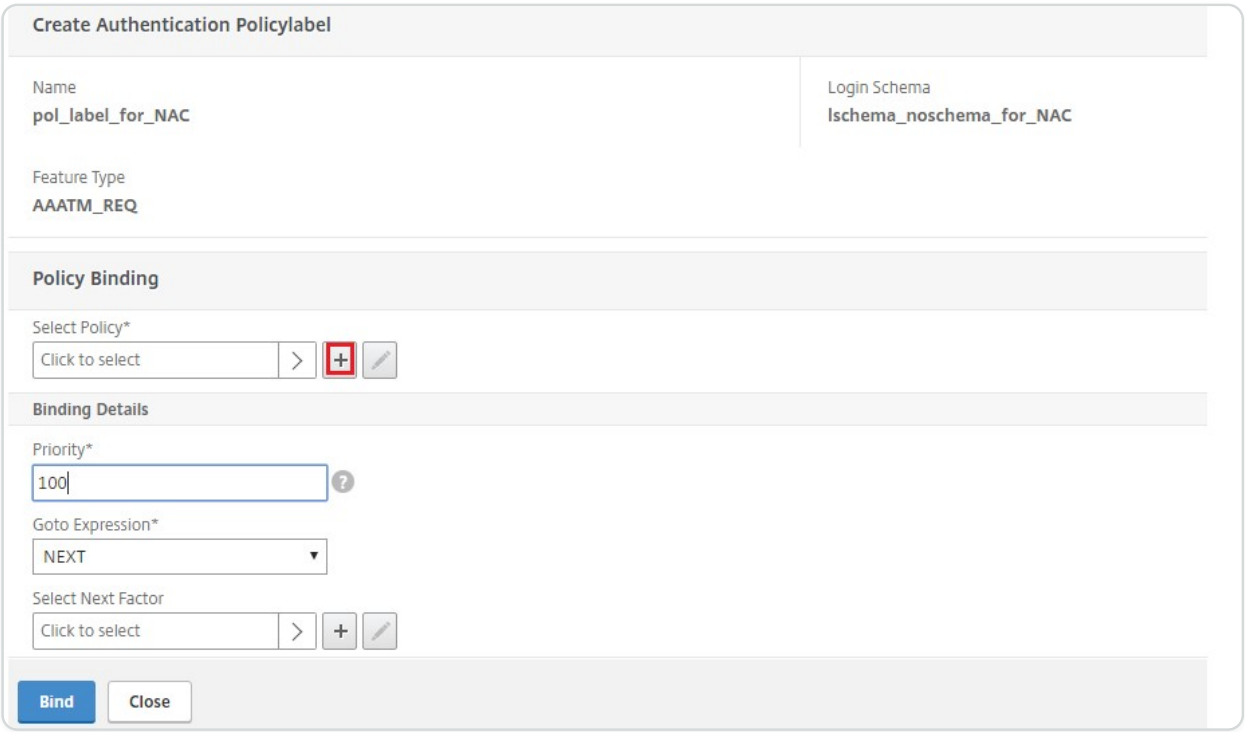
    选择身份验证架构(/en-us/netscaler-gateway/media/intune_17.jpg)

35. 选择已创建的登录架构后，单击**继续**。

    单击继续(/en-us/netscaler-gateway/media/intune_18.jpg)

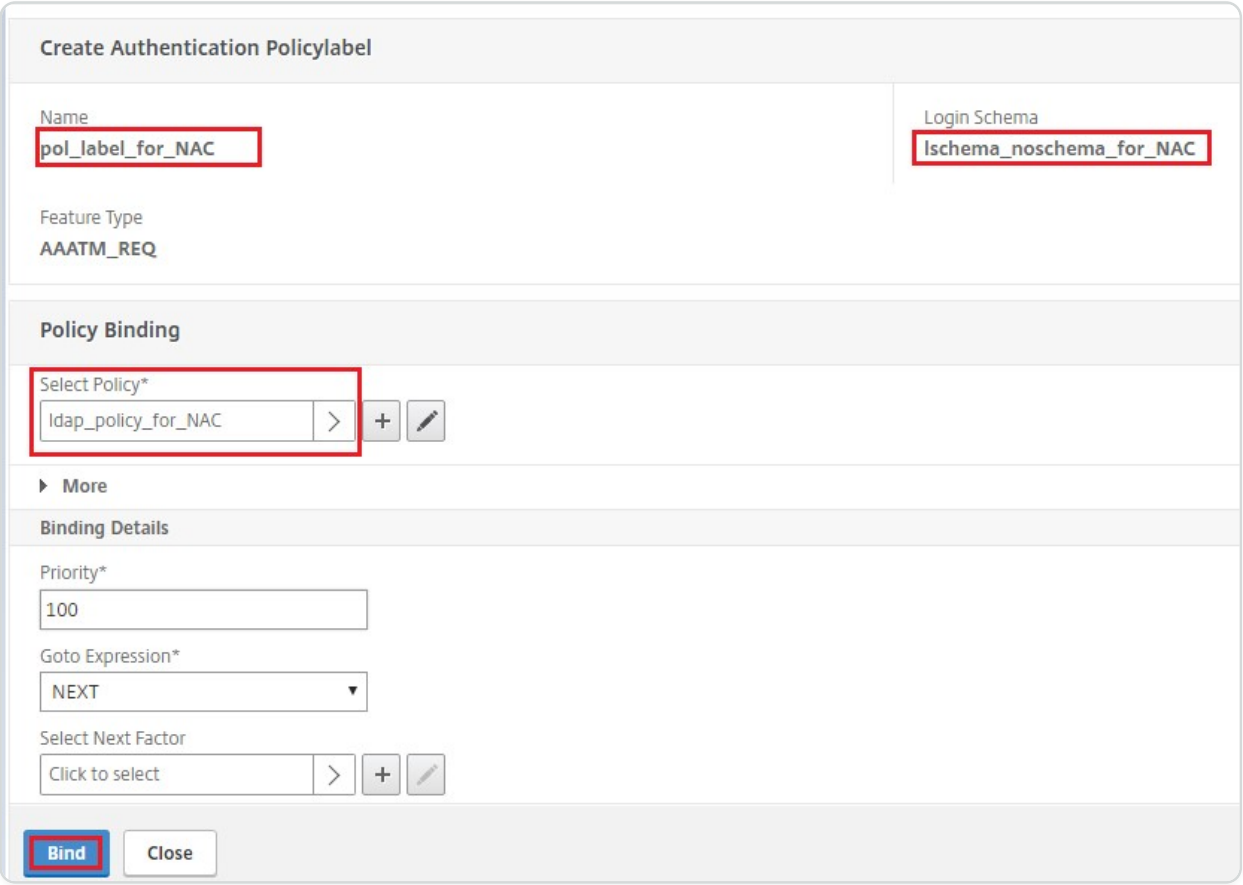
36. 在 **选择策略** 中，选择一个现有的用户登录认证策略，或点击加号图标 **+** 创建一个认证策略。

    有关创建认证策略的详细信息，请参阅 配置高级认证策略 和 配置 LDAP 认证。

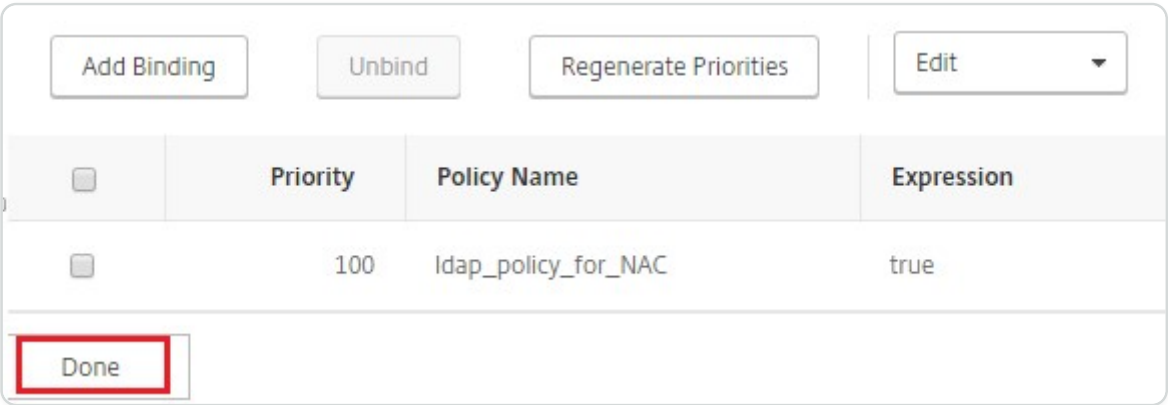


37. 点击 **绑定**。

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

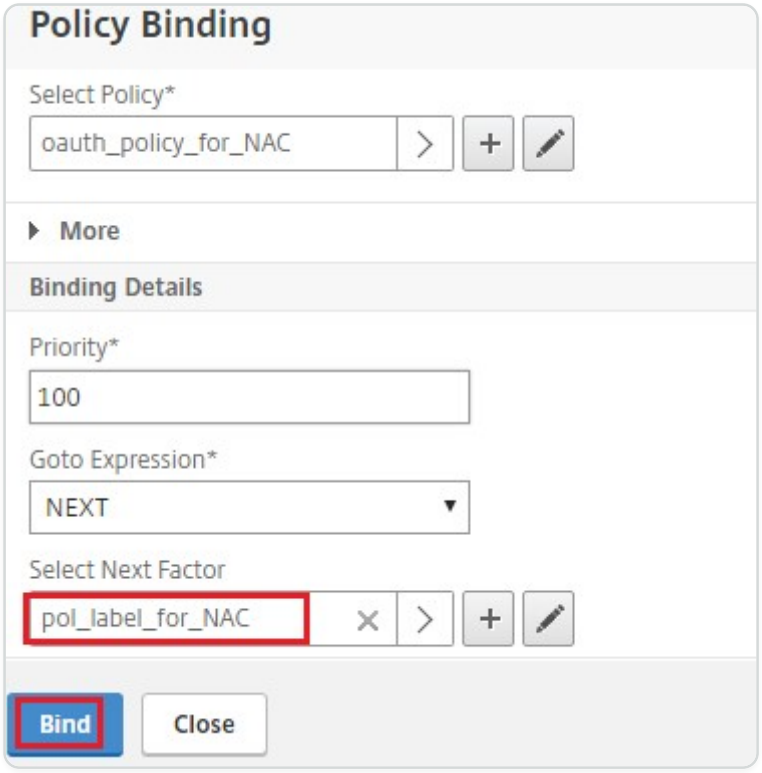


38. 点击 **完成**。

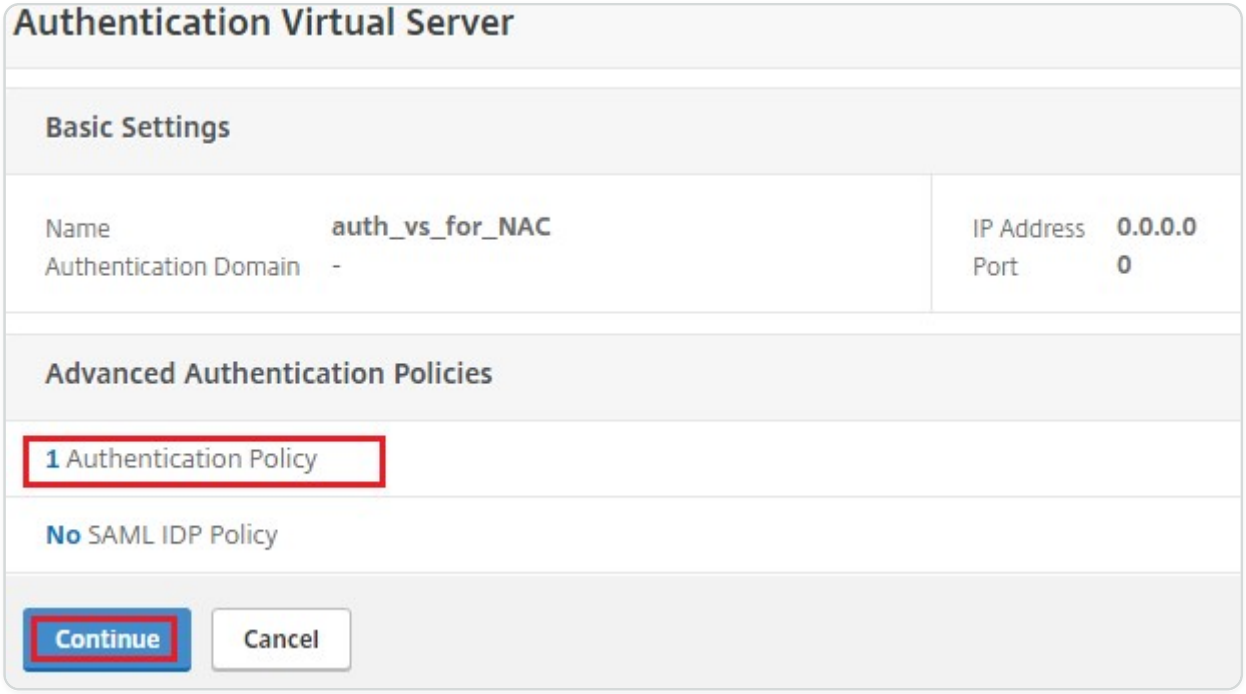


39. 点击 **绑定**。

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

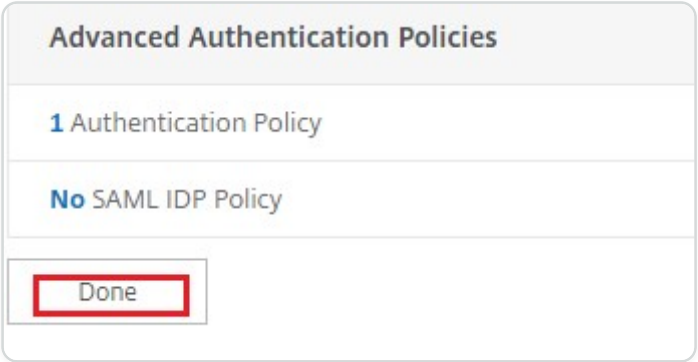


40. 点击 **继续**。

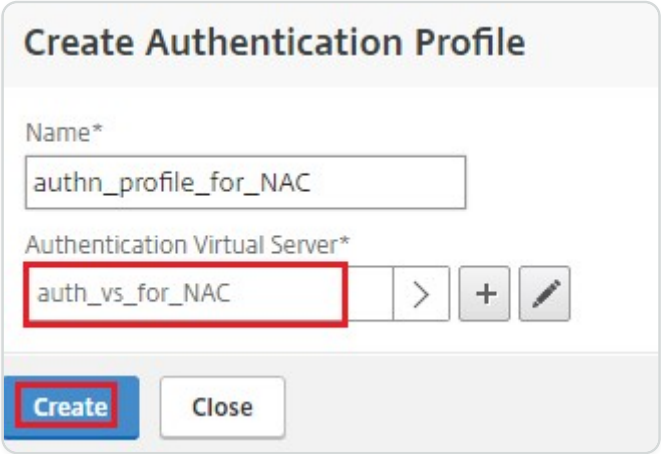


41. 点击 **完成**。

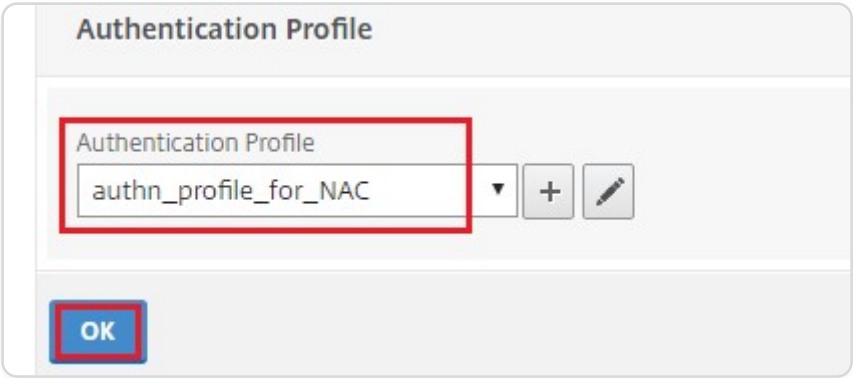
© 1997–2026 Citrix Systems, Inc. All rights reserved.



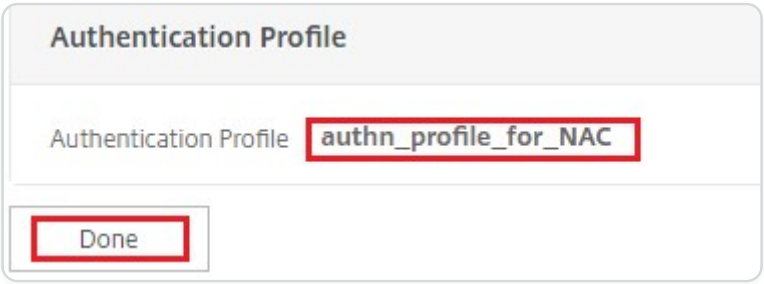
42. 点击 **创建**。



43. 单击 **确定**。



44. 单击 **完成**。

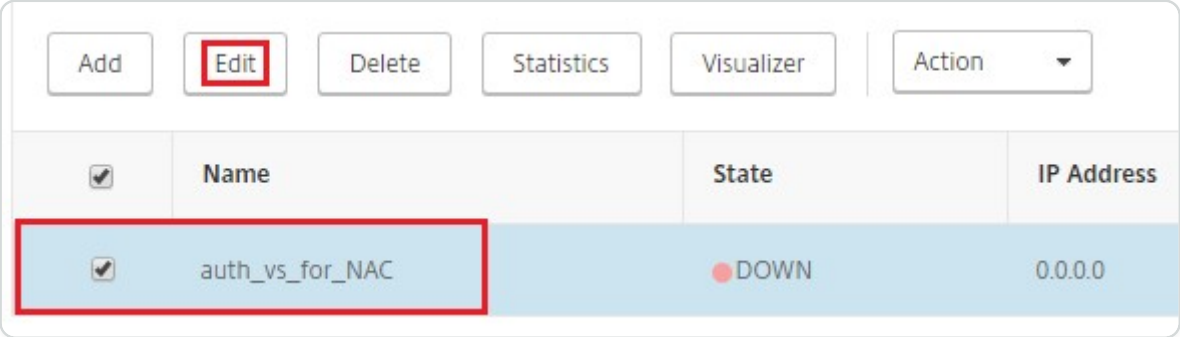


© 1997–2026 Citrix Systems, Inc. All rights reserved.

将身份验证登录方案绑定到身份验证虚拟服务器，以指示 VPN 插件发送设备 ID 作为 /cgi/login 请求的一部分

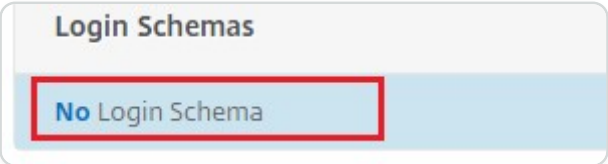
1. 导航到 **安全** > **AAA - 应用程序流量** > **虚拟服务器**。

2. 选择之前选择的虚拟服务器，然后单击 **编辑**。



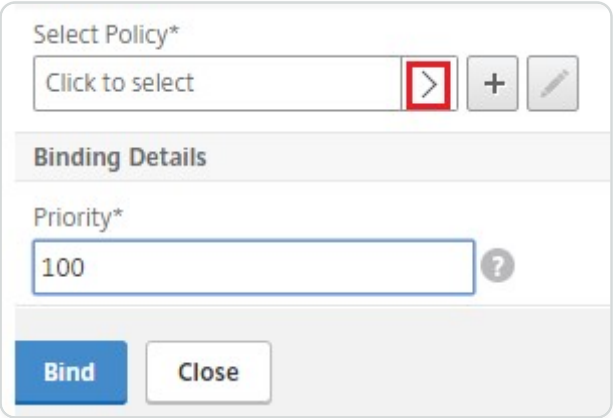
3. 在 **高级设置** 下单击 **登录方案**。

4. 单击 **登录方案** 以绑定。



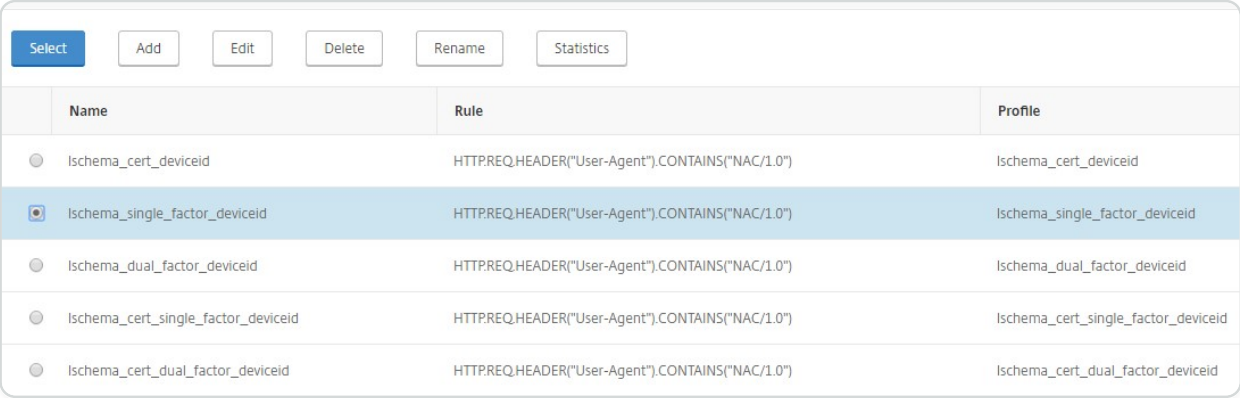
5. 单击 以选择并绑定用于 NAC 设备检查的现有内置登录方案策略。

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

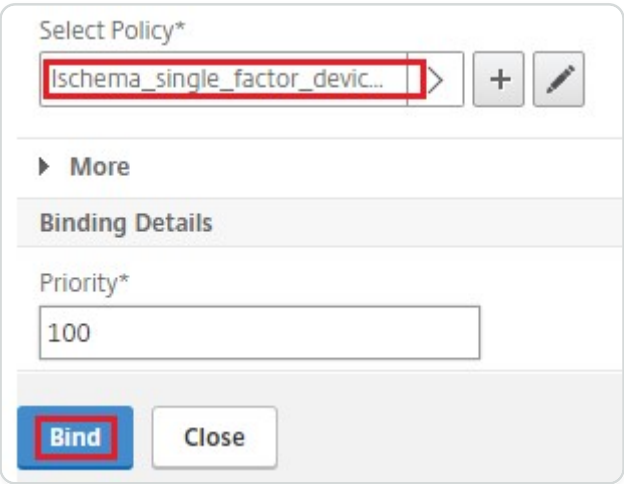


6. 选择适合您的身份验证部署所需的登录架构策略，然后单击 **Select**。

   在前面解释的部署中，使用了单因素身份验证 (LDAP) 以及 NAC OAuth 操作策略。因此，选择了 **lschema_single_factor_deviceid**。

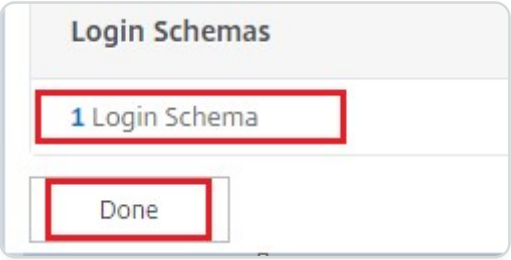


7. 单击 **Bind**。



8. 单击 **Done**。

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



Intune NAC v2 API 支持

作为 Intune NAC v2 API 支持的一部分，您必须绑定一个证书颁发机构文件（CA 证书），以确保 NetScaler 设备从移动设备获取有效证书。在 Intune NAC v2 中，移动设备将设备 ID 作为 CA 证书的一部分发送。此处绑定的 CA 证书必须是用于向最终用户 iOS 和 Android 设备颁发客户端证书的证书。如果存在中间证书，也必须在此处绑定。

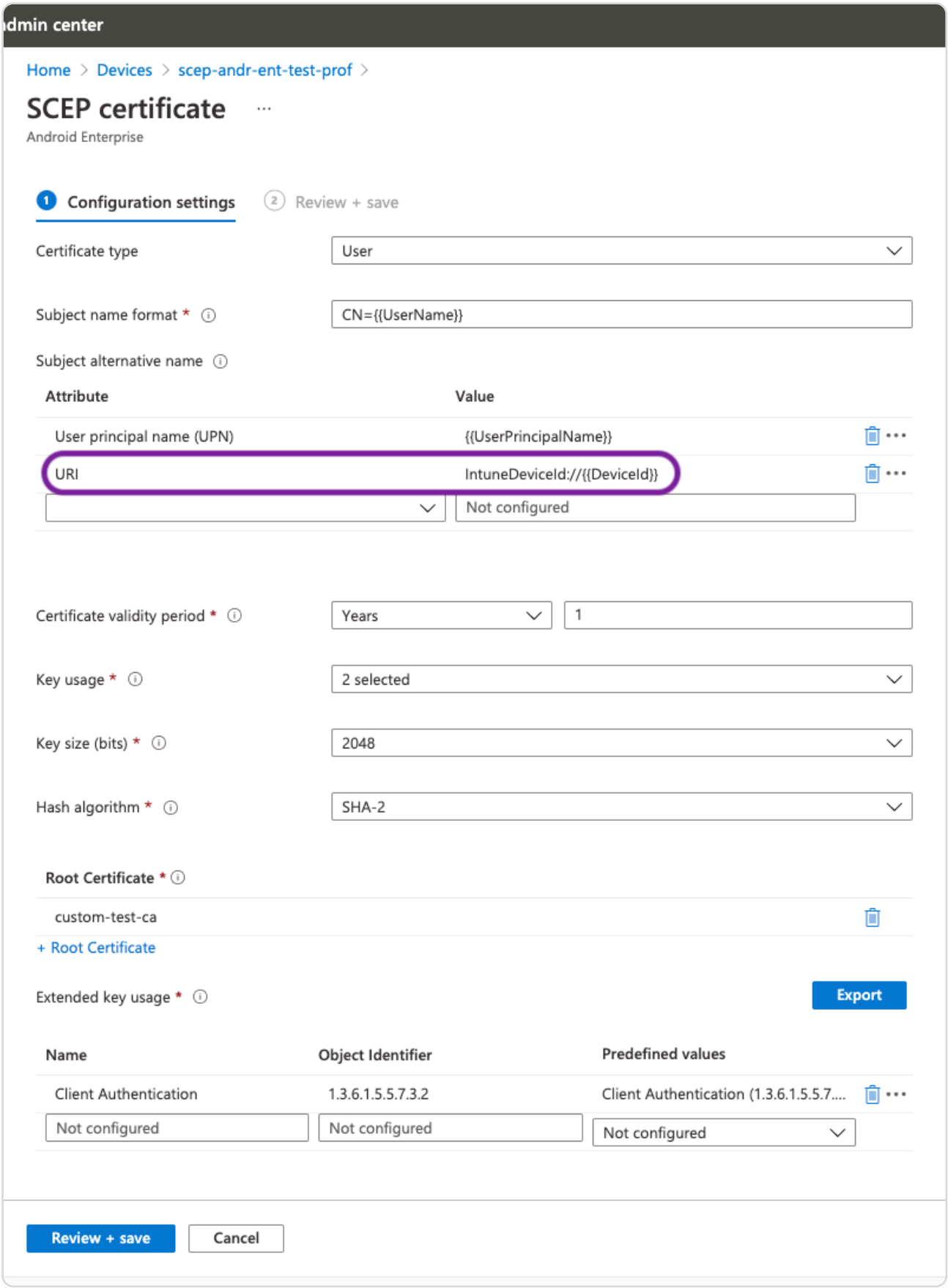
您可以使用以下示例命令来绑定您的 CA 证书。

```
bind ssl vserver intune_nac_check_443 -certkeyName clientca -CA -ocspCheck
Optional
```

重要提示：

- Intune NAC v2 API 支持在 NetScaler Gateway 13.1 build 12.50 或更高版本以及 13.0 build 84.11 或更高版本中可用。
- 您必须通过将 `clientAuth` 设置为 ENABLED 并将 `clientCert` 设置为 OPTIONAL 来在 VPN 和身份验证虚拟服务器上启用基于客户端证书的身份验证。`clientCert` 参数设置为 OPTIONAL，以便不需要 Intune NAC 检查的其他端点可以通过同一虚拟服务器进行身份验证，而无需提供客户端证书。Android 和 iOS 设备必须提供客户端证书。否则，Intune NAC 检查将失败。
- 您必须确保通过 Intune 在移动设备上配置的客户端证书在 URI 类型的 SAN 字段中包含 Intune 设备 ID，如网络访问控制文档的新 Microsoft Intune 服务中所述。有关详细信息，请参阅 `<https://techcommunity.microsoft.com/t5/intune-customer-success/new-microsoft-intune-service-for-network-access-control/ba-p/2544696>`。URI 值字段的格式必须与下图所示相同。此外，Citrix SSO 应用程序必须使用相同的证书与网关进行身份验证。

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



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

NetScaler Gateway 与 Intune NAC 集成中对强映射证书的支持

从 NetScaler Gateway 14.1 版本 build 47.46 开始，Intune NAC 集成支持强映射证书。此增强功能使 NetScaler Gateway 能够从客户端证书中提取并验证 `IntuneDevcieId`，即使强映射证书中采用 Microsoft 更新后的主题备用名称 (SAN) URI 格式。

NetScaler Gateway 要求为 `IntuneDeviceId` 提取的 SAN URI 满足以下条件：

- 它必须以 `IntuneDeviceId://` 开头。
- 其长度不得超过 4095 个字符。

从 SAN-URI 中提取的 `IntuneDeviceId` 值必须只包含有效字符（不允许使用特殊字符）。

此功能通过支持旧版证书格式来确保向后兼容性，避免对现有配置造成中断，并实现向更新标准的无缝过渡。

故障排除

常见问题

问题	解决方案
打开应用程序时显示“需要添加策略”消息	在 Microsoft Graph API 中添加策略
存在策略冲突	每个应用程序只允许一个策略
您的应用程序无法连接到内部资源	确保防火墙端口正确打开，使用了正确的租户 ID 等

NetScaler Gateway 问题

问题	解决方案
NetScaler Gateway 无法访问 `login.microsoftonline.comandgraph.windows.net`。	从 NS Shell 中，检查您是否能够访问以下 Microsoft 网站：cURL -v -k `<https://login.microsoftonline.com>`。然后，检查 NetScaler Gateway 上是否配置了 DNS。还要检查防火墙设置是否正确（以防 DNS 请求被防火墙阻止）。

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

配置 OAuthAction 后，ns.log 中出现错误。	检查 Intune 许可是否已启用，以及 Azure 网关应用程序是否已设置正确的权限。
`Sh OAuthAction` 命令未显示 OAuth 状态为“完成”。	检查 Azure 网关应用程序上的 DNS 设置和已配置的权限。
Android 或 iOS 设备未显示双重身份验证提示。	检查双因素设备 ID 登录方案是否已绑定到身份验证虚拟服务器。

NetScaler Gateway OAuth 状态和错误条件

状态	错误条件
AADFORGRAPH	密钥无效、URL 未解析、连接超时
MDMINFO	`*manage.microsoft.com` 已关闭或无法访问
GRAPH	Graph 端点已关闭或无法访问
CERTFETCH	无法与“令牌端点: `<https://login.microsoftonline.com>`”通信，因为存在 DNS 错误。要验证此配置，请转到 Shell 提示符并键入 cURL `<https://login.microsoftonline.com>`。此命令必须验证。

注意：当 OAuth 状态成功时，状态显示为 COMPLETE。

Intune 配置检查

确保在 **Citrix SSO 的基本 iOS VPN 配置 > 启用网络访问控制 (NAC)** 中选中 **我同意** 复选框。否则，NAC 检查将不起作用。

在 Azure 门户上配置 NetScaler Gateway 应用程序

以下部分列出了在 Azure 门户上配置 NetScaler Gateway 应用程序的步骤。

先决条件

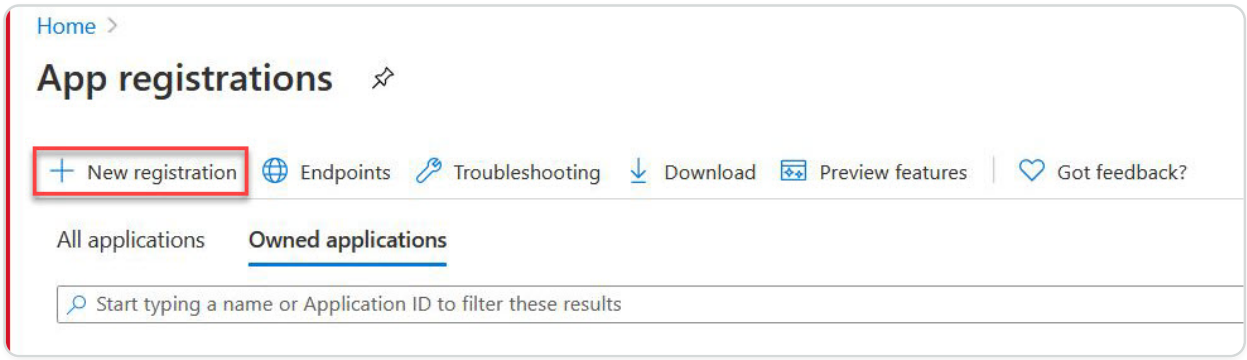
- Azure 全局管理员凭据
- Intune 许可已启用
- 对于 Intune 集成，您必须在 Azure 门户上创建 NetScaler Gateway 应用程序。

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

- 创建 NetScaler Gateway 应用程序后，使用以下应用程序特定信息在 NetScaler Gateway 上配置 OAuth 策略：
  - 客户端 ID / 应用程序 ID
  - 客户端密钥 / 应用程序密钥
  - 微软 Entra 租户 ID
- NetScaler Gateway 使用应用程序客户端 ID 和客户端密钥与 Azure 通信并检查 NAC 合规性。

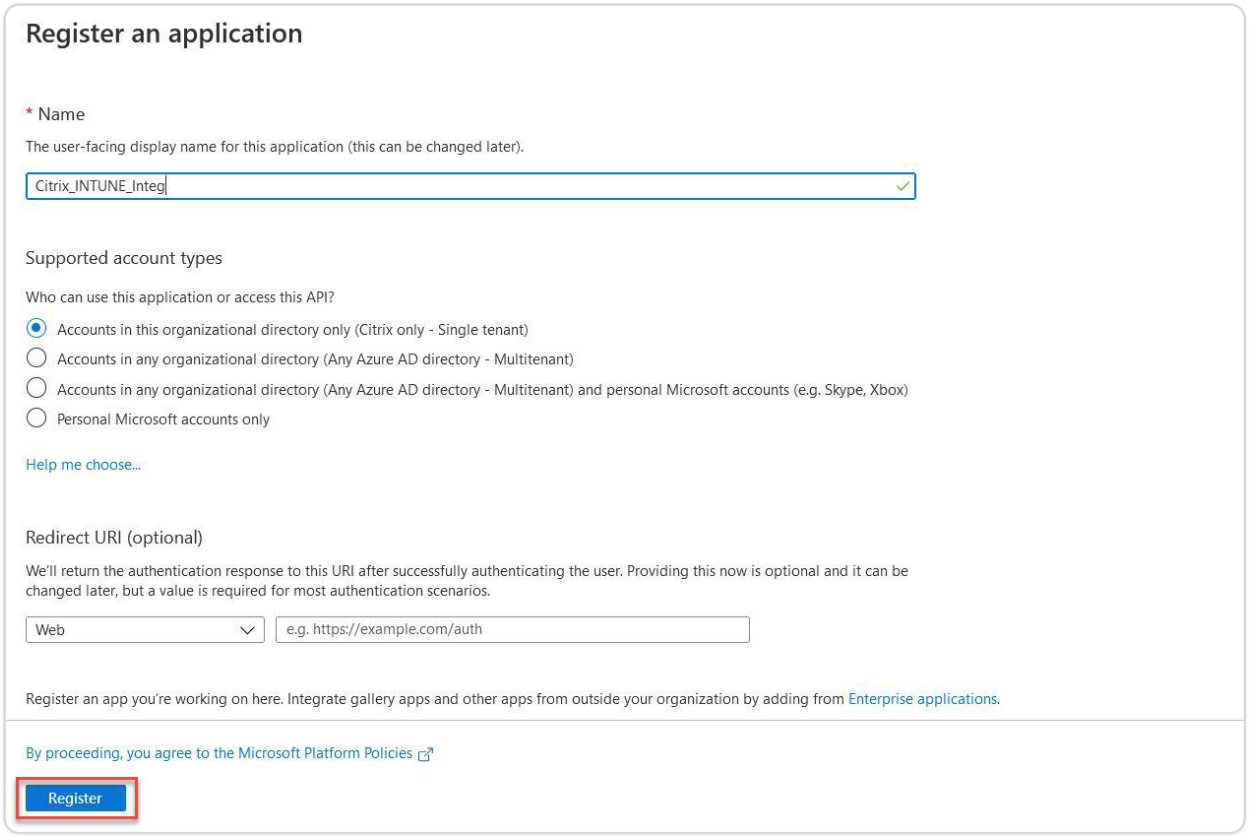
在 Azure 上创建 NetScaler Gateway 应用程序

1. 登录 portal.azure.com
2. 单击 **微软 Entra ID**。
3. 单击 **应用注册**，然后单击 **新注册**。

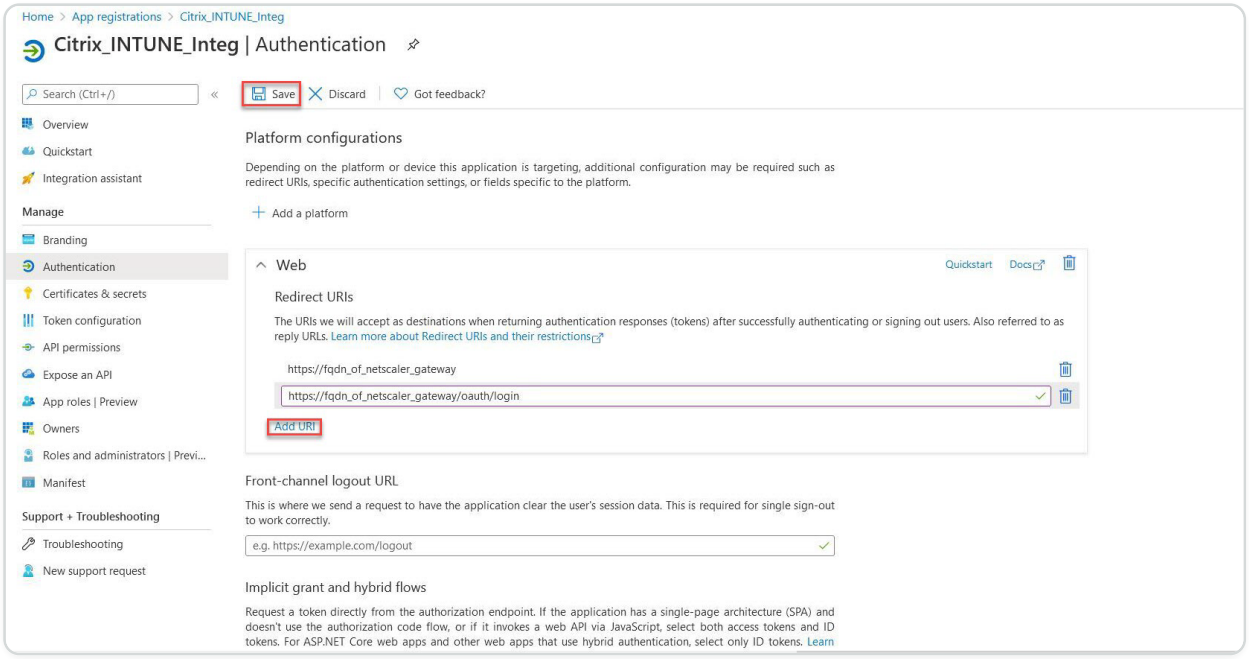


4. 在“**注册应用程序**”页面上，输入应用程序名称，然后单击“**注册**”。

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

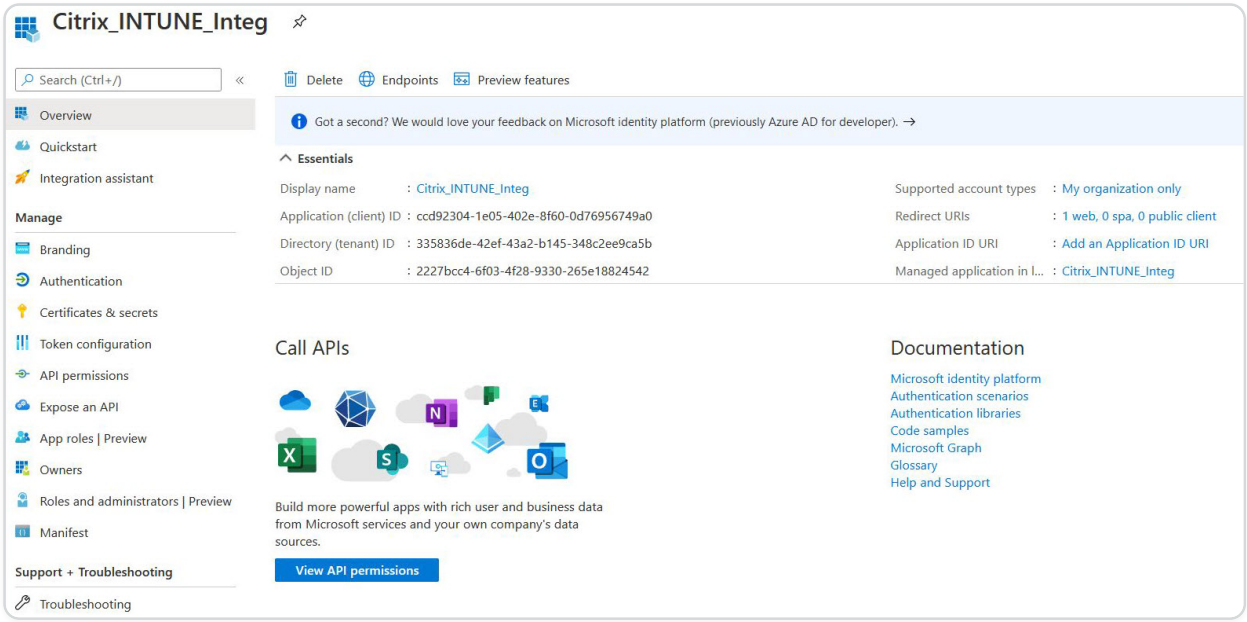


5. 导航到“**身份验证**”，单击“**添加 URI**”，输入 NetScaler Gateway 的 FDQN，然后单击“**保存**”。

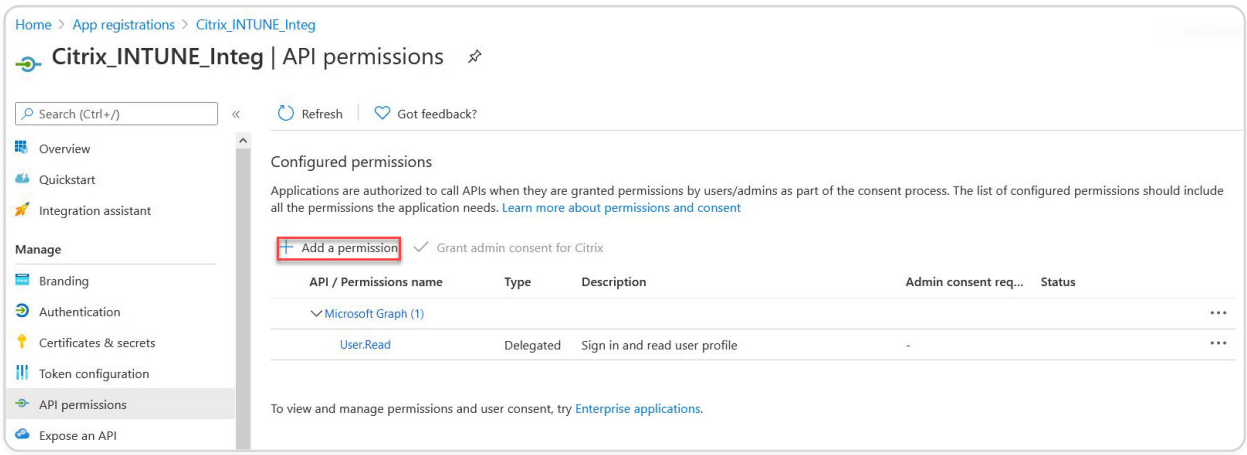


6. 导航到“**概述**”页面以获取客户端 ID、租户 ID 和对象 ID。

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



7. 导航到“**API 权限**”，然后单击“**添加权限**”。



注意：

所有调用 `https://login.microsoftonline.com`、`https://graph.microsoft.com` 或 `https://graph.windows.net` 服务端点的 Microsoft Entra ID 应用程序都需要分配 API 权限，以便网关能够调用 NAC API。可用的 API 权限包括：

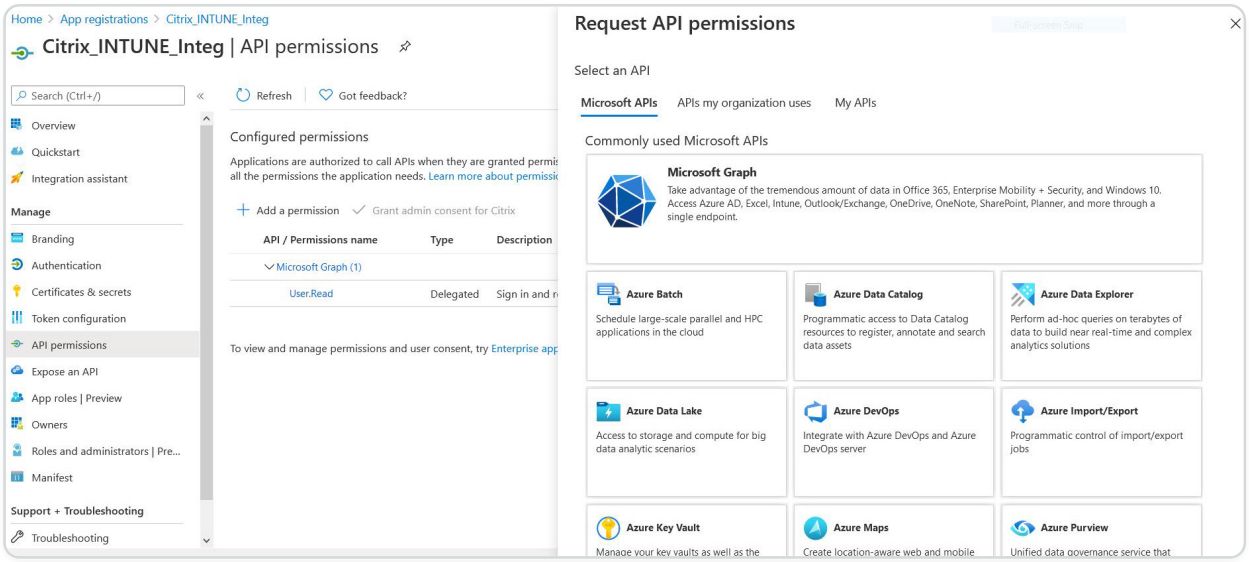
- Application.Read.All
- Application.ReadWrite.All
- Application.OwnedBy
- Directory.Read.All

首选权限是 **Application.Read.All**。

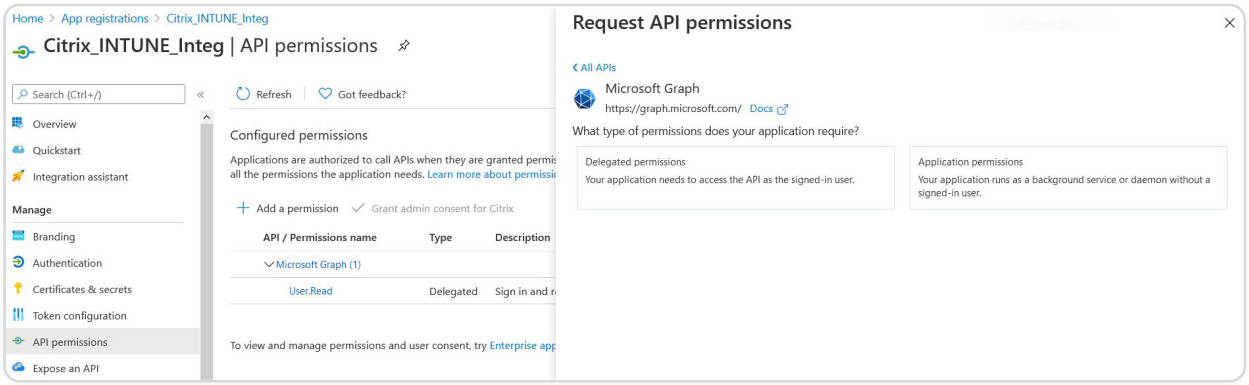
© 1997–2026 Citrix Systems, Inc. All rights reserved.

有关更多详细信息，请参阅 `<https://techcommunity.microsoft.com/t5/intune-customer-success/support-tip-intune-service-discovery-api-endpoint-will-require/ba-p/2428040>`

8. 单击 **Microsoft Graph** 磁贴以配置 Microsoft Graph 的 API 权限。



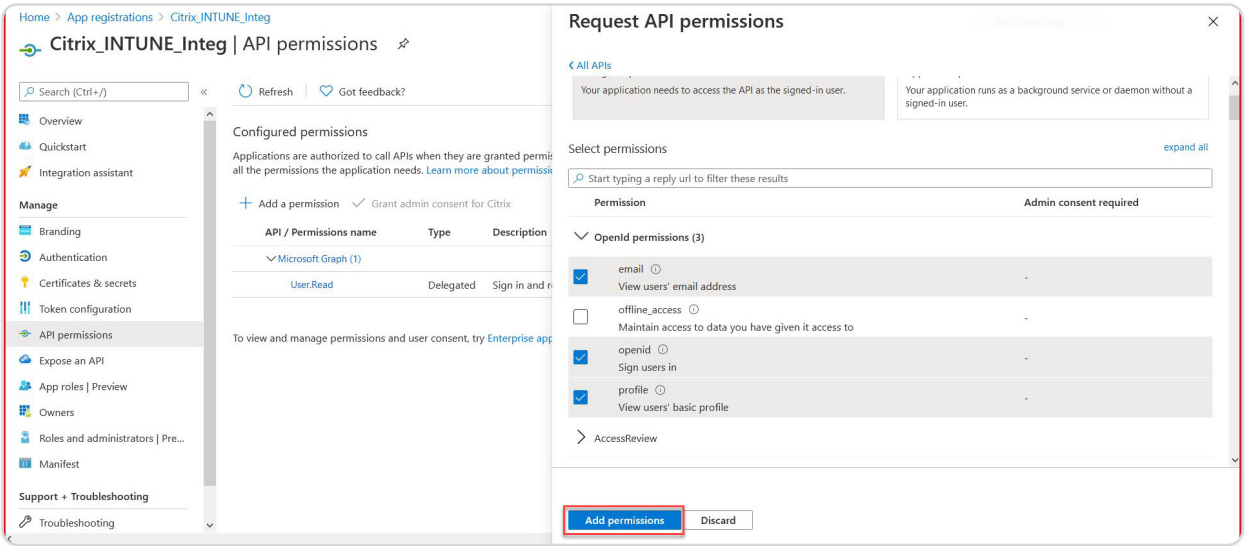
9. 单击 **Delegated permissions** 磁贴。

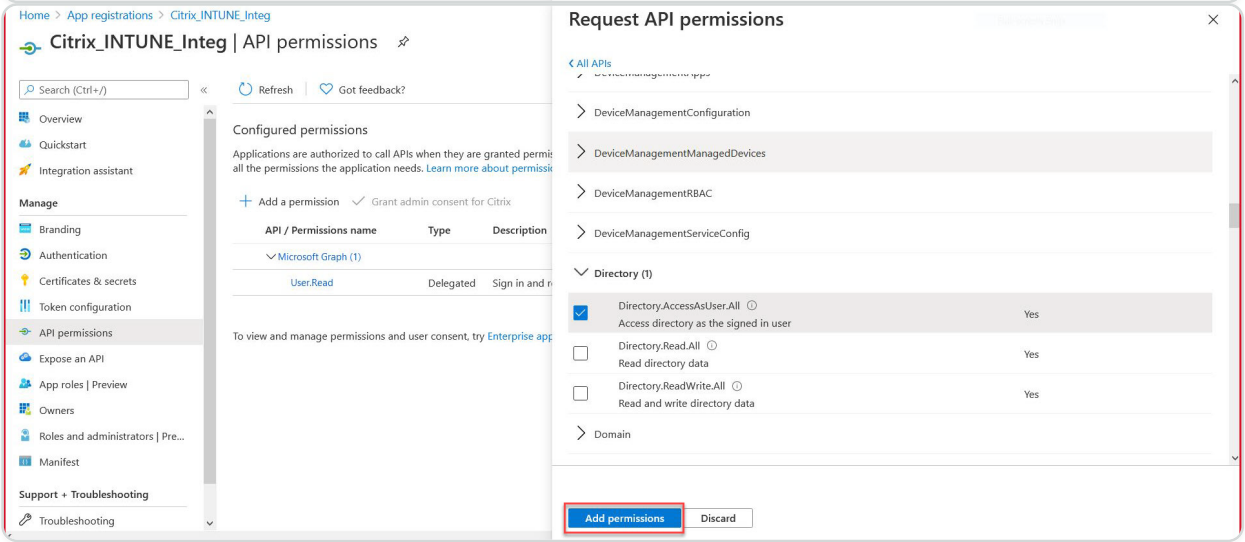


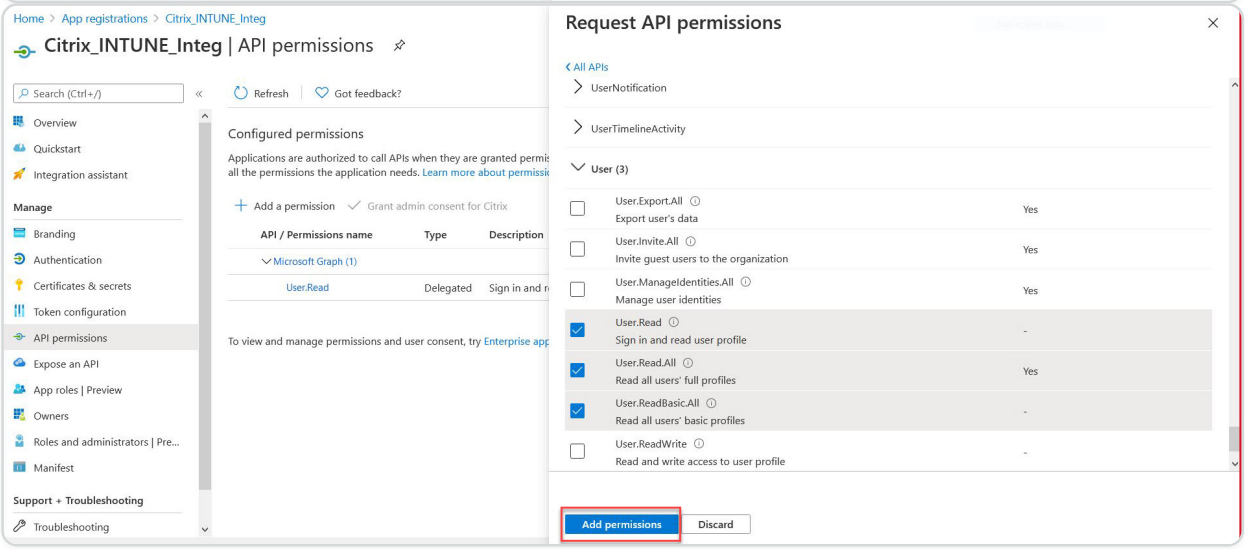
10. 选择以下权限，然后单击 **Add permissions**。

    - 电子邮件
    - `openid`
    - 配置文件
    - Directory.AccessAsUser.All
    - User.Read
    - User.Read.All
    - User.ReadBasic.All

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







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

INTUNE NAC 检查的权限：

所有调用 `https://login.microsoftonline.com`、`https://graph.microsoft.com` 或 `https://graph.windows.net` 服务端点的 Microsoft Entra ID 应用程序都需要分配 API 权限，以便网关能够调用 NAC API。可用的 API 权限包括：

- Application.Read.All
- Application.ReadWrite.All
- Application.OwnedBy
- Directory.Read.All

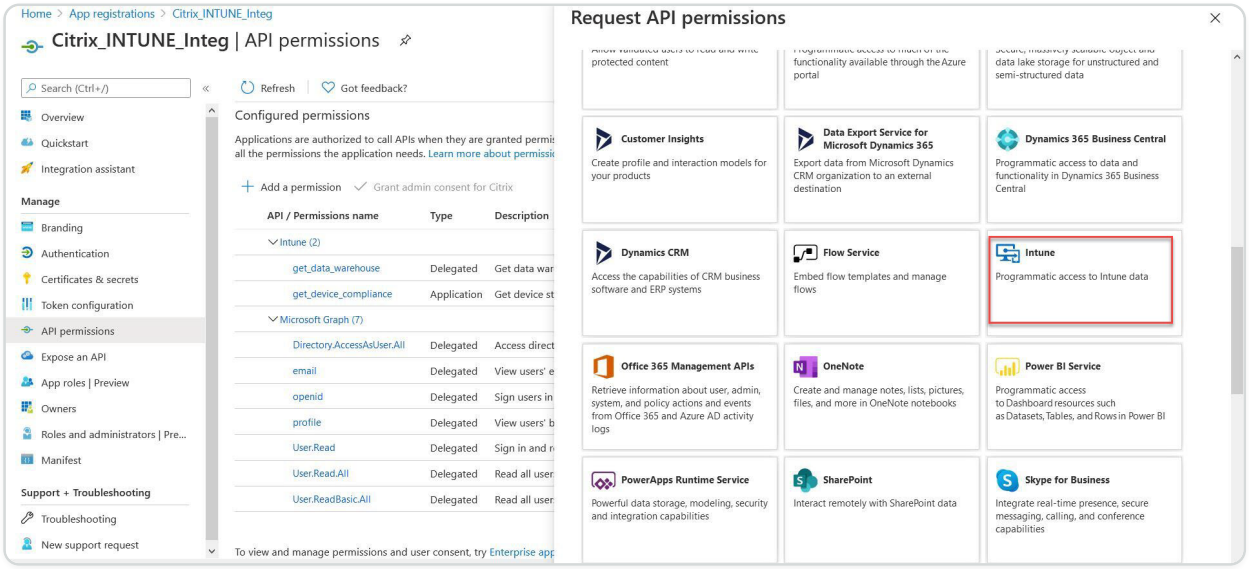
首选权限是 **Application.Read.All**。

有关更多详细信息，请参阅 `<https://techcommunity.microsoft.com/t5/intune-customer-success/support-tip-intune-service-discovery-api-endpoint-will-require/ba-p/2428040>`

注意：

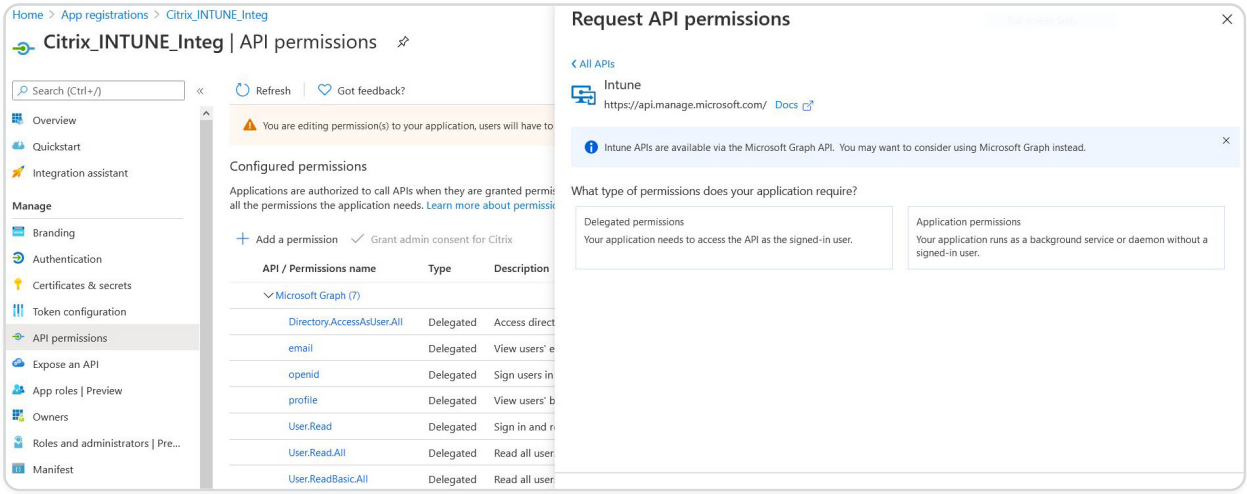
如果客户仅将 Intune Action 用于 NAC 检查，则唯一需要的权限是 Microsoft Graph 中的 **Application.Read.All**。

11. 单击“**Intune**”磁贴以配置 Intune 的 API 权限。



12. 单击“**应用程序权限**”磁贴和“**委派权限**”磁贴，以分别添加 Get_device_compliance 和 Get_data_warehouse 的权限。

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

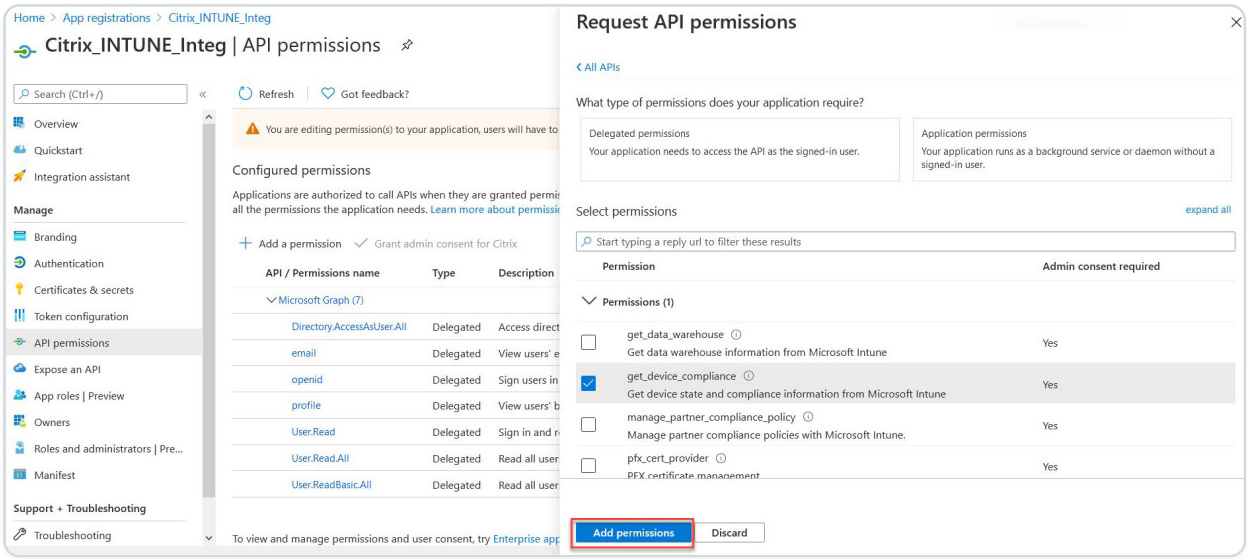


13. 选择以下权限，然后单击 **添加权限**。

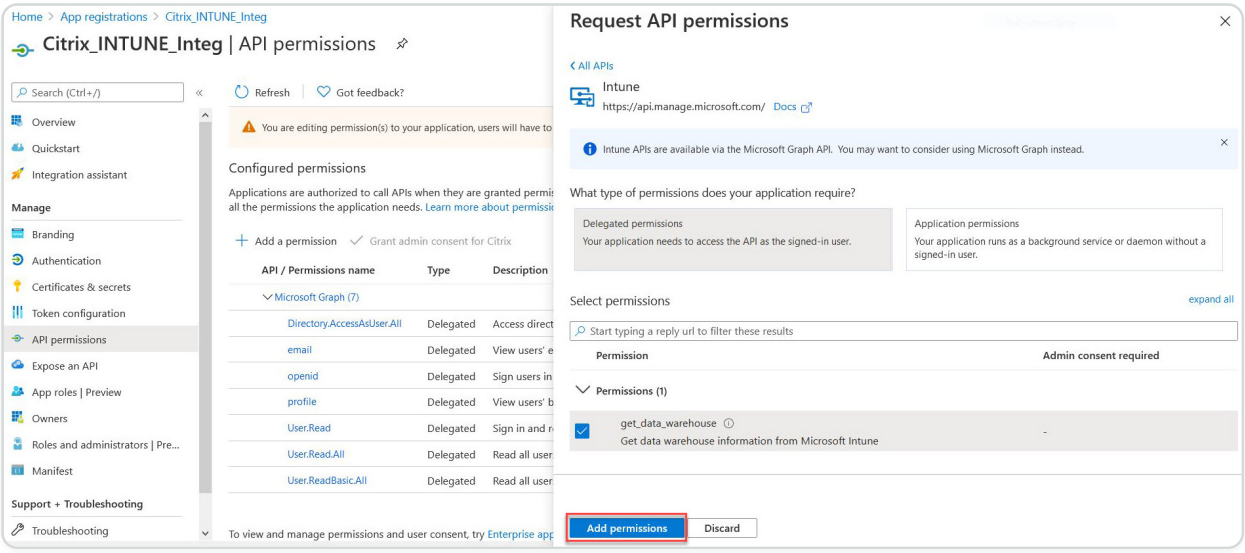
- Get_device_compliance - 应用程序权限
- Get_data_warehouse - 委派权限

注意：

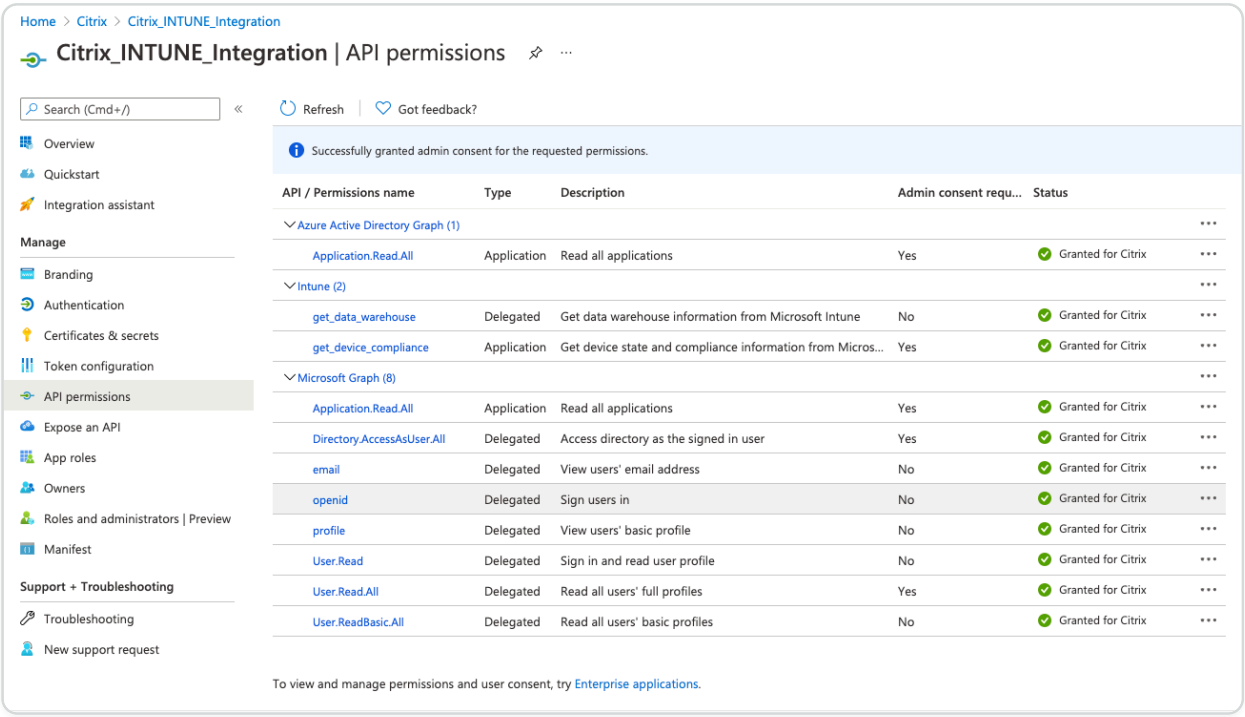
对于 Intune NAC 检查，唯一需要的权限是 **Get_device_compliance**。



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

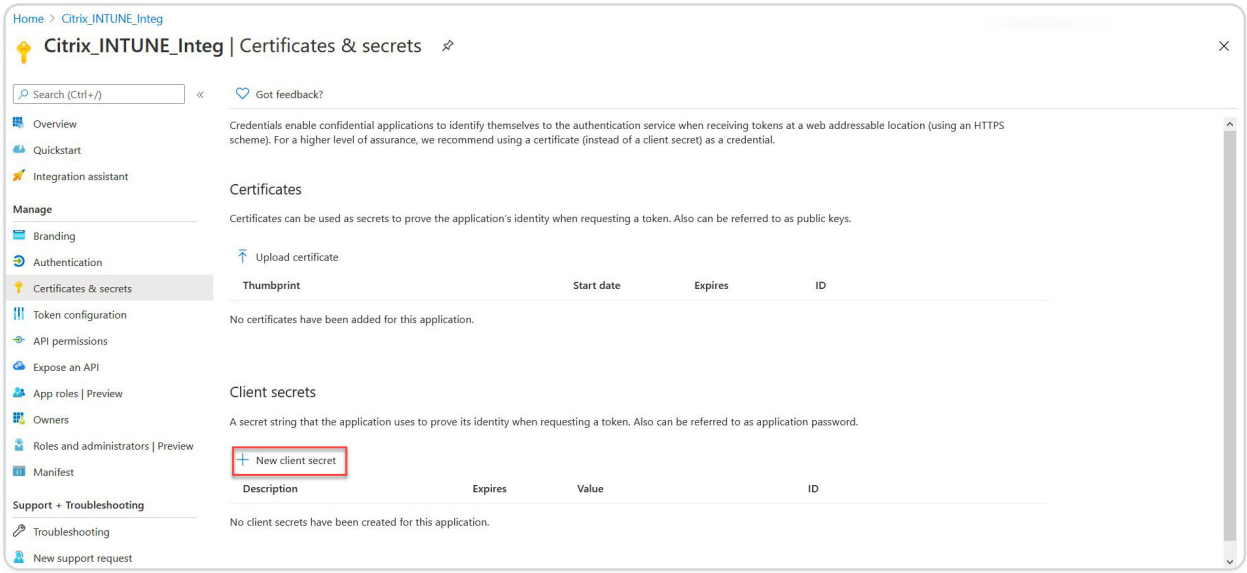


14. 以下页面列出了已配置的 API 权限。

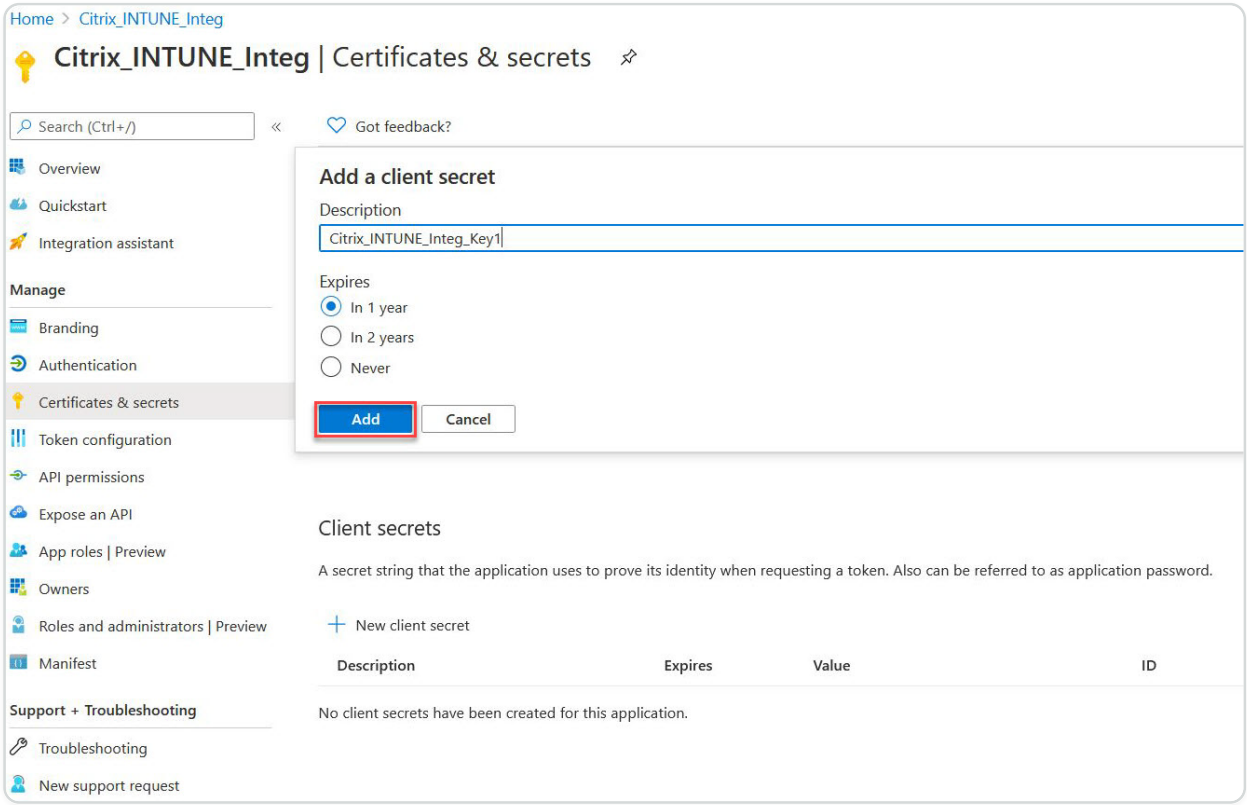


15. 导航到 **证书和机密**，然后单击 **新建客户端密码**。

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



16. 在 **添加客户端密码** 页面下，输入说明，选择过期时间，然后单击 **添加**。

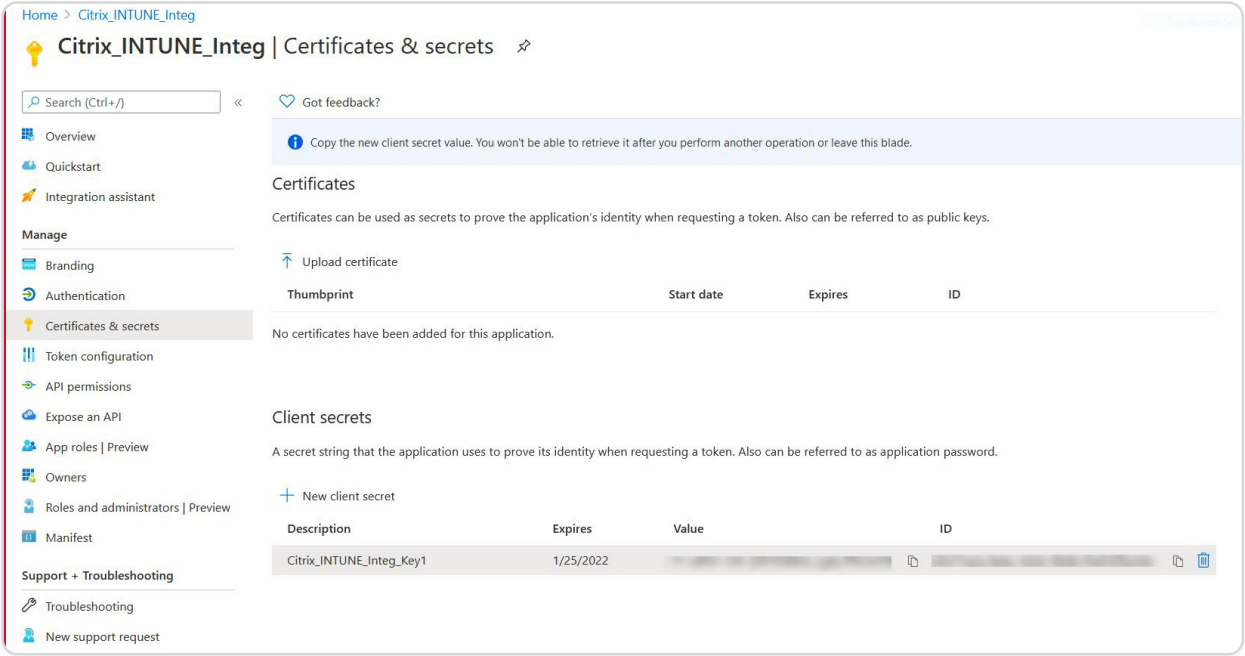


17. 以下屏幕显示已配置的客户端密码。

注意

客户端密钥生成后只显示一次。请将显示的客户端密钥复制到本地。在 NetScaler Gateway 设备上为 Intune 配置 OAuth 操作时，请使用此客户端密钥以及与新注册应用程序关联的客户端 ID。

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



Azure 门户上的应用程序配置现已完成。

理解 MSAL 令牌身份验证

以下是典型的 NetScaler Gateway-MSAL 令牌身份验证中的事件流程：

1. 当应用在 iOS 或 Android 中启动时，应用会联系 Microsoft。系统会提示用户使用用户凭据登录。成功登录后，应用会获取一个 MSAL 令牌。
2. 此 MSAL 令牌会提交给 NetScaler Gateway，该 NetScaler Gateway 已配置为验证 MSAL 令牌。
3. NetScaler Gateway 会使用来自 Microsoft 的相应证书验证 MSAL 令牌的签名。
4. 成功验证后，NetScaler Gateway 会提取用户主体名称 (UPN) 并授予应用对内部资源的 VPN 访问权限。

配置 NetScaler Gateway 虚拟服务器以进行 MSAL 令牌身份验证

要配置 NetScaler Gateway 虚拟服务器以监控 MSAL 令牌身份验证，您需要以下信息：

- **authorizationEndpoint**：未经验证的用户必须重定向到的端点 URL。NetScaler Gateway 通过添加查询参数（包括客户端 ID）将用户重定向到此 URL。如果未指定此参数，则默认情况下用户将重定向到在 **tokenEndpoint** 中配置的 URL。
- **tokenEndpoint**：NetScaler Gateway 发布 OAuth 令牌以验证其真实性的端点 URL。用户在成功身份验证后可以从授权服务器获取 OAuth 令牌。

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

- **GraphEndpoint**：Graph API 服务的 URL，用于了解企业移动服务 (EMS) 端点。
- **certEndpoint**：包含用于 MSAL 令牌验证的 JSON Web Key (JWK) 的端点 URL。
- **Audience**：应用程序向其发送 MSAL 令牌的 NetScaler 虚拟服务器的 FQDN。
- **Issuer**：Microsoft Entra ID 颁发者的名称。默认情况下会自动填充。
- **TenantID**：用于 MSAL 注册的租户 ID。
- **ClientID**：作为 MSAL 注册的一部分授予 Gateway 应用程序的唯一 ID。
- **ClientSecret**：作为 MSAL 注册的一部分授予 Gateway 应用程序的密钥。
- **ResourceURI**：一个可选参数，用于捕获资源 URI。如果未配置，NetScaler 将使用 Azure 商业资源 URI。

使用 CLI 执行以下步骤：

1. 创建 OAuth 操作。

```
add authentication OAuthAction <oauth_action_name> -OAuthType <INTUNE>
-authorizationEndpoint <authorization_endpoint_fqdn> -tokenEndpoint
<token_endpoint_fqdn> -clientID <client_id_val> -clientSecret
<client_secret_val> -tenantID <tenant_id_value> -GraphEndpoint
<graph_endpoint_fqdn> -CertEndpoint <cert_endpoint_fqdn>
```

2. 将身份验证策略标签添加到 OAuth 操作。

```
add authentication policylabel <policy_label_name>
```

3. 创建一个身份验证策略，并将其与新创建的 OAuth 操作关联。

```
add authentication Policy <policy_name> -rule <true> -action
<oauth_intune_action>
```

4. 将身份验证策略绑定到策略标签。

```
bind authentication policylabel <policy_label_name> -policyName
<policy_name> -priority 100
```

5. 配置身份验证虚拟服务器。

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

```
add authentication vserver <authvserver> SSL <0.0.0.0>

bind ssl vserver <authvserver> -certkeyName <cert_key_file_name>

bind authentication vserver <authvserver> -policy <ldap_policy_name>
-priority 100 -nextFactor <policy_label_name>
```

6. 配置 VPN 虚拟服务器。

```
add authentication authnProfile <vpn_profile_name> -authnVsName
<authvserver>

add vpn vserver <vserver_name> SSL <vpn_ip_address> -authnProfile
<vpn_profile_name>
```

示例配置：

```
add authentication OAuthAction oauth_action_for_NAC -OAuthType INTUNE
-authorizationEndpoint "https://login.microsoftonline.com/
ed10c531-5d7b-4a5c-bb29-564c20480754/oauth2/v2.0/authorize" -tokenEndpoint
"https://login.microsoftonline.com/ed10c531-5d7b-4a5c-bb29-564c20480754/
oauth2/v2.0/token" -clientID 1dc2adc3-0298-4ff5-9bf5-b98852ff58ba
-clientSecret 6zM8Q~b4Hr9wwHEGFla.VDsiMWjvG~PS6PKv7c2m -tenantID
ed10c531-5d7b-4a5c-bb29-564c20480754



add authentication policylabel intune_oauth_pol_label



add authentication Policy oauth_intune_pol -rule true -action
oauth_action_for_NAC



bind authentication policylabel intune_oauth_pol_label -policyName
oauth_intune_pol -priority 100
```

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

```
add authentication vserver av_vs SSL 0.0.0.0

bind ssl vserver av_vs -certkeyName crt_key_file_name

bind authentication vserver av_vs -policy ldap_policy_name -priority 100
-nextFactor intune_oauth_pol_label



add authentication authnProfile vpn_authnprofile -authnVsName av_vs

add vpn vserver vpn_sp SSL VPN_IP_Address 443 -authnProfile
vpn_authnprofile
```

注意：

示例配置中的参数必须根据要求进行修改。在示例配置中：

- `OAuthType`、`clientID`、`clientSecret` 和 `tenantID` 是强制参数。
- 如果用户在创建 OAuth 操作时未配置以下参数，则这些参数将填充默认值：
  - `GraphEndpoint`：`<https://graph.microsoft.com/>`
  - `AllowedTokenAlgorithms`：HS256、RS256、RS512
  - `TokenEndpointAuthMethod`：client_secret_post
  - `GrantType`：代码
- 在 `authorizationEndpoint` 和 `tokenEndpoint` 中使用的 `tenantID` 是 `ed10c531-5d7b-4a5c-bb29-564c20480754`。
- 所使用的 `loginSchema` 是默认方案。根据用例，必须选择适当的登录方案。
- `LDAP` 被选为第一个身份验证因素，`OAuth` 被选为下一个因素，并绑定到身份验证虚拟服务器。这可以根据使用情况进行修改。

为将微 VPN 与 Microsoft Endpoint Manager 结合使用而设置 NetScaler Gateway

Citrix 微 VPN 与 Microsoft Endpoint Management 集成后，您的应用程序可以访问本地资源。有关详细信息，请参阅Citrix 微 VPN 与 Microsoft Endpoint Manager 集成。

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

系统要求

- NetScaler Gateway 版本
  - 13.1
  - 13.0
  - 12.1.50.x 或更高版本
  - 12.0.59.x 或更高版本

  您可以从 NetScaler Gateway 下载页面下载最新版本的 NetScaler Gateway。
- 运行 Windows 7 或更高版本的 Windows 桌面（仅适用于 Android 应用程序打包）
- 微软
  - Microsoft Entra ID 访问权限（具有租户管理员权限）
  - 启用 Intune 的租户
- 防火墙规则
  - 启用防火墙规则，允许 SSL 流量从 NetScaler Gateway 子网 IP 流向 `*.manage.microsoft.com`、`https://login.microsoftonline.com` 和 `https://graph.microsoft.com`（端口 443）
  - NetScaler Gateway 必须能够外部解析上述 URL。

先决条件

- **Intune 环境：** 如果您没有 Intune 环境，请设置一个。有关说明，请参阅 Microsoft Intune 入门页面。
- **Edge 浏览器应用：** Micro VPN SDK 已集成到适用于 iOS 和 Android 的 Microsoft Edge 应用和 Intune 托管浏览器应用中。有关托管浏览器的更多信息，请参阅 使用 Intune 管理 iOS 和 Android 上的 Microsoft Edge 页面。
- **Citrix Endpoint Management™ 授权：** 确保拥有有效的 Citrix Endpoint Management 授权，以便在 Microsoft Edge 移动浏览器（iOS 和 Android）上持续支持 micro VPN SDK。有关更多信息，请联系您的销售、客户或合作伙伴代表。

授予 Microsoft Entra ID 应用程序权限

1. 同意 Citrix 与 Microsoft Entra ID 应用程序进行多租户集成，以允许 NetScaler Gateway 使用 Microsoft Entra 域进行身份验证。Azure 全局管理员必须访问以下 URL 并同意：

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

`<https://login.windows.net/common/adminconsent?client_id=b6a53a76-5d50-499e-beb3-c8dbdad5c40b&redirect_uri=https://www.citrix.com&state=consent>`。

2. 同意 Citrix 与 Microsoft Entra ID 应用程序进行多租户集成，以允许移动应用程序使用 NetScaler Gateway micro VPN 进行身份验证。仅当 Azure 全局管理员将“用户可以注册应用程序”的默认值从“是”更改为“否”时，才需要此链接。 此设置可在 Azure 门户的 **Microsoft Entra ID > 用户 > 用户设置** 下找到。 Azure 全局管理员必须访问以下 URL 并同意（添加您的 租户 ID） `<https://login.microsoftonline.com/[tenant_id]/adminconsent?client_id=9215b80e-186b-43a1-8aed-9902264a5af7>`。

配置 NetScaler Gateway 以用于 micro VPN

要将 micro VPN 与 Intune 结合使用，您必须将 NetScaler Gateway 配置为向 Microsoft Entra ID 进行身份验证。

1. 从 NetScaler 下载页面 下载安装脚本文件。
2. 在脚本文件中，更新以下值：
   - `<NSG_IP>`：要分配给 NetScaler Gateway 虚拟服务器的虚拟 IP 地址。此 IP 地址必须可从您的设备直接或通过 NAT 设备访问。您不能使用现有的 NetScaler Gateway 虚拟服务器。
   - `<ENV_NAME>`：NetScaler Gateway 虚拟服务器的显示名称。
   - `<SERVER_CERT_NAME>`: 将绑定到新 NetScaler Gateway 虚拟服务器的服务器证书的名称。
   - `<AAD_CLIENT_SECRET>`: 使用 `NsgCreateSecret.ps1` PowerShell 脚本生成的客户端密钥值（包含在设置脚本中）。
   - `<AAD_TENANT_ID>`: 存储客户 Microsoft Entra ID 的 Microsoft Entra 租户 ID。您可以从 Microsoft Entra ID 管理控制台获取，或使用 `NsgCreateSecret.ps1` PowerShell 脚本生成。
3. 将所有占位符替换为实际值后，通过在 CLI 中运行以下命令来运行整个脚本：

```
/netscaler/nscli -U :<NetScaler Management Username>:<NetScaler Management Password> batch -f "/var/<NsgCreateScriptFileName>"
```

注意：

确保运行脚本后返回值为 `Done`。

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

4. 现有的 NetScaler Gateway 虚拟服务器不适用于此用例。创建 NetScaler Gateway 虚拟服务器并确保虚拟服务器的状态为 **UP**。有关详细信息，请参阅创建虚拟服务器。

验证 NetScaler Gateway 与 Microsoft 服务的通信

1. 使用 SSL Checker 等在线工具从 Internet 访问新的 NetScaler Gateway 虚拟服务器。这可以确认服务器证书是否正确安装，并验证 Internet 与 DMZ 网络中托管的 NetScaler Gateway 虚拟服务器之间的连接。
2. 使用 SSH 客户端（例如 PuTTY）打开与 NetScaler Gateway 的 SSH 连接。
3. 运行以下命令以检查从 NetScaler Gateway 设备到 Microsoft URL 的出站连接：`https://login.microsoftonline.com`、`*.manage.microsoft.com` 和 `https://graph.microsoft.com`。

   ```
   root@netscaler# curl -s -k https://login.microsoftonline.com

   root@netscaler# curl -s -k https://graph.windows.net

   root@netscaler# curl -s -k https://manage.microsoft.com
   ```

4. 退出 SSH 连接并在 CLI 中运行 `show oauthAction` 命令。`OAuth Status` 必须为 `COMPLETE`。如果看到 `OAuth Status` 不是 `COMPLETE`，请参阅故障排除 部分。

配置 Microsoft Edge 浏览器

1. 登录到 `<https://endpoint.microsoft.com/>`，然后导航到 **Intune > 移动应用**。
2. 像往常一样发布 Edge 应用程序，然后添加应用程序配置策略。
3. 在 **管理** 下，点击 **应用配置策略**。
4. 点击 **添加**，然后输入要创建的策略名称。在 **设备注册类型** 中，选择 **托管应用**。
5. 点击 **关联应用**。
6. 选择要应用策略的应用（Microsoft Edge 或 Intune 托管浏览器），然后点击 **确定**。
7. 点击 **配置设置**。
8. 在 **名称** 字段中，输入下表中列出的其中一个策略的名称。
9. 在 **值** 字段中，输入要应用于该策略的值。点击字段外部以将策略添加到列表中。您可以添加多个策略。
10. 点击 **确定**，然后点击 **添加**。

该策略已添加到您的策略列表中。

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

名称 (IOS/ANDROID)	值	描述
MvpnGatewayAddress	`https://external.companyname.com`	您的 NetScaler Gateway 的外部 URL
MvpnNetworkAccess	Mvpn 网络访问隧道式 WebSSO 或 无限制	MvpnNetworkAccessTunneledWebSSO 是隧道的默认值
MvpnExcludeDomains	逗号分隔的要排除的域名列表	可选。默认值=空白
TunnelExcludeDomains	`app.launchdarkly.com,cis.citrix.com,cis-staging.citrix.com,cis-test.citrix.com,clientstream.launchdarkly.com,crashlytics.com,events.launchdarkly.com,fabric.io,firehose.launchdarkly.com,hockeyapp.net,mobile.launchdarkly.com,pushreg.xm.citrix.com,rttf.citrix.com,rttf-staging.citrix.com,rttf-test.citrix.com,ssl.google-analytics.com,stream.launchdarkly.com`	可选。使用此客户端属性可覆盖默认的排除域列表。

注意：

Web SSO 是设置中安全浏览的名称。其行为相同。

- **MvpnNetworkAccess** - MvpnNetworkAccessTunneledWebSSO 启用通过 NetScaler Gateway 的 HTTP/HTTPS 重定向，也称为隧道式 Web SSO。网关会内联响应 HTTP 身份验证质询，提供单点登录 (SSO) 体验。要使用 Web SSO，请将此策略设置为 **MvpnNetworkAccessTunneledWebSSO**。不支持完全隧道重定向。使用 **Unrestricted** 可关闭微 VPN 隧道。

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

- **MvpnExcludeDomains** - 逗号分隔的主机名或域名列表，这些主机名或域名将从通过 NetScaler Gateway 反向 Web 代理路由中排除。即使 NetScaler Gateway 配置的拆分 DNS 设置可能会选择该域或主机，这些主机名或域名仍将被排除。

  注意：

  - 此策略仅对 **MvpnNetworkAccessTunneledWebSSO** 连接强制执行。如果 `MvpnNetworkAccess` 为 **Unrestricted**，则此策略将被忽略。
  - 此策略仅适用于配置了反向拆分隧道的 NetScaler Gateway 的隧道式 Web SSO 模式。

- **TunnelExcludeDomains** - 默认情况下，MDX 会将某些服务终结点从微 VPN 隧道中排除。移动应用 SDK 和应用使用这些服务终结点来实现各种功能。例如，服务终结点包括不需要通过企业网络路由的服务，例如 Google Analytics、Citrix Cloud™ 服务和 Active Directory 服务。使用此客户端属性可覆盖默认的排除域列表。

  要配置此全局客户端策略，请在 Microsoft Endpoint Management 控制台上，导航到 **Settings > Client Properties**，添加自定义密钥 **TUNNEL_EXCLUDE_DOMAINS**，并设置值。

  值：要将默认列表替换为您要从隧道中排除的域，请键入一个以逗号分隔的域后缀列表。要将所有域都包含在隧道中，请键入 none。默认列表为：

  `app.launchdarkly.com,cis.citrix.com,cis-staging.citrix.com,cis-test.citrix.com,clientstream.launchdarkly.com,crashlytics.com,events.launchdarkly.com,fa hockeyapp.net,mobile.launchdarkly.com,pushreg.xm.citrix.com,rttf.citrix.com,rttf-staging.citrix.com,rttf-test.citrix.com,ssl.google-analytics.com,stream.launchdarkly.com`

故障排除

常见问题

问题	解决方案
打开应用时出现“需要添加策略”消息	在 Microsoft Graph API 中添加策略
存在策略冲突	每个应用只允许一个策略
打包应用时出现“未能打包应用”消息。有关完整消息，请参阅下表	该应用已与 Intune SDK 集成。您无需使用 Intune 包装该应用

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

问题	解决方案
您的应用程序无法连接到内部资源	确保防火墙端口已正确打开，租户 ID 正确，等等

应用程序打包失败错误消息：

应用程序打包失败。com.microsoft.intune.mam.apppackager.utils.AppPackagerException: 此应用程序已集成 MAM SDK。com.microsoft.intune.mam.apppackager.AppPackager.packageApp(AppPackager.java:113) com.microsoft.intune.mam.apppackager.PackagerMain.mainInternal(PackagerMain.java:198) com.microsoft.intune.mam.apppackager.PackagerMain.main(PackagerMain.java:56) 应用程序无法封装。

NetScaler Gateway 问题

问题	解决方案

NetScaler Gateway 无法访问 `login.microsoftonline.com and graph.windows.net`。	从 NS Shell 中，检查您是否能够访问以下 Microsoft 网站：cURL -v -k `<https://login.microsoftonline.com>`。然后，检查 NetScaler Gateway 上是否配置了 DNS。还要检查防火墙设置是否正确（以防 DNS 请求被防火墙阻止）。
配置 OAuthAction 后，ns.log 中出现错误。	检查 Intune 许可是否已启用，以及 Azure 网关应用程序是否已设置正确的权限。
Sh OAuthAction 命令未显示 OAuth 状态为“完成”。	检查 Azure 网关应用程序上的 DNS 设置和已配置的权限。
Android 或 iOS 设备未显示双重身份验证提示。	检查双因素设备 ID 登录方案是否已绑定到身份验证虚拟服务器。

NetScaler Gateway OAuth 状态和错误条件

状态	错误条件
AADFORGRAPH	密钥无效、URL 未解析、连接超时

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

状态	错误条件
MDMINFO	`*manage.microsoft.com` 已关闭或不可达
GRAPH	Graph 终结点已关闭或不可达
CERTFETCH	无法与“令牌终结点: `<https://login.microsoftonline.com>`”通信，因为存在 DNS 错误。要验证此配置，请转到 shell 并键入 cURL `<https://login.microsoftonline.com>`。此命令必须验证。

注意：

当 OAuth 状态成功时，状态显示为 COMPLETE。

最新的 OAuth 网络访问控制 (NAC) 服务终结点

从版本 14.1 build 29.x 开始，VPN 虚拟服务器支持最新的 OAuth NAC 服务终结点。此支持可实现端到端 MDM 功能。

以下是 NAC 服务终结点的 CLI 配置示例：

```
add authentication OAuthAction &lt;oauth_action_for_NAC> -OAuthType INTUNE
-authorizationEndpoint "https://login.microsoftonline.com/
&lt;ed10c590-5d7b-4a5c-bb29-564c20480756>/oauth2/v2.0/authorize"
-tokenEndpoint "https://login.microsoftonline.com/&lt;ed10c590-5d7b-4a5c-
bb29-564c20480756>/oauth2/v2.0/token" -clientID <1dc2adc3-0298-4ff5-9bf5-
b98852ff58ba> -clientSecret <6zM8Q~b4Hr9wwHEGFVDsiMWjvG~IS6PKv2m>
-tenantID &lt;ed10c590-5d7b-4a5c-bb29-564c20480756> -GraphEndpoint
"https://graph.microsoft.com" -refreshInterval 1440 -grantType CODE
-authentication DISABLED -allowedAlgorithms HS256 RS256 RS512 -PKCE
ENABLED -tokenEndpointAuthMethod client_secret_post
```

有关更多信息，请参阅 OAuth 身份验证。

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

Azure AD Graph 的扩展支持

由于 Azure AD Graph 已弃用，触发新应用程序的客户无法使用以前通过 Azure AD Graph 提供的权限。但是，拥有现有应用程序并希望在一段时间内继续使用 Azure AD Graph 旧权限的客户，可以通过对网关设备进行一些配置更改来继续这样做。此配置在 NetScaler Gateway 13.1-27.xx 及更高版本中受支持。

在 NetScaler Gateway 设备上执行以下配置更改：

1. 在命令提示符下，运行以下命令。

   ```
   shell nsapimgr_wr.sh -ys call=”ns_intune_enable_old_endpoints”
   ```

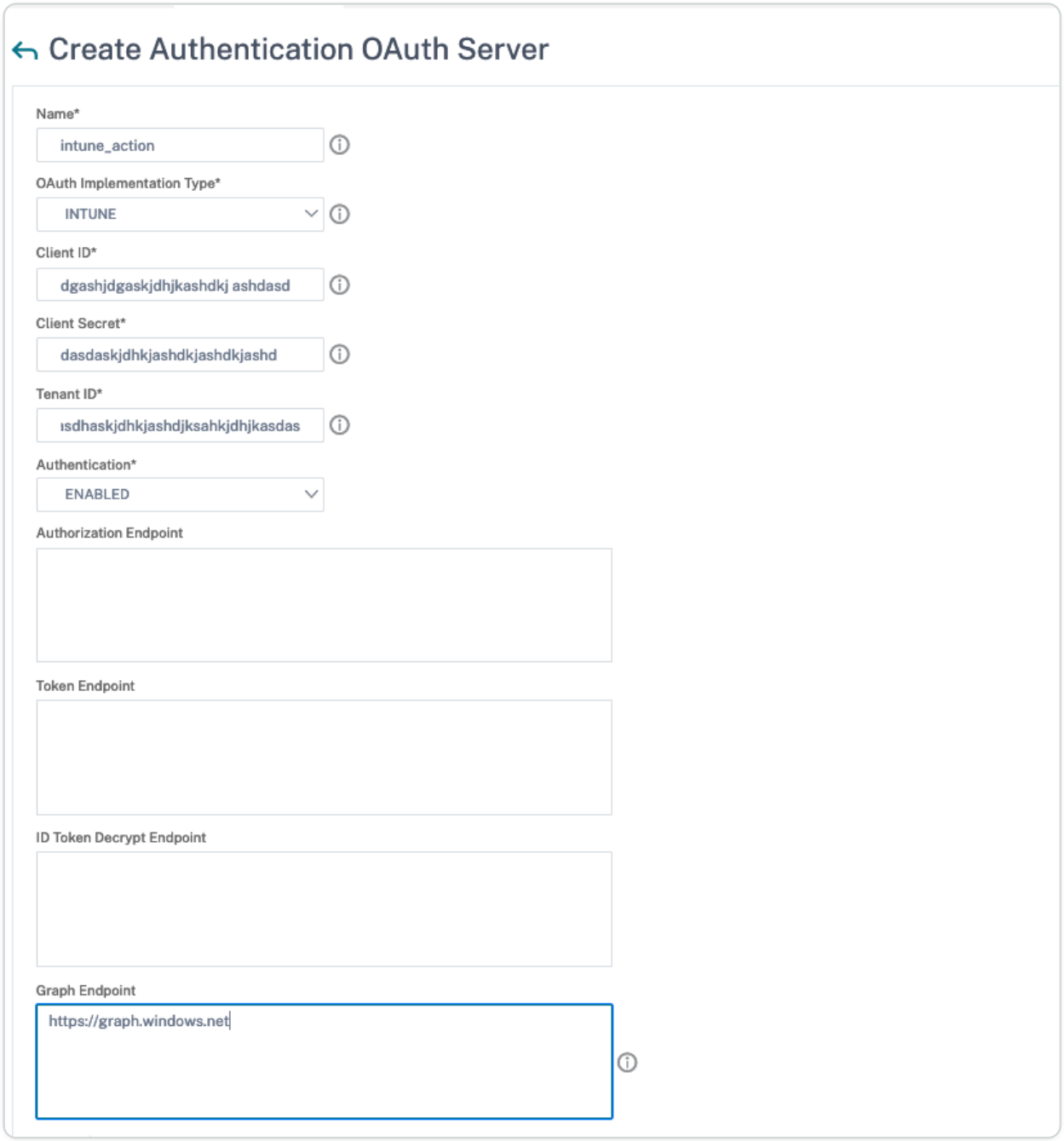
2. 导航到 **安全 > AAA-应用程序流量 > 策略 > 身份验证 > 高级策略 > 操作 > OAUTH 操作**。

   a. 选择现有 OAuth 服务器。

   b. 单击 **More**。

   c. 在 **Graph Endpoint** 中，确保 URL 与图中显示的 URL 相同。

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



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

HDX™ 智能数据传输支持

NetScaler Gateway 对智能数据传输 (EDT) 的支持，确保了运行 Citrix Workspace 应用程序的用户获得高清的虚拟桌面会话内用户体验。

此外，还促进了 Citrix Workspace 应用程序和 VDA 之间使用 DTLS 1.0 进行 EDT 终止的端到端加密。有关更多信息，请参阅 支持 DTLS 协议。

启用 EDT 的 NetScaler Gateway 在 LAN 和 WAN 条件下均可提供良好的用户体验。借助 EDT，在从一种网络漫游到另一种网络时，您无需进行任何管理或用户配置。此优势在高延迟且存在中等数据包丢失的网络中最为明显，在这些网络中，使用其他替代方案时用户体验通常会滞后。

何时使用 Enlightened Data Transport 支持

以下场景说明了启用 EDT 的 NetScaler Gateway 的使用。

- 用户在远程访问业务资源时，希望获得与 LAN 环境中一样好的体验。
- 用户希望在 Wi-Fi 和蜂窝网络上获得丰富的虚拟应用程序和桌面用户体验，即使网络质量因拥塞、高数据包丢失和高延迟而较差。

使用 EDT 时，需要牢记以下几点。

- 虚拟服务器级别的 DTLS 开关默认启用。
- 不支持带 DTLS 的 IPv6。
- 设备现在可以配置为在 Receiver 和 VDA 之间对 EDT 流量使用双跳功能。有关详细信息，请单击在双跳 DMZ 中部署。

注意： EDT 在 12.1 build 49.xx 及更高版本中支持 MPX FIPS 平台。在基于 Intel Coleto SSL 芯片的 MPX 设备上，EDT 从 12.1 build 51.16 及更高版本开始支持。

配置 NetScaler 网关以支持智能数据传输

通过 Gateway 的 EDT 流量现在具有端到端的可视性。实时和历史可见性数据的可用性使 NetScaler ADM 能够支持各种用例。

支持以下场景：

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

场景	EDT 支持
NetScaler 网关	是
带高可用性 (HA) 的 NetScaler Gateway	是
带高可用性 (HA) 优化的 NetScaler Gateway	是
带统一网关的 NetScaler	是
带 GSLB 的 NetScaler Gateway	是
NetScaler Gateway 群集	是
Citrix Workspace 应用程序到 NetScaler Gateway DTLS 加密	是
NetScaler Gateway 上的双重安全票证颁发机构 (STA)	是
NetScaler Gateway ICA 会话超时	是
NetScaler Gateway 多流 ICA	否
NetScaler Gateway 会话可靠性（端口 2598）	是
NetScaler Gateway 双跳	是
NetScaler 到 VDA DTLS 加密	是
HDX 洞察	是
IPv6 模式下的 NetScaler Gateway	否
NetScaler Gateway SOCKS（端口 1494）	否
NetScaler 纯 LAN 代理（请参阅注释）	否

注意：

如果 NetScaler LAN 代理配置为 LAN 用户模式或透明模式，则不支持 EDT。但是，支持 TCP。有关详细信息，请参阅配置出站 ICA 代理。

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

配置 NetScaler 网关以支持增强数据传输

如果使用 Enlightened Data Transport (EDT)，则必须启用数据报传输层安全性 (DTLS) 来加密 EDT 使用的 UDP 连接。必须在 Gateway VPN 虚拟服务器级别启用 DTLS 参数。此外，必须正确升级和配置 Citrix Virtual Apps and Desktops 组件，以实现 Gateway VPN 虚拟服务器与用户设备之间的加密流量。

注意：

必须在 DMZ 中打开为 NetScaler Gateway 前端虚拟服务器配置的 UDP 端口（例如端口 443），以便虚拟服务器接收 DTLS 连接。DTLS 和 CGP 是 EDT 与 NetScaler Gateway 兼容的先决条件。

使用 GUI 配置 NetScaler Gateway 以支持 EDT

1. 部署和配置 NetScaler Gateway 以与 StoreFront 通信并对 Citrix Virtual Apps and Desktops 的用户进行身份验证。
2. 在 NetScaler GUI 的“Configuration”（配置）选项卡上，展开 **NetScaler Gateway**，然后选择 **Virtual Servers**（虚拟服务器）。

   虚拟服务器页面(/en-us/netscaler-gateway/media/spyder_2.jpg)
3. 单击 **Edit**（编辑）以显示 VPN 虚拟服务器的“Basic Settings”（基本设置），然后验证 DTLS 设置的状态。

   编辑 DTLS 设置(/en-us/netscaler-gateway/media/spyder_3.jpg)
4. 单击 **More**（更多）以显示其他配置选项。

   查看其他设置(/en-us/netscaler-gateway/media/spyder_4.jpg)
5. 选择 **DTLS** 以提供数据报协议的通信安全。单击 **OK**（确定）。VPN 虚拟服务器的“**Basic Settings**”（基本设置）区域显示 DTLS 标志设置为 **True**。

   启用 DTLS(/en-us/netscaler-gateway/media/spyder_5.jpg)

使用 CLI 配置 NetScaler Gateway 以支持 EDT

```
set vpn vserver vs1 -DTLS ON
```

配置音频的容损模式

从版本 14.1 build 34.42 开始，NetScaler Gateway 支持 Citrix Virtual Apps and Desktops 中音频的容损模式。此模式可增强连接到高延迟和数据包丢失网络的用户的音频体验。用户必须使用 Citrix Virtual Apps and Desktops 7 2402 LTSR 或更高版本才能使用此功能。

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

音频的容损模式基于 EDT 容损传输协议，该协议允许在传输过程中丢失数据包而无需重新发送多媒体内容，从而为用户带来更实时的体验。在有损网络条件下，它是音频的首选模式，可确保与 EDT 相比具有卓越的音频质量。

默认情况下，NetScaler Gateway 上禁用音频的容损模式。

重要提示：

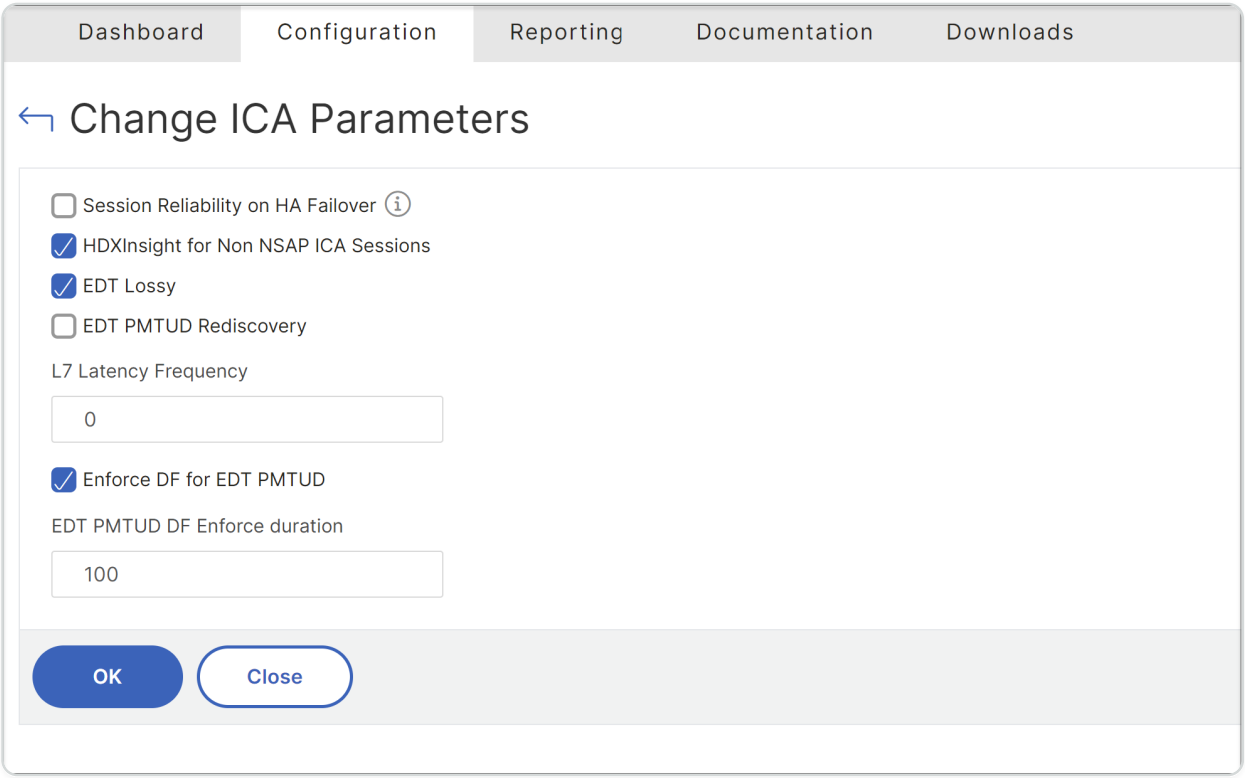
在将 NetScaler Gateway 升级到版本 14.1-43.50 之前，您必须禁用音频的容损模式，以避免丢失 ICA 参数配置。升级后，配置 **EDT Loss Tolerant** 参数以启用容损模式。

使用 GUI 配置 NetScaler Gateway 以启用容损模式

1. 导航到 **系统** > **设置** > **更改 ICA® 参数**。
2. 选择 **EDT Lossy** 以启用容损模式。

注意：

从 NetScaler Gateway 14.1-43.50 版本开始，ICA 参数 **EDT Lossy** 已重命名为 **EDT Loss Tolerant**。



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

使用 CLI 配置 NetScaler Gateway 以启用容损模式

在命令提示符下，输入以下命令以启用容损模式：

```
set ica parameter -EDTLossy ENABLED
```

注意：

从 NetScaler Gateway 14.1-43.50 版本开始，输入以下命令以启用容损模式：

```
set ica parameter -edtlosstolerant ENABLED
```

配置 NetScaler Gateway 以支持 HDX Insight

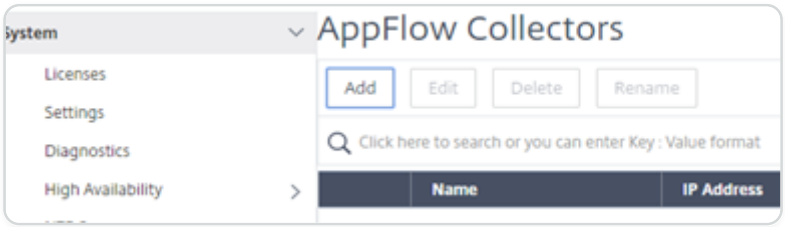
HDX Insight 为通过 NetScaler 的虚拟应用程序和桌面 HDX 流量提供端到端可见性。它还使管理员能够查看实时客户端和网络延迟指标、历史报告、端到端性能数据以及排查性能问题。

使用 GUI 配置 NetScaler Gateway 以支持 HDX Insight

注意：

- 本节适用于 NetScaler Gateway 14.1-51.x 及更早版本。
- 从 NetScaler Gateway 14.1 版本 56.x 开始，HDX Insight 数据将传输到 Citrix Director，无需配置 **AppFlow** 策略。管理员只需在 Delivery Controller 或 Citrix Studio 上启用**网络遥测**策略即可将 HDX Insight 数据传输到 Citrix Director。有关启用策略的详细信息，请参阅创建策略。

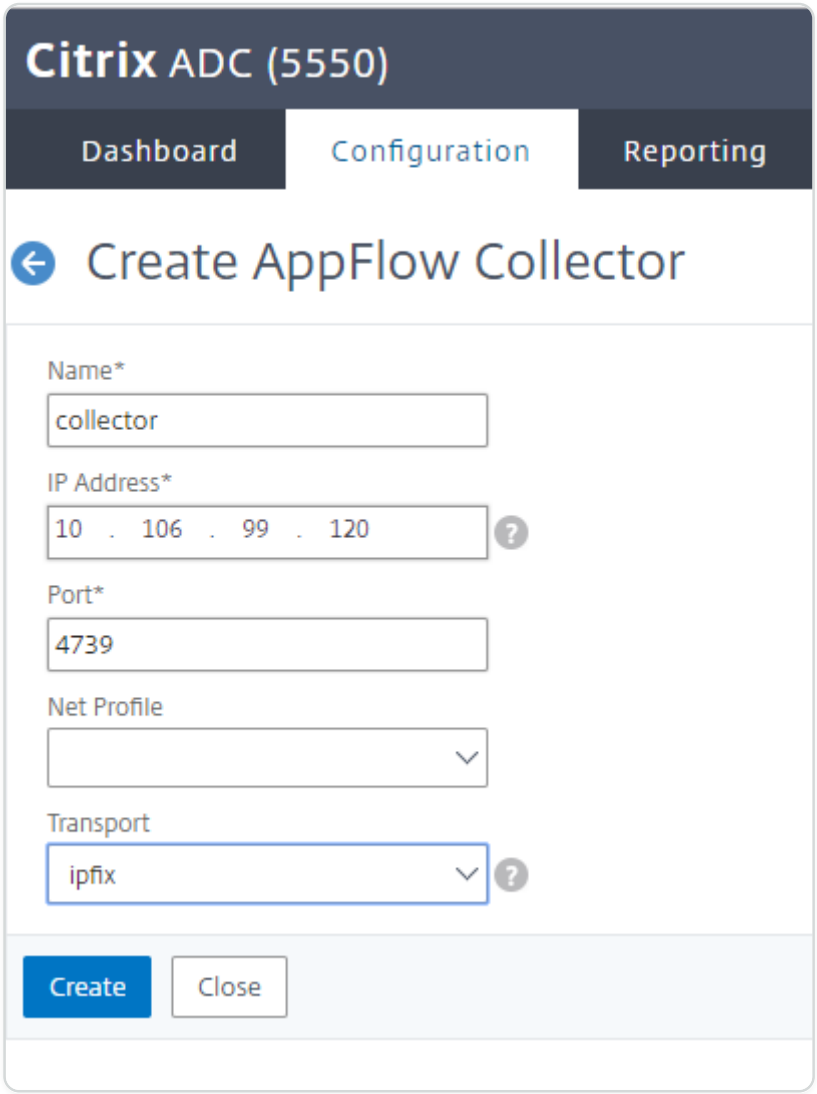
1. 在“**Configuration**”（配置）选项卡上，导航到“**System> AppFlow®>Collectors**”（系统 > AppFlow® > 收集器），然后单击“**Add**”（添加）。



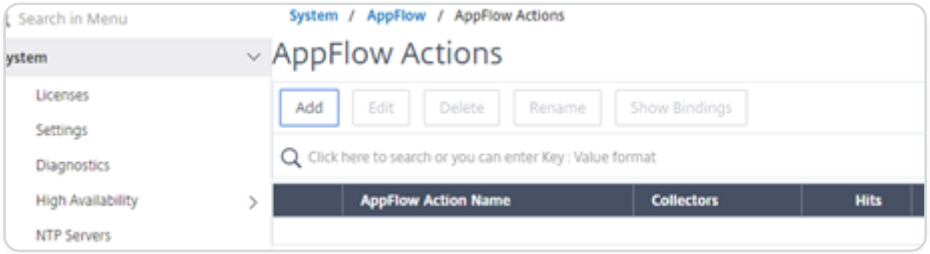
2. 在“**Create AppFlow Collector**”（创建 AppFlow 收集器）页面上，填写以下字段，然后单击“**Create**”（创建）。

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

- **名称：**收集器的名称
- **IP 地址：**收集器的 IPv4 地址
- **端口：**收集器侦听的端口
- **网络配置文件：**要与收集器关联的网络配置文件。配置文件中定义的 IP 地址用作此收集器的 AppFlow 流量的源 IP 地址。如果未设置此参数，则 NetScaler IP (NSIP) 地址将用作源 IP 地址。
- **传输：**收集器的传输类型。



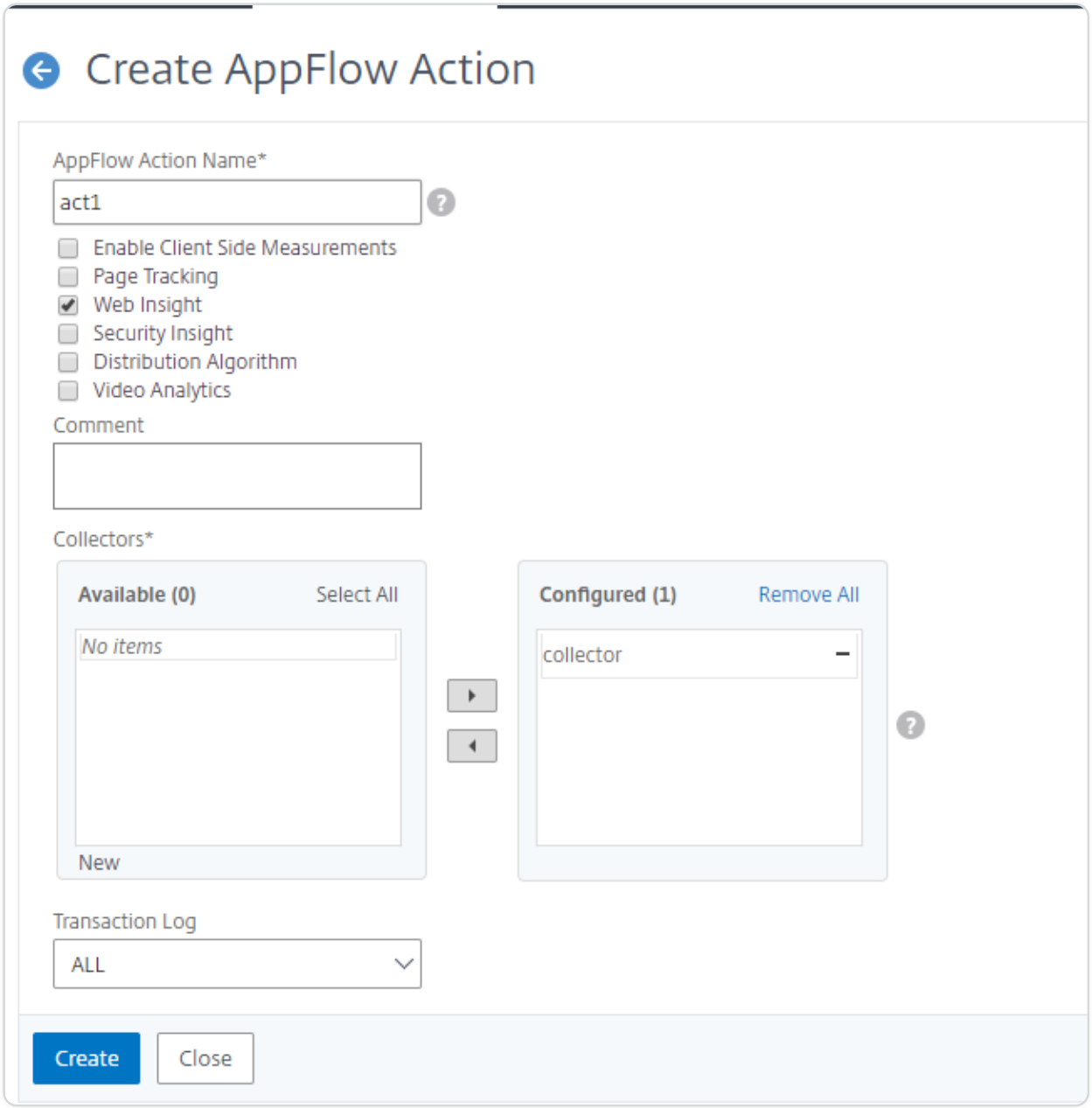
3. 导航到 **系统 > AppFlow > 操作**，单击 **添加**。



4. 在 **创建 AppFlow 操作** 页面上，填写以下字段，然后单击 **创建**。

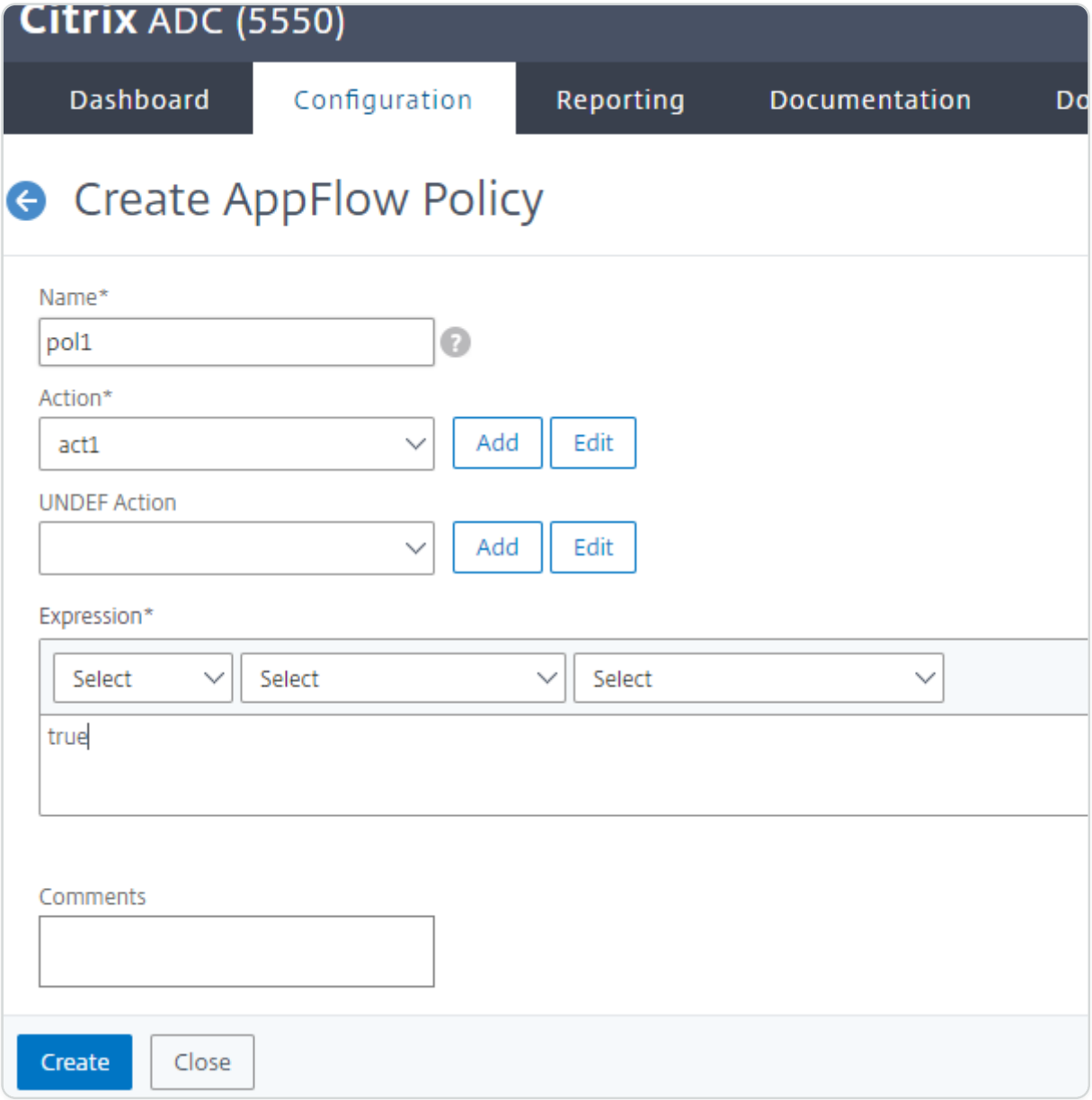
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **AppFlow 操作名称：** 操作的名称
- **注释：** 有关此操作的任何注释
- **收集器：** 选择要与 AppFlow 操作关联的收集器名称。
- **事务日志：** 要记录的事务类型。



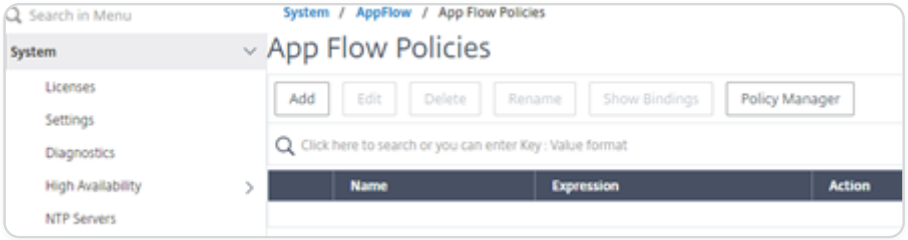
5. 导航到 **系统 > AppFlow > 策略**，单击 **添加**。

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



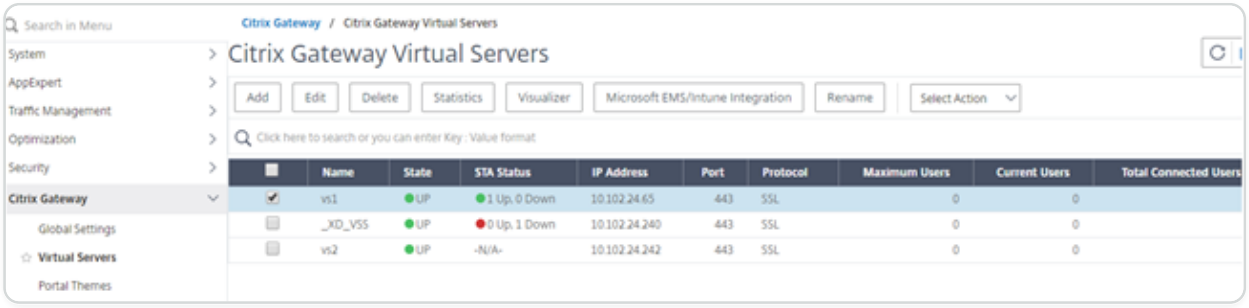
6. 在 **创建 AppFlow 策略** 页面上，填写以下字段，然后单击 **创建**。

   - **名称：** 策略的名称。
   - **操作：** 要与策略关联的操作名称。
   - **未定义：** 当发生未定义事件时要与此策略关联的 AppFlow 操作的名称。
   - **表达式：** 用于评估流量的表达式或其他值。必须是布尔表达式。
   - **注释：** 有关此策略的任何注释。

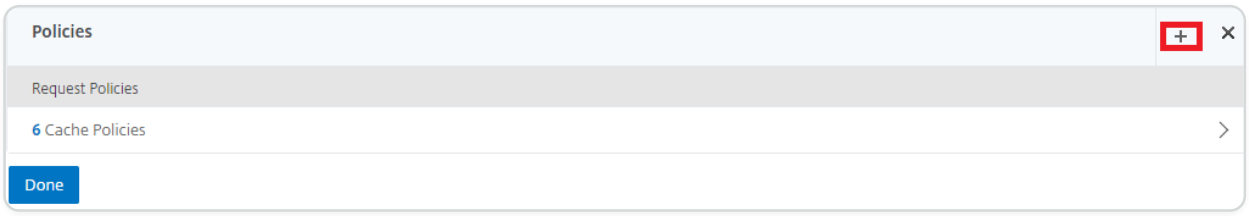


© 1997–2026 Citrix Systems, Inc. All rights reserved.

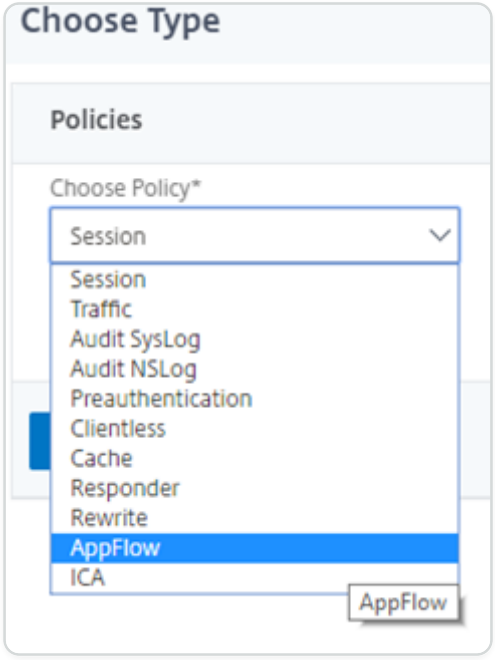
7. 导航到 **NetScaler Gateway>虚拟服务器**，选择虚拟服务器，然后单击“**编辑**”。



8. 向下滚动“**VPN 虚拟服务器**”页面，并在“**策略**”部分下，单击“**+**”。

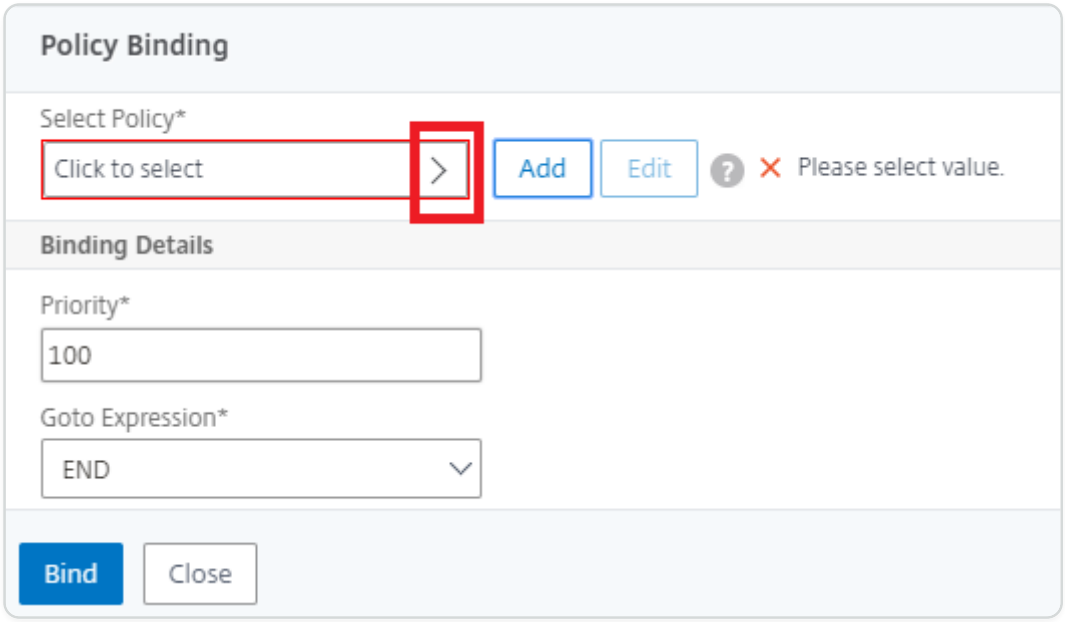


9. 在“**选择类型**”屏幕上，在“**选择策略**”下拉菜单中，选择“**AppFlow**”。在“**选择类型**”下拉菜单中，选择“**请求**”或“**ICA® 请求**”，然后单击“**继续**”。

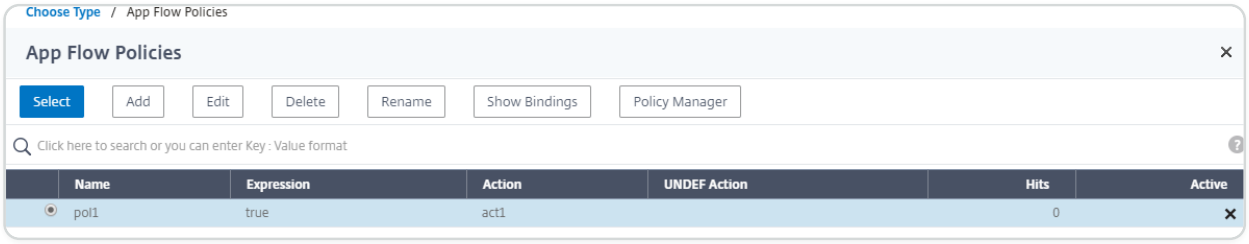


10. 单击“**选择策略**”下突出显示的箭头。

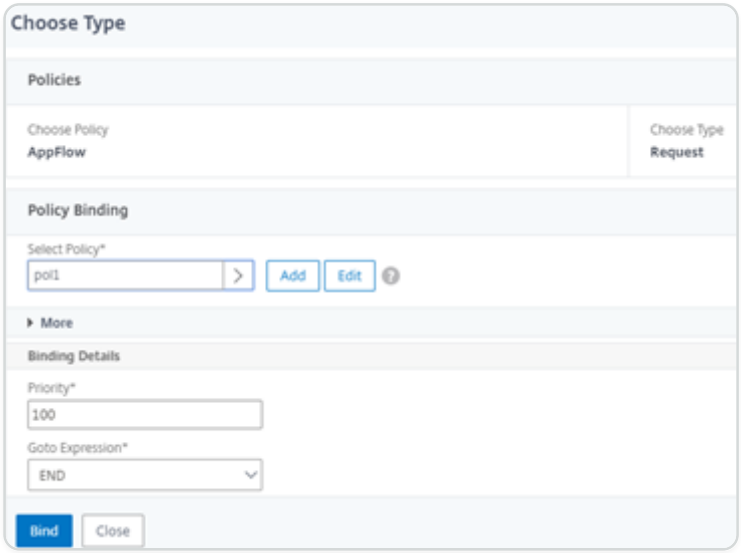
© 1997–2026 Citrix Systems, Inc. All rights reserved.



11. 选择“**AppFlow 策略**”，然后单击“**选择**”。



12. 最后单击“**绑定**”。



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

使用 CLI 配置 NetScaler Gateway 以支持 HDX Insight

注意：

- 本节适用于 NetScaler Gateway 14.1-51.x 及更早版本。
- 从 NetScaler Gateway 14.1 版本 56.x 开始，HDX Insight 数据将传输到 Citrix Director，无需以下 `appflow policy` 配置。管理员必须在 Delivery Controller 或 Citrix Studio 上启用**网络遥测**策略，才能将 HDX Insight 数据传输到 Citrix Director。有关启用此策略的详细信息，请参阅创建策略。

在命令提示符下，键入：

```
add appflow collector col3 -IPAddress<ip_mas>

add appflow action act1 <action_name>

add appflow policy <policy_name> true <action_name>

bind vpn Vserver <vserver_name>  -pol <policy_name> - priority101 END
-type <ICA_Request>
```

增强型 HDX Insight 传输，无需 NetScaler Gateway 配置依赖项

从 NetScaler Gateway 14.1 版本 56.x 开始，HDX Insight 数据将传输到 Citrix Director，无需在 NetScaler Gateway 上配置 **AppFlow** 策略。管理员只需在 Delivery Controller 或 Citrix Studio 上启用**网络遥测**策略，即可将 HDX Insight 数据传输到 Citrix Director。有关启用此策略的详细信息，请参阅创建策略。

此功能默认启用，简化了故障排除，增强了灵活性，并简化了网络性能监控。

以前，通过通用网关协议 (CGP) 启用 HDX Insight 需要在 Delivery Controller 或 Citrix Studio 上配置**网络遥测**策略，以及在 NetScaler Gateway 上配置 HDX Insight 的 **AppFlow** 策略。

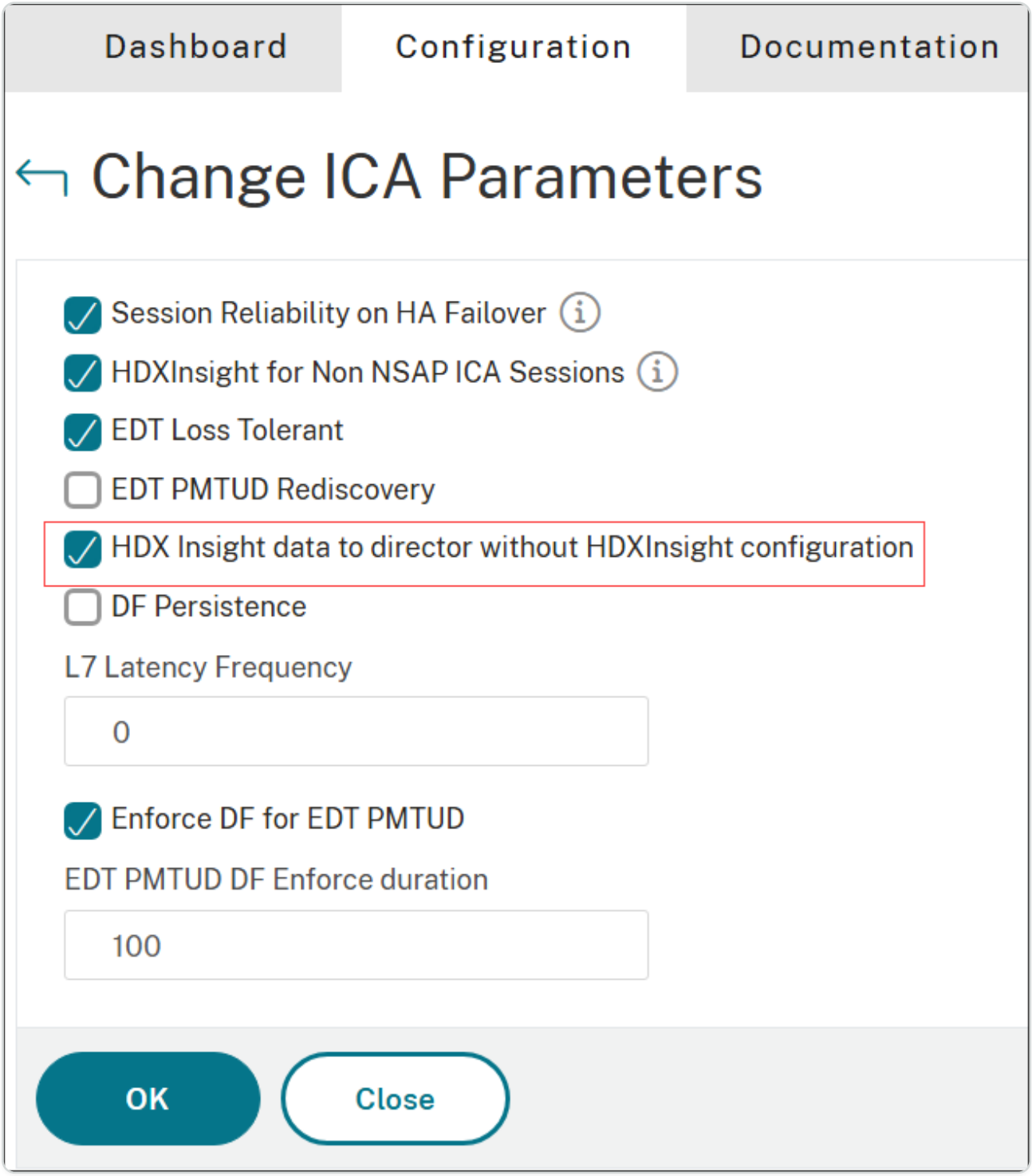
要使用 GUI 禁用 HDX Insight 传输

要通过在 NetScaler Gateway 上配置 **AppFlow** 策略来启用 HDX Insight 传输，请按照以下步骤禁用此功能：

1. 导航到**设置 > 更改 ICA 参数**。

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

2. 在**更改 ICA 参数**页面上，清除**无需 HDXInsight 配置即可将 HDX Insight 数据传输到 Director** 选项。
3. 单击**确定**。



要使用 CLI 禁用 HDX Insight 传输

在命令提示符下，键入：

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

```
set ica param -InsightOnlyToDirector DISABLED
```

禁用非 NetScaler® AppFlow (NSAP) HDX 会话的 HDX Insight

在 NetScaler 设备中，您现在可以为非 NSAP HDX 会话禁用 HDX Insight。

在命令提示符下，键入：

```
set ica parameter HDXInsightNonNSAP (YES | NO )
```

默认情况下，非 NSAP 会话的 HDX™ Insight 已启用。

HDX Insight 对 Secure HDX 的支持

Secure HDX 是一种应用层加密 (ALE) 解决方案，可防止流量路径中的网络元素检查 HDX 流量。从版本 14.1 build 47.x 开始，Secure HDX 支持通过 TCP 的 HDX Insight。对于通过 EDT 的 HDX Insight，此功能从 NetScaler 版本 14.1 build 72.x 开始随 Secure HDX 提供。有关 Secure HDX 的更多信息，请参阅 Secure HDX。

管理员可以通过 Director、Monitor 和 NetScaler Console 监控 HDX Insight。有关启用 Secure HDX 后的性能指标的更多信息，请参阅 在 Director 中诊断会话性能问题 和 在 Monitor 中诊断会话性能问题。NetScaler Console 服务上的 HDX Insight 功能无需任何更改。有关更多信息，请参阅 HDX Insight。

从版本 14.1 build 60.x 开始，NetScaler Gateway 支持在适用于 Linux 的 VDA 中启用 Secure HDX 的 HDX Insight。

主要优势

在 VDA 中启用网络遥测时：

- 可以在 Director 中监控 HDX Insight 的网络延迟。
- 通过 NetScaler Gateway 和 VDA 之间安全的 TLS/DTLS 连接增强了数据安全性。

系统要求

带有 Secure HDX 的 HDX Insight 目前仅在以下平台受支持：

- 适用于 Windows 的 Citrix Workspace™ 应用程序 - 2503 版及更高版本。
- 适用于 Windows 的 VDA - 2503 版及更高版本。
- 适用于 Linux 的 VDA - 2507 版及更高版本

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

- Director - 2503 版及更高版本。

有关在启用 Secure HDX 时访问 HDX Insight 的系统要求的更多信息，请参阅系统要求。

限制

HDX Insight 与 Secure HDX 不支持以下场景：

- HDX 多流 ICA (MSI) 连接
- IPv6 协议
- 透明模式和 LAN 代理模式拓扑
- SOCKS 协议

EDT 连接的 HDX Insight 需要 DTLS 1.2 配置。

使用 GUI 配置 DTLS 1.2

1. 导航到 **NetScaler Gateway** -> **全局设置** -> **更改全局设置**。
2. 在 **全局 NetScaler Gateway 设置** 页面上，在 **后端 DTLS 1.2** 中选择 **ENABLED**，然后单击 **确定**。

启用 DTLS 1.2(/en-us/netscaler-gateway/media/dtls-1-2-enable-gui-1.png)

使用 CLI 配置 DTLS 1.2

要为后端连接启用 DTLS 1.2，请在命令提示符下键入：

```
set vpn parameter -backenddtls12 ENABLED
```

注意：

可以使用以下命令之一禁用 DTLS 1.2：

- 将 vpn 参数 -backenddtls12 设置为 DISABLED
- 取消设置 vpn 参数 -backendDtls12

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

PMTUD 和 DF 位传播，适用于通过 NetScaler Gateway 的 EDT

NetScaler Gateway 设备支持不分段 (DF) 位强制执行，适用于 EDT 路径最大传输单元发现 (PMTUD)。PMTUD 有助于在建立会话时动态确定最大传输单元 (MTU)。从版本 14.1 build 34.42 及更高版本开始，PMTU 重新发现机制会识别由于已建立连接的路径 MTU 发生变化而导致的丢包，并启动 PMTU 重新发现。DF 位强制执行可防止 EDT 分段，这种分段可能导致性能下降或在 PMTUD 和 PMTU 重新发现期间无法建立会话。

从版本 14.1 build 38.53 开始，DF 位持久性功能可在整个会话期间保留数据包的原始 DF 位值。DF 位持久性功能提供以下优势：

- **确保正确通信：** 通过保留发送方的原始 DF 位设置，NetScaler Gateway 可防止因中间设备更改 DF 位而导致的通信错误或不正确行为。
- **避免意外分段：** NetScaler Gateway 可防止中间网络设备意外分段发送方不希望分段的数据包，反之亦然。
- **尊重发送方意图：** NetScaler Gateway 确保在整个网络路径中尊重发送方的意图（无论是允许分段还是不允许分段）。

有关更多详细信息，请参阅 Enlightened Data Transport。

在 NetScaler Gateway 中启用 PMTUD 支持

使用 CLI：

在命令提示符下，键入；

```
set ica parameter [-EnableSRonHAFailover ( YES | NO )] [-HDXInsightNonNSAP
( YES | NO )] [-EDTPmtudDF ( ENABLED | DISABLED )] [-EDTPmtudDFTimeout
<positive_integer>] [-L7LatencyFrequency <positive_integer>]
```

示例：

```
set ica parameter -EnableSRonHAFailover YES -EDTPmtudDF ENABLED
-EDTPmtudDFTimeout 100
```

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

注意：

从版本 13.1 build 42.x 及更高版本开始，EDTPmtudDF 参数默认启用。以前，此选项默认禁用。

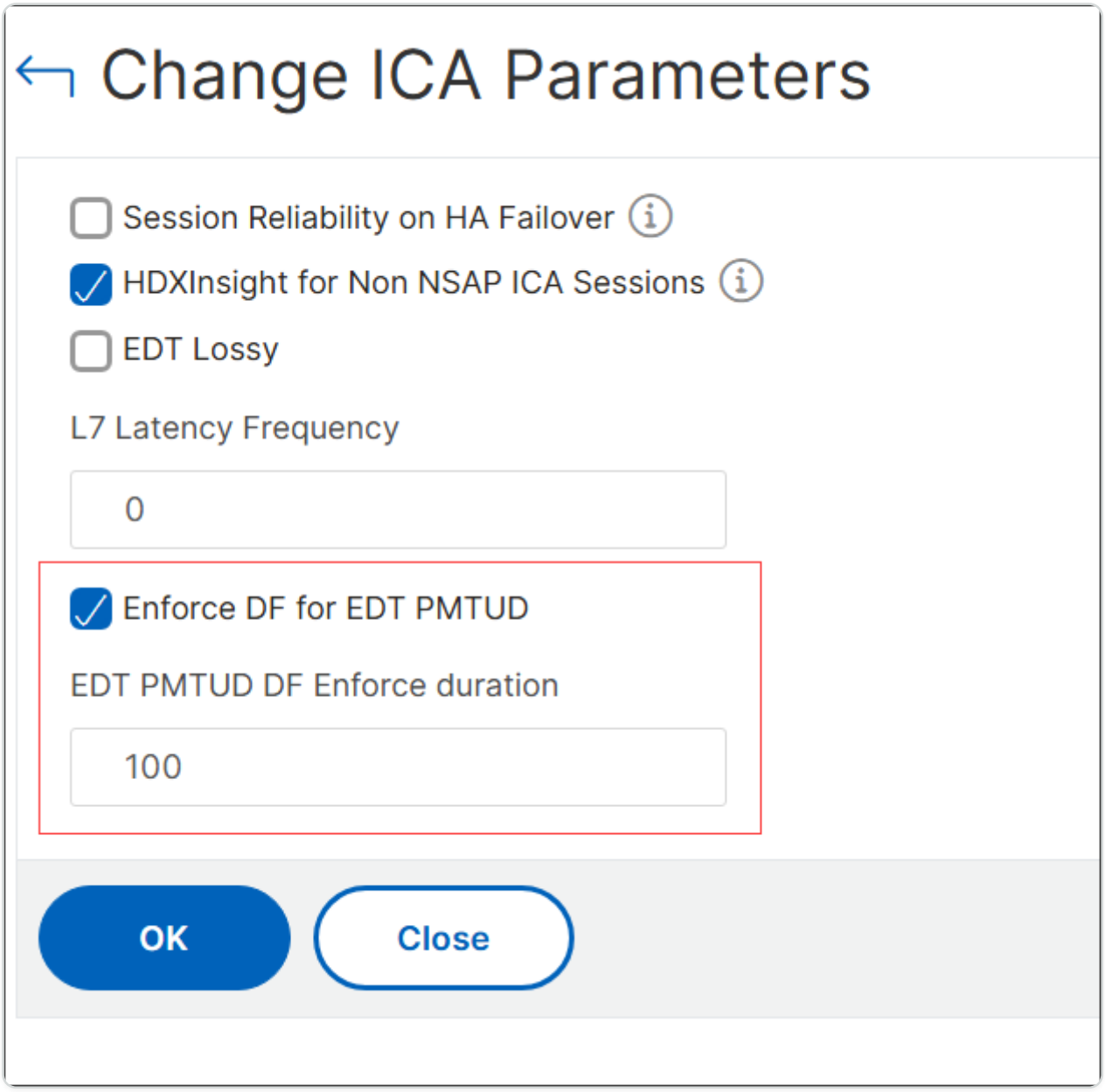
使用 GUI：

1. 导航到 **系统 > 设置 > 更改 ICA® 参数**。
2. 在 **EDT PMTUD DF 强制持续时间** 中，输入 PMTUD DF 强制的超时时间（以秒为单位）。

注意：

从版本 13.1 build 42.x 及更高版本开始，**为 EDT PMTUD 强制执行 DF** 选项默认启用。以前，此选项默认禁用。

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



在 NetScaler Gateway 中启用 PMTU 重新发现支持

使用 CLI：

在命令提示符下，键入；

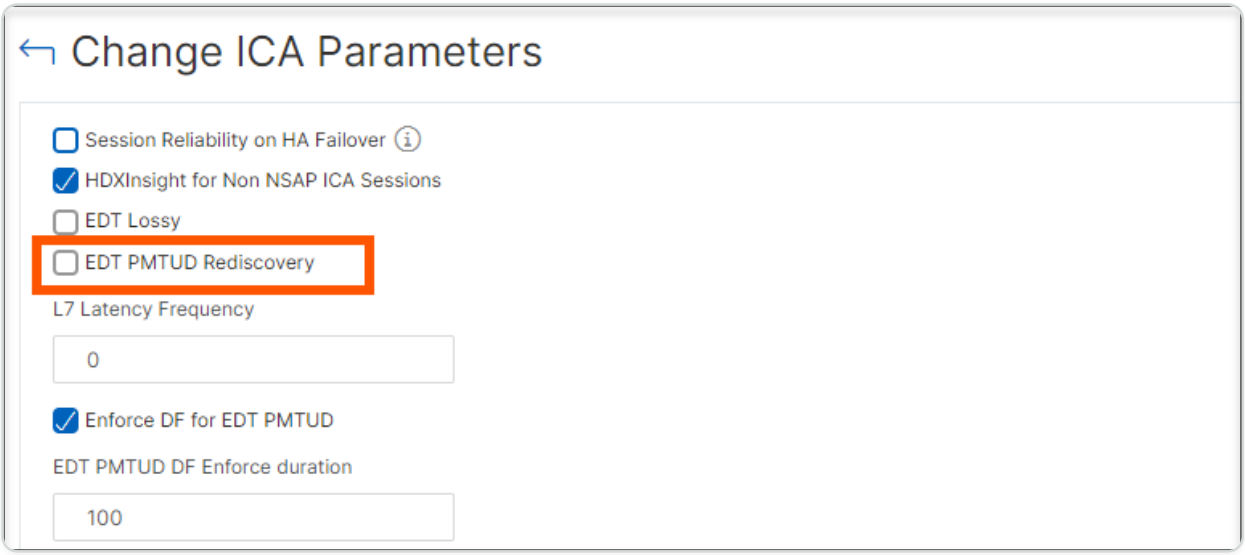
```
set ica parameter -EDTPmtudRediscovery ENABLED | DISABLED
```

此选项默认禁用。

使用 GUI：

1. 导航到 **系统** > **设置** > **更改 ICA 参数**。
2. 选中 **EDT PMTUD Rediscovery** 复选框。

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



在 NetScaler Gateway 中启用 DF 位持久性支持

使用 CLI：

在命令提示符下，键入；

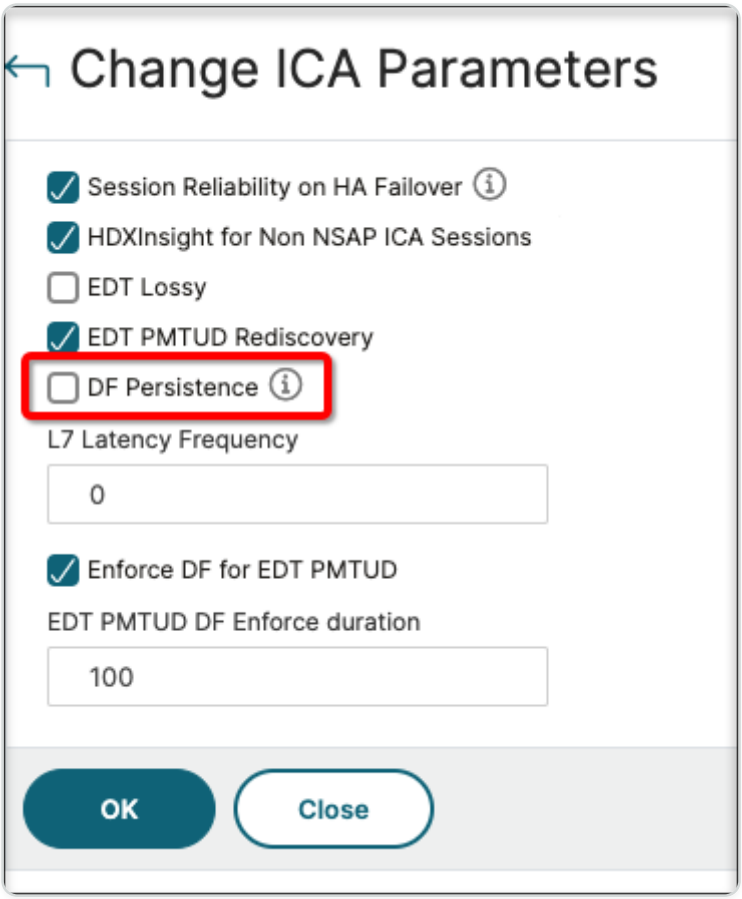
```
set ica parameter -DFPersistence ENABLED | DISABLED
```

此选项默认禁用。

使用 GUI：

1. 导航到 **System** > **Settings** > **更改 ICA 参数**。
2. 选中 **DF Persistence** 复选框。

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



L7 延迟阈值

HDX™ Insight 中的 L7 延迟阈值功能可主动检测应用程序级别的端到端网络延迟问题并采取主动措施。L7 延迟阈值功能执行实时延迟监控以检测峰值，如果延迟超过最小观测延迟，则向 HDX Insight 发送通知。

以前，客户端和服务器端的平均 L7 延迟值每 60 秒发送到 HDX Insight。在此间隔内出现的任何峰值都会被平均化，因此未被检测到。此外，当时也没有实时延迟监控来检测这些峰值。

L7 延迟与 L4 延迟有何不同

网络延迟也会在 L4 级别捕获和显示。这些延迟是从 TCP 层计算的，不需要解析 ICA 流量。因此，它们相对容易获取且 CPU 密集度较低。然而，L4 延迟的主要缺点是难以理解端到端延迟。如果路径中存在 TCP 代理，L4 延迟仅捕获从 NetScaler 到 TCP 代理的延迟。这可能导致信息不完整，从而导致调试问题时遇到困难。

L7 延迟通过解析 ICA® 流量计算。L7 延迟计算在 ICA 层完成，因此中间代理不会导致不完整的延迟值。因此，它提供了端到端延迟检测。

下图显示了有和没有 TCP 代理的部署类型。

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

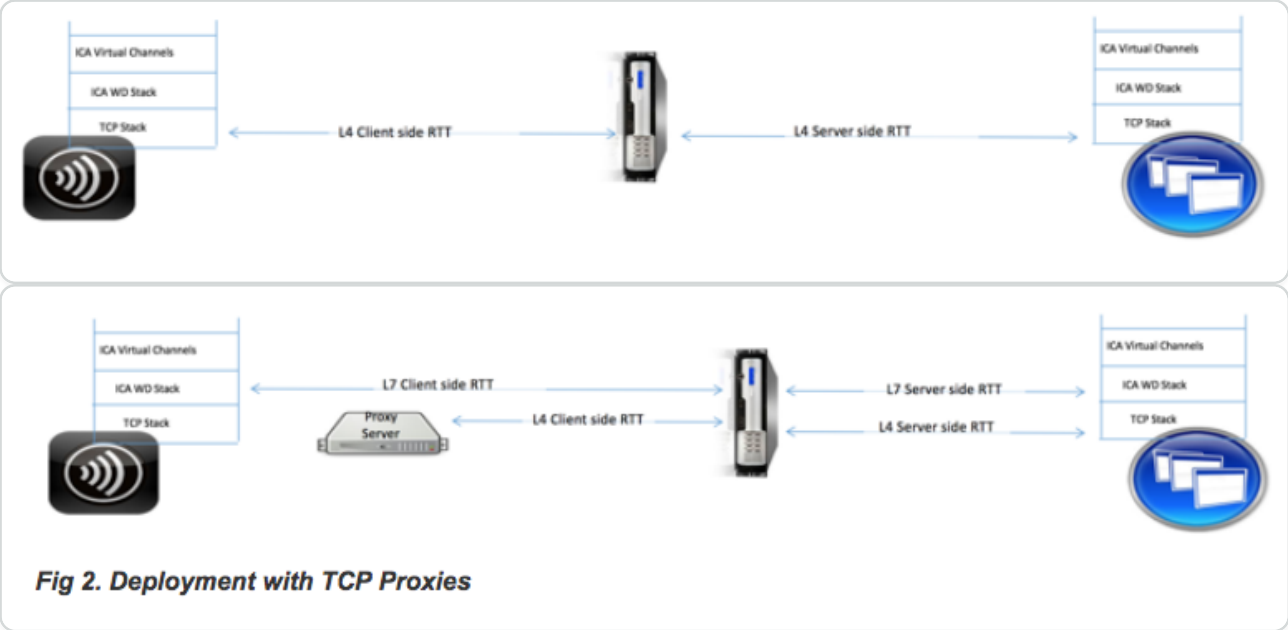


Fig 2. Deployment with TCP Proxies

ICA RTT 与 L7 延迟计算之间的区别

ICA RTT 表示从 Citrix Workspace 应用程序到虚拟投递代理 (VDA) 的总往返时间。L7 延迟提供有关客户端和服务器端延迟的详细信息。L7 客户端延迟是 Citrix Workspace 应用程序到 NetScaler Gateway 之间的延迟。L7 服务器延迟是 NetScaler Gateway 到 VDA 之间的延迟。

注意

- 服务器端的 L7 延迟计算仅支持 Citrix Virtual Apps and Desktops 7.13 及更高版本。

使用 CLI 配置 L7 延迟阈值

1. 添加 ICA 延迟配置文件。

```
add ica latencyprofile <name> [-l7LatencyMonitoring ( ENABLED |
DISABLED )] [-l7LatencyThresholdFactor <positive_integer>] [-
l7LatencyWaitTime <positive_integer>] [-l7LatencyNotifyInterval
<positive_integer>] [-l7LatencyMaxNotifyCount <positive_integer>]
```

2. 添加 ICA 操作。

```
add ica action <name> [-latencyprofileName <string>]
```

3. 添加 ICA 策略。

```
add ica policy <name> -rule <expression> -action <string> [-
comment<string>] [-logAction <string>
```

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

4. 将 ICA 策略绑定到 VPN 服务器或 ICA 全局绑定点。

```
bind ica global -policyName <string> -priority <positive_integer> [-
gotoPriorityExpression <expression>] [-type ( ICA_REQ_OVERRIDE |
ICA_REQ_DEFAULT )]
```

或者

```
bind vpn vserver <name> -policy <string>  [-priority
<positive_integer>]
```

或者

```
bind cr vserver <name> -policy <string> [-priority <positive _integer>]
```

参数

- **延迟监控**：用于启用或禁用 L7 阈值监控的参数。启用此参数后，当满足设定条件时，通知将发送到 HDX Insight。

  默认值：DISABLED

- **延迟阈值因子**：活动延迟必须大于观察到的最小延迟的因子，以确定阈值已超出，因此必须将通知发送到 HDX Insight。

  默认值：4

  最小值：2

  最大值：65535

- **延迟等待时间**：设备在超出延迟阈值后等待发送通知到 HDX Insight 的时间（以秒为单位）。

  默认值：20

  最小值：1

  最大值：65535

- **LatencyNotifyInterval**：设备在等待时间过后向 HDX Insight 发送后续通知的以秒为单位的时间间隔。

  默认值：20

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

最小值：1

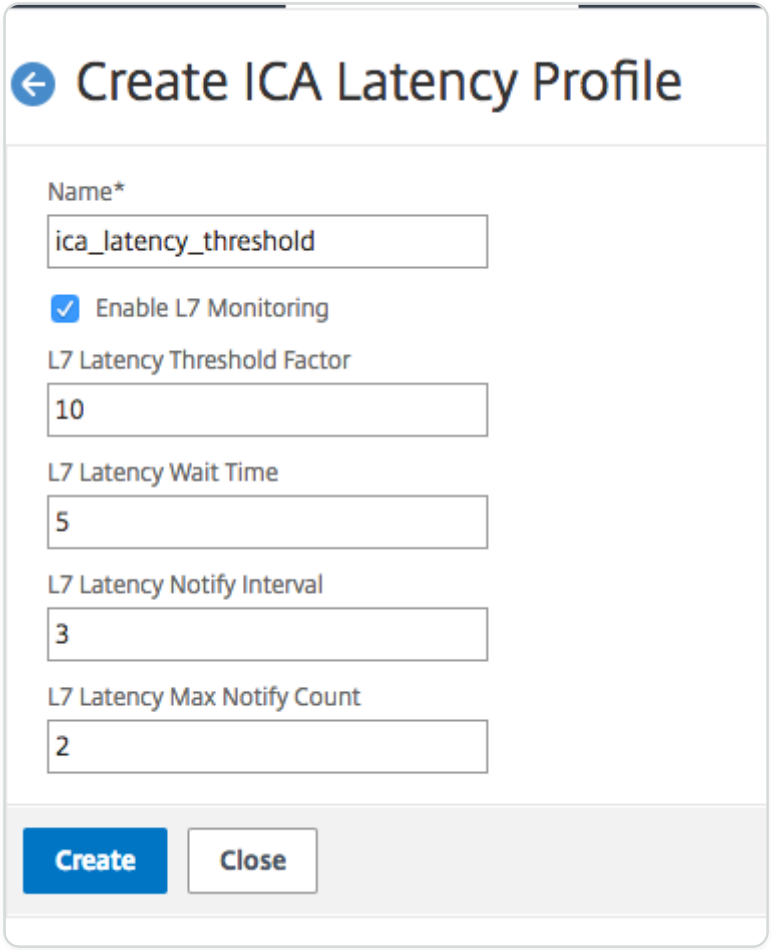
最大值：65535

- **LatencyMaxNotifyCount**：在延迟高于阈值的间隔内，可以发送到 HDX Insight 的最大通知数。

  默认值：5

使用 GUI 配置 L7 延迟阈值

1. 导航到 **配置** > **NetScaler® Gateway** > **策略** > **ICA**。
2. 选择 **ICA Latency Profiles** 选项卡，然后单击 **Add**。
3. 在 **Create ICA Latency Profile** 页面中，执行以下操作。



- 选择 **L7 Latency Monitoring** 以启用 L7 阈值监视。
- 在 **L7 Threshold Factor** 中，输入活动延迟必须超过观察到的最小延迟的倍数，才能向 HDX Insight 发送通知。
- 在 **L7 Latency Wait Time** 中，输入设备在超过阈值后等待的时间（以秒为单位），以向 HDX Insight 发送通知。

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

- 在 **L7 Latency Notification Interval** 中，输入设备在等待时间过后向 HDX Insight 发送后续通知的时间（以秒为单位）。
- 在 **L7 延迟最大通知计数**中，输入在延迟高于阈值的间隔内可以发送到 HDX Insight 的最大通知数。 **注意：** L7 延迟最大通知计数在超过阈值后适用，并在活动延迟低于阈值时重置。这些通知的周期由通知间隔决定。

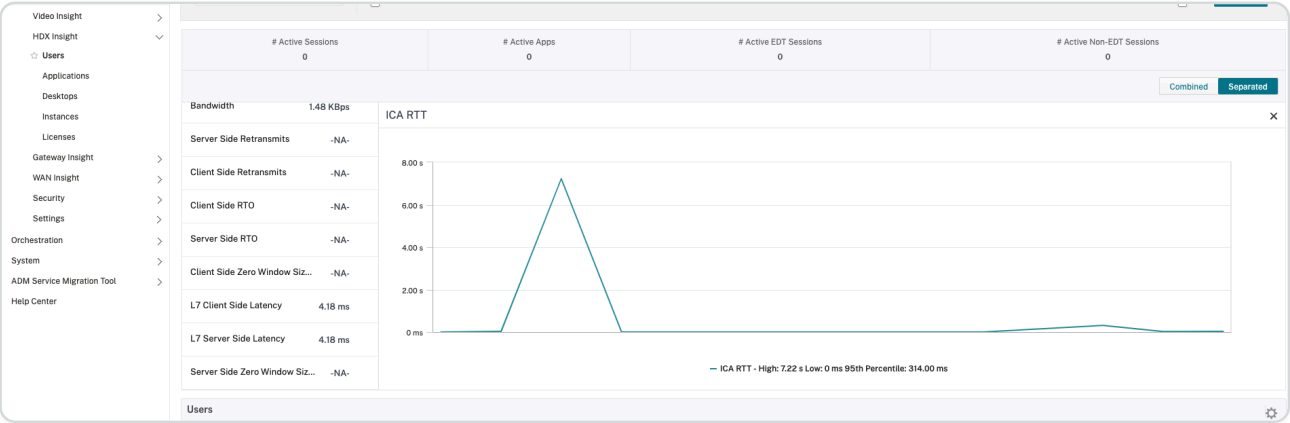
4. 单击**创建**。

重要提示：

配置 L7 延迟阈值参数后，您必须配置 HDX Insight。有关详细信息，请参阅配置 NetScaler Gateway 以支持 HDX Insight。

在 NetScaler ADM 中查看 L7 延迟参数

要在 NetScaler ADM 中查看 L7 延迟参数，请导航到 **Analytics（分析）> HDX Insight > Applications（应用程序）** 或 **Analytics（分析）> HDX Insight > Users（用户）**。



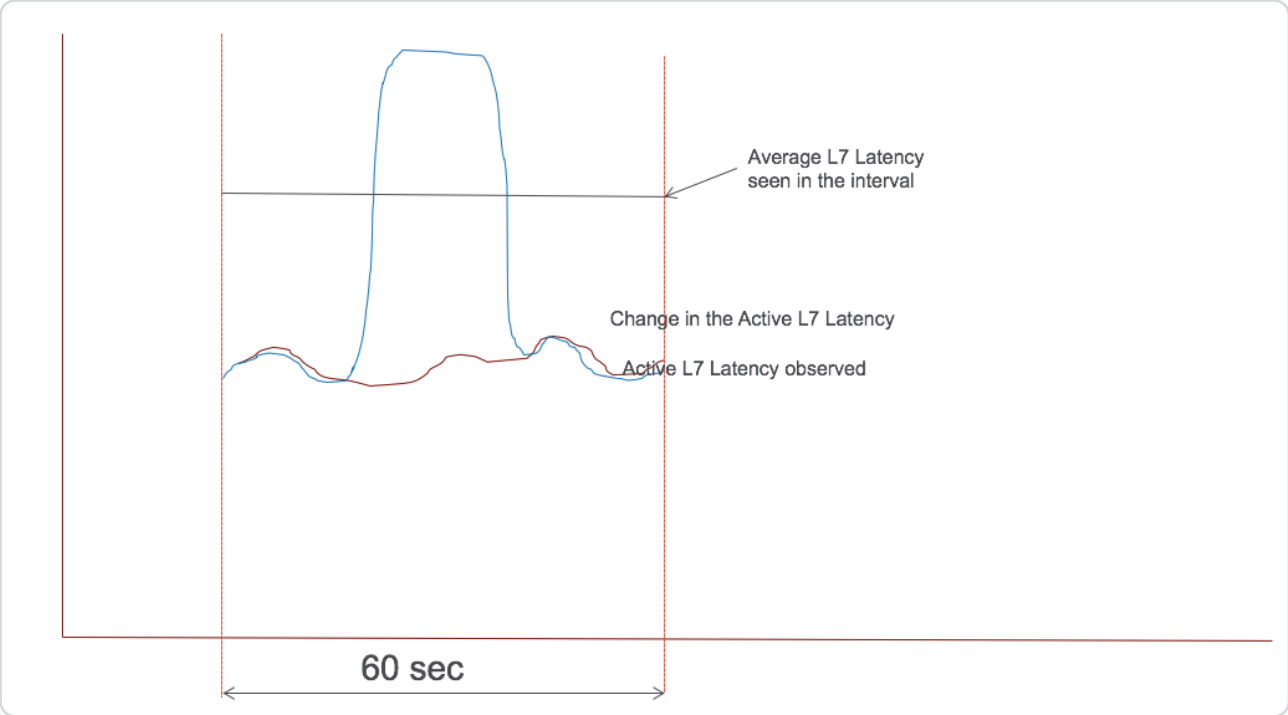
L7 延迟测量模型与 L7 延迟阈值报告模型

L7 延迟测量模型

在 L7 延迟测量模块中，客户端和服务器端的平均 L7 延迟值每 60 秒发送到 HDX Insight。因此，在此间隔内出现的峰值会被平均化，从而未被检测到。此外，L7 延迟测量模块不具备实时延迟监控功能。

下图说明了一个示例 L7 延迟测量模型。

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

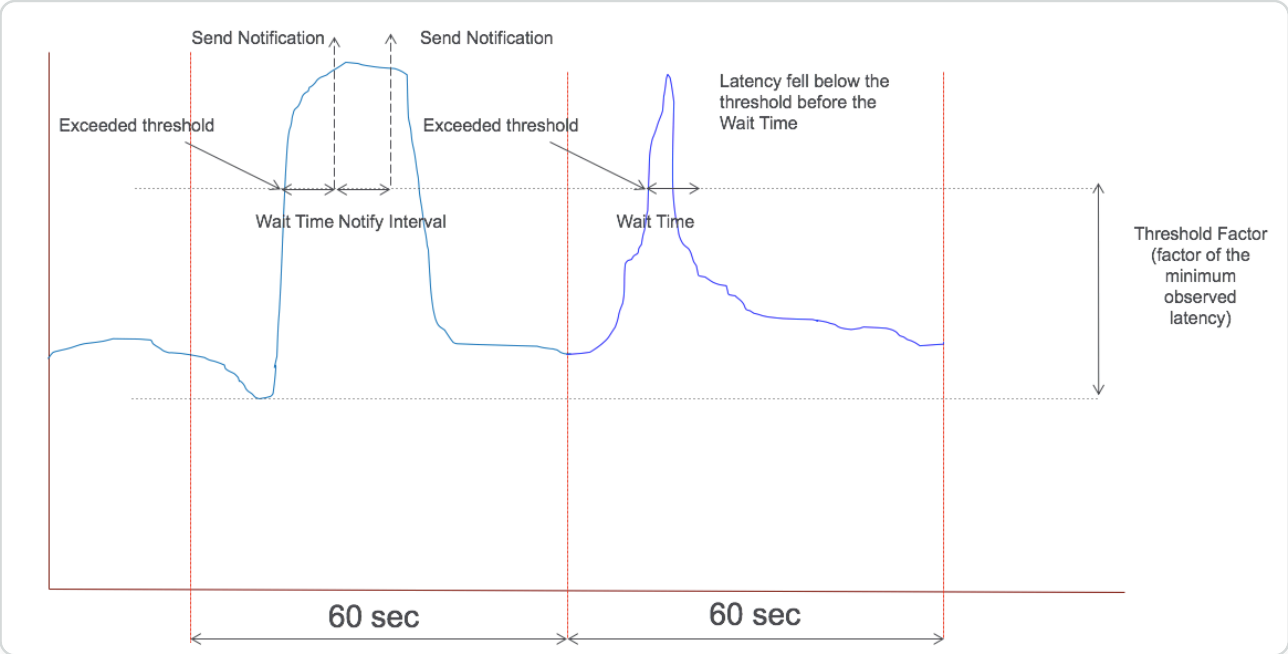


L7 延迟阈值报告模型

L7 延迟阈值报告模型具有实时延迟监控功能，可以检测峰值。如果延迟超过观察到的最小延迟，则会向 HDX Insight 发送通知。

每当超过阈值因子时，就会检测到延迟增加。配置的阈值等待时间到期后，会向 HDX Insight 发送通知。在等待时间到期且阈值因子仍被超过后，会向 HDX Insight 发送后续通知。 如果延迟值在等待时间到期之前低于阈值因子，则不会向 HDX Insight 发送通知。

以下图示说明了一个示例 L7 延迟阈值报告模型。



以下参数可在运行时配置：

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

- 阈值监控（开/关）
- 阈值因子
- 阈值等待时间
- 通知间隔
- 最大通知计数

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

HDX™ 压缩器

HDX 压缩器是一种通用压缩器，由 Citrix Virtual Apps and Desktops™ 管理，可跨虚拟通道工作。

NetScaler Gateway 14.1–8.50 及更高版本支持最新版本的 HDX 压缩器。最新压缩器通过以下功能提高了 NetScaler Gateway 的整体性能：

- 降低 ICA® 会话的网络带宽利用率。
- 提供更快的响应，因为数据包传输时间更短。

有关如何使用最新压缩器的详细信息，请参阅如何使用新压缩器。

以下软件版本支持最新压缩器。

- Citrix 虚拟应用和桌面 7 2303 (Windows) 及更高版本。
- Citrix Workspace™ app 2303 (Windows) 及更高版本。

注意：

如果您使用的是 Citrix Workspace app 2311 (Windows) 和 Citrix Virtual Apps and Desktops 7 2311 (Windows) 版本，则默认启用最新压缩器。

下表描述了在 NetScaler Gateway 14.1 版本上使用最新压缩器时 ICA 会话启动和 HDX 洞察的状态。

最新压缩器	NETSCALER 网关 14.1
最新压缩器协商 + NSAP HDX 洞察	ICA 连接启动成功。支持 HDX Insight。
最新的减速器协商 + NSAP HDX Insight + SmartControl	ICA 连接启动成功。支持 HDX Insight。
最新的减速器协商 + 非 NSAP HDX Insight	ICA 连接启动成功。不支持 HDX Insight。

注意：

NetScaler Gateway 13.1 及更早版本不支持使用最新减速器的 HDX Insight 和 SmartControl。

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

有关 HDX Insight 配置的详细信息，请参阅配置 NetScaler Gateway 以支持 HDX Insight。

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

RDP 代理

RDP 代理功能作为 NetScaler Gateway 的一部分提供。在典型的部署中，RDP 客户端在远程用户的计算机上运行。NetScaler Gateway 设备部署在 DMZ 中，RDP 服务器场位于内部公司网络中。

远程用户；

1. 连接到 NetScaler Gateway 公共 IP 地址
2. 建立 SSL VPN 连接
3. 进行身份验证
4. 通过 NetScaler Gateway 设备访问远程桌面

RDP 代理功能支持无客户端 VPN 和 ICA® 代理模式。

注意：

NetScaler Gateway 不支持远程桌面会话主机 (RDSH)、远程应用、RDS 多用户、RDP 会话或 RDP 应用。

以下 RDP 代理功能通过 NetScaler Gateway 提供对远程桌面场的访问。

- 通过无客户端 VPN 或 ICA 代理模式（不带完整隧道）保护 RDP 流量。
- 通过 NetScaler Gateway 对 RDP 服务器进行 SSO（单点登录）。如果需要，还提供禁用 SSO 的选项。

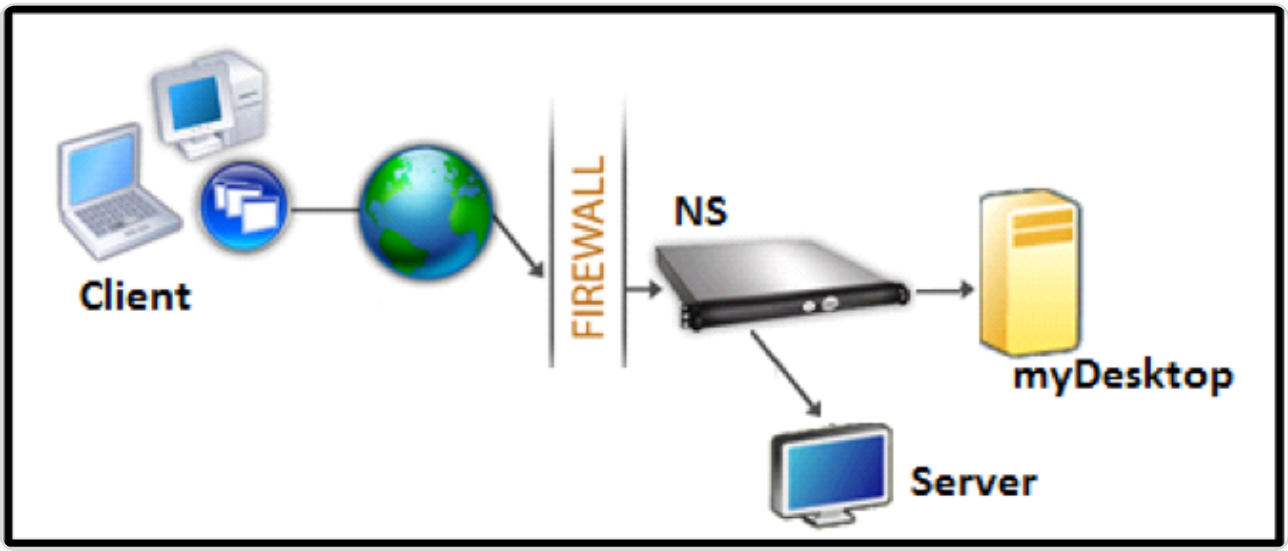
  注意：

  NetScaler Gateway 不支持用于 RDP 服务器 SSO 的 Kerberos 约束委派 (KCD)。

- 强制执行 (SmartAccess) 功能，NetScaler 管理员可以通过 NetScaler Gateway 配置禁用某些 RDP 功能。
- 单一/无状态（双）网关解决方案，满足所有需求（VPN/ICA/RDP/Citrix 端点管理）。
- 与本机 Windows MSTSC 客户端的 RDP 兼容性，无需任何自定义客户端。
- 在 macOS、iOS 和 Android 上使用现有的 Microsoft 提供的 RDP 客户端。

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

下图描绘了部署概述：



通过无客户端 VPN 部署

在此模式下，RDP 链接通过 `add vpn url` 配置或通过外部门户作为书签发布在网关主页或门户上。用户可以单击这些链接来访问远程桌面。

通过 ICA 代理部署

在此模式下，通过使用 `wihome` 参数在网关 VIP 上配置自定义主页。此主页可以根据用户被允许访问的远程桌面资源列表进行自定义。此自定义页面可以托管在 NetScaler 上，如果外部托管，则可以是现有网关门户页面中的 iFrame。有关详细信息，请参阅 配置访问接口。

在任一模式下，用户单击已配置的 RDP 链接或图标后，相应的资源 HTTPS 请求将到达 NetScaler Gateway。网关为请求的连接生成 RDP 文件内容并将其推送到客户端。本机 RDP 客户端被调用，并连接到网关上的 RDP 侦听器。网关通过支持强制执行 (SmartAccess) 对 RDP 服务器进行 SSO。网关根据 NetScaler 配置阻止客户端访问某些 RDP 功能，然后代理 RDP 客户端和服务器之间的 RDP 流量。

强制执行详细信息

NetScaler 管理员可以通过 NetScaler Gateway 配置某些 RDP 功能。NetScaler Gateway 为重要的 RDP 参数提供了“RDP 强制执行”功能。NetScaler 确保客户端无法启用被阻止的参数。如果启用了被阻止的参数，RDP 强制执行功能将取代客户端启用的参数，并且这些参数将不被遵守。

重要提示：

强制执行功能仅在启用 SSO 时适用。

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

支持强制执行的 RDP 参数

支持对以下重定向参数的强制执行。这些参数可作为 RDP 客户端配置文件的一部分进行配置。

- 剪贴板重定向
- 打印机重定向
- 磁盘驱动器重定向
- COM 端口重定向
- PNP 设备重定向

连接流程

连接流程可分为两个步骤：

- RDP 资源枚举和 RDP 文件下载。
- RDP 连接启动。

基于上述连接流程，有两种部署解决方案：

- 无状态（双）网关解决方案 - RDP 资源枚举和 RDP 文件下载通过身份验证器网关进行，但 RDP 连接启动通过 RDP 侦听器网关进行。
- 单一网关解决方案 - RDP 资源枚举、RDP 文件下载和 RDP 连接启动通过同一网关进行。

无状态（双）网关兼容性

下图描述了部署：

双网关兼容性(/en-us/netscaler-gateway/media/figure2_statelessgatewaycompatibility.png)

- 用户连接到身份验证器网关 VIP 并提供凭据。
- 成功登录网关后，用户将被重定向到主页或外部门户，其中列出了用户可以访问的远程桌面资源。
- 用户选择 RDP 资源后，身份验证器网关 VIP 会收到格式为 `https://vserver-vip/rdpproxy/rdptarget/listener` 的请求，该请求指示用户单击的已发布资源。此请求包含用户选择的 RDP 服务器的 IP 地址和端口信息。
- 身份验证器网关处理 /rdpproxy/ 请求。由于用户已通过身份验证，此请求附带有效的网关 Cookie。

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

- `RDPTarget` 和 `RDPUser` 信息存储在 STA 服务器上，并生成 STA 票证。存储在 STA 服务器上的信息使用配置的预共享密钥进行加密。身份验证器网关使用网关虚拟服务器上配置的 STA 服务器之一。
- /rdpproxy/ 请求中获取的“侦听器”信息作为“`fulladdress`”放入 `.rdp file` 中，STA 票证（前缀为 STA AuthID）作为“`loadbalanceinfo`”放入 `.rdp file` 中。
- `.rdp file` 被发送回客户端端点。
- 本机 RDP 客户端启动并连接到 `RDPListener Gateway`。它在初始数据包中发送 STA 票证。

  `RDPListener` 网关验证 STA 票证并获取 `RDPTarget` 和 `RDPUser` 信息。要使用的 STA 服务器通过 `loadbalanceinfo` 中存在的“AuthID”检索。
- 创建网关会话以存储授权/审计策略。如果用户已存在会话，则会重用该会话。
- `RDPListener` 网关连接到 `RDPTarget` 并使用 CREDSSP 进行单点登录。

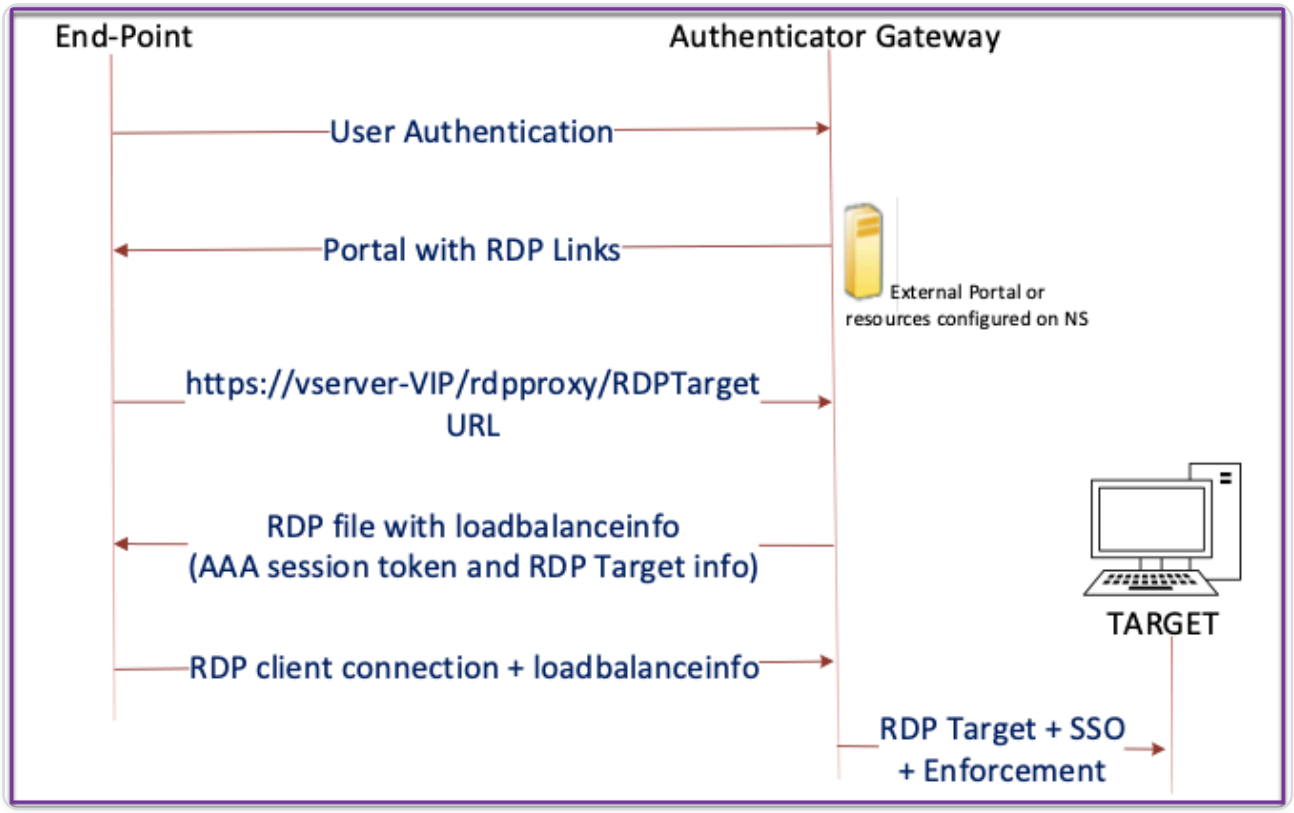
重要提示：

- 对于无状态 RDP 代理，STA 服务器验证 RDP 客户端发送的 STA 票证，以获取 `RDPTarget/RDPUser` 信息。除了 VPN 虚拟服务器之外，您还必须绑定 STA 服务器。
- 为了使 RDP 侦听器正常工作，RDP 服务器配置文件中指定的端口必须在客户的防火墙上打开。这允许 NetScaler Gateway 与后端 RDP 服务器通信。

单网关兼容性

下图描述了部署情况：

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



重要提示：

- 在单网关部署的情况下，不需要 STA 服务器。身份验证器网关对 `RDPTarget` 和 NetScaler 身份验证、授权和审计会话 cookie 进行安全编码，并将其作为 `loadbalanceinfo` 在 `.rdp file` 中发送。当 RDP 客户端在初始数据包中发送此令牌时，身份验证器网关会解码 `RDPTarget` 信息，查找会话，并连接到 `RDPTarget`。
- 在单网关部署中，RDP 服务器配置文件是强制性的，而 RDP 侦听器不是必需的。

支持单个侦听器

- RDP 和 SSL 流量的单个侦听器。
- RDP 文件下载和 RDP 流量可以通过 NetScaler 设备上的相同 2 元组（即 IP 和端口）进行处理。

RDP 代理的许可证要求

高级版、进阶版

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

注意：

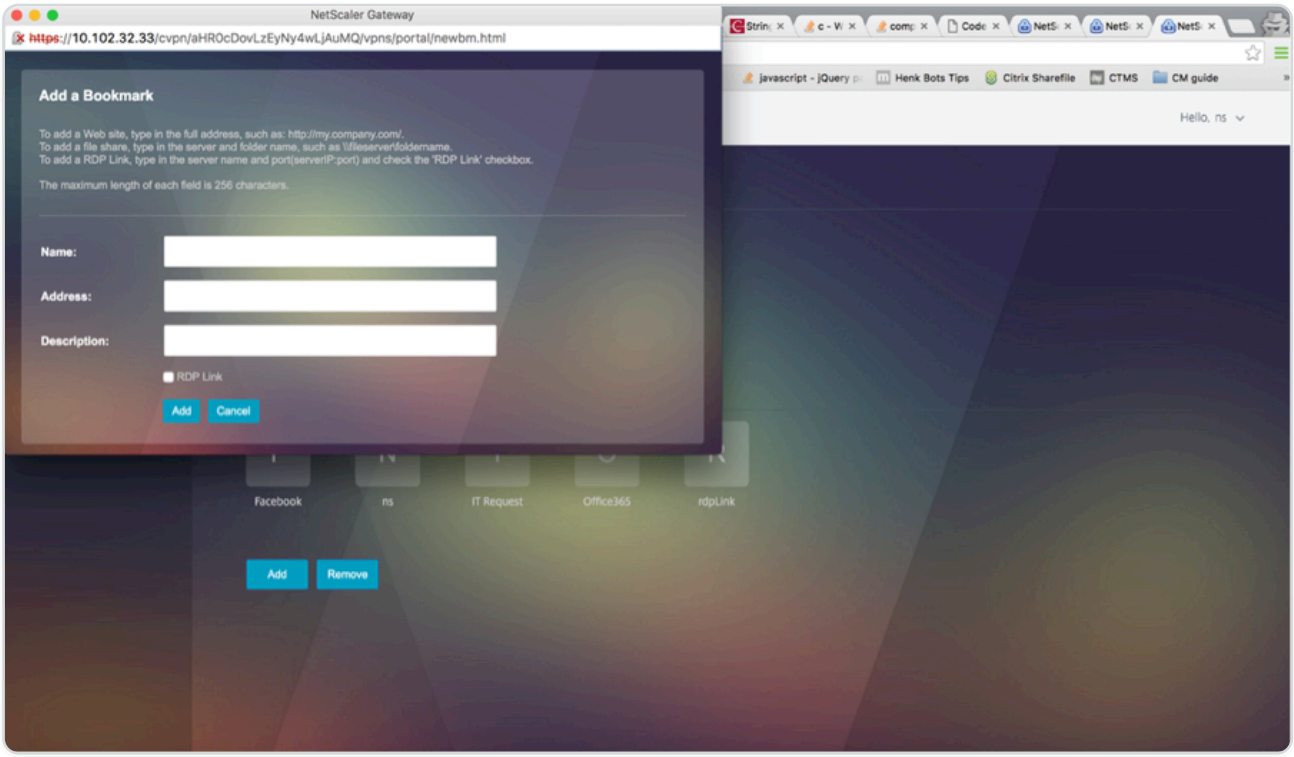
RDP 代理功能不适用于仅拥有网关平台许可证或仅拥有标准版的客户。

您可以使用以下命令启用 RDP 代理。

```
enable feature rdpProxy
```

书签

通过门户生成 RDP 链接。 用户无需配置 RDP 链接或通过外部门户发布 RDP 链接，您可以通过提供 `targetIP:Port` 让用户选择生成自己的 URL。对于无状态 RDP 代理部署，管理员可以在 RDP 客户端配置文件中以 FQDN: 端口格式包含 RDP 侦听器信息。这在 `rdpListener` 选项下完成。此配置用于在双网关模式下通过门户生成 RDP 链接。



创建书签

1. 在门户页面上创建书签以访问 RDP 资源：（实际 URL 以 `rdp`:// 开头）。
2. 添加 VPN URL `<urlName> <linkName>  <actualURL>`
   - URL 必须采用以下格式：`rdp://<TargetIP:Port>`。

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

- 对于无状态 RDP 代理模式，URL 必须采用以下格式：`rdp://<TargetIP:Port>/<ListenerIP:Port>`
- URL 以以下格式发布在门户上：`https://<VPN-VIP>/rdpproxy/<TargetIP:Port>` `https://<VPN-VIP>/rdpproxy/<TargetIP:Port>/<ListenerIP:Port>`

3. 将书签绑定到用户、组、VPN 虚拟服务器或 VPN 全局。

RDP 代理要启用的功能和模式

```
-  enable ns feature ssl



-  enable ns feature sslvpn



-  enable ns feature rdpproxy



-  enable mode usnip
```

RDP 代理高级配置步骤

无状态 RDP 代理配置涉及以下高级步骤。

- 创建 RDP 服务器配置文件
- 创建 RDP 客户端配置文件
- 创建并绑定虚拟服务器
- 创建书签
- 创建或编辑会话配置文件或策略
- 绑定书签

配置客户端配置文件

在身份验证器网关上配置客户端配置文件。以下是示例配置：

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

```
add rdpClient profile <name> [-addUserNameInRdpFile ( YES | NO )] [-
audioCaptureMode ( ENABLE | DISABLE )] [-keyboardHook <keyboardHook>] [-
multiMonitorSupport ( ENABLE | DISABLE )] [-psk <string>] [-
rdpCookieValidity <positive_integer>] [-rdpCustomParams <string>] [-
rdpFileName <string>] [-rdpHost <string>] [-rdpListener <string>] [-
randomizeRDPFilename ( YES | NO )] [-rdpLinkAttribute <string>] [-
rdpValidateClientIP ( ENABLE | DISABLE )] [-rdpUrlOverride ( ENABLE |
DISABLE )] [-redirectClipboard ( ENABLE | DISABLE )] [-redirectComPorts
( ENABLE | DISABLE )] [-redirectDrives ( ENABLE | DISABLE )] [-
redirectPnpDevices ( ENABLE | DISABLE )] [-redirectPrinters ( ENABLE |
DISABLE )] [-videoPlaybackMode ( ENABLE | DISABLE )] [-rdpUrlMaxLen
<positive_integer>] [-rdpUrlMaxLenCheck ( ENABLE | DISABLE )]
```

注意：

从 NetScaler Gateway 14.1 72.x 版本开始，支持以下参数：

- rdpUrlMaxLen - 指定 RDP URL 的最大允许长度。当在 StoreFront 中选择桌面书签时，此 URL 会从客户端发送到 NetScaler。该参数的值范围为 32 到 2048，默认值为 256。
- rdpUrlMaxLenCheck - 启用或禁用 RDP URL 最大长度验证（最大长度由 rdpUrlMaxLen 参数指示）。此参数默认禁用。

将 RDP 客户端配置文件与 VPN 虚拟服务器关联。

这可以通过配置 sessionAction+sessionPolicy 或设置全局 VPN 参数来完成。

示例：

```
add vpn sessionaction <actname> -rdpClientprofile <rdpprofilename>



add vpn sessionpolicy <polname> NS_TRUE <actname>



bind vpn vserver <vservername> -policy <polname> -priority
<prioritynumber>
```

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

或

```
set vpn parameter –rdpClientprofile <name>
```

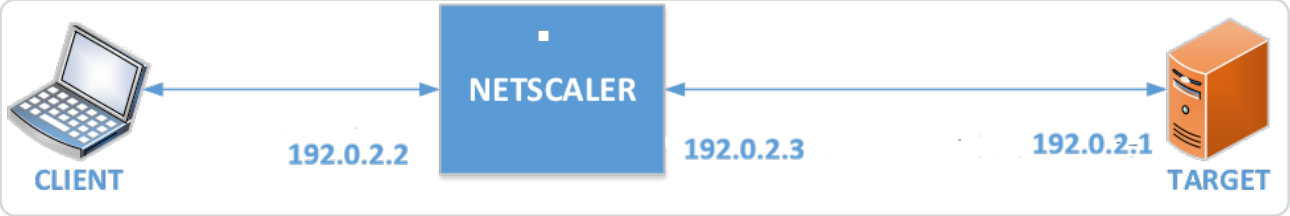
配置服务器配置文件

在侦听器网关上配置服务器配置文件。

```
add rdp ServerProfile <profilename> -rdpIP <IPV4 address of the RDP
listener> -rdpPort <port for terminating RDP client connections> -psk <key
to decrypt RDPTarget/RDPUser information, needed while using STA>`
```

必须在 VPN 虚拟服务器上配置 `rdp ServerProfile`。

```
add vpn vserver v1 SSL <publicIP> <portforterminatingvpnconnections>
-rdpServerProfile <rdpServer Profile>`
```



使用 CLI 配置 RDP 代理

以下是使用 CLI 的 RDP 代理配置示例。

- 为用户添加包含目标信息的 VPN URL。

```
add aaa user Administrator –password freebsd123$%^



add vpn url rdp RdpLink rdp://rdpserverinfo



add dns addrec rdpserverinfo 192.0.2.1
```

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

```
bind aaa user Administrator  –urlName rdp
```

- 为 VPN 连接配置 RDP 客户端和服务器配置文件。

```
add rdp clientprofile p1 –psk citrix -redirectClipboard ENABLE


add rdp serverprofile p1 -rdpIP 192.0.2.2 -psk citrix


add vpn vserver mygateway SSL  192.0.2.2 443 –rdpserverprofile p1


set vpn parameter -clientlessVpnMode ON -defaultAuthorizationAction
ALLOW -rdpClientProfileName p1


add ssl certKey gatewaykey -cert rdp_rootcert.pem  -key rdp_rootkey


bind ssl vserver mygateway -certkeyName gatewaykey
```

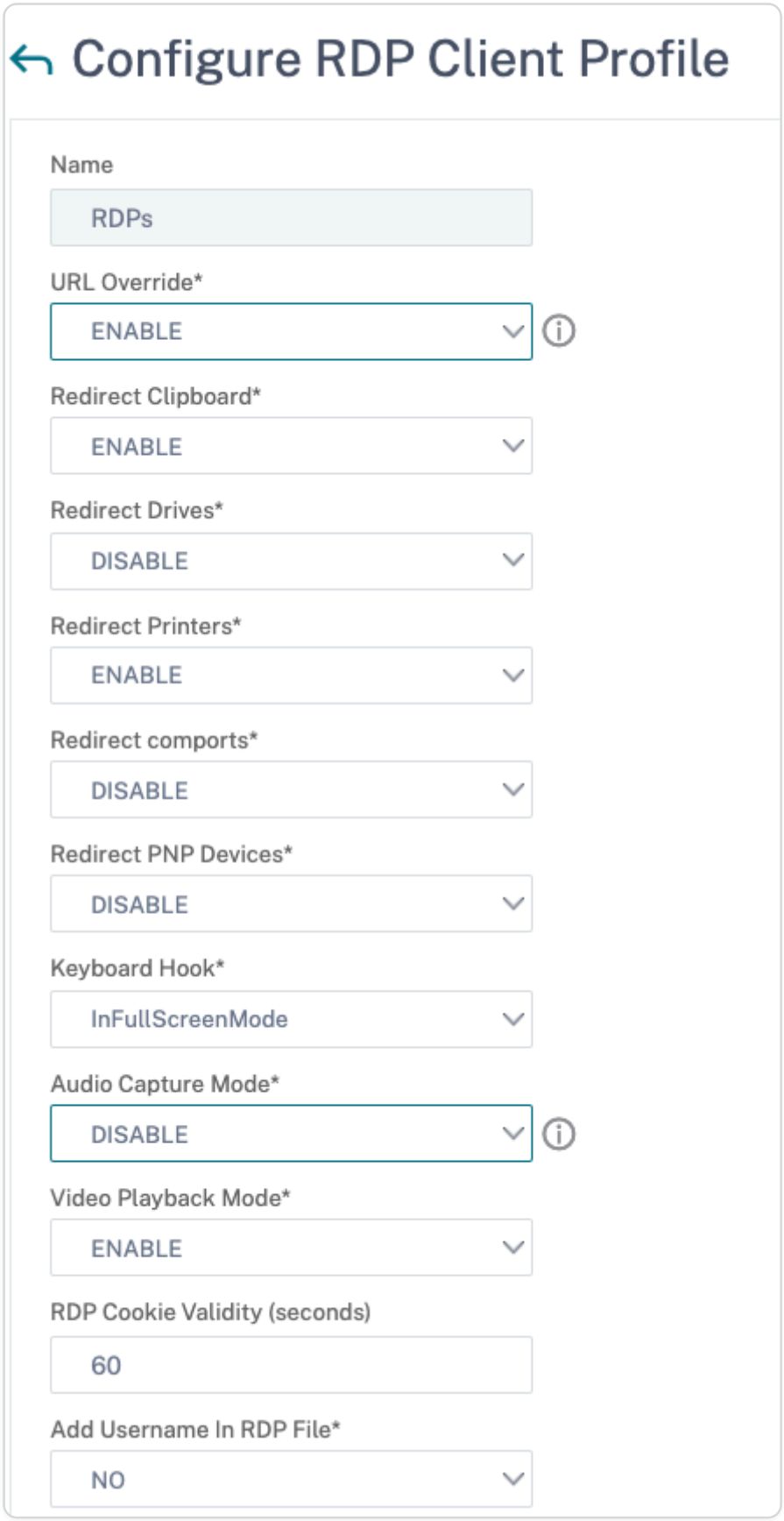
- 添加 SNIP 以实现从 NetScaler 到目标的连接。

```
add ns ip 192.0.2.3  255.255.255.0 –type SNIP
```

使用 GUI 配置 RDP 代理

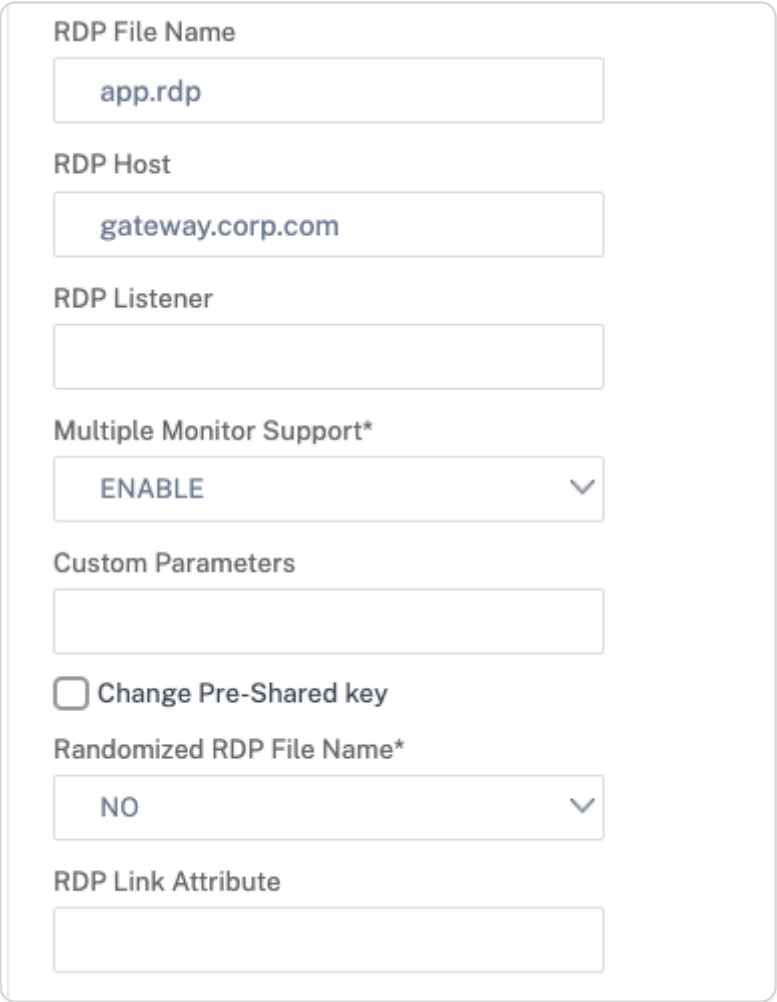
1. 导航到 **NetScaler Gateway > 策略**，右键单击 **RDP**，然后单击 **启用功能**。
2. 在导航窗格上单击 RDP。在右侧，选择 **客户端配置文件** 选项卡，然后单击 **添加**。
3. 输入客户端配置文件的名称并进行配置。

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



4. 在 RDP 主机字段中，输入解析为 RDP 代理侦听器的 FQDN，该 FQDN 通常与 NetScaler Gateway 设备的 FQDN 相同。
5. 在 **预共享密钥** 中，输入密码并单击 **确定**。

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



6. 输入服务器配置文件名称。
7. 输入您将绑定此配置文件的网关虚拟服务器的 IP 地址。
8. 输入您为 RDP 客户端配置文件配置的相同预共享密钥。单击 **创建**。

   重新输入预共享密钥密码(/en-us/netscaler-gateway/media/figure13_createrdpserverprofiles.png)

9. 如果要在无客户端访问门户页面上添加 RDP 书签，请在左侧展开 **NetScaler Gateway**，展开 **资源**，然后单击 **书签**。
10. 在右侧，单击 **添加**。
11. 为书签命名。
12. 对于 URL，输入 **rdp://MyRDPServer using IP or DNS**。
13. 选择使用 **NetScaler Gateway 作为反向代理**，然后单击 **创建**。
14. 根据您的要求创建书签。

    添加多个书签(/en-us/netscaler-gateway/media/figure16_createbookmarks.png)

15. 创建或编辑会话配置文件。导航到 **NetScaler Gateway > 策略 > 会话**。

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

16. 在“安全”选项卡上，将 **默认授权操作** 设置为 **允许**。或者，您可以使用授权策略来控制访问。

    设置默认身份验证操作(/en-us/netscaler-gateway/media/figure17_configuresessionprofile.png)

17. 在“远程桌面”选项卡上，选择您之前创建的 RDP 客户端配置文件。

    选择 RDP 客户端配置文件(/en-us/netscaler-gateway/media/figure18_configuresessionprofile2.png)

18. 如果要使用书签，请在“**客户端体验**”选项卡上，将“**无客户端访问**”设置为“**开**”。

    将无客户端访问设置为开(/en-us/netscaler-gateway/media/figure19_clientexperience.png)

19. 在“**已发布的应用程序**”选项卡上，确保 ICA 代理处于“**关闭**”状态。

    将 ICA 代理设置为关闭(/en-us/netscaler-gateway/media/figure20_publishedapplications.png)

20. 修改或创建网关虚拟服务器。
21. 在“**基本设置**”部分中，单击“**更多**”。

    设置基本设置(/en-us/netscaler-gateway/media/figure21_vpnvirtualserver.png)

22. 使用 RDP 服务器配置文件列表选择您之前创建的 RDP 服务器配置文件。

    使用 RDP 服务器配置文件(/en-us/netscaler-gateway/media/figure22_basicsettings.png)

23. 向下滚动。确保未选中“**仅限 ICA**”。

    将仅限 ICA 设置为关闭(/en-us/netscaler-gateway/media/figure22_ica_only.png)

24. 绑定证书。
25. 绑定身份验证策略。
26. 绑定已配置 RDP 客户端配置文件的会话策略/配置文件。

    绑定会话策略(/en-us/netscaler-gateway/media/figure23_vpnpolicybinding.png)

27. 您可以将书签绑定到 NetScaler Gateway 虚拟服务器或身份验证、授权和审计组。要绑定到 NetScaler Gateway 虚拟服务器，请在右侧的“高级设置”部分中，单击“**已发布的应用程序**”。

    单击已发布的应用程序(/en-us/netscaler-gateway/media/figure24_publishedapplications.png)

28. 在左侧的“**已发布的应用程序**”部分中，单击“**无 Url**”。

    设置无 URL(/en-us/netscaler-gateway/media/figure25_publishedapplications2.png)

29. 绑定您的书签。

    绑定书签(/en-us/netscaler-gateway/media/figure26_bindbookmarks.png)

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

30. 由于未为此 NetScaler Gateway 虚拟服务器指定“仅限 ICA”，请确保您的 NetScaler Gateway Universal 许可证已正确配置。在左侧，展开“**NetScaler Gateway**”，然后单击“**全局设置**”。

    设置全局设置(/en-us/netscaler-gateway/media/figure27_globalsettings.png)

31. 在右侧，单击“**更改身份验证 AAA 设置**”。

    更改身份验证设置(/en-us/netscaler-gateway/media/figure28_changeauthenticationaaasettings.png)

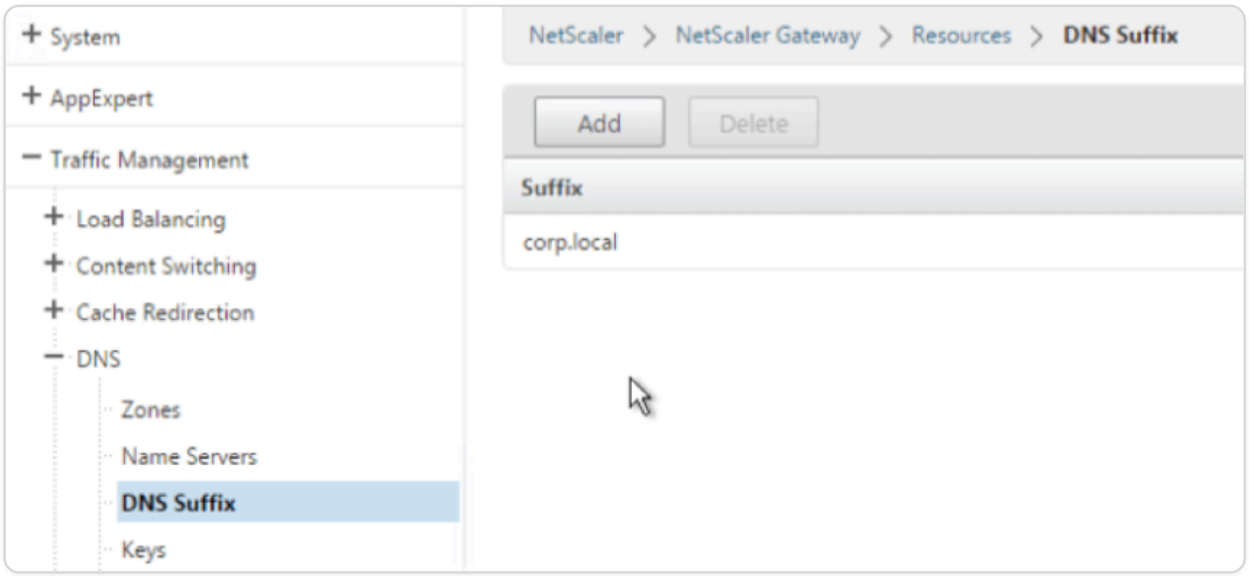
32. 将“**最大用户数**”更改为您的许可限制。

    设置最大用户数(/en-us/netscaler-gateway/media/figure29_configureaaaparameter.png)

33. 如果要使用 DNS 连接到 RDP 服务器，请确保设备上配置了 DNS 服务器（**流量管理 > DNS > 名称服务器**）。

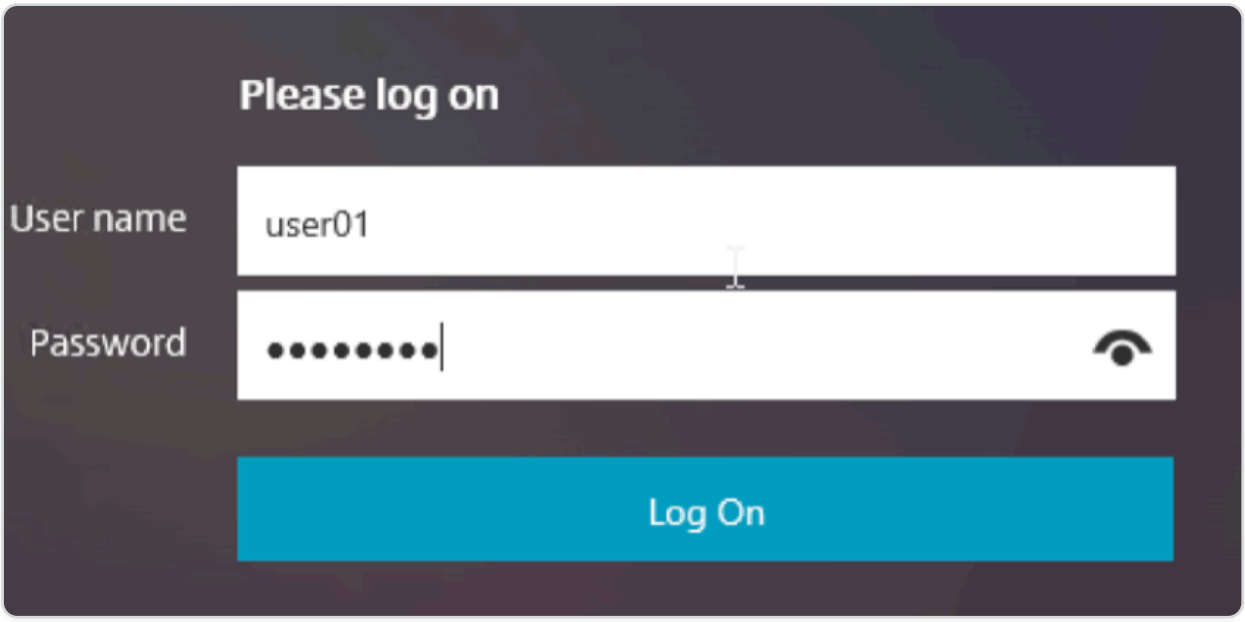
    配置 DNS 服务器(/en-us/netscaler-gateway/media/figure30_dnsservers.png)

34. 如果您想使用短名称而不是 FQDN，请添加 **DNS 后缀（流量管理 > DNS > DNS 后缀）**。

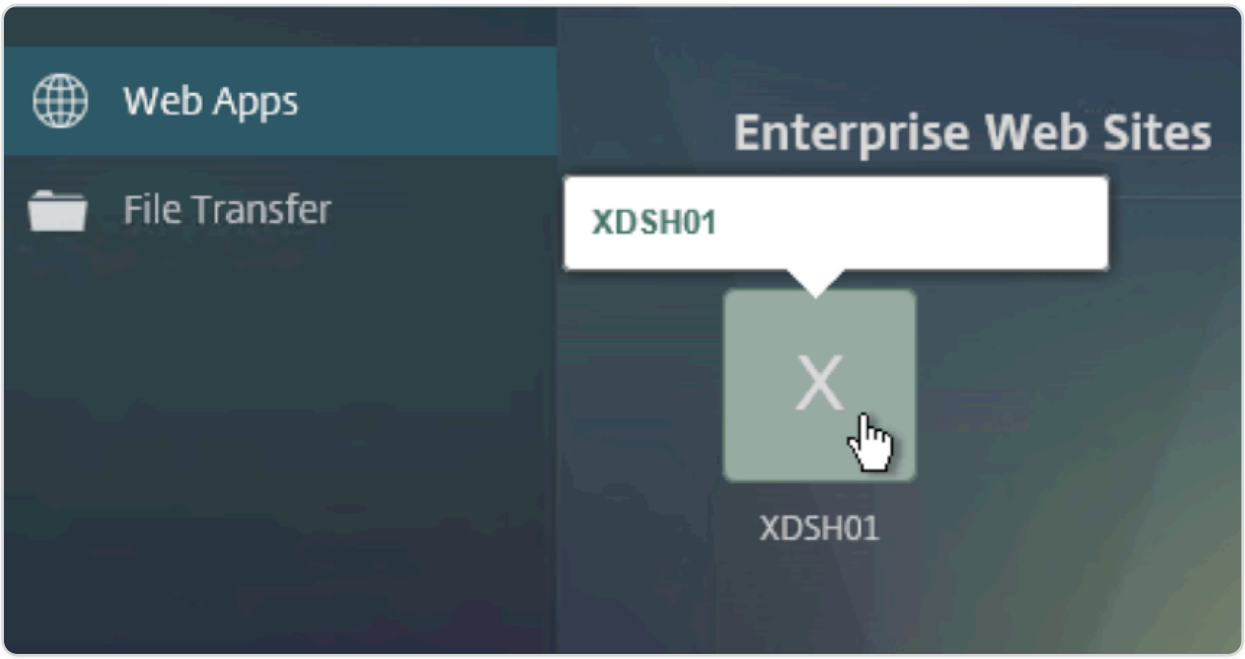


35. 连接到您的网关并登录。

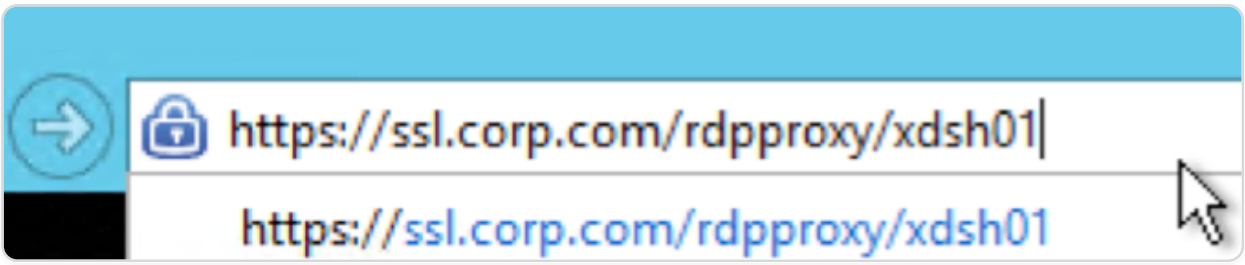
© 1997–2026 Citrix Systems, Inc. All rights reserved.



36. 如果您配置了**书签**，请单击**书签**。



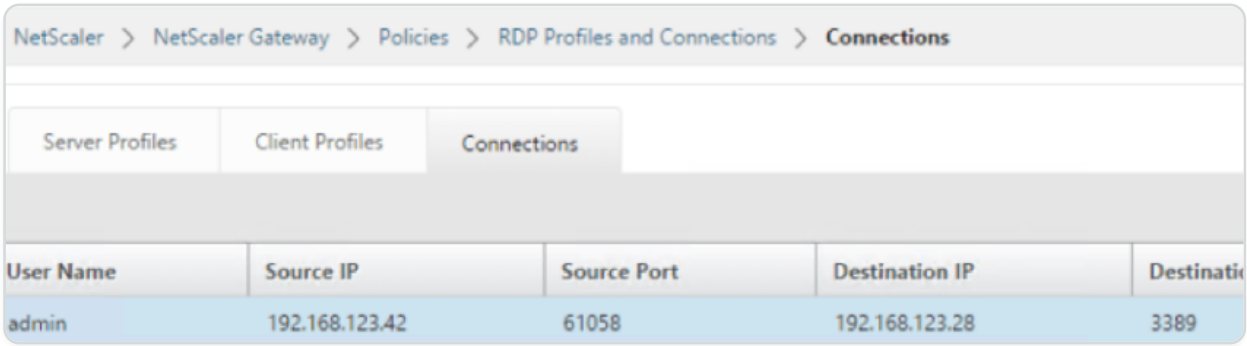
37. 您可以将地址栏更改为 **/rdpproxy/MyRDPServer**。您可以输入 IP 地址（例如 rdpproxy/192.168.1.50）或 DNS 名称（/rdpproxy/myserver）。



38. 打开下载的 `.rdp file`。

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

39. 您可以通过导航到 **NetScaler Gateway 策略 > RDP** 来查看当前连接的用户。右侧是**连接**选项卡。



禁用 SSO 的选项

通过配置 NetScaler 流量策略，可以禁用 RDP 代理的 SSO（单点登录）功能，以便始终提示用户输入凭据。禁用 SSO 后，RDP 强制执行 (SmartAccess) 将不起作用。

示例：

```
add vpn trafficaction <TrafficActionName> HTTP -SSO OFF
```

流量策略可以根据要求进行配置，以下是两个示例：

- 禁用所有流量的SSO：

```
add vpn trafficpolicy <TrafficPolicyName>  "url contains rdpproxy"
<TrafficActionName>
```

- 基于源/目标IP/FQDN禁用SSO

```
add vpn trafficPolicy <TrafficPolicyName>
 "HTTP.REQ.URL.CONTAINS(\"rdpproxy\") && CLIENT.IP.SRC.EQ(<IP>)"
<TrafficActionName>

bind vpnvserver rdp -policy <TrafficPolicyName> -priority 10
```

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

无状态 RDP 代理

无状态 RDP 代理访问 RDP 主机。当用户在单独的 NetScaler Gateway 身份验证器上进行身份验证时，通过 NetScaler Gateway 上的 `RDPListener` 授予访问权限。NetScaler Gateway 所需的 `RDPListener` 信息安全地存储在 STA 服务器上。只要 NetScaler Gateway 和应用程序枚举服务器可以访问，STA 服务器就可以放置在任何位置。有关详细信息，请参阅 `<https://support.citrix.com/article/CTX101997>`。

连接流程

RDP 代理流程涉及两种连接。第一种连接是用户到 NetScaler Gateway VIP 的 SSL VPN 连接，以及 RDP 资源的枚举。

第二种连接是本机 RDP 客户端到 NetScaler Gateway 上的 RDP 侦听器（使用 rdpIP 和 rdpPort 配置）的连接，以及随后安全地代理 RDP 客户端到服务器的数据包。

连接流程图 (/en-us/netscaler-gateway/media/figure2_statelessgatewaycompatibility.png)

1. 用户连接到身份验证器网关 VIP 并提供凭据。
2. 成功登录网关后，用户将被重定向到主页/外部门户，该门户枚举用户可以访问的远程桌面资源。
3. 用户选择 RDP 资源后，身份验证器网关 VIP 收到一个格式为 `https://AGVIP/rdpproxy/ip:port/rdptargetproxy` 的请求，指示用户点击的已发布资源。此请求包含用户选择的 RDP 服务器的 IP 和端口信息。
4. 身份验证器网关处理 /rdpproxy/ 请求。由于用户已通过身份验证，此请求附带有效的网关 cookie。
5. `RDPTarget` 和 `RDPUser` 信息存储在 STA 服务器上，并生成一个 STA 票证。该信息以 XML blob 的形式存储，可选择使用配置的预共享密钥进行加密。如果加密，则 blob 会进行 base64 编码并存储。身份验证器网关使用在网关虚拟服务器上配置的 STA 服务器之一。
6. XML blob 的格式如下

```
<Value name="IPAddress">ipaddr</Value>\n<Value name="Port">port</
Value\>n



<Value name="`Username`">username</Value\>\n<Value
name="Password">pwd\</Value\>
```

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

7. 在 /rdpproxy/ 请求中获得的 `rdptargetproxy` 被设置为 '`fulladdress`'，并且 STA 票证（前缀为 STA AuthID）被设置为 .rdp 文件中的 `loadbalanceinfo`。
8. `.rdp` 文件被发送回客户端端点。
9. 本机 RDP 客户端启动并连接到 `RDPListener Gateway`。它在初始 x.224 数据包中发送 STA 票证。
10. `RDPListener Gateway` 验证 STA 票证并获取 `RDPTarget` 和 `RDPUser` 信息。要使用的 STA 服务器是使用 `loadbalanceinfo` 中存在的“AuthID”检索的。
11. 为存储授权/审计策略创建网关会话。如果用户已存在会话，则会重用该会话。
12. `RDPListener Gateway` 连接到 `RDPTarget` 并使用 CREDSSP 进行单点登录。

先决条件

- 用户在 NetScaler Gateway 身份验证器上进行身份验证。
- 初始的 /rdpproxy URL 和 RDP 客户端连接到不同的 `RDPListener NetScaler Gateway`。
- 使用 STA 服务器的身份验证器网关安全地传递 `RDPListener Gateway` 信息。

使用 CLI 配置无状态 RDP 代理

- 添加 `rdpServer` 配置文件。服务器配置文件在 `RDPListener Gateway` 上配置。

  注意：

  - 一旦在 VPN 虚拟服务器上配置了 rdpServer 配置文件，就无法修改。此外，同一个 serverProfile 不能在另一个 VPN 虚拟服务器上重复使用。

  ```
  add rdpServer Profile [profilename] -rdpIP [IPV4 address of the RDP
  listener] -rdpPort [port for terminating RDP client connections] -psk
  [key to decrypt RDPTarget/RDPUser information, needed while using STA].
  ```

  使用以下命令在 VPN 虚拟服务器上配置 RDP 服务器配置文件：

  ```
  add vpn vserver v1 SSL [publicIP] [portforterminatingvpnconnections]
  -rdpServerProfile [rdpServer Profile]
  ```

  示例

  ```
  add vpn vserver v1 SSL 1.1.1.1 443 -rdpServerProfile rdp_server_prof
  ```

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

重要提示：

- 相同的 STA 服务器必须绑定到 RDP 身份验证器网关和侦听器网关。
- 对于无状态 RDP 代理，STA 服务器验证 RDP 客户端发送的 STA 票证，以获取 RDP 目标服务器和 RDP 用户信息。除了 VPN 虚拟服务器之外，您还必须绑定 STA 服务器。在以下示例中，RDP 目标服务器是 1.1.1.0，RDP 侦听器网关虚拟服务器是 1.1.1.2。

```
add vpn url url4 RDP2 "rdp://1.1.1.0/1.1.1.2:443"
```

使用以下命令在身份验证器网关上配置客户端配置文件：

```
add rdpClient profile <name> -rdpHost <optional FQDN that will be put in
the RDP file as ‘fulladdress’> [-rdpUrlOverride ( ENABLE | DISABLE )] [-
redirectClipboard ( ENABLE | DISABLE )] [-redirectDrives ( ENABLE |
DISABLE )]



        [-redirectPrinters ( ENABLE | DISABLE )] [-keyboardHook
<keyboardHook>] [-audioCaptureMode ( ENABLE | DISABLE )] [-
videoPlaybackMode ( ENABLE | DISABLE )]



        [-rdpCookieValidity <positive_integer>][-multiMonitorSupport
( ENABLE | DISABLE )] [-rdpCustomParams <string>]
```

–rdpHost 配置用于单个网关部署。只有 `psk` 是必填参数，它必须与 RDP 侦听器网关中 RDP 服务器配置文件中添加的 PSK 相同。

- 将 RDP 配置文件与 VPN 虚拟服务器关联。

您可以通过配置 sessionAction+sessionPolicy 或设置全局 VPN 参数来关联 RDP 配置文件。

示例：

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

```
add vpn sessionaction <actname> -rdpClientprofile <rdpprofilename>



add vpn sessionpolicy <polname> NS_TRUE <actname>



bind vpn vserver <vservername> -policy <polname> -priority
<prioritynumber>
```

或

```
set vpn parameter –rdpClientprofile <name>
```

使用 GUI 配置无状态 RDP 代理

无状态 RDP 代理配置涉及以下高级步骤。有关详细步骤，请参阅 RDP 代理配置。

- 创建 RDP 服务器配置文件
- 创建 RDP 客户端配置文件
- 创建虚拟服务器
- 创建书签
- 创建或编辑会话配置文件或策略
- 绑定书签

重要提示：

对于无状态 RDP 代理，除了 VPN 虚拟服务器之外，您还必须绑定一个 STA 服务器。

连接计数器

添加了一个新的连接计数器 ns_rdp_tot_curr_active_conn，用于记录正在使用的活动连接数。它可以在 NetScaler shell 上作为 `nsconmsg` 命令的一部分进行查看。查看这些计数器的 CLI 命令计划稍后添加。

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

升级说明

以前在 VPN 虚拟服务器上配置的 rdpIP 和 rdpPort 现在是 rdpServerProfile 的一部分。 `rdp Profile` 已重命名为 `rdp ClientProfile`，并且参数 clientSSL 已删除。因此，以前的配置将不再起作用。

RDP 连接重定向

NetScaler Gateway 设备现在支持在连接代理或会话目录存在的情况下进行 RDP 连接重定向。RDP 代理通信不再需要为客户端到服务器的每个连接提供独占 URL。相反，代理使用单个 URL 连接到 RDP 服务器场，从而减少了管理员的维护和配置开销。

注意：

- RDP 连接重定向仅在启用 SSO 时受支持，并且在单网关和无状态或双网关模式下均受支持，并带有强制执行 (SmartAccess)。
- RDP 代理功能仅支持基于令牌的重定向，该重定向支持 IP Cookie。当禁用“**使用 IP 地址重定向**”功能时，Windows 会话代理或连接代理会返回基于 IP 的路由令牌“msts=”。
- 您可以在以下位置禁用“**使用 IP 地址重定向**”设置以启用基于令牌的重定向。 `Computer Configuration > Policies > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > RD Connection Broker` 。
- 在 RDSH 计算机上禁用“使用 IP 地址重定向”设置，而不是在连接代理计算机上禁用。
- 可以配置 RDP 代理连接的专用重定向器。

先决条件

- 创建 RDP 服务器配置文件以在 NetScaler Gateway 虚拟服务器上启用 3389 侦听器。 如果您要 RDP 的计算机不是任何 RDS 连接代理基础结构的一部分，则不需要 3389 侦听器。
- 在 NetScaler Gateway 设备上启用 RDP 连接重定向，以在连接代理存在的情况下支持 RDP 代理。

在连接代理存在的情况下部署 RDP 代理

在连接代理存在的情况下，RDP 代理可以通过以下两种方式部署。

- RD 会话主机服务器参与 RD 连接代理负载平衡。
- 在 RDP 负载平衡功能存在的情况下。

当 RD 会话主机服务器参与 RD 连接代理负载平衡时：

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

在这种情况下，RDP URL 链接可以配置为指向其中一个 RDP 服务器作为目标服务器，该服务器充当重定向器。此外，也可以将场中的一个 RDP 服务器作为目标服务器（在这种情况下，该服务器不接受任何 RDP 会话）。

在 RDP 负载平衡功能存在的情况下：

当未启用连接代理负载平衡时，我们可以在 NetScaler 上使用 RDP 负载平衡功能，以便在存在连接代理的情况下对 RDP 会话进行所需的负载平衡。在这种情况下，RDP URL 链接必须配置为将 RDP 负载平衡器作为目标服务器。RDP 负载平衡器可以与 RDP 代理位于同一 NetScaler Gateway 设备上。有关详细信息，请参阅 负载平衡 RDP 服务器。

使用 CLI 在存在连接代理的情况下配置 RDP 代理

在命令提示符下，键入；

```
add rdpserverprofile <Name> -psk <string> -rdpRedirection ( ENABLE |
DISABLE )



add rdpserverprofile serverProfileName -psk “secretString” -rdpRedirection
ENABLE
```

使用 NetScaler GUI 配置 RDP 连接重定向

1. 导航到 **NetScaler Gateway > 策略 > RDP**。
2. 右键单击 **RDP** 以**启用**或**禁用** RDP 重定向功能。

根据 LDAP 属性填充 RDP URL

您可以将 NetScaler Gateway 设备配置为从 LDAP 服务器属性中检索 RDP 服务器（IP/FQDN）列表。根据检索到的列表，设备会显示用户可以访问的服务器的 RDP URL。

使用 CLI 根据 LDAP 属性填充 RDP URL

在命令提示符下，键入：

```
add rdpclientprofile <Name> –rdpUrlLinkAttribute <string>



add rdpclientprofile clientProfileName –rdpUrlLinkAttribute
```

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

```
rdpServerAttribute
```

在前面的示例中，rdpServerAttribute 对应于 LDAP 服务器上给定用户的 RDP 服务器详细信息。

注意：要从 LDAP 服务器获取 LDAP 属性详细信息，LDAP 操作必须配置与 `pUrlLinkAttribute` 相同的字符串，如下所示。

```
add authentication ldapAction dnpg_ldap -serverIP <IP address>-ldapBase
<"domain name"> -ldapBindDn <username> -ldapLoginName sAMAccountName
-ldapbindDnpassword <password>



add authentication ldapAction dnpg_ldap -serverIP 10.102.39.101 -ldapBase
"dc=dnpg-blr,dc=com" -ldapBindDn sqladmin@dnpg-blr.com -ldapLoginName
sAMAccountName -ldapbindDnpassword xxxx



add authentication ldapPolicy dnpg_ldap_pol ns_true dnpg_ldap



bind vpn vs vserver<name> -pol dnpg_ldap_pol



set ldapaction dnpg_ldap -attributes "rdpServerAttribute"



set rdpclientprofile ldap -rdpLinkAttribute rdpServerAttribute
```

LDAP 服务器配置

在 LDAP 服务器上，执行以下步骤：

1. 导航到特定的**用户**。
2. 在 **AD 用户和计算机**中，单击**查看**，然后单击**详细信息**。
3. 右键单击**用户名**，然后单击**属性编辑器**。

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

4. 更改所需的属性 (displayName) 值，然后单击**确定**。

使用 GUI 根据 LDAP 属性填充 RDP URL

1. 导航到 **NetScaler Gateway > 策略 > RDP**。
2. 在**RDP 配置文件和连接**页面上，单击**客户端配置文件**选项卡，然后选择要配置 RDP 链接属性的客户端配置文件。
3. 在“**配置 RDP 客户端配置文件**”页面中，在“**RDP 链接属性**”中，输入 LDAP 属性名称。

   注意： LDAP 属性值可以是逗号分隔列表。

使用 RDP 代理随机化 RDP 文件名

当您点击 RDP URL 时，会下载一个 RDP 文件。再次点击 **RDP URL** 时，会下载一个同名的新 RDP 文件，导致弹出窗口提示用新文件替换现有文件。为避免这种情况，管理员可以选择随机化 RDP 文件名。文件名现在通过在 \<rdpFileName\>_\< `outputof` time()\>.rdp 格式中附加 time() 函数的输出来进行随机化。通过这样做，设备在每次下载文件时都会生成一个唯一的 RDP 文件名。

配置使用 RDP 代理随机化 RDP 文件名的支持

要使用命令行界面在命令提示符下配置使用 RDP 代理随机化 RDP 文件名的支持，请键入：

```
    add rdpclientprofile <profileName> -rdpfileName <filename> -
randomizeRDPFilename <YES/NO>



    add rdpclientprofile clientProfileName -rdpfileName testRDP -
randomizeRDPFilename YES
```

要使用 NetScaler GUI 配置使用 RDP 代理随机化 RDP 文件名的支持，请执行以下操作：

1. 导航到 **NetScaler Gateway** > **策略** > **RDP**。
2. 在 **RDP 配置文件和连接** 页面上，点击 **客户端配置文件** 选项卡，然后选择要配置随机化 RDP 文件名功能的客户端配置文件。
3. 在 **配置 RDP 客户端配置文件** 页面上，在 **随机化 RDP 文件名** 字段旁边的菜单中选择 **YES**。

配置 RDP 文件的名称

下载 RDP 文件后，可以将其以配置的文件名存储在本地。

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

配置 RDP 文件的名称

要使用 CLI 配置 RDP 文件的名称，请在命令提示符下，键入**：

```
set rdpclientprofile <Name> -rdpfilename <filename>.rdp
```

要使用 GUI 配置 RDP 文件的名称：

1. 导航到 **NetScaler Gateway** > **策略** > **RDP**。
2. 在“**RDP 配置文件和连接**”页面上，单击“**客户端配置文件**”选项卡。选择要配置随机 RDP 文件名功能的客户端配置文件。
3. 在“**配置 RDP 客户端配置文件**”页面上，在“**RDP 文件名**”字段中输入 RDP 配置文件的名称。文件名必须采用以下格式：<filename.rdp>。名称最多允许 31 个字符。

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

出站 ICA® 代理支持

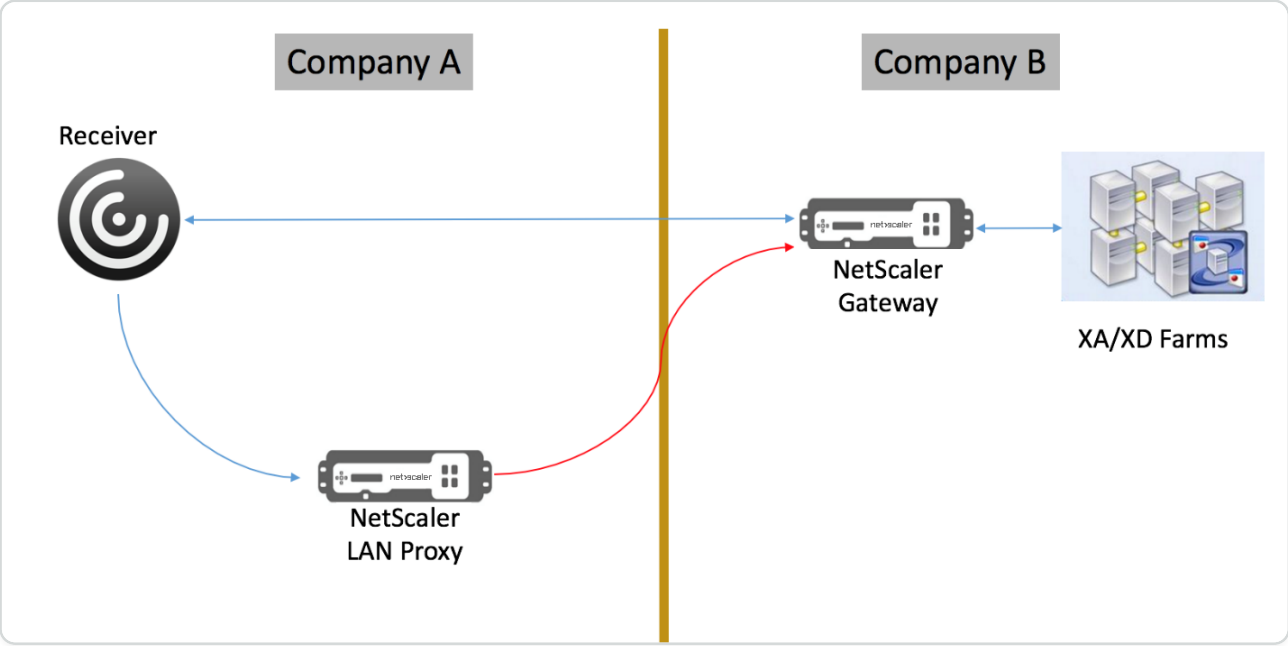
适用于 NetScaler Gateway 的出站 ICA 代理支持使网络管理员能够利用 SmartControl 功能，即使 Receiver 和 NetScaler Gateway 部署在不同的组织中。

以下场景说明了出站 ICA 代理解决方案的用法：

当 Receiver 和 NetScaler Gateway 部署在不同的组织中时，网络管理员需要控制 ICA 会话相关功能。

了解出站 ICA 代理支持

为了将 SmartControl 功能引入拥有接收器的企业组织 A 公司，我们需要添加一个充当 LAN 代理的 NetScaler 设备。NetScaler LAN 代理强制执行 SmartControl 并将流量代理到 B 公司的 NetScaler Gateway。在此部署场景中，Receiver 将流量转发到 NetScaler LAN 代理，这使得 A 公司的网络管理员能够强制执行 SmartControl。部署情况如下图所示。



在此场景中，LAN 代理和 NetScaler Gateway 之间的流量通过 SSL。

注意：

不要在 NetScaler Gateway 上启用基于客户端证书的身份验证。

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

NetScaler LAN 代理上的 SSL 支持

从版本 13.0 build xx.xx 开始，Citrix Workspace 应用程序和 NetScaler LAN 代理之间的流量也支持通过 SSL。Citrix Workspace 应用程序通过 SSL 加密其发送到 LAN 代理的流量。LAN 代理上的 SSL 支持可以与现有部署共存。

要在 Citrix Workspace 应用程序和 NetScaler LAN 代理之间启用通过 SSL 的流量加密，您必须在 NetScaler LAN 代理上执行以下操作：

- 禁用身份验证并在 VPN 虚拟服务器上启用双跳。
- 将 Windows 客户端上的主机设置为 VPN 虚拟服务器的 IP 地址。
- 启用 SNI 和证书验证。
- 添加适当的 CA 证书并全局启用它们。

配置出站 ICA® 代理

出站 ICA 代理配置涉及配置 NetScaler LAN 代理和 NetScaler Gateway。

为 ICA 出站代理配置 NetScaler LAN 代理

您可以使用 CLI 执行以下步骤来配置出站 ICA 代理。

- 添加 VPN 虚拟服务器。

```
add vpn vserver <name> <serviceType> [<IPAddress> [-range
<positive_integer>] [-ipset <string>]] [<port>] [-state ( ENABLED |
DISABLED )] [-authentication ( ON | OFF )] [-doubleHop ( ENABLED |
DISABLED )]
```

- 设置 VPN 参数。

```
set vpn parameter[-backendServerSni ( ENABLED | DISABLED )][-
backendCertValidation ( ENABLED | DISABLED )]
```

- 添加 SSL 证书-密钥对。

```
add ssl certKey ca_cert_verify -cert <certificate name>
```

- 全局绑定 SSL 证书-密钥对。

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

```
bind vpn global -cacert ca_cert_verify
```

示例：

```
-  add vpn vserver ssl_lan_proxy SSL 65.219.17.34 443 -authentication OFF
- doubleHop ENABLED



-  set vpn parameter backendserverSni ENABLED backendcertValidation
ENABLED



-  add ssl certKey dnpg_ca -cert dnpg_ca_cert.cer



-  bind vpn global -cacert dnpg_ca
```

注意：

对于 NetScaler LAN 代理上的 SSL 支持，NetScaler Gateway 配置中无需进行任何更改。

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

NetScaler Gateway 支持 VMware Horizon View 的 PCoIP 代理

NetScaler Gateway 12.0 支持 PC-over-IP (PCoIP) 协议，该协议是包括 VMware Horizon View 在内的多种非 Citrix VDI 解决方案的远程显示协议。PCoIP 类似于 Citrix HDX/ICA 协议和 Microsoft RDP 协议。PCoIP 使用 UDP 端口 4172。

当 PCoIP 通过 NetScaler Gateway 进行代理时，NetScaler Gateway 可以取代传统的 PCoIP 远程访问解决方案，例如 View Security Server 或 VMware Access Point。

以下场景说明了启用 NetScaler Gateway 的 VMWare Horizon View 解决方案的使用。

- 需要通过 NetScaler Gateway 远程访问 VMware Horizon View 桌面池和应用程序池的 VMware Horizon PCoIP 用户，无需部署 Horizon View Security Server 或 VMware Access Point。
- PCoIP 用户通过 NetScaler Gateway 远程访问其他基于 PCoIP 的虚拟桌面解决方案。

注意

NetScaler Gateway 作为远程访问解决方案部署。

配置 NetScaler Gateway 启用的 VMware Horizon View PCoIP 代理

先决条件

版本 - NetScaler 12.0 或更高版本

通用许可证 - PCoIP 代理使用 NetScaler Gateway 的无客户端访问功能，这意味着每个 NetScaler Gateway 连接都必须获得 NetScaler Gateway 通用许可证。在 NetScaler Gateway 虚拟服务器上，确保 **仅限 ICA** 已清除。

Horizon View 基础架构 - 一个功能正常的内部 Horizon View 基础架构。确保您能够在没有 NetScaler Gateway 的情况下内部连接到 Horizon View 代理。确保在 NetScaler 将代理连接到的 View Connection Server 上未启用 Horizon View **HTTP(S) 安全隧道** 和 **PCoIP 安全网关**。 支持以下版本的 VMware Horizon View。

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

- 连接服务器：7.0.1 及更高版本
- Horizon Client：4.2.0 及更高版本（Windows 和 Mac）

防火墙端口：

确保以下事项：

- 必须从 Horizon View 客户端到 NetScaler Gateway VIP 打开 UDP 4172 和 TCP 443。
- 必须从 NetScaler SNIP 到所有内部 Horizon View 代理打开 UDP 4172。
- 在 NAT 后部署的 NetScaler 上支持 PCoIP 代理。以下是需要考虑的重要事项：
  - 支持基于 VPN 虚拟服务器 FQDN 参数设置
  - 仅支持公共可访问的 FQDN，不支持 IP
  - 仅支持 443 和 4172 端口
  - 必须是静态 NAT

证书 – NetScaler Gateway 虚拟服务器的有效证书。

身份验证 – 使用高级语法的 LDAP 身份验证策略/服务器。

统一网关（可选） – 如果是统一网关，请在添加 PCoIP 功能之前创建统一网关。

RfWebUI 门户主题 – 对于通过 Web 浏览器访问 Horizon View，NetScaler Gateway 虚拟服务器必须配置 RfWebUI 主题。

Horizon View 客户端 – 即使使用 NetScaler RfWebUI 门户访问 Horizon 发布图标，也必须在客户端设备上安装 Horizon View 客户端。

配置 NetScaler Gateway 以支持 VMWare Horizon View 的 PCoIP 代理：

1. 导航到 **配置 > NetScaler Gateway 策略 > PCoIP**。
2. 在 **PCoIP Profiles and Connections** 页面上创建虚拟服务器配置文件和 PCoIP 配置文件。
   a. 要创建虚拟服务器配置文件，请在 **VServer Profiles** 选项卡上单击 **Add**。
   b. 输入虚拟服务器配置文件的名称。
   c. 输入用于 View Connection Server 单点登录的 Active Directory 域名，然后单击 **Create**。 **注意：** 每个 NetScaler Gateway 虚拟服务器仅支持一个 Active Directory 域。此外，此处指定的域名将显示在 Horizon View 客户端中。
   d. 单击 **Login**。
   e. 要创建 PCoIP 配置文件，请在 **Profiles** 选项卡上单击 **Add**。

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

   i. 输入 PCoIP 配置文件的名称。
   ii. 输入内部 VMware Horizon View Connection Server 的连接 URL，然后单击 **Create**。

f. 导航到 **配置 > NetScaler Gateway > 策略 > 会话**。
g. 在右侧，选择 **Session Profiles** 选项卡。
h. 在 **NetScaler Gateway Session Policies and Profiles** 页面上，创建或编辑 NetScaler Gateway 会话配置文件。
   i. 要创建 NetScaler Gateway 会话配置文件，请单击 **Add**，然后提供一个名称。
   ii. 要编辑 NetScaler Gateway 会话配置文件，请选择该配置文件，然后单击 **Edit**。
i. 在 **Client Experience** 选项卡上，确保 **Clientless Access** 值设置为 **On**。
j. 在 **Security** 选项卡上，确保 **Default Authorization Action** 值设置为 **ALLOW**。
k. 在 **PCoIP** 选项卡上，选择所需的 PCoIP 配置文件，然后单击 **Create**。您也可以在此选项卡中创建或编辑 PCoIP 配置文件。
l. 单击 **Create** 或 **OK** 完成会话配置文件的创建或编辑。
m. 如果您已创建会话配置文件，则还必须创建相应的会话策略。
   i. 导航到 **配置 > NetScaler Gateway > 策略 > 会话**。
   ii. 选择 **Session Policies** 选项卡，然后单击 **Add**。
   iii. 在“创建 NetScaler Gateway 会话策略”页面中，输入策略的名称。
   iv. 在 **Profile** 中，选择现有配置文件或单击 **Add** 并创建配置文件。
   v. 添加表达式。
      i. 单击“**高级策略**”，然后单击“**表达式编辑器**”。
      ii. 在“**表达式**”中，根据您的要求选择表达式。
   vi. 单击“**确定**”。
n. 将创建的 PCoIP 虚拟服务器配置文件和会话策略绑定到 NetScaler Gateway 虚拟服务器。
   i. 转到“**NetScaler Gateway > 虚拟服务器**”。
   ii. 在右侧，可以“**添加**”新的 NetScaler Gateway 虚拟服务器，也可以“**编辑**”现有的 NetScaler Gateway 虚拟服务器。
   iii. 如果您正在编辑现有的 NetScaler Gateway 虚拟服务器，请在“**基本设置**”部分中单击铅笔图标。
   iv. 对于添加和编辑操作，请在“**基本设置**”部分中单击“**更多**”。

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

v. 使用“**PCoIP VServer 配置文件**”菜单选择所需的 PCoIP 虚拟服务器配置文件。

vi. 向下滚动并确保未选中“仅限 ICA®”。然后单击“**确定**”以关闭“**基本设置**”部分。

vii. 如果您正在创建 NetScaler Gateway 虚拟服务器，请绑定“**证书**”并绑定 LDAP 身份验证策略。

viii. 向下滚动到“**策略**”部分，然后单击加号图标。

ix. “**选择类型**”页面默认显示“**会话**”和“**请求**”。单击“**继续**”。

x. 在“**策略绑定**”部分中，单击“**单击以选择**”。

xi. 选择已配置 PCoIP 配置文件的所需会话策略，然后单击 **选择**。

xii. 在 **策略绑定** 页面中，单击 **绑定**。

xiii. 如果要使用 Web 浏览器连接到 VMware Horizon View，请在 **高级设置** 下添加 **门户主题** 部分。如果您仅使用 Horizon View Client 连接到 NetScaler Gateway，则无需执行此步骤。

xiv. 使用 **门户主题** 菜单选择 **RfWebUI**，然后单击 **确定**。

xv. Horizon View 已发布的图标已添加到 RfWebUI 门户。

注意：

VMware 在使用除 RDP 之外的任何协议时，会使用两个或更多协议。这可能导致请求在两个不同的后端服务器之间进行负载平衡。您可以通过在所有协议之间设置单个持久性组来解决此问题，从而确保所有连接都保留在同一个 Citrix® 虚拟服务器上。

启用 USB 重定向的步骤

连接到客户端计算机的 USB 设备可以从虚拟桌面和应用程序访问。以下是启用 USB 重定向的步骤：

1. 登录到 VMware Horizon 管理控制台。
2. 导航到 **清单 > 查看配置服务器**。
3. 选择 **连接服务器** 选项卡。
4. 选择列出的连接服务器，然后单击 **编辑**。
5. 在 **常规** 选项卡下，在 **HTTP(S) 安全隧道** 下选择 **使用安全隧道连接到计算机** 选项。在 **外部 URL** 字段中提供 NetScaler Gateway 外部 URL。

更新统一网关的内容切换表达式

如果您的 NetScaler Gateway 虚拟服务器位于统一网关（内容切换虚拟服务器）之后，则必须更新内容切换表达式以包含 PCoIP URL 路径。

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

1. 在 NetScaler GUI 中，导航到 **配置 > 流量管理 > 内容切换 > 策略**。
2. 在 **Expression** 区域下附加以下表达式，然后单击 **OK**。

||http.req.url.path.eq("/broker/xml")|| http.req.url.path.contains("/broker/resources")|| http.req.url.path.eq("/pcoip-client")||http.req.url.path.contains("/ice-tunnel")

使用 PCoIP 网关

1. 要连接，您必须在客户端设备上安装 Horizon View Client。安装后，您可以使用 Horizon View Client 的用户界面连接到 NetScaler Gateway，也可以使用 NetScaler Gateway RfWebUI 门户页面查看从 Horizon 发布的图标。
2. 要查看活动的 PCoIP 连接，请转到 **NetScaler Gateway > PCoIP**。
3. 在右侧，切换到 **Connections** 选项卡。活动会话将显示以下数据：用户名、Horizon View Client IP 和 Horizon View Agent 目标 IP。
4. 要终止连接，请右键单击 **Connection** 选项卡，然后单击 **Kill Connection**。或者单击 **Kill All Connections** 以终止所有 PCoIP 连接。

配置 VMware Horizon View 连接服务器

为了通过 NetScaler Gateway 支持 PCoIP 代理：

登录到 **VMware Horizon 管理控制台**。

2. 导航到 **清单** --\> **视图配置** --\> **服务器**。
3. 选择**连接服务器**选项卡。
4. 选择一个列出的连接服务器，然后单击**编辑**。
5. 在**常规**选项卡下，取消选择 HTTP(S) 安全隧道下的**使用安全隧道连接**到计算机选项。
6. 单击**确定**以关闭**编辑连接服务器设置**窗口。
7. 对所有列出的连接服务器重复步骤 4 到 6。

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

NetScaler Gateway 出站代理支持的代理自动配置

当您配置 NetScaler Gateway 设备以支持代理自动配置 (PAC) 时，PAC 文件的 URL 会被推送到客户端浏览器。然后，客户端的流量将根据 PAC 文件中定义的条件重定向到相应的代理。

以下是 PAC 用于出站代理的一些常见用例：

- 配置多个处理客户端流量的代理服务器。
- 在子网之间对代理流量进行负载均衡。

使用 CLI 配置 NetScaler Gateway 全局参数以支持出站代理的 PAC

在命令提示符下，键入：

```
set vpn parameter -proxy BROWSER -autoProxyUrl <URL>
```

使用 CLI 在会话配置文件中配置 NetScaler Gateway 以支持 PAC

在命令提示符下，键入：

```
add vpn sessionAction <name> -proxy BROWSER -autoProxyUrl <URL>
```

其中；

- **URL** – 代理服务器的 URL
- **名称** – VPN 会话操作的名称

使用 GUI 配置 NetScaler Gateway 全局参数以支持出站代理的 PAC

1. 导航到 **配置 > NetScaler Gateway > 全局设置**。

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

2. 在 **Global Settings** 页面上，单击 **Change Global Settings**，然后选择 **Client Experience tab**。
3. 在**客户端体验**选项卡上，选择**高级设置**，然后选择**代理选项卡**。
4. 在**代理选项卡**上，选择**浏览器**，然后选择**使用自动配置**。
5. 在**自动代理配置文件 URL** 字段中，键入所需 PAC 文件的 URL。
6. 单击**创建**。

使用 GUI 配置 NetScaler Gateway 以支持会话配置文件上的 PAC

1. 导航到**配置> NetScaler Gateway> 策略> 会话**。
2. 在 NetScaler Gateway **会话策略和配置文件**页面上，创建 NetScaler Gateway 会话配置文件。
3. 选择**会话配置文件**选项卡，单击**添加**，然后输入名称。
4. 在**客户端体验**选项卡上，选择**高级设置**，然后选择**代理**选项卡。
5. 在**代理**选项卡上，选择**浏览器**，然后选择**使用自动配置**。
6. 在**自动代理配置文件 URL** 字段中，键入所需 PAC 文件的 URL。
7. 单击**创建**。
8. 单击**创建**。

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

SameSite cookie 属性的配置支持

`SameSite` 属性指示浏览器 cookie 是可用于跨站点上下文还是仅用于同站点上下文。如果应用程序打算在跨站点上下文中访问，则只能通过 HTTPS 连接进行访问。有关详细信息，请参阅 RFC6265。

直到 2020 年 2 月，NetScaler 设备中未明确设置 `SameSite` 属性。浏览器采用默认值 (None)。未设置 `SameSite` 属性并未影响 NetScaler Gateway 和 NetScaler AAA 部署。

随着某些浏览器（例如 Google Chrome 80）的升级，cookie 的默认跨域行为发生了变化。`SameSite` 属性可以设置为以下值之一。Google Chrome 的默认值设置为 Lax。对于其他浏览器的某些版本，`SameSite` 属性的默认值可能仍设置为 None。

- **None**：指示浏览器仅在安全连接上在跨站点上下文中使用 cookie。
- **Lax**：指示浏览器在同站点上下文的请求中使用 cookie。在跨站点上下文中，只有安全的 HTTP 方法（如 GET 请求）才能使用 cookie。
- **Strict**：仅在同站点上下文中使用 cookie。

如果 cookie 中没有 `SameSite` 属性，Google Chrome 会假定 `SameSite` = Lax 的功能。 因此，对于在需要浏览器插入 cookie 的跨站点上下文的 iframe 中进行的部署，Google Chrome 不会共享跨站点 cookie。因此，网站中的 iframe 可能无法加载。

配置 `SameSite` cookie 属性

已将名为 `SameSite` 的新 cookie 属性添加到 VPN 和 NetScaler AAA 虚拟服务器。此属性可在全局级别和虚拟服务器级别设置。

要配置 `SameSite` 属性，必须执行以下操作：

1. 为虚拟服务器设置 `SameSite` 属性
2. 将 cookie 绑定到 `patset` （如果浏览器丢弃了跨站点 cookie）

使用 CLI 设置 `SameSite` 属性

要在虚拟服务器级别设置 `SameSite` 属性，请使用以下命令。

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

```
set vpn vserver VP1 -SameSite  [ STRICT | LAX | None ]

set aaa vserver VP1 -SameSite  [ STRICT | LAX | None ]
```

要在全局级别设置 `SameSite` 属性，请使用以下命令。

```
set vpn param VP1 -SameSite  [ STRICT | LAX | None ]

set aaa param VP1 -SameSite  [ STRICT | LAX | None ]
```

注意：虚拟服务器级别设置优先于全局级别设置。Citrix 建议在虚拟服务器级别设置 `SameSite` cookie 属性。

使用 CLI 将 Cookie 绑定到 `patset`

如果浏览器丢弃跨站点 cookie，您可以将该 cookie 字符串绑定到现有的 `ns_cookies_SameSite patset`，以便将 `SameSite` 属性添加到 cookie 中。

示例：

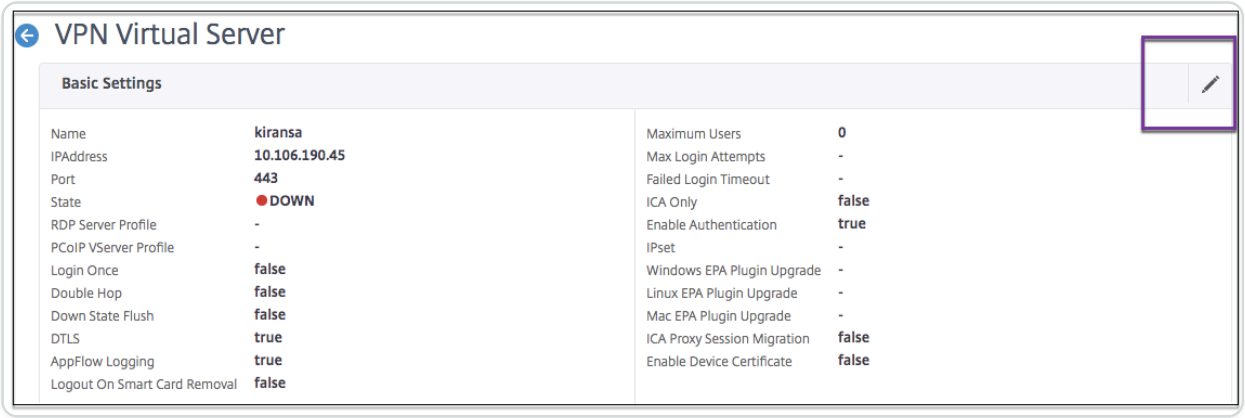
```
bind patset ns_cookies_SameSite "NSC_TASS"

bind patset ns_cookies_SameSite "NSC_TMAS"
```

使用 GUI 设置 SameSite 属性

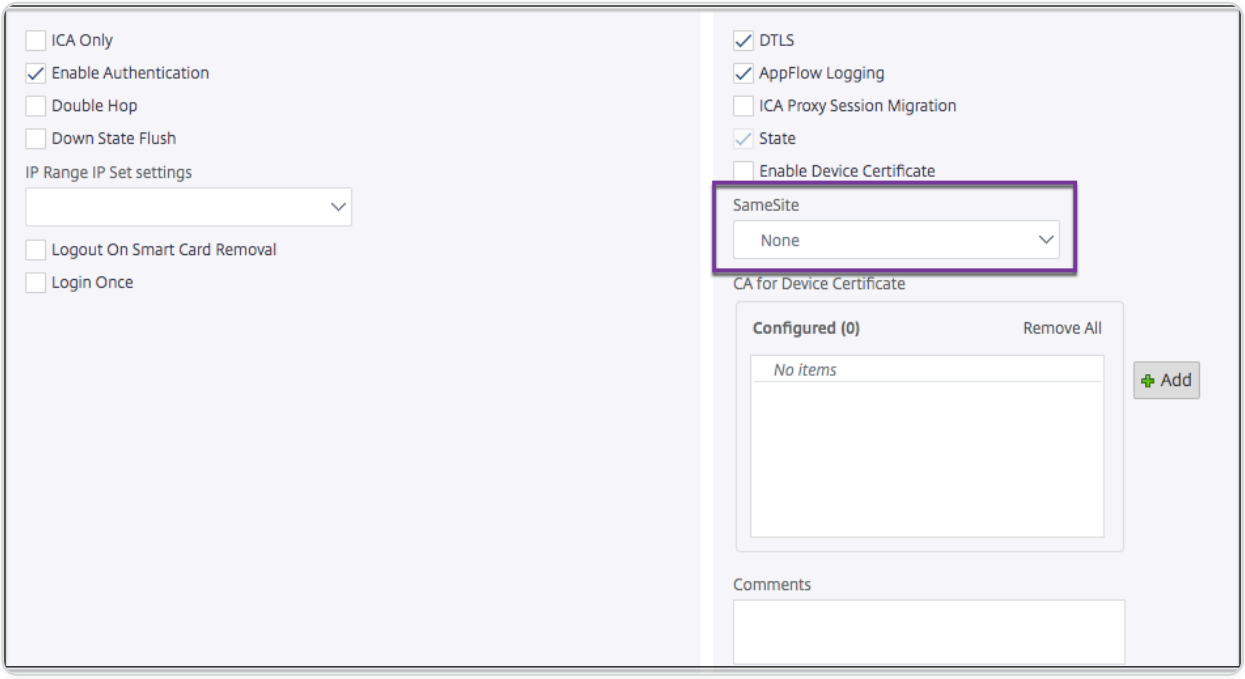
要在虚拟服务器级别设置 `SameSite` 属性：

1. 导航到 **NetScaler Gateway > 虚拟服务器**。
2. 选择一个虚拟服务器，然后单击**编辑**。
3. 在**基本设置**部分中选择编辑图标，然后单击**更多**。

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



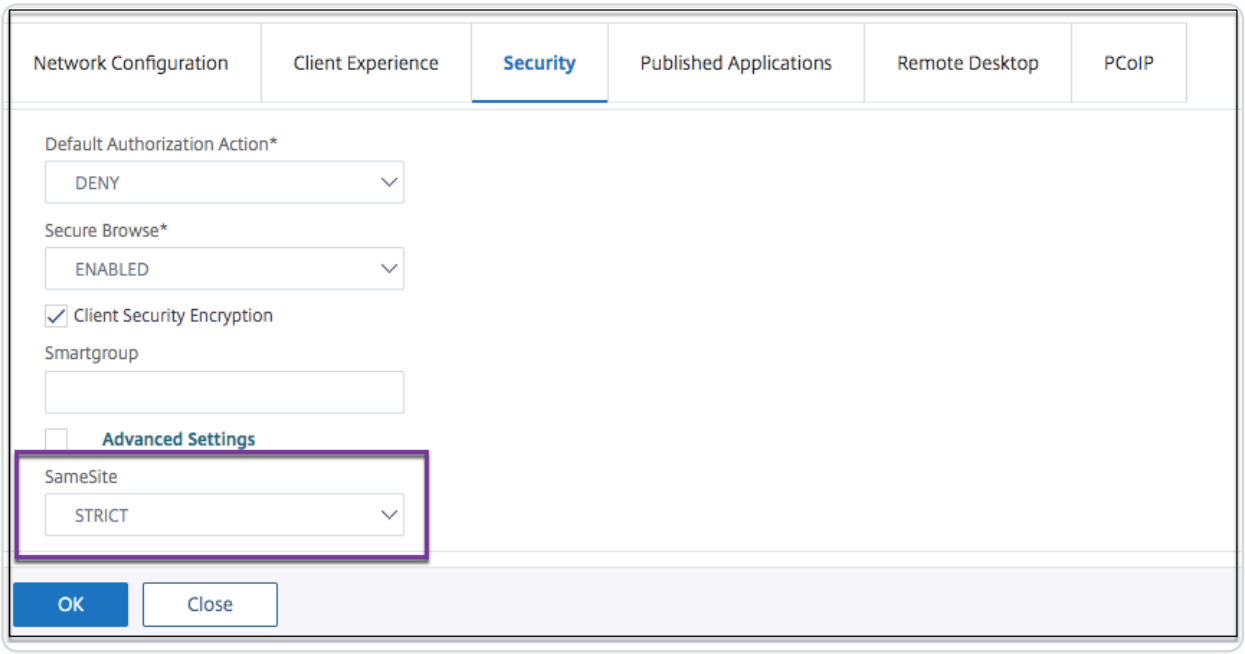
4. 在 **SameSite** 中，根据需要选择选项。



要在全局级别设置 `SameSite` 属性：

1. 导航到 **NetScaler Gateway > 全局设置 > 更改全局设置。**
2. 点击“**安全**”选项卡。
3. 在 `SameSite` 中，根据需要选择选项。

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



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

使用 Citrix SD-WAN™ WANOP 优化网络流量

当用户使用 Citrix Secure Access 客户端登录时，可以通过使用 Citrix SD-WAN WANOP 插件来优化连接，该插件从 Citrix SD-WAN WANOP 安装到用户设备上。当连接通过 Citrix SD-WAN WANOP 插件进行优化时，网络流量会通过 NetScaler Gateway 进行压缩和加速。当为连接启用 Citrix SD-WAN WANOP 时，NetScaler Gateway 上的 TCP 压缩策略将被禁用。

Citrix SD-WAN WANOP 插件已部署并与 Citrix Secure Access™ 客户端兼容。

NetScaler Gateway 支持 Repeater 插件的 5.5 和 6.1 版本以及 Citrix SD-WAN WANOP 插件的 6.2 和 7.0 版本。

Citrix SD-WAN WAN 优化和流量控制优先于需要动态内容修改的 NetScaler Gateway 优化功能。如果为 HTTP 流量启用了 Citrix SD-WAN WAN 优化，则以下 NetScaler Gateway 功能将不可用：

- Web 应用程序的单点登录
- 文件类型关联
- HTTP 授权

要允许 Web 应用程序的单点登录，可以禁用 HTTP 上的加速。为此，请使用命令行。登录到 NetScaler Gateway 串行控制台，然后在命令提示符下键入：

```
add vpn trafficAction ssoact http -SSO ON
```

目标为 NetScaler Gateway 上配置的 HTTP 端口的网络流量会自动从 Citrix SD-WAN WAN 优化中排除。这是默认设置。如果您为 HTTP 端口上的 Citrix SD-WAN WAN 优化配置了流量策略，则该流量策略将生效，并且网络流量将由 Citrix SD-WAN WANOP 进行优化。但是，对于受该策略影响的所有流量，NetScaler Gateway 优化功能将被禁用。Citrix SD-WAN WANOP 可以加速目标为非 HTTP 端口的网络流量，而不会影响其他 NetScaler Gateway 功能。

您可以使用流量策略来配置用户连接以使用 Citrix SD-WAN WANOP 插件。然后，您可以将策略绑定到用户、组、虚拟服务器或全局。策略的优先级取决于您绑定策略的位置或您为策略指定的优先级编号。

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

创建流量策略

1. 导航到 **NetScaler Gateway > 策略 > 流量**。
2. 在详细信息窗格中，单击 **添加**。
3. 在 **名称** 中，键入策略的名称。
4. 在请求配置文件旁边，单击 **新建**。
5. 在 **名称** 中，键入配置文件的名称。
6. 在 **分支中继器** 中，选择 **开**，然后单击 **创建**。
7. 在 **创建流量策略** 对话框中，在 **添加表达式** 旁边，选择或输入一个表达式，该表达式表示要启用 Citrix SD-WAN WANOP 加速的流量类型。
8. 单击 **添加表达式**，单击 **创建**。然后单击 **关闭**。

添加表达式时，选择一个网络表达式，以使用 Citrix SD-WAN WANOP 配置为加速的相同 IP 地址和端口范围。为了实现 Citrix SD-WAN WANOP 加速，在 NetScaler Gateway 上配置的流量类型必须与在 Citrix SD-WAN WANOP 上配置的服务类策略匹配。

所有 TCP 流量都受益于 Citrix SD-WAN WANOP 加速。如果您计划使用单点登录，请勿加速 HTTP 流量，因为加速会禁用单点登录。

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

网关用户体验配置中的 RfWebUI 角色

RfWebUI 角色是一种主题，为通过 NetScaler Gateway 登录的 NetScaler Gateway 用户提供新的登录和门户页面。该门户向 Receiver、StoreFront 和 Citrix Endpoint Management 用户提供与他们直接访问这些产品时相同的图形用户界面 (GUI)。

何时使用 RfWebUI 角色

当您需要不同 NetScaler 产品（例如 Web 和软件即服务 (SaaS) 应用程序、虚拟 Windows 应用程序和桌面）提供的所有应用程序的单一视图时，请在 NetScaler Gateway 中使用 RfWebUI 角色。

以下场景说明了 RfWebUI 角色的使用。

- 用户通过网关访问 StoreFront™ 时，发现其 GUI 与不通过网关访问产品时看到的 GUI 不同。

  解决方案： 当用户通过网关访问 StoreFront 时，RfWebUI 主题提供与他们不通过网关访问产品时看到的类似用户界面。

- 用户通过网关访问 Citrix Workspace 应用程序、StoreFront 和 Citrix Endpoint Management 应用程序时，由于应用程序未按逻辑方式分组，因此难以找到所需的应用程序。

  解决方案： RfWebUI 角色通过对不同产品（例如 Receiver、StoreFront、Citrix Endpoint Management™ 等）提供的应用程序进行逻辑捆绑，提供单一视图用户体验。

RfWebUI 角色提供的功能

新的 RfWebUI 提供以下功能：

- GO
- 应用程序聚合
- 用户配置的远程桌面协议 (RDP) 代理链接
- 常用应用程序

GO

GO： Go 功能通过无客户端 VPN 提供对网页的访问。用户只需在“**书签**”选项卡的“**URL**”部分中键入 URL，然后单击“**GO**”即可。

目前，**GO** 功能仅支持 Outlook Web Application (OWA) 和 SharePoint URL。

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

注意 仅当会话策略中的 `clientlessAccessVPNMode` 参数为“**已启用**”时，**GO** 选项卡才可见。

应用程序聚合

应用程序聚合： RfWebUI 主题通过将不同产品提供的应用程序捆绑在描述性横幅下，提供了一个单窗格视图。例如，NetScaler 管理员配置的所有 VPN URL 都位于名为“**Web 和 SaaS 应用程序**”的捆绑包中，而用户特定的 Web 书签则位于“**个人书签**”下。如果在 StoreFront 中配置了 Citrix Virtual Apps and Desktops 应用程序捆绑包，则 NetScaler Gateway 中的单窗格视图也会列出这些捆绑包。

用户配置的 RDP 代理链接

用户可以将 RDP 代理链接添加为个人书签。个人书签显示在“**桌面**”选项卡下。

支持以下 RDP 模式：

- 单个网关
- 无状态（双）网关

注意： 仅当配置了 `RDPclientprofile` 时，用户才能添加 RDP 代理链接。有关 RDP 配置的更多信息，请参阅 RDP 代理文档。

常用应用程序

用户可以通过单击应用程序名称旁边的“**添加到收藏夹**”链接，将“**Web 和 SaaS 应用程序**”以及“**个人书签**”下列出的所需应用程序添加到“**收藏夹**”选项卡。添加的应用程序可以在“**收藏夹**”选项卡下查看。也可以通过单击“**收藏夹**”选项卡中应用程序旁边的“**删除**”链接，将其从“**收藏夹**”选项卡中删除。

启用 RfWebUI Persona 时的注意事项

RfWebUI persona 不完全支持以下功能：

文件共享功能： 不支持用于访问 SMB 文件共享的文件共享功能。 **电子邮件主页：** “**电子邮件主页**”VPN 参数不作为 NetScaler Gateway 门户的嵌入式视图提供。它可以在 RfWebUI 的“**应用程序**”选项卡下的“**Web 和 SaaS 应用程序**”捆绑包中作为应用程序访问。 **Java 客户端：** 此主题中不提供用于建立 SSL 隧道的基于浏览器的 Java 客户端。

配置 RfWebUI 界面风格

应用 RfWebUI 界面风格：

1. 在 NetScaler 界面中，导航到 **Configuration > NetScaler Gateway Portal Themes**。

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

2. 在 **Portal Themes** 页面上，选择 **RfWebUI** 复选框。
3. 单击 **Portal Themes** 页面右上角的 **Save** 图标。
4. 在 **Save Confirmation** 对话框中，单击 **Yes**。

RfWebUI 配置参数

NetScaler Gateway 门户的整体行为受两个配置文件影响：本地 NetScaler Gateway 配置文件和 StoreFront 文件。

根据您的部署，您可以通过更改“plugins.xml”文件中的属性来修改 NetScaler Gateway 门户行为。此文件在浏览器上显示为配置文件，这是对 `/var/netscaler/logon/themes/<custom_theme>/plugins.xml` 的请求。

登录期间，使用 NetScaler Gateway 配置文件。但是，当连接到 StoreFront 时，StoreFront 会发送新的配置，并且早期配置会被覆盖。此行为对于无客户端 VPN 和 ICA 有所不同。

对于 ICA，StoreFront 配置始终优先，但无客户端 VPN 中受 NetScaler Gateway 配置影响的某些行为即使在 StoreFront 更新新配置后仍会保留。

下表列出了优先于无客户端 VPN 和 ICA 的配置参数。

配置类型	子配置类型	参数	无客户端 VPN	ICA	描述
无客户端 VPN 的会话 / ICA 的 AuthManager	-	loginFormTimeout	NetScaler 网关	-	定义登录页面超时时间（分钟）
插件助手	-	已启用	StoreFront	StoreFront	启用或禁用插件助手
插件助手	-	upgradeAtLogin	StoreFront	StoreFront	在登录时提示升级插件
插件助手	-	showAfterLogin	NetScaler 网关	StoreFront	登录后显示插件提示
插件助手	-	showOnlyIfRequiredByApps	NetScaler 网关	StoreFront	如果应用程序需要，登

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

配置类型	子配置类型	参数	无客户端 VPN	ICA	描述
					录后显示插件提示
插件助手	macOS/ win32	路径	NetScaler 网关	StoreFront	定义插件的下载路径
插件助手	protocolHandler	已启用	NetScaler 网关	StoreFront	在启动插件之前切换协议处理程序页面
插件助手	protocolHandler	平台	NetScaler 网关	StoreFront	标识插件支持的平台
插件助手	-	skipDoubleHopCheckWhenDisabled	• NetScaler 网关	StoreFront	切换 ICA 直通的双跳 NetScaler Gateway 配置检查
用户界面	-	frameOptions	NA	NA	-
用户界面		autoLaunchDesktop	StoreFront	StoreFront	启用或禁用桌面启动
用户界面	workspaceControl	已启用	StoreFront	StoreFront	启用或禁用工作区控制
用户界面	workspaceControl	autoReconnectAtLogon	StoreFront	StoreFront	切换以在可用时自动重新连接到上一个会话
用户界面	workspaceControl	logoffAction	StoreFront	StoreFront	定义 Citrix Workspace 的注销行为
用户界面	workspaceControl	showReconnectButton	StoreFront	StoreFront	显示或隐藏“**重新连接**”按钮

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

配置类型	子配置类型	参数	无客户端 VPN	ICA	描述
用户界面	workspaceControl	showDisconnectButton	StoreFront	StoreFront	显示或隐藏**断开连接**按钮
用户界面	workspaceControl	showDesktopsView	StoreFront	StoreFront	显示或隐藏桌面视图
用户界面	workspaceControl	showAppsView	StoreFront	StoreFront	显示或隐藏应用程序视图
用户界面	workspaceControl	defaultView	StoreFront	StoreFront	选择桌面视图或应用程序视图
用户界面	receiverConfiguration	启用	StoreFront	StoreFront	切换接收器配置
用户界面	receiverConfiguration	showOnlyIfRequiredByApps	NetScaler 网关	NetScaler 网关	如果应用程序需要，显示接收器提示
用户界面	receiverConfiguration	downloadURL	StoreFront	StoreFront	下载接收器的 URL
用户界面	appShortcuts	已启用	StoreFront	StoreFront	启用或禁用应用程序快捷方式选项卡
用户界面	appShortcuts	allowSessionReconnect	StoreFront	StoreFront	允许会话重新连接

为了在 RfWebUI 中反映无客户端 VPN 和 ICA 的修改后的 StoreFront 配置，请手动更新 NetScaler Gateway 配置文件中的相应参数。例如，如果 StoreFront 配置中 `if pluginAssistant.html5.enabled` 设置为 `Off`，请更新 NetScaler Gateway 配置文件中的相应参数。

请按照以下步骤自定义 NetScaler Gateway 配置文件中的 RfWebUI 参数以匹配 StoreFront 配置：

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

1. 打开 `/var/netscaler/logon/themes/<customtheme>/plugins.xml`。

   注意：

   如果自定义主题是在旧版本上创建的，则自定义主题文件夹中的“plugins.xml”文件可能为空。运行以下命令以使用所需内容填充“plugins.xml”。

   `cp /var/netscaler/logon/LogonPoint/homeconfig.xml /var/netscaler/logon/themes/<customtheme>/plugins.xml`

   请勿修改 `/var/netscaler/logon/LogonPoint/homeconfig.xml`。

2. 仅编辑所需参数，并使用以下命令刷新 NetScaler® 缓存：

   `flush cache contentgroup loginstaticobjects`

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

使用自定义插件进行网关门户定制

NetScaler Gateway RfWebUi 框架提供了添加自定义插件以定制其网关门户的功能。这些自定义插件可用于为网关添加大量功能，例如，如果您想在网关流程中添加一个全新的页面。对于其他用例，可以将代码添加到为网关主题提供的自定义脚本文件中的 `/var/netscaler/logon/themes/<custom_theme>/script.js` 位置。

注意：

NetScaler Gateway 仅支持为门户定制创建和使用自定义插件。NetScaler Gateway 不会根据客户要求创建或提供任何自定义插件。

1. 要添加自定义插件，请在 `/var/netscaler/logon/LogonPoint/plugins/ns-gateway/` 位置创建 JavaScript 文件。例如，您可以在 `/var/netscaler/logon/LogonPoint/plugins/ns-gateway/` 中找到以下插件。

   - ns-nfactor.js
   - nsg-epa.js
   - nsg-setclient.js

   建议以 `<plugin_name>`.js 格式输入插件名称。

   所有这些插件文件都由功能所需的 RfWebUI 框架获取。

2. 创建插件文件后，请使用以下代码作为示例，将插件注册到 RfWebUI 框架。

```
(function ($) {

            CTXS.ExtensionAPI.addPlugin( {

                        Name : “plugin name”,

                        initialize: function() {}

            });

    })(jQuery);
```

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

其中，

name 是赋予插件的名称。它用作插件的标识符。

initialize 将函数作为参数，用于初始化插件。

3. 在 `CTXS.ExtensionAPI.addPlugin()` 函数中输入插件名称和初始化函数以注册插件。 添加的插件名称和位置必须注册到 `/var/netscaler/logon/themes/<custom_theme>/plugins.xml` 位置的 plugins.xml 文件中。
4. 编写插件代码后，必须在 `/var/netscaler/logon/themes/<custom_theme>/plugins.xml` 位置的 `plugins.xml` 文件中注册新添加的插件名称和位置。必须使用 `plug-in` 标签注册插件。

```
<plugins>

<plugin name="nsg-epa" src="plugins/ns-gateway/nsg-epa.js"/>

<plugin name="nsg-setclient" src="plugins/ns-gateway/nsg-setclient.js"/
>

<plugin name="ns-nfactorn" src="plugins/ns-gateway/ns-nfactor.js"/>

</plugins>
```

5. 为插件输入名称和 src，以便 RFWebUI 可以识别并获取该插件。

示例配置

以下示例配置可用于添加自定义插件，以便为 NetScaler Gateway 登录页面添加页脚。

1. 在 `/var/netscaler/logon/LogonPoint/plugins/ns-gateway/.` 位置创建 JavaScript 插件文件.
2. 将插件命名为 ns-footer.js `/var/netscaler/logon/LogonPoint/plugins/ns-gateway/ns-footer.js`
3. 将以下代码添加到 RfWebUI 中已注册的插件，并在初始化函数中将页脚添加到网关。

```
(function ($) {

CTXS.ExtensionAPI.addPlugin({
```

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

```
    name: "ns-footer", // Name of plugin - must match name sent in
configuration

    initialize: function () {



    // Add the footer for the login page

    $("#customExplicitAuthBottom").append("<div style='text-
align:center;color:white;font-size:15px;'><br />Disclaimer<br /><br /
>"+" Access to this website is restricted to employees of Login
Consultants<br/></div>");



    // To Add the footer to the login timeout page

    $("#customAuthBottom").append("<div style='text-
align:center;color:white;font-size:15px;'><br >Disclaimer<br /><br /
>"+" Access to this website is restricted to employees of Login
Consultants<br /></div>");



    callback();

    }

});

})(jQuery);
```

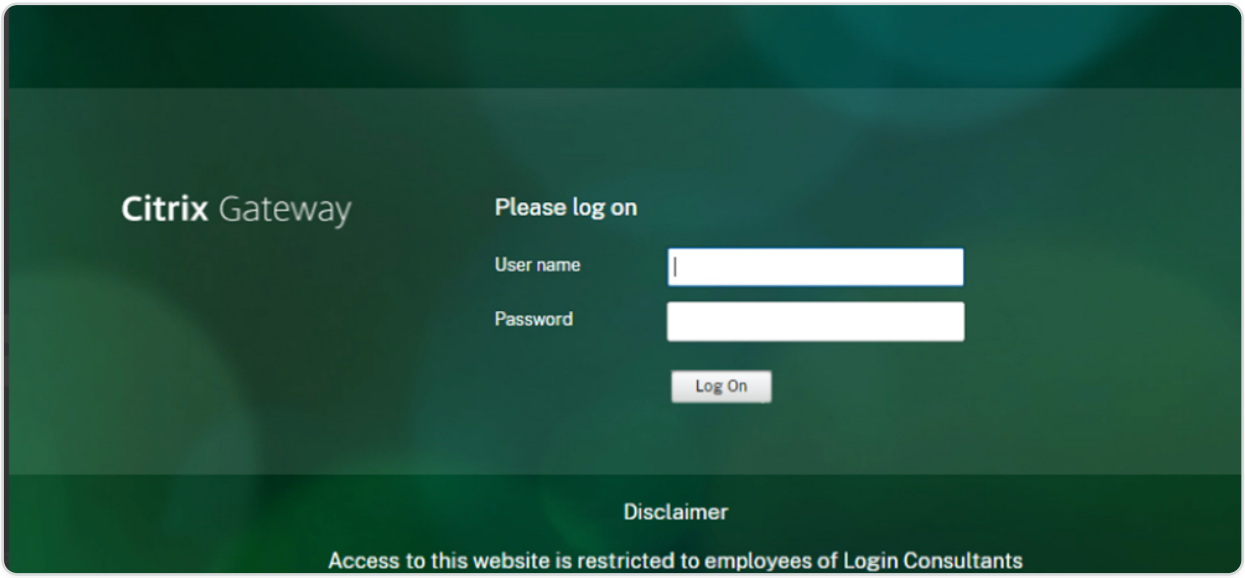
4. 保存文件。
5. 在 `var/netscaler/logon/themes/<custom_theme>/plugins.xml` 位置的 plugins.xml 中添加名称和 src。

```
<plugins>

<plugin name="nsg-epa" src="plugins/ns-gateway/nsg-epa.js" />
```

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

```
<plugin name="nsg-setclient" src="plugins/ns-gateway/nsg-
setclient.js" />

<plugin name="ns-nfactor" src="plugins/ns-gateway/ns-nfactor.js" />

<plugin name="ns-footer" src="plugins/ns-gateway/ns-footer.js" />

</plugins>
```

6. 配置添加了插件的自定义主题。
7. 使用命令 `flush cache contentgroup loginstaticobjects` 刷新缓存。
8. 重新加载门户屏幕。 页脚已添加到 NetScaler Gateway 登录页面。



使用自定义插件进行网关门户定制

NetScaler Gateway RfWebUi 框架提供了添加自定义插件以定制其网关门户的功能。这些自定义插件可用于为网关添加大量功能，例如，如果您想在网关流程中添加一个全新的页面。对于其他用例，可以将代码添加到为网关主题提供的自定义脚本文件中的 `/var/netscaler/logon/themes/<custom_theme>/script.js` 位置。

注意：

NetScaler Gateway 仅支持为门户定制创建和使用自定义插件。NetScaler Gateway 不会根据客户要求创建或提供任何自定义插件。

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

1. 要添加自定义插件，请在 `/var/netscaler/logon/LogonPoint/plugins/ns-gateway/` 位置创建 JavaScript 文件。例如，您可以在 `/var/netscaler/logon/LogonPoint/plugins/ns-gateway/` 中找到以下插件。

   - ns-nfactor.js
   - nsg-epa.js
   - nsg-setclient.js

   建议以 `<plugin_name>`.js 格式输入插件名称。

   所有这些插件文件都由功能所需的 RfWebUI 框架获取。

2. 创建插件文件后，请使用以下代码作为示例，将插件注册到 RfWebUI 框架。

```
(function ($) {

            CTXS.ExtensionAPI.addPlugin( {

                        Name : “plugin name”,

                        initialize: function() {}

            });

    })(jQuery);
```

   其中，

   name 是赋予插件的名称。它用作插件的标识符。

   initialize 将函数作为参数，用于初始化插件。

3. 在 `CTXS.ExtensionAPI.addPlugin()` 函数中输入插件名称和初始化函数以注册插件。 添加的插件名称和位置必须注册到 `/var/netscaler/logon/themes/<custom_theme>/plugins.xml` 位置的 plugins.xml 文件中。

4. 编写插件代码后，必须在 `/var/netscaler/logon/themes/<custom_theme>/plugins.xml` 位置的 `plugins.xml` 文件中注册新添加的插件名称和位置。必须使用 `plug-in` 标签注册插件。

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

```
<plugins>

<plugin name="nsg-epa" src="plugins/ns-gateway/nsg-epa.js"/>

<plugin name="nsg-setclient" src="plugins/ns-gateway/nsg-setclient.js"/
>

<plugin name="ns-nfactorn" src="plugins/ns-gateway/ns-nfactor.js"/>

</plugins>
```

5. 为插件输入名称和 src，以便 RFWebUI 可以识别并获取该插件。

示例配置

以下示例配置可用于添加自定义插件，以便为 NetScaler Gateway 登录页面添加页脚。

1. 在 `/var/netscaler/logon/LogonPoint/plugins/ns-gateway/.` 位置创建 JavaScript 插件文件.
2. 将插件命名为 ns-footer.js `/var/netscaler/logon/LogonPoint/plugins/ns-gateway/ns-footer.js`
3. 将以下代码添加到 RfWebUI 中已注册的插件，并在初始化函数中将页脚添加到网关。

```
(function ($) {

CTXS.ExtensionAPI.addPlugin({

    name: "ns-footer", // Name of plugin - must match name sent in
configuration

    initialize: function () {



    // Add the footer for the login page

    $("#customExplicitAuthBottom").append("<div style='text-
align:center;color:white;font-size:15px;'><br />Disclaimer<br /><br /
>"+" Access to this website is restricted to employees of Login
Consultants<br/></div>");
```

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

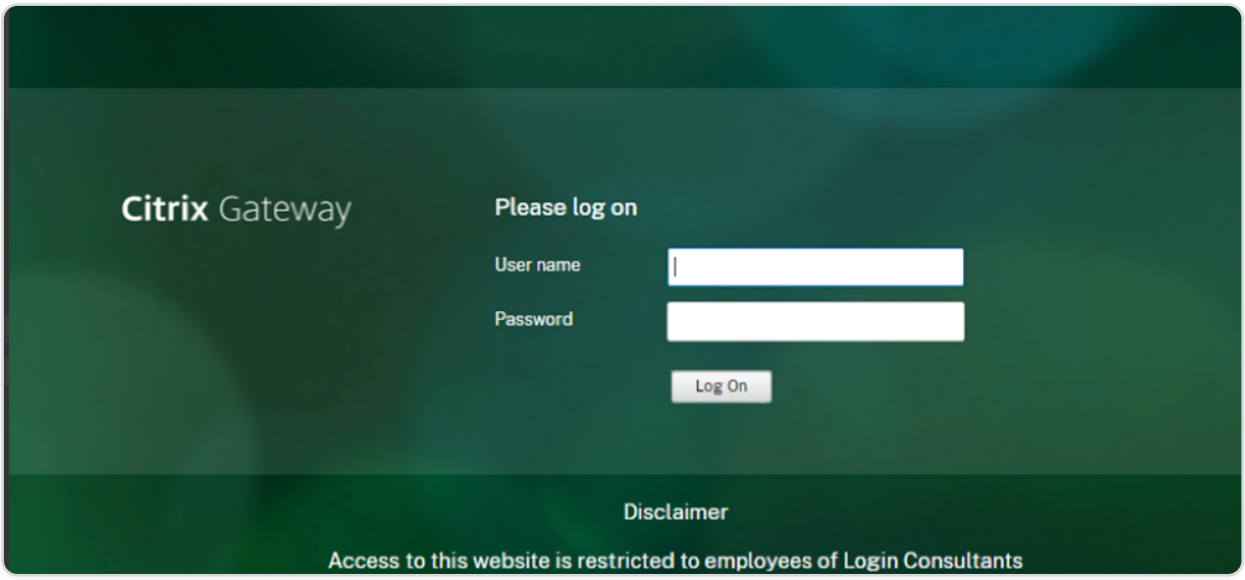
```
    // To Add the footer to the login timeout page

    $("#customAuthBottom").append("<div style='text-
align:center;color:white;font-size:15px;'><br >Disclaimer<br /><br /
>"+" Access to this website is restricted to employees of Login
Consultants<br /></div>");



    callback();

    }

});

})(jQuery);
```

4. 保存文件。
5. 在 `var/netscaler/logon/themes/<custom_theme>/plugins.xml` 位置的 plugins.xml 中添加名称和 src。

```
<plugins>

<plugin name="nsg-epa" src="plugins/ns-gateway/nsg-epa.js" />

<plugin name="nsg-setclient" src="plugins/ns-gateway/nsg-
setclient.js" />

<plugin name="ns-nfactor" src="plugins/ns-gateway/ns-nfactor.js" />

<plugin name="ns-footer" src="plugins/ns-gateway/ns-footer.js" />

</plugins>
```

6. 配置添加了插件的自定义主题。
7. 使用命令 `flush cache contentgroup loginstaticobjects` 刷新缓存。
8. 重新加载门户屏幕。 页脚已添加到 NetScaler Gateway 登录页面。

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



创建和自定义登录方案

登录方案是提供基于表单的身份验证结构的 XML 文件。 用户可以使用一组类似于基本 HTML 表单的用户界面构造来使用各种身份验证表单。

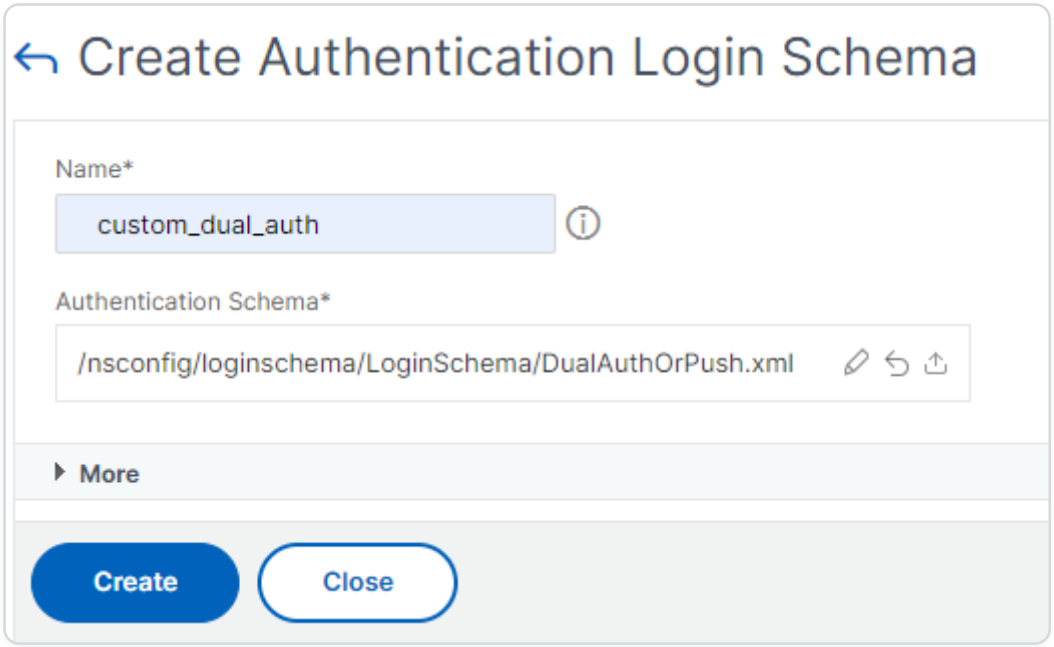
在 nFactor 身份验证中，身份验证因子是链式连接的。每个因子可以有不同的登录方案页面或文件。在某些身份验证场景中，用户可能会看到多个登录屏幕。您还可以让一个登录方案收集信息，然后将其传递给多个因子，这样后续因子就不必显示另一个登录方案了。

登录方案 XML 文件随 NetScaler 设备包含在 `/nsconfig/loginschema/LoginSchema` 中。

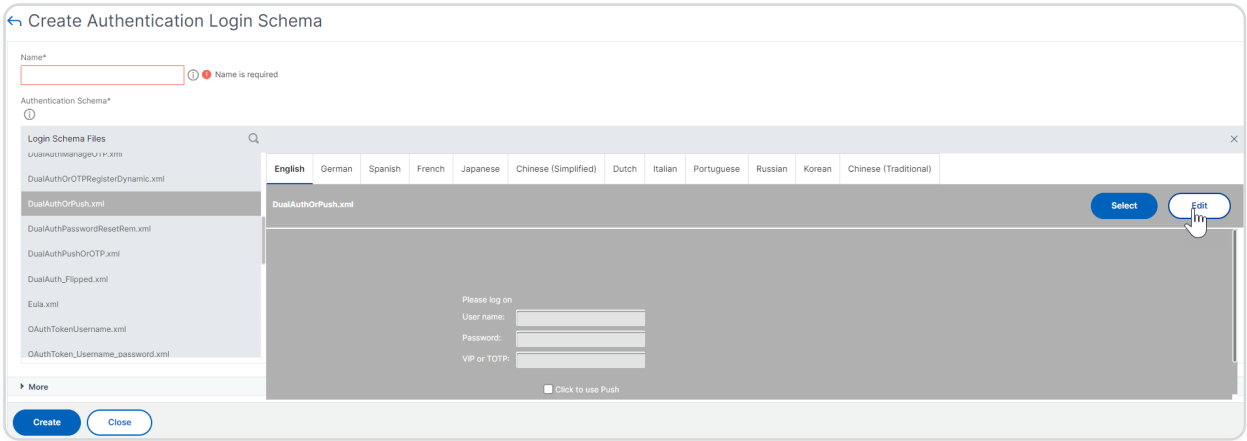
创建登录方案配置文件

1. 导航到 **安全 > AAA - 应用程序流量 > 登录方案**。
2. 单击“**配置文件**”选项卡，然后单击“**添加**”。
3. 在“**身份验证方案**”中，单击铅笔图标。

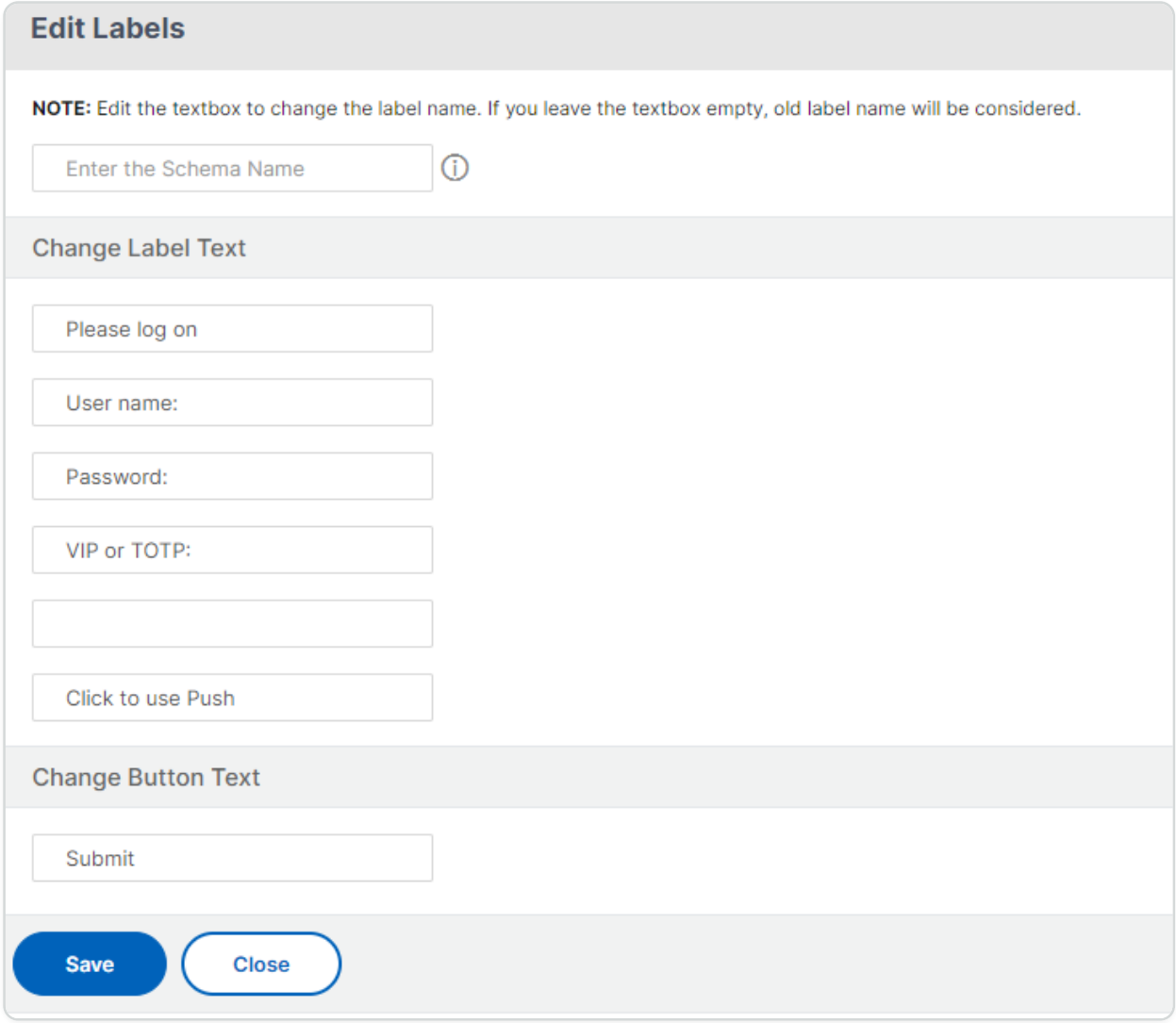
© 1997–2026 Citrix Systems, Inc. All rights reserved.



4. 单击“**LoginSchema**”文件夹以查看其中的文件。
5. 选择其中一个文件并根据需要进行更改。
   - 通过单击右上角的“编辑”按钮来更改标签。
   - 通过选择语言来编辑方案。



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

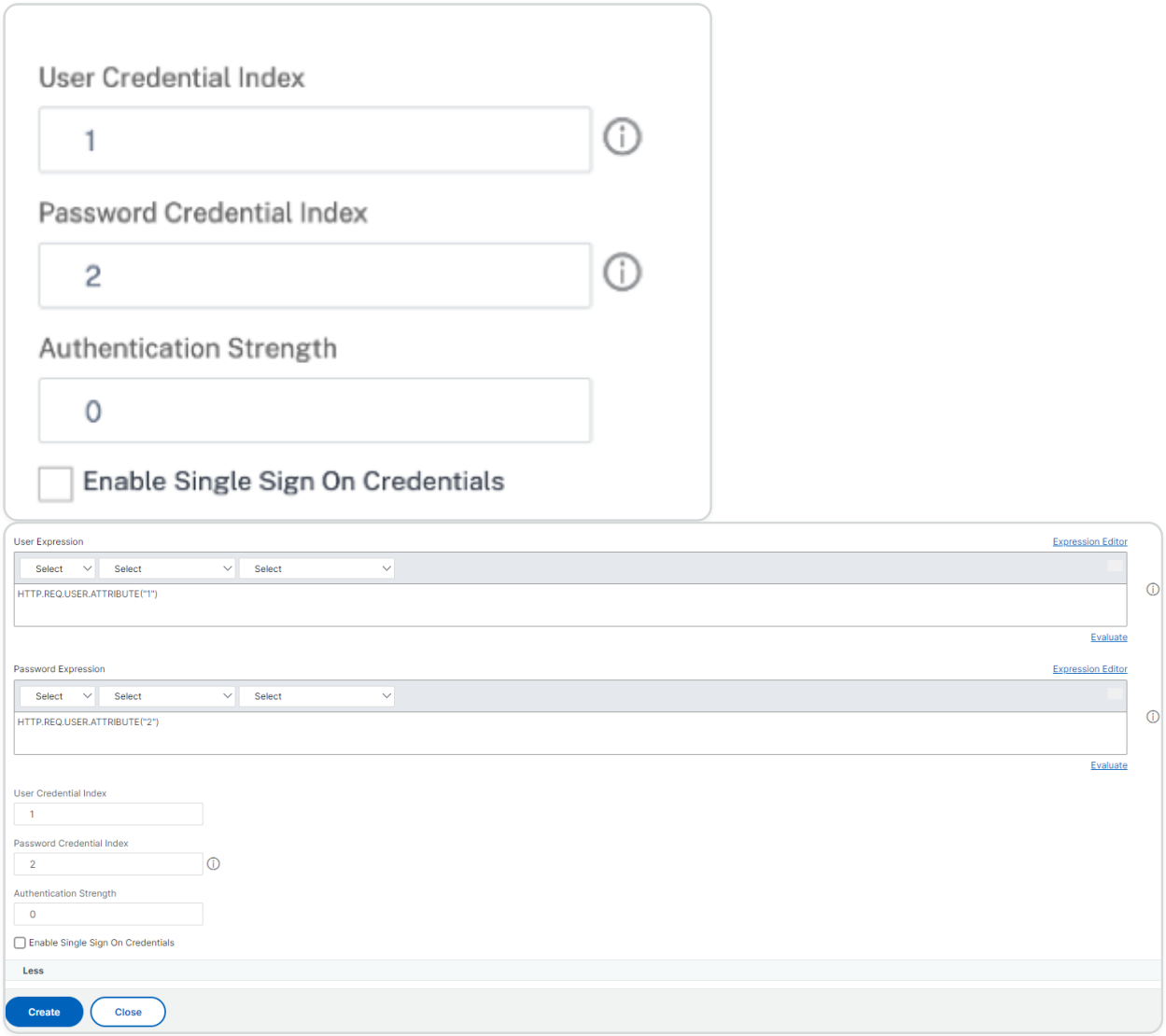


注意： 修改后保存更改时，将创建一个包含这些更改的新架构 XML 文件。

6. 在右上角，单击 **Select** 以选择修改后的架构 XML。
7. 输入登录架构名称，然后单击 **More**。

   注意： 您可以在其他地方使用已输入的凭据。例如，您可以使用用户名和其中一个密码进行 StoreFront 的单点登录。您可以单击 **More** 并为索引输入唯一值。这些值可以在 1 到 16 之间。您可以使用表达式 REQ.USER.ATTRIBUTE(#) 在流量策略或配置文件中引用这些索引值。

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



8. 单击 **Create** 以创建登录架构配置文件。

将登录架构配置文件绑定到身份验证、授权和审计虚拟服务器

要将登录架构配置文件绑定到身份验证、授权和审计虚拟服务器，您必须首先创建登录架构策略。将登录架构配置文件绑定到身份验证策略标签时，不需要登录架构策略。

要创建和绑定登录架构策略：

1. 导航到 **安全 > AAA > 登录方案**。
2. 单击 **Policies** 选项卡，然后单击 **Add**。
3. 在 **Profile** 中，选择之前创建的登录架构配置文件。
4. 在 **Rule** 中，输入默认语法表达式，然后单击 **Create**。

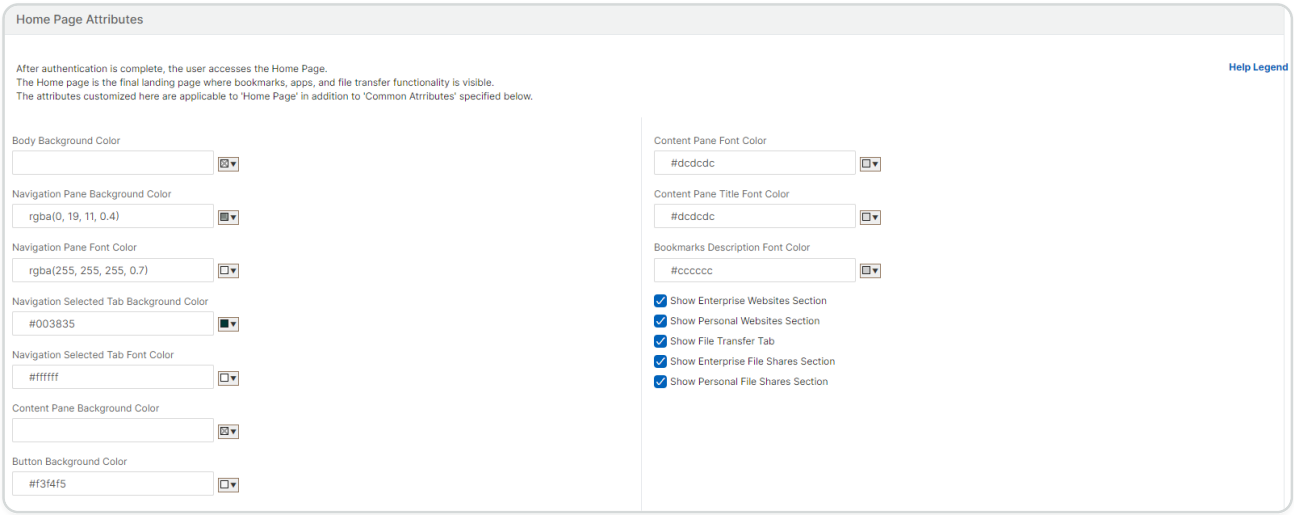
© 1997–2026 Citrix Systems, Inc. All rights reserved.

从管理 UI 进行门户自定义

管理员可以通过创建自定义主题来定制门户主题，以实现用户门户的个性化外观和体验。自定义主题可以基于 RfWebUI、Default、X1 和 GreenBubble 主题创建。

创建自定义主题：

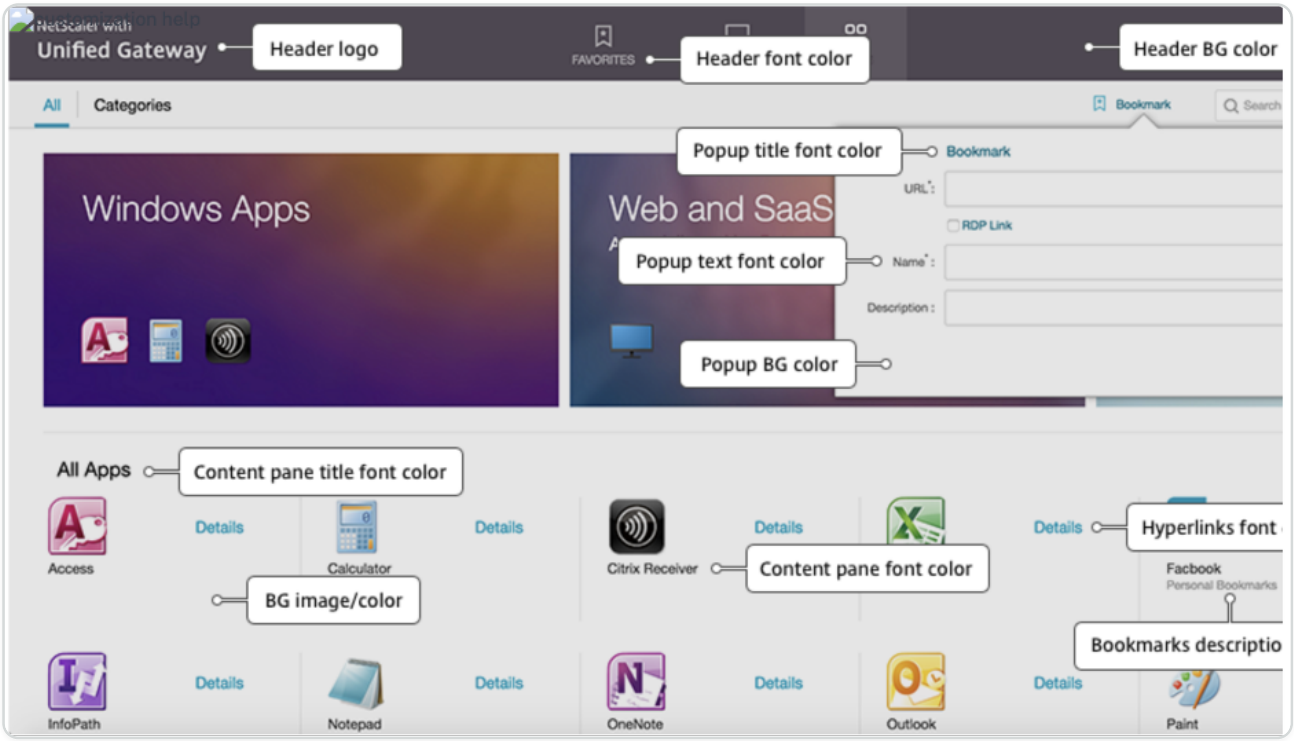
1. 在“配置”选项卡中，导航到 **NetScaler Gateway > 门户主题**，然后单击“**添加**”。
2. 输入自定义主题的名称。
3. 在“**模板主题**”中，根据您的要求选择基本主题。默认选择 **RfWebUI**。
4. 单击“**确定**”。
5. 在“**外观**”部分，根据您的主页要求修改属性，然后单击“**确定**”。



下图显示了基于 RfWebUi 的自定义主题。

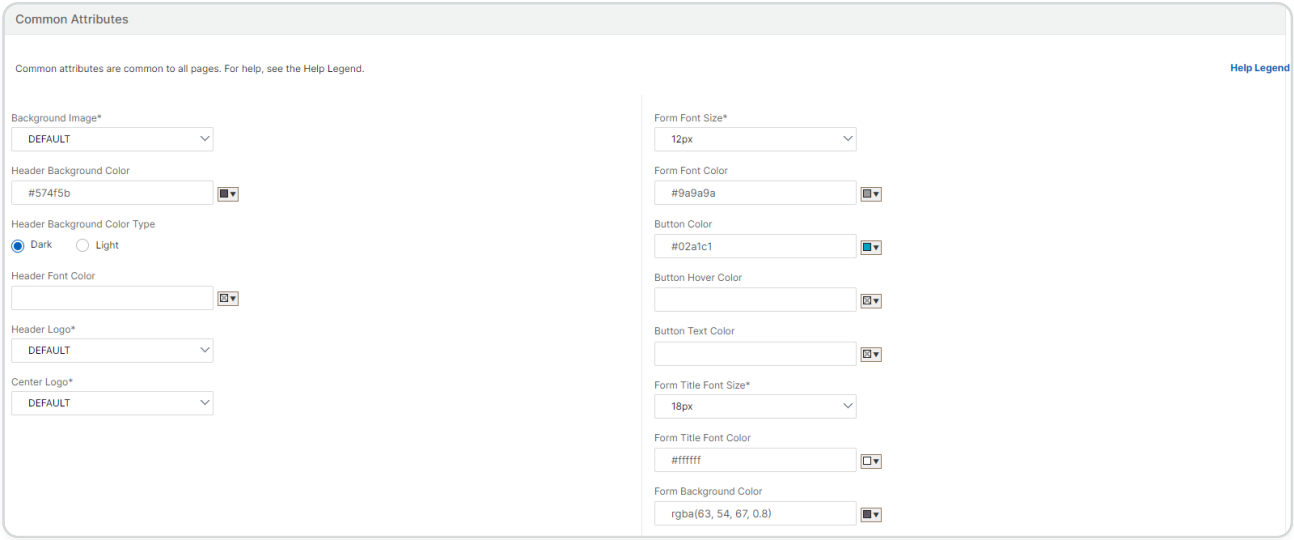
“**帮助图例**”链接显示了带有部分名称的图形页面显示，可帮助您选择要编辑的内容。

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



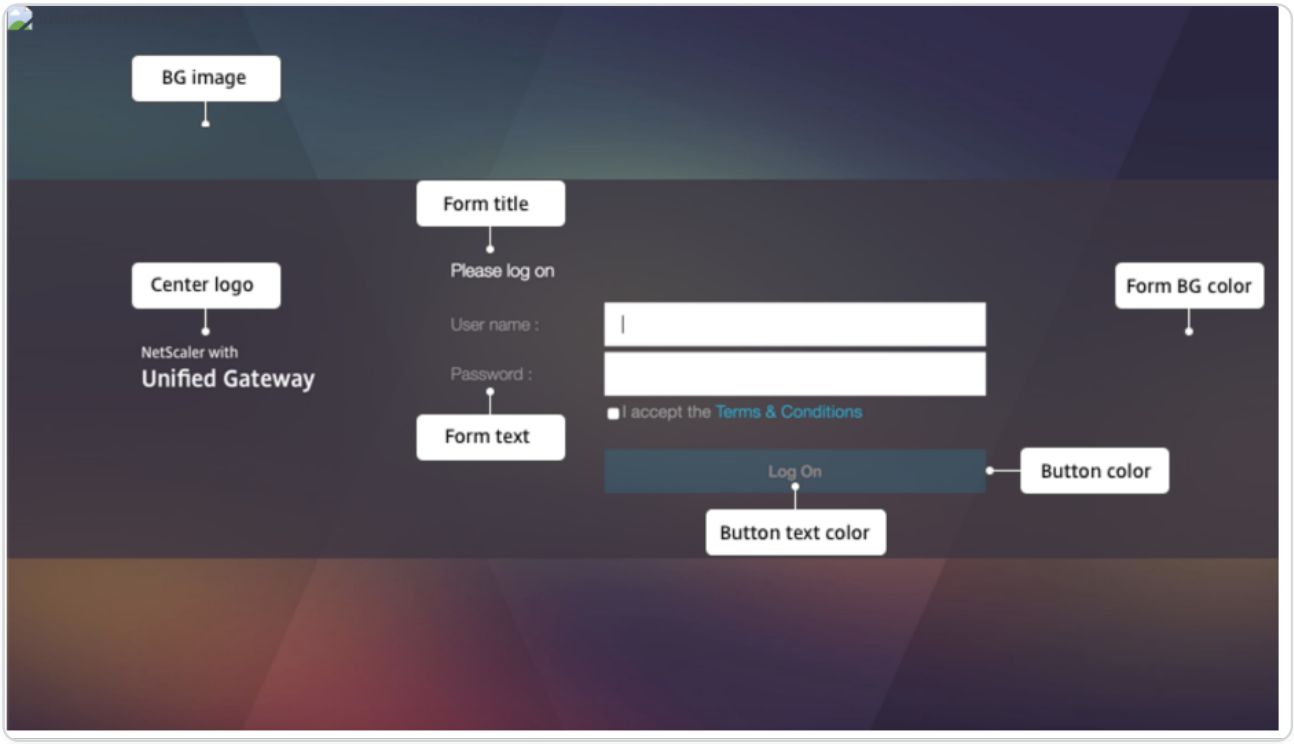
通用属性

“**通用属性**”部分提供了所有 NetScaler Gateway 登录页面通用的可配置设置。

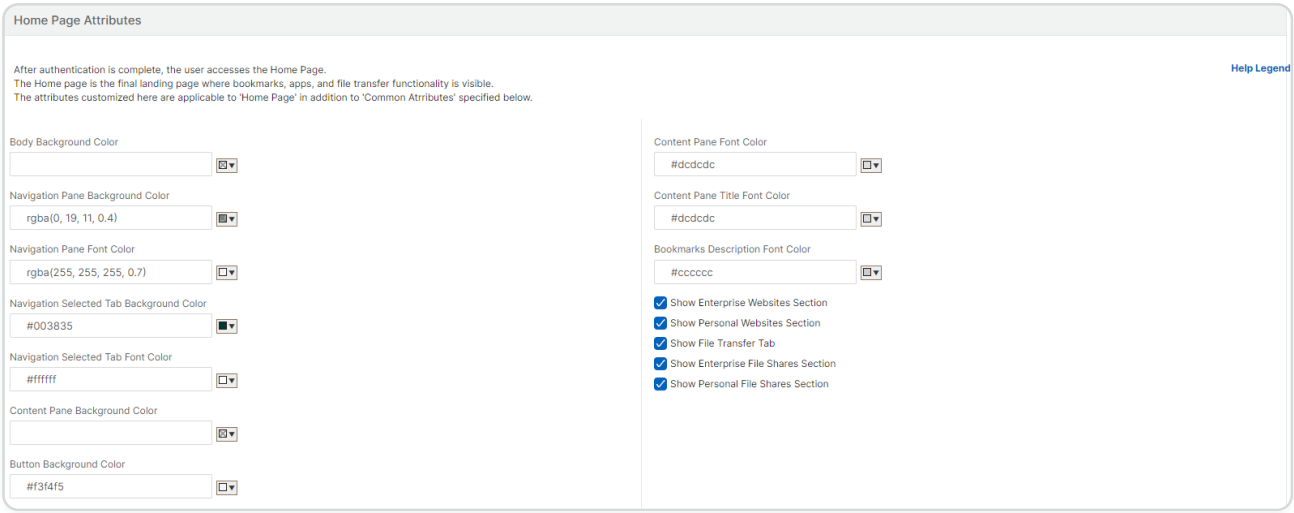


点击**帮助图例**链接以查看每个常见的可配置参数。

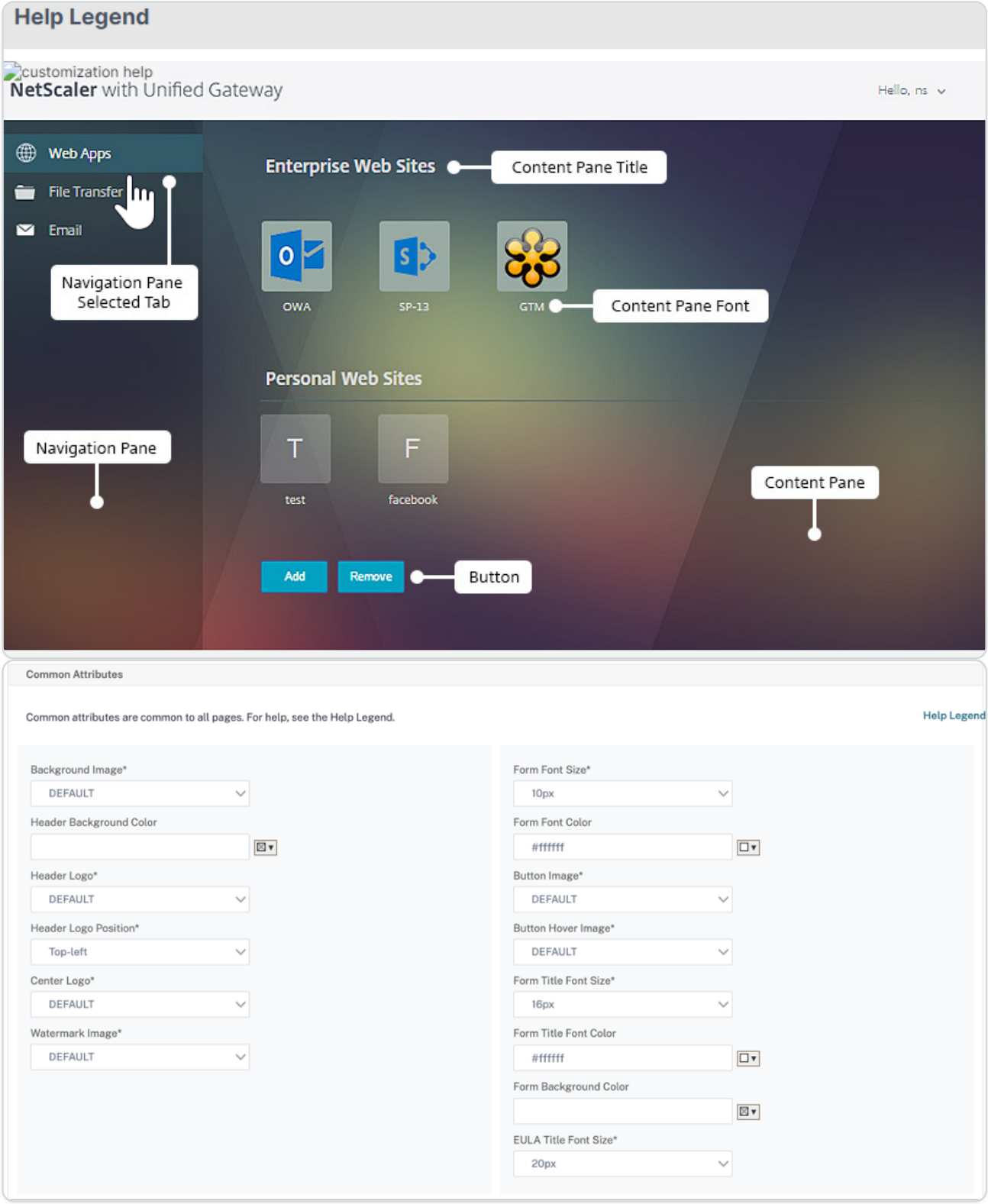
© 1997–2026 Citrix Systems, Inc. All rights reserved.



同样，对于基于**默认**的自定义主题，下图显示了主页的可用配置。 **注意：**此配置对于 x1 和 GreenBubble 不同。



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



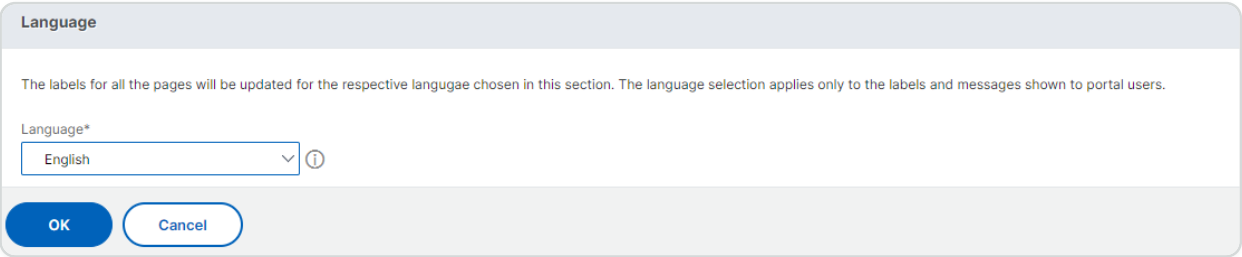
© 1997–2026 Citrix Systems, Inc. All rights reserved.

字符串自定义

除了网关门户主页的外观和感觉之外，管理 UI 还支持所有页面的字符串自定义。

执行以下步骤来自定义字符串：

1. 选择要编辑字符串的语言。字符串将以所选语言显示。默认选择英语。



   注意：您选择的语言不定义门户主题语言。它是正在自定义字符串的语言。

2. 在右侧的**高级设置**中，列出了可用于字符串自定义的页面。

   - 登录页面
   - EPA 页面
   - EPA 错误页面
   - EPA 后页面
   - VPN 连接页面
   - 主页

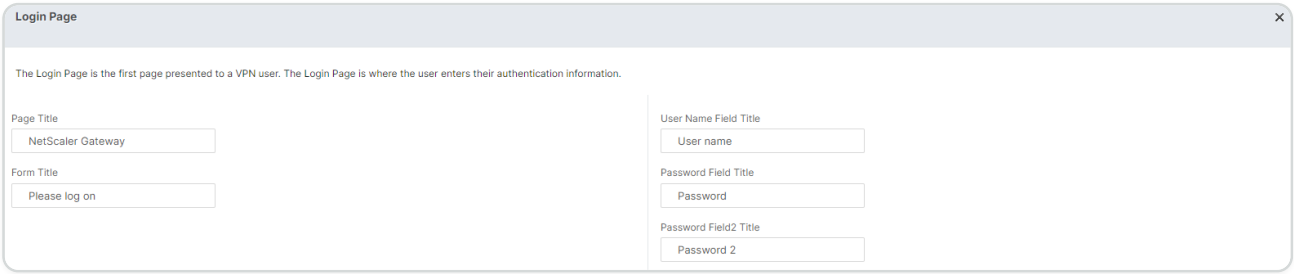
© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. 选择要自定义字符串的页面，然后单击编辑图标。将显示一个包含预填充字符串自定义项的表单。
4. 选择字段并根据您的要求添加或编辑字符串。
5. 单击 **Done** 完成自定义门户主题创建。您可以稍后从 **NetScaler Gateway > Portal Themes** 编辑主题。

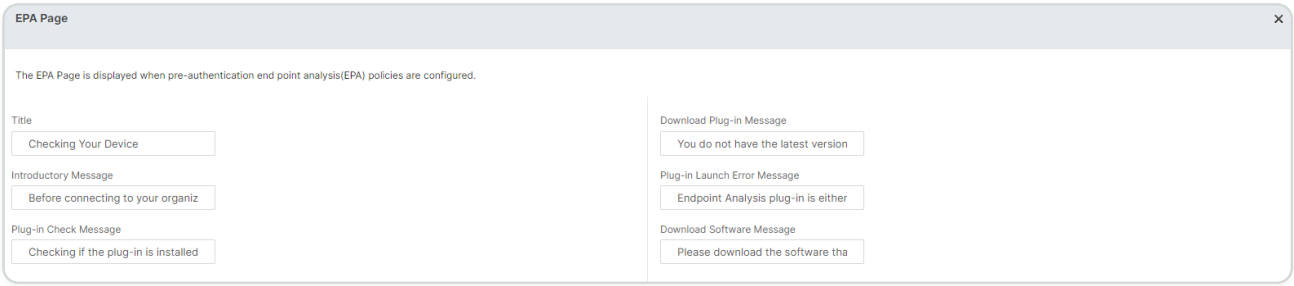
注意： 如果该部分仍以先前选择的语言显示字符串，则可能是因为在更改语言时该部分已打开。在这种情况下，请关闭该部分，选择语言，然后从 **Advanced Setting** 再次打开页面。

以下屏幕截图显示了每个页面可用的可自定义字符串集。

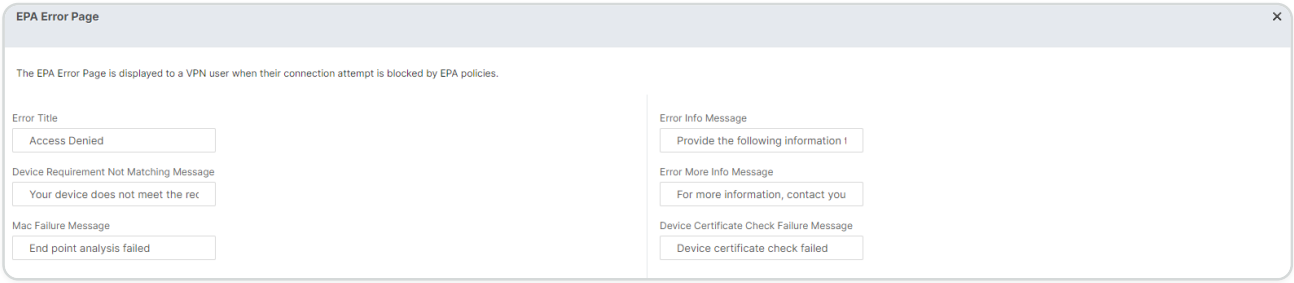
登录页面：



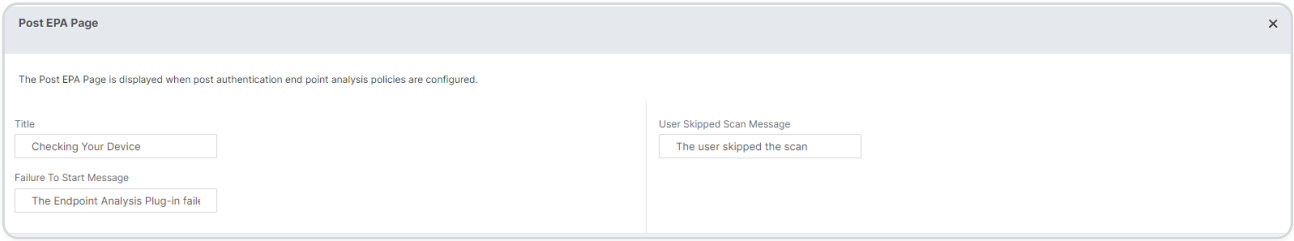
EPA 页面：



EPA 错误页面：

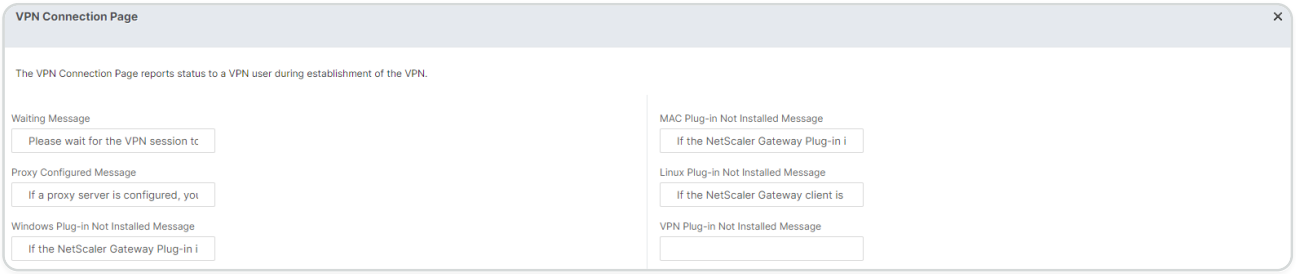


EPA 后页面：

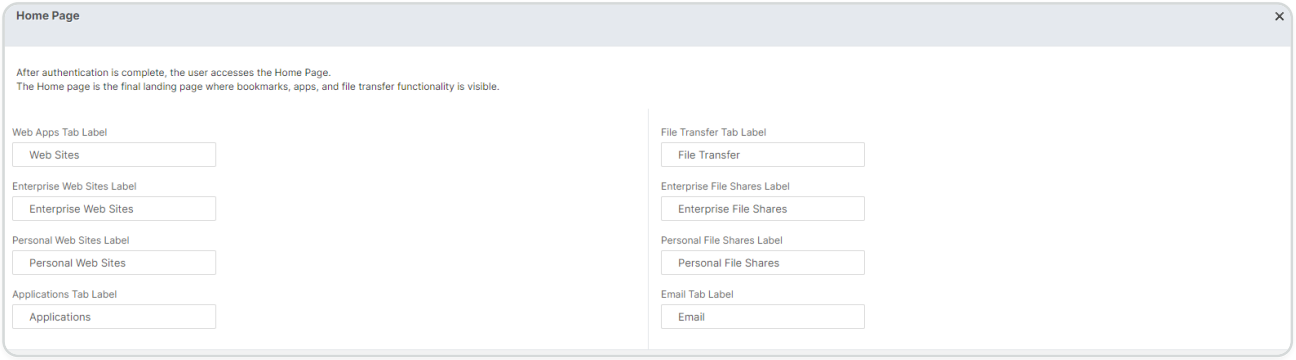


© 1997–2026 Citrix Systems, Inc. All rights reserved.

VPN 连接页面：



主页：



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

优化 NetScaler Gateway VPN 拆分隧道以用于 Office365

随着组织比以往更快地适应远程工作选项，必须优化远程访问基础设施，以在流量负载增加的情况下促进无缝连接。

重要提示：

Microsoft 建议通过使用已发布的 IPv4 和 IPv6 地址范围配置拆分隧道，将流向关键 Office 365 服务的流量排除在 VPN 连接范围之外。为了获得最佳性能和最有效地利用 VPN 容量，流向与以下应用程序关联的专用 IP 地址范围的流量必须直接路由，在 VPN 隧道之外：

- 办公 365 易捷在线
- SharePoint Online 服务
- Microsoft Teams（在 Microsoft 文档中称为“优化”类别）

有关此建议的更多详细信息，请参阅 Microsoft 指南。
NetScaler Gateway 中 Microsoft 的建议是通过使用拆分隧道反向配置，将 Microsoft 提供的 IP 地址列表直接路由到 Internet，以处理 O365 流量。

配置涉及以下内容，可以通过使用 GUI 或 CLI 手动执行：

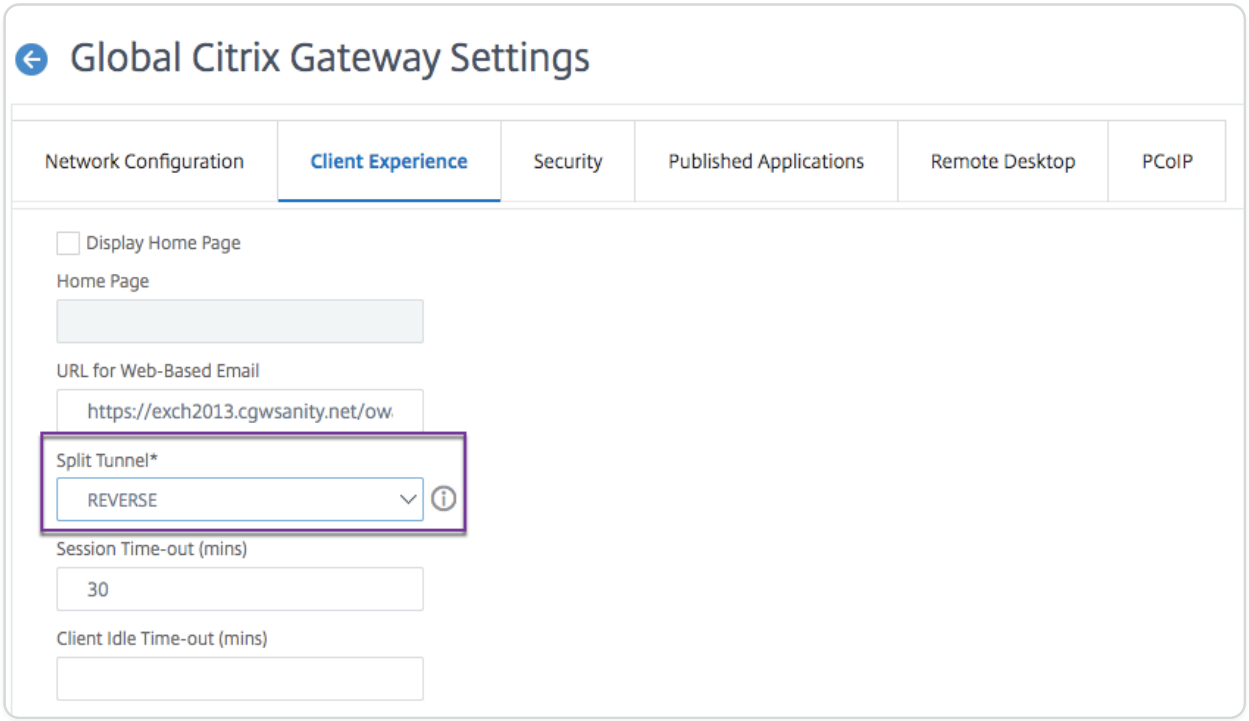
- 配置拆分隧道以进行反向配置。有关详细信息，请参阅 拆分隧道选项。
- 配置内网应用程序以供用户访问资源。

使用 GUI 进行配置

使用 GUI 配置拆分隧道

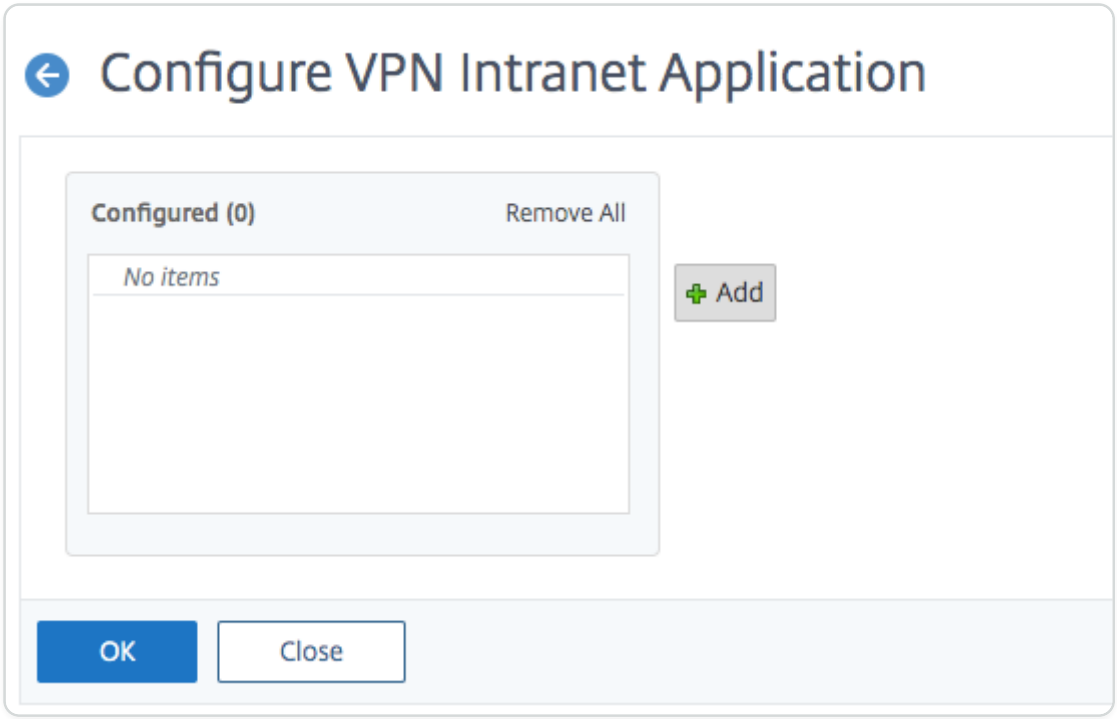
1. 在“配置”选项卡上，导航到 **NetScaler Gateway > 全局设置**。
2. 在详细信息窗格中，在**设置**下，单击**更改全局设置**。
3. 在**客户端体验**选项卡上，在**拆分隧道**中，选择**反向**。
4. 单击**确定**。

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

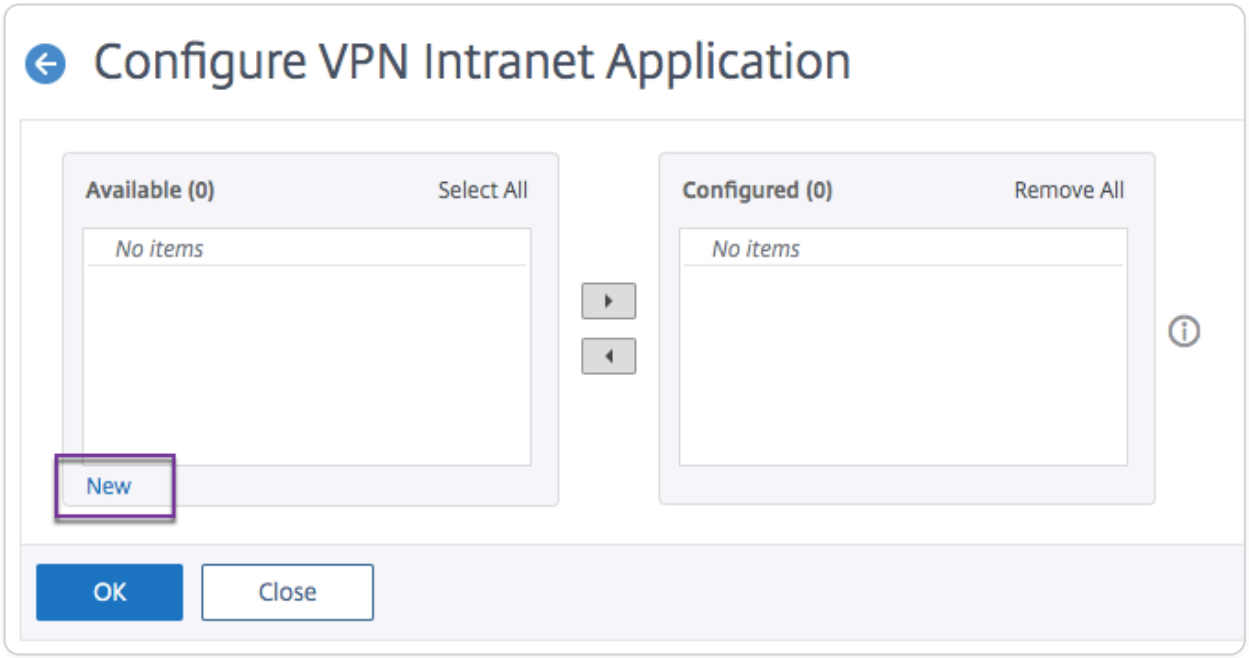


使用 GUI 创建 VPN 内网应用程序

1. 在“配置”选项卡上，导航到 **Citrix Gateway > 全局设置**。
2. 在详细信息窗格中，在**内网应用程序**下，单击链接。
3. 在**配置 VPN 内网应用程序**页面中，单击**添加**，然后单击**新建**。



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



4. 在**名称**中，键入配置文件的名称。
5. 在**协议**中，选择适用于网络资源的协议。
6. 在**目标类型**中，选择**IP 地址和子网掩码**。
7. 在**IP 地址**中，输入必须直接路由到 Internet 以用于 O365 流量的 IP 地址。有关 IP 地址列表，请参阅 IP 地址列表。
8. 在**子网掩码**中，输入子网掩码 IP 地址。

   添加内部网应用程序(/en-us/netscaler-gateway/media/microsoft-create-intranet-app-global.png)
9. 单击 **创建**，然后单击 **关闭**。

注意： 对所有 IP 地址重复此过程。

使用 CLI 进行配置

- 要在命令提示符下将拆分隧道设置为反向，请键入；

```
set vpn parameter -splitTunnel REVERSE
```

- 要在命令提示符下添加 VPN 内部网应用程序，请键入；

```
add vpn intranetApplication intranetapp1 ANY 13.107.6.152 -netmask
255.255.255.254 -destPort 1-65535 -interception TRANSPARENT
```

注意： 对所有 IP 地址重复此过程。

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

- 要在命令提示符下绑定内部网应用程序，请键入；

```
bind vpn global -intranetApplication intranetapp1
```

Office 365 服务（EXO、SPO 和 Microsoft Teams）的 IP 地址列表

参考：`<https://docs.microsoft.com/zh-cn/office365/enterprise/urls-and-ip-address-ranges>`

来自 MICROSOFT 的说明：

作为 Microsoft 应对 COVID-19 疫情的一部分，Microsoft 已宣布暂时暂停一些计划中的 URL 和 IP 地址更改。此暂停旨在为客户 IT 团队提供信心和简便性，以便在居家办公的 Office 365 场景中实施推荐的网络优化。从 March 24, 2020 到 June 30, 2020，此暂停将阻止对优化类别中包含的 IP 范围和 URL 的关键 Office 365 服务（Exchange Online、SharePoint Online 和 Microsoft Teams）进行更改。

IPv4 地址范围

104.146.128.0/17

13.107.128.0/22 13.107.136.0/22

13.107.18.10/31 13.107.6.152/31

13.107.64.0/18 131.253.33.215/32

132.245.0.0/16 150.171.32.0/22

150.171.40.0/22 191.234.140.0/22

204.79.197.215/32 23.103.160.0/20

40.104.0.0/15 40.108.128.0/17

40.96.0.0/13 52.104.0.0/14

52.112.0.0/14 52.96.0.0/14

52.120.0.0/14|

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

IPv6 地址范围

2603:1006::/40

2603:1016::/36 2603:1026::/36

2603:1036::/36 2603:1046::/36

2603:1056::/36 2603:1096::/38

2603:1096:400::/40 2603:1096:600::/40

2603:1096:a00::/39 2603:1096:c00::/40

2603:10a6:200::/40 2603:10a6:400::/40

2603:10a6:600::/40 2603:10a6:800::/40

2603:10d6:200::/40 2620:1ec:4::152/128

2620:1ec:4::153/128 2620:1ec:c::10/128

2620:1ec:c::11/128 2620:1ec:d::10/128

2620:1ec:d::11/128 2620:1ec:8f0::/46

2620:1ec:900::/46 2620:1ec:a92::152/128

2620:1ec:a92::153/128 2a01:111:f400::/48

2620:1ec:8f8::/46 2620:1ec:908::/46

2a01:111:f402::/48

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

UDP 流量的服务类型支持

UDP 的服务类型 (ToS) 支持可确保一旦发送方为 UDP 数据包配置了 ToS 值，NetScaler Gateway 就会保留该值，直到数据包到达其目的地。根据配置的值和目标网络的配置，目标网络会将 UDP 数据包放入优先级出站队列中。

注意：

使用 ToS 信息，您可以为每个 IP 数据包分配优先级，并请求特定的处理，例如高吞吐量、高可靠性、低延迟等。

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

配置服务器名称指示扩展

NetScaler Gateway 设备现在可以配置为在发送到后端服务器的 SSL“客户端 Hello”数据包中包含服务器名称指示 (SNI) 扩展。SNI 扩展有助于后端服务器在 SSL 握手期间识别所请求的 FQDN，并使用相应的证书进行响应。

注意

当多个 SSL 域托管在同一服务器上时，启用 SNI 支持。

要使用 GUI 配置 NetScaler Gateway 以支持 SNI：

1. 在 NetScaler GUI 中，导航到 **Configuration\> NetScaler\> Global Settings**。
2. 单击“**更改全局设置**”链接，然后从“**后端服务器 SNI**”菜单中，选择“**已启用**”。

要使用命令行界面配置 NetScaler Gateway 以支持 SNI，请在命令提示符下键入：

```
set vpn parameter backendServerSni <ENABLED><DISABLED>
```

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

SSL握手期间服务器证书的验证

可以将NetScaler Gateway配置为在SSL握手期间验证后端服务器提供的服务器证书。

从NetScaler Gateway 14.1版本56.x开始，当您启用服务器证书验证时，NetScaler Gateway除了验证安全票证颁发机构 (STA) 和StoreFront服务器证书外，还会验证SSL VDA证书。

注意：

对于双跳部署，服务器证书验证的配置必须在第二跳上完成。

使用GUI配置服务器证书验证

绑定CA证书

1. 导航到 **NetScaler Gateway > NetScaler Gateway 策略管理器 > 证书绑定**。
2. 在 **Certificate Bindings** 部分，单击 **+** 图标。
3. 在 **SSL Certificate(s) Binding** 页面中，单击 **Add Binding**。
4. 在 **CA Cert** 中，单击 **Add**。
5. 在 **Install CA Certificate** 页面中，在 **Certificate File Name** 字段中选择证书文件名，然后单击 **Install**。
6. 在 **SSL Certificate(s) Binding** 页面中，选择证书，然后单击 **Bind**。
7. 单击 **Done**。

启用证书验证

1. 导航到 **NetScaler Gateway > 全局设置**。
2. 单击 **更改全局设置**。
3. 从 **后端服务器证书验证** 下拉菜单中选择 **已启用**，然后单击 **确定**。

要使用 CLI 配置服务器证书验证

在命令提示符下，键入以下命令：

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

```
bind vpn global cacert <cacert_name>

set vpn parameter backendcertValidation ENABLED
```

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

使用模板简化 SaaS 应用程序配置

通过为常用 SaaS 应用程序提供模板下拉菜单，简化了 NetScaler Gateway 上的单点登录 SaaS 应用程序配置。可以从菜单中选择要配置的 SaaS 应用程序。该模板预填充了配置应用程序所需的大部分信息。但是，仍必须提供特定于客户的信息。

注意：

要配置和发布 SaaS 应用程序，请先在 NetScaler Gateway 上配置和发布，然后在其应用程序服务器上配置和发布。

下一节中的步骤将帮助您使用模板在 NetScaler Gateway 上配置和发布应用程序。然后转到解释如何在应用程序服务器上配置和发布的章节。

使用模板配置和发布应用程序 - NetScaler Gateway 特定配置

以下配置以 AWS Console 应用程序为例，说明如何使用模板配置和发布应用程序。

在开始之前，您需要以下内容：

- AWS Console 的管理员帐户
- NetScaler Gateway 的管理员帐户

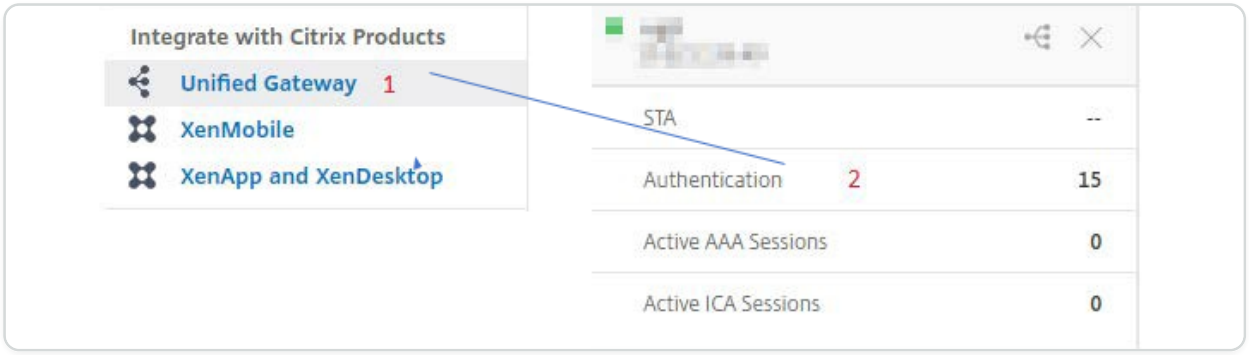
AWS Console 配置步骤如下：

1. 使用应用程序目录配置 AWS Console。
2. 从 NetScaler 导出 AWS Console IdP 元数据。
3. 将 IdP 配置到 AWS Console 中。

步骤 1： 使用应用程序目录配置 AWS Console

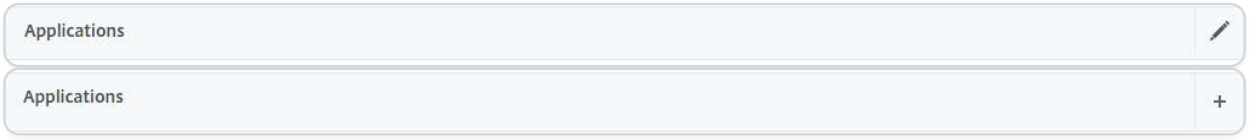
1. 点击 **统一网关 > 身份验证**。

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

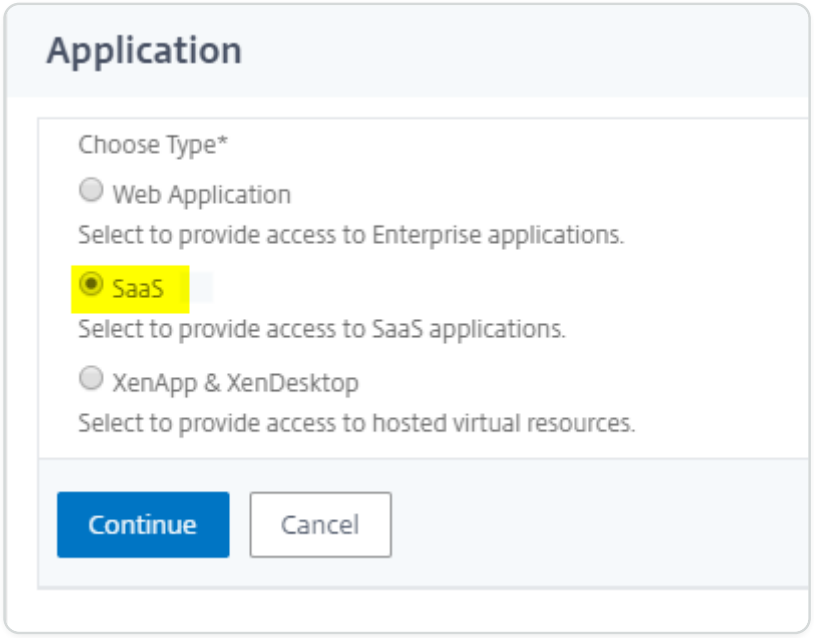


统一网关配置屏幕随即出现。

2. 在**应用程序**部分，点击编辑图标。现在，点击加号图标。应用程序窗口随即出现。

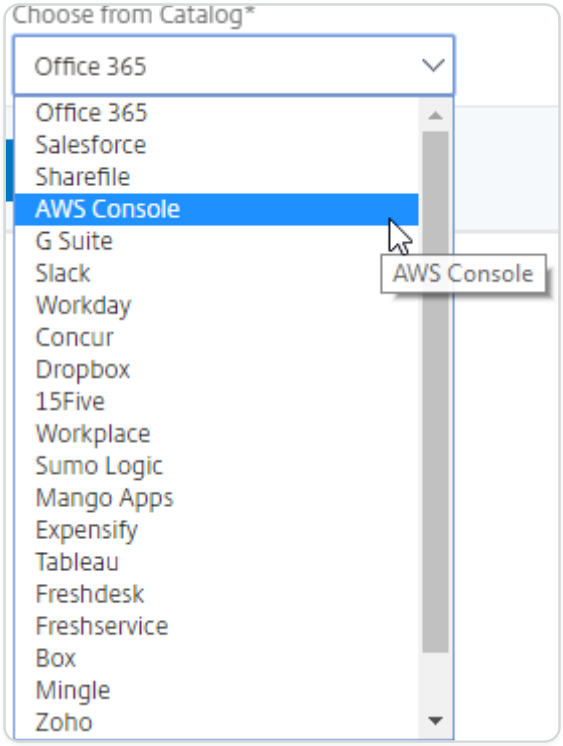


3. 从应用程序类型中选择 **SaaS**。

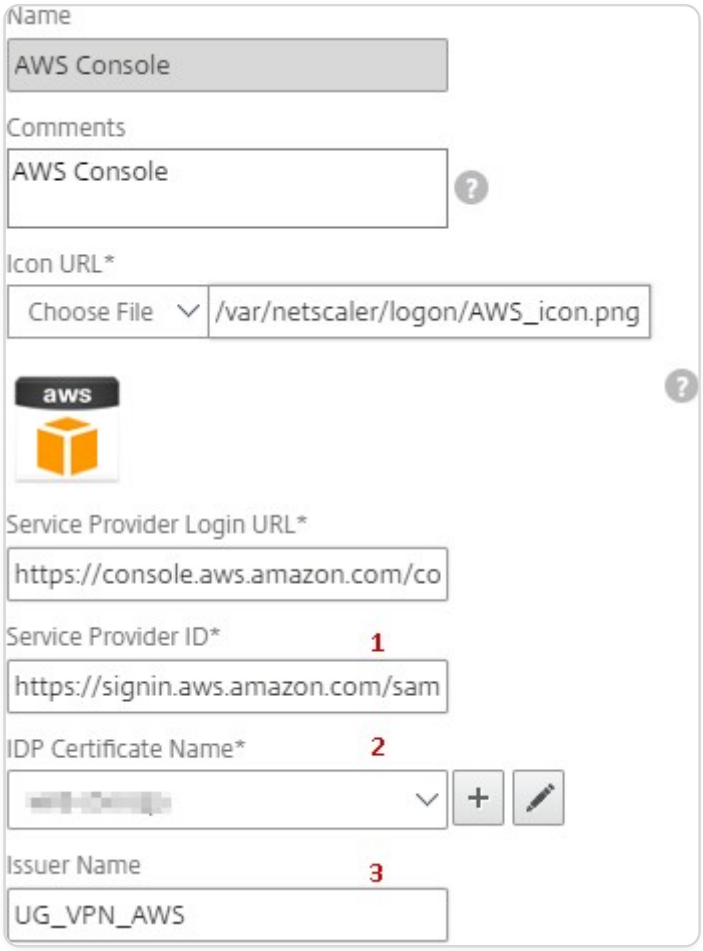


4. 从下拉列表中选择 **AWS Console**。

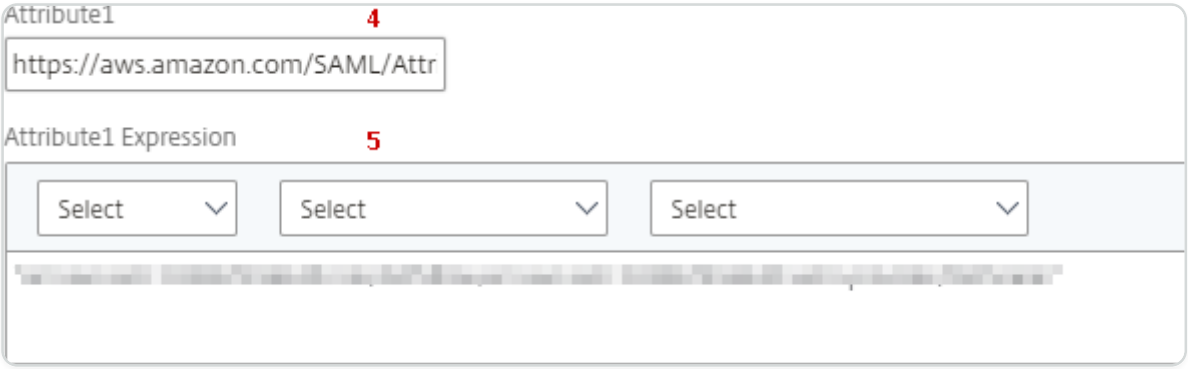
© 1997–2026 Citrix Systems, Inc. All rights reserved.



5. 使用适当的值填写应用程序模板。



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



6. 输入以下 SAML 配置详细信息，然后点击**继续**。

   服务提供商 ID – `<https://signin.aws.amazon.com/saml>`

   签名证书名称 – 必须选择 IdP 证书

   颁发者名称 – 颁发者名称可根据您的选择填写

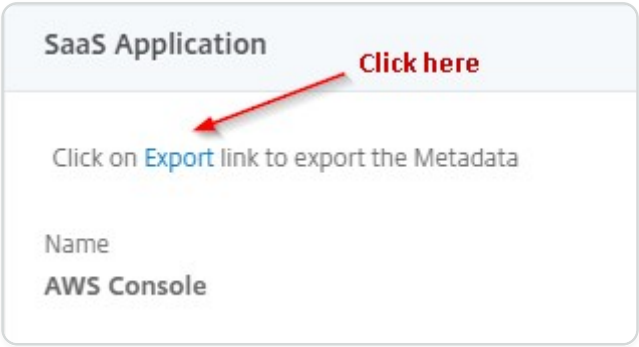
   属性1 – `https://aws.amazon.com/SAML/Attributes/Role`

   属性1表达式 `- Role ARN, IdP ARN`，如步骤 3 所示

7. 单击 **完成**。

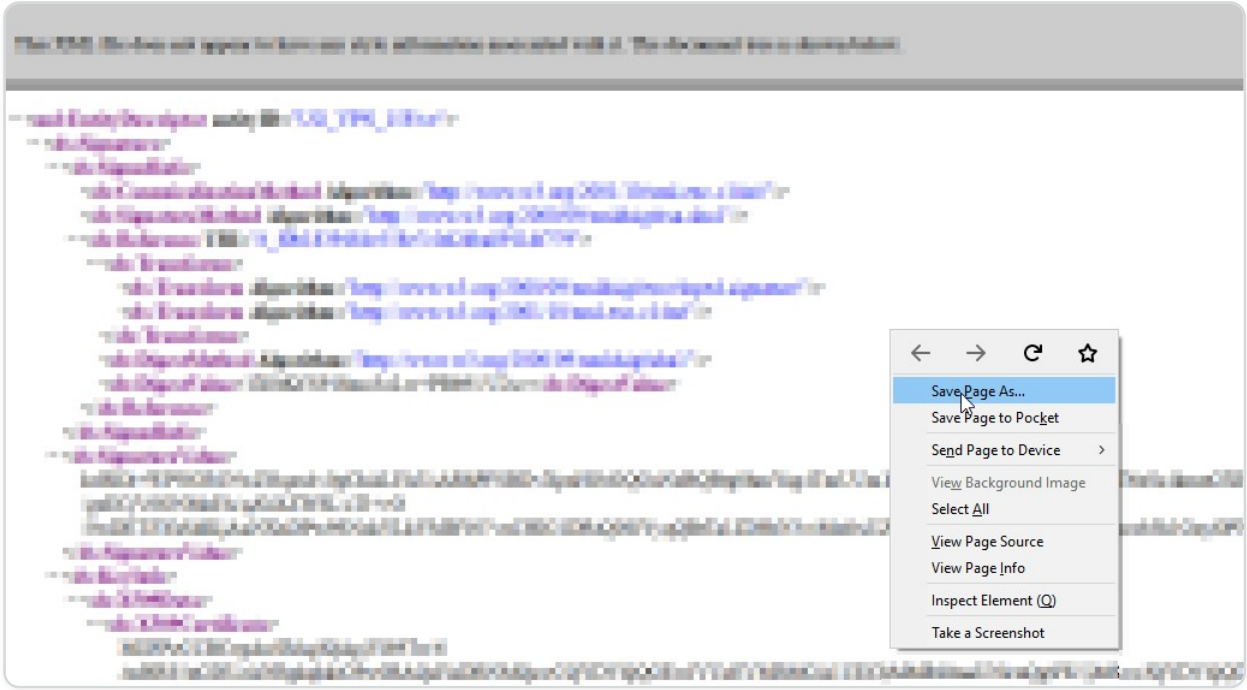
步骤 2： 从 NetScaler Gateway 导出 AWS 控制台 IdP 元数据。

1. 单击 **统一网关 > 身份验证**。
2. 向下滚动并单击 **AWS 控制台** 模板。SaaS 应用程序窗口随即出现。单击 **导出** 链接。



3. **元数据** 在新窗口中打开。保存 **IdP 元数据** 文件

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



步骤 3： 将 IdP 配置到 AWS 控制台。

使用模板配置和发布应用程序 — 应用程序服务器特定配置

以下链接打开 PDF 文档，提供使用模板配置和发布热门 SaaS 应用程序的具体指导。

- 15福艾弗
- 阿布索布
- 阿康帕
- 奥多比卡普蒂维特普莱姆
- 奥多比创意云
- Aha
- AlertOps
- 阿洛卡迪亚
- 阿里巴
- 阿森布拉
- AWS 控制台
- BambooHR
- 贝斯客户关系管理
- BitaBIZ
- BlueJeans

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

- 布利斯书
- 邦纳斯利
- Box
- 布格斯纳格
- 必可特
- CakeHR
- 卡德板
- 塞德西斯
- 赛洛西斯
- 思科 Meraki
- ClearSlide
- CloudCheckr
- ConceptShare
- 康卡
- 康福伦斯
- 康塔克特齐拉
- 康沃
- 西尔科努斯
- 达世通
- 数据狗
- 德斯克普罗
- 德普蒂
- DigiCert
- DocuSign
- 多摩
- 多宝箱
- Duo
- eFront
- 伊卡达
- 恩沃伊

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

- ERP
- 易捷报
- EZOfficeInventory
- EZRentOut
- 费沃罗
- 联合目录
- 菲德利
- 菲维特兰
- 弗拉特文件
- 弗洛道克
- 弗雷什桌面
- 弗朗特
- G套件
- GitHub
- GlassFrog
- GotoMeeting
- HappyFox
- 赫尔普果汁
- 赫尔普斯科特
- 霍欣计划
- 休曼尼蒂
- 伊格鲁
- 伊鲁米奥
- 图像中继
- 爱米特中心
- InteractGo
- iQualify One
- 吉拉
- 看板工具
- 基珀安全

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

- 肯蒂克
- 肯蒂克
- 基斯流
- KnowBe4
- KnowledgeOwl
- 酷朵
- LaunchDarkly
- 莱思赛斯
- 莱特莫斯
- LiquidPlanner
- LogDNA
- 芒果
- 曼纽斯克里普特
- 马克拓
- 敏格
- 迈克斯潘内尔
- MuleSoft
- MyWebTimesheets
- 纽睿力
- 恩姆伯斯
- 纽克利诺
- 微软 Office 365
- OneDesk
- OpsGenie
- 奥尔吉尼奥
- PagerDuty
- 帕诺拉玛9
- ParkMyCloud
- 皮肯
- 匹普尔 HR

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

- 聘板
- 派普驱动
- PlanMyLeave
- PlayVox
- 泊迪欧
- ProdPad
- Proto.io
- 普洛西点击
- PurelyHR
- 昆多拉
- 瑞克空间
- RealtimeBoard
- 瑞美迪福斯
- 罗宾
- 罗尔巴
- 销售易
- 萨马纳奇
- 赛姆佩奇
- 森特里
- 服务台增强版
- ServiceNow
- 沙弗勒
- 斯凯德利
- 技能库
- 史拉克
- 斯莱玛
- Sli.do
- 智能表格
- 斯波克
- 斯波特因斯特

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

- SproutVideo
- StatusCast
- 状态英雄
- StatusHub
- 状态页
- 苏摩逻辑
- 超慕
- 同步力
- 塔布洛
- 目标流程
- 团队福瑞
- 可测试
- TestFairy
- TextExpander
- TextMagic
- ThousandEyes
- 泰科秘密服务器
- 天福安全
- 特里索泰克
- 特伦巴
- TwentyThree
- UniFi
- UserEcho
- UserVoice
- 维尔皮克
- VictorOps
- VIDIZMO
- 可视化范式
- 维克顿
- 维波

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

- 当我工作时
- 沃克戴
- 工作路径
- 沃克普莱斯
- 沃克斯塔斯
- 沃克团队
- XaitPorter
- 辛布尔
- `XMatters`
- 优德克
- 赞德斯克
- ZIVVER
- Zoho 一号
- ZIVVER
- 祖姆

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

__index__

为您的 Citrix Endpoint Management Environment 配置设置

适用于 Citrix Endpoint Management 的 NetScaler 向导将指导您完成 Citrix Endpoint Management 部署的 NetScaler 功能的配置。您可以使用向导执行以下操作：

- **设置微型 VPN。**在这种情况下，远程用户可以访问内部网络中的应用程序和桌面。
  - 对于 Citrix Endpoint Management 仅 MAM 模式，必须使用 NetScaler Gateway 进行身份验证。
  - 对于 MDM 部署，Citrix 建议对移动设备 VPN 使用 NetScaler Gateway。
  - 对于耳鼻喉科部署，如果用户选择退出 MDM 注册，则设备将在旧版 MAM 模式下运行，并使用 NetScaler Gateway FQDN 进行注册。
- **配置基于证书的身份验证。**Citrix Endpoint Management 的默认配置是用户名和密码身份验证。要为 Citrix Endpoint Management 环境的注册和访问添加另一层安全性，请考虑使用基于证书的身份验证。
- **负载平衡 Citrix Endpoint Management 服务器。**如果您有多个 Citrix 端点管理服务器，或者 Citrix Endpoint Management 位于 DMZ 或内部网络内部（因此流量从设备流向 NetScaler 再到 Citrix 端点管理），则所有 Citrix 端点管理设备模式都需要 NetScaler 负载平衡。在这种情况下，NetScaler 设备位于用户设备和 Citrix Endpoint Management 服务器之间的 DMZ 中，用于对从移动设备发送到 Citrix Endpoint Management 服务器的加密数据进行负载平衡。
- **使用电子邮件筛选功能对 Microsoft Exchange 服务器进行负载平衡。**在这种情况下，NetScaler 设备位于用户设备和 Citrix Endpoint Management NetScaler Connector (XNC) 之间，以及在用户设备和 Microsoft Exchange CAS 服务器之间。来自用户设备的所有请求都将发送到 NetScaler Gateway 设备，然后该设备与 XNC 通信以检索有关设备的信息。根据 XNC 的响应，NetScaler 设备会将请求从列入白名单的设备转发到内部网络中的服务器，或者从列入黑名单的设备中断连接。
- **根据请求的内容类型对 ShareFile StorageZones 连接器进行负载平衡。**此方案会提示您输入有关存储区域控制器环境的基本信息，然后生成执行以下操作的配置：
  - 跨存储区域控制器负载平衡流量。
  - 为 StorageZones 连接器提供用户身份验证。

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

- 验证 ShareFile 上载和下载的 URI 签名。
- 在 NetScaler 设备上终止 SSL 连接。

有关配置 ShareFile 的更多信息，请参阅 为存储区域控制器配置 NetScaler。

重要：

在使用 Citrix Endpoint Management 向导之前，请务必参阅以下 Citrix Endpoint Management 部署文章以获取设计和部署信息以及建议：

Citrix Endpoint Management 集成
与 NetScaler Gateway 和 NetScaler 集成
MDX 应用程序的 SSO 和代理注意事项
身份验证
您只能使用适用于 Citrix Endpoint Management 的 NetScaler 向导一次。如果您想要多个 Citrix Endpoint Management 实例，例如用于测试、开发和生产环境，则必须为其他环境手动配置 NetScaler。以下支持文章列出了向导运行的命令，并提供了运行这些命令以创建 NetScaler 实例的说明：
NetScaler 上的 Citrix Endpoint Management 向导生成的命令-SSL 桥
NetScaler 上的 Citrix Endpoint Management 向导生成的命令-SSL 卸载

NetScaler 功能的许可要求

您必须安装许可证才能启用以下 NetScaler 功能：

- Citrix Endpoint Management MDM 负载平衡需要 NetScaler 标准许可证。
- 使用 StorageZones 进行 ShareFile 负载平衡需要 NetScaler 标准许可证。
- Exchange 负载平衡需要 NetScaler 许可证或高级许可证以及集成缓存许可证。

适用于 Citrix Endpoint Management 的 NetScaler 向导

本节提供了使用适用于 Citrix Endpoint Management 的 NetScaler 向导执行以下操作的示例：

- 设置微型 VPN 访问权限，以便远程用户连接到内部网络中 Citrix Endpoint Management 托管的资源
- 配置基于证书的身份验证。有关获取和安装公共 SSL 证书的信息，请参阅 安装和管理证书。
- 为 Citrix Endpoint Management 服务器配置负载平衡。

要使用向导：

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

1. 在 NetScaler GUI 中，单击“**配置**”选项卡，然后在“**与 Citrix 产品集成**”部分中单击 **XenMobile**。
2. 选择 Citrix Endpoint Management 版本，然后单击 **开始**使用。
3. 选择要配置的功能。此向导只能使用一次，因此必须手动执行后续配置。这些说明假设您选择了以下设置：**通过 NetScaler Gateway 进行访问**（适用于在 ENT 或 MAM 模式下运行的 Citrix Endpoint Management）和**平衡 Citrix Endpoint Management 服务器的负载**。
4. 在 **NetScaler Gateway 配置**页面上，输入面向外部的 NetScaler Gateway IP 地址、端口和虚拟服务器名称的值。
5. 在 **NetScaler Gateway 的服务器证书**页面的**证书**文件中，从**本地**或**设备**中选择证书文件。
   - 本地：在您的计算机上选择证书
   - 设备： 在 NetScaler Gateway（设备）上选择证书。
6. 在“**身份验证**”页面的“**主身份验证方法**”中，选择“**客户端证书**”，然后输入证书配置文件的名称。

   以下各步骤假定您已配置证书策略。

   如果必须创建证书策略，请单击“创建证书策略”。在 Citrix Endpoint Management 证书屏幕上，选择现有服务器证书或安装新证书。如果您运行多台 Citrix Endpoint Management 服务器，则需要为每台服务器添加一个证书。在“服务器登录名属性”中，根据您的要求指定 userPrincipalName 或 sAMAccountName。
7. 单击“**双重身份验证**”以启用双重身份验证，客户端证书身份验证，然后使用 LDAP 或 RADIUS 作为辅助身份验证类型。
8. 在**辅助身份验证方法**中，选择辅助身份验证方法。
   - 使用客户端证书作为主要身份验证类型，您可以选择将 LDPA（或 RADIUS）配置为辅助身份验证类型。

     要仅使用客户端证书身份验证，请将 **第二种身份验证方法** 保留为 **无** ，然后单击 **继**

     要使用客户端证书+域 (LDAP) 身份验证，请将**辅助身份验证方法**更改为 **LDAP** 并配置身份验证服务器设置。
9. 配置 **Citrix Endpoint Management 应用程序管理设置**。
   - 输入 **Citrix Endpoint Management FQDN**。这是 MAM 的负载平衡 FQDN。
   - 为 **负载平衡 Citrix Endpoint Management 服务器的虚拟服务器输入仅限 MAM 的内部负载平衡 IP 地址**。NetScaler Gateway 通过此 MAM 负载平衡虚拟 IP 与 Citrix Endpoint Management 进行通信。
   - 这是 SSL 卸载部署，因此**请在**与 Citrix Endpoint Management 服务器通信**中选择 HTTP**。

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

- **MicroVPN 的拆分 DNS 模式**字段会自动设置为**两者**。

如果您的部署需要拆分通道，请选择 **启用拆分通道**。接下来，如果启用拆分通道，请配置 Intranet 应用程序绑定。

默认情况下，安全 Web 访问通过通道传输到内部网络，这意味着 Secure Web 使用每个应用程序的 VPN 通道返回到内部网络进行所有网络访问，NetScaler 设备使用拆分通道设置。

10. 要在 NetScaler Gateway 上为用户连接配置拦截规则，必须配置 **Intranet 应用程序绑定**。单击 **+** 添加绑定。
11. 填写允许网络访问的参数，然后单击 **创建**。
12. 添加 Citrix Endpoint Management 证书。这用于 MAM 负载平衡虚拟服务器。
13. 在 **Citrix Endpoint Management 服务器**下，单击 **添加服务器** 以添加要绑定到负载平衡虚拟 **IP 的 Citrix Endpoint Management IP 地址**。

在 NetScaler 控制面板上，确认已配置 NetScaler Gateway 和 Citrix Endpoint Management 负载平衡。

如果您使用用户证书中的 sAMAccount 属性来替代用户主体名称 (UPN)，请按照手动配置 NetScaler Gateway 进行客户端证书身份验证中所述配置证书配置文件。

使用 Web Interface 访问 Citrix Virtual Apps and Desktops 资源

一台或多台运行 Citrix Virtual Apps and Desktops 的计算机将创建服务器场。如果您的企业网络包含服务器场，则可以部署 Citrix Gateway，以使用 Web Interface 提供对已发布应用程序或虚拟桌面的安全 Internet 访问。

在此类部署中，Citrix Gateway 支持 Web Interface 和安全票证颁发机构 (STA)，以向运行 Citrix Virtual Apps 的计算机上托管的已发布应用程序或 Citrix Virtual Desktops 提供的虚拟桌面提供身份验证、授权和重定向功能。

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

此功能可通过将 Citrix Gateway 与 Web Interface 、Citrix Virtual Apps 和桌面集成来实现。此集成为 Web Interface 提供高级身份验证和访问控制选项。有关 Web Interface 的详细信息，请参阅 Citrix 文档库中的 Web Interface 文档。

远程连接到服务器场不需要 Citrix Secure Access 代理。要访问已发布的应用程序或桌面，用户可以使用 Citrix Workspace 应用程序进

将 Citrix Gateway 与 Citrix Virtual Apps and Desktops 集成

为用户连接配置 Citrix Gateway 时，您可以包括针对 Citrix Virtual Apps、Citrix Virtual Desktops 或两者的网络流量的设置。为此，需要将 Citrix Gateway 和 Web Interface 配置为相互通信。

集成这些产品的任务包括：

- 在 Citrix Virtual Apps and Desktops 场中创建 Web Interface 站点。
- 在 Web Interface 中配置设置以通过 Citrix Gateway 路由用户连接。
- 配置 Citrix Gateway 以与 Web Interface 和安全票证颁发机构 (STA) 进行通信。

您还可以通过在双跳 DMZ 中部署 Citrix Gateway，将 Citrix Gateway 配置为与 Citrix Virtual Apps 服务器场进行通信。有关更多信息，请参阅在 双跃点 DMZ 中部署 Citrix Gateway。

Citrix Gateway 和 Web Interface 使用 STA 和 Citrix XML 服务来建立用户连接。STA 和 XML 服务在 Citrix Virtual Apps and Desktops 服务器上运行。

建立与服务器场的安全连接

以下示例说明了部署在 DMZ 中的 Citrix Gateway 如何工作，支持 Web Interface 提供对安全企业网络中可用的已发布资源的安全单点访问。

在此示例中，存在以下条件：

- 来自互联网的用户设备通过使用 Citrix Workspace 应用程序连接到 Citrix Gateway。
- Web Interface 位于安全网络中的 Citrix Gateway 后面。用户设备与 Citrix Gateway 建立初始连接，然后将连接传递到 Web Interface 。
- 安全网络包含一个服务器场。此服务器场中的一台服务器运行 Secure Ticket Authority (STA) 和 Citrix XML 服务。STA 和 XML 服务可以在 Citrix Virtual Apps and Desktops 上运行。

进程概述：用户访问服务器场中的已发布资源

1. 远程用户键入 Citrix Gateway 的地址；例如 `https://www.ag.wxyco.com`，在 Web 浏览器的地址字段中。用户设备在端口 443 上尝试此 SSL 连接，该端口必须通过防火墙打开才能成功连接。

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

2. Citrix Gateway 会收到连接请求，系统会要求用户提供凭据。凭据将通过 Citrix Gateway 传回，对用户进行身份验证，然后将连接传递到 Web Interface 。
3. Web Interface 会将用户凭据发送到服务器场中运行的 Citrix XML 服务。
4. XML 服务对用户凭据进行身份验证，并向 Web Interface 发送用户有权访问的已发布应用程序或桌面的列表。
5. Web Interface 使用用户有权访问的已发布资源（应用程序或桌面）的列表填充网页，然后将此网页发送到用户设备。
6. 用户单击已发布的应用程序或桌面链接。一个 HTTP 请求将发送到 Web Interface，指出用户所单击的已发布资源。
7. Web Interface 与 XML 服务进行交互，并收到一个表示运行已发布资源的服务器的票证。
8. Web Interface 向 STA 发送会话票证请求。此请求指定运行已发布资源的服务器的 IP 地址。STA 会保存此 IP 地址并将请求的会话票证发送到 Web Interface 。
9. Web Interface 会生成一个包含 STA 签发的票证的 ICA 文件，并将其发送到用户设备上的 Web 浏览器。Web Interface 生成的 ICA 文件包含 Citrix Gateway 的完全限定域名 (FQDN) 或域名系统 (DNS) 名称。运行所请求资源的服务器的 IP 地址永远不会泄露给用户。
10. ICA 文件包含指示 Web 浏览器启动 Citrix Workspace 应用程序的数据。用户设备通过使用 ICA 文件中的 Citrix Gateway FQDN 或 DNS 名称连接到 Citrix Gateway。进行初始 SSL/TLS 握手是为了建立 Citrix Gateway 的身份。
11. 用户设备将会话票证发送到 Citrix Gateway，然后 Citrix Gateway 联系 STA 进行票证验证。
12. STA 将请求的应用程序所在的服务器的 IP 地址返回到 Citrix Gateway。
13. Citrix Gateway 建立到服务器的 TCP 连接。
14. Citrix Gateway 完成与用户设备的连接握手，并向用户设备指示已与服务器建立连接。用户设备和服务器之间的所有进一步流量都通过 Citrix Gateway 进行代理。用户设备与 Citrix Gateway 之间的流量已加密。Citrix Gateway 与服务器之间的流量可以独立加密，但默认情况下不会加密。

配置 Web Interface 故障切换

您可以使用已发布的应用程序向导将 Citrix Gateway 配置为故障切换到运行 Web Interface 的辅助服务器。

如果主 Web Interface 出现故障，Web Interface 故障切换允许用户连接保持活动状态。配置故障切换时，除了系统 IP 地址、映射的 IP 地址或虚拟服务器 IP 地址之外，还要定义新的 IP 地址。新 IP 地址必须与系统或映射的 IP 地址位于同一子网中。

在 Citrix Gateway 上配置 Web Interface 故障切换时，发送到新 IP 地址的任何网络流量都将中继到主 Web Interface 。在 “已发布的应用程序” 向导中选择的虚拟服务器将用作网络地址转换 (NAT) IP

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

地址。真正的 IP 地址是 Web Interface 的 IP 地址。如果主 Web Interface 出现故障，网络流量将发送到辅助 Web Interface 。

配置 Web Interface 故障切换

1. 在配置实用程序中，单击配置选项卡，然后在导航窗格中单击 Citrix Gateway。
2. 在详细信息窗格的入门下，单击已发布的应用程序向导。
3. 单击下一步，选择虚拟服务器，然后单击下一步。
4. 在 “配置客户端连接” 页上，单击配置 Web Interface 故障切换。
5. 在主 Web Interface 下的 Web Interface 服务器中，键入主 Web Interface 的 IP 地址。
6. 在 Web Interface 服务器端口中，键入主 Web Interface 的端口号。
7. 在虚拟服务器 IP 中，键入用于故障切换的新 IP 地址。
8. 在虚拟服务器端口中，输入虚拟服务器的端口号。
9. 在 “备份 Web Interface ” 下的 “Web Interface 服务器” 中，键入运行 Web Interface 的服务器的 IP 地址，或从列表中选择一个服务器。
10. 在 Web Interface 服务器端口中，键入 Web Interface 的端口号，然后单击确定。
11. 单击 “下一步”，然后按照说明完成向导。

使用 Web Interface 配置智能卡访问

将 Web Interface 配置为使用智能卡身份验证时，可以配置以下部署方案以便集成 Citrix Gateway，具体取决于用户的登录方式：

- 如果用户使用 Citrix Workspace 应用程序和智能卡身份验证直接登录到 Web Interface ，则 Web Interface 必须与 DMZ 中的 Citrix Gateway 并行。运行 Web Interface 的服务器也必须是域成员。

  在这种情况下，Citrix Gateway 和 Web Interface 都会执行 SSL 终止。Web Interface 终止安全的 HTTP 流量，包括用户身份验证、显示已发布的应用程序以及启动已发布的应用程序。Citrix Gateway 为传入的 ICA 连接终止 SSL。
- 如果用户使用 Citrix Secure Access 代理登录，Citrix Gateway 将执行初始身份验证。Citrix Gateway 建立 VPN 隧道后，用户可以使用智能卡登录 Web Interface 。在这种情况下，您可以在 DMZ 或安全网络中的 Citrix Gateway 后面安装 Web Interface 。

注意

- Citrix Gateway 还可以使用客户端证书使用智能卡进行身份验证。

有关详细信息，请参阅 配置智能卡验证

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

Web Interface 功能

在为 Citrix Gateway 配置 Web Interface 之前，必须了解 Citrix Virtual Apps 网站与 Citrix Virtual Apps 服务站点之间的区别。

- **Citrix Virtual Apps 网站。**Web Interface 提供创建和管理 Citrix Virtual Apps 网站的功能。用户使用 Web 浏览器和插件远程访问已发布的资源和流式传输的应用程序。
- **Citrix Virtual Apps 服务站点。**Citrix Virtual Apps 是一款专为灵活性和易于配置而设计的插件。通过将 Citrix Virtual Apps 与 Web Interface 上的 Citrix Virtual Apps 服务站点结合使用，您可以将已发布的资源与用户的桌面用户可以通过单击桌面上的图标或 “开始” 菜单上的图标，或单击计算机桌面的通知区域来访问远程应用程序和流应用程序以及远程桌面和内容。您可以确定用户可以访问和修改的配置选项，例如音频、显示和登录设置。

  注意：
  如果选择此选项，则不支持访问虚拟桌面。

有关更多信息，请参阅 Citrix 产品文档。

设置 Web Interface 站点

如果在安全网络中部署 Web Interface 并在 Citrix Gateway 上配置身份验证，则当用户连接到 Citrix Gateway 时，设备将对用户进行身份验证。

重要提示：

在配置 Citrix Gateway 之前，请先安装并配置 Web Interface 。有关详细信息，请参阅 Citrix 产品文档中的 Web Interface 文档。

创建 Web Interface 站点的步骤包括：

- 选择用户的登录方式。您可以通过 Web 浏览器、Citrix Secure Access 代理或 Citrix Workspace 应用程序登录。有关信息，请参阅 Web Interface 功能。
- 确定用户从何处进行身份验证。Citrix Gateway 或 Web Interface 。

注意：

当 Web Interface 位于安全网络中时，您可以在 Citrix Gateway 上的虚拟服务器上启用身份验证。禁用身份验证后，未经身份验证的 HTTP 请求将直接发送到运行 Web Interface 的服务器。仅当 Web Interface 位于 DMZ 中且用户直接连接到 Web Interface 时，才建议在 Citrix Gateway 上禁用身份验证。

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

确保在 Citrix Gateway 上安装了有效的服务器证书。有关使用证书的详细信息，请参阅 安装和管理证书。

重要提示：

为了使 Web Interface 与 Citrix Gateway 10.1 正常工作，运行 Web Interface 的服务器必须信任 Citrix Gateway 证书，并能够将虚拟服务器完全限定域名 (FQDN) 解析为正确的 IP 地址。

配置 SmartAccess

您可以将 SmartAccess 与 Citrix Virtual Apps and Desktops 结合使用，智能地向用户交付已发布的应用程序和虚拟桌

SmartAccess 允许您使用 Citrix Gateway 会话策略控制对服务器上已发布的应用程序和桌面的访问。您可以将预身份验证和身份验证后检查以及其他条件用作访问已发布资源的条件。其他条件包括您可以使用 Citrix Virtual Apps and Desktops 策略控制的任何内容，例如打印机带宽限制、用户设备驱动器映射、剪贴板、音频和打印机映射。您可以根据用户是否通过 Citrix Gateway 检查来应用 Citrix Virtual Apps and Desktops 策略。

Citrix Gateway 可以使用与 Web Interface 、ICA 代理访问、无客户端访问和 Citrix Gateway 访问相同的选项来交付 Citrix Virtual Desktops。

此功能可通过将 Citrix Gateway 组件与 Web Interface 以及 Citrix Virtual Apps and Desktops 集成来实现。此集成为 Web Interface 提供高级身份验证和访问控制选项。有关详细信息，请参阅 Citrix 产品文档中 “技术” 节点中的 Web Interface 文档。

远程连接到服务器场不需要 Citrix Secure Access 代理。用户可以使用 Citrix Workspace 应用程序连接。用户可以使用 Citrix Secure Access 代理登录并通过访问界面（Citrix Gateway 的默认主页）接收其已发布的应用程序和虚拟桌面。

SmartAccess 如何适用于 Citrix Virtual Apps and Desktops

要配置 SmartAccess，您需要在 Web Interface/StoreFront 上配置 Citrix Gateway 设置，并在 Citrix Gateway 上配置会话策略。运行已发布的应用程序向导时，可以选择为 SmartAccess 创建的会话策略。

配置 SmartAccess 后，该功能的工作方式如下：

1. 当用户在 Web 浏览器中输入虚拟服务器的 Web 地址时，您配置的任何预身份验证策略都会下载到用户设备。

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

2. Citrix Gateway 将预身份验证和会话策略名称作为筛选器发送到 Web Interface/StoreFront。如果策略条件设置为 true，则始终以筛选器名称的形式发送策略。如果不满足策略条件，则不会发送筛选器名称。这使您可以根据端点分析的结果区分运行 Citrix Virtual Apps and Desktops 的计算机上已发布的应用程序和桌面的列表以及有效策略。
3. Web Interface/StoreFront 会联系 Citrix Virtual Apps and Desktops 服务器，并将已发布的资源列表返回给用户。除非满足筛选器的条件，否则应用了筛选器的任何资源都不会显示在用户列表中。

您可以在 Citrix Gateway 上配置 SmartAccess 端点分析。要配置端点分析，请创建启用 **ICA 代理** 设置的会话策略，然后配置客户端安全字符串。

用户登录时，端点分析策略将使用您在 Citrix Gateway 上配置的客户端安全字符串对用户设备运行安全检查。

例如，你想检查 Sophos Antivirus 的特定版本。在表达式编辑器中，客户端安全字符串显示为：

```
client.application.av(sophos).version == 10.0.2
```

配置会话策略后，将其绑定到用户、组或虚拟服务器。当用户登录时，SmartAccess 策略检查将启动并验证用户设备是否安装了 Sophos Antivirus 10.0.2 或更高版本。

当 SmartAccess 端点分析检查成功后，Web Interface/StoreFront 门户会出现在无客户端会话中。否则，将显示访问接口。

为 SmartAccess 创建会话策略时，会话配置文件没有配置任何设置，这会创建空配置文件。在这种情况下，Citrix Gateway 使用为 SmartAccess 全局配置的 Web Interface/StoreFront URL。

配置 Citrix Virtual Apps 策略和筛选器

在 Citrix Gateway 上创建会话策略后，可以在运行 Citrix Virtual Apps 的计算机上配置策略和筛选器。策略和筛选器将根据端点分析配置应用于用户。

有关配置 Citrix Virtual Apps 策略和筛选器的详细信息，请参阅 管理交付组。

在 Citrix Virtual Desktops 5 中配置策略和筛选器

您可以使用 Citrix Studio 或组策略编辑器在 Citrix Virtual Desktops 5 中配置设置。在 Citrix Virtual Desktops 中配置 Citrix Gateway 设置时，请使用 Citrix Gateway 虚拟服务器名称和会话策略名称。然后，配置访问控制以允许连接满足定义的过滤器。您还可以使用 SmartAccess 策略。

1. 在 Citrix Virtual Desktops 服务器上，单击 **开始 > 所有程序 > Citrix > Citrix Studio**。
2. 在左窗格中，单击以展开 HDX Policy，然后单击中间窗格中的 “用户” 选项卡。

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

3. 在用户下，单击新建。
4. 在 “新建策略” 对话框的 “识别您的策略” 下，然后在 “名称” 中键入名称。
5. 单击下一步两次。
6. 在 “新建策略” 对话框的 “筛选器” 选项卡的 “筛选器” 下，单击 “访问控制”，然后单击 “添加”。
7. 在 “新建筛选器” 对话框中，单击 “添加”。
8. 在 “新建过滤器元素” 对话框的 “连接类型” 中，选择 “使用接入网关”。

   要在不考虑 Citrix Gateway 策略的情况下将策略应用于通过 Citrix Gateway 建立的连接，请在 AG 场名称和访问条件中保留默认条目。
9. 如果要将策略应用于基于现有 Citrix Gateway 策略通过 Citrix Gateway 建立的连接，请执行以下操作：

   a. 在 AG 场名称中，键入虚拟服务器名称。

   b. 在访问条件中，键入端点分析策略或会话策略的名称。

   重要提示：
   Citrix Virtual Desktops 不会验证 Citrix Gateway 虚拟服务器、端点分析策略或会话策略名称。确保信息正确无误。
10. 单击确定两次，单击下一步，然后单击创建。

使用智能卡配置单点登录 Web Interface

如果使用智能卡进行用户登录，则可以配置 Web Interface 的单点登录。在 Citrix Gateway 上配置设置，然后将 Web Interface 配置为接受使用智能卡的单点登录。单点登录也称为直通身份验证。

Web Interface 版本 5.3 和 5.4 支持使用智能卡单点登录 Web Interface 。如果在 NetScaler 版本 10 中提供的 Citrix ADC 功能上启用 Web Interface ，则还可以通过智能卡使用单点登录。有关配置此功能的详细信息，请参阅 通过 Citrix Gateway 为 Web Interface 使用智能卡身份验证。

只要证书操作中的用户名提取为 SubjectALTName: PrincipalName，用户就可以位于 Active Directory 中的多个 CN 组中以便单点登录正常工作。如果使用参数 Subject: CN，则用户不能加入多个 CN 组。

要使用智能卡配置 Citrix Gateway 以便单点登录 Web Interface ，您需要执行以下操作：

- 从证书颁发机构 (CA) 安装签名的服务器证书。有关详细信息，请参阅 在 Citrix Gateway 上安装签名证书。
- 在 Citrix Gateway 和用户设备上安装根证书。

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

- 创建虚拟服务器作为 Web Interface 的登录点。配置虚拟服务器时，必须将客户端证书 SSL 参数设置为可选。有关配置虚拟服务器的详细信息，请参阅 创建虚拟服务器。
- 创建在 SSL 参数中禁用客户端身份验证的辅助虚拟服务器。此配置可防止用户接收其个人识别码 (PIN) 的辅助请求。
- 创建客户端证书身份验证策略。在用户名字段中，使用参数 SubjectaltName: PrincipalName 从多个组中提取用户。将 “组名称” 字段留空。
- 在 Citrix Gateway 上创建会话策略和配置文件。在会话配置文件中，您可以启用 ICA 代理并指定用于单点登录的 Web Interface 和域。

您可以使用以下过程为使用智能卡的单点登录创建会话配置文件。

使用智能卡为单点登录创建会话配置文件

1. 在配置实用程序中的配置选项卡的导航窗格中，展开 **Citrix Gateway P策略** ，然后单击 **会话**。
2. 在详细信息窗格中，单击 **配置文件选项卡，** 然后单击 **添加**。
3. 在 “ **客户端体验** ” 选项卡上的 “主页” 旁边，单击 “ **覆盖全局”，** 然后清除 “ **显示主页**”。
4. 在 **单点登录 Web 应用程序**旁边，单击 **覆盖全局，** 然后 **单击单点登录到 Web 应用程序**。
5. 单击 **Published Applications**（已发布的应用程序）选项卡。
6. 在 **ICA 代理**旁边，单击 **覆盖全局，** 然后选择 **开**。
7. 在 **Web Interface 地址**中，单击 **覆盖全局** ，然后键入完全限定域名 (FQDN) 或 Web Interface 。
8. 在 **单点登录域**中，单击 **覆盖全局，** 然后键入域名。

   注意

   ：使用格式域而不是格式域。

9. 单击 **Create**（创建），然后单击 **Close**（关闭）。

完成会话配置文件后，配置会话策略并将配置文件用作策略的一部分。然后，您可以将会话策略绑定到虚拟服务器。

与 Citrix Endpoint Management 或 StoreFront 集成

本节包含有关配置从远程用户通过 NetScaler Gateway 到 Endpoint Management 和 StoreFront 部署的连接的信息。

您可以将 NetScaler Gateway 配置为支持 Endpoint Management 和 StoreFront。将 NetScaler Gateway 配置为支持 Endpoint Management 或 StoreFront 时，Citrix 建议使用快速配置向导来配置

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

设置。快速配置向导配置虚拟服务器以及会话、无客户端访问和身份验证策略的设置。您还可以配置 DNS 服务器以连接到 StoreFront 和 Endpoint Management。

集成 NetScaler Gateway 和 Endpoint Management

如果在网络中部署 Endpoint Management，则可以通过集成 NetScaler Gateway 和 Endpoint Management 来允许来自远程用户的用户连接。此部署允许用户连接到 Endpoint Management 以获取他们的 Web、软件即服务 (SaaS)、Android 和 iOS 移动应用程序以及来自 ShareFile 的文档。用户使用 Secure Hub、Citrix Workspace 应用程序或 Citrix Secure Access 客户端进行连接。

在此 Endpoint Management 部署中，NetScaler Gateway 驻留在 DMZ 中，Endpoint Management 位于内部网络中。

要允许从远程用户连接到 Endpoint Management，Citrix 建议使用 NetScaler Gateway 中的快速配置向导为 Endpoint Management、StoreFront 或 Web Interface 配置 Web 地址。该向导配置用户连接到 Endpoint Management 所需的所有策略，其中包括身份验证、会话和无客户端访问策略。 有关向导的详细信息，请参阅使用快速配置向导配置设置。

您还可以通过使用配置实用程序创建策略来配置与 Endpoint Management 的连接，例如：

- 一个会话策略管理 Citrix Workspace 应用程序和与 StoreFront 的 Secure Hub 连接。此会话策略支持适用于 Windows 的 Citrix Workspace 应用程序、适用于 Mac 的 Citrix Workspace 应用程序、适用于 Android 的 Citrix Workspace 应用程序和适用于 iOS 如果用户在 iOS 设备上使用 Secure Hub、Secure Mail 或 WorxWeb 进行连接，则必须启用无客户端访问和 Secure Browse 才能允许通过 NetScaler Gateway 进行连接。仅为 iOS 设备配置 Secure Browse。iOS 和 Android 设备都使用 Micro VPN 来建立通往内部网络的 VPN 通道。
- 一个会话策略可管理浏览器与适用于 Web 的 Citrix Workspace 应用程序用户使用无客户端访问进行连接。
- 一台启用了 SmartAccess 模式的虚拟服务器，该模式还启用了无客户端此部署需要通用许可证。
- 自定义无客户端访问策略。这些策略定义了 XML 和 HTML 流量的重写策略，以及 NetScaler Gateway 如何处理 Cookie。

集成 NetScaler Gateway 和 StoreFront

用户可以通过 StoreFront 通过以下方式之一进行连接：

- 无客户端访问和适用于 Web 的 Citrix Workspace 应用
- Citrix Secure Access
- 适用于 Android 的 Citrix Workspace 应用程序

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

- 适用于 iOS 的 Citrix Workspace 应用程序
- 适用于 Mac 的 Citrix Workspace 应用程序
- 适用于 Windows 的 Citrix Workspace 应用程序
- Secure Hub

重要：

StoreFront 的完全限定域名 (FQDN) 必须唯一且不同于 NetScaler Gateway 虚拟服务器 FQDN。不能对 StoreFront 和 NetScaler Gateway 虚拟服务器使用相同的 FQDN。Citrix Workspace 应用程序要求 StoreFront FQDN 是唯一地址，只能从连接到内部网络的用户设备进行解析。否则，适用于 Windows 的 Citrix Workspace 应用程序将无法使用基于电子邮件的帐户发

用户连接后，Citrix Workspace 应用程序窗口中将显示可用应用程序、桌面和文档的列表。用户还可以从商店订阅应用程序。该应用商店枚举和聚合 Citrix Virtual Desktops 站点、Citrix Virtual Apps 场和 Endpoint Management 中的桌面和应用程序，使用户可以使用这些资源。

注意：

要允许用户访问 MDX 移动应用程序，必须在 StoreFront 前部署 Endpoint Management。如果您不提供对 MDX 移动应用程序的访问权限，则 StoreFront 将驻留在 Endpoint Management 之前。

将 NetScaler Gateway 配置为连接到 StoreFront 时，需要配置以下内容：

- 一个会话策略用于管理 Secure Hub 和 Citrix Workspace 应用程序与 StoreFront 的连接此会话策略支持适用于 Windows 的 Citrix Workspace 应用程序、适用于 Mac 的 Citrix Workspace 应用程序、适用于 Android 的 Citrix Workspace 应用程序和适用于 iOS 如果用户使用适用于 Android 的 Citrix Workspace 应用程序或适用于 iOS 的 Citrix Workspace 应用程序连接，则必须启用无客户端访问和 Secure Browse 才能允许通过 NetScaler Gateway
- 一个会话策略，用于管理浏览器与适用于 Web 的 Citrix Workspace 应用程序用户使用无客户端访问进行连接。
- 一个会话策略用于管理通过适用于 Android 的 Citrix Workspace 应用程序、适用于 iOS 的 Citrix Workspace 应用程序和其他移动设备建立的 PNA 服务连接（如果未启用 Secure Browse）。如果为 PNA 服务配置会话策略，则不支持适用于 Windows 的 Citrix Workspace 应用程序。
- 一台启用了 SmartAccess 模式的虚拟服务器，该模式还启用了无客户端此部署需要通用许可证。
- 自定义无客户端访问策略。这些策略定义了 XML 和 HTML 流量的重写策略，以及 NetScaler Gateway 如何处理 Cookie。

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

为 Endpoint Management 和 StoreFront 配置策略

如果您部署了 Endpoint Management 和 StoreFront，但不使用快速配置向导来配置设置，则需要配置以下策略。您可以为仅 NetScaler Gateway 和 Endpoint Management、NetScaler Gateway 和 StoreFront 或包含 NetScaler Gateway、Endpoint Management 和 StoreFront 的部署配置这些策略。

- 一个会话策略，用于管理 Citrix Workspace 应用程序与 Endpoint Management 或 StoreFront 的此会话策略支持适用于 Windows 的 Citrix Workspace 应用程序、适用于 Mac 的 Citrix Workspace 应用程序、适用于 Android 的 Citrix Workspace 应用程序和适用于 iOS 如果用户连接到适用于 Android 的 Citrix Workspace 应用程序或适用于 iOS 的 Citrix Workspace 应用程序，则必须启用无客户端访对于来自适用于 iOS 的 Citrix Workspace 应用程序的连接，必须启用 Secure Browse 才能允许通过 NetScaler Gateway 进行
- 一个会话策略，用于管理浏览器与适用于 Web 的 Citrix Workspace 应用程序用户使用无客户端访问进行连接。
- 一台启用了 SmartAccess 模式的虚拟服务器，该模式还启用了无客户端此部署需要通用许可证。
- 自定义无客户端访问策略。这些策略定义了 XML 和 HTML 流量的重写策略，以及 NetScaler Gateway 如何处理 Cookie。

如果您部署了 StoreFront 并且用户连接到旧版 Citrix Workspace 应用程序，请创建一个会话策略来管理通过适用于 Android 的 Citrix Workspace 应用程序、适用于 iOS 的 Citrix Workspace 应用程序以及其他移动设备建立的 PNA 服务连接（如果未启用 Secure Browse）。如果为 PNA 服务配置会话策略，则不支持适用于 Windows 的 Citrix Workspace 应用程序。

注意： 在 NetScaler Gateway 中配置 StoreFront URL（例如 `https://<SFLite-FQDN>/Citrix/StoreWeb`）时，StoreWeb 文本区分大小写。

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