Citrix Secure Private Access™

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

Contents

安全私有访问服务解决方案概述 25
- 自适应安全性 25
- 应用程序访问 25
- 单点登录 25
- 浏览器安全性 26
- 设备状态 26
- 支持 TCP 和 UDP 应用程序 26
- 示例用例 26
- 参考文章 27
- 参考视频 27
- 相关产品中的新增功能 27

最新功能 28
- 30 September 2026 28
- 03 September 2026 28
- 19 August 2026 29
- 05 August 2026 29
- 31 July 2026 29
- 24 June 2026 30
- 18 June 2026 30
- 09 June 2026 30
  - 重要通知 30
- 20 May 2026 31
- 28 April 2026 32
- 07 April 2026 32
- 04 March 2026 32
- 12 February 2026 32

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

05 February 2026 32
18 December 2025 33
16 December 2025 33
11 December 2025 33
30 October 2025 34
17 September 2025 34
13 August 2025 35
14 July 2025 35
03 June 2025 36
15 May 2025 36
24 April 2025 36
22 April 2025 37
20 February 2025 37
08 January 2025 38
07 January 2025 38
02 January 2025 39
03 December 2024 39
25 November 2024 39
14 November 2024 39
08 November 2024 40
07 November 2024 40
23 September 2024 40
15 August 2024 40
16 July 2024 41
11 June 2024 41
13 March 2024 41
12 February 2024 42
23 January 2024 42

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

20 December 2023 42
16 October 2023 42
11 September 2023 43
30 August 2023 43
28 August 2023 43
22 August 2023 43
17 August 2023 43
07 June 2023 44
29 May 2023 44
10 April 2023 44
29 March 2023 44
07 March 2023 44
23 January 2023 45
22 December 2022 45
03 October 2022 45
09 September 2022 46
01 June 2022 47
04 April 2022 47
16 February 2022 49
11 October 2021 49
30 July 2021 50
09 June 2021 50
22 May 2021 50
01 May 2021 51
15 March 2021 51
11 November 2020 51
15 October 2020 51
08 October 2020 52

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

24 September 2020 52
07 July 2020 52
19 June 2020 52
08 May 2020 53
V2019.04.02 53
V2019.04.01 53
V2019.03.01 53
与 谷歌 Chrome 企业高级版 集成 55
解决方案概述 55
Chrome Enterprise Premium 高级安全功能 56
适用于 Chrome Enterprise 的 Citrix Secure Access 控件 56
成功集成的先决条件 56
Citrix Secure Private Access - 支持的部署模式 57
法律声明 57
相关主题 57
集成解决方案的先决条件 58
许可证、应用程序版本和扩展 58
Google 管理控制台 59
安全专用访问服务 59
谷歌浏览器 60
管理用户 60
强制 - 填充用户的电子邮件地址字段 60
强制 - 填充用户组的电子邮件地址字段 60
电子邮件地址缺失或不一致的域映射注意事项 61
将 Citrix Secure Private Access 中配置的用户目录与 Google Cloud 用户目录关联 61
活动目录 61
微软 Entra ID 62
奥克塔 62

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

谷歌云身份 (谷歌目录) 62
绕过 TLS 检查 63
管理员角色和权限 63
Google 自定义管理员角色权限 64
创建和分配角色和权限 65
配置出口中心区域 66
SaaS 应用程序出口区域面板 66
选择区域 68
取消选择区域 68
没有电子邮件地址的用户组的域映射 70
域映射的工作原理 70
电子邮件地址构建 73
限制 73
托管配置文件身份 73
设置用户属性类型 74
Open ID Connect 与 Citrix 身份和访问管理 74
概述 75
先决条件 75
OIDC 集成概述 76
创建 Google OIDC SSO 配置文件 77
创建 Citrix OIDC 客户端 79
OIDC SSO 配置文件分配 80
更新 Citrix OIDC 客户端 80
删除 OIDC 客户端 81
最终用户体验 82
适用于 Chrome Enterprise Premium 的 Citrix Secure Access 扩展程序 84
Secure Access 扩展程序日志 84
适用于 Chrome Enterprise 的 Citrix Secure Access 控件 85

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

支持的控件 87
策略中的用户和组 87
搜索用户或组 87
使用同步的用户和组 88
防键盘记录控制 88
先决条件 89
配置防键盘记录策略 89
剪贴板容器控制 89
先决条件 90
启用剪贴板容器控制 90
启用剪贴板共享范围 91
Web 应用程序的域后缀 93
先决条件 94
配置 DNS 后缀 94
会话录制控制 95
体系结构 95
必备条件 95
系统要求 96
设置环境 96
浏览器会话重新身份验证控制 97
先决条件 97
启用浏览器会话重新身份验证控制 97
SSH 控制 99
此集成的优势 99
用例 99
系统要求 100
先决条件 100
配置安全专用访问以进行 SSH 访问 100

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

配置 SSH 策略 100

远程桌面控制 101

此集成的优势 102

用例 102

系统要求 102

先决条件 102

配置 Secure Private Access 以进行 RDP 访问 102

配置远程桌面策略 103

排查 CEP 集成问题 103

用于 CEP 故障排除的诊断日志 104

确认用户已登录到正确的 Chrome 配置文件 105

检查 Secure Enterprise Browser 扩展是否已安装 105

检查 ExtensionInstallForcelist 策略 105

排查冲突的扩展程序安装列表策略 106

检查 Secure Enterprise Browser 扩展策略 106

检查 Google 管理控制台中的用户扩展配置 108

检查路由是否正在获取 108

在 Secure Private Access 管理控制台中验证 CEP 集成 109

排查 Google 安全网关可达性问题 110

确认应用程序包含在路由中 110

排查路由应用程序访问问题 110

确保 IdP 和 Google Directory 对齐 111

检查 Google Admin Console 中组的访问设置 112

CEP 集成中的已知问题 112

Secure Private Access 用户界面 112

自适应访问策略配置 112

Google Chrome 浏览器 112

开放身份连接 (OIDC) 113

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

开始使用 Citrix 安全私有访问 114
系统要求 114
工作原理 114
开始使用 Citrix Secure Private Access 服务 115
Secure Private Access 服务部署模型 116
Citrix Secure Private Access™ 服务的存在点 (PoP) 位置 117
Secure Private Access 管理接入点 117
安全私有访问数据接入点 118
Secure Private Access 的入门和设置 119
将用户载入 Secure Private Access 119
在 Citrix StoreFront Cloud 中配置商店 URL 121
设置 Google Chrome 集成 122
添加 SaaS 应用程序的 IP 地址 124
主体访问边界策略配置 124
载入后更新 Google 集成详细信息 124
为 Google Directory 组织单位配置 CEP 126
已知验证故障和警告 129
多个用户组的预配失败问题 131
后续步骤 131
数据区域化 132
支持的部署 132
配置 133
限制 133
应用程序配置和管理 134
配置企业 Web 应用程序 134
系统要求 134
工作原理 135
配置 Web 应用程序 135

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

删除应用程序时自动清理路由条目 145
配置 SaaS 应用程序 146
Secure Private Access 服务如何支持 SaaS 应用程序 146
配置 SaaS 应用程序 147
通过 Google Secure Gateway 路由 156
删除应用程序时自动清理路由条目 156
SaaS 应用程序服务器特定配置 157
端到端应用程序配置 168
无代理访问企业 Web 应用程序 168
工作原理 169
配置 Citrix Secure Private Access 以实现对企业 Web 应用程序的无代理访问 169
删除应用程序时自动清理路由条目 179
使用无代理访问应用程序的设备状态服务 180
仅为合规设备启用无代理访问的步骤 180
最终用户体验 183
支持 TCP/UDP 应用程序 184
先决条件 184
为 TCP/UDP 应用程序配置 Secure Private Access 184
管理员配置 – Citrix Secure Access 客户端对 HTTP/HTTPS 应用程序的访问 190
先决条件 190
注意事项 190
对 TCP/UDP 和 HTTP(S) 应用程序的自适应访问 191
创建自适应访问策略 191
登录和注销脚本配置注册表 192
排查应用程序域 IP 地址冲突 192
注意事项 194
Windows 登录前始终开启 194
Always On 如何工作? 195

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

活动目录和 Microsoft Entra ID 混合 AD 配置 196

安全私有访问配置 199

连接器设备配置 202

在 Windows 登录后配置 Always On（计算机/用户隧道） 203

限制 203

参考 204

用于 TCP 和 UDP 服务器的保留 CIDR 地址 204

配置保留的 CIDR IP 地址 204

DNS 后缀以将 FQDN 解析为 IP 地址 205

先决条件 206

如何添加 DNS 后缀 206

用例示例 206

使用 HAR 文件发现相关域 208

示例 209

先决条件 209

导入 HAR 文件 209

管理相关域 212

验证和文件要求 212

使用路由例外的基于端口的路由 - 预览 213

基于端口的路由用例 213

演示基于端口的路由的示例 219

在 Secure Private Access 控制台中管理证书 220

管理计算机身份验证证书 220

添加证书 220

禁用证书 221

删除证书 221

设置证书的优先级 221

管理 SSL 证书 221

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

添加证书 221

搜索证书 222

修改证书 222

删除证书 222

外部通知 223

思杰安全访问™ 客户端 223

适用于 Windows 的 Citrix Secure Access 客户端 223

适用于 macOS 的 Citrix Secure Access 客户端 223

适用于 iOS 的 Citrix Secure Access 客户端 223

适用于 Android 的 Citrix Secure Access 客户端 223

适用于 Linux 的 Citrix Secure Access 客户端 224

Web 和 SaaS 应用程序配置的最佳实践 224

Secure Private Access 中已发布和未发布应用程序的应用程序访问 224

访问策略匹配和优先级 225

应用程序配置最佳实践 226

IdP 域必须拥有自己的应用程序 226

相同的相关域不得属于多个应用程序 228

深层链接 URL 230

应用程序访问最终用户体验说明 230

通过 Citrix Secure Access 客户端访问 Web 应用程序 231

通过 Citrix Secure Access 客户端访问 TCP/UDP 应用程序 231

用于安全专用访问的连接器设备 232

使用连接器设备配置安全专用访问 232

验证您的 Kerberos 配置 242

规模和大小注意事项 243

Web 和 SaaS 应用程序 243

TCP 应用程序 243

混合流量（Web、SaaS、TCP） 243

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

连接器通知 244
自适应访问策略配置和管理 245
工作原理 245
创建包含多个规则的访问策略 245
先决条件 246
搜索用户或组 251
验证用户和组同步 251
创建策略后需要记住的要点 252
基于设备的自适应访问 252
基于位置的自适应访问 253
基于设备姿态的自适应访问 254
会话策略 255
路由优先级 255
支持的 Citrix Secure Access™ 客户端 255
用例示例 255
使用会话策略在公司网络中配置直接路由 256
Citrix 企业浏览器到 Chrome 企业高级版迁移 259
配置 Chrome 企业高级版 259
没有电子邮件的用户组的策略丰富 260
用于 CEP 兼容性分析的 Secure Private Access 配置解析器 261
如何使用该工具 262
完全迁移到 CEP 之前的配置更改 266
单点登录配置更改 266
访问策略和会话策略更新 266
跨应用程序标准化操作 267
策略更新的应用程序要求 267
Web 过滤策略更新（可选） 267
其他策略调整（可选） 267

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

安全组清理（可选） 268
向组织部署 CEP（完全迁移） 268
迁移过程摘要 269
电子邮件丰富化过程中的挑战 269
最佳实践 269
结论 269
高级安全私有访问功能 270
Secure Private Access 服务的混合数据路径 271
使用混合数据路径的主要优势 271
混合数据路径的工作原理 271
支持的客户端 272
支持的 NetScaler Gateway 版本 272
连接要求 272
出站连接允许的 URL 列表 273
为 Secure Private Access 应用程序设置混合数据路径 273
连接到网关以建立连接 273
向 Citrix Cloud 注册您的 NetScaler Gateway 275
通过本地 NetScaler Gateway 启用数据流量路由 277
限制 279
Secure Private Access 注册脚本问题 279
发现网络中的应用程序、域或 IP 地址 280
新环境中的内部域应用程序发现 282
从应用程序发现页面创建应用程序 284
更新现有应用程序 284
查看所有选定的嵌入式域 285
已知限制 286
基于上下文的应用程序路由和资源位置选择 286
用例：基于上下文的路由 287

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

用例：基于用户上下文的资源位置选择 288
更改路由类型或资源位置的步骤 288
用例：将内部企业用户直接路由到后端应用程序 290
Monitor 中的上下文路由洞察 291
无缝访问本地局域网资源（打印机、文件服务器） 293
重要注意事项 293
启用本地局域网访问功能 293
策略建模工具 294
访问策略建模工具 294
分析一组用户或计算机的策略 294
分析针对特定目标的策略 295
深入查看访问策略 296
应用程序导入工具 - 预览 298
导入工作原理 299
准备 CSV 文件 299
CSV 文件中要输入的值 302
使用基于 CSV 的工具迁移应用程序的步骤 304
使用 CSV 文件时导入或创建应用程序失败 309
参考 310
客户端内部 IP 地址池 - 预览 310
客户端内部 IP 地址池的用例 310
IP 地址池限制 311
创建内部网 IP 地址池 311
删除 IP 地址池 313
查看 IP 地址利用率数据 313
保持一致的连接 314
连接器粘性 315
客户端 IP 地址粘性 - 预览 316

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

先决条件 316

为 TCP/UDP 应用程序启用客户端 IP 地址粘滞性 316

终止活动会话并将用户/计算机添加到阻止列表 317

用例 318

使用 Chrome Enterprise Premium 时阻止用户的先决条件 318

将用户/计算机添加到阻止列表 318

用户/计算机添加到阻止列表后的最终用户体验 320

通过云访问的应用程序 320

通过本地 NetScaler® Gateway 访问的应用程序（混合数据路径） 320

用户会话超时 321

Web 应用程序服务器超时 321

Citrix Secure Access 客户端超时 321

配置报告 322

生成配置报告 322

ADFS 与安全私有访问集成 323

在 ADFS 中添加声明提供程序信任 324

声明提供程序信任 ID 327

信赖方标识符 328

在 IdP 发起的流程中启用中继状态 329

在 ADFS 服务器上启用 RelayState 参数 330

Citrix Secure Private Access 上的应用程序配置 330

IdP 发起的流程 330

SP 发起的流程 331

Citrix 安全私有访问 Terraform 提供程序 332

主要优势 332

用例 333

系统要求 333

先决条件 333

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

权限 334
安装 334
Terraform 配置 334
故障排除 335
限制 335
重要注意事项 336
参考 336
可见性和监控 337
监控 337
Secure Private Access 使用情况控制面板 337
Secure Private Access 应用程序和会话监控 337
连接器设备运行状况监控 337
Secure Private Access 使用情况仪表板 338
诊断日志 338
连接器状态 340
按启动次数排名的热门应用程序 340
按应用程序启动次数排名的热门用户 341
按强制执行次数排名的热门访问策略 341
热门发现应用程序 342
从图表创建应用程序 343
搜索运算符 345
安全私有访问应用程序、会话和趋势 346
应用程序、会话和趋势 346
运行状况监控 347
连接器设备 347
会话和应用程序趋势 347
会话和应用程序趋势 348
会话监控 348

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

应用程序趋势 348

分类和故障排除 349

排查应用程序相关问题 349

DaaS Monitor 中的 Secure Private Access 会话代码 349

在 Monitor 中排查会话相关问题 349

排查设备姿态相关问题 349

排查身份验证相关问题 349

使用日志进行故障排除 350

安全私有访问日志 350

设备姿态日志 350

使用 Monitor 进行实时会话故障排除 350

诊断日志错误代码 350

应用程序启动失败，因为身份验证服务已关闭 353

应用程序启动失败，因为应用程序 FQDN 长度超出限制 353

Web 应用程序启动失败，因为无法连接到后端 Web 应用程序 354

未找到用户详细信息 354

由于在准备 SAML 令牌时未找到用户属性，Web/SaaS 应用程序启动失败 354

由于无法识别应用程序 FQDN，Web/SaaS 应用程序启动失败 354

由于 SAML 服务提供商提供了无效的 appId，Web/SaaS 应用程序启动失败 355

由于应用访问请求无效，Web/SaaS 应用启动失败 355

由于内部错误，应用在策略评估期间启动失败 355

解析策略评估响应时应用启动失败 355

应用程序启动失败，策略评估期间结果无效 356

应用程序启动失败，资源位置配置无效 356

应用程序启动失败，因为应用程序名称的长度过长 357

应用程序启动失败，原因是在与专用 TCP 服务器建立连接期间应用程序 ID 无效 357

应用程序启动在策略评估期间被拒绝 357

应用程序启动失败，因为目标 FQDN 过长 357

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

应用程序启动失败，因为目标 IP 无效 357
应用程序启动失败，因为未收到来自连接器设备的响应 357
应用程序启动失败，因为请求来自无效的 IP/主机名或端口 357
应用程序启动失败，因为目标服务器拒绝了连接 358
应用程序启动失败，因为未找到目标 358
由于目标网络不可达，应用程序启动失败 358
由于无法连接到目标，应用程序启动失败 358
连接器到 Secure Private Access 服务的连接失败 358
连接器未能读取代理详细信息 359
配置的代理不可达 359
连接器设备无法访问 FR（边缘节点） 359
由于内部连接错误，应用程序启动失败 360
Web/SaaS 应用程序启动失败 360
由于应用程序配置无效，Web/SaaS FormFill SSO 失败 360
Web/SaaS 的 Kerberos SSO 失败 360
Web/SaaS SSO 因内部服务器错误而失败 360
Web/SaaS 应用程序启动失败，因为配置的代理无法访问 361
Web/SaaS 应用程序启动失败，因为无法通过配置的代理进行身份验证 361
Citrix Secure Access™ 客户端未能执行 SSO 361
会话代码 361
应用程序枚举消息代码 362
应用程序启动消息代码 363
应用程序启动错误代码 363
Secure Private Access 日志和事件 366
诊断仪表板 366
错误列表 366
审计日志 366
系统日志 366

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

设备态势日志 366
诊断日志 367
常见问题 367
什么是 Secure Private Access 诊断日志? 367
在哪里可以找到 Secure Private Access 日志? 367
显示 Secure Private Access 诊断日志的小组件? 367
Secure Private Access 诊断日志中的详细信息? 368
如何筛选诊断日志? 369
Secure Private Access 诊断日志中捕获了哪些事件? 369
错误列表 370
诊断日志信息代码 370
解决步骤 381
如何收集客户端日志 406
常见问题 407
参考 408
审计和系统日志 409
设备姿态日志和事件 410
Identity and Access Management 控制台中的设备姿态仪表板 410
日志位置 412
安全私有访问仪表板 412
设备姿态错误日志 413
设备姿态数据导出 413
数据导出和第三方集成 414
安全信息和事件管理集成 414
使用 OData API 构建自定义报告 414
导出系统日志 414
从 Kafka 导出数据 415
安全私有访问事件 415

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

Device Posture 服务事件 415
导出审计和系统日志 415
使用 SystemLog API 导出 Secure Private Access 事件 415
使用 OData 导出会话数据 416
基于角色的访问控制 417
角色和权限 418
为管理员启用基于角色的访问 419
支持多会话虚拟桌面基础设施 421
主要功能和优势 421
启用多会话 VDI 422
适用于移动设备的 Citrix Secure Private Access 424
支持的版本和平台 424
支持的功能 424
先决条件 425
适用于使用 Citrix Secure Access 客户端的 iOS 和 Android 用户的流程 425
相关主题 426
使用 iOS Kerberos 扩展进行 Kerberos 身份验证 426
iOS 客户端配置 426
先决条件 426
验证 iOS 设备上的 MDM 注册 426
MDM 服务器配置 427
Intune 策略配置 427
IIS 配置 431
域控制器端配置 433
功能弃用 434
关于弃用无客户端 VPN 访问以进行 Web 应用访问 435
数据治理 437
数据驻留 437

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

数据收集 438
数据传输 439
数据控制 439
数据保留 439
数据导出 439
定义 440
产品认证和合规性 441
认证和审计 441
证书和审计报告 442
index 443
将网关连接器迁移到连接器设备 443
将 Gateway Connector 迁移到 Connector Appliance 的高级步骤 443
安装连接器设备 444
常见问题 444
路由表，用于解决由相同相关域引起的冲突 445
路由表的工作原理 445
主路由表 445
迷你路由表 446
向迷你路由表添加路由 446
通过 Citrix Workspace 应用程序单点登录到 Citrix Secure Access™ 客户端 448
先决条件 448
适用于 Windows 的功能要求 448
ADFS 与 安全私有访问 集成 449
在 ADFS 中添加声明提供程序信任 449
声明提供程序信任 ID 453
信赖方标识符 454
在 IdP 发起的流程中启用中继状态 455
在 ADFS 服务器上启用 RelayState 参数 456

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

Citrix Secure Private Access 上的应用程序配置 456
IdP 发起的流程 456
SP 发起的流程 458
Citrix 安全私有访问™ 458
Citrix Secure Private Access 的主要功能 458
安全私有访问 REST API 460
将 DNS 查询路由到特定于应用程序的资源位置 460
系统要求 460
功能启用 460
配置 DNS 查询路由 460
配置 G Suite 462
配置 Jira 465
Citrix Gateway SaaS 应用程序 465
配置 O365 473
先决条件 473
域联合的工作原理 475
Office 365 应用程序支持的身份验证方法 475
在 Secure Private Access 服务中配置 O365 应用程序 476
配置从 Microsoft Entra ID 到 Citrix Workspace 的域联合 477
配置从 Microsoft Entra ID 到 Citrix Workspace 的域联合的步骤 478
从 Microsoft Entra ID 到 Citrix Workspace 的自动化域联合 479
自动联合域的步骤 480
抑制多重身份验证 (MFA) 481
在 Citrix Workspace 中配置单个 Office 套件应用程序 481
集成到 Microsoft Entra ID 中的第三方应用程序 482
参考链接 486
配置 ERP Cloud 486
Citrix Gateway SaaS 应用程序 486

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

配置 ServiceNow 491
配置 Tableau 499
配置 Workday 502
Citrix Gateway SaaS 应用程序 502
配置 Zoom 504
Citrix Gateway SaaS 应用程序 504
基于访问模式的策略实施 506
工作原理 506
最终用户体验 507
支持服务器到客户端连接 - 预览 507
服务器到客户端连接的工作原理 508
创建服务器到客户端应用程序 509
先决条件 509
执行以下步骤配置服务器到客户端 TCP/UDP 应用程序 509

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

安全私有访问服务解决方案概述

传统 VPN 解决方案要求管理最终用户设备，在网络级别提供访问，并强制执行静态访问控制策略。Citrix Secure Private Access™ 为 IT 部门提供一套安全控制措施，以防范来自 BYO 设备的威胁，使用户可以选择从任何设备（无论是受管设备还是 BYO 设备）访问其 IT 批准的应用程序。

Citrix Secure Private Access 提供自适应身份验证、单点登录支持以及针对应用程序的增强安全控制。Secure Private Access 还提供通过使用设备状态服务在建立会话之前扫描最终用户设备的功能。根据自适应身份验证或设备状态结果，管理员可以为应用程序定义身份验证方法。

安全私有访问概述(/en-us/citrix-secure-private-access/media/tech-briefs_secure-private-access-use-cases_conceptual-architecture.png)

自适应安全性

自适应身份验证确定当前请求的正确身份验证流程。自适应身份验证可以识别设备状态、地理位置、网络段、用户组织/部门成员身份。根据获取的信息，管理员可以定义他们希望如何对用户进行身份验证以访问其 IT 批准的应用程序。这允许组织在所有资源（包括公共 SaaS 应用程序、私有 Web 应用程序、私有客户端-服务器应用程序和桌面即服务 (DaaS)）中实施相同的身份验证策略框架。有关详细信息，请参阅自适应安全性。

应用程序访问

Secure Private Access 可以创建与本地 Web 应用程序的连接，而无需依赖 VPN。这种无 VPN 连接使用本地部署的连接器设备。连接器设备会创建到组织 Citrix Cloud 订阅的出站控制通道。从那里，Secure Private Access 可以将连接隧道传输到内部 Web 应用程序，而无需 VPN。有关详细信息，请参阅应用程序访问。

单点登录

借助自适应身份验证，组织可以提供强大的身份验证策略，以帮助降低用户帐户泄露的风险。Secure Private Access 的单点登录功能对所有 SaaS、私有 Web 和客户端-服务器应用程序使用相同的自适应身份验证策略。有关详细信息，请参阅单点登录。

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

浏览器安全性

Secure Private Access 与 Google Chrome Enterprise Premium (CEP) 集成，其中包括数据丢失防护 (DLP)、恶意软件和网络钓鱼防护以及 URL 过滤等功能。在客户端计算机本地运行的 Google Chrome 浏览器充当安全浏览器，通过 Chrome 托管配置文件实施每个用户级别的策略。有关详细信息，请参阅与 Google Chrome Enterprise Premium 集成。

设备状态

设备状态服务允许管理员定义策略，以检查尝试远程访问公司资源的端点设备的状态。根据端点的合规性状态，设备状态服务可以拒绝访问或提供对公司应用程序和桌面的受限/完全访问。

当最终用户从其商店发起连接时，设备状态客户端会收集有关端点参数的信息，并将此信息与设备状态服务共享，以确定端点状态是否符合策略要求。

Device Posture 服务与 Citrix Secure Private Access 的集成，可从任何位置安全访问 SaaS、Web、TCP 和 UDP 应用程序，并提供 Citrix Cloud 的弹性与可扩展性。有关详细信息，请参阅 设备状态。

支持 TCP 和 UDP 应用程序

有时，远程用户需要访问其前端位于端点、后端位于数据中心的私有客户端-服务器应用程序。组织可以正当地对这些内部和私有应用程序实施严格的安全策略，这使得远程用户在不损害安全协议的情况下难以访问这些应用程序。

Secure Private Access 服务通过启用 ZTNA 来提供对这些应用程序的安全访问，从而解决了 TCP 和 UDP 安全漏洞。用户现在可以通过在其计算机上运行的 Citrix Secure Access™ 客户端，使用 Chrome 浏览器或本机客户端应用程序访问所有私有应用程序，包括 TCP、UDP 和 HTTPS 应用程序。

用户必须在其客户端设备上安装 Citrix Secure Access 客户端。

- 对于 Windows，客户端版本（22.3.1.5 及更高版本）可以从 下载 下载。
- 对于 macOS，客户端版本（22.02.3 及更高版本）可以从 App Store 下载。

有关详细信息，请参阅 支持客户端-服务器应用程序。

示例用例

- 使用零信任方法访问内部应用程序（Web/TCP/UDP），而无需在防火墙上打开入站流量
- 通过发现用户访问的应用程序，转向零信任方法

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

- 将 SaaS 应用程序的访问权限限制为公司拥有的公共 IP 地址
- 增强 Azure 管理的 SaaS 应用程序的安全性
- 增强 Office 365 的安全性
- 增强 Okta 应用程序的安全性

参考文章

- 安全私有访问简介
- 技术简报
- 参考架构
- Secure Private Access 入门和设置

参考视频

- 零信任网络访问 (ZTNA) 应用程序
- 使用 Citrix Secure Private Access 访问私有 Web 应用程序
- 使用 Citrix Secure Private Access 访问公共 SaaS 应用程序
- 使用 Citrix Secure Private Access 访问私有客户端-服务器应用程序
- 使用 Citrix Secure Private Access 进行键盘记录器保护
- 使用 Citrix Secure Private Access 进行屏幕共享保护
- 使用 Citrix Secure Private Access 的最终用户体验
- 使用 Citrix Secure Private Access 的 ZTNA 与 VPN 登录体验
- 使用 Citrix Secure Private Access 的 ZTNA 与 VPN 端口扫描

相关产品中的新增功能

- Citrix StoreFront Cloud：新增功能
- Citrix DaaS：新增功能
- 思杰安全访问：思杰安全访问

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

最新功能

30 September 2026

- **面向新客户扩展 Secure Private Access 数据区域化**

  Secure Private Access 现在将管理和数据流量路由到新客户的正确区域数据 POP 和端点。有关更多信息，请参阅数据区域化。

- **基于访问模式的策略实施**

  基于访问模式的策略实施允许管理员限制用户连接到应用程序的方式。连接可以通过基于浏览器的客户端或 Citrix Secure Access 客户端进行。有关更多信息，请参阅基于访问模式的策略实施。

03 September 2026

- **访问策略中按域、林和 IdP 类型显示的用户和组详细信息：**

  当您按显示名称、电子邮件 ID 或用户主体名称搜索用户或组时，您选择的用户和组将显示在一个网格中。每行显示身份详细信息，例如名称、电子邮件地址、IdP 类型、OID 和域。您可以清楚地区分不同域、林或身份提供商 (IdP) 中同名用户或组。有关详细信息，请参阅创建具有多条规则的访问策略。

- **使用 HAR 文件发现相关域：**

  Secure Private Access 现在允许您上传 HAR 文件以自动发现应用程序访问的域。您可以查看发现的域并选择要添加到应用程序相关域配置中的域。这通过减少手动识别和配置相关域的需要来简化应用程序的入职。有关更多信息，请参阅使用 HAR 文件发现相关域。

- **将 Chrome Enterprise Premium (CEP) 配置应用于 Google Directory 组织单位：**

  除了所有用户和 Google Directory 用户组之外，您现在还可以将 CEP 配置应用于选定的 Google Directory 组织单位。有关更多信息，请参阅为 Google Directory 组织单位配置 CEP。

- **条件身份验证支持：**

  使用 Citrix Cloud 作为 OpenID Connect (OIDC) 身份验证提供程序的 Chrome Enterprise Premium (CEP) 单点登录 (SSO) 现在支持条件身份验证。有关更多信息，请参阅使用 Citrix 身份和访问管理进行 Open ID Connect。

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

- **设置用户属性类型：**

  您现在可以从 Secure Private Access 管理控制台的“托管配置文件身份”页面设置用户属性。有关详细信息，请参阅托管配置文件身份。

- **验证用户和组同步：**

  在选择用户或组时，管理员可以验证所选用户目录中的条目是否已与 Google Directory 同步并正确配置。只有当用户和组同步时，Secure Private Access 策略才能正确评估。有关详细信息，请参阅验证用户和组同步。

- **删除应用程序时自动清理路由条目：**

  现在，当您删除应用程序时，Secure Private Access 也会清理路由条目。有关详细信息，请参阅删除应用程序时自动清理路由条目。

19 August 2026

- **Google Cloud 身份支持 Chrome 企业高级版 (CEP)**

  Google Cloud Identity 现在可以作为 CEP 的身份提供程序使用。当 Google Cloud Identity 是您的身份提供程序时，用户和组原生驻留在 Google Cloud 目录中，因此不需要目录关联。有关详细信息，请参阅集成解决方案的先决条件。

05 August 2026

- **访问 SaaS 应用程序的新路由方法：**

  您现在可以将 SaaS 应用程序的路由类型设置为“**通过 Google Secure Gateway 外部**”以通过 Google Secure Gateway 路由流量，或设置为“**外部**”以将流量直接从客户端路由到应用程序。有关详细信息，请参阅配置 SaaS 应用程序。

31 July 2026

- **适用于 Chrome Enterprise 的 Citrix Secure Access 控件：**

  Citrix Secure Private Access 支持由适用于 Google Chrome Enterprise Premium (CEP) 的 Citrix Secure Access 扩展程序交付和强制执行的安全策略。

  Secure Private Access 支持以下策略。

  - 防键盘记录
  - 剪贴板容器

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

- Web 应用程序的域后缀
- 会话录制
- 浏览器会话重新身份验证

24 June 2026

- **支持配置出口中心区域：**

  Secure Private Access 使管理员能够选择 Chrome Enterprise Premium 用于 SaaS 应用程序流量的出口区域。每个选定的区域都提供一组专用的出口 IP 地址，管理员可以将其添加到 SaaS 应用程序允许列表中，以允许通过 Google Secure Gateway 路由的流量。此功能适用于云部署和混合部署。有关详细信息，请参阅配置出口中心区域。

- **移除对 Google Directory 的 citrix-schema 同步的依赖：**

  Chrome Enterprise Premium 中对 Google Directory 的 Citrix 架构同步的依赖已移除。现在可以使用用户电子邮件 ID 执行 Google Directory 同步。要启用此功能，请联系 Citrix 支持。

- **OIDC 的 SAML 2.0 身份验证支持：**

  OIDC 现在支持 SAML 2.0 身份提供商 (IdP)。有关 OIDC 与 Citrix Identity 集成的更多信息，请参阅使用 Citrix Identity 的 OpenID Connect。

18 June 2026

- **在基于 CSV 的应用程序导入期间定义主要和次要资源位置：**

通过 CSV 文件导入应用程序现在允许管理员在批量创建应用程序时定义主要和次要资源位置。这使得在不同位置运行的企业部署能够高效地进行入职。有关详细信息，请参阅 应用程序导入工具。

09 June 2026

以下部分提供了有关 09 June 2026 发布的更多信息。

重要通知

- **Citrix Secure Private Access™ 边缘配置更新：**

  作为 Citrix Secure Private Access 持续性能和基础设施优化的一部分，某些 Citrix Secure Private Access Edge 配置更新将很快部署。

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

注意：

此通知**仅**适用于可能在防火墙或代理级别设置了特定 PoP 级别 FQDN 允许列表或在文档建议之外设置了自定义条目的客户。

正在发生的变化：

Citrix Secure Private Access Edge FQDN 正在更新为新格式，如下所示：

旧 FQDN: `<pop>-rdvz.g.nssvc.net`

新 FQDN: `<pop>-spa-rdvz.g.nssvc.net`

示例：

`az-us-e-rdvz.g.nssvc.net` 更改为 `az-us-e-spa-rdvz.g.nssvc.net`

`az-eu-w-rdvz.g.nssvc.net` 更改为 `az-eu-w-spa-rdvz.g.nssvc.net`

我需要采取行动吗：

- **无需采取行动：** 如果您使用推荐的通配符域（例如 `*.nssvc.net`），则新旧名称均已涵盖，无需采取任何行动。有关详细信息，请参阅 适用于 Secure Private Access 的连接器设备。
- **需要采取行动：** 如果您使用显式、PoP 级别的 FQDN 允许列表或文档建议之外的自定义条目，请执行所需操作。

所需操作：

允许出站流量到特定 PoP 的客户必须更新其防火墙规则。对于每个当前允许的 `<pop>-rdvz.g.nssvc.<suffix>` 条目，添加相应的 `<pop>-spa-rdvz.g.nssvc.<suffix>` 记录以确保服务不中断。有关 PoP 列表，请参阅 Citrix Secure Private Access 服务的接入点 (PoP) 位置。

20 May 2026

- **数据区域化**

  Citrix Secure Private Access 中的数据区域化使客户能够通过选择首选地理区域来控制其数据存储位置。客户可以选择其数据存储区域，选项包括全球、欧洲 (EU)、亚太地区 (APAC) 和北美 (NA)。所有静态配置数据都保留在所选区域内，确保其不会离开指定地理区域。有关详细信息，请参阅 数据区域化。

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

28 April 2026

- **简化的 Secure Private Access 服务配置**

  Secure Private Access 服务配置已简化为单一统一流程。系统配置页面现在包含一个拓扑图，显示了 Secure Private Access 云部署中使用的组件。管理员可以直接从此页面配置连接器设备和 Google Chrome Enterprise Premium。有关详细信息，请参阅 Secure Private Access 入门和设置。

- **用于遥测目的的强制性 Google 管理员权限**

  必须在 Google 管理控制台中为服务帐户分配一组新的权限。这些权限主要用于遥测目的（例如，DLP 活动事件和安全警报）。有关详细信息，请参阅 设置 Google Chrome 集成。

- **Okta IdP 对 CEP 的支持**

  Okta 现在可以作为身份提供程序与 Chrome Enterprise Premium (CEP) 配合使用。有关详细信息，请参阅创建 Citrix OIDC 客户端。有关详细信息，请参阅 创建 Citrix OIDC 客户端。

07 April 2026

- **列出五个最常用的模板，以简化和加速应用程序载入**

  应用程序配置页面中的“**选择模板**”部分现在列出了五个最常用的模板，以简化和加速应用程序载入。有关详细信息，请参阅配置 SaaS 应用程序。

04 March 2026

- **Secure Private Access 管理员 UI 域过渡到 secureaccess.cloud.com**

  Secure Private Access 管理员 UI 域现已更新为 `secureaccess.cloud.com`。您当前的 URL 将继续运行并自动重定向到新域。无需执行任何操作或更改配置。

12 February 2026

- **使用路由例外进行基于端口的路由**

  基于端口的路由功能允许管理员使用路由例外，针对 TCP/UDP 应用程序以不同方式路由同一目标的流量，即使是不同端口的流量。有关详细信息，请参阅使用路由例外进行基于端口的路由。

05 February 2026

- **Citrix 企业浏览器 到 Chrome 企业高级版 的迁移**

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

Citrix Enterprise Browser 到 Chrome Enterprise Premium 的分阶段迁移方法允许组织在过渡期间通过并行运行两种浏览器解决方案来保持业务连续性。通过分阶段迁移，客户可以验证现有应用程序和工作流与 Chrome Enterprise Premium 的兼容性。有关详细信息，请参阅Citrix Enterprise Browser 到 Chrome Enterprise Premium 迁移。

- **没有电子邮件地址的用户组的域映射**

  Google 目录要求所有用户和组对象都具有经过验证的电子邮件地址。但是，对于 Secure Private Access 支持的目录（特别是 Active Directory (AD) 和 Microsoft Entra ID），这并非总是可用。AD 和 Microsoft Entra ID 对象可能缺少电子邮件地址，或者其电子邮件地址指向 Google 目录无法验证的内部或特殊域（例如，@fabrikam.onmicrosoft.com）。

  由于电子邮件地址通常是 Secure Private Access 和 Google 目录之间的通用标识符，因此来自 AD/Entra 且没有经过验证的 Google 电子邮件地址的组通常不受 Secure Private Access 策略的支持。域映射功能通过允许管理员针对组配置策略来解决此问题，即使这些组缺少电子邮件地址或其电子邮件地址具有未经验证的域。有关详细信息，请参阅没有电子邮件地址的用户组的域映射。

18 December 2025

- **在浏览器中安全访问 SSH 和 RDP 应用程序**

  Citrix Secure Private Access 已与 Chrome Enterprise Premium 集成，可在浏览器中直接启用安全的 SSH 和 RDP 会话。有关详细信息，请参阅以下主题：

  - 在浏览器中安全访问 SSH 应用程序
  - 在浏览器中安全访问 RDP 应用程序

16 December 2025

- **将 DNS 查询路由到特定于应用程序的资源位置**

  管理员可以将特定应用程序的 DNS 查询直接路由到其专用资源位置。这可以实现更准确的 DNS 解析、智能流量管理和更好的用户体验。有关详细信息，请参阅将 DNS 查询路由到特定于应用程序的资源位置。

11 December 2025

- **思杰企业浏览器迁移到 Chrome 企业高级版**

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

现有的 Secure Private Access 服务客户可以逐步从 Citrix Enterprise Browser 迁移到 Chrome Enterprise Premium (CEP)。这种分阶段的迁移方法允许组织在过渡期间通过并行运行两种浏览器解决方案来保持业务连续性。通过分阶段迁移，客户可以验证现有应用程序和工作流与 Chrome Enterprise Premium 的兼容性。有关更多信息，请参阅Citrix Enterprise Browser 到 Chrome Enterprise Premium 的迁移。

30 October 2025

- **Citrix Secure Private Access 与 Chrome Enterprise 解决方案的无代理访问版本正式发布**

  通过将 Citrix Secure Private Access™ 与 Google Chrome Enterprise Premium 集成，最终用户现在可以使用 Google Chrome 浏览器作为其企业浏览器，安全地访问私有 Web 和 SaaS 应用程序，而无需零信任网络访问 (ZTNA) 代理，并实现具有数据丢失防护 (DLP) 控制、Web 过滤和 ZTNA 策略强制执行的按应用程序访问。有关详细信息，请参阅Citrix Secure Private Access 与 Google Chrome Enterprise Premium 的集成。

  针对拥有生产租户的现有 Secure Private Access / Citrix Enterprise Browser 客户的建议

  我们建议当前生产客户在单独的租户中测试无代理访问版本，而不是在他们的生产租户中测试。计划于 2025 年 11 月下旬发布的产品更新将包含增强功能，允许现有 Secure Private Access 客户启用无代理访问功能，同时保留其现有的应用程序配置和访问策略。2025 年 11 月的版本还将提供一个用户界面，允许现有 Secure Private Access 客户将其当前 Web 和 SaaS 应用程序（目前通过 Citrix Enterprise Browser 启动）的应用程序启动迁移到 Chrome 浏览器中启动。

  希望在 2025 年 11 月更新之前使用此版本的客户必须将其现有的 Secure Private Access 租户重置为全新状态，然后再次将客户载入 Secure Private Access 服务。执行以下步骤：

  a. 删除 Secure Private Access 控制台中的所有访问策略、应用程序和相关域。
  b. 返回 Citrix Cloud 控制台上的 Secure Private Access 磁贴。
  c. 选择 **完全云交付服务架构**，然后单击**继续**。有关详细信息，请参阅 Secure Private Access 入门和设置。

17 September 2025

- **Secure Private Access 对 iOS 设备的支持**

  Secure Private Access 现在支持移动设备，从适用于 iOS 的 Secure Access Client 25.08.1 版开始。移动用户可以从其 iOS 设备访问企业应用程序。有关详细信息，请参阅 适用于移动设备的 Citrix Secure Private Access。

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

13 August 2025

- **通过 Citrix Enterprise Browser™ 访问应用程序的自定义应用商店 URL**

  自定义应用商店 URL 功能允许组织通过品牌化的、组织拥有的域（例如 workspace.company.com）为用户提供对 SaaS 和私有 Web 应用程序的访问，而不是默认的 *.cloud.com 域。

- **策略建模工具的增强功能**

  策略建模工具现在显示影响应用程序路由决策的路由类型和特定策略类型。此增强功能有助于管理员排查路由问题并验证应用程序是否符合配置的策略。有关详细信息，请参阅 策略建模工具 。

14 July 2025

- **在 Monitor 中监视和排查 Secure Private Access 无代理应用程序**

  管理员和技术支持人员现在可以在 Monitor 中监控和排查 Secure Private Access 无代理应用程序会话和事件。有关详细信息，请参阅 Secure Private Access 与 Monitor 集成。

- **支持 UDP 应用程序的服务器到客户端连接**

  除了 TCP 应用程序之外，现在还支持 UDP 应用程序的服务器到客户端连接。客户资源位置中的服务器可以与远程客户端建立 UDP 连接。有关详细信息，请参阅 支持服务器到客户端连接。

- **面向技术支持人员的新基于角色的访问控制角色**

  除了完全访问管理员和只读管理员角色之外，Secure Private Access 管理员还可使用以下角色。

  - 完全监控管理员
  - 技术支持管理员

  有关详细信息，请参阅 基于角色的访问控制。

- **将 UDP DNS 查询路由到特定于应用程序的资源位置**

  现在，特定主机名的 UDP DNS 查询可以直接路由到托管相应应用程序的资源位置。这种路由通过确保 DNS 查询到达最相关的资源位置来提高应用程序性能。以前，所有 UDP DNS 查询默认情况下都会路由到地理位置最近的资源位置，而不管应用程序的实际位置。

  工作原理：

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

a. 默认情况下，将 UDP DNS 查询路由到特定于应用程序的资源位置的功能处于禁用状态。要启用此功能，请联系 Citrix 支持。

b. 启用此功能后，DNS 查询将路由到 Secure Private Access 以识别与应用程序关联的特定资源位置。根据 Secure Private Access 的响应，DNS 查询随后会路由到应用程序的专用资源位置。

c. 如果未识别出特定于应用程序的资源位置，则查询将回退到最近的可用资源位置。

03 June 2025

- **在 Secure Private Access 控制台中管理证书**

  Secure Private Access 证书存储现在为管理员提供了一个集中位置，可以高效地管理证书颁发机构 (CA) 和安全套接字层 (SSL) 证书。此专用存储通过允许管理员无缝添加新证书、修改现有证书以及删除不再需要的证书来简化证书管理。有关详细信息，请参阅 在 Secure Private Access 控制台中管理证书。

15 May 2025

- **Citrix 安全私有访问™ 与 Google Chrome 企业高级版 的集成**

  Citrix Secure Private Access 与 Google Chrome Enterprise Premium 的集成使客户能够将 Google Chrome Enterprise Premium 用作企业浏览器解决方案，以安全访问私有 Web 应用程序和 SaaS 应用程序，并结合 Citrix Secure Private Access 提供的安全连接。有关详细信息，请参阅 Citrix Secure Private Access 与 Google Chrome Enterprise Premium 的集成。

24 April 2025

- **混合数据路径支持**

  Secure Private Access 服务的混合数据路径利用本地和云基础设施来提供对应用程序的安全访问。组织可以使用混合数据路径通过本地 NetScaler Gateway 路由所有数据流量。有关详细信息，请参阅 Secure Private Access 服务的混合数据路径。

- **在 Monitor 中显示上下文路由见解**

  上下文路由可能导致应用程序路由的动态变化。例如，当用户在公司网络外部时，应用程序可能会通过 Secure Private Access 服务路由，但当用户在内部时，则直接路由到应用程序。为管理员提供这些路由决策的可见性对于故障排除路由问题至关重要。有关详细信息，请参阅 Monitor 中的上下文路由见解。

- **配置备份资源位置**

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

管理员可以通过配置辅助资源位置或使用“首个可用”选项来确保应用程序即使在中断期间也具有高可用性。有关详细信息，请参阅以下主题：

- 支持企业 Web 应用程序
- 无代理访问企业 Web 应用程序
- 支持软件即服务应用程序
- 支持客户端-服务器应用程序

- **立即或随时间推移删除 IP 地址池**

  新增了通过以下选项立即或随时间推移删除 IP 地址池的支持。

  - **强制删除 IP 池：** 停止向新用户分配 IP 地址并立即释放未使用的 IP 地址。使用已删除 IP 地址的活动用户会话可能会被终止，导致突然关闭和强制注销。只有在创建了不同的 IP 地址池后，会话终止的用户才会获得新的 IP 地址。
  - **随时间推移删除 IP 池：** 停止向新用户分配 IP 地址并立即释放未使用的 IP 地址。系统会等待活动会话注销或过期，然后才完全删除该池。只有在创建了不同的 IP 地址池后，会话终止的用户才会获得新的 IP 地址。

  有关详细信息，请参阅删除 IP 地址池。

22 April 2025

- **使用 nsconfig 文件导入应用程序**

  Secure Private Access 管理控制台包含一个文件导入工具，允许管理员除了使用 CSV 文件外，还可以使用 nsconfig 文件将多个应用程序批量导入系统。此工具对于从传统 VPN 转向 Secure Private Access 等更高级解决方案的组织特别有用。有关详细信息，请参阅应用程序导入工具。

  使用 nsconfig 文件导入应用程序功能正在预览中。

20 February 2025

- **管理员审计日志功能的增强**

  管理员审计日志功能已增强，可捕获 Secure Private Access 服务中所有管理员操作的详细日志。有关详细信息，请参阅审计日志。

- **根据 UPN 和电子邮件地址搜索并添加用户**

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

您现在除了可以通过显示名称外，还可以根据 UPN 和电子邮件地址在 Secure Private Access 中搜索并添加用户。此搜索选项允许管理员准确识别正确的用户并授予其访问权限，即使他们有多个帐户。有关详细信息，请参阅配置访问策略。

08 January 2025

- **使用会话策略动态路由整个会话**

  管理员可以配置会话策略，将内部企业用户直接路由到后端应用程序，而无需通过 Secure Private Access 隧道传输流量。会话策略根据网络位置和设备姿态等因素提供动态路由。有关详细信息，请参阅将内部企业用户直接路由到后端应用程序。

07 January 2025

- **连接器粘性支持**

  Secure Private Access 支持连接器粘性。连接器粘性可确保客户端与连接器设备建立连接后，来自同一客户端的所有后续请求都定向到同一源（连接器设备）。有关详细信息，请参阅连接器粘性。

- **客户端 IP 地址粘性支持**

  Secure Private Access 支持客户端 IP 地址粘性。客户端 IP 地址粘性可确保来自特定客户端 IP 地址的请求始终路由到同一后端服务器。有关详细信息，请参阅客户端 IP 地址粘性。

  客户端 IP 地址粘性功能正在预览中。

- **支持创建客户端内部 IP 地址池**

  已添加对创建客户端内部 IP 地址池的支持。这些 IP 地址池对于为用户和关联设备分配唯一的 IP 地址以支持以下用例至关重要：

  - 服务器到客户端连接
  - 客户端 IP 地址粘性支持

  有关详细信息，请参阅客户端内部 IP 地址池。

  注意：

  客户端内部 IP 地址池功能处于预览阶段。要启用此功能，请联系 Citrix 支持。

- **支持服务器到客户端连接**

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

Secure Private Access 支持服务器到客户端连接，其中客户资源位置中的服务器可以与远程客户端建立 TCP 连接。为了启用服务器到客户端连接，Secure Private Access 引入了服务器到客户端应用程序。此应用程序可以配置客户端详细信息（端口、协议）和后端服务器的 IP CIDR 范围。有关详细信息，请参阅支持服务器到客户端连接。

服务器到客户端应用程序支持处于预览阶段。

02 January 2025

- **基于 CSV 的应用程序导入工具**

  Secure Private Access 管理控制台包含一个基于 CSV 的导入工具，允许管理员使用 CSV 文件将多个应用程序批量导入系统。此工具对于从传统 VPN 转向 Secure Private Access 等更高级解决方案的组织特别有用。有关详细信息，请参阅基于 CSV 的应用程序导入工具。

03 December 2024

- **Secure Private Access 支持云托管多会话 VDI**

  适用于 Windows 的 Citrix Secure Access 客户端现在支持使用 Secure Private Access 从云托管多会话 VDI 实现对公司资源的零信任访问。有关详细信息，请参阅支持多会话虚拟桌面基础结构。

25 November 2024

- **DaaS Monitor 中的 Secure Private Access 会话代码**

  Secure Private Access 会话相关代码现在显示在 DaaS Monitor 中。有关代码列表，请参阅 Monitor 中的 Secure Private Access 会话相关代码。

14 November 2024

- **策略建模工具的增强功能**

  管理员现在可以查看与每个应用程序关联的策略的完整列表，并利用向下钻取功能来了解具体的策略应用逻辑、为什么应用了特定策略以及为什么未应用其他策略。有关详细信息，请参阅向下钻取访问策略。

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

08 November 2024

- **安全私有访问与监控集成**

  Secure Private Access 已与 Monitor 集成，Monitor 是 Citrix DaaS 的监控和故障排除控制台。管理员和技术支持人员可以从 DaaS Monitor 监控和排查 Web/SaaS 和 TCP/UDP 应用程序会话和事件。有关详细信息，请参阅与 DaaS Monitor 集成。

07 November 2024

- **Secure Private Access 图形用户界面的增强功能**

  Secure Private Access 服务现在提供改进的图形用户界面 (GUI)，以提供更好的用户体验。主菜单树结构已替换为悬停显示功能，以便于导航。次级菜单项在悬停时出现，显示子菜单以实现更快的选择。

  此外，您可以通过单击图标来折叠或展开整个菜单。

23 September 2024

- **支持基于上下文的应用程序路由和资源位置选择**

  访问策略中的动态域路由配置现在允许管理员根据用户上下文编辑每个 URL 的内部路由类型。管理员可以修改资源位置，以便将用户请求路由到最佳数据中心，从而确保高效处理用户请求并优化性能。有关详细信息，请参阅基于上下文的应用程序路由和资源位置选择。

15 August 2024

- **配置清除被阻止用户列表中条目的时间持续时间的选项**

  管理员现在可以设置一个特定持续时间（1 到 99 天）来清除被阻止用户列表中的条目。有关详细信息，请参阅终止活动用户会话并将用户添加到用户阻止列表。

- **附加安全控制**

  以下附加安全控制现已可用，用于限制应用程序访问。

  - 麦克风
  - 网络摄像头
  - 通知
  - 弹出窗口

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

- 不安全内容

- **未经授权的网站（Web 过滤）功能增强**

  未经授权的网站（Web 过滤）功能允许管理员默认阻止所有未经授权的流量访问，或通过 Citrix Enterprise Browser 默认允许访问。

16 July 2024

- **附加安全控制**

  以下附加安全控制可用于限制应用程序访问。

  - 按文件类型限制下载
  - 按文件类型限制上传
  - 个人数据遮蔽
  - 打印机管理
  - 安全组的剪贴板限制

- **在应用程序发现页面中显示嵌入式域**

  应用程序发现功能允许管理员创建新应用程序，或者在主域、嵌入式域 (HTTP/HTTPS) 或目标 IP 地址 (TCP/UDP) 未与应用程序关联时，将这些域添加到现有应用程序。**应用程序发现**页面以树状结构显示主域及其底层嵌入式域。有关详细信息，请参阅发现最终用户访问的域或 IP 地址。

11 June 2024

- **策略建模工具**

  策略建模工具（**访问策略 > 策略建模**）可帮助管理员在管理控制台中分析和排查配置问题。有关详细信息，请参阅策略建模工具。

- **支持诊断日志图表中的筛选器**

  诊断日志图表中的筛选器选项可帮助管理员根据应用程序类型、类别和描述等各种条件优化搜索，以便更轻松地进行日志分析和故障排除。有关详细信息，请参阅诊断日志。

13 March 2024

- **支持终止活动用户会话并将用户添加到禁用用户列表**

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

管理员现在可以立即终止所有活动的最终用户会话，并将用户添加到禁用用户列表。将用户添加到此禁用用户列表会终止所有活动的 Secure Private Access 应用程序会话，并阻止将来的应用程序访问。有关详细信息，请参阅终止活动用户会话并将用户添加到禁用用户列表。

12 February 2024

- **浏览器和防病毒扫描的普遍可用性**

  Device Posture 服务支持的浏览器和防病毒扫描现已普遍可用。有关详细信息，请参阅设备状态支持的扫描。

23 January 2024

- **设备姿态服务设备证书检查的普遍可用性**

  设备姿态服务的设备证书检查现已普遍可用。有关详细信息，请参阅设备姿态服务的设备证书检查。

20 December 2023

- **本地安全专用访问的普遍可用性**

  Citrix 本地安全专用访问现已普遍可用。有关详细信息，请参阅新增功能。

16 October 2023

- **本地安全专用访问解决方案预览功能**

  本地安全专用访问解决方案现在提供以下功能：

  - 首次设置的管理员 UI。
  - 用于配置应用程序和访问策略的管理员 UI。
  - 日志仪表板。

  有关详细信息，请参阅本地安全专用访问。

- **设备姿态服务预览功能**

  设备姿态服务现在支持以下检查：

  - 设备姿态服务现在支持 IGEL 平台。
  - 设备姿态服务现在支持地理位置和网络位置检查。

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

有关详细信息，请参阅 设备姿态。

11 September 2023

- **设备姿态与 Microsoft Intune 集成正式发布**

  设备姿态与 Microsoft Intune 集成现已正式发布。有关详细信息，请参阅 Microsoft Intune 与设备姿态集成。

30 August 2023

- **管理用于设备姿态服务的 Citrix Endpoint Analysis 客户端**

  EPA 客户端可与 NetScaler 和设备姿态一起使用。与 NetScaler 和设备姿态一起使用时，需要进行一些配置更改才能管理 EPA 客户端。有关详细信息，请参阅 管理用于设备姿态服务的 Citrix Endpoint Analysis 客户端。

28 August 2023

- **iOS 平台上支持设备姿态服务**

  设备姿态服务现在支持 iOS 平台。有关详细信息，请参阅 设备姿态。

  此功能处于预览阶段。

22 August 2023

- **使用 Citrix 设备姿态服务进行设备证书检查**

  Citrix Device Posture 服务现在可以通过将终端设备的证书与企业证书颁发机构进行核对，以确定终端设备是否可信，从而为 Citrix DaaS 和 Secure Private Access 资源启用上下文访问（智能访问）。有关详细信息，请参阅 使用 Device Posture 服务进行设备证书检查。

  此功能处于预览阶段。

17 August 2023

- **Citrix DaaS™ Monitor 上的设备姿态事件**

  Device Posture 服务事件和监控日志现在可在 DaaS Monitor 上搜索。有关详细信息，请参阅 Citrix DaaS Monitor 上的设备状态事件。

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

07 June 2023

- **用于配置本地 Secure Private Access 的工具**

  现在提供了一个简化的用户界面，用于配置本地 Secure Private Access 解决方案。该配置工具可以在 Citrix Virtual Apps and Desktops™ 交付控制器上运行，以快速创建 SaaS 或 Web 应用程序。此外，您可以使用此工具设置应用程序限制、流量路由和 NetScaler Gateway 设置。

29 May 2023

- **具有多条规则的访问策略创建功能正式发布**

  您可以在单个策略中创建多个访问规则，并为不同的用户或用户组配置不同的访问条件。这些规则可以分别应用于 HTTP/HTTPS 和 TCP/UDP 应用程序，所有这些都在一个策略中。有关详细信息，请参阅 配置具有多条规则的访问策略。

10 April 2023

- **应用程序发现**

  应用程序发现功能可帮助管理员了解其组织中的内部私有应用程序（例如 Web 应用程序和客户端服务器应用程序（基于 TCP 和 UDP 的应用程序））以及访问这些应用程序的用户。管理员可以通过指定域（通配符域）或 IP 子网的范围来发现应用程序。有关详细信息，请参阅 应用程序发现。

29 March 2023

- **适用于本地部署的 Secure Private Access 解决方案**

  作为 Citrix StoreFront 和 NetScaler Gateway 客户，您现在可以使用适用于本地部署的 Citrix Secure Private Access 解决方案，与 Citrix Virtual Apps 和虚拟桌面一起无缝访问 Web 和 SaaS 应用程序。有关详细信息，请参阅适用于本地部署的 Secure Private Access。

07 March 2023

- **配置 DNS 后缀**

  Citrix Secure Private Access 服务的 DNS 后缀功能可用于以下用例：

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

- 通过为后端服务器添加 DNS 后缀域，使 Citrix Secure Access™ 客户端能够将非完全限定域名（主机名）解析为完全限定域名 (FQDN)。
- 使管理员能够使用 IP 地址（IP CIDR/IP 范围）配置应用程序，以便最终用户可以使用 DNS 后缀域下的相应 FQDN 访问应用程序。

有关详细信息，请参阅 用于将 FQDN 解析为 IP 地址的 DNS 后缀。

23 January 2023

- **设备状态检查服务**

  Citrix 设备状态检查服务是一种基于云的解决方案，可帮助管理员强制执行最终设备必须满足的某些要求，才能访问 Citrix DaaS（虚拟应用程序和桌面）或 Citrix Secure Private Access 资源（SaaS、Web 应用程序、TCP 和 UDP 应用程序）。有关详细信息，请参阅 设备状态检查。

- **Microsoft Endpoint Manager 与设备姿态集成**

  除了设备姿态服务提供的本机扫描外，设备姿态服务还可以与其他第三方解决方案集成。设备姿态已与 Windows 和 macOS 上的 Microsoft Endpoint Manager (MEM) 集成。有关详细信息，请参阅 Microsoft Endpoint Manager 与设备姿态集成。

22 December 2022

- **通过 Citrix Workspace™ 应用程序登录的用户对 Workspace URL 的单点登录支持**

  Citrix Secure Access 客户端现在支持在通过 Citrix Workspace 应用程序登录后对 Workspace URL 进行单点登录。此 SSO 功能通过避免多次身份验证来增强用户体验。有关详细信息，请参阅 Workspace URL 的单点登录支持。

- **使用访问策略启用对应用程序的访问**

  为了授予用户对应用程序的访问权限，管理员现在需要创建访问策略，并附带匹配的用户订阅列表，以便最终用户可以使用这些应用程序。以前，管理员必须将用户添加为订阅者才能启用访问。有关详细信息，请参阅 创建访问策略。

03 October 2022

- **授予对应用程序访问权限的访问策略**

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

“应用程序订阅者”配置选项已从配置向导的“应用程序”部分中删除。为了授予用户对应用程序的访问权限，管理员需要创建访问策略。在访问策略中，管理员添加应用程序订阅者并配置安全控制。有关详细信息，请参阅 创建访问策略。

- **支持 UDP 应用程序**

  Secure Private Access 服务现在支持访问 UDP 应用程序。有关详细信息，请参阅预览功能。

09 September 2022

- **基于用户风险评分的自适应访问**

  管理员现在可以使用 Citrix Analytics for Security (CAS) 提供的用户风险评分配置自适应访问策略。有关详细信息，请参阅基于用户风险评分的自适应访问。

- **基于用户网络位置的自适应访问**

  管理员现在可以根据用户访问应用程序的位置配置自适应访问策略。该位置可以是用户访问应用程序的国家/地区，也可以是用户的网络位置。有关详细信息，请参阅基于位置的自适应访问。

- **增强型自适应访问策略构建器**

  现在，只有在满足配置条件后才能访问应用程序。仅应用程序订阅并不能为您的客户提供对应用程序的访问权限。管理员必须添加访问策略才能在应用程序订阅之外提供对应用程序的访问权限。此外，用户或组是访问策略中的强制条件，必须满足此条件才能访问应用程序。有关详细信息，请参阅创建访问策略。

- **限制文件上传到 SaaS/Web 应用程序**

  此功能允许客户管理员控制（允许或限制）谁可以将文件上传到其关键业务应用程序。这样，只有授权用户才能将文件上传到应用程序。有关详细信息，请参阅创建访问策略。

- **增强型仪表板**

  Secure Private Access 仪表板现在提供对多个用户指标的详细可见性，例如应用程序使用情况、热门应用程序用户、热门访问应用程序、诊断日志等。有关详细信息，请参阅仪表板。

- **库弃用**

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

Secure Private Access 应用程序现在在 Citrix Cloud™ 库中不可见。所有 Secure Private Access 配置的应用程序都位于 Secure Private Access 服务磁贴中的应用程序部分。这有助于管理员轻松导航、编辑和配置应用程序。

- **Secure Private Access 的审核日志**

  Citrix Secure Private Access 服务相关事件现在已捕获到 **Citrix Cloud > 系统日志**中。有关详细信息，请参阅审核日志。

- **企业 Web 和 SaaS 应用程序访问的诊断日志**

  Citrix Secure Private Access 事件现已与 Citrix Analytics 集成。Citrix Analytics 提供了一个公共端点，使管理员能够访问和下载事件。可以通过 PowerShell 脚本访问这些事件。有关详细信息，请参阅企业 Web 和 SaaS 应用程序访问的诊断日志。

- **故障排除指南**

  管理员可以使用故障排除指南来解决与配置相关的问题。有关详细信息，请参阅排查应用程序相关问题。

01 June 2022

- **自适应身份验证服务**

  自适应身份验证现已正式发布 (GA)。有关自适应身份验证的详细信息，请参阅自适应身份验证服务。

04 April 2022

- **品牌重塑更改**

  Citrix 安全工作区访问服务现已更名为 Citrix 安全私有访问服务。

- **管理员引导式工作流，以便于入门和设置**

  Secure Private Access 现在具有全新的精简管理员体验，通过分步流程配置零信任网络访问到 SaaS 应用程序、内部 Web 应用程序和 TCP 应用程序。它包括配置自适应身份验证、应用程序（包括用户订阅）、自适应访问策略以及单个管理员控制台中的其他内容。有关详细信息，请参阅管理员引导式工作流，以便于入门和设置。

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

此功能现已正式发布 (GA)。

- **安全私有访问控制板**

  Secure Private Access 控制板为管理员提供了对其热门应用程序、热门用户、连接器运行状况、带宽使用情况的全面可见性，并可在单个位置进行使用。此数据从 Citrix Analytics 获取。有关详细信息，请参阅Secure Private Access 控制板。

  此功能现已正式发布 (GA)。

- **直接访问企业 Web 应用程序**

  客户现在可以直接从 Chrome、Firefox、Safari 和 Microsoft Edge 等本机 Web 浏览器，为内部 Web 应用程序启用零信任网络访问 (ZTNA)。有关详细信息，请参阅直接访问企业 Web 应用程序。

  此功能现已正式发布 (GA)。

- **基于 ZTNA 代理的 TCP/HTTPS 应用程序访问**

  Citrix 客户现在除了内部 Web 应用程序之外，还可以为所有客户端-服务器应用程序和基于 IP/端口的资源启用零信任网络访问 (ZTNA)。有关详细信息，请参阅支持客户端-服务器应用程序。

  此功能现已正式发布 (GA)。

- **企业 Web、TCP 和 SaaS 应用程序的自适应访问和安全控制**

  Citrix Secure Private Access 服务自适应访问功能提供了一种全面的零信任网络访问 (ZTNA) 方法，可为应用程序提供安全访问。自适应访问使管理员能够根据上下文为用户可以访问的应用程序提供精细级别的访问。“上下文”一词在此处指：

  - 用户和组（用户和用户组）
  - 设备（桌面或移动设备）
  - 位置（地理位置或网络位置）
  - 设备状态（设备状态检查）
  - 风险 (用户风险评分)

  有关详细信息，请参阅 企业 Web、TCP 和 SaaS 应用程序的自适应访问和安全控制。

  此功能现已正式发布 (GA)。

- **Secure Private Access 的审计日志**

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

Citrix Secure Private Access 服务相关事件现已捕获到 **Citrix Cloud > 系统日志**中。有关详细信息，请参阅 审计日志。

此功能现已正式发布 (GA)。

- **企业 Web 和 SaaS 应用程序访问的诊断日志**

  Citrix Secure Private Access 事件现已与 Citrix Analytics 集成。Citrix Analytics 提供了一个公共端点，使管理员能够访问和下载这些事件。这些事件可以通过 PowerShell 脚本访问。有关详细信息，请参阅 企业 Web 和 SaaS 应用程序访问的诊断日志。

  此功能现已正式发布 (GA)。

- **自适应身份验证服务**

  Citrix Cloud 客户现在可以使用 Citrix Workspace 为 Citrix Virtual Apps and Desktops 提供自适应身份验证。自适应身份验证是一种 Citrix Cloud 服务，可为登录到 Citrix Workspace 的客户和用户启用高级身份验证。自适应身份验证服务是 Citrix 管理和 Citrix Cloud 托管的 ADC。有关详细信息，请参阅 自适应身份验证服务。

  此功能处于预览状态。

16 February 2022

- **支持客户端-服务器应用程序** 借助 Citrix Secure Private Access 中对客户端-服务器应用程序的支持，您现在可以消除对传统 VPN 解决方案的依赖，以便为远程用户提供对所有私有应用程序的访问。

  有关详细信息，请参阅 支持客户端-服务器应用程序 - 预览

11 October 2021

- **将 Citrix Gateway 服务磁贴合并到 Citrix Cloud 中的单个 Secure Private Access 中**

  Citrix Gateway 服务磁贴现已合并到 Citrix Cloud 中的单个 Secure Private Access 中。

  - 所有 Secure Private Access 客户，包括 Citrix Workspace Essentials™ 和 Citrix Workspace Standard，现在可以使用一个 Secure Private Access 磁贴来配置 SaaS 和企业 Web 应用程序、增强的安全控制、上下文策略以及 Web 过滤策略。

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

- 所有 Citrix DaaS 客户仍然可以从 Workspace Configuration 中将 Citrix Gateway 服务启用为 HDX 代理。但是，从网关服务磁贴启用 Citrix Gateway 服务的快捷方式已删除。您可以从 **StoreFront Cloud > 访问 > 外部连接** 启用 Citrix Gateway 服务。有关详细信息，请参阅 外部连接。否则，功能没有变化。

30 July 2021

- **基于用户地理位置的企业 Web 和 SaaS 应用程序的上下文访问和安全控制**

  Citrix Secure Private Access 服务现在支持基于用户地理位置对企业 Web 和 SaaS 应用程序进行上下文访问。

- **从 Citrix Workspace 门户隐藏特定 Web 或 SaaS 应用程序的选项**

  管理员现在可以从 Citrix Workspace 门户隐藏特定的 Web 或 SaaS 应用程序。当应用程序从 Citrix Workspace 门户隐藏时，Citrix Gateway 服务在枚举期间不会返回此应用程序。但是，用户仍然可以访问隐藏的应用程序。

09 June 2021

- **路由表，用于定义路由应用程序流量的规则**

  管理员现在可以使用路由表来定义规则，以将应用程序流量直接路由到 Internet 或通过 Citrix Gateway Connector。管理员可以根据他们希望如何定义流量流，将应用程序的路由类型定义为“外部”、“内部”、“内部-绕过代理”或“通过网关连接器外部”。

22 May 2021

- **对企业 Web 和 SaaS 应用程序的上下文访问**

  Citrix Secure Private Access 服务的上下文访问功能提供了一种全面的零信任访问方法，可为应用程序提供安全访问。上下文访问使管理员能够根据上下文为用户提供对应用程序的精细访问。这里的“上下文”一词是指用户、用户组以及用户访问应用程序的平台（移动设备或台式计算机）。

- **Citrix Gateway Connector 用户界面品牌重塑**

  Citrix Cloud Gateway Connector™ 用户界面已根据 Citrix 品牌指南进行了品牌重塑。

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

01 May 2021

- **从 Citrix Secure Private Access 服务数据存储中删除客户数据**

  客户数据（包括备份）将在服务授权到期 90 天后从 Citrix Secure Private Access 服务数据存储中删除。

- **将域从 Azure AD 联合到 Citrix Workspace 的简化步骤**

  将域从 Azure AD 联合到 Citrix Workspace 应用程序的步骤现已简化，以便在 Citrix Workspace 中更快地进行载入。域联合现在可以在 Citrix Gateway 服务用户界面中，从“单点登录”页面执行。

- **连接测试工具的增强功能**

  Citrix Gateway Connector 中的连接测试工具已增强，可处理超时错误并生成必要的日志。

15 March 2021

- **平台增强功能**

  进行了各种平台增强，以提高将客户的管理配置传播到 Citrix Gateway Connector 的可靠性。

- **改进的 Web 应用程序性能**

  当通过系统浏览器使用无客户端 VPN 访问 Web 应用程序时，Web 应用程序性能已得到改进。

- **启用 Citrix Gateway Connector 以使用 TLS1.2 A 级或更高级别的密码套件**

  Citrix Gateway Connector 现在使用 TLS1.2 A 级或更高级别的密码套件连接到 Citrix Cloud 服务和其他后端服务器。

11 November 2020

- **Citrix Access Control™ 服务重命名**

  Access Control 服务现已重命名为 Secure Private Access。

15 October 2020

- **在 Remote Browser Isolation 服务中启动 SaaS 和企业 Web 应用程序的增强安全选项**

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

管理员现在可以使用增强的安全选项“**始终在 Citrix Remote Browser Isolation™ 服务中启动应用程序**”，以便无论其他增强安全设置如何，都始终在 Remote Browser Isolation 服务中启动应用程序。

08 October 2020

- **为 Citrix Secure Private Access 浏览器扩展配置会话超时**

  管理员现在可以为 Citrix Secure Private Access 浏览器扩展配置会话超时。管理员可以从 Citrix Gateway 服务用户界面中的“**管理**”选项卡配置此设置。

- **Citrix Secure Private Access 浏览器扩展管理员设置上的 RBAC 控制**

  RBAC 控制现已在 Citrix Secure Private Access 浏览器扩展管理员设置上强制执行。

24 September 2020

- **通过本地浏览器启用对企业 Web 应用程序的无 VPN 访问**

  您现在可以使用 **Citrix Secure Private Access** 浏览器扩展，通过本地浏览器启用对企业 Web 应用程序的无 VPN 访问。**Citrix Secure Private Access** 浏览器扩展同时支持 Google Chrome 和 Microsoft Edge 浏览器。

07 July 2020

- **在 Citrix Gateway Connector 上验证 Kerberos 配置**

  您现在可以使用**单点登录**部分中的**测试**按钮来验证 Kerberos 配置。

19 June 2020

- **授予 Citrix Gateway 服务和 Citrix Secure Private Access 服务的管理员只读访问权限**

  使用 Citrix Gateway 服务的安全管理员团队现在可以提供精细控制，例如授予 Citrix Gateway 服务和 Citrix Secure Private Access 服务的管理员只读访问权限。

  - 具有 Citrix Gateway 服务只读访问权限的管理员只能查看应用程序详细信息。
  - 具有 Citrix Secure Private Access 服务只读访问权限的管理员只能查看内容访问设置。

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

08 May 2020

- **Citrix Gateway Connector 13.0 中的新增故障排除工具**
  - **网络跟踪：** 您现在可以使用 **跟踪** 功能来排查 Citrix Gateway Connector 注册问题。您可以下载跟踪文件并与管理员共享以进行故障排除。
  - **连接测试：** 您现在可以使用 **连接测试** 功能来确认 Gateway Connector 配置中没有错误，并且 Gateway Connector 能够连接到 URL。

V2019.04.02

- **Citrix Gateway Connector 到出站代理的 Kerberos 身份验证支持**

  现在，Citrix Gateway Connector 到出站代理的流量支持 Kerberos 身份验证。Gateway Connector 使用配置的代理凭据向出站代理进行身份验证。

V2019.04.01

- **Web/SaaS 应用程序流量现在可以通过企业网络托管的 Gateway Connector 进行路由，从而避免双因素身份验证。** 如果客户发布了托管在企业网络之外的 SaaS 应用程序，现在已添加支持，以通过本地 Gateway Connector 对该应用程序的流量进行身份验证。

  例如，假设客户有一个受 Okta 保护的 SaaS 应用程序（如 Workday）。客户可能希望，即使实际的 Workday 数据流量未通过 Citrix Gateway 服务路由，到 Okta 服务器的身份验证流量也通过本地 Gateway Connector 经由 Citrix Gateway 服务路由。这有助于客户避免 Okta 服务器的二次身份验证，因为用户是从企业网络内部连接到 Okta 服务器的。

- **禁用过滤网站列表和网站分类**。如果管理员选择不对特定客户应用这些功能，则可以禁用过滤网站列表和网站分类。

- **远程浏览器隔离服务重定向的自动地理路由。** 远程浏览器隔离服务重定向现已启用自动地理路由。

V2019.03.01

- **“检测”按钮已添加到“添加网关连接器”页面。** **检测**按钮用于刷新连接器列表，使新添加的连接器反映在 Web 应用程序连接部分。

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

- **“访问控制 Web 过滤”类别中新增“恶意和危险”类别。** 在“**恶意软件和垃圾邮件**”组下，“**访问控制 Web 过滤**”类别中新增了一个名为“**恶意和危险**”的类别。

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

与 谷歌 Chrome 企业高级版 集成

以下部分提供了有关集成解决方案的详细信息。

解决方案概述

Citrix 客户可以利用全球最流行、最安全的网络浏览器 Chrome，以熟悉的体验原生访问授权的企业网络应用程序。Citrix Secure Private Access 根据管理员定义的策略强制执行每个应用程序的最小权限访问，这些策略通过 Secure Private Access 控制台进行集中管理。管理员可以在 Secure Private Access 控制台上轻松配置企业应用程序域和零信任访问策略。他们可以对策略进行建模，以验证和测试安全结果，并提供适当级别的用户访问和最终用户体验。

此集成的优势在于，通过 Citrix Secure Private Access 基础设施的自动化流量引导，从 Chrome 浏览器向私有 Web 和 SaaS 应用程序提供无代理访问。当用户通过 Chrome 访问应用程序时，系统会自动通过 Google Secure Gateway 将其流量发送到 Citrix Secure Private Access。这确保了安全且受控的网络访问，而无需在用户设备上安装额外的软件。它还简化了部署，减少了 IT 管理，改善了用户体验，并简化了 IT 运营。

集成解决方案包括以下组件：

- Google Chrome Enterprise Premium (CEP)，其中包括数据丢失防护 (DLP)、恶意软件和网络钓鱼防护、URL 过滤以及 Google 管理控制台等功能。
    - 在客户端计算机本地运行的 Google Chrome 浏览器作为安全浏览器，通过 Chrome 托管配置文件强制执行用户级策略。
    - 通过 Google Cloud 门户访问的 Google Chrome Enterprise Premium 控制台提供用于 Chrome Enterprise Premium 安全策略的管理、治理和监控控制台。
- Citrix Secure Private Access，其中包括对云基础设施、ZTNA 策略引擎以及部署在客户环境中的连接器设备的访问。
- Citrix 控制台，包括用于私有应用程序零信任访问策略的 Secure Private Access 控制台以及用于监控和故障排除的 Citrix Monitor。

Citrix Secure Private Access 服务强制执行管理员配置的所有访问策略，确保用户仅被授予对特定 Web 应用程序的访问权限。

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

Chrome Enterprise Premium 高级安全功能

以下是 Chrome Enterprise Premium 提供的一些高级安全功能：

- **数据丢失防护 (DLP)**：实施精细控制和策略，以防止敏感数据泄露或意外共享。
- **恶意软件深度扫描**：使用高级扫描技术检测并隔离未知或高风险文件，防止恶意代码执行并抵御零日攻击。
- **网络钓鱼防护**：通过识别和阻止网络钓鱼尝试，保护用户免受有害网站的侵害，防止登录凭据和个人信息被盗。
- **URL 分类和过滤**：根据网站内容类别限制访问，防止用户访问不当或恶意内容。
- **Web 使用情况洞察和分析**：提供详细的 Web 流量报告和分析，使管理员能够监控用户活动、识别潜在安全威胁并优化网络带宽。

有关详细信息，请参阅 Chrome Enterprise Premium 概述。

适用于 Chrome Enterprise 的 Citrix Secure Access 控件

Secure Private Access 和 Chrome Enterprise Premium 集成支持以下增值功能。

- **RDP** - 直接在浏览器中启用安全的 RDP 会话。有关详细信息，请参阅 远程桌面控制。
- **SSH** - 在浏览器中启用对 SSH 应用程序的安全访问。有关详细信息，请参阅 SSH 控制。
- **防键盘记录** - 在访问 CEP 中的资源时防止键盘记录器。有关详细信息，请参阅防键盘记录控制。
- **剪贴板容器** - 限制或允许浏览器与虚拟化应用程序之间的剪贴板共享。有关详细信息，请参阅 剪贴板容器控制。
- **会话录制** - 录制浏览器中的用户会话。有关详细信息，请参阅会话录制控制
- **浏览器会话重新身份验证** - 在配置的时间间隔后强制对浏览器会话进行定期重新身份验证。有关详细信息，请参阅浏览器会话重新身份验证控制。
- **域后缀** - 通过将域附加到短 URL 来优化用户体验。有关详细信息，请参阅Web 应用程序的域后缀。

成功集成的先决条件

为确保 Citrix Workspace™ 应用程序与 Chrome Enterprise Premium 之间的最佳集成，必须满足以下先决条件。成功完成这些先决条件后，从 Citrix Workspace 应用程序或基于 Web 的用户界面启动应用程序时，将获得更高效、更无缝的体验。

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

先决条件大致分为以下几类。

- 许可证、应用程序版本和扩展
- Google 管理控制台
- 安全私有访问服务
- Chrome 浏览器
- 将 Citrix Workspace 中配置的用户目录与 Google Cloud 用户目录同步

Citrix Secure Private Access - 支持的部署模式

集成解决方案支持 Citrix Secure Private Access 的以下部署模式：

- **Citrix Secure Private Access 服务**：在此部署模式下，所有组件（包括控制平面和网关基础结构）都托管在 Citrix Cloud 中。有关详细信息，请参阅 Citrix Secure Private Access。
- **Citrix Secure Private Access 混合部署**：此部署允许客户使用本地 StoreFront 和 NetScaler Gateway 组件实施零信任网络访问 (ZTNA) 解决方案，并使用 Citrix Cloud 管理配置、管理和监控功能。这意味着客户可以利用现有的本地 NetScaler Gateway 来控制用户流量路由，同时使用 Citrix Cloud 托管的用户界面来管理配置和策略，还可以使用 Citrix Cloud 中托管的 Citrix Monitor 来进行监控和故障排除。有关详细信息，请参阅 Citrix Secure Private Access 混合部署。

重要提示：

对于 Chrome Enterprise Premium (CEP)，仅支持 HTTPS 企业 Web 和 SaaS 应用程序。不支持 HTTP 企业 Web 和 SaaS 应用程序。

法律声明

Chrome Enterprise Premium 由 Google LLC 提供，您的使用受 Google 的可接受使用政策 和 服务特定条款 的约束。

相关主题

- Secure Private Access 入门和设置
- 入门后更新 Google 集成详细信息
- 应用程序配置和管理
- 技术简报：Citrix Secure Access 与 Chrome 企业版

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

集成解决方案的先决条件

为确保 Citrix Workspace™ 应用程序与 Chrome Enterprise Premium 之间的最佳集成，必须满足以下先决条件。成功完成这些先决条件后，从 Citrix Workspace 应用程序或基于 Web 的用户界面启动应用程序时，体验将更加高效和无缝。

先决条件大致分为以下几类。

- 许可证、应用程序版本和扩展
- Google 管理控制台
- 安全私有访问服务
- Chrome 浏览器
- 管理用户
- 关联用户目录
- 绕过 TLS 检查

许可证、应用程序版本和扩展

- **Chrome Enterprise Premium 许可证**：确保您拥有通过 Citrix Cloud Platform License (CPL) 计划获得的有效 Chrome Enterprise Premium 许可证。
- **Citrix Workspace 应用程序 (CWA) 版本**：
  - Windows：2025.07 及更高版本
  - macOS：2025.08 及更高版本
  - ChromeOS: 25.7.0.25 及更高版本

  注意：

  Citrix Workspace app 对于此解决方案是可选要求。

- **Citrix Endpoint Analysis (EPA) 客户端版本**：
  - Windows: 25.9.1.9 及更高版本
  - macOS: 25.10.3 及更高版本

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

注意：

我们建议以管理员模式安装 Windows EPA 客户端，以支持定期设备状态扫描。此外，必须在设备状态 **设置** 页面下启用定期设备状态扫描。有关详细信息，请参阅 设备的定期扫描。

- **Chrome 浏览器版本**：端点必须使用最新版本的 Google Chrome。
- **操作系统**：Windows、macOS 和 ChromeOS。

Google 管理控制台

- **Google 客户 ID**：从 Google 管理控制台获取您的 Google 客户 ID。此 ID 是配置 Google 服务和集成的必需项。您可以通过 Google 管理控制台中的 **帐户 > 帐户设置** 检索您的客户 ID。
- **在 Google 管理控制台中创建自定义角色**：为了让客户加入 Chrome Enterprise Premium (CEP) 并启用 Google Chrome 集成，管理员必须在 Google 管理控制台中创建自定义角色并分配相应的权限。有关详细信息，请参阅 管理员角色和权限。
- **限制 DevTools 扩展**：必须禁用用于强制安装扩展的 Chrome DevTools，以防止敏感数据泄露。这是 Google 管理控制台中的默认选项。

安全专用访问服务

- **IPv6 端点限制**：Citrix Secure Private Access 服务与 Google 云端点集成时，可能会接收来自具有 IPv6 地址的最终用户设备的流量。目前，Secure Private Access 的地理位置和网络位置访问策略不支持 IPv6。

  因此，对于具有 IPv6 地址的最终用户设备，包含地理位置或网络位置条件的访问策略可能会失败。不利用此类条件的其他访问策略适用于启用 IPv4 和 IPv6 的最终用户设备。
- **CEP 的访问限制现在在 Google 管理控制台中配置**：以前在 Secure Private Access 控制台中配置的访问限制仅适用于 Citrix Enterprise Browser。当 Google Chrome 是企业浏览器时，访问限制必须在 Google 管理控制台中配置为策略和规则。
  - 策略在 **Google 管理控制台 > 设备 > Chrome > 设置**中配置。这些设置允许您管理浏览器设置，例如阻止 JavaScript 和允许打印机列表。
  - 规则在 **Google 管理控制台 > 规则**中配置。这些规则是与 DLP 相关的高级设置，例如添加水印、阻止下载包含社会安全号码的文件以及 URL 过滤。

  有关在 Google Workspace 管理控制台中创建策略和规则的详细信息，请参阅以下主题：
  - 为 Chrome Enterprise 设置 Chrome Enterprise 连接器策略
  - 数据保护规则

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

谷歌浏览器

托管的 Chrome 配置文件：所有最终用户都必须使用托管配置文件访问 Chrome。托管配置文件可确保在用户设备上强制执行 Chrome 策略、扩展程序和安全设置。

管理用户

为了实现无缝集成，Citrix Secure Private Access 中配置的用户与 Google Identity（目录）之间必须存在关联。这可确保只有授权用户才能访问其分配的应用程序。支持以下用户目录进行集成：

- 活动目录
- Microsoft Entra ID（以前称为 Azure 活动目录）

强制 - 填充用户的电子邮件地址字段

Google Identity 要求填充电子邮件地址字段。为此，Secure Private Access 使用的目录中的用户对象必须具有以下之一：

- 一个电子邮件地址，其域部分已在 Google 管理控制台中配置和验证。例如，电子邮件地址为 `alice@example.com` 的 `Alice` 在 Google Identity 中映射为 `alice@example.com`。
- 一个电子邮件地址，其域部分未在 Google 管理控制台中配置。例如，`Bob` 的电子邮件地址为 `bob@example.internal.net`，该地址未在 Google 中配置。在这种情况下，他在 Google Identity 中映射为 `bob@example.com`，其中 `example.com` 是一个已验证的域。
- 另一个目录字段，可在没有电子邮件的情况下用于域映射。典型方法是利用用户主体名称 (UPN)，无论是否进行域替换。例如，`Charlie` 的 UPN 为 `charlie@ADdomain.com`，并在 Google Identity 中映射为 `charlie@example.com`。

对于 Secure Private Access 目录和 Google 目录中电子邮件地址不匹配的用户，存在显著限制。有关详细信息，请参阅域映射注意事项 部分。

强制 - 填充用户组的电子邮件地址字段

与用户类似，Secure Private Access 使用的目录中的组对象必须具有以下之一：

- 一个电子邮件地址，其域部分已在 Google 管理控制台中配置和验证。
- 一个电子邮件地址，其域部分未在 Google 管理控制台中配置。
- 另一个目录字段，可在没有电子邮件地址的情况下用于域映射。典型方法是利用通用名称 (CN)，并在 Google Directory 中附加相应的域。例如，CN 为 `group1` 的组在 Google Identity 中映射为 `group1@example.com`。

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

电子邮件地址缺失或不一致的域映射注意事项

用户：

如果用户的电子邮件地址在 Secure Private Access 目录中缺失，或者在 Secure Private Access 目录与 Google Identity 之间不一致，则适用以下注意事项：

- 在 Secure Private Access 控制台中配置 Secure Private Access 策略时，没有电子邮件地址的用户将不可供选择。
- 对于 Secure Private Access 目录和 Google 目录之间电子邮件地址不匹配的用户，Secure Private Access 策略将不起作用。
- 这些用户不支持从云商店（使用 Citrix Workspace 应用程序或 Web 浏览器）启动 Web 或 SaaS 应用程序。

组：

如果组的电子邮件地址在 Secure Private Access 目录中缺失，或者与 Google Identity 不一致，则需要进行适当的 域映射配置，以确保 Secure Private Access 组级别策略正常工作。

将 Citrix Secure Private Access 中配置的用户目录与 Google Cloud 用户目录关联

您必须将 Citrix Secure Private Access 中配置的用户目录与 Google Cloud 目录关联。具体而言，支持以下用户目录：

- 活动目录
- 微软 Entra ID（以前称为 Azure 活动目录）
- 奥克塔

请注意，用户目录关联必须定期进行，以确保应用程序访问得到适当的强制执行。关联仅需要最少数量的属性。

活动目录

对于 Active Directory，必须关联名称、电子邮件地址、对象全局唯一标识符 (objectGUID) 和安全标识符 (SID)。密码和所有其他属性无需与 Google Cloud 目录关联。

有关如何将您的 AD 与 Google Cloud 关联以在自定义架构 `citrix-schema` 下包含自定义 AD 字段的详细信息，请参阅 将 Google Cloud Identity 作为身份提供程序连接到 Citrix Cloud 和 Active Directory 用户帐户预配。

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

微软 Entra ID

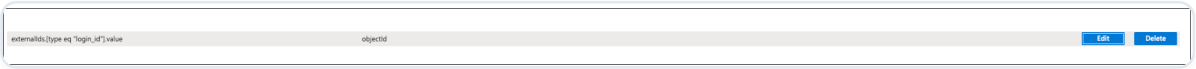
您必须将 Microsoft Entra ID 与 Google Cloud 用户目录同步，以便在 Google 和 Microsoft 云平台之间进行用户和组管理。有关详细信息，请参阅 Microsoft Entra ID（以前称为 Azure AD）用户预配和单点登录。

配置同步时，您必须考虑以下要求：

- **电子邮件地址：** 所有用户和组都必须填写电子邮件地址字段。有关详细信息，请参阅管理用户。
- **objectId 属性映射：** Entra ID 用户的 objectId 属性必须映射到 Google Directory。

  在 G-Suite 连接器配置中执行此映射：

  a. 在左侧菜单中，单击 **管理 > 预配**。
  b. 在新菜单中，单击 **管理 > 属性映射**。
  c. 单击 **预配 Microsoft Entra ID 用户**。
  d. 找到 objectId 的相应行。
     - 单击 **编辑**，然后在 **目标属性** 下选择 **externalIds**..value。
     - 验证生成的配置是否与以下屏幕截图匹配。



- **单点登录：** 单点登录 (SSO) 配置是可选的。您可以在 Google 目录中配置单独的密码，使用 Entra ID 配置 SSO，或者使用通过 Citrix Identity 的 Open ID Connect 配置 SSO。

奥克塔

您可以通过将 Okta 中的用户和组预配到 Google Cloud 用户目录（Cloud Identity / Google Workspace）中，来使用 Okta 作为身份源。预配后，与 Secure Private Access 的关联遵循与其他受支持目录相同的模型。只需要最少量的属性，并且所有用户和组都必须填写电子邮件地址字段。

有关从 Okta 预配到 Google 的详细信息，请参阅Okta 用户预配和单点登录。您可以按照相同的指南配置针对 Okta 的 SSO，或者参阅通过 Citrix Workspace 的 Open ID Connect。

谷歌云身份 (谷歌目录)

当 Google Cloud Identity 已经是您的身份提供商时，用户和组将本地驻留在 Google Cloud 目录中。无需进行目录关联或同步，因为没有单独的外部目录需要与 Google 进行协调。Google 是 Citrix Workspace 和 Chrome 托管配置文件的身份源。

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

注意：

Chrome Enterprise Premium 的设备姿态服务集成依赖于 OpenID Connect (OIDC) 流程，其中 Google Cloud 目录充当 Citrix Workspace 的依赖方。当 Google Cloud Identity 本身是底层 IdP 时，不支持该流程。因此，在此配置中无法使用设备姿态服务集成。

绕过 TLS 检查

为确保 Chrome Enterprise Premium 端点在采用 TLS 检查（或 SSL 检查）的网络上正常运行，您必须将以下主机名从检查中排除。

- `ingress.cloudproxy.app`
- `securegateway.goog`
- `*.securegateway.goog`

此排除至关重要，因为许多 TLS 检查解决方案（例如 SSE 供应商或代理服务器）不完全支持 Chrome Enterprise Premium 使用的 HTTP CONNECT 方法，这可能导致流量突然中断。

此外，建议将以下主机名从 TLS 检查中排除，以避免潜在的最终用户性能问题和连接延迟。

- `safebrowsingrealtime.googleapis.com`
- `secureconnect-pa.clients6.google.com`
- `secureconnect-pa.mtls.clients6.google.com`
- `secureconnect-pa.googleapis.com`
- `chromereporting-pa.googleapis.com`

管理员角色和权限

Citrix 服务帐户由 Secure Private Access 用于将用户载入 Chrome Enterprise Premium (CEP) 并启用 CEP 集成。因此，您必须在 Google 管理控制台中为服务帐户分配具有所需权限的角色。

Google 管理控制台中提供两种类型的角色：

系统角色： 这些是 Google 提供的默认角色。除了超级管理员角色外，其余系统角色不包含 CEP 与 Secure Private Access 集成所需的所有必要权限。

自定义角色： 这些角色可以包含 Admin API 权限的任何子集。您必须创建一个自定义角色，其中包含 CEP 与 Secure Private Access 集成所需的所有权限。

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

您必须以超级管理员身份登录 Google 管理控制台才能执行此任务。

注意：

超级管理员角色不能分配给服务帐户。

Google 自定义管理员角色权限

对于 CEP 和 Secure Private Access 集成，Citrix 服务帐户必须在 Google 管理控制台中具有自定义角色，并具有以下特定权限：

所需的管理员权限	为什么需要此权限
管理客户 > 读取客户	用于读取 Google 客户组织的友好名称。
组织单位 > 读取	验证配置的组织单位在 Google Directory 中可用。
服务 > Chrome 管理 > 设置 > 管理用户设置 **注意：** 确保您选择顶级权限 **管理用户设置** 和子权限（**管理应用程序设置** 和 **管理 Web 设置**）。	添加用户配置文件中 CEP 和 SPA 集成所需的强制扩展及其配置。
服务 > Chrome 管理 > 设置 托管浏览器 > 读取	读取托管的 Chrome 配置文件和托管的浏览器。
许可证管理 > 读取	查询为组织预配的 Chrome Enterprise Premium 分配的许可证总数。
报告	读取正在主动使用其分配的许可证的用户。 读取数据丢失防护 (DLP) 规则触发时的活动事件。 读取故障事件。

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

所需的管理员权限	为什么需要此权限
群组 > 读取	用于验证配置的集成群组在 Google Directory 中是否可用。
服务 > 警报中心 > 完全访问 > 查看访问	用于读取数据丢失防护的安全警报和登录失败事件。
管理设备和设置	用于读取设备元数据，以便在监控网络拓扑视图中显示它们。
用户 > 读取	用于验证配置的集成用户在 Google Directory 中是否可用。

注意：

- 还需要为这些管理员权限授予等效的 OAuth 范围。
- 所有管理权限现在都可以在“**管理员权限**”部分中找到。这包括以前在“**管理员控制台权限**”和“**管理员 API 权限**”部分中列出的权限。此更改不影响权限的分配方式，并且现有权限将继续像以前一样工作。
- 确保选择顶级权限“**管理用户设置**”和子权限（“**管理应用程序设置**”和“**管理 Web 设置**”）。仅选择子权限是不够的。
- Citrix Secure Private Access 使用配置的 Citrix 服务帐户将配置部署到您的 Google 帐户。在 Citrix Secure Private Access 和 Google CEP 集成完成后，打开 Google 管理控制台并导航到“**Chrome 浏览器 > 应用和扩展程序**”。请注意，已在根组织级别配置了多个浏览器扩展。这些扩展由子组织单位继承。当用户使用此租户加入 Google Chrome 配置文件时，这些扩展将自动预配。

创建和分配角色和权限

执行以下步骤以创建自定义管理员角色并分配权限：

1. 在 Google 管理控制台中，转到 **帐户** > **管理员角色**。
2. 单击 **创建新角色**，并输入角色的名称和描述。

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

3. 将 Google Chrome 集成所需的所有权限添加到此自定义角色。有关所需权限的列表，请参阅 Google 自定义管理员角色权限。

   有关角色和权限的更多信息，请参阅 Google 文档。

4. 保存自定义角色。

配置出口中心区域

Secure Private Access 使管理员能够选择 Chrome Enterprise Premium 用于 SaaS 应用程序流量的出口区域。每个选定的区域都提供一组专用的出口 IP 地址，管理员可以将其添加到 SaaS 应用程序的允许列表中，以允许通过 Google Secure Gateway 路由的流量。此功能适用于云部署和混合部署。

您可以通过以下任一路径访问**SaaS 应用程序出口区域**面板。

- 单击 Chrome Enterprise Premium 设置卡上的**管理出口区域**按钮。

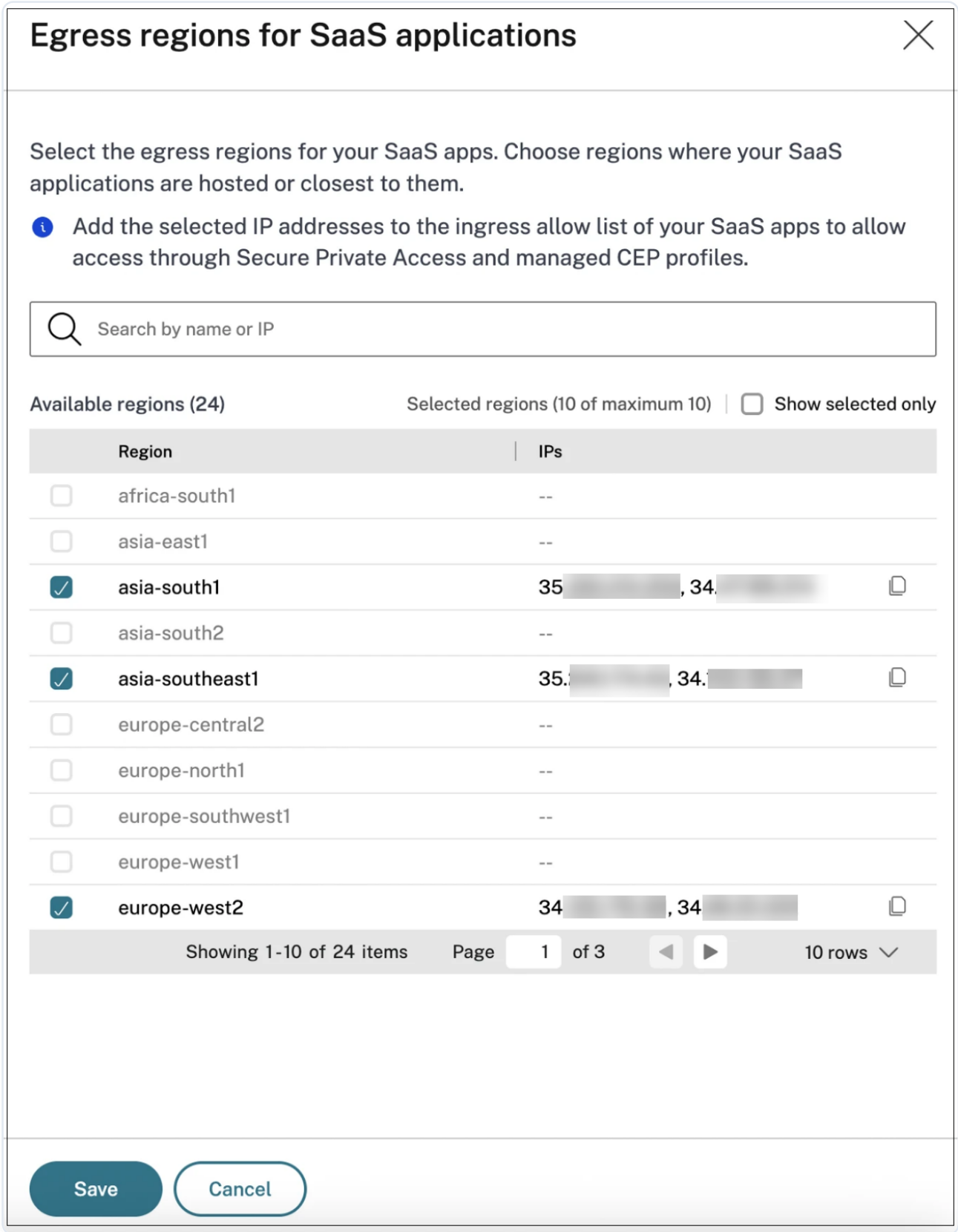


- 在**浏览器设置 > 浏览器配置 > SaaS 应用程序出口区域**中单击**编辑**。

SaaS 应用程序出口区域面板

SaaS 应用程序出口区域面板显示可用的出口区域以及与每个选定区域关联的 IP 地址。您可以按名称或 IP 地址搜索区域，然后复制区域的 IP 地址，将其添加到 SaaS 应用程序的允许列表中。

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



IP 地址仅在您选择区域、保存更改并且 Google 完成部署后才可用。在部署完成之前，新选择的区域不会显示任何 IP 地址。部署通常需要几分钟，但具体时间可能会有所不同。

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

选择区域

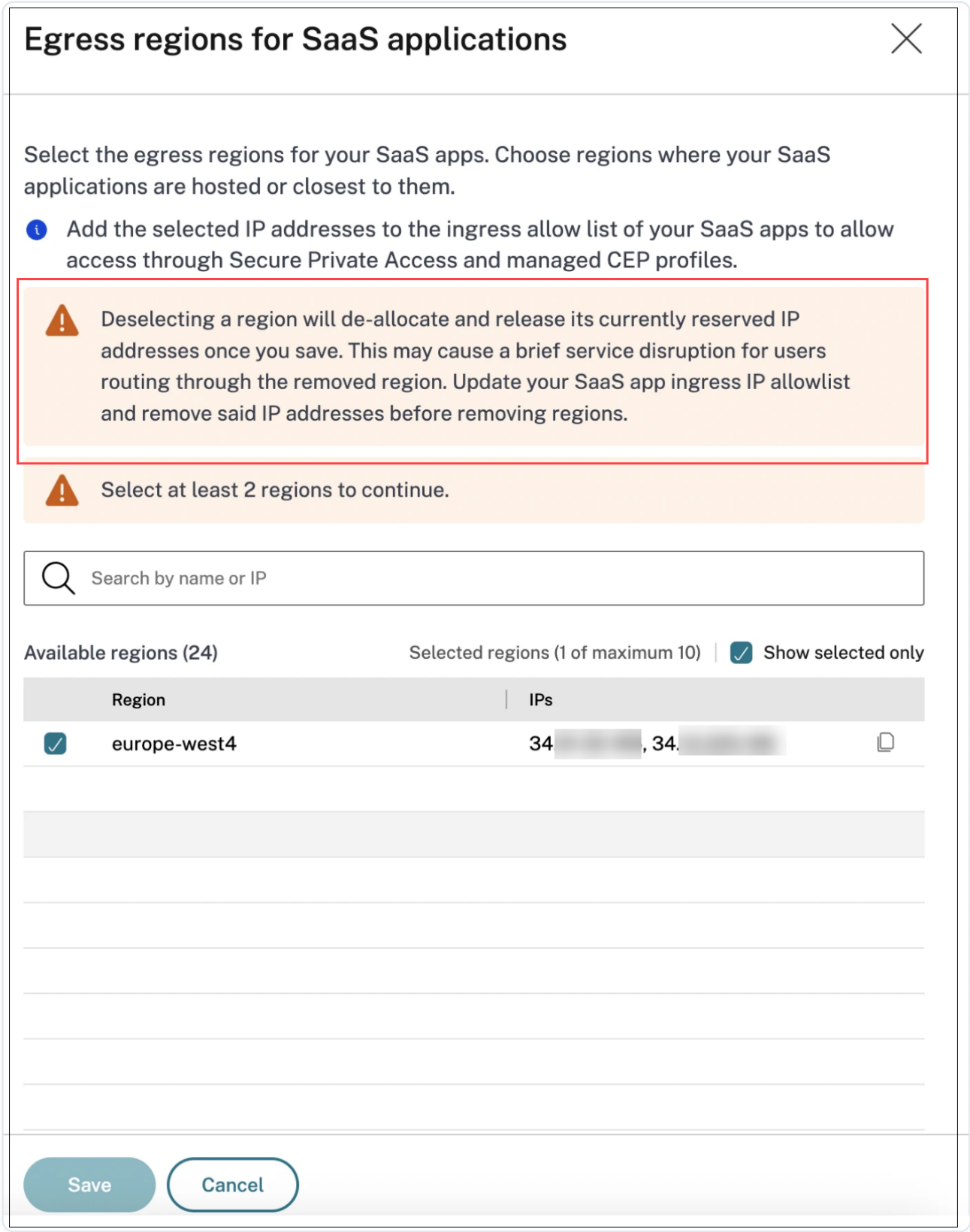
选择托管 SaaS 应用程序的区域或离它们最近的区域。为确保在区域中断期间的冗余，请至少选择两个区域。您最多可以选择 10 个区域。

在 Google 部署选定区域并且关联的 IP 地址可用后，将这些 IP 地址添加到 SaaS 应用程序的入口允许列表中。

取消选择区域

取消选择区域会显示警告消息。

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



您必须在保存更改之前更新您的SaaS应用程序允许列表。如果您选择**取消**，所有更改都将被丢弃。

如果您稍后取消选择并重新选择同一区域，Google会分配一组新的出口IP地址。这些IP地址通常与之前分配的不同，因此您必须相应地更新您的SaaS应用程序允许列表。

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

没有电子邮件地址的用户组的域映射

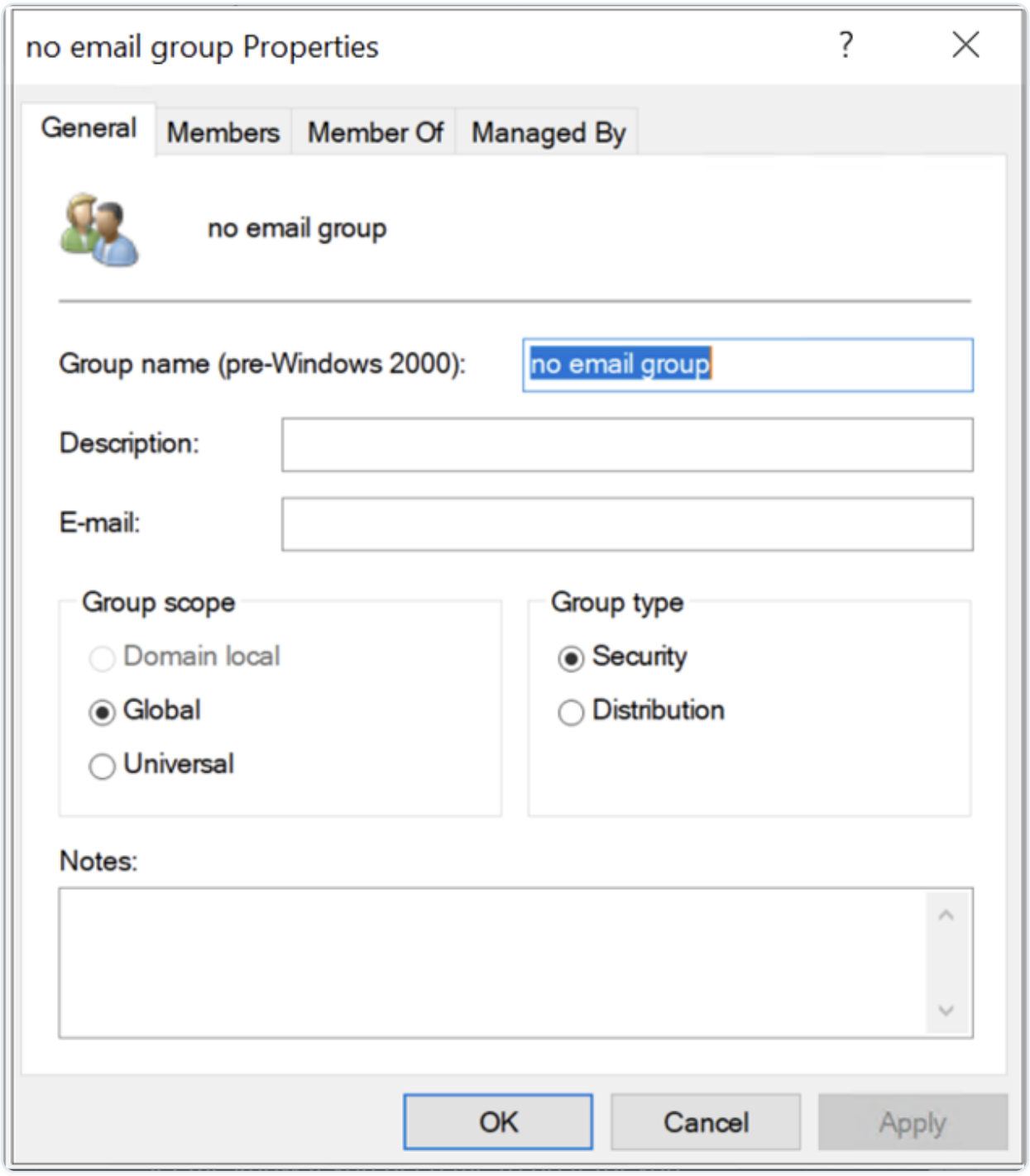
Google 目录要求所有用户和组对象都具有经过验证的电子邮件地址。但是，对于 Secure Private Access 支持的目录（特别是 Active Directory (AD) 和 Microsoft Entra ID），这并非总是可用。AD 和 Microsoft Entra ID 对象可能缺少电子邮件地址，或者其电子邮件地址指向 Google 目录无法验证的内部或特殊域（例如，@fabrikam.onmicrosoft.com）。

由于电子邮件地址通常是 Secure Private Access 和 Google 目录之间的通用标识符，因此来自 AD/Entra 且没有经过验证的 Google 电子邮件地址的组通常不受 Secure Private Access 策略的支持。域映射功能通过允许管理员针对没有电子邮件地址或电子邮件地址具有未经验证域的组配置策略来解决此问题。

域映射的工作原理

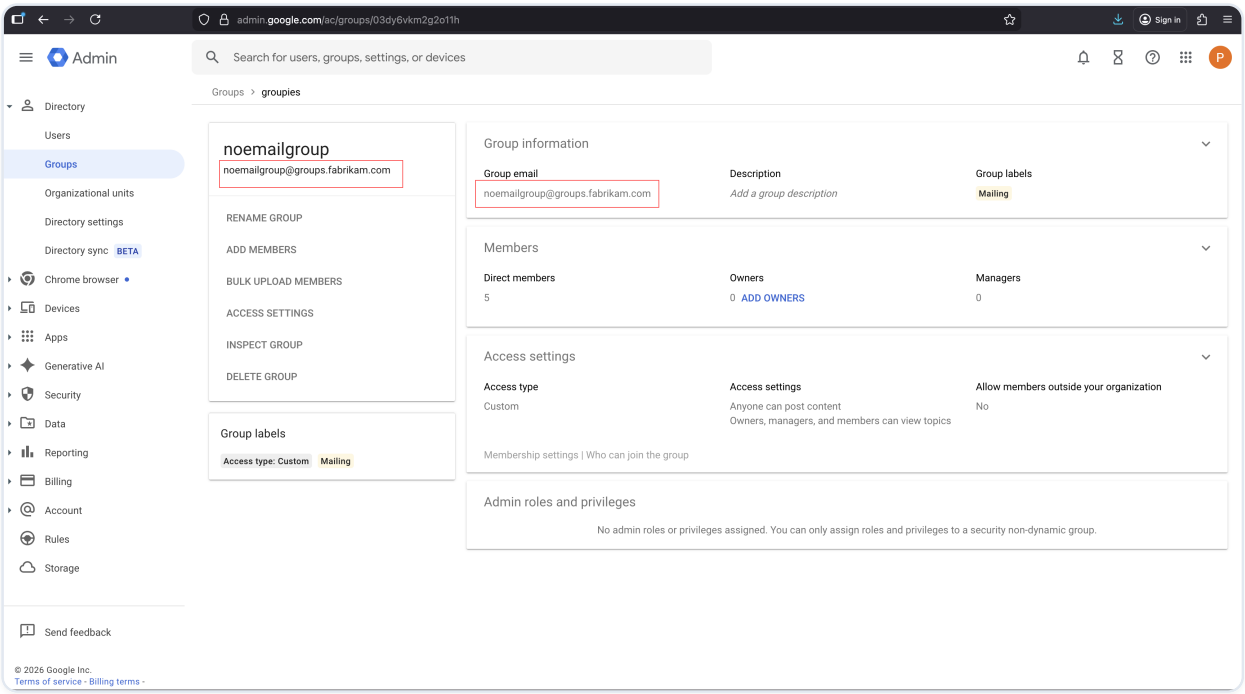
- 考虑您的 AD 中没有电子邮件地址的组。

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



- 此组在 Google 目录中复制，其电子邮件地址由组通用名称（请注意，由于电子邮件地址不支持“空格”，因此省略了空格）和经过验证的 Google 域 `@groups.fabrikam.com` 合成。有效的 Google 组电子邮件地址 `noemailgroup@groups.fabrikam.com` 在源目录中不存在。

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



- 管理员可以为没有电子邮件地址的组配置域映射。

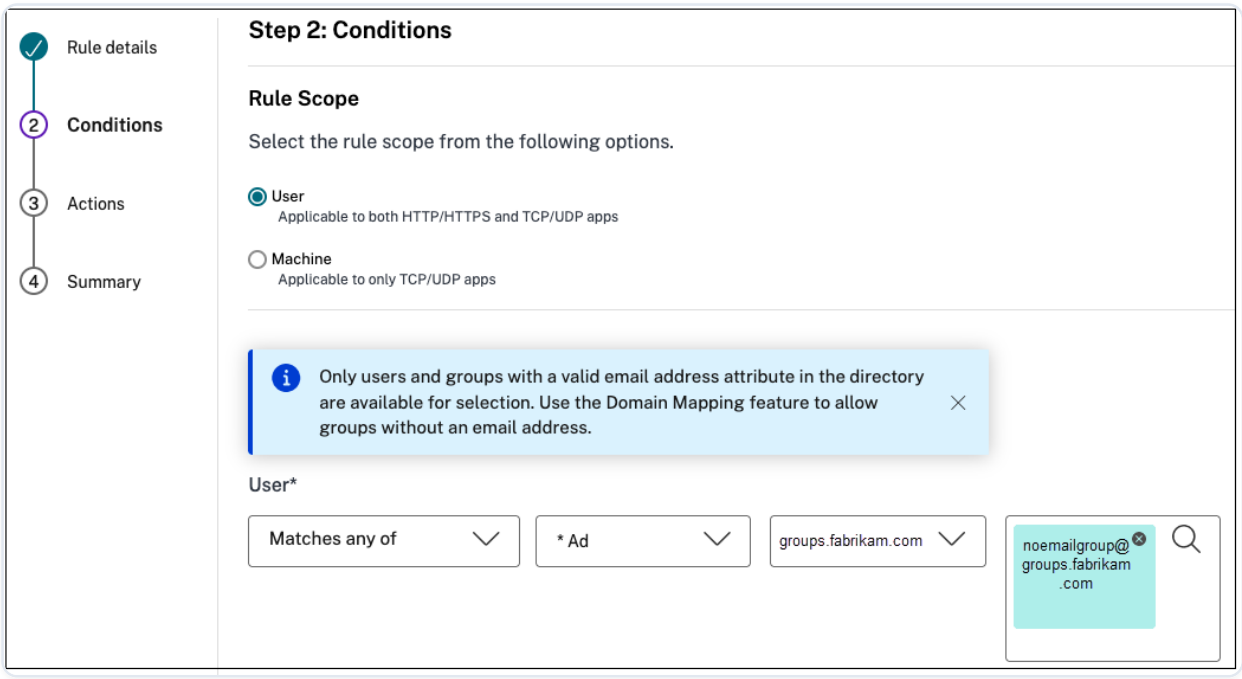
  a. 在 Secure Private Access 管理控制台中，导航到 **浏览器设置 > 域映射**。

  b. 将 **包含空域** 开关切换为“开”以启用没有电子邮件地址的组的映射。

  c. 在 **Google 域 > 域** 字段中，输入目标组域（本例中为 `groups.fabrikam.com`）。通过添加目标组域，您可以在配置策略时，使管理员能够将没有电子邮件的组映射到相应的 Google 域电子邮件 (`groups.fabrikam.com`)。

将组分配给策略时，如果您搜索没有电子邮件地址的组 (`noemailgroup`)，则会根据您的域映射配置合成一个电子邮件地址，并且 `noemailgroup@groups.fabrikam.com` 将变为可用。此转换基于预定的转换逻辑。有关详细信息，请参阅电子邮件地址构建。

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



电子邮件地址构建

- 对于没有现有电子邮件地址的组：
  - 电子邮件本地部分使用组通用名称 (cn) 的小写版本填充，并省略“空格”字符。
  - 电子邮件域部分使用 Google 域 (google-domain) 的小写版本填充。
  - 域选择（当存在多个 Google 域时）：如果一个组与多个 Google 域关联，管理员可以选择电子邮件地址的相应域。
- 对于在未验证域中具有现有 onmicrosoft.com 或其他电子邮件地址的组：
  - 电子邮件本地部分：电子邮件本地部分使用现有电子邮件地址的本地部分的小写版本填充。
  - 域选择（当存在多个 Google 域时）：如果一个组与多个 Google 域关联，管理员可以选择电子邮件地址的相应域。

限制

域映射功能仅支持包含字母数字字符、破折号、下划线和空格的组。

托管配置文件身份

Google 目录通过主电子邮件地址识别每个用户帐户。当您的组织将用户从 Active Directory 或 Microsoft Entra ID 同步到 Google 目录时，您可以选择哪个源属性成为该地址。大多数组织映射电子邮件地址。对于未为每个用户填充电子邮件属性的组织，可以映射用户主体名称 (UPN)，因为 UPN 始终存在于 Active Directory 中。

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

Secure Private Access 必须使用目录同步用作主地址的相同属性来查找每个用户，否则它无法将用户与其在 Google 目录中的帐户匹配。您可以从 Secure Private Access 管理控制台中的“托管配置文件身份”页面设置该属性。

设置用户属性类型

1. 在 Secure Private Access 管理控制台中，导航到 **浏览器设置 > 托管配置文件身份**。
2. 在 **Google 用户 ID 类型**中，选择 Secure Private Access 用于识别 CEP 最终用户的属性。

   属性类型(/en-us/citrix-secure-private-access/media/spa-cep-attribute-type.png)

   - **电子邮件** - Secure Private Access 通过最终用户的电子邮件地址识别他们。这是默认值，也是现有部署使用的值。
   - **用户主体名称** - Secure Private Access 通过最终用户的用户主体名称 (UPN) 识别他们。
3. 单击 **保存**。
4. 在 **更新 Google 用户 ID 类型？** 确认窗口中，查看消息并单击 **更新**。

设置保存后，将显示确认消息。

注意：

- **Google 用户 ID 类型**设置仅适用于用户。Google 群组没有用户主体名称，因此群组身份不受影响。如果您的群组在源目录中没有电子邮件地址，请参阅 没有电子邮件地址的用户组的域映射。
- 此设置应用于整个租户。您不能为单个用户选择不同的身份属性。

Open ID Connect 与 Citrix 身份和访问管理

您可以使用适用于 Citrix Cloud 的 OpenID Connect (OIDC) 身份验证提供程序，为 Chrome Enterprise Premium (CEP) 配置单点登录 (SSO)。OIDC 与 Citrix 身份的集成提供以下优势：

- **设备状态服务集成：** 通过将设备状态服务与 Google Chrome Enterprise Premium 集成，您可以将设备合规性检查扩展到基于 Chrome 浏览器的访问场景。此集成使组织能够在用户通过其托管的 Google Chrome 配置文件访问应用程序时强制执行设备状态策略。要将设备状态服务用于此集成，我们建议配置定期设备状态扫描。

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

注意：

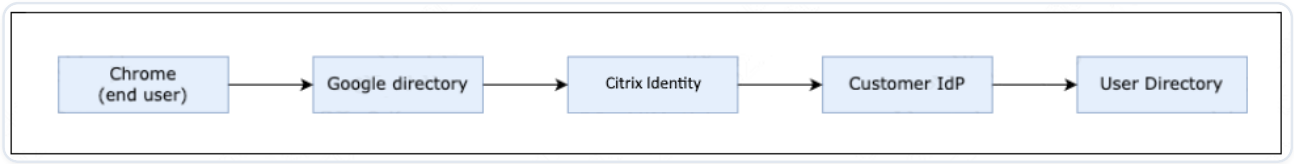
当设备状态服务配置为多存储模式时，此集成不起作用。

有关设备状态服务的更多信息，请参阅 设备状态概述。

- **统一登录体验：** 尽管您可以为 Chrome 配置针对大多数常见身份提供程序的 SSO，包括但不限于 Active Directory (AD) 和 Microsoft Entra（以前称为 Azure AD），但您可以选择为云存储和 CEP 提供统一的登录体验。

概述

OIDC 允许使用 Citrix 身份作为 OIDC 身份验证提供程序进行 SSO。OIDC 中涉及的组件如下图所示：



Google Chrome 在创建托管配置文件时，始终尝试针对 Google 目录进行身份验证。借助 OIDC，Google 目录实质上成为针对 Citrix 身份的信赖方 (RP)，Citrix 身份是一个 OIDC 连接提供程序。反过来，Citrix 身份支持以下功能：

- 设备状态功能
- Chrome 和云存储的通用统一登录体验。

先决条件

在配置 OIDC 身份验证与 Citrix 身份之前，请确保满足以下先决条件：

- 您拥有 Google 管理控制台的管理访问权限。
- 您已配置并执行了目录同步。有关详细信息，请参阅 将 Citrix 身份中配置的用户目录与 Google Cloud 用户目录同步。
- 用户身份提供程序 (IdP) 已在 Citrix Cloud 身份和访问管理中设置和配置。支持以下身份提供程序：
  - Active Directory (AD) - 标准本地 Active Directory 集成
  - 带令牌的 Active Directory - 基于令牌身份验证的 AD 集成
  - Microsoft Entra ID - 基于云的身份服务（以前称为 Azure AD）
  - 奥克塔

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

- SAML 2.0

注意：

使用 Citrix Cloud 作为 OpenID Connect (OIDC) 身份验证提供程序的 Chrome Enterprise Premium (CEP) 单点登录 (SSO) 现在支持条件身份验证。

- 有关 Citrix Cloud 身份和访问管理的更多信息，请参阅 身份和访问管理。
- 您已通过选择上述身份提供程序之一来配置订阅者如何对其商店进行身份验证。有关如何配置商店身份验证的说明，请参阅 配置身份验证。
- 您已完成 Secure Private Access 的初始设置和入门。有关详细信息，请参阅 Secure Private Access 入门和设置。

OIDC 集成概述

要使 Google Chrome 托管配置文件登录与您配置的 Citrix 身份提供程序集成，必须将 Google OIDC SSO 配置文件与 Citrix OIDC 客户端关联。为此，请执行以下步骤：

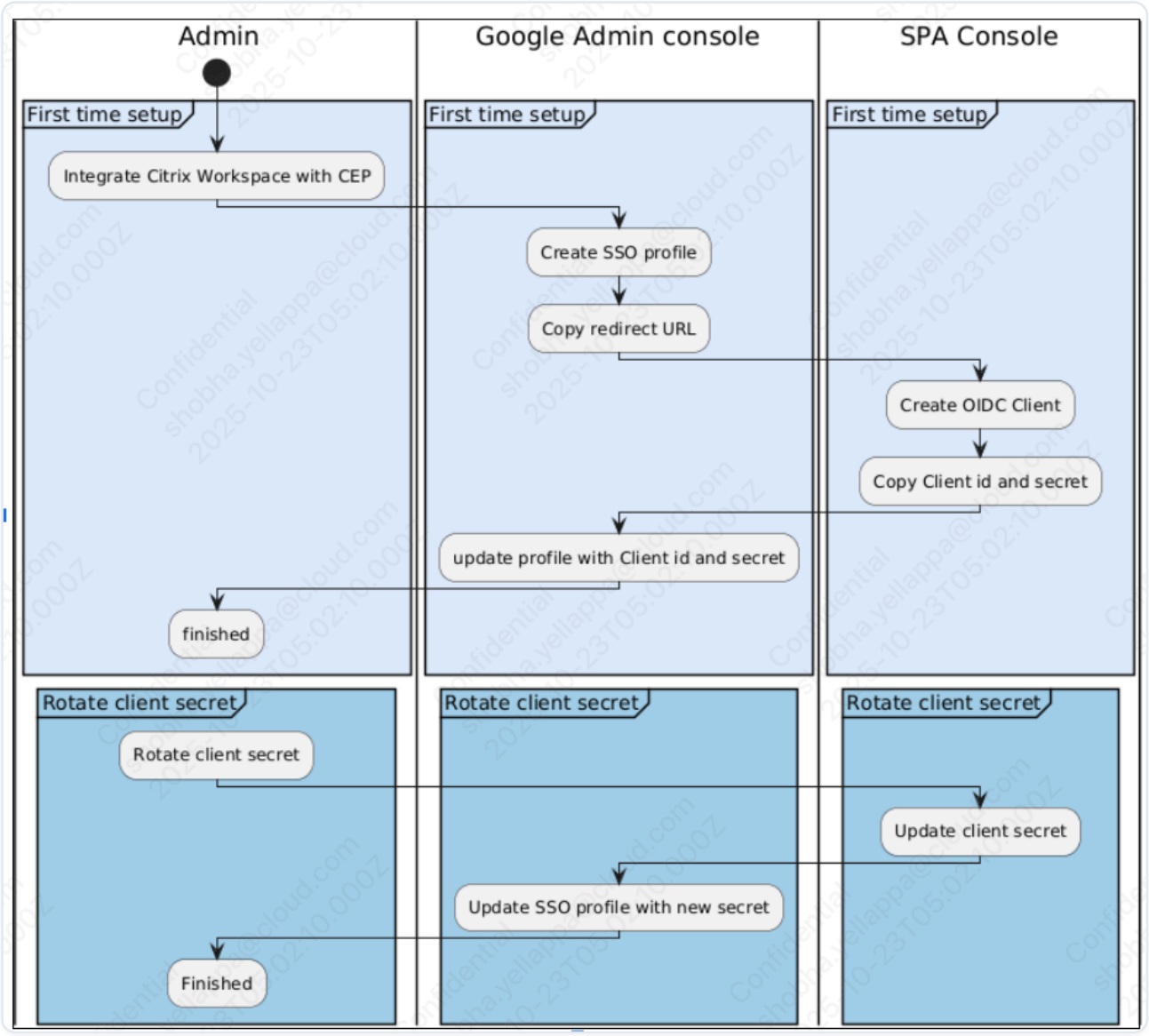
1. 在 Google 管理控制台中，通过输入配置文件名称来创建新的 SSO 配置文件。您现在可以将其余字段留空。有关创建新的 SSO 配置文件和重定向 URL 的详细信息，请参阅 创建 Google OIDC SSO 配置文件。
2. 创建 SSO 配置文件后，复制为此配置文件生成的重定向 URL。
3. 在 Secure Private Access 控制台中，创建 Citrix OIDC 客户端并将重定向 URL（来自 Google SSO 配置文件）粘贴到“**重定向 URL**”字段中。有关创建 Citrix OIDC 客户端的详细信息，请参阅 创建 Citrix OIDC 客户端。
4. 创建 OIDC 客户端后，记下 Secure Private Access 控制台中显示的客户端 ID、客户端密钥和颁发者 URL。
5. 返回 Google 管理控制台，并使用 Secure Private Access 控制台中的客户端 ID、客户端密钥和颁发者 URL 更新 SSO 配置文件。
6. 在“**管理 SSO 配置文件分配**”中，选择您配置的 Google SSO 配置文件以完成集成。

注意：

创建 OIDC 客户端后，您可以在 Secure Private Access 控制台中轮换客户端密钥，并在 Google 管理控制台中更新 SSO 配置文件。

下图说明了 OIDC 集成工作流：

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

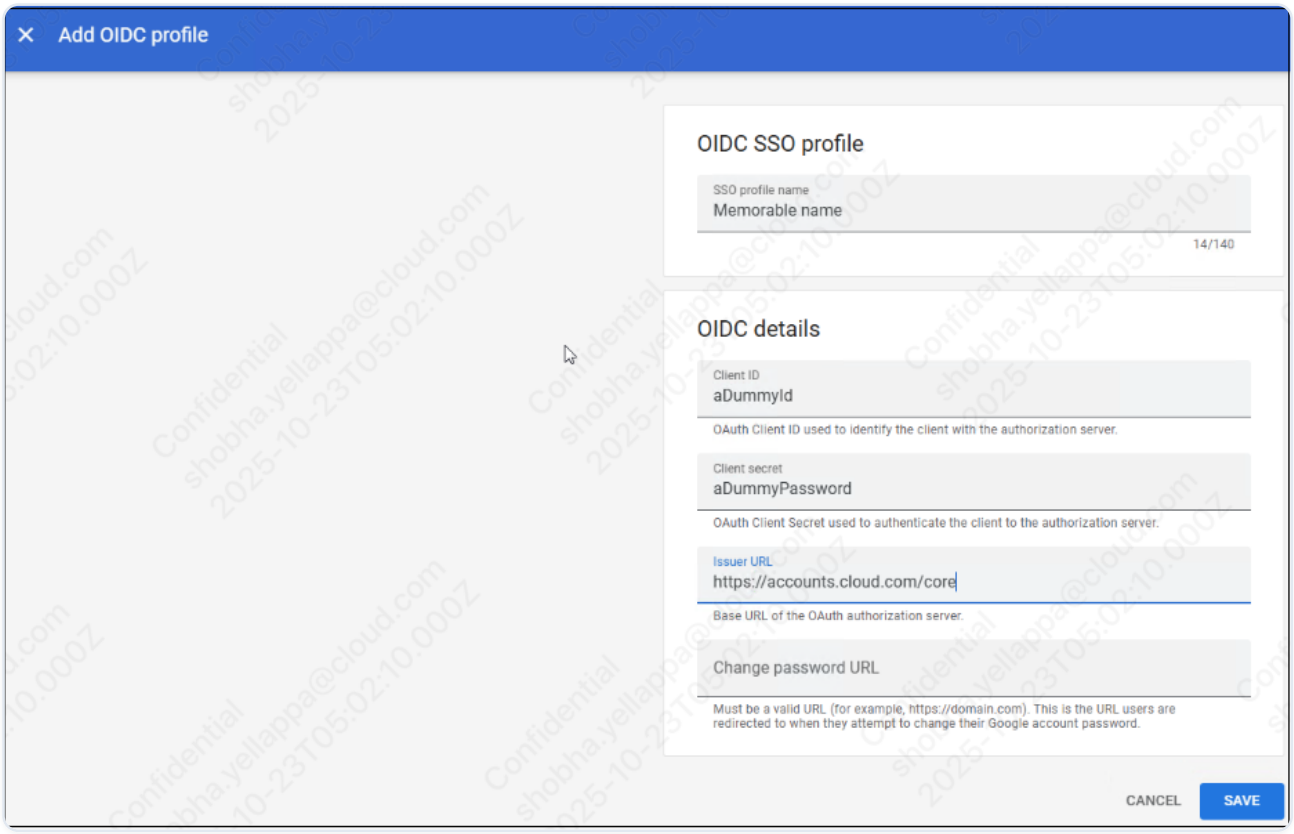


创建 Google OIDC SSO 配置文件

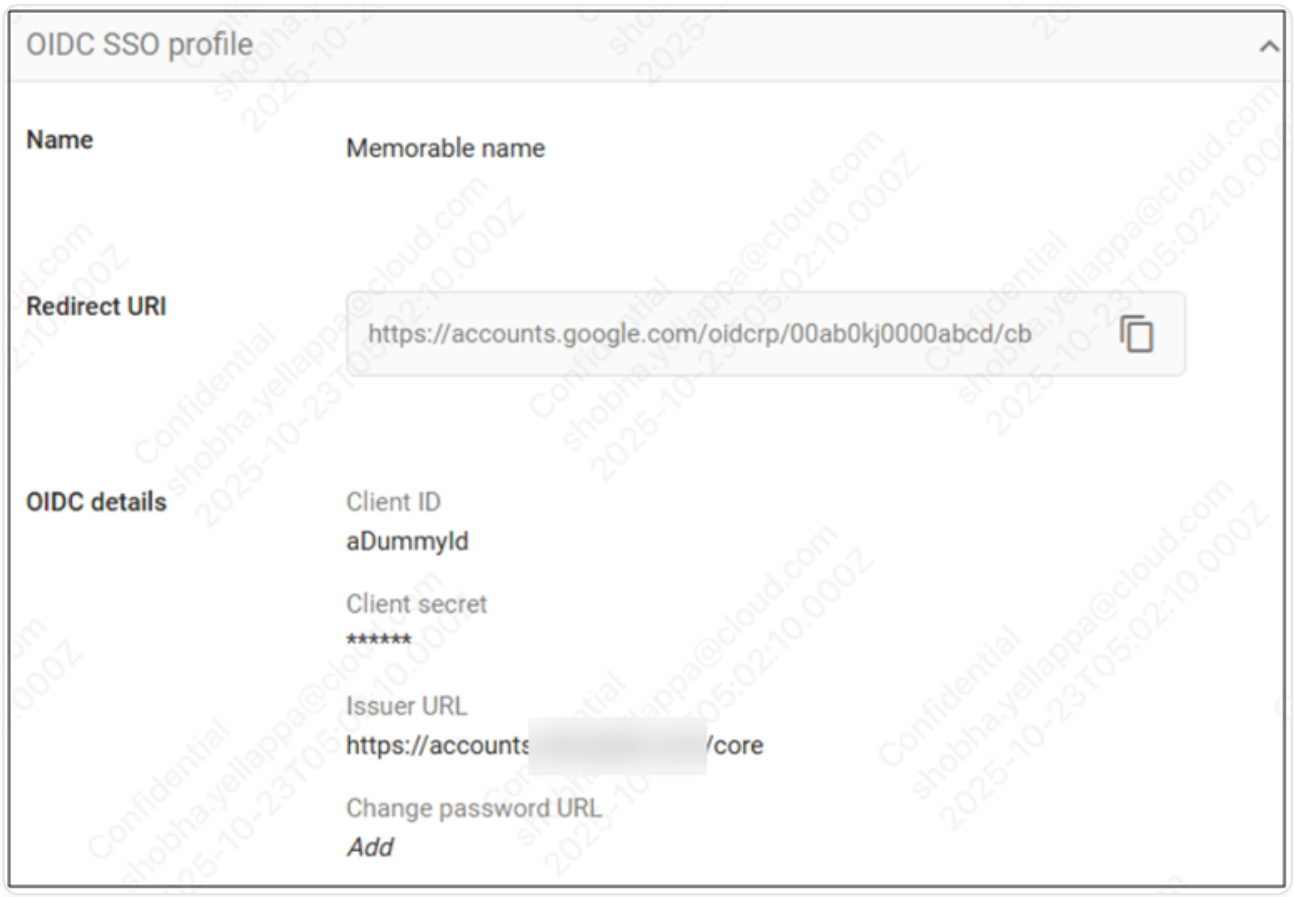
在 Google 管理控制台中执行以下步骤。

1. 转到“**安全 > 身份验证 > 使用第三方 IdP 进行 SSO**”，然后选择“**添加 OIDC 配置文件**”。
2. 为配置文件提供一个名称。
3. 为客户端 ID 和客户端密钥分配一个虚拟值，或者将其留空。这些字段稍后会更新。
4. 在 **颁发者 URL** 中，输入 `https://accounts.cloud.com/core`。
5. 单击 **保存**。

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



创建配置文件后，单击它以获取重定向 URI，创建 OIDC 客户端需要此 URI。



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

创建 Citrix OIDC 客户端

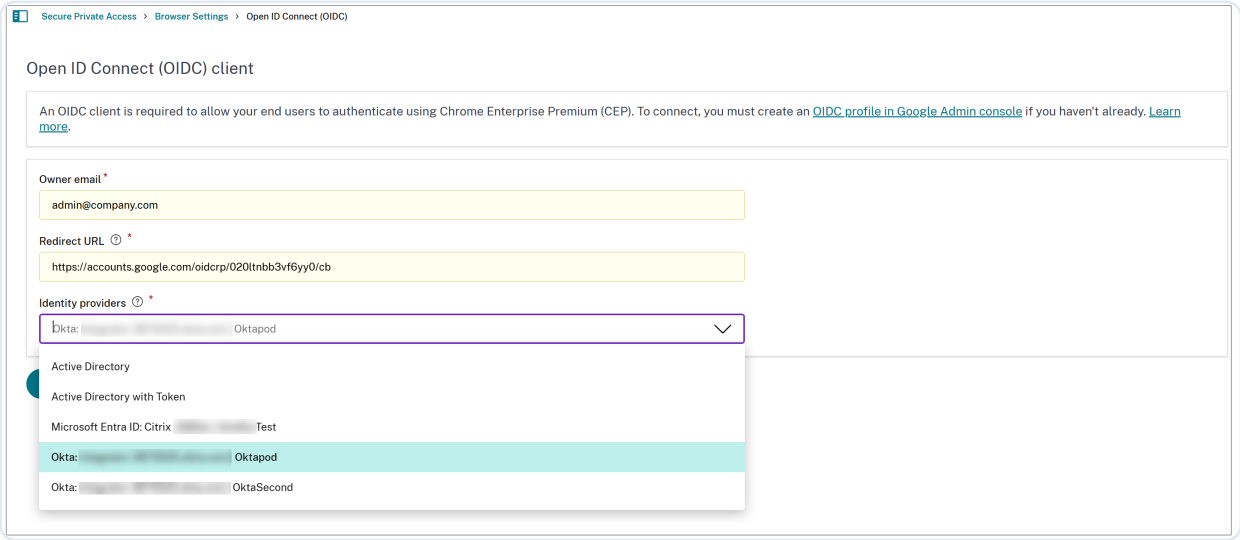
在 Secure Private Access 管理控制台中执行以下步骤：

1. 在导航窗格中，单击 **浏览器设置 > Open ID Connect (OIDC)**。

   注意：

   浏览器设置 菜单中的 **Open ID Connect (OIDC)** 选项仅在完成载入过程后可用。

2. 在 **所有者电子邮件** 中，输入用户的电子邮件 ID 地址。当 OIDC 客户端密钥过期时，需要此电子邮件 ID 地址来发送警报。
3. 在 **重定向 URL** 中，输入在 Google Admin 控制台中创建 Google OIDC SSO 配置文件时生成的重定向 URI。身份提供程序使用此 URL 响应用户身份验证请求。
4. 选择在您的环境中配置的身份提供程序。
5. 单击 **创建**。



成功创建 OIDC 客户端后，将弹出一个窗口显示客户端 ID、客户端密钥和颁发者 URL。您必须将这些详细信息复制到您的 Google 管理控制台配置中。您可以通过以下方法之一检索凭据：

- 直接从弹出窗口复制值
- 将详细信息下载为 CSV 文件以进行安全存储

重要提示：

客户端密钥仅在此初始设置步骤中可见。您必须在关闭弹出窗口或继续下一步之前检索客户端密钥。窗口关闭后，客户端密钥将无法再次查看，您必须轮换密钥以获取新密钥。

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

6. 单击 **关闭**。

OIDC SSO 配置文件分配

创建 OIDC 客户端并使用客户端 ID 和密钥更新 Google OIDC SSO 配置文件后，必须将 OIDC SSO 配置文件分配给用户和组，SSO 才能生效。

1. 在 Google 管理控制台中，转到 **安全性 > 身份验证 > 使用第三方 IdP 的 SSO**。
2. 在 **管理 SSO 配置文件分配** 中，单击 **管理**。
3. 在左侧导航窗格中，选择根组织单位 (OU) 和您的 SSO 配置文件，为组织的所有用户启用 SSO。或者，您可以将 SSO 配置文件分配给特定的组或 OU。

更新 Citrix OIDC 客户端

Citrix OIDC 客户端密钥的默认有效期为两年。您可以通过轮换客户端密钥来维护 OIDC 安全性，或响应潜在的安全事件。客户端密钥轮换是一项关键的安全措施，必须在现有密钥即将到期时或作为主动安全维护的一部分执行。 每次轮换客户端密钥时，都会生成一个新密钥。旧密钥在其原始到期日期之前仍然有效，以确保平稳过渡而不会导致 SSO 身份验证中断。请务必在每次轮换后尽快使用新客户端密钥更新您的 Google 管理控制台配置。

执行以下步骤轮换客户端密钥

1. 在管理控制台中，单击 **设置 > Open ID Connect (OIDC) 客户端** 页面。
2. 点击 **旋转客户端密钥** 以生成新密钥。将出现确认消息。
3. 启用切换开关以同意确认消息，然后点击 **旋转**。

注意：

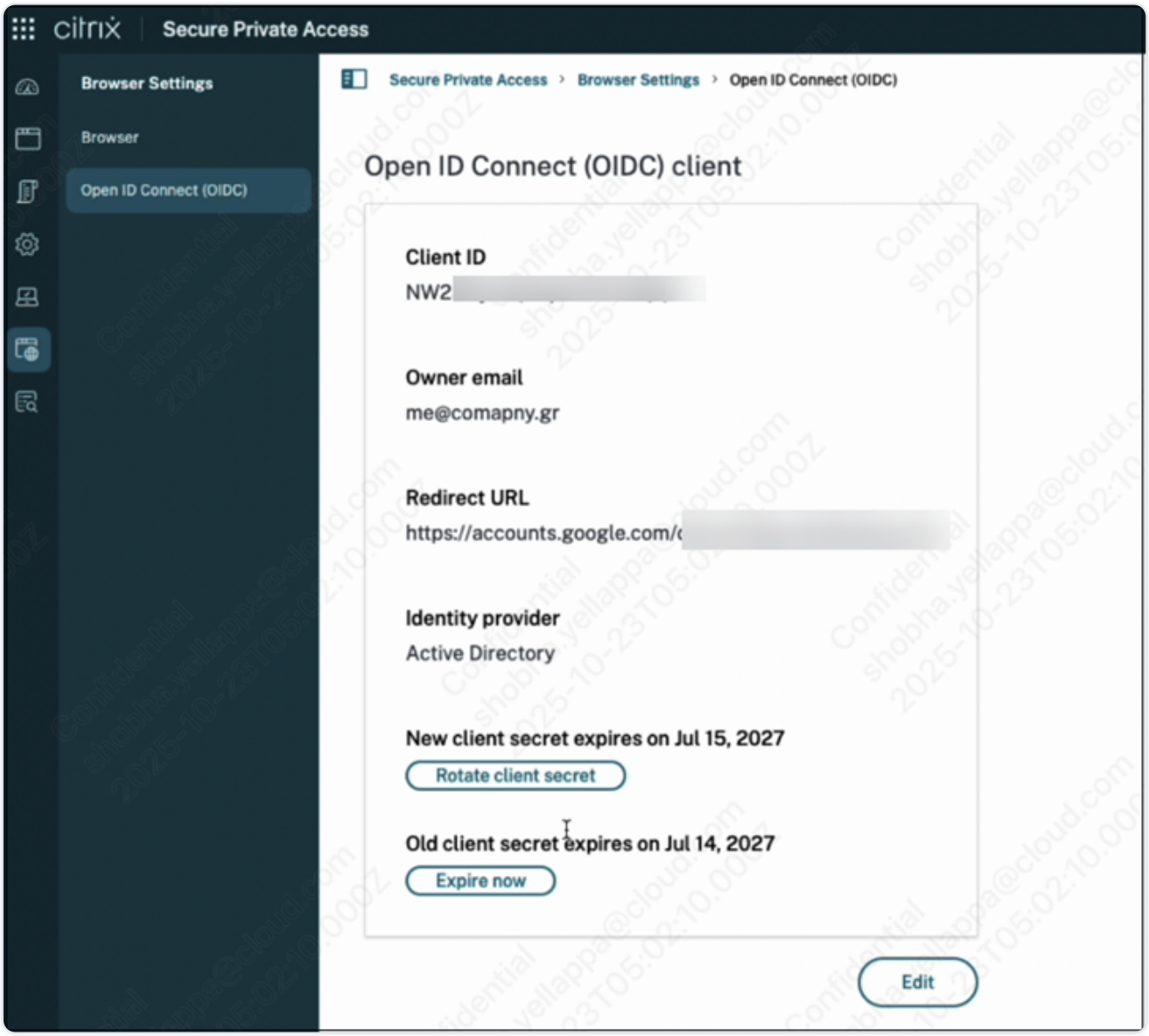
- 旧客户端密钥在其过期之前仍然有效。这使您能够在不中断身份验证的情况下更新 Google Workspace。
- 如果出于安全目的您希望立即使其过期，请点击 **立即过期**。
- 客户端 ID 在此过程中保持不变。

4. 点击 **关闭**。
5. 立即在您的 Google Workspace 配置中更新新密钥。

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

重要提示：

- 您必须在旧密钥过期之前在 Google OIDC SSO 配置文件配置中更新新的客户端密钥，以保持不间断的 OIDC 身份验证。未能及时更新密钥会中断身份验证，并可能导致用户和服务访问问题。
- 建议定期轮换客户端密钥，以降低未经授权的访问风险并维护身份验证系统的完整性。
- 更新 Google OIDC SSO 配置文件的密钥后，建议您使旧密钥过期。



删除 OIDC 客户端

客户端密钥过期后无法轮换。如果客户端密钥在轮换之前过期，它将变为无效。在这种情况下，您必须删除现有客户端并创建一个新客户端。

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

在 Secure Private Admin 控制台中执行以下步骤。

1. 在 Open ID Connect (OIDC) 客户端页面中，单击“**编辑**”。
2. 单击“**删除客户端**”。

   将显示确认消息。
3. 将切换开关滑动到“开”，然后单击“**删除客户端**”。

最终用户体验

用户可以通过以下方法通过 Secure Private Access 访问应用程序。每种访问方法都提供不同的用户体验，组织可以根据其期望的用户体验和部署策略选择最合适的方法。

- **Citrix Workspace 应用程序** - 本机桌面应用程序，提供最安全、功能最丰富的访问体验，具有完整的策略实施和单点登录功能。
- **在 Web 浏览器中存储 URL** - 用户可以在 Web 浏览器中打开其商店：
  - 非 Chrome 浏览器（例如 Firefox、Safari 或 Edge）
  - 具有非托管配置文件的 Chrome（没有企业策略的个人 Chrome 浏览器）
  - 具有托管配置文件的 Chrome（具有 Chrome Enterprise Premium 策略的企业托管 Chrome 浏览器）
- **Chrome 托管配置文件** - 用户通过使用书签或在 Chrome 托管配置文件的地址栏中手动键入应用程序 URL 来直接访问应用程序。

下表总结了使用各种方法访问应用程序时的最终用户体验：

	直接	在 WEB 浏览器中存储 URL	CITRIX WORKSPACE 应用程序
非 Chrome 浏览器	SaaS 应用程序访问被拒绝（假设 SaaS 应用程序已配置适当的 IP 地址允许列表）。	应用程序在用户界面中枚举。	不适用
	私有应用程序无法访问。	应用程序在相应的 Chrome 托管配置文件中启动。	

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

	直接	在 WEB 浏览器中存储 URL	CITRIX WORKSPACE 应用程序
		如果尚未创建相应的托管配置文件，则会启动配置文件创建向导。	
Chrome（非托管配置文件）	SaaS 应用程序访问被拒绝（假设 SaaS 应用程序已配置了相应的 IP 地址允许列表）。	应用程序在相应的 Chrome 托管配置文件中启动。	不适用
	私有应用程序无法访问。	如果尚未创建相应的托管配置文件，则会启动配置文件创建向导。	
Chrome（托管配置文件）	应用程序的允许或拒绝取决于 Secure Private Access 配置。	枚举的应用程序在新选项卡中启动。	不适用
Citrix Workspace 应用程序	不适用	不适用	应用程序在用户界面中枚举。
			应用程序在相应的 Chrome 托管配置文件中启动。
			如果尚未创建相应的托管配置文件，则会启动配置文件创建向导。

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

适用于 Chrome Enterprise Premium 的 Citrix Secure Access 扩展程序

适用于 Chrome Enterprise Premium (CEP) 的 Citrix Secure Access 扩展程序可直接从 Chrome 浏览器安全地无客户端访问内部和外部应用程序。它结合了 Citrix Secure Private Access 和 Chrome Enterprise 功能，可提供企业级安全性、零信任访问、上下文控制和现代用户体验。

组织可以使用此扩展程序提供对 SaaS 应用程序、内部 Web 应用程序、SSH 服务器和 RDP 系统的安全访问，所有这些都无需 VPN 或本机客户端安装。

当您将 Secure Private Access 与 Chrome Enterprise Premium 集成时，Secure Access 浏览器扩展程序会自动安装。有关设置说明，请参阅 设置 Google Chrome 集成。安装后，您可以从 Chrome 浏览器右上角的图标访问该扩展程序。

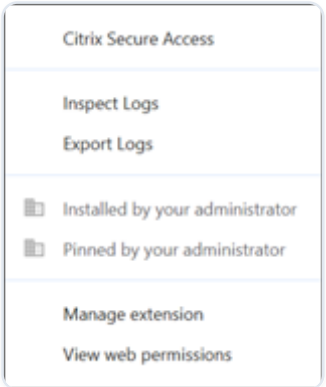


Secure Access 扩展程序日志

Secure Access 浏览器扩展程序日志对于监视和故障排除至关重要。最终用户可以查看和下载日志，以便在出现问题时与管理员或支持团队共享。

要查看或下载日志：

1. 右键单击浏览器扩展程序图标。
    - 单击“**检查日志**”以查看日志。
    - 单击“**导出日志**”以下载日志。



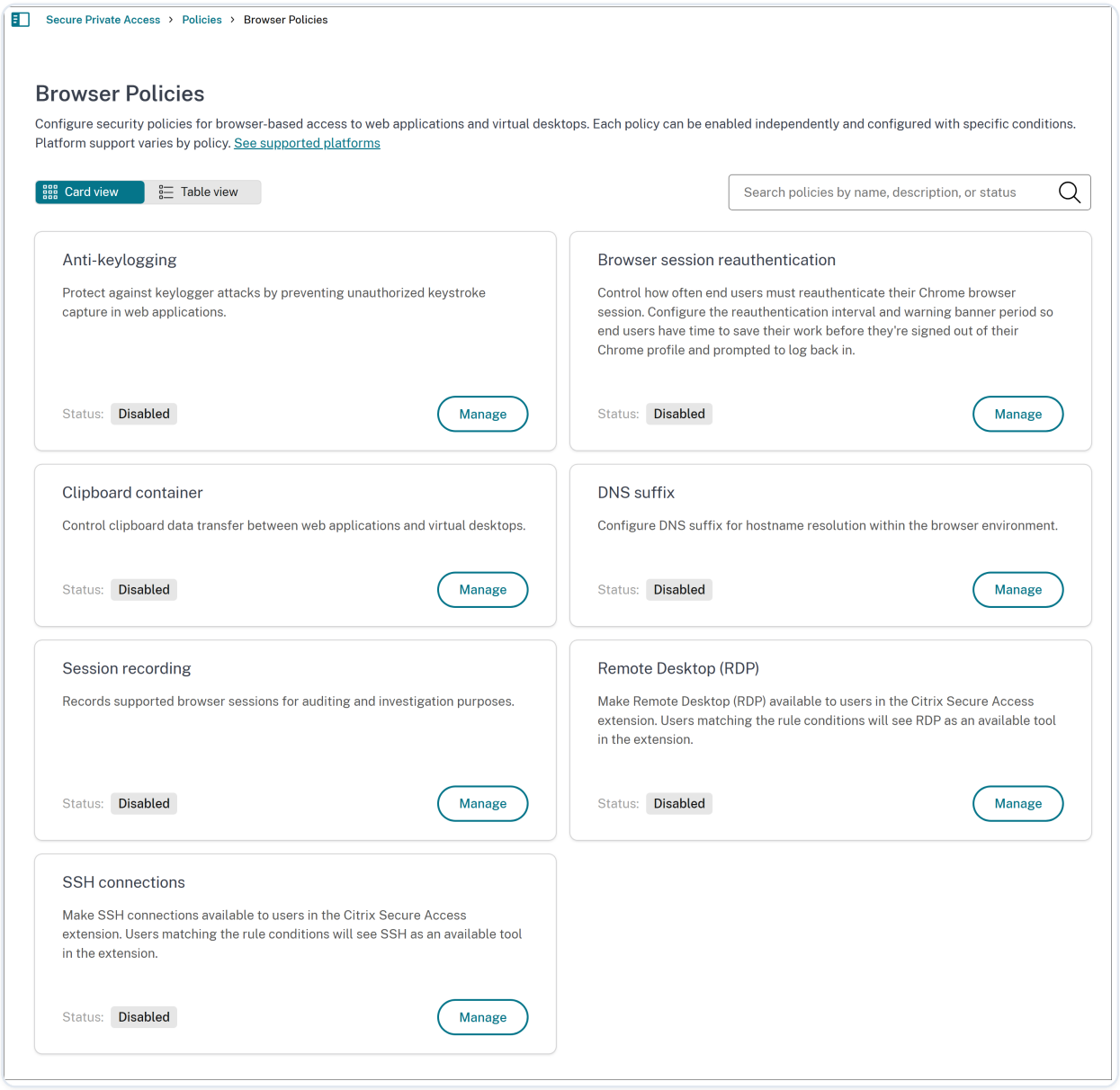
© 1997–2026 Citrix Systems, Inc. All rights reserved.

适用于 Chrome Enterprise 的 Citrix Secure Access 控件

Citrix Secure Private Access 支持由适用于 Google Chrome Enterprise Premium (CEP) 的 Citrix Secure Access 扩展程序交付和强制执行的安全策略。有关详细信息，请参阅 支持的控件。

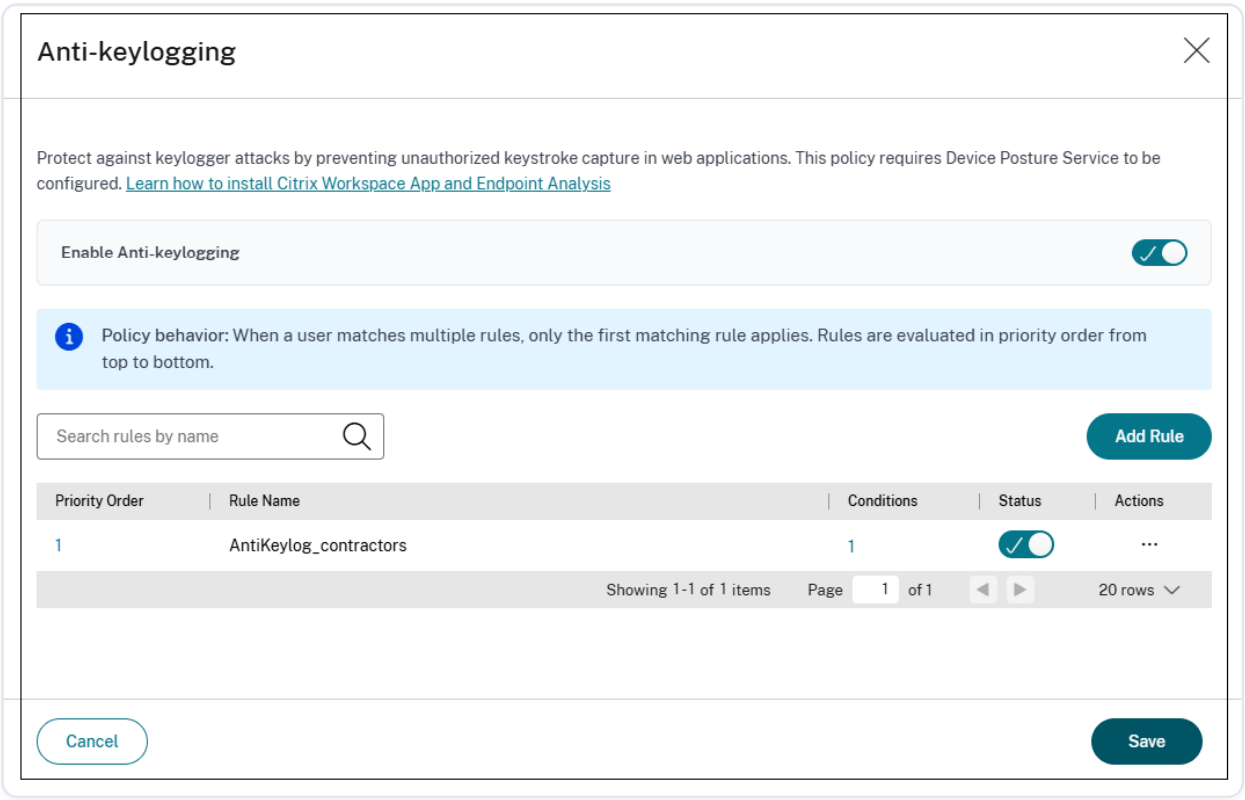
您可以从 Secure Private Access 管理控制台配置这些策略。

1. Go to **策略 > 浏览器策略**，然后点击**创建浏览器策略**。
2. 选择策略，然后点击**管理**。

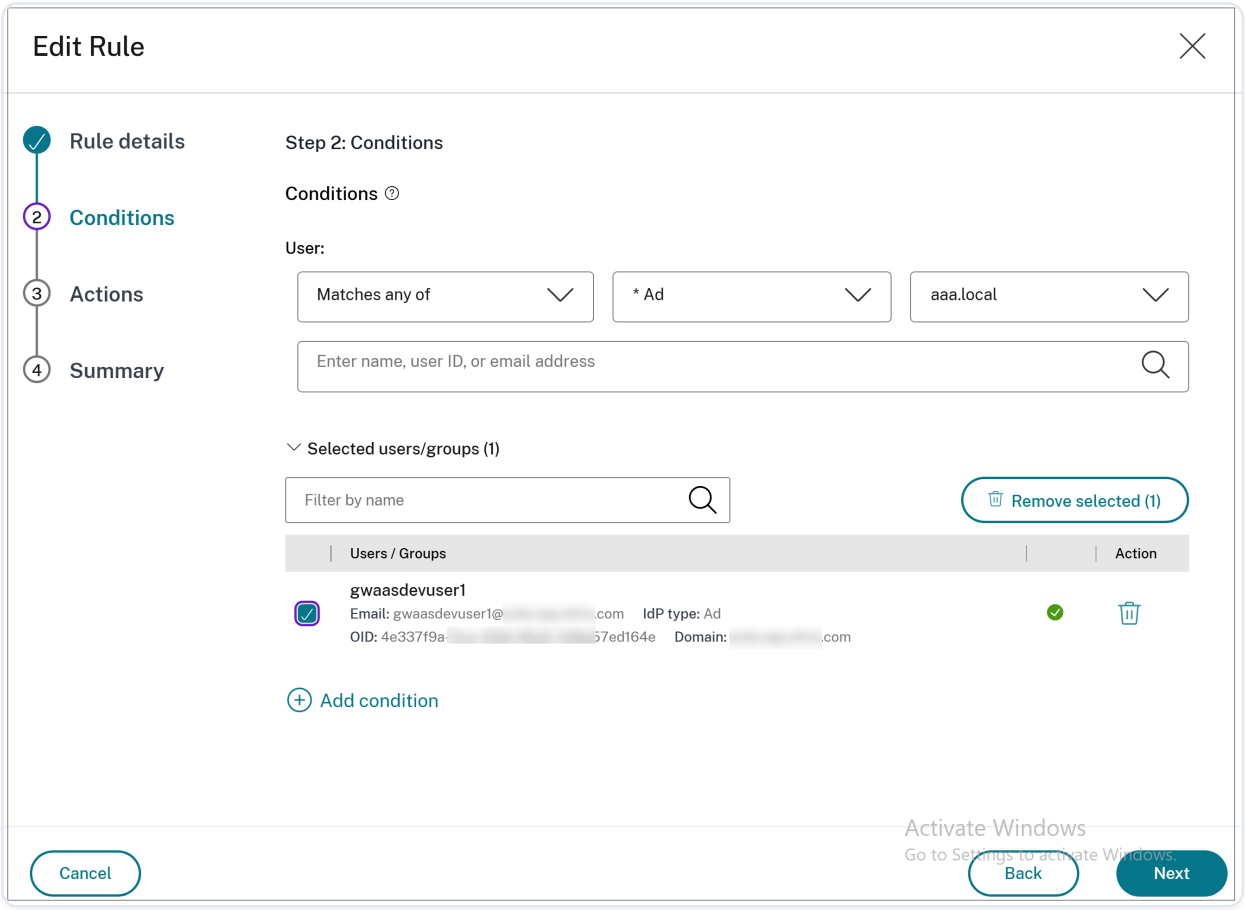


3. 为策略添加规则。

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



4. 添加**访问模式**条件，将浏览器控件限定在浏览器会话中。对于浏览器策略，该值通常为**浏览器**。有关访问模式的更多信息，请参阅基于访问模式的策略实施。
5. 选择必须评估策略的条件。



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

注意：

选择用户或组时，管理员可以验证所选用户目录中的条目是否已与 Google Directory 同步并正确配置。Secure Private Access 策略仅在使用同步的用户和组时才能正确评估。否则，可能会出现警告。有关详细信息，请参阅验证用户和组同步。

有关详细配置步骤，请参阅每个控件的文档。

支持的控件

Citrix 通过 Secure Private Access 和 Chrome Enterprise Premium 集成支持以下安全访问控件：

控件	功能
防键盘记录	混淆击键以防止端点上的键盘记录器恶意软件捕获用户输入。
剪贴板容器	控制用户可以在浏览器和其他应用程序之间复制和粘贴的内容。
DNS 后缀	自动将短内部 URL（如“wiki/”）补全为完整地址。
会话录制	记录浏览器会话活动以进行审计和合规性检查。
浏览器会话重新身份验证	在配置的时间间隔后，强制对浏览器会话进行定期重新身份验证。
SSH 连接	允许用户直接在浏览器选项卡中建立 SSH 连接，而无需终端客户端。
远程桌面 (RDP)	允许用户直接在浏览器选项卡中启动远程桌面会话，而无需 RDP 客户端。

策略中的用户和组

以下部分提供了有关用户和组的更多信息：

搜索用户或组

您选择的用户和组将显示在网格中。网格中的每一行都显示以下身份详细信息，以便您可以清楚地区分不同域、林或身份提供商 (IdP) 中同名用户或组：

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

- **名称** – 用户或组的显示名称。
- **电子邮件** – 与身份关联的电子邮件地址。
- **IDP 类型** – 身份提供商，例如 Azure AD、Active Directory、Okta 或 Google。
- **OID** – 身份的对象 ID 或安全标识符。
- **域** – 用户或组所属的域。

您可以通过名称筛选网格，删除单个行，或者选择多个条目并使用**删除所选**将其一起删除。

使用同步的用户和组

在选择用户或组时，管理员可以验证所选用户目录中的条目是否已与 Google Directory 同步并正确配置。Secure Private Access 策略仅在使用同步的用户和组时才能正确评估。否则，可能会出现以下警告：

- **缺少租户帐户权限。**

  补救措施： 在 Google Admin console 中，将 **Users > Read** 和 **Groups > Read** 权限分配给租户服务帐户。SPA 需要这些权限来验证用户或组是否存在。

- **用户或组未同步。**

  补救措施： 搜索或选定的用户或组未与 Google Directory 同步。在使用目录实体之前，请将其与 Google Directory 同步到 SPA 策略中。

- **组访问设置不足。**

  补救措施： 在 Google 管理控制台中，打开所选组的访问设置，并确保“**谁可以查看成员**”至少选择了“**组成员**”选项。

注意：

此功能仅在 Google Chrome 集成成功完成后可用。

防键盘记录控制

网络犯罪分子使用恶意软件（例如键盘记录器）窃取敏感信息，例如密码、信用卡号和机密公司数据。

适用于 Chrome Enterprise Premium (CEP) 的 Citrix Secure Access 浏览器扩展支持防键盘记录，以帮助保护您的数据。此功能会扰乱击键，这样，如果恶意程序尝试捕获键入的输入，它只会记录不可读的字符，而实际文本会安全地传送到您的工作应用程序。

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

支持的部署： Citrix Secure Private Access 服务和混合部署。

支持的平台： Windows 11 及更高版本。

> **注意：**
>
> 防键盘记录不支持本机 RDP 会话。

先决条件

在启用防键盘记录之前，请确保满足以下先决条件：

- CWA 2603 及更高版本已安装。
- Citrix Secure Access 与 Chrome Enterprise Premium (CEP) 之间的集成已完成。

配置防键盘记录策略

1. 登录到 Secure Private Access 管理控制台。
2. 转到**策略 > 浏览器策略**，然后单击**创建浏览器策略**。
3. 选择**防键盘记录**，然后单击**管理**。
4. 点击 **添加规则** 为用户添加规则以启用防键盘记录功能。
    a. 输入规则名称，然后点击 **下一步**。
    b. 根据您的要求选择条件，例如用户或组。您还可以添加诸如 **地理位置**、**网络位置** 和 **设备状态检查** 等条件。
    c. 点击 **下一步**。
5. 点击 **保存**。

    为防键盘记录策略配置的规则数量显示在 **浏览器策略 > 防键盘记录** 选项卡中。

剪贴板容器控制

使用 Chrome 进行 Web 访问和使用 VDI 进行本机应用程序的部署可以使用剪贴板容器功能来控制浏览器和 VDI 会话之间的数据共享。剪贴板数据在 Citrix 会话之间直接传输，而不会写入本地端点剪贴板。 这提高了安全性，同时仍为用户提供了跨两个环境工作的灵活性。

支持的部署： Secure Private Access 服务和混合部署。

支持的平台： Windows。

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

先决条件

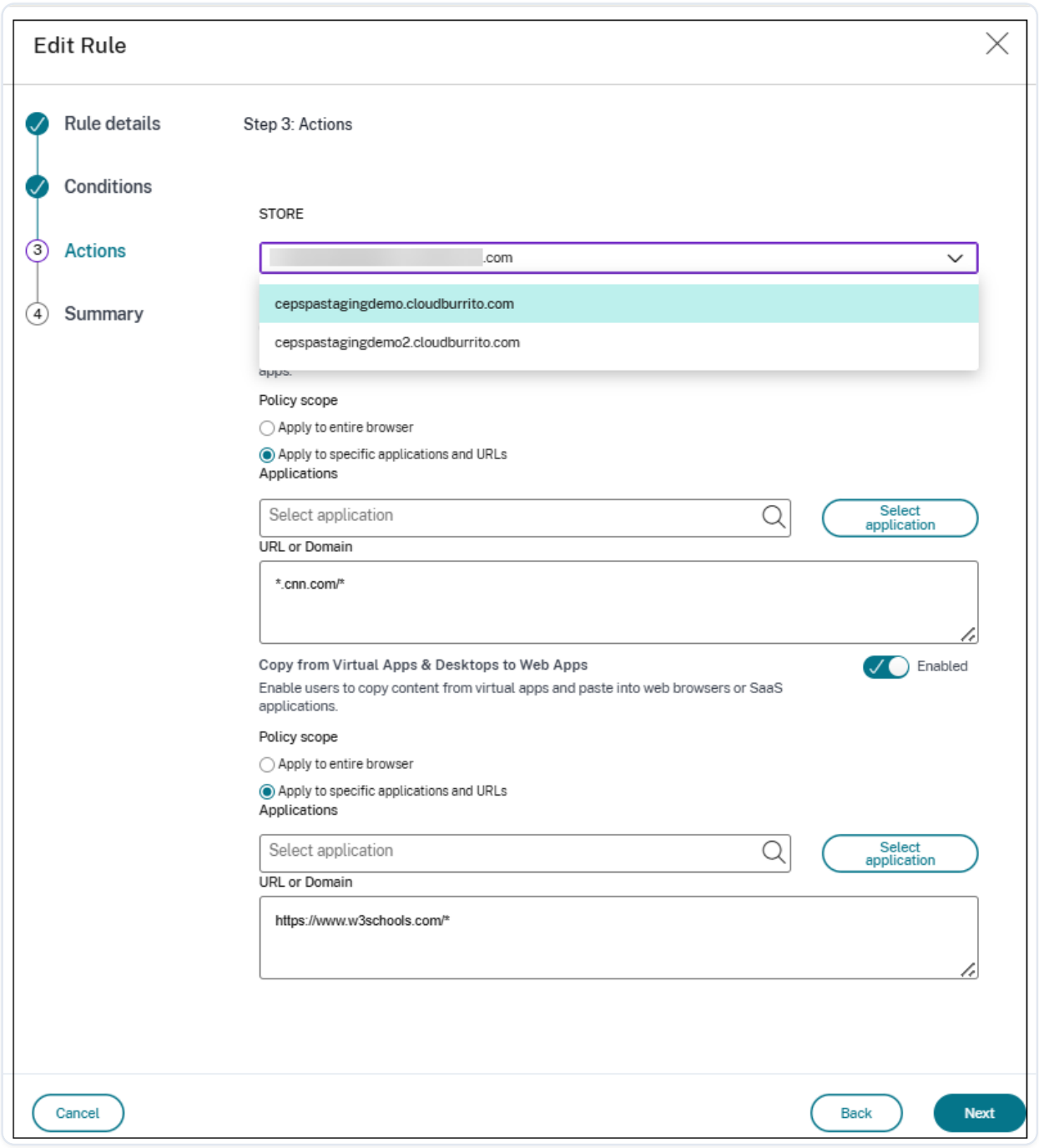
确保满足以下先决条件：

- Citrix Secure Access 和 Chrome Enterprise Premium (CEP) 之间的集成已完成。
- Citrix Workspace 应用程序 2603.10 或更高版本。
- 运行 2607 LTSR 或更高版本的 Windows VDA（Clipboard Sharing Scope 的 GA 版本）。有关详细信息，请参阅 Clipboard Sharing Scope。
- 运行 2507 LTSR 的 Windows VDA（Clipboard Sharing Scope 的预览版本），请启用以下功能：
  - **与 DaaS 交叉剪贴板容器**功能。有关详细信息，请参阅 与 DaaS 交叉剪贴板容器。此功能目前在 DaaS 中作为预览版提供。
  - **剪贴板共享范围**注册表。有关详细信息，请参阅 启用剪贴板共享范围注册表。

启用剪贴板容器控制

1. 登录到 Secure Private Access 管理控制台。
2. 转到 **策略 > 浏览器策略**，然后单击 **创建浏览器策略**。
3. 选择**剪贴板容器**，然后点击**管理**。
4. 点击**添加规则**，为VDA和浏览器之间的剪贴板共享添加规则。
   a. 输入规则名称，然后点击**下一步**。
   b. 根据您的要求选择条件，例如用户或组。您还可以添加**地理位置**、**网络位置**和**设备状态检查**等条件。
   c. 点击**下一步**。
   d. 定义允许剪贴板共享的URL和Secure Private Access应用程序。
   e. 选择策略范围。
   - **应用于整个浏览器** — 该策略管理托管配置文件中的所有剪贴板活动。
   - **应用于特定应用程序和URL** — 该策略仅限于选定的应用程序和输入的URL/域模式。
     - **选择应用程序** — 使用应用程序选择器选择特定的已发布应用程序。
     - **URL或域** - 输入特定应用程序的URL或域。

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



5. 点击**保存**。

为剪贴板容器策略配置的规则数量显示在**浏览器策略 > 剪贴板容器**选项卡中。

启用剪贴板共享范围

适用于 VDA 版本 2607：

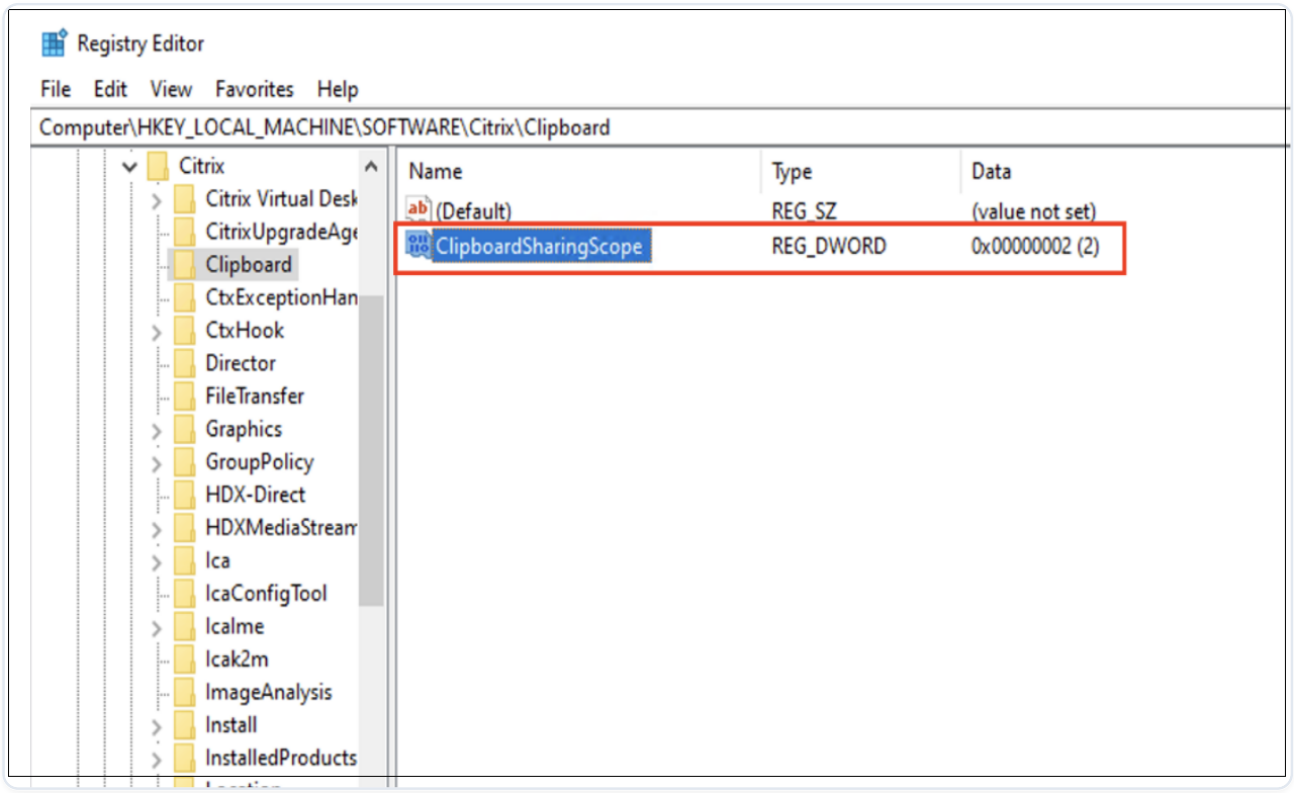
请参阅工作原理。

适用于 VDA 版本 2507：

启用此注册表项 **Clipboard Sharing Scope**。

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

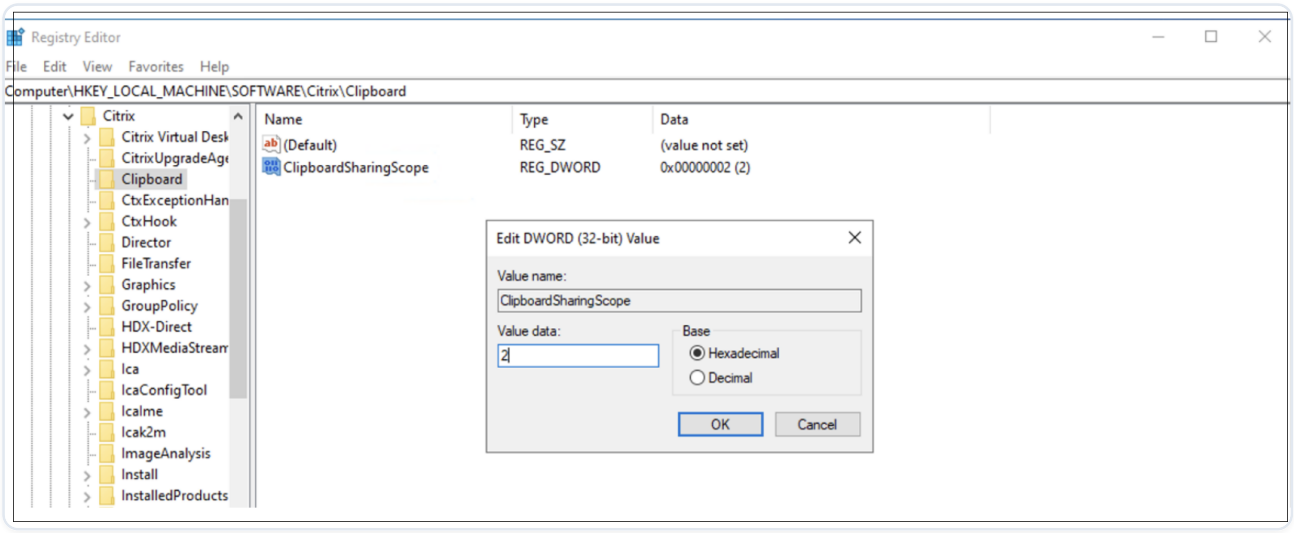
1. 使用 regedit.exe 打开 Windows 注册表编辑器。
2. 导航到 HKEY_LOCAL_MACHINE\Software\Citrix\Clipboard\。
3. 创建一个名为 `ClipboardSharingScope` 的 REG_DWORD 值。



`ClipboardSharingScope` 策略控制 VDA 剪贴板数据可以在何处共享。在新 DDC 策略可用之前，可以使用上述注册表项配置此设置。

支持的值	范围	描述
0	无限制	剪贴板数据将复制到客户端系统剪贴板，并且可以由客户端、VDA 和 CEP 访问。
1	仅 VDA	剪贴板数据仅 VDA 可访问。客户端系统剪贴板和 CEP 无法访问剪贴板内容。
2	仅 CEP	剪贴板数据仅 CEP 可访问。客户端系统剪贴板和 VDA 无法访问剪贴板内容。
3	VDA 和 CEP	剪贴板数据 VDA 和 CEP 均可访问。客户端系统剪贴板无法访问剪贴板内容。

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



注意：

- 仅 CEP (2) 和 VDA 和 CEP (3) 模式旨在与 CEP 扩展中的剪贴板容器功能配合使用。
- 启用剪贴板容器策略后，只有管理员配置的 URL 才能与 VDI 交换剪贴板数据。

```
>-  Content copied from the approved web applications can be pasted into
the VDI.

>-  Content copied from the VDI can be pasted only into administrator-
configured, paste-allowed URLs.

>-  If a user attempts to paste VDI clipboard content into a website that
is not included in the policy, the paste operation is blocked and an error
message appears.
```

Web 应用程序的域后缀

在用户在浏览器中输入简短的内部主机名（例如 `sw` 或 `server001`）的场景中，域后缀功能会自动附加 DNS 后缀，并将其转换为完全限定域名 (FQDN)，使用浏览器管理的 DNS 后缀策略，而不是依赖操作系统的 DNS 后缀配置。

DNS 后缀功能支持 **Windows** 和 **macOS** 平台，并始终适用于常见的 URL 输入格式，包括：

- `sw`
- `http://sw`
- `https://sw/`

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

- `sw/`
- `http://sw/`
- `https://sw/`

支持的部署： Secure Private Access 服务和混合部署。

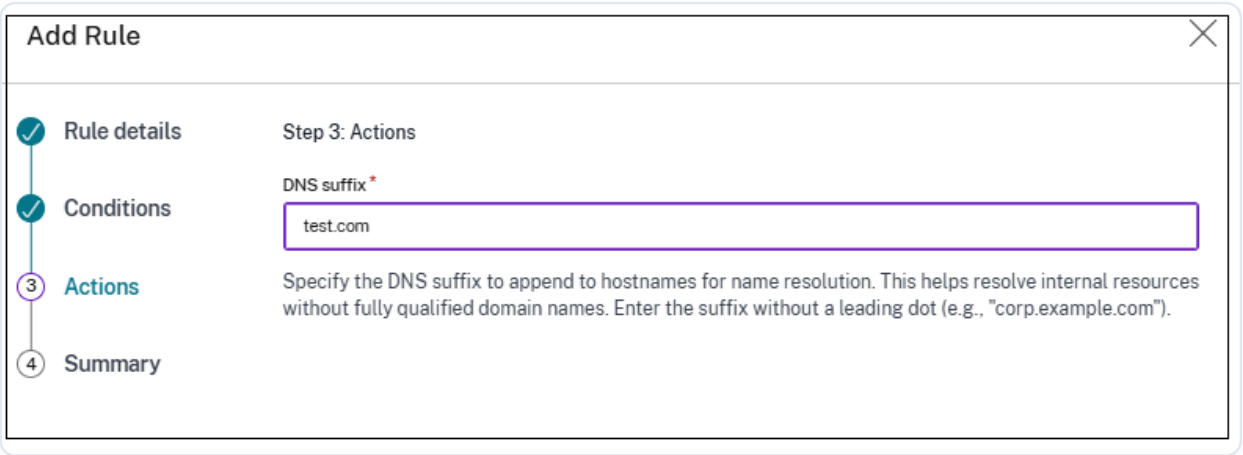
支持的平台： Windows 和 macOS。

先决条件

确保已配置 Citrix Secure Access 与 Chrome Enterprise 的集成。有关详细信息，请参阅 与 Google Chrome Enterprise Premium 集成。

配置 DNS 后缀

1. 登录到 Secure Private Access 管理控制台。
2. a. 转到 **策略 > 浏览器策略**，然后单击 **创建浏览器策略**。
3. 选择 **DNS 后缀**，然后单击 **管理**。
4. 单击 **添加规则**，为要添加到 URL 的域添加规则。
   a. 输入规则名称，然后单击 **下一步**。
   b. 根据您的要求（例如用户或组）选择条件。您还可以添加 **地理位置**、**网络位置** 和 **设备状态检查** 等条件。
   c. 单击 **下一步**。
   d. 定义要附加以进行访问的域。



5. 单击 **保存**。

为 DNS 后缀策略配置的规则数量显示在 **浏览器策略 > DNS 后缀** 选项卡中。

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

会话录制控制

会话录制可记录、编目和存档会话，以便检索和回放。

会话录制提供以下主要优势：

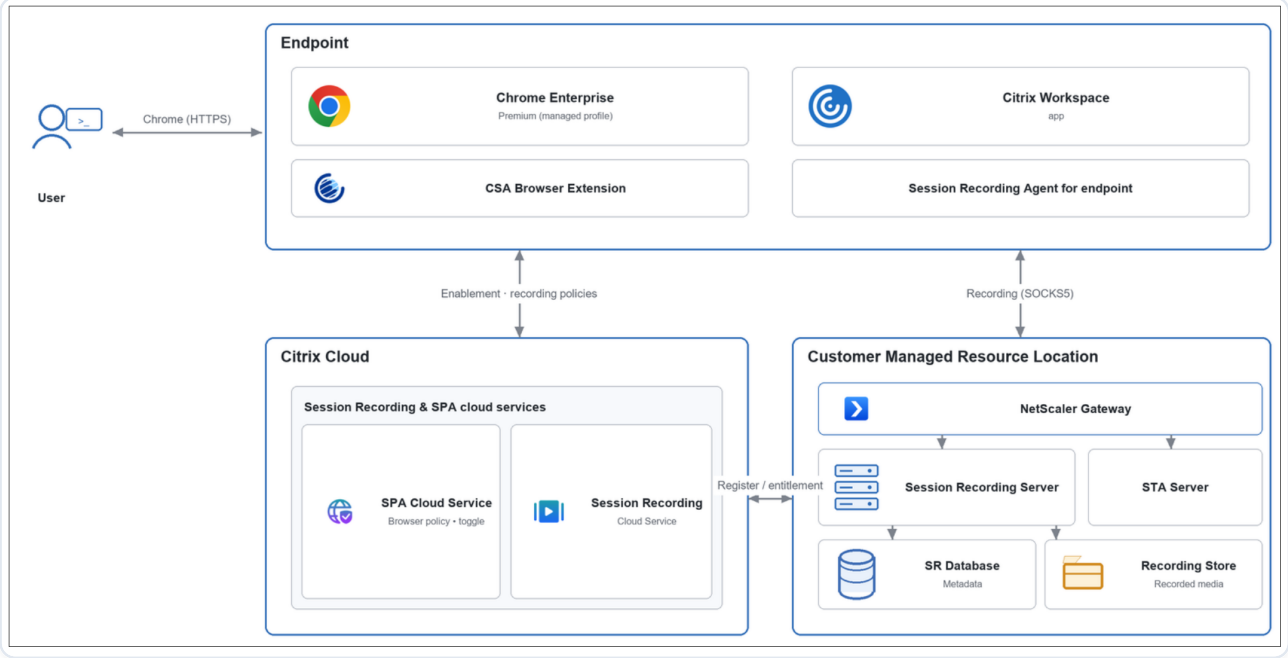
- 提供灵活的策略，可自动触发应用程序和桌面会话的录制。
- 使 IT 人员能够监控和检查用户活动，并支持内部控制以实现法规遵从性和安全监控。
- 通过加快问题识别和缩短解决时间来协助技术支持。

有关详细信息，请参阅优势。

体系结构

会话录制解决方案涵盖三个层面：

- 包含托管 Chrome 配置文件、Citrix Secure Access 扩展和适用于端点的会话录制代理的端点。
- Citrix Cloud 控制平面，其中包含 Secure Private Access 和会话录制云服务。
- 客户管理的资源位置，包括 NetScaler Gateway、STA 服务器、会话录制服务器及其数据库和录制存储。



必备条件

- 适用于 Windows 的 Citrix Workspace 应用程序 2603.10 或更高版本
- 端点分析 (EPA) 版本：26.5.1.7 及更高版本

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

系统要求

- Citrix Secure Private Access，以服务模式或混合模式部署，并结合 Chrome Enterprise Premium（带托管配置文件）。
- 会话录制云服务，使用会话录制服务器 2511 或更高版本。有关详细信息，请参阅入门。
- 具有以下组件的 Windows 64 位或 32 位端点：
  - Citrix Endpoint Analysis (EPA) 插件 26.5.1.7 或更高版本。
  - 适用于 Windows 的 Citrix Workspace 应用程序，版本 2603.10 或更高版本，并安装了会话录制端点代理

设置环境

完成以下步骤以启用和验证 Chrome Enterprise 会话的端点录制。

配置会话录制站点

按照配置端点录制策略中记录的步骤进行操作。

> **注意：**
>
> 端点录制需要 NetScaler Gateway。它在两种 Secure Private Access 部署类型中都通过 STA 将录制流量路由到会话录制服务器。即使在使用 Secure Private Access 服务（其中 NetScaler 不管理用户到应用程序的访问）的情况下，您也必须为录制流量提供网关 URL。

在 Secure Private Access 中配置会话录制浏览器策略

1. 登录 Secure Private Access 管理控制台。
2. 转到 **策略 > 浏览器策略**，然后单击 **创建浏览器策略**。
3. 选择 **会话录制**，然后单击 **管理**。
4. 单击 **添加规则**，输入规则名称，然后单击 **下一步**。
5. 设置条件（用户和组）。（可选）添加 **地理位置**、**网络位置** 和 **设备状态检查**，然后单击 **下一步**。
6. 单击 **保存**。规则计数显示在 **浏览器策略 > 会话录制** 选项卡上。

为端点安装带会话录制代理的 Workspace 应用程序

请按照 会话录制附加组件支持 中记录的步骤操作。

回放录制的会话

录制内容可在会话录制控制台中查看。

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

- 与用户的 Chrome 工作配置文件关联的所有窗口都将被录制。
- 跨一个或多个显示器的多个窗口都将被录制。
- 失焦的窗口或被其他应用程序遮挡的窗口仍将完整录制。
- 最小化的窗口以及启用了防屏幕捕获的窗口在回放期间显示为黑色矩形。

最佳实践

- **保留一个全局站点**。使用单个全局端点录制站点并记录配置。更改它可能会无意中禁用其他站点的已配置策略。
- **区域对齐**。将会话录制云服务 URL、云客户端和后端保留在同一 Citrix Cloud 区域中，以避免延迟和数据驻留问题。
- **规划存储**。全屏 Web/SaaS 录制可能会占用大量存储空间。相应地调整服务器、会话录制数据库和录制存储的大小，并密切监控存储消耗。
- **首先验证授权和角色**。Citrix DaaS 和 Citrix Secure Private Access 授权不匹配是部署失败最常见的原因。在启用策略之前，请确认存在单个活动的客户记录，并且已分配所需的管理角色。

浏览器会话重新身份验证控制

Citrix Secure Private Access 允许管理员对 Chrome Enterprise Premium (CEP) 浏览器会话实施会话超时策略。用户需要在配置的会话持续时间后重新进行身份验证，无论浏览器活动如何。这增强了通过 Google Chrome 工作配置文件访问的应用程序的零信任访问控制。

会话过期后，用户必须使用企业凭据和多重身份验证 (MFA) 重新进行身份验证。重新身份验证成功后，将恢复他们上次活动的页面并重新启动会话计时器。

支持的部署： Secure Private Access 服务和混合部署。

支持的平台： Windows、macOS、Linux、ChromeOS。

先决条件

确保满足以下先决条件：

- Citrix Secure Access 和 Chrome Enterprise Premium (CEP) 之间的集成已完成。

启用浏览器会话重新身份验证控制

1. 登录 Secure Private Access 管理控制台。
2. 转到**策略 > 浏览器策略**，然后单击**创建浏览器策略**。
3. 选择**浏览器会话重新身份验证**，然后单击**管理**。

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

4. 单击**添加规则**以添加规则来启用浏览器会话重新身份验证。

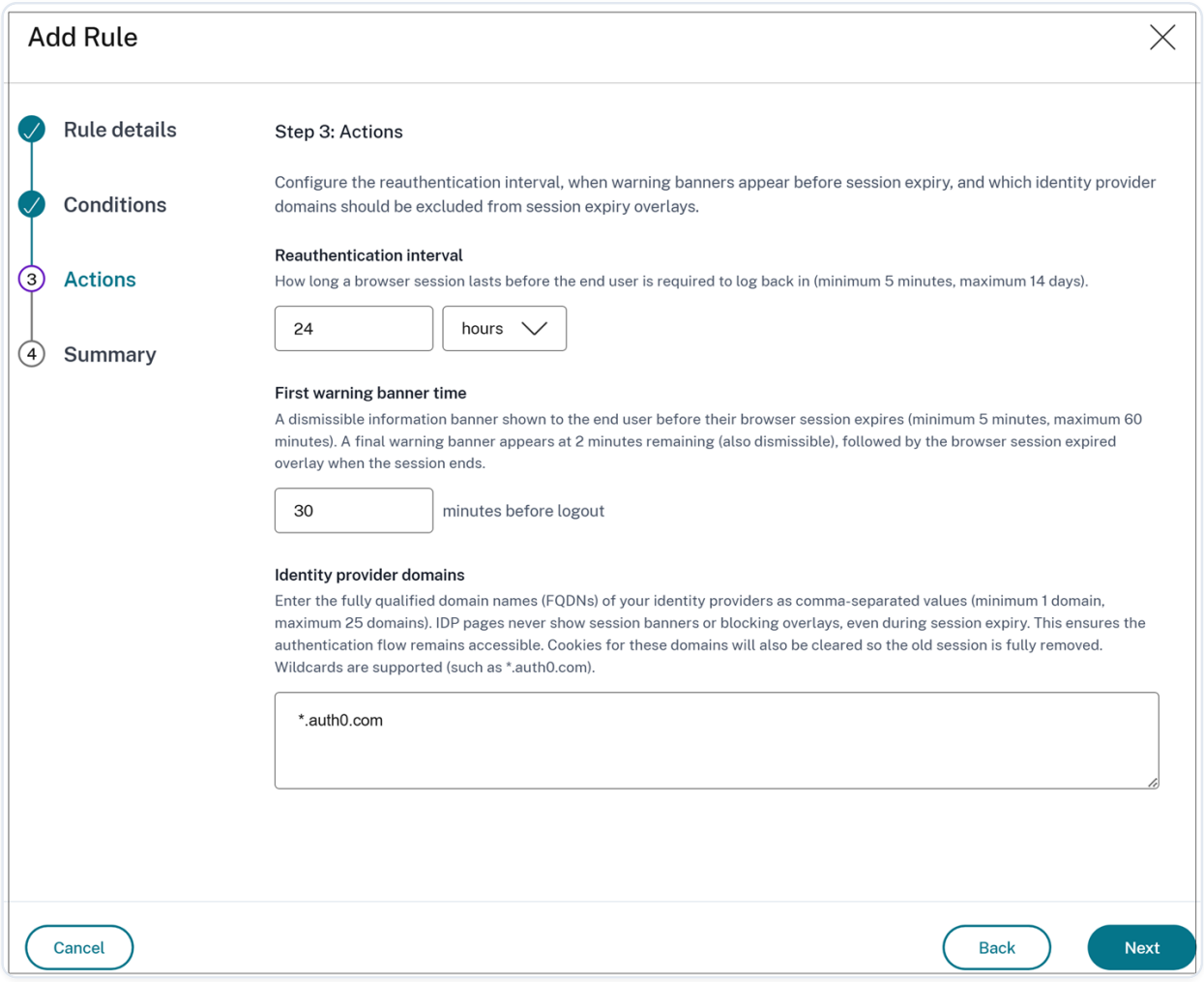
   a. 输入规则名称，然后单击**下一步**。

   b. 根据您的要求选择条件，例如用户或组。您还可以添加诸如**地理位置**、**网络位置**和**设备态势检查**等条件。

   c. 点击 **下一步**。

   d. 配置以下内容：

- **重新身份验证间隔**：用户需要重新进行身份验证之前浏览器会话的持续时间。间隔可以设置为 5 分钟到 14 天，并以分钟、小时或天为单位进行配置。
- **首次警告横幅时间**：在浏览器会话过期之前向用户显示的可关闭警告横幅。该值可以在过期前 5 到 60 分钟之间设置。当剩余 2 分钟时，会出现第二个警告横幅；会话结束时，会出现会话过期叠加层。
- **身份提供程序域**：您的身份提供程序的完全限定域名 (FQDN)，以逗号分隔值表示。您可以指定 1 到 25 个域。在 IdP 页面上会抑制会话横幅和阻止叠加层，以确保身份验证流程不中断。当会话过期时，这些域的 Cookie 将被清除，以确保旧会话完全移除。支持通配符（例如，*.auth0.com）。



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

5. 点击 **下一步**，然后点击 **保存**。

   为剪贴板容器策略配置的规则数量显示在 **浏览器策略 > 浏览器会话重新身份验证** 选项卡中。

SSH 控制

Citrix Secure Private Access 与 Chrome Enterprise Premium 集成，以实现在浏览器内直接进行安全的 SSH 会话。这种集成增强了安全性，并简化了管理员和用户的访问。

组织需要对基于 SSH 的系统进行安全的远程管理。使用独立 SSH 客户端的传统方法通过将端点暴露给非托管环境而带来风险，并且缺乏强大的数据丢失防护 (DLP) 强制执行，使合规性变得具有挑战性。

SSH 会话现在在 Chrome 浏览器中启动，而不是使用独立的 SSH 客户端，这减少了对本地安装的依赖，并提高了合规性。

注意：

- 此功能适用于集成了 Chrome Enterprise Premium 的 Secure Private Access 设置，用于混合和云部署。有关详细信息，请参阅以下主题：
- 您必须拥有管理员权限才能配置 Secure Private Access 和 Chrome Enterprise Premium 策略。
- 不支持连接到 FreeBSD 服务器。

此集成的优势

此集成提供以下主要优势：

- **增强安全性：** 消除了对非托管 SSH 客户端的依赖，降低了安全风险。
- **简化访问：** 提供浏览器原生访问，无需额外安装软件。
- **合规性：** 直接在浏览器内强制执行企业 DLP 策略，有助于满足法规要求。
- **运营效率：** 降低了与端点管理和客户端部署相关的 IT 开销。

用例

此功能支持多种用例，例如：

- **医疗自助服务终端：** 无需安装本机客户端即可实现安全的 SSH 访问，用于设备故障排除。
- **IT 管理：** 允许管理员从受管理的 Chrome 浏览器安全地访问 Linux 服务器，并强制执行 DLP 策略。

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

- **承包商访问：** 为第三方供应商提供临时 SSH 访问，而不会损害组织的安全态势。

系统要求

确保您的环境满足以下要求：

- 最新版本的 Chrome Enterprise Premium。
- Citrix Secure Private Access 已配置为集成。
- 必须在 Secure Private Access 管理控制台中创建允许 SSH 流量的访问策略。

先决条件

确保满足以下先决条件，以启用对 SSH 应用程序的安全访问：

- Citrix Secure Private Access 已配置 Google Chrome Enterprise Premium 集成。有关详细信息，请参阅 与 Google Chrome Enterprise Premium 集成。
- 最终用户已安装最新版本的 Google Chrome 浏览器以及 Citrix Secure Access 浏览器扩展。
- 有关部署特定的先决条件，请参阅以下主题：
  - 云部署 - Citrix Secure Private Access 入门
  - 混合部署 – 系统要求和必备条件

配置安全专用访问以进行 SSH 访问

1. 登录到 Citrix Cloud，然后单击**安全专用访问**。
2. 在管理控制台中，单击**应用程序 > 应用程序配置**，然后单击**添加应用程序**。
3. 在安全专用访问中将 SSH 应用程序配置为 TCP/UDP 应用程序。
   - 该应用程序可以具有服务器的精确 IP 地址或范围、FQDN 或主机名。
   - 支持通过默认端口和非默认端口使用 SSH。
4. 将访问权限分配给相关用户组。

有关创建 TCP/UDP 应用程序的详细信息，请参阅以下主题。

- 云部署 - 对 TCP/UDP 应用程序的支持
- 混合部署 – 对 TCP/UDP 应用程序的支持

配置 SSH 策略

1. 登录到安全专用访问管理控制台。
2. 转到**策略 > 浏览器策略**，然后单击**创建浏览器策略**。

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

3. 选择**SSH**，然后单击**管理**。
4. 点击 **添加规则** 为用户添加规则以启用 SSH。
5. 输入规则名称，然后点击 **下一步**。
6. 根据您的要求选择条件，例如用户或组。1. 您还可以添加条件，例如 **地理位置、网络位置** 和 **设备姿态检查**。
7. 点击 **下一步**。
8. 点击 **保存**。

为防键盘记录策略配置的规则数量显示在 **浏览器策略 > SSH** 选项卡中。

远程桌面控制

Citrix Secure Private Access 与 Chrome Enterprise Premium 集成，可在浏览器中直接启用安全的 RDP 会话。此集成增强了管理员和用户的安全性并简化了访问。

传统的远程桌面访问通常依赖于本机 RDP 客户端，这些客户端通常缺乏基于浏览器的 DLP 强制执行。这种缺陷会增加安全风险，尤其是在非托管环境中，并使合规性变得具有挑战性。组织需要一个安全、合规且简化的远程访问解决方案来解决这些问题。

此集成使管理员能够强制执行企业级 DLP 控制，例如剪贴板控制和屏幕截图预防。

注意：

- 此功能适用于混合和云部署的 Chrome Enterprise Premium 集成 Secure Private Access 设置。有关详细信息，请参阅以下主题：
- 您必须拥有管理员权限才能配置 Secure Private Access 和 Chrome Enterprise Premium 策略。

不支持的功能：

不支持以下功能：

- 剪贴板共享
- 音频/网络摄像头/智能卡/USB 重定向
- 双因素和生物识别身份验证

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

此集成的优势

此集成提供以下主要优势：

- **安全性：** 通过强制执行精细的 DLP 策略，防止远程会话期间的数据泄露。
- **合规性：** 通过强大的安全控制，帮助满足敏感环境的法规要求。
- **易用性：** 无需安装单独的 RDP 客户端，简化了用户访问和部署。
- **灵活性：** 支持从托管的 Chrome 浏览器安全访问 RDP，提供一致且安全的体验。

用例

此功能支持各种用例，例如：

- **企业承包商：** 为第三方供应商提供安全的远程桌面访问，同时不损害内部安全性。
- **医护人员：** 允许在医疗环境中从自助服务终端或共享工作站安全访问 Windows 系统。
- **IT 支持：** 允许 IT 人员对远程桌面进行故障排除，而无需安装额外的软件。

系统要求

确保您的环境满足以下要求：

- 最新版本的 Chrome Enterprise Premium。
- Citrix Secure Private Access 已配置为集成。
- 必须在 Secure Private Access 管理控制台中创建允许 RDP 流量的访问策略。

先决条件

确保满足以下先决条件，以启用对 RDP 应用程序的安全访问：

- Citrix Secure Private Access 已配置 Google Chrome Enterprise Premium 集成。有关详细信息，请参阅 与 Google Chrome Enterprise Premium 集成。
- 最终用户已安装带有 Citrix Secure Access 浏览器扩展的最新 Google Chrome 浏览器。
- 有关部署特定的先决条件，请参阅以下主题：
  - 云部署 - Citrix Secure Private Access 入门
  - 混合部署 – 系统要求和先决条件

配置 Secure Private Access 以进行 RDP 访问

1. 登录 Citrix Cloud，然后单击 **Secure Private Access**。
2. 在管理控制台中，单击 **应用程序 > 应用程序配置**，然后单击 **添加应用程序**。

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

3. 将 RDP 应用程序配置为 Secure Private Access 中的 TCP/UDP 应用程序。
    - 该应用程序可以具有服务器的精确 IP 地址或范围、FQDN 或主机名。
    - RDP 支持默认端口和非默认端口。
4. 将访问权限分配给相关的用户组。

有关创建 TCP/UDP 应用程序的详细信息，请参阅以下主题。

- 云部署 - 支持 TCP/UDP 应用程序
- 混合部署 – 支持 TCP/UDP 应用程序

配置远程桌面策略

1. 登录到 Secure Private Access 管理控制台。
2. 转到 **策略 > 浏览器策略**，然后单击 **创建浏览器策略**。
3. 选择 **远程桌面**，然后单击 **管理**。
4. 单击 **添加规则** 为用户添加规则以启用远程桌面。
5. 输入规则名称，然后单击 **下一步**。
6. 根据您的要求选择条件，例如用户或组。 1. 您还可以添加条件，例如 **地理位置、网络位置** 和 **设备姿态检查**。
7. 单击 **下一步**。
8. 单击 **保存**。

为防键盘记录策略配置的规则数量显示在 **浏览器策略 > 远程桌面** 选项卡中。

排查 CEP 集成问题

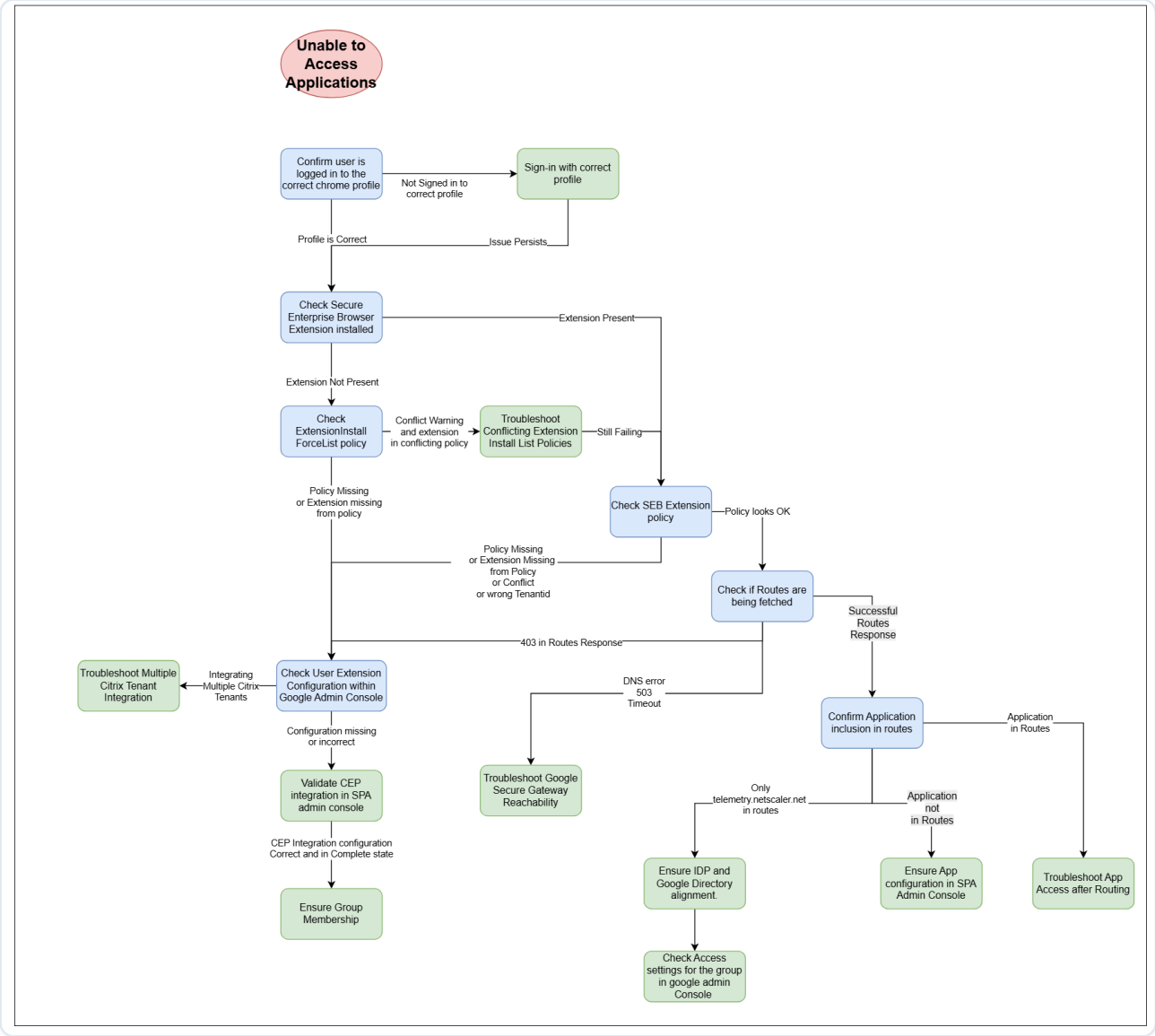
本文提供了一个故障排除工作流，面向已完成 Chrome Enterprise Premium (CEP) 与 Citrix Secure Private Access 集成但无法访问应用程序的客户管理员。

基本假设：

- 客户管理员已完成与 Google Directory 的目录同步。
- 客户已在 Secure Private Access 中成功完成 Chrome Enterprise 入门。
- 应用程序和访问策略已在 Secure Private Access 管理控制台中配置，以允许用户或用户所属的组访问相关应用程序。
- 用户正在登录已载入的域。

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

- 浏览器具有互联网连接。



用于 CEP 故障排除的诊断日志

为了简化调查，请在提交支持案例之前收集以下诊断信息，并在每次提交时附上。

1. 导出 Chrome 策略。
   a. 打开 Chrome 并导航到 chrome://policy/。
   b. 单击**更多操作**，然后选择**导出为 JSON**。
   c. 将导出的文件附加到您的支持案例。
2. 启用 Secure Enterprise Browser 扩展程序的详细日志记录。
   a. 单击 Secure Enterprise Browser 扩展程序旁边的省略号图标。
   b. 单击选项，然后将 **日志级别** 设置为 **所有**。

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

c. 关闭并重新打开 Chrome。

d. 返回扩展程序选项（省略号图标），然后单击 **下载日志**。

3. 收集扩展程序日志。

a. 关闭并重新打开 Chrome。

b. 重复步骤 2 以访问 **扩展程序** 选项，然后单击 **下载日志**。

c. 将下载的文件附加到您的支持案例。

4. 捕获网络日志。

a. 在 Chrome 中，导航到 chrome://net-export/，然后单击 **开始记录到磁盘**（默认文件名为 chrome-net-export-log.json）。

b. 访问一些 SaaS 和 Web 应用程序，然后返回 chrome://net-export/ 并单击 **停止记录**。

c. 将生成的文件附加到您的支持案例。

确认用户已登录到正确的 Chrome 配置文件

如何检查： 在 Chrome 浏览器的右上角，单击个人资料图标。它必须显示您打算通过其访问应用程序的配置文件的正确用户和正确域。

另外，请确保配置文件未显示“**已暂停**”或“**单击以登录**”。如果显示，则必须重新进行身份验证。

- **配置文件正确且已通过身份验证：** 继续执行检查 Secure Enterprise Browser 扩展是否已安装。
- **配置文件不正确或未通过身份验证：** 使用正确的配置文件登录或重新进行身份验证。确保用户电子邮件的域后缀与安装了 Secure Private Access 的 Google 管理员帐户的域一致。

检查 Secure Enterprise Browser 扩展是否已安装

如何检查： 在 Chrome 浏览器的右上角，必须有一个与 Secure Enterprise Browser 扩展对应的绿色盾牌图标。您可能需要单击拼图图标才能看到所有扩展。

- **扩展程序存在：** 继续执行检查 Secure Enterprise Browser 扩展策略。
- **扩展程序不存在：** 继续执行检查 ExtensionInstallForcelist 策略。

检查 ExtensionInstallForcelist 策略

如何检查： 导航到 chrome://policy，然后在“**Chrome 策略**”下查找名为 **ExtensionInstallForcelist** 的策略。单击相应行末尾的“**显示更多**”以查看策略详细信息。

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

在此强制列表中，您应该会看到一个 ID 为 `ekajlcmdfcigmdbphhifahdfjbkciflj` 的扩展程序。这对应于 Secure Enterprise Browser 扩展。

您可能会看到一条警告，提示存在两个冲突的策略。

- **冲突警告和冲突策略中的扩展程序：** 继续执行排查冲突的扩展程序安装列表策略。
- **策略缺失：** 策略完全缺失表明用户未配置为使用 Secure Enterprise Browser，您必须检查 Google 管理控制台中的用户扩展程序配置。
- **策略中缺少扩展程序：** 继续执行检查 Google 管理控制台中的用户扩展程序配置。

排查冲突的扩展程序安装列表策略

冲突的策略不一定是支持 CEP 与 Secure Private Access 的障碍。但是，有效策略必须强制安装以下三个扩展：

- 安全企业浏览器 (`ekajlcmdfcigmdbphhifahdfjbkciflj`)
- Citrix 安全访问 (`loifegnemklkgbmonigcdkmniboielgl`)
- 端点验证 (`callobklhcbilhphinckomhgkigmfocg`)

要解决 Secure Private Access 的扩展策略冲突，请根据 Chrome Policy Hierarchy Guide 遵循以下步骤。

1. **识别冲突：** 导航到 `chrome://policy`。找到 **ExtensionInstallForcelist** 并检查 **Status** 和 **Source**。
2. **分析优先级：** 请注意，机器级策略 (GPO) 通常会取代云/用户级策略。
3. **协调：** 确保最高优先级的策略包含所有三个必需的扩展 ID（如果包含其他扩展，则没有问题）。或者，如果浏览器和配置文件由同一个 Google Workspace 组织管理，则可以使用策略合并功能。
4. **验证：** 单击 **Reload policies**。“**Applies to**”和“**Level**”列必须确认所需的扩展是 **Mandatory** 且在有效级别处于活动状态。

如果在更正扩展安装列表策略后问题仍然存在，请继续执行 Check Secure Enterprise Browser Extension policy。

检查 Secure Enterprise Browser 扩展策略

如何检查： 导航到 chrome://policy 并在 **Secure Enterprise Browser** 下查找名为 **securityGateway** 的策略。单击 **Show More** 以显示完整的策略配置。其值应具有以下格式：

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

```
{

  "authentication": {},

  "context": {

    "resource": "projects/project-<tenant_id>-<random-hex-characters>/
locations/global/securityGateways/securitygateway-<tenant_id>-<random-hex-
characters>"

  },

  "externalHelper": {

    "id": "com.citrix.device_posture_context_provider",

    "metadata": {

      "action": "device/metadata",

      "input": [

        {

          "key": "tenantId",

          "stringValue": "<tenant_id>"

        }

      ]

    }

  },

  ...

}
```

确保 `tenant_id` 字段的值与您的 Citrix Cloud 租户 ID 对应。如果此值不同，则可能是配置了第二个租户以与此 Google 帐户集成。

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

- **策略缺失或为空：** 策略完全缺失表明 Secure Enterprise Browser 扩展不仅由 Secure Private Access 配置，而且也由客户配置，并且用户正在从以前或手动配置中获取扩展的空配置。您必须 Check user extension configuration within Google Admin Console。
- **策略填充了错误的 Citrix 租户 ID：** 如果策略存在但值与示例不符，则租户 ID 不同或存在两个冲突的策略。继续执行 Check user extension configuration within Google Admin Console。
- **策略看起来正确：** 请继续检查路由是否正在获取。

检查 Google 管理控制台中的用户扩展配置

如何检查： 导航到 https://admin.google.com。在此处，转到 **Chrome 浏览器 > 应用和扩展程序**。在此视图中，您必须找到所有正在应用的策略配置。

单击“**概览**”选项卡（如果存在）并选择 **Secure Enterprise Browser** 应用程序。在左侧，“**安装策略**”下必须显示“**在 \<primary domain\> 中强制安装并固定**”，其中 \<primary domain\> 对应于您的 Google 管理控制台的顶级组织单位。

单击以查看扩展程序“**部署设置**”时，查找“**扩展程序策略**”配置。这必须与检查 Secure Enterprise Browser 扩展策略部分中描述的内容一致。

- **看起来正确的单一策略：** 如果父 OU 的策略看起来正确，您必须确保您正在测试的用户属于相关帐户，并且在子 OU 或组级别没有其他配置可能覆盖父 OU 的策略。如果成员资格已确认但问题仍然存在，请联系 Citrix 支持。
- **策略缺失：** 策略完全缺失表明此 Google 帐户未配置为使用 Secure Enterprise Browser，并且您必须在 Secure Private Access 管理控制台中验证 CEP 集成。
- **多个策略 - 多个 Citrix 帐户：** 如果您看到 Secure Enterprise Browser 扩展的多个配置，则这可能是关联策略配置不正确的原因。将多个 Citrix 帐户关联到同一个 Google 帐户并非禁止，但可能会导致集成无法正常工作。
- **多个策略 - 单个 Citrix 帐户：** 如果您只集成了一个 Citrix 租户，则必须确保组织中没有其他管理员功能可能正在配置此扩展。如果您确信没有其他人为此扩展提供策略配置，则可以继续删除那些与您通过 Secure Private Access 管理控制台集成的 Citrix 租户不对应的策略配置。

  如果您删除了多余的扩展配置，并且在重新启动浏览器后仍然无法访问您的应用程序，请联系 Citrix 支持。

检查路由是否正在获取

如何检查： 导航到 chrome://extensions/?options=ekajlcmdfcigmdbphhifahdfjbkciflj 或右键单击 Secure Enterprise Browser 扩展并选择“**选项**”。

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

将日志级别设置为“**ALL**”并单击“**SHOW LOG**”。日志显示后，关闭浏览器并重复此过程以转到日志页面。这可确保您已检索到故障排除所需的完整日志集。

在日志中，搜索包含以下内容的日志行：

`Calling 'https://api.prod.securegateway.goog/api/v1/routes'`

之后必须有如下响应：

`[260220 17:07:51.64] [SG.ApiClient] [DEBUG] Response: {expirationTime: '2026-02-20T15:37:51Z', proxyUrl: 'https://api.prod.securegateway.goog',...`.

- **上下文路由在日志中显示 403 状态代码：** 此 403 错误可能由 Zscaler、Umbrella 等拦截防火墙返回。
  - 在这种情况下，请确保允许发往 Google 安全网关的流量，如集成解决方案的必备条件中所述。
  - 如果不是，则可能是用户配置文件存在身份验证问题，并且可能意味着 Secure Private Access 与 CEP 的集成不完整。请继续执行在 Secure Private Access 管理控制台中验证 CEP 集成。
- **上下文路由显示超时、DNS 错误或 503 错误：** 请继续执行排查 Google 安全网关可达性问题。
- **上下文路由显示成功 (200 OK)：** 请继续执行确认路由中包含应用程序。

在 Secure Private Access 管理控制台中验证 CEP 集成

访问 Citrix Cloud 控制台的 Secure Private Access 中的**浏览器设置**部分。

在此部分中，验证以下内容：

- **Google Chrome 集成状态**必须显示为**完成**。如果发现失败，请确保已按照文档完成 CEP 集成的必备步骤，然后重试。如果问题仍然存在，请联系 Citrix 支持。
- **客户 ID** 必须具有与您正在集成的 Google 帐户相对应的值。您可以在 Google 管理控制台的**帐户 > 帐户设置**下找到该值。

如果以上所有值都正确，但您的 Chrome 浏览器仍未获得正确的扩展程序配置，请联系 Citrix 支持。

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

排查 Google 安全网关可达性问题

如何检查： 复制 URL `https://api.prod.securegateway.goog/api/v1/routes` 并在浏览器地址栏中导航到此 URL。您必须收到 HTTP 401 错误响应。这是预期行为，表示可以成功建立与 Google 安全网关的网络连接。

- **DNS 解析错误：** 这表明您的公司可能存在一些限制性 DNS 解析配置，阻止查找 Google 安全网关的 FQDN。然而，这是使用此功能的先决条件，并且相应的 FQDN 必须可解析。
- **请求挂起或显示超时错误页面：** 这强烈表明浏览器和互联网之间的防火墙正在丢弃发往 Google 安全网关的流量。请遵循 (/zh-cn/citrix-secure-private-access/service/prerequisites-for-cep-spa-integration.html) 中的，以确保您的网络可以访问必要的互联网位置。

如果您仍然没有收到正确的路由，请联系 Citrix 支持。

确认应用程序包含在路由中

成功的路由响应包括与您的 Secure Private Access 管理员配置的应用程序对应的 FQDN。例如：

```
[260318 06:42:38.99] [SG.ApiClient] [DEBUG] Response: {expirationTime:
'2026-03-18T14:15:05Z', proxyUrl: 'https://via.prod.securegateway.goog',
endpointMatchers: [{hostname: 'telemetry.netscalergateway.net'},
{hostname: 'www.workday.com'}, {hostname: '*.workday.com'}, {hostname:
'jira.internal.corp'}, {hostname: '*.jira.internal.corp'}]}.
```

此行是否包含您尝试访问的应用程序？

- **路由响应中包含无法访问的应用程序：** 请继续参阅 (#troubleshoot-routed-application-access) 中的。
- **路由响应中仅包含 telemetry.netscalergateway.net：** 尝试配置其他应用程序和包容性应用程序策略。如果您仍然在路由中看不到它，这强烈表明组员资格存在问题，或者 Citrix 中配置的 IdP 与 Google Directory 之间的组不一致。请继续参阅 (#ensure-idp-and-google-directory-alignment) 中的。
- **路由响应中不包含无法访问的应用程序：** 这表明应用程序未在 Secure Private Access 管理控制台中正确配置。验证应用程序是否存在并关联了策略（允许或拒绝访问）。如果您确定应用程序已配置但仍缺少上述路由，请联系 Citrix 支持。

排查路由应用程序访问问题

尝试访问您的应用程序（该应用程序确实显示在路由列表中）时，观察到的行为是什么？

- **您收到域名解析错误 (ERR_NAME_NOT_FOUND)**

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

这很可能表明应用程序配置不正确或未正确接收上下文路由。

- **显示“访问被拒绝”的米黄色页面**

  这表明 Secure Private Access 控制台中的策略配置未设置为包含当前用户。

- **一个显示“哎呀！出错了。”的米黄色页面**

  此错误页面最常见的原因是连接器无法访问目标应用程序。在这种情况下，请按照 Citrix 文档对连接器访问内部应用程序的问题进行故障排除。常见问题包括：

  - 内部 DNS 可达性
  - 后端服务已关闭
  - 防火墙规则

- **一个以大红色字体显示“服务不可用”的白色页面**

  这可能是一个暂时性错误，并且可能在几分钟后自行解决。

  如果问题仍然存在，请联系 Citrix 支持。

- **超时**

  - 首先，通过在 Chrome 的地址栏中输入 `via.prod.securegateway.goog` 来验证其是否可达。您必须收到 401 响应。如果超时，则表示中间防火墙或代理正在阻止访问，必须先解决此问题才能访问应用程序。
  - 应用程序超时的另一个潜在原因是防火墙阻止了流向互联网（特别是 Google 安全网关）的流量。这在客户需要显式代理才能访问互联网的场景中很常见。Secure Private Access 与 Chrome Enterprise Premium 的集成不支持此代理配置。

- **证书错误**

  应用程序可能正在使用私有 CA 证书，因此浏览器可能会抛出“不受信任的证书错误”。通过 Chrome Enterprise Premium 配置，客户可以将其受信任的根 CA 推送到浏览器。有关详细信息，请参阅使用 Chrome Enterprise Premium 管理根证书配置。

确保 IdP 和 Google Directory 对齐

对于 Secure Private Access 与 Chrome Enterprise Premium 的集成，您的目录与 Google Directory 的同步必须遵循一些规范，这些规范在集成解决方案的先决条件中有所介绍。

如果用户和用户组电子邮件正确且与源目录中配置的内容一致，请继续执行检查 Google Admin Console 中组的访问设置。

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

检查 Google Admin Console 中组的访问设置

在 Google Admin Console 中，导航到 **Directory > Groups**，然后选择您已配置访问策略但应用程序未加载的组。

在此处，选择 **Access settings** 并确保 **Who can view members** 行已启用 **Group Members** 选项。此配置必须应用于您希望在 Secure Private Access 中创建策略的所有组。

如果此选项已启用，请联系 Citrix 支持。

CEP 集成中的已知问题

Secure Private Access 与 Chrome Enterprise Premium 集成中存在以下已知问题。

Secure Private Access 用户界面

- **问题：** 会话策略配置目前只允许用户添加两个模拟条件，尽管有三个条件可用。这限制了策略创建的灵活性。

  解决方法： 创建两个单独的会话策略；一个包含两个模拟条件，另一个策略包含剩余的条件。

- **问题：** TCP/UDP 服务器到客户端配置选项并非在所有客户环境的应用配置 UI 中都可用。这限制了定义服务器到客户端流量行为的能力。

自适应访问策略配置

- **问题：** 当规则中指定 Okta 组时，访问策略创建失败。此问题仅影响 Okta 目录中存在的组。

  解决方法： 您可以将 Okta 用作身份提供程序，但不能用作目录。要将 Okta 用作 IdP，您必须首先将本地 AD 与 Okta 集成。有关详细信息，请参阅 将 Okta 作为身份提供程序连接到 Citrix Cloud。

Google Chrome 浏览器

- **问题：** 如果 Google 配置文件选择器处于打开状态，并且用户尝试从 CWA 或非 Chrome 浏览器启动应用程序，而此时没有现有配置文件，则不会触发配置文件创建工作流。

  解决方法： 关闭配置文件选择器并重新启动应用程序。

- **问题：** 使用托管 Chrome 配置文件登录 CWA 并启动应用程序后，用户不会被带到配置文件创建后的原始内部应用程序 URL。

  解决方法： 配置文件创建后，重新启动应用程序。

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

- **问题：** 从 Google 管理控制台同步组时，组中的用户不会自动同步。在同步过程中，`whoCanViewGroupMembership` 设置被明确覆盖为 `ALL_MANAGERS_CAN_VIEW`。因此，受限可见性是预期的。

  解决方法： 在 Google 管理控制台或通过 API 手动更新 Google 组权限。有关详细信息，请参阅 `<https://developers.google.com/workspace/admin/groups-settings/manage>`。

- **问题：** 用户通过托管 Chrome 配置文件访问已发布的 SaaS/Web 应用程序时，系统会通过代理弹出窗口提示用户使用用户名和密码进行身份验证。这通常发生在一段时间不活动之后：

  原因：

  - 代理令牌不可用，或者代理令牌可用但随后已过期。
  - 由于延迟初始化，SEB 扩展需要重新初始化。

  解决方法： 在新窗口中重新启动 Chrome 会话。

- **问题：** 用户通过托管 Chrome 配置文件或 Citrix Workspace 应用程序访问外部 SaaS 应用程序时，可能会遇到间歇性“服务不可用”错误。此问题是由于 Google 基础设施上未解决的后端问题造成的。

  解决方法： 联系 Google 团队寻求支持。

开放身份连接 (OIDC)

问题： 当客户与同一 Azure 租户有多个 Microsoft Entra ID 连接时，在 OIDC 客户端配置期间无法可靠地区分 Entra ID IdP。此问题仅影响 IdP 选择的可靠性。OIDC 客户端配置和身份验证行为不受影响。

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

开始使用 Citrix 安全私有访问

本文档指导您如何首次开始载入和设置 SaaS 应用程序交付。本文档面向应用程序管理员。

系统要求

- **操作系统支持：** Citrix Workspace 应用程序支持：
  - Windows 7、8、10 和 11 操作系统
  - macOS - 10.11 及更高版本
- **浏览器支持：** 通过云商店 URL 使用最新版本的 Edge、Chrome、Firefox 或 Safari 访问应用程序。
- **Citrix Workspace™ 应用程序支持：** 使用适用于任何桌面平台（Windows、Mac）的 Citrix Workspace 应用程序访问商店。
- 如果用户使用 自定义 URL 访问其商店，则他们必须使用以下最低版本：
  - 适用于 Windows 的 Citrix Workspace 应用程序：2503.10 或更高版本
  - 适用于 Mac 的 Citrix Workspace 应用程序：2505.10 或更高版本
  - 适用于 Mac 的 Citrix Secure Access 应用程序：26.04.1.1 及更高版本
  - 适用于 iOS 的 Citrix Secure Access 应用程序：26.04.1 及更高版本

工作原理

Citrix Secure Private Access 帮助 IT 和安全管理员管理授权的最终用户对批准的 SaaS 和企业托管 Web 应用程序的访问。用户身份和属性用于确定访问权限，访问控制策略确定执行操作所需的权限。用户通过身份验证后，访问控制将授权适当级别的访问以及与该用户凭据关联的允许操作。

Citrix Secure Private Access 结合了多个 Citrix Cloud™ 服务的元素，为最终用户和管理员提供集成体验。

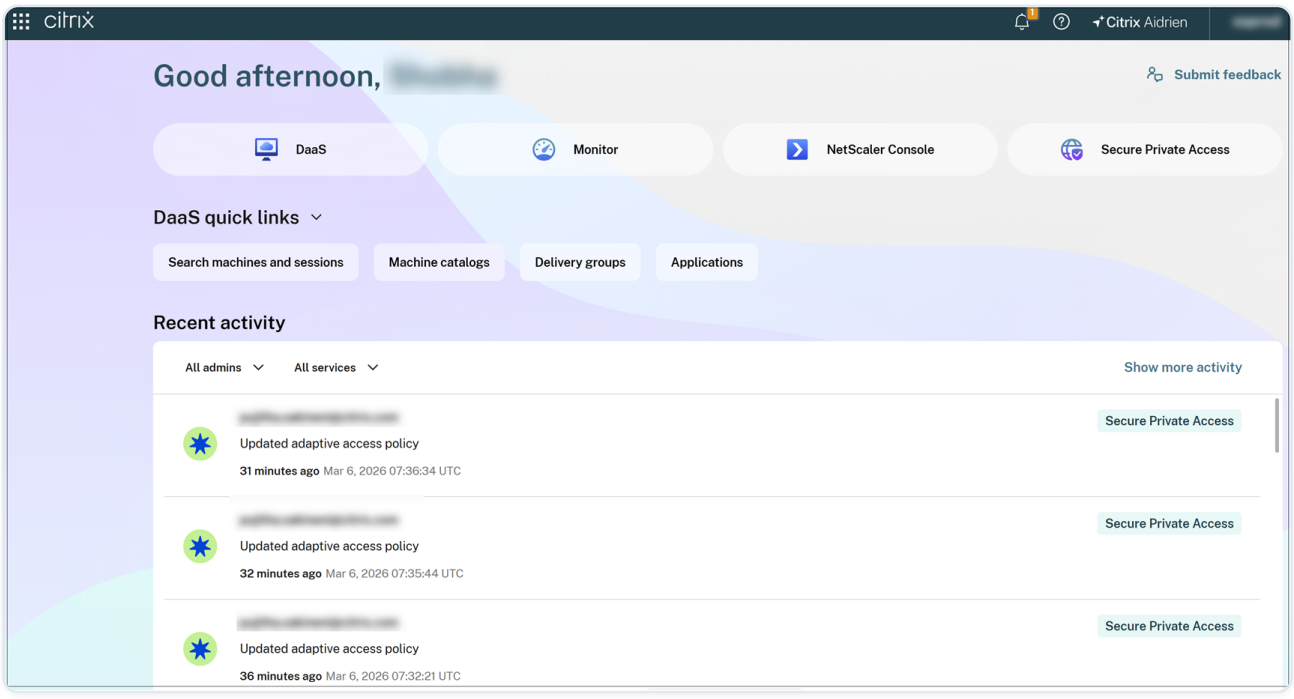
功能	提供功能的 服务/组件
访问应用程序的一致用户界面	StoreFront 云

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

功能	提供功能的 服务/组件
对 SaaS 和 Web 应用程序的 SSO	Citrix Gateway 服务标准版
Web 过滤和分类	Web 过滤服务
针对 SaaS 的增强安全策略	云应用程序控制
安全浏览	远程浏览器隔离服务
网站访问和风险行为的可视性	Citrix 分析

开始使用 Citrix Secure Private Access 服务

1. 注册 Citrix Cloud。
2. 请求 Secure Private Access 服务授权。
3. 授予授权后，将为您的帐户预配 Secure Private Access 服务。
4. 访问 Secure Private Access 服务管理 UI。
5. 配置最终用户用于在 StoreFront Cloud 中查看和启动其应用程序的商店。



注意：

- 最终用户若要使用商店并访问应用程序，必须下载并使用 Citrix Workspace 应用程序，或者从其 Web 浏览器打开商店 URL。您必须在商店中发布一些 SaaS 应用程序才能测试 Citrix Secure

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

Private Access 解决方案。可以从 下载 下载 Workspace 应用程序。在**查找下载**列表中，选择 **Citrix Workspace 应用程序**。

- 如果您配置了出站防火墙，请确保允许访问以下域。
  - *.cloud.com
  - *.nssvc.net
  - *.netscalergateway.net

  更多详细信息请参阅 Cloud Connector 代理和防火墙配置 和 Internet 连接要求。

Secure Private Access 服务部署模型

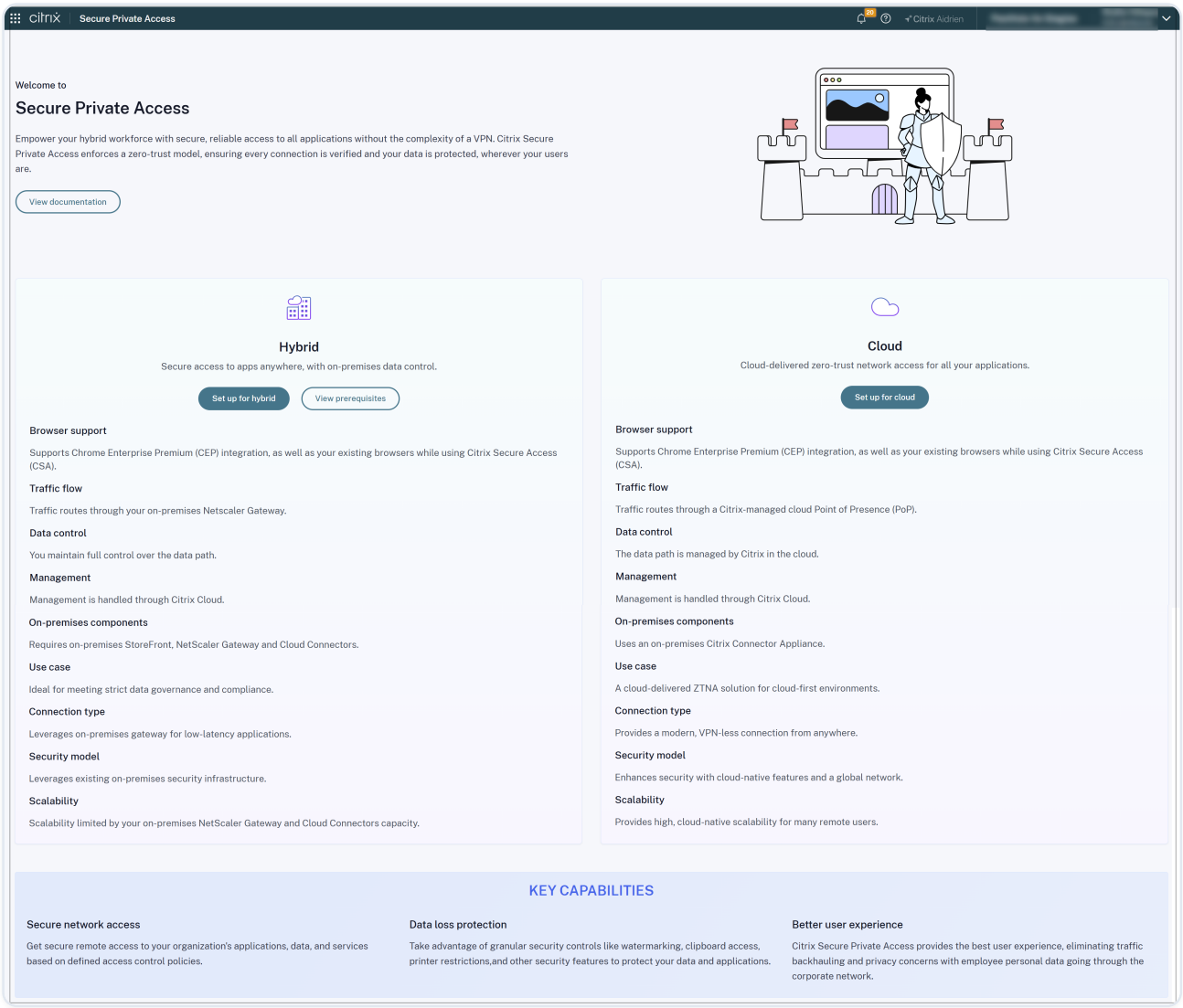
Secure Private Access 服务为客户提供两种架构选项。

- **混合服务架构：** 混合服务架构允许您使用本地 StoreFront 和 NetScaler Gateway 组件，确保所有用户流量都在您的控制之下。此外，站点管理组件由 Citrix 托管和管理。有关详细信息，请参阅混合部署。
- **云原生服务架构：** 云原生服务架构是一种云交付的 ZTNA 解决方案，可为 IT 批准的应用程序提供自适应访问，无论这些应用程序是部署在本地还是云中。有关详细信息，请参阅 Citrix Secure Private Access。

您可以从 Secure Private Access 服务管理控制台中选择这些选项。

1. 登录 Citrix Cloud™，然后单击 **Secure Private Access**。
2. 根据您的要求选择**混合设置**或**云设置**。

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



Citrix Secure Private Access™ 服务的存在点 (PoP) 位置

Citrix 正在全球范围内增加更多 PoP，以确保为 Citrix Secure Private Access 客户提供业务连续性和优质服务。

Secure Private Access 管理接入点

以下是 Secure Private Access 管理 PoP 位置列表。

POP 名称	区域	地区
Azure 欧洲西部管理	Azure 西欧	荷兰
Azure 印度南部管理	Azure 南印度	金奈
Azure 美国东部管理	Azure 美国东部	弗吉尼亚

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

安全私有访问数据接入点

以下是 Secure Private Access 数据 PoP 位置列表。

POP 名称	可用区	区域
Azure 美国东部	Azure 美国东部	弗吉尼亚
az-美国西部	Azure 美国西部	加利福尼亚
az-美国中南部	Azure 美国中南部	德克萨斯
澳大利亚东部	Azure 澳大利亚东部	新南威尔士州
欧洲北部	Azure 北欧	爱尔兰
欧洲西部	Azure 西欧	荷兰
日本东部	Azure 日本东部	东京，埼玉
巴西南部	Azure 巴西南部	圣保罗州
az-东南亚	Azure 东南亚	新加坡
az-阿联酋北部	Azure 阿联酋北部	迪拜
az-印度南部	Azure 印度南部	钦奈
az-亚洲香港	Azure 东亚	香港
az-西北欧	Azure 挪威东部	挪威

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

Secure Private Access 的入门和设置

Secure Private Access™ 管理控制台使管理员能够载入和管理 SaaS、Web 和 TCP/UDP 应用程序，并定义精细的访问策略，以管理用户如何与这些应用程序交互。

Citrix Secure Private Access 与 Google Chrome Enterprise Premium 集成，允许客户使用 Google Chrome Enterprise Premium 作为其企业浏览器安全地访问私有 Web 和 SaaS 应用程序。

载入和设置 Secure Private Access 的高级步骤如下：

1. 将用户载入 Secure Private Access
2. 在 Citrix® StoreFront Cloud 中配置商店 URL
3. 设置 Google Chrome 集成。
4. 配置连接器设备
5. 为您的用户添加应用程序。
6. 通过创建所需的访问策略来分配应用程序访问权限。

重要提示：

您可以将 Google Chrome 设置为您的企业浏览器。有关详细信息，请参阅以下主题。

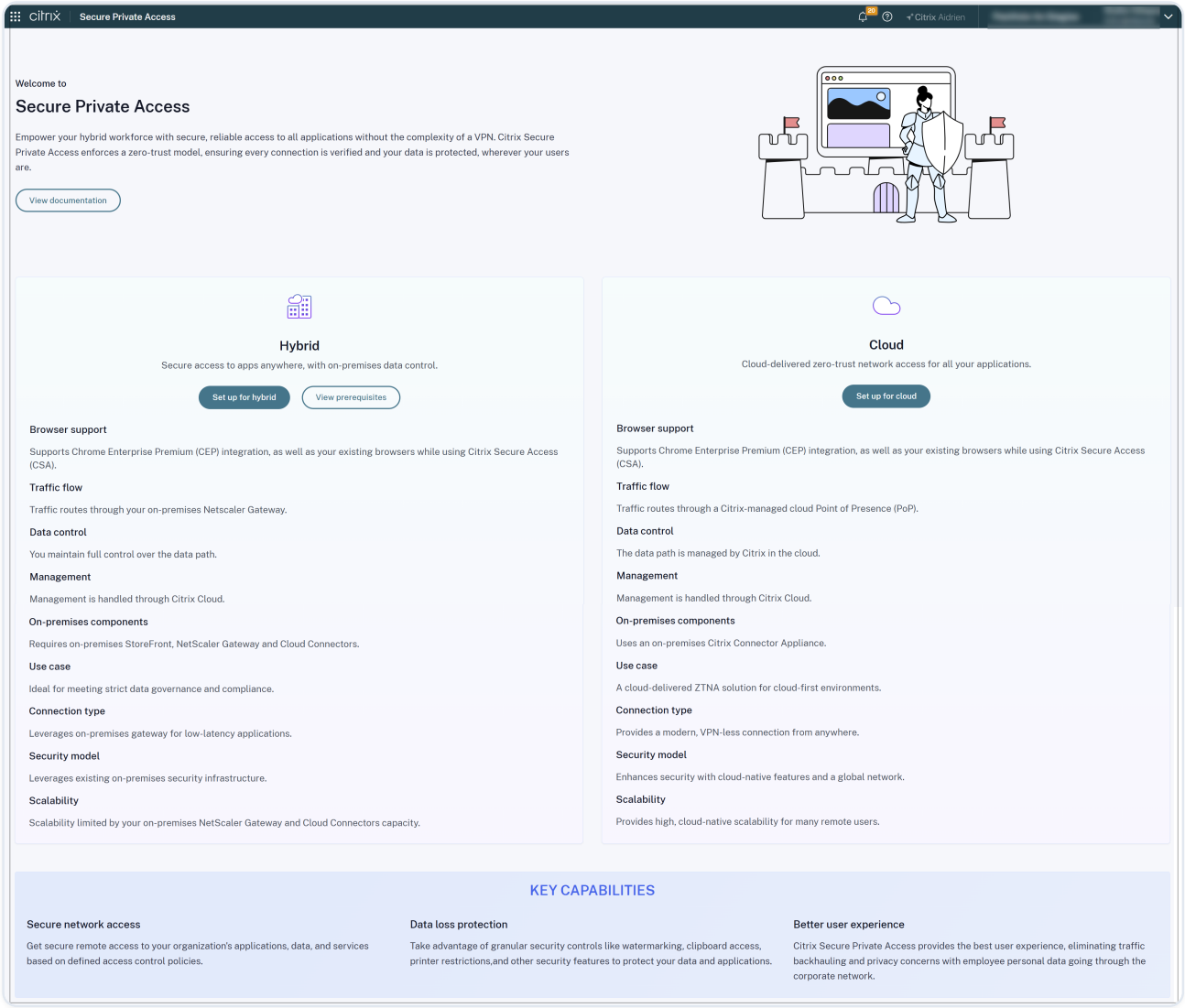
- 将 Google Chrome 设置为您的企业浏览器
- 切换浏览器前的注意事项

将用户载入 Secure Private Access

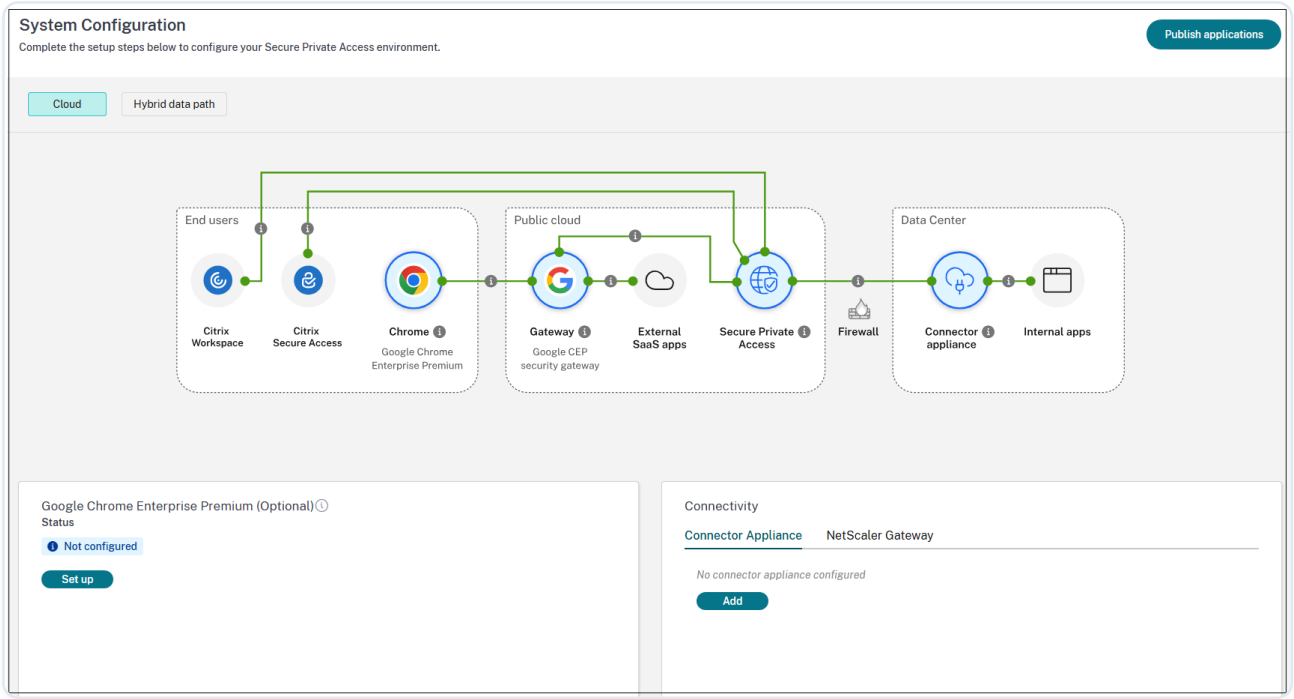
按照以下步骤将用户载入 Secure Private Access。

1. 登录 Citrix Cloud™，然后单击 **Secure Private Access**。
2. 选择 **Setup for cloud**，然后单击 **Continue**。

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



拓扑图显示了 Secure Private Access 云部署中使用的组件。您可以单击帮助图标以查看流程中每个组件的简短说明。



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

- **对于新客户**，在 Citrix Cloud 控制台中选择 Secure Private Access 服务会打开设置页面，允许他们配置 Connector Appliance 和 CEP。
  - 要配置 Connector Appliance，请在 **Connector Appliance Configuration** 窗格中单击 **Add**。有关详细信息，请参阅 配置 Connector Appliance。
  - 要配置 Google Chrome Enterprise Premium (CEP)，请在 **Google Chrome Enterprise Premium** 窗格中单击 **Set up** 并按照屏幕上的说明进行操作。有关详细信息，请参阅 设置 Google Chrome 集成。

  设置完成后，在后续访问中，管理员在 Citrix Cloud 控制台中单击 Secure Private Access 时，将被重定向到 Secure Private Access 控制板。
- **对于现有客户**，系统会检查：
  - 连接器设备可用性
  - Chrome 企业高级版状态

  Connector Appliance 检查： 系统检查是否配置了一个或多个 Connector Appliance 以及有多少可用。此检查有助于管理员了解，配置 Connector Appliance 对于用户成功连接到内部企业应用程序（Web、TCP/UDP）是强制性的。Connector Appliance 通过本机 Citrix Secure Access 客户端实现最终用户连接，支持客户选择的任何浏览器。

  Chrome Enterprise Premium 配置检查： Chrome Enterprise Premium 配置检查有助于管理员确定 Citrix Secure Private Access 与 Chrome Enterprise Premium 之间的集成是否已启用。此集成允许最终用户通过 Chrome 浏览器安全地访问企业 Web 应用程序，而无需本机 Citrix Secure Access 客户端。

注意：

Google Chrome Enterprise Premium 设置是可选的，可以跳过。

在 Citrix StoreFront Cloud 中配置商店 URL

您可以将 Secure Private Access 服务与 Citrix® StoreFront Cloud 集成。您为用户提供一个商店 URL，他们可以在 Web 浏览器或 Citrix Workspace™ 应用程序中打开该 URL。该商店为已配置的 SaaS 应用程序、Web 应用程序、虚拟应用程序和其他已配置资源提供统一的用户体验。

默认情况下，会创建一个 URL 为 `customerid.cloud.com` 的商店。您可以更改此 URL，或添加自己的自定义 URL，例如 `store.company.com`。要配置商店，请参阅 配置对商店的访问。

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

设置 Google Chrome 集成

在 Google Chrome 集成页面中，执行以下步骤：

1. 复制自动生成的服务帐户电子邮件，并将其粘贴到 Google 管理控制台中的相应字段中。

   a. 在 Google 管理控制台中，转到 **管理员角色**。

   b. 选择为 Secure Private Access 服务创建的角色，并应用建议的权限。有关权限列表，请参阅管理员角色和权限。

   c. 在 **管理员** 下，选择 **分配服务帐户**。

   d. 粘贴 Citrix 服务帐户 (`tenant-sa-<random-string>.iam.gserviceaccount.com`)，然后选择 **添加**。然后选择 **分配角色**。

      有关角色的详细信息，请参阅 关于管理员角色。

   e. 在 Google 管理控制台中，导航到 **目录 > 用户**。

   f. 单击 **添加新用户** 并创建一个新用户（名字：Citrix Service，姓氏：Account，主要电子邮件：caccount）。保留新创建用户的电子邮件。

   g. 新用户创建后，选择该用户并转到**用户详细信息**。在**管理员角色和权限**中，选择并为此用户分配相同的角色。

   h. 转到**安全 > 访问和数据控制 > API 控件**，然后单击**管理域范围委派**。

   i. 在**API 客户端**上，单击**添加新项**，并使用 Google Chrome 集成页面中提供的相应信息填写客户端 ID 和 OAuth 范围。

   j. 将 Google 管理控制台的**Google 帐户设置**中提供的 Google 客户 ID 复制到 **Google Chrome 集成**页面中的**Google 客户 ID**字段。

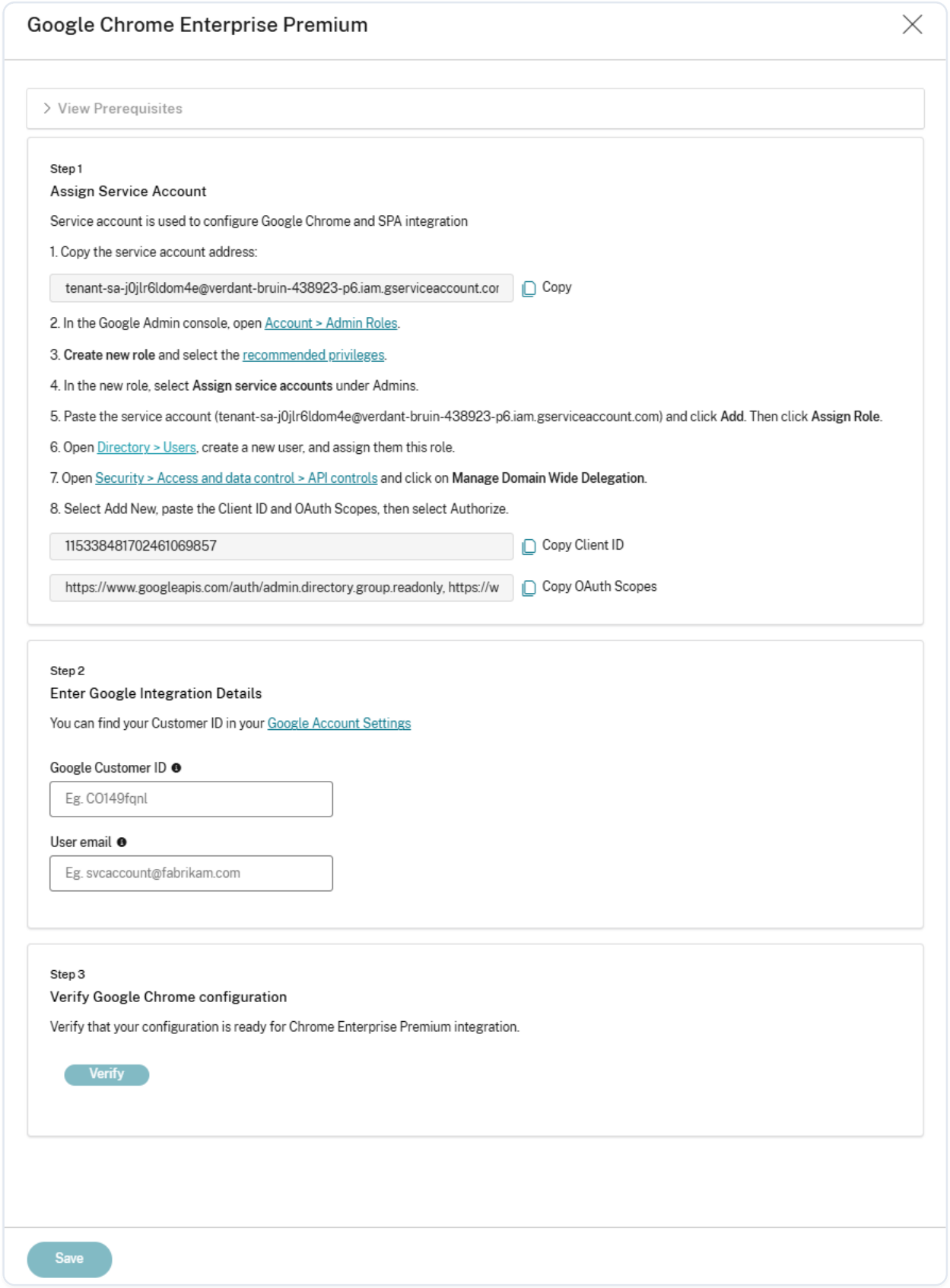
   k. 在 Google Chrome 集成页面中，使用之前创建的用户的电子邮件填充**用户电子邮件字段**。

2. 单击**运行 CEP 验证**以验证您的 Google Workspace 配置，确保其已准备好进行 Chrome Enterprise Premium 集成，然后再继续下一步。

   - 如果验证返回失败或警告，请参阅已知验证失败和警告 以获取故障排除指南。
   - CEP 验证成功后，Secure Private Access 服务将成功连接到 Google 客户 ID 并创建安全网关。
   - 成功创建安全网关后，系统会显示分配给它的出站 IP 地址。管理员可以选择 Chrome Enterprise Premium 用于 SaaS 应用程序流量的出站区域。有关详细信息，请参阅配置出站中心区域。

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

- 当用户尝试访问 SaaS 应用程序时，请求不会直接发送到 SaaS 提供商。相反，流量首先通过充当合作伙伴连接器的安全网关进行路由。此网关充当中间人，在所有流量到达目标应用程序之前对其进行检查和保护。



3. 单击**保存**。

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

重要提示：

- 客户加入 CEP 后，您还可以更新集成详细信息。有关详细信息，请参阅加入后更新 Google 集成详细信息。
- 除了所有用户和用户组之外，您还可以在加入期间将 CEP 配置应用于选定的 Google Directory 组织单位。有关详细信息，请参阅为 Google Directory 组织单位配置 CEP。

- 有关 Secure Private Access 与 Google Chrome Enterprise Premium 集成的更多详细信息，请参阅 与 Google Chrome Enterprise Premium 集成。

添加 SaaS 应用程序的 IP 地址

在将客户载入 Secure Private Access 和 Chrome Enterprise Premium 后，您必须允许您的 SaaS 应用程序使用的 IP 地址列表。此步骤对于确保以下事项至关重要：

- 用户可以访问 SaaS 应用程序，而不会出现连接问题或因网络安全控制而导致的阻止。
- 来自 Citrix Secure Private Access 和 Chrome Enterprise Premium 的流量被识别为合法流量，不会被意外过滤或拒绝。

注意：

对于使用“通过 连接器”路由类型通过连接器设备路由的应用程序，客户必须使用 Citrix IP 允许列表。

主体访问边界策略配置

主体访问边界策略可以阻止最终用户访问 Citrix 管理的 Google Secure Gateway。

如果您的 GCP 组织具有默认阻止访问跨租户资源的主体访问边界策略，请创建一个允许访问 Google Secure Gateway 的主体访问边界策略。您可以从“**浏览器设置 > 浏览器**”页面检索 Secure Gateway 标识符。有关配置相应策略的详细信息，请参阅 Google Cloud IAM - 主体访问边界策略文档。

载入后更新 Google 集成详细信息

客户成功载入 Chrome Enterprise Premium 后，Secure Private Access 允许对其集成详细信息进行载入后管理。这包括更新客户 ID 等关键标识符以及修改关联用户组的功能。

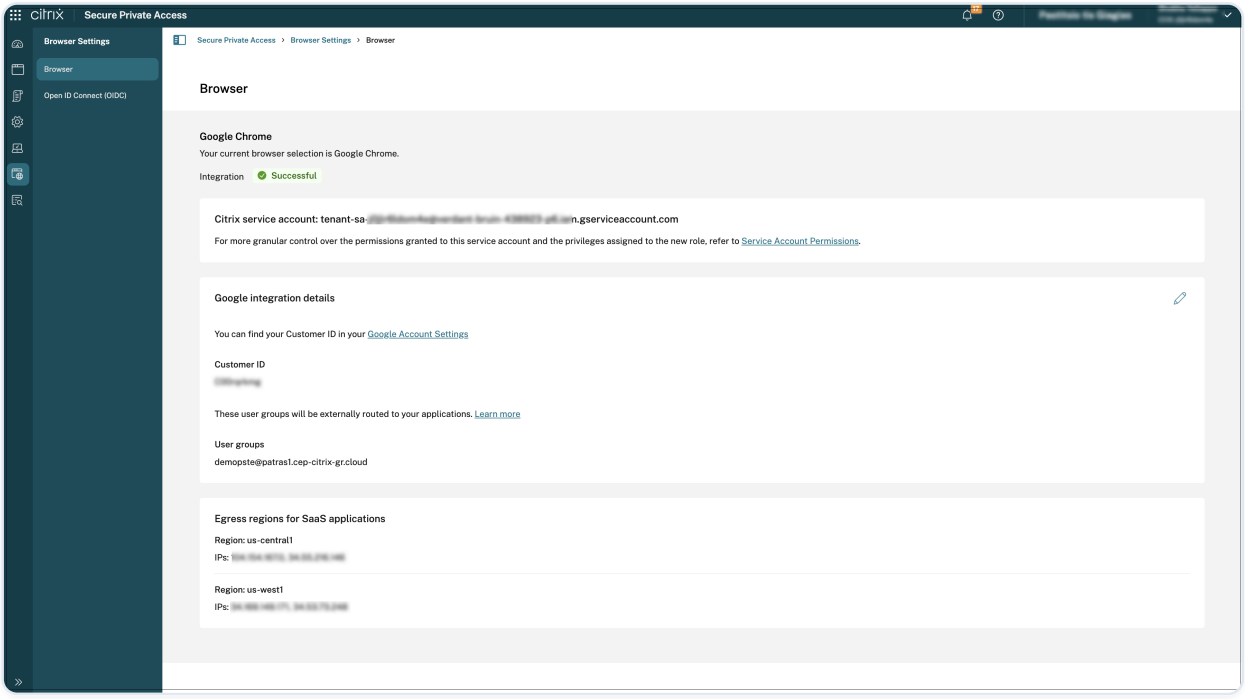
© 1997–2026 Citrix Systems, Inc. All rights reserved.

执行以下步骤以在载入后更新集成详细信息：

1. 在 Secure Private Access 管理控制台中，转到“**浏览器设置 > 浏览器**”。

   “浏览器”页面显示 Google Chrome 集成详细信息。

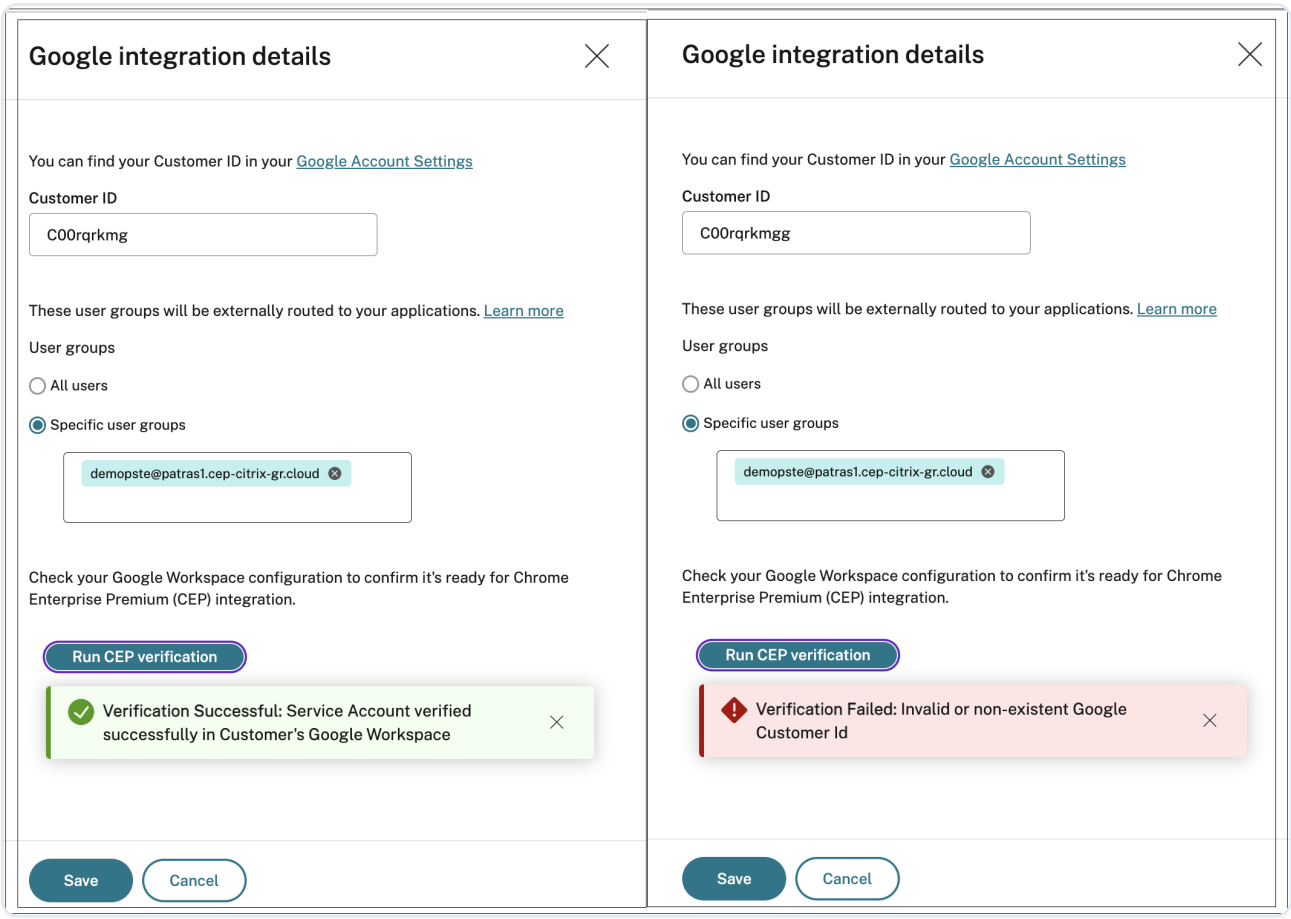
   系统还会显示与安全网关关联的出口 IP 地址。每次用户尝试在此集成中访问软件即服务 (SaaS) 应用程序时，流量都会通过充当合作伙伴连接器的 Google 安全网关进行路由，而不是直接连接到 SaaS 应用程序。此网关会检查并保护流量，强制执行安全策略和访问控制，并确保符合组织的安全态势。



2. 单击编辑图标并更新客户 ID 或用户组，或两者都更新。
3. 单击 **运行 CEP 验证** 以验证您的 Google Workspace 配置是否已准备好进行 Chrome Enterprise Premium 集成。

   如果集成详细信息存在问题，CEP 验证会显示失败或警告消息，其中包含详细信息以帮助您解决这些问题。有关指导，请参阅 已知验证失败和警告。

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



为 Google Directory 组织单位配置 CEP

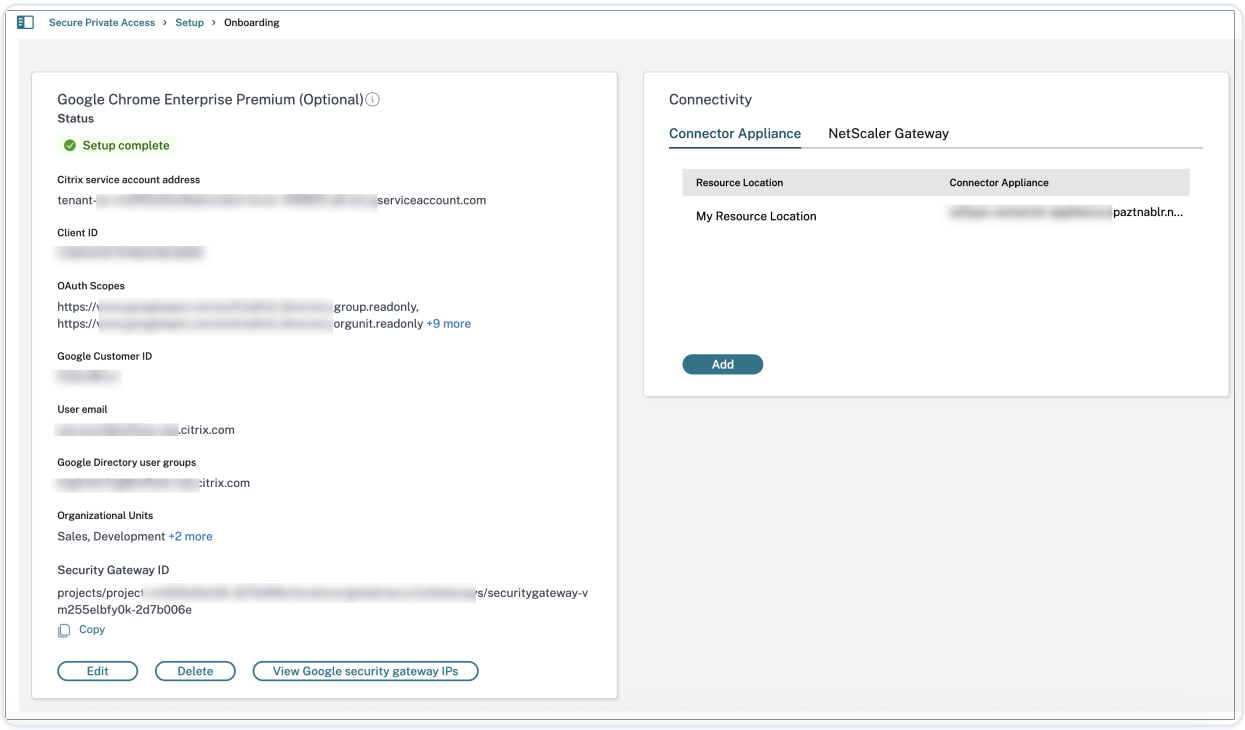
除了所有用户和 Google Directory 用户组之外，您还可以将 Chrome Enterprise Premium (CEP) 配置应用于选定的 Google Directory 组织单位。用户组和组织单位并非相互排斥，因此单个配置可以同时针对两者。您还可以保存一个仅使用组织单位且未选择用户组的配置。此选项适用于 Secure Private Access 云部署和混合部署。

选定的组织单位是继承的：该配置适用于该组织单位中的用户及其所有子组织单位，包括以后创建的任何子组织单位。

组织单位与 Google Directory 用户组在同一面板中选择。执行以下步骤：

1. 在 Chrome Enterprise Premium 设置卡上，单击 **编辑**。

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

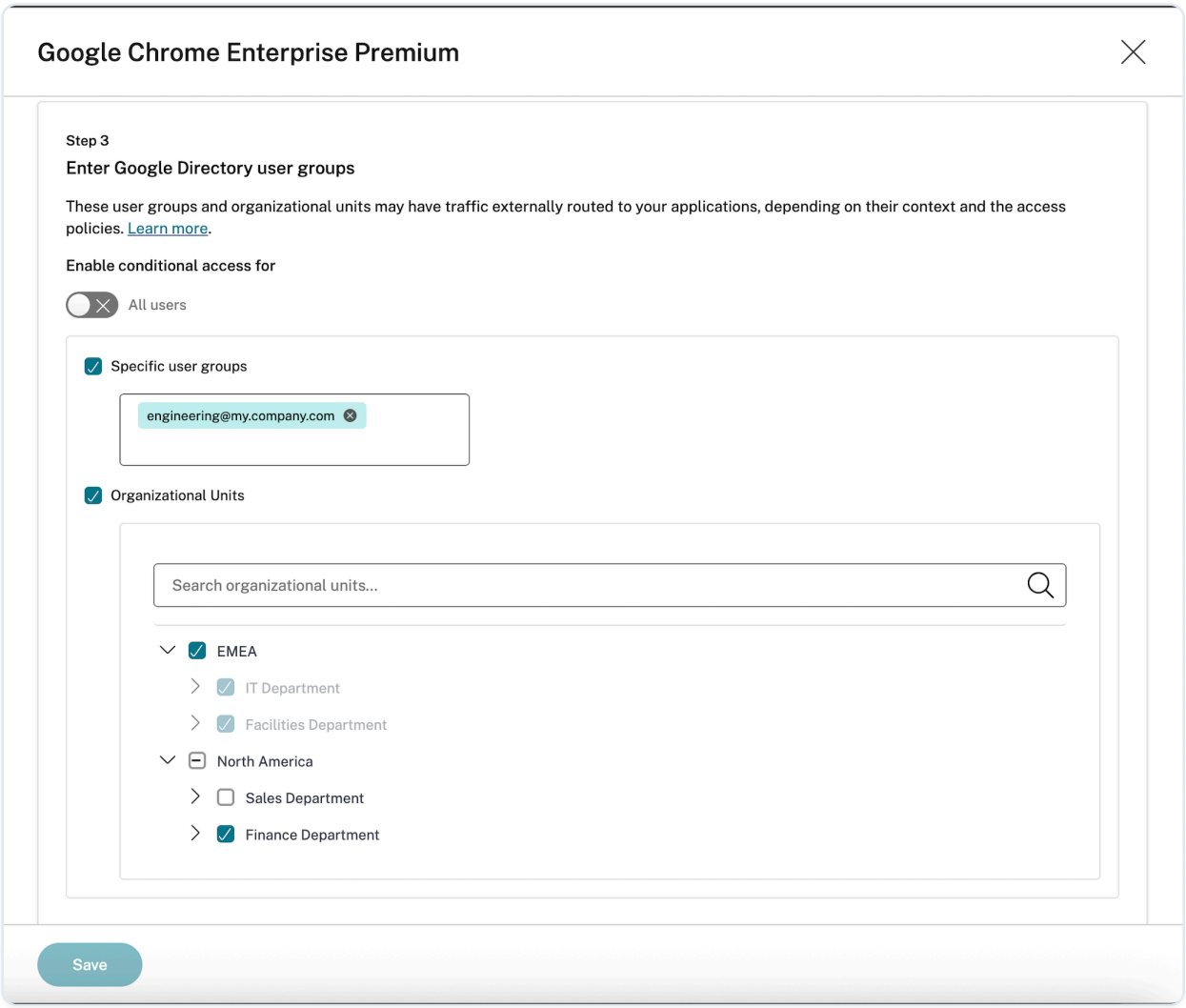


或者，在 Secure Private Access 管理控制台中，转到 **浏览器设置 > 浏览器** 并单击编辑图标。

该卡列出了当前选定的组织单位。

2. 单击 **组织单位** 以树状复选框的形式显示您的 Google Directory 层次结构。

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



注意：

- 根组织单位未在树中显示。要为所有人启用 CEP 集成，请选择“所有用户”。
- 层次结构是使用 Citrix 服务帐户从您的 Google 目录中读取的。如果服务帐户没有**组织单位 > 读取权限**，则无法加载层次结构，并且树的位置会显示错误。有关详细信息，请参阅Google 管理员角色和权限。

3. 选择要包括的组织单位。

   选择一个组织单位也会选择其子组织单位。子单位显示为已选中并灰显。它们无法单独清除。若要仅包含子集，请清除父级并选择所需的特定子组织单位。

4. 单击**运行 CEP 验证**，然后单击**保存**。如果在成功验证后更改了选择，请在保存之前再次运行验证。有关验证报告的故障和警告，请参阅已知验证故障和警告。

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

当您重新打开面板时，树会展开以显示您已保存的选择。在 Google 目录中已删除的组织单位将从面板中删除。

已知验证故障和警告

在验证 CEP 配置时，Secure Private Access 会在允许完成配置之前标记为选定设置识别出的任何故障或警告。

在继续配置之前，必须解决所有已识别的故障。使用下表识别并修复在验证期间检测到的特定故障：

故障消息	操作
Google 客户 ID 无效或服务帐户缺少访问 Google Workspace 的权限。	验证 Google 客户 ID 是否正确。
\^	确保所需权限已分配给服务帐户。有关详细信息，请参阅管理员角色和权限。
服务帐户缺少访问 Chrome 扩展策略的权限。	确保所需权限已分配给服务帐户。有关详细信息，请参阅管理员角色和权限。
\^服务帐户缺少访问用户组的 Chrome 扩展策略的权限。	\^
\^服务帐户缺少访问 Chrome 客户端证书策略的权限。	\^
在 Google Workspace 中发现空或无效的用户组 ID。	这可能是一个临时问题。如果问题持续存在，则可能是 Google 群组存在问题。
\^	如果问题在多个 Google 群组中持续存在，请联系 Citrix 支持。
用户组无效或不存在	检查 Google 群组名称中是否存在拼写错误。
\^	在 Google 管理控制台中验证该组是否仍然存在。
服务帐户没有权限将 Chrome 扩展程序策略应用于组织单位。	确保所需权限已分配给服务帐户。有关详细信息，请参阅管理员角色和权限。

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

任何已识别的警告都必须记录并调查，但它们不会阻止配置完成。以下列表描述了常见的警告以及如何解决它们：

警告消息	操作
Google 客户 ID 已在使用中	您的组织有多个 Citrix Secure Private Access 租户使用相同的 Google 客户 ID 进行 Chrome Enterprise Premium 集成。请谨慎配置，因为重叠的 Google 群组（包括为一个或多个租户选择“所有用户”）可能会覆盖或部分覆盖您其他 Citrix 租户中现有的 Chrome Enterprise Premium 设置。
检测到重叠的 Google Directory 用户组	检查您其他 Citrix 租户中针对给定 Google 群组的 Chrome Enterprise Premium 集成。
\^	决定哪个 Citrix 租户必须为每个相关的 Google 群组设置 Chrome Enterprise Premium。
\^	从其他 Citrix 租户中删除相应的设置。
\^	如果它在清理过程中被移除，请为选定的 Citrix 租户重新应用 Google 群组设置。
“所有用户”选项可能会干扰链接到此 Google 客户 ID 的其他客户	为“所有用户”（根 Google 组织单位）配置 Chrome Enterprise Premium 可能会覆盖使用相同 Google 客户 ID 的其他 Secure Private Access 设置。
\^	仅当其他 Citrix 租户未被用户主动使用时，才使用此设置。
“所有用户”选项正被至少一个链接到此 Google 客户 ID 的客户使用	如果另一个 Citrix 租户已为“所有用户”（根 Google 组织单位）配置了 Chrome Enterprise Premium，则它可能会覆盖为此 Citrix 租户计划的 Google 群组集成。
\^	确认其他 Citrix 租户是否需要“所有用户”集成。如果不需要，请将该租户更改为特定的 Google 群组。
检测到重叠的 Google Directory 组织单位	链接到此 Google 客户 ID 的另一个客户已在使用此组织单位，或其路径中的某个组织单位。

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

警告消息	操作
\^	重叠适用于此组织单位及其所有子组织单位。请检查您其他 Citrix 租户上针对所列组织单位的 Chrome Enterprise Premium 集成。
服务帐户缺少权限 `Services > Chrome Management > Settings > Managed Browsers > Read`	确认已分配相应的权限。如果已分配，请验证您是否在 Google 管理控制台（在“结算”>“订阅”下）中拥有 Chrome Enterprise Core 或 Chrome Enterprise Premium 的订阅。

多个用户组的预配失败问题

在 Secure Private Access 中配置 Chrome Enterprise 集成时（在载入期间或从 **浏览器设置** 页面），指定八个以上的用户组可能会导致预配失败。作为一种解决方法，请执行以下操作：

- 使用包含所有必需组的专用目录父组。
- 在载入期间配置此父组。
- 如果目录中的组成员身份发生更改，请重复同步过程到 Google 的目录。

后续步骤

配置 Connector Appliance 和 Chrome Enterprise Premium 后，您可以为用户配置应用程序和策略。

- 配置应用程序。
- 配置访问策略。

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

数据区域化

Citrix Secure Private Access 中的数据区域化功能使客户能够通过选择首选地理区域来控制其数据的存储位置。客户可以选择存储其数据的区域，选项包括全球、欧洲 (EU)、亚太地区 (APAC) 和北美 (NA)。所有静态配置数据都保留在所选区域内，确保其不会离开指定地理区域。

对于任何用户访问请求，应用程序流量都在所选区域内处理，不会跨越或离开该地理区域。这适用于所有用户，无论用户身在何处。即使用户分布在全球各地，每个用户的流量也会通过所选区域路由，而不会跨越任何其他地理区域。

数据区域化功能提供以下优势：

- 通过将所有配置数据保留在所选区域内，确保强大的数据驻留控制。
- 通过将配置数据以及适用的管理和支持服务数据保留在所选区域内，并使用区域数据 PoP 和管理端点进行客户部署，确保强大的数据驻留控制。
- 通过利用基于地理位置的路由，确保任何应用程序的用户访问请求流量保留在所选区域内，该路由将用户流量导向特定的 PoP，无论用户身在何处。
- 帮助组织满足法规和数据主权要求。
- 通过防止数据离开指定地理区域来降低风险。
- 支持具有区域特定需求的灵活全球部署，使客户能够自信地采用符合其驻留策略的云交付安全访问。

注意：

如果没有数据区域化，跨区域运营的组织可能面临严格的数据驻留和合规性要求，同时无法控制其服务数据的存储位置。如果没有区域数据边界，配置数据可能会存储在所需地理区域之外，从而增加监管风险并限制云交付安全访问解决方案的采用。

支持的部署

此功能适用于所有 Citrix Secure Private Access 部署，包括服务模型和混合模型，对于具有区域数据驻留、合规性和监管要求的组织尤其重要。

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

配置

选择区域是 Secure Private Access 服务或混合部署在入门期间的一次性设置。设置后，所有数据都将保留在所选区域中，对正在进行的操作或用户工作流程没有影响。

1. 登录到 Citrix Cloud，然后单击 **Secure Private Access**。
2. 选择 **Setup for cloud** 或 **Hybrid**，然后单击 **Continue**。
3. 在 **Select deployment region** 中，选择必须存储数据的区域。可用区域基于您的 Citrix Cloud 帐户区域。
4. 单击 **Continue**。

限制

数据区域化的一些限制包括：

- 数据区域化适用于客户拥有的静态配置数据和应用程序数据的用户访问请求。其他数据类型（例如遥测数据或传输中的数据）可能不受限于所选区域。
- 存在对其他全球运营的 Citrix Cloud 服务的依赖关系，这些服务可能不遵循相同的区域边界。
- 这是入门期间的一次性配置，以后无法更改。
- 此功能仅适用于新客户。

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

应用程序配置和管理

Citrix Secure Private Access 提供了一个用户友好、集中式的平台，用于配置和管理对各种应用程序（SaaS/Web 和 TCP/UDP）的访问。Secure Private Access 控制台通过为各种配置任务提供单一控制点来简化管理。管理员可以使用配置向导轻松设置自适应身份验证、配置应用程序、定义访问策略以控制用户权限，并实施安全限制以保护敏感数据，所有这些都可以在同一个控制台中完成。此外，Secure Private Access 支持对企业 Web 应用程序进行无代理访问，无需安装 VPN 客户端。

有关详细信息，请参阅以下主题：

- 支持企业 Web 应用程序
- 无代理访问企业 Web 应用程序
- 支持软件即服务应用程序
- 支持客户端-服务器应用程序
- 支持服务器到客户端连接
- Citrix 安全访问客户端
- Web 和 SaaS 应用程序配置的最佳实践
- 最终用户应用程序访问 - 说明

配置企业 Web 应用程序

使用 Secure Private Access 服务交付 Web 应用程序，可将企业专用应用程序作为基于 Web 的服务远程交付。常用的 Web 应用程序包括 SharePoint、Confluence、OneBug 等。

您可以将 Secure Private Access 服务与 Citrix® StoreFront Cloud 集成。用户可以通过 Web 浏览器或 Citrix Workspace™ 应用程序访问其云商店。该商店为配置的 SaaS 应用程序、配置的虚拟应用程序或任何其他资源提供统一的用户体验。

系统要求

连接器设备 - 将连接器设备与 Citrix Secure Private Access 服务结合使用，以支持客户数据中心中企业 Web 应用程序的无 VPN 访问。有关详细信息，请参阅 适用于 Secure Private Access 的连接器设备。

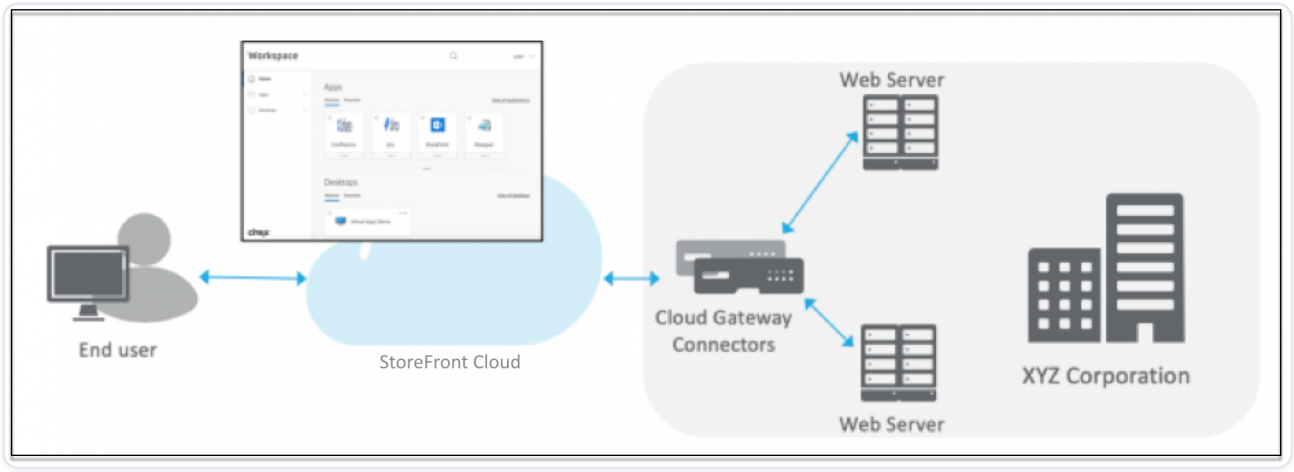
© 1997–2026 Citrix Systems, Inc. All rights reserved.

工作原理

Citrix Secure Private Access™ 服务使用部署在本地的连接器安全地连接到本地数据中心。此连接器充当部署在本地的企业 Web 应用程序与 Citrix Secure Private Access 服务之间的桥梁。这些连接器可以部署为高可用性对，并且只需要出站连接。

连接器设备与云中的 Citrix Secure Private Access 服务之间的 TLS 连接可保护枚举到云服务中的本地应用程序。Web 应用程序通过其商店使用无 VPN 连接进行访问和交付。

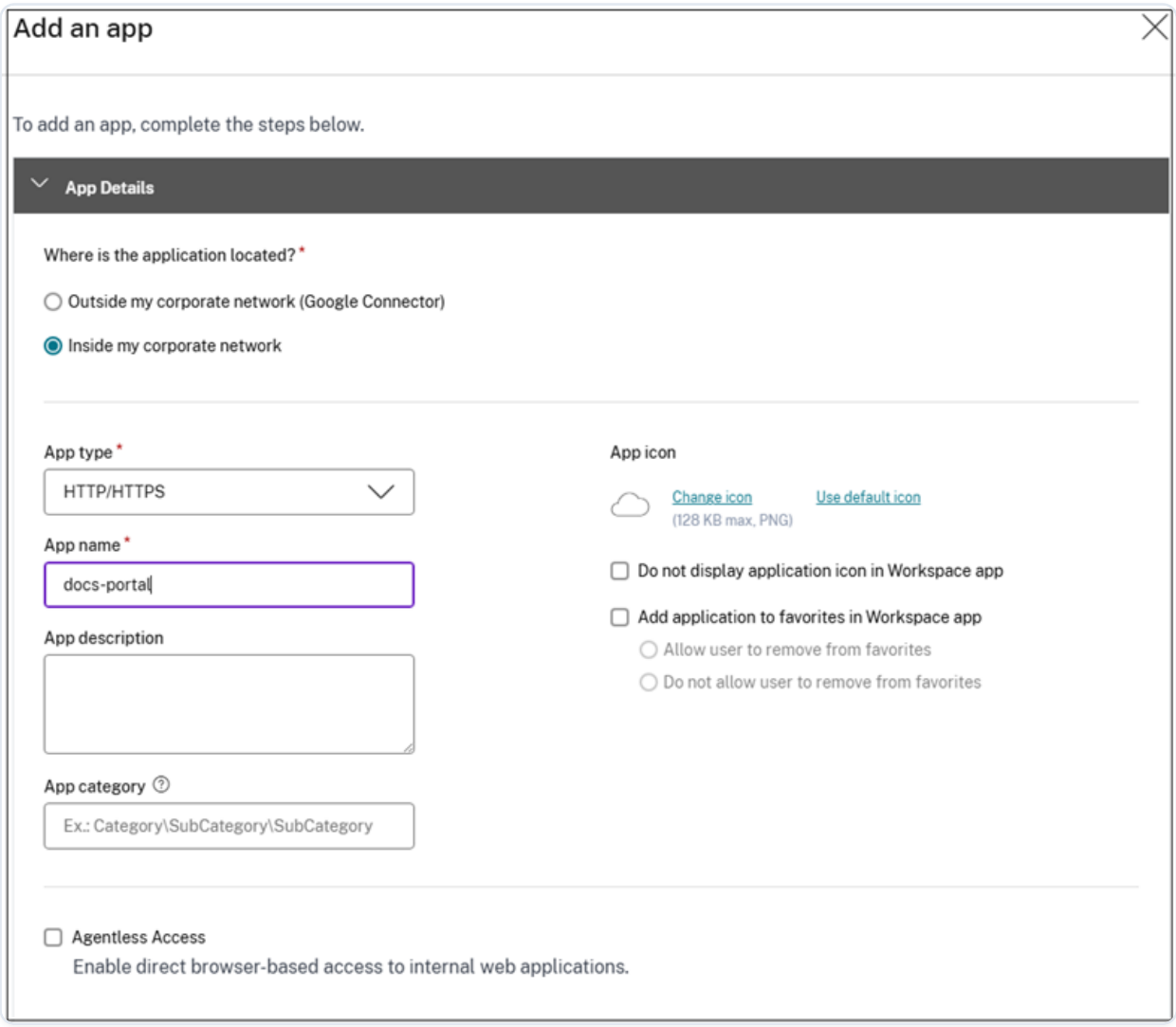
下图说明了如何使用 StoreFront Cloud 从其商店访问 Web 应用程序。



配置 Web 应用程序

1. 登录 Citrix Cloud 并选择 **安全私有访问**。
2. 单击 **应用程序 > 应用配置**，然后单击 **添加应用程序**。
3. 在 **Choose a template** 部分中，单击 **Skip**。模板仅适用于 SaaS 应用程序。
4. 在 **应用程序位置在哪里？** 中，选择 **在我的公司网络中**。
   - 选择 **我的公司网络内部**，适用于托管在组织内部私有网络基础设施中、位于防火墙后且只能通过内部网络连接访问的应用程序。
   - 选择 **我的公司网络外部（Google 连接器）**：适用于托管在组织私有网络基础设施外部的应用程序。流量通过 Google Cloud Connector 直接从用户路由到外部应用程序。
5. 在 **应用程序详细信息** 部分输入以下详细信息，然后单击 **下一步**。

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



- **应用程序类型** – 选择应用程序类型。

  注意：

  对于 Chrome Enterprise Premium (CEP)，仅支持 HTTPS 企业 Web 和 SaaS 应用程序。不支持 HTTP 企业 Web 和 SaaS 应用程序。

- **应用程序名称** – 应用程序的名称。
- **应用程序描述** - 应用程序的简要描述。此描述将显示给商店中的用户。
- **应用程序类别** - 添加您要发布的应用程序必须在商店 UI 中显示的类别和子类别名称（如果适用）。您可以为每个应用程序添加新类别，或使用商店 UI 中的现有类别。为 Web 或 SaaS 应用程序指定类别后，该应用程序将显示在商店 UI 中的特定类别下。
  - 类别/子类别可由管理员配置，管理员可以为每个应用程序添加新类别。
  - **应用程序类别** 字段适用于 HTTP/HTTPS 应用程序，并对 TCP/UDP 应用程序隐藏。

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

- 类别/子类别名称必须用反斜杠分隔。例如，**Business And Productivity\Engineering**。此外，此字段区分大小写。管理员必须确保他们定义了正确的类别。如果商店 UI 中的名称与在 **应用程序类别** 字段中输入的类别名称不匹配，则该类别将作为新类别列出。

  例如，如果您在 **应用程序类别** 字段中错误地将 **Business and Productivity** 类别输入为 **Business And productivity**，那么除了 **Business And Productivity** 类别之外，商店 UI 中还会列出一个名为 **Business And productivity** 的新类别。

- **应用程序图标** – 单击 **更改图标** 以更改应用程序图标。图标文件大小必须为 128x128 像素。如果您不更改图标，则会显示默认图标。

  如果您不想显示应用程序图标，请选择 **不向用户显示应用程序图标**。

- 选择 **无代理访问** 以允许用户直接从客户端浏览器访问应用程序。有关详细信息，请参阅 直接访问企业 Web 应用程序。

- **URL** – 包含您的客户 ID 的 URL。该 URL 必须包含您的客户 ID (Citrix Cloud™ 客户 ID)。要获取您的客户 ID，请参阅注册 Citrix Cloud。如果 SSO 失败或您不想使用 SSO，用户将被重定向到此 URL。

  客户域名 和 **客户域 ID** - 客户域名和 ID 用于在 SAML SSO 页面中创建应用程序 URL 和其他后续 URL。

  例如，如果您要添加 Salesforce 应用程序，您的域名是 `salesforceformyorg`，ID 是 123754，则应用程序 URL 是 `https://salesforceformyorg.my.salesforce.com/?so=123754.`.

  客户域名和客户 ID 字段特定于某些应用程序。

- **相关域** – 相关域会根据您提供的 URL 自动填充。相关域有助于服务将 URL 识别为应用程序的一部分并相应地路由流量。您可以添加多个相关域。

  注意：

  如果添加了重复的相关域，或者如果相关域也作为不同应用程序的 URL 添加，则会出现警告消息。为避免这些问题，请参阅 Web 和 SaaS 应用程序配置的最佳实践。

- **导入 HAR** – 您可以上传 HAR 文件以自动发现应用程序访问的域。查看发现的域并选择要添加到应用程序相关域配置的域。这通过减少手动识别和配置相关域的需要来简化应用程序的载入。有关详细信息，请参阅 使用 HAR 文件发现相关域。

- **保持一致连接** - 选中此复选框可启用与同一连接器设备的持续连接。有关一致连接的详细信息，请参阅 保持一致连接。

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

注意：

选择 **保持一致连接** 选项时，应用程序的路由类型必须在“应用程序连接”部分中设置为 **通过连接器进行内部连接**。

- 单击 **将应用程序添加到收藏夹 Workspace 应用程序** 以将此应用程序添加为 Citrix Workspace 应用程序中的收藏夹应用程序。
  - 单击 **允许用户从收藏夹中删除** 以允许应用程序订阅者从 Citrix Workspace 应用程序中的收藏夹应用程序列表中删除该应用程序。选择此选项后，Citrix Workspace 应用程序中应用程序的左上角会出现一个黄色星形图标。
  - 单击**不允许用户从收藏夹中删除**以防止订阅者从 Citrix Workspace 应用程序中的收藏夹应用列表中删除该应用。选择此选项后，Citrix Workspace 应用程序中应用的左上角会显示一个带挂锁的星形图标。

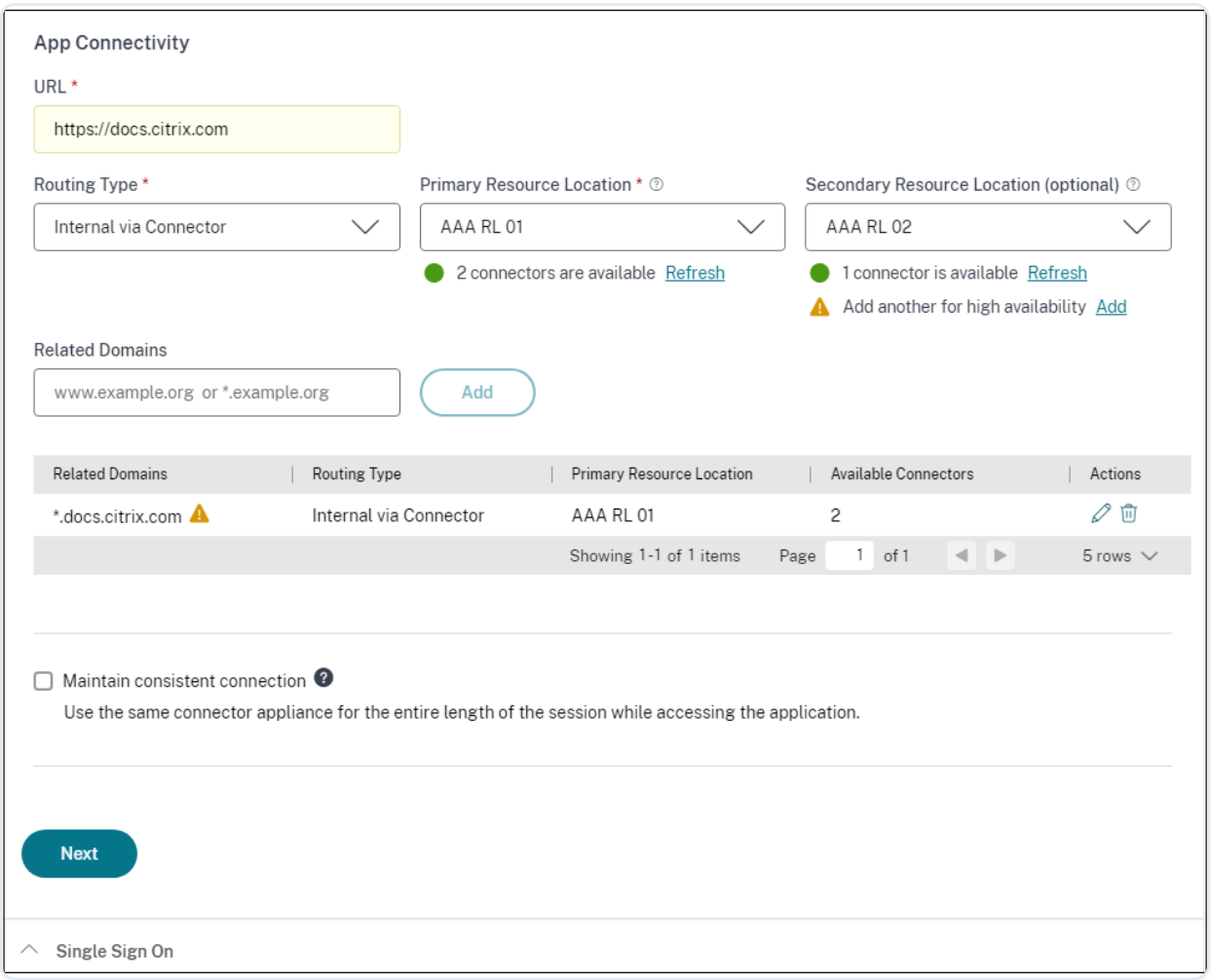
    如果您从 Secure Private Access 服务控制台中删除标记为收藏夹的应用，则用户必须手动从其商店中的收藏夹列表中删除该应用。如果从 Secure Private Access 服务控制台中删除应用，则这些应用不会从商店中自动删除。

重要提示：

- 为了启用基于零信任的应用访问，默认情况下会拒绝应用访问。仅当访问策略与应用程序关联时，才启用对应用的访问。
- 如果多个应用配置了相同的 FQDN 或通配符 FQDN 的某种变体，这可能会导致配置冲突。
- 这些问题可以通过遵循一些最佳实践来解决。有关详细信息，请参阅Web 和 SaaS 应用程序配置的最佳实践。

6. 在**应用连接**部分，您可以定义应用程序相关域的路由，如果这些域必须通过 Citrix Connector™ Appliance 外部或内部路由。

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



- **路由类型** - 选择以下选项之一：
  - **内部 – 绕过代理** - 域流量通过 Connector Appliance™ 路由，绕过在 Connector Appliance 上配置的客户 Web 代理。
  - **通过连接器内部** - 应用可以是外部的，但流量必须通过 Connector Appliance 流向外部网络。
  - **外部** – 流量直接流向互联网。
- **主要和次要资源位置** - 管理员可以通过配置次要资源位置或使用**第一个可用**选项来确保应用程序的高可用性，即使在中断期间也是如此。
  - **主要资源位置：** 选择应用程序托管的主要资源位置。或者，管理员可以在**主要资源位置**中选择**第一个可用**选项。
  - **第一个可用：** **第一个可用**选项可确保使用可用的资源位置。选择**第一个可用**后，系统会自动将流量路由到第一个可用的位置。这可确保无需手动干预即可持续访问应用程序。例如，如果 ResourceLocation1 不可用但 ResourceLocation2 可访问，则默认选择 ResourceLocation2 作为应用程序的前端。

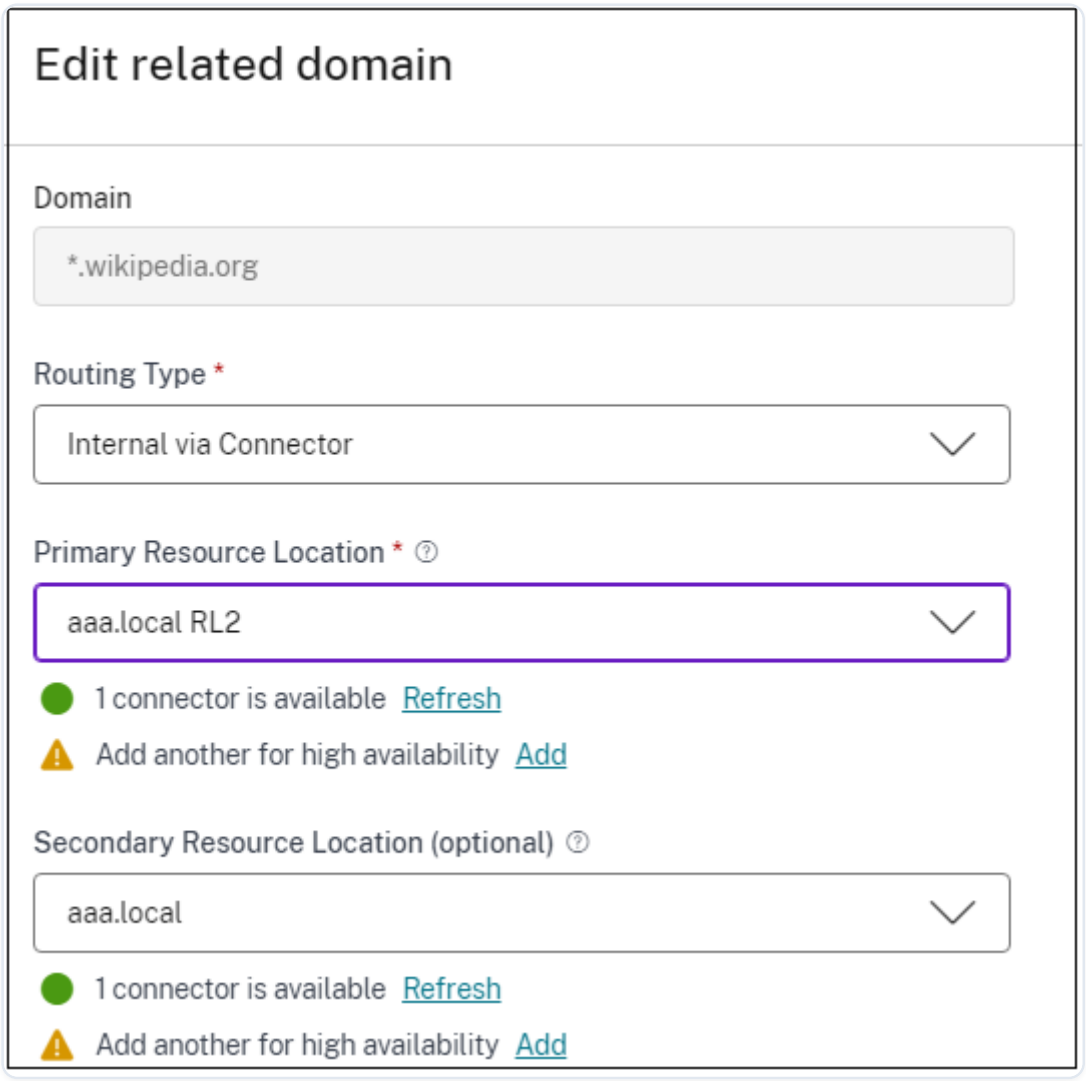
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **辅助资源位置** - 仅当明确指定主资源位置时，**辅助资源位置**选项才可用。如果主资源位置因连接器设备或数据中心故障等原因而变得不可用，应用程序将故障转移到指定的辅助资源位置。即使应用程序托管在另一个数据中心，辅助资源位置也可以充当故障转移。

您还可以为每个相关域设置主资源位置和辅助资源位置，或选择**第一个可用**选项。

a. 单击“相关域”表**操作**列中的编辑图标。

b. 设置主资源位置和辅助资源位置，或选择**第一个可用**选项。



注意：

- 设置备份资源位置和使用**第一个可用**选项功能目前处于预览阶段。
- 删除应用程序时，其路由条目会自动删除。有关详细信息，请参阅删除应用程序时自动清理路由条目。

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

- **保持一致连接** - 选中此复选框可启用与同一连接器设备的持续连接。有关一致连接的详细信息，请参阅保持一致连接。

  注意：

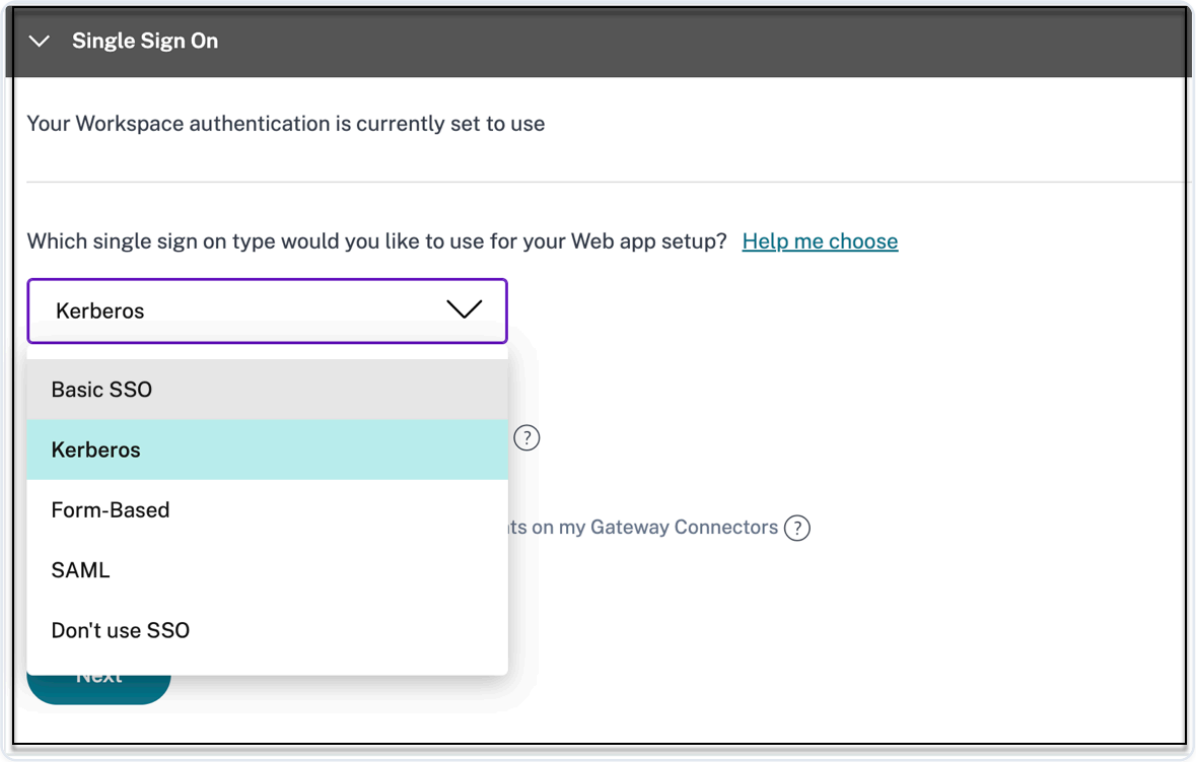
  选择**保持一致连接**选项时，应用程序的路由类型必须在“应用程序连接”部分设置为**通过连接器内部**。

7. 设置首选登录方法。

   注意：

   单点登录选项不适用于 Citrix Secure Access with Chrome Enterprise (CEP)。

   a. 在**单点登录**部分，选择您希望用于应用程序的单点登录类型，然后单击**保存**。以下单点登录类型可用。



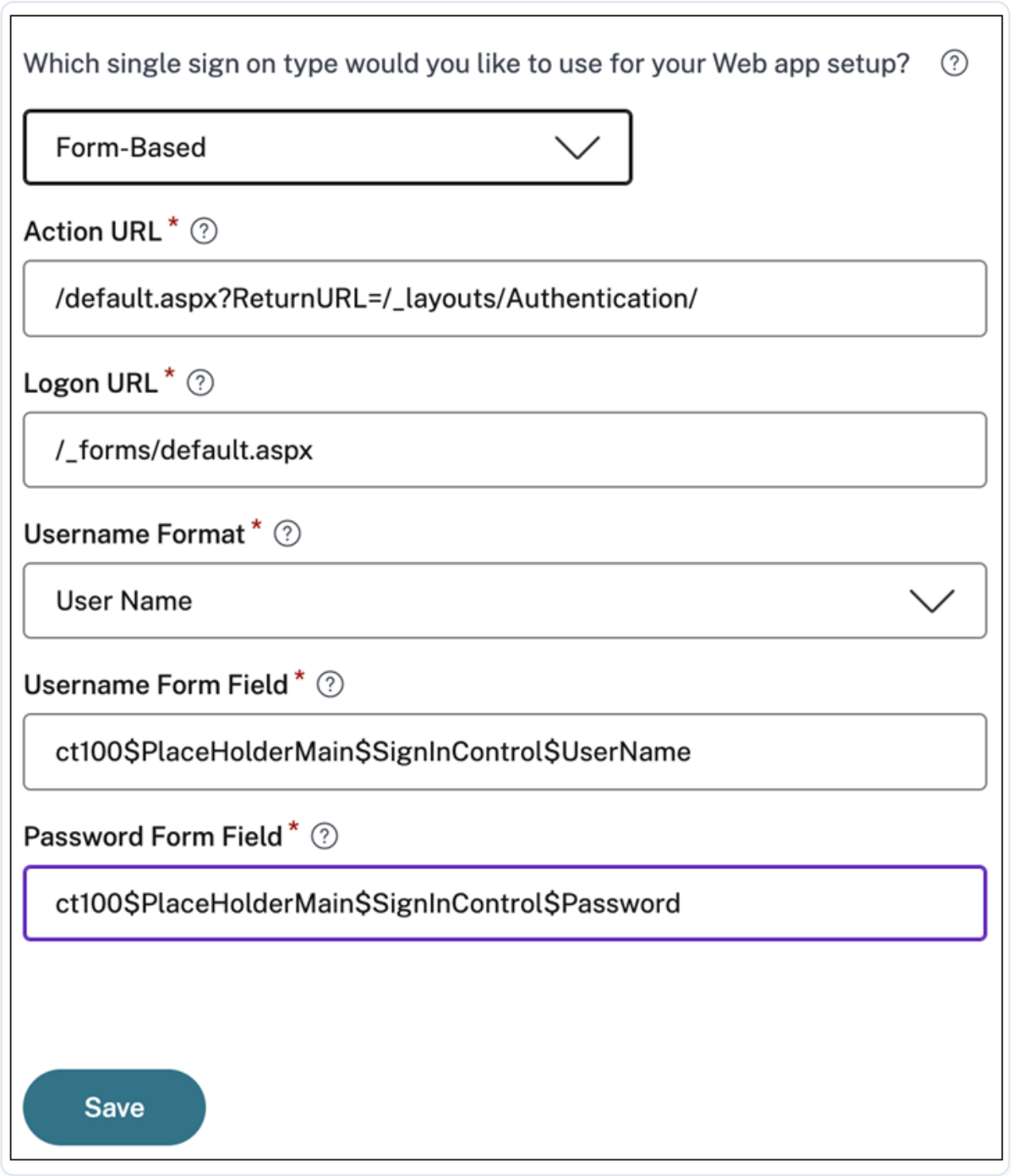
   - **基本** – 如果您的后端服务器向您发出 basic-401 质询，请选择**基本 SSO**。您无需为**基本** SSO 类型提供任何配置详细信息。
   - **Kerberos** – 如果您的后端服务器向您发出 negotiate-401 质询，请选择**Kerberos**。您无需为**Kerberos** SSO 类型提供任何配置详细信息。

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

- **基于表单** – 如果您的后端服务器向您提供用于身份验证的 HTML 表单，请选择**基于表单**。输入**基于表单**SSO 类型的配置详细信息。
- **SAML** - 选择**SAML**用于基于 SAML 的 Web 应用程序 SSO。输入**SAML** SSO 类型的配置详细信息。
- **不使用 SSO** – 当您不需要在后端服务器上对用户进行身份验证时，请使用**不使用 SSO**选项。选择**不使用 SSO**选项后，用户将被重定向到**应用程序详细信息**部分下配置的 URL。

基于表单的详细信息：

在“单点登录”部分中输入以下基于表单的配置详细信息，然后单击**保存**。



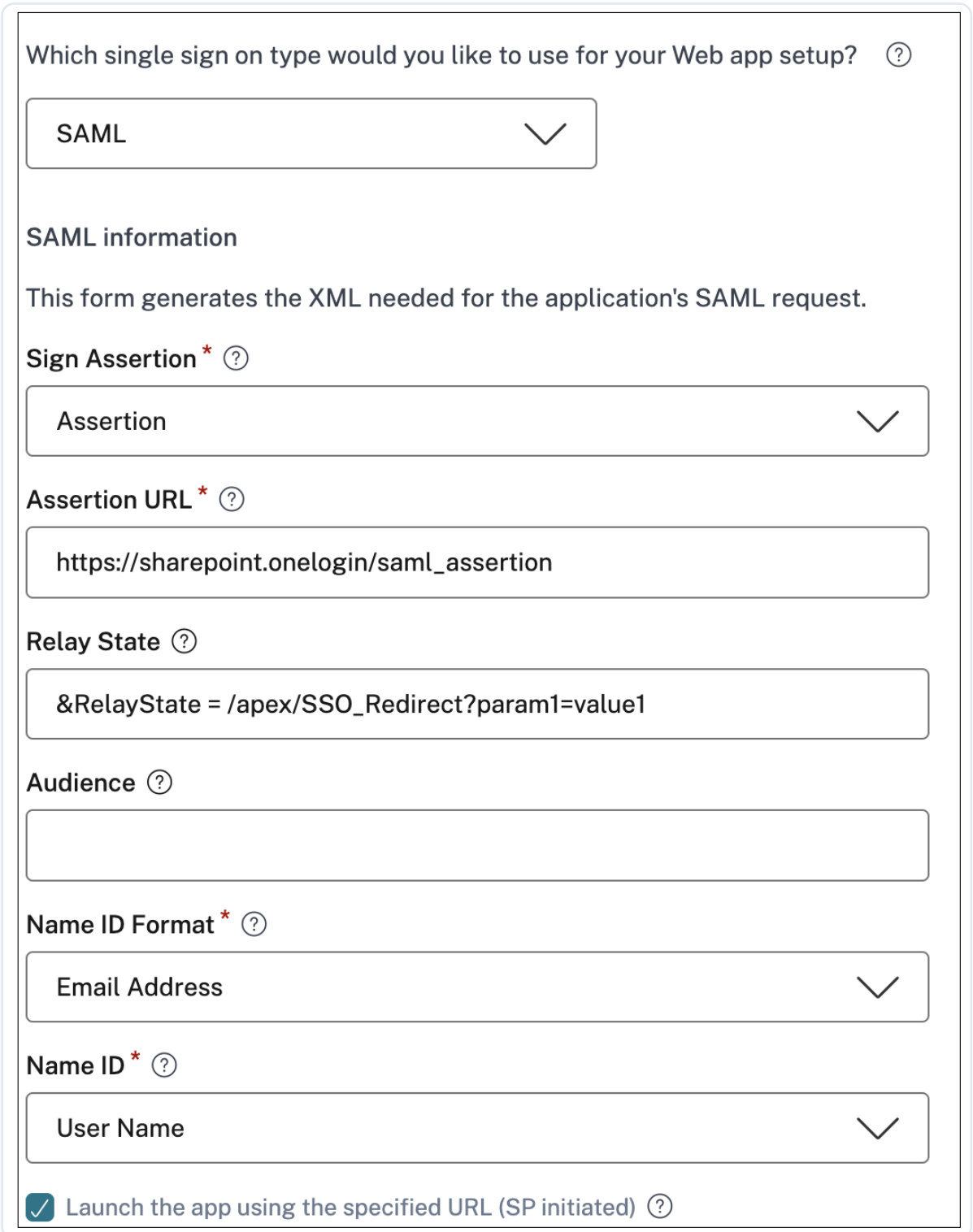
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **操作 URL** - 键入提交已完成表单的 URL。
- **登录表单 URL** – 键入显示登录表单的 URL。
- **用户名格式** - 选择用户名的格式。
- **用户名表单字段** – 键入用户名属性。
- **密码表单字段** – 键入密码属性。

SAML：

在单点登录部分输入以下详细信息，然后点击 **保存**。

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



- **签名断言** - 当响应或断言交付给依赖方 (SP) 时，对断言或响应进行签名可确保消息完整性。您可以选择 **断言、响应、两者** 或 **无**。
- **断言 URL** – 断言 URL 由应用程序供应商提供。SAML 断言将发送到此 URL。
- **中继状态** – 中继状态参数用于标识用户在登录并定向到依赖方的联合服务器后访问的特定资源。中继状态为用户生成一个单一 URL。用户可以点击此 URL 登录到目标应用程序。
- **受众** – 受众由应用程序供应商提供。此值确认 SAML 断言是为正确的应用程序生成的。

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

- **名称 ID 格式** – 选择支持的名称标识符格式。
- **名称 ID** – 选择支持的名称 ID。

i. 在 **高级属性（可选）** 中，添加有关用户的附加信息，这些信息将发送到应用程序以进行访问控制决策。

ii. 点击 **SAML 元数据** 下的链接下载元数据文件。使用下载的元数据文件在 SaaS 应用程序服务器上配置 SSO。

- 您可以复制 **登录 URL** 下的 SSO 登录 URL，并在 SaaS 应用程序服务器上配置 SSO 时使用此 URL。
- 您还可以从 **证书** 列表中下载证书，并在 SaaS 应用程序服务器上配置 SSO 时使用该证书。

8. 点击 **保存**，然后点击 **完成**。

点击 **完成** 后，应用程序将添加到“应用程序”页面。配置应用程序后，您可以从“应用程序”页面编辑或删除应用程序。为此，请点击应用程序上的省略号按钮并相应地选择操作。

- **编辑应用程序**
- **删除**

重要提示：

- 要授予用户对应用程序的访问权限，管理员需要创建访问策略。在访问策略中，管理员添加应用程序订阅者并配置安全控制。有关详细信息，请参阅创建访问策略。

删除应用程序时自动清理路由条目

配置应用程序时，其目标（FQDN 或应用程序域）会添加到路由表，Secure Private Access 使用该路由表进行路由决策。删除应用程序时，Secure Private Access 会根据以下规则清理路由条目：

- **删除未引用的条目** - 如果与已删除应用程序关联的路由条目（FQDN 或应用程序域）未被任何其他应用程序引用，Secure Private Access 会自动将其从路由表中删除。
- **保留共享条目** - 如果路由条目被多个应用程序使用，删除其中一个应用程序不会删除共享条目。只要至少有一个活动应用程序引用该条目，该条目就会保留在路由表中。
- **无追溯性删除** - 路由条目仅作为应用程序删除的一部分进行评估和删除。除非确认现有条目未被任何应用程序使用，否则不会追溯性删除。

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

注意：

- 当从“应用程序”页面（使用省略号 (...) 菜单）删除应用程序时，清理会自动运行。无需管理员操作。
- 由于共享路由条目会保留，因此删除应用程序不会中断对共享相同目标的其他应用程序的访问。

配置 SaaS 应用程序

软件即服务 (SaaS) 是一种软件分发模型，它以基于 Web 的服务形式远程交付软件。常用的 SaaS 应用程序包括 Salesforce、Workday、Concur、GoToMeeting 等。

您可以将 Secure Private Access 服务与 Citrix® StoreFront Cloud 集成。用户可以通过 Web 浏览器或 Citrix Workspace™ 应用程序访问其云商店。该商店为配置的 SaaS 应用程序、配置的虚拟应用程序或任何其他资源提供统一的用户体验。使用 Secure Private Access 服务交付 SaaS 应用程序为您提供了一种简单、安全、强大且可扩展的解决方案来管理这些应用程序。

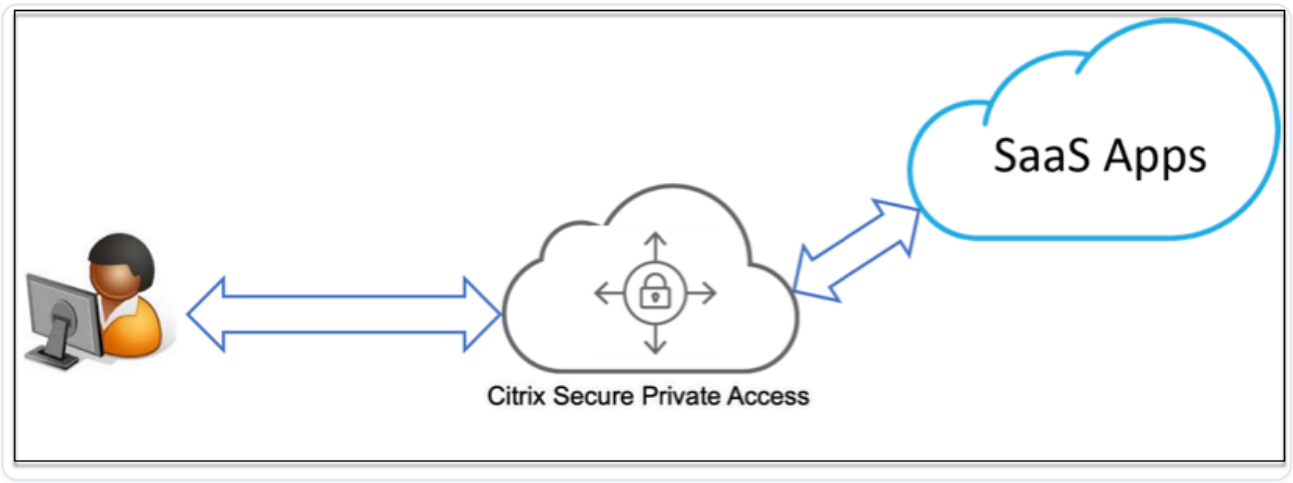
Secure Private Access 服务如何支持 SaaS 应用程序

1. 客户管理员使用 Secure Private Access 服务 UI 配置 SaaS 应用程序。
2. 管理员向最终用户提供商店 URL。
3. 要启动应用程序，用户单击枚举的 SaaS 应用程序图标。
4. SaaS 应用程序信任 Secure Private Access 服务提供的 SAML 断言，然后应用程序启动。

注意：

- 要授予用户对应用程序的访问权限，管理员需要创建访问策略。在访问策略中，管理员添加应用程序订阅者并配置安全控制。有关详细信息，请参阅创建访问策略。
- 配置的 SaaS 应用程序与虚拟应用程序和商店中的其他资源一起聚合，以提供统一的用户体验。

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



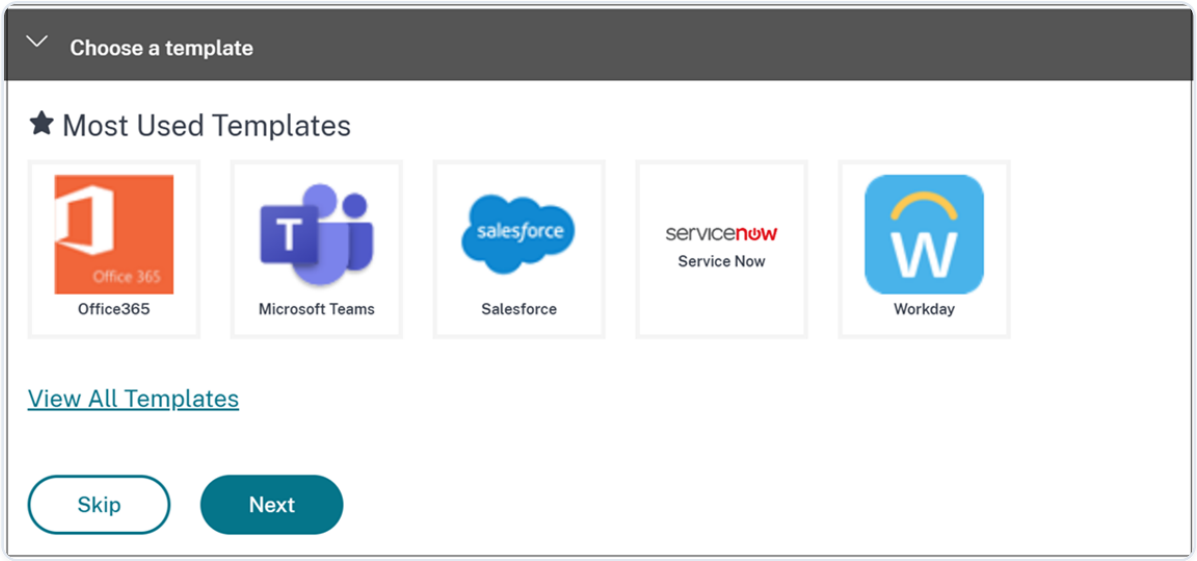
配置 SaaS 应用程序

1. 登录 Citrix Cloud 并选择 **安全私有访问**。
2. 单击 **应用程序 > 应用配置**，然后单击 **添加应用程序**。

> **注意：**
>
> 您可以手动配置应用程序，也可以使用模板。模板会预填充大部分应用程序设置，但您仍需提供客户特定的详细信息。

手动配置： 在“**选择模板**”部分中单击“**跳过**”，然后在“**应用程序详细信息**”部分中配置应用程序。从步骤 3 开始。
基于模板的配置： 单击“**选择模板**”，选择一个模板，然后单击“**下一步**”。根据需要查看并更新应用程序详细信息。

- 应用程序配置页面突出显示了五个最常用的模板，以简化和加速应用程序的载入。
- 选择“**查看模板**”以浏览其他受支持的 SaaS 应用程序的模板。

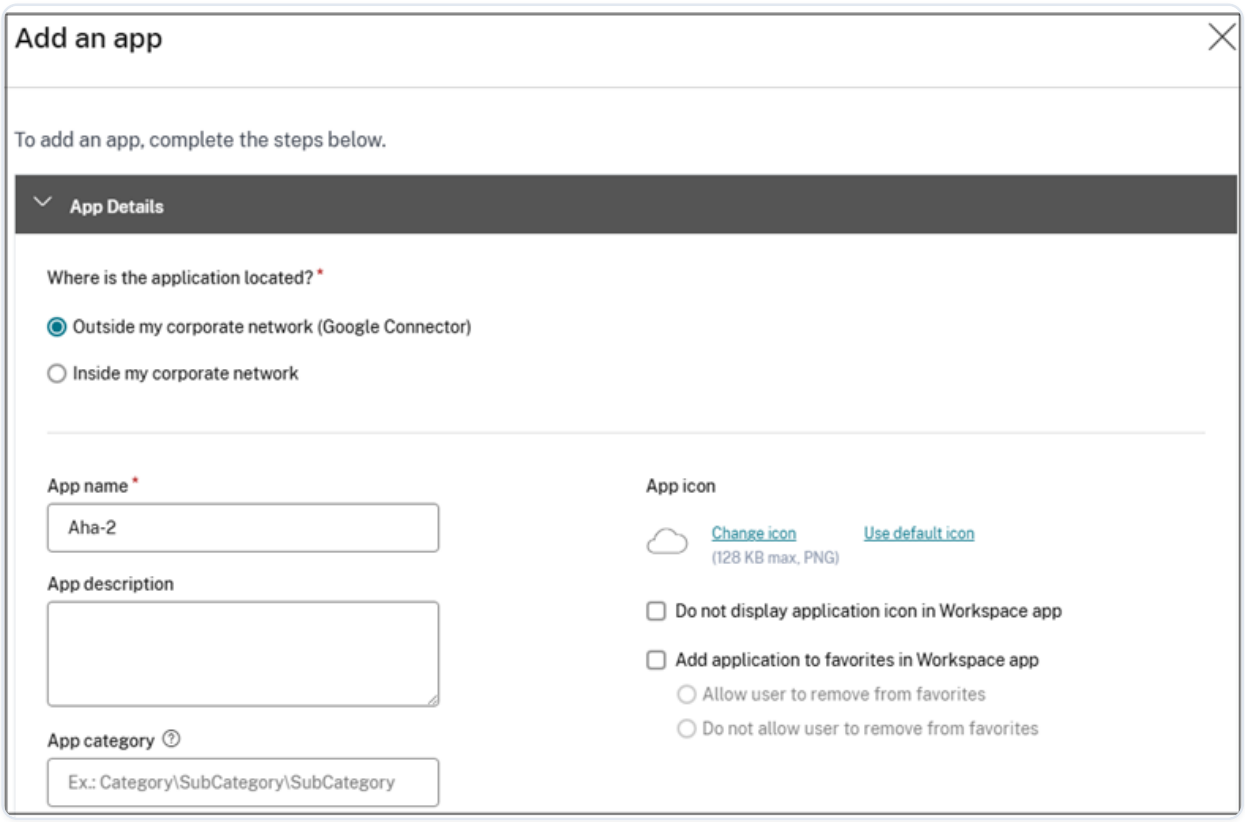


© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. 在“**应用程序位置在哪里？**”中，选择目标应用程序的位置，以确定必须应用的路由路径、策略和访问机制。对于 SaaS 应用程序，选择“**我的公司网络外部（Google 连接器）**”。

   - **我的公司网络外部（Google 连接器）：** 适用于托管在组织专用网络基础结构外部的应用程序。流量通过 Citrix Cloud 直接从用户路由到外部应用程序。
   - **我的公司网络内部**：适用于托管在组织专用网络基础结构内部、位于防火墙后并且只能通过内部网络连接访问的应用程序。

4. 在“**应用程序详细信息**”部分中输入以下详细信息，然后单击“**下一步**”。



   - **应用程序名称** – 应用程序的名称。
   - **应用程序描述** - 应用程序的简要描述。此描述将显示给商店中的用户。
   - **应用程序类别** - 添加类别和子类别名称（如果适用），您发布的应用程序必须在商店 UI 中显示在该类别下。您可以为每个应用程序添加新类别，也可以使用商店 UI 中的现有类别。为 Web 或 SaaS 应用程序指定类别后，该应用程序将显示在商店 UI 中的特定类别下。

     - 类别/子类别可由管理员配置，管理员可以为每个应用程序添加新类别。
     - “**应用程序类别**”字段适用于 HTTP/HTTPS 应用程序，并对 TCP/UDP 应用程序隐藏。
     - 类别/子类别名称必须用反斜杠分隔。例如，**Business And Productivity\Engineering**。此外，此字段区分大小写。管理员必须确保他们定义了正确的类别。如果商店 UI 中的名称与在“**应用程序类别**”字段中输入的类别名称不匹配，则该类别将作为新类别列出。

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

例如，如果您在“**应用程序类别**”字段中错误地将“**Business and Productivity**”类别输入为“**Business And productivity**”，则除了“**Business And Productivity**”类别之外，商店 UI 中还会列出名为“**Business and productivity**”的新类别。

- **应用程序图标** – 单击“**更改图标**”以更改应用程序图标。图标文件大小必须为 128x128 像素。如果您不更改图标，则会显示默认图标。

  如果您不想显示应用程序图标，请选择“**不向用户显示应用程序图标**”。

- **URL** – 包含您的客户 ID 的 URL。URL 必须包含您的客户 ID (Citrix Cloud™ 客户 ID)。要获取您的客户 ID，请参阅注册 Citrix Cloud。如果 SSO 失败或您不想使用 SSO，用户将被重定向到此 URL。
- **客户域名**和**客户域 ID** - 客户域名和 ID 用于在 SAML SSO 页面中创建应用程序 URL 和其他后续 URL。

  例如，如果您要添加 Salesforce 应用程序，您的域名是 `salesforceformyorg`，ID 是 123754，则应用程序 URL 是 `https://salesforceformyorg.my.salesforce.com/?so=123754.`。

  客户域名和客户 ID 字段特定于某些应用程序。

- **相关域** – 相关域会根据您提供的 URL 自动填充。相关域有助于服务将 URL 识别为应用程序的一部分并相应地路由流量。您可以添加多个相关域。

  注意：

  如果添加了重复的相关域，或者相关域也作为不同应用程序的 URL 添加，则会出现警告消息。为避免这些问题，请参阅Web 和 SaaS 应用程序配置的最佳实践。

- **导入 HAR** – 您可以上传 HAR 文件以自动发现应用程序访问的域。查看发现的域并选择要添加到应用程序相关域配置中的域。这通过减少手动识别和配置相关域的需要来简化应用程序的入职。有关更多信息，请参阅使用 HAR 文件发现相关域。
- **保持一致连接** - SaaS 应用程序支持与连接器设备的一致连接。选中“**保持一致连接**”复选框，并在“**应用程序连接**”部分中选择“**通过连接器内部**”作为连接类型。有关一致连接的详细信息，请参阅保持一致连接。
- Click **将应用程序添加到 Workspace 应用程序中的收藏夹** 以将此应用程序添加为 Citrix Workspace 应用程序中的收藏应用程序。

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

- Click **允许用户从收藏夹中删除** 以允许应用程序订阅者从 Citrix Workspace 应用程序中的收藏应用程序列表中删除该应用程序。选择此选项后，Citrix Workspace 应用程序中应用程序的左上角将显示一个黄色星形图标。
- Click **不允许用户从收藏夹中删除** 以防止订阅者从 Citrix Workspace 应用程序中的收藏应用程序列表中删除该应用程序。选择此选项后，Citrix Workspace 应用程序中应用程序的左上角将显示一个带挂锁的星形图标。

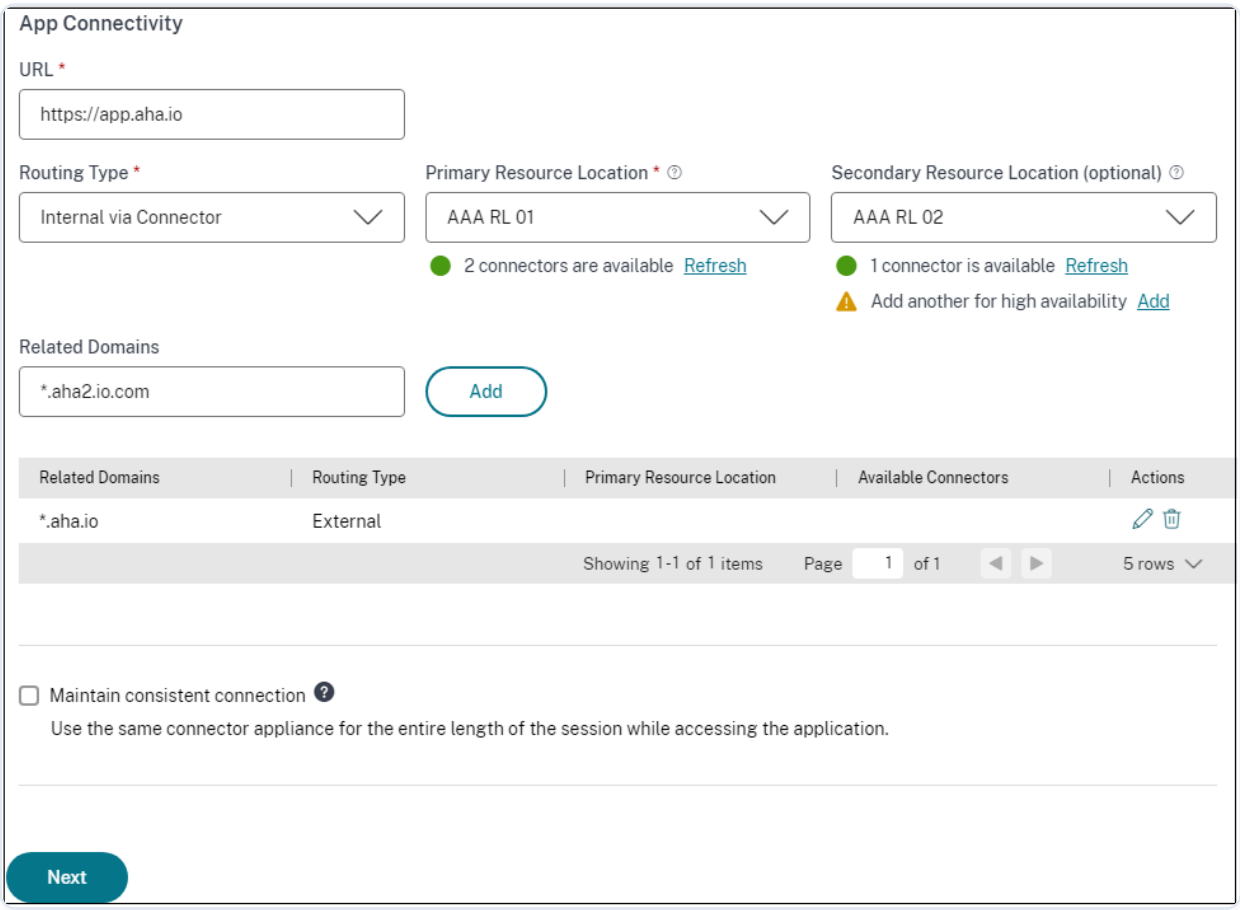
如果您从 Secure Private Access 服务控制台删除标记为收藏的应用程序，则用户必须手动从其商店中的收藏列表删除这些应用程序。如果从 Secure Private Access 服务控制台删除，应用程序不会自动从商店中删除。

重要提示：

- 对 SaaS 应用程序的访问由其访问策略控制。根据与用户匹配的访问策略规则，应用程序被授予访问权限、阻止或保持非托管状态。如果没有规则与用户匹配，或者没有访问策略与应用程序关联，则应用程序不会被阻止。它将保持非托管状态，浏览器将直接连接到它。要阻止未被任何规则覆盖的用户访问应用程序，请在最低优先级添加“所有用户”>“拒绝访问”规则。有关详细信息，请参阅默认阻止 SaaS 应用程序。
- 如果多个应用程序配置了相同的 FQDN 或通配符 FQDN 的某些变体，这可能会导致配置冲突。
- 这些问题可以通过遵循一些最佳实践来解决。有关详细信息，请参阅Web 和 SaaS 应用程序配置的最佳实践。

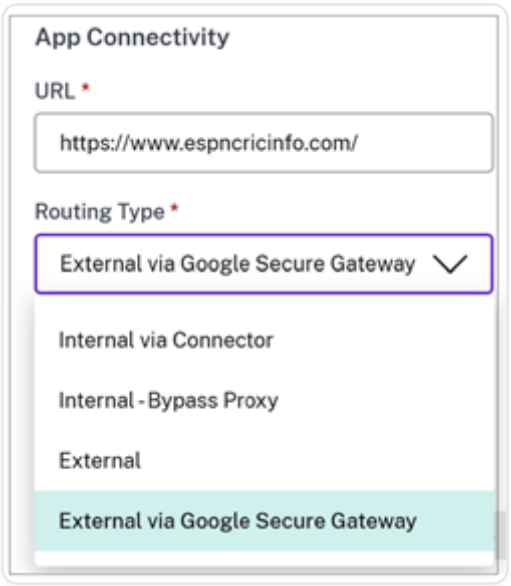
5. 在**应用程序连接**部分中，您可以定义应用程序相关域的路由，如果这些域必须通过 Citrix Connector™ Appliance 外部或内部路由。

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



- **路由类型** - 选择以下选项之一：
  - **内部 – 绕过代理** - 域流量通过 Connector Appliance™ 路由，绕过在 Connector Appliance 上配置的客户 Web 代理。
  - **通过连接器内部** - 应用程序可以是外部的，但流量必须通过 Connector Appliance 流向外部网络。
  - **外部** – 流量直接流向互联网。
  - **通过 Google Secure Gateway 外部** — 流量通过 Google Secure Gateway 流向互联网。有关详细信息，请参阅通过 Google Secure Gateway 路由。

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



- **主资源位置和辅助资源位置** - 管理员可以通过配置辅助资源位置或使用“**首先可用**”选项，确保即使在中断期间应用程序也具有高可用性。

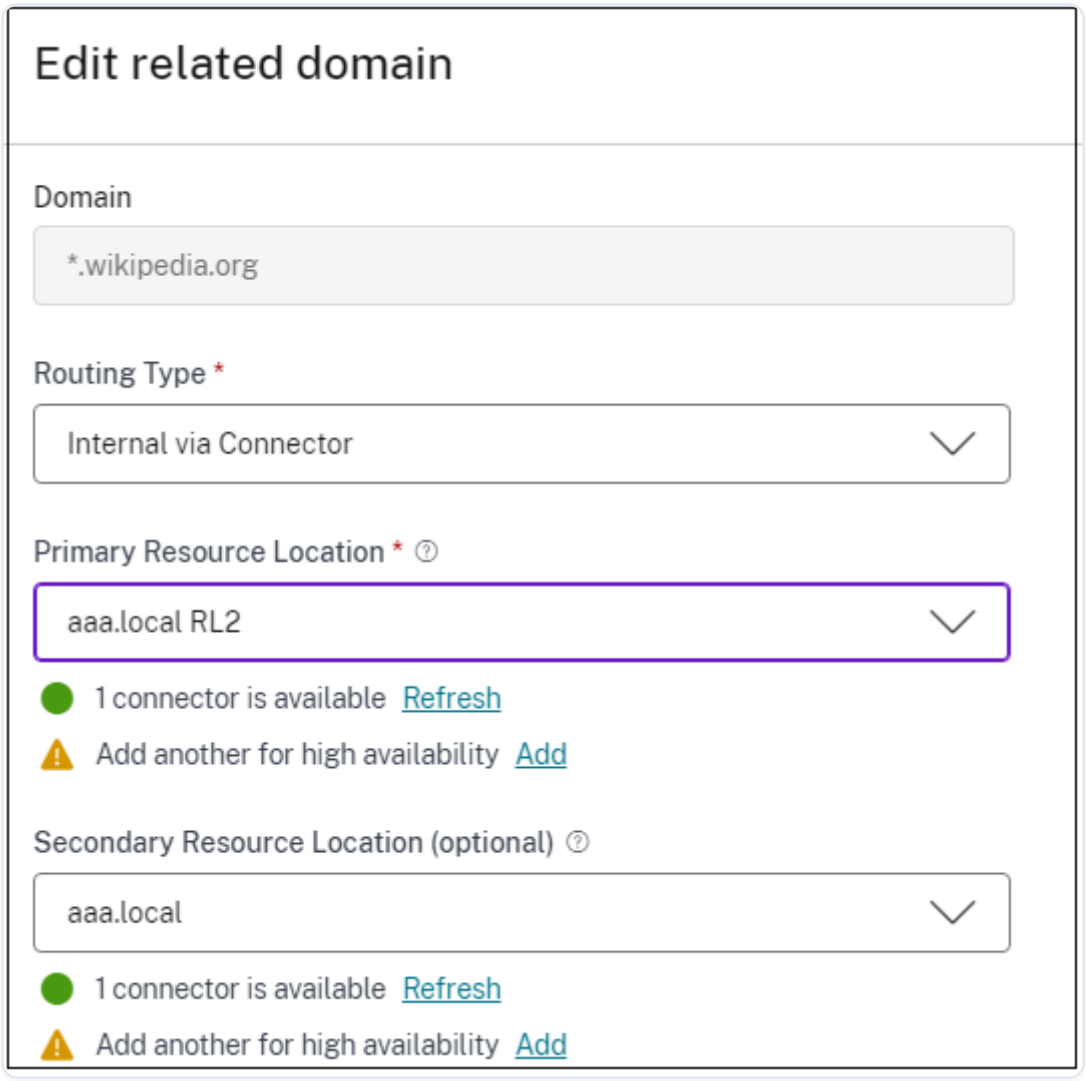
  - **主资源位置：** 选择托管应用程序的主资源位置。或者，管理员可以在“**主资源位置**”中选择“**首先可用**”选项。
  - **首先可用：** “**首先可用**”选项可确保使用正常工作的资源位置。选择“**首先可用**”后，系统会自动将流量路由到第一个可用位置。这可确保无需手动干预即可持续访问应用程序。例如，如果 ResourceLocation1 不可用但 ResourceLocation2 可访问，则默认选择 ResourceLocation2 作为应用程序的前端。
  - **辅助资源位置** - 只有明确指定主资源位置后，“**辅助资源位置**”选项才可用。如果主资源位置因连接器设备或数据中心故障等原因变得不可用，应用程序将故障转移到指定的辅助资源位置。即使应用程序托管在另一个数据中心，辅助资源位置也可以充当故障转移。

  您还可以为每个相关域设置主资源位置和辅助资源位置，或选择“**首先可用**”选项。

  a. 单击“相关域”表“**操作**”列中的编辑图标。

  b. 设置主资源位置和辅助资源位置，或选择“**首先可用**”选项。

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



注意：

- 设置备份资源位置和使用“**首先可用**”选项功能目前处于预览阶段。
- 删除应用程序时，其路由条目会自动删除。有关详细信息，请参阅删除应用程序时自动清理路由条目。

- **保持一致连接** - 选中此复选框可启用与同一连接器设备的一致连接。有关一致连接的详细信息，请参阅保持一致连接。

注意：

选择“**保持一致连接**”选项后，应用程序的路由类型必须在“应用程序连接”部分设置为“**通过连接器内部**”。

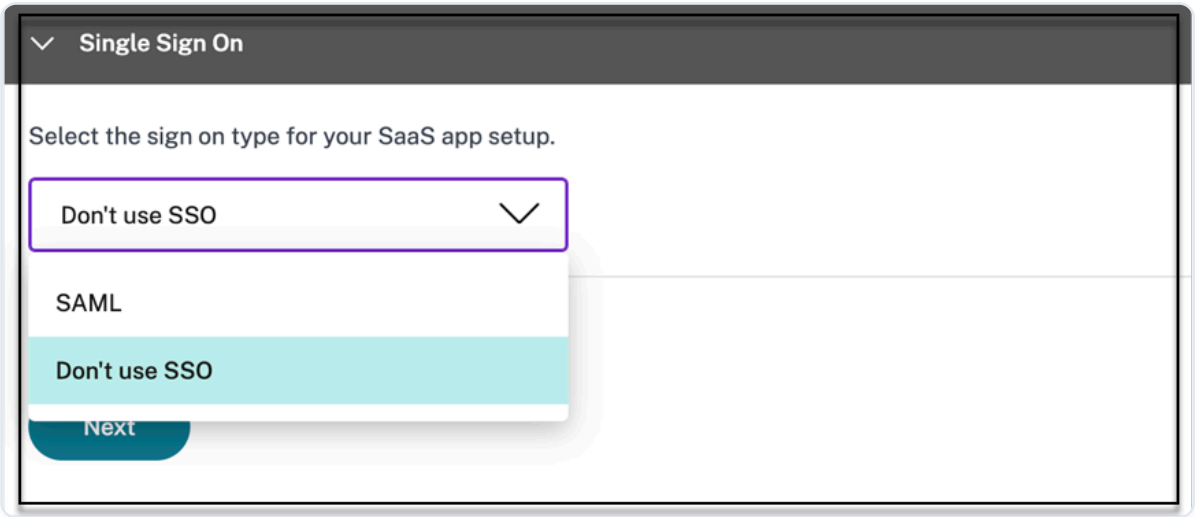
6. 设置首选登录方法。

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

注意：

单点登录选项不适用于 Citrix Secure Access with Chrome Enterprise (CEP)。

a. 在“**单点登录**”部分中，选择您的应用程序要使用的首选单点登录类型，然后单击“**保存**”。以下单点登录类型可用。



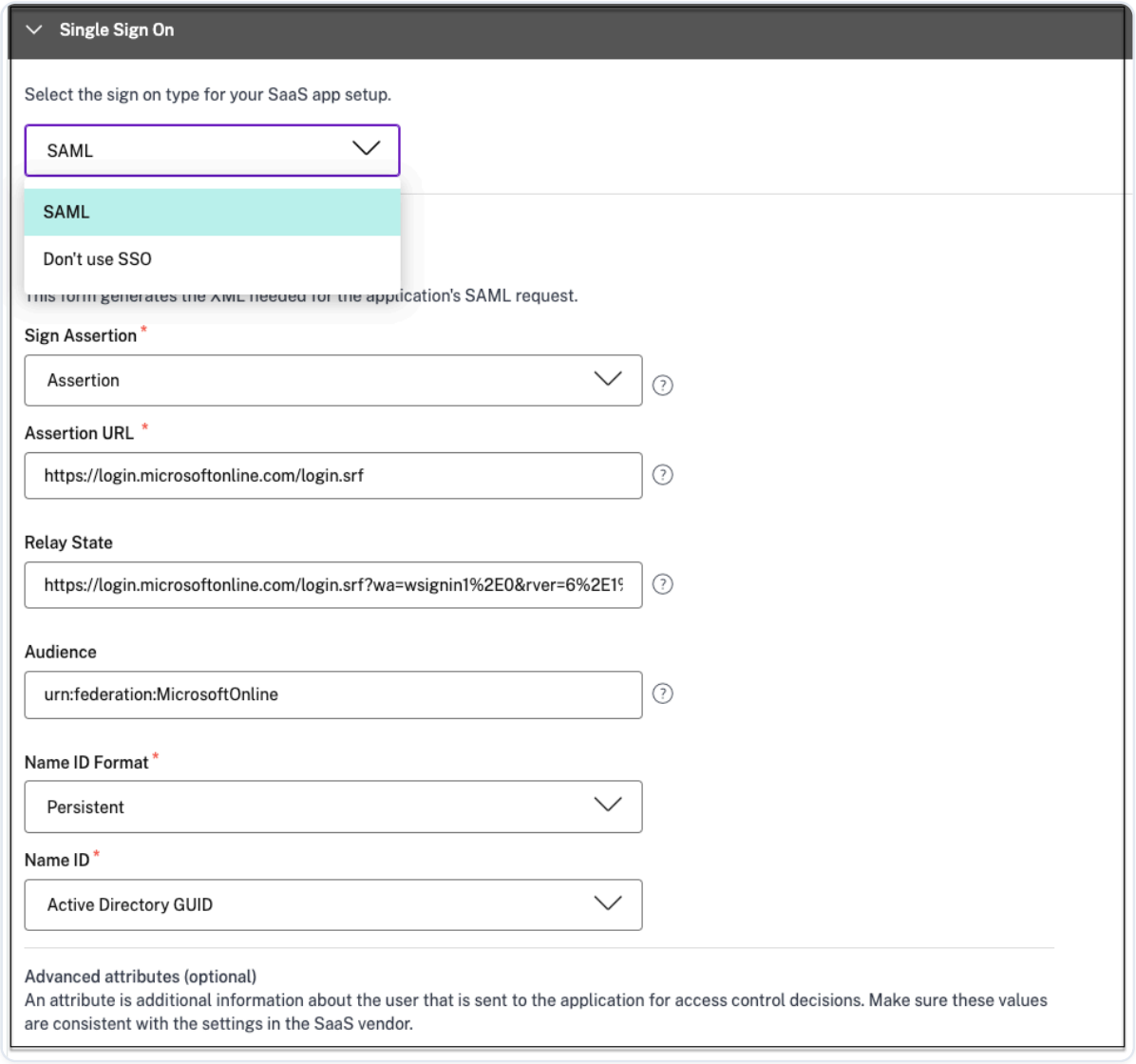
- **不使用 SSO** – 当您不需要在后端服务器上对用户进行身份验证时，请使用“**不使用 SSO**”选项。选择“**不使用 SSO**”选项后，用户将被重定向到“**应用程序详细信息**”部分下配置的 URL。
- **SAML** - 选择 **SAML** 以实现基于 SAML 的 Web 应用程序 SSO。输入 **SAML** SSO 类型的配置详细信息。

在“登录”部分中输入以下详细信息，然后单击“**保存**”。

- **签名断言** - 签名断言或响应可确保在将响应或断言传递给信赖方 (SP) 时消息的完整性。您可以选择 **断言、响应、两者** 或 **无**。
- **断言 URL** – 断言 URL 由应用程序供应商提供。SAML 断言将发送到此 URL。
- **中继状态** – 中继状态参数用于标识用户登录并定向到信赖方联合服务器后访问的特定资源。中继状态为用户生成一个 URL。用户可以单击此 URL 登录到目标应用程序。
- **受众** – 受众由应用程序供应商提供。此值确认 SAML 断言是为正确的应用程序生成的。
- **名称 ID 格式** – 选择支持的名称标识符格式。
- **名称 ID** – 选择支持的名称 ID。
- 选择“**使用特定 URL 启动应用程序（SP 发起）**”以覆盖身份提供程序发起的流程，并仅使用服务提供程序发起的流程。

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

b. 在 **高级属性（可选）** 中，添加有关用户的其他信息，这些信息将发送到应用程序以进行访问控制决策。



c. 通过单击 **SAML 元数据** 下的链接下载元数据文件。使用下载的元数据文件在 SaaS 应用程序服务器上配置 SSO。

- 您可以复制 **登录 URL** 下的 SSO 登录 URL，并在 SaaS 应用程序服务器上配置 SSO 时使用此 URL。
- 您还可以从 **证书** 列表中下载证书，并在 SaaS 应用程序服务器上配置 SSO 时使用该证书。

7. 单击 **保存**，然后单击 **完成**。

单击 **完成** 后，应用程序将添加到“应用程序”页面。配置应用程序后，您可以从“应用程序”页面编辑或删除应用程序。为此，请单击应用程序上的省略号按钮并相应地选择操作。

- **编辑应用程序**

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

- **删除**

通过 Google Secure Gateway 路由

当您将 SaaS 应用程序的路由类型设置为 **通过 Google Secure Gateway 外部路由** 时，该应用程序的流量将通过 Google Secure Gateway 路由到互联网，而不是直接从客户端路由。

- 您可以在应用程序配置期间设置此路由类型，它将成为该应用程序的默认路由。
- 您还可以将其设置为访问策略中的路由例外，它仅适用于该策略中的用户，并覆盖应用程序的默认路由。
- 此路由类型仅适用于 SaaS 应用程序，并且仅适用于与 Google Chrome Enterprise Premium 集成的客户。它不适用于内部 Web 应用程序。
- 在 Citrix Secure Access 客户端中，此选项的行为与 **外部** 相同。在导入期间，将 **路由类型** 值设置为 **通过 Google Secure Gateway 外部路由**。

注意：

对于通过 Citrix Enterprise Browser™ 访问的 SaaS 应用程序，**路由类型**显示为**通过 Google Secure Gateway 外部**，而不是**外部**。这仅仅是 UI 显示差异，不会改变路由行为。流量将继续直接流向互联网。

删除应用程序时自动清理路由条目

配置应用程序时，其目标（FQDN 或应用程序域）会添加到路由表，Secure Private Access 使用该路由表进行路由决策。删除应用程序时，Secure Private Access 会根据以下规则清理路由条目：

- **未引用的条目将被删除** - 如果与已删除应用程序关联的路由条目（FQDN 或应用程序域）未被任何其他应用程序引用，Secure Private Access 将自动将其从路由表中删除。
- **共享条目将保留** - 如果路由条目被多个应用程序使用，删除其中一个应用程序不会删除共享条目。只要至少有一个活动应用程序引用该条目，该条目就会保留在路由表中。
- **不追溯删除** - 路由条目仅作为应用程序删除的一部分进行评估和删除。除非确认现有条目未被任何应用程序使用，否则不会追溯删除。

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

注意：

- 当从“应用程序”页面（使用省略号 (...) 菜单）删除应用程序时，清理会自动运行。无需管理员操作。
- 由于共享路由条目会保留，删除应用程序不会中断对共享相同目标的其他应用程序的访问。

SaaS 应用程序服务器特定配置

以下是有关使用模板进行应用程序服务器特定配置的文档链接。Citrix 目前支持以下 SaaS 应用程序，并正在不断增加对更多应用程序的支持。

- 15Five - 持续绩效管理工具，用于指导员工。
- 10000 ft - 项目管理工具，用于规划增长。
- 4me - 服务管理工具，用于内部、外部和外包团队之间的协作。
- Abacus - 实时费用报告软件。
- Absorb - 学习管理工具。
- Accompa - 用于构建产品的需求管理工具。
- Adobe Captivate Prime - 学习管理系统，用于在不同设备上提供个性化学习体验。
- Aha - 产品路线图和营销规划工具，用于构建产品和启动营销活动。
- AlertOps - 协作事件响应工具，用于管理 IT 事件。
- Allocadia - 营销绩效管理工具，用于管理组织的营销规划流程。`
- Ana plan - 规划工具，通过连接数据、人员和计划来帮助组织进行决策。
- &frankly - 一种用于推动工作场所变革的参与工具。
- Anodot - 一个 AI 平台，用于实时监控时间序列数据、检测异常并预测业务绩效。
- App Follow - 产品管理工具，用于加速全球应用增长并提高客户忠诚度。
- Assembla - 软件开发的版本控制和源代码管理工具。
- Automox - 补丁管理工具，用于跟踪、控制和管理补丁过程。
- Azendoo - 团队沟通协作工具。
- BambooHR - 人力资源管理工具，用于管理员工数据。
- Bananatag - 用于跟踪和安排电子邮件、跟踪文件和创建电子邮件模板的工具
- Base CRM - 用于管理电子邮件、电话和笔记的销售管理工具。

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

- Beekeeper - 用于将多个运营系统和通信渠道集成到一个可从桌面和移动设备访问的安全中心中的工具。
- BitaBIZ - 用于请假和缺勤管理的缺勤和休假规划及通信工具。
- BlazeMeter - 测试套件。
- Blissbook - 用于创建员工手册的策略管理工具。
- BlueJeans - 视频会议解决方案。
- Bold360 - 用于客户互动的实时聊天工具。
- Bonusly - 用于表彰团队贡献的员工表彰和奖励管理工具。
- Box - 内容管理和文件共享工具，用于管理、共享和访问您的内容。
- Branch - 一个为深度链接和移动设备提供支持的移动链接平台。
- Brandfolder - 用于存储和共享数字资产的数字资产管理工具。
- Breezy HR - 招聘软件和申请人跟踪系统。
- `Buddy Punch` - 用于监控员工出勤的时间管理工具。
- Bugsnag - 用于管理应用程序稳定性并报告错误和诊断数据的监控工具。
- Buildkite - 用于持续集成软件开发的基础设施工具。
- Bullseye Locations - 用于在设备上定位商店或经销商的商店定位工具。
- CA Flowdock - 团队交流与协作的协作工具。
- CakeHR - 用于考勤和绩效管理的人力资源管理工具。
- Cardboard - 用于跟踪无序信息的协作产品规划工具。
- Citrix Cedexis - 大型网站的流量管理工具，可利用数据中心、云提供商和内容分发网络的多供应商采购。
- CipherCloud - 为采用云应用程序的企业提供端到端数据保护、高级威胁防护和全面合规功能的平台。
- Celoxis - 用于创建项目计划、自动化工作和协作的项目管理工具。
- CircleHD - 用于在组织内共享视频和幻灯片的培训、学习和协作工具。
- Circonus - 用于提供警报、图表、仪表板和机器学习智能的数据分析和监控工具。
- Cisco Umbrella - 提供互联网威胁第一道防线的云安全平台。
- ClearSlide - 销售互动工具，允许用户共享内容和销售材料以进行客户互动。
- Cloudability - 云成本管理平台，用于提高云环境的可见性、优化和治理。

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

- CloudAMQP - 用于在进程和其他系统之间传递消息的消息队列工具。
- CloudCheckr - 成本管理、安全、报告和分析工具，可帮助用户优化其 AWS 和 Azure 部署。
- CloudMonix - 用于云和本地资源监控及自动化的工具。
- CloudPassage - 用于降低网络风险和保持合规性的可见性和持续监控工具。
- CloudRanger - 用于简化 AWS 云备份、灾难恢复和服务器控制的工具。
- Clubhouse - 软件开发项目管理工具。
- Coggle - 用于创建分层结构文档（如分支树）的思维导图 Web 应用程序。
- Comm100 - 面向客户服务专业人员的客户服务软件和通信工具。
- Confluence - 帮助团队协作和共享知识的内容协作工具。
- ConceptShare - 用于更快、更迅速、更经济地交付内容的校对工具。
- Concur - 用于随时随地管理开支的差旅和费用管理工具。
- ConnectWise Control - 用于提供远程支持和访问的业务管理工具。
- Contactzilla - 用于访问最新联系人信息的联系人管理工具。
- ContractSafe - 用于跟踪、存储和管理合同的合同管理工具。
- Contentful - 用于创建、管理和分发内容到任何平台的内容软件。
- Convo - 用于内部对话的团队沟通和协作工具。
- Copper - CRM 工具。
- Cronitor - 用于 cron 作业的监控工具。
- Crowdin - 为开发人员提供无缝、持续本地化解决方案的工具。
- Dashlane - 密码管理工具，同时管理数字钱包。
- Declaree - 用于商务旅行的差旅和费用管理工具。
- Dell Boomi - 连接云和本地应用程序及数据的集成工具。
- Deskpro - 帮助台工具，用于促进工单管理、客户自助服务和客户反馈。
- Deputy - 劳动力管理工具，用于安排和跟踪员工的时间、任务和沟通。
- DigiCert - 网站 SSL 证书的证书管理和故障排除工具。
- Dmarcian - 电子邮件监控工具，用于过滤垃圾邮件、恶意软件和网络钓鱼。
- DocuSign - 用于不同文档（如保险、医疗和房地产）的在线签名工具。
- DOME9 ARC - 用于管理公共云环境的安全和合规工具。
- Dropbox - 用于安全文件共享和存储的云存储工具。

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

- Duo - 提供对应用程序安全访问的安全工具。
- Dynatrace - 医疗实验室服务。
- Easy Projects - 项目管理工具。
- EdApp - 用于工作区学习的学习管理工具。
- EduBrite - 用于创建、交付和跟踪培训程序的学习管理工具。
- Ekarda - 电子贺卡设计工具。
- Envoy - 用于管理人员和包裹的访客管理工具。
- Evernote - 用于笔记、整理、任务列表和归档的应用程序。
- Expensify - 用于费用报告管理、收据跟踪和商务差旅的费用管理工具。
- ezeep - 打印基础架构管理工具，可从任何设备、任何位置打印到云中的任何打印机。
- EZOfficeInventory - 用于跟踪所有资产和设备的库存管理工具。
- EZRentOut - 用于跟踪设备质量和可用性的设备租赁工具。
- Fastly - 边缘云平台，用于向更接近用户的应用程序提供服务并确保其安全。
- Favro - 用于组织流程的规划和协作工具。
- Federated Directory - 跨公司联系人目录工具，用于搜索不同公司的企业通讯录。
- 馈送器
- Feedly - 新闻聚合工具，用于从不同来源编译新闻源。
- FileCloud - 为组织提供强大且安全的文件托管和共享平台的软件解决方案。
- Fivetran - 帮助分析师将数据复制到云数据仓库的工具。
- Flatter Files - 用于图纸和文档的数字扁平文件柜，提供安全简单的方式来访问内容。
- Float - 用于项目调度和管理团队利用率的资源规划工具。
- Flock - 协作工具。
- Formstack - 在线表单构建器和数据收集工具。
- FOSSA - 内置于 CI/CD 中的自动化开源许可证扫描和漏洞管理工具。
- Freshdesk - 客户支持工具，帮助满足客户需求。
- Freshservice - IT 帮助台工具，用于简化 IT 运营。
- FrontApp - 协作工具，用于在一个地方管理所有对话。
- Frontify - 一个平台，用于促进和简化日常品牌、营销和开发运营。
- Fulcrum - 移动数据收集平台，可让您轻松构建移动表单并收集数据。

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

- Fusebill - 账单管理和循环计费软件。
- G-Suite - 一套智能应用程序，用于连接公司内部人员。
- GetGuru - 知识管理软件。
- GitBook - 用于创建和维护文档的工具。
- GitHub - 一个基于网络的托管服务，用于使用 Git 对企业防火墙后托管的存储库进行版本控制。
- GitLab - 一个完整的 DevOps 平台，以单个应用程序的形式交付。
- GlassFrog - 用于 Holacracy 实践的软件。
- GoodData - 一个嵌入式 BI 和分析平台，提供快速、可靠且易于使用的分析功能
- GotoMeeting - 具有高清视频会议功能的在线会议软件。
- HackerRank - 为消费者和企业提供竞争性编程挑战。
- HappyFox - 在线帮助台软件和基于网络的工单支持系统。
- Helpjuice - 用于创建和维护知识库的知识管理解决方案。
- Help Scout - 面向客户服务专业人员的客户服务软件和知识库工具。
- Hello sign - 电子签名界面，可随时随地在任何设备上进行签名。
- HelpDocs - 知识库软件，可在用户遇到困难时提供指导。
- Honeybadger - 应用程序健康监控工具。
- Harness - 用于在 AWS、GCP、Azure 和裸机上对 Java、.NET 应用程序进行持续交付和集成的工具。
- HelpDocs - 用于创建权威知识库的工具，可在用户遇到困难时提供指导。
- Helpmonks - 一个用于团队协作的协作式电子邮件平台。
- Hoshinplan - 用于在一个画布上可视化您的战略计划并跟踪状态的工具。
- Hosted Graphite - 用于监控您的网站、应用程序、服务器和容器性能的工具。
- Humanity - 用于管理班次、日程、工资单和考勤的在线员工排班软件。
- Igloo - 解决您组织中 IT 挑战的数字工作场所和内网解决方案提供商。
- iLobby - 基于云的访客登记管理解决方案。
- Illumio - 用于防止数据中心和云环境中漏洞扩散的安全系统。
- Image Relay - 用于安全地组织和共享数字文件的数字资产管理和品牌管理软件。
- Informatica - 用于 SaaS 应用程序集成的工具，以及用于开发和部署自定义集成服务的平台。
- Intelligent contract - 合同管理软件。

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

- iMeet Central - 适用于营销人员、创意机构和企业级业务的项目管理软件。
- InteractGo - 用于测量系统性能的实时和历史数据的工具。
- iQualify One - 用于提供真实学习体验的学习和管理工具。
- InsideView - 用于解决销售、营销和其他业务挑战的数据和智能解决方案。
- Insightly - 适用于中小型企业的基于云的客户关系管理 (CRM) 和项目管理工具。
- ITGlue - 一个基于云的 IT 文档平台，可帮助 MSP 规范文档、创建知识库、管理密码和跟踪设备。
- Jitbit - 帮助台软件和票证系统，用于管理和跟踪传入的支持请求电子邮件及其相关票证。

JupiterOne - 用于创建和管理整个安全流程的软件平台。

- Kanbanize - 一款用于精益管理的在线投资组合看板软件。
- Klipfolio - 一个在线仪表板平台，用于为您的团队或客户构建强大的实时业务仪表板。
- Jira - 用于规划、跟踪和管理您的议题和项目的工具。
- Kanban Tool - 可视化管理软件，可提高团队绩效并提高生产力。
- Keeper Security - 密码管理器和安全软件，用于保护您的密码和私人信息。
- Kentik - 一款利用大数据进行网络和性能监控、DDoS 防护以及实时即席网络流量分析的工具。
- Kissflow - 工作流工具和业务流程工作流管理软件，可自动执行您的工作流流程。
- KnowBe4 - 提供安全意识培训和模拟网络钓鱼的工具。
- KnowledgeOwl - 知识库和创作工具。
- Kudos - 零售、工作、项目和履行流程系统。
- LaunchDarkly - 功能管理平台，使开发和运维团队能够控制功能生命周期。
- Lifesize - 视频会议解决方案。
- Litmos - 用于员工培训、客户培训、合规性培训和合作伙伴培训的学习管理系统。
- LiquidPlanner - 适用于您企业的在线项目管理软件。
- LeanKit - 基于精益的企业流程和工作管理软件，可帮助企业可视化工作、优化流程并更快地交付。
- LiveChat - 适用于企业的实时聊天和帮助台软件。
- LogDNA - 用于在一个集中式日志记录工具中收集、监控、解析和分析来自所有来源的日志的工具。
- Mango - 团队协作软件，可将孤立的应用程序整合并简化到一个单一平台中。
- Manuscript - 一款写作工具，可帮助您规划、编辑和分享您的作品。

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

- Marketo - 自动化软件，可帮助营销团队掌握数字营销的艺术和科学。
- Matomo - 一个网络分析平台，用于评估所有访问网站的用户的完整用户旅程。
- Meisterplan - 帮助组织创建项目组合的软件。
- Mingle - 一款敏捷项目管理和协作工具，为整个团队提供一个组合式工作场所。
- MojoHelpdesk - 帮助台软件和票务系统。
- Monday - 团队管理软件，可在一个工具中规划、跟踪和协作您的所有工作。
- Mixpanel - 用于跟踪用户与网络和移动设备交互的系统。
- MuleSoft - 集成软件，用于连接云端和本地的 SaaS 和企业应用程序。
- MyWebTimesheets - 在线时间跟踪系统，用于跟踪在各种项目/工作/活动上花费的时间。
- New Edge - 适用于混合 IT 的安全应用程序网络服务。
- NextTravel - 企业差旅管理软件工具。
- N2F - 用于管理您的业务和差旅费用的费用报告管理工具。
- New Relic - 用于衡量和监控应用程序和基础设施性能的数字智能平台。
- Nmbrs - 适用于企业的云 HR 和薪资软件。
- Nuclino - 用于实时协作和共享信息的协作软件。
- Office365 - 微软的云订阅服务。
- OfficeSpace - 一个基于云的平台，可帮助组织分配工作空间。
- OneDesk - 项目管理和帮助台软件，用于与客户建立联系并提供支持。
- OpsGenie - 一个事件管理平台，供 DevOps 和 IT 运维团队简化警报和事件解决流程。
- Orginio - 一个在线组织结构图创建工具，用于可视化组织结构。
- Oomnitza - IT 资产管理平台解决方案，用于跟踪和管理资产。
- OpenEye - 用于在 Apex 录像机上观看实时和录制视频的移动应用程序。
- Oracle ERP Cloud - 基于云的软件应用程序套件，用于管理企业功能。
- Pacific Timesheet - 基于网络的工时表工具，用于薪资、项目工时和费用。
- PagerDuty - 数字化运营管理系统。
- PandaDoc - 一款移动应用程序，供 iPhone 用户直接在其手机上访问文档、分析和仪表板。
- Panopta - 基础设施监控工具。
- Panorama9 - 用于企业网络监控的基于云的 IT 管理平台。
- Papyrs - 用于设计您自己的内网页面的编辑器。
- ParkMyCloud - 一款用于连接 AWS、Azure 服务或 GCP 的单一用途 SaaS 工具。

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

- Peakon - 用于衡量和提高员工敬业度的工具。
- People HR - 适用于所有关键 HR 职能的 HR 软件系统。
- Pingboard - 用于构建组织结构图以组织团队和进行劳动力规划的工具。
- Pigeonhole Live - 交互式问答平台。
- Pipedrive - 销售 CRM 和渠道管理软件。
- PlanMyLeave - 用于管理和跟踪员工休假的请假管理系统。
- PlayVox - 客户服务质量监控工具。
- Podbean - 播客服务提供商。
- Podio - 一款基于网络的工具，用于在项目管理工作区中组织团队沟通、业务流程、数据和内容。
- POPin - 众包解决平台和移动应用程序，可将团队协作用于解决问题
- Postman - API 开发环境。
- Prescreen - 用于在线和离线发布职位空缺的申请人跟踪工具。
- ProductBoard - 产品管理工具。
- ProdPad - 用于制定产品策略的产品管理软件。
- Proto.io - 应用程序原型设计平台，用于创建完全交互式的高保真原型。
- Proxyclick - 基于云的访客管理解决方案，用于管理访客、建立品牌形象并确保安全性。
- Pulumi - 用于容器、无服务器、基础设施和 Kubernetes 的云原生开发平台。
- PurelyHR - 用于访问员工休假数据的休假管理工具。
- Promapp - 业务流程管理 (BPM) 工具。
- Prescreen - 基于云的申请人跟踪系统，用于在线和离线发布职位空缺。
- QAComplete - 软件测试管理工具。
- Qualaroo - 用于从客户那里获取见解的反馈工具。
- Quality Built, LLC - 为保险、金融和建筑行业提供可靠且创新的第三方质量保证服务。
- Qubole - 基于 Amazon 构建的用于大数据分析的自助服务平台。
- Questetra BPM Suite - 用于日常工作流的基于 Web 的业务流程平台。
- QuestionPro - 用于创建调查和问卷的在线调查软件。
- Quandora - 基于问答的知识管理解决方案。
- Quip - 适用于移动设备和 Web 的协作生产力软件套件。
- Rackspace - 托管式云计算服务。

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

- ReadCube - 用于 Web、桌面和移动参考管理的工具。
- RealtimeBoard - 白板协作工具，供组织跨格式、工具、地点和时区进行协作。
- Receptive - 在一个地方收集客户、团队和市场反馈的工具。
- Remedyforce - IT 服务管理和帮助台系统。
- Retrace - 一个应用程序性能管理工具，提供错误跟踪、数据聚合和自动警报。
- Robin - 工作场所体验工具，用于安排会议室和办公桌预订。
- Rollbar - 为开发人员提供的实时错误警报和调试工具。
- Really Simple Systems - 基于云的 CRM 软件，供小型企业管理其销售和营销。
- Reamaze - 客户支持软件，可在单个平台上通过聊天、社交媒体、短信、常见问题解答和电子邮件支持、吸引和转化客户。
- Resource Guru - 资源管理软件，用于安排人员、设备和其他资源。
- Retrace - 应用程序性能管理，用于集成代码分析、错误跟踪、应用程序日志和指标。
- Roadmunk - 产品路线图软件和路线图工具，用于创建产品路线图。
- Runscope - 用于创建、管理和运行功能性 API 测试和监视器的工具。
- Salesforce – CRM 工具，用于管理客户联系信息、集成社交媒体并促进实时客户协作。
- SalesLoft - 销售互动平台，可实现高效且提高收入的销售。
- Salsify - 产品体验管理 (PXM) 平台。
- Samanage - IT 服务管理工具。
- Samepage - 协作软件，用于管理在线项目。
- Screencast-O-Matic – 用于屏幕录制和视频编辑的工具。
- ScreenSteps – 用于创建以屏幕截图为中心的视觉文档的工具。
- SendSafely – 用于安全交换文件和电子邮件的加密平台。
- Sentry - 开源错误跟踪软件。
- ServiceDesk Plus - IT 服务台工具。
- ServiceNow - 用于创建数字工作流的云平台。
- SharePoint – 用于文档管理和存储的协作平台。
- Shufflrr - 用于创建、更新、共享和广播演示文稿的演示文稿管理工具。
- Sigma Computing – 用于探索、分析和可视化数据的分析工具。
- Signavio – 业务流程建模工具。
- Skeddly - 自动化 AWS 资源的工具。

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

- Skills Base - 用于跟踪和记录员工绩效和技能的人才管理工具。
- Skyprep - 用于培训客户和员工的学习管理系统 (LMS)。
- Slack - 用于沟通和共享信息的协作工具。
- Slemma - 用于从多个数据集创建数据报告的数据分析工具。
- Sli.do - 用于会议、活动和大会的互动工具。
- SmartDraw - 用于制作流程图、组织结构图、思维导图、项目图表和其他业务可视化的图表工具。
- SmarterU - 用于培训客户和员工的学习管理系统 (LMS)。
- Smartsheet - 用于分配任务、跟踪项目进度、管理日历和共享文档的协作工具。
- SparkPost - 电子邮件投递服务。
- Split - 账单分摊应用程序。
- Spoke - 用于提交服务工单的服务台工具。
- Spotinst - 一个SaaS优化平台，帮助公司购买和管理云基础设施容量。
- SproutVideo - 用于托管商业视频的平台。
- Stackify - 故障排除工具，提供包括Prefix和Retrace在内的工具套件支持。
- StatusCast - 托管页面，用于让您的员工和客户了解停机时间和网站维护情况。
- StatusDashboard - 用于托管状态仪表板并向客户广播事件通知的通信平台。
- Status Hero - 用于跟踪团队状态更新和每日目标的工具。
- StatusHub - 用于托管服务状态页面的平台。
- Statuspage - 用于沟通状态和事件的工具。
- SugarCRM - 用于销售自动化、营销活动、客户支持、协作、移动CRM、社交CRM和报告的CRM工具。
- Sumo Logic - 专注于安全性、运营和BI用例的数据分析软件。
- Supermood - 用于实时收集员工反馈的人力资源平台。
- Syncplicity - 用于共享和同步文件的工具。
- Tableau - 用于创建交互式数据可视化的工具。
- TalentLMS - 学习管理系统 (LMS)，用于促进在线研讨会、课程和其他培训计划。
- Tallie – 用于捕获和上传收据、生成费用报告以及自定义费用详细信息的工具。
- Targetprocess - 敏捷项目管理软件，支持 Scrum、看板、SAFe 等。
- Teamphoria - 提供实时员工敬业度指标、员工评价和表彰的软件。

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

- TeamViewer - 用于远程控制、桌面共享、在线会议、网络会议以及计算机之间文件传输的专有软件应用程序。
- Tenable.io - 提供数据以识别、调查并优先处理 IT 环境中漏洞和错误配置修复的工具。
- Testable - 用于创建行为实验和调查的工具。
- TestingBot - 提供各种浏览器版本以进行实时和自动化测试的工具。
- TestFairy - 移动测试平台，为公司提供移动会话的视频录制、日志和崩溃报告。
- TextExpander - 通信工具，可在您键入时从电子邮件和其他内容存储库中插入文本片段。
- TextMagic - 用于与客户联系的消息服务。
- ThousandEyes - 用于监控网络基础设施、排查应用程序交付问题和映射互联网性能的工具。
- Thycotic Secret server - 用于管理密码的账户管理软件工具。
- TimeLive – 提供时间表和跟踪时间的工具。
- Tinfoil Security - 用于检查漏洞的安全解决方案软件。
- Trisotech - 允许客户发现、建模和分析其数字企业的工具。
- Trumba - 用于发布在线交互式活动日历的工具。
- TwentyThree - 视频营销平台，用于将视频集成并添加到营销堆栈。
- Twilio - 一个用于通信的开发人员平台。
- Ubersmith - 业务管理软件，用于基于使用量的计费、报价、订单管理、基础设施管理和帮助台票务解决方案。
- UniFi - 具有语音、网络协作和视频会议功能的通信和协作软件。
- UPTRENDS – 网站监控解决方案，用于跟踪网站正常运行时间和性能。
- UserEcho - 社区论坛工具，可帮助企业管理客户反馈。
- UserVoice - 产品反馈管理软件，使企业能够做出数据驱动的产品决策。
- VALIMAIL - 电子邮件身份验证软件，用于验证合法电子邮件并阻止网络钓鱼攻击。
- Veracode - 源代码分析器和代码扫描器，可保护企业免受网络威胁和应用程序后门攻击。
- Velpic - 学习管理系统 (LMS)，旨在简化工作场所培训。
- VictorOps - 事件管理软件，提供 DevOps 可观察性、协作和实时警报。
- VIDIZMO - 企业直播和点播视频流软件。
- Visual Paradigm - 用于团队协作的可视化建模和图表在线平台。
- Vtiger - CRM 工具，使销售、支持和营销团队能够进行组织和协作。
- WaveMaker – 用于构建和运行自定义应用程序的软件。

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

- Weekdone - 为公司创建经理仪表板和团队管理服务的工具。
- Wepow - 通过移动和视频面试解决方案连接招聘人员、求职者和雇主的工具。
- When I Work - 用于员工排班和时间跟踪的工具。
- WhosOnLocation – 用于跟踪人员在站点和区域之间流动的工具。
- Workable - 申请人跟踪系统。
- Workday - 用于财务管理、人力资源和规划的工具。
- Workpath - 用于管理组织目标和绩效的工具。
- Workplace - Facebook 的协作工具，可帮助员工通过熟悉的界面进行沟通。
- Workstars - 用于社交和同事员工表彰计划的平台。
- Workteam - 用于跟踪员工时间和出勤的工具。
- Wrike - 社交项目管理和协作软件。
- XaitPorter - 用于投标、提案和其他业务文档的文档协同创作软件。
- Ximble - 用于员工排班和时间跟踪的工具。
- XMatters - 协作平台，包含警报软件，可与其他工具集成，从而创建无缝流程和有效沟通。
- Yodeck - 通过网络或移动设备远程管理屏幕的工具。
- Zendesk - 用于请求客户服务和记录支持工单的软件。
- Ziflow - 面向创意制作团队的工具。
- Zillable – 具有通信功能的协作平台。
- Zing tree - 用于创建交互式决策树和故障排除程序的工具包。
- ZIVVER - 允许您从熟悉的电子邮件程序安全地传输电子邮件和文件的工具。
- Zoho - 业务应用程序套件。
- Zoom - 具有语音、网络协作和视频会议功能的通信和协作软件。
- Zuora - 一种基于订阅的软件，可帮助公司启动、管理并转型为订阅业务。

端到端应用程序配置

有关应用程序的完整端到端配置，请参阅 Admin-guided workflow for easy onboarding and set up。

无代理访问企业 Web 应用程序

客户在本地或公共云上托管的 SharePoint、JIRA、Confluence 等企业 Web 应用程序现在可以直接从客户端浏览器访问。最终用户不再需要从商店启动对其企业 Web 应用程序的访问。此功能还允许

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

最终用户通过单击电子邮件、协作工具或浏览器书签中的链接来访问 Web 应用程序，从而为客户提供真正的零足迹解决方案。

工作原理

- 为已配置的企业 Web 应用程序添加新的 DNS 记录或修改现有 DNS 记录。
- IT 管理员为已配置的企业 Web 应用程序 FQDN 添加新的公共 DNS 记录或修改现有公共 DNS 记录，以将用户重定向到 Citrix Secure Private Access™ 服务。
- 当最终用户启动对已配置的企业 Web 应用程序的访问时，应用程序流量将被引导至 Citrix Secure Private Access 服务，该服务随后将代理对应用程序的访问。
- 请求到达 Citrix Secure Private Access 服务后，它会检查用户身份验证和应用程序授权，包括上下文访问策略检查。
- 验证成功后，Citrix Secure Private Access 服务会与部署在客户环境（本地或云中）的 Citrix Cloud Connector™ 设备通信，以启用对已配置企业 Web 应用程序的访问。

配置 Citrix Secure Private Access 以实现对企业 Web 应用程序的无代理访问

先决条件：

在开始之前，您需要为要配置的应用程序准备以下各项。

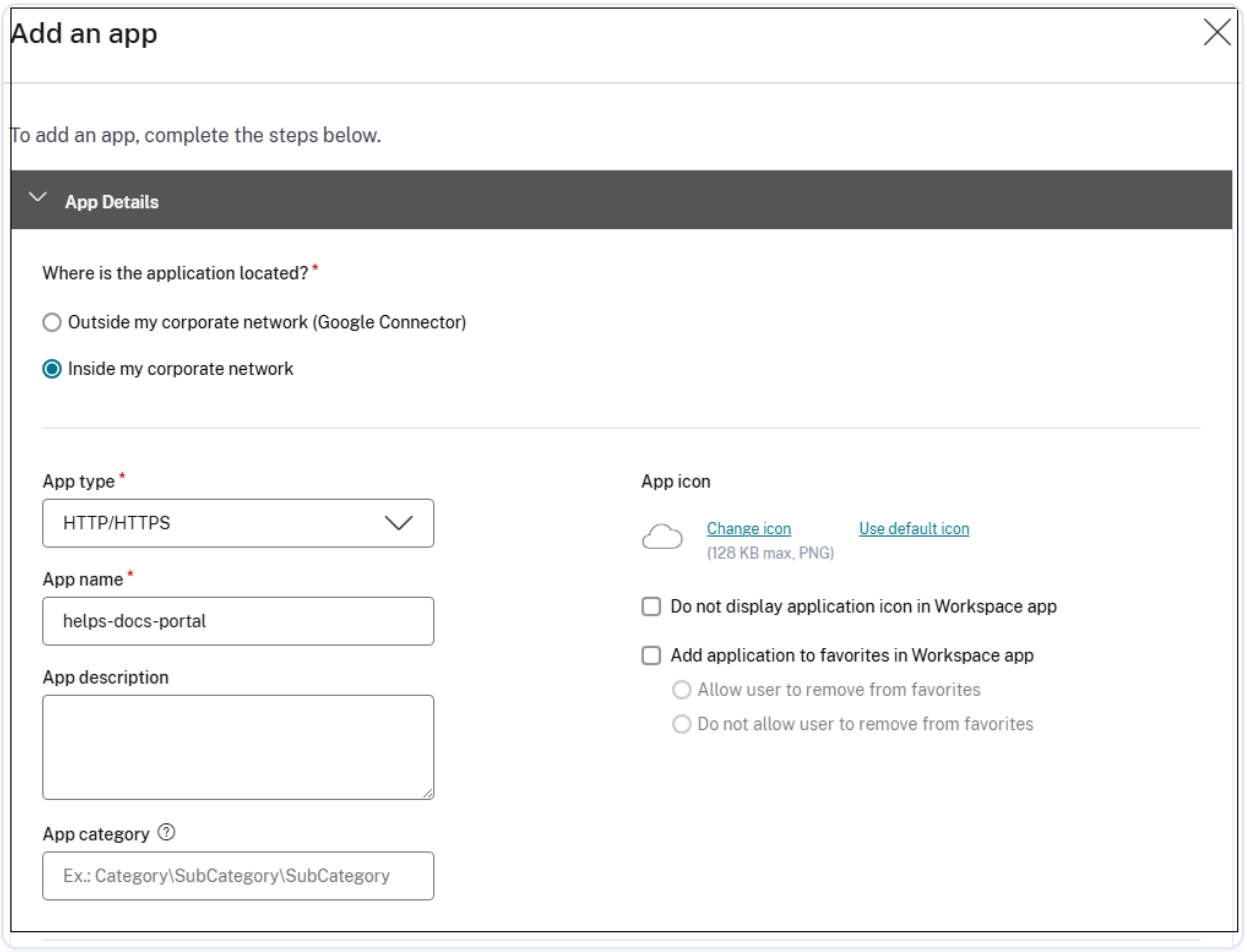
- 应用程序 FQDN
- SSL 证书 – 用于配置应用程序的公共证书
- 资源位置 – 安装 Citrix Cloud™ Connector 设备
- 访问公共 DNS 记录，以便使用 Citrix® 在应用程序配置期间提供的规范名称 (CNAME) 更新它。

配置企业 Web 应用程序的无代理访问：

1. 登录 Citrix Cloud 并选择 **安全私有访问**。
2. 单击 **应用程序 > 应用程序配置**，然后单击 **添加应用程序**。
3. 在**选择模板**部分中，单击**跳过**。模板仅适用于 SaaS 应用程序。
4. 在**应用程序位置在哪里？中，选择在我的公司网络内部**。
    - 选择**在我的公司网络内部**，适用于托管在组织专用网络基础设施内、防火墙后且仅通过内部网络连接访问的应用程序
    - 选择**在我的公司网络外部（Google 连接器）：**适用于托管在组织专用网络基础设施外部的应用程序。流量通过 Google Cloud Connector 直接从用户路由到外部应用程序。

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

5. 在**应用程序详细信息**部分中输入以下详细信息，然后单击**下一步**。



- **应用程序类型** – 选择应用程序类型（HTTP 或 HTTPS）。

  注意：

  对于 Chrome Enterprise Premium (CEP)，仅支持 HTTPS 企业 Web 和 SaaS 应用程序。不支持 HTTP 企业 Web 和 SaaS 应用程序。

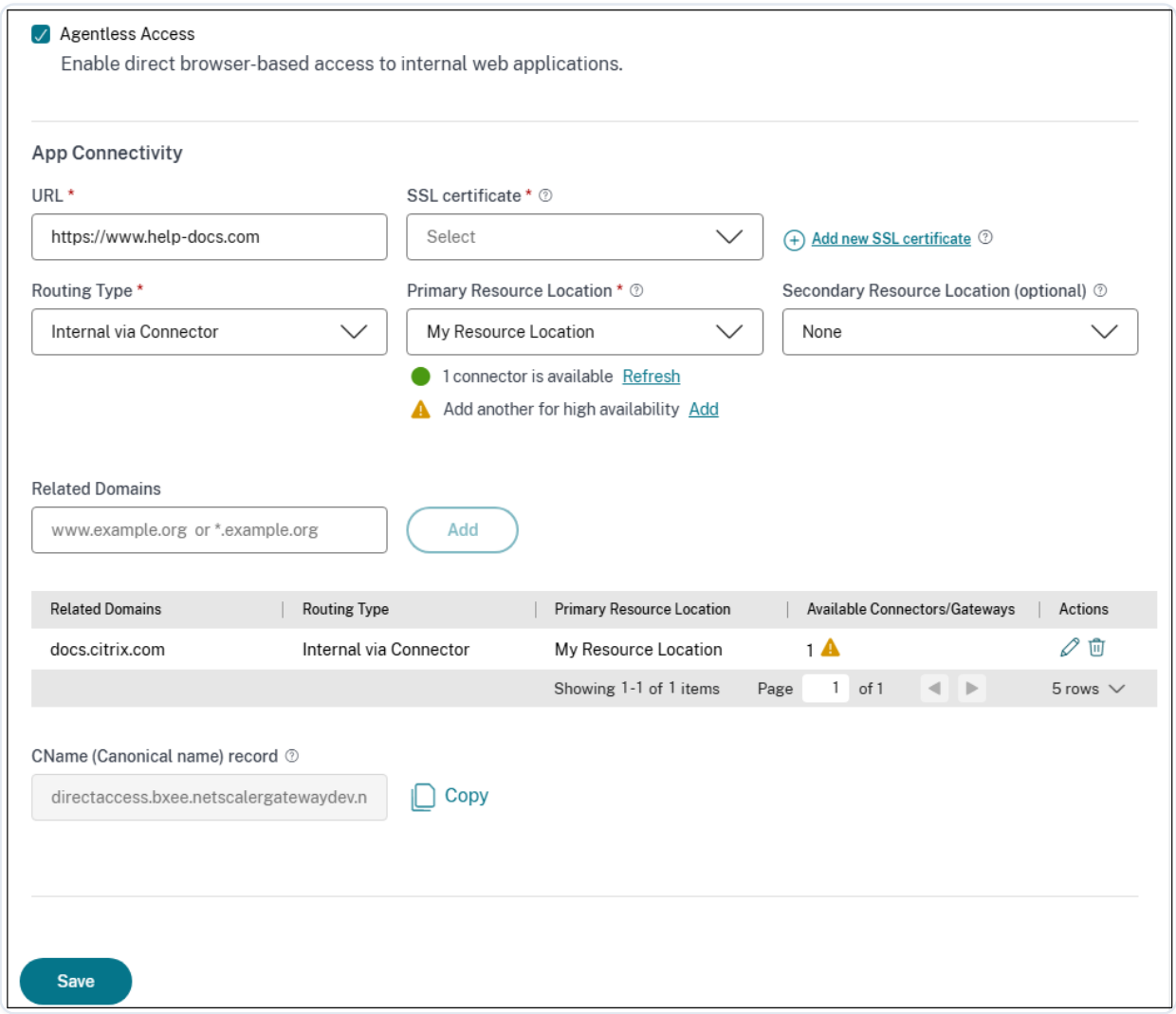
- **应用程序名称** – 应用程序的名称。
- **应用程序描述** - 应用程序的简要描述。此描述将显示给商店中的用户。
- **应用程序图标** – 单击**更改图标**以更改应用程序图标。图标文件大小必须为 128x128 像素。如果您不更改图标，则会显示默认图标。

  如果您不想显示应用程序图标，请选择 **不向用户显示应用程序图标**。

6. 选择 **无代理访问** 以使用户能够直接从客户端浏览器访问应用程序。输入以下详细信息。

   无代理访问 选项仅适用于企业 Web 应用程序。

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



- **URL** – 后端应用程序的 URL。URL 必须采用 HTTPS 格式，并且管理员必须添加相应的 DNS 条目。
- **SSL 证书** – 从下拉菜单中选择现有 SSL 证书，或通过单击 **添加新 SSL 证书** 添加新 SSL 证书。
  - 仅支持公共或受信任的 CA 证书。
  - 必须上传完整的证书链。

重要提示：

- 管理员必须将证书直接上传到 Secure Private Access 控制台，因为 Secure Private Access 管理其自己的证书存储。有关详细信息，请参阅 在 Secure Private Access 控制台中管理证书。
- 添加到 NetScaler® 控制台的证书不能再用于 Secure Private Access，因为证书在这两个系统之间不同步。

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

- **相关域** – 相关域会根据您提供的 URL 自动填充。相关域有助于服务将 URL 识别为应用程序的一部分并相应地路由流量。您可以添加多个相关域。您可以将 SSL 证书绑定到每个相关域，这是可选的。

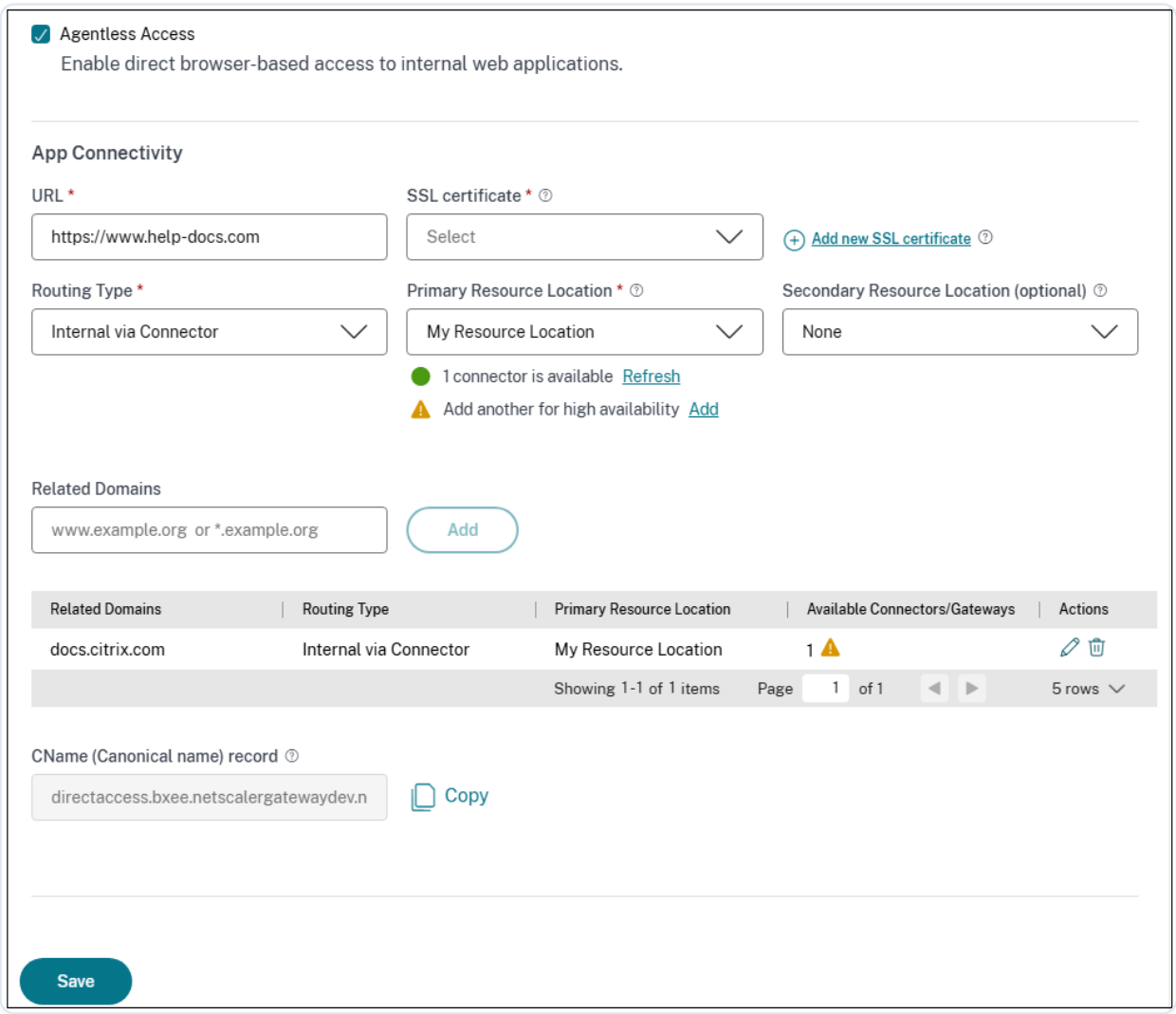
  注意：

  如果添加了重复的相关域，或者相关域也作为不同应用程序的 URL 添加，则会出现警告消息。为避免这些问题，请参阅 Web 和 SaaS 应用程序配置的最佳实践。

- **导入 HAR** – 您可以上传 HAR 文件以自动发现应用程序访问的域。查看发现的域并选择要添加到应用程序相关域配置中的域。这通过减少手动识别和配置相关域的需要来简化应用程序的入门。有关详细信息，请参阅 使用 HAR 文件发现相关域。
- **CName 记录** – 由 Secure Private Access 自动生成。此值必须输入到 DNS 中，才能启用对应用程序的无代理访问。

7. 在**应用程序连接**部分中，您可以定义应用程序相关域的路由，如果这些域必须通过 Citrix Connector™ Appliance 外部或内部路由。

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



- **路由类型** - 选择以下选项之一：
  - **内部 – 绕过代理** - 域流量通过 Connector Appliance™ 路由，绕过在 Connector Appliance 上配置的客户 Web 代理。
  - **通过连接器内部** - 应用程序可以是外部的，但流量必须通过 Connector Appliance 流向外部网络。
  - **外部** – 流量直接流向互联网。
- **主要和辅助资源位置** - 管理员可以通过配置辅助资源位置或使用**第一个可用**选项来确保应用程序即使在中断期间也具有高可用性。
  - **主要资源位置：** 选择托管应用程序的主要资源位置。或者，管理员可以在**主要资源位置**中选择**第一个可用**选项。
  - **第一个可用： 第一个可用**选项可确保使用正常工作的资源位置。选择**第一个可用**后，系统会自动将流量路由到第一个可用位置。这可确保持续的应用程序访问，无需手动干预。例如，如果 ResourceLocation1 不可用但 ResourceLocation2 可访问，则默认选择 ResourceLocation2 作为应用程序的前端。

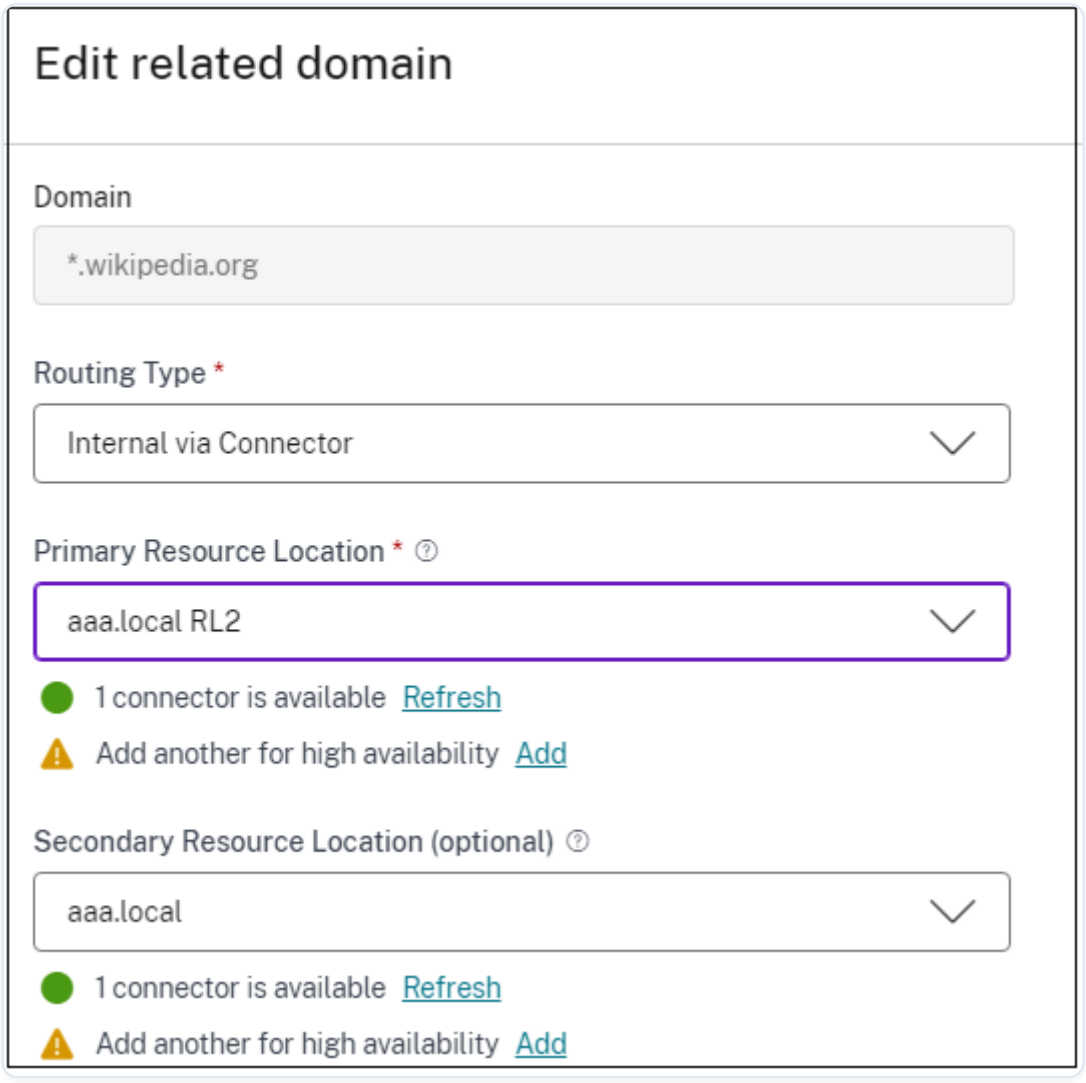
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **辅助资源位置** - 仅当明确指定了主要资源位置时，**辅助资源位置**选项才可用。如果主要资源位置因 Connector Appliance 或数据中心故障等原因变得不可用，应用程序将故障转移到指定的辅助资源位置。即使应用程序托管在另一个数据中心，辅助资源位置也可以充当故障转移。

您还可以为每个相关域设置主要和辅助资源位置，或选择**第一个可用**选项。

a. 单击“相关域”表“**操作**”列中的编辑图标。

b. 设置主要和辅助资源位置或选择**第一个可用**选项。

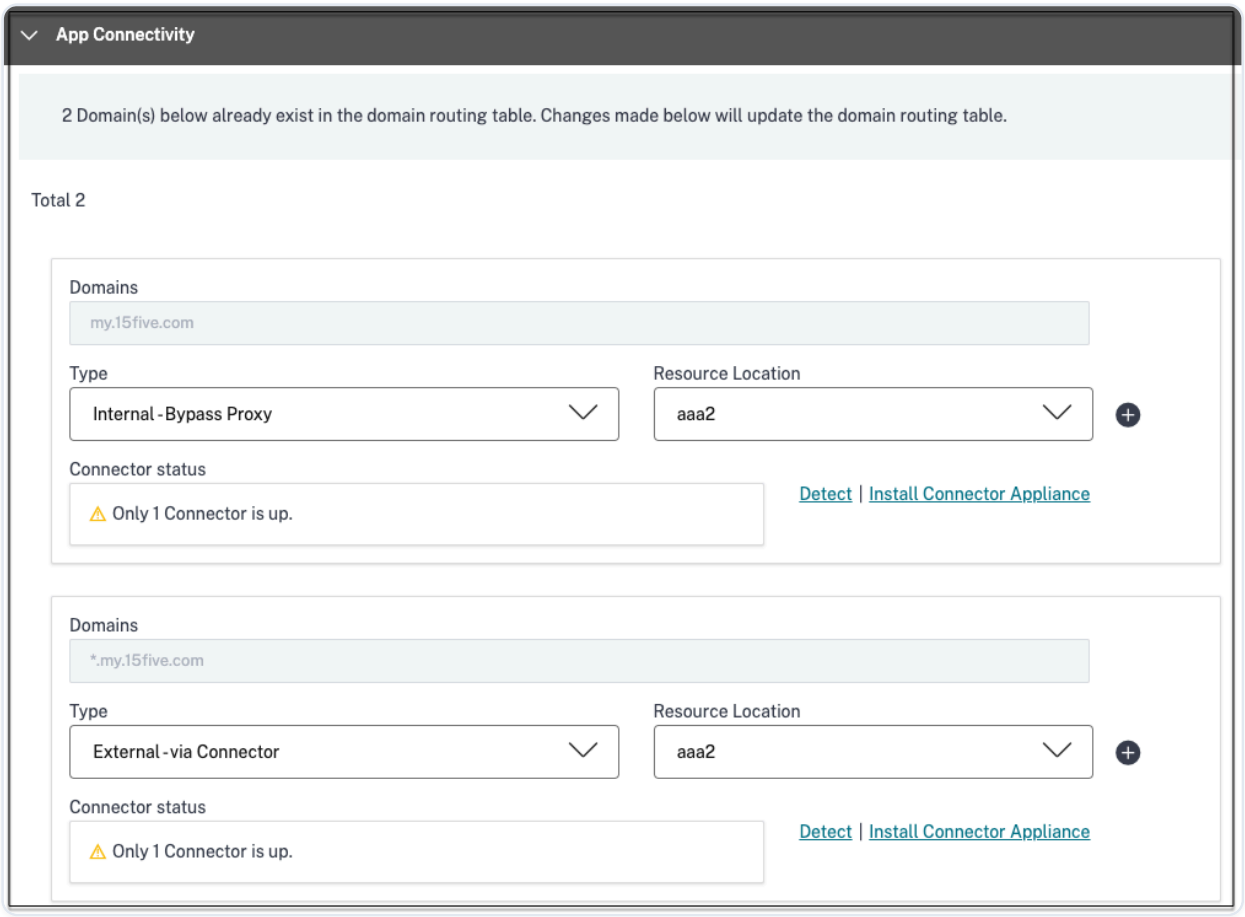


注意：

- 设置备份资源位置和使用“**First Available**”选项功能处于预览阶段。
- 删除应用程序时，其路由条目会自动删除。有关详细信息，请参阅删除应用程序时自动清理路由条目。

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

8. 在“**应用程序连接**”部分中，如果应用程序的相关域必须通过 Citrix Connector™ Appliance 外部或内部路由，则可为其定义路由。



9. **保持一致连接** - 选中此复选框可启用与同一 Connector Appliance 的一致连接。有关一致连接的详细信息，请参阅保持一致连接。

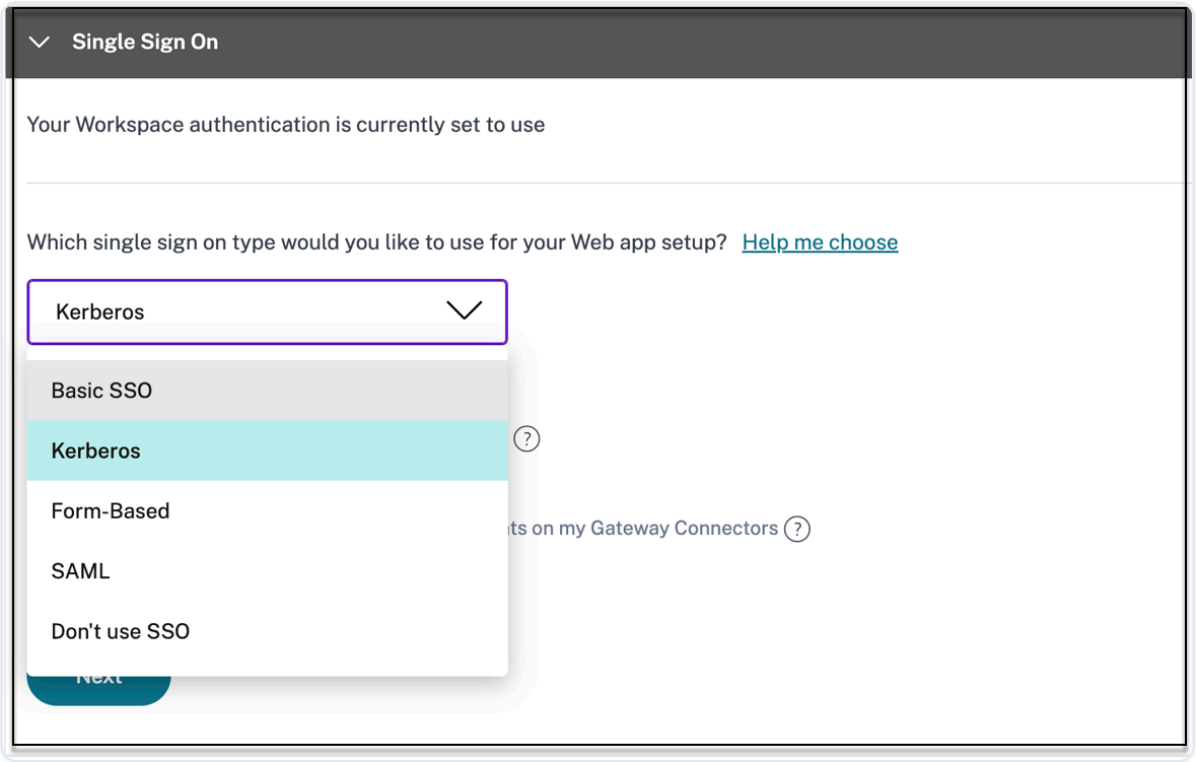
> **注意：**
>
> 选择“**保持一致连接**”选项时，应用程序的路由类型必须在“应用程序连接”部分中设置为“**通过连接器内部**”。

10. 设置首选登录方法。

> **注意：**
>
> 单点登录选项不适用于 Citrix Secure Access with Chrome Enterprise (CEP)。

a. 在“**单点登录**”部分中，选择要用于应用程序的首选单点登录类型，然后单击“**保存**”。提供以下单点登录类型。

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

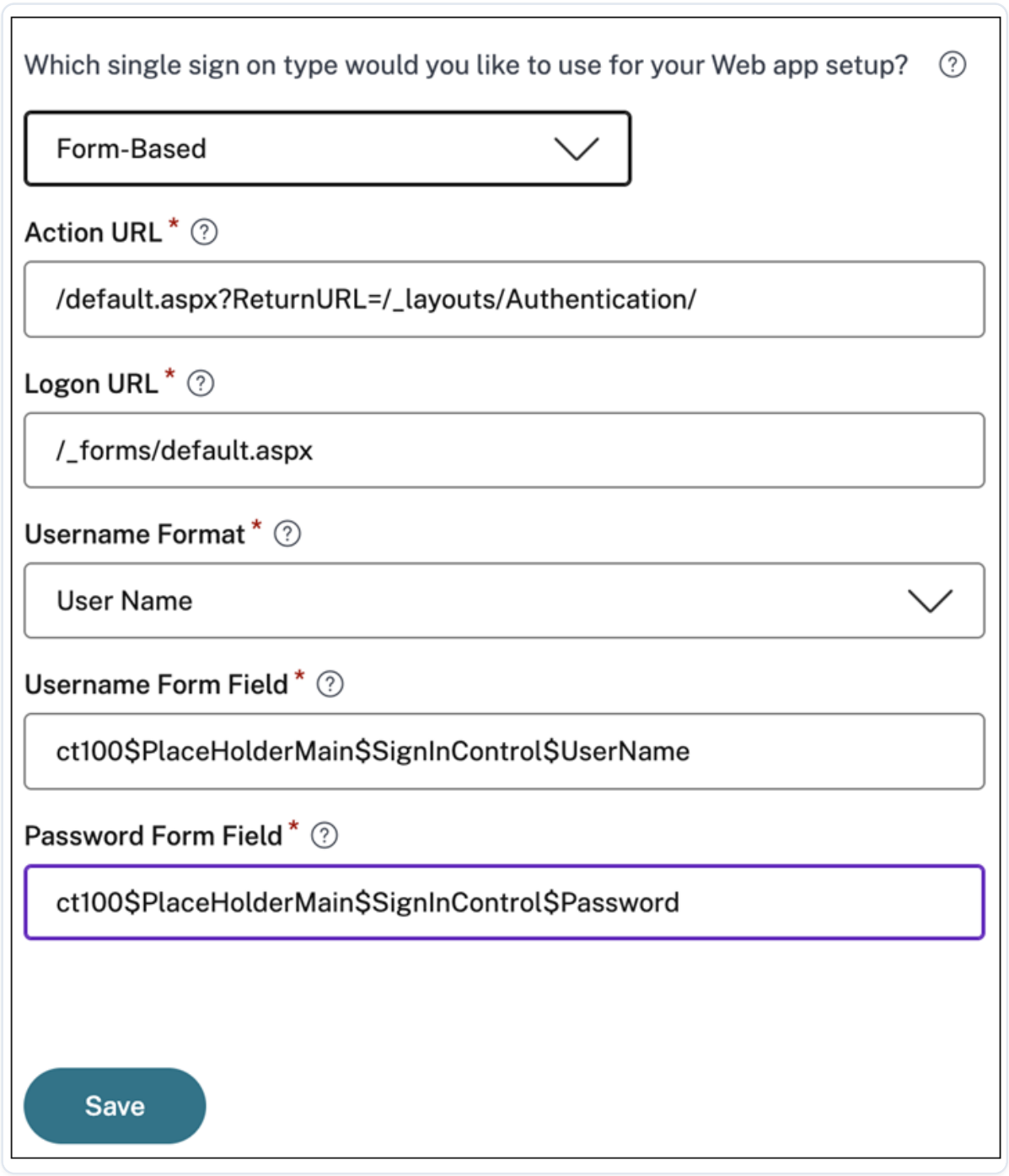


- **基本** – 如果您的后端服务器向您发出 basic-401 质询，请选择“**基本 SSO**”。您无需为“**基本**”SSO 类型提供任何配置详细信息。
- **Kerberos** – 如果您的后端服务器向您发出 negotiate-401 质询，请选择“**Kerberos**”。您无需为“**Kerberos**”SSO 类型提供任何配置详细信息。
- **基于表单** – 如果您的后端服务器向您显示 HTML 表单以进行身份验证，请选择**基于表单**。输入**基于表单** SSO 类型的配置详细信息。
- **SAML** - 选择 **SAML** 以用于基于 SAML 的 Web 应用程序 SSO。输入 **SAML** SSO 类型的配置详细信息。
- **不使用 SSO** – 当您不需要在后端服务器上验证用户身份时，请使用**不使用 SSO** 选项。选择**不使用 SSO** 选项后，用户将被重定向到**应用程序详细信息**部分下配置的 URL。

基于表单的详细信息：

在单点登录部分输入以下基于表单的配置详细信息，然后单击**保存**。

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

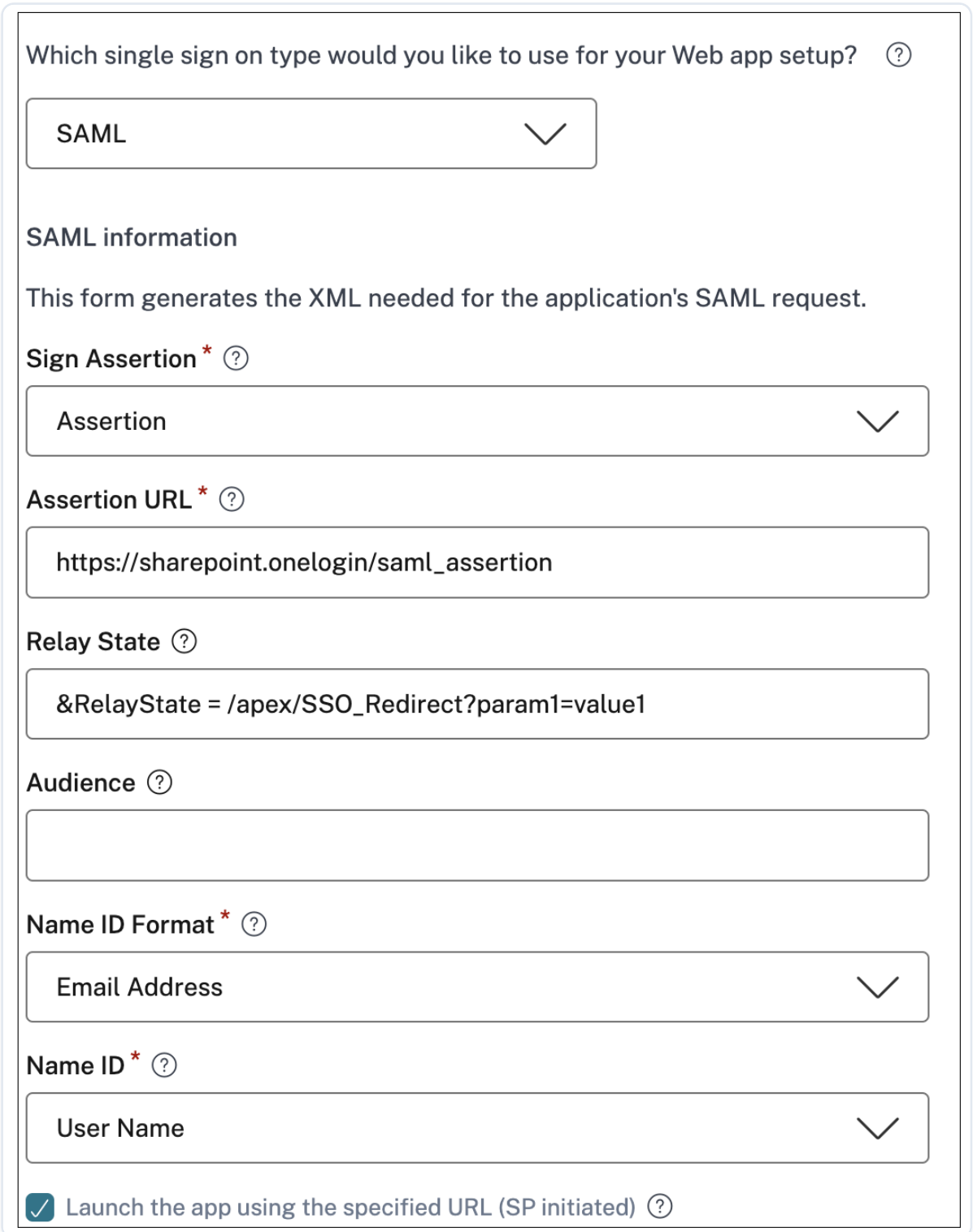


- **操作 URL** - 键入已完成的表单将提交到的 URL。
- **登录表单 URL** – 键入显示登录表单的 URL。
- **用户名格式** - 选择用户名的格式。
- **用户名表单字段** – 键入用户名属性。
- **密码表单字段** – 键入密码属性。

SAML：

在单点登录部分输入以下详细信息，然后单击保存。**

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



- **签名断言** - 对断言或响应进行签名可确保当响应或断言传递给信赖方 (SP) 时消息的完整性。您可以选择**断言、响应、两者、** 或 **无**。
- **断言 URL** – 断言 URL 由应用程序供应商提供。SAML 断言将发送到此 URL。
- **中继状态** – 中继状态参数用于标识用户登录并定向到信赖方联合服务器后访问的特定资源。中继状态为用户生成一个 URL。用户可以单击此 URL 登录到目标应用程序。
- **受众** – 受众由应用程序供应商提供。此值确认 SAML 断言是为正确的应用程序生成的。

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

- **名称 ID 格式** – 选择支持的名称标识符格式。
- **名称 ID** – 选择支持的名称 ID。

i. 在**高级属性（可选）**中，添加有关用户的其他信息，这些信息将发送到应用程序以进行访问控制决策。

ii. 单击**SAML 元数据**下的链接下载元数据文件。使用下载的元数据文件在 SaaS 应用程序服务器上配置 SSO。

- 您可以复制**登录 URL**下的 SSO 登录 URL，并在 SaaS 应用程序服务器上配置 SSO 时使用此 URL。
- 您还可以从**证书**列表中下载证书，并在 SaaS 应用程序服务器上配置 SSO 时使用该证书。

11. 单击**保存**，然后单击**完成**。应用程序将添加到“应用程序”页面。配置应用程序后，您可以从“应用程序”页面编辑或删除应用程序。为此，请单击应用程序上的省略号按钮并相应地选择操作。

- **编辑应用程序**
- **删除**

重要提示：

- 为了启用基于零信任的应用程序访问，默认情况下应用程序被拒绝访问。仅当访问策略与应用程序关联时，才启用对应用程序的访问。有关创建访问策略的详细信息，请参阅创建访问策略。
- 如果多个应用程序配置了相同的 FQDN 或通配符 FQDN 的某种变体，这可能会导致配置冲突。为防止配置冲突，请参阅Web 和 SaaS 应用程序配置的最佳实践。

删除应用程序时自动清理路由条目

配置应用程序时，其目标（FQDN 或应用程序域）会添加到路由表中，Secure Private Access 使用该表进行路由决策。删除应用程序时，Secure Private Access 会根据以下规则清理路由条目：

- **删除未引用的条目** - 如果与已删除应用程序关联的路由条目（FQDN 或应用程序域）未被任何其他应用程序引用，Secure Private Access 会自动将其从路由表中删除。
- **保留共享条目** - 如果路由条目被多个应用程序使用，删除其中一个应用程序不会删除共享条目。只要至少有一个活动应用程序引用该条目，该条目就会保留在路由表中。

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

- **无追溯性删除** - 路由条目仅作为应用程序删除的一部分进行评估和删除。除非确认现有条目未被任何应用程序使用，否则不会追溯性删除。

注意：

- 从“应用程序”页面（使用省略号 (...) 菜单）删除应用程序时，清理会自动运行。无需管理员操作。
- 由于共享路由条目得以保留，删除应用程序不会中断对共享相同目标的其他应用程序的访问。

使用无代理访问应用程序的设备状态服务

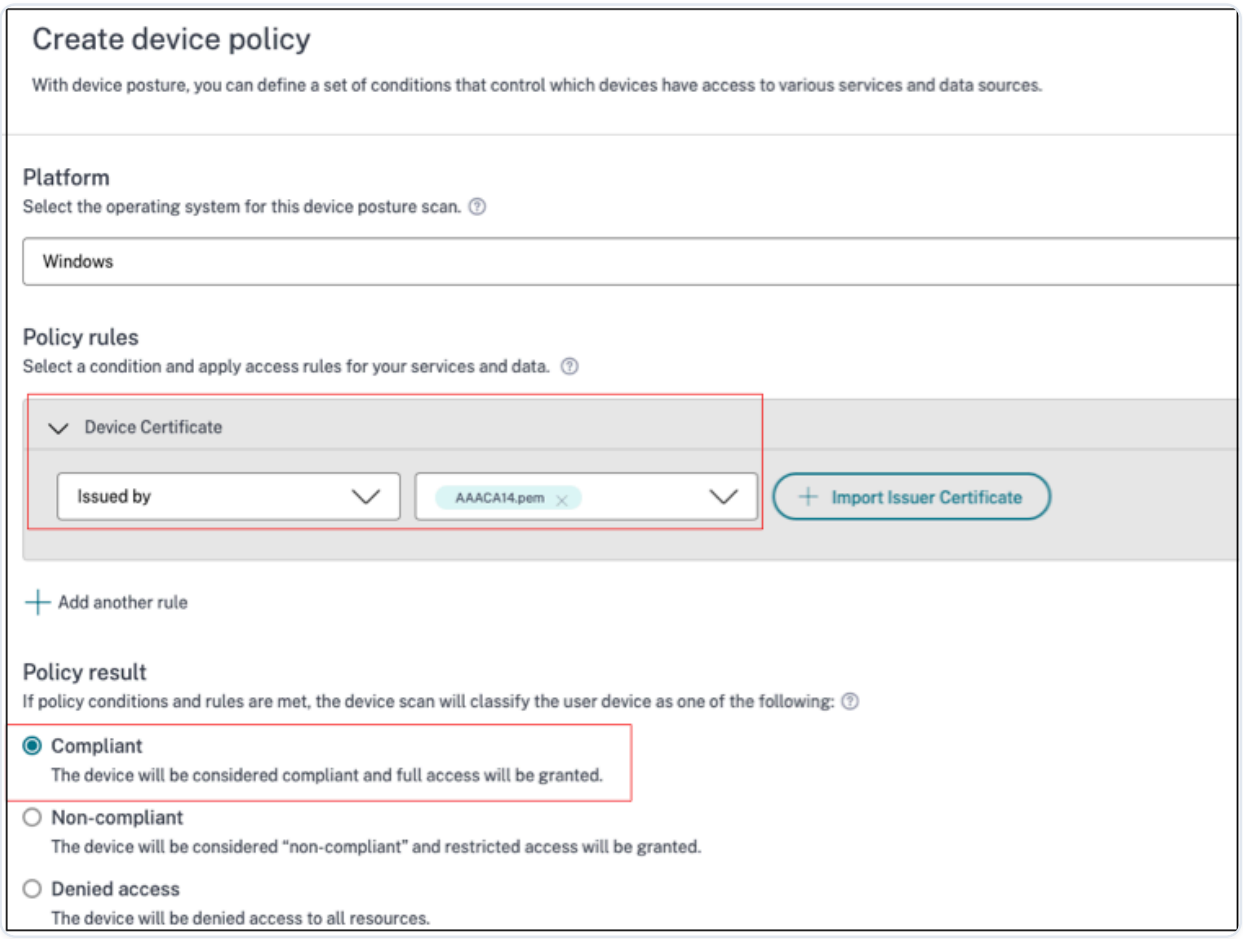
Citrix Secure Private Access 与无代理访问应用程序结合设备状态服务，可以确保只有合规设备通过无代理访问敏感应用程序。管理员可以根据设备状态服务扫描结果阻止不合规或非托管设备的访问。

仅为合规设备启用无代理访问的步骤

要仅为合规设备启用无代理访问，管理员必须执行以下步骤：

1. 在设备状态服务管理控制台中，创建设备状态策略以检查设备状态扫描条件，例如设备证书、防病毒、浏览器，然后选择“**合规**”作为策略结果操作。有关详细信息，请参阅配置设备状态。

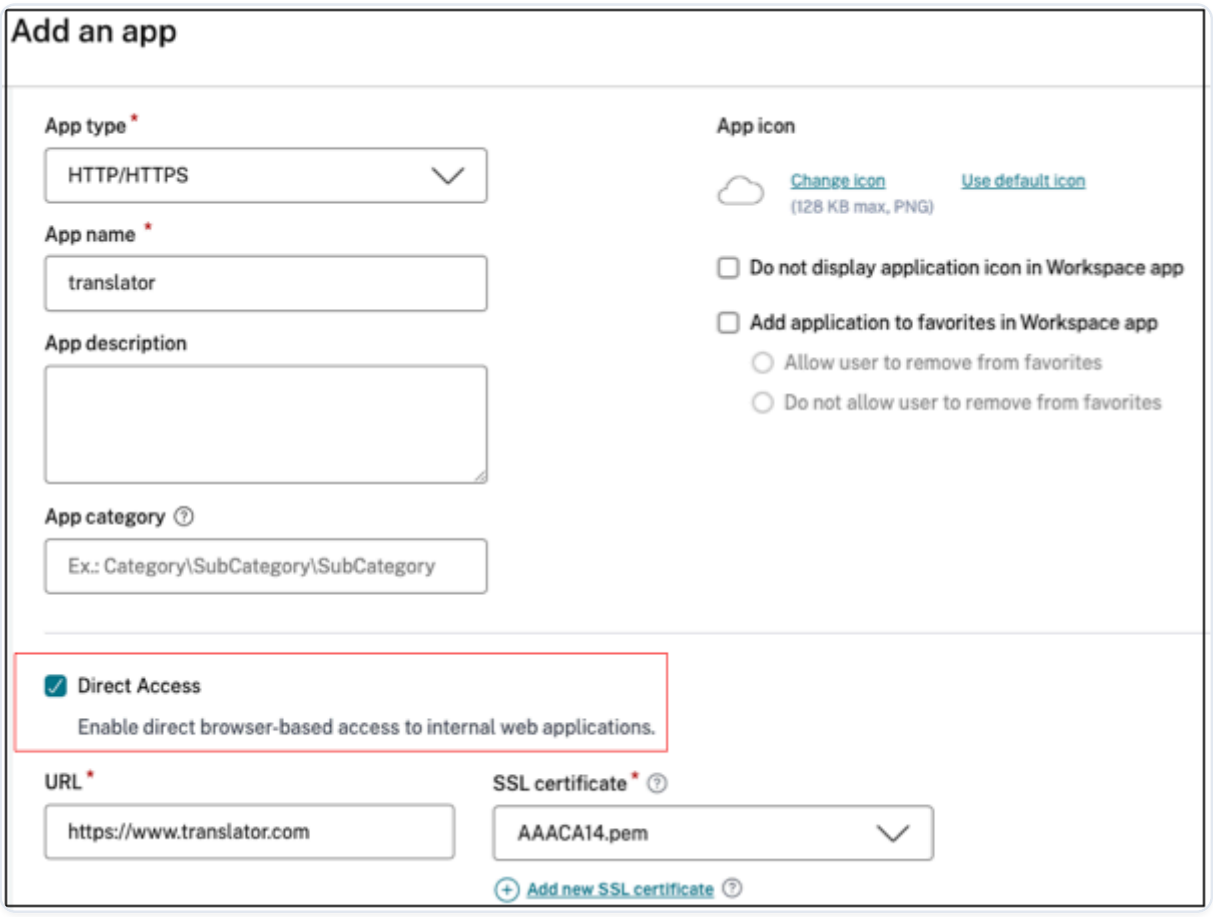
© 1997–2026 Citrix Systems, Inc. All rights reserved.



2. 在 Secure Private Access 管理控制台中，执行以下操作：

   - 创建要为其启用无代理访问的应用程序。有关详细信息，请参阅 直接访问企业 Web 应用程序。

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

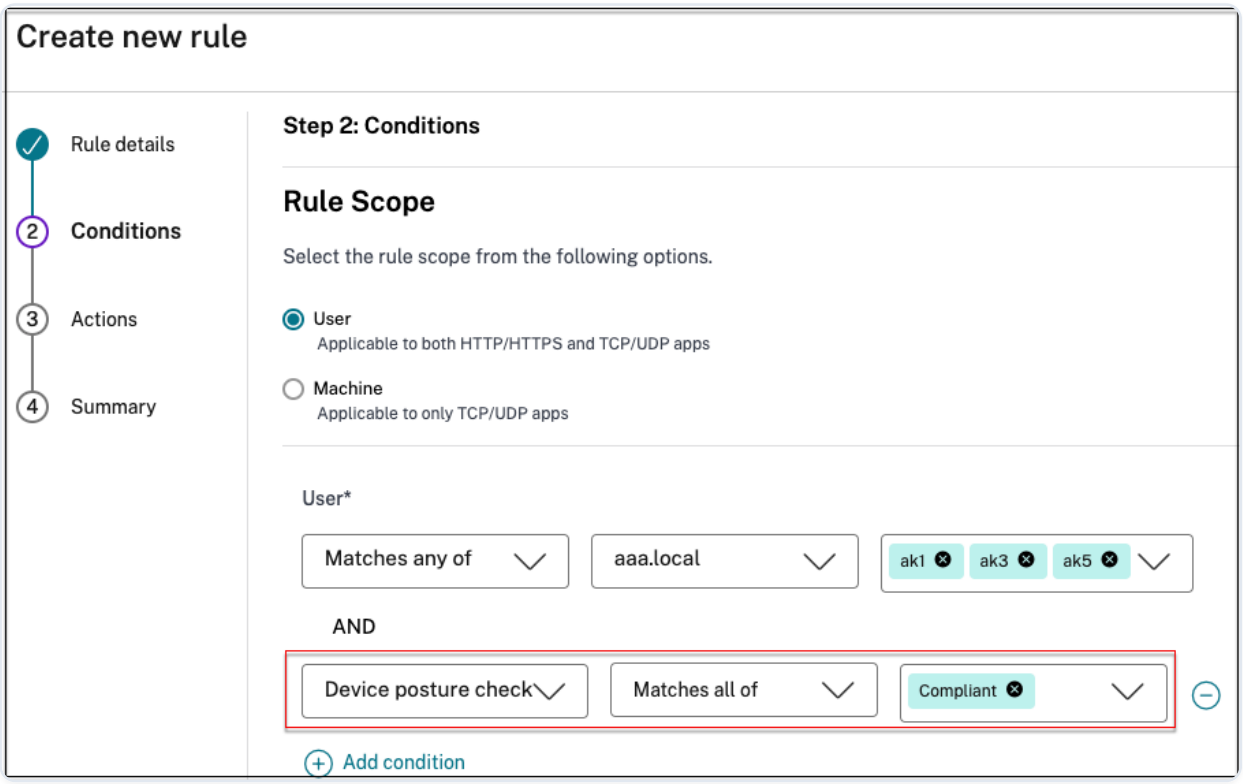


- 使用设备姿态配置 Secure Private Access。在 **规则范围** 中，选择 **设备姿态检查 > 匹配以下任意项**，然后输入标签 **Compliant**。此标签由设备姿态服务发送。

注意：

必须完全按照之前捕获的方式输入标签，使用首字母大写 (Compliant)。否则，设备姿态策略将无法按预期运行。有关详细信息，请参阅 使用设备姿态配置 Citrix Secure Private Access。

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



完成此配置后，根据设备姿态扫描结果，设备将被标记为合规、不合规或拒绝登录，并相应地启用应用程序访问。

示例：

假设您已创建设备姿态策略，以检查终端设备上是否存在设备证书并确定其登录状态。设置设备姿态策略并启用设备姿态后，当最终用户登录其商店时，将发生以下操作。

1. 设备姿态扫描会检查终端设备是否存在设备证书。
    - 如果设备上存在设备证书，则该设备将被标记为 **合规**。
    - 如果设备上不存在设备证书，则该设备将被标记为 **不合规**。
2. 此信息随后作为标签传递给 Citrix Secure Private Access 服务。
3. 访问策略根据设备分类进行评估。
    - 如果设备合规，则允许应用程序进行无代理访问。
    - 如果设备不合规，则禁用这些应用程序的无代理访问。

最终用户体验

最终用户体验基于设备是否合规的分类。

- **合规设备：**

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

用户可以从应用商店或使用应用程序 URL 从浏览器启动无代理访问应用程序。

- **不合规设备：**
  - 应用程序未在应用商店中列出。
  - 用户无法使用应用程序 URL 从浏览器启动应用程序。
  - 系统会向用户显示一个访问被阻止页面。

支持 TCP/UDP 应用程序

Secure Private Access 服务使您能够通过在您的计算机上运行的 Citrix Secure Access 客户端，使用本机浏览器或本机客户端应用程序访问本地环境中的 TCP/UDP 应用程序。有关详细信息，请参阅以下部分：

- 先决条件
- 为 TCP/UDP 应用程序配置 Secure Private Access
- 管理员配置 – 基于 Citrix Secure Access 客户端的 HTTP/HTTPS 应用程序访问
- 对 TCP/UDP 和 HTTP(S) 应用程序的自适应访问
- 排查应用程序域 IP 地址冲突

先决条件

- Citrix Secure Access 客户端 - 有关详细信息，请参阅 Citrix Secure Access 客户端。
- Connector Appliance – Citrix 建议在您的资源位置以高可用性设置安装两个 Connector Appliance。连接器可以安装在本地、数据中心虚拟机管理程序中或公有云中。有关 Connector Appliance 及其安装的更多信息，请参阅 适用于云服务的 Connector Appliance。您必须为 TCP/UDP 应用程序使用 Connector Appliance。Connector Appliance 必须具有用于 DNS 解析的 DNS 服务器配置。

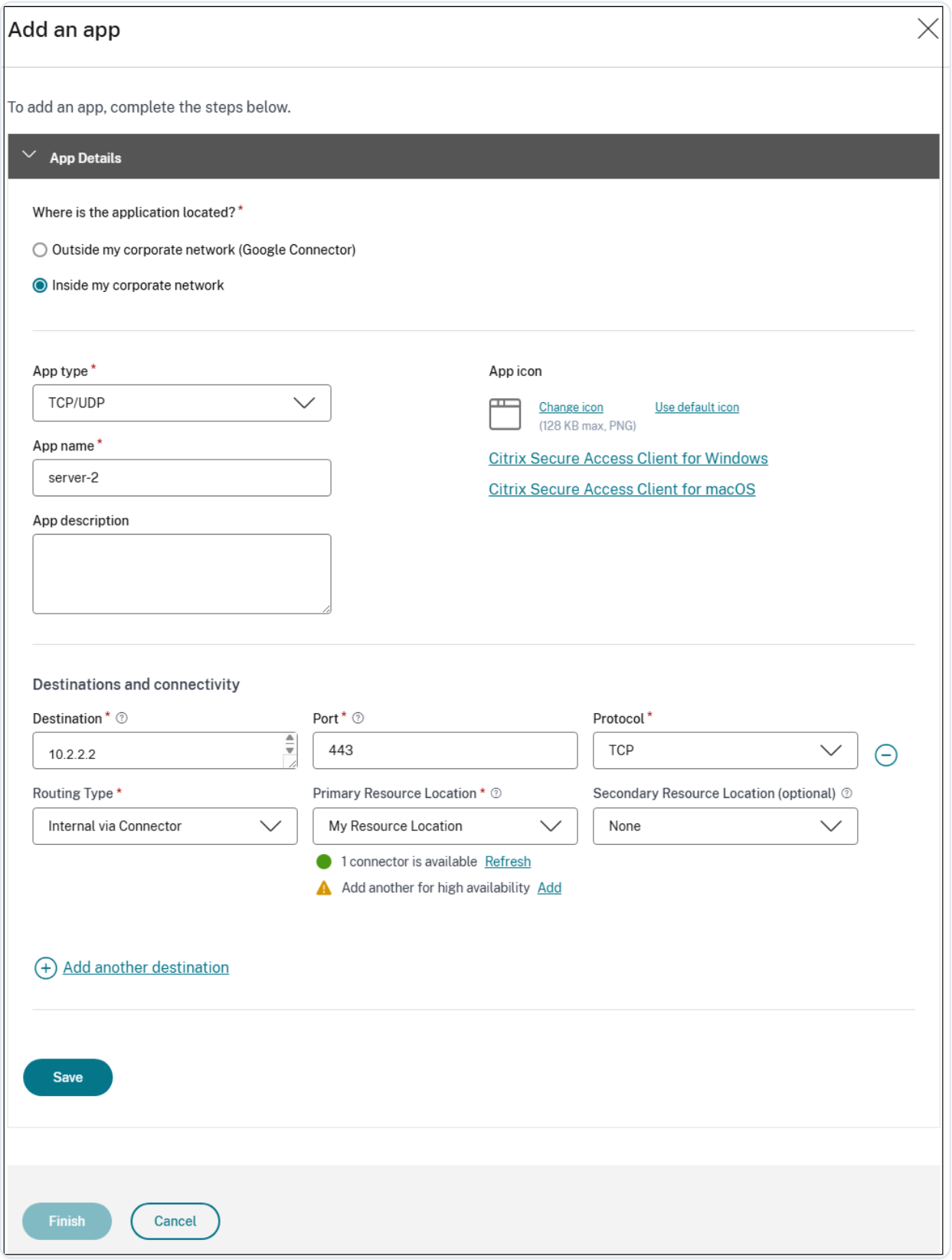
为 TCP/UDP 应用程序配置 Secure Private Access

1. 登录 Citrix Cloud 并选择 **安全私有访问**。
2. 单击 **应用程序 > 应用配置**，然后单击 **添加应用**。
3. 在 **Choose a template** 部分中，单击 **Skip**。模板仅适用于 SaaS 应用程序。

   应用程序是目标的逻辑分组。我们可以为多个目标创建一个应用程序 – 每个目标意味着后端中的不同服务器。例如，一个应用程序可以有一个 SSH、一个 RDP、一个数据库服务器和一个 Web 服务器。您不必为每个目标创建一个应用程序，但一个应用程序可以有许多目标。

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

4. 在“**应用程序详细信息**”部分中，选择“**在我的公司网络中**”，输入以下详细信息，然后单击“**下一步**”。



- **应用程序类型** – 选择 TCP/UDP。
- **应用程序名称** – 应用程序的名称。

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

- **应用程序图标** – 显示应用程序图标。此字段是可选的。
- **应用程序描述** – 您正在添加的应用程序的描述。此字段是可选的。
- **目标** – 位于资源位置的后端计算机的 IP 地址或 FQDN。可以按如下方式指定一个或多个目标。
  - **IP 地址 v4**
  - **IP 地址范围** – 示例：10.68.90.10-10.68.90.99
  - **CIDR** – 示例：10.106.90.0/24
  - **计算机的 FQDN 或域名** – 单个或通配符域。示例：ex.destination.domain.com, *.domain.com

重要提示：

即使管理员使用 IP 地址配置了应用程序，最终用户也可以使用 FQDN 访问应用程序。这是因为 Citrix Secure Access™ 客户端可以将 FQDN 解析为真实的 IP 地址。下表提供了各种目标的示例以及如何使用这些目标访问应用程序：

目标输入	如何访问应用程序
10.10.10.1-10.10.10.100	最终用户只能通过此范围内的 IP 地址访问应用程序。
10.10.10.0/24	最终用户只能通过 IP CIDR 中配置的 IP 地址访问应用程序。
10.10.10.101	最终用户只能通过 10.10.10.101 访问应用程序。
`*.info.citrix.com`	最终用户应访问 `info.citrix.com` 的子域以及 `info.citrix.com`（父域）。例如，`info.citrix.com`, `sub1.info.citrix.com`, `level1.sub1.info.citrix.com` **注意：** 通配符必须始终是域的起始字符，并且只允许一个 *.
info.citrix.com	最终用户只能访问 `info.citrix.com`，不能访问任何子域。例如，`sub1.info.citrix.com` 不可访问。

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

- **端口** – 应用程序运行的端口。管理员可以为每个目标配置多个端口或端口范围。

  下表提供了可为目标配置的端口示例。

端口输入	描述
*	默认情况下，端口字段设置为 “*”（任意端口）。目标支持 1 到 65535 的端口号。
1300–2400	目标支持 1300 到 2400 的端口号。
38389	目标仅支持端口号 38389。
22,345,5678	目标支持端口 22、345、5678。
1300–2400, 42000-43000,22,443	目标支持 1300 到 2400、42000 到 43000 的端口号范围以及端口 22 和 443。

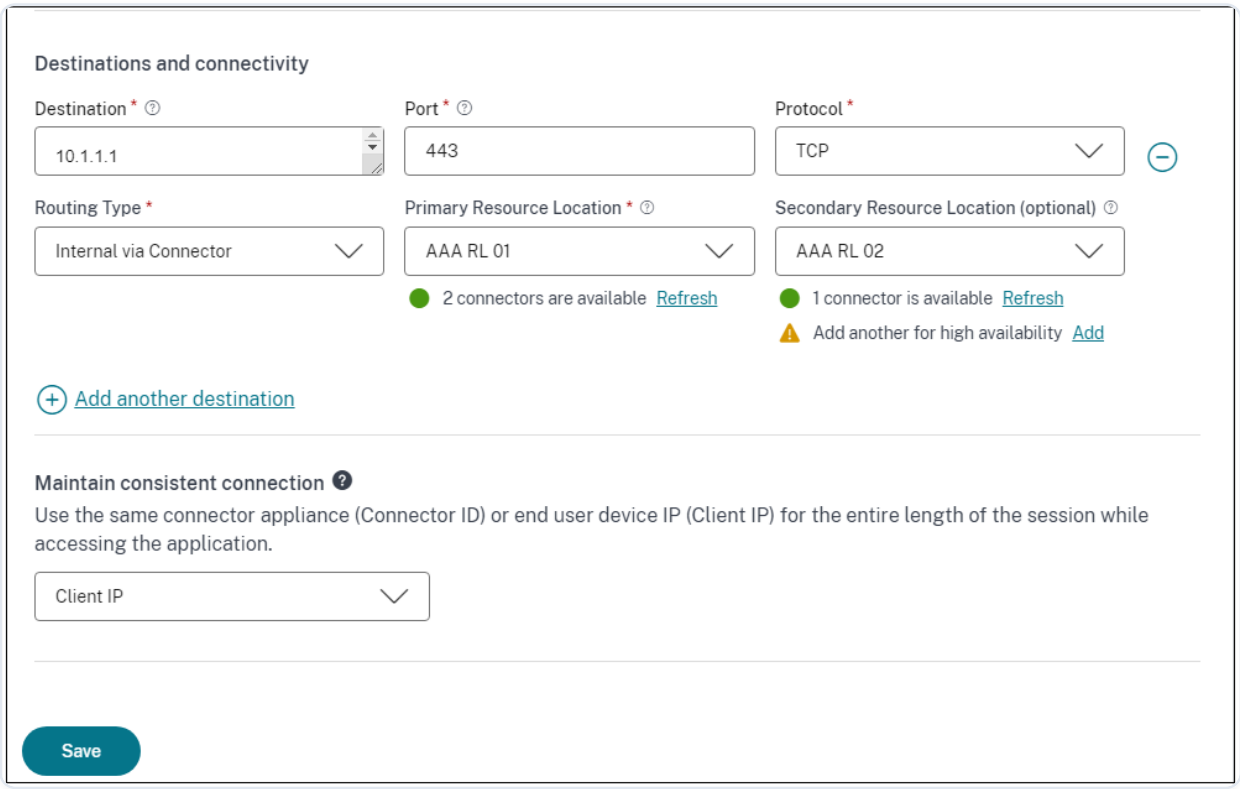
  注意：

  通配符端口 (*) 不能与端口号或范围共存。

- **协议** – TCP/UDP

5. 在“**应用程序连接**”部分中，您可以定义应用程序的路由，以确定域是必须通过 Citrix Connector™ Appliance 外部路由还是内部路由。

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



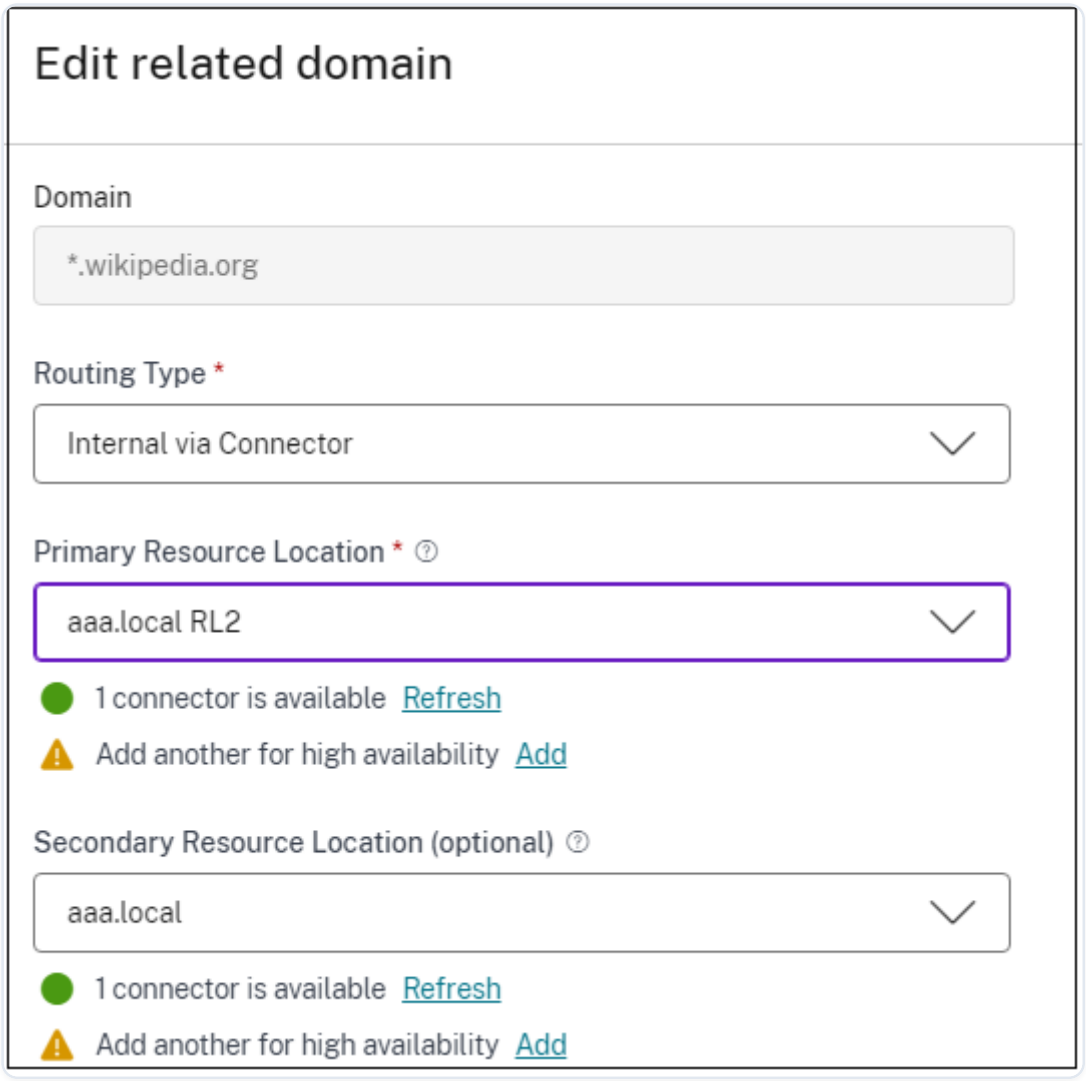
- **路由类型** - 选择以下选项之一：
  - **通过连接器内部** - 应用程序可以是外部的，但流量必须通过连接器设备流向外部网络。
  - **外部** – 流量直接流向互联网。
- **主要和次要资源位置** - 管理员可以通过配置次要资源位置或使用**首个可用**选项，确保应用程序即使在中断期间也具有高可用性。
  - **主要资源位置：** 选择托管应用程序的主要资源位置。或者，管理员可以在**主要资源位置**中选择**首个可用**选项。
  - **首个可用：** **首个可用**选项可确保使用一个可用的资源位置。选择**首个可用**后，系统会自动将流量路由到第一个可用的位置。这确保了无需手动干预即可持续访问应用程序。例如，如果 ResourceLocation1 不可用但 ResourceLocation2 可达，则默认选择 ResourceLocation2 作为应用程序的前端。
  - **次要资源位置** - **次要资源位置**选项仅在明确指定主要资源位置时才可用。如果主要资源位置因连接器设备或数据中心故障等原因变得不可用，应用程序将故障转移到指定的次要资源位置。即使应用程序托管在另一个数据中心，次要资源位置也可以充当故障转移。

  您还可以为每个相关域设置主要和次要资源位置，或选择**首个可用**选项。

  a. 单击“相关域”表**操作**列中的编辑图标。

  b. 设置主要和次要资源位置，或选择**首个可用**选项。

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



注意：

设置备份资源位置和使用**首个可用**选项功能目前处于预览阶段。

- **保持一致连接** - 您可以为 TCP/UDP 应用程序启用连接器粘性或客户端 IP 粘性。选中**保持一致连接**复选框，然后选择以下选项：
  - **不使用：** 应用程序不需要任何持久性。应用程序可以使用任何源 IP 地址。
  - **客户端 IP：** 应用程序在每次连接时都为客户端使用相同的源 IP 地址。
  - **连接器 ID：** 应用程序在每个会话中连接到相同的连接器设备。选择以下选项之一：

  有关一致连接的详细信息，请参阅维护一致连接。

6. 单击“**保存**”，然后单击“**完成**”。

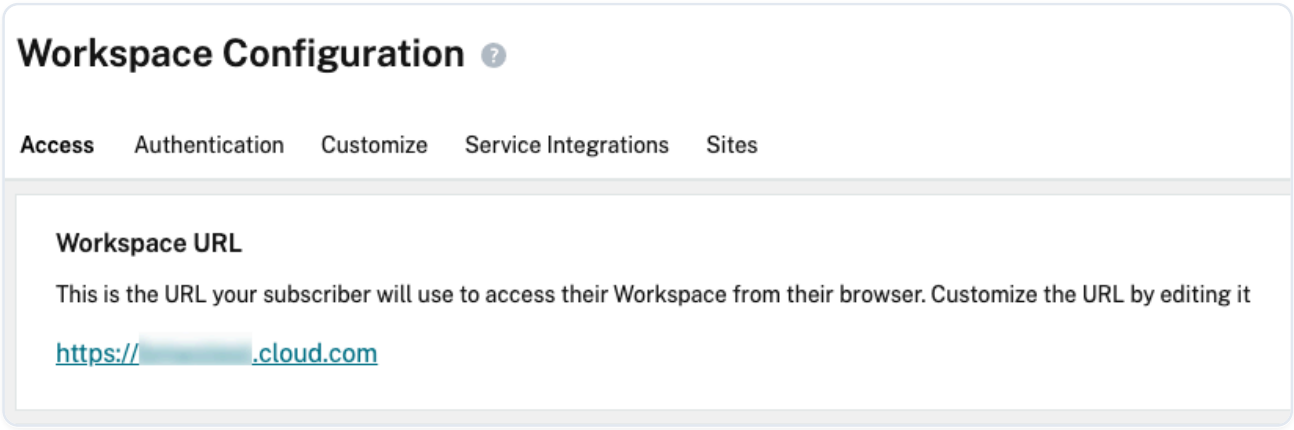
该应用程序已添加到“**应用程序**”页面。配置应用程序后，您可以从“**应用程序**”页面编辑或删除应用程序。为此，请单击应用程序上的省略号按钮并相应地选择操作。

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

- **编辑应用程序**
- **删除**

注意：

- 要授予用户对应用程序的访问权限，管理员需要创建访问策略。在访问策略中，管理员添加应用程序订阅者并配置安全控制。有关详细信息，请参阅创建访问策略。
- 要配置用户所需的身份验证方法，请参阅设置身份和身份验证。
- 要获取要与用户共享的商店 URL，请从 Citrix Cloud™ 菜单中单击“**StoreFront Cloud**”，然后选择“**访问**”选项卡。



管理员配置 – Citrix Secure Access 客户端对 HTTP/HTTPS 应用程序的访问

注意：

要使用 Citrix Secure Access 客户端访问现有或新的 HTTP/HTTPS 应用程序，您必须在资源位置安装至少一个（建议两个以实现高可用性）连接器设备。连接器设备可以安装在本地、数据中心管理程序中或公共云中。有关连接器设备及其安装的详细信息，请参阅云服务连接器设备。

先决条件

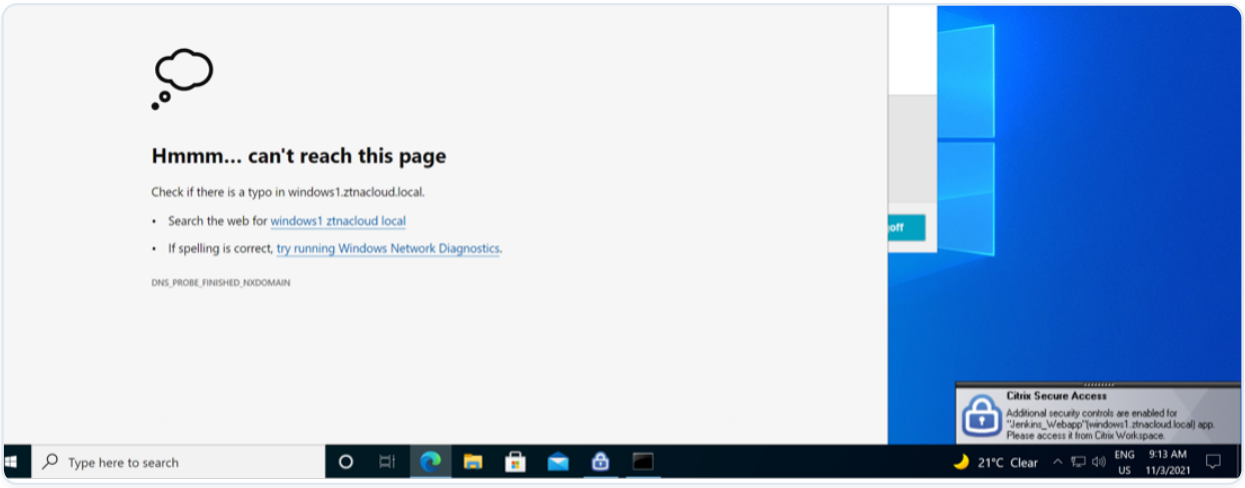
- 在思杰云中访问思杰安全私有访问。

注意事项

- 通过增强安全控制强制执行的内部 Web 应用程序无法通过 Citrix Secure Access 客户端访问。

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

- SaaS 应用程序无法通过 Citrix Secure Access 客户端访问。
- 如果您尝试访问已启用增强安全控制的 HTTP(S) 应用程序，则会显示以下弹出消息。**已为“应用程序名称”(FQDN) 应用程序启用附加安全控制。请从 Citrix Workspace 访问。**



- 如果您想启用 SSO 体验，请使用 Citrix Workspace 应用程序或 Web 门户访问 Web 应用程序。

配置 HTTP(S) 应用程序的步骤与 (/zh-cn/citrix-secure-private-access/service/add-and-manage-apps/support-web-apps.html) 中所述的现有功能相同。

对 TCP/UDP 和 HTTP(S) 应用程序的自适应访问

自适应访问使管理员能够根据多种上下文因素（例如设备状态检查、用户地理位置、用户角色以及 Citrix Analytics 服务提供的风险评分）来管理对业务关键型应用程序的访问。

注意：

- 您可以拒绝访问 TCP/UDP 应用程序，管理员可以根据用户、用户组、用户访问应用程序的设备以及访问应用程序的位置（国家/地区）创建策略。默认情况下允许访问应用程序。
- 为某个应用程序创建的用户订阅适用于为 ZTNA 应用程序配置的所有 TCP/UDP 应用程序目标。

创建自适应访问策略

管理员可以使用管理员引导式工作流向导在 Secure Private Access 服务中配置对 SaaS 应用程序、内部 Web 应用程序和 TCP/UDP 应用程序的零信任网络访问。

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

注意：

- 有关创建自适应访问策略的详细信息，请参阅 Create access policies。
- 有关 Secure Private Access 服务中 SaaS 应用程序、内部 Web 应用程序和 TCP/UDP 应用程序的零信任网络访问的端到端配置，请参阅 Admin-guided workflow for easy onboarding and set up。

登录和注销脚本配置注册表

当 Citrix Secure Access 客户端连接到 Citrix Secure Private Access 云服务时，Citrix Secure Access 客户端会从以下注册表访问登录和注销脚本配置。

注册表：HKEY_LOCAL_MACHINE>SOFTWARE>思杰>安全访问客户端

- 登录脚本路径：SecureAccessLogInScript type REG_SZ
- 注销脚本路径：SecureAccessLogOutScript type REG_SZ

排查应用程序域 IP 地址冲突

创建应用程序时添加的目标会添加到主路由表。 路由表是做出路由决策以将连接建立和流量定向到正确资源位置的真实来源。

- 目标 IP 地址在所有资源位置中必须是唯一的。
- Citrix 建议您避免路由表中 IP 地址或域的重叠。如果遇到重叠，则必须解决它。

以下是冲突场景的类型。**完全重叠**是唯一一种在冲突解决之前限制管理员配置的错误场景。

冲突场景	现有应用程序域条目	来自应用添加的新条目	行为
子集重叠	10.10.10.0-10.10.10.255 RL1	10.10.10.50-10.10.10.60 RL1	允许；警告信息 - IP 域与现有条目存在子集重叠
子集重叠	10.10.10.0-10.10.10.255 RL1	10.10.10.50-10.10.10.60 RL2	允许；警告信息 - IP 域与现有条目存在子集重叠
部分重叠	10.10.10.0-10.10.10.100 RL1	10.10.10.50-10.10.10.200 RL1	允许；警告信息 - IP 域与现有条目存在部分重叠

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

冲突场景	现有应用程序域条目	来自应用添加的新条目	行为
部分重叠	10.10.10.0-10.10.10.100 RL1	10.10.10.50-10.10.10.200 RL2	允许；警告信息 - IP 域与现有条目部分重叠
完全重叠	10.10.10.0/24 RL1	10.10.10.0-10.10.10.255 RL1	错误；`<Completely overlapping IP domain's value>` IP 域与现有条目完全重叠。更改现有路由 IP 条目或配置不同的目标
完全重叠	10.10.10.0/24 RL1	10.10.10.0-10.10.10.255 RL2	错误；`<Completely overlapping IP domain's value>` IP 域与现有条目完全重叠。更改现有路由 IP 条目或配置不同的目标
精确匹配	20.20.20.0/29 RL1	20.20.20.0/29	允许；域已存在于域路由表中。更改将更新域路由表

注意：

- 如果添加的目标导致完全重叠，则在**应用程序详细信息**部分配置应用程序时会显示错误。管理员必须通过修改**应用程序连接**部分中的目标来解决此错误。

  如果**应用程序详细信息**部分没有错误，管理员可以继续保存应用程序详细信息。但是，在**应用程序连接**部分中，如果目标与主路由表中的其他目标或现有条目存在子集和部分重叠，则会显示警告消息。在这种情况下，管理员可以选择解决错误或继续配置。
- Citrix 建议保持**应用程序域**表整洁。如果将 IP 地址域分解为适当的块且没有重叠，则更容易配置新的路由条目。

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

注意事项

- 启用了增强安全性的现有 Web 应用程序的访问权限将通过 Secure Access 客户端拒绝。将显示一条错误消息，建议使用 Citrix Workspace 应用程序登录。
- 通过 Citrix Workspace 应用程序基于用户风险评分、设备姿态检查等进行的 Web 应用程序策略配置，在通过 Secure Access 客户端访问应用程序时适用。
- 绑定到应用程序的策略适用于应用程序中的所有目标。

Windows 登录前始终开启

Secure Private Access 始终开启连接确保托管设备在 Windows 登录前（仅限计算机隧道）和登录后始终连接到企业网络。始终开启功能在用户登录 Windows 系统之前建立计算机级 VPN 隧道。用户登录后，计算机级 VPN 隧道将替换为用户级 VPN 隧道。应用程序访问基于为计算机级隧道分配给计算机的策略以及为用户级隧道分配给用户的策略。

Secure Private Access Windows 登录前始终开启（计算机隧道）功能支持以下计算机：

- 已加入 Active Directory 域的 Windows 计算机
- 已加入 Microsoft Entra ID 混合域的 Windows 计算机

Windows 登录前始终开启通过使用基于计算机设备证书的 Active Directory 身份验证进行身份验证。

设备证书由 Active Directory 企业证书颁发机构 (CA) 颁发。设备证书对于每台已加入域的 Windows 计算机都是唯一的。

注意：

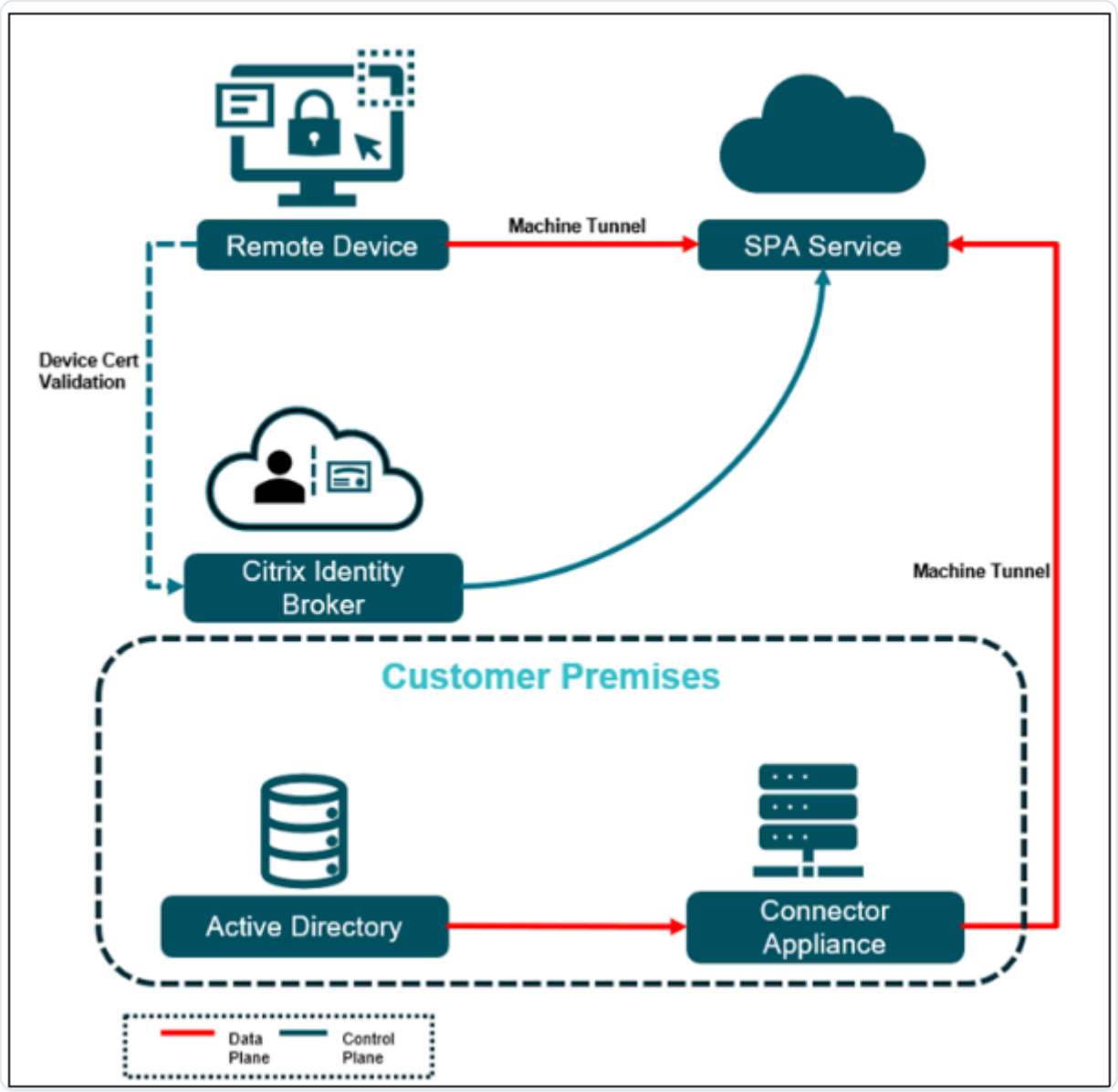
- 支持从单层到多层的 Microsoft 企业证书颁发机构。
- Secure Private Access Windows 登录后始终开启（用户隧道）通过以下 Active Directory 自动登录身份验证方法之一实现：
  - 使用 Windows 登录期间提供的 Active Directory 凭据对 Citrix Secure Access™ 客户端进行单点登录 (SSO)。如果配置了第二个因素，SSO 将不起作用。
  - 基于 Kerberos 的 Citrix Gateway SSO。有关详细信息，请参阅 将本地 Citrix Gateway 连接为 Citrix Cloud 的身份提供程序并预配自适应身份验证。
  - 自适应身份验证配置。有关详细信息，请参阅 预配自适应身份验证。
- Secure Private Access Windows 登录后始终开启（用户隧道）通过以下适用于 Microsoft Entra ID 混合加入计算机的自动登录身份验证方法实现：使用 Microsoft Entra ID 身份验证的主刷新令牌 (PRT) 进行 SSO。

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

禁用 始终提示最终用户输入其凭据。

Always On 如何工作?

下图说明了 Windows 登录前 Always On 功能的工作流程。



- Citrix Identity Broker 在设备启动后立即验证设备证书以对设备进行身份验证。以下是设备证书验证步骤：
  - 客户端根据上传到 Secure Private Access 管理控制台的 CA 证书提供设备证书。
  - Citrix 身份提供程序执行基于设备证书的身份验证。
  - Citrix 身份提供程序验证以下详细信息：
    - 设备证书签名
    - 基于 CRL 的设备证书吊销检查

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

    - 根据 Active Directory 计算机对象验证设备证书

- 成功验证设备证书后，将根据访问策略在设备与公司内部资源之间建立安全的机器隧道。
- 允许访问 Active Directory 后，Windows 登录会使用 Active Directory 验证用户凭据，并支持密码过期和密码更改。
- 在 Windows 登录之后，机器级别的隧道会自动被具有自动登录功能的用户隧道取代。当用户隧道出现故障或断开连接时，连接会回退到机器隧道。
- Active Directory 和混合 Microsoft Entra ID 环境支持自动登录功能。

活动目录和 Microsoft Entra ID 混合 AD 配置

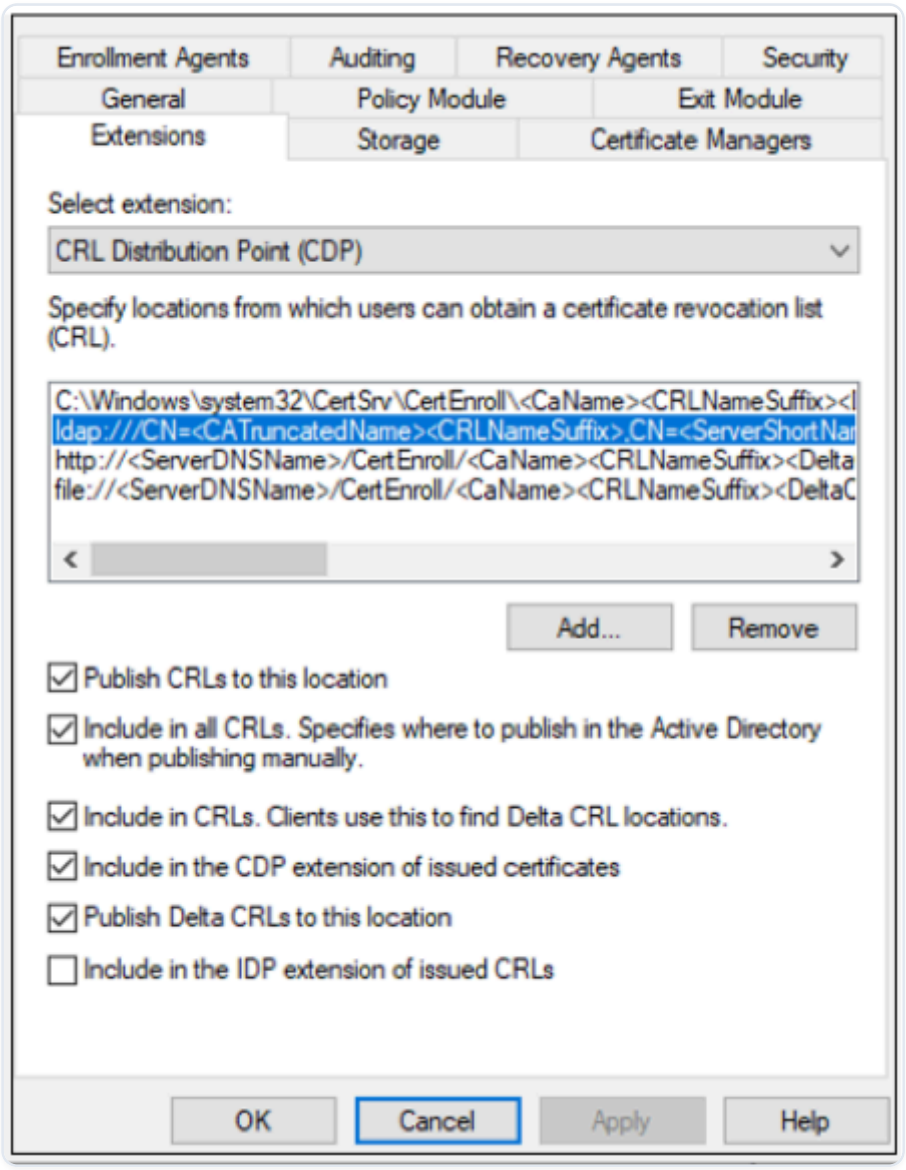
Windows 计算机必须是 Active Directory 或 Microsoft Entra ID 混合加入的，这是 Always On 的先决条件。需要 Active Directory 企业证书颁发机构来颁发用于 Always On 计算机身份验证的设备证书。证书吊销是根据证书颁发机构中配置了 LDAP URL 的 CDP 扩展进行验证的。

设备证书注册配置

设备证书注册涉及以下步骤：

1. Active Directory 企业证书颁发机构颁发用于计算机身份验证的设备证书。
2. 证书颁发机构必须发布 CRL 分发点 (CDP) 扩展的 LDAP URL。

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



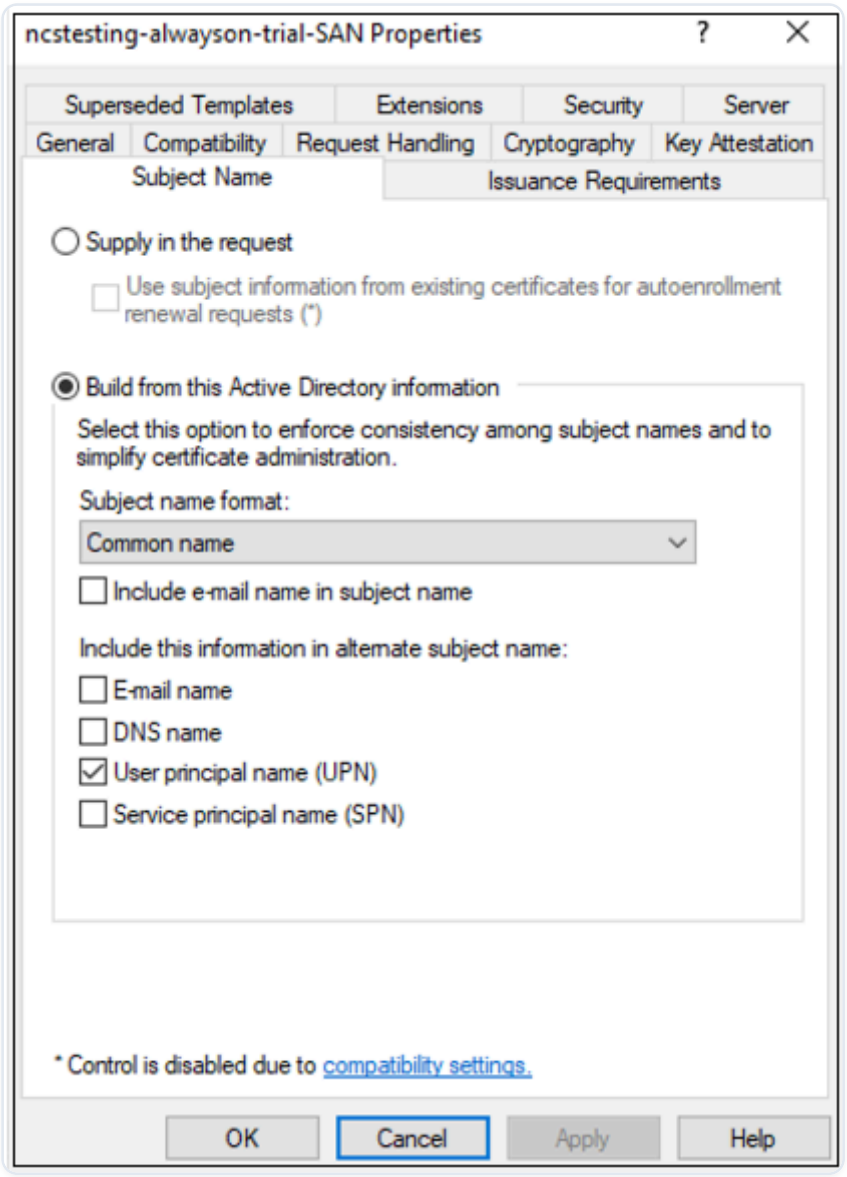
3. 必须在此证书颁发机构中创建证书模板，以注册具有以下详细信息的设备证书。

   a. 打开证书模板管理单元，并复制 **计算机** 或 **工作站身份验证**（首选）模板。

   b. 为证书提供一个新名称。

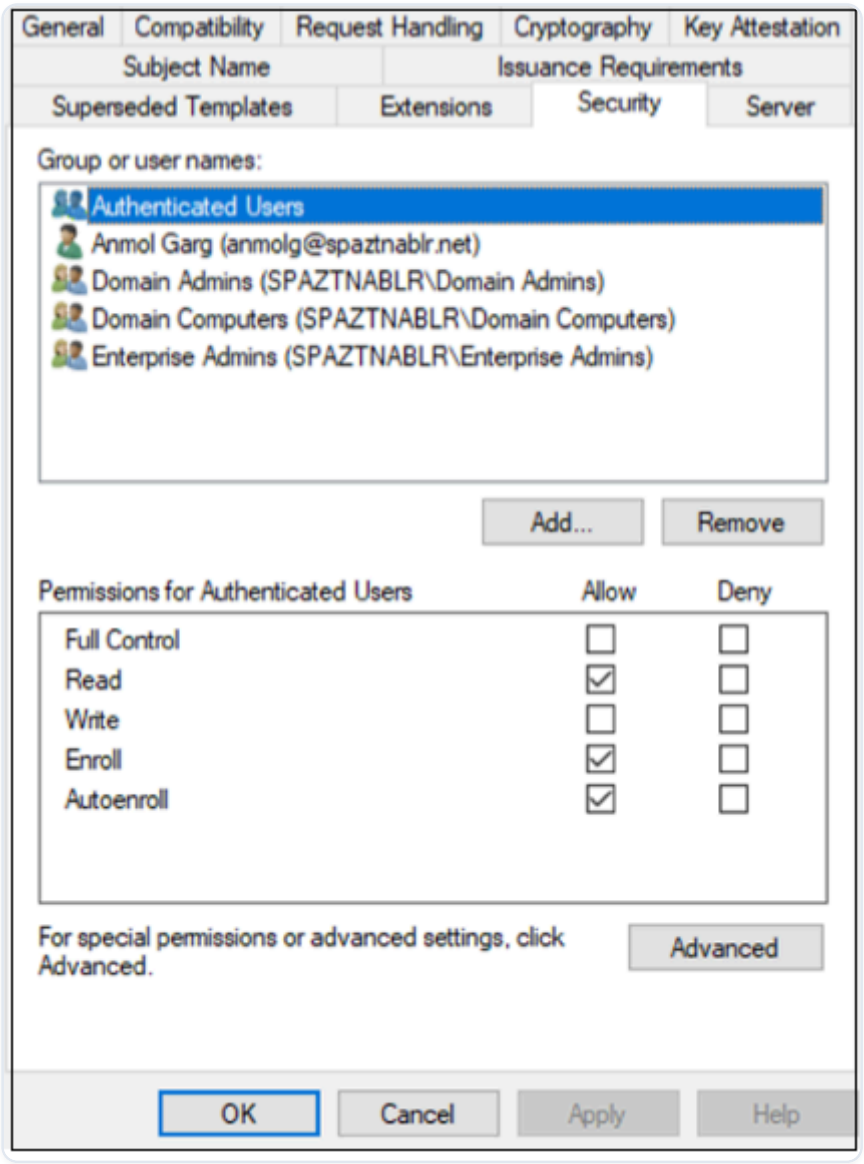
   c. 切换到**使用者名称**选项卡，将**使用者名称格式**设置更改为**通用名称**，并勾选**用户主体名称 (UPN)** 以包含在备用使用者名称中。

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



d. 切换到**安全**选项卡，并添加一个安全组（仅包含计算机帐户），您希望将新的证书模板自动注册到该组。选择添加的组，然后为**自动注册**选择**允许**。

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



注意：

在上一张图片中，**已验证用户**（所有计算机对象）被允许注册/自动注册新的证书模板。

e. (可选) 创建一个允许自动证书注册的组策略对象 (GPO)，并将其绑定到组织单位 (OU) 或域级别。

始终开启自动注册证书(/en-us/citrix-secure-private-access/media/spa-ztna-always-on-autoenroll-certificate.png)

安全私有访问配置

以下部分提供了有关配置 Secure Private Access 的更多信息。

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

在 Windows 登录前配置始终开启 (计算机隧道)

1. 在 Secure Private Access 管理控制台中，导航到 **设置 > 证书存储**。

   > **注意：**
   >
   > 我们建议您使用 **设置 > 证书存储** 下的 **基于计算机的身份验证** 选项，而不是 **设置 > 基于计算机的身份验证**。**设置 > 基于计算机的身份验证** 选项计划在即将发布的版本中移除。

2. 在**证书**页面中，单击**计算机身份验证**选项卡。

   对于 Windows 登录前始终开启功能，**在用户登录前强制执行计算机级别隧道** 切换开关默认处于启用状态。

3. 上传 CA 证书：单击**添加证书**，选择证书，然后单击**打开**。
4. 在**名称**中，输入证书的名称。
5. 在**证书文件**中，浏览到本地驱动器并上传证书文件。

   - 支持根 CA 和中间 CA 证书。要上传的证书必须是 PEM 格式，并包含整个链。证书必须从中间证书一直到根 CA 生成。
   - 如果证书是 CER 格式，请在 Linux 或 Mac 终端上运行以下命令将其转换为 PEM 格式。将证书转换为 PEM 格式后，在 Secure Private Access 用户界面中上传证书。

     ```
     openssl x509 -in /Users/t_abhishes2/Downloads/cert12.crt out/Users/t_abhishes2/Downloads/cer_pem12_ao.pem
     ```

6. 单击 **保存**。

   证书将添加到“**计算机身份验证**”选项卡中可用证书的列表中。

7. 创建一个 TCP/UDP 应用程序以将 Active Directory 作为 TCP/UDP 服务器访问。例如，Active Directory 域、IP 地址和端口。这适用于使用 AD 凭据的 Windows 用户登录。有关创建 TCP/UDP 应用程序的详细信息，请参阅 管理员配置 – Citrix Secure Access 客户端对 TCP/UDP 应用程序的访问。
8. 如果需要在 Windows 登录前和用户级隧道迁移前访问，请创建其他应用程序。
9. 创建访问策略并为已加入域的计算机或其 AD 组提供访问权限。

   a. 在 Secure Private Access 管理控制台中，单击“**访问策略**”，然后单击“**创建策略**”。

   b. 输入策略名称和策略描述。

   c. 在“**应用程序**”中，选择必须强制执行此策略的应用程序或应用程序集。

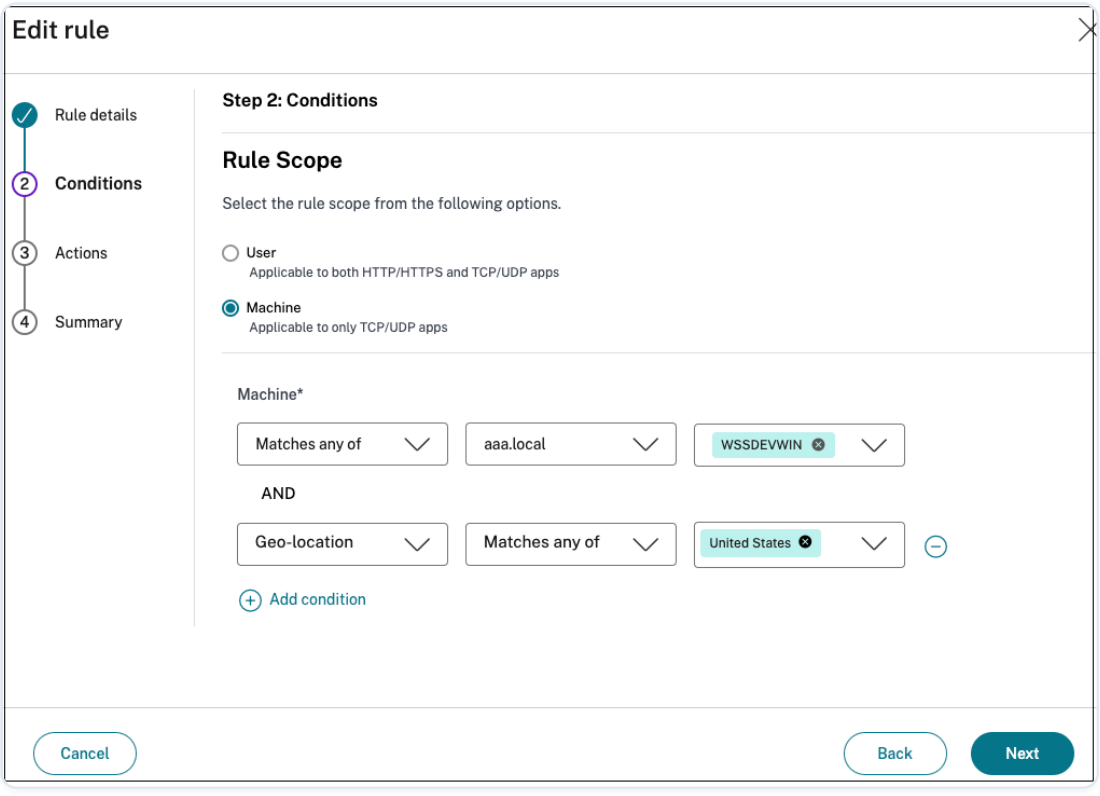
© 1997–2026 Citrix Systems, Inc. All rights reserved.

d. 单击“**创建规则**”为策略创建规则。

- 输入规则名称和规则的简要说明，然后单击“**下一步**”。
- 在“**规则范围**”中，选择“**计算机**”。

> **注意：**
>
> 当您选择一台计算机时，访问权限会受到限制，因为计算机级隧道基于单因素身份验证。

- 选择匹配条件和域，然后搜索必须应用策略的计算机/组。如果需要，添加更多条件。完成后，单击“**下一步**”。
  - **匹配其中任意一个** – 只有与字段中列出的任何名称匹配且属于所选域的计算机/组才允许访问。
  - **不匹配任何一个** – 除了字段中列出且属于所选域的计算机/组之外，所有计算机/组都允许访问。



10. 选择以下操作之一，根据条件评估进行应用。

- **允许访问**
- **拒绝访问**

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

11. 单击“**下一步**”，然后单击“**完成**”。
12. （可选）为地理位置和网络位置等创建其他规则。有关详细信息，请参阅配置访问策略。

    该策略列在“访问策略”页面上。默认情况下，会为策略分配优先级顺序。值越低的优先级越高。优先级编号最低的策略会首先进行评估。如果策略不符合定义的条件，则会评估下一个策略。如果条件匹配，则会跳过其他策略。

连接器设备配置

连接器设备执行设备证书验证、证书吊销检查 (CRL) 和设备对象验证，以实现始终在线设备证书身份验证。连接器设备必须加入 Active Directory 域，才能支持设备证书身份验证。

客户端配置

- 需要始终在线支持的 Windows 计算机必须加入 Active Directory 或 Entra ID 混合域。
- Windows 计算机必须从企业证书颁发机构注册设备证书，以用于 Secure Private Access 始终在线。
- 设备证书属性必须包含以下详细信息。
  - 设备证书中的颁发者名称必须与上传到 Secure Private Access 管理控制台的 CA 证书的通用名称匹配。

    始终在线 CA 颁发者名称(/en-us/citrix-secure-private-access/media/spna-ztna-always-on-issuer.png)
  - 主题必须包含计算机的通用名称。

    始终在线主题名称(/en-us/citrix-secure-private-access/media/spna-ztna-always-on-subject.png)
  - 主题备用名称 (SAN) 必须包含计算机的 UPN。

    始终在线 SAN(/en-us/citrix-secure-private-access/media/spna-ztna-always-on-san.png)
  - CRL 分发点必须包含相应的 LDAP URL。

    始终在线 CRL DP(/en-us/citrix-secure-private-access/media/spna-ztna-always-on-crl-cdp.png)
  - 认证路径必须与证书颁发机构链相符。

    始终在线 CRL DP(/en-us/citrix-secure-private-access/media/spna-ztna-always-on-cert-path.png)
- 安装用于 Always On 的 Citrix Secure Access 客户端。

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

- 必须在客户端上创建以下注册表项，才能在 Windows 登录前启用 Always On。
  - 在注册表路径 HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Client 中的 **CloudAlwaysOnURL**。

    注册表类型 - STRING

    注册表值 - `<Customer store FQDN>` (例如，company.cloud.com)
  - **AlwaysOnService** 位于 HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Client 中。

    注册表类型 - DWORD

    注册表值 - 0x00000002

在 Windows 登录后配置 Always On（计算机/用户隧道）

成功登录 Windows 后，计算机隧道将继续运行，直到用户使用 Citrix Secure Access 客户端成功登录。

- 如果用户自动登录成功，计算机隧道将迁移到用户隧道。
- 如果用户自动登录失败，计算机隧道将继续运行。
- 如果用户隧道断开连接，连接将自动回退到计算机隧道。

StoreFront Cloud 身份验证配置中支持 Windows 登录后的用户自动登录，支持以下身份验证方法。

- 使用 Active Directory 进行身份验证（无第二因素）- AD 凭据 SSO
- 使用配置了 Kerberos SSO 的 Citrix Gateway/自适应身份验证进行身份验证
- 使用 Azure Active Directory 进行身份验证（使用 Microsoft Entra ID 身份验证的主刷新令牌 (PRT) 进行 SSO）。

注意：

禁用 始终提示最终用户输入其凭据。

限制

- 计算机 UPN 主机名不得超过 15 个字符。
- 仅当计算机已加入域且设备证书存在时，才支持 Windows 自动登录（首次用户 (FTU)）情况。
- 仅在 Windows 10 或更高版本上支持 Windows 登录前始终开启功能。

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

- Windows Server 操作系统不支持 Windows 登录前始终开启功能。
- Windows 登录前始终开启功能不支持云连接器。即使您未选择连接器设备作为首选连接器，计算机隧道流量也会通过连接器设备。

参考

- 在 Secure Private Access 控制台中创建 TCP/UDP 应用程序
- 将访问策略分配给 TCP/UDP 应用程序
- 将本地 Citrix Gateway 作为身份提供程序连接到 Citrix Cloud
- 预配自适应身份验证

用于 TCP 和 UDP 服务器的保留 CIDR 地址

管理员可以为 TCP/UDP 服务器配置保留的 CIDR IP 地址。在 DNS 解析期间，这些 IP 地址会在 DNS 响应中共享，而不是实际的 IP 地址。

以下是允许的保留 CIDR IP 地址范围：

- 10.0.0.0/8
- 172.16.0.0/12
- 192.168.0.0/16

注意：

确保保留的 IP 地址不与以下内容冲突：

- 在客户资源位置为 TCP/UDP 应用程序配置的 IP 地址。
- 客户端计算机的网络子网。

配置保留的 CIDR IP 地址

1. 单击“**设置**”，然后单击“**全局配置**”。



2. 在“**Secure Access Agent 的保留网络子网**”中，单击“**管理**”。

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

3. 在“**IP CIDR**”中，输入专用 IP 地址范围。
4. 点击 **保存**。

DNS 后缀以将 FQDN 解析为 IP 地址

DNS 后缀是应用于所有最终用户的全局配置。Citrix Secure Private Access™ 服务的 DNS 后缀功能可用于以下用例：

- 通过为后端服务器添加 DNS 后缀域，使 Citrix Secure Access™ 客户端能够将非完全限定域名（主机名）解析为完全限定域名 (FQDN)。
- 使管理员能够使用 IP 地址（IP CIDR/IP 范围）配置应用程序，以便最终用户可以使用 DNS 后缀域下的相应 FQDN 访问应用程序。

例如，在解析非完全限定域名“workday”时，如果配置了 DNS 后缀“citrix.net”，则操作系统会附加后缀“citrix.net”并解析为“workday.citrix.net”。

如果配置了多个 DNS 后缀，则 DNS 后缀会按顺序解析。例如，假设添加了以下后缀：

- `".citrix.net"`
- `".citrix.com"`
- `".xenserver.com"`

当最终用户键入“workday”时，操作系统会尝试按以下顺序解析 FQDN。如果使用一个后缀成功，则会跳过其余后缀。

1. workday.citrix.net
2. workday.citrix.com
3. workday.xenserver.com

重要提示：

- DNS 后缀配置只能通过附加使用 DNS 后缀功能配置的域来使客户端解析非完全限定域名。最终用户要访问 DNS 后缀域下的 FQDN，管理员必须使用 IP 地址、FQDN 或通配符域配置应用程序。有关详细信息，请参阅用例示例中的第 4 点。
- 如果配置了两个不同的应用程序，一个使用 FQDN，另一个使用 IP 地址，并且两者都对应同一个后端服务器，则使用 IP 地址的应用程序的策略具有更高的优先级。有关详细信息，请参阅用例示例中的第 5 点。

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

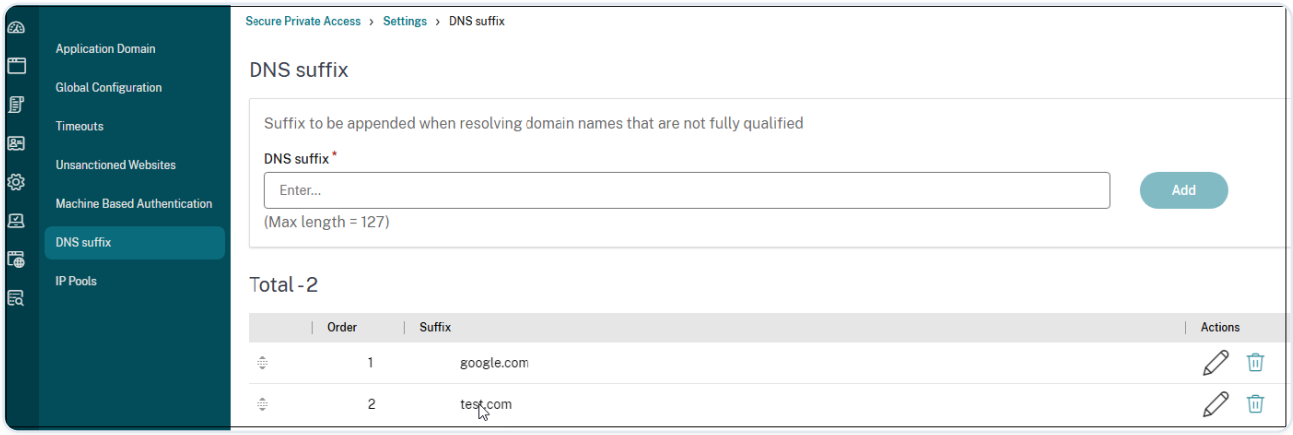
先决条件

- 客户必须拥有 Secure Private Access Advanced 版本的使用权限才能使用 DNS 后缀功能。
- 请联系 Citrix 产品管理团队以启用 DNS 后缀功能标志。

如何添加 DNS 后缀

1. 在 Secure Private Access 磁贴上，单击“**管理**”。
2. 在 Secure Private Access 登录页面上，单击“**设置**”，然后单击“**DNS 后缀**”。
3. 在“**DNS 后缀**”字段中，输入解析非完全限定名称时必须附加的后缀。
4. 单击“**添加**”。

后缀按添加顺序排列。管理员可以删除或修改后缀。



用例示例

请考虑以下事项：

- 管理员已将 IP 地址 192.0.2.1 分配给客户网络中的一台计算机。
- 该计算机的 FQDN（IP 地址为 192.0.2.1）位于“citrix.net”域下（例如，workday.citrix.net）。

	DNS 后缀和应用程序配置	最终用户体验
1	管理员将 DNS 后缀配置为“citrix.net”，并创建一个 IP 地址为 192.0.2.1 的应用程序，其访问策略为 user1 设置为“允许”。	当 user1 尝试连接到“workday”时，FQDN 会附加“citrix.net”（workday.citrix.net），并且 IP 地址解析为 192.0.2.1。由于已为 user1 配置了应用程序并允许访问 192.0.2.1，因此授予访问权限。

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

	DNS 后缀和应用程序配置	最终用户体验
	注意： 最终用户可以使用 192.0.2.1、workday.citrix.net 或“workday”访问 Workday 应用程序。	
	如果没有 DNS 后缀配置，通过 “workday” 和“workday.citrix.net”的访问将被拒绝。	
2	管理员将 DNS 后缀配置为“citrix.net”，创建一个 FQDN 为 (workday.citrix.net) 的应用程序，并将访问策略为 user1 设置为“允许”。	当 user1 尝试连接到“workday”时，“citrix.net”会附加到 “workday” （workday.citrix.net）。最终用户可以访问 Workday，因为已配置了“workday.citrix.net”的应用程序，并且访问策略为 user1 设置为“允许”。
	注意： 最终用户可以使用 workday.citrix.net 或“workday”访问 Workday 应用程序。	
	访问 192.0.2.1 被拒绝，因为没有配置使用此 IP 地址的应用程序。	
3	管理员将 DNS 后缀配置为“citrix.net”，创建一个通配符域为“*.citrix.net”的应用程序，并将访问策略为 user1 设置为“允许”。	当 user1 尝试连接到“workday”时，“citrix.net”会附加到 “workday” （workday.citrix.net）。最终用户可以访问 Workday，因为已配置了“*.citrix.net”的应用程

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

	DNS 后缀和应用程序配置	最终用户体验
		序，并且访问策略为 user1 设置为“允许”。
	注意： 最终用户可以使用 workday.citrix.net 或“workday”访问 Workday。	
	由于没有配置此 IP 地址的应用程序，因此拒绝访问 192.0.2.1。	
4	管理员将 DNS 后缀配置为“citrix.net”。没有为 user1 配置 FQDN (workday.citrix.net) 或 192.0.2.1 的应用程序。	当 user1 尝试连接到“workday”时，客户端会将“workday”后缀为“citrix.net”，并将“workday.citrix.net”解析为 192.0.2.1。但是，user1 无法连接到私有服务器 (workday.citrix.net/ 192.0.2.1)，因为没有为 user1 配置 192.0.2.1 或 workday.citrix.net 或 *.citrix.net 的应用程序。
5	管理员将 DNS 后缀配置为“citrix.net”。添加一个 IP 地址为 192.0.2.1 的应用程序，并将 user1 的访问策略设置为“拒绝”。然后添加另一个 FQDN (workday.citrix.net) 解析为 192.0.2.1 的应用程序，并将 user1 的访问策略设置为“允许”。	当 user1 尝试连接到“workday”时，“citrix.net”会作为后缀添加到 Workday (workday.citrix.net)，并且 IP 地址会解析为 192.0.2.1。但是，由于配置了 IP 192.0.2.1 的应用程序策略优先于配置了 FQDN 的应用程序，因此拒绝访问 Workday。

使用 HAR 文件发现相关域

Secure Private Access 允许您上传 HTTP 存档 (HAR) 文件，以自动发现应用程序访问的域。您可以查看发现的域，并选择要添加到应用程序相关域配置中的域。这通过减少手动识别和配置相关域的需求，简化了应用程序的入职过程。

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

以前，管理员必须提前了解应用程序的所有相关域，或者在用户遇到被阻止的 URL 时被动地发现它们。因为默认情况下，除了已配置的 URL 之外，所有 URL 都会被阻止，所以这种被动方法会导致糟糕的用户体验。Secure Private Access 无法识别应用程序中的内部或嵌入式 URL。

示例

假设您正在配置一个应用程序，其主域是 `example.com`。在使用该应用程序时，浏览器还会访问其他几个域。例如：

- `api.example.com` – 处理应用程序的后端 API 调用。
- `auth.example.com` – 管理登录和身份验证。
- `cdn.example.com` – 提供静态内容，例如图像、脚本和样式表。
- `login.microsoftonline.com` – 提供第三方身份验证。
- `player.vimeo.com` – 加载嵌入式视频内容。

无需手动识别这些域，而是：

1. 在使用应用程序时捕获 HAR 文件。
2. 将 HAR 文件导入 Secure Private Access 中。
3. 查看 Secure Private Access 发现的域。例如，导入可能会显示所需的 `api.example.com`、`auth.example.com` 和 `cdn.example.com`，以及您可以选择排除的域，例如 `player.vimeo.com`。
4. 选择应用程序所需的域。
5. 根据需要配置路由和资源位置。

这提供了一种更快的方法来识别和配置应用程序连接所需的域。

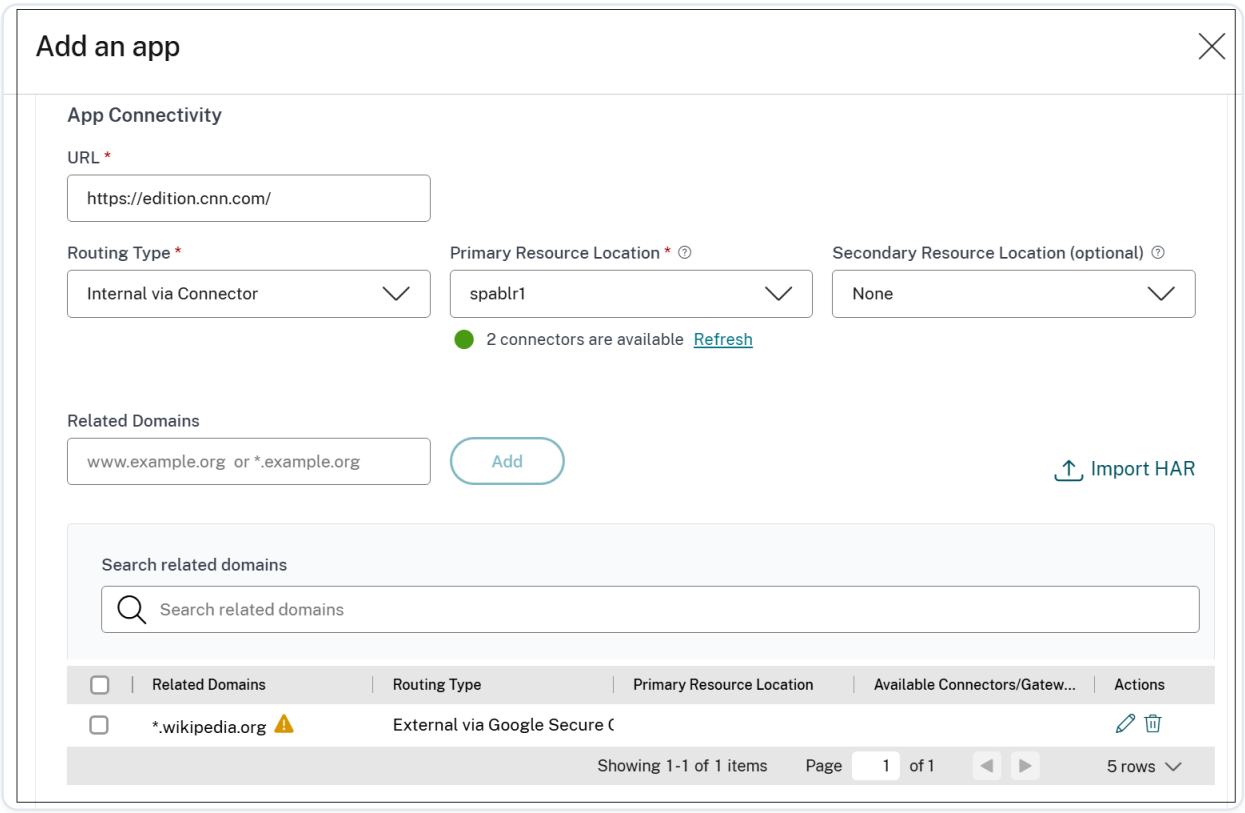
先决条件

确保在访问 Web 或 SaaS 应用程序时已捕获 HAR 文件。HAR 文件必须包含网络请求信息，并且大小必须小于或等于 50 MB。

导入 HAR 文件

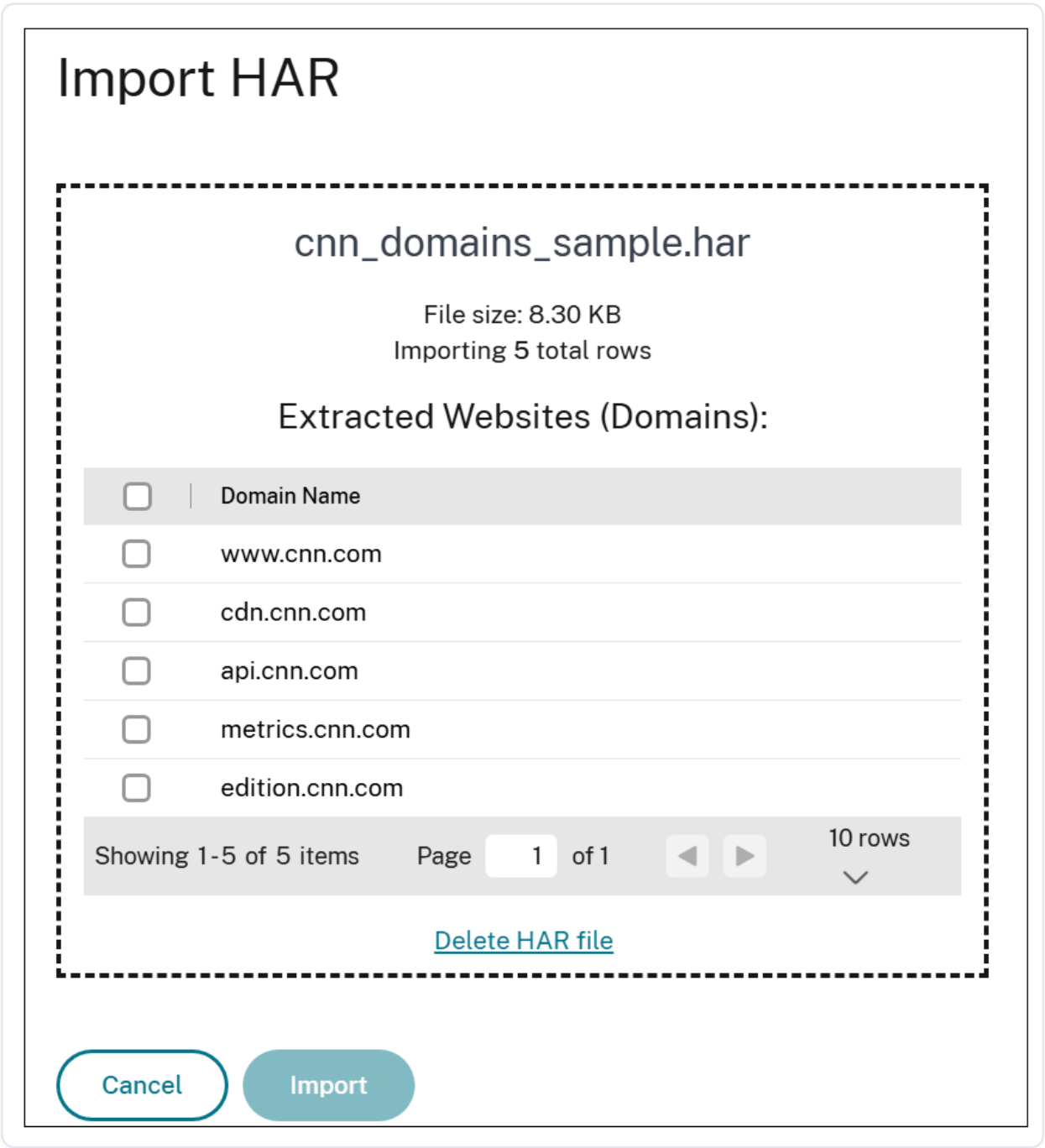
1. 在 Secure Private Access 管理门户中，打开要配置的 Web 或 SaaS 应用程序。
2. 转到 **App Connectivity** 并单击 **Import HAR**。

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



3. 将 HAR 文件拖放到导入窗口中，或从设备中选择文件。
4. Secure Private Access 分析 HAR 文件并显示从网络请求中识别的域。

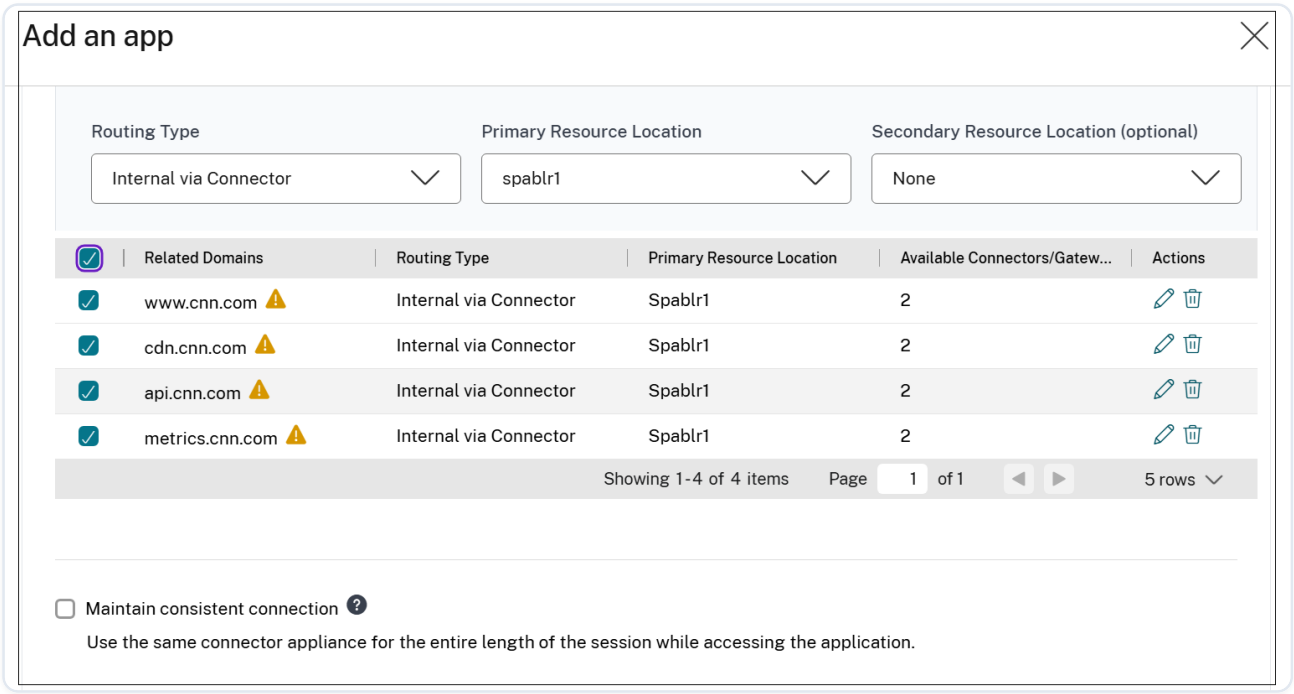
© 1997–2026 Citrix Systems, Inc. All rights reserved.



5. 审查发现的域。
6. 选择要添加到应用程序的域。
7. 选择 **Import**。

所选域将添加到应用程序的 **Related Domains** 配置中。

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



注意：

在导入之前，请查看发现的域。HAR 文件可能包含应用程序连接不需要的域。

管理相关域

导入域后，您可以从“**相关域**”表中管理它们：

- **搜索域** – 使用搜索字段筛选表并快速查找特定域。
- **选择域** – 选择单个域，或使用表头复选框选择多个域。此选择可用于同时对多个域执行操作。
- **编辑域配置** – 更新相关域的配置，包括路由类型、主资源位置和辅助资源位置。
- **批量编辑域** – 选择多个符合条件的域，并同时更新其路由和资源位置设置。批量编辑适用于适用的内部域。外部域可能不支持所有配置选项。
- **资源位置** – 配置相关域时，分配一个主资源位置，并在适用情况下分配一个辅助资源位置。使用这些设置来定义 Secure Private Access 如何路由相关域的流量，以及使用哪些资源位置来提供连接。

验证和文件要求

HAR 导入功能在处理上传的文件之前会对其进行验证。

- 只有包含网络请求条目的有效 HAR 文件才能导入。
- 支持的最大文件大小为 **50 MB**。

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

- 域会自动从 HAR 文件中的 URL 中提取。
- 重复的域会自动移除。
- 域在添加到相关域配置之前会进行规范化。

使用路由例外的基于端口的路由 - 预览

基于端口的路由功能允许管理员针对同一目标的不同端口，使用路由例外以不同方式路由 TCP/UDP 应用程序的流量。在 Secure Private Access 上载入应用程序时，管理员可以使用以下选项之一定义应用程序流量的路由方式：

- **通过连接器内部**：流量通过连接器安全地隧道传输。
- **通过 NetScaler Gateway 内部**：流量通过 NetScaler Gateway 使用混合数据路径进行路由。
- **外部**：流量直接路由，无需通过 Secure Private Access 进行隧道传输。

为了以不同方式路由同一目标的不同端口的流量，管理员必须使用访问策略路由例外。每个需要不同路由决策的目标和端口组合都必须配置为单独的应用程序并绑定到单独的策略。UI 会强制执行唯一性检查，因此不能在具有相同目标的不同应用程序中配置不同的路由。

基于端口的路由用例

场景： 管理员在同一服务器 (10.102.124.135) 上托管两个应用程序。

- 在端口 22 上进行 SSH 访问
- 在端口 80、443 上进行 Web 访问

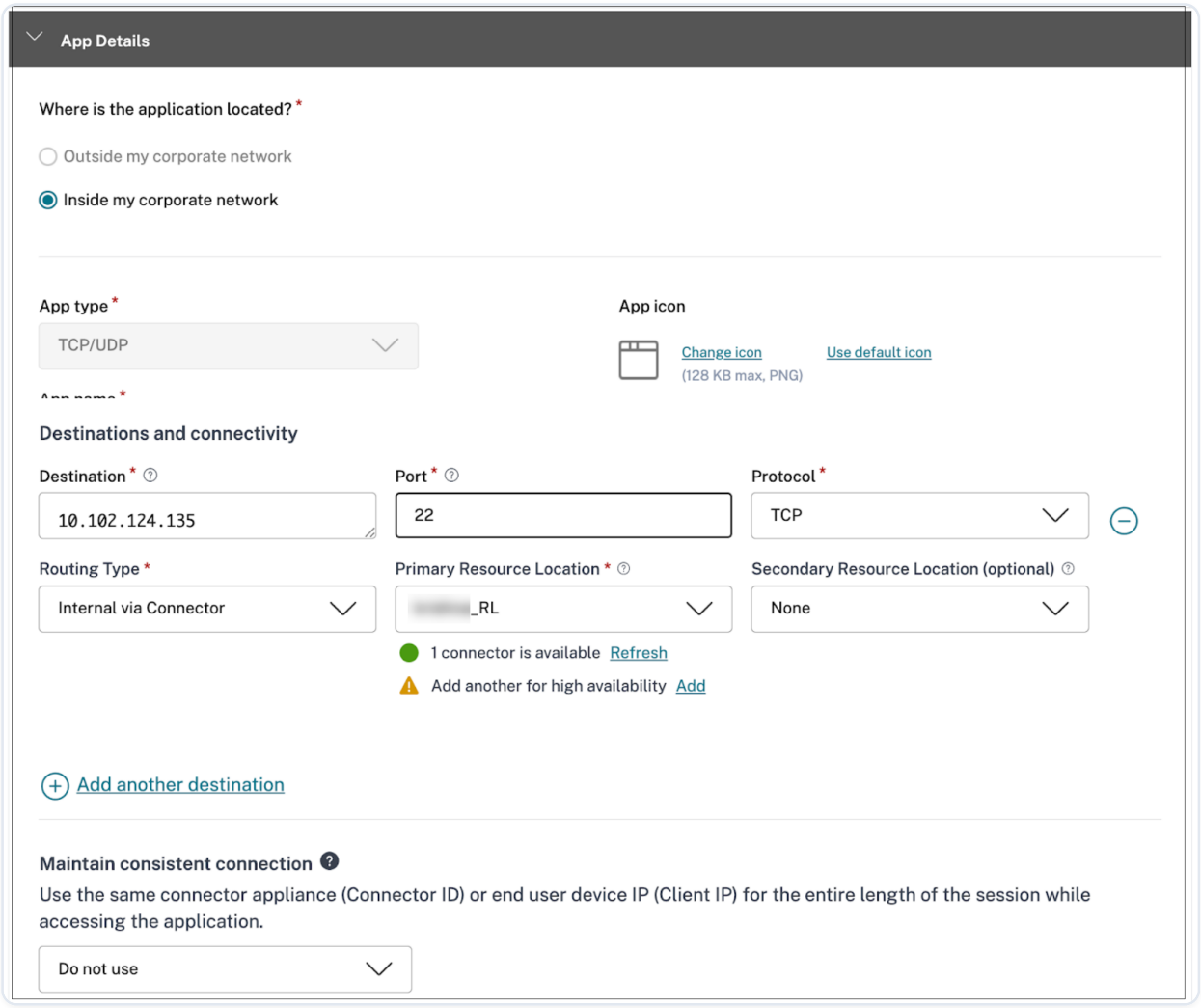
要求：

- 允许开发人员用户组通过连接器内部访问 SSH。
- 允许业务部门用户组直接从公司网络访问 Web 应用程序。

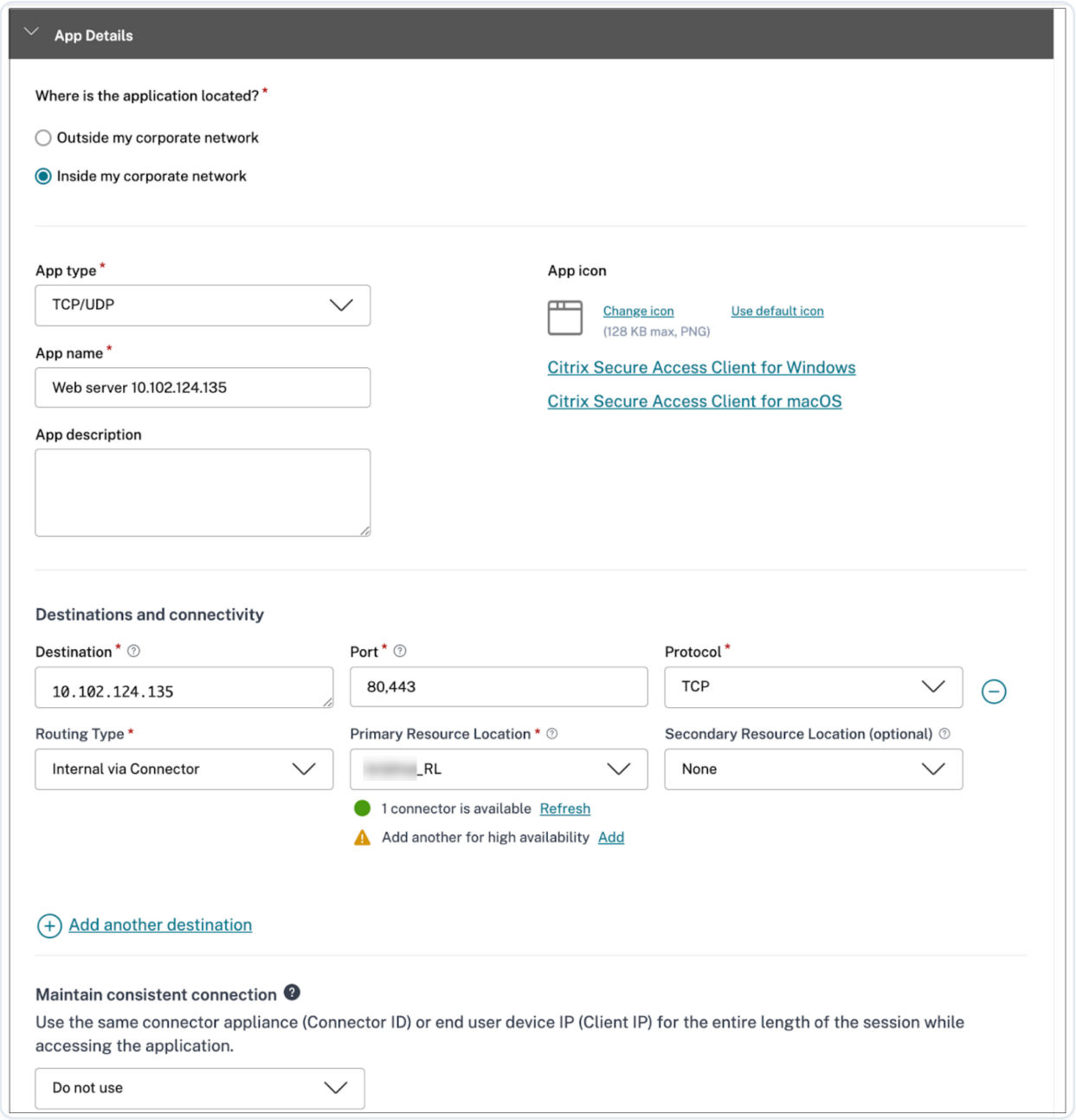
配置：

1. 为每个要求创建单独的应用程序。有关详细信息，请参阅对 TCP/UDP 应用程序的支持。
    - 为 SSH 访问创建应用程序 (destination:10.102.124.135, port 22)
    - 为 Web 访问创建另一个应用程序 (destination :10.102.124.135, port 80,443)

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

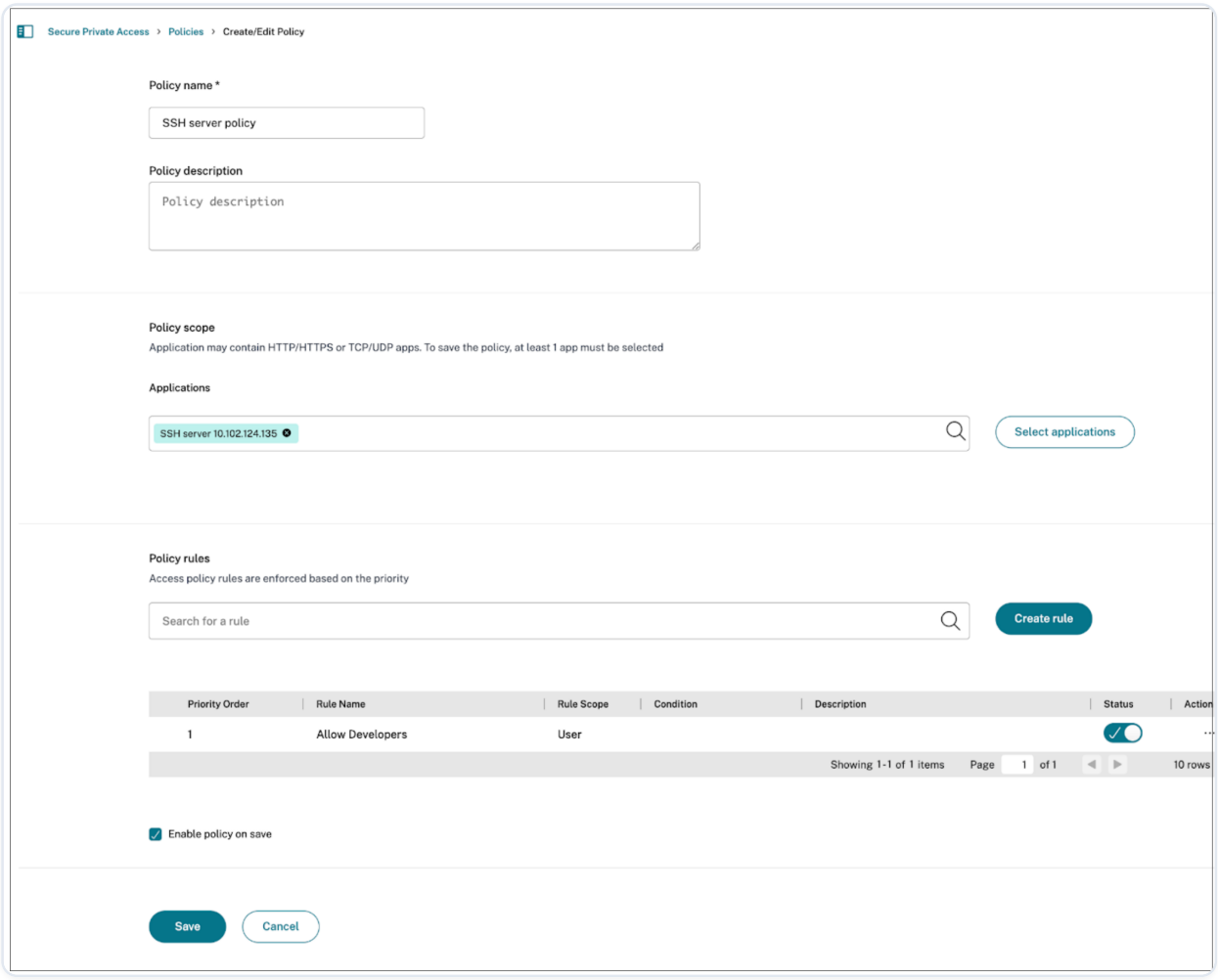


© 1997–2026 Citrix Systems, Inc. All rights reserved.

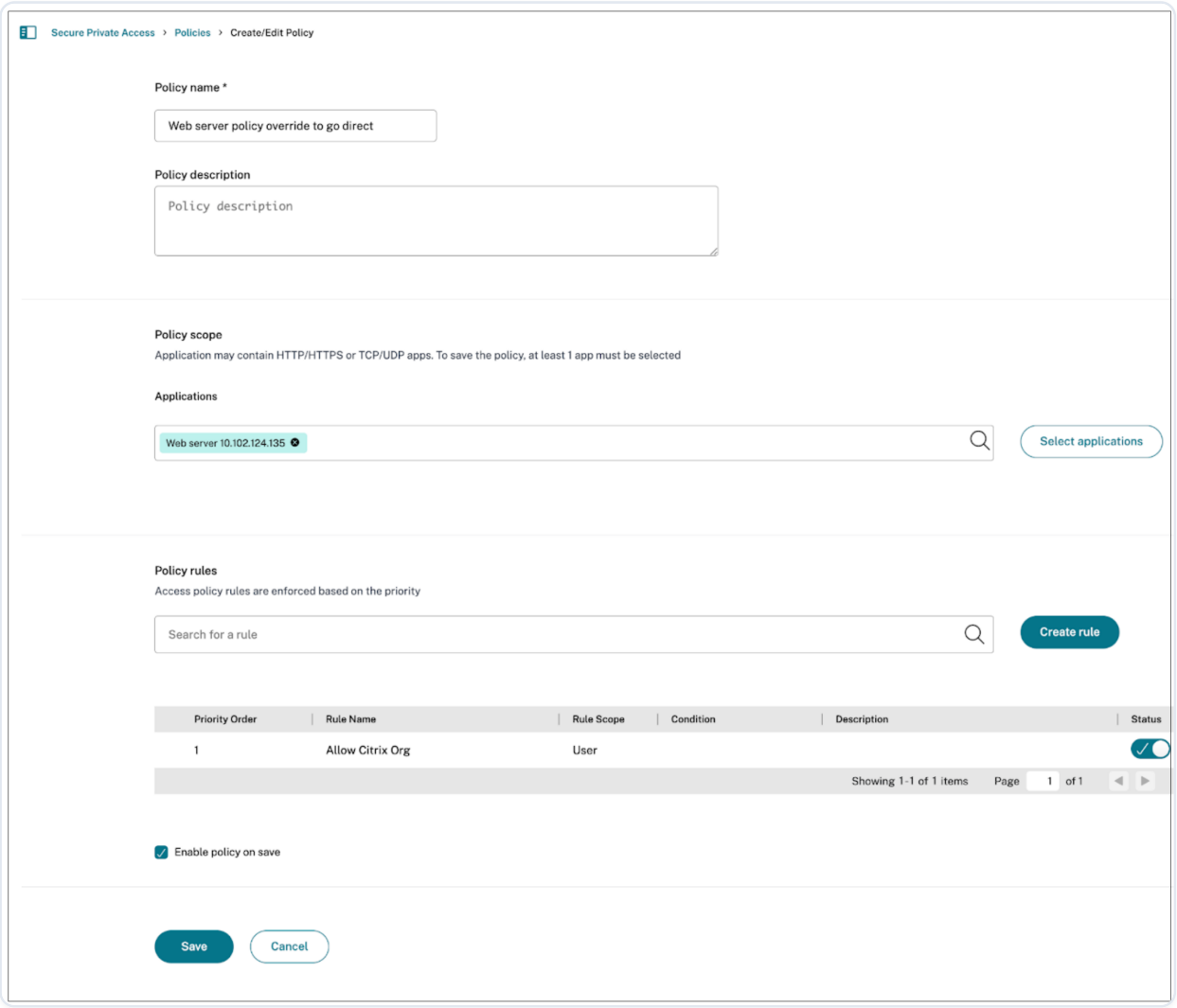


2. 根据需要配置每个应用程序的其他详细信息。
3. 创建单独的访问策略。
   - 为每个应用程序定义单独的策略。
   - 使用路由例外指定针对每个已配置应用程序的所需路由行为。

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

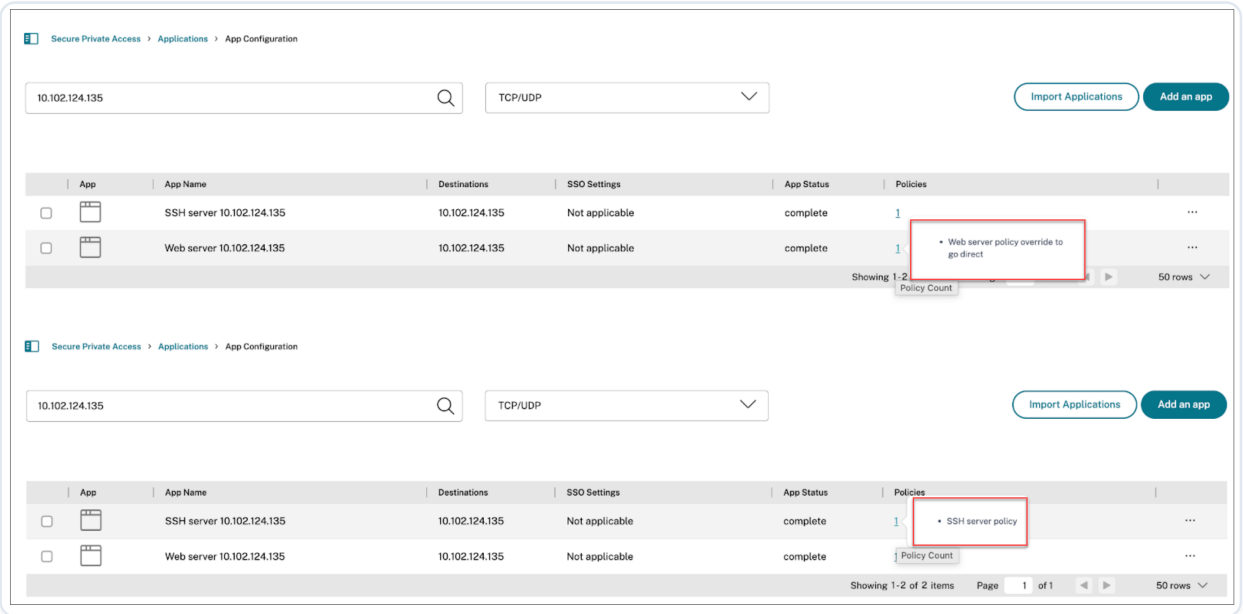


© 1997–2026 Citrix Systems, Inc. All rights reserved.



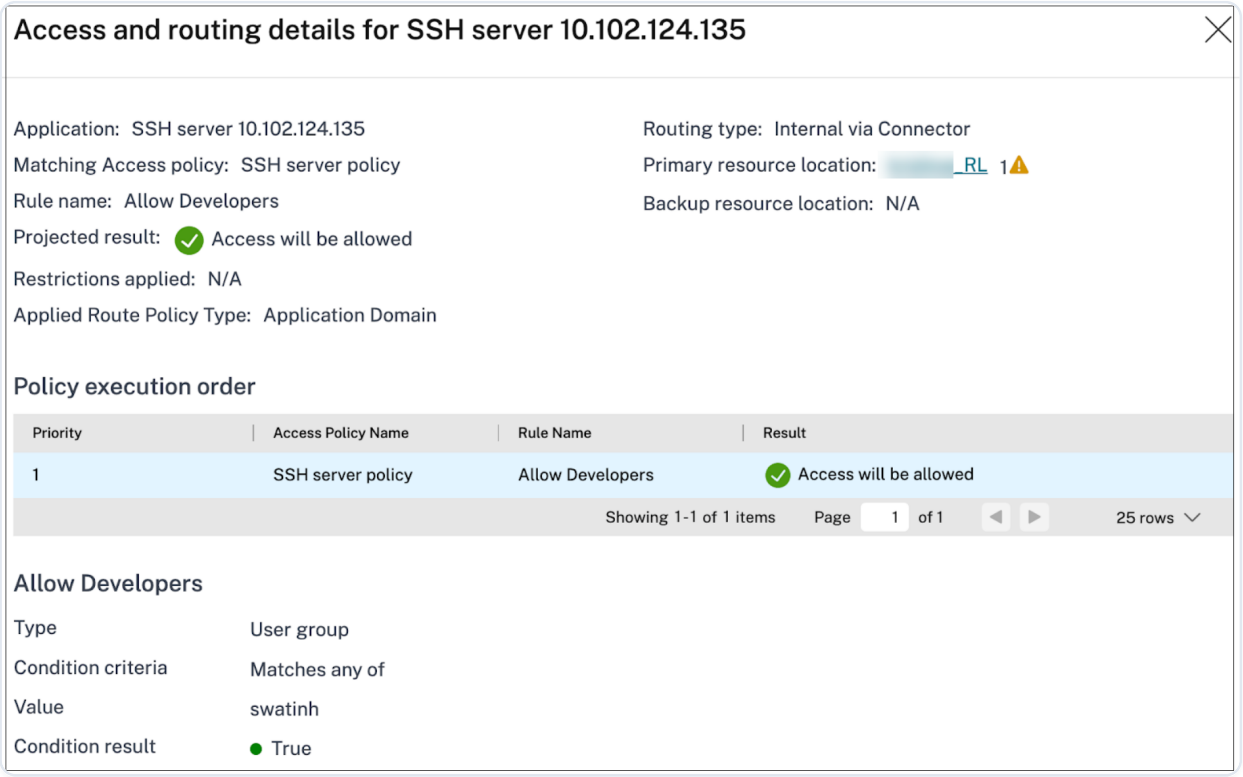
4. 将策略绑定到应用程序。

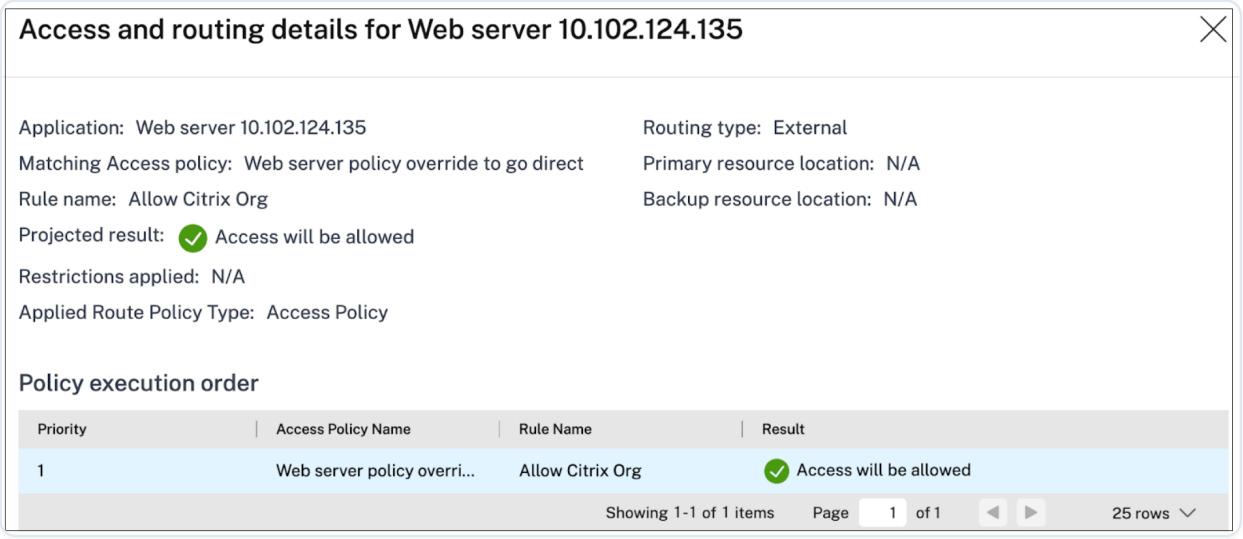
   - 将 SSH 访问策略绑定到 SSH 应用程序。
   - 将 Web 访问策略绑定到 Web 应用程序。



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

5. 使用策略建模器审查和验证应用程序、策略和路由确认。





路由选项限制：

- 访问策略从上到下进行评估，因此将应用与用户、上下文和应用程序匹配的第一个策略。对于基于主机名的应用程序，应用策略中定义的路由配置（路由类型和资源位置）用于解析目标。
- 如果访问策略中未定义路由例外，则使用应用程序配置中的路由配置。 路由隧道和直接路由是互斥的。因此，对于基于主机名的目标，我们不能为其不同的端口同时通过隧道（内部）和通过直接（外部）进行路由。

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

- 内部路由（通过连接器或 NetScaler Gateway）和直接路由（外部）是互斥的。因此，基于主机名的目标不能同时进行内部和外部路由。如果要求应用程序的流量同时进行内部和外部路由，建议使用基于 IP 的目标来载入应用程序。

演示基于端口的路由的示例

下图演示了策略优先级和路由例外如何影响最终用户体验：

Table	Configured applications and policies for a user		Expected behaviour for the user
	App name: LDAP_app Destination URL: example.com Port Number:389 Selected routing in application: 1. Routing Type:Internal via connector 2. Primary resource location: ResourceLocation1 Access policy: LDAP_policy for LDAP_app Routing Exception : None Higher priority	App name: SSH_app Destination URL: example.com Port Number: 22 Pre-selected routing in application (from LDAP_app destination URL) • Routing Type:Internal via connector • Primary resource location: ResourceLocation1 Access policy: SSH_policy for SSH_app Routing Exception: External Lower priority	Both example.com:389 and example.com:22 are resolved via Secure Private Access(Resourcelocation1). example.com:389 is launched successfully. example.com:22 fails to launch as it is supposed to go via External. **Note:** It is not recommended to configure the same domain to go via External and Internal. This limitation is only for FQDN.
	App name: LDAP_app Destination URL: example.com Port Number:389 Selected routing in application: • Routing Type:Internal via connector • Primary resource location: ResourceLocation1 Access Policy :LDAP_policy for LDAP_app Routing Exception : None Lower priority	App name: SSH_app Destination URL: example.com Port Number:22 Pre-selected routing in application (from LDAP_app destination URL) • Routing Type:Internal via connector • Primary resource location: ResourceLocation1 Access Policy:SSH_policy for SSH_app Routing Exception: External Higher priority	Both example.com:389, example.com:22 are launched via External.
	App name: LDAP_app Destination URL: 10.0.0.1 Port Number: 389 Selected routing in application: • Routing Type:Internal via connector • Primary resource Location: ResourceLocation1 Access policy: LDAP_policy for LDAP_app Routing Exception: None Higher priority	App name: SSH_app Destination URL: 10.0.0.1 Port Number: 22 Pre-selected routing in application (from LDAP_app destination URL) • Routing Type:Internal via connector • Primary resource Location: ResourceLocation1 Access policy: SSH_policy for SSH_app Routing Exception: External Lower priority	10.0.0.1:389 is launched via Secure Private Access (ResourceLocation1). 10.0.0.1:22 is launched via External.
	App name: LDAP_app Destination URL: 10.0.0.1 Port Number: 389 Selected routing in application: • Routing Type:Internal via connector • Primary resource Location: ResourceLocation1 Access policy : LDAP_policy for LDAP_app Routing Exception: None Lower priority	App name: SSH_app Destination URL: 10.0.0.1 Port Number: 22 Pre-selected routing in application (from LDAP_app destination URL) • Routing Type:Internal via connector • Primary resource Location: ResourceLocation1 Access policy: SSH_policy for SSH_app Routing Exception: External Higher priority	10.0.0.1:389 is launched via Secure Private Access (ResourceLocation1). 10.0.0.1:22 is launched via External.

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

在 Secure Private Access 控制台中管理证书

Secure Private Access 证书存储为管理员提供了一个集中位置，可以高效管理证书颁发机构 (CA) 和安全套接字层 (SSL) 证书。这个专用存储通过允许管理员无缝添加新证书、修改现有证书以及删除不再需要的证书来简化证书管理。

以前，Secure Private Access 证书存储在 NetScaler® Console 的证书存储中。有了专用的 Secure Private Access 证书存储，在 NetScaler Console 中管理的证书将不再自动同步或可用于 Secure Private Access。管理员必须将必要的证书直接上传到 Secure Private Access 控制台。

Secure Private Access 中使用的证书在“证书”页面中分为两个选项卡。

- **服务器** - 包含证书列表，主要是与直接访问（无代理访问）操作相关的 SSL 服务器证书。
- **计算机身份验证** - 包含与管理从 Citrix Secure Access™ 客户端启动的计算机隧道相关的证书列表。当管理员登录 Citrix Secure Access 客户端时，会使用这些证书。

  计算机身份验证证书对于“始终开启”功能至关重要，它利用受信任的证书颁发机构 (CA) 颁发的设备证书。这些 CA 证书在“计算机身份验证”选项卡（**设置 > 证书存储**）中安全上传和管理，确保“始终开启”功能的无缝且强大的设备身份验证。

管理计算机身份验证证书

以下部分提供了有关管理计算机身份验证证书的更多信息。

添加证书

添加计算机身份验证证书的步骤。

1. 导航到 **设置 > 证书存储**。

   注意：

   我们建议您使用 **设置 > 证书存储** 下的 **基于计算机的身份验证** 选项，而不是 **设置 > 基于计算机的身份验证**。**设置 > 基于计算机的身份验证** 选项计划在即将推出的服务版本中移除。

2. 单击“**计算机身份验证**”选项卡，然后单击“**添加证书**”。
3. 在“**名称**”中，输入证书的名称。
4. 在“**证书文件**”中，浏览到本地驱动器并上传证书文件。

   - 支持根 CA 和中间 CA 的证书。
   - 要上传的证书必须采用 PEM 格式并包含整个链。证书必须从中间证书一直生成到根 CA。

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

5. 单击“**保存**”。

证书将添加到“**计算机身份验证**”选项卡中可用证书的列表中。

添加计算机身份验证证书(/en-us/citrix-secure-private-access/media/spa-cert-store-machine-authentication.png)

禁用证书

您可以通过在“**状态**”列中将切换开关滑动到“关”来禁用不再使用的证书。

删除证书

1. 单击删除图标以删除证书。

设置证书的优先级

如果同一台计算机使用多个证书，您可以通过使用“**优先级顺序**”列中的上下拖动图标来更改证书的优先级。

管理 SSL 证书

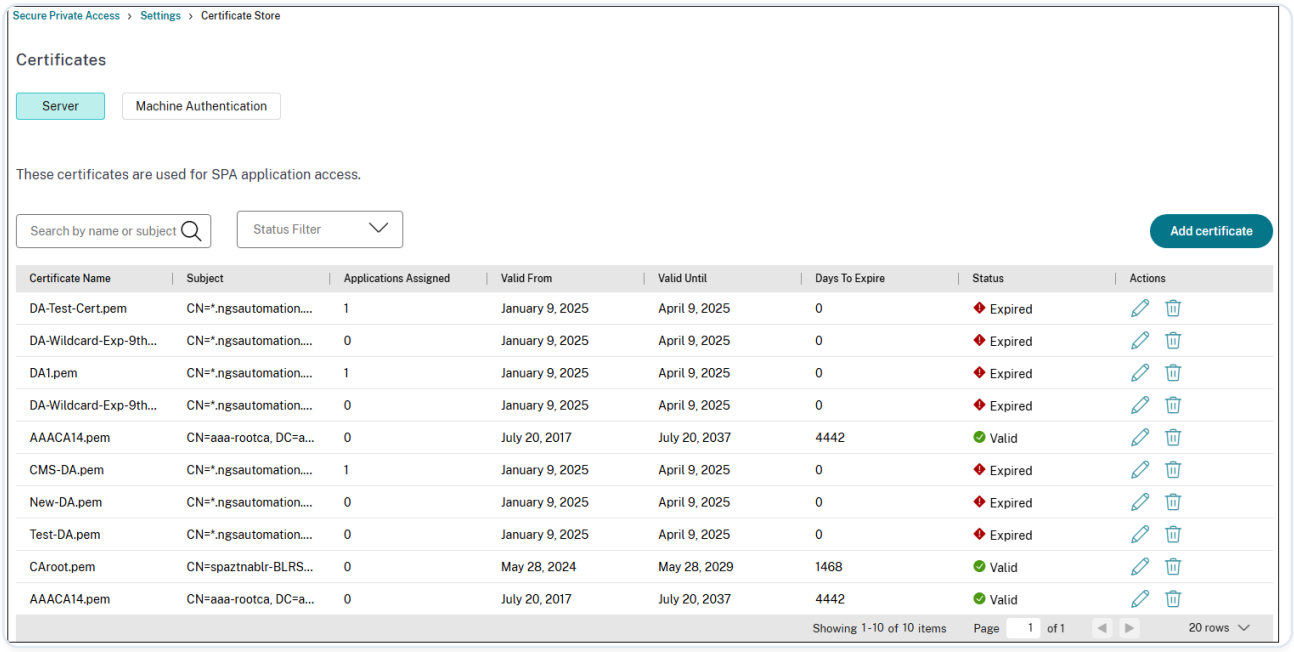
以下部分提供了有关管理 SSL 证书的更多信息。

添加证书

添加 SSL 证书的步骤。

1. 导航到 **设置 > 证书存储**。
2. 单击 **服务器** 选项卡。
3. 输入证书名称。
4. 在 **证书文件** 中，浏览到本地驱动器并上传证书文件。
   - 支持根 CA 和中间 CA 证书。
   - 要上传的证书必须采用 PEM 格式并包含整个链。证书必须从中间证书一直生成到根 CA。
5. **密码**（可选）- 适用于 PFX 证书。如果您有加密的 RSA 私钥，请键入用于加密私钥的 RSA 密码。
6. 单击 **保存**。

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



注意：

- 证书将添加到 **服务器** 选项卡下可用证书列表中。
- **已分配应用程序** 列显示已分配证书的应用程序数量。

搜索证书

您可以按证书名称或主题搜索 SSL 证书。您还可以根据证书状态搜索证书。

搜索 SSL 证书(/en-us/citrix-secure-private-access/media/spa-cert-store-server-search.png)

修改证书

修改 SSL 证书的步骤。

1. 单击证书旁边的编辑图标。
2. 在 **证书文件** 中，浏览到本地驱动器并上传修改后的证书文件。

   确保更新的证书适用于同一域或通配符域。否则，上传将失败。
3. 单击 **保存**。

删除证书

单击删除图标以删除证书。

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

外部通知

当客户帐户中的证书临近过期日期时（在过期前的 30 天窗口期内），系统会自动向特定的客户管理员发送电子邮件通知。

思杰安全访问™ 客户端

借助 Citrix Secure Private Access，您现在可以通过在计算机上运行的 Citrix Secure Access 客户端，使用本机浏览器或本机客户端应用程序访问所有私有应用程序，包括 TCP/UDP 和 HTTPS 应用程序。您现在可以消除对传统 VPN 解决方案的依赖，从而为远程用户提供对所有私有应用程序的访问。

适用于 Windows 的 Citrix Secure Access 客户端

有关安装适用于 Windows 的 Citrix Secure Access 客户端的详细信息，请参阅 安装适用于 Windows 的 Citrix Secure Access 客户端。

有关适用于 Windows 的 Citrix Secure Access 客户端的更多信息，请参阅 适用于 Windows 的 Citrix Secure Access。

适用于 macOS 的 Citrix Secure Access 客户端

有关安装适用于 macOS 的 Citrix Secure Access 客户端的详细信息，请参阅 安装适用于 macOS 的 Citrix Secure Access 客户端。

有关适用于 macOS 的 Citrix Secure Access 客户端的更多信息，请参阅 适用于 macOS 的 Citrix Secure Access。

适用于 iOS 的 Citrix Secure Access 客户端

有关设置适用于 iOS 的 Citrix Secure Access 客户端的详细信息，请参阅 设置适用于 iOS 的 Citrix Secure Access。

有关适用于 iOS 的 Citrix Secure Access 客户端的更多信息，请参阅 适用于 iOS 的 Citrix Secure Access。

适用于 Android 的 Citrix Secure Access 客户端

有关设置适用于 Android 的 Citrix Secure Access 客户端的详细信息，请参阅 设置适用于 Android 的 Citrix Secure Access。

有关适用于 Android 的 Citrix Secure Access 客户端的更多信息，请参阅 适用于 Android 的 Citrix Secure Access。

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

适用于 Linux 的 Citrix Secure Access 客户端

有关在 Linux 上安装 Citrix Secure Access 客户端的详细信息，请参阅 安装 Citrix Secure Access 客户端和 Citrix EPA 客户端。

有关适用于 Linux 的 Citrix Secure Access 客户端的更多信息，请参阅 适用于 Linux 的 Citrix Secure Access。

Web 和 SaaS 应用程序配置的最佳实践

已发布和未发布的应用程序的应用程序访问取决于 Secure Private Access 服务中配置的应用程序和访问策略。

Secure Private Access 中已发布和未发布应用程序的应用程序访问

- **访问已发布的 Web 应用程序和相关域：**
  - 当最终用户访问与已发布的 Web 应用程序关联的 FQDN 时，仅当为该用户明确配置了操作为 **允许** 或 **允许（带限制）** 的访问策略时，才允许访问。

    注意：

    建议不要让多个应用程序共享相同的应用程序 URL 域或相关域以进行精确匹配。如果多个应用程序共享相同的应用程序 URL 域或相关域，则根据精确的 FQDN 匹配和策略优先级提供访问。有关详细信息，请参阅访问策略匹配和优先级。
  - 如果没有访问策略与已发布的应用程序匹配，或者应用程序未与任何访问策略关联，则默认情况下拒绝访问该应用程序。有关访问策略的详细信息，请参阅自适应访问策略配置和管理。
- **访问未发布的内部 Web 应用程序和外部 Internet URL：**

  为了启用零信任，Secure Private Access 拒绝访问未与应用程序关联且未配置应用程序访问策略的内部 Web 应用程序或内网 URL。要允许特定用户访问，请确保为您的内网 Web 应用程序配置了访问策略。

  对于 Secure Private Access 中未配置为应用程序的任何 URL，流量将直接流向 Internet。
  - 在这种情况下，对内网 Web 应用程序 URL 域的访问将直接路由，因此访问被拒绝（除非用户已在内网中）。
  - 对于未发布的 Internet URL，如果启用，访问将基于为未经批准的应用程序配置的规则。默认情况下，Secure Private Access 允许此访问。

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

访问策略匹配和优先级

Secure Private Access 在匹配应用程序以进行访问时执行以下操作：

1. 将访问的域与应用程序 URL 的域或相关域进行精确匹配。
2. 如果找到配置了精确 FQDN 匹配的 Secure Private Access 应用程序，则 Secure Private Access 会评估为该应用程序配置的所有策略。
   - 策略按优先级顺序进行评估，直到用户上下文匹配。操作（允许/拒绝）将根据优先级顺序中第一个匹配的策略应用。
   - 如果没有策略匹配，则默认拒绝访问。
3. 如果未找到精确的 FQDN 匹配，则 Secure Private Access 会根据最长匹配（例如通配符匹配）来匹配域，以查找应用程序和相应的策略。

   示例 1：考虑以下应用程序和策略配置：

应用程序	应用程序 URL	相关域
内网	`https://app.intranet.local`	*.cdn.com
维基	`https://wiki.intranet.local`	*.intranet.local

策略名称	优先级	用户和关联应用程序
PolicyA	高	Eng-User5 (内网)
PolicyB	低	HR-User4 (维基)

   如果 `HR-User4` 访问 `app.intranet.local`，则会发生以下情况：

   a. Secure Private Access 会搜索所有策略，以查找与所访问域（在本例中为 `app.intranet.local`）的精确匹配项。
   b. Secure Private Access 找到 `PolicyA`，并检查条件是否匹配。
   c. 由于条件不匹配，Secure Private Access 在此处停止，并且不会继续检查通配符匹配项，即使 `PolicyB` 本来会匹配（因为 `app.intranet.local` 确实与 Wiki 应用程序的 `*.intranet.local` 相关域匹配）并授予访问权限。
   d. 因此，`HR-User4` 被拒绝访问 Wiki 应用程序。

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

示例 2：考虑以下应用程序和策略配置，其中在多个应用程序中使用相同的域：

应用程序	应用程序 URL	相关域
App1	xyz.com	app.intranet.local
App2	app.intranet.local	-

策略名称	优先级	用户和关联的应用程序
PolicyA	高	Eng-User5 (应用1)
PolicyB	低	HR-用户7 (应用2)

当用户 `Eng-User5` 访问 `app.intranet.local` 时，App1 和 App2 都将根据精确的 FQDN 匹配进行匹配，因此 `Eng-User5` 用户通过 `PolicyA` 获得访问权限。

但是，如果 App1 将 `*.intranet.local` 作为相关域，那么对 `Eng-User5` 的访问将被拒绝，因为 `app.intranet.local` 将精确匹配 `PolicyB`，而用户 `Eng-User5` 没有访问权限。

应用程序配置最佳实践

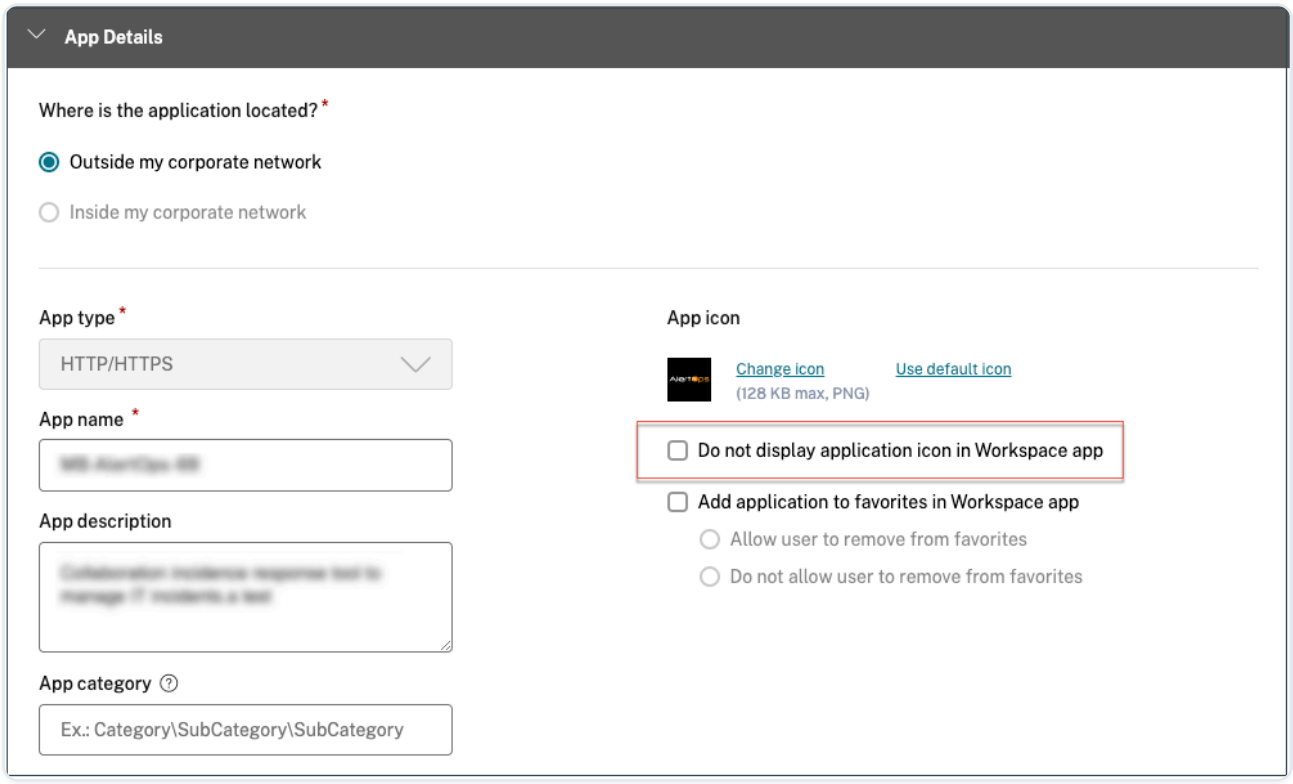
以下部分提供了有关应用程序配置最佳实践的更多信息。

IdP 域必须拥有自己的应用程序

建议不要将 IdP 域作为相关域添加到您的内部网应用程序配置中，而是建议执行以下操作：

- 为所有 IdP 域创建单独的应用程序。
- 创建策略以允许所有需要访问 IdP 身份验证页面的用户访问，并将该策略设置为最高优先级。
- 从应用程序配置中隐藏此应用程序（通过选择“**不向用户显示应用程序图标**”选项），以使其不会在商店中列出。有关信息，请参阅 配置应用程序详细信息。

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



注意：

此应用程序配置仅启用对 IdP 身份验证页面的访问。对单个应用程序的进一步访问仍取决于各个应用程序配置及其各自的访问策略。

示例配置：

1. 将所有常见的 FQDN 配置到各自的应用程序中，并在适用时将其分组。

   例如，如果您有几个应用程序使用 Azure AD 作为 IdP，并且您必须配置 `login.microsoftonline.com` 和其他相关域 (`*.msauth.net`)，请执行以下操作：

   - 创建一个通用应用程序，其中 `https://login.microsoftonline.com` 作为应用程序 URL，`*.login.microsoftonline.com` 和 `*.msauth.net` 作为相关域。

2. 在配置应用程序时，选择**不向用户显示应用程序图标**选项。有关详细信息，请参阅配置应用程序详细信息。
3. 为通用应用程序创建访问策略，并为所有用户启用访问。有关详细信息，请参阅配置访问策略。
4. 为访问策略分配最高优先级。有关详细信息，请参阅优先级顺序。
5. 验证诊断日志，确认 FQDN 与应用程序匹配，并且策略按预期执行。

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

相同的相关域不得属于多个应用程序

相关域必须是应用程序独有的。冲突的配置可能会导致应用程序访问问题。如果多个应用程序配置了相同的 FQDN 或通配符 FQDN 的某种变体，则可能会遇到以下问题：

- 网站停止加载或可能显示空白页。
- 访问 URL 时可能会出现**访问被阻止**页面。
- 登录页面可能无法加载。

因此，我们建议在单个应用程序中配置唯一的关联域。

不正确的配置示例：

- **示例：跨多个应用程序的重复相关域**

  假设您有两个应用程序，两者都需要访问 Okta (example.okta.com)：

应用程序	应用程序 URL 域	相关域
App1	`https://code.example.net`	example.okta.com
App2	`https://info.example.net`	example.okta.com

策略名称	优先级	用户和关联的应用程序
拒绝 App1 访问 HR	高	用户组 `HR` 适用于 `App1`
授予“所有人”访问 App1 的权限	中	允许用户组“所有人”访问 App1
授予“所有人”访问 App2 的权限	低	允许用户组“所有人”访问 App2

  配置问题： 尽管目的是让所有用户访问 App2，但用户组 HR 无法访问 App2。用户组 HR 被重定向到 Okta，但由于第一个拒绝访问 App1 的策略而被阻止（App1 也具有与 App2 相同的相关域 `example.okta.com`）。

  这种情况对于 Okta 等身份提供商很常见，但也可能发生在其他具有共同相关域的紧密集成应用程序中。有关策略匹配和优先级的详细信息，请参阅访问策略匹配和优先级。

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

上述配置的建议：

a. 从所有应用程序中删除 example.okta.com 作为相关域。

b. 专门为 Okta 创建一个新应用程序（其应用程序 URL 为 `https://example.okta.com`，相关域为 `*.okta.com`）。

c. 从商店中隐藏此应用程序。

d. 为策略分配最高优先级以消除任何冲突。

最佳实践：

- 一个应用程序的相关域不得与另一个应用程序的相关域重叠。
- 如果发生这种情况，必须创建一个新的已发布应用程序来覆盖共享的相关域，然后相应地设置访问权限。
- 管理员必须评估此共享相关域是否必须作为实际应用程序出现在商店中。
- 如果应用程序不应出现在商店中，则在发布应用程序时，选择**不向用户显示应用程序图标**选项以将其从商店中隐藏。

解决相同相关域导致的冲突

在应用程序相关域与另一个应用程序域重叠的场景中，管理员可以根据特定要求，通过连接器设备将这些应用程序路由到外部或内部。 Secure Private Access 控制台中的路由表（**设置 > 应用程序域**）提供了所有应用程序所有已配置域的全面列表。此表显示了每个域的关键信息，包括路由类型。管理员可以通过单击相应域条目旁边的编辑图标轻松修改路由类型。

主路由表显示任何域的以下信息：

- **FQDN/IP：** 期望配置流量路由类型的 FQDN 或 IP 地址。
- **类型：** 应用程序类型。添加应用程序时选择的**内部**、**内部 – 绕过代理**或**外部**。
  - **内部** - 应用程序是外部的，但流量必须通过连接器设备流向外部网络。
  - **内部 – 绕过代理** - 域流量通过 Citrix Cloud Connector™ 路由，绕过在连接器设备上配置的客户 Web 代理。
  - **外部** – 流量直接流向互联网。

> **重要：**
>
> 如果存在冲突，则表中相应行会显示一个警报图标。要解决冲突，管理员应单击与该条目关联的三角形图标并更改应用程序类型。

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

- **资源位置：** 内部类型路由的资源位置。如果未分配资源位置，则在相应应用程序的“资源位置”列中显示一个三角形图标。将鼠标悬停在图标上时，将显示以下消息。

  缺少资源位置。确保此 FQDN 关联了资源位置。

- **状态：** “状态”列中的切换开关可用于禁用路由条目的路由，而无需删除应用程序。当切换开关关闭时，路由条目不生效。此外，如果存在精确匹配的 FQDN，管理员可以选择启用或禁用路由。
- **备注：** 显示备注（如果有）。
- **操作：** 编辑图标用于添加资源位置或更改路由条目类型。删除图标用于删除路由。

注意：

应用程序域表的迷你版本可用于在应用程序配置期间做出路由决策。迷你路由表可在 Citrix Secure Private Access™ 服务管理控制台的“应用程序连接”部分中找到。

深层链接 URL

对于深层链接 URL，必须将内部网应用程序 URL 域添加为相关域：

示例：

内部网应用程序的 URL 配置为 `https://example.okta.com/deep-link-app-1` 作为主应用程序 URL 域，相关域具有内部网应用程序 URL 域，即 `*.issues.example.net`。

在这种情况下，单独创建一个 URL 为 `https://example.okta.com` 的 IdP 应用程序，然后将相关域设置为 `*.example.okta.com`。

应用程序访问最终用户体验说明

Citrix Secure Private Access™ 应用程序可以通过以下方式访问：

- **通过 Citrix Secure Access™ 客户端：**
  - 访问 Web/SaaS 应用程序：登录 Citrix Secure Access 客户端后，最终用户可以使用其本机浏览器（例如 Chrome）访问 Web/SaaS 应用程序。
  - 访问 TCP/UDP 应用程序：登录 Citrix Secure Access 客户端后，最终用户可以通过客户端应用程序（例如远程桌面协议 (RDP)）访问 TCP/UDP 应用程序。
- **无代理访问：** 允许用户访问企业 Web 应用程序，而无需客户端。最终用户无需在其设备上安装专用客户端即可访问企业 Web 应用程序。最终用户只需在其本机浏览器中输入应用程序 URL 即可。

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

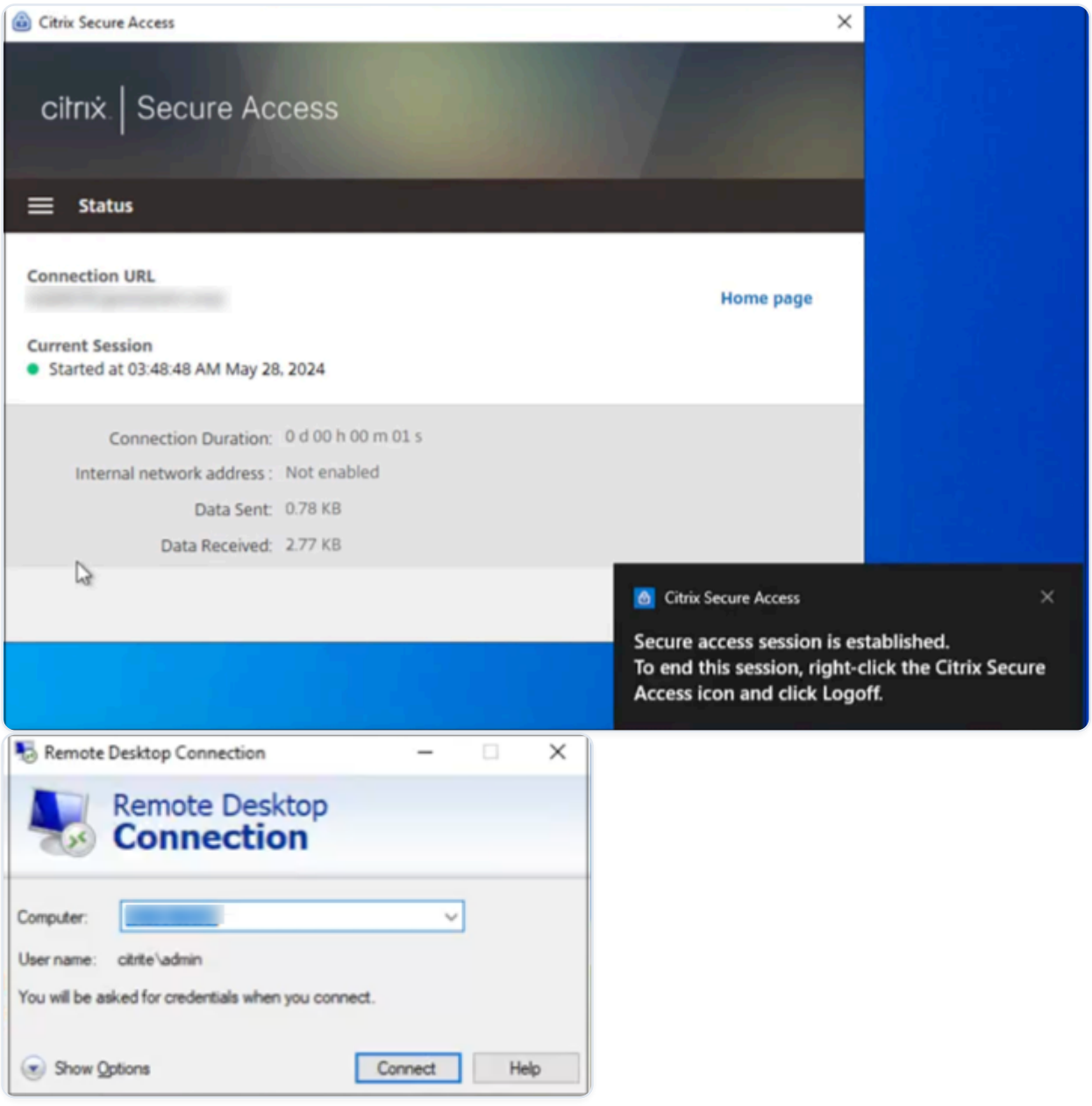
通过 Citrix Secure Access 客户端访问 Web 应用程序

1. 登录 Citrix Secure Access 客户端。
2. 建立安全访问会话后，打开本机浏览器（例如 Chrome）。
3. 在浏览器中，输入您要访问的企业 Web 应用程序的 URL。

通过 Citrix Secure Access 客户端访问 TCP/UDP 应用程序

如果配置了 RDP，最终用户必须执行以下步骤才能访问 TCP/UDP 应用程序。

1. 登录 Citrix Secure Access 客户端。
2. 建立安全访问会话后，启动远程桌面连接。



a. 按 **Windows** 键，键入 **远程桌面连接**，然后按 **Enter**。

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

b. 输入您要连接的计算机的 IP 地址或主机名。

c. 单击 **连接**。系统可能会提示您输入凭据。

d. 输入远程计算机的用户名和密码，然后单击 **确定**。

现在已建立远程桌面连接，最终用户可以与远程计算机进行交互。

有关 Citrix Secure Access 客户端的更多信息，请参阅 Citrix Secure Access 客户端。

用于安全专用访问的连接器设备

连接器设备是托管在您的虚拟机管理程序中的 Citrix 组件。它充当 Citrix Cloud™ 与您的资源位置之间的通信通道，无需复杂的网络或基础架构配置即可实现云管理。连接器设备使您能够管理并专注于为用户提供价值的资源。

所有连接都使用标准 HTTPS 端口 (443) 和 TCP 协议从连接器设备建立到云。不接受任何传入连接。允许 TCP 端口 443 和以下 FQDN 出站：

- *.nssvc.net
- *.netscalermgmt.net
- *.citrixworkspacesapi.net
- *.citrixnetworkapi.net
- *.citrix.com
- *.servicebus.windows.net
- *.adm.cloud.com

使用连接器设备配置安全专用访问

1. 在您的资源位置中安装两个或更多连接器设备。

   有关设置连接器设备的更多信息，请参阅适用于云服务的连接器设备。

2. 要配置安全专用访问以使用 KCD 连接到本地 Web 应用程序，请完成以下步骤来配置 KCD：

   a. 将您的连接器设备加入到 Active Directory 域。

      加入 Active Directory 林使您能够在配置 Secure Private Access 时使用 Kerberos 约束委派 (KCD)，但这并不能使身份请求或身份验证使用 Connector Appliance。

      - 使用 Connector Appliance 控制台中提供的 IP 地址，在浏览器中连接到 Connector Appliance 管理网页。

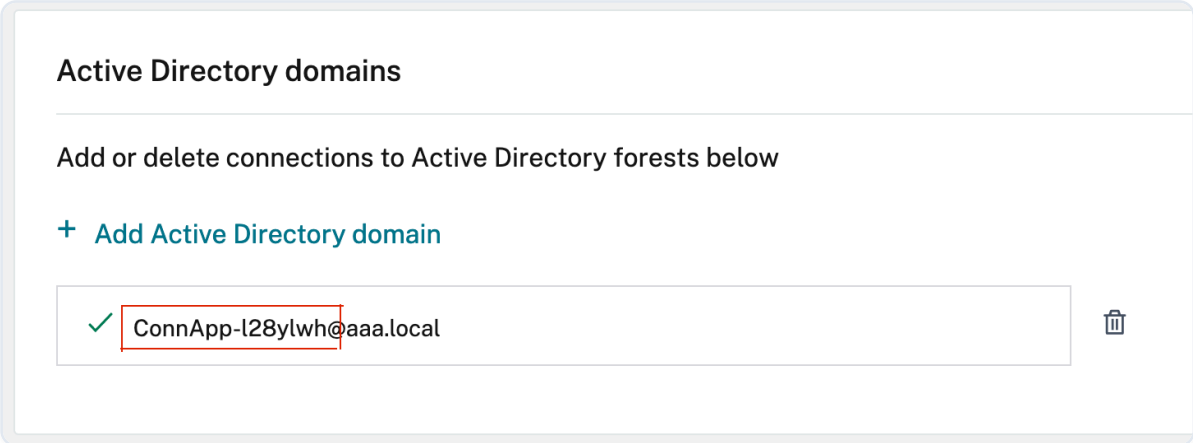
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 在 **Active Directory 域**部分，单击 **+ 添加 Active Directory** 域。

  如果您的管理页面中没有 **Active Directory 域**部分，请联系 Citrix® 请求加入预览版。
- 在 **域名**字段中输入域名。单击**添加**。
- Connector Appliance 检查域。如果检查成功，将打开**加入 Active Directory** 对话框。
- 输入具有此域加入权限的 Active Directory 用户的用户名和密码。
- Connector Appliance 会建议一个计算机名称。您可以选择覆盖建议的名称，并提供您自己的计算机名称，长度最多为 15 个字符。记下计算机帐户名称。

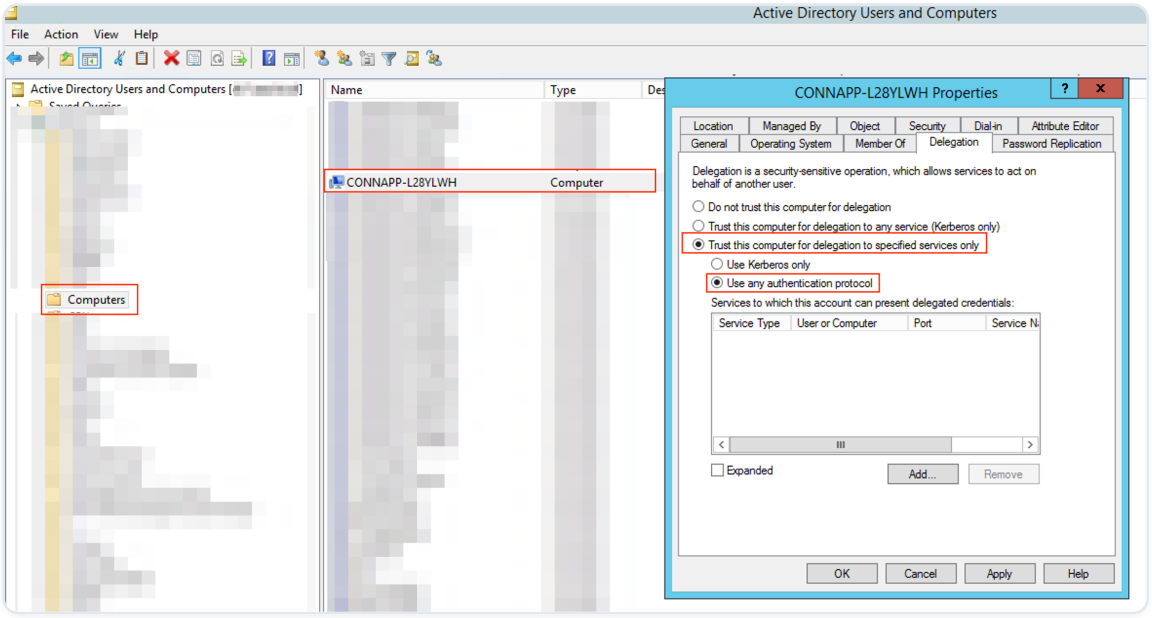
  当 Connector Appliance 加入 Active Directory 域时，此计算机名称将在其中创建。
- 单击**加入**。

b. 为没有负载均衡器的 Web 服务器配置 Kerberos 约束委派。

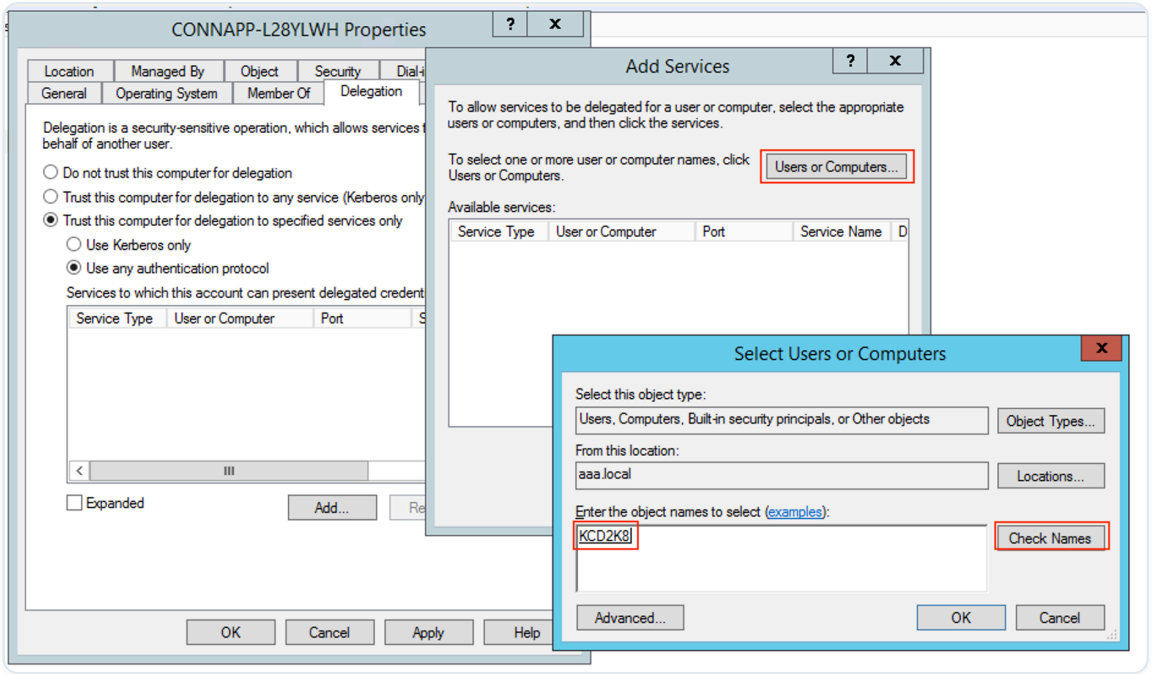


- 识别连接器设备的计算机名称。您可以从托管位置或直接从连接器 UI 获取此名称。
- 在您的 Active Directory 控制器上，查找连接器设备计算机。
- 转到 Connector Appliance 计算机帐户的属性，然后导航到**委派**选项卡。
- 选择**仅信任此计算机以委派给指定服务。**，然后选择**使用任何身份验证协议。**

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

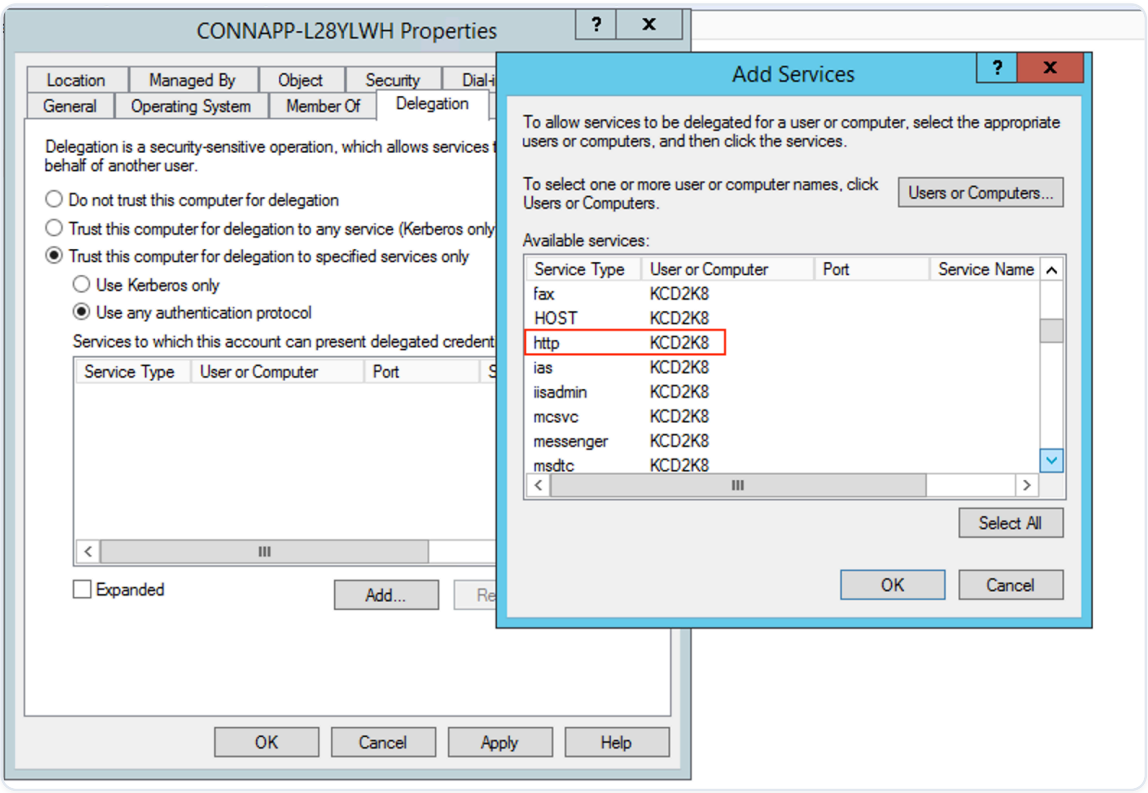


- 单击**添加**。
- 单击**用户或计算机**。
- 输入目标 Web 服务器计算机名称，然后单击**检查名称**。 在上图中，**KCD2K8** 是 Web 服务器。



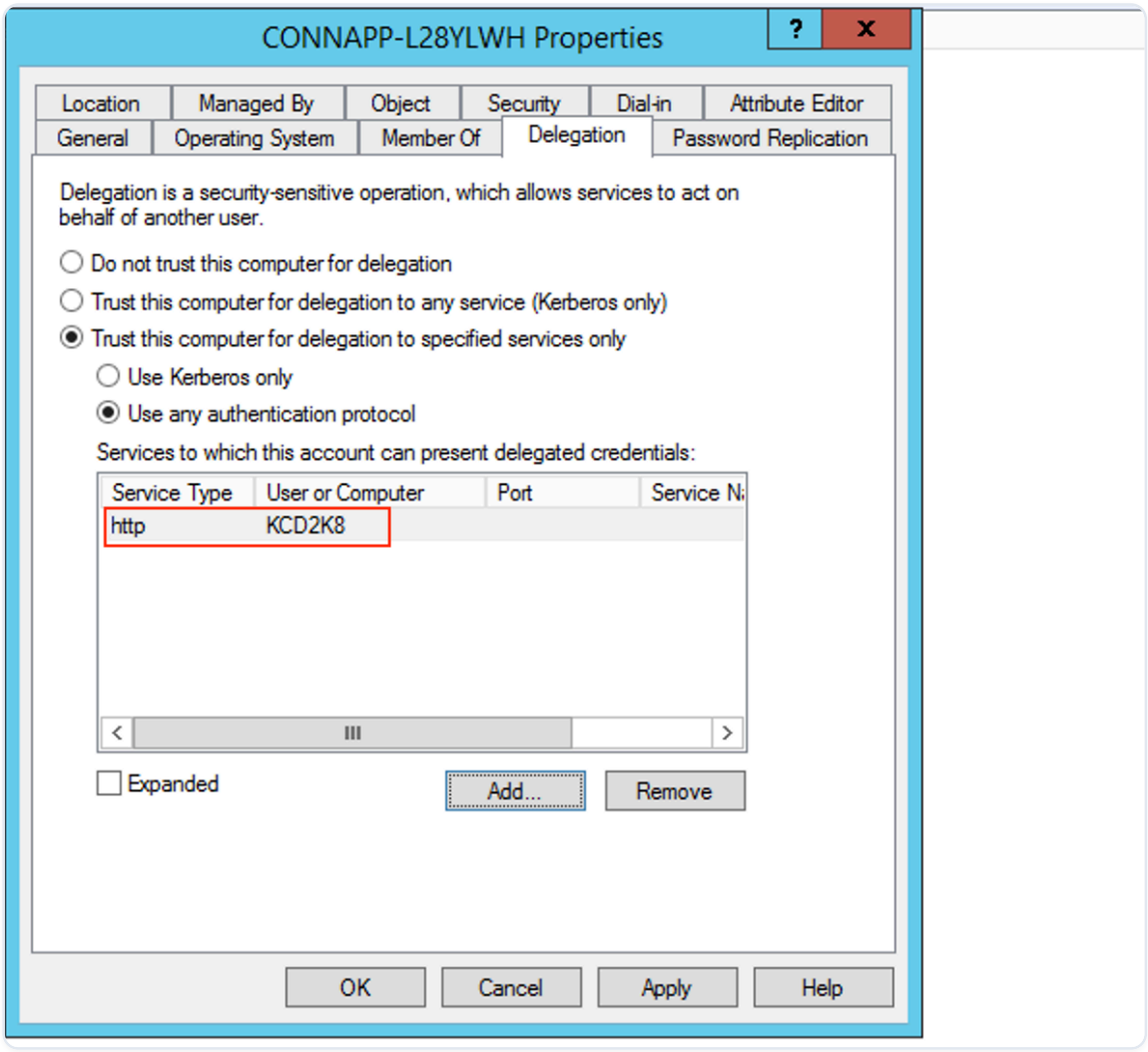
- 单击**确定**。
- 选择服务类型 **http**。

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



- 单击**确定**。
- 单击**应用**，然后单击**确定**。

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



至此，为 Web 服务器添加委派的过程已完成。

c. 为负载均衡器后面的 Web 服务器配置 Kerberos 约束委派 (KCD)。

- 使用以下 `setspn` 命令将负载均衡器 SPN 添加到服务帐户。 `setspn -S HTTP/<web_server_fqdn> <service_account>`

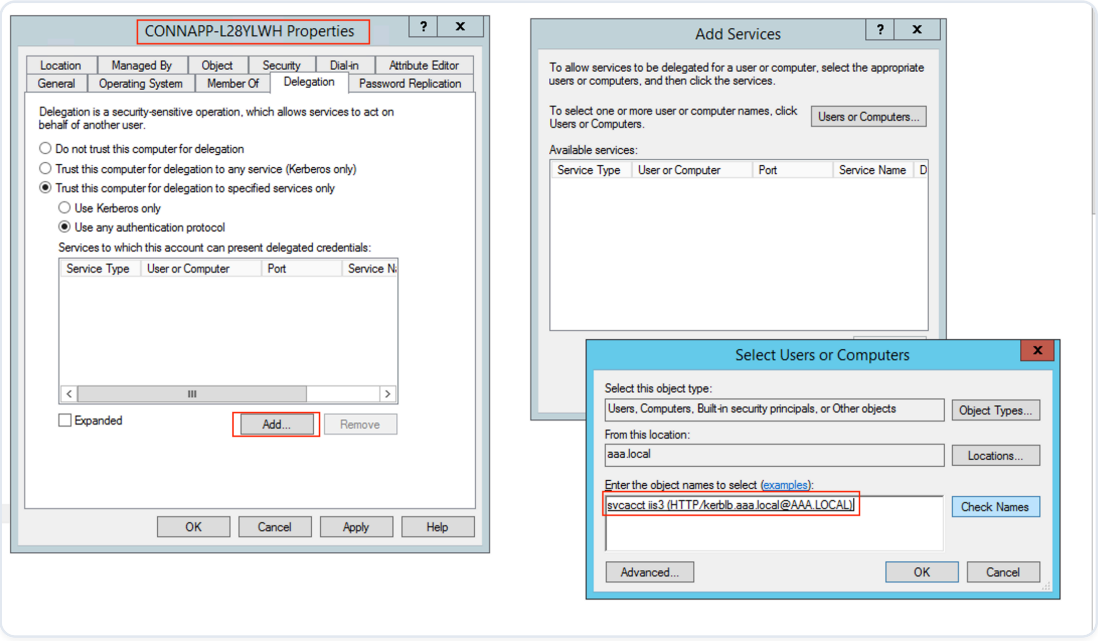


- 使用以下命令确认服务帐户的 SPN。 `setspn -l <service_account>`

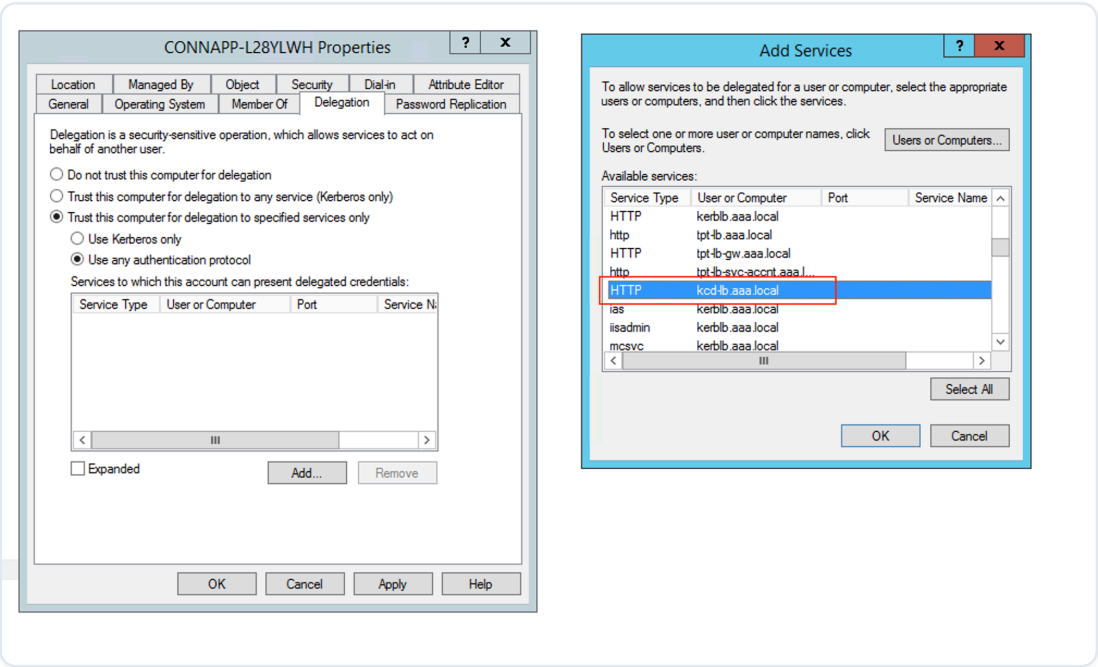


© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 为连接器设备计算机帐户创建委派。
  - 按照步骤*为 Web 服务器配置 Kerberos 约束委派*（不带负载均衡器），以识别 CA 计算机并导航到委派 UI。
  - 在选择**用户和计算机**中，选择服务帐户（例如，aaa\svc_iis3）。

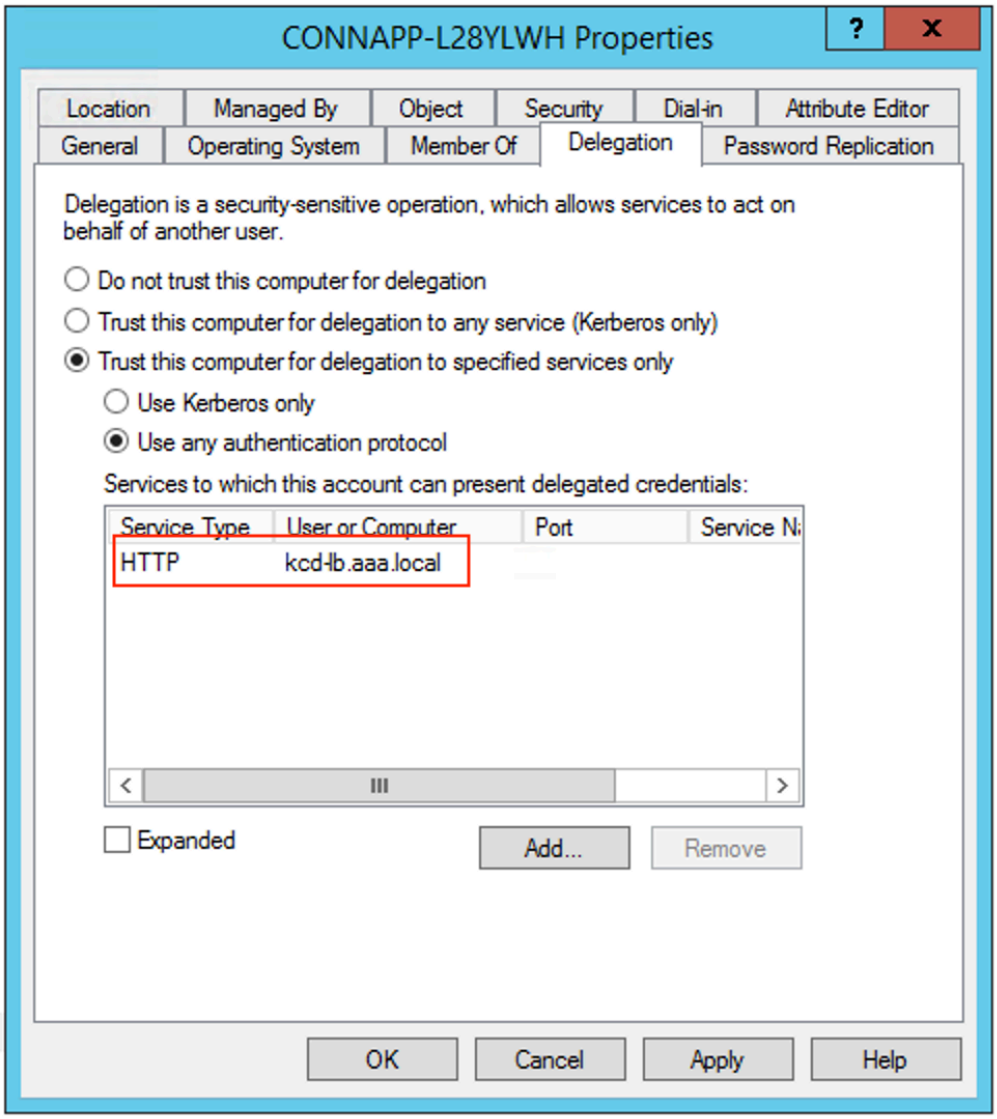


  - 在服务中，选择条目**ServiceType: HTTP**和用户或计算机：Web 服务器（例如，`kcd-lb.aaa.local`）



  - 单击**确定**。
  - 单击**应用**，然后单击**确定**。

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



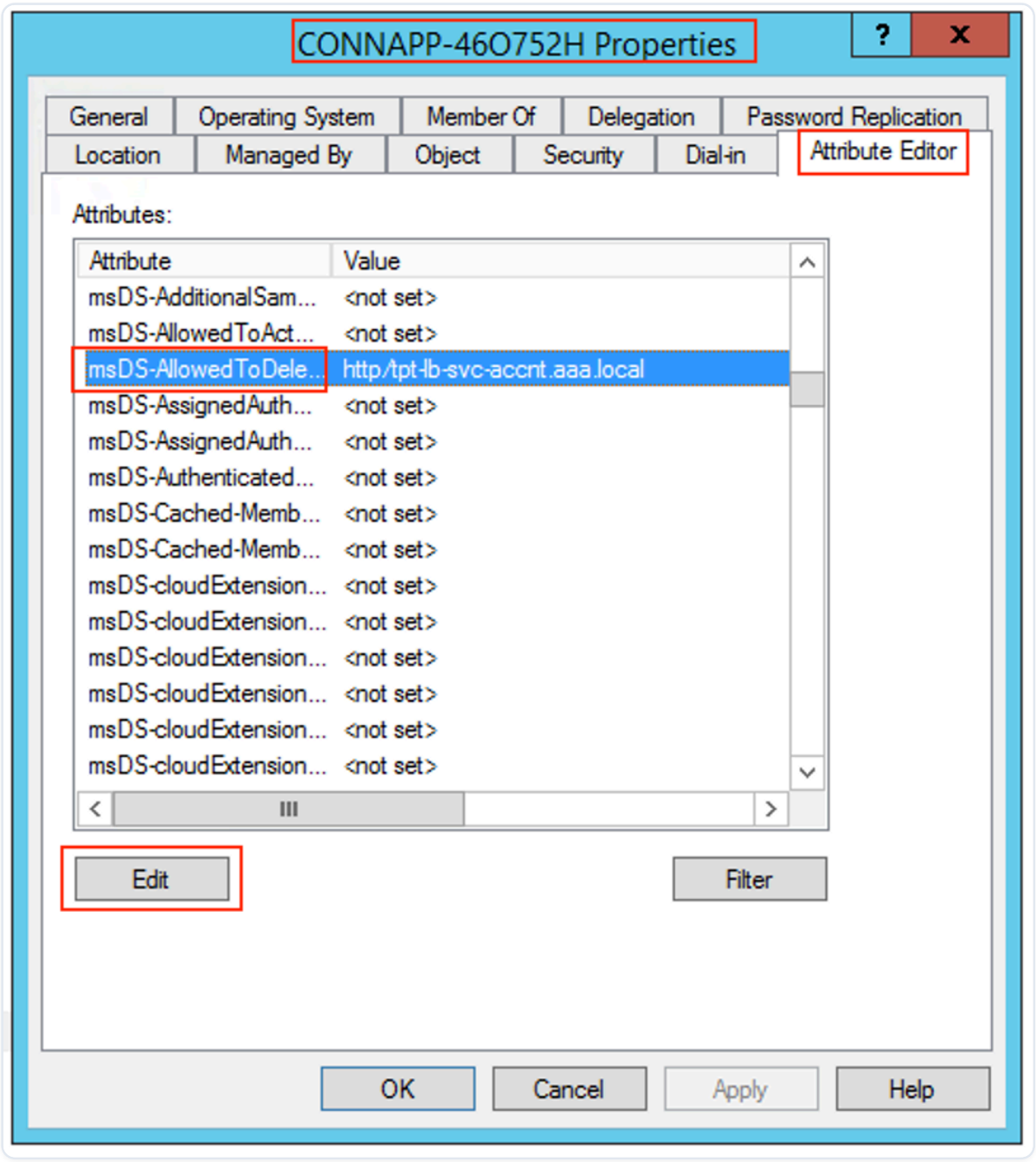
d. 为组托管服务帐户配置 Kerberos 约束委派 (KCD)。

- 如果尚未完成，请将 SPN 添加到组托管服务帐户。 `setspn -S HTTP/<web_server_fqdn> <group_manged_service_account>`
- 使用以下命令确认 SPN。 `setspn -l <group_manged_service_account>`

由于在为计算机帐户添加委派条目时，组托管服务帐户无法在 `Users and Computers` 搜索中显示，因此您无法使用常规方法为计算机帐户添加委派。因此，您可以通过属性编辑器将此 SPN 作为委派条目添加到 CA 计算机帐户。

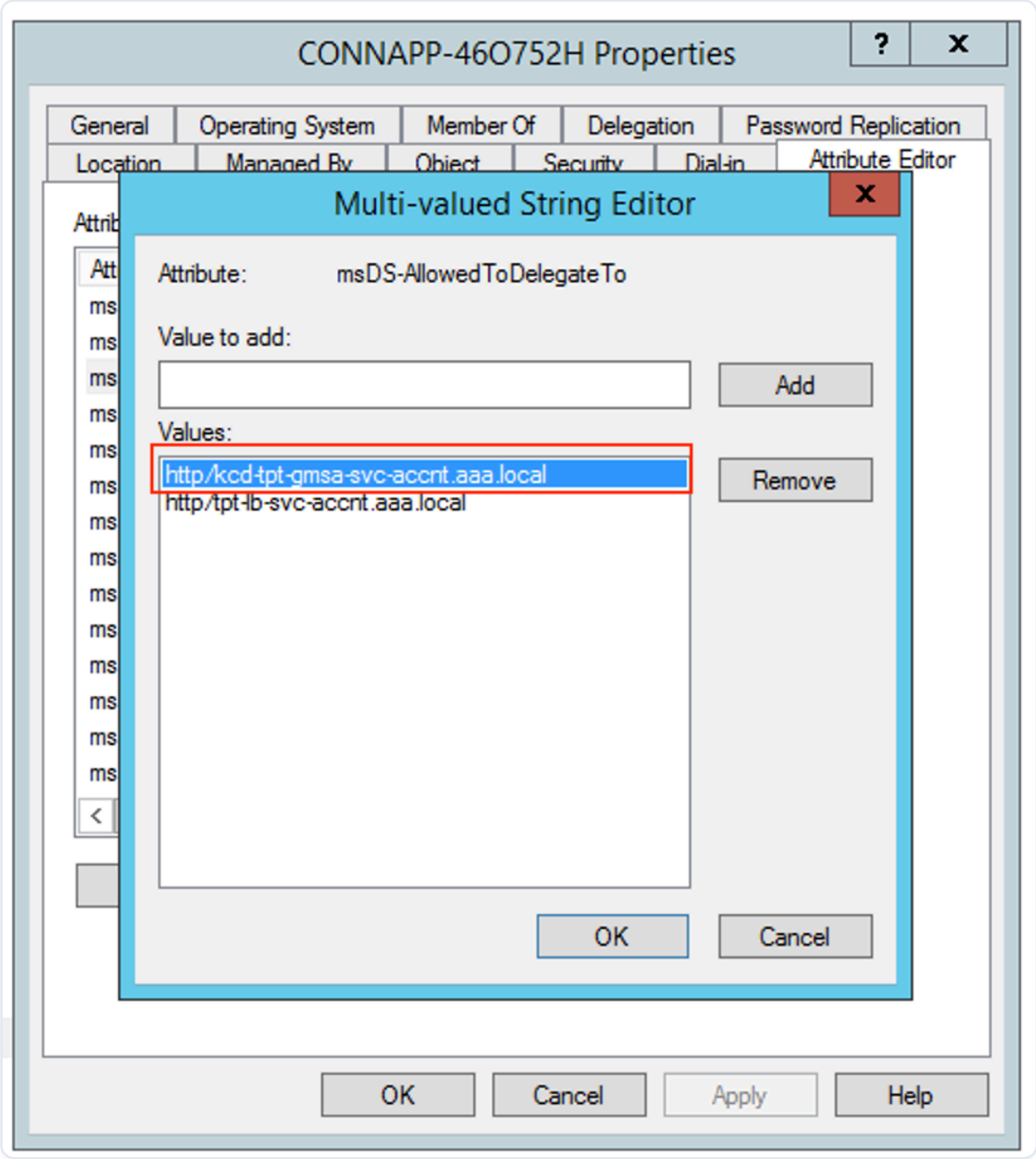
- 在连接器设备计算机属性中，导航到**属性编辑器**选项卡，并查找 `msDA-AllowedToDeleteTo` 属性。
- 编辑 `msDA-AllowedToDeleteTo attribute`，然后添加 SPN。

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



)

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



)

e. 从 Citrix Gateway 连接器™ 迁移到 Citrix Connector 设备。

- 由于在配置网关连接器时已将 SPN 设置为服务帐户，因此如果未配置新的 Kerberos 应用程序，则无需为服务帐户添加任何其他 SPN。您可以通过以下命令查看为服务帐户分配的所有 SPN 列表，并将其指定为 CA 计算机帐户的委派条目。

```
setspn -l <service_account>
```

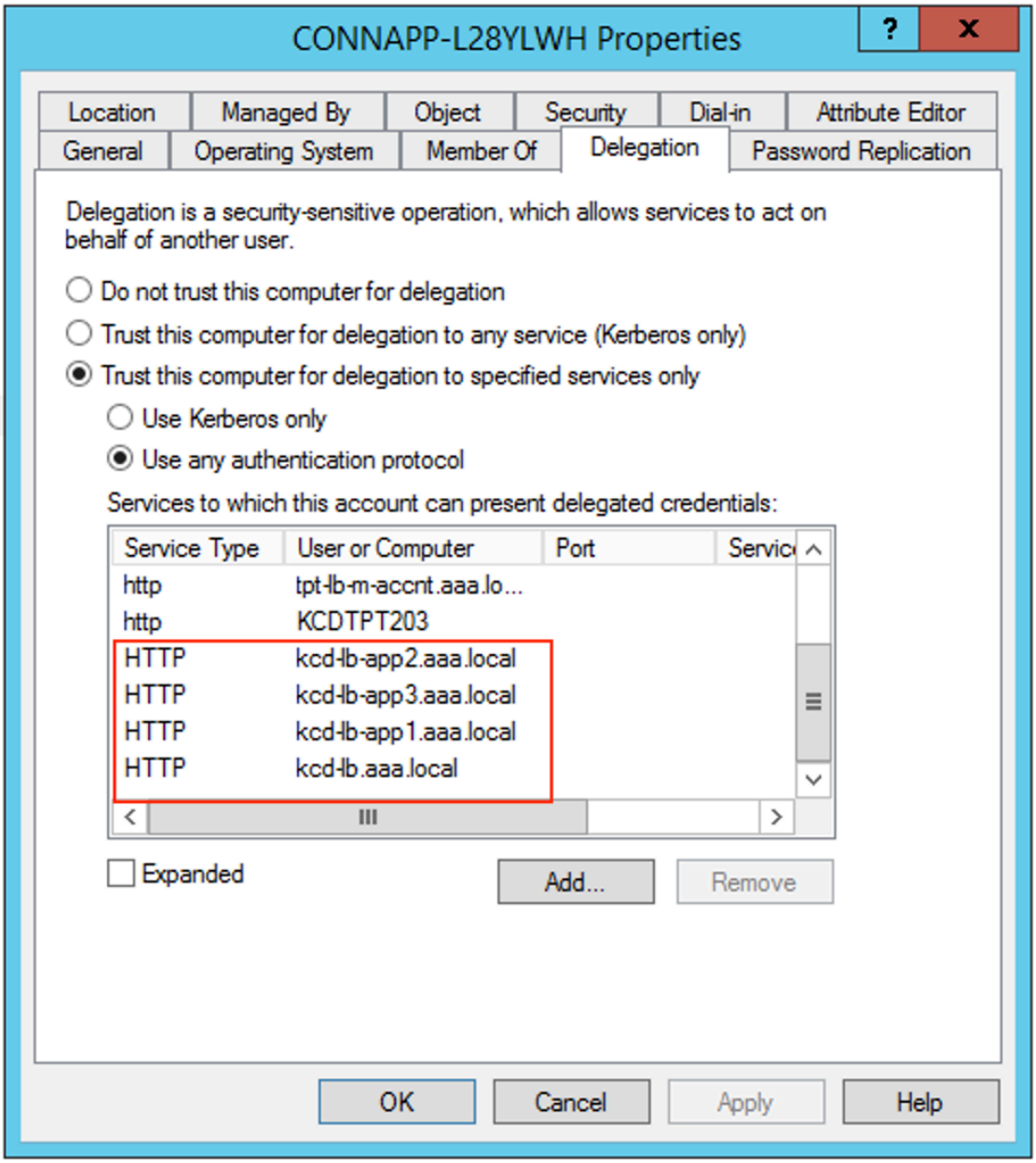
© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
C:\Windows\system32>setspn -l aaa\svc_iis3
Registered ServicePrincipalNames for CN=svcacct iis3,OU=Users,OU=KCD,DC=aaa,DC=l
ocal:
        HTTP/kcd-lb-app3.aaa.local
        HTTP/kcd-lb-app2.aaa.local
        HTTP/kcd-lb-app1.aaa.local
        HTTP/kcd-lb.aaa.local
        HTTP/kerblb.aaa.local
        host/kerblb.aaa.local

C:\Windows\system32>_
```

在此示例中，SPN (`kcd-lb.aaa.local, kcd-lb-app1.aaa.local, kcd-lb-app2.aaa.local, kcd-lb-app3.aaa.local`) 已为 KCD 配置。

- 将所需的 SPN 作为委派条目添加到连接器设备计算机帐户。有关详细信息，请参阅步骤*为连接器设备计算机帐户创建委派*。



在此示例中，所需的 SPN 已作为委派条目添加到 CA 计算机帐户。

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

注意： 在配置网关连接器时，这些 SPN 已作为委派条目添加到服务帐户。由于您不再使用服务帐户委派，因此可以从服务帐户的“**委派**”选项卡中删除这些条目。

f. 请遵循 Citrix Secure Private Access™ 文档来设置 Citrix Secure Private Access 服务。在设置过程中，Citrix Cloud 会识别您的 Connector 设备的存在，并使用它们连接到您的资源位置。

- 思杰安全私有访问入门
- 配置思杰安全私有访问
- 适用于云服务的 Connector 设备
- 互联网连接要求。
- 支持企业 Web 应用程序(/zh-cn/citrix-secure-private-access/service/add-and-manage-apps/support-web-apps.html)

验证您的 Kerberos 配置

如果您使用 Kerberos 进行单点登录，您可以从 **Connector Appliance 管理页面**验证 Active Directory 控制器上的配置是否正确。**Kerberos 验证**功能使您能够验证 Kerberos 仅域模式配置或 Kerberos 约束委派 (KCD) 配置。

1. 转到 **Connector Appliance 管理页面**。
   a. 从您的虚拟机管理程序中的 Connector Appliance 控制台，将 IP 地址复制到浏览器地址栏。
   b. 输入您注册 Connector Appliance 时设置的密码。
2. 从右上角的“管理”菜单中，选择**Kerberos 验证**。
3. 在**Kerberos 验证**对话框中，选择**Kerberos 验证模式**。
4. 指定或选择**Active Directory 域**。
   - 如果您正在验证 Kerberos 仅域模式配置，则可以指定任何 Active Directory 域。
   - 如果您正在验证 Kerberos 约束委派配置，则必须从已加入林中的域列表中进行选择。
5. 指定**服务 FQDN**。默认服务名称假定为 `http`。如果您指定“computer.example.com”，则这被视为与 `http/computer.example.com` 相同。
6. 指定**用户名**。
7. 如果您正在验证 Kerberos 仅域模式配置，请为该用户名指定**密码**。
8. 单击**测试 Kerberos**。

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

如果 Kerberos 配置正确，您会看到消息 `Successfully validated Kerberos setup`。如果 Kerberos 配置不正确，您会看到一条错误消息，其中提供了有关验证失败的信息。

规模和大小注意事项

本文详细介绍了用于确定单个连接器设备在一个资源位置的并发 TCP 连接限制和并发 Web 应用请求限制的指导。

Web 和 SaaS 应用程序

连接器设备虚拟机的最低推荐大小为 2 个 vCPU 和 4 GB RAM。为了实现高可用性和弹性，建议部署两个连接器设备。

部署指南：2 个 vCPU、4 GB 内存和 10 Gbps 网卡大小的连接器设备可支持以下功能：

- 每秒最多 500 个 Web 应用请求（安全浏览）。
- 数据传输吞吐率高达 1 Gbps。

这些数字是在 90% CPU 利用率和 80% 内存使用率下得出的。

TCP 应用程序

连接器设备虚拟机的最低推荐大小为 2 个 vCPU 和 4 GB RAM。

部署指南：2 个 vCPU、4 GB 内存和 10 Gbps 网卡大小的连接器设备可支持以下功能：

- 最多 50,000 个并发 TCP 连接。
- 数据传输吞吐率高达 1 Gbps。

这些数字是在 90% CPU 利用率和 80% 内存使用率下得出的。

混合流量（Web、SaaS、TCP）

部署指南：一个具有 2 个 vCPU 和 4 GB 内存的连接器设备可以支持以下功能：

- 每秒最多 300 个 Web 应用程序请求（安全浏览）。
- 最多 10,000 个并发 TCP 连接。
- 总体数据传输吞吐率高达 1 Gbps。

这些数字是在 CPU 利用率达到 90% 和内存使用率达到 80% 的情况下得出的。

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

重要提示：

为了管理超出每秒 Web 应用程序请求（安全浏览）、并发 TCP 连接或吞吐量建议限制的流量需求，必须通过添加更多连接器设备来横向扩展连接器设备。

连接器通知

当连接器在一小时采样期内 CPU 利用率超过 80% 时，它会生成通知。有关更多信息，请参阅 连接器通知。

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

自适应访问策略配置和管理

在当今瞬息万变的形势下，应用程序安全对任何企业都至关重要。制定上下文感知的安全决策，然后启用对应用程序的访问，可以降低相关风险，同时为用户提供访问权限。

Citrix Secure Private Access™ 服务的自适应访问功能提供了一种全面的零信任访问方法，可为应用程序提供安全访问。自适应访问使管理员能够根据上下文为用户提供对应用程序的精细级别访问。这里的“上下文”一词指：

- 用户和组（用户和用户组）
- 设备（桌面或移动设备）
- 位置（地理位置或网络位置）
- 设备态势（设备态势检查）

自适应访问功能将自适应策略应用于正在访问的应用程序。这些策略根据上下文确定风险，并做出动态访问决策，以授予或拒绝访问企业 Web、SaaS、TCP 和 UDP 应用程序。

工作原理

为了授予或拒绝访问应用程序，管理员根据用户、用户组、用户访问应用程序的设备以及用户访问应用程序的位置（国家或网络位置）创建策略。

自适应访问策略在以下场景中进行评估：

- 在 Secure Private Access 服务中枚举 Web、SaaS、TCP 或 UDP 应用程序期间 – 如果此用户被拒绝访问应用程序，则该用户无法在商店中看到此应用程序。
- 启动应用程序时 – 在您枚举应用程序后，如果自适应策略更改为拒绝访问，即使应用程序之前已被枚举，用户也无法启动该应用程序。

创建包含多个规则的访问策略

您可以在单个策略中创建多个访问规则，并为不同的用户或用户组配置不同的访问条件。这些规则可以分别应用于 HTTP/HTTPS 和 TCP/UDP 应用程序，所有这些都在一个策略中完成。

访问限制必须通过 Google Admin console 配置，而不是在 Secure Private Access 界面中配置。

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

规则在 **Google Admin console > 规则** 中配置。这些规则是与 DLP 相关的高级设置，例如添加水印、阻止下载包含社会安全号码的文件以及 URL 过滤。

有关在 Google Admin console 中为 Google Chrome 创建策略和规则的详细信息，请参阅以下主题：

- 为 Chrome Enterprise 设置 Chrome Enterprise 连接器策略
- 数据保护规则

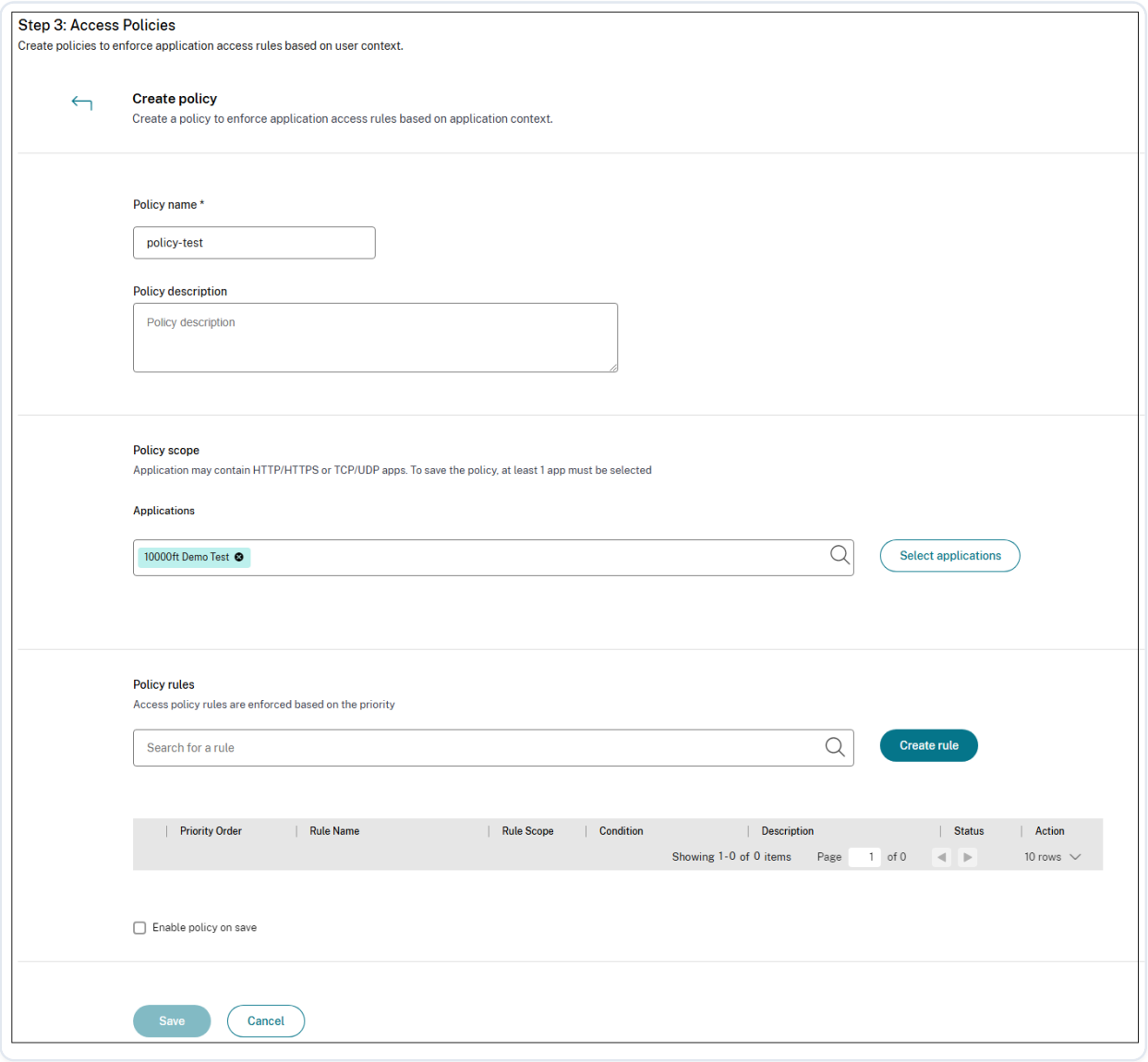
先决条件

确保您已为用户配置应用程序。有关详细信息，请参阅 为用户添加应用程序。

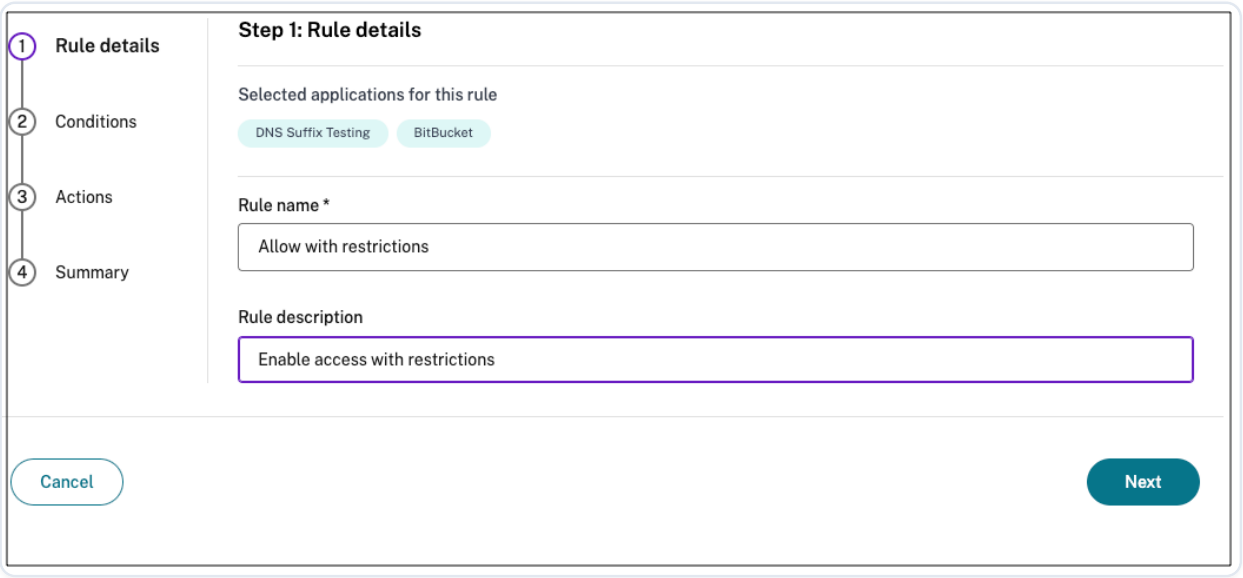
创建访问策略的步骤：

1. 打开 **访问策略** 页面，然后单击 **创建策略**。
2. 输入策略名称和策略描述。
3. 在 **应用程序** 中，选择必须强制执行此策略的应用程序或应用程序集。
4. 单击 **创建规则** 为策略创建规则。

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

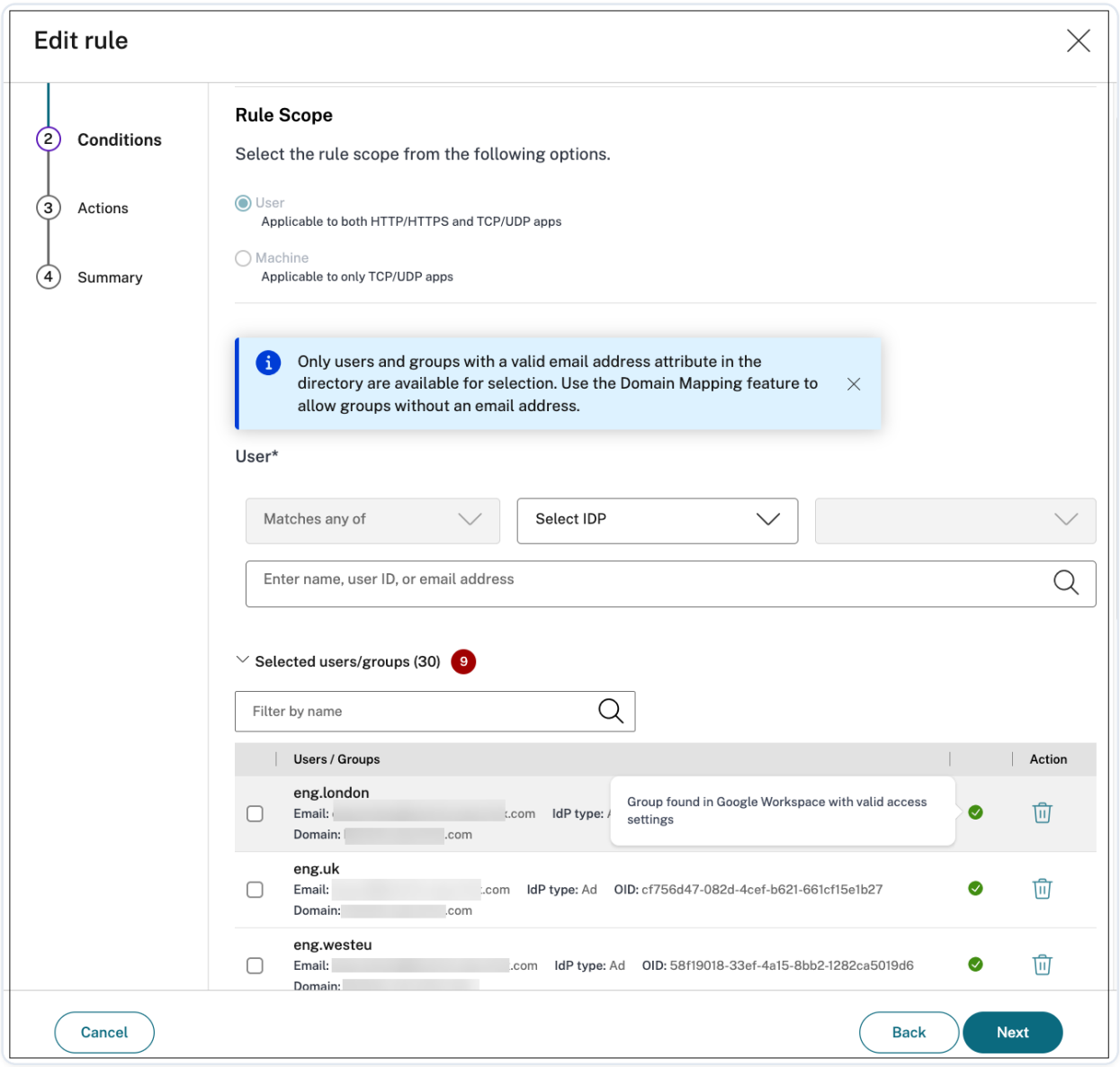


5. 输入规则名称和规则的简要描述，然后单击 **下一步**。



6. 选择用户条件。**用户**条件是授予用户访问应用程序的强制性条件。您可以选择条件，然后选择域，再选择用户。

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



选择以下其中一项：

- **匹配以下任意项** – 仅允许与字段中列出的任何名称匹配且属于所选域的用户或组访问。
- **不匹配任何项** - 允许除字段中列出且属于所选域的用户或组之外的所有用户或组访问。

注意：

- 您可以通过显示名称、电子邮件 ID 或用户主体名称搜索用户或组。这有助于您准确识别并授予正确用户访问权限，即使同一用户拥有多个帐户也是如此。有关详细信息，请参阅搜索用户或组。
- 您还必须使用同步的用户和组，以便正确评估 Secure Private Access 策略。否则，将显示警告消息。有关详细信息，请参阅验证用户和组同步。

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

7. 添加**访问模式**条件，以根据用户是通过基于浏览器的客户端还是 Citrix Secure Access 客户端连接来限制应用程序访问。有关详细信息，请参阅基于访问模式的策略实施。

   注意：

   您可以将访问模式与强制性**用户**条件和任何其他条件结合使用。

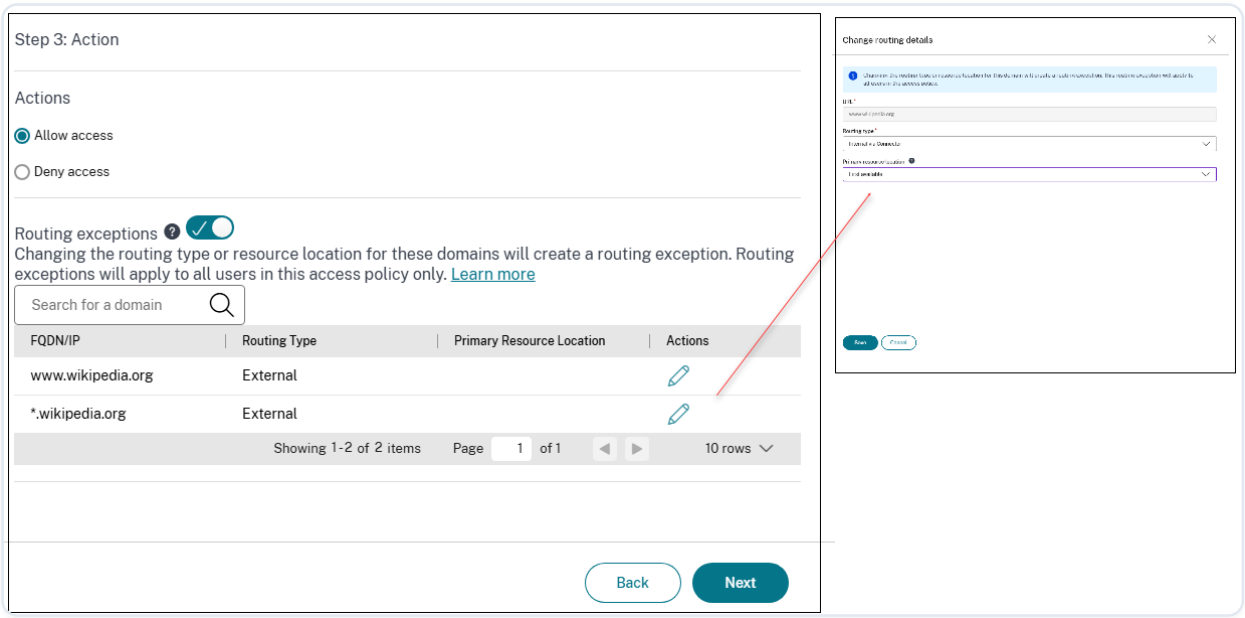
8. （可选）单击 + 可根据上下文添加多个条件。

   当您根据上下文添加条件时，将对这些条件应用 AND 运算，并且仅当满足**用户**和可选的基于上下文的条件时，才会评估策略。您可以根据上下文应用以下条件。

   - **地理位置** – 选择条件以及用户访问应用程序的地理位置。
     - **匹配以下任意项：** 仅允许从列出的任何地理位置访问应用程序的用户或用户组访问应用程序。
     - **不匹配任何项：** 除了来自所列地理位置的用户或用户组之外，所有用户或用户组都已启用访问权限。
   - **网络位置** – 选择用户访问应用程序所使用的条件和网络。
     - **匹配以下任意项：** 只有从所列网络位置中的任意一个访问应用程序的用户或用户组才被允许访问应用程序。
     - **不匹配任何项：** 除了来自所列网络位置的用户或用户组之外，所有用户或用户组都已启用访问权限。
   - **设备状态检查** – 选择用户设备必须满足的条件才能访问应用程序。

9. 单击“**下一步**”。
10. 根据条件评估结果选择要应用的操作。
    - **允许访问**
    - **拒绝访问**

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

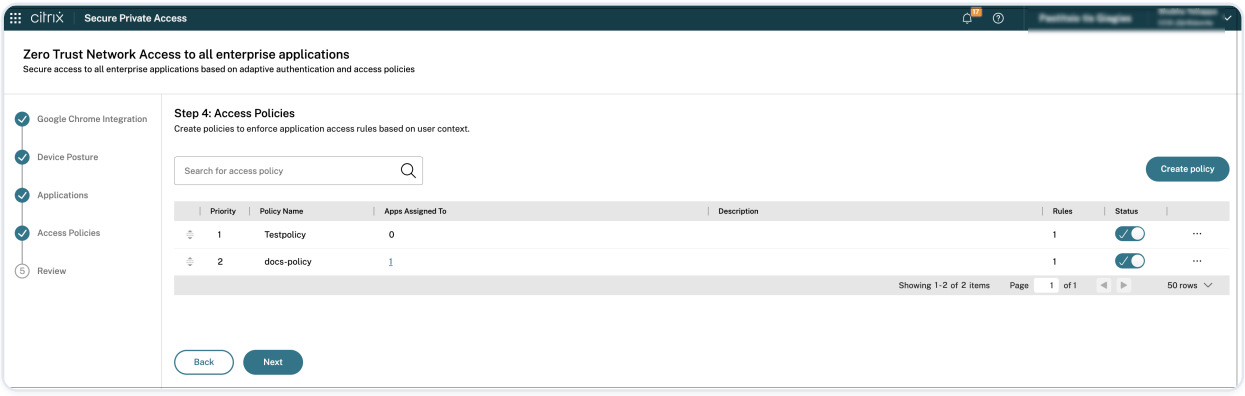


11. （可选）如果需要，修改特定域的路由类型或资源位置。**路由例外**切换开关允许您编辑访问策略中添加的应用程序域的资源位置和路由信息。

    - 在“**路由类型**”中，修改路由类型：
        - **内部**：流量通过连接器设备传输。对于 Web 应用程序，流量在数据中心内部传输。对于 SaaS 应用程序，流量通过连接器设备路由到网络外部。
        - **内部 - 绕过代理**：域流量通过 Citrix Cloud Connector™ 设备路由，绕过在连接器设备上配置的客户 Web 代理。
        - **外部**：流量直接流向互联网。
    - 在**资源位置**中，如有必要，修改资源位置。此选项仅适用于内部路由域。

    有关上下文路由的更多信息，请参阅基于上下文的应用程序路由和资源位置选择。

    创建策略后，它们将列在**访问策略**页面中。



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

搜索用户或组

您选择的用户和组将显示在一个网格中。网格中的每一行都显示以下身份详细信息，以便您可以清楚地区分不同域、林或身份提供商 (IdP) 中同名用户或组：

- **名称** – 用户或组的显示名称。
- **电子邮件** – 与身份关联的电子邮件地址。
- **IdP 类型** – 身份提供商，例如 Azure AD、Active Directory、Okta 或 Google。
- **OID** – 身份的对象 ID 或安全标识符。
- **域** – 用户或组所属的域。

您可以按名称筛选网格、删除单个行，或者选择多个条目并使用**删除所选内容**将其一起删除。

验证用户和组同步

选择用户或组时，管理员可以验证所选用户目录中的条目是否已与 Google Directory 同步并正确配置。Secure Private Access 策略只有当用户和组同步时才能正确评估。否则，可能会出现以下警告：

- **租户帐户权限缺失。**

  解决方法：

  在 Google 管理控制台中，将“**用户 > 读取**”和“**群组 > 读取**”权限分配给租户服务帐户。SPA 需要这些权限来验证用户或群组是否存在。

- **用户或群组未同步。**

  解决方法：

  搜索或选定的用户或群组未与 Google Directory 同步。在使用 SPA 策略之前，请将目录实体与 Google Directory 同步。

- **群组访问设置不足。**

  解决方法：

  在 Google 管理控制台中，打开所选群组的访问设置，并确保“**谁可以查看成员**”至少选择了“**群组成员**”选项。

注意：

此功能仅在 Google Chrome 集成成功完成后可用。

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

创建策略后需要记住的要点

- 您创建的策略将显示在“策略规则”部分下，并默认启用。如果需要，您可以禁用这些规则。但是，请确保至少启用一个规则，以便策略处于活动状态。
- 默认情况下，策略会分配一个优先级顺序。值越低的优先级越高。优先级编号最低的规则会首先进行评估。如果规则 (n) 不符合定义的条件，则会评估下一个规则 (n+1)，依此类推。

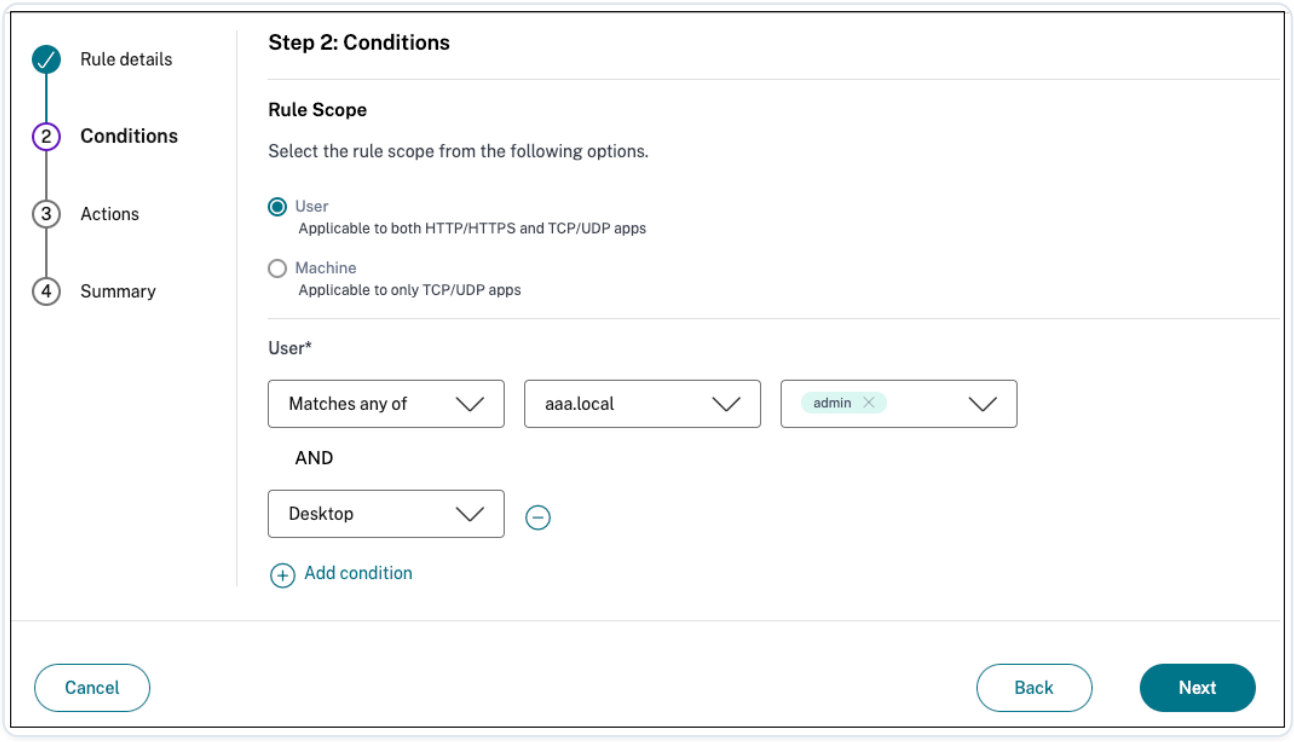
按优先级顺序评估规则示例：

假设您创建了两个规则，规则 1 和规则 2。 规则 1 分配给用户 A，规则 2 分配给用户 B，然后这两个规则都会被评估。 假设规则 1 和规则 2 都分配给用户 A。在这种情况下，规则 1 具有更高的优先级。如果规则 1 中的条件得到满足，则应用规则 1 并跳过规则 2。否则，如果规则 1 中的条件未得到满足，则将规则 2 应用于用户 A。

基于设备的自适应访问

要根据用户访问应用程序的平台（移动设备或台式计算机）配置自适应访问策略，请参阅自适应访问策略配置和管理。

- 在“**步骤 2：条件**”页面中，单击“**添加条件**”。
- 选择“**桌面**”或“**移动设备**”。
- 完成策略配置。



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

基于位置的自适应访问

管理员可以根据用户访问应用程序的位置配置自适应访问策略。该位置可以是用户访问应用程序的国家/地区，也可以是用户的网络位置。网络位置是使用 IP 地址范围或子网地址定义的。

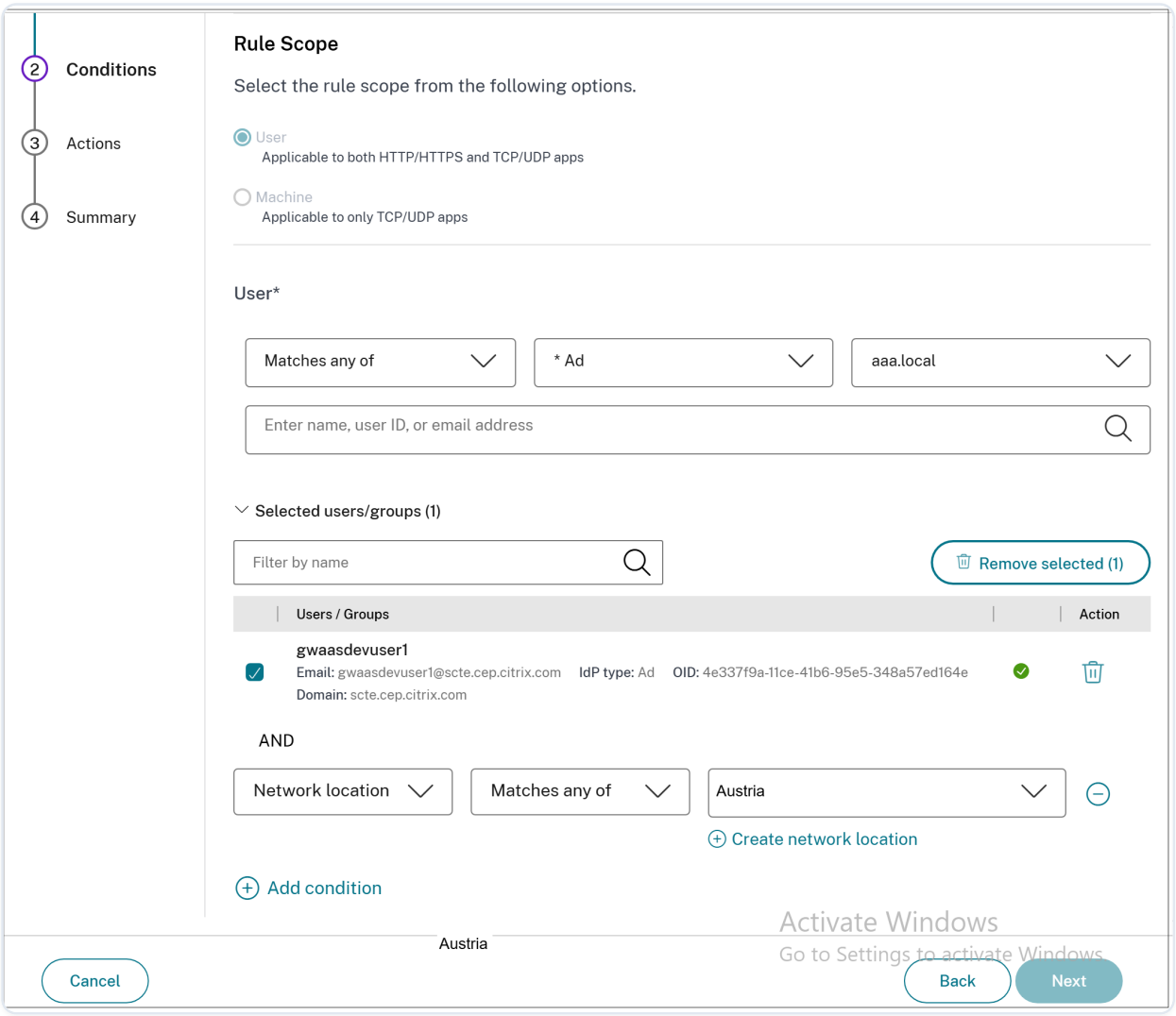
要根据位置配置自适应访问策略，请使用创建具有多个规则的自适应访问策略过程，并进行以下更改。

- 在“**步骤 2：条件**”页面中，单击“**添加条件**”。
- 选择“**地理位置**”或“**网络位置**”。
- 如果您已配置多个地理位置或网络位置，请根据您的要求选择以下选项之一。
    - “**匹配其中任何一个**” – 地理位置或网络位置与数据库中配置的任何地理位置或网络位置匹配。
    - “**不匹配任何一个**” – 地理位置或网络位置与数据库中配置的任何地理位置或网络位置不匹配。

“**注意：**”:

- 如果选择**地理位置**，则会根据国家/地区数据库的 IP 地址评估用户的源 IP 地址。如果用户的 IP 地址映射到策略中的国家/地区，则应用该策略。如果国家/地区不匹配，则跳过此自适应策略并评估下一个自适应策略。
- 对于**网络位置**，您可以选择现有网络位置或创建网络位置。要创建新的网络位置，请单击**创建网络位置**。
- 确保您已从 **Citrix Cloud > StoreFront Cloud > Access > Adaptive Access** 启用自适应访问。否则，您无法添加位置标签。有关详细信息，请参阅启用自适应访问。
- 您还可以从 Citrix Cloud 控制台创建网络位置。有关详细信息，请参阅Citrix Cloud 网络位置配置。

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



- 完成策略配置。

基于设备姿态的自适应访问

您可以配置 Secure Private Access 服务以使用设备姿态标签强制实施访问控制。设备姿态验证后允许设备登录，设备可以分类为合规或不合规。此信息作为标签提供给 Citrix DaaS™ 服务和 Citrix Secure Private Access 服务，并用于根据设备姿态提供上下文访问。

有关设备姿态服务的完整详细信息，请参阅设备姿态。

要根据设备姿态配置自适应访问策略，请使用创建具有多个规则的自适应访问策略过程并进行以下更改。

- 在**步骤 2: 条件**页面中，单击**添加条件**。
- 从下拉菜单中选择**设备姿态检查**和逻辑表达式。
- 在自定义标签中输入以下值之一：
  - **合规** - 适用于合规设备

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

- **不合规** - 适用于不合规设备

> **注意：**
>
> 设备分类标签的语法必须与之前捕获的方式相同，即首字母大写（Compliant 和 Non-Compliant）。否则，设备姿态策略将无法按预期工作。

基于设备的自适应访问策略(/en-us/citrix-secure-private-access/media/access-policy-device-posture.png)

会话策略

管理员可以配置会话策略，将内部企业用户直接路由到后端应用程序，而无需通过 Secure Private Access 隧道传输流量。会话策略根据网络位置和设备状态等因素提供动态路由。

> **注意：**
>
> - 会话策略设置在会话级别应用于所有应用程序，而不是绑定到特定应用程序。
> - 会话策略可以分配给所有用户或部分用户。

路由优先级

会话策略与访问策略协同工作，如果存在冲突，访问策略优先。在这种情况下，访问策略路由例外会覆盖会话策略。 如果既未配置访问策略也未配置会话策略，则应用全局路由设置（**设置 > 应用程序域**）。

支持的 Citrix Secure Access™ 客户端

以下版本的 Citrix Secure Access 客户端支持将用户直接路由到后端应用程序。

- macOS - 24.11.1 及更高版本
- Windows - 24.11.1.17 及更高版本。此外，必须启用 **EnableContextualAccess** VPN 客户端注册表。有关详细信息，请参阅 NetScaler Gateway Windows VPN 客户端注册表项。

用例示例

场景：

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

在组织中，当用户连接到企业网络“corporate_network1”时，来自应用程序的流量必须直接流向后端应用程序，因为这些应用程序在企业网络上可以直接访问。如果用户在企业网络之外，则应用程序流量必须通过隧道传输。

解决方案：

1. 添加 app1、app2，并将路由设置为**通过连接器内部**。
2. 为应用程序 (app1, app2) 添加访问策略以授予访问权限。
3. 添加会话策略以配置条件，指定授予访问权限时必须考虑的用户组和网络位置。
4. 选择**用户**条件并将其设置为**所有用户**。
5. 添加**网络位置**条件。将其设置为**匹配以下任意项**，并指定网络位置“corporate_network1”。这可确保来自“corporate_network1”的流量直接流向后端应用程序。

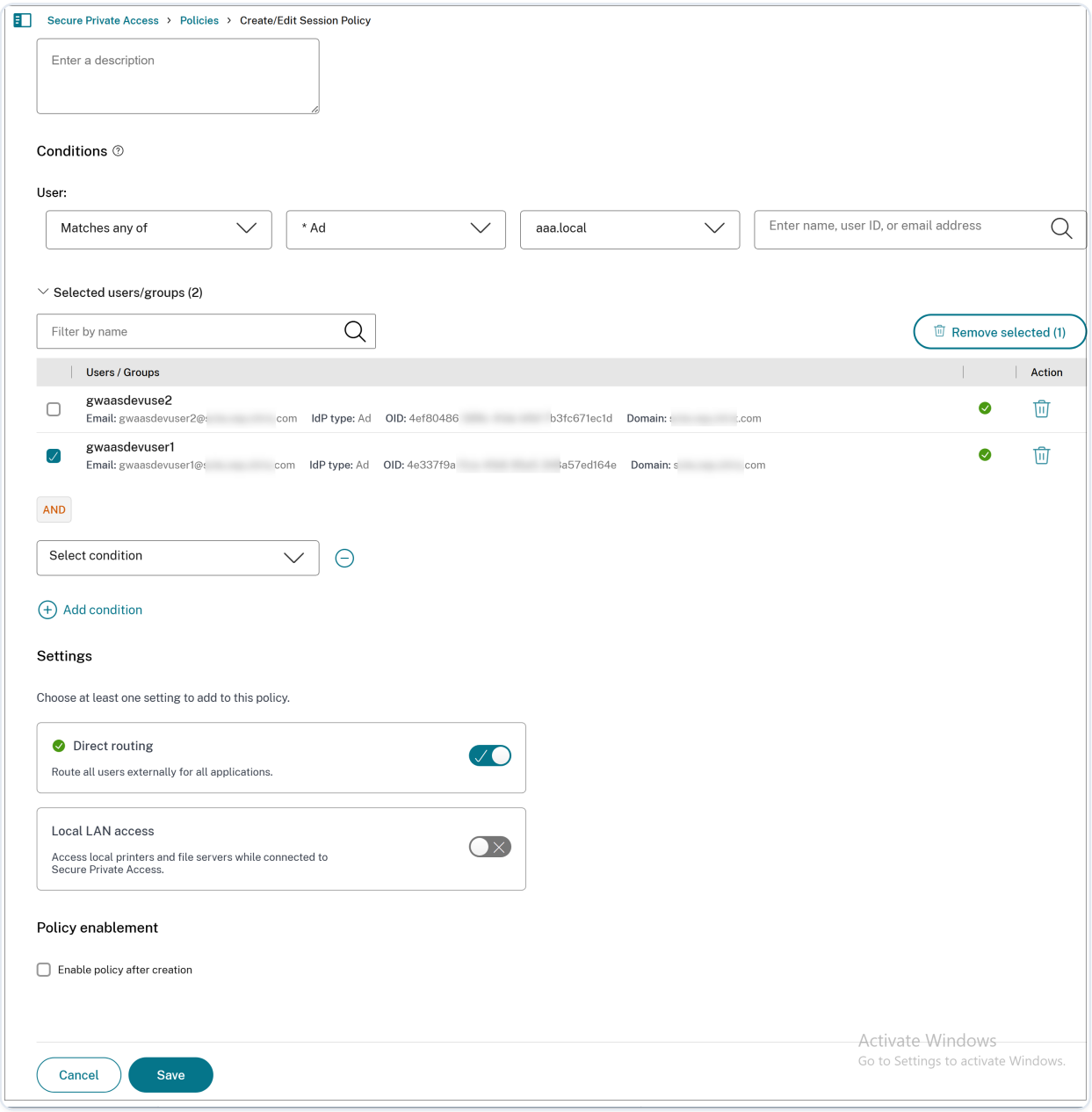
您还可以为此场景启用路由例外。例如，如果 app1 即使在公司网络上也必须始终通过隧道传输，则可以在访问策略中为 app1 的域配置路由例外。完成此操作后，路由例外将优先于会话策略。

使用会话策略在公司网络中配置直接路由

您必须创建会话策略，以使用户能够直接访问后端应用程序，从而绕过 Secure Private Access 隧道。为此，首先，您选择此策略必须应用到的用户。其次，在“网络位置”下，选择您的公司网络的名称。这是确保仅当用户位于公司内部网络时才启用直接路由的重要步骤。

1. 导航到**策略 > 会话策略**，然后单击**创建会话策略**。

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



2. 输入策略名称和策略描述。
3. 选择要应用这些设置的用户和条件。
4. 您可以选择将条件应用于所有用户或指定部分用户。

> **注意：**
>
> 您可以通过显示名称、电子邮件 ID 或用户主体名称搜索用户或组。这有助于您准确识别并授予正确用户访问权限，即使同一用户拥有多个帐户。

您选择的用户和组将显示在网格中。网格中的每一行都显示以下身份详细信息，以便您能够清楚地区分不同域、林或身份提供商 (IdP) 中同名用户或组：

- **名称** – 用户或组的显示名称。

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

- **电子邮件** – 与身份关联的电子邮件地址。
- **IDP 类型** – 身份提供商，例如 Azure AD、Active Directory、Okta 或 Google。
- **OID** – 身份的对象 ID 或安全标识符。
- **域** – 用户或组所属的域。 您可以按名称筛选网格、删除单个行，或者选择多个条目并使用“删除选定项”将其一起删除。

5. 添加**访问模式**条件，将会话设置范围限定为预期的客户端类型。在 Secure Private Access 路由期间评估的会话策略被视为 CSA 访问模式。有关访问模式的更多信息，请参阅基于访问模式的策略实施。
6. （可选）单击 + 可根据上下文添加多个条件。
7. 定义**网络位置**条件以启用整个会话的动态路由。这确认仅当用户位于公司企业网络内部时才启用直接路由。

   当您根据上下文添加条件时，将对这些条件应用 AND 运算，其中仅当用户和可选的基于上下文的条件都满足时，才会评估策略。有关条件的详细信息，请参阅配置访问策略。
8. 选择**直接路由**以将所有用户外部路由到后端应用程序。
9. 选择**本地 LAN 访问**以启用对本地 LAN 资源的无缝访问。有关更多详细信息，请参阅无缝访问本地 LAN 资源（打印机、文件服务器）。
10. 选择**创建后启用策略**。如果您不选择此选项，则策略仅创建而不对应用程序强制执行。或者，您也可以通过使用“状态”列中的切换开关从“会话策略”页面启用策略。
11. 单击**保存**。

注意：

网络位置更改会触发会话策略刷新，这可能会对最终客户端产生以下影响：

- **Citrix Secure Access 代理：** 策略刷新可能会更改路由配置，从而影响应用程序访问。
- **Citrix Enterprise Browser™：** 策略每 30 分钟刷新一次。用户必须重新启动浏览器或等待刷新才能访问应用程序。

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

Citrix 企业浏览器到 Chrome 企业高级版迁移

从 Citrix Enterprise Browser (CEB) 到 Citrix Enterprise Premium (CEP) 的过渡标志着 Citrix Secure Private Access 在提供安全、自适应、高性能的零信任网络访问 (ZTNA) 以支持所有应用程序方面迈出了重要一步。本主题为 IT 管理员和 Citrix 专业人员提供了详细信息，以规划和执行成功的逐步迁移，确保最大限度地减少中断并优化用户体验。

这种分阶段迁移方法允许组织在过渡期间通过并行运行两种浏览器解决方案来保持业务连续性。通过分阶段迁移，客户可以验证现有应用程序和工作流与 Chrome Enterprise Premium 的兼容性。

CEB 到 CEP 迁移涉及以下关键步骤：

- 配置 Chrome 企业高级版
- 为没有电子邮件地址的用户组进行域映射
- 用于 CEP 兼容性分析的 Secure Private Access 配置解析器
- 在完全迁移到 CEP 之前的配置更改
- 向组织推出 CEP（完全迁移）

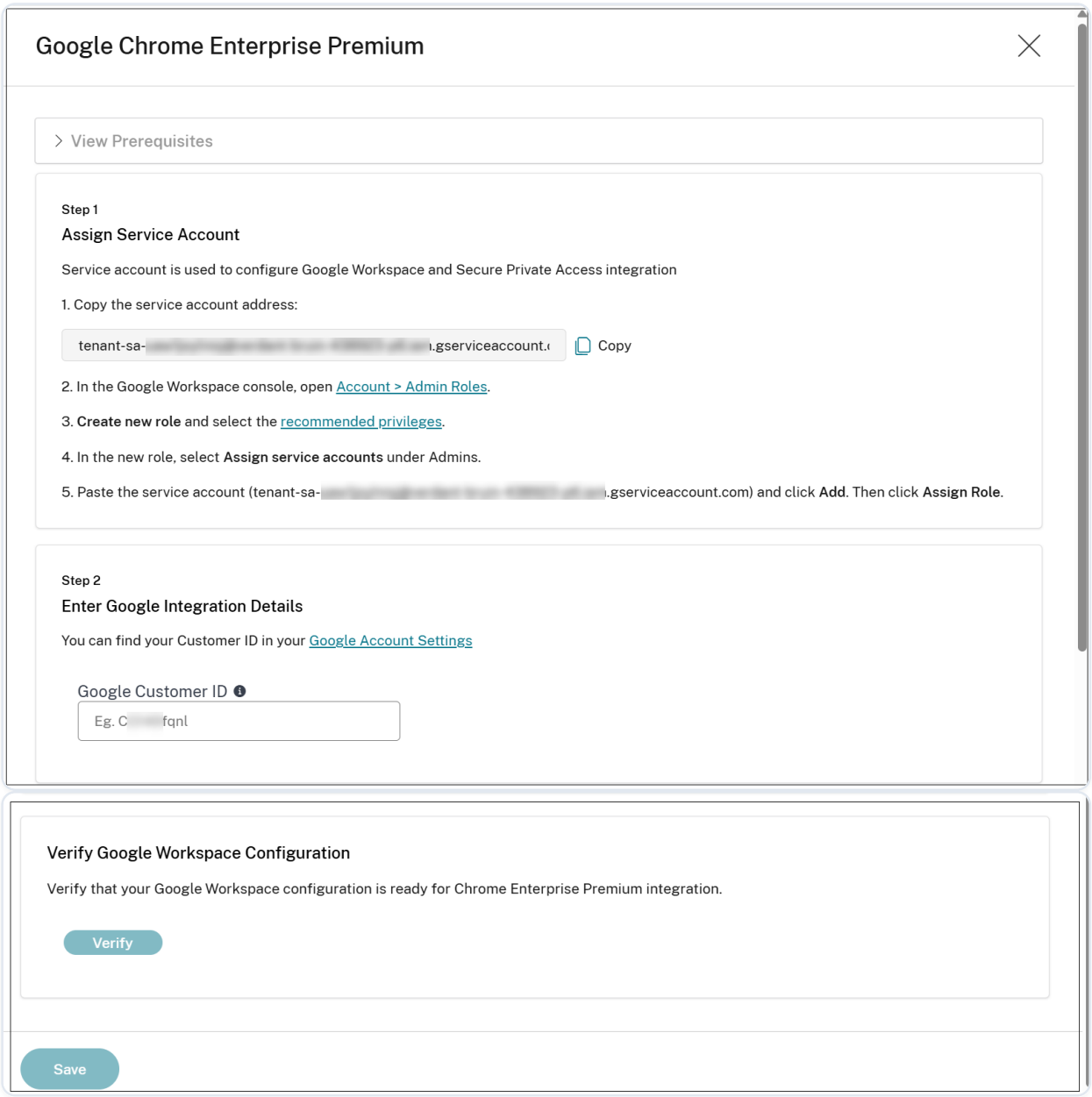
配置 Chrome 企业高级版

对于现有的 Secure Private Access 客户，Secure Private Access 控制台中的迁移向导可促进 CEP 预配、为用户安装扩展，并提供逐步应用程序和用户迁移的路径。

1. 在 Secure Private Access 管理控制台中，导航到 **Chrome Enterprise Premium > 配置**。

   您可以查看 Google 集成详细信息。

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



2. 点击 **设置 Google CEP**。
3. 在 Google WorkSecure Private Access 控制台中分配 Citrix 服务帐户详细信息。有关详细信息，请参阅 设置 Google Chrome 集成。
4. 点击 **保存** 并关闭。

Chrome 企业高级版 的预配开始。

没有电子邮件的用户组的策略丰富

Chrome Enterprise Premium 预配成功完成后，将自动触发针对访问策略和会话策略的策略更新过程。

此更新过程执行以下操作：

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

- 审查现有策略（访问和会话）。
- 检查其规则中没有电子邮件的用户和用户组。
- 查询 CC Directory 服务以检索其电子邮件，并将其添加到策略中。

有关详细信息，请参阅 没有电子邮件地址的用户组的域映射。

用于 CEP 兼容性分析的 Secure Private Access 配置解析器

以下关键策略元素在 CEP 中不受直接支持：

- 应用程序
  - 单点登录
- 访问策略
  - 允许受限访问
  - 混合允许/拒绝操作（HTTP/HTTPS 与 TCP/UDP）
  - 存储 URL 条件
  - 桌面/移动条件
- 会话策略
  - 存储 URL 条件
  - 桌面/移动条件
- 安全组
- Web 过滤

在将应用程序从 CEB 迁移到 CEP 之前，必须解决这些不兼容问题。

不兼容性识别过程由 Secure Private Access 配置解析器 `<parse_citrix_spa_configuration.py>` 促进。此工具分析 Citrix Secure Private Access 配置导出，以在迁移到 CEP 期间识别兼容性问题，例如以下问题。

- 与 CEP 不兼容的应用程序
- 与 CEP 不兼容的访问策略
- 已配置的安全组
- Web 过滤配置

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

注意：

Citrix Secure Private Access 与 CEP 的集成不支持安全组和 Web 过滤。

分析后，该工具会根据 CEP 部署是否已在整个组织中完成（所有应用程序的迁移）提供不同的建议。

如何使用该工具

1. 从以下位置下载脚本：用于解析安全专用访问配置的 Python 脚本。
2. 在 Secure Private Access 管理控制台中，导航到**设置 > 全局配置 > 创建报告**，然后将现有 Secure Private Access 配置导出为 JSON 格式。
3. 下载 Python 脚本并使用导出的报告作为输入运行脚本。您必须安装 Python 3 才能运行此脚本。

   ```
   # python3 parse_citrix_spa_configuration.py <path_to_spa_report>
   ```

   该脚本可以在完全迁移之前或之后使用，提供不同的建议操作。

注意：

该脚本不提供不兼容会话策略的建议。

示例报告：

```
% python3 parse_citrix_spa_configuration.py
CitrixSpaConfigurationDump.json



Has the CEP rollout to the entire organization been completed?



Enter yes/no (default: no): no



CEP INCOMPATIBLE APPLICATIONS (7 out of 185):
```

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

```
1. Application_1 ⚠

   Reason: Has SSO configuration other than 'Don't use SSO'

2. Application_2 ⚠

   Reason: Has SSO configuration other than 'Don't use SSO'

....

--------------------------------------------------

Mitigation guidance:

--------------------------------------------------

Has SSO configuration other than 'Don't use SSO':

  • Navigate to the application's SSO settings

  • Change the SSO setting to 'Don't use SSO'
```

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

```
================================================


CEP INCOMPATIBLE POLICIES (15 out of 136):


1. Access_policy_1 ⚠


   Reasons: Contains user(s)/group(s) without email


2. Access_policy_2 ⚠


   Reasons: Mixed actions (HTTP/HTTPS vs TCP/UDP), Contains user(s)/
group(s) without email


...


--------------------------------------------------


Mitigation guidance:


--------------------------------------------------
```

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

Platform filter (Desktop/Mobile):

- Remove the unsupported Desktop/Mobile condition

Workspace URL:

- Remove the unsupported Workspace URL rule

Access with restrictions:

- Configure access controls without using restrictions

Mixed actions (HTTP/HTTPS vs TCP/UDP):

- Ensure both actions have the same value

- If that's not possible, create separate policies for HTTP/HTTPS and TCP/UDP applications

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

```
Policy contains user(s)/group(s) without email
```

- Add email to the user(s)/group(s) without email and update the policy

完全迁移到 CEP 之前的配置更改

在启动到 CEP 的完全迁移之前，Secure Private Access 管理员必须手动应用以下配置更改。这些更新可确保所有应用程序和策略的兼容性和就绪性。

单点登录配置更改

为确保与 CEP 兼容，必须更新所有现有应用程序的单点登录 (SSO) 配置。Secure Private Access 管理员必须执行以下步骤：

1. 导航到应用程序配置页面（**Secure Private Access > 应用程序配置**）。
2. 编辑应用程序以修改单点登录配置。

   在“单点登录”部分中，在“**您希望为 Web 应用程序设置使用哪种单点登录类型？**”下，选择“**不使用 SSO**”。

重要提示：

- 此更新是强制性的，因为 CEP 中已删除 SSO 步骤。通过将应用程序设置为“**不使用 SSO**”，您可以确保持续的功能并与新的迁移流程保持一致。
- 如果未按说明更改单点登录配置，则在迁移到 CEP 后，应用程序将无法访问。

访问策略和会话策略更新

为确保访问策略与 CEP 标准兼容，需要对访问策略和会话策略进行特定更新。Secure Private Access 管理员必须执行以下步骤：

1. 导航到 **Secure Private Access > 策略 > 访问策略**。
2. 单击相关策略上的“**编辑**”并修改操作设置。

   a. 在策略中，导航到“**策略规则**”部分，单击策略规则行中的省略号图标，然后单击“**编辑**”。

   b. 导航到“**操作**”页面并更改“**操作**”设置。

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

跨应用程序标准化操作

为 HTTP/HTTPS 和 TCP/UDP 应用程序配置操作时，请确保以下事项：

- 在两个部分中都选择了相同的操作，即**允许访问**或**拒绝访问**。
- 如果当前为 HTTP/HTTPS 应用程序启用了**允许受限访问**选项，则必须将其移除，因为 CEP 不支持此设置。
- 根据您预期的策略行为，将**允许受限访问**替换为**允许访问**或**拒绝访问**。

策略更新的应用程序要求

未分配应用程序的访问策略无法更新。要修改这些策略，请首先将应用程序分配给策略。

重要提示：

如果未执行这些更新，则与包含混合操作的访问策略关联的应用程序将无法访问，或者拒绝操作设置可能会被忽略。

Web 过滤策略更新（可选）

为了与新的 CEP 迁移标准保持一致，需要更新 Secure Private Access 中的 Web 过滤设置。执行以下步骤以更新 Web 过滤配置：

1. 导航到 **Secure Private Access > 设置 > 未经批准的网站**。
2. 删除当前在此部分下列出的所有网站和远程浏览器隔离 (RBI) 条目。
3. 删除这些条目后，禁用位于页面顶部的**Web 过滤已启用**切换开关。

在迁移到 CEP 后，这些配置不再相关。

重要提示：

如果这些步骤未完成，则在完全迁移后对系统操作没有影响。但是，**未授权网站**页面将不可见。

其他策略调整（可选）

审查并删除未使用的条件：

作为迁移和策略优化过程的一部分，建议审查访问和会话策略，以查找可能不再适用的任何条件。此类条件的示例包括：

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

- 工作区 URL
- 桌面和移动选项

如果这些条件与您当前的环境或业务需求不相关，则可以将其删除。

注意：

如果未进行这些策略调整，则对系统操作没有影响。

安全组清理（可选）

审查 Secure Private Access 中的安全组配置。

导航到 **Secure Private Access > 应用程序 > 安全组**以评估任何现有条目。

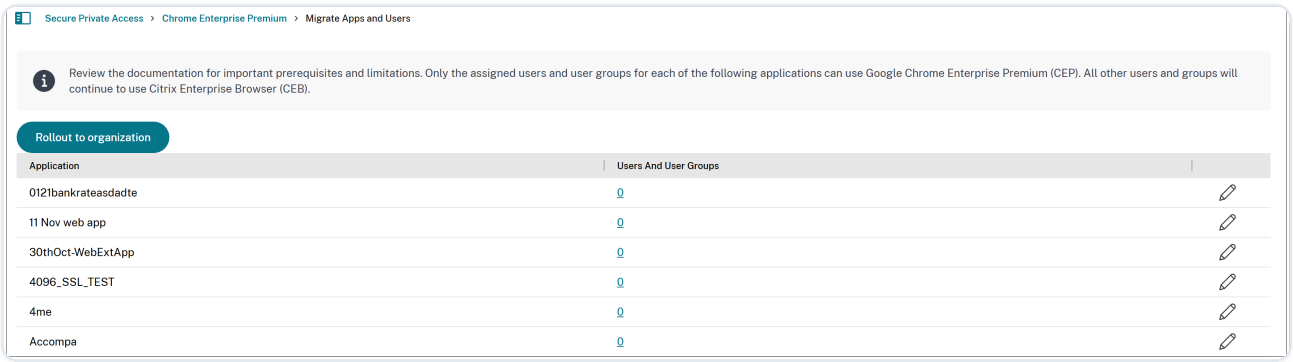
迁移后，安全组配置将不再可用。因此，当前在此选项卡下显示的任何条目都可以删除，因为它们将不再与迁移后的环境相关。

注意：

如果未更新此配置，则对系统没有影响。删除这些条目是可选的，有助于维护精简的环境，但对于持续运行并非必需。

向组织部署 CEP（完全迁移）

完成前面提到的步骤后，在**迁移应用和用户**页面中点击**部署到组织**。这是迁移过程的最后阶段。



重要提示：

部署完成后，CEP 将成为默认的企业浏览器。无法回滚到 CEB，并且不兼容的设置将在 Secure Private Access 管理控制台中隐藏。

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

迁移过程摘要

请按照以下步骤将应用程序从 CEB 迁移到 CEP：

1. 预配 Chrome 企业高级版。
2. 为特定用户组迁移一个应用程序。
    a. 为组添加电子邮件信息（如果不存在）。
    b. 修复任何不兼容问题。
    c. 将应用程序迁移到 CEP。
    d. 验证应用程序是否可以通过 CEP 访问（直接、通过 CWA 和 WSUI）。
3. 为用户和用户组添加电子邮件信息。
4. 迁移更多应用程序、用户和用户组。
5. 将 CEP 推广到整个组织（完全迁移）。
6. 修复任何遗留的不兼容问题。
    a. 再次运行脚本，在提示中指出 CEP 推广已完成。
    b. 修复不兼容问题。
    c. 验证应用程序是否可通过 CEP 访问（直接访问、通过 CWA 和 WSUI 访问）。

电子邮件丰富化过程中的挑战

电子邮件丰富化任务可能很复杂，因为它通常涉及多个团队之间的协作，以将电子邮件分配给跨多个域的各种组。域映射功能有助于简化此过程。有关详细信息，请参阅没有电子邮件地址的用户组的域映射。

最佳实践

1. 在全面推广之前，先对一小部分用户组进行试点迁移。
2. 利用 Citrix 的官方迁移工具和文档。
3. 维护所有更改和配置的清晰文档。
4. 制定回滚计划，以防出现严重问题。

结论

从 CEB 迁移到 CEP 可通过增强的功能使您的 Citrix 环境现代化。精心规划、全面测试和积极的用户参与可确保顺利过渡到 CEP。

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

高级安全私有访问功能

以下是安全私有访问支持的一些高级功能：

- **基于访问模式的策略实施：** 基于访问模式的策略实施允许管理员限制用户连接应用程序的方式。连接可以通过基于浏览器的客户端或 Citrix Secure Access 客户端进行。有关更多信息，请参阅 基于访问模式的策略实施。
- **本地 LAN 访问支持：** 安全私有访问支持无缝访问本地 LAN 资源，同时保持与公司资源的安全连接。有关详细信息，请参阅 无缝访问本地 LAN 资源（打印机、文件服务器）。
- **将 DNS 查询路由到特定于应用程序的资源位置：** 管理员可以将特定应用程序的 DNS 查询直接路由到其专用资源位置。这可以实现更准确的 DNS 解析、智能流量管理和更好的用户体验。有关详细信息，请参阅 将 DNS 查询路由到特定于应用程序的资源位置。
- **安全私有访问服务的混合数据路径：** 安全私有访问服务的混合数据路径利用本地和云基础设施来提供对应用程序的安全访问。组织可以使用混合数据路径通过本地 NetScaler Gateway 路由所有数据流量。这确保敏感数据保留在公司网络内。即使数据流量通过本地 NetScaler Gateway 路由，Citrix Cloud 仍可用于监视和管理应用程序和用户。有关详细信息，请参阅 安全私有访问服务的混合数据路径。
- **发现网络中的应用程序、域或 IP 地址：** 帮助管理员了解组织中正在访问的外部和内部应用程序（HTTP/HTTPS 和 TCP/UDP 应用程序）。此功能发现并列出所有已发布或未发布的域/IP 地址。因此，管理员可以查看正在访问哪些域/IP 地址、由谁访问，并决定是否将其发布为应用程序，从而为这些用户提供访问权限。有关详细信息，请参阅 发现网络中的应用程序、域或 IP 地址。
- **基于上下文的应用程序路由和资源位置选择：** 允许管理员根据用户上下文编辑每个 URL 或资源位置的内部路由类型。有关详细信息，请参阅 基于上下文的应用程序路由和资源位置选择。
- **策略建模工具：** 根据现有配置，为管理员提供预期应用程序访问结果（允许/受限允许/拒绝）的完整可见性。管理员可以根据设备类型、设备姿态、地理位置、网络位置和工作区 URL 等条件检查任何用户的访问结果。有关详细信息，请参阅 策略建模工具。
- **应用程序导入工具：** 安全私有访问管理控制台包含一个文件导入工具，允许管理员使用 CSV 文件或 nsconfig 文件将多个应用程序批量导入系统。此工具对于从传统 VPN 转向更高级解决方案（如安全私有访问）的组织特别有用。例如，组织可以使用此工具将通过 VPN 交付的应用程序迁移到安全私有访问，并转向基于 ZTNA 的架构。批量上传应用程序使组织能够消除手动配置的需要。有关详细信息，请参阅 应用程序导入工具。

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

- **终止活动会话并阻止用户/计算机：** - 使管理员能够立即终止所有活动会话并将用户/计算机添加到阻止列表。将用户/计算机添加到阻止列表会终止所有活动的 Secure Private Access 应用程序会话并阻止将来的应用程序访问。有关详细信息，请参阅 终止活动会话并将用户/计算机添加到阻止列表。
- **用户会话超时：** 允许管理员为 Web 应用程序和 Citrix Secure Access 客户端配置超时期限，以便在指定时间内没有网络活动时结束用户会话。有关详细信息，请参阅 用户会话超时。

Secure Private Access 服务的混合数据路径

Secure Private Access 服务的混合数据路径利用本地和云基础设施来提供对应用程序的安全访问。组织可以使用混合数据路径将所有数据流量通过本地 NetScaler Gateway 路由。这确保了敏感数据保留在公司网络内。即使数据流量通过本地 NetScaler Gateway 路由，Citrix Cloud™ 仍可用于监视和管理应用程序和用户。

使用混合数据路径的主要优势

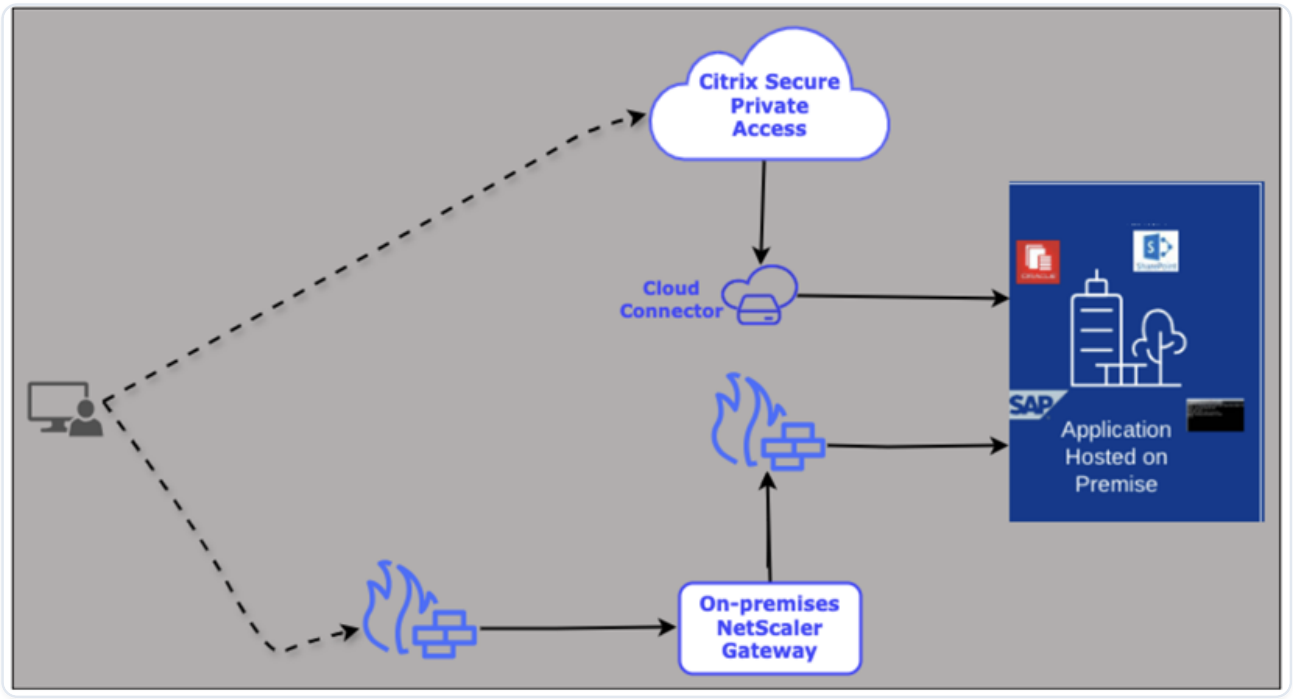
以下是使用混合数据路径的一些主要优势：

- 通过本地网关扩展覆盖范围：
  - 在云 PoP 较远的区域，利用本地 NetScaler® Gateway 提供对本地应用程序的访问。
  - 避免通过遥远的云 PoP 路由流量，从而确保一致的性能。
- 精细的安全性和控制：
  - 实施选择性路由，将敏感应用程序通过安全的本地路径引导，并将不太关键的应用程序通过云路由。
  - 为应用程序启用自定义路由，以根据应用程序数据敏感性满足数据安全和合规性要求
- 直接连接以增强用户体验：
  - 在远程用户和所需应用程序之间建立直接连接，绕过云 PoP。

混合数据路径的工作原理

下图显示了混合数据路径的工作流程。

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



以下列表解释了混合数据路径中涉及的工作流程：

1. 用户登录到 Citrix Secure Access™ 客户端。
2. 成功身份验证后，会建立一个会话。
3. 最终用户尝试启动应用程序。
4. 评估与应用程序关联的访问策略，然后启动应用程序。
    - 如果应用程序配置为通过 Secure Private Access 服务路由，则请求将发送到 Cloud Connector，然后启动特定的应用程序。
    - 如果应用程序配置为通过本地 NetScaler Gateway 路由，则请求将发送到本地 NetScaler Gateway，然后启动特定的应用程序。

支持的客户端

以下 Citrix Secure Access 客户端支持混合数据路径：

- Windows - 25.1.1.17 及更高版本
- macOS - 25.02.1 及更高版本

支持的 NetScaler Gateway 版本

从 NetScaler Gateway 14.1 版本 47.46 开始支持混合数据路径。

连接要求

以下部分提供了有关连接要求的更多信息。

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

出站连接允许的 URL 列表

必须允许 NetScaler Gateway 出站连接访问以下 URL：

- `https://trust.citrixnetworkapi.net`：用于向 Citrix Cloud 注册网关。
- `https://trust.citrixworkspacesapi.net`：用于向 Citrix Cloud 注册网关。
- `https://policy.netscalergateway.net`：用于通过网关授权应用程序启动请求。
- `https://cacerts.digicert.com`：用于策略服务引擎证书验证。

为 Secure Private Access 应用程序设置混合数据路径

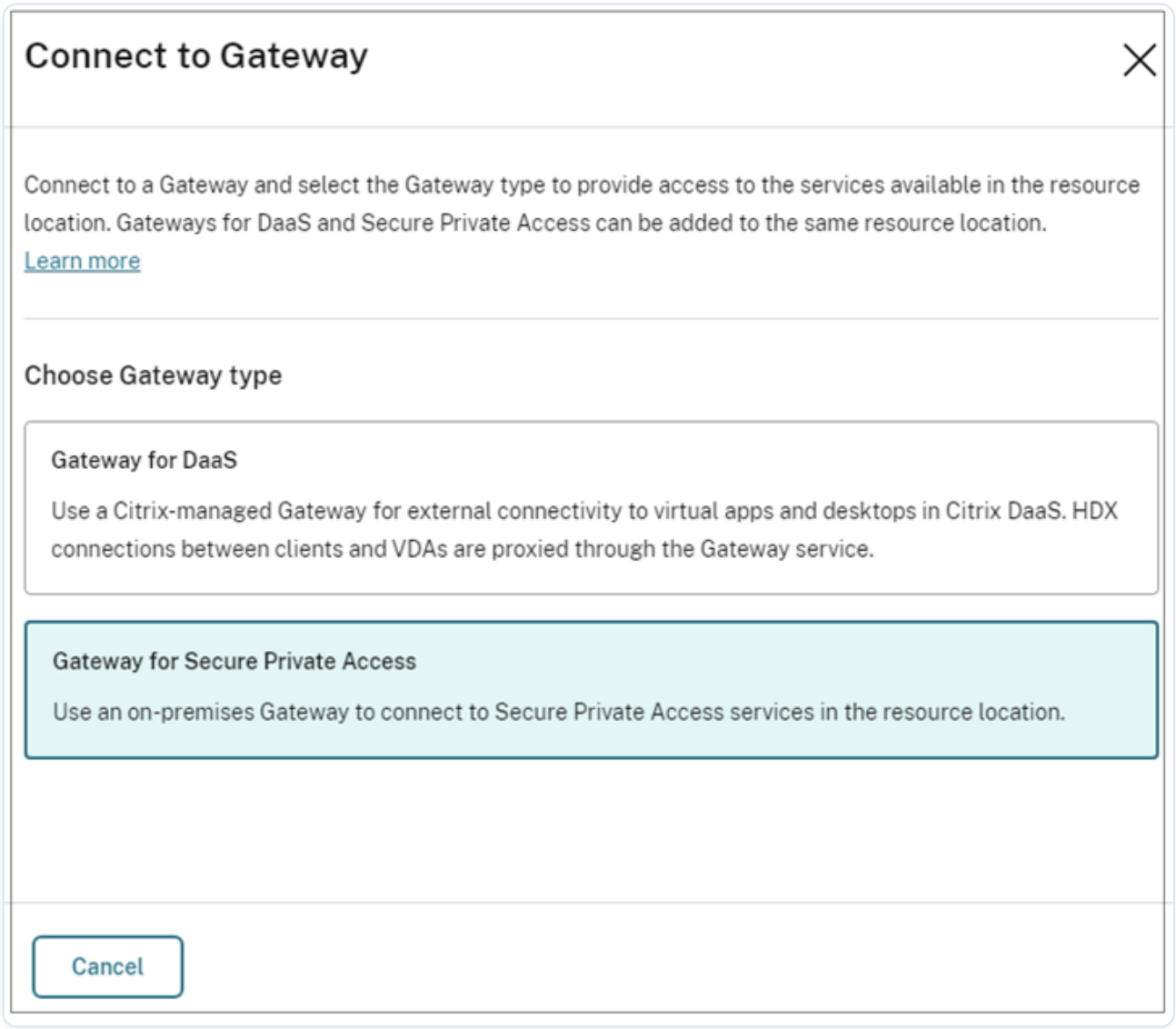
设置混合数据路径涉及以下高级步骤：

1. 连接到网关以建立连接
2. 将 NetScaler Gateway 注册到 Citrix Cloud
3. 通过本地 NetScaler Gateway 启用数据流量路由

连接到网关以建立连接

要与特定资源位置中的 Secure Private Access 资源建立连接，您必须首先连接到网关。Citrix Cloud 使您能够与特定资源位置中的 DaaS 和 Secure Private Access 资源建立连接。您选择的网关类型决定了您可以访问的服务。为了增强灵活性并优化资源利用率，您可以在同一资源位置中添加 DaaS 网关和 Secure Private Access 网关。

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



- **DaaS 网关：** Citrix 管理的网关充当 Citrix DaaS™ 环境中托管的虚拟应用程序和桌面的外部访问点。此网关充当安全代理，协调和管理客户端（用户设备）与 Citrix Cloud 中驻留的虚拟桌面代理 (VDA) 之间的 HDX 连接。

  您可以根据不同的业务需求选择如何允许访问虚拟应用程序和桌面。

- **用于安全私有访问的网关：** 用于安全私有访问的网关通过将所有数据流量路由到本地 NetScaler Gateway，确保数据保留在公司网络边界内，从而确保组织对敏感数据的控制。

  虽然本地 NetScaler Gateway 处理数据流量，但 Citrix Cloud 可用于集中管理和监控功能，使管理员能够无缝地监督和管理应用程序和用户。

执行以下步骤连接到网关：

1. 登录 Citrix Cloud。
2. 选择 **资源位置 > 概述**，然后单击 **网关**。
3. 在 **选择网关类型** 中，选择 **用于安全私有访问的网关**。

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

4. 向 Citrix Cloud 注册您的网关。有关详细信息，请参阅 向 Citrix Cloud 注册您的 NetScaler Gateway。

向 Citrix Cloud 注册您的 NetScaler Gateway

您必须首先选择用于安全私有访问的网关，然后将本地 NetScaler Gateway 注册到 Citrix Cloud。此注册在您的本地 NetScaler Gateway 与 Citrix Cloud 环境之间为安全私有访问服务建立安全连接。

先决条件：

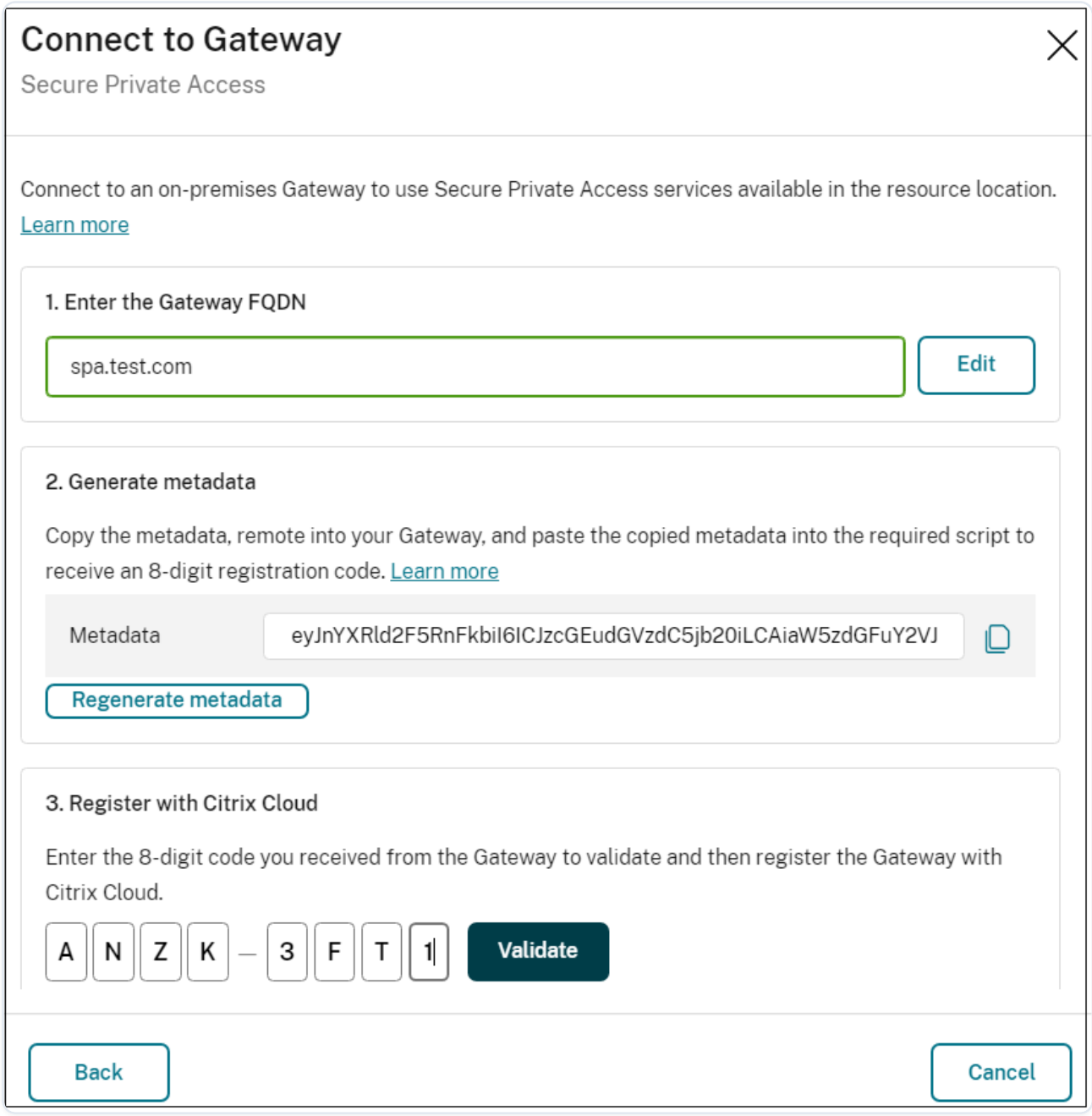
确保完成以下配置，以便成功执行注册脚本：

- 必须在 NetScaler 上配置子网 IP (SNIP)。
- 如果尚未配置，则必须配置 DNS 名称服务器。
- 需要为新的 VPN 虚拟服务器指定一个 IP 地址。
- 必须指定用于绑定到新 VPN 虚拟服务器的 SSL 证书密钥名称。此 SSL 证书密钥名称必须在脚本执行之前添加到 NetScaler 中。

执行以下步骤以向 Citrix Cloud 注册您的网关：

1. 登录 Citrix Cloud。
2. 选择 **资源位置 > 概述**，然后单击 **网关**。
3. 在 **选择网关** 类型中，选择 **Secure Private Access 的网关**。

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



1. 输入要向 Citrix Cloud 注册的网关的 FQDN。
2. 单击 **生成元数据**。您也可以通过单击 **重新生成元数据** 来重新生成元数据。

   - 将元数据复制到剪贴板中。
   - 与位于本地环境中的 NetScaler Gateway 建立安全外壳 (SSH) 连接。此连接使您能够在 NetScaler 设备上远程运行命令和脚本。
   - 成功连接到 NetScaler Gateway 后，运行以下命令：

     ```
     python3 /var/spa/scripts/spa_registration.py <copied metadata>
     ```

   - 将 `<copied metadata>` 替换为您之前复制的实际元数据。

     脚本会生成一个 8 位数的注册码。此代码对于注册过程至关重要。

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

3. 在 **向 Citrix Cloud 注册** 部分输入 8 位数代码。
4. 单击 **Validate**。

   如果代码无效，将显示警告消息。如果验证成功，将显示 **Register** 按钮。
5. 单击 **Register**。
6. 返回脚本执行窗口。系统将进入下一步，并提示您输入以下详细信息以完成配置。

   - 指定用于 VPN 虚拟服务器的 IP 地址。
   - 要与 VPN 虚拟服务器关联的 SSL 证书密钥名称。

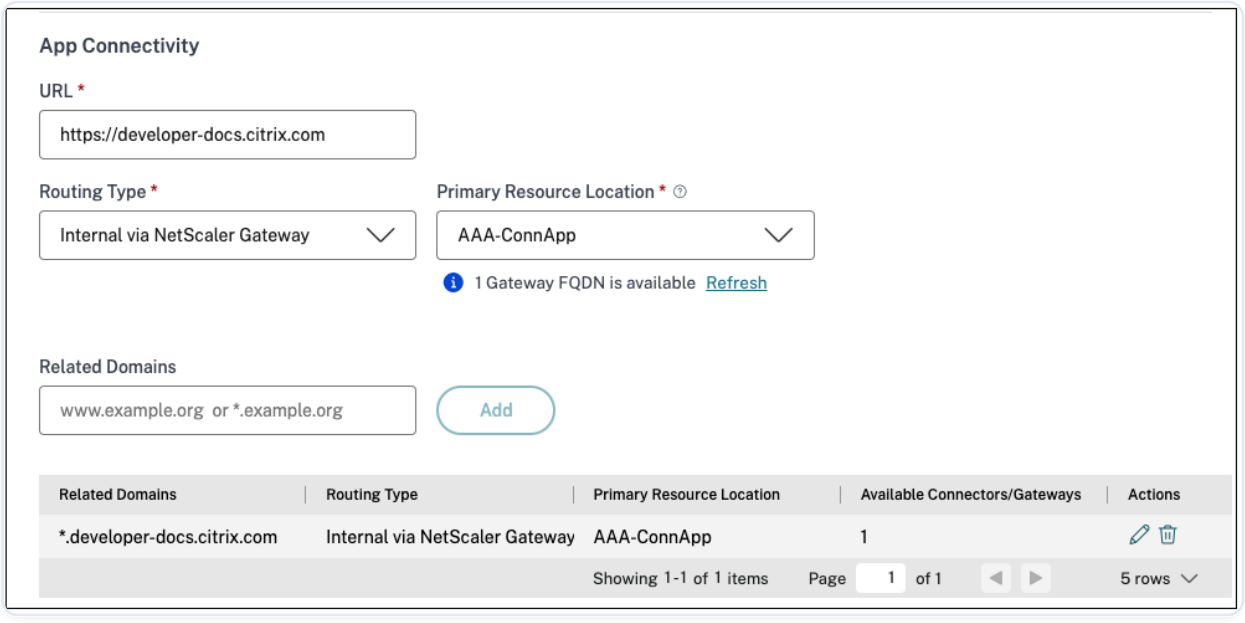
您现在可以通过本地 NetScaler 配置应用程序的路由。

通过本地 NetScaler Gateway 启用数据流量路由

执行以下步骤以启用通过本地 NetScaler Gateway 的数据流量路由。

1. 配置应用程序。有关详细信息，请参阅以下主题：

   - 支持企业 Web 应用程序
   - 无代理访问企业 Web 应用程序
   - 支持软件即服务应用程序
   - 支持客户端-服务器应用程序
2. 在 **App Connectivity** 部分中，您可以定义应用程序域的路由首选项，指定流量是必须通过外部路由还是通过内部路由，即通过 Citrix Connector™ Appliance 或通过本地 NetScaler Gateway。



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

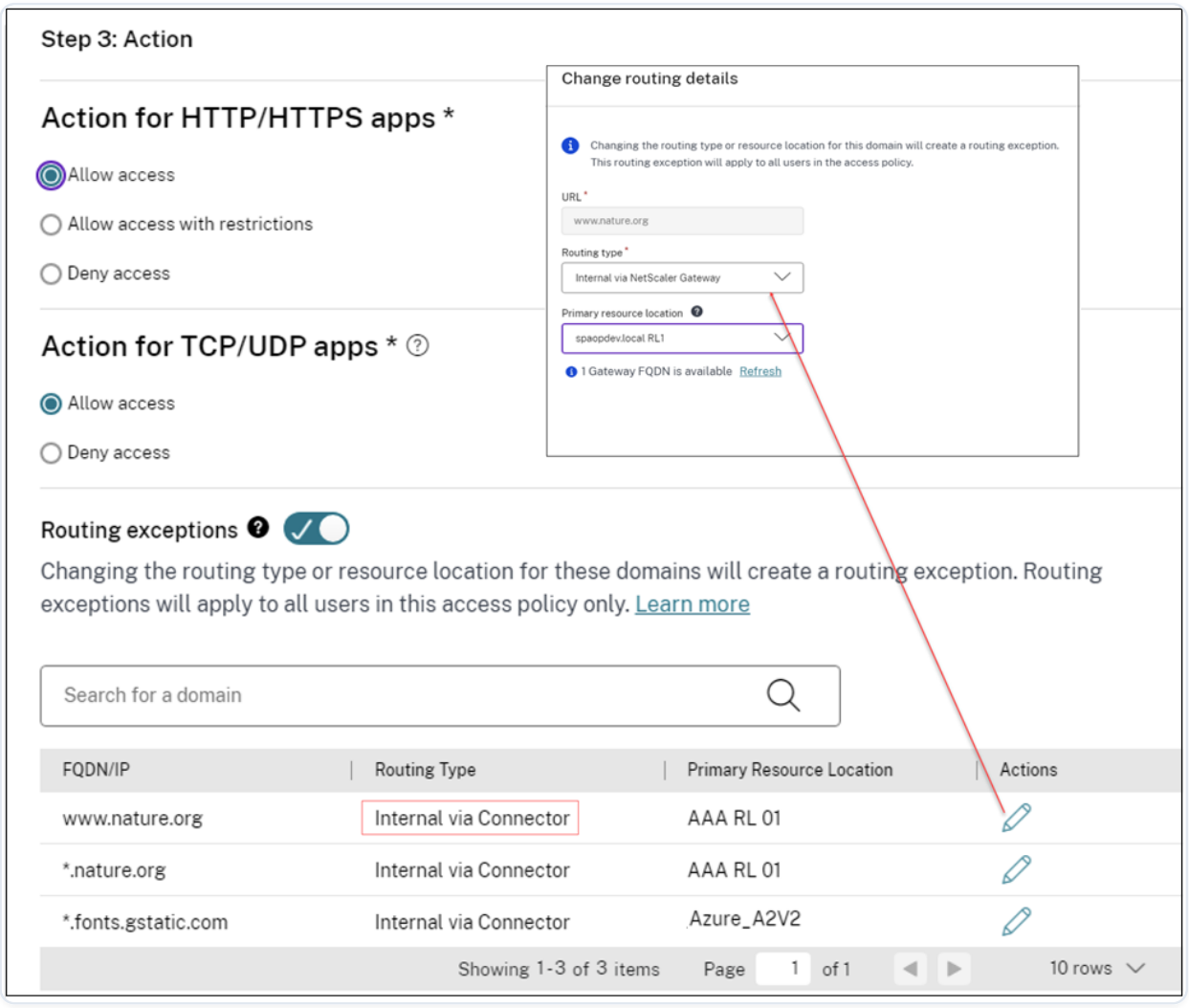
3. 在“**路由类型**”中，选择“**通过 NetScaler Gateway 内部**”。这可确保数据流量通过本地 NetScaler Gateway 路由。您还可以将相关域的路由类型更新为“**通过 NetScaler Gateway 内部**”。
   - 单击“**相关域**”表“**操作**”列中的编辑图标。
   - 在“**路由类型**”中，选择“**通过 NetScaler Gateway 内部**”。
   - 单击“**保存**”。

从访问策略修改路由详细信息

您可以覆盖路由行为，使其根据特定上下文而异。这些上下文可以包括用户组、地理位置、平台和其他相关条件等因素。通过根据上下文修改路由行为，您可以提供优化的用户体验。

执行以下步骤，从访问策略修改通过本地 NetScaler Gateway 的数据流量路由。

1. 创建或编辑访问策略。有关详细信息，请参阅创建访问策略。



2. 在“**步骤 3: 操作**”页面中，启用“**路由例外**”切换。“**路由例外**”切换允许您编辑访问策略中添加的应用程序域的资源位置和路由信息。
3. 单击要修改其路由类型的域旁边的编辑图标。

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

4. 在“**路由类型**”中，选择“**通过 NetScaler Gateway 内部**”。
5. 单击“**保存**”。

限制

- 支持的 NetScaler Gateway 部署类型 - 混合数据路径目前仅支持高可用性设置的环境。
- 回退机制 - 在当前版本中，没有故障转移或回退机制可以在本地网关发生中断或不可用时自动将流量重定向到云基础设施。
- 当前版本中，混合数据路径不支持以下功能：
  - 应用程序发现
  - 策略建模
  - 会话策略
  - 可观测性
- 运行 `installns` 脚本安装 NetScaler 版本时，会创建 /var/spa/scripts/ 文件夹。此文件夹在新部署的 NetScaler VPX 实例上不存在，必须通过安装过程创建。有关更多信息，请参阅以下主题：
  - 升级 NetScaler 独立设备
  - 升级高可用性对

Secure Private Access 注册脚本问题

由于某些内置命令的配置问题，Secure Private Access 注册脚本无法直接在 Azure 上新部署的 VPX 实例上运行。要解决此问题，请按照以下步骤操作：

- 在 Azure 上预配新的 VPX 实例。
- 不要添加任何新配置。
- 使用命令 `set system user nsroot <your-password>` 为 nsroot 用户设置新密码。此步骤很重要，因为在运行 `clear config` 命令后，预配期间创建的自定义用户将被删除。您可以使用 nsroot 和此新密码访问 NetScaler。
- 使用命令 `save config` 保存配置。
- 检查 `show cache policylabel` 的输出。它必须为空。
- 运行命令 `clear config basic` 并键入 Y。
- 再次检查 `show cache policylabel` 的输出。它必须显示 _reqBuiltinDefaults 作为标签。

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

```
show cache policylabel



Label Name: _reqBuiltinDefaults

Evaluates: REQ

Number of bound policies: 3

Number of times invoked: 02)  Label Name: _resBuiltinDefaults

Evaluates: RES

Number of bound policies: 8

Number of times invoked: 03)  Label Name: _httpquicReqBuiltinDefaults

Evaluates: HTTPQUIC_REQ

Number of bound policies: 3

Number of times invoked: 04)  Label Name: _httpquicResBuiltinDefaults

Evaluates: HTTPQUIC_RES

Number of bound policies: 8

Number of times invoked: 0Warning: Feature(s) not enabled [IC]
```

- 如果在命令输出中没有看到 _reqBuiltinDefaults，请联系 Citrix 支持。
- 配置 SNIP、SSL 证书密钥和 DNS 名称服务器。
- 使用命令 `save config` 保存配置。
- 再次运行 Secure Private Access 注册脚本。

发现网络中的应用程序、域或 IP 地址

应用程序发现功能可帮助管理员了解组织中正在访问的外部和内部应用程序（HTTP/HTTPS 和 TCP/UDP 应用程序）。此功能可发现并列出所有已发布或未发布的域/IP 地址。因此，管理员可以

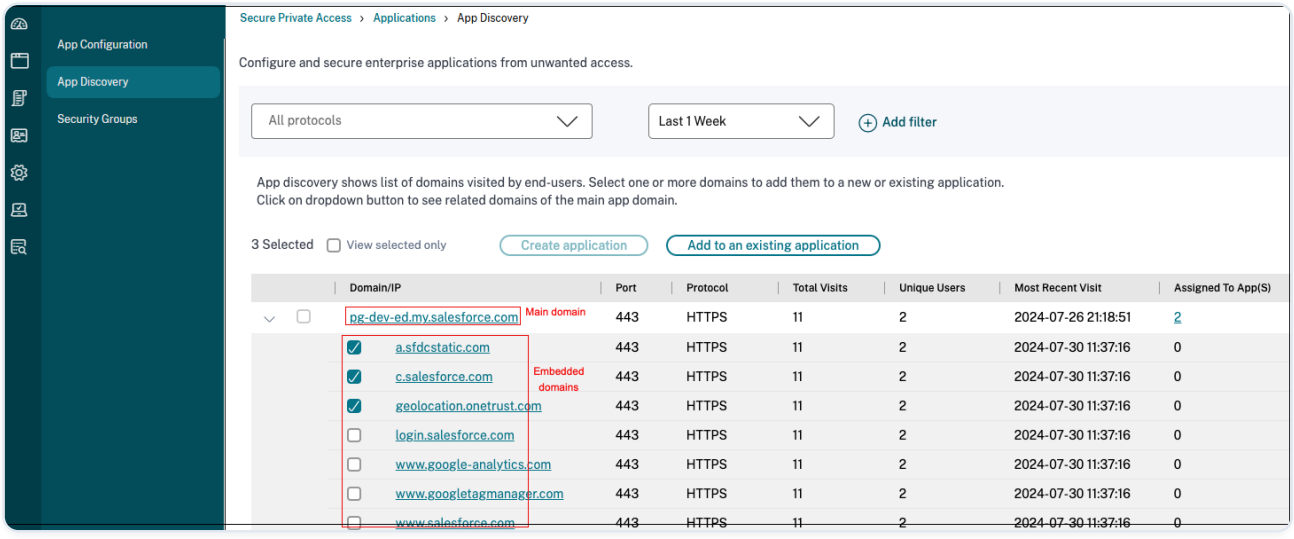
© 1997–2026 Citrix Systems, Inc. All rights reserved.

查看正在访问哪些域/IP 地址、由谁访问，并决定是否将其发布为应用程序，从而为这些用户提供访问权限。

应用程序发现功能为管理员提供以下功能：

- 提供对最终用户访问的内部或外部域/IP 地址的可见性。
- 全面了解所有类型的访问应用程序（HTTP、HTTPS、TCP 和 UDP）。支持所有访问方法，即通过 Citrix Enterprise Browser™、Secure Access Agent、直接访问或从商店访问。
- 显示最终用户访问的已发布或未发布的域/IP 地址。
- 显示主域及其底层嵌入域，这些域在发布通过 Citrix Enterprise Browser 访问的应用程序时需要配置为相关域。
- 以树状结构显示嵌入域。管理员可以单击主域旁边的展开符号 (**>**) 以查看嵌入域。
- 如果主域或嵌入域（HTTP/HTTPS）或目标 IP 地址（TCP/UDP）未与应用程序关联，则使管理员能够创建新应用程序或将这些域添加到现有应用程序。

下图显示了一个示例“**应用程序发现**”页面。“**应用程序发现**”页面允许根据协议（HTTP/HTTPS、TCP/UDP）以及域/IP 地址和端口号筛选域。它还显示了最终用户访问的未发布（未分配给任何应用程序）域。您可以看到一个主域，其下方有一个嵌入域的下拉列表。在发布应用程序时，这些域必须配置为相关域。



注意：

- 嵌入域仅在主域下分组，仅适用于通过 Citrix Enterprise Browser 访问的 HTTP/HTTPS 应用程序。TCP/UDP 域不分组在一个主域下。
- 嵌入域的分组仅适用于从 Citrix Enterprise Browser（v119 及更高版本）访问的应用程序。

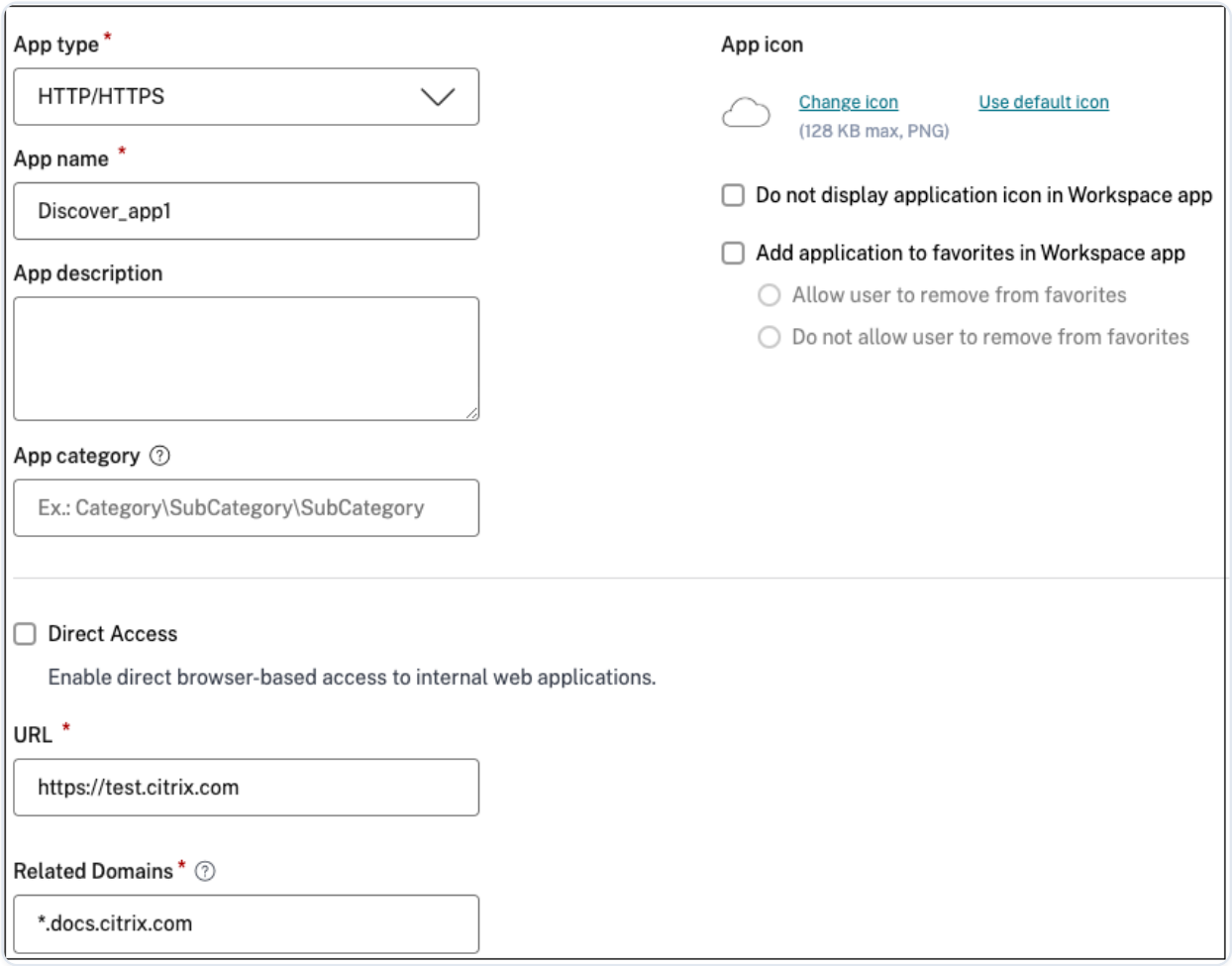
© 1997–2026 Citrix Systems, Inc. All rights reserved.

新环境中的内部域应用程序发现

如果您正在设置新的 Secure Private Access 环境并希望了解要配置的应用程序，则可以使用应用程序发现功能。此功能可发现并列出最终用户访问的所有域/IP 地址，以便您可以将其配置为应用程序。在设置 Secure Private Access 环境时，请按照以下步骤启用应用程序发现功能：

- 要发现内部 Web 应用程序，请在 Secure Private Access 中配置应用程序，并指定属于要发现的应用程序的域/子域的通配符相关域。

  例如，如果要发现域为 citrix.com 的所有应用程序，请创建应用程序，并将相关通配符域设置为 `*.citrix.com`。为了完成应用程序配置，请将任何测试 URL 添加为主 Web 应用程序 URL 部分。



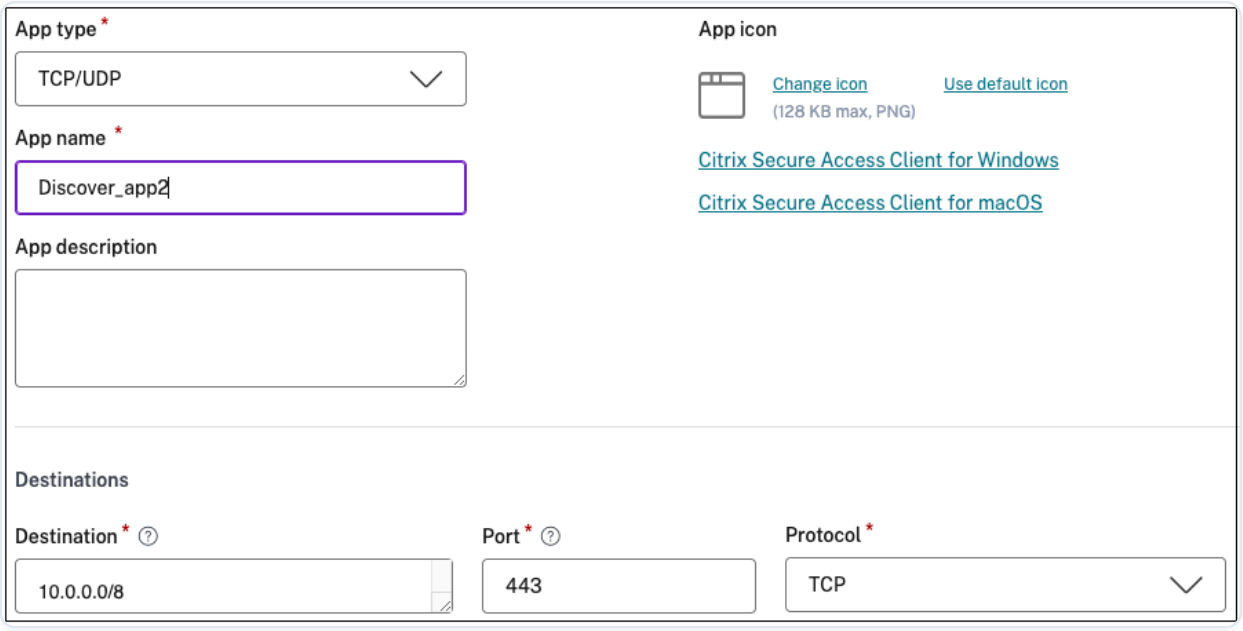
  Web 应用程序 URL: `https://test.citrix.com/` 相关域: `*.citrix.com`

- 对于内部 TCP/UDP 应用程序，请在 Secure Private Access 中配置应用程序，并指定子网以及 TCP/UDP 协议和端口范围（输入 `*` 以包含整个范围）。这允许从 Citrix Secure Access 代理发现所有 TCP 和 UDP 应用程序。例如，如果要发现子网 10.0.0.0/8 中的所有应用程序，请使用以下详细信息配置应用程序：示例：10.0.0.0/8：

  端口: (*)

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

协议: TCP



- 创建应用程序后，您还必须定义允许访问具有已配置域和 IP 子网的应用程序的用户。创建访问策略，并将用户分配给您希望允许访问已创建应用程序中配置的 FQDN/IP 地址的用户。这些可以是初始测试用户集，也可以是您最初希望授予访问权限的有限数量的用户。
- 创建应用程序和相应的访问策略后，用户可以继续从 Citrix Workspace 应用程序访问应用程序并访问不同的域。最终用户访问的所有 FQDN/IP 地址都将开始显示在应用程序发现页面中。

注意：

- 在几天/几周内发现并识别了大多数应用程序后，我们建议删除最初创建的应用程序，以便通过通配符域和 IP 子网授予的更广泛访问权限可以关闭，并且只允许通过新应用程序访问已发现的特定应用程序 URL 和 IP 地址。
- 在应用程序名称中添加前缀 `Discover`，以指示这是一个特殊的应用程序配置，用于启用发现监视和报告。此命名有助于您识别以删除通配符域或 IP 子网或两者，这样您就可以在几周或一个月后将整体应用程序访问区域缩小到特定的 FQDN 和 IP/端口组合。
- 要访问 TCP/UDP 应用程序，用户必须使用 Citrix Secure Access 代理。根据应用程序的域和子网配置监视来自各种访问方法的应用程序访问，并在 **应用程序发现** 页面中报告。
- 即使您已移除发现的应用程序，此功能仍会继续发现用户访问的域/IP 地址。因此，您可以随时返回到 **应用程序发现** 页面，查看正在访问的内容以及是否有任何新发现的域/IP 地址需要配置为应用程序。

有关添加域、FQDN 或 IP 地址的详细信息，请参阅以下主题。

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

- 支持企业 Web 应用程序
- 支持软件即服务应用程序
- 支持客户端-服务器应用程序

从应用程序发现页面创建应用程序

要从 **应用程序发现** 页面为嵌入式域或未发布的域创建应用程序，请执行以下步骤：

1. 导航到 **应用程序 > 应用程序发现**。
2. 从列表中选择一个域。如果该域包含嵌入式域，请单击主域旁边的展开符号 (**>**) 并选择嵌入式域。

   注意：

   - 您不能选择属于不同协议的域来创建应用程序。当您选择属于不同协议的域时，将显示错误消息。
   - 如果某个域已与应用程序关联，则不能再次选择该域来创建应用程序。与该域对应的复选框将显示为灰色，当您将鼠标悬停在该复选框上时，将显示一个工具提示。
   - 您不能选择并将分组在不同主域下的嵌入式域添加到应用程序。应用程序发现功能仅允许将分组在单个主域下的嵌入式域添加到应用程序。如果选择了来自不同主域的嵌入式域并将其添加到同一应用程序，则会显示错误消息。

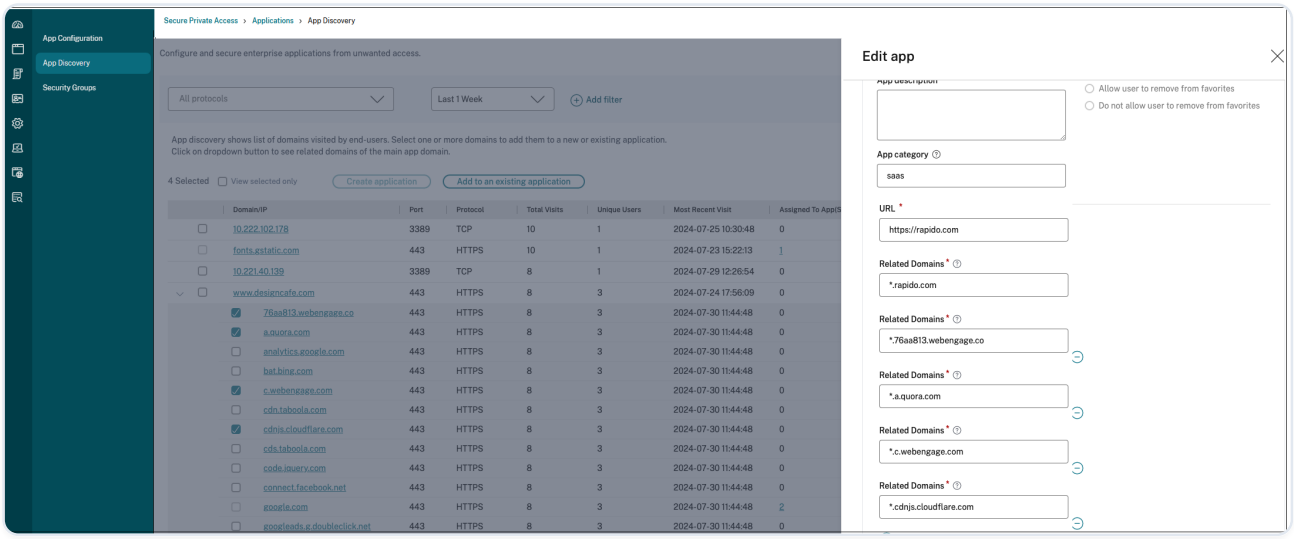
3. 单击 **创建应用程序**。有关创建应用程序的详细信息，请参阅 支持企业 Web 应用程序、支持软件即服务应用程序 和 。

更新现有应用程序

要将域添加到现有应用程序，请从列表中选择该域。如果该域包含嵌入式域，请单击主域旁边的展开符号 (**>**) 并选择嵌入式域。

1. 选择必须添加到应用程序的嵌入式域。
2. 单击 **添加到现有应用程序**。
3. 在 **应用程序** 中，选择要添加这些域的应用程序。
4. 单击 **获取应用程序详细信息**。
5. **相关域** 字段在单独的行中显示您之前选择的所有嵌入式域。
6. 单击 **完成**。

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



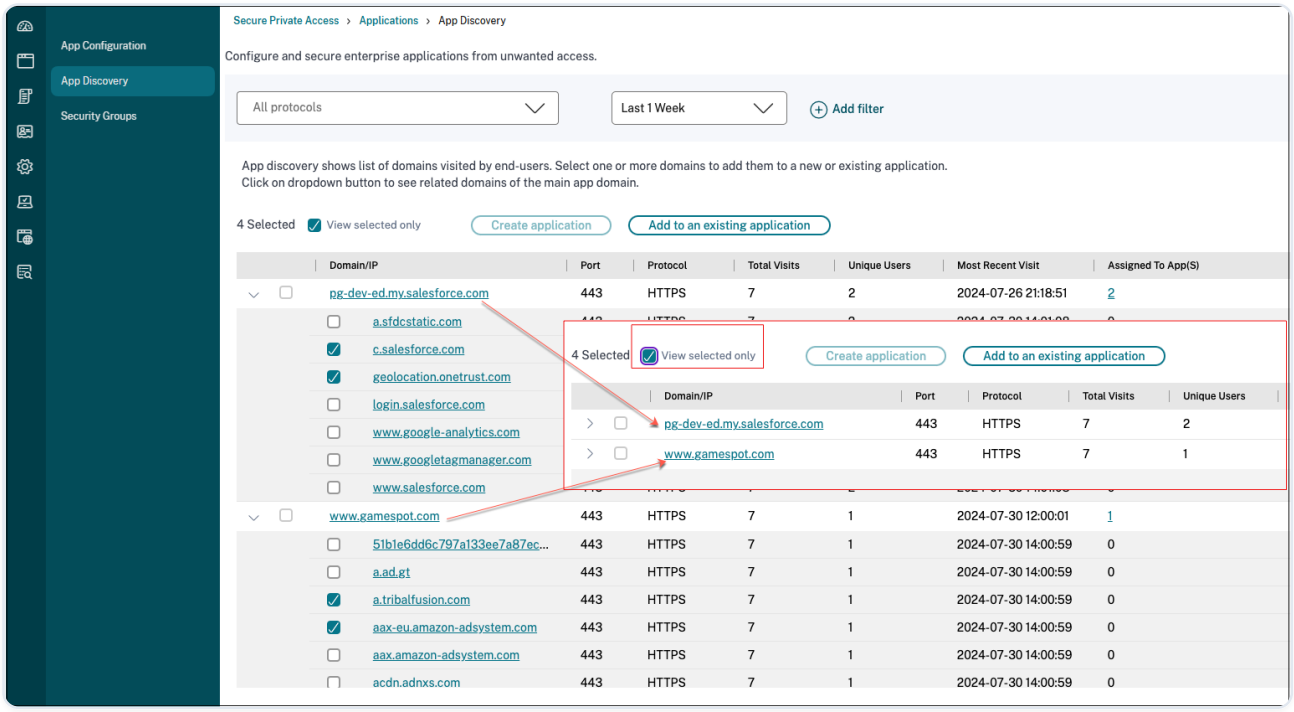
注意：

- 您只能将 TCP/UDP 目标 IP 地址添加到现有 TCP/UDP 应用程序。应用程序字段仅列出系统中配置的 TCP/UDP 应用程序。
- 您可以选择现有的 HTTP/HTTPS 或 TCP/UDP 应用程序来添加协议为 HTTP/HTTPS 的域（主域、单个条目或嵌入式域）。
- 您不能选择已与应用程序关联的域。

查看所有选定的嵌入式域

选择域后，您可以单击 **仅查看选定项** 复选框，然后继续创建或更新应用程序。此外，如果应用程序发现页面上的 FQDN/IP 地址列表跨多个页面，您可以使用 **仅查看选定项** 复选框来查看您已选择用于创建或更新应用程序的所有主域和嵌入式域。选中此复选框时，将显示所有选定嵌入式域的主域。

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



已知限制

- 尽管 Secure Private Access 控制板（**按总访问量排名的热门发现应用程序**图表）中提供了**创建应用程序**和**添加到现有应用程序**选项，但建议您从**应用程序发现**页面（**应用程序 > 应用程序发现**）创建或更新应用程序。这是因为，当您从控制板添加或更新应用程序并取消操作时，页面会重新加载，从而导致所有设置重置。
- 有时，您可能会注意到主域旁边有展开符号 (>)，但未针对该特定 FQDN 获取嵌入式域。此问题可能在以下情况下发生：
  - 由于某些用户访问限制，主网页加载错误。
  - 阻止网页加载的错误。
  - Citrix Enterprise Browser 缓存嵌入式域资源，导致无法从源获取嵌入式域。

基于上下文的应用程序路由和资源位置选择

配置应用程序时，应用程序 URL 和相关域会分配给路由类型和资源位置。这在应用程序配置期间完成。此应用程序路由和资源位置配置随后适用于所有有权访问该应用程序的用户。但可能存在以下情况：

- 管理员希望针对不同用户以不同方式路由同一应用程序。例如，内部应用程序 URL 必须针对少数用户进行外部路由，以防止流量路由到 Secure Private Access 服务。
- 需要为不同用户使用不同的资源位置，以将请求路由到最佳数据中心，从而提高性能。

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

现在可以使用路由例外在访问策略中完成此操作。访问策略中的路由例外配置允许管理员根据用户上下文编辑每个 URL 或资源位置的内部路由类型。由于此设置位于访问策略中，因此它仅适用于属于该访问策略的用户。

您还可以使用 **会话策略** 动态路由整个会话。有关详细信息，请参阅 将内部企业用户直接路由到后端应用程序。

注意：

如果访问策略中存在路由和资源位置配置，则它会覆盖应用程序配置。

以下示例演示了路由例外用例。

- 基于上下文的路由
- 基于用户上下文的资源位置选择
- 将内部企业用户直接路由到后端应用程序

用例：基于上下文的路由

场景：

- A 组用户：ABC 公司的员工，他们通过内部路由的 Secure Private Access 访问 Outlook 应用程序和 Microsoft Teams 应用程序。
- B 组用户：与 ABC 合作的第三方公司的员工。他们通过 Secure Private Access 访问某些应用程序（不包括 Outlook）。他们也有自己的 Outlook 应用程序，通过互联网访问，并且不希望通过 Secure Private Access 路由其 Outlook 流量。

问题：

- B 组用户登录 Secure Access Agent 以访问 ABC 应用程序。
- 他们通过本机浏览器访问 Outlook 的请求被路由到 Secure Private Access，导致访问被拒绝。
- Outlook 应用程序的目标域对于 A 组和 B 组用户都是相同的。
- 访问策略仅允许 A 组用户访问，导致 B 组用户尝试启动 Microsoft Teams 或 Outlook 时被拒绝访问。
- 由于此路由问题，B 组用户无法访问其公司 Outlook。

解决方案：

ABC 公司管理员可以进行以下配置更改来解决此问题：

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

1. 专门为访问 Office 365 应用程序的 B 组用户定义新的访问策略。
2. 在访问策略中，启用**路由例外**选项。

   管理员可以查看与访问策略关联的所有内部应用程序的所有 URL 和相关域的列表。
3. 对于所有 Office365 应用程序 URL，将路由配置为在外部进行。

   这确保了 B 组用户访问其 Outlook 应用程序的请求通过互联网路由，从而绕过 Secure Private Access。

   通过实施这些更改，B 组用户可以通过互联网访问其公司 Outlook 应用程序，而无需通过 Secure Private Access 路由，同时仍可根据需要访问其他 ABC 应用程序。

用例：基于用户上下文的资源位置选择

场景：

- XYZ 公司：它有两组用户，分别位于美国东海岸和美国西海岸。
- 数据中心：两个数据中心，一个在东海岸，一个在西海岸，都托管着相同的 Jira 应用程序。
- 目标：管理员希望根据用户上下文（地理位置、网络位置、用户名和用户组）将最终用户的访问请求路由到选定的资源位置，以确保最佳性能和路由。

解决方案：

1. 编辑与 Jira 应用程序关联的访问策略，以适应新的路由要求。
2. 在访问策略中，启用“**路由例外**”选项。
3. 根据用户上下文修改资源位置。

管理员可以确保用户请求根据其上下文路由到最佳数据中心，从而提高性能并有效管理公司中所有用户的路由。

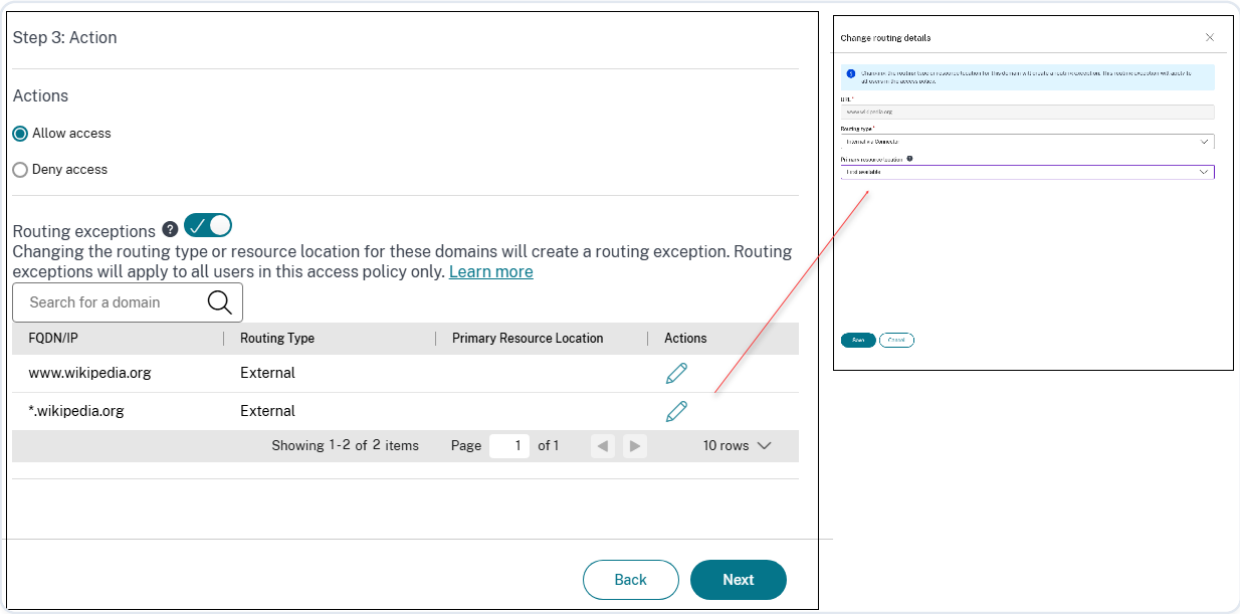
更改路由类型或资源位置的步骤

1. 创建或编辑访问策略。有关详细信息，请参阅创建访问策略。
2. 在“**步骤 3: 操作**”页面上，通过滑动“**路由例外**”切换开关来启用上下文路由域配置。 “**路由例外**”切换开关允许您编辑访问策略中添加的应用程序的域的资源位置和路由信息。

   - **当开关处于“开”状态时：** 将以表格形式显示所有应用程序的 URL 和相关域的列表，以及它们的全局路由和资源位置配置。此列表包含访问策略中添加的所有应用程序的 URL 和相关域。您可以单击域旁边的编辑图标来修改其资源位置和路由类型。此路由例外仅适用于访问策略中的所有用户。

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

- **当开关处于“关”状态时：** 域的现有路由例外将被移除且不再适用。最终用户仅根据应用程序设置期间的全局配置进行路由。



3. 单击要修改路由类型的域旁边的编辑图标。
4. 在 **路由类型** 中，修改路由类型：
   - **内部：** 流量通过连接器设备流动。
     - 对于 Web 应用程序，流量在数据中心内流动。
     - 对于 SaaS 应用程序，流量通过连接器设备路由到网络外部。
   - **内部 – 绕过代理：** 域流量通过 Citrix Cloud Connector™ 设备路由，绕过在连接器设备上配置的客户 Web 代理。
   - **外部：** 流量直接流向互联网。
   - **通过 Google 安全网关外部：** 流量通过 Google 安全网关流向互联网。

   注意：

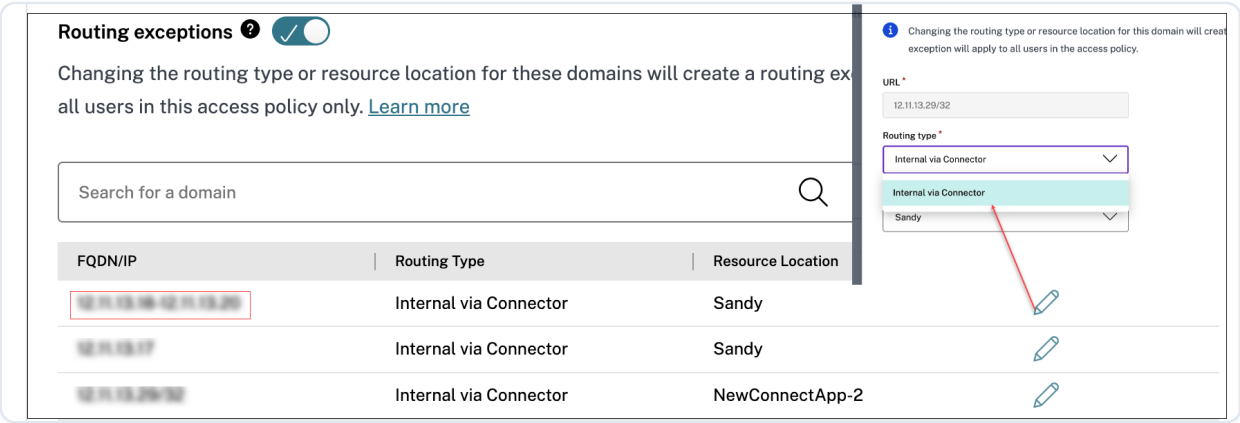
   此路由类型仅适用于在 Secure Private Access 云和混合部署中与 Google Chrome Enterprise Premium 集成的客户的 SaaS 应用程序。

5. 在 **资源位置** 中，如有必要，修改资源位置。此选项仅适用于内部路由的域。

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

注意：

如果应用程序是使用 IP 地址创建的，则无法将路由类型修改为 **外部**，因为在 **路由类型** 列表中仅显示 **通过连接器内部** 选项。您只能修改资源位置。但是，此限制不适用于使用 FQDN 创建的应用程序。



6. 点击**保存**。

注意：

- 您只能更改路由和资源位置，但不能在路由表中添加或删除路由域。
- 如果您从主路由表中删除启用了上下文路由的域，则该域不会从访问策略中的**路由例外**表中删除。这意味着该域的上下文路由配置在访问策略中保持不变。
- 如果您删除启用了上下文路由的应用程序，则该域会从访问策略中的**路由例外**表中删除。这意味着与该应用程序关联的所有上下文路由配置都将从访问策略中删除。
- 当条件满足此访问策略中的用户时，所选的相关域会覆盖默认设置。否则将应用默认路由。
- 如果路由未修改，或者未启用**路由例外**功能，路由将根据主路由表中的默认设置进行（**设置 > 应用程序域**）。

用例：将内部企业用户直接路由到后端应用程序

管理员可以配置会话策略，以将内部企业用户直接路由到后端应用程序，而无需通过 Secure Private Access 隧道传输流量。会话策略根据网络位置和设备状态等因素提供动态路由。有关详细信息，请参阅会话策略。

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

Monitor 中的上下文路由洞察

上下文路由可能导致应用程序路由的动态变化。例如，当用户在公司网络外部时，应用程序可能会通过 Secure Private Access 服务路由，但当用户在内部时，则直接路由到应用程序。为管理员提供这些路由决策的可见性对于排查路由问题至关重要。

DaaS Monitor 中的**应用程序拓扑**页面提供了对通过 Citrix Secure Access 客户端访问的 Secure Private Access 应用程序的路由决策和策略详细信息的全面洞察。这些洞察使管理员能够高效地排查路由问题，从而增强用户体验。

应用程序拓扑页面中捕获了与应用程序路由相关的以下详细信息：

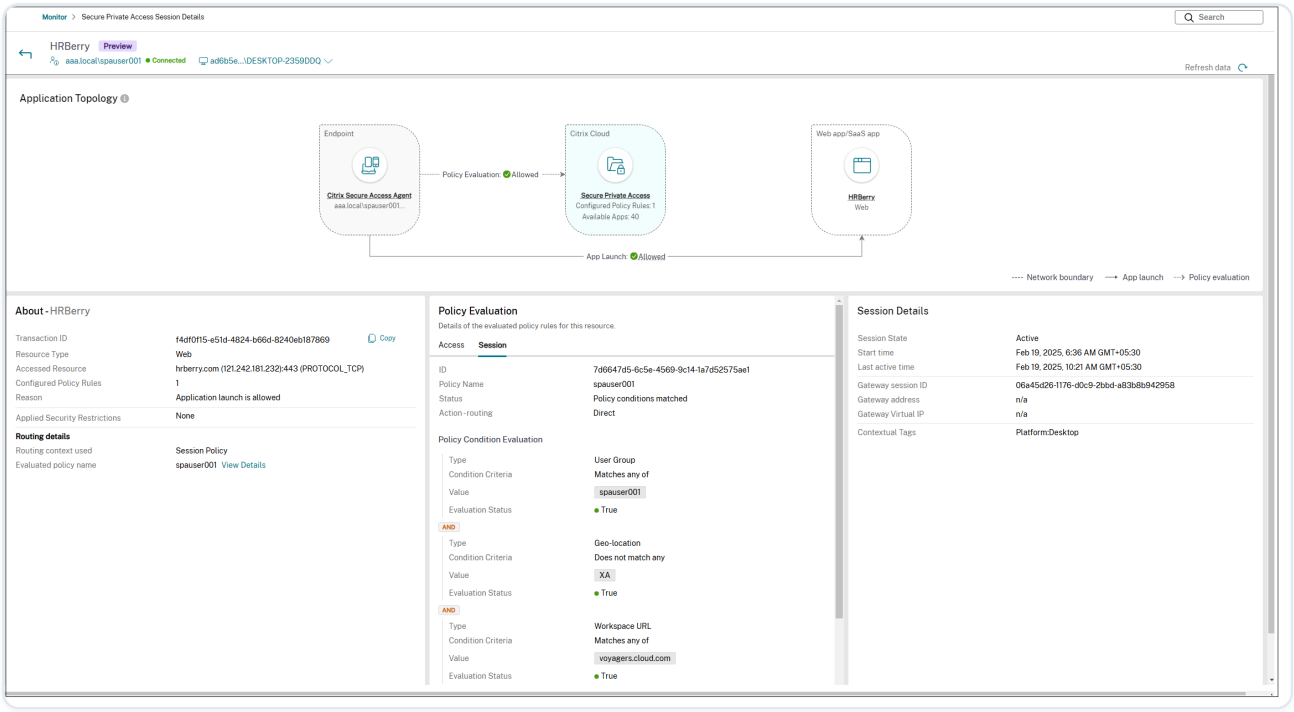
- **路由上下文：** 在**关于**部分中，**路由上下文**字段指定了路由期间应用的策略类型（访问策略、会话策略或应用程序域）。路由上下文有助于识别影响路由决策的优先级层次结构（访问策略 > 会话策略 > 默认应用程序配置）。

  对于会话策略，**查看详细信息**链接提供了有关会话策略的更多详细信息。
- **操作路由：**“**策略评估**”部分中的“**操作路由**”字段显示用户请求通过 Secure Private Access 服务所采用的路由路径（**直接、通过连接器内部、通过网关内部**）。

> **注意：**
>
> 当应用默认应用程序域（应用程序配置）路由时，“**策略评估**”部分会显示策略详细信息，但“**操作路由**”字段会显示值 **n/a**，因为在此场景中未强制执行任何策略。

下图显示了一个应用程序的拓扑图，其路由类型定义为直接，因此流量不通过 Secure Private Access 服务。

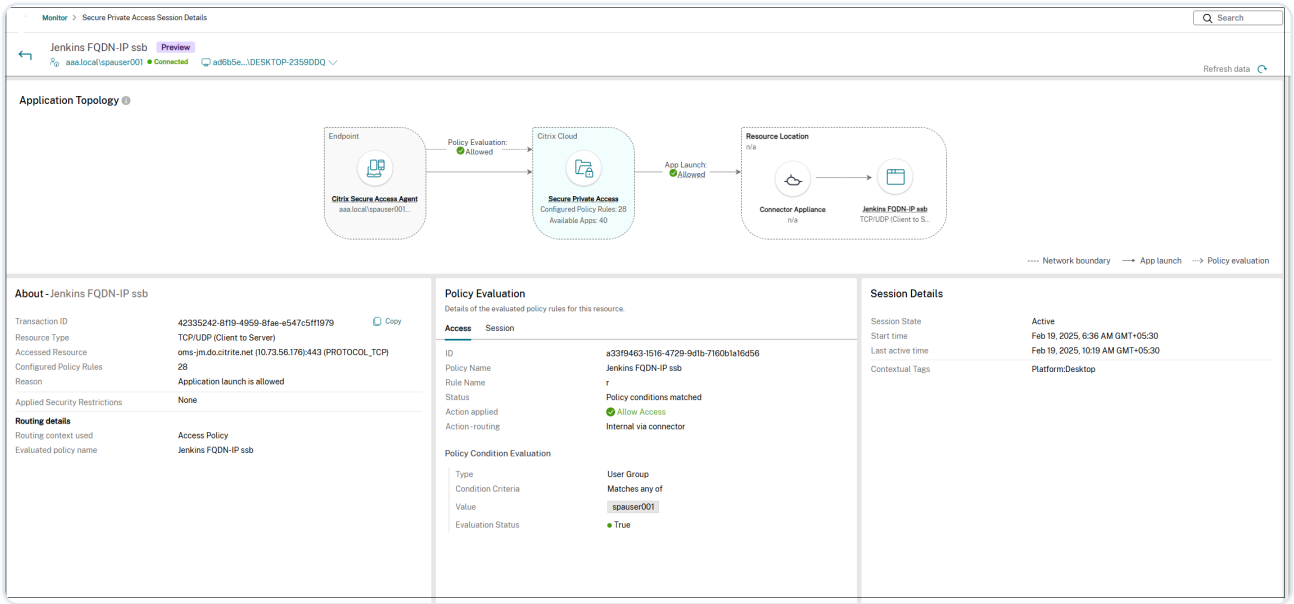
© 1997–2026 Citrix Systems, Inc. All rights reserved.



注意：

对于通过 Citrix Secure Access 客户端隧道传输的 Web 应用程序，拓扑图会显示资源位置名称和连接器名称。

下图显示了一个应用程序的拓扑图，其路由类型定义为通过 Secure Private Access 服务使用连接器进行内部路由。



有关详细信息，请参阅与 DaaS 监视器集成。

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

无缝访问本地局域网资源（打印机、文件服务器）

当员工使用 Citrix Secure Access 客户端从家中或远程位置通过 Secure Private Access 连接时，如果私有 IP 地址范围与已发布的企业应用程序冲突，他们可能会失去访问本地网络资源的能力。Secure Private Access 支持无缝访问本地局域网资源，同时保持与企业资源的安全连接。

例如，如果家用打印机配置的 IP 地址为 192.0.2.0，并且企业应用程序配置的私有 IP 地址范围为 192.0.2.0/30，那么当用户尝试访问打印机时，打印机流量也会通过 SPA 隧道传输，从而导致错误。通过启用本地局域网访问，用户无需断开 Citrix Secure Access 客户端即可通过本地局域网访问打印机。

注意：

- 管理员可以在会话策略中为所有用户或一组用户启用本地局域网访问功能。有关详细信息，请参阅 使用会话策略配置企业网络内的直接路由。
- 如果用户在登录 Citrix Secure Access 客户端时启用本地局域网访问功能，他们可以在连接到 Secure Private Access 的同时访问本地局域网资源，例如家用打印机、网络附加存储 (NAS) 设备。这有助于用户以最小的中断执行基本的本地任务。

重要注意事项

- **为所有用户启用本地局域网访问：** 会话策略按优先级顺序进行评估。如果所有用户都需要本地局域网访问，则必须在每个活动会话策略中明确启用**本地局域网访问**选项。当用户匹配会话策略时，评估将在第一个适用的策略处停止。如果该策略不允许本地局域网访问，则即使后续策略启用了**本地局域网访问**选项，也不会对用户进行评估。
- **Citrix Secure Access 客户端在 Windows 和 macOS 上处理打印机流量的差异：** 适用于 Windows 的 Citrix Secure Access 优先处理本地局域网访问。也就是说，如果打印机的 IP 地址与企业应用程序的 IP 地址冲突，适用于 Windows 的 Citrix Secure Access 客户端可能会将应用程序流量本地发送，而不是通过 Secure Private Access 发送。相比之下，适用于 macOS 的 Citrix Secure Access 客户端可以将打印机流量发送到本地局域网，同时通过 Secure Private Access 隧道传输应用程序流量。
- **定期更新：** 由于本地局域网访问功能是会话特定的，因此对 Windows 筛选器 (WFP) 上的本地局域网设置进行的任何配置更改都会在登录时生效并保持到注销。不支持定期更新。

启用本地局域网访问功能

Secure Private Access 管理控制台：

1. 导航到**策略 > 会话策略**，然后单击“创建会话策略”。

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

2. 创建会话策略。有关详细信息，请参阅 使用会话策略配置企业网络内的直接路由。
3. 确保选择**本地局域网访问**选项。

SPA 控制台中的本地 LAN 访问(/en-us/citrix-secure-private-access/media/spa-session-policy.png)

Citrix Secure Access 客户端应用程序：

1. 在 Citrix Secure Access 客户端窗口中，选择 **允许本地 LAN 访问**。
2. 单击 **连接**。

本地 LAN 访问(/en-us/citrix-secure-private-access/media/spa-local-lan-access.png)

已启用本地 LAN 访问(/en-us/citrix-secure-private-access/media/spa-local-lan-access-enabled.png)

策略建模工具

在管理多个应用程序和访问策略时，管理员可能难以确定最终用户的确切访问结果。例如，用户是否根据所有当前配置被允许或拒绝访问某个应用程序。

策略建模工具位于**访问策略 > 策略建模**下，它根据当前配置为管理员提供对预期应用程序访问结果（允许、受限允许或拒绝）的全面可见性。管理员可以根据设备类型、设备姿态、地理位置、网络位置和商店 URL 等条件检查任何用户的访问结果。管理员还可以评估特定应用程序目标的访问策略。

访问策略建模工具

1. 在 Secure Private Access 控制台中，单击**访问策略**，然后单击**策略建模**选项卡。
2. 策略建模工具用户界面随即出现。
    - 默认选择**所有应用程序**选项卡。此选项卡可用于分析适用于环境中多个用户、用户组或计算机的策略。
    - 要了解策略如何应用于特定的网络目标（例如特定的网站域、IP 地址或网络端口），您必须使用**URL**或**IP/端口**选项卡并输入目标详细信息。

分析一组用户或计算机的策略

1. 选择**用户**或**计算机**选项卡，然后输入以下详细信息。
    - **设备类型：** 选择最终用户的设备类型。（默认选择“桌面”）。
    - **域：** 选择与用户关联的域。

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

- **用户名或用户组：**（仅当您选择了**用户**选项卡时适用）选择要分析其应用程序和关联策略的用户名。
- **计算机名称：**（仅当您选择了**计算机**选项卡时适用）输入要分析其应用程序和关联策略的计算机名称。

2. 要搜索准确结果，请添加确切的用户或计算机条件。
   - 点击**模拟条件。**
   - 选择条件（设备姿态、地理位置、网络位置、用户风险评分和存储 URL），然后选择关联值。
   - 点击 + 号以添加更多条件。
   - 点击**应用。**

分析针对特定目标的策略

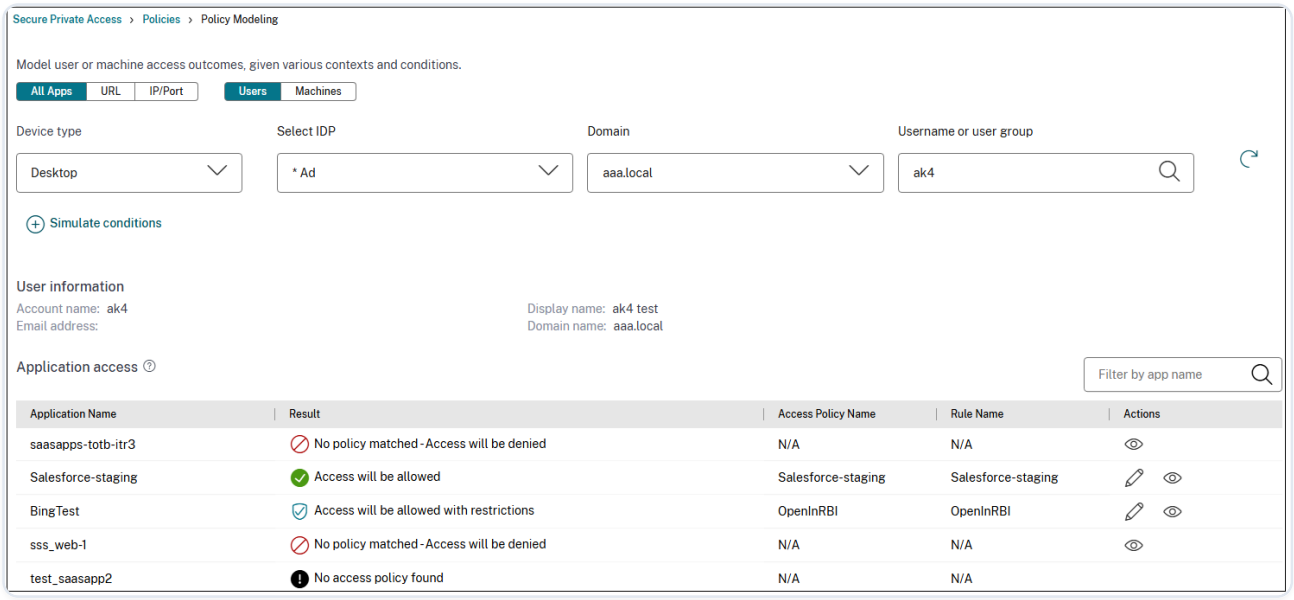
1. 点击用于 Web/SaaS 应用程序的**URL**选项卡，以及用于 TCP/UDP 应用程序的**IP/端口**选项卡。
2. 输入以下详细信息：
   - **URL：** 您要分析其访问策略的应用程序的 URL。
   - **IP:端口：** 您要分析其访问策略的 TCP/UDP 应用程序的 IP 和端口号。您还可以输入主机名，后跟端口号。

   示例：192.0.2.20:443; example.test.net:443
3. 点击**应用。**

应用程序访问部分根据您的搜索显示应用程序列表和关联策略。应用程序旁边会出现一个眼睛图标，表示已发生精确策略匹配或无策略匹配。管理员还可以编辑允许访问或限制访问的应用程序的策略。

下图显示了所有应用程序的策略分析器：

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



下图显示了 Web 应用程序的策略分析器：

Web 应用程序的策略模型(/en-us/citrix-secure-private-access/media/spa-policy-model1.png)

下图显示了针对 TCP 应用程序的策略分析器：

TCP 应用程序的策略模型(/en-us/citrix-secure-private-access/media/spa-policy-model-tcp-app.png)

深入查看访问策略

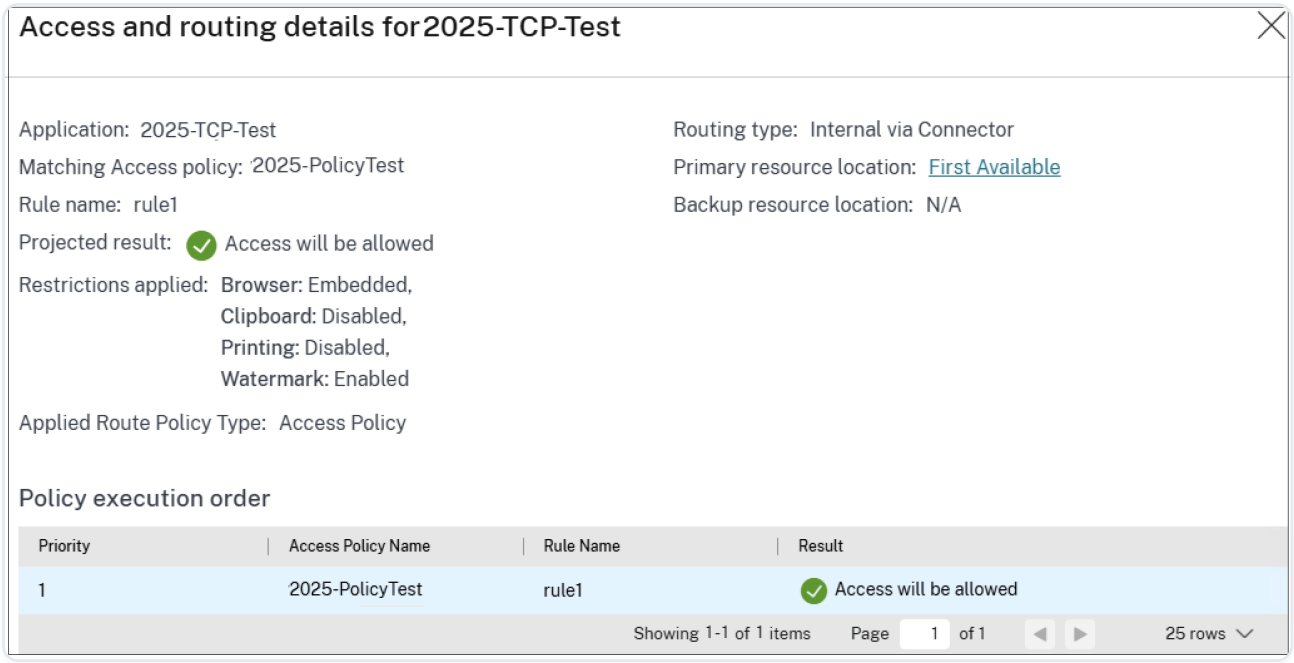
在**应用程序访问**部分中，单击眼睛图标以查看访问和路由详细信息页面。**访问和路由详细信息**页面显示了影响该应用程序访问决策的所有相关策略的完整列表。此页面显示以下信息：

字段	描述
应用程序	应用程序名称。
匹配的访问策略	与应用程序完全匹配或主要匹配的访问策略的名称。
规则名称	与匹配策略关联的特定规则。
预测结果	根据策略评估确定的操作（例如，允许、拒绝、允许但受限制）。
应用的限制	对应用程序强制执行的访问限制（如果有）。
应用的路由策略类型	指示确定应用程序路由行为的策略类型。策略类型为访问策略、会话策略或应用程序域。

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

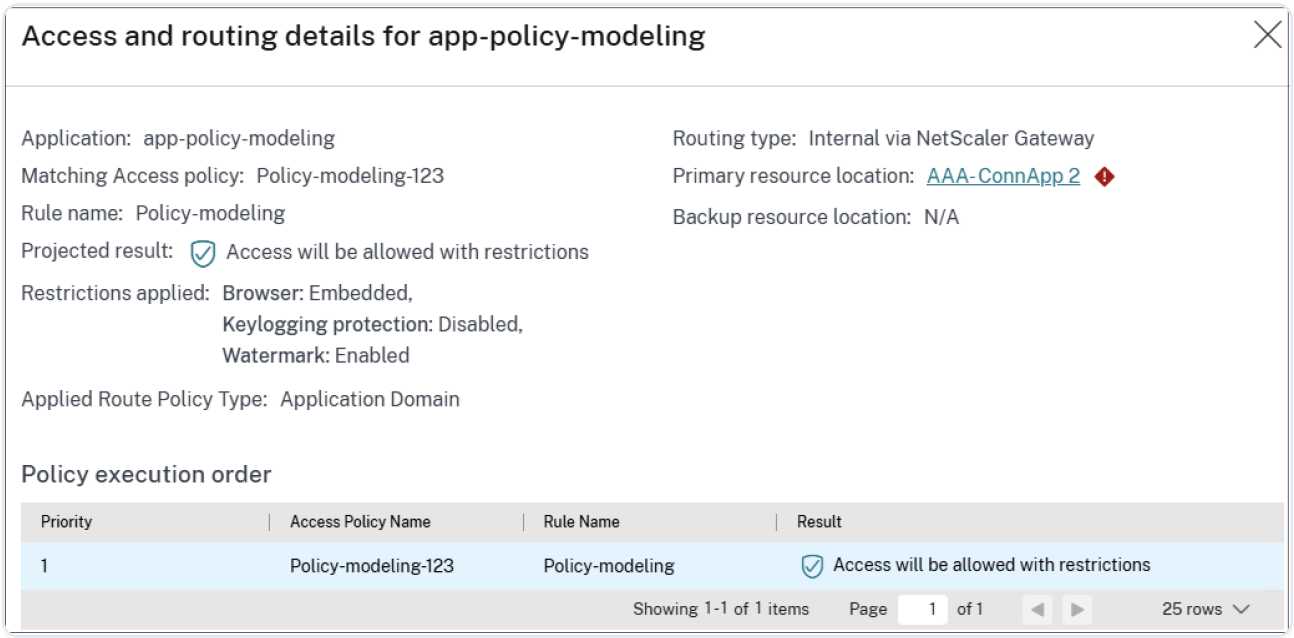
字段	描述
	标识路由决策中的层次结构。优先级顺序为访问策略（最高优先级），其次是会话策略，然后是默认应用程序域（最低优先级）。
路由类型	路由类型详细说明了用户请求通过 Secure Private Access 服务所采用的路径。
	外部 请求直接路由到预期目标。
	通过连接器内部 请求通过连接器路由。
	通过网关内部 请求通过 NetScaler Gateway 路由。此路由类型仅适用于 Citrix Secure Access 客户端支持的混合数据路径。有关详细信息，请参阅 Secure Private Access 服务的混合数据路径。
主要资源位置	与应用程序主要位置关联的名称。
备份资源位置	备份位置的名称（如果已配置）。

下图显示了允许访问的 TCP 应用程序的策略深入分析结果。

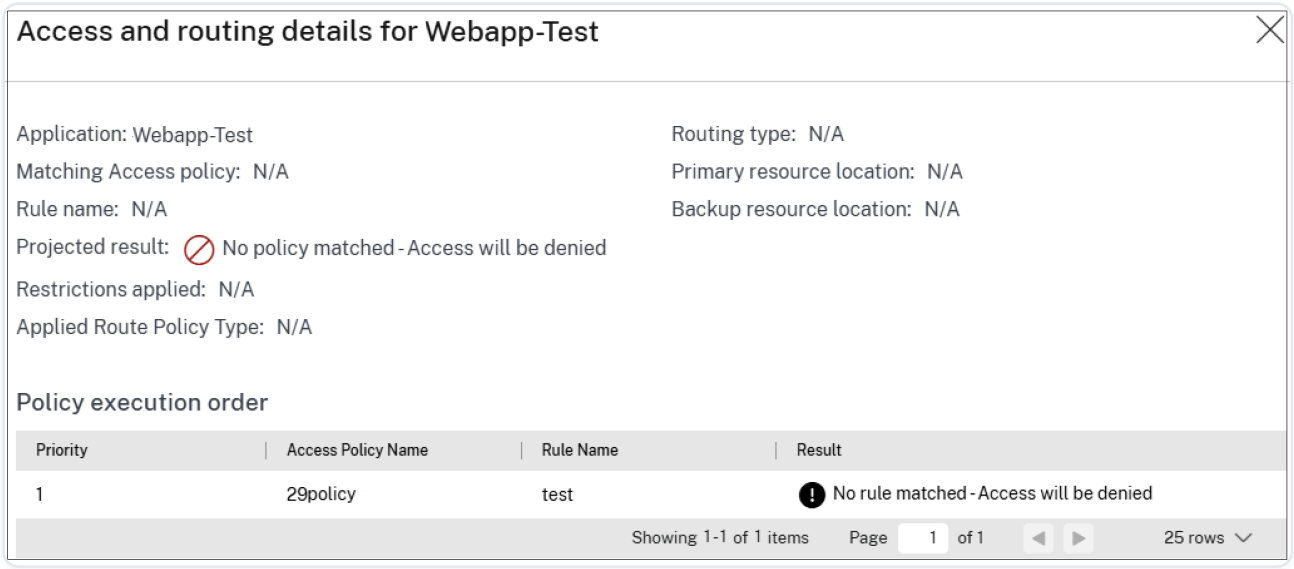


下图显示了允许受限访问的 Web 应用程序的策略深入分析结果。

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



下图显示了拒绝访问的 Web 应用程序的策略深入分析结果：



应用程序导入工具 - 预览

Secure Private Access 管理控制台包含一个文件导入工具，管理员可以使用 CSV 文件或 nsconfig 文件将多个应用程序批量导入系统。此工具对于从传统 VPN 转向 Secure Private Access 等更高级解决方案的组织特别有用。例如，组织可以使用此工具将通过 VPN 交付的应用程序迁移到 Secure Private Access，并转向基于 ZTNA 的架构。批量上传应用程序使组织无需手动配置。

- **CSV 文件：** 您必须确保 CSV 中包含所有相关的应用程序详细信息。这些详细信息包括应用程序名称、路由类型、资源位置以及任何其他必要的配置参数。
- **NetScaler 文件：** 您还可以通过使用预生成的 CSV 文件导入应用程序。此 CSV 文件由一个脚本创建，该脚本从 ns.conf 和 ns.log 文件中解析并提取相关的应用程序配置。脚本生成的 CSV 能够将应用程序配置高效准确地导入 Citrix Secure Private Access 控制台。

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

导入工作原理

以下是管理员在使用基于 CSV 的应用程序导入工具时必须执行的高级步骤：

1. **准备 CSV 文件：** 如果您是手动添加应用程序，请在 CSV 文件中填写应用程序详细信息。有关详细信息，请参阅准备 CSV 文件。
2. **导入 CSV 文件：** 将已完成的 CSV 文件导入 Secure Private Access 控制台。
3. **查看应用程序详细信息：** 查看并验证导入的应用程序数据。
4. **更新路由和资源位置：** 如果需要，查看并更新路由类型和资源位置详细信息。确保指定资源位置中至少有一个连接器处于活动状态。
5. **在“应用程序”页面中查看应用程序：** 在“应用程序”页面中查看导入的应用程序。检查您选择导入的所有应用程序是否已成功导入。

此结构化流程可确保应用程序的彻底迁移和正确配置，以便在 Secure Private Access 环境中实现安全无缝的访问。

准备 CSV 文件

从 Secure Private Access 控制台下载 CSV 文件并添加应用程序详细信息。

1. 导航到 **应用程序 > 应用程序配置**。
2. 点击 **导入应用程序**。
3. 在 **了解如何使用 CSV 和 NetScaler 文件导入** 中，点击 **CSV** 或 **NetScaler**。

   使用 CSV 导入 或 **使用 NetScaler 文件导入** 页面会相应显示。

   - **CSV** - 下载 CSV 文件（CSV 模板）并填写应用程序详细信息。该页面还显示了必须输入的应用程序数据的示例信息。
   - **NetScaler**
     - 下载并保存 Python 脚本到 NetScaler 中的指定文件夹 (/var/spa/scripts)。
     - 以 `python3 ztna-migration.py` 运行脚本，以从 ns.conf 和 ns.log 文件生成 CSV 文件。
     - 生成 CSV 文件后，将其上传以进行导入。

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

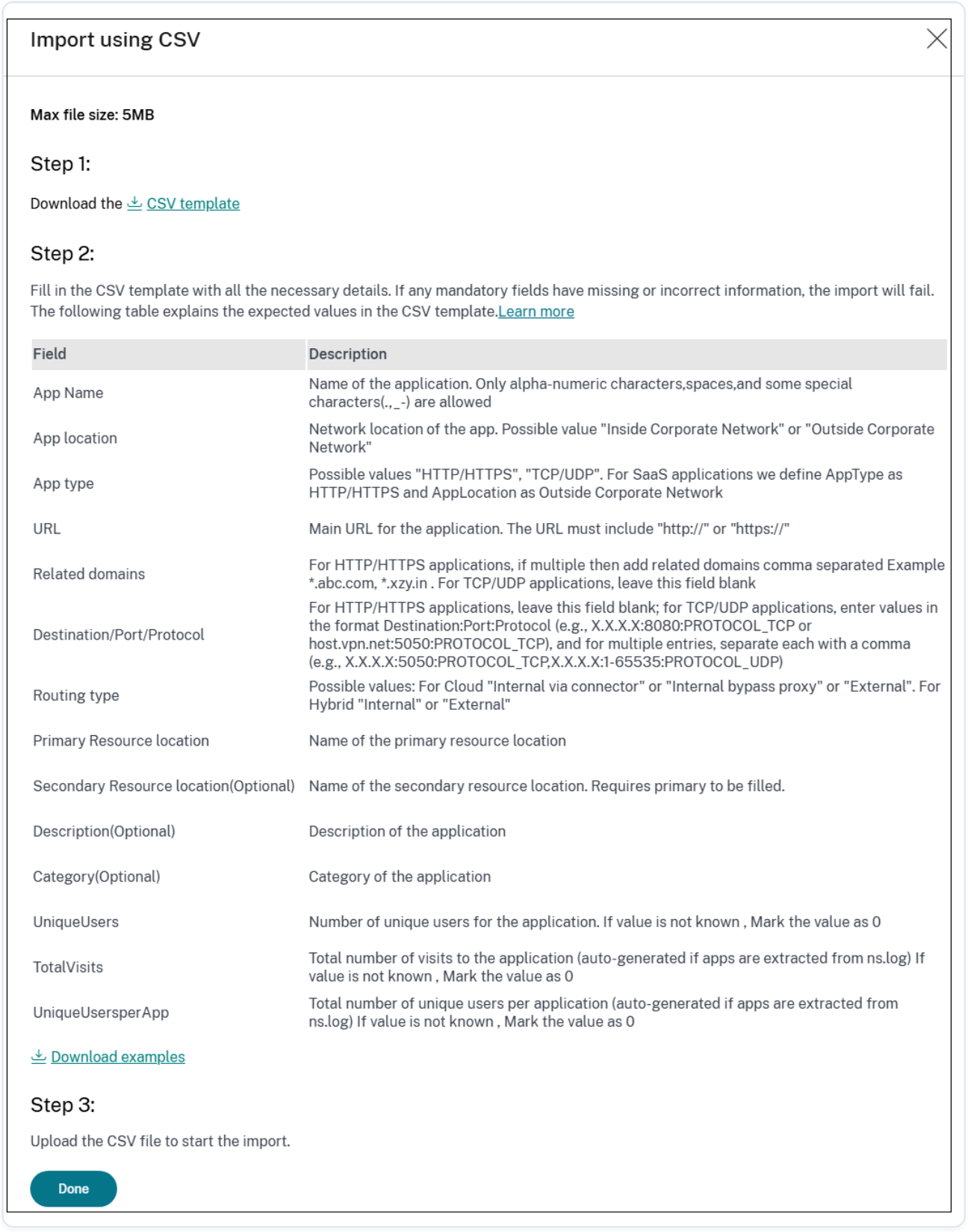
注意：

从 CSV 文件导入大量应用程序时，请分批处理，每批 50 个。上传 CSV 后，选择前 50 个应用程序并完成导入，然后选择接下来的 50 个并重复此操作，直到所有应用程序都导入完成。

点击 **下载示例** 以查看包含数据的示例 CSV 文件。

使用 CSV 文件导入应用程序的指南：

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



Import using CSV

Max file size: 5MB

Step 1:

Download the CSV template

Step 2:

Fill in the CSV template with all the necessary details. If any mandatory fields have missing or incorrect information, the import will fail. The following table explains the expected values in the CSV template.Learn more

Field	Description
App Name	Name of the application. Only alpha-numeric characters,spaces,and some special characters(.,_-) are allowed
App location	Network location of the app. Possible value "Inside Corporate Network" or "Outside Corporate Network"
App type	Possible values "HTTP/HTTPS", "TCP/UDP". For SaaS applications we define AppType as HTTP/HTTPS and AppLocation as Outside Corporate Network
URL	Main URL for the application. The URL must include "http://" or "https://"
Related domains	For HTTP/HTTPS applications, if multiple then add related domains comma separated Example *.abc.com, *.xzy.in . For TCP/UDP applications, leave this field blank
Destination/Port/Protocol	For HTTP/HTTPS applications, leave this field blank; for TCP/UDP applications, enter values in the format Destination:Port:Protocol (e.g., X.X.X.X:8080:PROTOCOL_TCP or host.vpn.net:5050:PROTOCOL_TCP), and for multiple entries, separate each with a comma (e.g., X.X.X.X:5050:PROTOCOL_TCP,X.X.X.X:1-65535:PROTOCOL_UDP)
Routing type	Possible values: For Cloud "Internal via connector" or "Internal bypass proxy" or "External". For Hybrid "Internal" or "External"
Primary Resource location	Name of the primary resource location
Secondary Resource location(Optional)	Name of the secondary resource location. Requires primary to be filled.
Description(Optional)	Description of the application
Category(Optional)	Category of the application
UniqueUsers	Number of unique users for the application. If value is not known , Mark the value as 0
TotalVisits	Total number of visits to the application (auto-generated if apps are extracted from ns.log) If value is not known , Mark the value as 0
UniqueUsersperApp	Total number of unique users per application (auto-generated if apps are extracted from ns.log) If value is not known , Mark the value as 0

Download examples

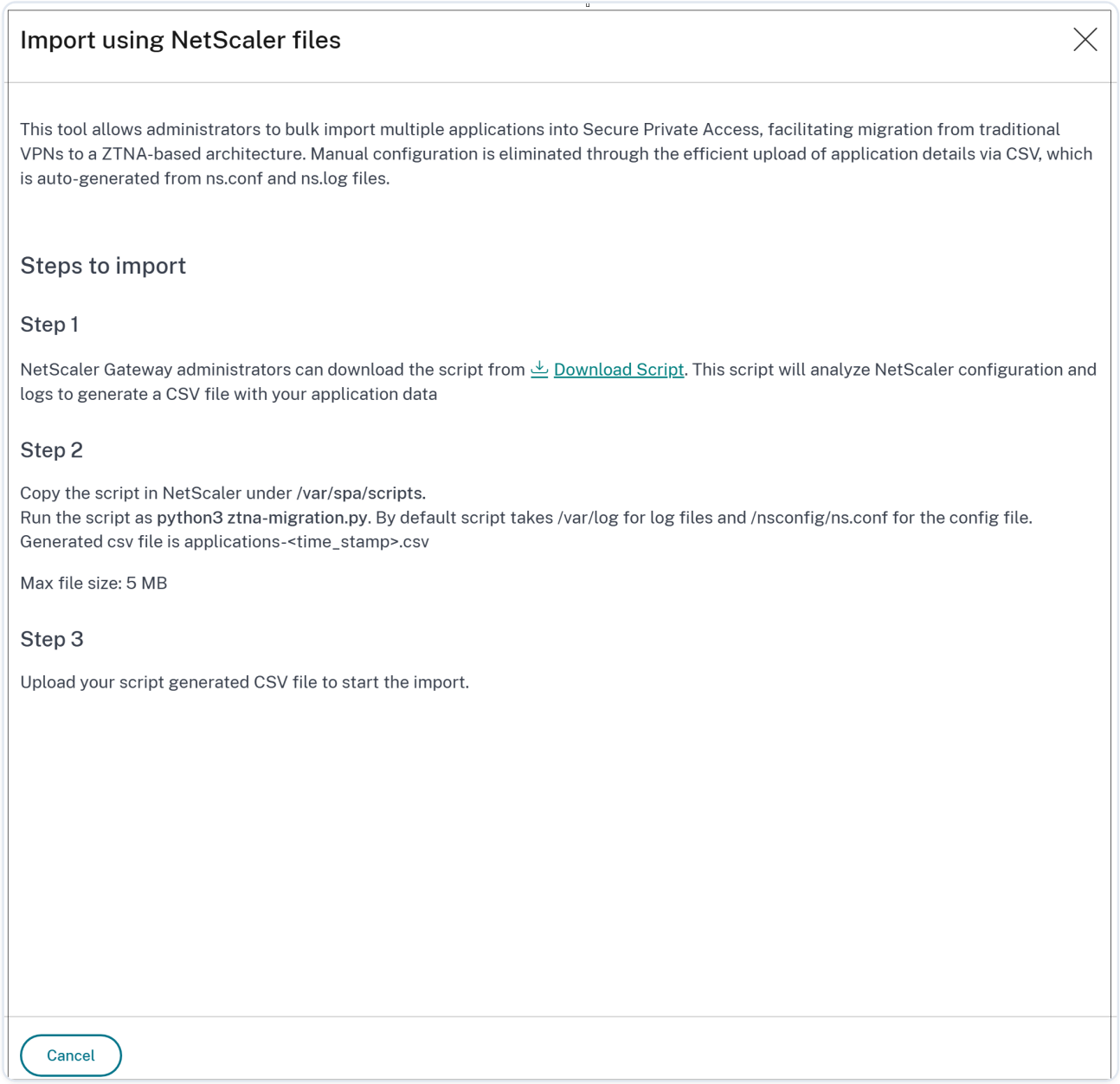
Step 3:

Upload the CSV file to start the import.

Done

使用 NetScaler 文件导入应用程序的指南：

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



CSV 文件中要输入的值

下表提供了手动创建应用程序时，CSV 文件中每列要输入的值的指导原则：

列名	值
应用程序位置	公司网络内部（适用于内部 Web 应用程序、TCP、UDP 应用程序）
	公司网络外部（适用于 SaaS 应用程序）
应用程序类型	必须是以下值之一。
	HTTP/HTTPS

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

列名	值
	TCP/UDP
URL	仅适用于 HTTP/HTTPS 应用程序。应用程序的 URL。URL 必须包含“http://”或“https://”
相关域	仅适用于 HTTP/HTTPS 应用程序。您可以添加多个相关域，用逗号 (,) 分隔。
	对于 TCP/UDP 应用程序，请将此字段留空。
DestinationPortProtocol	仅适用于 TCP/UDP 应用程序。您必须列出所有 IP 地址、IP 地址范围或 IP/CIDR 和端口，并用冒号 (:) 分隔。
	对于 HTTP/HTTPS 应用程序，请将此字段留空。
	手动输入数据时，目标、端口和协议必须按以下格式设置。
	目标:端口:协议。示例: 192.0.2.254:5050:PROTOCOL_TCP。
	如果 TCP/UDP 应用程序中有多个目标，则多个目标条目之间用逗号分隔（例如，X.X.X.X:5050:PROTOCOL_TCP,X.X.X.X:1-65535:PROTOCOL_UDP）
	目标可以是 IP 地址、IP 地址范围、CIDR、主机名、域或 FQDN。端口可以是单个端口（例如 5050）或端口范围（例如 1–65335）。
路由类型（云环境）	根据应用程序类型，选择以下值之一。
	内部 – 绕过代理 - 域流量通过 Citrix Cloud Connector™ 路由，绕过在连接器设备上配置的客户 Web 代理。
	通过连接器内部 - 应用程序可以是外部的或内部的，但流量必须通过连接器设备。
	外部 – 流量直接流向互联网。

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

列名	值
路由类型（混合环境）	**内部** 或 **外部**。
主要资源位置	应用程序所在的主要资源位置的名称。
	注意： 不适用于混合环境。
辅助资源位置（可选）	应用程序所在的辅助资源位置的名称。辅助资源位置仅在明确指定主资源位置时适用。
	注意： 不适用于混合环境。
描述	（可选）应用程序描述。
类别	（可选）应用程序类别。
UniqueUsers	应用程序的唯一用户数。
	如果应用程序是从 ns.log 文件中提取的，则此值是自动生成的。
	如果您手动更新 CSV 文件，请将其留空。
总访问量	应用程序被访问的总次数。
	如果应用程序是从 ns.log 文件中提取的，则此值是自动生成的。
	如果您正在手动更新 CSV 文件，请将其留空。
每个应用的独立用户数	访问应用程序的独立用户总数。
	如果应用程序是从 ns.log 文件中提取的，则此值是自动生成的。
	如果您正在手动更新 CSV 文件，请将其留空。

使用基于 CSV 的工具迁移应用程序的步骤

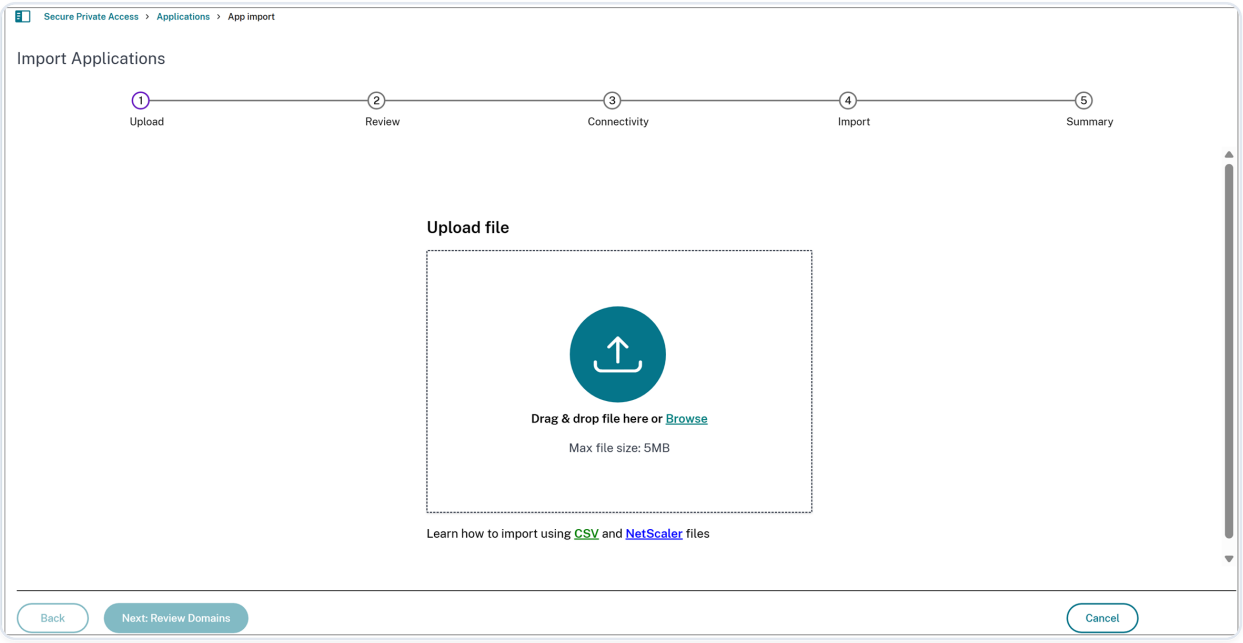
您可以在设置 Secure Private Access 时或设置完成后导入应用程序。

1. 在 Secure Private Access 服务磁贴上，单击“**管理**”。
2. 在概览页面，单击 **继续**。

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

3. 为用户设置身份和身份验证，以便他们登录其商店。有关详细信息，请参阅设置身份和身份验证。
4. 在 **步骤2：应用程序** 页面中，单击 **导入应用程序**。

   或者，如果您的 Secure Private Access 已设置，请从“应用程序”页面（**Secure Private Access > 应用程序**）单击 **导入应用程序**。

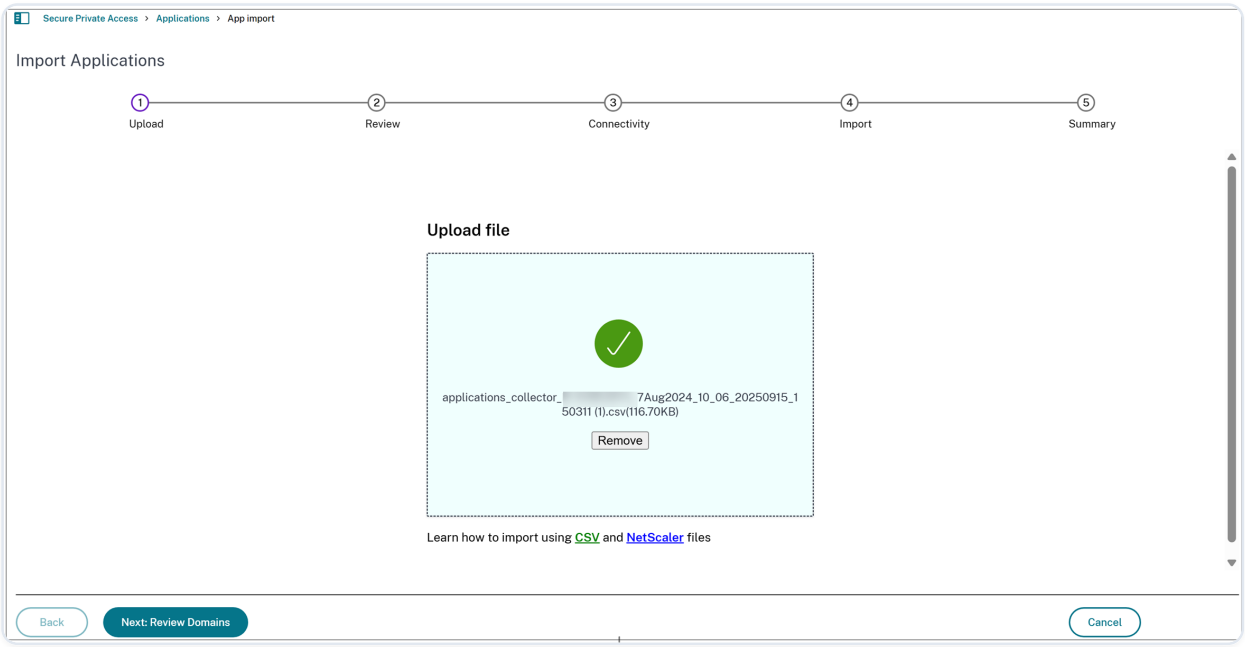


5. 上传 CSV 文件。您可以将 CSV 文件拖到此处，或浏览以选择它。
6. 单击 **下一步：查看域**。

注意：

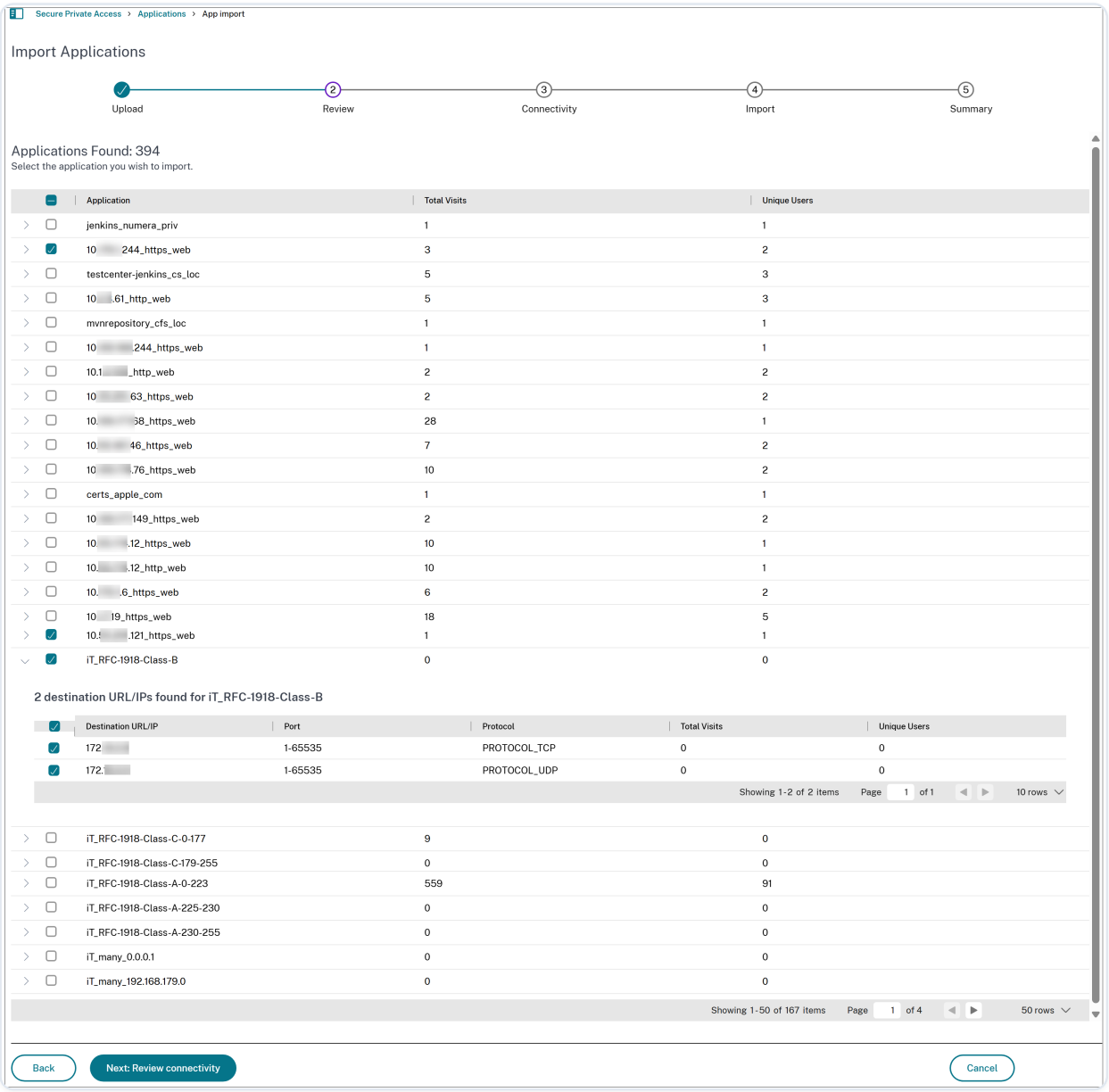
- 仅当文件不包含任何错误时，**下一步：查看域** 按钮才可用。
- 如果您上传包含其他应用程序的相同 CSV/nsconfig 文件，则仅导入差异部分。

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



7. 选择要导入的应用程序。

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

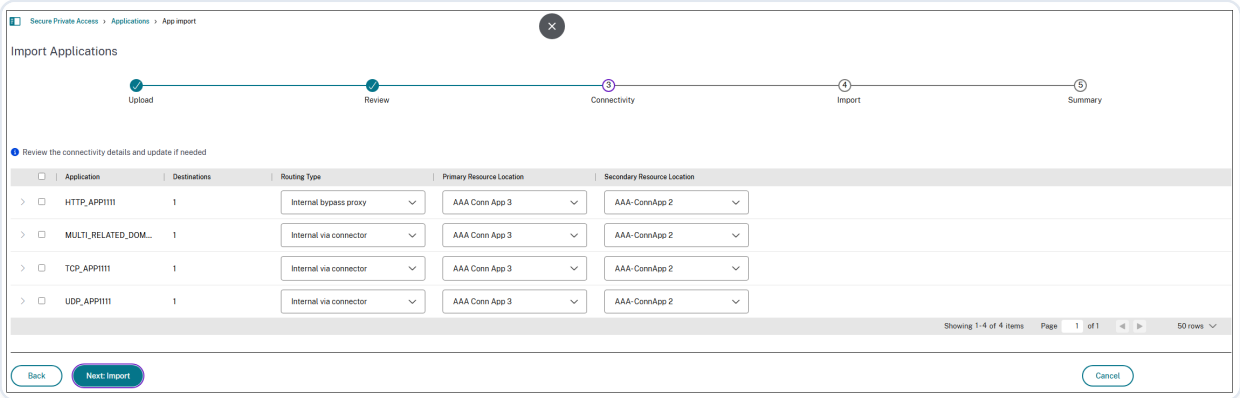


© 1997–2026 Citrix Systems, Inc. All rights reserved.

注意：

- 如果具有相同域或通配符域的应用程序已存在，则该应用程序将禁用导入。您无法选择这些应用程序。
- 与每个应用程序对齐的展开图标显示有关该应用程序的更多详细信息。
- 对于 SaaS/Web 和 TCP/UDP 应用程序，**导入应用程序**页面显示应用程序的总访问次数和唯一用户数（访问过该应用程序的不同用户）。使用展开图标可查看应用程序的端口和协议详细信息。
- 通过 CSV 手动上传的 SaaS 应用程序（在公司网络外部）被标记为未发布，并且即使上传成功，也不会显示在“导入应用程序”UI 中。因此，要通过在 CSV 文件中手动添加条目来创建 SaaS 应用程序，您必须将**应用程序位置**设置为**公司网络外部**，并将**应用程序类型**设置为**HTTP/HTTPS**。
- 对于 TCP/UDP 应用程序，该工具会列出所有相关的目标 URL 和 IP 地址。默认情况下，选择应用程序会自动选择其相关的 URL 和 IP 地址进行导入。您不能取消选择单个目标。

8. 单击**下一步: 审查连接**。
9. 仅当至少选择一个应用程序时，**下一步: 审查连接**按钮才启用。
10. 审查并更新连接设置。如果需要，对路由类型和资源位置进行必要的更改，然后单击**完成**。

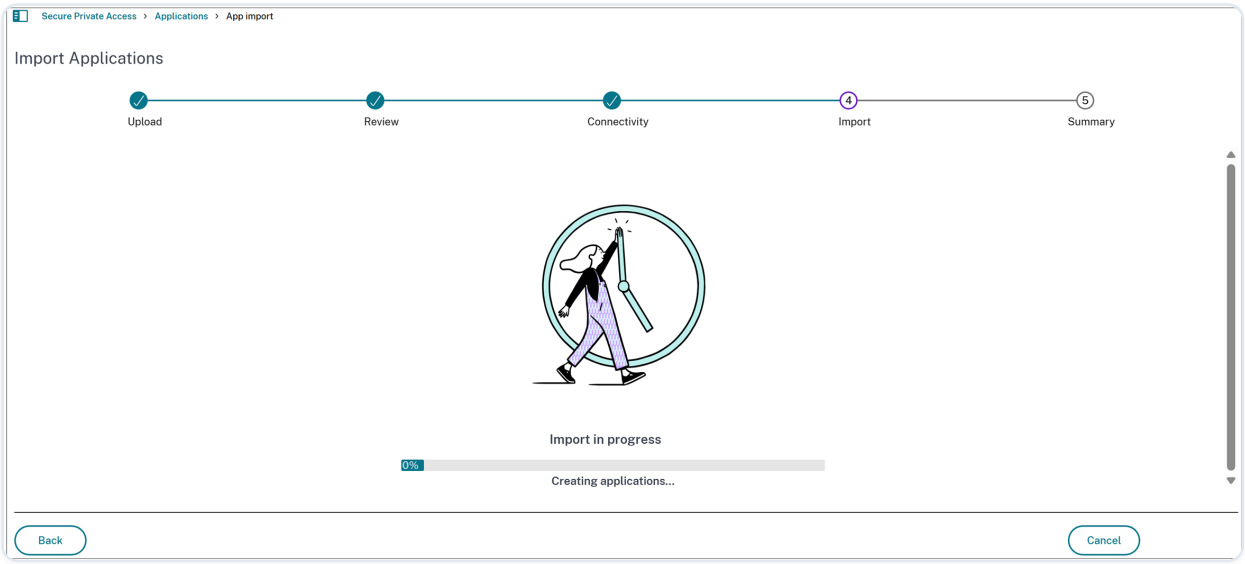


注意：

- 如果指定的资源位置不存在，则默认选择与客户关联的资源位置列表中的第一个可用资源位置。 如果指定资源位置中的连接器设备未启动，则应用程序创建失败。

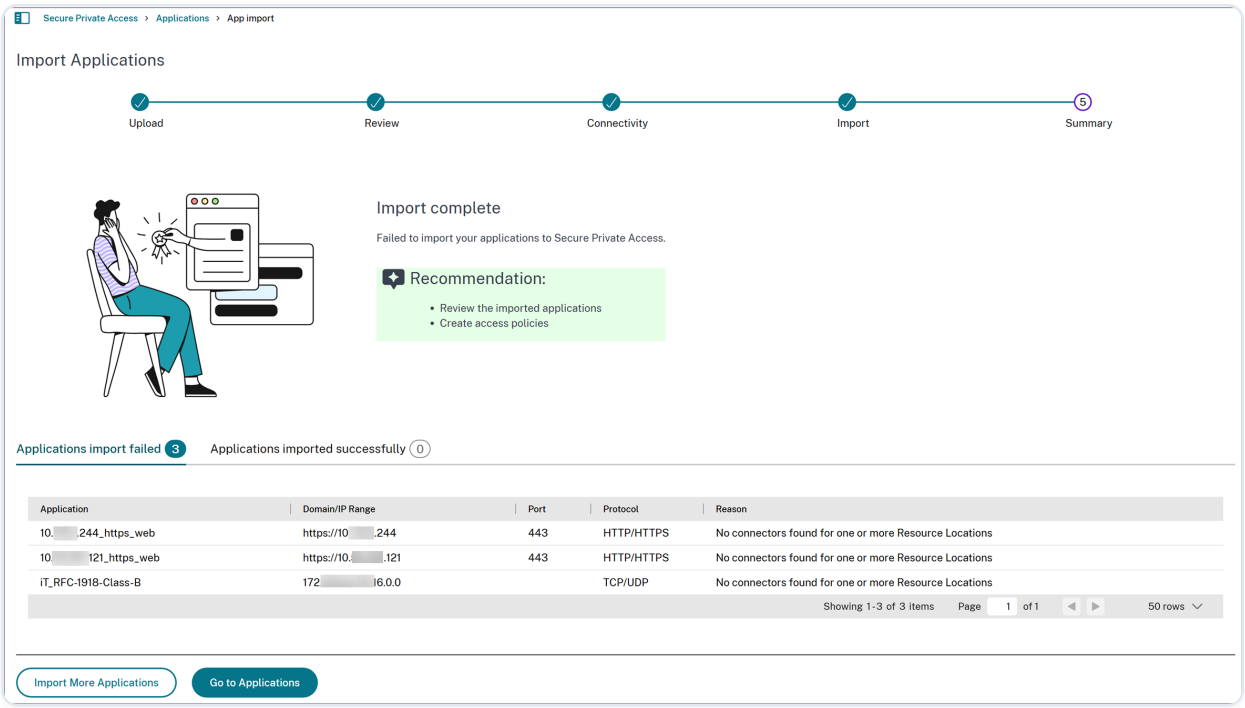
11. 单击：**下一步: 导入**。

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



注意：

- **导入应用程序**页面显示导入的应用程序详细信息。这些应用程序也会添加到**应用程序**页面中的应用程序列表中。
- 对于任何失败的应用程序导入，失败原因将显示在**原因**列中。使用此信息更正 CSV 文件并重新导入这些应用程序。



12. 单击 **转到应用程序** 以查看在 **应用程序** 页面中导入的应用程序。

使用 CSV 文件时导入或创建应用程序失败

以下问题可能导致在使用 CSV 文件时导入或应用程序创建失败：

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

- 对列名称或其大小写进行的修改或更改。
- 删除或交换 CSV 文件中的列。
- CSV 文件中缺少强制性应用程序字段。
- 导入了空的 CSV 文件或仅包含列名称的 CSV 文件。对于空文件，将显示错误消息。如果文件仅包含列名称，则“**下一步**”按钮将保持禁用状态。
- 在 CSV 文件中指定的资源位置中没有可用的连接器设备。
- 指定了辅助资源位置，而主资源位置缺失或为空。导入失败并出现验证错误，指示需要主资源位置。

参考

请参阅以下主题，以获取有关在 Secure Private Access 中创建应用程序的信息。

- 支持企业 Web 应用程序
- 支持 SaaS 应用程序
- 支持 TCP/UDP 应用程序

客户端内部 IP 地址池 - 预览

客户端内部 IP 地址池包含分配给已登录用户的 IP 地址范围。每个用户及其设备都会获得一个唯一的内部 IP 地址，这是在 Secure Private Access 中进行身份识别和会话管理所必需的。此内部客户端 IP 地址仅在客户的资源位置内可访问。

利用这些内部 IP 地址，客户资源位置中的设备可以将流量直接隧道传输到特定已登录用户的设备，从而实现服务器到客户端的连接。客户端内部 IP 地址还支持现有客户端到服务器隧道流量的源 IP 粘性，确保连接稳定一致。

注意：

客户端内部 IP 地址池功能处于预览阶段。要启用此功能，请联系 Citrix® 支持。

客户端内部 IP 地址池的用例

- **启用服务器到客户端的连接：** 某些任务，例如推送配置、提供远程协助或安装软件，需要服务器启动与客户端设备的连接。客户端内部 IP 地址池通过分配用于识别客户端设备的定义 IP 地址范围来实现此目的。这些内部 IP 池根据用户上下文和位置进行分配。例如，可以将特定的 IP 地址范围专用于某个用户组，例如人力资源团队。

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

要启用服务器到客户端的通信，您必须创建一个服务器到客户端的应用程序，并指定客户端设备的端口和协议详细信息，以及用于访问客户端的后端 IP 地址范围。有关详细信息，请参阅服务器到客户端应用程序配置。

- **启用客户端内部 IP 地址粘性：** 为了保持连接一致性，某些应用程序需要与同一客户端保持连续会话。要启用客户端 IP 地址持久性，请参阅客户端 IP 地址粘性。

  重要提示：

  要将源 IP 地址用作内部 IP 地址或使用服务器发起的连接功能，请确保以下事项：

  - 连接到 Connector Appliance 子网的交换机或路由器支持无偿 ARP。
  - 端口安全和动态 ARP 检查 (DAI) 配置不会影响源 IP 地址或服务器发起的连接功能。

IP 地址池限制

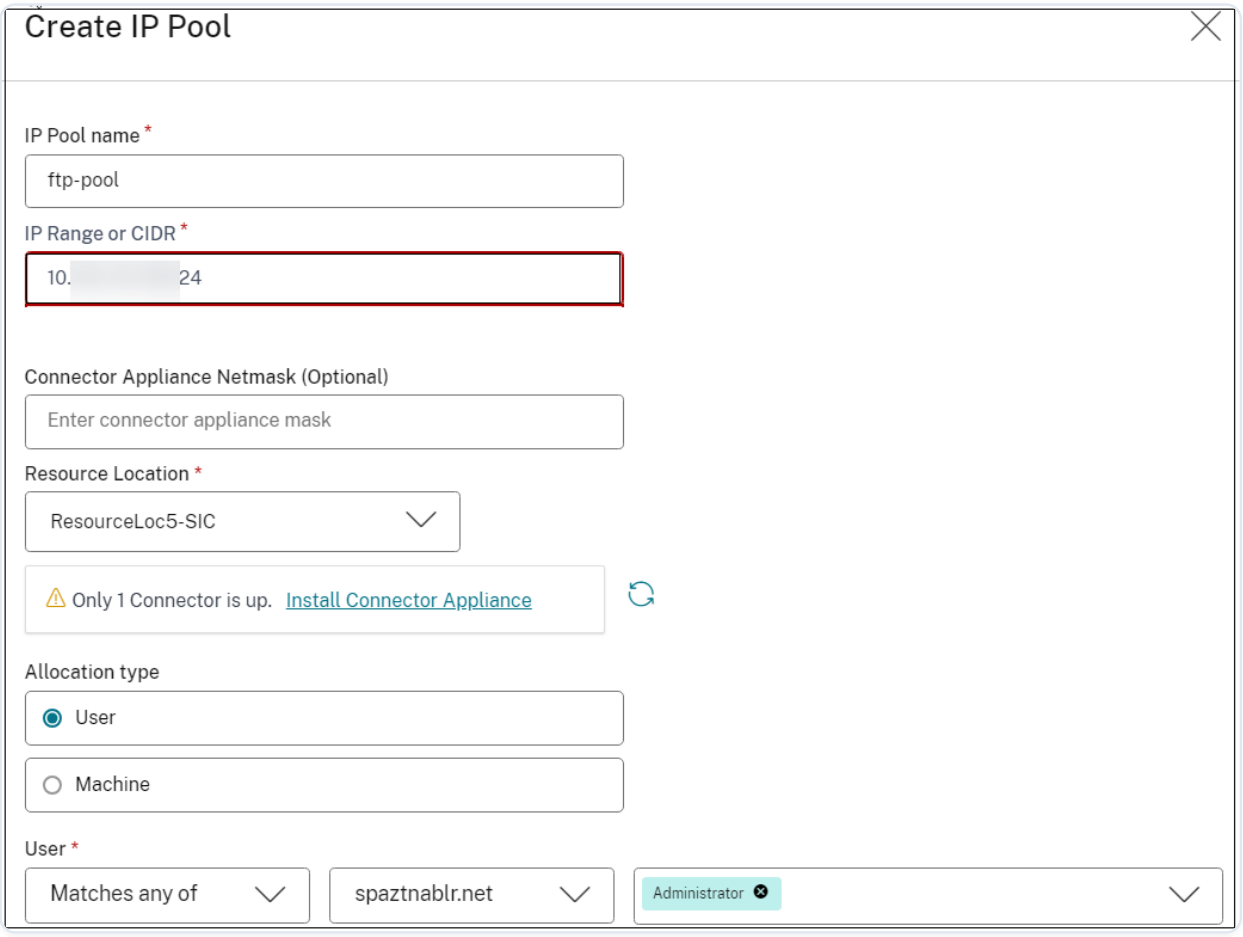
IP 地址池的一些限制如下：

- 资源位置中的所有连接器设备必须位于同一 IP 子网内。
- 内部 IP 地址池必须由同一资源位置中连接器设备子网的 IP 地址组成。
- 内部 IP 地址池中的 IP 地址不得与连接器设备或同一子网中其他设备的任何已用 IP 地址重叠。
- 如果池中的 IP 地址已用尽，则不会为用户分配 IP 地址，因此无法使用服务器到客户端连接和客户端内部 IP 粘滞功能。
- 最多可为用户分配 3 个不同的 IP 地址，允许从最多 3 个不同的设备登录。如果同一用户从第四个设备登录，则不会分配 IP 地址，从而阻止使用服务器到客户端发起的连接和客户端内部 IP 粘滞。
- 分配的内部 IP 地址是粘滞的，在同一设备上每日登录和注销时保持不变。但是，如果用户连续 15 天不活动，其粘滞内部 IP 地址将被释放并重新分配给其他用户。

创建内部网 IP 地址池

1. 导航到 **设置 > IP 池**，然后单击 **创建 IP 池**。

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



2. **IP 池名称**：输入 IP 池的名称。
3. **IP 范围或 CIDR**：输入为客户端保留的 IP 地址范围。其中一个 IP 地址将分配给客户端计算机。
4. **连接器设备网络掩码**：（可选）。如果连接器设备网络子网与内部 IP 地址子网不同，则必须输入连接器设备网络掩码。
5. **资源位置**：选择后端服务器所在的资源位置。确保至少有一个连接器设备已启动。
6. **分配类型**：选择用户，并选择此池适用的条件、域以及用户或用户组。
7. 单击 **创建**。

您创建的 IP 地址池将列在“IP 池”页面中。

IP 地址池页面(/en-us/citrix-secure-private-access/media/ip-pools-page.png)

客户端登录成功后，将从客户端内部 IP 地址池中为用户分配一个内网 IP 地址。

如上图所示，管理员可以使用优先级机制来控制池的优先级。管理员可以为每个 IP 池定义明确的优先级级别。Secure Private Access 服务从最高优先级到最低优先级（从上到下）分配 IP 地址，从而确保可预测的分配和操作控制。

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

注意：

值越低的优先级具有最高的偏好。

删除 IP 地址池

IP 地址池可以通过以下任一选项立即删除或在一段时间后删除。

- **强制删除 IP 池：** 停止向新用户分配 IP 地址并立即释放未使用的 IP 地址。使用已删除 IP 地址的活动用户会话可能会被终止，从而导致突然关闭和强制注销。只有在创建了不同的 IP 地址池后，才会为会话已终止的用户分配新的 IP 地址。
- **在一段时间后删除 IP 池：** 停止向新用户分配 IP 地址并立即释放未使用的 IP 地址。系统会等待活动会话注销或过期，然后才完全删除该池。只有在创建了不同的 IP 地址池后，才会为会话已终止的用户分配新的 IP 地址。

注意：

我们建议您安排维护窗口并通知用户注销，然后启动在一段时间后删除 IP 池。如果在预定时间后大部分 IP 地址都已释放，您可以强制删除剩余的正在使用的 IP 地址。但是，我们建议您不要强制删除大型 IP 地址池。

执行以下步骤删除 IP 池：

1. 导航到 **设置 > IP 池**。

   将显示 IP 地址池及其详细信息的列表。
2. 点击要删除的地址池旁边的省略号（…），然后选择**强制删除 IP 池**或**按时间删除 IP 池**。

删除 IP 地址池(/en-us/citrix-secure-private-access/media/ip-pools-delete.png)

删除 IP 池选项(/en-us/citrix-secure-private-access/media/ip-pools-force-delete.png)

注意：

当池被删除或计划删除时，管理员必须降低其优先级。此池的优先级必须低于其他活动池，以确保 Secure Private Access 停止从该池分配新的 IP 地址。IP 地址分配会自动回退到优先级更高的池。

查看 IP 地址利用率数据

您可以从“IP 池利用率”页面监控 IP 地址利用率数据。此页面提供了 IP 地址状态的概述。

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

- 用户列表以及分配给这些用户的 IP 地址。
- 已分配的可用 IP 地址的百分比以及可供分配的 IP 地址总数。

管理员可以使用此数据来监控 IP 地址消耗，并确保有足够的 IP 地址可供用户使用。

执行以下步骤查看 IP 地址利用率详细信息：

1. 导航到**设置 > IP 池**。

   IP 地址池列表及其详细信息以表格形式显示。
2. 单击地址池旁边的省略号 (...)，然后单击**查看 IP 利用率**。

保持一致的连接

为了确保需要会话连续性的应用程序的持久且一致的连接，管理员可以启用连接器粘性或客户端 IP 地址粘性，具体取决于应用程序类型（Web/SaaS 或 TCP/UDP）。Secure Private Access 支持连接器粘性和客户端 IP 地址粘性。

- **连接器粘性**确保客户端与连接器设备建立连接后，来自该客户端的所有后续请求都定向到同一源（连接器设备）。
- **客户端 IP 地址粘性**确保来自特定客户端 IP 地址的请求始终路由到同一后端服务器。

连接器或客户端 IP 地址粘性可以在创建应用程序时启用。

- 对于 Web/SaaS 应用程序，管理员可以启用**保持一致的连接**选项。
- 对于 TCP/UDP 应用程序，管理员可以根据需要选择**客户端 IP** 和**连接器 ID** 粘性。

有关详细信息，请参阅以下部分：

- 连接器粘性
- 客户端 IP 地址粘性

重要提示：

- 客户端 IP 地址粘性功能处于预览阶段。
- 要启用客户端 IP 地址粘性，管理员必须配置客户端内部 IP 地址池。IP 地址池对于为用户和关联设备分配唯一的 IP 地址至关重要。客户资源位置的设备可以使用客户端的内部 IP 地址将流量隧道传输到特定已登录用户的设备。有关详细信息，请参阅客户端内部 IP 地址池。

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

连接器粘性

某些应用程序需要连接器粘性，这意味着用户会话的所有请求，包括初始登录和后续请求，都来自同一个连接器设备（相同的 IP 地址）。如果请求通过不同的连接器设备路由，则应用程序可能无法正常运行。

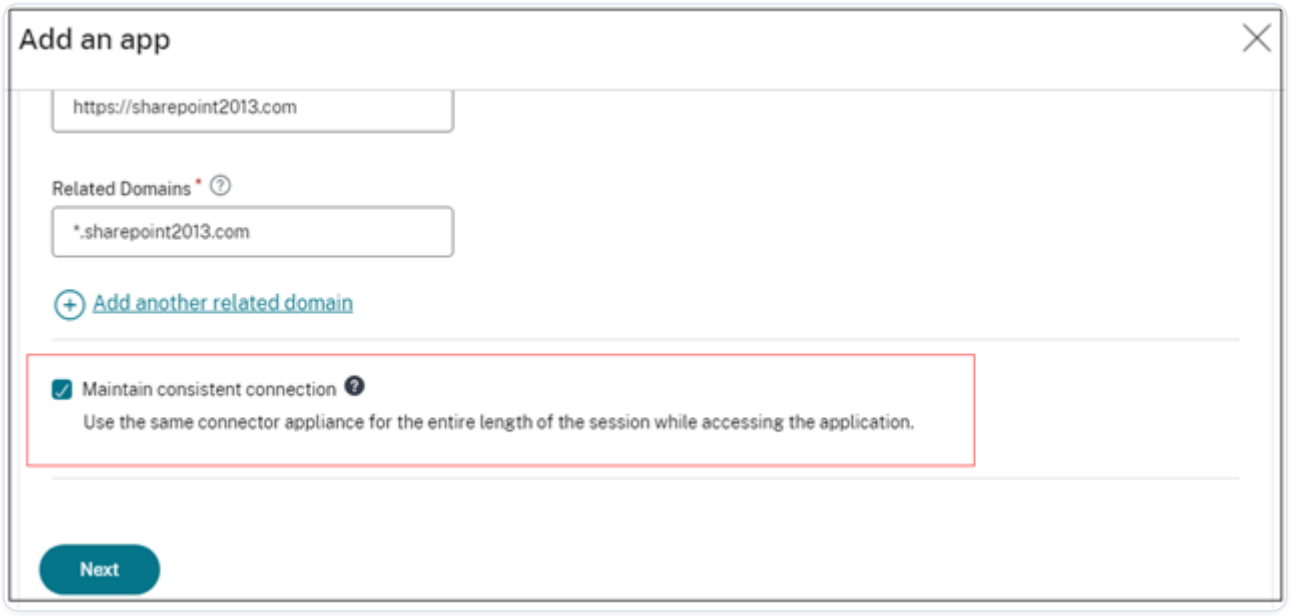
- 连接器粘性特定于某个用户会话。如果同一用户再次打开应用程序，流量可能会被路由到不同的连接器设备。
- 连接器设备是从给定资源位置的可用连接器设备中随机选择的。
- 如果连接器设备发生故障，连接将重定向到同一资源位置的另一个设备。

连接器粘性在以下场景中很重要：

- NTLM 协议，它们依赖于 IP 地址来维护会话状态。如果请求通过不同的连接器路由，NTLM 身份验证可能会失败，导致错误或登录失败。
- 基于被动 FTP 的应用程序，它们需要连接粘性以确保控制和数据连接都路由到同一个后端服务器。如果没有这种粘性，FTP 会话可能会失败。

有关为应用程序启用连接器粘性的信息，请参阅以下主题：

- 配置 Web 应用程序
- 配置 SaaS 应用程序
- 配置 TCP/UDP 应用程序



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

客户端 IP 地址粘性 - 预览

当客户端通过资源位置中的多个连接器设备进行负载均衡连接到后端服务器时，流量源 IP 地址可能会显示为不同的连接器设备 IP 地址。IP 地址的这种差异可能会导致以下问题：

- **TCP/UDP 应用程序：** 某些应用程序要求特定客户端和服务器之间保持一致的会话。如果源 IP 地址发生变化，这些应用程序可能无法启动。被动 FTP、主动 FTP 和某些 Web 服务器等应用程序依赖于 IP 地址亲和性（粘性）才能正常运行。
- **安全和监控系统：** 如果源 IP 地址频繁更改，这些系统可能难以跟踪和分析流量。

为了保持源 IP 地址的亲和性/粘滞性，可以为 TCP/UDP 应用程序（客户端到服务器）配置客户端内部 IP 地址粘滞性。通过客户端 IP 地址粘滞性，在登录期间会为用户会话分配一个唯一的内部 IP 地址。此 IP 地址将用于资源位置中，而不是连接器设备 IP 地址。此分配确保从客户端到后端服务器的所有连接都使用在登录时分配的客户端内部 IP 地址作为源 IP 地址。客户端 IP 地址粘滞性可保持会话持久性，无论连接期间使用哪个连接器设备。

有关启用客户端 IP 地址持久性的信息，请参阅为 TCP/UDP 应用程序启用客户端 IP 地址粘滞性。

先决条件

确保已创建 IP 地址池。IP 地址池对于为用户和关联设备分配唯一 IP 地址至关重要。有关详细信息，请参阅客户端内部 IP 地址池。

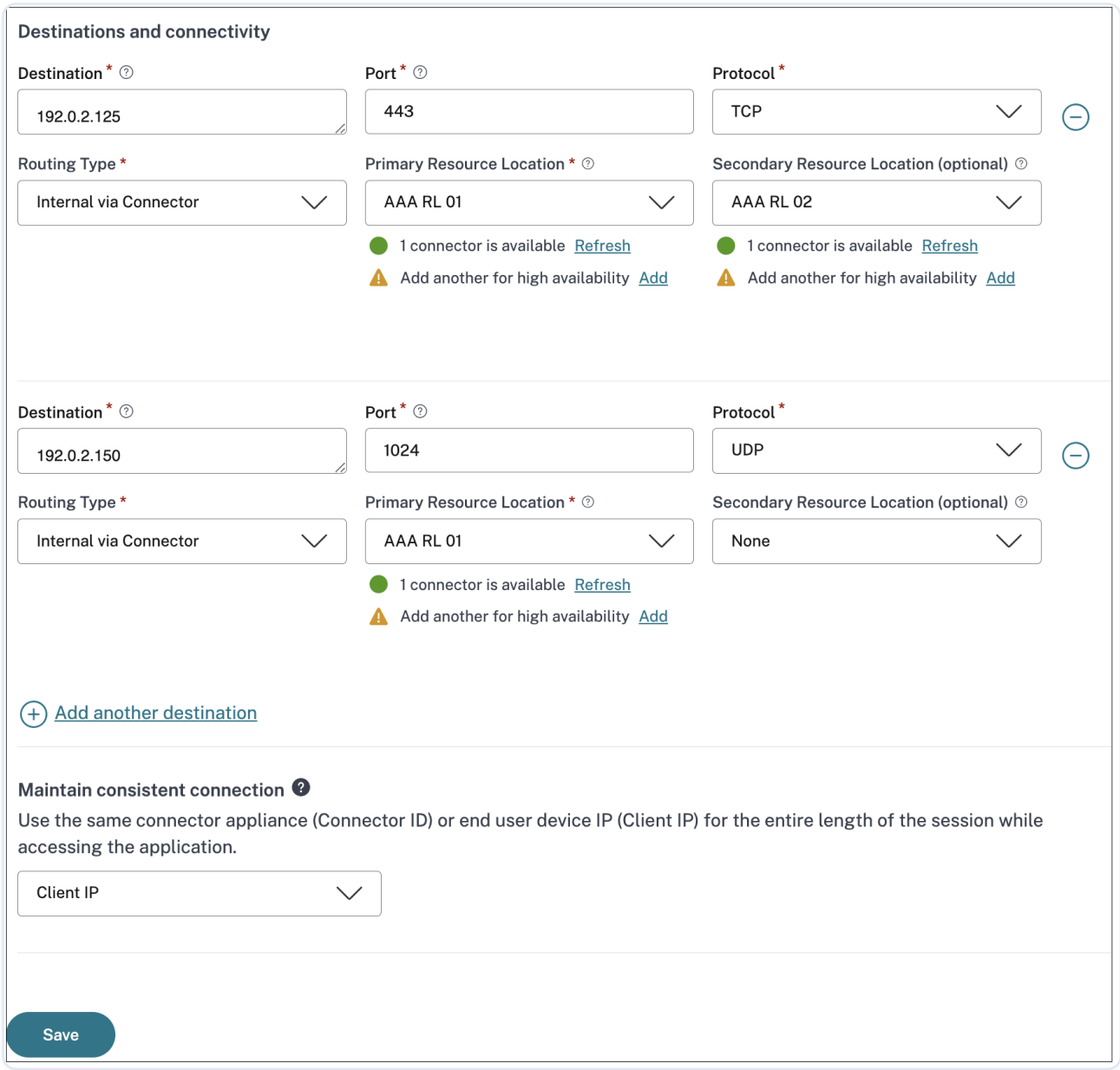
为 TCP/UDP 应用程序启用客户端 IP 地址粘滞性

执行主题对 TCP/UDP 应用程序的支持中概述的步骤。

在**应用程序详细信息**部分中，通过在**保持一致连接**中选择以下值之一来启用或禁用客户端 IP 粘滞性。

- **不使用：** 应用程序不需要任何持久性。应用程序可以使用任何源 IP 地址。
- **客户端 IP：** 应用程序在每次连接时都为客户端使用相同的源 IP 地址。
- **连接器 ID：** 应用程序在每个会话中连接到相同的连接器设备。

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



注意：

要启用客户端 IP 地址粘滞性，请选择创建内部 IP 地址池时使用的相同资源位置，并确保在“应用程序连接性”部分中设置了相同的资源位置。

终止活动会话并将用户/计算机添加到阻止列表

管理员可以立即终止所有活动会话，并将用户/计算机添加到阻止列表。将用户/计算机添加到阻止列表会终止所有活动的 Secure Private Access 应用程序会话，并阻止将来的应用程序访问。

通过 Chrome Enterprise Premium 浏览器、直接访问、适用于 HTML5 的 Citrix Workspace 应用程序和 Secure Access 代理的所有活动应用程序会话都将被终止和阻止。通过 Secure Access 代理连

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

接的所有资源（例如文件共享、RDP、SSH 会话）也将被终止和阻止。在将用户/计算机从阻止列表中删除之前，用户无法启动任何新应用程序。

当使用 Chrome Enterprise Premium 浏览器访问应用程序时，任何活动的基于浏览器的会话也会被终止，并且根据 Secure Private Access 阻止列表策略，将拒绝来自禁用用户的进一步访问请求。

注意：

- 将用户/计算机添加到阻止列表不会更改或编辑已配置的 Secure Private Access 访问策略。无论配置了何种访问策略，都会发生访问终止和阻止。一旦用户/计算机从列表中删除，该用户的现有 Secure Private Access 访问策略将恢复。
- 即使将用户添加到阻止列表后，仍允许通过 Citrix Enterprise Premium 浏览器进行 Internet 访问。仅阻止对已发布的 Secure Private Access 应用程序的访问。

用例

您可以在以下场景中使用此功能。

- 员工辞职或被公司解雇。在这种情况下，管理员通过终止活动的 Secure Private Access 会话并阻止任何将来的应用程序访问来撤销所有 Secure Private Access 应用程序访问。
- 设备丢失或被盗。在这种情况下，访问将被阻止，所有当前会话都将终止。在情况得到控制后，可以将用户从阻止列表中删除。
- 用户滥用应用程序访问权限。在这种情况下，可以立即撤销该用户的访问权限。访问将被阻止，直到用户被添加到列表中。

使用 Chrome Enterprise Premium 时阻止用户的先决条件

要使用 Chrome Enterprise Premium 和 Secure Private Access 阻止用户，请确保满足以下先决条件：

- 通过 Microsoft 的 Google Cloud / G Suite 连接器同步 Microsoft Entra ID 用户时，请确保配置了正确的属性映射，以便用户身份与 Citrix Secure Private Access 用户记录匹配。

如果未设置此配置，则对于通过 Chrome Enterprise Premium 浏览器访问应用程序的用户，阻止用户策略可能不会强制执行。

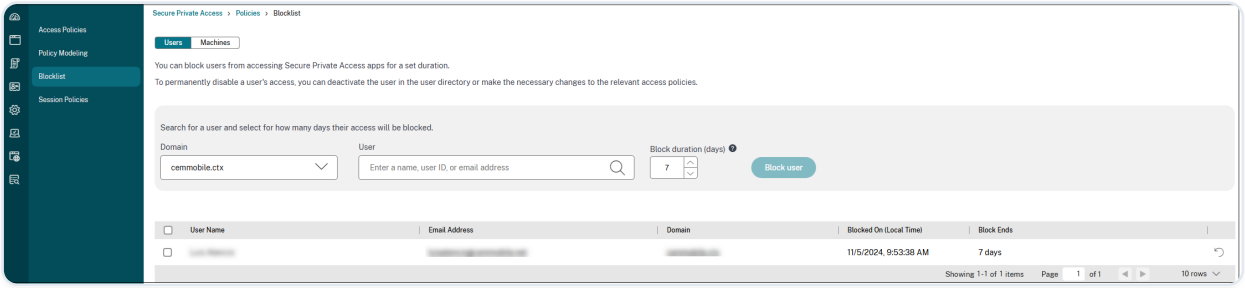
将用户/计算机添加到阻止列表

1. 导航到 **安全私有访问 > 策略 > 阻止列表**。

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

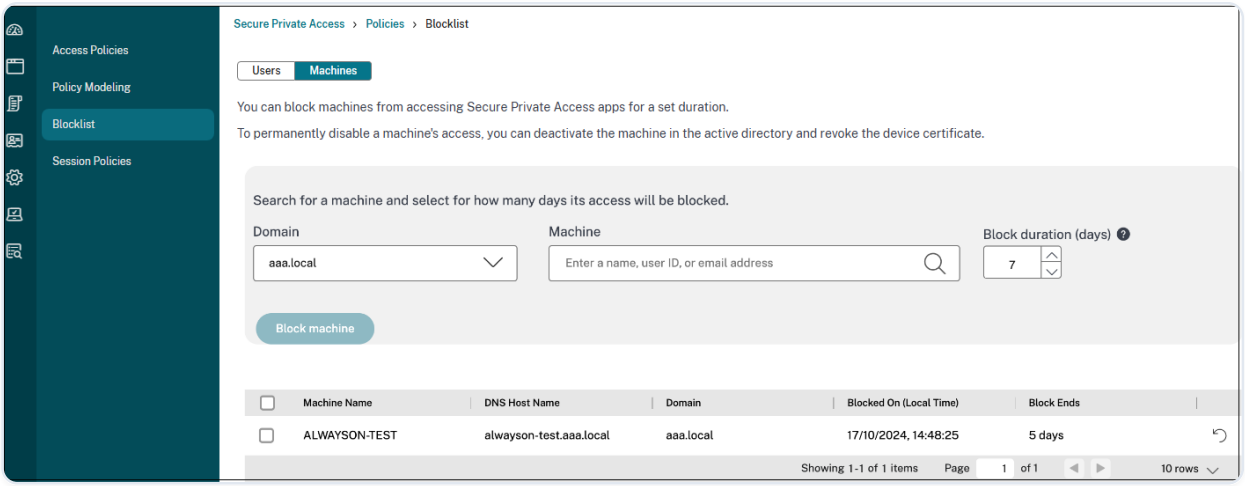
2. 在 **Domain** 中，选择必须禁用访问的域。
3. 在 **User** 中，搜索必须添加到阻止列表的用户名。将显示所有符合搜索条件的用户名。如果用户从目录服务中删除，则该用户名不会出现在 **User** 列表中。

> **注意：**
>
> **User** 字段仅在选择了 **Users** 选项卡时显示。



4. 在 **Machine** 中，搜索必须添加到阻止列表的计算机名称。将显示所有符合搜索条件的计算机名称。如果计算机从目录服务中删除，则该计算机名称不会出现在 **User** 列表中。

> **注意：**
>
> **Machine** 字段仅在选择了 **Machines** 选项卡时显示。



5. 在 **Block duration (days)** 中，输入此用户/计算机必须被阻止的天数。将用户/计算机添加到阻止列表后，默认情况下会阻止他们 7 天。但是，您可以将持续时间更改为 1 到 99 天之间的任意值。持续时间结束后，将根据用户目录和策略配置恢复访问权限。此外，此值对于用户在将来添加时保持不变。例如，如果管理员将用户/计算机的阻止持续时间设置为 30 天，则此设置对于用户/计算机在将来添加时保持不变。
6. 相应地单击 **Block user** 或 **Block machine**。

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

> **注意：**
>
> “**阻止用户**”或“**阻止计算机**”字段的显示取决于所选选项卡（“**用户**”或“**计算机**”）。

用户/计算机已添加到阻止列表。

建议：

- 您可以通过执行以下任一操作，在阻止期限结束之前恢复访问。
  - 选择必须恢复访问的访问权限，然后单击“**恢复访问**”。
  - 单击与要恢复访问的用户对应的恢复图标。

    在这两种情况下，都会出现一个确认对话框。
- 为了无限期撤销用户/计算机的访问权限，请从相应的目录服务（例如 Active Directory）中删除该用户/计算机，然后将其添加到阻止列表。这会终止活动的 Secure Private Access 会话，阻止将来的应用程序访问，并且一旦用户/计算机从商店注销，由于目录凭据无效，用户/计算机将无法再次登录。

用户/计算机添加到阻止列表后的最终用户体验

以下部分提供了有关用户/计算机添加到阻止列表后的最终用户体验的更多信息。

通过云访问的应用程序

当用户被阻止时：

- 所有活动的 Secure Private Access 会话将立即终止。
- 将阻止将来访问所有 Secure Private Access 已发布的应用程序。
- 即使在用户添加到阻止列表后，也允许通过 Citrix Enterprise Premium 浏览器访问 Internet。仅阻止访问已发布的 Secure Private Access 应用程序。

当设备被阻止时：

- 一旦设备被添加到阻止列表，用户对所有当前正在运行的应用程序的访问都将被阻止。
- 任何尝试访问新应用程序的操作都会触发注销请求。

通过本地 NetScaler® Gateway 访问的应用程序（混合数据路径）

- 当云会话终止时（无论是由于用户操作还是由于撤销），相应的活动 NetScaler Gateway 会话将自动终止。

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

- 当被阻止的用户尝试通过 NetScaler Gateway 访问新应用程序时，系统会触发注销请求。

用户会话超时

您可以为 Web 应用程序和 Citrix Secure Access™ 客户端配置超时期限，以便在指定时间内没有网络活动时结束用户会话。 对于 Citrix Secure Access 客户端，您还可以配置 Citrix Secure Access 客户端，以便在指定时间内没有用户活动时终止会话。此外，一旦配置的期限到期，无论用户和网络活动如何，您都可以在 Citrix Secure Access 客户端上配置强制断开连接。

Web 应用程序服务器超时

1. 导航到 **设置 > 超时**。
2. 在 **Web 应用程序服务器空闲会话超时** 中，选择 Web 应用程序会话可以保持空闲状态的持续时间（以小时和分钟为单位）。如果会话保持空闲状态，Secure Private Access 服务将在该时间到期后终止会话。

   最短持续时间为 1 小时，最长持续时间为 168 小时。默认值为 2 小时。

配置 Web 应用程序超时(/en-us/citrix-secure-private-access/media/secure-private-access-timeout-for-webapps.png)

Citrix Secure Access 客户端超时

您可以为 Citrix Secure Access 客户端配置以下超时：

- 客户端不活动
- 强制超时

1. 导航到 **设置 > 超时**。

   配置 ZTNA 应用程序超时(/en-us/citrix-secure-private-access/media/secure-private-access-timeout-for-client-server-appss.png)
2. 在 **Secure Access 代理超时** 中，选择您要强制执行的超时持续时间（以小时和分钟为单位）。

   - **客户端不活动超时**：如果在配置的期限内没有用户活动（鼠标或键盘），Citrix Secure Access 客户端将在此持续时间后终止会话。默认情况下，此选项处于禁用状态。您必须使用切换开关启用此选项以强制执行配置的超时期限。但是，如果在保存配置后禁用切换开关，客户端将不会启动超时。

     最短持续时间为 5 分钟，最长持续时间为 168 小时。默认值为 8 小时。

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

- **强制超时**：Citrix Secure Access 客户端终止会话的持续时间，无论用户或网络活动如何。此选项默认处于禁用状态。您必须使用切换开关启用此选项，以强制执行配置的超时期限。但是，如果在保存配置后禁用切换开关，客户端将不会启动超时。

  会话终止前 15 分钟会显示通知消息。

  最短持续时间为 1 小时，最长持续时间为 168 小时。默认值为 168 小时。

注意：

如果启用多个此类设置，则第一个到期的超时间隔将关闭用户连接。

配置报告

客户管理员可以生成配置报告，以深入了解 Secure Private Access 设置。配置报告包含以下类别的信息：

- 管理对应用程序和资源访问的访问策略。
- 在 Secure Private Access 中配置的应用程序。
- 为应用程序设置的路由域。
- 与客户关联的资源位置。
- 用于验证用户身份的身份验证域。
- 用于用户身份的身份提供程序 (IdP)。
- 为特定客户定义的客户参数。
- 与云存储相关的存储配置。

配置报告可用于以下场景：

- 识别并解决配置问题。
- 与 Citrix 支持团队共享，用于调查和故障排除。
- 将报告用作新设置的参考或修改现有设置详细信息。

生成配置报告

执行以下步骤以生成配置报告。

1. 在 Secure Private Access 管理控制台中，转到 **设置 > 全局配置**。
2. 单击 **创建报告** 以启动报告生成过程。

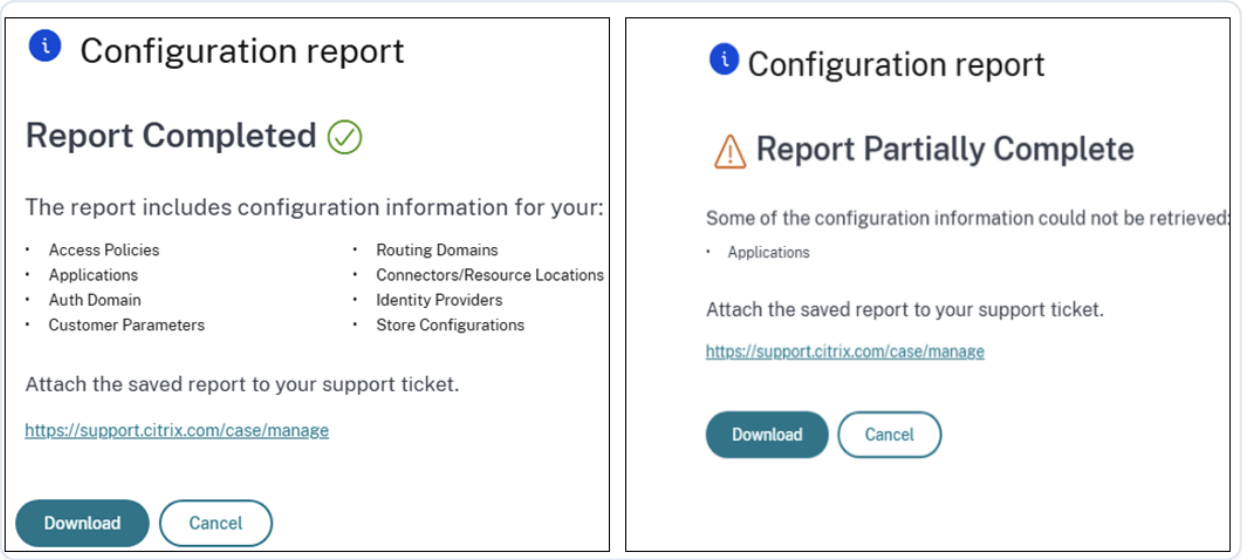
© 1997–2026 Citrix Systems, Inc. All rights reserved.

报告生成后，**配置报告** 对话框将显示以下状态：

- **报告已完成：** 表示所有必需的详细信息都已成功包含在报告中。
- **报告部分完成：** 表示某些详细信息缺失或未生成。

  对话框还会列出报告生成不完整的类别。

下图显示了一个配置报告对话框示例，其中包含完整和部分完成的状态。



3. 单击 **下载** 可将报告手动导出到本地驱动器。

重要提示：

生成配置报告仅限于具有以下 Secure Private Access 角色的管理员：

- 完全访问管理员
- 只读管理员
- 完全监控管理员

具有帮助台管理员角色的管理员无法生成配置报告。

ADFS 与安全私有访问集成

声明规则对于控制声明通过声明管道的流向是必要的。声明规则还可用于在声明规则执行过程中自定义声明流。有关声明的更多信息，请参阅 Microsoft 文档。

要将 ADFS 设置为接受来自 Citrix Secure Private Access™ 的声明，您必须执行以下步骤：

1. 在 ADFS 中添加声明提供程序信任。

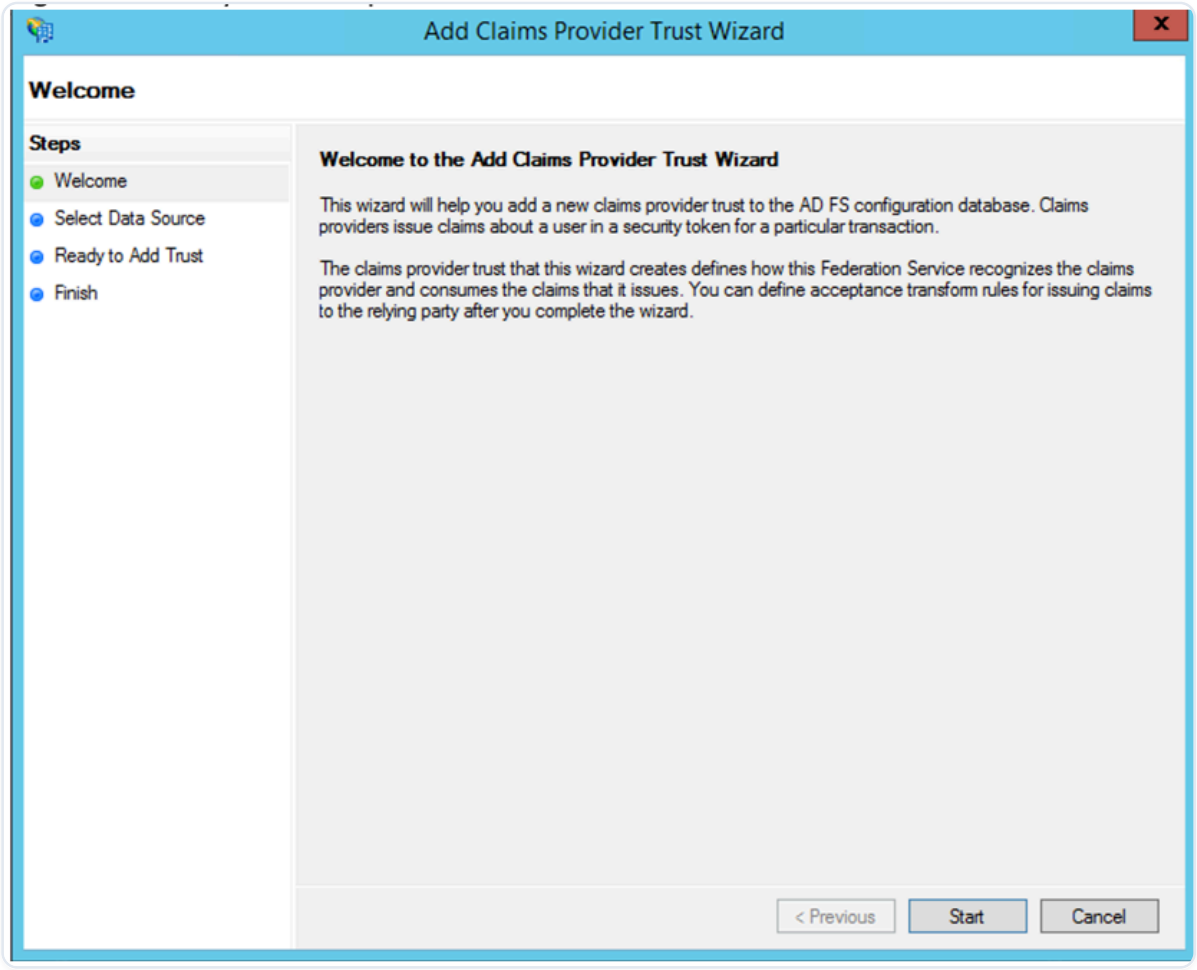
© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. 完成 Citrix Secure Private Access 上的应用程序配置。

在 ADFS 中添加声明提供程序信任

1. 打开 ADFS 管理控制台。转到 **ADFS > 信任关系 > 声明提供程序信任**。

   a. 右键单击并选择 **添加声明提供程序信任**。

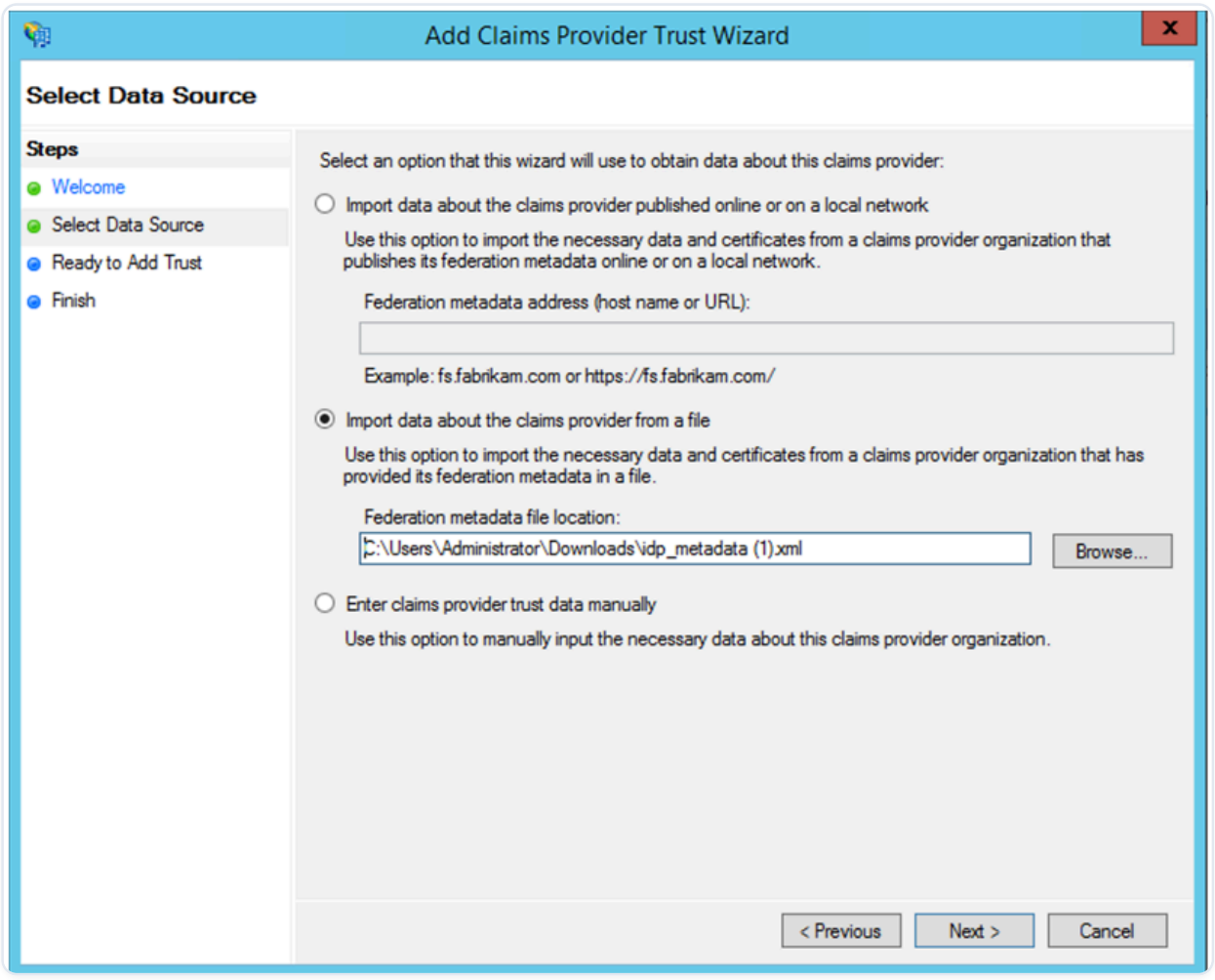


   b. 在 Secure Private Access 中添加一个用于联合到 ADFS 的应用程序。有关详细信息，请参阅 Citrix Secure Private Access 上的应用程序配置。

注意：

首先添加应用程序，然后从应用程序的 SSO 配置部分，您可以下载 SAML 元数据文件，然后将元数据文件导入 ADFS。

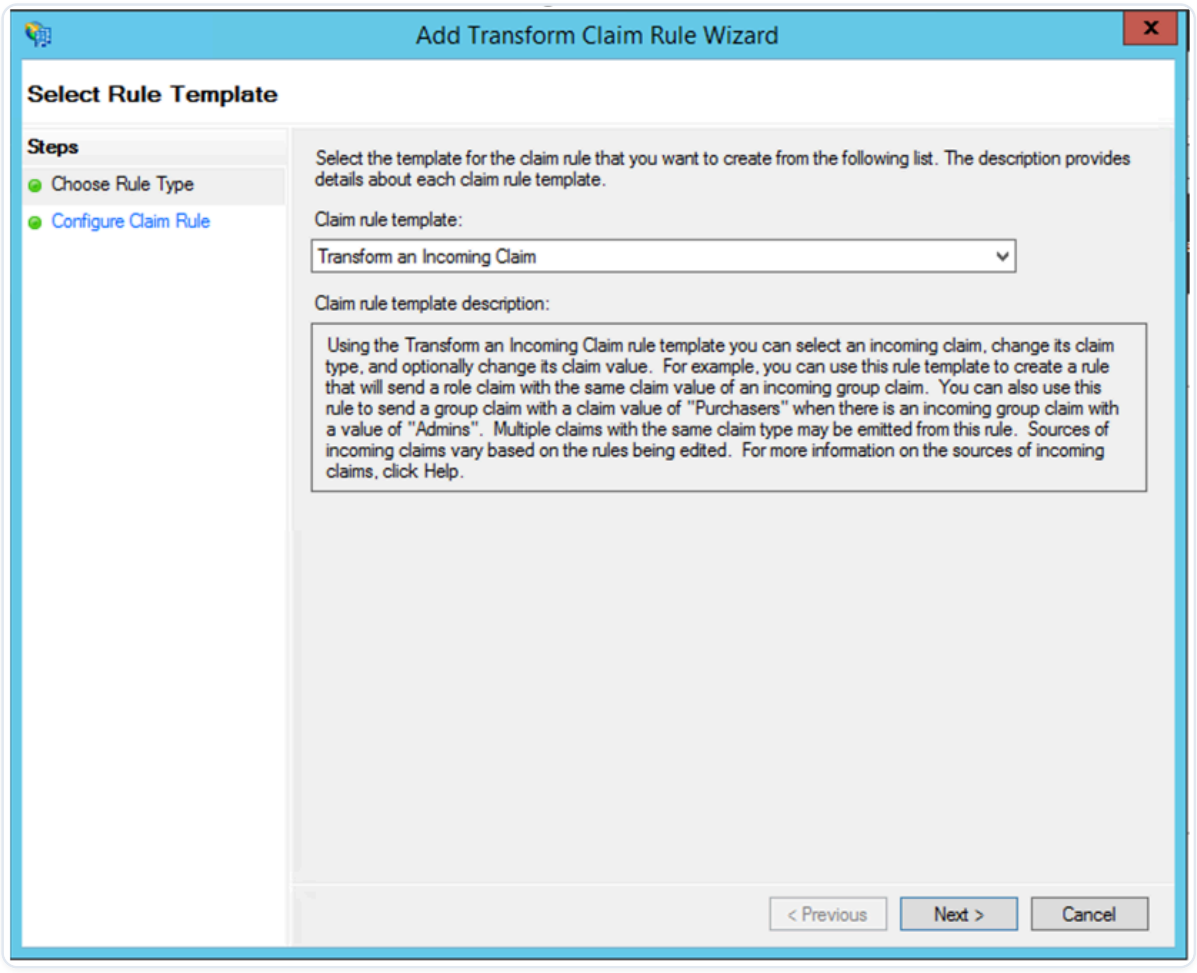
© 1997–2026 Citrix Systems, Inc. All rights reserved.



a. 完成步骤以完成添加声明提供程序信任。完成添加声明提供程序信任后，将出现一个编辑声明规则的窗口。

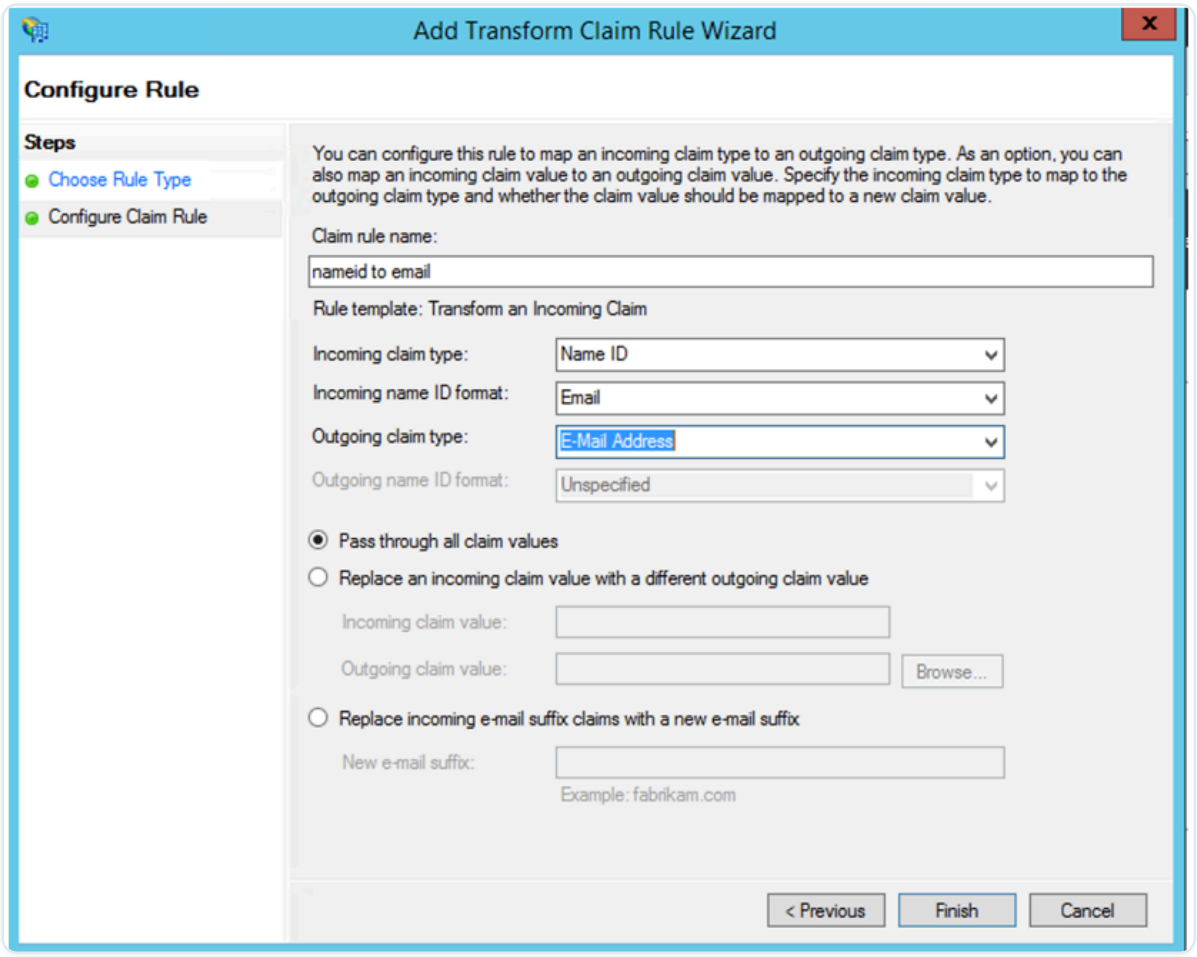
b. 添加一个带有 **转换传入声明** 的声明规则。

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



c. 完成以下图中所示的设置。如果您的 ADFS 接受其他声明，则使用这些声明并相应地在 Secure Private Access 中配置 SSO。

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

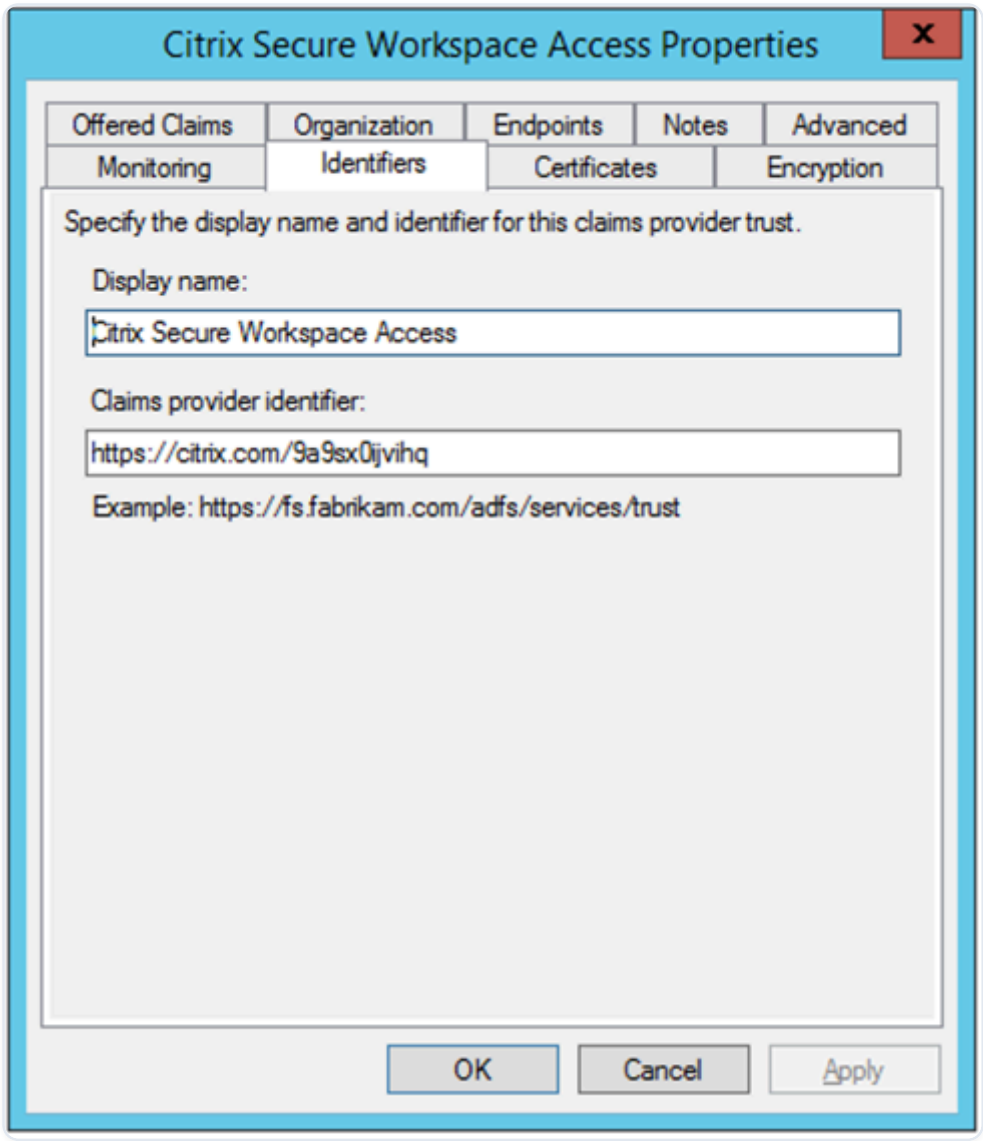


您现在已配置声明提供程序信任，确认 ADFS 现已信任 Citrix Secure Private Access 用于 SAML。

声明提供程序信任 ID

记下您添加的声明提供程序信任 ID。在 Citrix Secure Private Access 中配置应用程序时需要此 ID。

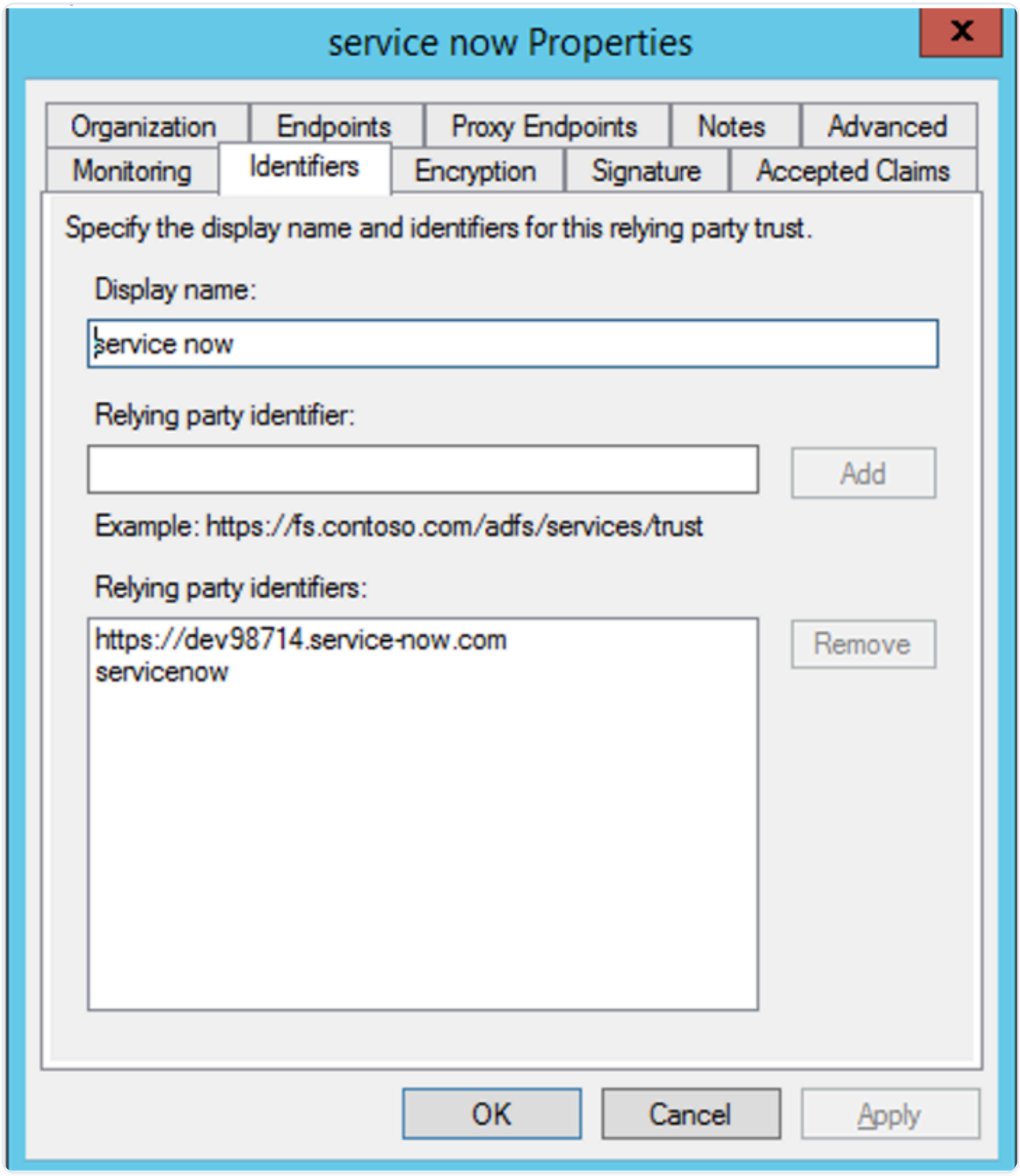
© 1997–2026 Citrix Systems, Inc. All rights reserved.



信赖方标识符

如果您的 SaaS 应用程序已使用 ADFS 进行身份验证，则您必须已为该应用程序添加了信赖方信任。在 Citrix Secure Private Access 中配置应用程序时需要此 ID。

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



在 IdP 发起的流程中启用中继状态

RelayState 是 SAML 协议的一个参数，用于标识用户登录并定向到信赖方联合服务器后访问的特定资源。如果在 ADFS 中未启用 RelayState，则用户在向需要它的资源提供程序进行身份验证后会看到错误。

对于 ADFS 2.0，您必须安装更新 KB2681584（更新汇总 2）或 KB2790338（更新汇总 3）以提供 RelayState 支持。ADFS 3.0 内置了 RelayState 支持。在这两种情况下，RelayState 仍然需要启用。

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

在 ADFS 服务器上启用 RelayState 参数

1. 打开文件。
   - 对于 ADFS 2.0，在记事本中输入以下文件：%systemroot%\inetpub\adfs\ls\web.config
   - 对于 ADFS 3.0，在记事本中输入以下文件：%systemroot%\ADFS\Microsoft.IdentityServer.Servicehost.exe.config
2. 在 microsoft.identityServer.web 部分中，按如下所示为 useRelyStateForIdpInitiatedSignOn 添加一行，并保存更改：`<microsoft.identityServer.web> ... <useRelayStateForIdpInitiatedSignOn enabled="true" /> ...</microsoft.identityServer.web>`
   - 对于 ADFS 2.0，运行 `IISReset` 以重新启动 IIS。
3. 对于这两个平台，请重新启动 Active Directory Federation Services `(adfssrv) service.` **注意：** 如果您使用的是 Windows 2016 或 Windows 10，请使用以下 PowerShell 命令启用它。`Set-AdfsProperties -EnableRelayStateForIdpInitiatedSignOn $true`

命令链接

Citrix Secure Private Access 上的应用程序配置

您可以配置 IdP 发起的流程或 SP 发起的流程。在 Citrix Secure Private Access 中配置 IdP 或 SP 发起的流程的步骤是相同的，不同之处在于，对于 SP 发起的流程，您必须在 UI 中选择**使用指定 URL 启动应用程序 (SP 发起)**复选框。

IdP 发起的流程

1. 在设置 IdP 发起的流程时，请配置以下内容。
   - **应用程序 URL** – 应用程序 URL 使用以下格式。`https://<adfs fqdn>/adfs/ls/idpinitiatedsignon.aspx?LoginToRP=<rp id>&RedirectToIdentityProvider=<idp id>`
   - **ADFS FQDN** – 您的 ADFS 设置的 FQDN。
   - **RP ID** – RP ID 是您可以从信赖方信任中获取的 ID。它与信赖方标识符相同。如果它是 URL，则会进行 URL 编码。
   - **IDP ID** – IdP ID 与声明提供程序信任 ID 相同。如果它是 URL，则会进行 URL 编码。

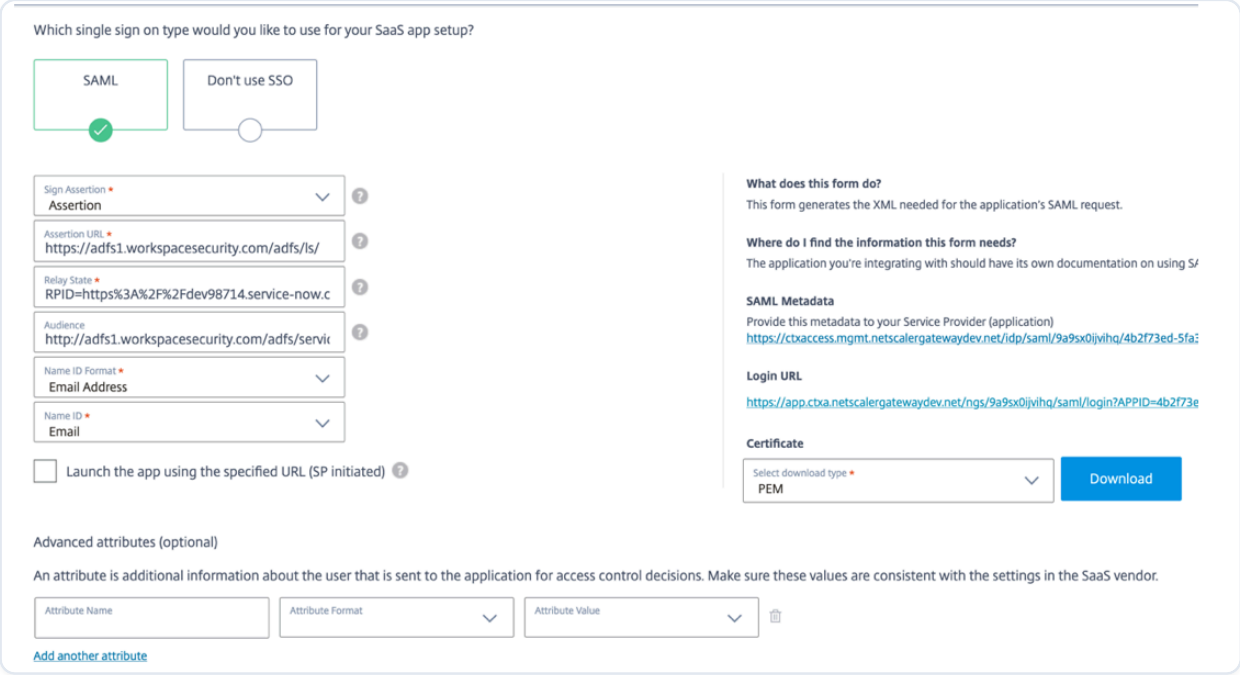
     示例
2. SAML SSO 配置。

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

以下是 ADFS 服务器的默认值。如果任何值发生更改，请从 ADFS 服务器的元数据中获取正确的值。ADFS 服务器的联合元数据可以从其联合元数据端点下载，该端点可以从 **ADFS > 服务 > 端点**中得知。

- **断言 URL** – `https://<adfs fqdn>/adfs/ls/`
- **中继状态** – 中继状态对于 IdP 发起的流程很重要。请按照此链接正确构建它 - 中继状态

  示例： RPID=https%3A%2F%2Fdev98714.service-now.com&RelayState=https%3A%2F%2Fdev98714.service-now.com%2F
- **受众** – `http://<adfsfqdn>/adfs/services/trust`
- 有关其他 SAML SSO 配置设置，请参阅下图。有关更多详细信息，请参阅支持 SaaS 应用程序。



3. 保存并将应用程序订阅给用户。

SP 发起的流程

对于 SP 发起的流程，请按照“**IDP 发起的流程**”部分中的说明配置设置。此外，请启用“**使用指定 URL 启动应用程序 (SP 发起)**”复选框。

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

Citrix 安全私有访问 Terraform 提供程序

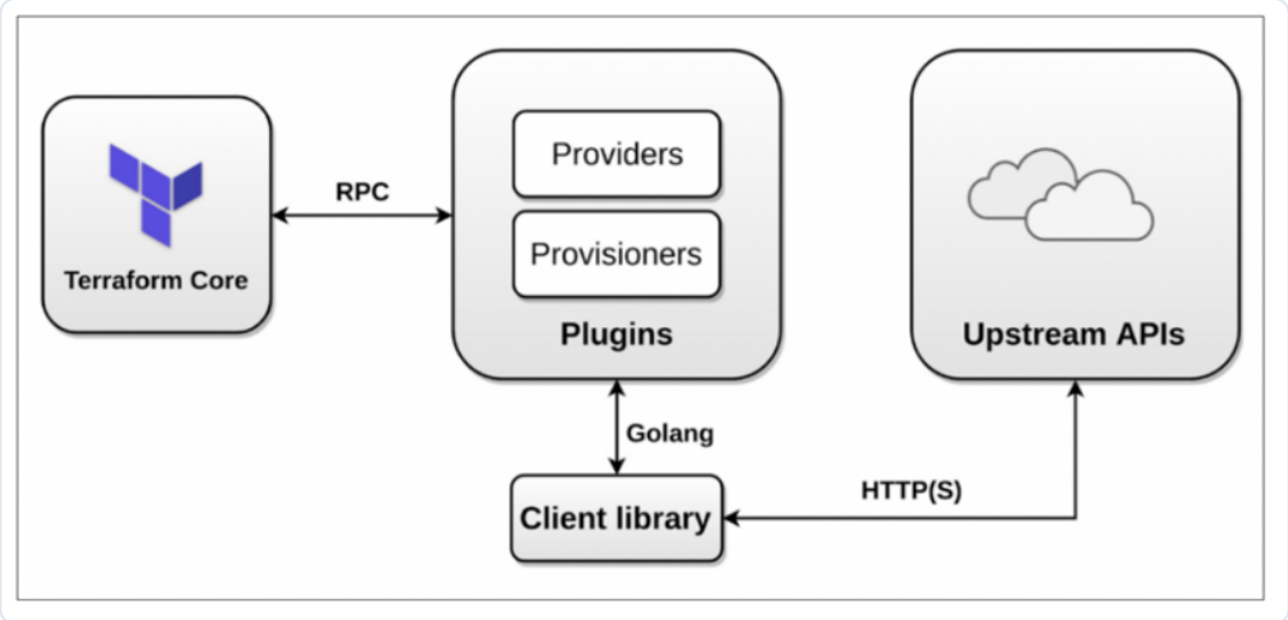
通过 UI 手动管理 Secure Private Access™ 配置耗时、易出错，并且难以在不同环境中扩展。采用基础设施即代码实践的客户需要一种方法来自动化 Secure Private Access 配置、强制保持一致性，并将 Secure Private Access 更改集成到 CI/CD 管道中。

Citrix Secure Private Access Terraform 提供程序使客户能够使用 Terraform 以编程方式预配、配置和管理 Secure Private Access 资源。它允许作为基础设施即代码工作流的一部分，以一致、可重复和可扩展的方式管理 Secure Private Access 环境。

Citrix Secure Private Access Terraform 提供程序适用于：

- Citrix 安全私有访问云部署。
- 使用 Terraform 进行基础设施或配置管理的客户。

下图显示了 Terraform 提供程序架构：



主要优势

Citrix Secure Private Access Terraform 提供程序将 Secure Private Access 资源公开为 Terraform 管理的对象。客户可以声明性地定义 Secure Private Access 配置，将其与应用程序基础设施一起进行版本控制，并以可预测的方式应用更改。

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

使用此解决方案的主要优势包括：

- Secure Private Access 的基础设施即代码管理。
- 跨环境（开发、测试、生产）的一致配置。
- 减少手动工作量和配置漂移。
- 易于与 CI/CD 管道和 GitOps 工作流集成。
- 更快的入门和可重复的部署。

用例

您可以将 Citrix Secure Private Access Terraform 提供程序用于以下用例：

- 实现新应用程序和策略在 Secure Private Access 中的自动化载入。
- 跨多个环境标准化 Secure Private Access 配置。
- 使用版本化的 Terraform 状态重新创建或恢复 Secure Private Access 环境。
- 将 Secure Private Access 配置更改集成到现有 Terraform 工作流中。
- 使 DevOps 团队能够与基础架构一起管理访问策略。
- 将 Secure Private Access 配置从试用租户迁移到生产租户。
- 合并 2 个客户的 Secure Private Access 配置以应对收购场景。

系统要求

确保满足以下系统要求：

- Terraform v1.3 或更高版本。
- 获取对 Citrix Secure Private Access 租户的访问权限。
- 与 Citrix Cloud™ API 的网络连接。

先决条件

在使用 Citrix Secure Private Access Terraform Provider 之前，请确保满足以下先决条件：

- 您拥有有效的 Citrix Secure Private Access 订阅。
- 您拥有在 Citrix 租户中管理 Secure Private Access 资源的权限。
- Terraform 已安装并在您的环境中可用。
- 用于 Citrix Cloud 的 API 凭据或身份验证方法已配置。

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

权限

Terraform 使用的服务主体身份验证帐户必须拥有以下权限：

- 创建、更新和删除 Secure Private Access 资源。
- 读取现有的 Secure Private Access 配置以进行状态协调。

安装

请参阅 安装 Terraform 并配置 Citrix Terraform Provider。

Terraform 配置

借助 Terraform Provider，可以在 Citrix UI 之外管理 Secure Private Access 配置。客户可以根据需要继续使用 UI，但 Terraform 是用于自动化和大规模部署的推荐方法。

要将 Terraform Provider 用于 Secure Private Access，您必须在您的 Terraform 配置中定义该 Provider，如下所示：

```
terraform {

  required_providers {

    citrixspa = {

      source = "citrix/citrixspa"

      version = `<version>`

    }

  }

}



provider "citrixspa" {

  base_url      = "<https://api.cloud.com/accessSecurity>"  # for
commercial deployment
```

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

```
  customer_id   = "xxxxxxxxxxxxx" # the CC customer id

  client_id     = "xxxxxxxxxxxxx" # client id of service principal

  client_secret = "xxxxxxxxxxxxx" # client secret of service principal

}
```

一旦配置了提供程序，您就可以使用 Terraform 资源块定义 Secure Private Access 资源，并使用标准 Terraform 命令（例如：）应用它们。

- `terraform plan`
- `terraform apply`

注意：

Terraform 提供程序在 Terraform 配置中声明并初始化后，默认启用。

故障排除

- **`terraform apply` 操作因身份验证错误而失败。**

  原因： Citrix Cloud 凭据无效或缺失。

  解决方案： 验证提供程序身份验证配置和权限。

- **在 `terraform plan` 中检测到意外更改。**

  原因： 由于手动 UI 更改导致配置漂移。

  解决方案： 通过 Terraform 对齐更改，并在需要时刷新状态。

限制

- 并非所有 Secure Private Access 功能都可能在提供程序的初始版本中可用。
- 直接在 UI 中进行的更改可能会导致 Terraform 状态漂移。
- `terraform destroy` 操作可能不会自动删除所有依赖资源。

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

重要注意事项

- Terraform 状态文件可能包含敏感配置数据，必须安全存储（例如，远程后端）。
- 我们建议您在采用后，仅使用 Terraform 管理 Secure Private Access 资源。
- 我们强烈建议固定提供程序版本，以避免意外更改。
- 在应用更改之前，请务必查看 `terraform plan` 输出。

参考

- Terraform 注册表文档
- Terraform 文档

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

可见性和监控

管理员可以利用以下功能和资源，对 Secure Private Access 进行可见性和监控。

监控

Secure Private Access 已与 Monitor（Citrix DaaS 的监控和故障排除控制台）集成。管理员和技术支持人员除了 Secure Private Access 控制面板之外，还可以从 DaaS Monitor 监控和排除 Web/SaaS 和 TCP/UDP 应用程序会话和事件。有关详细信息，请参阅 与 DaaS Monitor 集成。

Secure Private Access 使用情况控制面板

Secure Private Access 用户、应用程序、策略和连接器状态的可见性可在 Secure Private Access 控制面板中获取。管理员可以使用控制面板监控这些事件。有关详细信息，请参阅 控制面板。

Secure Private Access 应用程序和会话监控

通过使用 Citrix Monitor 监控您的 Secure Private Access 会话和整个组织中的应用程序趋势。有关详细信息，请参阅以下主题：

- Monitor 为会话和应用程序提供筛选功能，从而更轻松地分析用户活动并解决应用程序性能问题。有关详细信息，请参阅 会话和应用程序监控。
- 管理员可以在 Monitor 中查看会话和错误趋势，这有助于识别模式并排除故障。有关详细信息，请参阅 错误和会话趋势。

连接器设备运行状况监控

部署 Secure Private Access 时，连接器设备组件会自动作为基础结构监控的一部分添加。连接到 Citrix DaaS 站点的任何连接器设备都会自动加入以进行全面监控，为管理员提供这些关键基础结构组件的运行状况和性能的实时可见性。

有关连接器设备运行状况监控的更多信息，请参阅 连接器设备运行状况指标。

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

Secure Private Access 使用情况仪表板

Secure Private Access 服务仪表板显示 SaaS、Web、TCP 和 UDP 应用程序的诊断和使用情况数据。该仪表板为管理员提供对其应用程序、用户、连接器运行状况以及带宽使用情况的全面可见性，所有这些都集中在一个位置供其使用。此数据从 Citrix Analytics 获取。可以针对预设时间或自定义时间线查看各种实体的数据。对于某些实体，您可以向下钻取以查看更多详细信息。

指标大致分为以下几类。

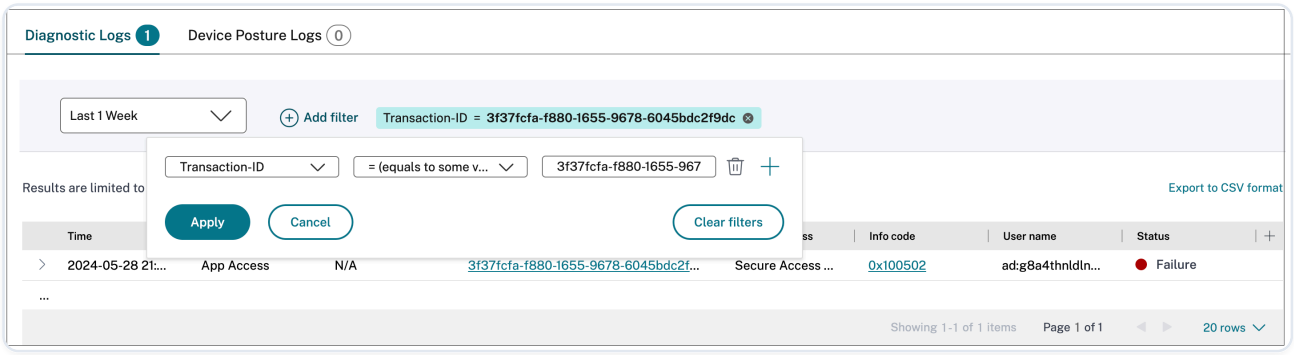
- **日志记录和故障排除**
  - 诊断日志：与身份验证、应用程序启动、应用程序枚举和设备状态检查相关的日志。
- **用户**
  - 活跃用户：在选定时间间隔内访问应用程序（SaaS、Web 和 TCP）的唯一用户总数。
  - 上传：在选定时间间隔内通过 Secure Private Access 服务上传的数据总量。
  - 下载：在选定时间间隔内通过 Secure Private Access 服务下载的数据总量。
- **应用程序：**
  - 应用程序：当前配置的应用程序总数（与时间间隔无关）。
  - 应用程序启动计数：在选定时间间隔内每个用户启动的应用程序（应用程序会话）总数。
  - 已配置域：在选定时间间隔内配置的域总数。
  - 已发现应用程序：已访问但未与任何应用程序关联的唯一独立域的总数。
- **访问策略**
  - 访问策略：当前配置的访问策略总数（与时间间隔无关）。

诊断日志

使用“**诊断日志**”图表查看与身份验证、应用程序启动、应用程序枚举以及设备状态相关的日志。您可以单击“**查看更多**”链接查看日志详细信息。详细信息以表格形式呈现。您可以查看预设时间或自定义时间范围内的日志。您可以通过单击“+”号向图表添加列，具体取决于您希望在仪表板中看到的信息。您可以将用户日志导出为 CSV 格式。

- 您可以使用“**添加筛选器**”选项根据应用程序类型、类别、描述等各种条件优化搜索。例如，在搜索字段中，您可以按此顺序选择 `Transaction ID`、`= (equals to some value)` 并输入 `7456c0fb-a60d-4bb9-a2a2-edab8340bb15`，以搜索与此事务 ID 相关的所有日志。有关可与筛选器选项一起使用的搜索运算符的详细信息，请参阅搜索运算符。

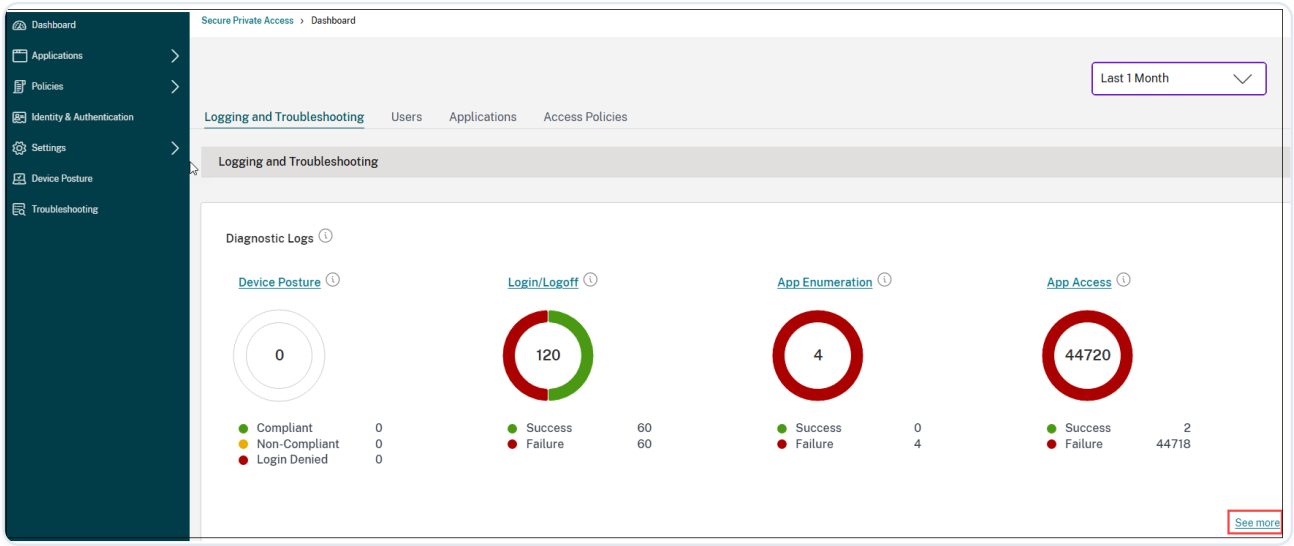
© 1997–2026 Citrix Systems, Inc. All rights reserved.



- **设备状态日志：** 您可以根据策略结果（**合规、不合规和拒绝登录**）优化搜索。有关设备状态的详细信息，请参阅设备状态。

注意：

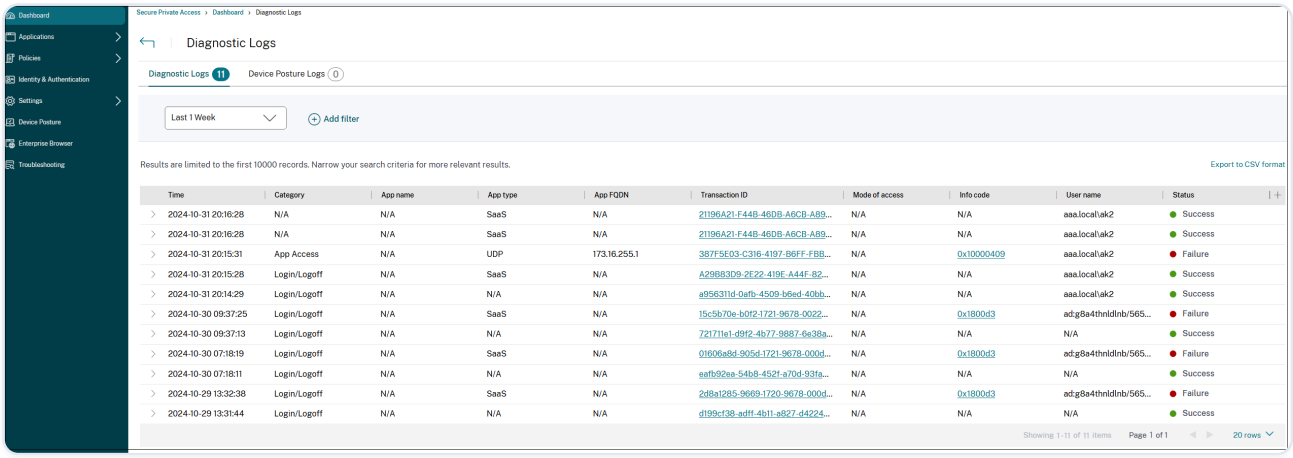
- Secure Private Access 诊断日志仪表板中的每个失败事件都有一个关联的信息代码。有关详细信息，请参阅信息代码。
- 事务 ID 关联访问请求的所有 Secure Private Access 日志。有关详细信息，请参阅事务 ID。



- 您可以单击展开图标 (>) 查看日志的完整详细信息。
- “**诊断日志**”页面显示所访问的每个主 URL 的嵌入式域。管理员可以通过单击主 URL 旁的展开图标 (>) 查看嵌入式域。管理员可以使用嵌入式域列表来解决与应用程序访问或应用程序呈现相关的问题。例如，如果应用程序配置中缺少某个域，则最终用户无法访问该特定应用程序。在这种情况下，管理员可以查看嵌入式域列表，识别缺失的域，然后使用缺失的域更新应用程序配置。

默认情况下，“**诊断日志**”页面显示当前周的数据和最近的 10000 条记录。使用自定义日期搜索和筛选器进一步优化您的搜索结果。

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

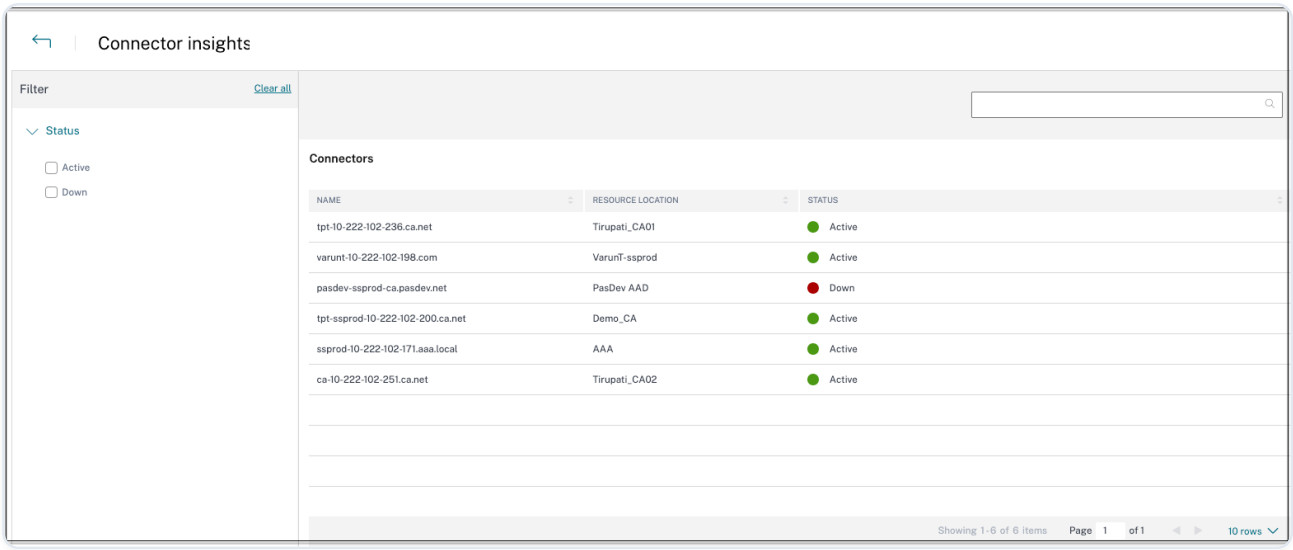


重要提示：

有关用户在使用 Secure Private Access 服务时可能遇到的错误的完整列表，请参阅 信息代码查找表。

连接器状态

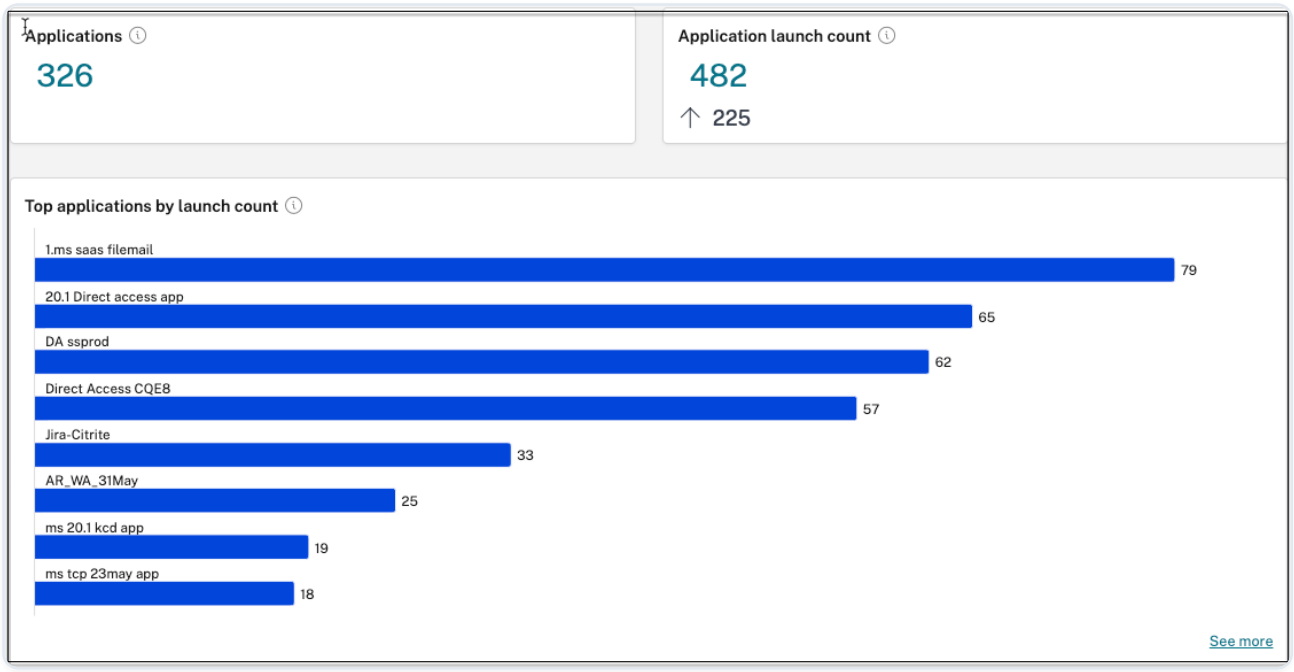
使用“**连接器状态**”图表查看连接器的状态以及部署连接器的资源位置。单击“**查看更多**”链接以查看详细信息。在“**连接器洞察**”页面中，您可以使用“**活动**”或“**非活动**”筛选器根据连接器的状态对其进行筛选。



按启动次数排名的热门应用程序

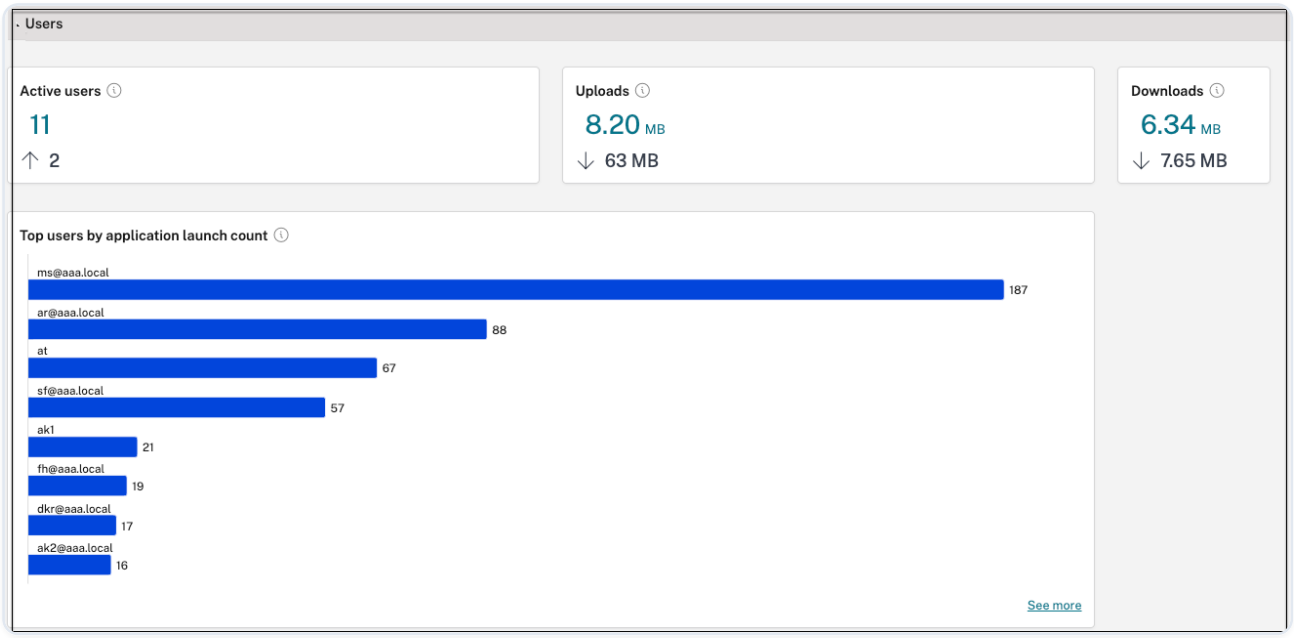
使用“**按启动次数排名的热门应用程序**”图表可查看根据应用程序启动次数、上传到应用程序服务器的数据总量以及从应用程序服务器下载的数据总量列出的热门应用程序列表。您可以应用“**SaaS 应用程序**”、“**Web 应用程序**”或“**TCP/UDP 应用程序**”筛选器来缩小搜索范围，以查找特定应用程序。您可以按预设时间线或自定义时间线筛选数据。

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



按应用程序启动次数排名的热门用户

使用“**按应用程序启动次数排名的热门用户**”图表可查看每个用户的数据。例如，用户启动 TCP 应用程序的次数、上传到应用程序服务器的数据总量以及从应用程序服务器下载的数据总量。您可以按预设时间线或自定义时间线筛选数据。



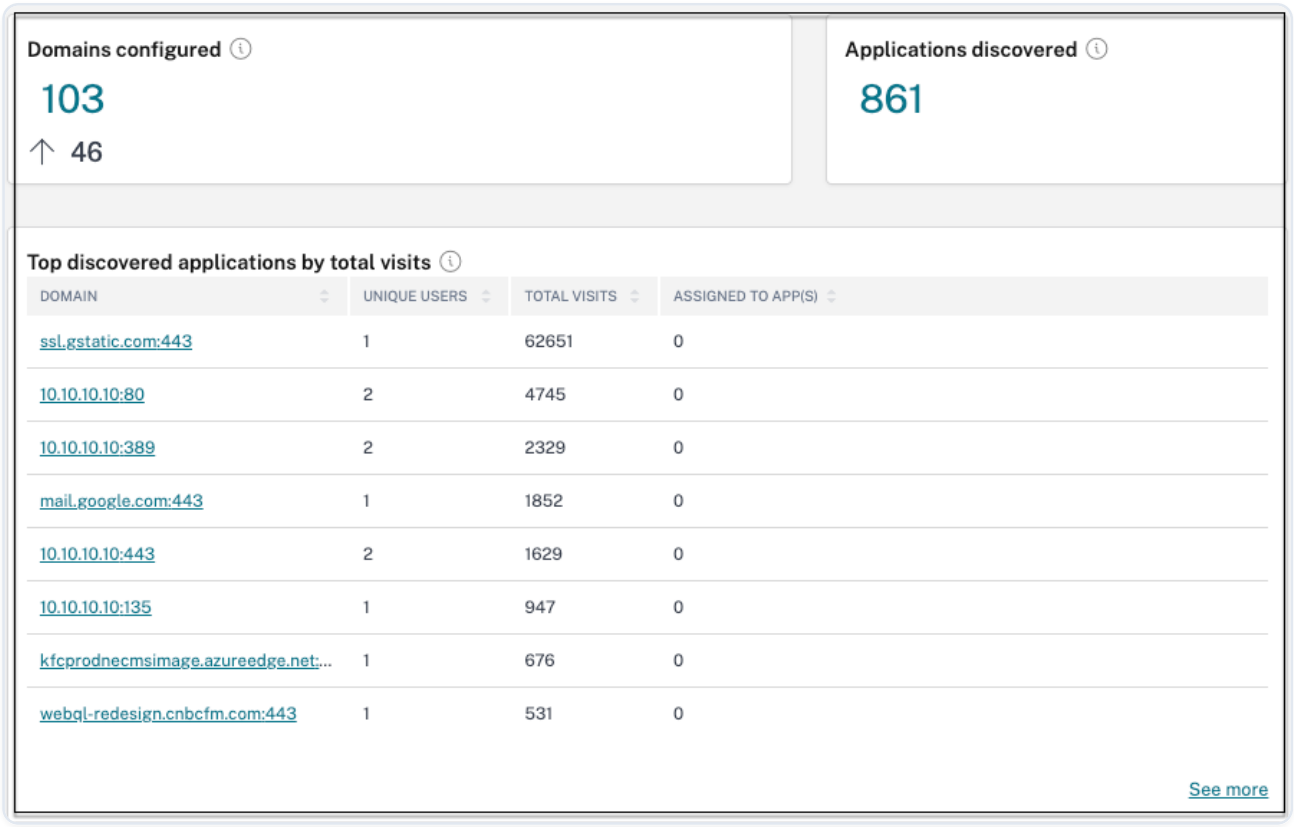
按强制执行次数排名的热门访问策略

使用“**按强制执行次数排名的热门访问策略**”图表可查看在应用程序上强制执行的访问策略列表。单击“**查看更多**”链接可查看与应用程序关联的策略列表以及策略的强制执行次数。您还可以使用“访问策略”页面中的“**搜索**”选项根据策略名称筛选策略。您还可以使用搜索运算符搜索特定策略，以进一步优化搜索。有关详细信息，请参阅 搜索运算符。

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

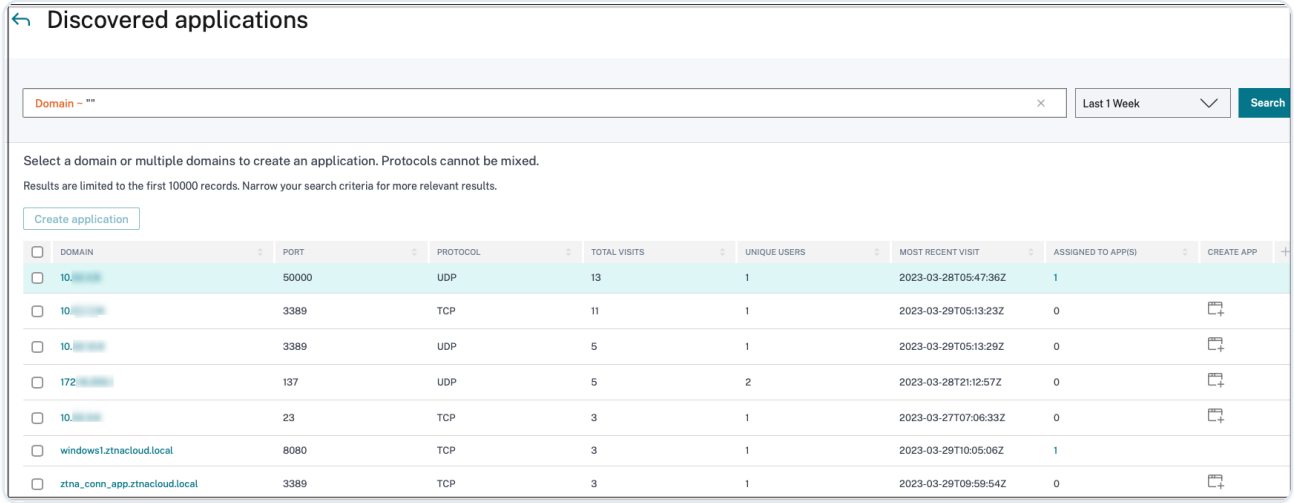
热门发现应用程序

使用“**按总访问量排名的热门发现应用程序**”可查看在某个时间点被访问过但未与任何应用程序关联的唯一独立域列表。这些域根据对这些域的总访问次数进行列出。管理员可以使用此图表查看是否有许多用户访问了任何特别感兴趣的域。在这种情况下，管理员可以创建包含该域的应用程序，以便于访问。



在图表中，**分配给应用程序**列显示将此域配置为其相关 URL 或目标 URL 值一部分的应用程序总数。单击该数字会显示分配给此域的应用程序。

您可以单击**查看更多**链接以查看所有域的更多详细信息。



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

发现的应用程序页面显示域的详细信息，例如域名、端口、协议、总访问量、唯一用户和最近访问日期。图表中的所有列均可排序。您可以使用搜索栏根据域进行搜索。

注意：

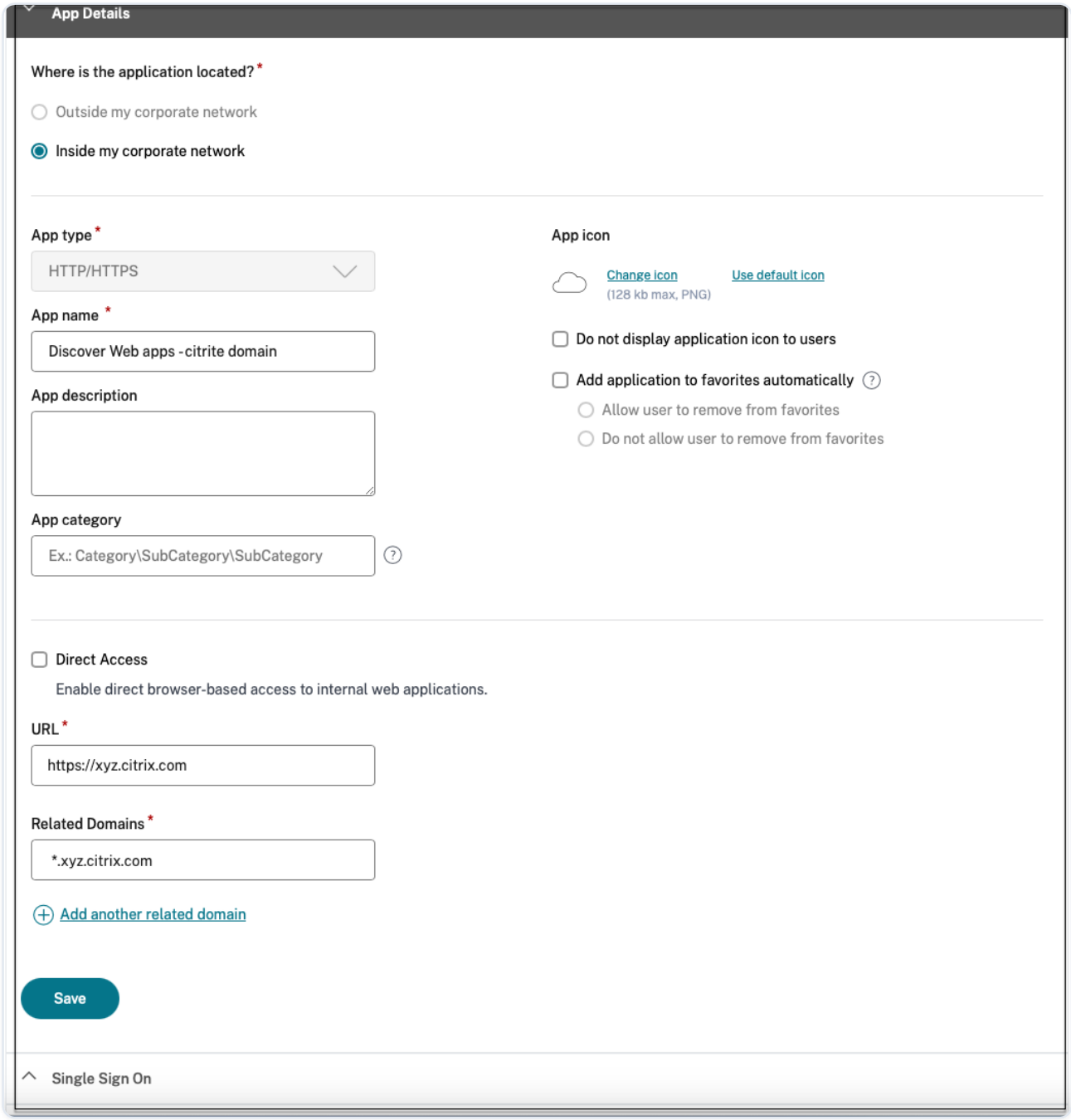
- 协议是根据客户使用的标准端口派生的。
- 发现的域列表限制为 10000 条记录。

从图表创建应用程序

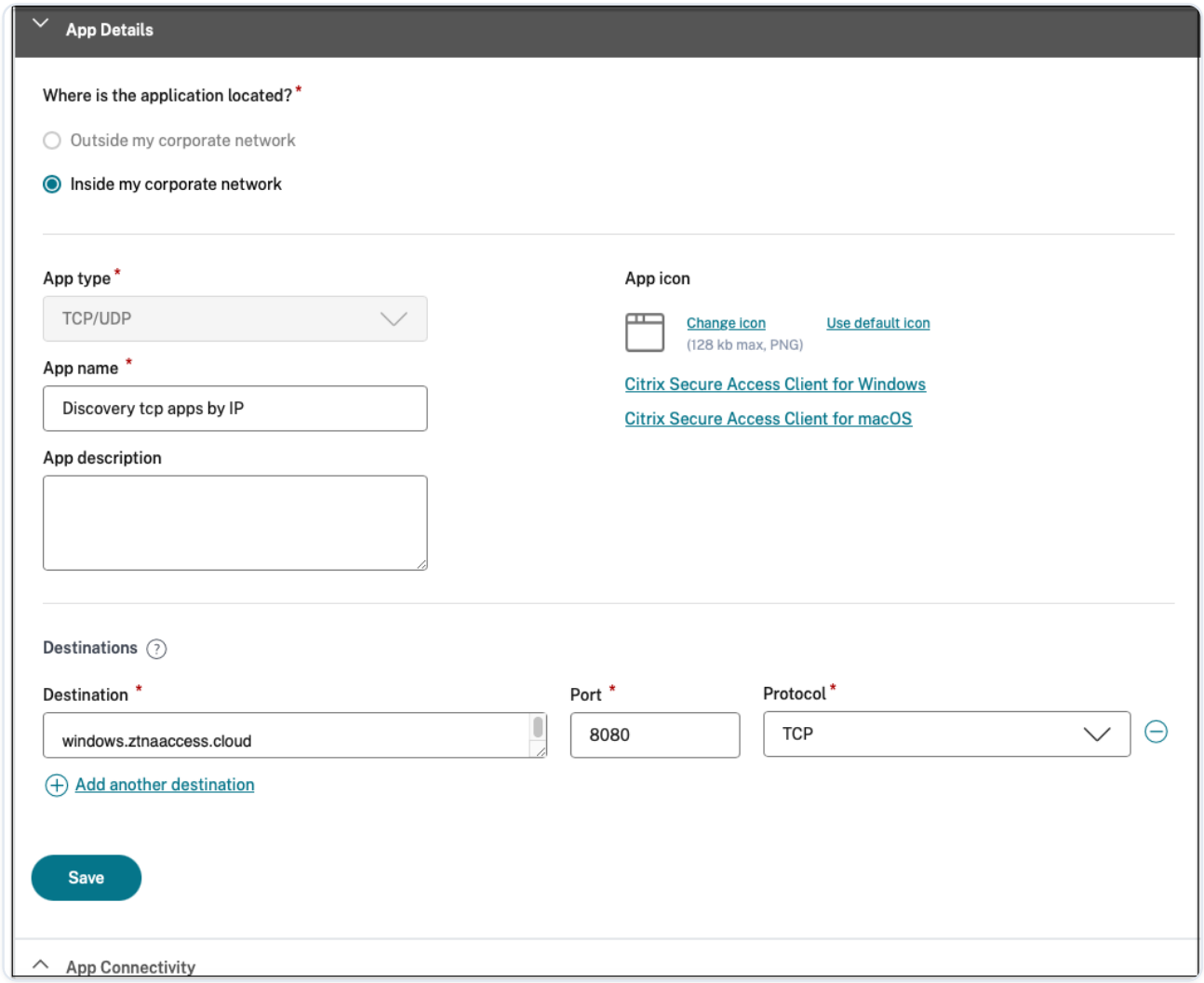
单击相应域旁边的 **+** 图标以创建应用程序。应用程序配置向导弹出。对于已使用相同域、端口和协议组合创建且处于完成状态的行，不会显示创建应用程序图标。

- 应用程序类型会根据您选择的应用程序协议自动填充。但是，如有必要，您可以更改类型。
- **URL、相关域、目标、端口、协议**字段中的值都会自动填充。完成添加应用程序的步骤。有关详细信息，请参阅管理员引导的轻松入门和设置工作流。

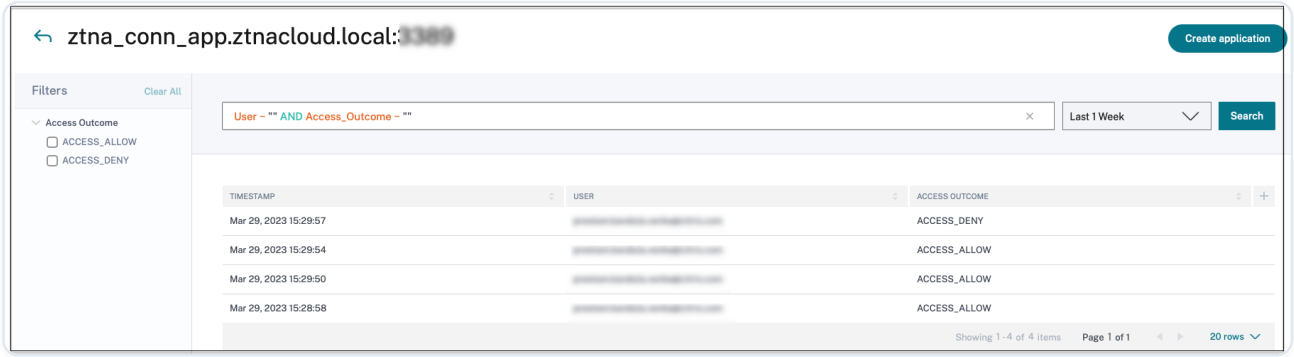
© 1997–2026 Citrix Systems, Inc. All rights reserved.



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



您还可以单击唯一域链接以查看更多详细信息并为该域创建应用程序。当您单击域链接时，将显示该域的用户身份验证日志。单击**创建应用程序**按钮。完成添加应用程序的步骤。



搜索运算符

以下是可用于优化搜索的搜索运算符：

- **= (等于某个值)**：用于搜索与搜索条件完全匹配的日志/策略。
- **!= (不等于某个值)**：用于搜索不包含指定条件的日志/策略。
- **~ (包含某个值)**：用于搜索部分匹配搜索条件的日志/策略。

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

- **!~ (不包含某个值)**：用于搜索不包含某些指定条件的日志/策略。

安全私有访问应用程序、会话和趋势

安全私有访问与 Monitor 集成，Monitor 是 Citrix DaaS 的监控和故障排除控制台。管理员和技术支持人员可以使用此集成，从 DaaS Monitor 控制台监控和排除 Web/SaaS 和 TCP/UDP 应用程序会话和事件。这提供了额外的监控功能，补充了安全私有访问控制面板。

要将 DaaS Monitor 功能与安全私有访问结合使用，您必须同时拥有安全私有访问和 DaaS 授权。

您可以从安全私有访问控制面板 (**转到 Monitor**) 或从 Citrix DaaS 服务磁贴访问 Monitor。

要了解有关与 Monitor 集成的更多信息，请参阅 安全私有访问。

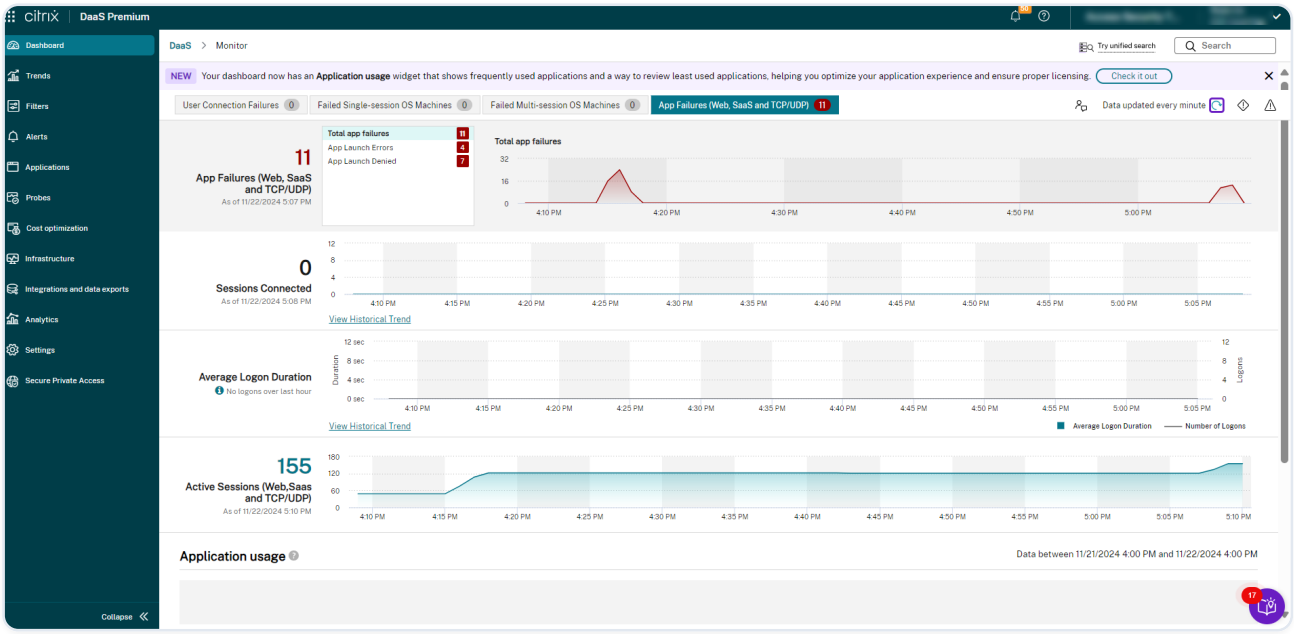
应用程序、会话和趋势

Monitor 提供了对安全私有访问会话及其相关趋势的增强可见性。这种全面的监控功能提供了对应用程序如何被访问和使用的精细洞察，以及这些会话中单个用户活动的详细信息。这使管理员能够更深入地了解用户行为、应用程序性能，从而实现对安全私有访问环境的积极管理和优化。

要了解安全私有访问上下文中的会话定义，请参阅 会话定义。

要按用户查看安全私有访问会话，请参阅 查看用户会话。

要查看会话详细信息，请参阅 安全私有访问服务的可见性。



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

运行状况监控

以下各节提供了有关运行状况监控的更多信息。

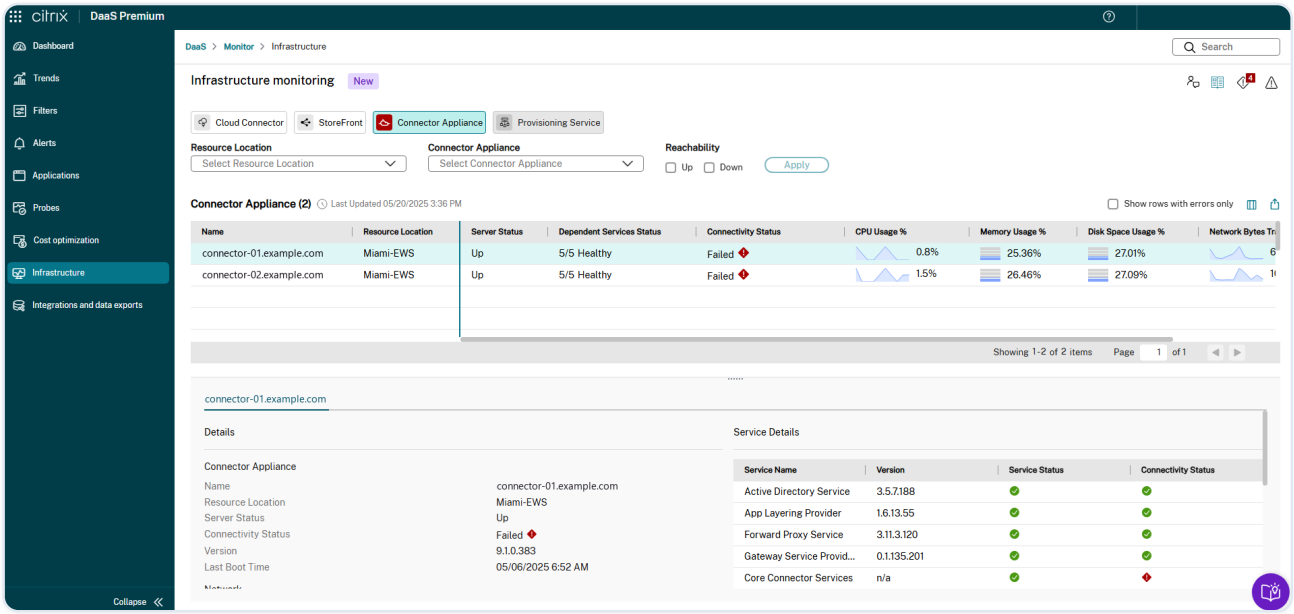
连接器设备

连接器设备是托管在您的虚拟机管理程序中的 Citrix 组件。它充当 Citrix Cloud 与您的资源位置之间的通信渠道，无需任何复杂的网络或基础结构配置即可实现云管理。连接器设备使您能够管理并专注于为用户提供价值的资源。有关详细信息，请参阅适用于 Secure Private Access 的连接器设备。

连接器设备运行状况指标功能提供了监控 Citrix 基础结构中连接器设备组件运行状况和性能的基本功能。此组件在连接到 Citrix DaaS 站点时会自动加入监控，从而确保无缝集成到基础结构监控控制板中。

运行状况指标显示在基础结构监控控制板中，提供连接器设备状态的集中视图。管理员可以访问详细的指标和趋势，以主动识别和解决问题。

下图显示了 Monitor 中连接器设备运行状况的示例。



会话和应用程序趋势

管理员可以从 DaaS Monitor 监控其组织中的会话和应用程序趋势。这包括跟踪部署、了解策略和配置的运行情况以及分析潜在问题。

有关详细信息，请参阅Secure Private Access Service 的可见性。

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

会话和应用程序趋势

使用 Citrix Monitor 监控整个组织中的 Secure Private Access 会话和应用程序趋势。跟踪部署进度，了解策略和配置的执行情况，并确定它们是否导致了广泛的用户问题。Citrix Monitor 提供对用户活动和应用程序使用模式的全面可见性，以优化您的部署。

Citrix Monitor 提供对 Secure Private Access 环境的实时和历史洞察，使管理员能够就资源分配、策略调整和用户体验改进做出数据驱动的决策。监控功能可帮助您保持最佳性能，同时确保安全合规性。

会话监控

管理员可以使用 Monitor 实时监控活动用户会话。您可以在控制板中监控 Web/SaaS 和 TCP/UDP 应用程序的应用程序故障，并查看 Web/SaaS 应用程序的活动会话。有关详细信息，请参阅 Secure Private Access 服务的可见性。

应用程序趋势

监控 Secure Private Access 应用程序访问趋势，查看活动应用程序会话，并识别出现问题或故障的应用程序。Citrix Monitor 提供全面的分析，帮助您了解应用程序使用模式、优化性能并确保可靠访问组织的关键应用程序。

有关访问这些监控功能和解释数据的详细信息，请参阅 Secure Private Access 服务的可见性。

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

分类和故障排除

本主题概述了有效排查和分类与 Citrix Secure Private Access 相关问题的重要注意事项和步骤。管理员可以使用本文档作为识别、诊断和解决问题的指南，确保用户获得无缝且安全的访问。

有关详细信息，请参阅以下主题：

排查应用程序相关问题

查看与设备姿态状态、登录/注销状态、应用程序枚举和应用程序访问相关的问题。有关详细信息，请参阅排查应用程序相关问题。

DaaS Monitor 中的 Secure Private Access 会话代码

在 Citrix Monitor 中查看与应用程序枚举、应用程序启动和会话相关的错误代码列表。有关详细信息，请参阅DaaS Monitor 中的 Secure Private Access 会话代码。

在 Monitor 中排查会话相关问题

使用 Monitor 的帮助台视图（活动管理器页面）查看有关用户或端点的信息。有关详细信息，请参阅在 Monitor 中排查会话相关问题。

排查设备姿态相关问题

当用户通过 Secure Private Access 或 DaaS 连接时，会为每个会话生成一个事务 ID，您可以使用此事务 ID 在 DaaS Monitor 中排查设备姿态问题/错误。找到事务 ID 后，DaaS Monitor 会显示有关会话和所应用的关联设备姿态策略的信息。Monitor 还会显示策略结果，包括设备是否通过了姿态检查。有关详细信息，请参阅设备姿态服务故障排除。

排查身份验证相关问题

每当任何条件身份验证失败时，您都可以使用失败消息中提供的事务 ID，并在 Monitor 中搜索失败详细信息。Monitor 通过在 Monitor UI 上显示失败原因和条件策略，帮助您排查条件身份验证失败事件。有关详细信息，请参阅身份验证故障排除。

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

使用日志进行故障排除

Secure Private Access 和 Device Posture 日志可帮助管理员识别配置问题、连接问题、策略配置错误和设备合规性问题，从而更快地识别和解决问题。

安全私有访问日志

您可以从 Secure Private Access 控制板查看 Secure Private Access 日志。有关诊断日志中捕获的各种事件的信息，请参阅 事件。

有关 Secure Private Access 诊断日志的更多信息，请参阅 诊断日志。

有关与每个事件关联的各种错误代码，请参阅 诊断日志信息代码。

设备姿态日志

Device Posture 控制板中的诊断日志提供了设备合规性（合规、不合规和登录被拒绝）的见解。这些日志使管理员能够监控端点安全性，确保遵守组织策略，并识别可能带来环境风险的设备。

您可以在 Secure Private Access 控制板 和 身份和访问管理控制台 中查看 Device Posture 日志和事件。

有关更多信息，请参阅 Device Posture 日志和事件。

使用 Monitor 进行实时会话故障排除

管理员可以使用 Monitor 控制台实时监控和排除 Secure Private Access 会话的故障。

有关相关信息，请参阅以下主题：

- 有关将 Secure Private Access 与 Monitor 集成的信息，请参阅 与 DaaS Monitor 集成。
- 您可以在 Monitor 中搜索 Secure Private Access 用户会话，以快速定位特定会话，用于故障排除和报告。有关详细信息，请参阅 按用户查看 Secure Private Access 会话。
- 有关 Monitor 的更多信息，请参阅 DaaS Monitor。

诊断日志错误代码

下表提供了用户在使用 Secure Private Access 服务时可能遇到的各种错误及其相应的解决方案的完整列表。

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

信息代码	描述	解决方案
0x180022	应用程序启动失败，因为身份验证服务已关闭	应用程序启动失败，因为身份验证服务已关闭
0x1800B7	应用程序启动失败，因为应用程序 FQDN 长度超出限制	应用程序启动失败，因为应用程序 FQDN 长度超出限制
0x1800A0, 0x1800A2, 0x1800A3, 0x1800A5, 0x1800A6, 0x1800A7	Web 应用程序启动失败，因为无法连接到后端 Web 应用程序	Web 应用程序启动失败，因为无法连接到后端 Web 应用程序
0x18001A, 0x18001B	未找到用户详细信息	未找到用户详细信息
0x1800AA	Web/SaaS 应用程序启动失败，因为在准备 SAML 令牌时未找到用户属性	Web/SaaS 应用程序启动失败
0x180010	Web/SaaS 应用程序启动失败，因为无法识别应用程序 FQDN	Web/SaaS 应用程序启动失败，因为无法识别应用程序 FQDN
0x180040	Web/SaaS 应用程序启动失败，原因是 SAML 服务提供商提供了无效的 appId	应用程序启动失败，原因是 SAML 服务提供商提供了无效的 appId
0x180011, 0x180012, 0x180013, 0x180017, 0x180032, 0x180033, 0x180034, 0x180035, 0x180048	Web/SaaS 应用程序启动失败，原因是应用程序访问请求无效	Web/SaaS 应用程序启动失败，原因是应用程序访问请求无效
0x1800D4, 0x1800E1, 0x180106, 0x180107, 0x1800EB, 0x1800EC	应用程序启动在策略评估期间失败，原因是内部错误	应用程序启动在策略评估期间失败，原因是内部错误
0x1800D9	应用程序启动在解析策略评估响应时失败	应用程序启动在解析策略评估响应时失败
0x1800DA	应用程序启动在策略评估期间因结果无效而失败	应用程序启动在策略评估期间因结果无效而失败

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

信息代码	描述	解决方案
0x1800DB	应用程序启动失败，原因是资源位置配置无效	应用程序启动失败，原因是资源位置配置无效
0x1800E0	应用程序启动失败，原因是应用程序名称的长度过长	应用程序启动失败，原因是应用程序名称的长度过长
0x1800EE	应用程序启动失败，原因是在连接到专用 TCP 服务器期间应用程序 ID 无效	应用程序启动失败，原因是在连接到专用 TCP 服务器期间应用程序 ID 无效
0x1800E3	应用程序启动在策略评估期间被拒绝	应用程序启动在策略评估期间被拒绝
0x1800EA	应用程序启动失败，原因是目标 FQDN 过长	应用程序启动失败，原因是目标 FQDN 过长
0x1800ED	应用程序启动失败，因为目标 IP 无效	应用程序启动失败，因为目标 IP 无效
0x180102	应用程序启动失败，因为未从连接器设备收到响应	应用程序启动失败，因为未从连接器设备收到响应
0x10000005	Web/SaaS 应用程序启动失败，因为无法与后端应用程序服务器建立连接	Web/SaaS 应用程序启动失败，因为无法与后端应用程序服务器建立连接
0x10000101, 0x10000102, 0x10000103, 0x10000104	Web/SaaS FormFill SSO 失败，因为应用程序配置无效	Web/SaaS FormFill SSO 失败，因为应用程序配置无效
0x10000202	Web/SaaS 的 Kerberos SSO 失败	Web/SaaS 的 Kerberos SSO 失败
0x10000203	Web/SaaS SSO 因内部服务器错误而失败	Web/SaaS SSO 因内部服务器错误而失败
0x10000303, 0x10000304	Web/SaaS 应用程序启动失败，因为配置的代理不可达	Web/SaaS 应用程序启动失败，因为配置的代理不可达
0x10000305	Web/SaaS 应用程序启动失败，因为无法通过配置的代理进行身份验证	Web/SaaS 应用程序启动失败，因为无法通过配置的代理进行身份验证

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

信息代码	描述	解决方案
0x10000414	应用程序启动失败，因为请求来自无效的 IP/主机名或端口	应用程序启动失败，因为请求来自无效的 IP/主机名或端口
0x10000415	应用程序启动失败，因为目标服务器拒绝了连接	应用程序启动失败，因为目标服务器拒绝了连接
0x10000416	应用程序启动失败，因为未找到目标	应用程序启动失败，因为未找到目标
0x10000417	应用程序启动失败，因为目标网络不可达	应用程序启动失败，因为目标网络不可达
0x10000405	应用程序启动失败，因为无法连接到目标	应用程序启动失败，因为无法连接到目标
0x10000301	连接器到 SPA 服务的连接失败	连接器到 Secure Private Access 服务的连接失败
0x10000302	连接器未能读取代理详细信息	连接器未能读取代理详细信息
0x10000306	配置的代理不可达	配置的代理不可达
0x10000401	连接器设备无法连接到 FR	连接器设备无法连接到 FR (边缘节点)
0x10000403, 0x10000404, 0x10000407	由于内部连接错误，应用程序启动失败	由于内部连接错误，应用程序启动失败
6003, 6007	Citrix Secure Access 客户端未能执行 SSO	Citrix Secure Access 客户端未能执行 SSO

应用程序启动失败，因为身份验证服务已关闭

信息代码： 0x180022

Secure Private Access 允许管理员配置第三方身份验证服务，例如传统的 Active Directory、AAD、Okta 或 SAML。这些身份验证服务的中断可能导致此问题。

检查第三方服务器是否已启动并可访问。

应用程序启动失败，因为应用程序 FQDN 长度超出限制

信息代码： 0x1800B7

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

应用程序 FQDN 不得超过 512 个字符。请检查应用程序配置页面中的应用程序 FQDN，确保其未超出此限制。

1. 转到管理控制台中的**应用程序**选项卡。
2. 查找 FQDN 超过 512 个字符的应用程序。
3. 编辑应用程序并修复应用程序 FQDN 长度。

Web 应用程序启动失败，因为无法连接到后端 Web 应用程序

信息代码： 0x1800A0, 0x1800A2, 0x1800A3, 0x1800A5, 0x1800A6, 0x1800A7

企业网络中运行的 Web 应用程序的浏览体验中断。

1. 筛选诊断日志，查找无法解析的 FQDN。
2. 检查从企业网络内部到后端服务器的可达性。
3. 检查代理设置，查看连接器是否被阻止访问后端服务器。

未找到用户详细信息

信息代码： 0x18001A, 0x18001B

Secure Private Access 服务处理请求时未找到域用户详细信息。当 Citrix Cloud™ 中缺少必要的域用户属性时，可能会出现此问题。

1. 确保 Citrix Cloud Connector™ 在将用户同步到 Citrix Cloud 时没有问题。
2. 确保 **Citrix Cloud > Identity and Access Management** 中的域可访问。
3. 注销并重新登录 Citrix Workspace。

由于在准备 SAML 令牌时未找到用户属性，Web/SaaS 应用程序启动失败

信息代码： 0x1800AA

Secure Private Access 服务在准备 SAML 令牌时未找到必需的用户属性。当 Citrix Cloud 中缺少必需的域用户属性时，可能会出现此问题。

1. 确保 Citrix Cloud Connector 在将用户同步到 Citrix Cloud 时没有问题。
2. 确保 **Citrix Cloud > Identity and Access Management** 中的域可访问。
3. 注销并重新登录 Citrix Workspace。

由于无法识别应用程序 FQDN，Web/SaaS 应用程序启动失败

信息代码： 0x180010

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

未找到给定域名的应用程序。

确保域名长度不超过配置限制。

由于 SAML 服务提供商提供了无效的 appId，Web/SaaS 应用程序启动失败

信息代码： 0x180040

SAML 服务提供商提供的 AppId 无效。无法通过 SAML 服务提供商提供的给定应用 ID 找到该应用。

1. 检查 SAML 服务提供商配置。
2. 确保在 SAML 服务提供商处配置的 IdP URL 是正确的。
3. 此应用 ID 必须与在 Secure Private Access 服务中配置的应用相对应。

由于应用访问请求无效，Web/SaaS 应用启动失败

信息代码： 0x180011, 0x180012, 0x180013, 0x180017, 0x180032, 0x180033, 0x180034, 0x180035, 0x180048

由于 Secure Private Access 服务收到无效请求，应用访问失败。

无法识别 Secure Private Access 服务收到的应用程序。收到的请求参数可能无效。

1. 重新启动应用程序或注销并重新登录 Citrix Workspace。
2. 如果问题仍然存在，请联系 Citrix 支持。

由于内部错误，应用在策略评估期间启动失败

信息代码： 0x1800D4, 0x1800E1, 0x180106, 0x180107, 0x1800EB, 0x1800EC

请联系 Citrix 支持，并提供事务 ID 和客户端收集的调试日志。

解析策略评估响应时应用启动失败

信息代码： 0x1800D9

应用程序配置可能包含特殊字符，或者策略配置可能存在问题。

确保 TCP/UDP/HTTP 应用程序配置不包含不支持的字符。

1. 在 Secure Private Access 管理控制台中，单击“**应用程序**”。
2. 检查应用程序名称或目标是否包含任何特殊字符。

检查策略是否配置正确并已分配给正确的应用程序。

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

1. 在 Secure Private Access 管理门户中，单击“**访问策略**”。
2. 检查策略配置、策略名称和条件。
3. 检查策略是否已分配给正确的应用程序。

如果配置正确，请联系 Citrix 支持部门，并提供事务 ID 和客户端调试日志。

应用程序启动失败，策略评估期间结果无效

信息代码： 0x1800DA

可能存在应用程序或策略配置问题。确保 TCP/UDP/HTTP 应用程序配置不包含不支持的字符。

1. 在 Secure Private Access 管理控制台中，单击“**应用程序**”。
2. 检查应用程序名称或目标域/FQDN 是否包含任何特殊字符。
3. 还要检查目标 IP/IP 范围/IP CIDR 是否有效。

确保**应用程序域**表（**安全私有访问 > 设置 > 应用程序域**）已启用应用程序目标条目。

检查策略是否已正确配置并分配给正确的应用程序。

1. 在安全私有访问管理门户中，单击**访问策略**。
2. 查看策略配置、策略名称和条件。
3. 检查策略是否已分配给正确的应用程序。

应用程序启动失败，资源位置配置无效

信息代码： 0x1800DB

资源位置和配置可能存在问题

确保已配置资源位置。

1. 登录到 Citrix Cloud 门户，然后从菜单中单击**资源位置**。
2. 检查是否已配置预期的资源位置。

确保资源位置健康且处于活动状态。

1. 登录到 Citrix Cloud 门户，然后从菜单中单击**资源位置**。
2. 检查预期的资源位置是否处于活动状态且健康。

确保在**应用程序域**表（**安全私有访问 > 设置 > 应用程序域**）中为目标选择了正确的资源位置。

1. 在 Secure Private Access 管理控制台中单击**设置**。

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

2. 单击**应用程序域**选项卡。
3. 检查访问的目标是否配置了正确的资源位置。
4. 检查访问的目标条目在**应用程序域**表中是否处于活动状态。

   在 TCP/UDP/HTTP 应用程序中配置的目标会自动添加到**应用程序域**表中。建议不要删除/禁用活动 TCP/UDP/HTTP 应用程序的目标/URL。

应用程序启动失败，因为应用程序名称的长度过长

信息代码： 0x1800E0

请联系 Citrix 支持并提供事务 ID 和客户端收集的调试日志。

应用程序启动失败，原因是在与专用 TCP 服务器建立连接期间应用程序 ID 无效

信息代码： 0x1800EE

请联系 Citrix 支持并提供事务 ID 和客户端收集的调试日志。

应用程序启动在策略评估期间被拒绝

信息代码： 0x1800E3

请联系 Citrix 支持并提供事务 ID 和客户端收集的调试日志。

应用程序启动失败，因为目标 FQDN 过长

信息代码： 0x1800EA

确保 FQDN 长度小于 256 个字符。

应用程序启动失败，因为目标 IP 无效

信息代码： 0x1800ED

仅从客户端访问有效的私有 IP 地址。

应用程序启动失败，因为未收到来自连接器设备的响应

信息代码： 0x180102

检查连接器设备的可达性。

应用程序启动失败，因为请求来自无效的 IP/主机名或端口

信息代码： 0x10000414

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

检查主机名、IP 地址或端口号的有效性。

应用程序启动失败，因为目标服务器拒绝了连接

信息代码： 0x10000415

检查目标服务器的状态。

应用程序启动失败，因为未找到目标

信息代码： 0x10000416

检查目标服务器主机名。

由于目标网络不可达，应用程序启动失败

信息代码： 0x10000417

连接器设备与后端私有 TCP/UDP 服务器存在连接问题。检查 连接器设备的网络设置。

- 检查最终用户尝试连接的后端服务器是否正在运行并能够接收请求。
- 检查从公司网络内部访问后端服务器的可达性。
- 检查代理设置，查看连接器是否被阻止访问后端服务器。
- 如果请求是基于 FQDN 的应用程序，请检查 DNS 服务器中相应应用程序的 DNS 条目。

由于无法连接到目标，应用程序启动失败

信息代码： 0x10000405

连接器设备与后端私有 TCP/UDP 服务器存在连接问题。检查 连接器设备的网络设置。

- 检查最终用户尝试连接的后端服务器是否正在运行并能够接收请求。
- 检查从公司网络内部访问后端服务器的可达性。
- 检查代理设置，查看连接器是否被阻止访问后端服务器。
- 如果是基于 FQDN 的应用程序请求，请检查 DNS 服务器中相应应用程序的 DNS 条目。

连接器到 Secure Private Access 服务的连接失败

信息代码： 0x10000301

- 查找错误代码的事务 ID。
- 在 Secure Private Access 控制板中筛选所有与事务 ID 匹配的事件。

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

- 检查其他组件中是否发生与事务 ID 匹配的任何错误，如果发现，请执行与该错误代码匹配的相应解决方法。
- 如果在其他组件中未发现错误，请执行以下操作：
  - 转到连接器设备管理页面。
  - 下载诊断报告。有关详细信息，请参阅生成诊断报告。
  - 捕获数据包跟踪。有关详细信息，请参阅验证您的网络连接。
- 请联系 Citrix 支持，并提供此诊断报告、数据包跟踪以及错误代码和事务 ID。

连接器未能读取代理详细信息

信息代码： 0x10000302

连接器设备与后端专用 TCP/UDP 服务器存在连接问题。请检查连接器设备的网络设置。

- 检查最终用户尝试连接的后端服务器是否已启动并正在运行，并且能够接收请求。
- 检查企业网络内部后端服务器的可达性。
- 检查代理设置，查看连接器是否被阻止访问后端服务器。
- 如果是基于 FQDN 的应用程序请求，请检查 DNS 服务器中相应应用程序的 DNS 条目。

配置的代理不可达

信息代码： 0x10000306

连接器设备与后端私有 TCP/UDP 服务器存在连接问题。检查 连接器设备的网络设置。

- 检查最终用户尝试连接的后端服务器是否已启动并正在运行，并且能够接收请求。
- 检查企业网络内部后端服务器的可达性。
- 检查代理设置，查看连接器是否被阻止访问后端服务器。
- 如果是基于 FQDN 的应用程序请求，请检查 DNS 服务器中相应应用程序的 DNS 条目。

连接器设备无法访问 FR（边缘节点）

信息代码： 0x10000401

检查与 Citrix Secure Private Access 服务的网络连接。

有关详细信息，请参阅 连接器设备的网络设置。

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

由于内部连接错误，应用程序启动失败

信息代码： 0x10000403, 0x10000404, 0x10000407

- 查找错误代码的事务 ID。
- 在 Secure Private Access 控制板中筛选与事务 ID 匹配的所有事件。
- 检查与事务 ID 匹配的其他组件中是否发生任何错误。如果发现错误，请执行与该错误代码匹配的相应解决方法。
- 如果在其他组件中未发现错误，请执行以下操作：
  - 转到连接器设备管理页面。
  - 下载诊断报告。有关详细信息，请参阅 生成诊断报告。
  - 捕获数据包跟踪。有关详细信息，请参阅 验证您的网络连接。
- 请联系 Citrix 支持人员，并提供此诊断报告、数据包跟踪以及错误代码和事务 ID。

Web/SaaS 应用程序启动失败

由于无法与后端应用程序服务器建立连接，Web/SaaS 应用程序启动失败。

信息代码： 0x10000005

检查目标 URL 或检查连接器设备网络设置。有关详细信息，请参阅 连接器设备的网络设置。

由于应用程序配置无效，Web/SaaS FormFill SSO 失败

信息代码： 0x10000101, 0x10000102, 0x10000103, 0x10000104

检查 SSO 表单应用程序配置，并确保在应用程序设置中正确配置了用户名、密码、操作和登录 URL 字段。

Web/SaaS 的 Kerberos SSO 失败

信息代码： 0x10000202

Web/SaaS 的 Kerberos SSO 失败，原因可能是 Connector Appliance 内部服务器错误，或者无法从域控制器获取令牌。

检查后端服务器和域控制器上的 Kerberos SSO 设置。同时检查回退 NTLM 身份验证设置。

有关详细信息，请参阅 验证您的 Kerberos 配置。

Web/SaaS SSO 因内部服务器错误而失败

信息代码： 0x10000203

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

检查 Secure Private Access 服务和后端服务器中的 SSO 设置。对于 Secure Private Access 服务，请参阅 设置首选登录方法。

Web/SaaS 应用程序启动失败，因为配置的代理无法访问

信息代码： 0x10000303, 0x10000304

检查代理服务器设置，并确保 Connector Appliance 可以访问它。有关详细信息，请参阅 将您的 Connector Appliance 注册到 Citrix Cloud。

Web/SaaS 应用程序启动失败，因为无法通过配置的代理进行身份验证

信息代码： 0x10000305

检查代理服务器凭据，并确保它们在 Connector Appliance 中配置正确。有关详细信息，请参阅 注册您的 Connector Appliance 后。

Citrix Secure Access™ 客户端未能执行 SSO

信息代码： 6003

从 Broker Agent 服务检索 Secure Private Access 单点登录句柄时出错。

检查交付组上是否启用了 Secure Private Access SSO 标志。有关详细信息，请参阅 从 VDA 上的 Citrix Secure Access 客户端无缝登录。

信息代码： 6007

登录 Secure Private Access 失败。

如果 Citrix Secure Access 客户端会话超时，请重新启动 VDA。

会话代码

代码	状态	描述
2101	失败	会话失败
2102	活动/非活动/失败	会话处于活动状态或已终止，或者会话中至少有一个应用程序启动失败
2000	活动	会话处于活动状态
2001	非活动	会话已终止/非活动

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

应用程序枚举消息代码

代码	状态	描述
1000	成功	枚举成功。至少枚举了一个应用程序
1001	成功	未枚举任何应用程序，因为它们都被策略拒绝了
1002	成功	未枚举任何应用程序，因为没有策略匹配
1003	成功	未枚举任何应用程序，因为有些被拒绝，而另一些没有策略匹配
1004	成功	未枚举任何应用程序，因为没有要评估的策略
1101	失败	枚举过程中发生内部错误
1102	失败	某些应用程序已枚举，但至少有一个应用程序评估失败
1103	失败	没有枚举任何应用程序，并且至少有一个应用程序评估失败
3000	允许	允许应用程序枚举
3001	拒绝	应用程序枚举被策略拒绝
3002	拒绝	未枚举应用程序，因为没有策略匹配
3003	未知	应用程序枚举状态未知
3004	从 CEB 启动应用程序	尝试从 Citrix Enterprise Browser™ 启动应用程序
3101	失败	应用程序枚举 - 发生内部错误（当前未使用）

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

代码	状态	描述
3102	失败	由于策略评估期间发生异常，应用程序未被枚举
3103	失败	应用程序枚举状态为空 - 策略评估期间发生内部错误
3104	允许/拒绝/失败	检索应用程序策略详细信息时出错

应用程序启动消息代码

代码	状态	描述
4000	允许	允许应用程序启动
4001	拒绝	由于策略原因，应用程序启动被拒绝
4002	拒绝	应用程序启动被拒绝，因为没有匹配的策略
4101	失败	应用程序启动错误 - 应用程序启动期间发生内部错误
4102	失败	应用程序启动错误（内部）
4103	允许/拒绝/失败	检索应用程序策略详细信息时出错
4104	失败	应用程序启动错误 - 未找到应用程序配置

应用程序启动错误代码

代码	描述	解决方案/变通方法
5001	TCP - 连接失败	验证到目标的网络可达性（从 NetScaler Gateway ping `-S <SNIP>`）。
5003	TCP - 探测失败	

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

代码	描述	解决方案/变通方法
5002	TCP - 代理服务器已关闭	确保代理主机已启动。
5004	TCP - 网关内存分配失败	启用调试级别日志记录并从 NetScaler 收集支持包。
5005	TCP - 服务器宕机	验证到目标的网络可达性（从 NetScaler Gateway ping `-S <SNIP>`），并检查服务器是否宕机。
5006	TCP - 代理连接失败	确保代理主机已启动并接受连接。
5007	TCP - 代理探测失败	验证到目标的网络可达性（从 NetScaler Gateway ping `-S <SNIP>`）。启用调试级别日志记录并从 NetScaler 收集支持包。
5008	SPA - 服务器宕机	验证 Secure Private Access 站点 URL 是否已启动。（使用 NetScaler CLI 上的 `show vpn securePrivateAccessProfile` CLI 命令检查 URL 状态）。
5009	SPA - 呼出请求错误	验证 Secure Private Access 站点 URL 是否已启动。启用调试级别日志记录并从 NetScaler 收集支持包。
5010	SPA - 呼出响应错误	
5011	TCP - 会话已过期	这表示在用户会话不再处于活动状态时访问了应用程序。启动新的活动用户会话。
5013	TCP - 网关内部错误	启用调试级别日志记录并从 NetScaler 收集支持包。
5014	TCP - DNS 服务器已关闭	确保 DNS 服务器已启动。

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

代码	描述	解决方案/变通方法
5015	TCP - 网关 DNS 内部错误	确保 DNS 服务器已启动。启用调试级别日志记录并从 NetScaler 收集支持包。
5016	目标服务器连接失败	验证到目标的网络可达性（从 NetScaler Gateway 使用 ping -S `<SNIP>`）。
5017	目标服务器 DNS 解析失败	确保您的应用程序使用的主机名由预期的 DNS 服务器（内部或公共）解析。
5018	网关内部错误	启用调试级别日志记录并从 NetScaler 收集支持包。
0x1300000C	应用程序域的 DNS 解析失败	确保您的应用程序使用的主机名由预期的 DNS 服务器（内部或公共）解析。

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

Secure Private Access 日志和事件

日志和事件对于监控、故障排除和确保合规性至关重要。Citrix Secure Private Access 服务相关的日志和事件可以从以下来源访问：

诊断仪表板

诊断仪表板提供了一个集中式界面，用于查看和分析日志和事件。管理员可以使用此仪表板来监控和排查与 Secure Private Access 相关的问题。有关详细信息，请参阅Secure Private Access 仪表板。

错误列表

有关用户在使用 Secure Private Access 服务时可能遇到的错误完整列表，请参阅诊断日志信息代码。

审计日志

审计日志捕获用户活动和系统更改的详细记录。这些日志对于合规性和安全目的至关重要，因为它们有助于跟踪谁访问了系统、进行了哪些更改以及这些操作发生的时间。有关详细信息，请参阅审计和系统日志。

系统日志

系统日志包含有关 Secure Private Access 服务内部操作的信息。这些日志对于诊断系统级问题（例如性能问题或服务功能错误）非常有用。有关详细信息，请参阅系统日志。

设备态势日志

设备态势日志提供了对访问 Secure Private Access 服务的设备安全态势的深入了解。这些日志有助于确保设备在授予访问权限之前满足所需的安全标准，从而增强整体安全性。有关详细信息，请参阅设备态势日志。

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

诊断日志

以下部分提供了有关诊断日志的更多信息。

常见问题

以下部分提供了有关常见问题的更多信息。

什么是 Secure Private Access 诊断日志?

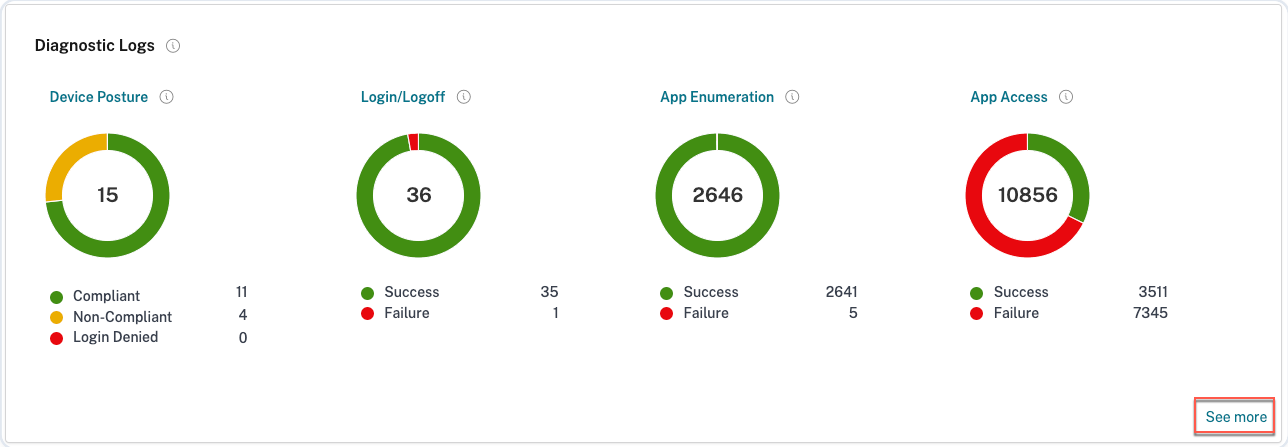
Secure Private Access 诊断日志会捕获用户访问任何应用程序（包括 Web、SaaS、TCP 和 UDP 类型）时发生的所有事件。这些日志记录了设备状态、应用程序身份验证、应用程序枚举以及应用程序访问情况。详细信息以表格形式呈现。您可以查看预设时间段或自定义时间范围内的日志。您可以通过单击“+”号向图表添加列，以显示您希望在仪表板中查看的信息。您可以将用户日志导出为 CSV 格式。

在哪里可以找到 Secure Private Access 日志?

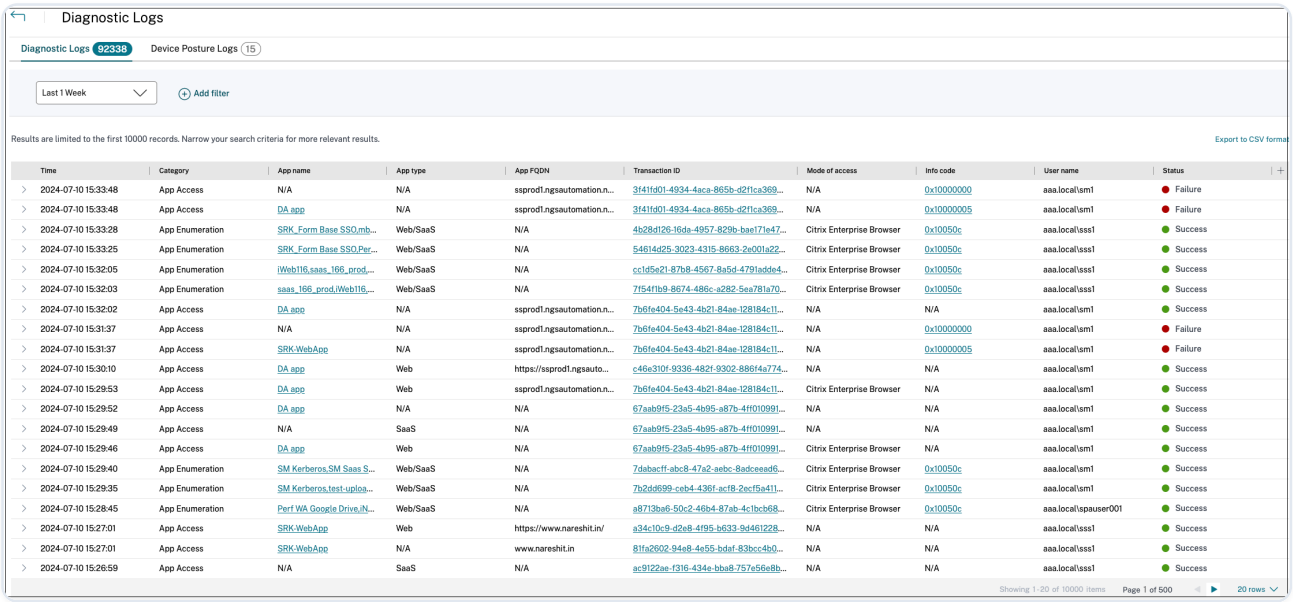
1. 登录 Citrix Cloud。
2. 在 Secure Private Access 服务磁贴上，单击“**管理**”。
3. 在管理员用户界面的左侧导航栏中，单击“**仪表板**”。
4. 在“**诊断日志**”图表中，单击“**查看更多**”链接。

显示 Secure Private Access 诊断日志的小组件?

“**日志记录和故障排除**”部分中的“**诊断日志**”小组件以饼图形式显示所有与身份验证、应用程序启动、应用程序枚举以及设备状态相关的 Secure Private Access 事件。Secure Private Access 诊断日志从多个内部组件获取事件，每个组件在最终用户访问应用程序时发送一个事件。这些事件分为以下类别：**登录/注销**、**应用程序枚举**和**应用程序访问**。饼图显示每个类别的总体成功/失败比率。单击任何图表上的彩色饼图部分，即可转到诊断日志，您可以在其中找到相应的事件。如果您启用了设备状态服务，还会显示设备状态日志。您还可以单击“**查看更多**”链接以查看完整的诊断日志。



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



Secure Private Access 诊断日志中的详细信息?

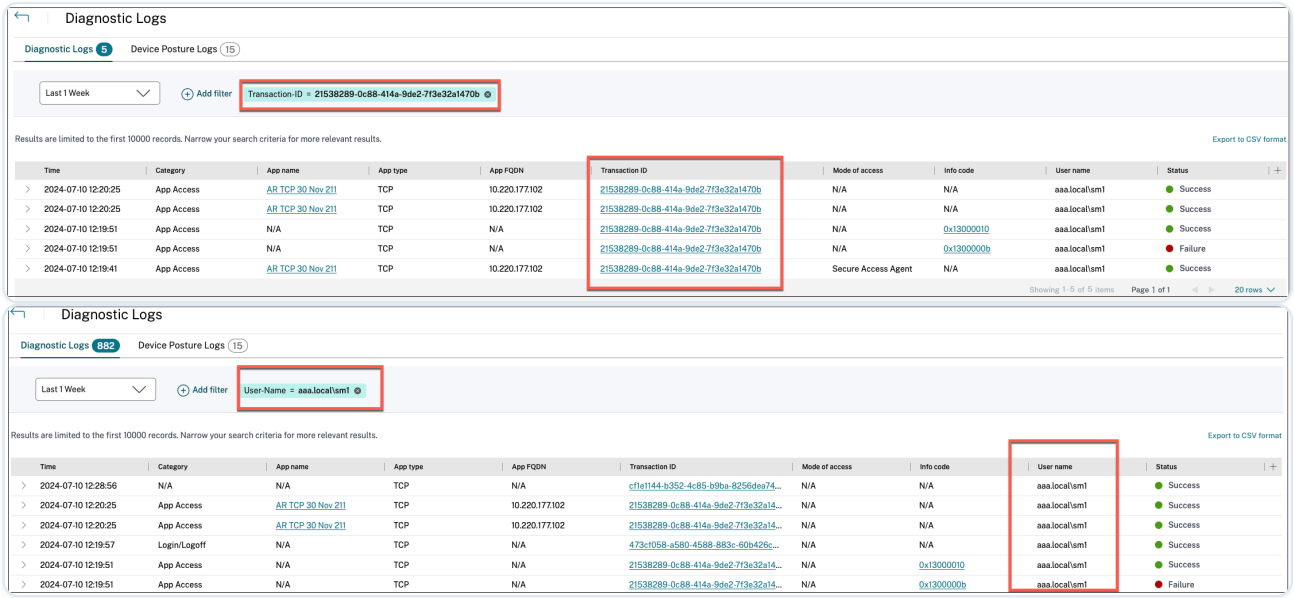
Secure Private Access 用户日志仪表板默认提供以下详细信息。

- **时间戳** - 事件的 UTC 时间。
- **用户名** - 访问应用程序的最终用户的用户名。
- **应用程序名称** - 已访问应用程序的名称。
- **策略信息** - 事件期间触发的访问策略的名称。
- **状态** - 事件状态，成功或失败。
- **信息代码** - Secure Private Access 诊断日志仪表板中与每个失败事件关联的代码。 查看有关信息代码的更多信息。
- **描述** - 失败原因或有关事件的更多详细信息。
- **应用程序 FQDN**：已访问应用程序的 FQDN。
- **事件类型** - 与执行的操作关联的事件类型。
- **操作类型** - 生成日志的操作。
- **类别** - 可用类别，取决于事件类型。可用选项包括：应用程序身份验证、应用程序枚举或应用程序访问。这些选项也可用作筛选选项。您可以使用这些选项根据您面临的问题类型筛选日志。
- **事务 ID** - 事务 ID 关联访问请求的所有 Secure Private Access 日志。 了解如何使用事务 ID。 通过单击仪表板最右侧的 + 按钮，可以获取以下详细信息：
- **SPA PoP 位置** - 应用程序访问期间使用的 Secure Private Access 服务 PoP 位置的名称/ID。请参阅 Secure Private Access PoP 位置。

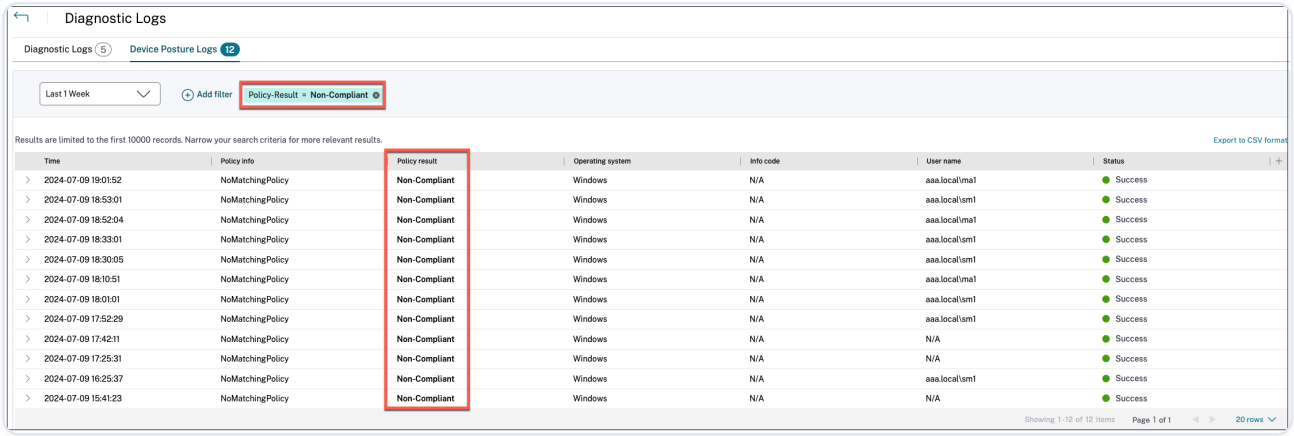
© 1997–2026 Citrix Systems, Inc. All rights reserved.

如何筛选诊断日志?

您可以使用**添加筛选器**选项，根据各种条件（例如应用程序类型、类别、描述）优化搜索。例如，在**搜索**字段中，您可以单击**事务 ID，=（等于某个值），然后输入 21538289-0c88-414a-9de2-7f3e32a1470b**，以搜索与此事务 ID 关联的所有日志。有关可与筛选器选项一起使用的搜索运算符的详细信息，请参阅搜索运算符。



您还可以使用各种筛选选项来优化设备状态日志的搜索。



Secure Private Access 诊断日志中捕获了哪些事件?

Secure Private Access 诊断日志捕获以下事件：

- **设备状态：** 最终用户设备状态。这些日志捕获有关设备状态结果的信息，包括设备是根据您的设备状态策略被视为合规、不合规还是拒绝访问。
- **登录/注销**：与最终用户登录或注销 Citrix Secure Access 客户端以及对存储（内部或外部提供商）进行身份验证相关的事件。
- **应用程序枚举**：在 Secure Private Access 服务中，由管理员配置的访问策略决定哪些用户可以访问哪些应用程序。被拒绝的应用程序在 Citrix Workspace 应用程序中对最终用户不可见（未枚

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

举）。这些事件可帮助您了解根据 Secure Private Access 服务中配置的访问策略，哪些应用程序被允许或拒绝用户访问。

- **应用程序访问**：根据所选时间间隔的配置访问策略，最终用户应用程序/端点访问、允许/拒绝状态、单点登录状态和连接状态的事件。

错误列表

有关用户在使用 Secure Private Access 服务时可能遇到的错误的完整列表，请参阅诊断日志信息代码。

诊断日志信息代码

使用本主题排查一些应用程序配置、身份验证和 SSO 或应用程序访问相关问题。从 Secure Private Access 诊断日志中的“信息代码”列复制信息代码，然后在此页面上搜索该代码以查找相应的故障排除步骤。以下是一些常见问题解答，可帮助您更好地使用本主题。

有关诊断日志的更多信息，请参阅诊断日志。

以下错误查找表全面概述了用户在使用 Secure Private Access 服务时可能遇到的各种错误。

信息代码	描述	解决方案
0x180006, 0x1800B7	应用程序启动失败，因为应用程序 FQDN 长度超出限制	应用程序启动失败，因为应用程序 FQDN 长度超出限制
0x180022	应用程序启动失败，因为身份验证服务已关闭	应用程序启动失败，因为身份验证服务已关闭
0x180001, 0x18001A, 0x18001B, 0x18008A	单点登录错误、Citrix Cloud 与本地连接器之间的连接建立失败、SAML SSO 失败、无效的应用程序 FQDN	应用程序访问被拒绝
0x1800A9, 0x1800AA, 0x1800AB, 0x1800AC		
0x1800AD, 0x1800AE, 0x1800AF, 0x1800B0		
0x1800B1, 0x1800B2, 0x1800B3, 0x180048		
0x1800EF	连接到连接器设备时出现问题	连接到连接器设备时出现问题

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

信息代码	描述	解决方案
0x18009D	DNS 查找/连接失败	安全浏览器服务 - DNS 查找/连接错误
0x1800A0, 0x1800A2, 0x1800A3, 0x1800A5	Web 应用程序启动失败，因为无法连接到后端 Web 应用程序	Web 应用程序启动失败，因为无法连接到后端 Web 应用程序
0x1800A6, 0x1800A7		
0x1800BC, 0x1800BF	用户无权访问 Web/SaaS 应用程序	用户无权访问 Web/SaaS 应用程序
0x1800BD	用户无权访问用于 DirectAccess 的 Web/SaaS 应用程序	用户无权访问用于 DirectAccess 的 Web/SaaS 应用程序
0x1800D0	Citrix Secure Access 代理会话在获取应用程序配置时启动失败	Citrix Secure Access agent 会话启动失败，因为无法获取应用程序配置(/zh-cn/citrix-secure-private-access/service/secure-private-access-troubleshooting.html#citrix-secure-access-agent-session-launch-has-failed-while-fetching-the-application-configuration)
0x1800CD, 0x1800CE, 0x1800D6, 0x1800EA	Citrix Secure Access agent 会话启动失败，因为无法获取应用程序配置，Citrix Secure Access agent 应用程序启动失败，因为策略评估失败，Citrix Secure Access agent 应用程序启动失败	客户端请求格式错误(/zh-cn/citrix-secure-private-access/service/secure-private-access-troubleshooting.html#tcpudp-apps---malformed-client-requests)
0x1800DE	Citrix Secure Access agent 应用程序启动失败，因为策略评估失败	Citrix Secure Access agent 应用程序启动失败，因为策略评估失败(/zh-cn/citrix-secure-private-access/service/secure-private-access-troubleshooting.html#citrix-

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

信息代码	描述	解决方案
		secure-access-agent-app-launch-has-failed-during-the-policy-evaluation)
0x180055, 0x1800DF, 0x1800E3	应用程序受上下文策略限制，由于策略配置，访问被拒绝	用户仪表板中未列出一个或多个应用程序(/zh-cn/citrix-secure-private-access/service/secure-private-access-troubleshooting.html#one-or-more-apps-not-listed-in-the-user-dashboard)
0x1800EB	Citrix Secure Access agent 应用程序启动失败，因为不支持 IPv6	Citrix Secure Access agent 应用程序启动失败，因为不支持 IPv6(/zh-cn/citrix-secure-private-access/service/secure-private-access-troubleshooting.html#citrix-secure-access-agent-app-launch-has-failed-as-ipv6-is-not-supported)
0x1800EC, 0x1800ED	Citrix Secure Access agent 应用程序启动失败，因为 IP 地址无效	Citrix Secure Access 代理应用程序启动失败，因为 IP 地址无效
0x10000001, 0x10000002, 0x10000003, 0x10000004	Citrix Secure Access 客户端登录失败，因为网络问题	Citrix Secure Access 客户端的网络连接可达性问题
0x10000006	Citrix Secure Access 客户端登录失败，因为中间存在代理	代理服务器干扰客户端与服务的连接
0x10000007	Citrix Secure Access 客户端登录失败，因为证书颁发机构不受信任	检测到不受信任的服务器证书问题
0x10000008	Citrix Secure Access 客户端登录失败，因为证书无效	检测到无效的服务器证书问题

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

信息代码	描述	解决方案
0x1000000A	Citrix Secure Access 客户端登录失败，因为配置问题	由于用户的配置为空，登录失败
0x1000000B	由于连接失败，Citrix Secure Access 客户端登录失败	连接被网络或最终用户终止
0x10000010	由于会话过期，Citrix Secure Access 客户端登录失败	由于会话已过期，配置下载失败
0x10000013	由于配置列表过大，Citrix Secure Access 客户端登录失败	Citrix Secure Access 客户端登录失败
0x11000003	由于控制通道创建失败，Citrix Secure Access 客户端登录失败	由于会话过期，控制通道建立失败
0x11000004	由于控制通道创建失败，Citrix Secure Access 客户端登录失败	控制通道建立失败
0x11000005	由于控制通道创建失败，Citrix Secure Access 客户端登录失败	控制通道建立失败
0x11000006	由于控制通道创建失败，Citrix Secure Access 客户端登录失败	由于网络问题，控制通道建立失败
0x12000001	由于会话已过期，Citrix Secure Access 客户端注销失败	由于会话已终止，无法注销
0x12000002	由于会话已超时，Citrix Secure Access 客户端注销失败	会话被强制终止
0x13000001	由于会话过期，应用访问失败	应用程序启动失败，因为会话已过期(/zh-cn/citrix-secure-private-access/service/secure-private-access-troubleshooting.html#applicati

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

信息代码	描述	解决方案
		on-launch-failed-as-session-is-expired)
0x13000002	应用访问失败，因为许可证不足	应用程序启动失败，因为许可证问题(/zh-cn/citrix-secure-private-access/service/secure-private-access-troubleshooting.html#application-launch-failed-because-of-license-issue)
0x13000003, 0x13000008, 0x001800DF	应用访问失败，因为访问被禁止，TCP/UDP 应用启动根据策略被拒绝	应用程序启动失败，因为服务拒绝访问(/zh-cn/citrix-secure-private-access/service/secure-private-access-troubleshooting.html#application-launch-failed-as-access-is-denied-by-service)
0x13000004, 0x13000005	应用访问失败，因为服务器不可用	应用程序启动失败，因为客户端无法访问服务(/zh-cn/citrix-secure-private-access/service/secure-private-access-troubleshooting.html#application-launch-failed-as-the-client-is-unable-to-reach-the-service)
0x13000007	应用访问失败，因为访问策略已禁用或用户未订阅	应用程序启动失败，因为策略评估和配置验证失败(/zh-cn/citrix-secure-private-access/service/secure-private-access-troubleshooting.html#application-launch-failed-as-policy-evaluation-and-config-validation-failed)
0x13000009	应用访问失败，因为路由条目缺失	应用程序启动失败，因为应用程序域表存在问题(/zh-cn/citrix-secure-private-access/

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

信息代码	描述	解决方案
		service/secure-private-access-troubleshooting.html#application-launch-failed-because-of-issues-in-application-domain-table)
0x1300000B	客户端关闭了连接	客户端关闭了与 Secure Private Access 服务的连接(/zh-cn/citrix-secure-private-access/service/secure-private-access-troubleshooting.html#client-closed-the-connection-with-secure-private-access-service)
0x1300000C	通过 ZTNA 解析 FQDN 失败	DNS 服务器无法解析 FQDN(/zh-cn/citrix-secure-private-access/service/secure-private-access-troubleshooting.html#unable-to-resolve-fqdn-by-the-dns-server)
0x1300000E	由于使用了非 Chrome 浏览器，应用程序启动失败	由于使用了非 Chrome 浏览器，应用程序启动失败(/zh-cn/citrix-secure-private-access/service/secure-private-access-troubleshooting.html#app-launch-failed-due-to-use-of-non-chrome-browser)
0x001800D3	登录时应用程序配置下载失败	未能获取配置的应用程序目标列表(/zh-cn/citrix-secure-private-access/service/secure-private-access-troubleshooting.html#failed-to-fetch-configured-application-destinations-list)

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

信息代码	描述	解决方案
0x001800D9, 0x001800DA	TCP/UDP 应用程序启动在解析策略评估响应时失败，TCP/UDP 应用程序启动在策略评估期间因结果无效而失败	应用程序配置问题(/zh-cn/citrix-secure-private-access/service/secure-private-access-troubleshooting.html#application-configuration-issue)
0x001800DB	TCP/UDP 应用程序启动失败，原因是资源位置配置无效	资源位置问题(/zh-cn/citrix-secure-private-access/service/secure-private-access-troubleshooting.html#issue-with-resource-location)
0x13000006, 0x001800DC, 0x001800DD	TCP 应用程序启动失败，原因是为该应用程序配置了不受支持的增强安全策略，TCP 应用程序启动失败，原因是为 TCP 应用程序配置了不受支持的安全浏览器服务重定向	增强安全策略绑定到 HTTP 应用程序(/zh-cn/citrix-secure-private-access/service/secure-private-access-troubleshooting.html#enhanced-security-policy-is-bound-to-the-http-application)
0x001800DE	TCP/UDP 应用程序启动失败，因为未找到目标的应用程序配置	无法找到应用程序(/zh-cn/citrix-secure-private-access/service/secure-private-access-troubleshooting.html#unable-to-locate-the-application)
0x001800EA	TCP 应用程序启动失败，原因是目标 FQDN 过长	主机名长度超过 256 个字符(/zh-cn/citrix-secure-private-access/service/secure-private-access-troubleshooting.html#host-name-length-exceeds-256-characters)
0x001800ED	TCP 应用程序启动失败，原因是目标 IP 无效	无效 IP 地址

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

信息代码	描述	解决方案
0x001800EF	在与私有 TCP 服务器建立连接期间，TCP 应用程序启动失败	无法建立端到端连接
0x001800F5	由于 IPV6 地址，UDP 应用程序启动失败	应用程序请求中收到 IPv6
0x001800F9	由于客户端连接丢失，UDP 流量未能交付	UDP 流量未能交付
0x001800FF	UDP 数据流量交付失败	UDP 数据流量交付失败
0x10000401	Citrix rendezvous 服务器拨号失败	应用程序启动失败，因为网络连接问题(/zh-cn/citrix-secure-private-access/service/secure-private-access-troubleshooting.html#application-launch-failed-due-to-network-connectivity-issues)
0x10000402, 0x1000040C	无法注册连接器设备，UDP 网络连接初始化失败	连接器设备未能注册到 Secure Private Access 服务(/zh-cn/citrix-secure-private-access/service/secure-private-access-troubleshooting.html#connector-appliance-failed-to-register-to-secure-private-access-service)
0x10000403, 0x10000404, 0x10000407, 0x1000040A	连接错误、控制包传输失败、读取网关服务时出错、控制包解析失败、写入网关服务时出错	与连接器设备的连接问题(/zh-cn/citrix-secure-private-access/service/secure-private-access-troubleshooting.html#connectivity-issue-with-connector-appliance)
0x1000040B, 0x1000040F, 0x10000410		
0x10000405, 0x10000408, 0x10000409, 0x1000040D	后端不可达、UDP 数据包传输失败、UDP 数据包接收失	与连接器设备和后端私有 TCP/UDP 服务器的连接问题(/zh-cn/citrix-secure-private-

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

信息代码	描述	解决方案
0x1000040E, 0x10000412	败、写入后端时出错、后端关闭连接	access/service/secure-private-access-troubleshooting.html#connectivity-issues-with-connector-appliance-and-back-end-private-tcpudp-servers)
0x10000406	DNS 解析失败	连接器设备无法解析 FQDN 的 DNS
0x10000411	网关服务关闭了连接	私有服务器连接已终止
0x10000413	确定连接终止原因时出错	无法连接到私有服务 IP 或 FQDN 或向其发送数据
0x100508	用户上下文与访问规则条件不匹配	无匹配的策略条件
0x100509	访问策略未与应用程序关联	没有与应用程序关联的访问策略
0x10050C	用户可能有权使用的多个应用程序的策略评估结果	应用程序枚举信息
0x00180101	TCP/UDP 应用程序启动失败，因为应用程序域表中缺少路由条目	TCP/UDP 应用程序启动失败，因为应用程序域表中缺少路由条目
0x00180102	TCP/UDP 应用程序启动失败，因为连接器不正常	TCP/UDP 应用程序启动失败，因为连接器不正常
0x00180103	UDP/DNS 请求失败，因为连接器不可达	UDP/DNS 请求失败，因为连接器不可达
0x20580001	加载页面失败，因为 NGS Cookie 已过期	由于NGS Cookie已过期，页面加载失败(/zh-cn/citrix-secure-private-access/service/secure-private-access-troubleshooting.html#failed-to-load-the-page-as-the-ngs-cookie-is-expired)

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

信息代码	描述	解决方案
0x20580002	由于网络故障，访问策略获取失败	由于网络故障，访问策略获取失败(/zh-cn/citrix-secure-private-access/service/secure-private-access-troubleshooting.html#access-policy-fetch-failed-because-of-a-network-failure)
0x20580003	解析JSON Web令牌时，访问策略获取失败	解析JSON Web令牌时，访问策略获取失败(/zh-cn/citrix-secure-private-access/service/secure-private-access-troubleshooting.html#access-policy-fetch-failed-while-parsing-the-json-web-token)
0x20580004	获取访问策略详细信息时网络故障	获取访问策略详细信息时网络故障(/zh-cn/citrix-secure-private-access/service/secure-private-access-troubleshooting.html#network-failure-to-fetch-access-policy-details)
0x20580005	获取公共证书时，策略获取失败	获取公共证书时，策略获取失败(/zh-cn/citrix-secure-private-access/service/secure-private-access-troubleshooting.html#policy-fetch-failed-while-fetching-the-public-certificate)
0x20580007	验证JWT签名时，策略获取失败	在验证 JWT 签名时策略获取失败(/zh-cn/citrix-secure-private-access/service/secure-private-access-troubleshooting.html#policy-fetch-failed-while-validating-signature-of-the-json-web-token)

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

信息代码	描述	解决方案
0x20580008	在验证公共证书时策略获取失败	在验证公共证书时策略获取失败(/zh-cn/citrix-secure-private-access/service/secure-private-access-troubleshooting.html#policy-fetch-failed-while-validating-the-public-certificate)
0x2058000A	未能确定存储环境以形成策略 URL	未能确定存储环境以形成策略 URL(/zh-cn/citrix-secure-private-access/service/secure-private-access-troubleshooting.html#failed-to-determine-the-store-environment-to-form-a-policy-url)
0x2058000B	未能获取访问策略获取请求的响应	未能获取访问策略获取请求的响应(/zh-cn/citrix-secure-private-access/service/secure-private-access-troubleshooting.html#failed-to-get-a-response-for-access-policy-fetch-request)
0x2058000C	由于辅助 DS 身份验证令牌已过期，访问策略获取失败	由于辅助 DS 身份验证令牌已过期，访问策略获取失败(/zh-cn/citrix-secure-private-access/service/secure-private-access-troubleshooting.html#access-policy-fetch-failed-due-to-an-expired-secondary-ds-auth-token)
0x10200002	连接器设备未注册	连接器设备未注册
0x10200003	无法连接到连接器设备	无法连接到连接器设备
0x10000301	连接到 Citrix SPA 服务失败	连接到 Citrix Secure Private Access 服务失败

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

信息代码	描述	解决方案
0x10000303, 0x10000304	代理服务器不可达	代理服务器不可达
0x10000305	代理服务器身份验证失败	代理服务器身份验证失败
0x10000306	配置的代理服务器不可达	配置的代理服务器不可达
0x10000307	从后端服务器收到错误响应	从后端服务器收到错误响应
0x10000005	无法向目标 URL 发送请求	无法向目标 URL 发送请求
0x10000107	处理 SSO 失败	处理 SSO 失败
0x10000108, 0x1000010B	处理 SSO 失败，无法确定 SSO 设置	处理 SSO 失败，无法确定 SSO 设置
0x10000101, 0x10000102, 0x10000103, 0x10000104	表单填充 SSO 失败，表单应用配置不正确	FormFill SSO 失败，表单应用配置不正确
0x1000010A	FormFill SSO 失败，表单应用配置不正确	FormFill SSO 失败，表单应用配置不正确
0x10000202	Kerberos SSO 失败	Kerberos SSO 失败
0x10000203	未能处理此身份验证类型的 SSO	未能处理此身份验证类型的 SSO
0x10000204	Kerberos SSO 失败，但回退到 NTLM	Kerberos SSO 失败，但回退到 NTLM
0x14000001	Citrix Workspace 应用程序中配置了多个 ZTNA 授权帐户	在 Citrix Workspace 应用程序中配置了多个 ZTNA 授权帐户 (/zh-cn/citrix-secure-private-access/service/secure-private-access-troubleshooting.html#multiple-ztna-entitled-accounts-configured-in-citrix-workspace-application)

解决步骤

以下部分提供了大多数信息代码的解决步骤。对于没有捕获解决步骤的代码，请联系 Citrix 支持。

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

用户仪表板中未列出一个或多个应用程序

信息代码： 0x180055, 0x1800DF, 0x1800E3

由于上下文策略设置，某些用户或设备可能无法看到应用程序。信任因素（设备姿态或风险评分）等参数会影响应用程序的可访问性。

1. 从诊断日志 CSV 文件中，复制错误代码 `0x18005C` 的 `reasons` 列中的事务 ID。
2. 修改 CSV 文件中的 `prod` 列筛选器，以显示来自名为 `SWA.PSE` 或 `SWA.PSE.EVENTS` 的组件的事件。此筛选器仅显示与策略评估相关的日志。
3. 在 `reason` 列中搜索评估的策略负载。此负载显示了用户订阅的所有应用程序的用户上下文的评估策略。
4. 如果策略评估显示用户应用程序被拒绝，可能的原因是：
    - 策略中的匹配条件不正确 - 检查 Citrix Cloud™ 中的应用程序策略配置
    - 策略中的匹配规则不正确 - 检查 Citrix Cloud 中的应用程序策略配置
    - 策略中的默认匹配规则不正确 - 这是一个穿透情况。请相应地调整条件。

用户无权访问 Web/SaaS 应用程序

信息代码： 0x1800BC, 0x1800BF

用户可能点击了其未订阅的应用程序链接。

确保用户已订阅这些应用程序。

1. 在管理门户中转到应用程序。
2. 编辑应用程序并转到“**订阅**”选项卡。
3. 确保目标用户在订阅列表中有条目。

后端应用程序性能缓慢

信息代码：0x18000F

在某些情况下，客户网络可能不稳定，原因可能是资源位置中的连接器已关闭，或者后端服务器本身没有响应。

1. 确保连接器设备在地理位置上靠近后端服务器，以排除网络延迟。
2. 检查后端服务器的防火墙是否未阻止连接器设备。
3. 检查客户端是否连接到最近的云 POP。

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

例如，在客户端上，`nslookup nssvc.dnsdiag.net` 答案中的规范名称表示地理特定服务器，例如 `aws-us-w.g.nssvc.net.`。

应用程序启动失败，因为应用程序 FQDN 长度超出限制

信息代码： 0x180006, 0x1800B7

应用程序 FQDN 的长度不得超过 512 个字符。检查应用程序配置页面中的应用程序 FQDN。确保长度不超过 512 字节。

1. 导航到管理控制台上的“**应用程序**”选项卡。
2. 查找 FQDN 超过 512 个字符的应用程序。
3. 编辑应用程序并修复应用程序 FQDN 长度。

应用程序详细信息长度超出

信息代码： 0x18000E

检查策略是否阻止了应用程序访问。

1. 导航到“**访问策略**”。
2. 查找应用程序具有授权的策略。
3. 审查针对最终用户的策略规则和条件。

应用程序访问被拒绝

信息代码： 0x180001, 0x18001A, 0x18001B, 0x18008A, 0x1800A9, 0x1800AB, 0x1800AC, 0x1800AD, 0x1800AE, 0x1800AF, 0x1800B0, 0x1800B1, 0x1800B2, 0x1800B3, 0x180048

这与上下文策略相关，其中策略拒绝了特定用户的应用程序访问。

检查策略是否阻止了应用程序访问

1. 导航到“**访问策略**”。
2. 查找应用程序具有授权的策略。
3. 审查最终用户的策略规则和条件。

应用程序未枚举

应用程序可能由于策略拒绝或未启用安全私有访问集成而从枚举列表中缺失。

- 如果必须为某些应用程序启用访问权限，但您看到零个应用程序，请尝试启用安全私有访问集成。

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

- 登录 Citrix Cloud。
- 从汉堡菜单中选择 **StoreFront Cloud**，然后单击 **服务集成**。
- 单击安全私有访问中的省略号按钮，然后单击 **启用**。

- 如果安全私有访问集成已启用，请将其禁用，然后再次启用，以查看是否有任何应用程序。

连接到连接器设备时出现问题

信息代码： 0x1800EF

由于无法与本地连接器建立 TCP 连接，应用程序路由失败。

审查控制器组件中的事件

1. 在诊断日志 CSV 文件中查找错误代码 `0x1800EF` 的 `transaction ID`。
2. 筛选 CSV 文件中与事务 ID 匹配的所有事件。
3. 另外，筛选 CSV 文件中与 `SWA.GOCTRL` 匹配的 `prod` 列。

   如果您看到带有 `connectType` 消息 `multiconnect::success` 的事件，则；

   - 这表明隧道建立请求已成功中继到控制器。
   - 检查日志消息中的 `Resource Location` 是否正确。如果错误，请在 Citrix 管理门户的应用程序配置部分中修复资源位置。
   - 检查日志消息中的 `VDA Ip and Port` 是否正确。VDA IP 和端口表示后端应用程序 IP 和端口。如果错误，请在 Citrix 管理门户的应用程序配置部分中修复应用程序 FQDN 或 IP 地址。
   - 如果您没有发现任何前面提到的问题，请继续查看 连接器事件。

   如果您看到带有 `connectType` 消息 `connect::failure` 或 `multiconnect::success` 的事件，则；

   - 检查此日志消息的建议修复是否为 - `Check if connector is still connected to same pop`。这表明资源位置的连接器可能已关闭。继续查看 连接器事件。
   - 如果未看到前面提到的消息，请联系 Citrix 客户支持。

   如果您看到带有 `connectType` 消息 `IntraAll::failure` 的事件，请联系 Citrix 客户支持。

查看连接器组件中的事件

1. 在诊断日志 CSV 文件中查找错误代码 `0x1800EF` 的 `transaction ID`。
2. 筛选 CSV 文件中与事务 ID 匹配的所有事件。

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

3. 同时筛选 CSV 文件中与 `SWA.ConnectorAppliance.WebApps` 匹配的 `prod` 列。
4. 如果您看到 `status` 为 `failure` 的事件，则；
    - 查看每个这些失败事件的 `reason` 消息。
    - `UnableToRegister` 表示连接器未能成功注册到 Citrix Cloud。请联系 Citrix 支持。
    - `IsProxyRequiredCheckError` 或 `ProxyDialFailed` 或 `ProxyConnectionFailed` 或 `ProxyAuthenticationFailure` 或 `ProxiesUnReachable` 表示连接器无法通过代理配置解析后端 URL。请检查代理配置是否正确。
    - 有关进一步的调试，请参阅 连接器 SSO 事件。

单点登录错误

对于单点登录，在应用程序启动期间会提取并应用应用程序配置中的不同 SSO 属性。如果特定用户没有这些属性或属性不正确，则单点登录可能会失败。请确保配置正确无误。

1. 转到 **访问策略**。
2. 查找应用程序具有授权的策略。
3. 查看最终用户的策略规则和条件。

表单 SSO、Kerberos 和 NTLM 等 SSO 方法由本地连接器执行。请查看连接器的以下诊断日志。

查看连接器组件中的 SSO 事件

1. 筛选 csv 文件中与 `SWA.ConnectorAppliance.WebApps` 匹配的 `component name`。
2. 您是否看到状态为“失败”的事件？
    - 查看每个失败事件的消息。
    - `IsProxyRequiredCheckError` 或 `ProxyDialFailed` 或 `ProxyConnectionFailed` 或 `ProxyAuthenticationFailure` 或 `ProxiesUnReachable` 表示连接器无法通过代理配置解析后端 URL。请检查代理配置是否正确。
    - `FailedToReadRequest` 或 `RequestReceivedForNonSecureBrowse` 或 `UnableToRetrieveUserCredentials` 或 `CCSPolicyIsNotLoaded` 或 `FailedToLoadBaseClient` 或 `ProcessConnectionFailure` 或 `WebAppUnSupportedAuthType` 表示隧道故障。请联系 Citrix 支持。
    - `UnableToConnectTargetServer` 表示后端服务器无法从连接器访问。请再次检查后端配置。
    - `IncorrectFormAppConfiguration` 或 `NoLoginFormFound` 或 `FailedToConstructForLoginActionURL` 或 `FailedToLoginViaFormBasedAuth` 表示

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

基于表单的身份验证失败。请检查 Citrix 管理门户中“应用程序配置”中的表单 SSO 配置部分。

- `NTLMAuthNotFound` 表示基于 NTLM 的身份验证失败。请检查 Citrix 管理门户中“应用程序配置”中的 NTLM SSO 配置部分。
- 有关进一步的调试，请参阅连接器事件。

身份验证服务关闭，导致应用程序启动失败

信息代码： 0x180022

Secure Private Access 允许管理员配置第三方身份验证服务，例如传统 Active Directory、AAD、Okta 或 SAML。这些身份验证服务中断可能导致此问题。

检查第三方服务器是否已启动且可访问。

SAML SSO 失败

信息代码： 0x18008A, 0x1800A9, 0x1800AA, 0x1800AB, 0x1800AC, 0x1800AD, 0x1800AE, 0x1800AF, 0x1800B0, 0x1800B1, 0x1800B2, 0x1800B3

当应用程序启动由 IdP 发起时，用户会遇到身份验证失败；当应用程序启动由 SP 发起时，用户可能会看到无法访问的链接。请检查 Secure Private Access 服务端的 SAML 应用程序配置以及服务提供商配置。

安全专用访问配置：

1. 转到“**应用程序**”选项卡。
2. 查找有问题的 SAML 应用程序。
3. 编辑应用程序并转到“**单点登录**”选项卡。
4. 检查以下字段。
    - 断言 URL
    - 中继状态
    - 受众
    - 名称 ID 格式、名称 ID 和其他属性

服务提供商配置：

1. 登录到服务提供商。
2. 转到 **SAML 设置。**
3. 检查 IdP 证书、受众和 IdP 登录 URL。

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

如果配置正确，请联系 Citrix 支持。

无效的应用 FQDN

信息代码： 0x180048

客户管理员可能提供了无效的 FQDN，或者 DNS 解析在后端服务器上失败的 FQDN。

在这种情况下，最终用户会在网页上看到错误。检查应用程序设置。

SAAS 应用验证

检查是否可以从网络访问该应用程序。

WEB 应用程序验证

1. 转到“**应用程序**”选项卡。
2. 编辑有问题的应用程序。
3. 转到“**应用程序详细信息**”页面。
4. 检查 URL。该 URL 必须在内网或互联网中可访问。

安全浏览器服务 - DNS 查找/连接失败

信息代码： 0x18009D

通过远程浏览器隔离服务浏览体验中断。检查最终用户尝试连接的后端服务器。

1. 转到后端服务器，检查其是否正在运行并能够接收请求。
2. 检查代理设置，看其是否阻止了与后端服务器的连接。

注意：

Citrix Remote Browser Isolation™ 服务以前称为 Secure Browser 服务。

CWA Web - Web 应用程序的 DNS 查找/连接错误

信息代码： 0x1800A0、0x1800A2、0x1800A3、0x1800A5、0x1800A6、0x1800A7

企业网络中运行的 Web 应用程序的浏览体验中断。

1. 筛选诊断日志，查找无法解析的 FQDN。
2. 检查企业网络内部是否可以访问后端服务器。
3. 检查代理设置，查看连接器是否被阻止访问后端服务器。

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

直接访问 - 配置为 Web 应用程序时出错

由于 Web 应用程序流量始终通过连接器路由，因此在其上配置直接访问会导致应用程序访问错误。

检查路由域表和应用程序配置之间是否存在冲突配置。

1. 转到管理门户中的应用程序。
2. 编辑应用程序并检查是否启用了直接访问。
3. 检查路由域表中的应用程序 FQDN 是否已标记为内部。

用户无权通过 DirectAccess 访问 Web/SaaS 应用程序

信息代码： 0x1800BD

应用程序配置会禁用源自基于浏览器的客户端的流量的直接访问。

确保用户已订阅这些应用程序。

1. 转到管理门户中的应用程序。
2. 编辑应用程序并检查无代理访问配置。

增强安全策略 - 安全浏览器服务配置错误

信息代码： 0x1800C3

观察到的行为与策略规则预期不符。请检查上下文访问策略。

1. 转到“**策略**”选项卡。
2. 检查与应用程序关联的策略。
3. 检查这些策略的规则。

增强安全策略 - 策略配置错误

观察到的行为与策略规则预期不符。请检查增强安全设置。

1. 转到应用程序。
2. 单击“**访问策略**”选项卡。
3. 检查“**可用安全限制：**”部分中的设置。

Citrix Secure Access™ 代理会话在获取应用程序配置时启动失败

信息代码： 0x1800D0

Citrix Secure Access 应用程序无法成功建立到 Citrix Cloud 的完整隧道。

1. 检查 TCP/UDP 应用程序的路由域配置。

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

2. 确保最大条目数远低于 16k 限制。

TCP/UDP 应用程序 - 客户端请求格式错误

信息代码： 0x1800CD, 0x1800CE, 0x1800D6, 0x1800EA

VPN 隧道未建立，或者某些 FQDN 可能未被隧道化。

1. 确保请求未被中间代理伪造或重构。
2. 疑似中间人攻击。

TCP/UDP 应用程序 - Secure Browser Service 重定向配置错误

信息代码： 0x1800DD

远程浏览器隔离服务重定向仅适用于 Web 应用程序，不适用于 TCP/UDP 应用程序。请在 Secure Private Access 服务 GUI 中查看应用程序配置。

> **注意：**
>
> Citrix 远程浏览器隔离服务以前称为 Secure Browser 服务。

Citrix Secure Access 代理应用程序在策略评估期间启动失败

信息代码： 0x1800DE

确保所有将由 Citrix Secure Access 客户端隧道化的内部 FQDN 在路由域表中都有相应的条目。

Citrix Secure Access 代理应用程序启动失败，因为不支持 IPv6

信息代码： 0x1800EB

检查路由域条目。确保表中没有 IPv6 条目。

Citrix Secure Access 代理应用程序启动失败，因为 IP 地址无效

信息代码：0x1800EC, 0x1800ED

检查路由域条目。确保 IP 地址有效并指向正确的后端。

Citrix Secure Access 客户端的网络连接可达性问题

信息代码： 0x10000001, 0x10000002, 0x10000003, 0x10000004

1. 检查客户端计算机网络是否可达。如果网络可达，请联系 Citrix 支持并提供客户端调试日志。
2. 检查代理或防火墙是否正在阻止网络。

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

要收集客户端调试日志，请参阅如何收集客户端日志。

代理服务器干扰客户端与服务的连接

信息代码： 0x10000006

1. 检查客户端计算机网络是否可达。
2. 检查客户端中是否正确配置了代理。
3. 如果两者都没有问题，请联系 Citrix 支持并提供客户端调试日志。

要收集客户端调试日志，请参阅 如何收集客户端日志。

观察到不受信任的服务器证书问题

信息代码： 0x10000007

请联系 Citrix 支持，检查服务器证书是否由有效的 CA 正确生成。

观察到无效的服务器证书问题

信息代码： 0x10000008

请联系 Citrix 支持，检查服务器证书是自签名、已过期还是来自不受信任的源。

由于用户的配置为空，登录失败

信息代码： 0x1000000A

1. 确保至少配置了一个 TCP/UDP/HTTP 应用程序。有关详细信息，请参阅 添加和管理应用程序。
2. 确保“应用程序域”表 (**Secure Private Access > Settings > Application Domain**) 不为空或所有条目均未禁用。在 TCP/UDP/HTTP 应用程序中配置的目标会自动添加到此表中。

建议您不要删除或禁用活动 TCP/UDP/HTTP 应用程序的目标或 URL。

连接被网络和/或最终用户终止

信息代码： 0x1000000B

检查网络是否中断，或者最终用户是否在 ZTNA 会话连接期间取消了连接。

配置下载失败，因为会话已过期

信息代码： 0x10000010

在 ZTNA 会话配置下载请求期间，VPN 会话可能已过期。请尝试重新登录 Citrix Secure Access 客户端。

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

Citrix Secure Access 客户端登录失败

信息代码： 0x10000013

Citrix Secure Access 客户端登录失败，因为配置大小超出了最大配置限制。

1. 查看 **Secure Private Access > 设置 > 应用程序域**中 TCP/UDP 应用程序的路由域配置
2. 确保条目数量不大。如果条目列表很大，请禁用或删除未使用的目标。

   如果目标列表预计超过 1000 个，请尝试通过更新 ConfigSize 注册表项来增加最大配置下载大小。有关详细信息，请参阅 Citrix Gateway VPN 客户端注册表项。

控制通道建立失败，因为会话已过期

信息代码： 0x11000003

用于 DNS 请求建立的控制通道已失败，因为会话已过期。

ZTNA 会话可能在控制通道设置期间已过期。

尝试重新登录 Citrix Secure Access 客户端。

控制通道建立失败

信息代码： 0x11000004

DNS 请求建立的控制通道失败。

- **保持资源位置健康：**

1. 登录到 Citrix Cloud。
2. 从汉堡菜单中单击“**资源位置**”。
3. 对相应资源位置上的连接器设备运行健康检查。
4. 如果这不能解决问题，请尝试重新启动连接器虚拟机。

- **维护 HA 连接器设备：**

1. 登录到 Citrix Cloud。
2. 从汉堡菜单中单击“**资源位置**”。
3. 确保预期的资源位置至少有两个连接器设备。

确保以下事项：

- 资源位置 LAN 处于正常工作状态。
- 没有防火墙或代理在中间阻止连接器设备连接到服务或后端服务器。

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

- 客户端网络正常。
- 后端私有服务器正在运行。
- DNS 服务器正在运行。
- FQDN 可解析。

如果您满足上述建议，请执行以下操作。

1. 从此错误的诊断日志中获取事务 ID。
2. 在 Secure Private Access 控制板中筛选所有与事务 ID 匹配的事件。
3. 检查客户端、连接器设备或服务诊断日志中是否发生与事务 ID 匹配的任何错误。然后采取相应的措施。
4. 检查在应用程序域表（**Secure Private Access > 设置 > 应用程序域**）中是否为目标正确选择了资源位置。
5. 检查应用程序是否配置了正确的端口、IP 范围和域。有关详细信息，请参阅添加和管理应用程序。

如果您仍然无法解决此问题，请联系 Citrix 支持，并提供与事务 ID 和客户端日志相关的错误代码。

要收集客户端调试日志，请参阅如何收集客户端日志。

控制通道建立失败

信息代码： 0x11000005

控制通道（用于 DNS 请求）建立失败。

1. 检查 Secure Private Access 服务许可证授权。
2. 如果未获得授权，请联系 Citrix 支持部门检查许可证。

有关详细信息，请参阅 `<https://www.citrix.com/buy/licensing/product.html>`。

由于网络问题，控制通道建立失败

信息代码： 0x11000006

由于网络问题，控制通道（用于 DNS 请求）建立失败。

1. 检查 Secure Private Access 服务是否可访问。
2. 如果无法访问，请联系 Citrix 支持部门并提供错误代码和客户端日志。

要收集客户端调试日志，请参阅 如何收集客户端日志。

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

由于 IIP 不足，控制通道建立失败

信息代码： 0x11000007

由于 IIP 不足，控制通道（用于 DNS 请求）建立失败。

请联系 Citrix 支持部门并提供错误代码和客户端日志。

要收集客户端调试日志，请参阅 如何收集客户端日志。

会话已终止，无法注销

这个问题可能发生是因为客户端机器（键盘或鼠标）空闲时间超过了配置的超时期限。

信息代码： 0x12000001

尝试重新登录到 Citrix Secure Access 客户端。

会话被强制终止

由于达到了配置的强制超时时间，会话被强制终止。

信息代码： 0x12000002

尝试重新登录到 Citrix Secure Access 客户端。

应用程序启动失败，因为会话已过期

信息代码： 0x13000001

1. 在应用程序启动期间，ZTNA 会话已过期。
2. 尝试重新登录到 Citrix Secure Access 客户端。

应用程序启动失败，因为许可证问题

信息代码： 0x13000002

1. 检查 Secure Private Access 服务许可证是否已授权。
2. 如果未授权，请联系 Citrix 支持以检查许可证。

有关详细信息，请参阅 `<https://www.citrix.com/buy/licensing/product.html>`。

由于服务拒绝访问，应用程序启动失败

信息代码： 0x13000003, 0x13000008, 0x001800DF

根据用户和应用程序的策略配置，应用程序启动被拒绝。

请确保以下事项。

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

- 多个应用程序中未使用相同的目标（HTTP、HTTPS、TCP、UDP）
- 多个应用程序上没有重叠的目标。
- 访问策略已绑定到应用程序。

还要检查为被拒绝的应用程序配置的策略的条件和操作。然后审查策略条件和操作。

有关详细信息，请参阅 访问策略。

由于客户端无法访问服务，应用程序启动失败

信息代码： 0x13000004, 0x13000005

1. 检查安全专用访问服务是否可访问。
2. 再次启动应用程序。
3. 如果应用程序长时间无法访问，请联系 Citrix 支持并提供错误代码和客户端日志。

要收集客户端调试日志，请参阅如何收集客户端日志。

应用程序启动失败，因为策略评估和配置验证失败

信息代码： 0x13000007

应用程序启动失败，因为 Secure Private Access 服务未能通过策略评估和配置验证。

无法找到访问目标的应用程序。

应用程序启动失败，因为服务拒绝访问。

应用程序启动失败，因为应用程序域表存在问题

信息代码： 0x13000009

应用程序启动失败，因为应用程序域表中没有访问目标的条目。

检查应用程序的路由条目是否在 **Secure Private Access > 设置 > 应用程序域** 中正确配置。

客户端关闭了与 Secure Private Access 服务的连接

信息代码： 0x1300000B

1. 检查终端用户是否手动关闭了连接。
2. 如果不是，请联系 Citrix 支持并提供错误代码和客户端日志。

要收集客户端调试日志，请参阅如何收集客户端日志。

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

DNS 服务器无法解析 FQDN

信息代码： 0x1300000C

当连接器设备无法解析 FQDN 的 DNS 时，会出现此问题。

1. 检查 DNS 服务器中相应应用程序 FQDN 的 DNS 条目。
2. 确保在连接器设备中配置了适当的 DNS 服务器。有关详细信息，请参阅在连接器设备管理页面上配置网络设置。

由于使用了非 Chrome 浏览器，应用程序启动失败

信息代码： 0x1300000E

应用程序启动失败，因为浏览器模式设置为 Google Chrome Enterprise Premium，并且使用了非 Chrome 浏览器。

使用 Chrome 浏览器启动应用程序。

- 检查用户系统中的默认系统浏览器是否设置为 Chrome。
- 检查用户是否未尝试使用非 Chrome 浏览器手动启动应用程序。

无法找到应用程序

信息代码： 0x001800DE

您可能无法为用户访问的目标找到应用程序。如果应用程序域表中缺少目标到资源位置的映射，则可能会发生这种情况。

- 确保为访问的目标配置了 TCP/UDP 或 HTTP 应用程序。
- 确保用户已订阅所访问目标对应的应用程序。

1. 转到管理门户中的应用程序。
2. 编辑应用程序并转到“**订阅**”选项卡。
3. 确保目标用户在订阅列表中有条目。
4. 确保“**应用程序域**”表包含目标和相应的资源位置。

未能获取已配置的应用程序目标列表

信息代码： 0x001800D3

- 确保至少配置了一个 TCP/UDP/HTTP 应用程序。有关详细信息，请参阅添加和管理应用程序。

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

- 确保“应用程序域”表（**Secure Private Access > 设置 > 应用程序域**）页面不为空，或者并非所有条目都被禁用。在 TCP/UDP/HTTP 应用程序中配置的目标会自动添加到此表中。建议不要删除或禁用“应用程序域”表中活动的 TCP/UDP/HTTP 应用程序的目标或 URL。

应用程序配置问题

应用程序配置包含特殊字符或存在某些策略配置问题。

信息代码： 0x001800D9, 0x001800DA

确保以下事项：

- 应用程序配置不包含不支持的字符。
- 目标 IP 地址、IP 地址范围或 IP CIDR 有效。
- 应用程序目标在应用程序域表中已启用 (**Secure Private Access > Settings > Application Domain**)。
- 策略已配置并绑定到相应的应用程序。
- 访问策略配置正确。

资源位置问题

信息代码： 0x001800DB

- 确保已配置资源位置。
  a. 在 Citrix Cloud 汉堡菜单中，选择 **资源位置**。
  b. 确保已配置预期的资源位置，并且该资源位置处于活动状态。
- 确保在应用程序域表 (**Secure Private Access > Settings > Application Domain**) 中为目标选择了正确的资源位置。

在 TCP/UDP/HTTP 应用程序中配置的目标会自动添加到此表。建议不要在应用程序域表中删除或禁用活动的 TCP/UDP/HTTP 应用程序的目标或 URL。

增强型安全策略已绑定到 HTTP 应用程序

信息代码： 0x001800DC, 0x001800DD, 0x13000006

已绑定增强型安全策略的 HTTP 应用程序通过 Citrix Secure Access 客户端访问。

- 确保 TCP/UDP 和 HTTP 应用程序不使用相同的目标。
- 如果为 HTTP/HTTPS 应用程序启用了增强型安全策略，建议仅通过 Citrix Workspace 应用程序或 Citrix Remote Browser Isolation 服务访问该应用程序。

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

- 禁用 HTTP/HTTPS 应用程序的增强安全控制，以便通过 Citrix Secure Access 客户端访问应用程序。
  - 转到 Secure Private Access 管理门户。
  - 单击“**应用程序**”选项卡，然后搜索所访问的目标 HTTP/HTTPS 应用程序的策略名称。
  - 单击“**访问策略**”选项卡，然后搜索之前确定的策略名称。
  - 选择策略，然后单击“**编辑**”。
  - 将操作从“**允许受限访问**”更改为“**允许访问**”。

有关配置的详细信息，请参阅添加和管理应用程序。

注意：

Citrix 远程浏览器隔离服务以前称为 Secure Browser 服务。

主机名长度超过 256 个字符

信息代码： 0x001800EA

应用程序启动请求中收到的主机名超过 256 个字符。

建议 FDQN 字符不超过 256 个字符。

无效 IP 地址

信息代码： 0x001800ED

应用程序启动请求中收到的 IP 地址无效。

建议客户端仅访问有效的私有 IP 地址。

无法建立端到端连接

信息代码： 0x001800EF

无法在客户端与资源位置中配置的服务器之间建立端到端连接。

- 确保资源位置处于活动状态。
  - 在 Citrix Cloud 汉堡菜单中，选择 **资源位置**。
  - 对相应资源位置上的连接器设备运行运行状况检查。
  - 如果这不能解决问题，请重新启动连接器虚拟机。
- 维护高可用性连接器设备

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

  - 在 Citrix Cloud 汉堡菜单中，选择 **资源位置**。
  - 确保资源位置至少有两个连接器设备。
- 确保以下各项：
  - 资源位置 LAN 处于正常工作状态。
  - 中间没有防火墙或代理阻止连接器设备连接到服务或后端服务器。
  - 客户端网络正常。
  - 后端私有服务器正常。
  - DNS 服务器正常。
  - FQDN 可解析。

如果这些都没有问题，请执行以下操作：

1. 从此错误的诊断日志中获取事务 ID。
2. 在 Secure Private Access 服务控制板中筛选所有与事务 ID 匹配的事件。
3. 从 Secure Private Access 服务控制板中检查与事务 ID 对应的诊断日志，然后采取相应的措施。
4. 检查在应用程序域表（**Secure Private Access > 设置 > 应用程序域**）中是否选择了正确的资源位置作为目标。
5. 检查应用程序（**Secure Private Access > 应用程序**）是否配置了正确的 IP 地址、端口和 FQDN。

如果这些步骤都无法解决问题，请联系 Citrix 支持，提供与事务 ID 对应的错误代码并收集客户端日志。

要收集客户端调试日志，请参阅 如何收集客户端日志。

应用程序请求中收到的 IPv6

信息代码： 0x001800F5

应用程序请求中收到了不受支持的 IPv6。目前仅支持 IPv4。

编辑应用程序以修复应用程序 IP 地址问题。

1. 转到 Secure Private Access 管理门户。
2. 单击“**应用程序**”选项卡。
3. 搜索应用程序并单击“**编辑**”。

有关详细信息，请参阅添加和管理应用程序。

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

UDP 流量传输失败

信息代码： 0x001800F9

由于客户端连接丢失，UDP 流量传输失败

1. 检查客户端会话是否处于活动状态。
2. 注销并重新登录。

UDP 数据流量传输失败

信息代码： 0x001800FF

- 在 Secure Private Access 服务控制板中查找错误代码的事务 ID，并筛选所有与该事务 ID 匹配的事件。
- 检查与事务 ID 匹配的其他组件中是否发生任何错误。如果在其他组件中发现问题，请相应地采取适当措施。
- 如果这不能解决问题，请联系 Citrix 支持，并提供错误代码和相应的事务 ID。

由于网络连接问题，应用程序启动失败

信息代码： 0x10000401

由于连接器设备与 Secure Private Access 服务之间的网络连接问题，应用程序启动失败

1. 检查连接器设备的公共互联网连接。
2. 检查是否有任何代理或防火墙规则正在阻止连接。
3. 如果任何代理导致此问题，请绕过代理并再次尝试启动应用程序。
4. 检查连接器设备的运行状况（**Citrix Cloud > 资源位置**）。

有关网络设置的详细信息，请参阅连接器设备的网络设置。

连接器设备未能注册到 Secure Private Access 服务

信息代码： 0x10000402, 0x1000040C

1. 转到连接器设备管理页面并检查连接器摘要。
2. 如果连接器状态不佳，请转到管理门户中的资源位置。
3. 在相应的资源位置对连接器设备运行运行状况检查。
4. 如果运行状况检查失败，请重新启动连接器虚拟机。
5. 检查连接器摘要并再次运行运行状况检查。

有关网络设置的详细信息，请参阅Connector Appliance 的网络设置。

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

与 Connector Appliance 的连接问题

信息代码： 0x10000403, 0x10000404, 0x10000407, 0x1000040A, 0x1000040B, 0x1000040F, 0x10000410

- 查找错误代码的事务 ID。
- 在 Secure Private Access 控制板中筛选与事务 ID 匹配的所有事件。
- 检查其他组件中是否发生与事务 ID 匹配的任何错误，如果发现，请执行与该错误代码匹配的相应解决方法。
- 如果在其他组件中未发现错误，请执行以下操作：
  - 转到 Connector Appliances 管理页面。
  - 下载诊断报告。有关详细信息，请参阅生成诊断报告。
  - 捕获数据包跟踪。有关详细信息，请参阅验证您的网络连接。
- 联系 Citrix 支持，并提供此诊断报告和数据包跟踪以及错误代码和事务 ID。

与 Connector Appliance 和后端专用 TCP/UDP 服务器的连接问题

信息代码： 0x10000405, 0x10000408, 0x10000409, 0x1000040D, 0x1000040E, 0x10000412

Connector Appliance 与后端专用 TCP/UDP 服务器存在连接问题。

- 检查最终用户尝试连接的后端服务器是否已启动并正在运行，并且能够接收请求。
- 检查企业网络内部是否可以访问后端服务器。
- 检查代理设置，查看连接器是否被阻止访问后端服务器。
- 如果是基于 FQDN 的应用程序请求，请检查 DNS 服务器中相应应用程序的 DNS 条目。

连接器设备无法解析 FQDN 的 DNS

信息代码： 0x10000406

- 检查 DNS 服务器中相应应用程序 FQDN 的 DNS 条目。
- 确保在连接器设备中配置了适当的 DNS 服务器。有关详细信息，请参阅在连接器设备管理页面上配置网络设置。

私有服务器连接已终止

信息代码： 0x10000411

与私有服务器的连接由客户端或 Secure Private Access 服务终止。

1. 检查最终用户是否已关闭应用程序。

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

2. 检查与此日志的事务 ID 匹配的其他诊断日志，并采取相应的措施。
3. 再次启动应用程序。
4. 如果这不能解决问题，请联系 Citrix 支持并提供错误代码和事务 ID。

无法连接到私有服务 IP 或 FQDN 或向其发送数据

信息代码： 0x10000413

- 私有服务器连接已终止
- 与连接器设备和后端私有 TCP/UDP 服务器的连接问题。 检查路由域条目。确保 IP 地址有效并指向正确的后端。

无匹配策略条件

信息代码： 0x100508

用户上下文与分配给应用程序的策略中定义的访问规则条件不匹配。

更新策略配置以匹配用户上下文。

没有与应用程序关联的访问策略

信息代码： 0x100509

1. 在 Citrix Secure Private Access™ 服务 GUI 中，单击左侧导航栏中的“**访问策略**”。
2. 确保访问策略与相应的应用程序关联。
3. 如果访问策略未与应用程序关联，请为该应用程序创建访问策略。有关详细信息，请参阅创建访问策略。
4. 如果这不能解决问题，请联系 Citrix 支持。

未找到 FQDN 或 IP 地址的应用程序配置

信息代码： 0x10050A

未找到与传入的 FQDN 或 IP 地址请求匹配的应用程序。因此，该应用程序被归类为未发布的应用程序。如果这不是预期行为，请执行以下操作。

1. 转到 Secure Private Access 服务管理门户。
2. 单击左侧导航栏中的 **应用程序**。
3. 搜索应用程序，然后单击 **编辑**。
4. 将 FQDN 或 IP 地址添加到应用程序。您可以添加确切的域、IP 地址或通配符域。

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

注意： 在 **Secure Private Access > 设置 > 应用程序域** 中添加 FQDN 或 IP 地址无法解决此问题。它必须作为应用程序配置的一部分添加。

应用程序枚举信息

信息代码： 0x10050C

此代码捕获用户可能有权访问的多个应用程序的策略评估结果。应用程序访问可能因以下原因被拒绝：

- 用户上下文与分配给应用程序的策略中定义的访问规则条件不匹配 – 有关详细信息，请参阅 无匹配策略条件。
- 没有与应用程序关联的访问策略 – 有关详细信息，请参阅 无与应用程序关联的访问策略。
- 与应用程序关联的策略配置为拒绝访问 – 在这种情况下，无需采取任何操作，因为这是预期行为。
- 执行访问策略时发生意外内部错误。有关详细信息，请联系 Citrix 支持。

TCP/UDP 应用程序启动失败，因为应用程序域表中缺少路由条目

信息代码： 0x00180101

如果应用程序配置存在但路由条目缺失或之前已删除，则可能会出现此问题。

为访问的目标添加路由条目（**Secure Private Access > Settings > Application Domain**）。

TCP/UDP 应用程序启动失败，因为连接器不正常

信息代码： 0x00180102

如果没有连接器启动/响应新连接，则可能会出现此问题。

对相应资源位置上的连接器设备运行健康检查。

UDP/DNS 请求失败，因为连接器无法访问

信息代码： 0x00180103

如果 UDP/DNS 流量无法到达连接器，则可能会出现此问题。

对相应资源位置上的连接器设备运行健康检查。

页面加载失败，因为 NGS cookie 已过期

信息代码： 0x20580001

1. 重启浏览器并尝试再次打开应用程序。

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

2. 如果这不能解决问题，请联系 Citrix 支持。

由于网络故障，访问策略获取失败

信息代码： 0x20580002

1. 检查 URL 和网络连接。
2. 重新启动浏览器，然后再次尝试打开应用程序。
3. 如果这不能解决问题，请联系 Citrix 支持。

解析 JSON Web 令牌时访问策略获取失败

信息代码:0x20580003

1. 重新启动浏览器，然后再次尝试打开应用程序。
2. 如果这不能解决问题，请联系 Citrix 支持。

获取访问策略详细信息时网络故障

信息代码:0x20580004

1. 检查访问策略是否已启用。
2. 重新启动浏览器，然后再次尝试打开应用程序。
3. 如果这不能解决问题，请联系 Citrix 支持。

获取公共证书时策略获取失败

信息代码： 0x20580005

1. 重启浏览器，然后尝试再次打开应用程序。
2. 如果这不能解决问题，请联系 Citrix 支持。

验证 JSON Web 令牌签名时策略获取失败

信息代码： 0x20580007

1. 检查网络时间和用户设备时间是否同步。
2. 重启浏览器，然后尝试再次打开应用程序。
3. 如果这不能解决问题，请联系 Citrix 支持。

验证公共证书时策略获取失败

信息代码： 0x20580008

1. 重启浏览器，然后尝试再次打开应用程序。

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

2. 如果这不能解决问题，请联系 Citrix 支持。

未能确定存储环境以形成策略 URL

信息代码： 0x2058000A

1. 重启浏览器，然后尝试再次打开应用程序。
2. 如果这不能解决问题，请联系 Citrix 支持。

无法获取访问策略获取请求的响应

信息代码： 0x2058000B

1. 重启浏览器，然后再次尝试打开应用程序。
2. 如果这不能解决问题，请联系 Citrix 支持。

由于辅助 DS 身份验证令牌已过期，访问策略获取失败

信息代码： 0x2058000C

1. 重启浏览器，然后再次尝试打开应用程序。
2. 如果这不能解决问题，请联系 Citrix 支持。

连接器设备未注册

信息代码： 0x10200002

检查连接器设备注册。

有关详细信息，请参阅 将连接器设备注册到 Citrix Cloud。

无法连接到连接器设备

信息代码： 0x10200003

连接器设备无法在 Citrix Cloud 和资源位置之间进行通信。

检查连接器注册。

有关详细信息，请参阅 将连接器设备注册到 Citrix Cloud。

连接到 Citrix Secure Private Access 服务失败

信息代码： 0x10000301

检查连接器设备的网络设置。有关详细信息，请参阅 连接器设备的网络设置。

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

代理服务器不可访问

信息代码： 0x10000303, 0x10000304

检查代理服务器设置，并确保连接器设备可以访问它。有关详细信息，请参阅 将连接器设备注册到 Citrix Cloud。

代理服务器身份验证失败

信息代码： 0x10000305

检查代理服务器凭据，并确保它们在连接器设备中配置正确。有关详细信息，请参阅 注册连接器设备后。

配置的代理服务器不可访问

信息代码： 0x10000306

检查连接器设备的网络设置、防火墙设置或代理服务器设置。有关详细信息，请参阅以下主题：

- 连接器设备的网络设置
- 将您的连接器设备注册到 Citrix Cloud
- 连接器设备通信

从后端服务器收到错误响应

信息代码： 0x10000307

检查后端 Web 服务器的 HTTP 状态代码，看它是否为预期代码。

无法向目标 URL 发送请求

信息代码： 0x10000005

检查目标 URL 或检查连接器设备的网络设置。有关详细信息，请参阅连接器设备的网络设置。

SSO 处理失败

信息代码： 0x10000107

无法从 Citrix Cloud 检索应用程序配置数据。

检查连接器设备的网络设置，并确保 NTP 服务器已配置且没有时间偏差问题。有关详细信息，请参阅连接器设备的网络设置。

连接到 Citrix Secure Private Access 服务失败

信息代码： 0x10000108, 0x1000010B

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

检查连接器设备的网络设置。有关详细信息，请参阅连接器设备的网络设置。

无法处理 SSO，无法确定 SSO 设置

信息代码： 0x1000010A

检查 SSO 配置，并确保服务器可访问 Connector Appliance。

表单填充 SSO 失败，表单应用配置不正确

信息代码： 0x10000101, 0x10000102, 0x10000103, 0x10000104

检查 SSO 表单应用配置，并确保在应用设置中正确配置了用户名、密码、操作和登录 URL 字段。

Kerberos SSO 失败

信息代码： 0x10000202

检查后端服务器和域控制器上的 Kerberos SSO 设置。同时检查回退 NTLM 身份验证设置。

有关 Kerberos SSO 设置，请参阅 验证您的 Kerberos 配置。

无法处理特定身份验证类型的 SSO

信息代码： 0x10000203

检查 Secure Private Access 服务和后端服务器中的 SSO 设置。有关 Secure Private Access 服务，请参阅 设置首选登录方法。

Kerberos SSO 失败但回退到 NTLM

信息代码： 0x10000204

从域控制器检索 Kerberos 票证失败。作为辅助身份验证，Connector Appliance 已尝试回退 NTLM 身份验证。

要启用成功的 Kerberos 身份验证，请检查后端服务器和域控制器上的 Kerberos SSO 设置。

有关详细信息，请参阅验证您的 Kerberos 配置。

Citrix Workspace™ 应用程序中配置了多个 ZTNA 授权帐户

信息代码： 0x14000001

在 Citrix Workspace 应用程序中仅配置一个 ZTNA 授权帐户。

如何收集客户端日志

- **Windows 客户端：**

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

a. 打开应用程序并确保已启用日志记录。

b. 现在连接到 Secure Private Access 服务并重现您遇到的问题。

c. 在应用程序中，转到**日志记录**并单击**收集日志文件**。这将生成日志文件。

d. 将日志文件保存到客户端计算机的桌面。

- **Mac 客户端：**

a. 打开应用程序并转到**日志 > 详细**。

b. 清除日志并继续重现问题。

c. 返回到 **日志 > 导出日志**。这将创建一个包含日志文件的 zip 文件。

常见问题

以下部分提供了有关常见问题的更多信息。

在哪里可以找到有关诊断日志的更多信息?

有关诊断日志的更多信息，请参阅主题 诊断日志。

如何使用 Secure Private Access 故障排除主题来解决我遇到的故障?

1. 获取您尝试解决的故障的 信息代码。
2. 在 错误查找表 中查找信息代码。
3. 按照该信息代码提供的解决方案步骤操作。

什么是信息代码？在哪里可以找到它们?

某些日志事件（例如故障）具有关联的信息代码。在 错误查找表 中搜索此信息代码，以查找解决方案步骤或有关该事件的更多信息。

什么是事务 ID？如何使用它?

通过 Citrix Enterprise Browser 访问故障/问题时，会向最终用户显示事务 ID。管理员可以从最终用户那里获取此事务 ID，并使用此事务 ID 筛选 导致问题的确切日志，从而使他们能够识别确切的问题。一旦管理员使用事务 ID 筛选事件，将仅显示与当前问题相关的事件，从而向管理员提供有关故障或问题发生原因的所有详细信息。然后，管理员可以使用这些日志上的 错误代码 进一步解决问题。

Secure Private Access 的所有 PoP 位置有哪些?

以下是 Secure Private Access 数据 PoP 位置的列表。

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

POP 名称	区域	区域
Azure 美国东部	Azure 美国东部	弗吉尼亚
Azure 美国西部	Azure 美国西部	加利福尼亚
Azure 美国中南部	Azure 美国中南部	德克萨斯
Azure 澳大利亚东部	Azure 澳大利亚东部	新南威尔士
az-欧洲-北	Azure 北欧	爱尔兰
az-欧洲-西	Azure 西欧	荷兰
az-日本-东	Azure 日本东部	东京，埼玉
az-巴西-南	Azure 巴西南部	圣保罗州
az-亚洲-东南	Azure 东南亚	新加坡
Azure 阿联酋北部	Azure 阿联酋北部	迪拜
Azure 印度南部	Azure 印度南部	钦奈
Azure 东亚	Azure 东亚	香港

以下是 Secure Private Access 管理 PoP 位置的列表。

POP 名称	区域	区域
AWS 美国东部管理	AWS 美国东部-1	弗吉尼亚北部
aws 印度西部管理区域	AWS 亚太（孟买）区域	孟买
aws 欧洲中部管理区域	AWS 欧洲（法兰克福）区域	法兰克福

如果我无法使用信息代码和错误查找表解决故障，该怎么办?

联系 Citrix 支持。

参考

- **添加 Web 应用程序**

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

    - 支持企业 Web 应用程序
    - 配置对 Web 应用程序的直接访问
- **添加 SaaS 应用程序**
    - 支持软件即服务应用程序
    - SaaS 应用程序服务器特定配置
- **配置客户端-服务器应用程序**
    - 对客户端-服务器应用程序的支持
- **创建访问策略**
    - 创建访问策略
- **路由表**
    - 路由表

审计和系统日志

Secure Private Access 服务相关事件捕获在 **Citrix Cloud > 系统日志**中。管理员在 Citrix Secure Private Access™ 服务中执行的所有事件都发送到 Citrix Cloud 并捕获在**系统日志**中。管理员事件可以包括但不限于以下内容：

- 创建或更新应用程序
- 删除应用程序
- 配置或删除自适应访问策略
- 连接器升级
- 创建允许或阻止的网站

默认情况下，**系统日志**显示过去 30 天内发生的事件。最新事件最先显示。

日志显示事件的详细信息，并且可以通过以下方式进行筛选：

- **日期和时间：** 事件发生的日期和时间（UTC 格式）。
- **参与者：** 触发事件的用户或系统。例如，管理员、安全客户端、服务主体。
- **服务：** 记录事件的服务。Secure Private Access 事件必须将 **Secure Private Access** 作为服务。

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

- **事件：** 事件的简短描述。例如，创建 SaaS 应用程序、删除 TCP/UDP 应用程序、更新自适应访问策略、更新应用程序域。
- **目标：** 受事件影响或因事件而更改的对象。例如，用于应用程序的域。

  目标标识符采用人类可读的格式，而不是实际 ID。

下图显示了**系统日志**中的 Secure Private Access 事件。

系统日志(/en-us/citrix-secure-private-access/media/spa-system-logs.png)

有关导出事件、检索特定时间段的事件、转发日志事件和数据保留等详细信息，请参阅系统日志。

设备姿态日志和事件

管理员可以通过设备姿态仪表板监控设备合规性。他们可以查看所有已配置的设备姿态策略，这些策略定义了访问组织资源的端点的合规性要求。他们还可以查看所有设备的实时合规性状态，包括按以下类别划分的详细评估结果：

- **合规：** 满足所有指定安全要求和策略条件的设备。
- **不合规：** 未能满足一项或多项安全要求但可能仍具有有限访问权限的设备。
- **拒绝访问：** 存在重大安全风险并被阻止访问资源的设备。

您可以在 Secure Private Access 仪表板 和 Identity and Access Management 控制台中的设备姿态仪表板 中查看设备姿态日志和事件。

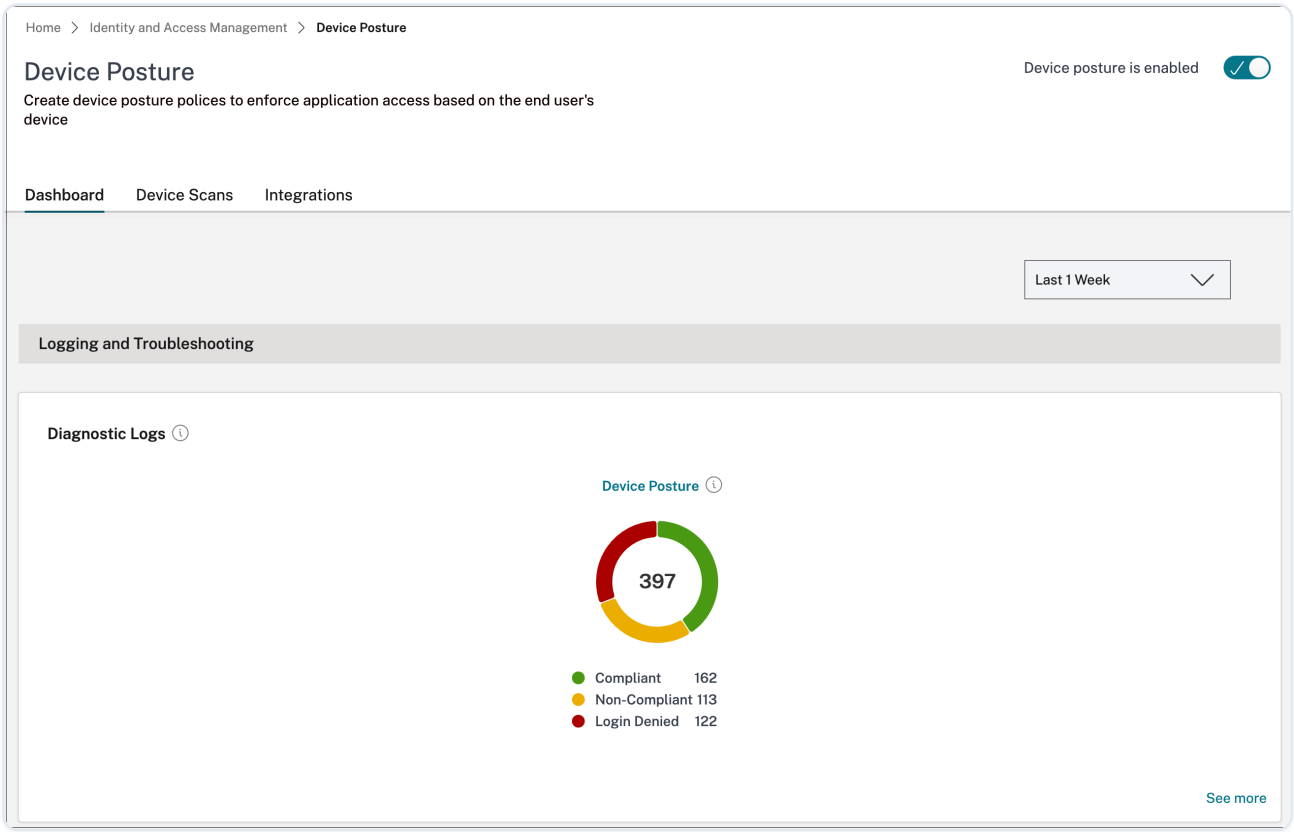
Identity and Access Management 控制台中的设备姿态仪表板

执行以下步骤以查看 Identity and Access Management 控制台中设备姿态仪表板的日志和事件。

1. 登录 Citrix Cloud。
2. 从 Citrix Cloud 菜单中，选择 **身份和访问管理**，
3. 单击 **Device Posture > Manage**，然后单击 **Dashboard**。

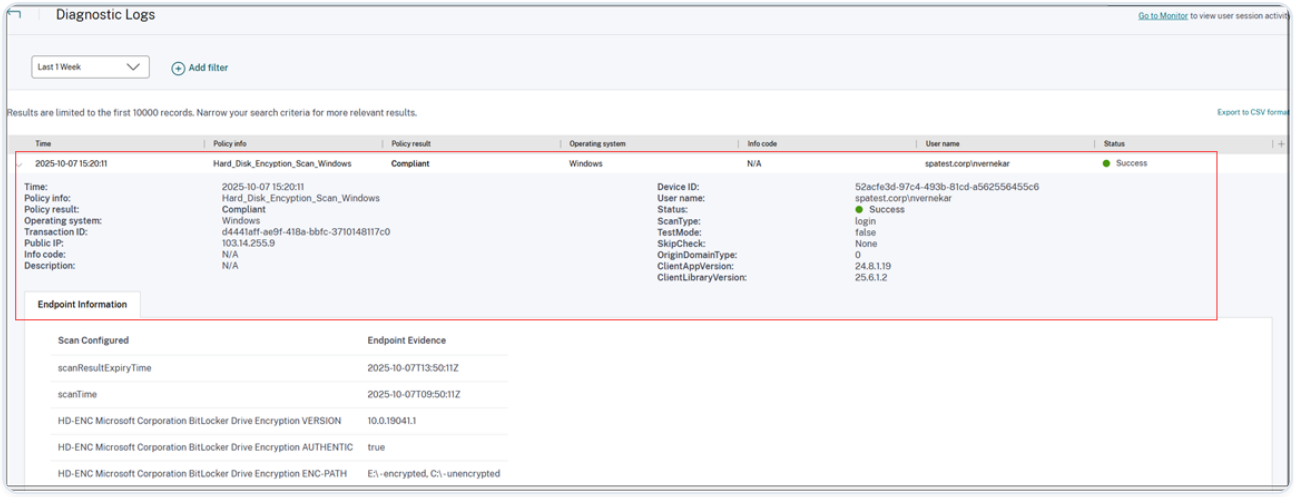
   Logging and Troubleshooting（日志记录和故障排除）部分显示与设备姿态服务相关的诊断日志。
4. 单击**查看更多**链接以查看日志详细信息。您可以根据策略结果（**合规**、**不合规**和**登录被拒绝**）优化搜索。

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



您可以使用**添加筛选器**选项根据各种条件（例如策略信息、策略结果、操作系统、事务 ID、信息代码或设备 ID）优化搜索。例如，在搜索字段中，您可以单击 **Device-ID**，选择 **~ (包含某些值)**，然后输入 6273。将显示与包含 6273 的设备 ID 相关的所有日志。

点击每个日志条目旁边的展开图标，查看详细信息，例如扫描类型、客户端应用程序版本、客户端库版本和端点信息。



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

注意：

- **ClientAppVersion** 和 **ClientLibraryVersion** 字段分别显示 EPA 客户端版本和库版本。
- 每当访问被拒绝时，事务 ID 也会显示给最终用户。
- 如果出现错误或扫描失败，设备姿态服务会显示一个事务 ID。此事务 ID 在 Secure Private Access 服务仪表板中可用。如果日志无法帮助解决问题，最终用户可以与 Citrix 支持部门共享事务 ID 以解决问题。

日志位置

Windows 客户端日志位于：

- %localappdata%\Citrix\EPA\dpaCitrix.txt
- %localappdata%\Citrix\EPA\epalib.txt

macOS 客户端日志位于：

- ~/Library/Application Support/Citrix/EPAPlugin/EpaCloud.log
- ~/Library/Application Support/Citrix/EPAPlugin/epaplugin.log

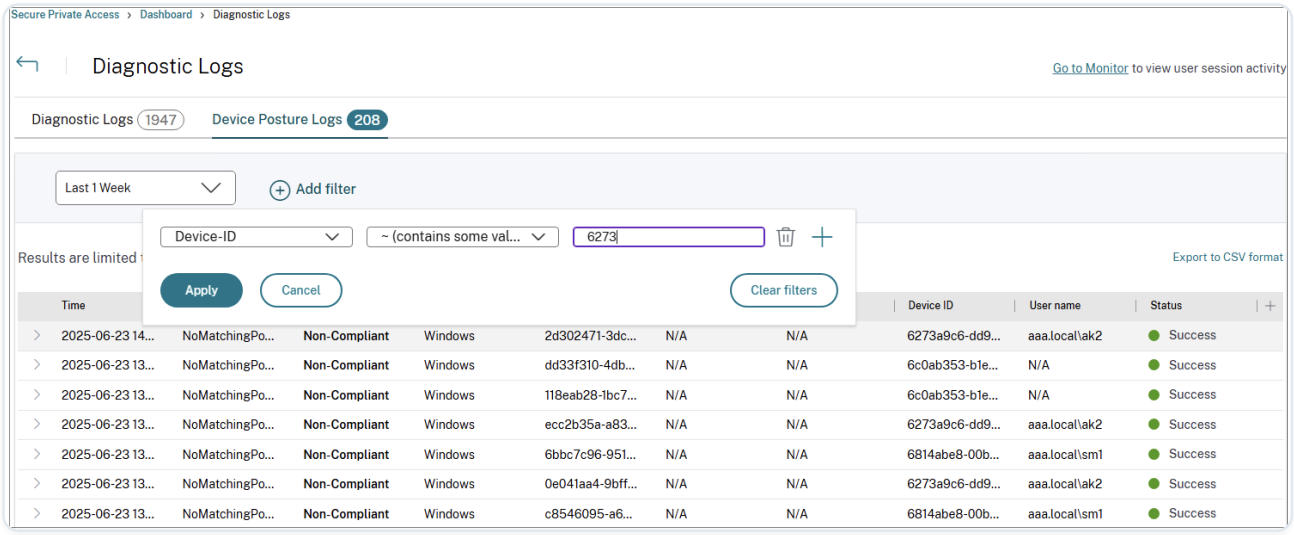
安全私有访问仪表板

执行以下步骤以查看设备姿态服务的日志和事件。

1. 登录 Citrix Cloud。
2. 在 Secure Private Access 磁贴上，单击**管理**，然后单击**控制板**。

   “**日志记录和故障排除**”部分显示与设备姿态服务相关的诊断日志。
3. 单击**查看更多**链接以查看日志详细信息。您可以根据策略结果（**合规**、**不合规**和**登录被拒绝**）优化搜索。

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



设备姿态错误日志

可以在 Citrix Monitor 和 Secure Private Access 控制板上查看与设备姿态服务相关的以下日志。对于所有这些日志，建议您联系 Citrix 支持部门以获取解决方案。

- 未能读取已配置的策略
- 未能评估端点扫描
- 未能处理策略/表达式
- 未能保存端点详细信息
- 未能处理来自端点的扫描结果

设备姿态数据导出

设备姿态服务事件（例如设备姿态结果和事件类型）可以导出到安全信息和事件管理 (SIEM) 服务。当 Citrix Endpoint Analysis (EPA) 客户端对尝试访问 Citrix Virtual Apps and Desktops™ 或 Citrix Secure Private Access 资源的设备执行姿态检查时，会生成这些事件。

- 要了解如何设置、配置设备姿态服务日志并将其导出到 SIEM，请参阅安全信息和事件管理 (SIEM) 集成。
- 要详细了解可以从设备姿态服务导出的事件和日志，请参阅设备姿态服务事件。
- 要了解如何诊断和排查设备姿态服务事务，请参阅诊断设备姿态服务事务。

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

数据导出和第三方集成

以下部分提供了有关数据导出和第三方集成的更多信息。

安全信息和事件管理集成

Secure Private Access 与安全信息和事件管理 (SIEM) 的集成使管理员能够使用 Kafka 推送机制将关键日志、策略结果和用户活动数据导出到第三方 SIEM 系统。此集成可为使用 Citrix Secure Private Access 服务的组织提供增强的可见性、合规性跟踪和安全洞察。

您可以使用任何 SIEM，例如 Splunk、Google Chronicle、Microsoft Sentinel 或 Elastic。

有关 SIEM 中与 Secure Private Access 和设备状态服务相关的用户事件列表，请参阅以下主题：

- 安全私有访问事件
- 设备状态服务事件

使用 OData API 构建自定义报告

Secure Private Access Monitor OData REST API 使管理员能够导出会话数据并构建自定义报告。此功能有助于跟踪部署、分析用户活动以及深入了解 Secure Private Access 服务的性能和使用情况。

有关可用于导出的 Secure Private Access 数据类型的信息，请参阅以下主题：

- 安全私有访问会话
- Secure Private Access 应用程序
- 安全私有访问枚举

导出系统日志

Citrix Cloud 中的 **系统日志** 功能提供在 Secure Private Access 服务中发生的事件的时间戳记录。管理员可以将这些日志导出为 CSV 文件，以便进一步分析和验证。有关详细信息，请参阅来自 Citrix Cloud 的 Syslog。

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

从 Kafka 导出数据

Kafka 是一个开源的分布式流处理平台，专为实时数据处理和分析而设计。通过使用 Kafka，组织可以实时分析流数据，以获得更快的洞察力，实现主动决策，并支持高级安全监控功能。

您可以从 Kafka 导出 Secure Private Access 事件和 Device Posture 服务事件，以便与外部安全信息和事件管理 (SIEM) 系统、分析平台和自定义监控解决方案集成。

安全私有访问事件

当用户通过 Citrix Secure Private Access（例如 Citrix Workspace 应用程序、Citrix Secure Access 客户端或 Citrix Enterprise Browser）访问应用程序时，用户事件会实时接收到 Citrix Analytics for Security 中。

有关更多信息，请参阅 Secure Private Access 事件。

Device Posture 服务事件

当 Citrix Endpoint Analysis (EPA) 客户端对尝试访问 Citrix Virtual Apps and Desktops 或 Citrix Secure Private Access 资源的设备执行姿态检查时，会生成用户事件。

有关更多信息，请参阅 Device Posture 服务事件。

导出审计和系统日志

Citrix Cloud 中的 **系统日志** 功能捕获 Secure Private Access 服务中发生的事件的完整、带时间戳的记录。这些审计日志对于法规遵从性、安全监控和故障排除管理操作至关重要。管理员可以将日志数据导出为 CSV 文件，以便进行详细分析、合规性验证以及与外部安全监控系统无缝集成。

Secure Private Access 服务的 **系统日志** 中捕获以下事件：

- 应用程序配置更改，包括创建、修改和删除。
- 策略更新，例如访问规则、安全配置和条件访问设置。
- 用户和组管理操作，例如添加或删除用户和组。
- 应用程序域相关信息。
- 允许和阻止的 URL 列表。

使用 SystemLog API 导出 Secure Private Access 事件

您可以使用 SystemLog API 导出 Secure Private Access 事件。SystemLog API 允许您检索在指定时间段内 Citrix Cloud 帐户中发生的事件。

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

- 有关使用 SystemLog API 导出事件的详细信息，请参阅 Citrix Developer 文档中的 Citrix Cloud - SystemLog。
- 要了解 **系统日志** 为 Secure Private Access 服务捕获的事件数据，请参阅 系统日志事件参考。
- 要了解有关 Monitor 服务 API 的更多信息，请参阅 关于 Citrix Monitor 服务 API。

使用 OData 导出会话数据

Secure Private Access Monitor OData REST API 使管理员能够导出会话数据并构建自定义报告。此功能对于跟踪部署、分析用户活动以及深入了解 Secure Private Access 服务的性能和使用情况特别有用。

- 管理员可以利用 OData REST API 创建满足特定组织需求的自定义报告。这种灵活性有助于对会话数据、用户活动和应用程序使用情况进行详细分析。
- 这些 API 能够跟踪部署，帮助管理员监控整个组织中 Secure Private Access 配置和策略的采用和有效性。
- 使用 OData API，可以导出会话数据以在外部工具或系统中进行进一步分析。

有关 Secure Private Access Monitor OData REST API 的详细信息，请参阅以下主题：

- 安全私有访问会话
- Secure Private Access 应用程序
- 安全私有访问枚举

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

基于角色的访问控制

Secure Private Access 使用基于角色的访问控制模型来管理用户权限和访问级别。这意味着每个用户都被分配一个特定角色，该角色决定了他们可以在系统中执行哪些操作以及不能执行哪些操作。此模型有助于确保用户拥有执行任务所需的适当访问级别，同时防止他们访问不应访问的敏感数据或功能。

Secure Private Access 管理员有以下四个主要角色。每个角色都有一组不同的权限，旨在满足不同类型用户的需求。

- 完全访问管理员
- 只读管理员
- 完全监控管理员
- 技术支持管理员

注意：

要使用 DaaS Monitor 监控 Secure Private Access，管理员除了 Secure Private Access 角色之一外，还必须分配 DaaS 角色。

下表简要说明了每个角色：

角色	描述
完全访问管理员	适用于需要完全控制 Secure Private Access 环境的配置、管理和操作的个人。完全访问管理员拥有以下权限。
	访问所有 Secure Private Access 功能。
	在 Secure Private Access 控制台中创建、编辑和修改应用程序、策略和设置的权限。
只读管理员	适用于需要监控和分析 Secure Private Access 活动和系统性能的个人。只读管理员具有以下权限。

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

角色	描述
	访问 Secure Private Access 控制板。
	能够查看所有 Secure Private Access 应用程序配置和设置。
	只读管理员无权使用任何创建/更新/删除功能。
完全监控管理员	适用于负责在监控控制台中监控 Secure Private Access 活动和性能的用户。完全监控管理员具有以下权限。
	访问 Secure Private Access 中的所有监控控制板和报告工具。
	能够查看所有 Secure Private Access 配置和设置。
	完全监视管理员无权创建、编辑或修改 Secure Private Access 配置、策略或设置。
帮助台管理员	适用于负责故障排除和分类用户访问问题的帮助台人员。帮助台管理员具有以下权限。
	对 Secure Private Access 配置和设置的可见性有限，侧重于监视控制台中与故障排除相关的信息。
	访问 Secure Private Access 控制台中的特定故障排除工具和诊断实用程序。
	查看故障排除和监视控制板。
	帮助台管理员无权创建、编辑或修改 Secure Private Access 配置或策略。

角色和权限

下表总结了角色和权限：

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

	完全访问管理员	只读管理员	完全监控管理员	服务台管理员
创建/编辑/删除应用程序	是	否	否	否
创建/编辑/删除策略	是	否	否	否
编辑配置/设置	是	否	否	否
查看配置/设置	是	是	是	有限
在 Secure Private Access 控制板中查看日志记录和故障排除小组件	是	是	是	是
搜索用户	是	是	是	否
检索已配置的域	是	是	是	否
查看 Secure Private Access 仪表板中的用户、应用程序、访问策略小组件	是	是	是	否
在监控仪表板中查看会话和应用程序	是	是	是	有限
访问报告工具	是	否	是	有限

为管理员启用基于角色的访问

执行以下步骤为管理员启用基于角色的访问：

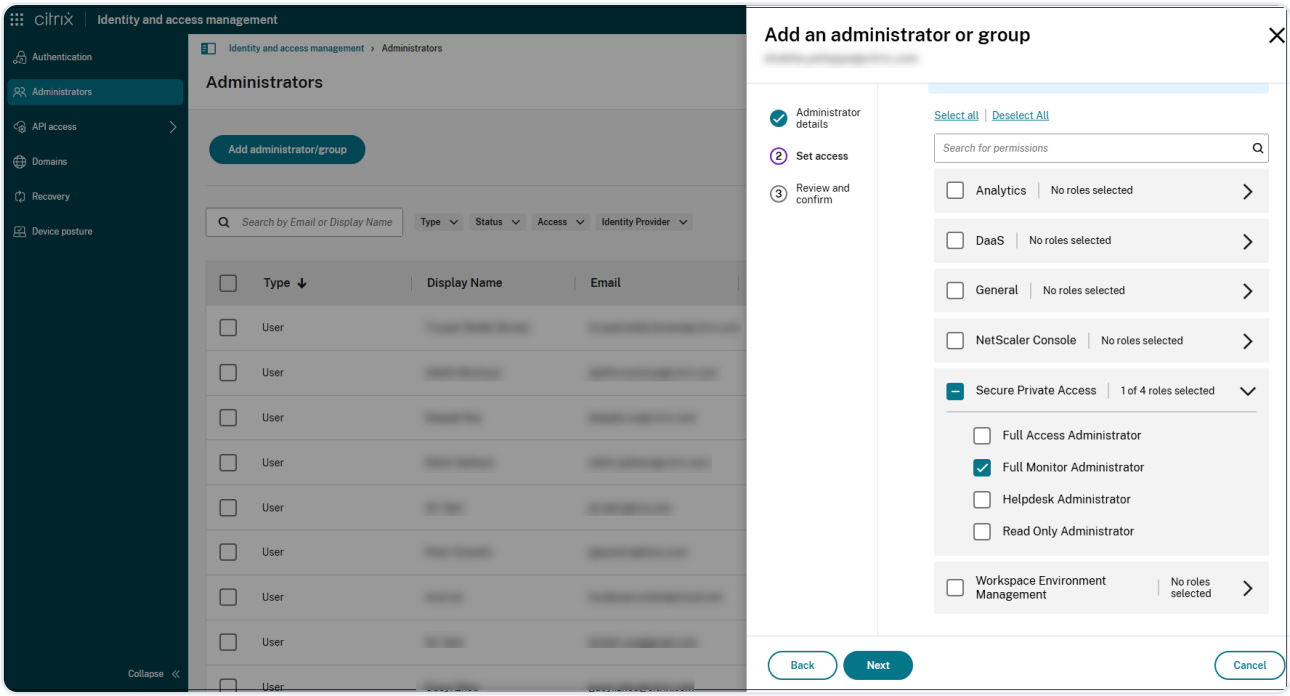
1. 登录 Citrix Cloud™ 后，从菜单中选择 **身份和访问管理**。
2. 在 **身份和访问管理** 页面上，单击 **管理员**，然后单击 **添加管理员/组**。控制台将显示帐户中的所有当前管理员。

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

3. 在 **添加管理员或组** 中，选择要从中选择管理员的身份提供程序。有时，Citrix Cloud 可能会提示您首先登录身份提供程序（例如，Azure Active Directory）。
4. 如果选择了 **Citrix Identity**，请输入用户的电子邮件地址，然后单击 **Next**。
5. 选择 **Custom access**，然后单击 **Secure Private Access** 中的 **>** 图标。
6. 选择以下角色之一，然后单击 Next。
   - 完全访问管理员
   - 只读管理员
   - 完全监控管理员
   - 服务台管理员
7. 点击 **发送邀请**。

注意：

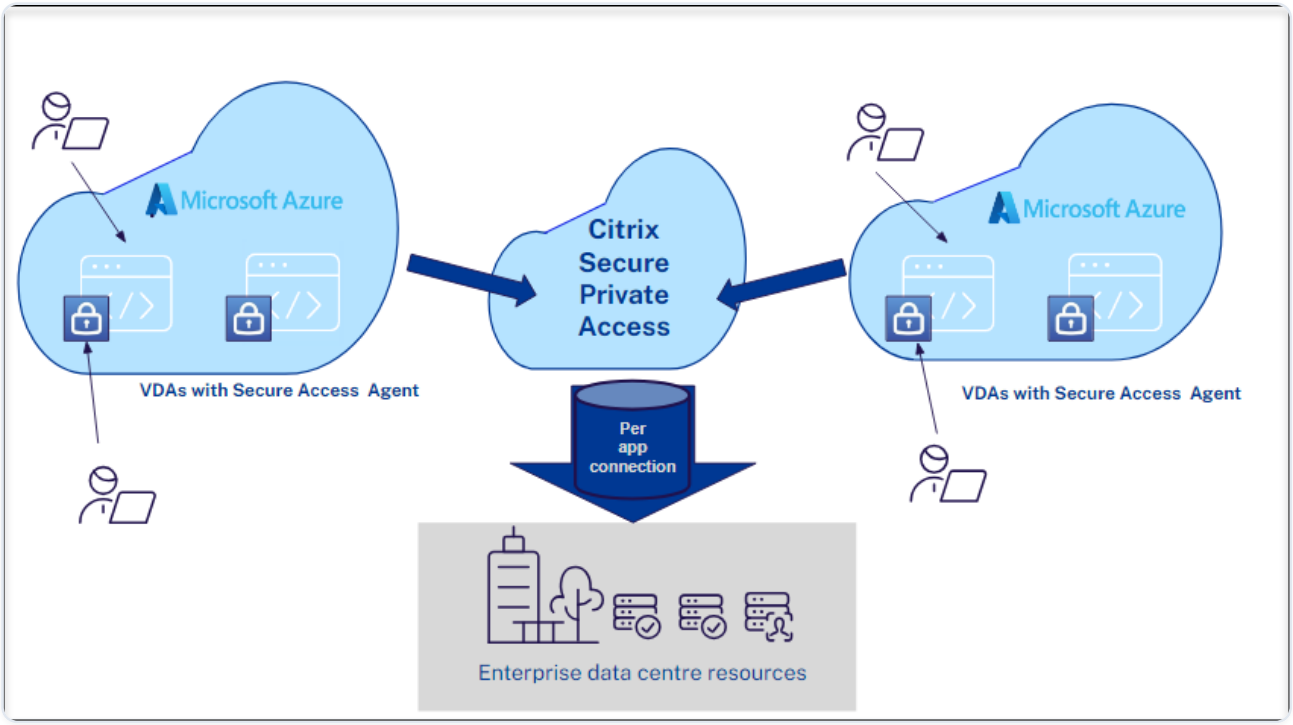
必须为所有 Secure Private Access 角色启用 **Analytics** 和 **General** 服务。**Analytics** 服务对于监控和报告是必需的，而 **General** 服务对于身份验证、域、授权、流量路由和其他功能是必需的。



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

支持多会话虚拟桌面基础设施

在多会话虚拟桌面基础设施 (VDI) 中，多个用户共享一台虚拟机，同时保持独立的桌面环境。从 Citrix Secure Access 客户端 for Windows 24.8.1.19 版本开始，您可以通过确保每个用户的会话保持隔离、私密和受保护，从多会话 VDI 访问您的企业应用程序，以用于 Secure Private Access 部署。



注意：

- 多会话 VDI 在 Windows 操作系统上受支持，从 Windows 10 和 Windows Server 2019 开始。
- 多会话 VDI 仅适用于基于 Azure 的 VDI。

主要功能和优势

- **身份验证：** 支持各种身份验证方法，包括基于条件的身份验证。
- **上下文访问：** 仅允许基于 Secure Private Access 策略，根据位置、设备和组等因素，为用户访问授权应用程序。

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

- **降低成本：** 允许多个用户共享计算机，这有助于组织节省硬件成本。Citrix Secure Access™ 客户端 for Windows 应用程序通过让用户从任何设备访问其虚拟桌面，进一步提高了这些成本节约，减少了对专用工作站的需求，而无需依赖专线或传统 VPN。
- **增强的灵活性：** 使最终用户能够从任何地方连接，遵守 Secure Private Access 策略，仅允许授权应用程序访问。

启用多会话 VDI

要在 Citrix Secure Access 客户端 for Windows 应用程序中启用多会话 VDI 支持，管理员必须确保多会话操作系统计算机上已安装 Citrix Secure Access 客户端 for Windows 24.8.1.19 或更高版本。

管理员必须执行以下步骤，为多会话操作系统计算机上的用户提供上下文访问：

1. 打开 **注册表编辑器** (**regedit.exe**)。
2. 导航到 **HKEY_LOCAL_MACHINE\Software\Citrix\Secure Access Client**。
3. 创建 `EnableMultiSessionFlow` 和 `EnableWFP` 注册表项以启用多会话 VDI。有关详细信息，请参阅 NetScaler Gateway Windows VPN 客户端注册表项。
4. 关闭 **注册表编辑器**。
5. 重新启动计算机以确保设置生效。

对于域控制器 IP 地址与 DNS IP 地址相同的域加入计算机，管理员必须执行以下步骤才能启用多会话 VDI。

1. 打开 **注册表编辑器** (**regedit.exe**)。
2. 导航到 **HKEY_LOCAL_MACHINE\Software\Citrix\Secure Access Client**。
3. 创建 `EnableMultiSessionFlow` 和 `AlwaysOnService` 注册表项以启用多会话 VDI。有关详细信息，请参阅 NetScaler Gateway Windows VPN 客户端注册表项。
4. 创建类型为 **REG_SZ** 的 `CloudAlwaysOnUrl` 注册表项并提供连接 URL。
5. 关闭 **注册表编辑器**。
6. 重新启动计算机以确保设置生效。
7. 在 Secure Private Access 控制板上，为域控制器和云连接器创建应用程序。

> **注意：**
>
> 当域控制器 IP 地址与 DNS IP 地址相同时，所有发往域控制器的调用都将被拦截并丢弃。为避免域控制器数据包被丢弃，建议创建应用程序并为所有用户启用访问。

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

8. 将与 DNS 服务器 IP 地址匹配的域控制器 IP 地址添加到应用程序，并允许所有 TCP/UDP 端口。
9. 设置访问策略以确保所有用户可以访问域控制器。
10. 将云连接器添加到流量路由类型**外部**，以防止其被隧道化，如果云连接器的主机名与您的后缀匹配（例如，云连接器的主机名为 cloudconnector.cloud.com，后缀为 *.cloud.com）。

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

适用于移动设备的 Citrix Secure Private Access

Citrix Secure Private Access 部署支持移动设备，从适用于 iOS 的 Secure Access Client 25.08.1 版和适用于 Android 的 Secure Access Client 25.11.1 版开始。移动用户可以在 Secure Private Access 零信任模型下访问企业应用程序和 Web 资源，提供与桌面用户相同的安全控制、策略实施和无缝体验。

支持的版本和平台

iOS 设备：

- **CSA 客户端**：iOS 25.08.1（可在 App Store 上获取）
- **iOS 操作系统版本**：最低 iOS 16
- **部署模型**
  - 适用于云部署的 Secure Private Access
  - 适用于混合部署的 Secure Private Access

Android 设备：

- **CSA 客户端**：Android 25.11.1（可在 Google Play 商店上获取）
- **Android 操作系统版本**：最低 Android 12
- **部署模型**
  - 适用于云部署的 Secure Private Access
  - 适用于混合部署的 Secure Private Access

支持的功能

对于 Secure Private Access 部署，资源访问通过策略配置进行控制。管理员可以定义策略，指定哪些用户或组在特定条件下以及从经批准的设备或位置可以访问特定的应用程序和资源。

- 根据您的 Secure Private Access 策略条件访问 Web、SaaS 和 TCP/UDP 应用程序。

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

- 会话安全策略：Chrome Enterprise 支持的数据丢失防护 (DLP) 控制。

有关支持功能的完整列表，请参阅 NetScaler Gateway 中支持的 Citrix Secure Access 客户端功能。

先决条件

Secure Private Access 服务必须已配置并保持最新。有关详细信息，请参阅以下主题：

- 思杰安全私有访问入门
- Secure Private Access 入门和设置
- 应用程序配置和管理

适用于使用 Citrix Secure Access 客户端的 iOS 和 Android 用户的流程

以下步骤总结了使用 Citrix Secure Access 客户端的 iOS 和 Android 设备用户的 Secure Private Access 流程。

- **Citrix Secure Access 客户端安装**：必须在移动设备上安装 Citrix Secure Access 客户端。这可以通过企业设备的移动设备管理 (MDM) 实现，或者由用户从设备的应用商店手动下载应用程序来完成。
- **访问应用商店/网关 URL**：用户随后访问指定的应用商店或网关 URL。此 URL 用作访问组织资源的入口点。
- 用户身份验证：系统会提示用户验证其身份。这通常涉及输入凭据（例如用户名和密码），或使用多重身份验证 (MFA) 方法。
- **策略评估和访问授权**:
  - 策略满足：如果用户的身份验证和设备姿态满足定义的安全性策略，则授予访问权限。这允许用户访问授权的 Web、SaaS 和私有 Web 应用程序。
  - 策略失败：如果用户未能满足策略要求（例如，过时的操作系统、未经批准的设备、不正确的凭据），则根据策略配置，访问权限将受到限制或完全拒绝。
- **强制会话保护**：授予访问权限后，将强制执行 Chrome Enterprise 支持的数据丢失防护 (DLP) 控件。例如：
  - 禁用隐身模式
  - 阻止打印

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

- URL 过滤
- 阻止下载
- 配置的（托管的）书签

相关主题

- 适用于云部署的 Citrix Secure Private Access
- 适用于混合部署的 Citrix Secure Private Access

使用 iOS Kerberos 扩展进行 Kerberos 身份验证

本主题概述了通过适用于 iOS 的 Citrix Secure Access 应用程序为内部 Web 应用程序启用基于 Kerberos 的单点登录 (SSO) 所需的端到端配置。

- iOS 客户端配置
- MDM 服务器配置
- IIS 配置
- 域控制器配置

iOS 客户端配置

以下部分提供了有关 iOS 客户端配置的更多信息。

先决条件

确保 iOS 设备已注册 MDM。 在应用任何 SSO 配置之前，iOS 设备必须注册 MDM 解决方案（例如 Microsoft Intune）。MDM 注册允许将 Kerberos SSO 扩展配置文件推送到设备。

验证 iOS 设备上的 MDM 注册

1. 在 iOS 设备上，转到“**设置 > 通用 > VPN 与设备管理**”。

   在“设备管理”下，您必须看到列出了您组织的 MDM 配置文件（例如，Microsoft Intune 或您公司的 MDM 配置文件名称）。
2. 点击配置文件以确认其已安装，并且状态显示为“**已验证**”或“**已安装**”。
3. 要确认 Kerberos SSO 扩展已由 MDM 推送：

   - 前往 **设置 > 通用 > VPN 与设备管理**。
   - 点击 MDM 配置文件，在配置文件详细信息下查找 **单点登录扩展** 或 **Kerberos**。

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

- 或者，前往 **设置 > 通用 > VPN 与设备管理 > 单点登录** 并验证 Kerberos 扩展是否已列出。

如果设备未注册或配置文件缺失，请联系您的 MDM 管理员在继续操作之前注册设备。

MDM 服务器配置

注意：

MDM SSO 扩展负载配置基于官方 Apple 文档。

- 适用于 Apple 设备的单点登录设备管理负载设置
- 适用于 Apple 设备的 Kerberos 单点登录扩展

确保在 MDM SSO 扩展负载中配置了以下字段：

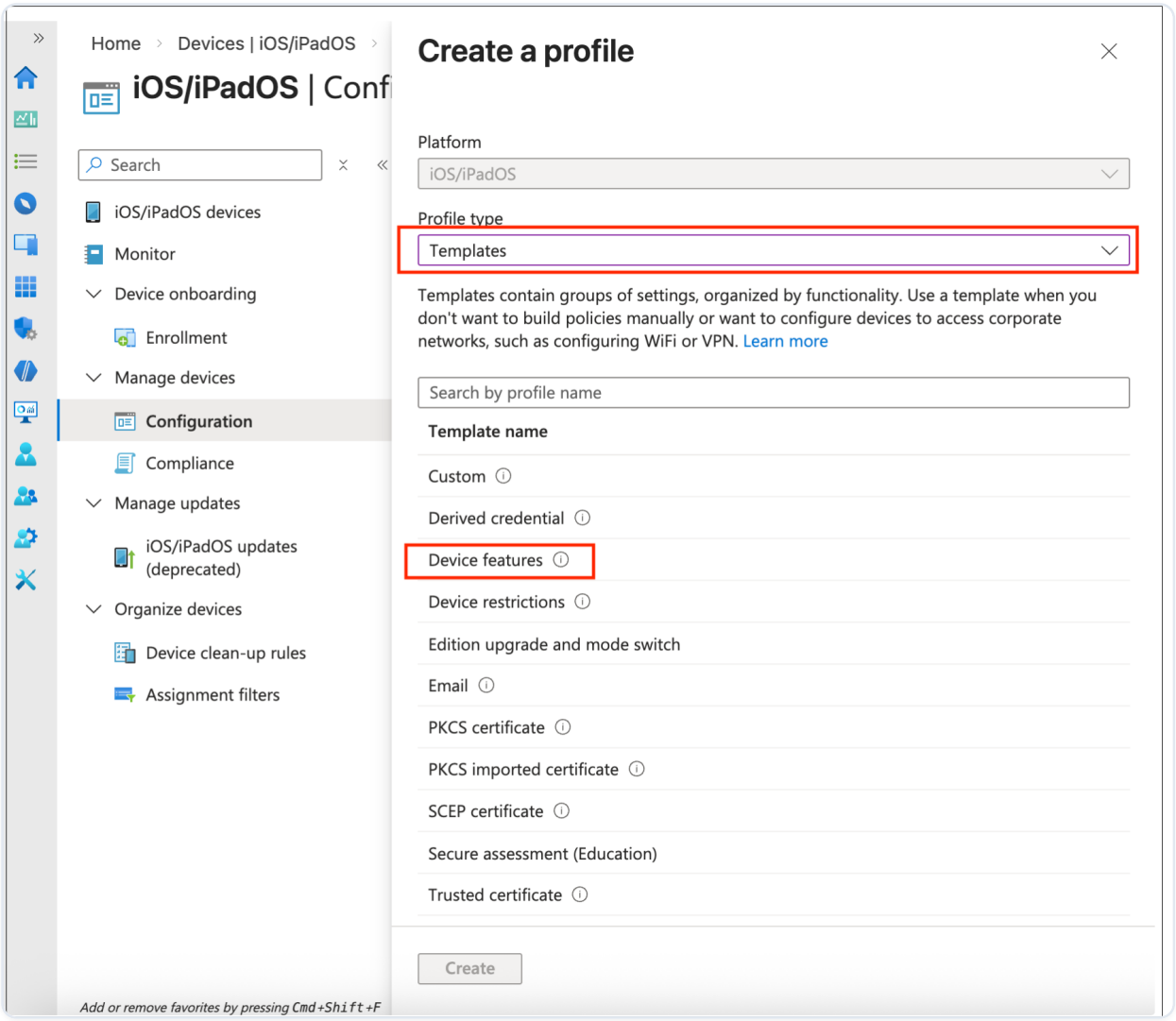
1. **域：** 用于 Kerberos 的 URL。
2. **AppBundleIDs：** 将使用的应用程序的允许列表。（例如，Chrome：`com.google.chrome.ios`，Citrix Secure Access：`com.citrix.securehub`）
3. **领域：** 您的数据中心位置。

Intune 策略配置

先决条件： 确保 iOS 设备已注册到 Intune。

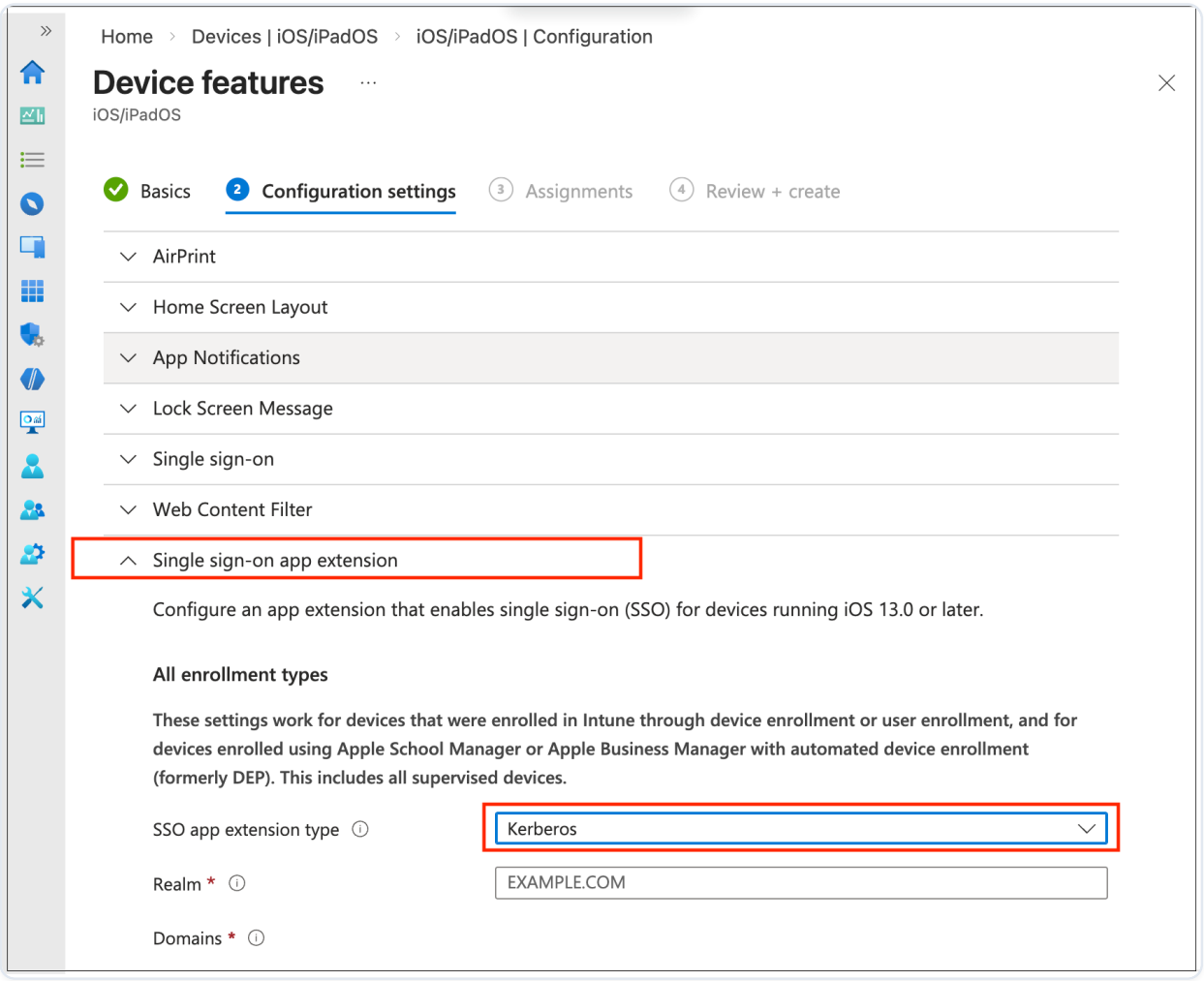
1. 在 Intune 管理控制台中，转到**主页 > 设备** | **iOS/iPadOS → iOS/iPadOS** | **配置**。
2. 创建新策略。
3. 在**配置文件类型**中选择**模板**，然后选择**设备功能**。

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



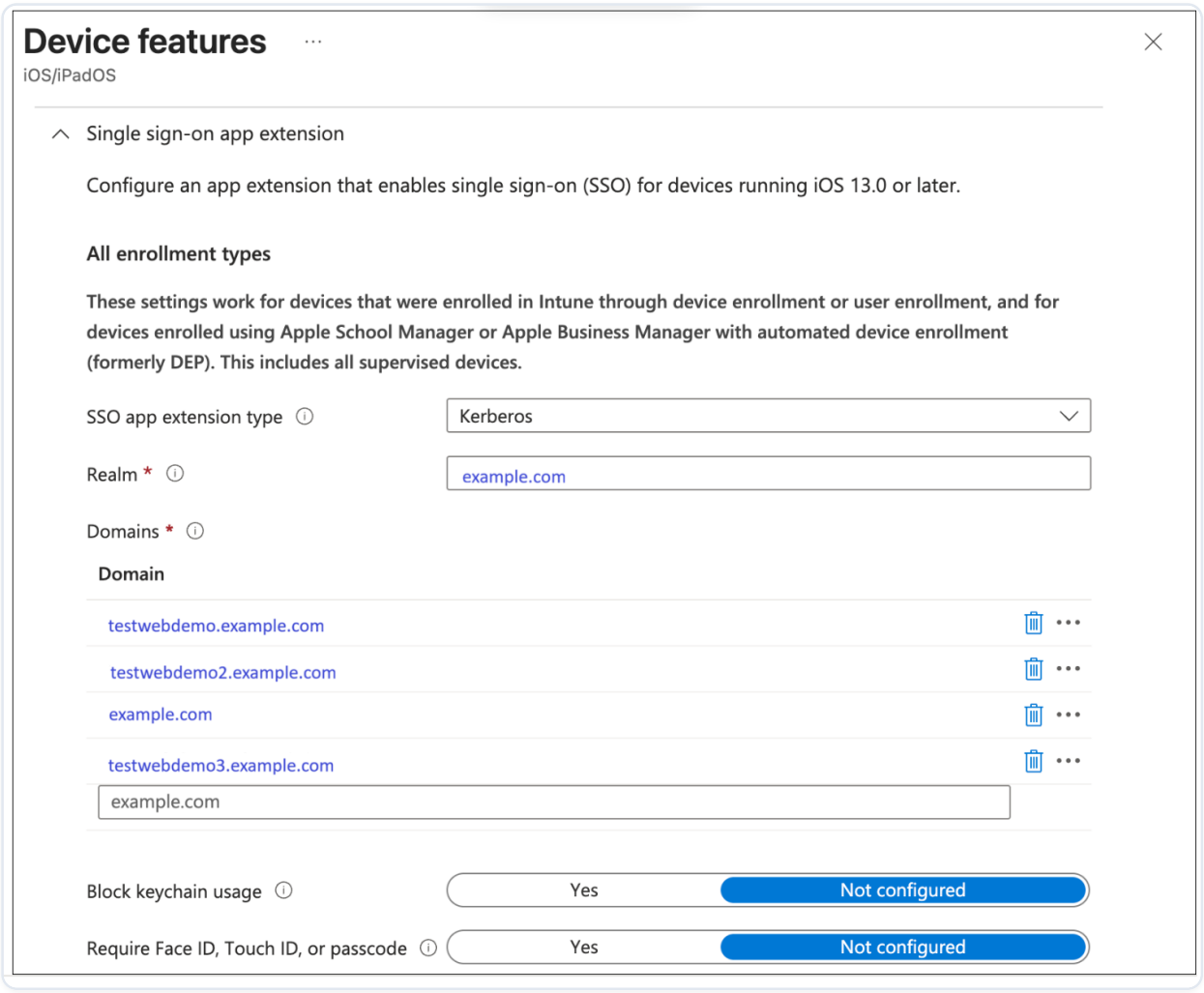
4. 按**创建**。
5. 输入策略名称，然后继续进行**配置设置**。
6. 在**单一登录应用扩展 > SSO 应用扩展类型**中选择 **Kerberos**。

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

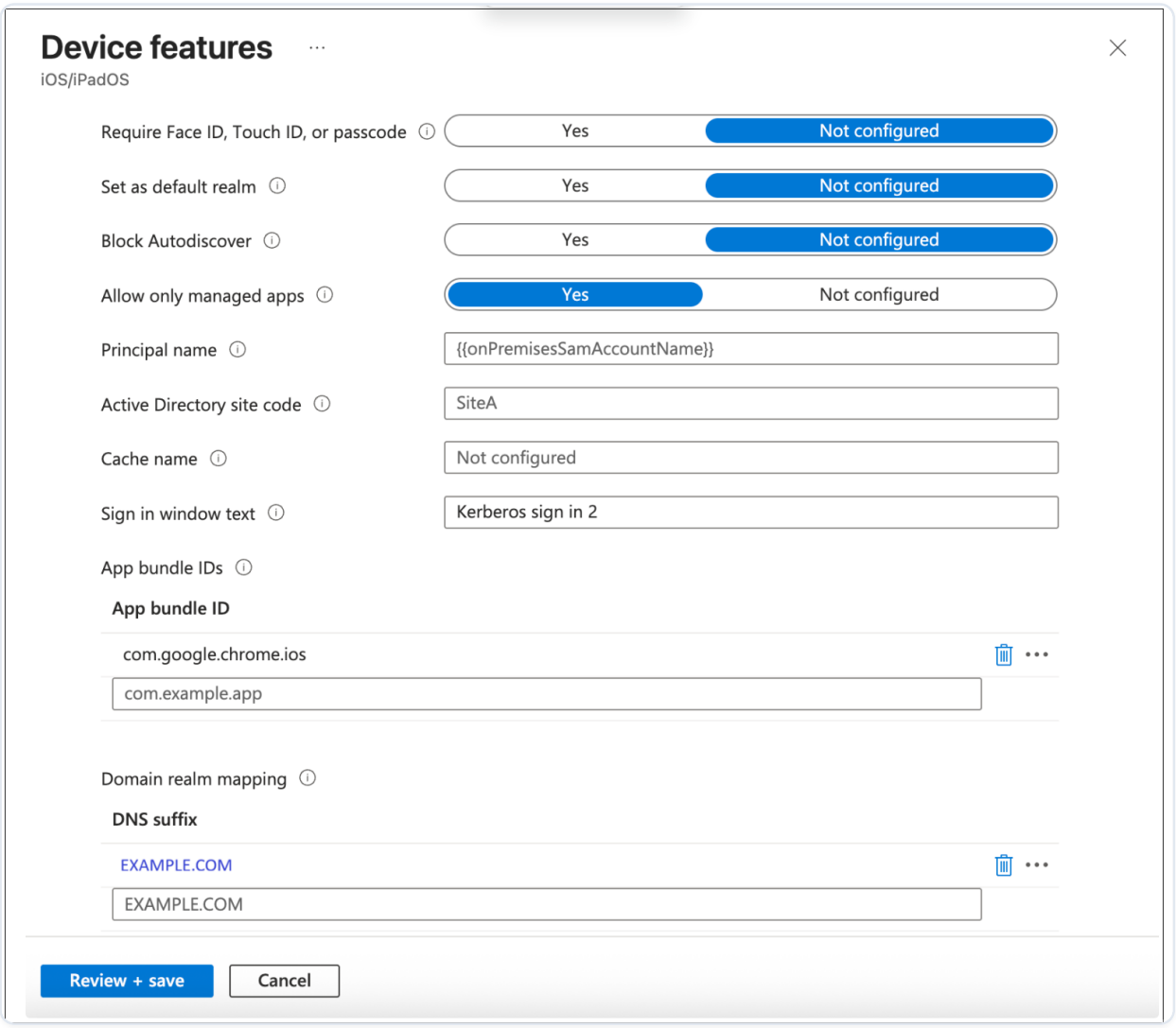


7. 根据您的设置要求填写信息。

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



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



8. 按**审查 + 保存**。
9. 将策略绑定到您的设备：
   - 转到**编辑策略**，单击该策略。
   - 编辑**分配**。
   - 选择您的设备组（如果尚未创建，请先使用您的设备创建一个设备组）。
10. 同步设备。

IIS 配置

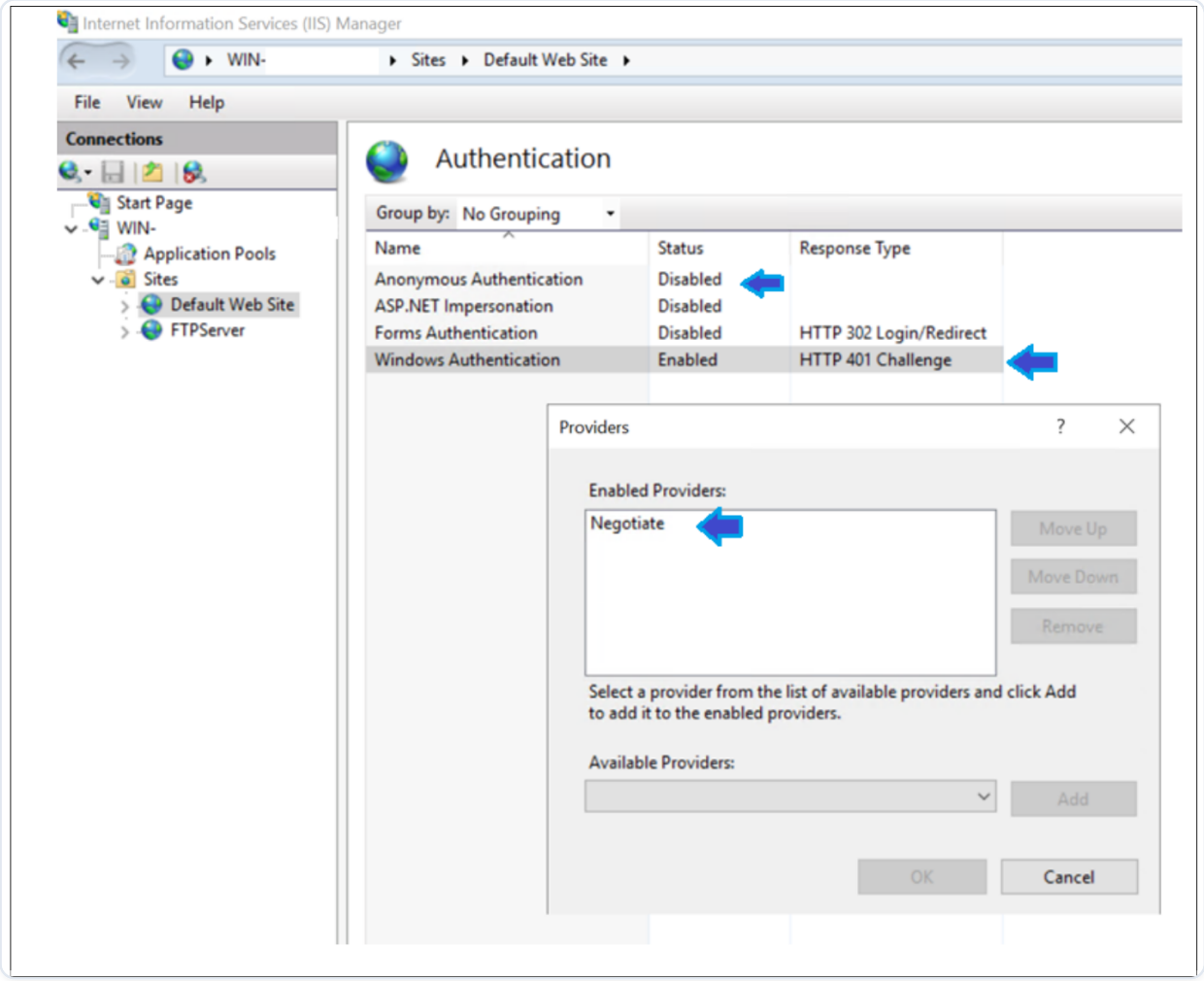
在 IIS Web 服务器上，启用带 Negotiate 提供程序的 **Windows 身份验证**，并禁用 **匿名身份验证** 以强制执行基于 Kerberos 的身份验证。

配置 IIS 身份验证的步骤：

1. 打开 IIS 管理器（从“**运行**”或“**开始**”中选择 **inetmgr**）。
2. 在“**连接**”窗格中，选择要配置的站点或应用程序。

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

3. 在“功能视图”的 IIS 部分中，双击“**身份验证**”。
4. 禁用“**匿名身份验证**”。
   - 选择“**匿名身份验证**”，然后在“**操作**”窗格中单击“**禁用**”。
5. 启用“**Windows 身份验证**”。
   - 选择“**Windows 身份验证**”，然后在“**操作**”窗格中单击“**启用**”。
6. 设置 Negotiate 提供程序。
   - 在选中“**Windows 身份验证**”的情况下，在“**操作**”窗格中单击“**提供程序...**”。
   - 确保 **Negotiate** 列在首位（在 NTLM 之上）。如果缺少，请添加。
   - 点击**确定**。
7. 点击**操作**窗格中的**应用**以保存更改。
8. （可选）从提升的命令提示符运行 `iisreset` 以立即应用配置。



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

域控制器端配置

短名称和 FQDN 的 SPN 注册：Kerberos 要求客户端使用的 URL 与域上注册的 SPN 之间精确匹配。访问 `http://testwebdemo` 的客户端使用的 SPN 与访问 `http://testwebdemo.example.com` 的客户端使用的 SPN 不同，因此两者都必须注册。

1. 将下面的 `<dc-hostname>` 替换为您的域控制器的主机名。
2. 注册这两种形式。
   - 短主机名（当客户端通过短名称访问时使用，例如 `http://testwebdemo`）

     `setspn -s HTTP/testwebdemo example.com\<dc-hostname>`
   - FQDN（当客户端通过完全限定域名访问时使用，例如 `http://testwebdemo.example.com`）

     `setspn -s HTTP/testwebdemo.example.com example.com\<dc-hostname>`
3. 验证两者都已在正确的帐户上注册
   - setspn -L example.com\<dc-hostname>
4. 预期输出必须包含两者：
   - 超文本传输协议/测试网络演示
   - HTTP/testwebdemo.example.com

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

功能弃用

本文提前通知您 Secure Private Access 服务中正在逐步淘汰的功能，以便您及时做出业务决策。Citrix 会监控客户使用情况和反馈，以确定何时撤回功能。公告可能会在后续版本中更改，并且可能不包括所有已弃用的功能。有关产品生命周期支持的详细信息，请参阅 产品生命周期支持策略。

下表列出了已弃用或计划弃用的 Secure Private Access 服务功能。

项目	弃用公告发布于	弃用日期	替代方案
用于 Web 应用程序访问的无客户端 VPN 访问方法	2023 年 1 月	October 17, 2023	根据您的用例，使用 Citrix Enterprise Browser 或 Direct Access。有关更多详细信息，请参阅 关于 Web 应用程序访问的无客户端 VPN 访问弃用。
基于类别的 Web 过滤	2022 年 12 月	December 31, 2022	Secure Private Access 中每个网站的允许、拒绝或 RBI 重定向功能将保留，以通过 Citrix Enterprise Browser 提供对非工作相关网站的选择性访问。
限制导航安全控制	2022 年 4 月	15 June 2022	不适用
Citrix 网关连接器	2022 年 5 月	30 September 2022	连接器设备。要将您的网关连接器迁移到连接器设备，请参阅 将网关连接器迁移到连接器设备。

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

关于弃用无客户端 VPN 访问以进行 Web 应用访问

- 什么是无客户端 VPN (clientless VPN) 访问方法？

  当通过 Web 浏览器中的商店 URL 访问未配置任何增强安全限制的内部 Web 应用时，Citrix Secure Private Access™ 使用基于 CVPN 的访问方法。

  > **注意：**
  >
  > 无客户端 VPN 访问方法仅在通过 Web 浏览器中的商店 URL 访问内部应用时使用。只有未配置增强安全限制的应用才会被阻止。

- 我们为什么要弃用此功能？

  无客户端 VPN 方法使用客户端 URL 重写，这具有某些行业范围的技术限制。在某些情况下，当 Web 应用中的某些链接被重写时，可能会导致应用访问失败。这会导致糟糕的最终用户体验。为了向我们的客户提供最佳的应用访问体验，我们正在弃用此功能，并建议改用下面提到的替代方案之一。

- 它将如何影响访问安全私有访问配置应用程序的最终用户？

  如果通过 Web 浏览器从商店 URL 访问任何未配置增强安全限制的 Web 应用程序，则对该应用程序的访问将被阻止。 它不会影响最终用户通过 Citrix Workspace 应用程序、直接访问、远程浏览器隔离服务 (RBI) 或安全访问代理访问应用程序。

- 有哪些替代方案？管理员应该怎么做？

  Citrix Enterprise Browser： 使用 Citrix Workspace 应用程序通过 Citrix Enterprise Browser 访问这些应用程序。此方法通过增强的安全设置（例如限制下载、打印限制、水印、限制剪贴板访问）和浏览器管理提供最佳的最终用户体验。 **直接访问：** 如果您希望使用无客户端方法访问 Web 应用程序，请使用直接访问方法，通过该方法可以直接从任何本机浏览器（如 Chrome）访问应用程序。此方法可用于无法在最终设备上安装 Citrix Workspace 应用程序或用于非托管设备的使用场景。有关更多详细信息，请参阅直接访问企业 Web 应用程序。

- 它是否会影响通过 Citrix Workspace 应用程序或安全访问代理访问的任何现有应用程序？

  不，我们只阻止通过 Web 浏览器中打开的商店 URL 访问的 Web 应用程序。此弃用不会影响通过 Citrix Workspace 应用程序或安装在最终设备上的安全访问客户端访问的任何应用程序。如果通过 Web 浏览器访问配置了增强安全限制的 Web 应用程序，则对这些应用程序的访问将被阻止。

- 还有其他问题吗？

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

请联系Citrix 支持。

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

数据治理

本主题提供有关 Citrix Secure Private Access 服务收集、存储和保留日志的信息。任何未在 定义部分 中定义的术语，均具有 Citrix 最终用户服务协议 中指定的含义。

数据驻留

Citrix Secure Private Access 采用多区域架构，可确保高可用性和冗余。有关详细信息，请参阅 (/zh-cn/citrix-secure-private-access/service/secure-private-access-service-pops.html)。

- 美国东部
- 美国西部
- 巴西南部
- 东南亚
- 欧洲北部
- 欧洲西部
- 澳大利亚东部
- 印度南部

以下是服务配置和运行时日志的不同目标。

- 仅限美国地区的 Splunk 服务，用于系统监控和调试日志。
- Citrix Analytics Service 用于诊断和用户访问日志，有关详细信息，请参阅 (/zh-cn/citrix-analytics/data-governance.html)。
- Citrix Application Delivery Management 服务用于聚合的用户访问日志，有关更多信息，请参阅 Citrix ADM 数据治理。
- Citrix Cloud™ 系统日志服务用于管理员审计日志，请参阅以下链接

有关 Citrix Cloud Services 的一般信息，请参阅 Citrix Cloud Services 客户内容和日志处理 和 地理注意事项。

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

数据收集

Citrix Secure Private Access 使管理员能够通过集中式管理界面配置和管理服务及其关联的连接器设备。该服务处理以下类型的客户数据：

- 适用于 Secure Private Access 服务
  - 客户的私有和 SaaS 应用程序
  - Web 应用程序的 FQDN 和 URL，或两者兼有
  - IP 地址/范围、端口和协议
  - 关联的资源位置
  - Web 和 SaaS 应用程序的单点登录参数
- 应用程序授权的用户标识符
- 自适应访问策略的条件
  - 用户身份
  - 用户/设备的地理位置
  - 用户/设备网络位置，通过 Citrix Cloud 网络位置配置。有关详细信息，请参阅 使用直接工作负载连接优化与商店的连接。
  - 设备类型
- 有关连接器设备平台，请参阅与 Secure Private Access 相关的 适用于云服务的连接器设备。
  - IP 地址或 FQDN
  - 用户、设备和资源位置标识符
  - 内部代理配置

对于服务组件收集的运行时日志，关键信息包括以下内容：

- 用户名
- 用户对象 ID
- 用户电子邮件地址
- 用户 UPN
- 用户组成员身份
- 客户端 IP 地址和端口
- 目标 FQDN/地址和端口

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

- 客户端 User-Agent
- 应用程序名称
- 应用程序 URL 路径
- 应用程序访问时间和持续时间
- 请求字节数
- 响应字节数
- 针对未经批准的应用程序的 Web 过滤决策
- HTTP 事务 ID

有关发送到 Citrix Analytics Service 的数据的完整列表，请参阅 Citrix Analytics Service 数据治理。

数据传输

Citrix Secure Private Access 将日志发送到受传输层安全保护的目标。

数据控制

Citrix Secure Private Access 服务目前不提供客户关闭日志发送或阻止客户内容在全球范围内复制的选项。

数据保留

根据 Citrix Cloud 数据保留策略，客户配置数据将在订阅过期 90 天后从服务中清除。

日志目标维护其服务特定的数据保留策略。

- 有关详细信息，请参阅 数据治理，了解 Analytics 日志的保留策略。
- 有关存储在 Citrix Application Delivery Management 中的事件，请参阅 数据治理。
- Splunk 日志会在 90 天后存档并最终删除。

数据导出

针对不同类型的日志，有不同的数据导出选项。

- 管理员审计日志可从 Citrix Cloud 系统日志控制台访问。
- Secure Private Access Service 诊断日志可以从 Citrix Analytics Service 导出为 CSV 文件。
- Splunk 日志不供客户使用。这些事件也可以从 Splunk 导出为 CSV 文件。

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

定义

- 客户内容 是指上传到客户帐户进行存储的任何数据，或 Citrix 被授予访问权限以执行服务的客户环境中的数据。
- 日志 是指与服务相关的事件记录，包括衡量性能、稳定性、使用情况、安全性和支持的记录。
- 服务 是指为 Citrix Analytics 目的而概述的 Citrix Cloud 服务。

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

产品认证和合规性

Citrix Secure Private Access 是一种零信任网络访问 (ZTNA) 解决方案，可帮助组织安全地将用户连接到应用程序，而无需将网络直接暴露给互联网。Secure Private Access 作为更广泛的 Citrix Cloud 和混合服务组合的一部分提供，并受 Citrix 云服务合规性和审计计划的管辖。

本页面总结了适用于 Secure Private Access 的认证和合规性证明。

认证和审计

- **SOC 2® 第二类：**

  Secure Private Access 包含在 Citrix 的 SOC 2 Type 2 审计计划中。

  SOC 2 Type 2 审计已评估了适用于 Citrix Cloud 服务的安全性、可用性、保密性、处理完整性和隐私控制，其中包括 Secure Private Access。

- **ISO 27001 和 ISO 27701：**

  Secure Private Access 包含在 Citrix 的 ISO 27001（信息安全管理）和 ISO 27701（隐私信息管理）认证服务组合中。

  这些全球公认的认证确认了安全和隐私管理实践已正式建立、记录并持续改进。

- **HIPAA：**

  Secure Private Access 适用于需要 HIPAA 合规性的环境，前提是经过适当配置和签订合同。Citrix 的云合规性文档表明 Secure Private Access 适用于 HIPAA。

- **PCI DSS 4.0：**

  Secure Private Access 包含在 Citrix 针对适用云服务的年度 PCI DSS 评估中。在 PCI 范围环境中部署 Secure Private Access 的客户可能需要实施额外的控制措施以满足 PCI 要求。PCI DSS 合规性遵循 Citrix 和客户之间的共同责任模型。

- **FIPS / 通用标准：**

  Secure Private Access 可以作为 FIPS 合规解决方案的一部分进行部署，当与 FIPS 认证或 FIPS 启用的 NetScaler 平台以及 Citrix Workspace 应用程序使用的 FIPS 认证 Citrix CryptoKit 结合使用时。

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

对于通用标准，Secure Private Access 与通用标准 (NDcPP) 认证的 NetScaler 平台和通用标准认证的 Citrix Workspace 应用程序集成，从而实现与解决方案级别的通用标准要求保持一致的部署。

- **澳大利亚 IRAP（信息安全注册评估员计划）：**

  Secure Private Access 包含在 Citrix 的云服务中，这些服务由经认可的澳大利亚政府评估员进行 IRAP 评估。

  IRAP 提供独立验证，证明 Citrix Cloud 服务符合澳大利亚政府信息安全手册 (ISM) 的安全控制措施。

证书和审计报告

通过 Citrix Trust Center 下载可用的证书和审计报告。

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

index

- 将网关连接器迁移到连接器设备
- 路由表，用于解决由相同相关域引起的冲突
- 通过 Citrix Workspace 应用程序单点登录到 Citrix Secure Access™ 客户端
- ADFS 与 安全私有访问 集成
- Citrix 安全私有访问™
- 将 DNS 查询路由到特定于应用程序的资源位置
- 配置 G Suite
- 配置 Jira
- 配置 O365
- 配置 ERP Cloud
- 配置 ServiceNow
- 配置 Tableau
- 配置 Workday
- 配置 Zoom
- 基于访问模式的策略实施
- 支持服务器到客户端连接 - 预览

将网关连接器迁移到连接器设备

Citrix Gateway Connector™ 已弃用。Citrix 建议其环境中正在使用 Citrix Gateway Connector 的客户开始为所有以前由 Citrix Gateway Connector 支持的安全私有访问用例部署 Connector Appliance。本主题提供了将 Gateway Connector 迁移到 Connector Appliance 的指南。

将 Gateway Connector 迁移到 Connector Appliance 的高级步骤

1. 在同一资源位置安装 Connector Appliance，以及 Gateway Connector。
2. 关闭 Gateway Connector 并测试现有 Web 应用程序的连接性。检查同一资源位置上托管的 Web 应用程序是否可访问。

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

3. 测试完成后，移除 Citrix Gateway Connector。

安装连接器设备

使用以下步骤安装 Connector Appliance。

1. 登录 Citrix Cloud。
2. 从屏幕左上角的菜单中，选择 **资源位置**。
3. 对于要添加 Connector Appliance 的资源位置，单击 Connector Appliance 旁边的加号图标。
4. 选择管理程序，然后单击 **下载映像**。
5. 在您的管理程序上下载并安装 Connector Appliance。
6. 登录 Web UI（管理程序控制台上提供的 IP 地址），并在必要时设置代理。
7. 单击 **注册** 按钮并获取短代码。
8. 粘贴短代码到下载 Connector Appliance 时使用的 Citrix Cloud 用户界面中（步骤 5）。

   连接器设备已注册。

有关详细步骤，请参阅 适用于云服务的 Connector Appliance。

常见问题

- 如何下载 Connector Appliance？

  下载连接器设备。
- 如何安装 Connector Appliance？

  安装连接器设备。
- 如何注册 Connector Appliance？

  注册连接器设备。
- Connector Appliance 的连接要求是什么？

  Connector Appliance 互联网连接要求。
- Connector Appliance 的系统要求是什么？

  Connector Appliance 系统要求。
- Connector Appliance 如何更新？

  连接器设备更新

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

路由表，用于解决由相同相关域引起的冲突

Citrix Secure Private Access™ 服务的应用程序域功能使客户能够做出路由决策，从而允许应用程序的相关域通过连接器设备进行外部或内部路由。

假设客户已在 SaaS 应用程序和内部 Web 应用程序中配置了相同的相关域。 例如，如果 Okta 是 Salesforce（SaaS 应用程序）和 Jira（内部 Web 应用程序）的 SAML IdP，则管理员可能会在两个应用程序的配置中将 `*.okta.com` 配置为相关域。这会导致冲突，最终用户会遇到不一致的行为。在这种情况下，管理员可以根据要求定义规则，通过连接器设备将这些应用程序进行外部或内部路由。

路由表的工作原理

管理员可以根据他们希望如何定义流量流来为应用程序定义以下路由类型。

- **内部 – 绕过代理** - 域流量通过 Citrix Cloud Connector™ 路由，绕过在连接器设备上配置的客户 Web 代理。
- **通过连接器内部** - 应用程序是外部的，但流量必须通过连接器设备流向外部网络。
- **外部** – 流量直接流向互联网。

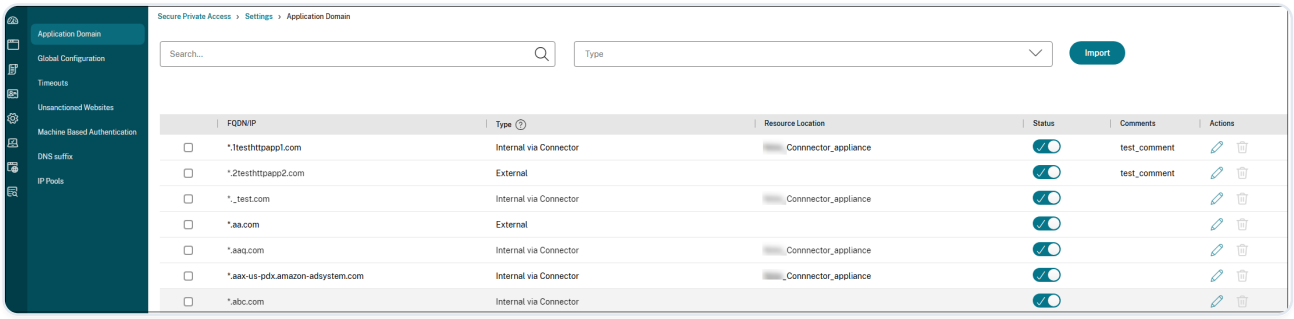
注意：

- 路由条目不影响在应用程序上配置的安全策略。
- 如果管理员不打算使用路由表中的条目，或者如果相应的应用程序未按预期工作，管理员可以简单地禁用该条目而不是删除它。
- 特定客户的所有连接器设备，无论应用程序类型如何，都会获取 SSO 设置。以前，特定应用程序的 SSO 设置与资源位置绑定。

主路由表

Secure Private Access 控制台中的主路由表 (**设置 > 应用程序域**) 是一个只读仪表板，它提供了所有应用程序中已配置域的所有详细信息。这可用于查看任何域的以下信息：

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



主路由表可用于查看任何域的以下信息：

- **FQDN/IP**： 期望配置流量路由类型的 FQDN 或 IP 地址。
- **类型**：应用程序类型。添加应用程序时选择的**内部**、**内部 – 绕过代理**或**外部**。

> **重要提示：**
>
> 如果存在冲突，则会在表中相应行显示一个警报图标。要解决冲突，管理员必须单击三角形图标并从主表中更改应用程序类型。

- **资源位置**：**内部**类型路由的资源位置。如果未分配资源位置，则在相应应用程序的**资源位置**列中会出现一个三角形图标。将鼠标悬停在该图标上时，将显示以下消息。

  缺少资源位置。请确保此 FQDN 已关联资源位置。
- **状态**：**状态**列中的切换开关可用于禁用路由条目的路由，而无需删除应用程序。当切换开关关闭时，路由条目不生效。此外，如果存在精确匹配的 FQDN，管理员可以选择启用或禁用路由。
- **备注**：显示备注（如果有）。
- **操作**：编辑图标用于添加资源位置或更改路由条目类型。删除图标用于删除路由。

迷你路由表

应用程序域表的迷你版本可用于在应用程序配置期间做出路由决策。迷你路由表位于 Citrix Secure Private Access 服务用户界面的**应用程序连接**部分。

向迷你路由表添加路由

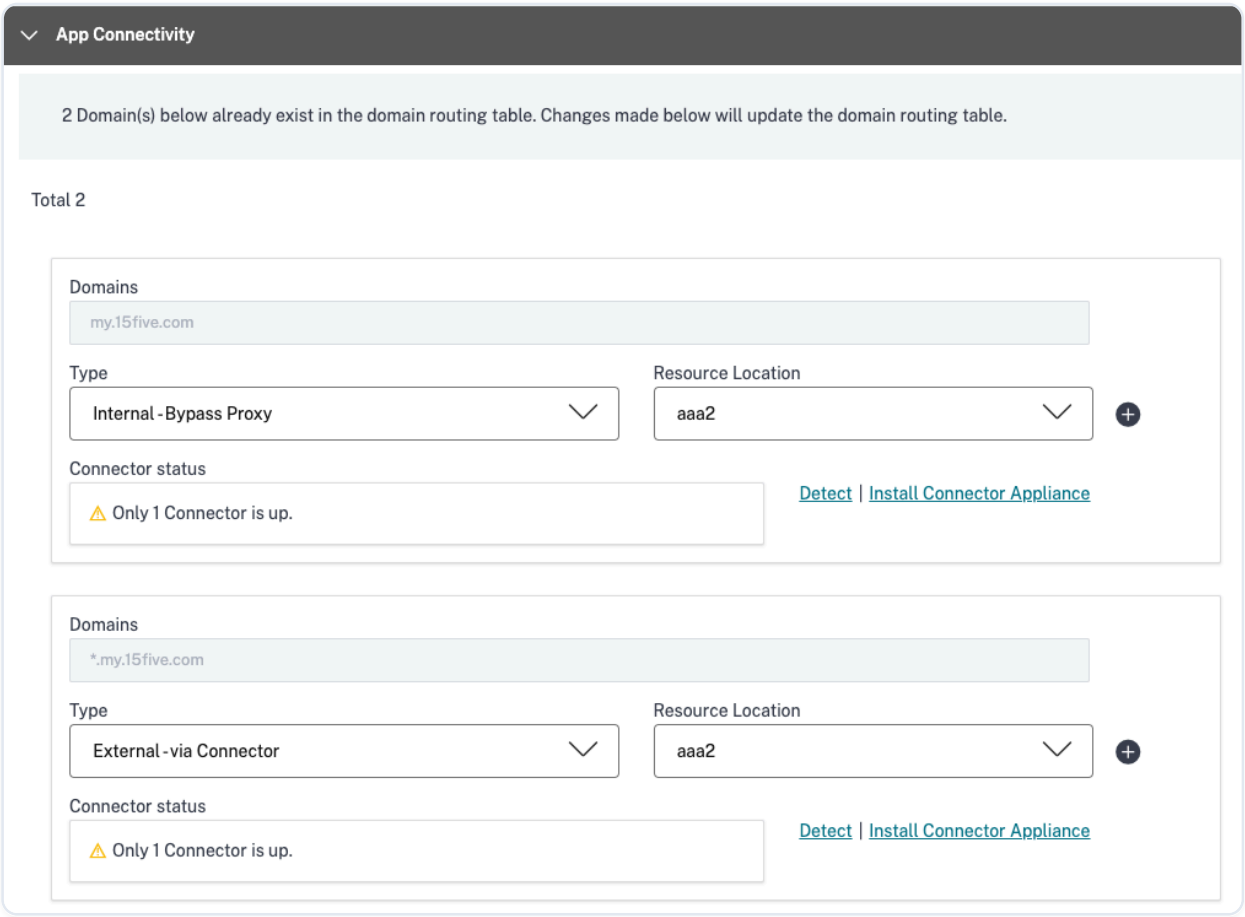
在 Citrix Secure Private Access 服务中添加应用程序的步骤与主题 对软件即服务应用程序的支持 和 对企业 Web 应用程序的支持 中所述的步骤相同，但有以下两项更改：

1. 完成以下步骤：
   - 选择一个模板。
   - 输入应用程序详细信息。

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

- 根据需要选择增强的安全详细信息。
- 根据需要选择单点登录方法。

2. 点击 **应用程序连接**。- 应用程序域表的迷你版本可用于在应用程序配置期间做出路由决策。



- **域：** “域”列显示特定应用程序的一行或多行。第一行显示管理员在添加应用程序详细信息时输入的实际应用程序 URL。其他行都是在添加应用程序详细信息时输入的所有相关域。如果应用程序 URL 和相关域相同，它们将显示在同一行中。

如果选择了 SAML SSO，则会显示 SAML 断言 URL。

- **类型：** 选择以下选项之一。
  - **内部 – 绕过代理** - 域流量通过 Citrix Cloud™ Connector 路由，绕过在 Connector Appliance 上配置的客户 Web 代理。
  - **通过连接器内部** - 应用程序是外部的，但流量必须通过 Connector Appliance 流向外部网络。
  - **外部** – 流量直接流向互联网。
- **资源位置：** 当您为应用程序选择“内部”类型时，此字段会自动填充。如果需要不同的资源位置，请进行更改。

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

- **连接器设备状态：** 当您为应用程序选择“内部”类型时，此字段会与资源位置一起自动填充。

通过 Citrix Workspace 应用程序单点登录到 Citrix Secure Access™ 客户端

Citrix Secure Access 客户端现在支持在已通过 Citrix Workspace 应用程序登录时，对商店 URL 进行单点登录。此 SSO 功能通过避免多次身份验证来增强用户体验。

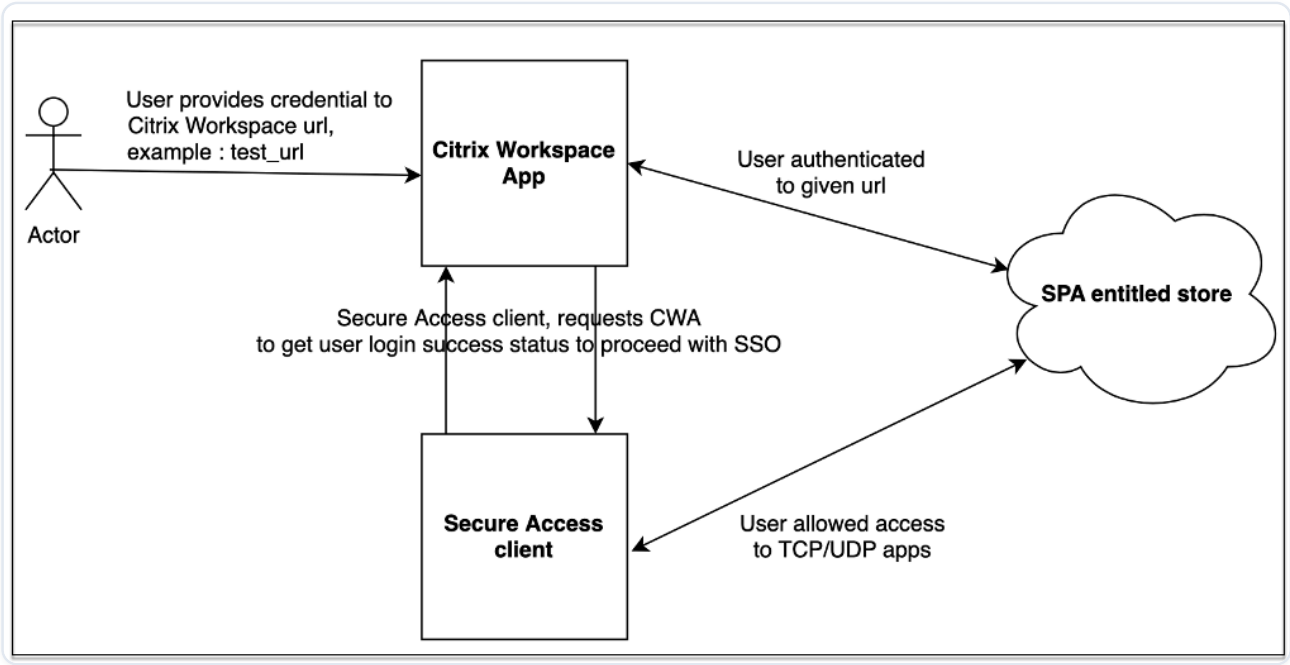
先决条件

- Citrix Workspace 应用程序和 Secure Access 客户端都必须安装在设备上。
- 用户必须首先登录 Citrix Workspace 应用程序，才能在 Citrix Secure Access 客户端中实现自动 SSO。

注意：

单点登录功能仅支持在 Citrix Workspace 应用程序中配置的主存储。如果用户登录到主存储以外的任何其他存储，则不会发生 SSO。用户必须手动登录 Citrix Secure Access 客户端。

下图显示了 Citrix Workspace 应用程序和 Citrix Secure Access 客户端之间的 SSO 流程。



适用于 Windows 的功能要求

- Citrix Workspace 应用程序版本 - **22.10.5.14(2210.5) 或更高版本**
- Citrix Secure Access 版本 - **22.10.1.9 或更高版本**

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

- Citrix 安全访问 Windows 注册表 - **EnableCWASSO**

SSO 功能默认处于禁用状态。要启用此功能，请在最终用户计算机上添加以下注册表。

- 注册表名称 - EnableCWASSO
- 注册表路径 - HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Client
- 注册表类型 - REG_DWORD
- 注册表值 - 1

重要提示：

有时，最终用户设备可能需要重新启动，才能成功建立与 Citrix Workspace 应用程序的单点登录。

ADFS 与 安全私有访问 集成

声明规则对于控制声明通过声明管道的流向是必要的。声明规则还可以在声明规则执行过程中用于自定义声明流。有关声明的更多信息，请参阅 Microsoft 文档。

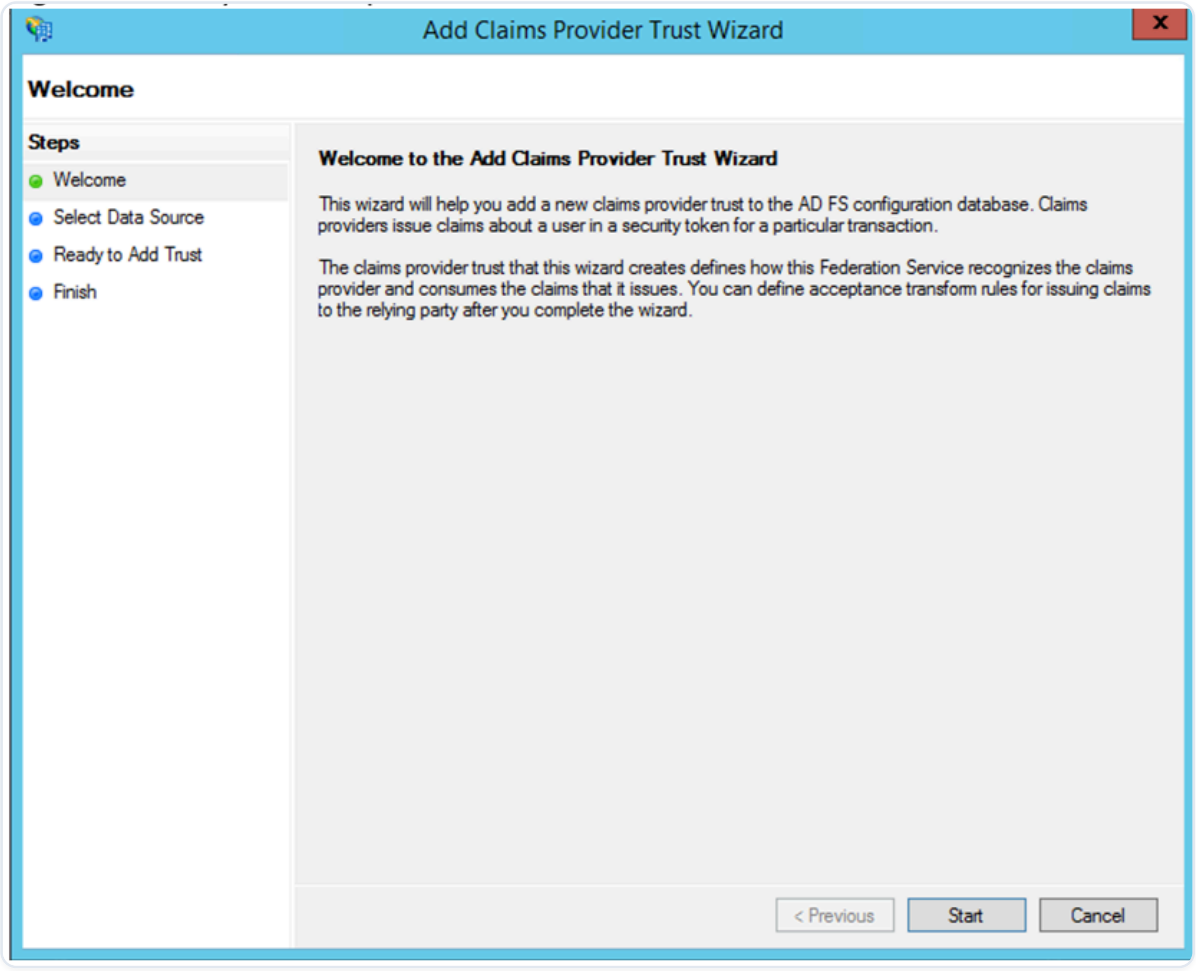
要将 ADFS 设置为接受来自 Citrix Secure Private Access™ 的声明，您必须执行以下步骤：

1. 在 ADFS 中添加声明提供程序信任。
2. 完成 Citrix Secure Private Access 上的应用程序配置。

在 ADFS 中添加声明提供程序信任

1. 打开 ADFS 管理控制台。转到 **ADFS > 信任关系 > 声明提供程序信任**。
    a. 右键单击并选择 **添加声明提供程序信任**。

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

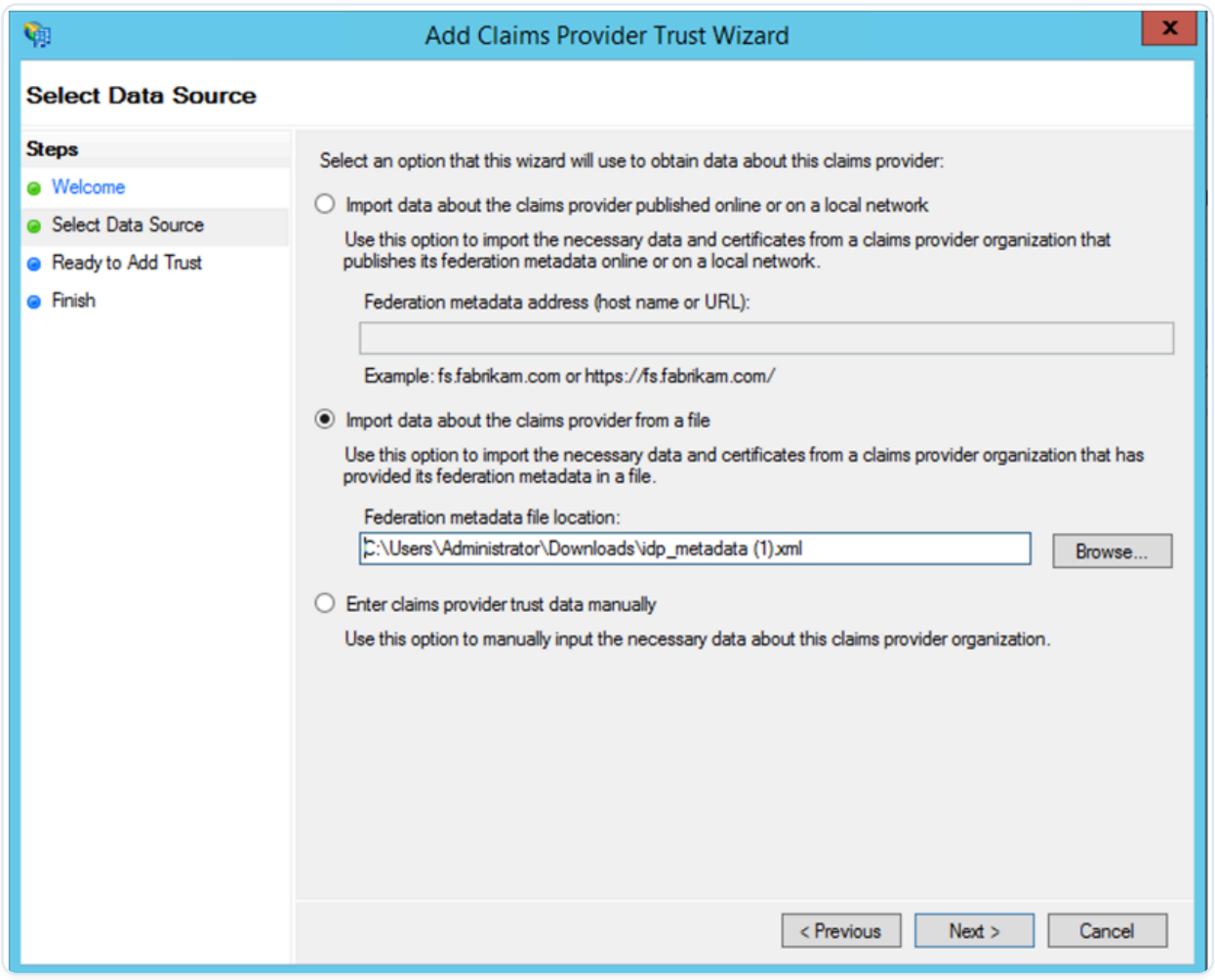


b. 在 Secure Private Access 中添加一个用于联合到 ADFS 的应用程序。有关详细信息，请参阅 Citrix Secure Private Access 上的应用程序配置。

注意：

首先添加应用程序，然后从应用程序的 SSO 配置部分，您可以下载 SAML 元数据文件，然后将元数据文件导入 ADFS。

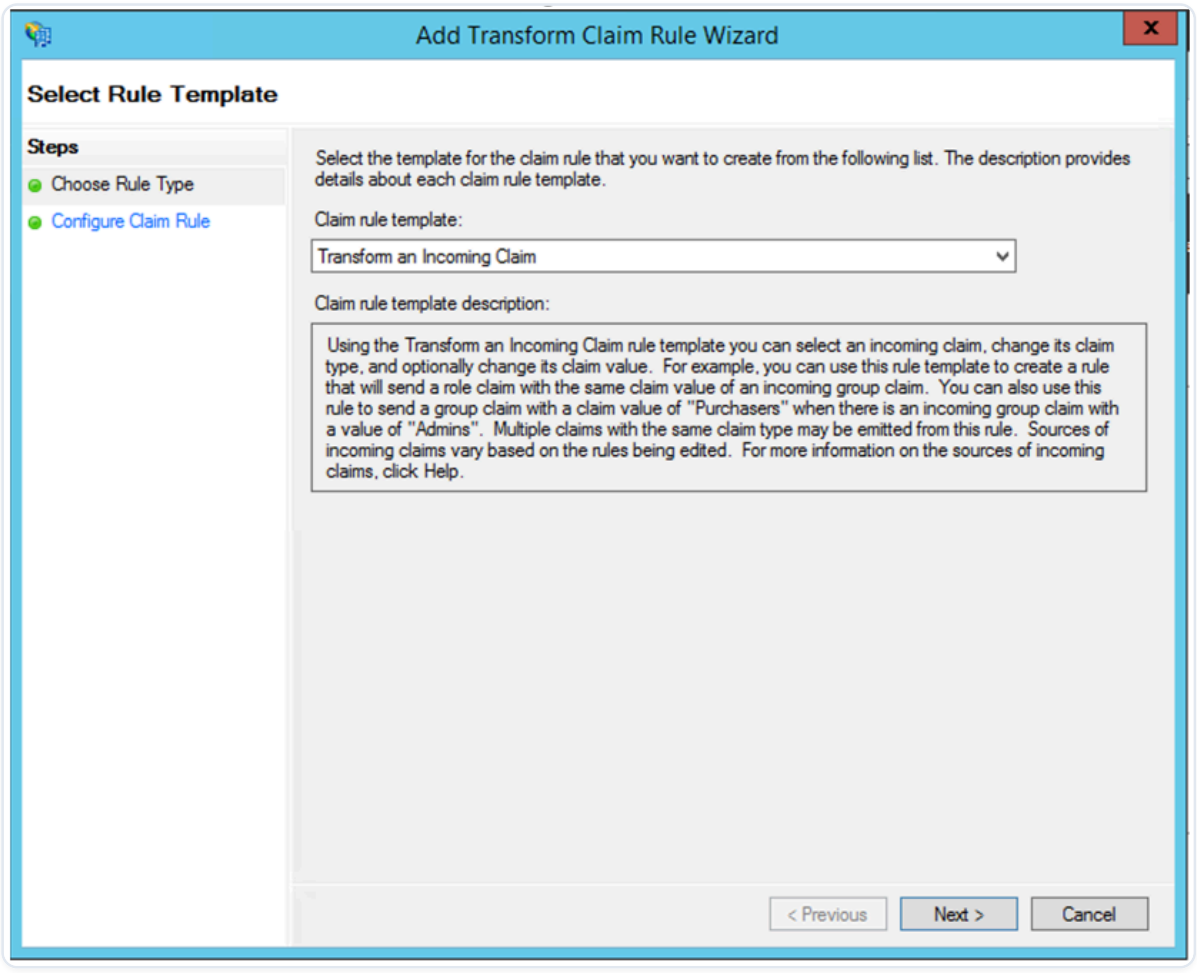
© 1997–2026 Citrix Systems, Inc. All rights reserved.



a. 完成步骤以完成添加声明提供程序信任。完成添加声明提供程序信任后，将出现一个编辑声明规则的窗口。

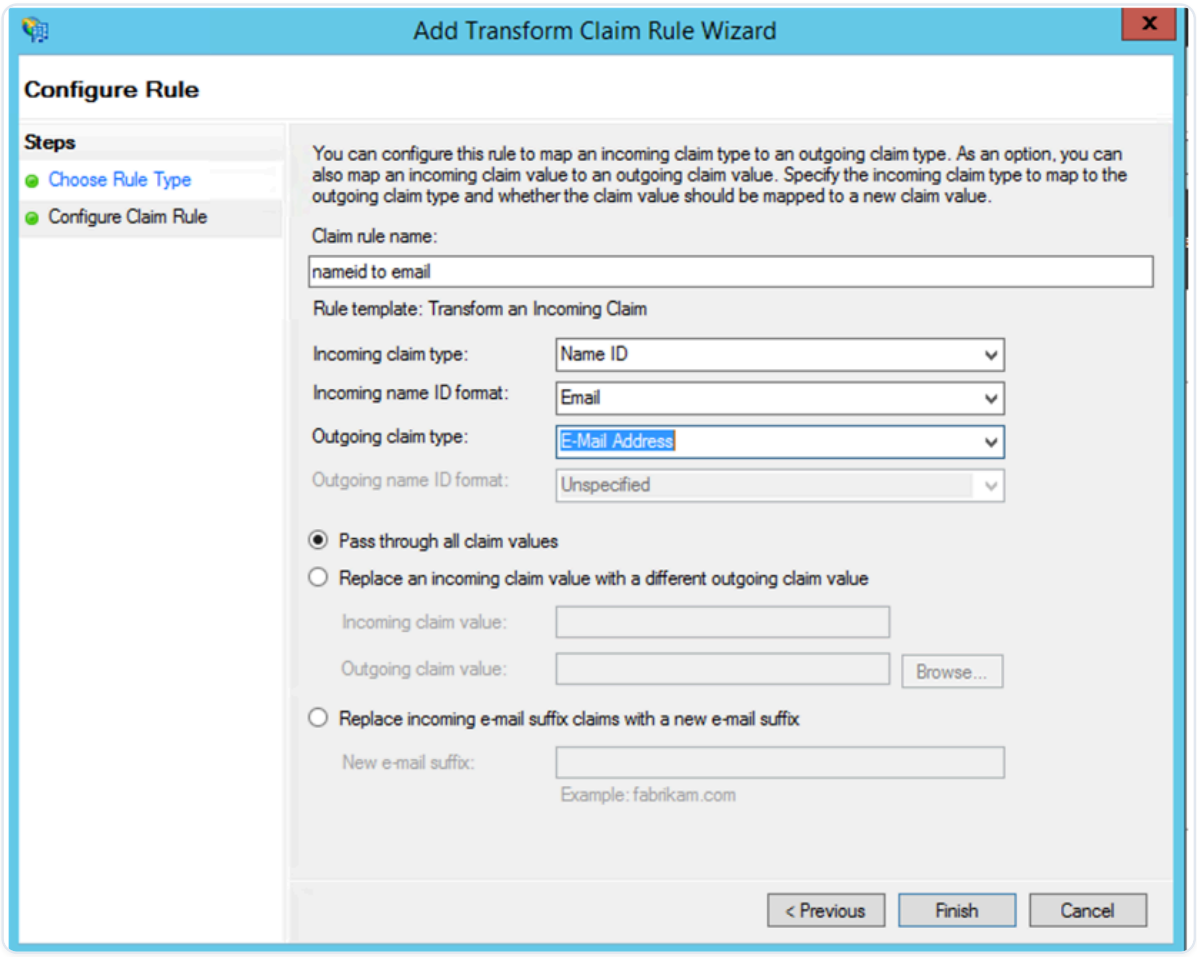
b. 添加一个声明规则，其类型为 **转换传入声明**。

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



c. 完成以下图中所示的设置。如果您的 ADFS 接受其他声明，则使用这些声明并相应地在 Secure Private Access 中配置 SSO。

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

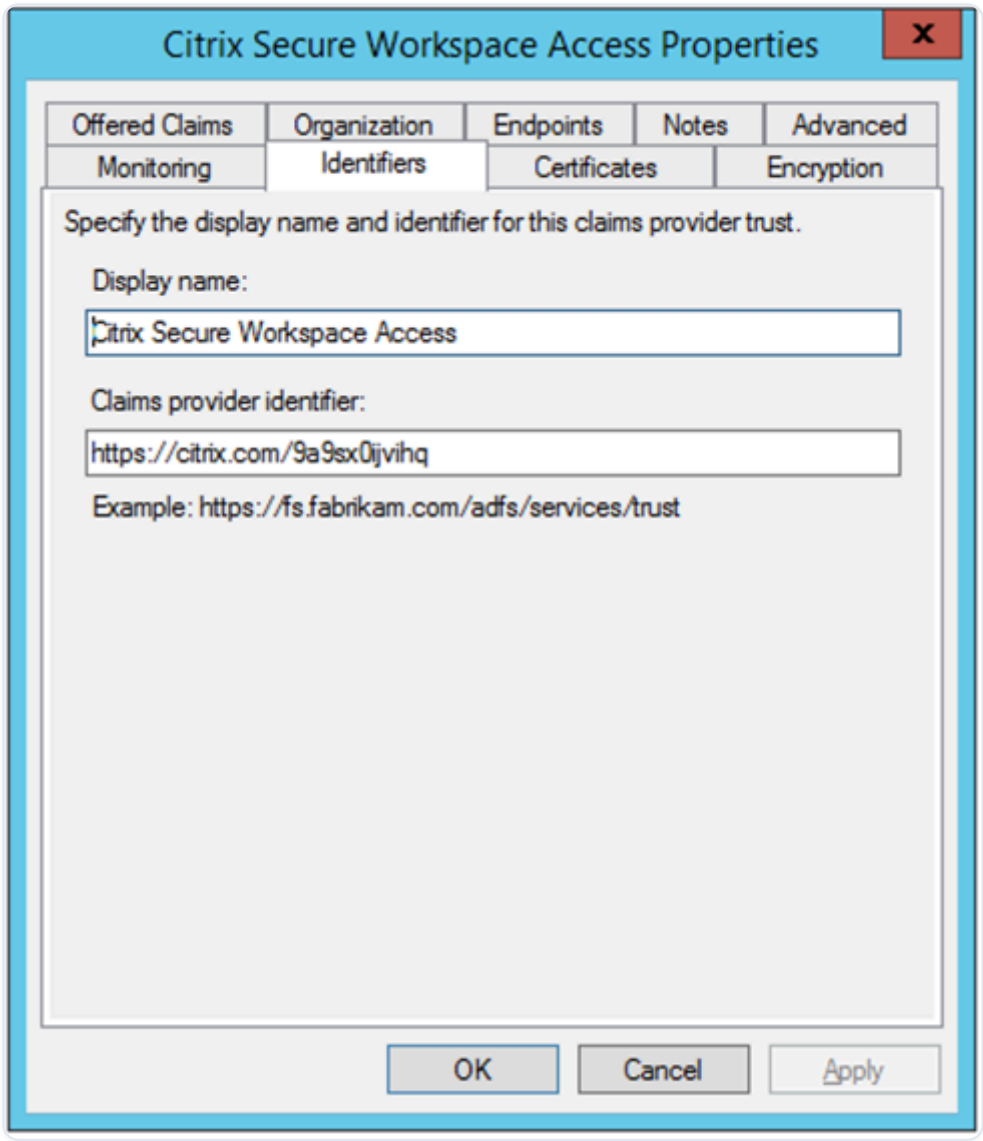


您现在已配置声明提供程序信任，确认 ADFS 现在信任 Citrix Secure Private Access 进行 SAML 身份验证。

声明提供程序信任 ID

记下您添加的声明提供程序信任 ID。在 Citrix Secure Private Access 中配置应用程序时需要此 ID。

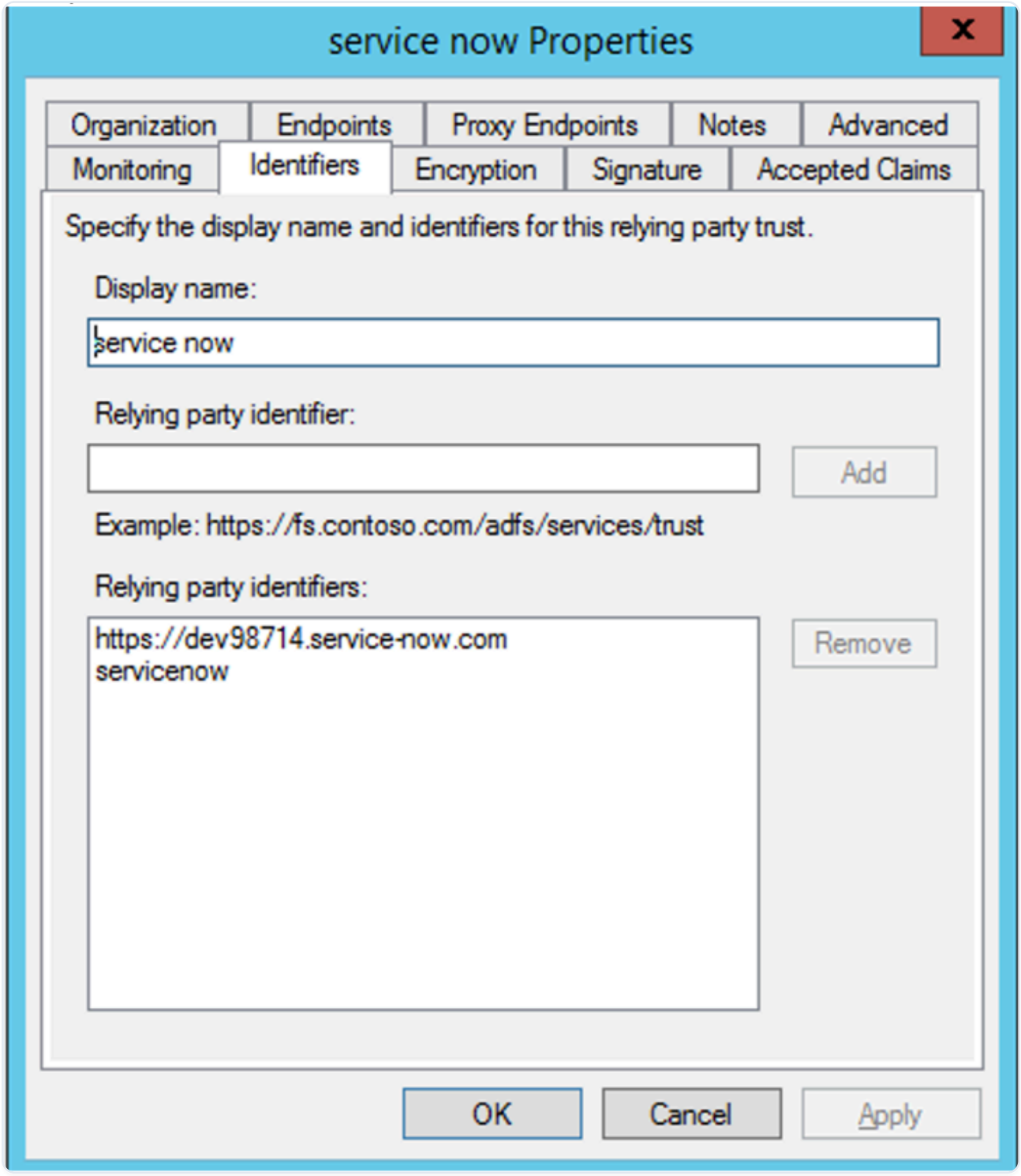
© 1997–2026 Citrix Systems, Inc. All rights reserved.



信赖方标识符

如果您的 SaaS 应用程序已使用 ADFS 进行身份验证，那么您必须已为该应用程序添加了信赖方信任。在 Citrix Secure Private Access 中配置应用程序时需要此 ID。

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



在 IdP 发起的流程中启用中继状态

RelayState 是 SAML 协议的一个参数，用于标识用户登录并定向到信赖方联合服务器后访问的特定资源。如果在 ADFS 中未启用 RelayState，则用户在向需要它的资源提供程序进行身份验证后会看到错误。

对于 ADFS 2.0，您必须安装更新 KB2681584（更新汇总 2）或 KB2790338（更新汇总 3）以提供 RelayState 支持。ADFS 3.0 内置了 RelayState 支持。在这两种情况下，RelayState 仍然需要启用。

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

在 ADFS 服务器上启用 RelayState 参数

1. 打开文件。
   - 对于 ADFS 2.0，在记事本中输入以下文件：%systemroot%\inetpub\adfs\ls\web.config
   - 对于 ADFS 3.0，在记事本中输入以下文件：%systemroot%\ADFS\Microsoft.IdentityServer.Servicehost.exe.config
2. 在 microsoft.identityServer.web 部分中，按如下所示为 useRelyStateForIdpInitiatedSignOn 添加一行，然后保存更改：`<microsoft.identityServer.web> ... <useRelayStateForIdpInitiatedSignOn enabled="true" /> ...</microsoft.identityServer.web>`
   - 对于 ADFS 2.0，运行 `IISReset` 以重新启动 IIS。
3. 对于这两个平台，请重新启动 Active Directory Federation Services `(adfssrv) service.` **注意：** 如果您使用的是 Windows 2016 或 Windows 10，请使用以下 PowerShell 命令启用它。`Set-AdfsProperties -EnableRelayStateForIdpInitiatedSignOn $true`

命令链接 - `<https://docs.microsoft.com/zh-cn/powershell/module/adfs/set-adfsproperties?view=win10-ps>`

Citrix Secure Private Access 上的应用程序配置

您可以配置 IdP 发起的流程或 SP 发起的流程。在 Citrix Secure Private Access 中配置 IdP 或 SP 发起的流程的步骤是相同的，不同之处在于，对于 SP 发起的流程，您必须在 UI 中选择**使用指定 URL 启动应用程序 (SP 发起)**复选框。

IdP 发起的流程

1. 设置 IdP 发起的流程时，请配置以下内容。
   - **应用程序 URL** – 应用程序 URL 使用以下格式。`https://<adfs fqdn>/adfs/ls/idpinitiatedsignon.aspx?LoginToRP=<rp id>&RedirectToIdentityProvider=<idp id>`
   - **ADFS FQDN** – 您的 ADFS 设置的 FQDN。
   - **RP ID** – RP ID 是您可以从信赖方信任中获取的 ID。它与信赖方标识符相同。如果它是 URL，则会进行 URL 编码。
   - **IDP ID** – IdP ID 与声明提供程序信任 ID 相同。如果它是 URL，则会进行 URL 编码。

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

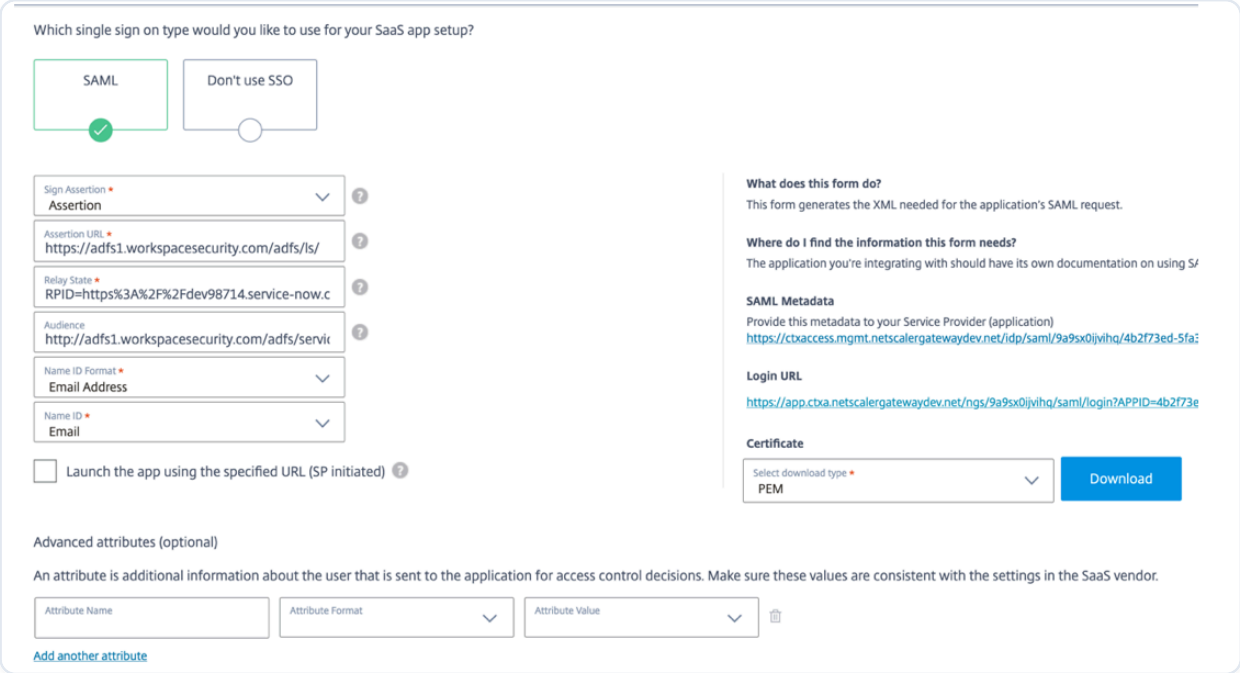
示例： `<https://adfs1.workspacesecurity.com/adfs/ls/idpinitiatedsignon.aspx?LoginToRP=https%3A%2F%2Fdev98714.service-now.com&RedirectToIdentityProvider=https%3A%2F%2Fcitrix.com%2F9a9sx0ijvihq>`

2. SAML SSO 配置。

   以下是 ADFS 服务器的默认值。如果任何值发生更改，请从 ADFS 服务器的元数据中获取正确的值。ADFS 服务器的联合元数据可以从其联合元数据端点下载，该端点可以从 **ADFS > 服务 > 端点**中得知。

   - **断言 URL** – `https://<adfs fqdn>/adfs/ls/`
   - **Relay State** – Relay State 对于 IdP 发起的流程很重要。请按照此链接正确构建它 - `https://docs.microsoft.com/zh-cn/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/jj127245(v=ws.10)`

     示例： RPID=https%3A%2F%2Fdev98714.service-now.com&RelayState=https%3A%2F%2Fdev98714.service-now.com%2F
   - **受众** – `http://<adfsfqdn>/adfs/services/trust`
   - 对于其他 SAML SSO 配置设置，请参阅下图。有关更多详细信息，请参阅支持 SaaS 应用程序。



3. 保存并将应用程序订阅给用户。

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

SP 发起的流程

对于 SP 发起的流程，请按照“**IDP 发起的流程**”部分中的说明配置设置。此外，启用“**使用指定 URL 启动应用程序 (SP 发起)**”复选框。

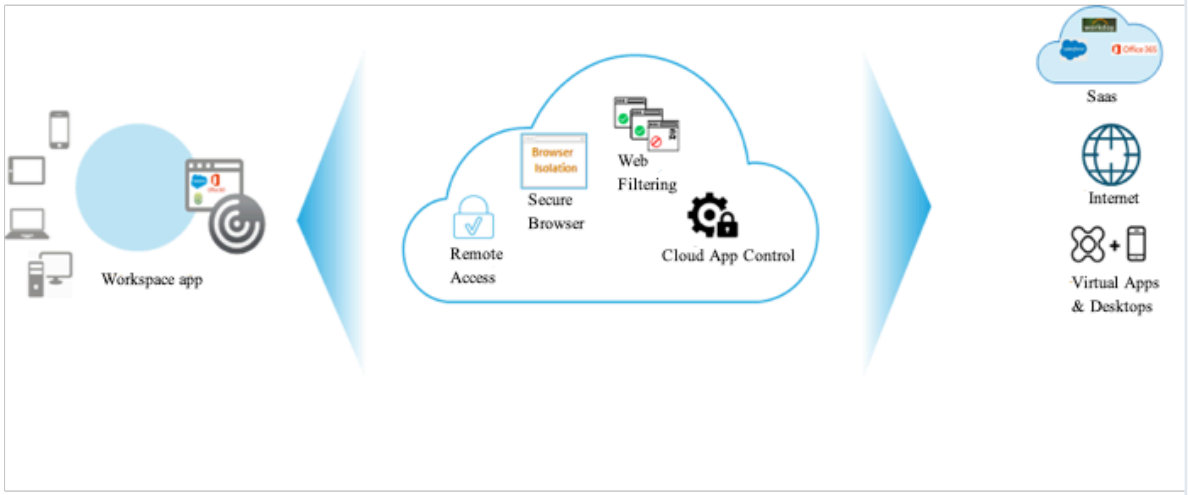
Citrix 安全私有访问™

Citrix Secure Private Access 服务使管理员能够提供一个整合了单点登录、远程访问和内容检查的统一解决方案，以实现端到端访问控制。IT 管理员可以通过简化的单点登录体验来管理对已批准的 SaaS 应用程序的访问。借助 Citrix Secure Private Access 服务，管理员还可以通过过滤对特定网站和网站类别的访问，保护组织的网络和最终用户设备免受恶意软件和数据泄露的侵害。管理员可以强制执行增强的访问安全策略，以安全访问 SaaS 应用程序。一旦通过身份验证，员工就可以从任何设备访问所有关键业务应用程序，无论他们是在办公室、家中还是在旅途中。

管理员可以监控用户活动，例如访问过的恶意、危险或未知网站，消耗的带宽，以及危险的下载和上传行为。通过对访问过的网站和网站类别进行分析，管理员可以采取纠正措施来保护企业网络。同时，该服务为最终用户提供对其所有托管应用程序的无缝且安全的访问。

管理员还可以限制操作，例如受限打印、下载和剪贴板访问（复制-粘贴）。

下图是 Secure Private Access 服务的直观描述。



Citrix Secure Private Access 的主要功能

以下是您可以使用 Citrix Secure Private Access 服务完成的一些主要任务：

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

- **通过单点登录访问发布 SaaS 应用程序** - 一旦用户使用主身份对其商店进行身份验证，后续对 SaaS 和 Web 应用程序的身份验证挑战将通过 Citrix Cloud™ 中的单点登录功能使用 SAML 断言自动完成。

默认情况下，SAML 断言使用与用户 Active Directory 帐户（身份提供商）关联的电子邮件地址，以及与用户 SaaS 或 Web 应用程序帐户（服务提供商）关联的电子邮件地址。

- **为 SaaS 应用程序设置增强的安全策略。（例如，水印、复制-粘贴限制和阻止下载。）** - 为了保护内容，组织在 SaaS 应用程序中实施增强的安全策略。每项策略在使用桌面版 Workspace 应用程序时对 Citrix Enterprise Browser™ 强制执行限制，或在使用 Workspace 应用程序网页版或移动版时对 Secure Browser 强制执行限制。
    - 首选浏览器：禁用本地浏览器使用，并依赖 Citrix Enterprise Browser 引擎（Workspace 应用程序 - 桌面版）或 Secure Browser（Workspace 应用程序 – 移动版和网页版）。
    - 限制剪贴板访问：禁用应用程序和端点剪贴板之间的剪切/复制/粘贴操作。
    - 限制打印：禁用从应用程序浏览器内部进行打印的功能。
    - 限制下载：禁用用户从 SaaS 应用程序内部进行下载的功能。
    - 显示水印：在屏幕上叠加水印，显示用户的用户名和端点 IP 地址。如果用户尝试打印或截屏，水印将按屏幕上显示的方式出现。
- **提供上下文访问** - 尽管授权的 SaaS 应用程序被认为是安全的，但 SaaS 应用程序中的内容实际上可能很危险，构成安全风险。当用户在 SaaS 应用程序中单击超链接时，流量会通过 Web 过滤功能进行路由，该功能为超链接提供风险评估。根据超链接的风险评估和自定义的 URL 类别列表，Web 过滤功能会按如下方式允许、拒绝或重定向用户的超链接请求：
    - 已批准：超链接被认为是安全的，Citrix Enterprise Browser 在 Workspace 应用程序中访问该超链接。
    - 已拒绝：超链接被认为是危险的，访问被拒绝。
    - 已重定向：超链接请求被重定向到远程浏览器隔离服务，用户的互联网浏览活动在该服务中与端点设备、公司网络和 SaaS 应用程序隔离。
- **安全和性能分析** - 用户总是访问本身具有增强安全性的 SaaS 应用程序。Citrix Workspace 应用程序、Secure Private Access 服务和远程浏览器隔离服务向安全分析服务提供有关以下用户和应用程序行为的信息。这些分析会影响用户的总体风险评分：
    - 应用程序启动时间
    - 应用程序结束时间
    - 打印操作

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

- 剪贴板访问
- URL 访问
- 数据上传
- 数据下载

Web 过滤功能会评估 SaaS 应用程序中选择的每个超链接的风险。访问这些站点并监控用户行为变化会增加用户的总体风险评分，因为它表明端点设备已受到威胁并开始感染或加密数据，或者用户和设备正在窃取知识产权。

安全私有访问 REST API

您可以使用 Secure Private Access REST API 直接配置多个应用程序和策略。有关详细信息，请参阅 Citrix Secure Private Access。

将 DNS 查询路由到特定于应用程序的资源位置

管理员可以将特定应用程序的 DNS 查询直接路由到其专用资源位置。这可以实现更准确的 DNS 解析、智能流量管理和更好的用户体验。以前，所有 DNS 查询默认路由到地理位置最近的可用 DNS 服务器，无论应用程序托管在哪里。这要求所有资源位置的 DNS 服务器同步，这并非总是可以实现。

系统要求

思杰安全访问客户端：

- macOS - V25.08.1.1 及更高版本 (Citrix 下载)，V25.08.1 及更高版本 (App Store)。
- Windows - 25.7.1.11 或更高版本。

功能启用

特定于应用程序的 DNS 路由功能默认处于禁用状态。要为您的组织启用此功能，请联系 Citrix 支持。

配置 DNS 查询路由

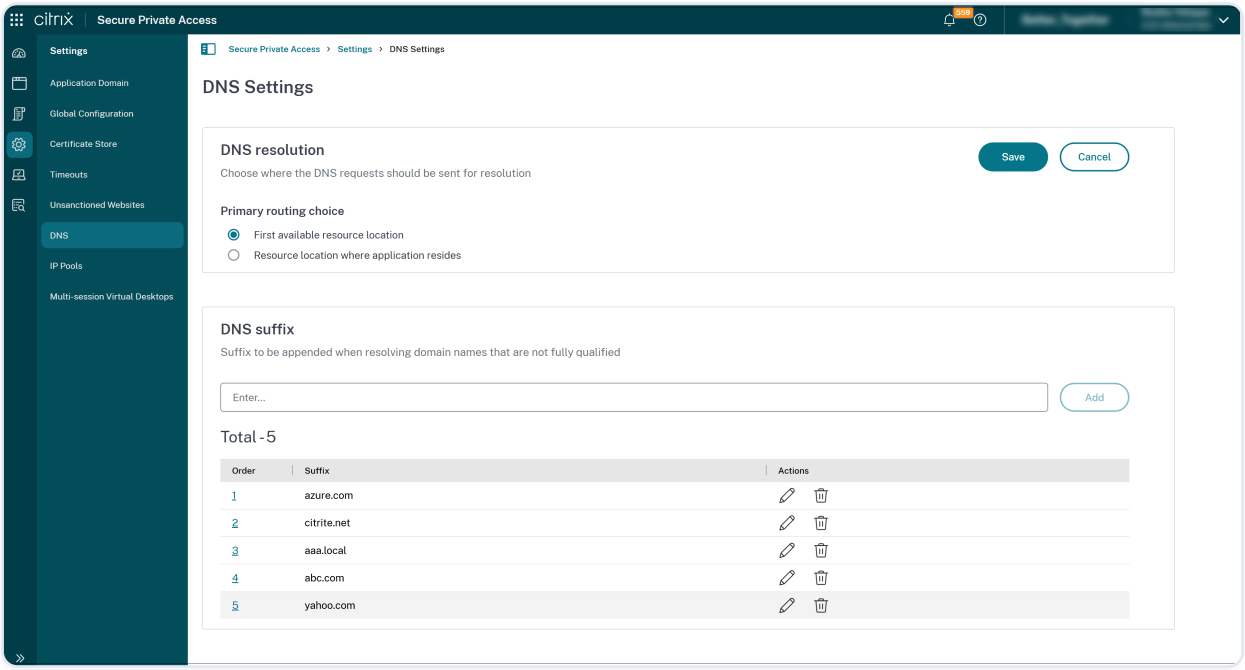
启用该功能后，您可以使用以下两个选项之一路由 DNS 查询：

- **第一个可用资源位置：** 保留所有查询都路由到地理位置最近的资源位置的传统行为。如果您选择使用此选项，请确保所有资源位置中的所有 DNS 服务器都已同步。
- **应用程序所在的资源位置：** 路由到特定于应用程序的资源位置：您可以根据应用程序的主机名将 DNS 查询定向到其专用资源位置。

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

执行以下步骤配置 DNS 路由：

1. 导航到 **设置 > DNS > DNS 解析**。
2. 单击**添加**。



3. 选择以下选项之一:
   - **第一个可用资源位置**
   - **应用程序所在资源位置**
4. 单击 **保存**。

Secure Private Access 支持强大的 DNS 路由回退机制，以确保服务连续性。如果无法为给定 DNS 查询识别特定于应用程序的资源位置，请求将自动回退到指定的备用路由。

注意：

未映射或未发布的域的路由只能在您将主要路由选择设置为 **应用程序所在资源位置** 时进行配置。

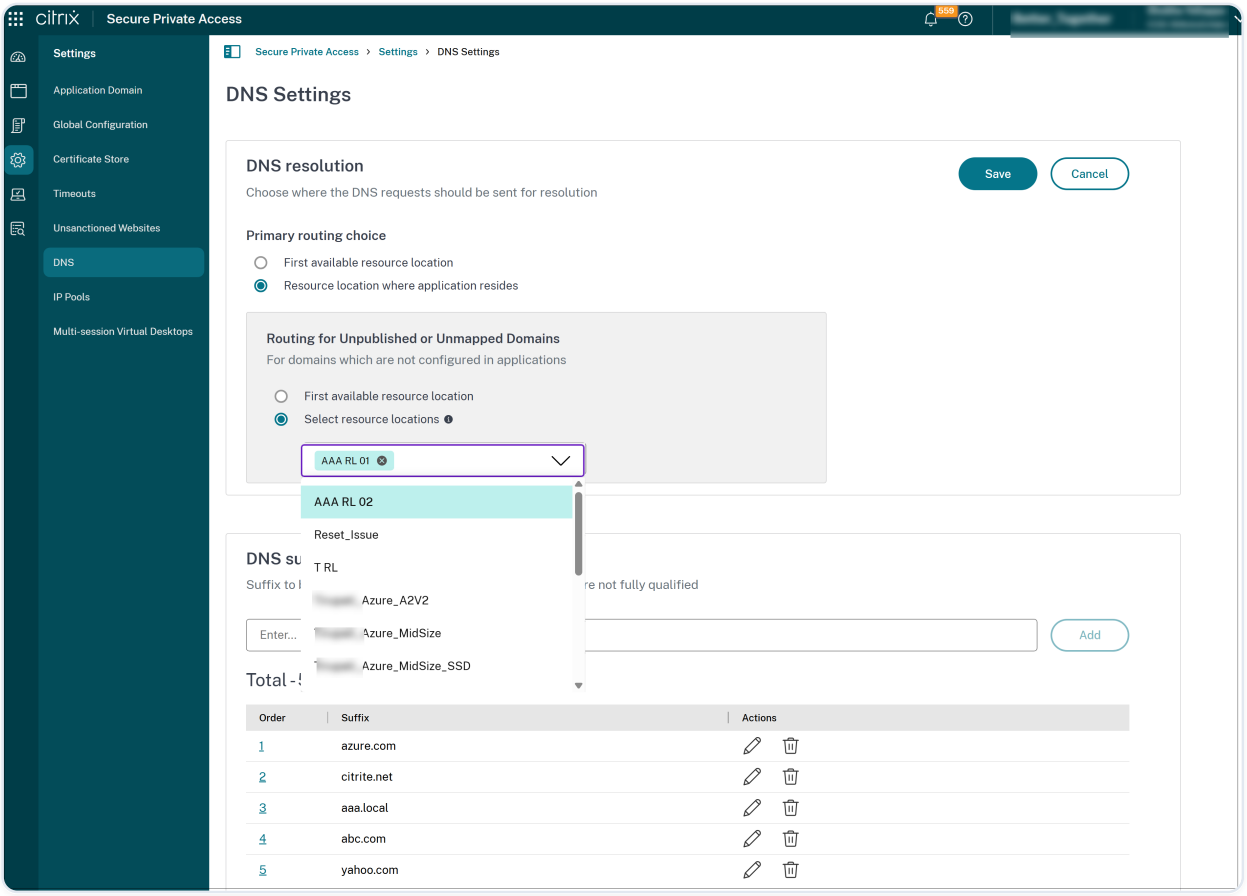
您可以将回退机制配置为以下选项之一:

- **第一个可用资源位置：** 最近的地理资源位置。
- **选择资源位置：** 管理员定义的已配置资源位置列表中的一个位置。

配置 DNS 查询的回退路由:

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

1. 导航到 **设置 > DNS > DNS 解析**。
2. 单击 **添加**。



3. 在“**主要路由选择**”中，选择“**应用程序所在的资源位置**”。
4. 在“**未发布或未映射域的路由**”中，选择以下选项之一：

   - “**第一个可用的资源位置**”
   - “**选择资源位置**”

   如果您选择“**选择资源位置**”选项，然后从列表中选择所需的资源位置。您可以选择多个资源位置。

5. 单击“**保存**”。

配置 G Suite

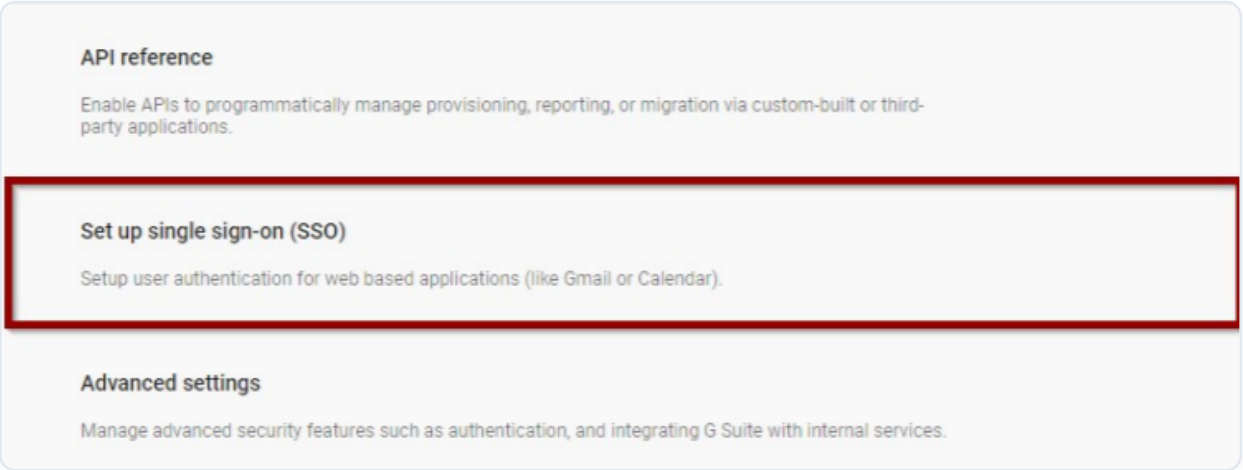
要通过 SAML 配置 G Suite 以实现单点登录，请执行以下操作：

1. 以管理员用户身份登录 G Suite。

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

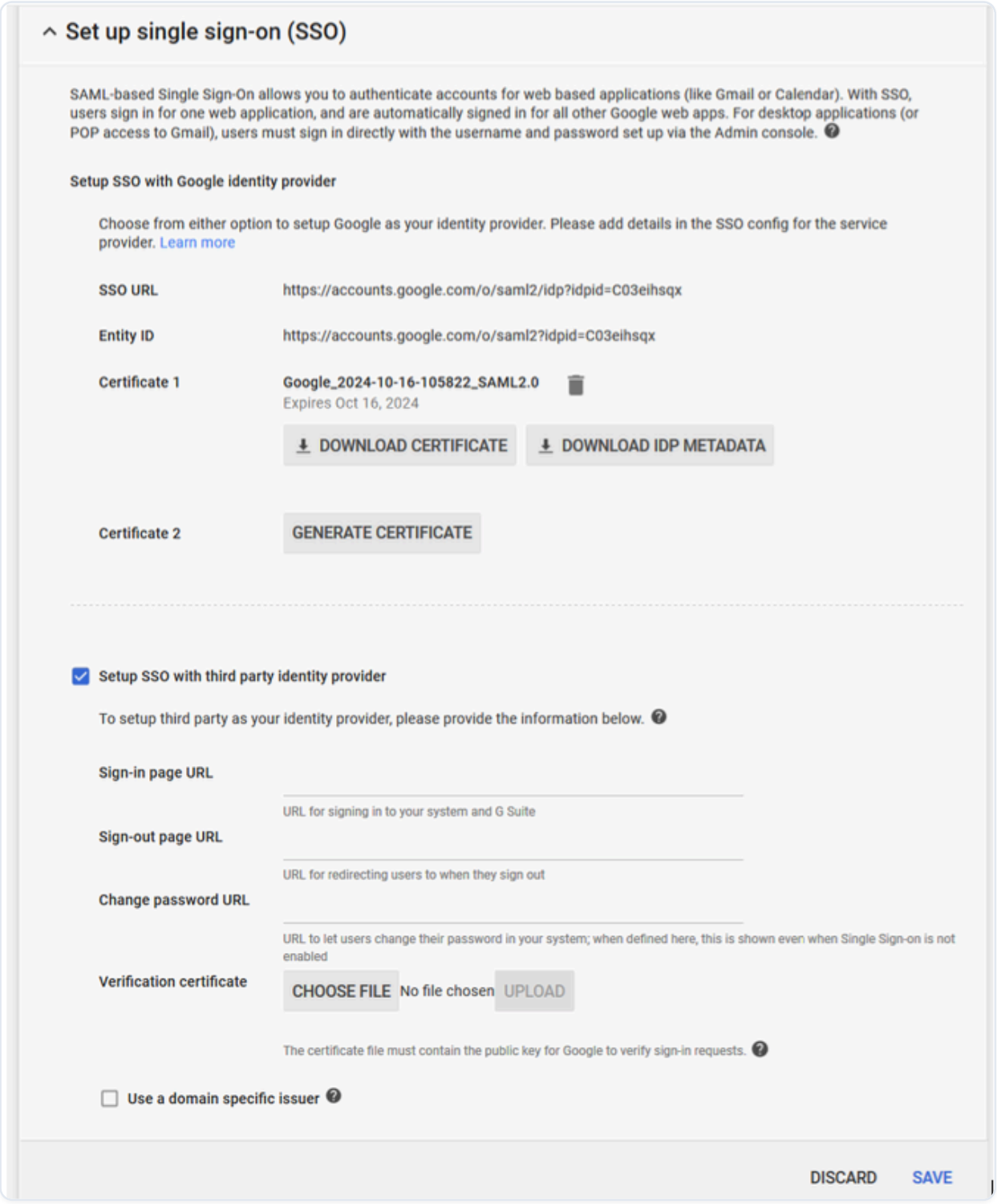


2. 单击“**安全**”。



3. 在“**安全**”页面中，单击“**设置单点登录 (SSO)**”。

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



4. 在“**设置单点登录 (SSO)**”页面中，选择“**使用第三方身份提供程序设置 SSO**”并输入详细信息。

   - **登录页面 URL** - 您可以从 Citrix Cloud 向导（**Citrix Gateway Service > 添加 Web/SaaS 应用程序 > 单点登录 > 登录 URL**）复制 SAML SSO 登录 URL。
   - **验证证书** - 您可以从 Citrix Cloud 向导（**Citrix Gateway Service > 添加 Web/SaaS 应用程序 > 单点登录 > 证书**）下载证书。
   - **使用特定于域的颁发者** - 选中此复选框。

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

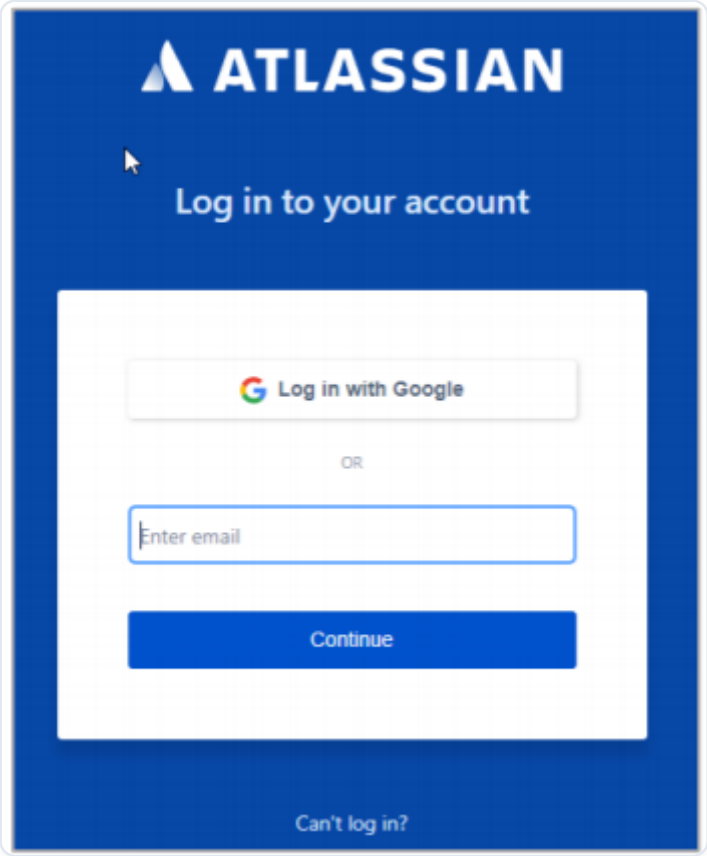
配置 Jira

以下部分提供了有关配置 Jira 的更多信息。

Citrix Gateway SaaS 应用程序

为 SSO 配置 Jira 使管理员能够使用 NetScaler 管理其用户。用户可以使用其企业凭据安全登录 Jira。 要通过 SAML 为 SSO 配置 Jira，请执行以下操作：

1. 在浏览器中，键入您组织的 Atlassian 云 URL，然后按 Enter 键。
2. 登录您的 Atlassian 帐户。

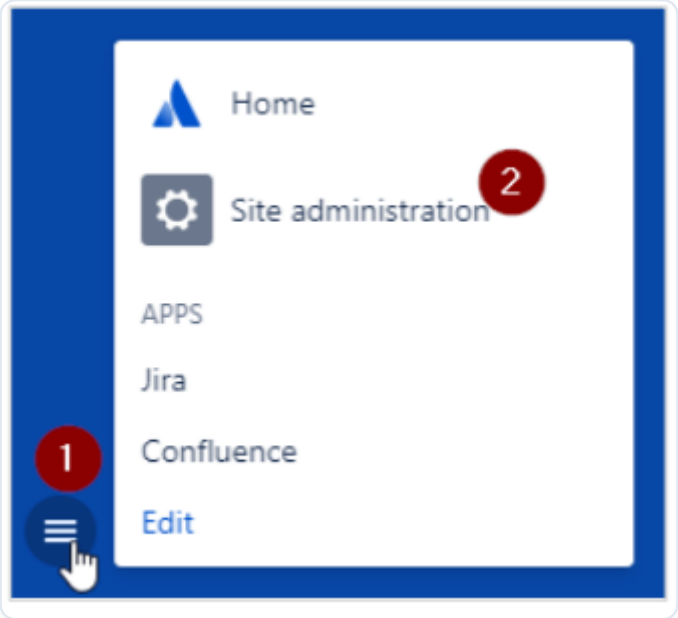


3. 在“主页”的左下角，单击省略号图标。

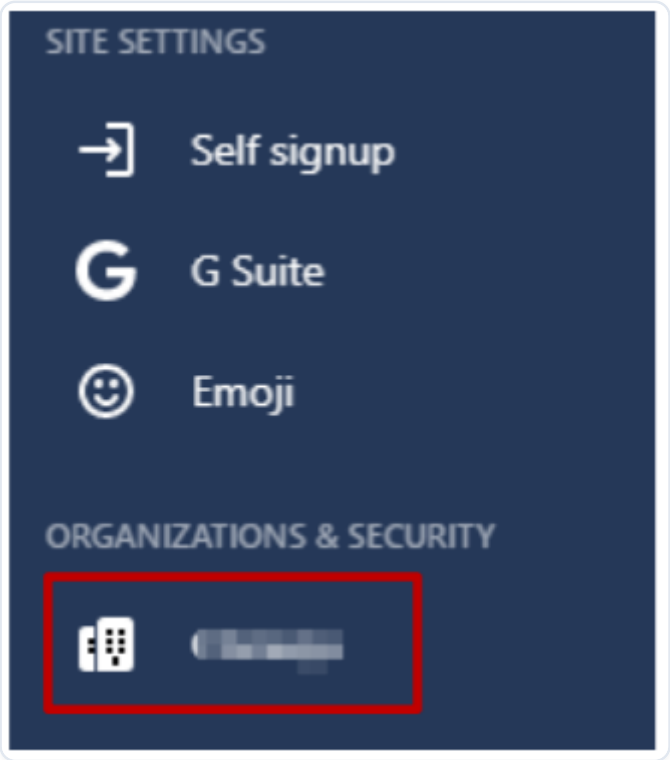


© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. 单击 **站点管理**。

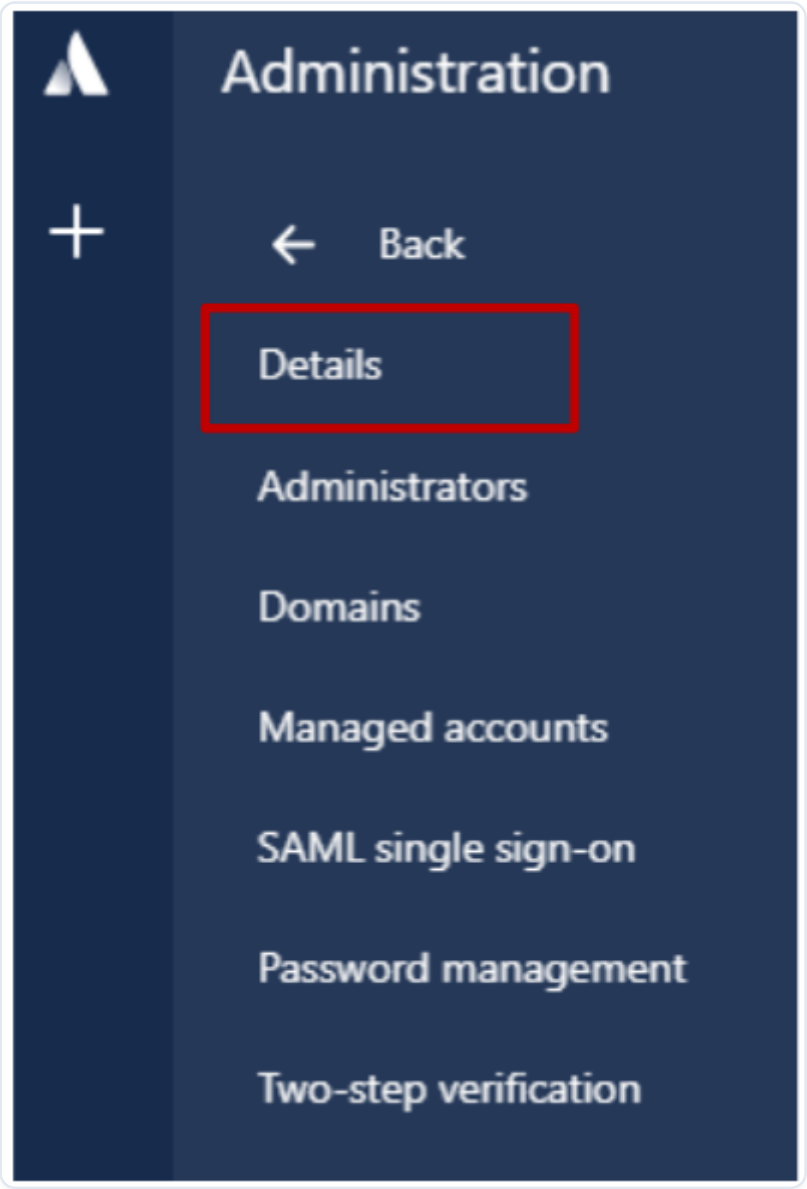


5. 在“管理”页面上的“组织与安全”部分中，单击要为其配置 SAML 身份验证的组织名称。



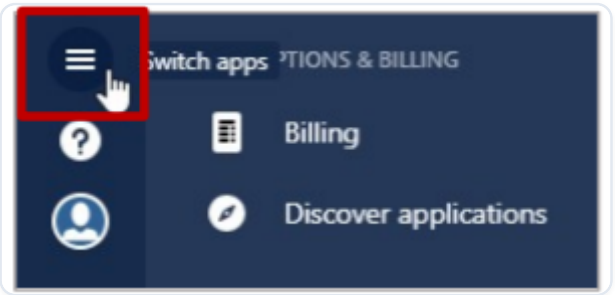
6. 单击 **详细信息** 并验证域。

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



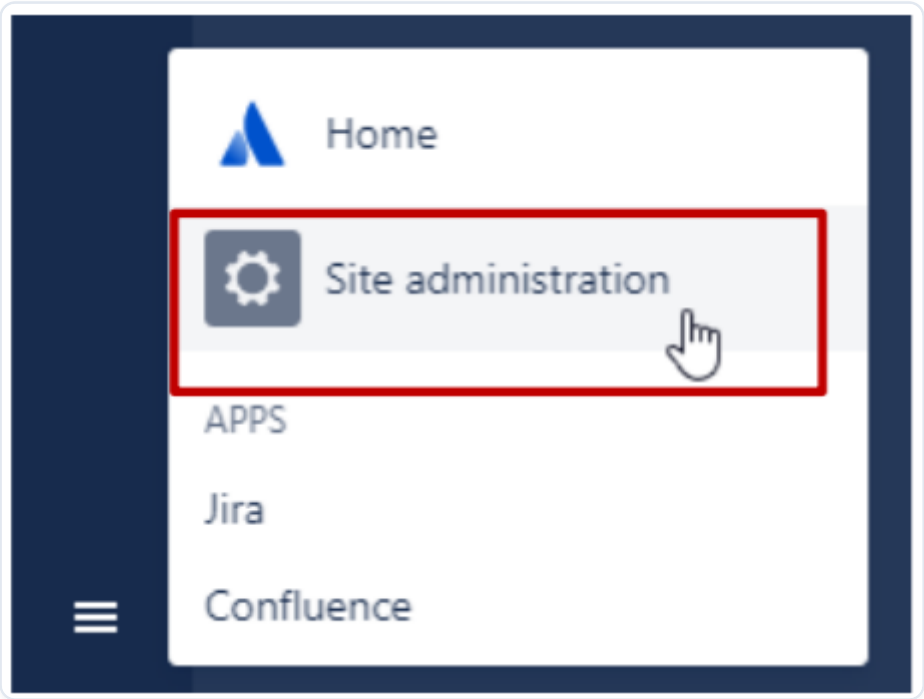
要验证域，请执行以下操作：

a. 单击左下角的“**切换应用程序**”图标。



a. 单击“**站点管理**”。

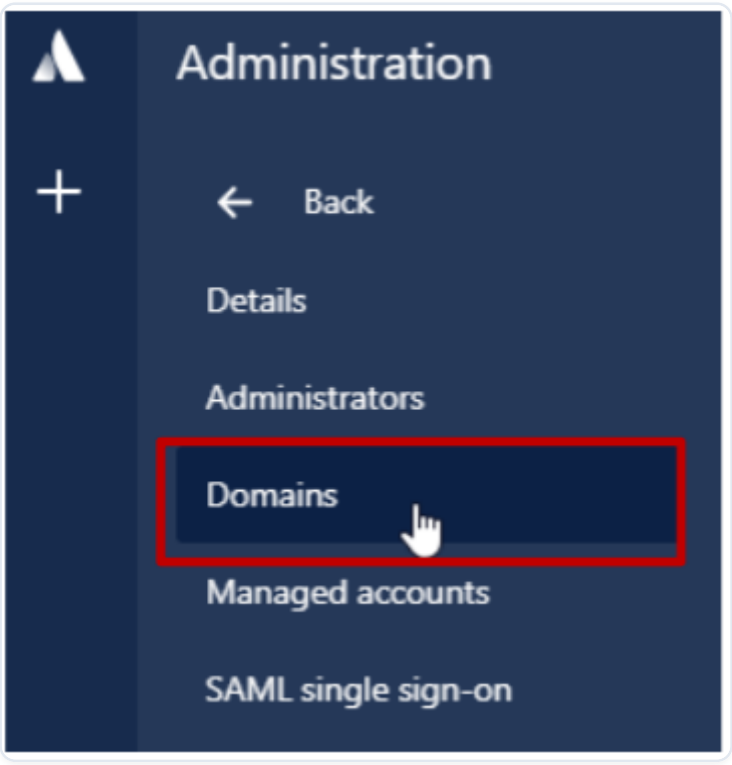
© 1997–2026 Citrix Systems, Inc. All rights reserved.



a. 单击组织名称。

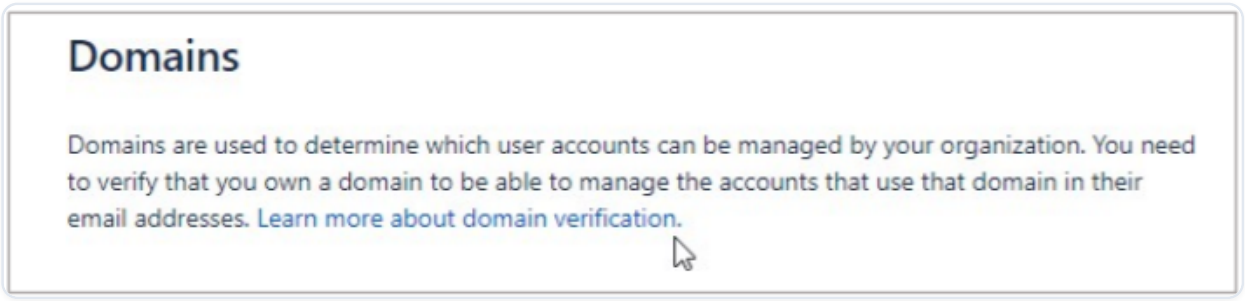


a. 单击“**域**”。

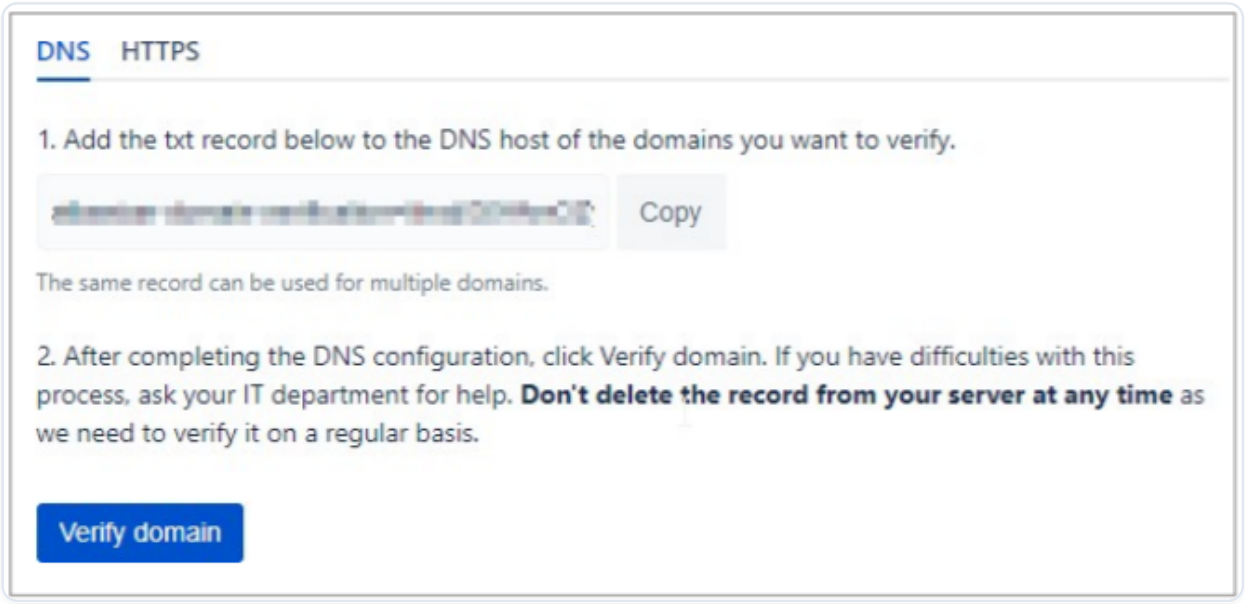


© 1997–2026 Citrix Systems, Inc. All rights reserved.

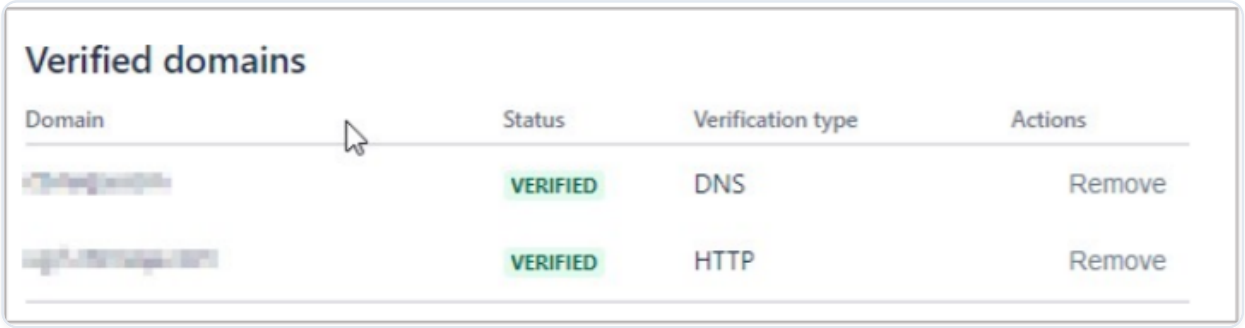
a. 您可以使用 DNS 或 HTTPS 验证域。有关验证域的步骤的更多信息，请在右侧窗格的“域”部分下，单击“了解有关域验证的更多信息”链接。



a. 完成这些步骤后，单击“**验证域**”。

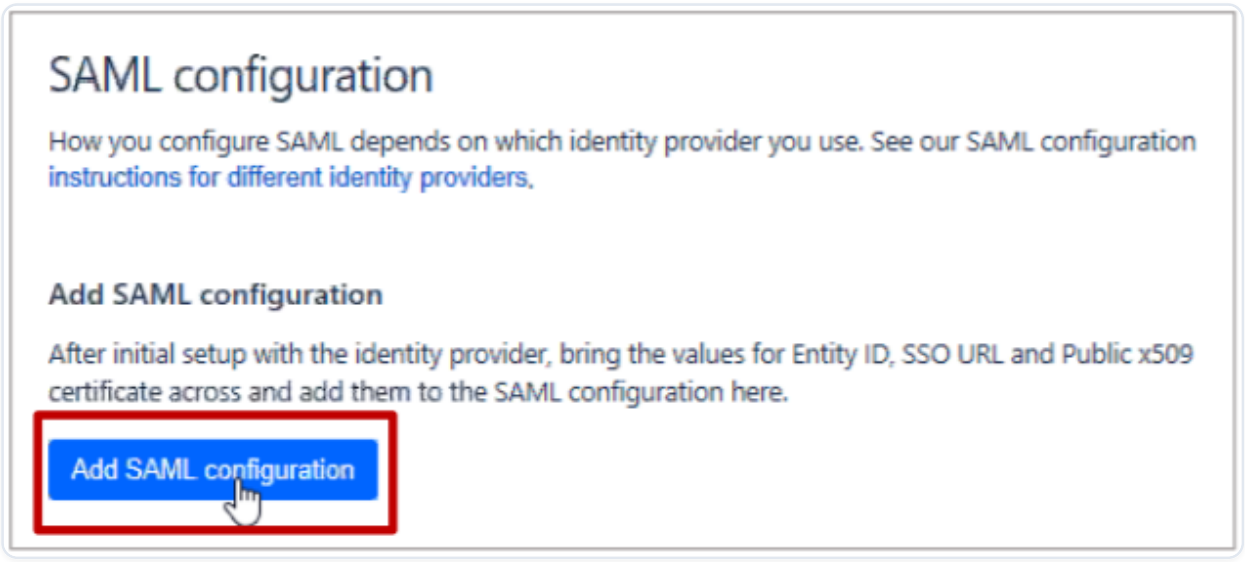


a. “已验证域”部分中的“状态”列显示“**已验证**”。



7. 单击“**SAML 单一登录**”。
8. 在右侧窗格的“SAML 配置”下，单击“**添加 SAML 配置**”。

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

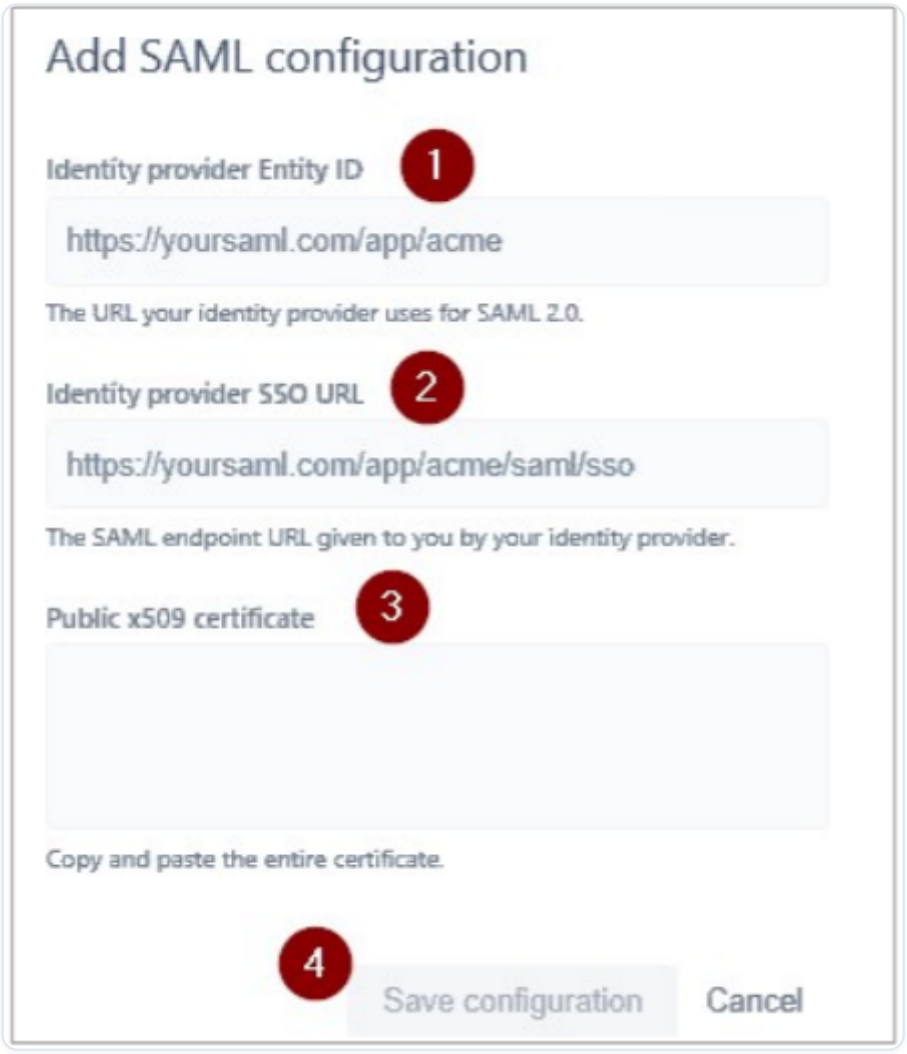


9. 在“**添加 SAML 配置**”区域中，指定以下信息：

   - 身份提供程序实体 ID - 键入唯一的颁发者 ID。例如：`yourcompany_NS_Jira`
   - 身份提供程序 SSO URL - 输入 IdP URL。

     注意：您可以从 Citrix Cloud 向导（**Citrix Gateway Service > 添加 Web/SaaS 应用程序 > 单一登录 > 登录 URL**）复制 URL。

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



- 公共 x509 证书 – 复制并粘贴 SAML IdP 签名证书。

  a. 从 Citrix Cloud 向导（**Citrix Gateway Service > 添加 Web/SaaS 应用程序 > 单一登录 > 证书**）下载证书。

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

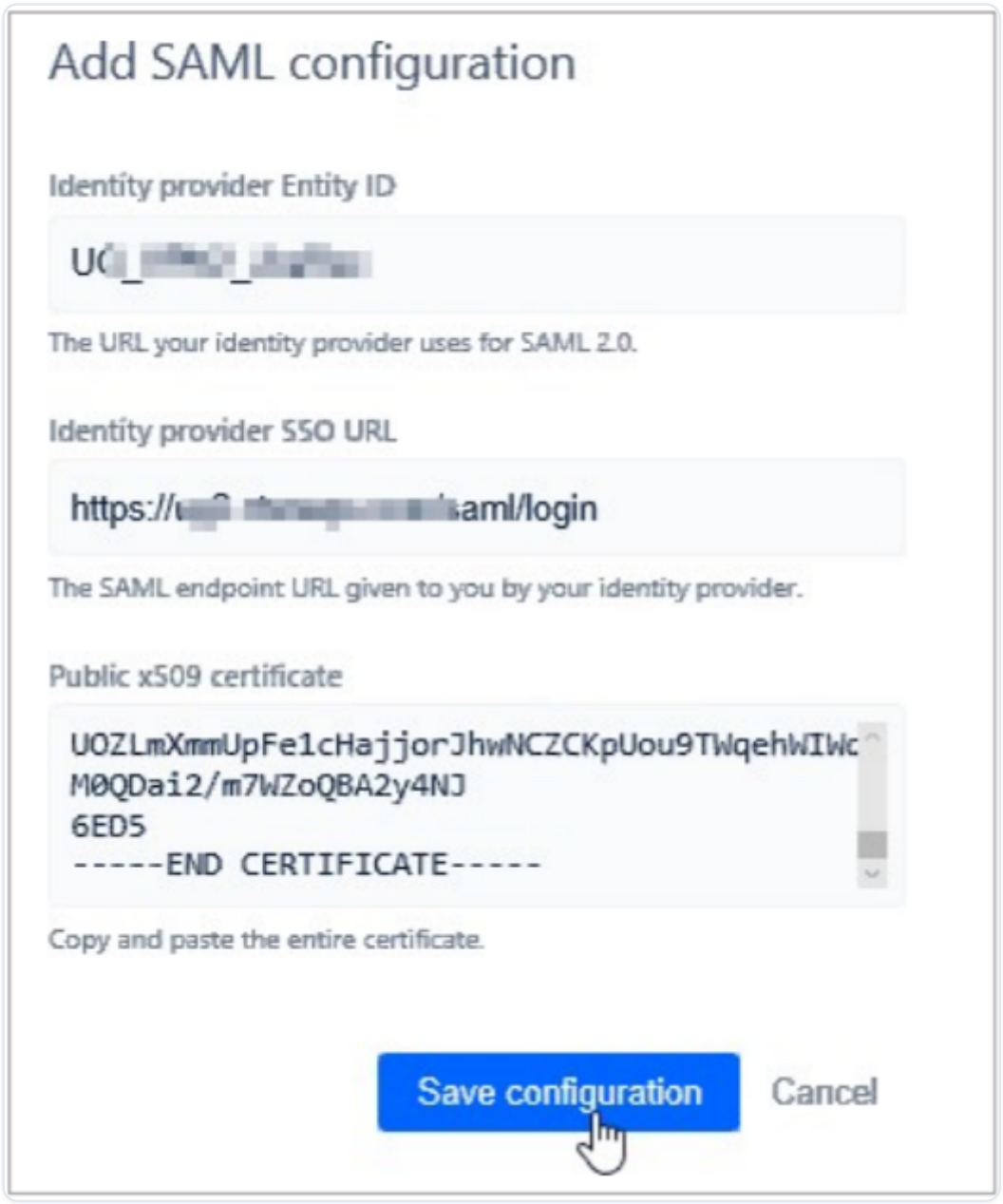


b. 复制 -----BEGIN CERTIFICATE----- 和 -----END CERTIFICATE----- 之间的文本

c. 将文本粘贴到文本编辑器中，并以适当的格式（例如 `your company name`.pem）保存文件。

10. 单击“**保存配置**”。

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



配置 O365

以下部分提供了有关配置 O365 的更多信息。

先决条件

要在 Citrix Workspace 应用程序中配置 O365 应用程序，请务必完成以下操作：

- **如果您的 Microsoft Entra ID 中有一个未与其他服务联合的主域**，则可以使用该域联合到 Citrix Secure Private Access。确保此域（无论是其父域还是子域）尚未联合，并且其父域尚未添加到 Microsoft Entra ID 中。

  例如，如果您的用户使用 `user1@demo.citrix.com` 登录，则 demo.citrix.com 是主域，citrix.com 是父域，us.demo.citrix.com 是子域。

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

- **如果您无法联合主域**，请向 Microsoft Entra ID 添加一个新域并将其联合到 Citrix Secure Private Access。创建域并完成验证。有关详细信息，请参阅 `<https://docs.microsoft.com/zh-cn/azure/active-directory/fundamentals/add-custom-domain>`。

  或者

  您可以将子域添加到 Microsoft Entra ID，该子域可用于联合到 Citrix Secure Private Access 以实现 SSO。为此，您必须添加子域并将其提升为根域。有关详细信息，请参阅 `<https://docs.microsoft.com/zh-cn/azure/active-directory/enterprise-users/domains-verify-custom-subdomain>`。

  注意： 您可能需要使用 Microsoft Entra ID Graph Explorer 而不是 Microsoft Graph Explorer 来执行 POST 请求，以将子域更改为根域。

  有关为何需要联合域的详细信息，请参阅 域联合的工作原理。
- **确认您添加的新域或子域在 Microsoft Entra ID 中处于“已验证”状态。**
- **在您的 SAML 身份提供商和 Microsoft Entra ID 之间建立信任**。要建立信任，您必须拥有一个在 Microsoft Entra ID 中已验证的域。当在 Microsoft Entra ID 中使用域配置联合时，Microsoft Entra ID 会信任 SAML 提供商进行用户对 Microsoft Entra ID 的身份验证，即使该用户来自与联合域不同的域。在 SP 启动的流程中，当 Microsoft Entra ID 必须识别要用于身份验证的 IdP（将用户加速到联合 IdP）时，它是通过传递给 URL `<https://docs.microsoft.com/zh-cn/azure/active-directory/manage-apps/configure-authentication-for-federated-users-portal>` 的 `whr query param` 或 `domain_hint` 来识别的。

  为新域添加联合不会影响您现有设置中的联合。如果您已将 ADFS 联合到某个域，则不会受到影响，因为您正在联合一个不同的域，该域既不是已联合域的子域也不是父域。

  SSO 可以有以下两种流程：

  IDP 发起的流程： 通常用于您想要登录 Microsoft Entra ID 门户时。Citrix Secure Private Access 服务将 SAML 断言发布到 Microsoft Entra ID。Microsoft Entra ID 根据我们之前进行的联合设置对其进行验证。如果验证通过，它会提取 SAML 的 `nameid` 属性。`nameid` 属性必须与 Microsoft Entra ID 中存在的用户的 `immutableId` 匹配。

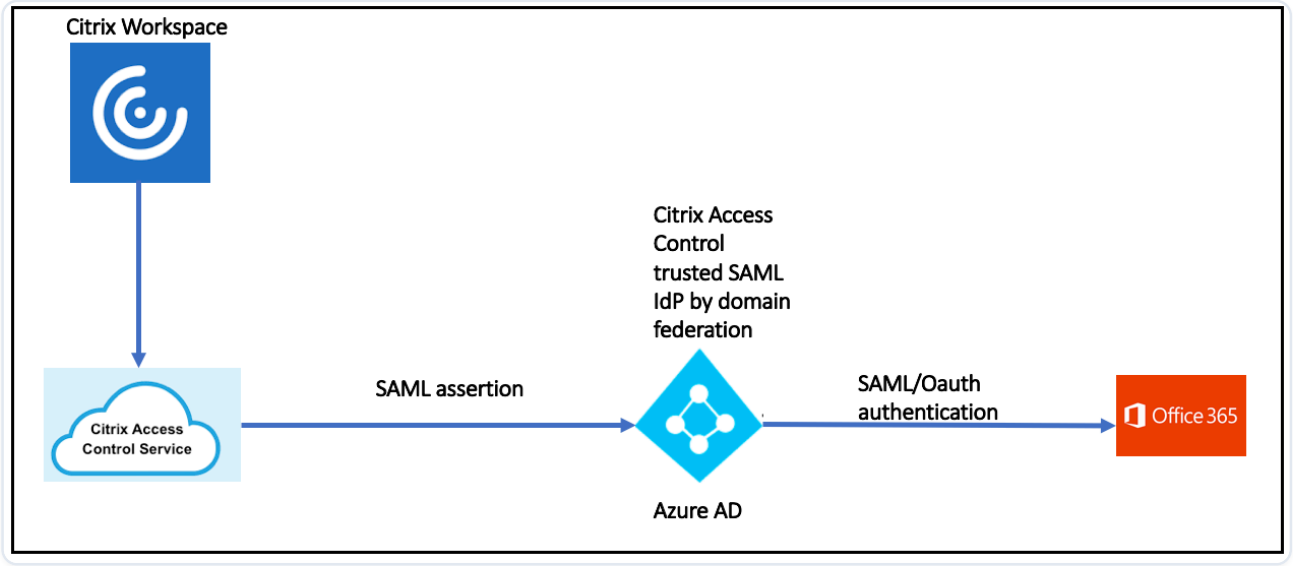
  SP 发起的流程： 通常用于您想要直接访问应用程序而不是 Microsoft Entra ID 门户时。在此流程中，Citrix Secure Private Access 服务加载应用程序设置中配置的 URL。URL 会发送到 Microsoft Entra ID，并且由于 URL 包含联合域的一些指示，用户会被重定向到 Citrix Secure Private Access 服务，并带有一个 SAML 请求和中继状态。Citrix Secure Private Access 服务将 SAML 断言发布到 Microsoft Entra ID，并使用请求中传入的相同中继状态。SAML 验证通过后，Microsoft Entra ID 会将用户重定向到中继状态中的上下文，因此用户直接访问应用程序。

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

- **在 Citrix Secure Private Access 服务中配置 O365 应用程序**。有关详细信息，请参阅 对软件即服务应用程序的支持。

域联合的工作原理

下图说明了域联合完成后涉及的典型流程。



假设您想将 Office 365 应用程序添加到 Citrix Workspace 并启用水印和限制下载。典型流程如下：

1. 您在 Citrix Workspace 中启动 Office 365 应用程序。
2. 请求发送到 Citrix Secure Private Access 服务。
3. Citrix Secure Private Access 服务创建 SAML 断言并将其转发到 Microsoft Entra ID。
4. 由于请求来自受信任的 SAML IdP，Microsoft Entra ID 通过已创建的域联合识别它，并将 SAML 断言传递给 Office 365 应用程序。

   Office 365 应用程序已启动。

Office 365 应用程序支持的身份验证方法

默认情况下，Citrix Cloud™ 使用 Citrix 身份提供程序来管理您的 Citrix Cloud 帐户中所有用户的身份信息。

Citrix Workspace 支持 Office 365 的以下身份验证方法。目前不支持 Okta 和 Google IdP。

- 本地活动目录
- Active Directory 加令牌
- 微软 Entra ID

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

注意： 如果使用 Microsoft Entra ID 对工作区进行身份验证，则无法联合主域（用户的登录域），因为这会形成循环。在这种情况下，您必须联合一个新域。

- 思杰安全专用访问
- 活动目录加 RADIUS

有关更多详细信息，请参阅身份和访问管理。

在 Secure Private Access 服务中配置 O365 应用程序

以下是在 Secure Private Access 服务中配置 O365 应用程序的高级步骤。有关更多详细信息，请参阅对软件即服务应用程序的支持。

1. 转到 Citrix Cloud 中的 Secure Private Access 服务。
2. 搜索 Office 365 并选择 **Office365** 模板。有关使用模板配置应用程序的详细信息，请参阅对软件即服务应用程序的支持。

   注意：

   选择 **Office365** 模板后，以下相关域将自动填充到“**应用程序详细信息**”部分。

   - *.office.com
   - *.office365.com
   - *.sharepoint.com
   - *.live.com
   - *.onenote.com
   - *.microsoft.com
   - *.powerbi.com
   - *.dynamics.com
   - *.microsoftstream.com
   - *.powerapps.com
   - *.yammer.com
   - *.windowsazure.com
   - *.msauth.net
   - *.msauthimages.net
   - *.msocdn.com

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

- *.microsoftonline.com
- *.windows.net
- *.microsoftonline-p.com
- *.akamaihd.net
- *.sharepointonline.com
- *.officescriptsservice.com
- *.live.net
- *.office.net
- *.msftauth.net

3. 如果需要，启用增强的安全控制。
4. 配置 SSO。

   注意：您唯一需要做的更改是确保“名称 ID”是 Active Directory GUID。

5. 确保高级属性也发送 `IDPEmail`。

   - 属性名称：`IDPEmail`
   - 属性格式：未指定
   - 属性值：电子邮件

6. 单击 SAML 元数据以在新选项卡中打开。

   - 复制“entityID”
   - 复制“Login URL”
   - 下载 CRT 格式的证书

配置从 Microsoft Entra ID 到 Citrix Workspace 的域联合

先决条件：

- 在 Microsoft Entra ID 中启用 PowerShell
- 安装 Microsoft MSOnline 模块

以下是用于安装所需模块的 PowerShell 命令。

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

```
`PS> Install-Module AzureAD -Force`


`PS> Import-Module AzureAD -Force`


`PS> Install-Module MSOnline -Force`


`PS> Import-module MSOnline -Force`
```

如果模块已安装，则运行以下命令。

```
PS> connect-msolservice
```

注意：需要 Microsoft 云帐户才能连接到 `msolservice`。例如，`admin.user@onmicrosoft.com`。

配置从 Microsoft Entra ID 到 Citrix Workspace 的域联合的步骤

1. **在 PowerShell 中运行以下命令以配置联合：**

   - `PS> $dom = "ad-domain.com"`

   注意：ad-domain.com 是添加到 Microsoft Entra ID 的新域

   - `PS> $IssuerUri = "https://citrix.com/[customerID]"`

   注意：customerID 可从以下位置找到：

   - **Citrix Cloud > 身份和访问管理 > API 访问**
   - **Citrix Cloud > Citrix Secure Private Access。** customer ID 可以在应用程序配置详细信息中找到（**单点登录 > SAML 元数据文件 > entityID**）。
   - `PS> $fedBrandName = “CitrixWorkspace”`
   - `PS> $logoffuri = "https://app.netscalergateway.net/cgi/logout"`
   - `PS> $uri = "https://app.netscalergateway.net/ngs/[customerID]/saml/login?APPID=[AppID]”`

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

注意：$uri 可以从 Citrix Secure Private Access Service > 添加 Web/SaaS 应用程序 > 单点登录 > 登录 URL 或从 SAML 元数据 > 位置复制。

- `PS> $cert = New-Object System.Security.Cryptography.X509Certificates.X509Certificate2("<location of certificate downloaded from Citrix Secure Private Access service/ filename.crt>")`

  例如：`PS> $cert = New-Object System.Security.Cryptography.X509Certificates.X509Certificate2("c:\cert\saml_idp.crt")`

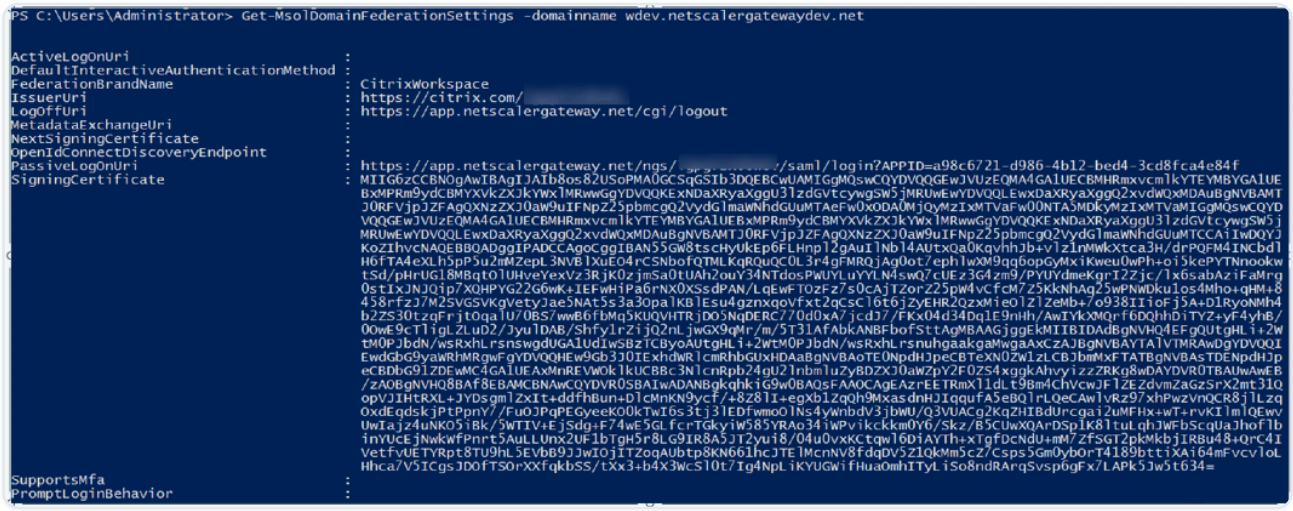
`PS> $certData = [system.convert]::tobase64string($cert.rawdata)`

2. **运行 PS 字符串以完成与 Citrix Secure Private Access 的联合：**

   `PS> Set-MsolDomainAuthentication -DomainName $dom –federationBrandName $fedBrandName -Authentication Federated -PassiveLogOnUri $uri -LogOffUri $logoffuri -SigningCertificate $certData -IssuerUri $IssuerUri -PreferredAuthenticationProtocol SAMLP`

3. **通过运行以下命令验证域联合设置：**

   `Get-MsolDomainFederationSettings -DomainName <domain name>`



从 Microsoft Entra ID 到 Citrix Workspace 的自动化域联合

在从 Microsoft Entra ID 到 Citrix Workspace 的手动域联合中，用户必须在云门户和 PowerShell 之间切换以复制数据并运行脚本。例如；

- 从云门户复制数据，例如客户 ID 和应用 ID。

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

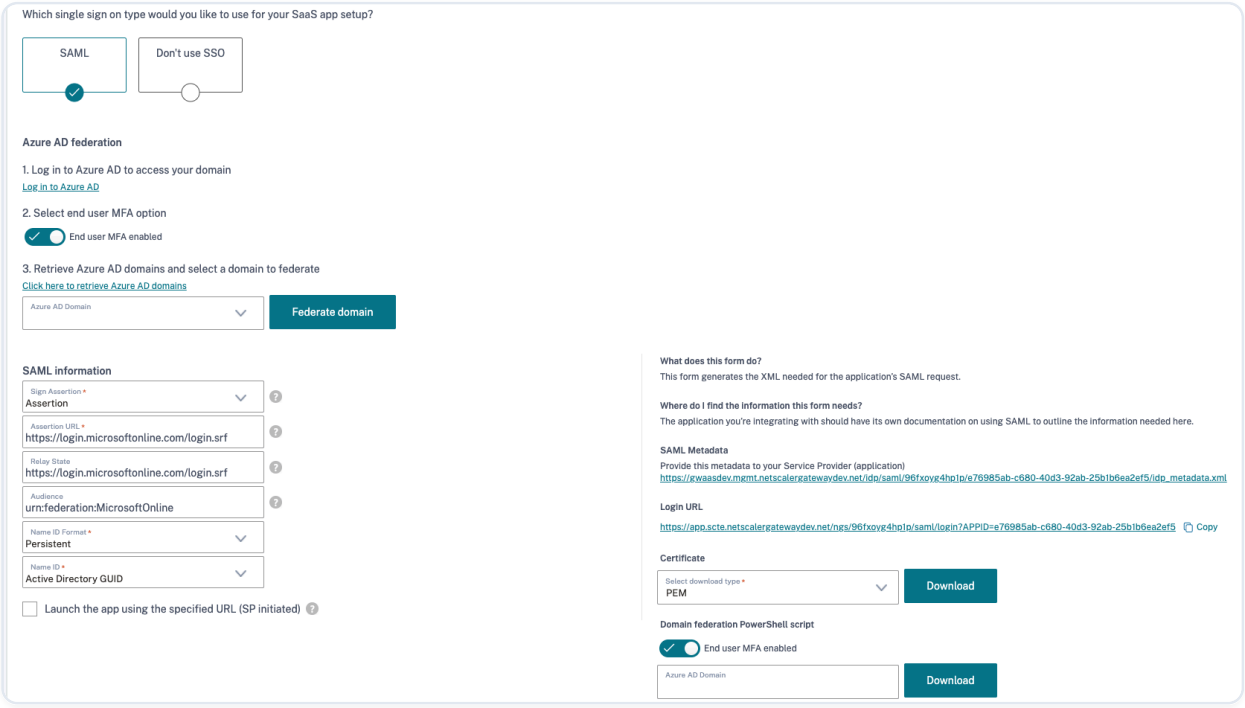
- 从云门户下载证书。
- 运行 PowerShell 脚本。

这种手动复制粘贴操作可能会引入错误，从而导致联合不成功。

现在，域联合的步骤已集成到 Citrix Secure Private 服务用户界面中，从而使联合过程自动化。当用户单击界面中的相应链接时，PowerShell 脚本会在后端运行。用户无需在云门户和 PowerShell 之间切换。

自动联合域的步骤

1. 配置 O365 应用程序。有关详细信息，请参阅在 Secure Private Access 服务中配置 O365 应用程序。
2. 在单点登录中，选择 **SAML**。



3. 使用您的凭据登录 Microsoft Entra ID。 当您单击**登录到 Entra ID**时，您将被定向到 Microsoft Entra ID 登录门户进行身份验证。
   - OAuth 协议用于身份验证。身份验证成功后，您必须提供联合域的同意。
   - **选择最终用户 MFA 选项**默认启用。
4. 单击**单击此处检索 Entra ID 域**以查看所有域的列表。
5. 选择您要联合的域，然后单击 **联合域**。

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

注意：

- 当您单击 **联合域** 时，PowerShell 脚本会在后端运行，并且域会联合。
- 如有必要，您还可以从界面下载 PowerShell 脚本。在 **域联合 PowerShell 脚本** 中，单击 **下载**。

抑制多重身份验证 (MFA)

O365 应用程序的高级属性中添加了一个选项，当用户在对 Citrix Workspace 进行用户身份验证期间已输入 MFA 时，该选项会抑制 MFA。

- **属性名称：** “`http://schemas.microsoft.com/ws/2008/06/identity/claims/authenticationmethod`”，
- **属性值：** “`http://schemas.microsoft.com/claims/multipleauthn`”

要使 Microsoft Entra ID 接受此声明，请使用以下 PowerShell 命令进行联合：

```
Set-MsolDomainAuthentication -DomainName $dom –federationBrandName $fedBrandName
-Authentication Federated -PassiveLogOnUri $uri -LogOffUri $logoffuri
-SigningCertificate $certData -IssuerUri $IssuerUri
-PreferredAuthenticationProtocol SAMLP -SupportsMfa $true
```

注意：

IdP 启动的流程不遵循中继状态。使用 SP 启动的流程直接访问应用程序。

在 Citrix Workspace 中配置单个 Office 套件应用程序

执行以下操作以配置单个 Office 套件应用程序：

1. 按照前面章节中的详细说明完成域联合。
2. 选择 O365 模板。
3. 将应用程序名称更改为，例如，MS Word。
4. 相应地更改应用程序 URL。

微软 Word： `https://login.microsoftonline.com/login.srf?wa=wsignin1%2E0&rver=6%2E1%2E6206%2E0&wreply=https%3A%2F%2Fwww.office.com%2Flaunch%2FWord%3domain>`

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

演示文稿： `<https://login.microsoftonline.com/login.srf?wa=wsignin1%2E0&rver=6%2E1%2E6206%2E0&wreply=https%3A%2F%2Fwww.office.com%2Flaunch%2Fpowerp domain>`

电子表格： `https://login.microsoftonline.com/login.srf?wa=wsignin1%2E0&rver=6%2E1%2E6206%2E0&wreply=https%3A%2F%2Fwww.office.com%2Flaunch%2FExcel% domain>`

客户关系管理/Dynamics Online： `https://<tenant>.crm.dynamics.com/?whr=<federated domain>`

OneDrive 商务版： `https://login.microsoftonline.com/login.srf?wa=wsignin1%2E0&rver=6%2E1%2E6206%2E0&wreply=https%3A%2F%2F<tenant>-my.sharepoint.com%2F&whr=<federated domain>`

Outlook 日历： `https://outlook.office.com/owa/?realm=<federated domain>&path=/calendar/view/Month`

Outlook 网页版访问 Exchange Online： `https://outlook.com/owa/<federated domain>`

SharePoint 在线版： `https://login.microsoftonline.com/login.srf?wa=wsignin1%2E0&rver=6%2E1%2E6206%2E0&wreply=https%3A%2F%2F<tenant>.sharepoint.com%2F&whr=< domain>`

团队： `https://login.microsoftonline.com/common/oauth2/authorize?client_id=cc15fd57-2c6c-4117-a88c-83b1d56b4bbe&response_mode=form_post&response_type=code+id_token&scope=openid+profile& domain>`

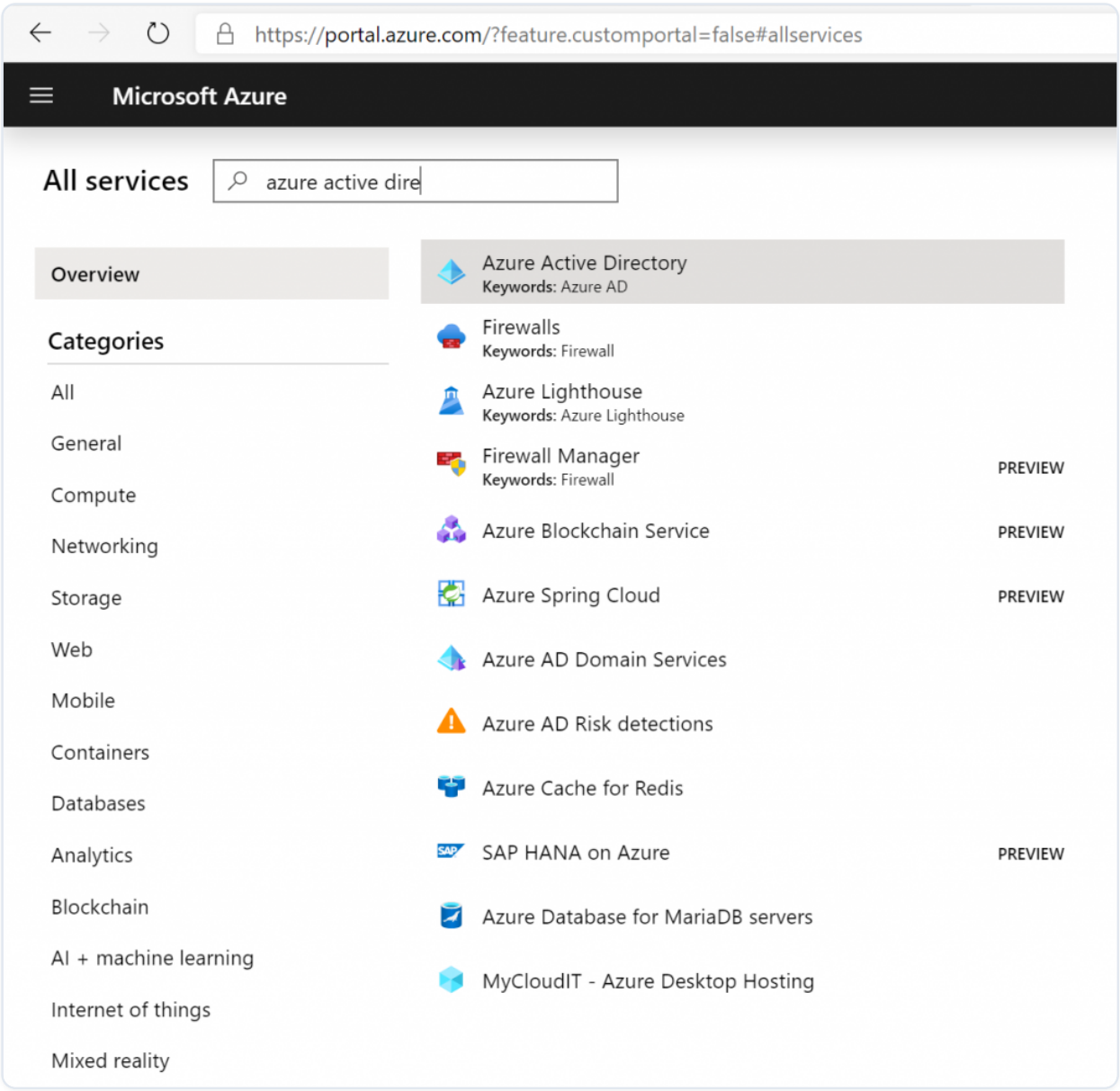
集成到 Microsoft Entra ID 中的第三方应用程序

如果您集成了 Box、Salesforce、ServiceNow、Workday 等第三方应用程序，您可以从 Microsoft Entra ID 获取这些应用程序的智能链接。

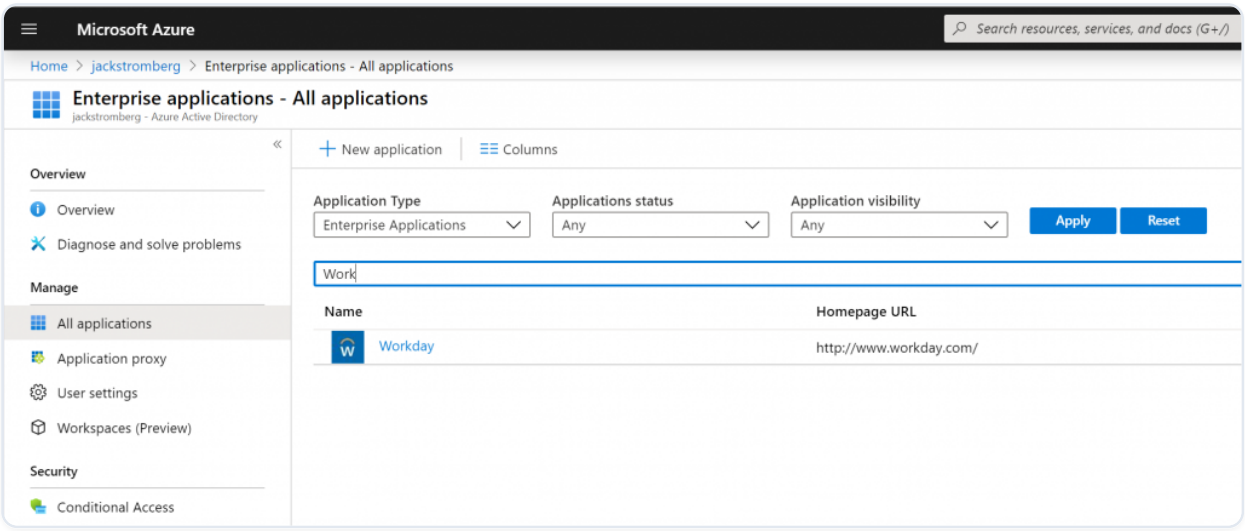
执行以下步骤。

1. 登录到您的 Microsoft Entra ID 门户 `<https://portal.azure.com>`。
2. 选择 **所有服务 > Azure Active Directory**，然后选择您的目录。

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

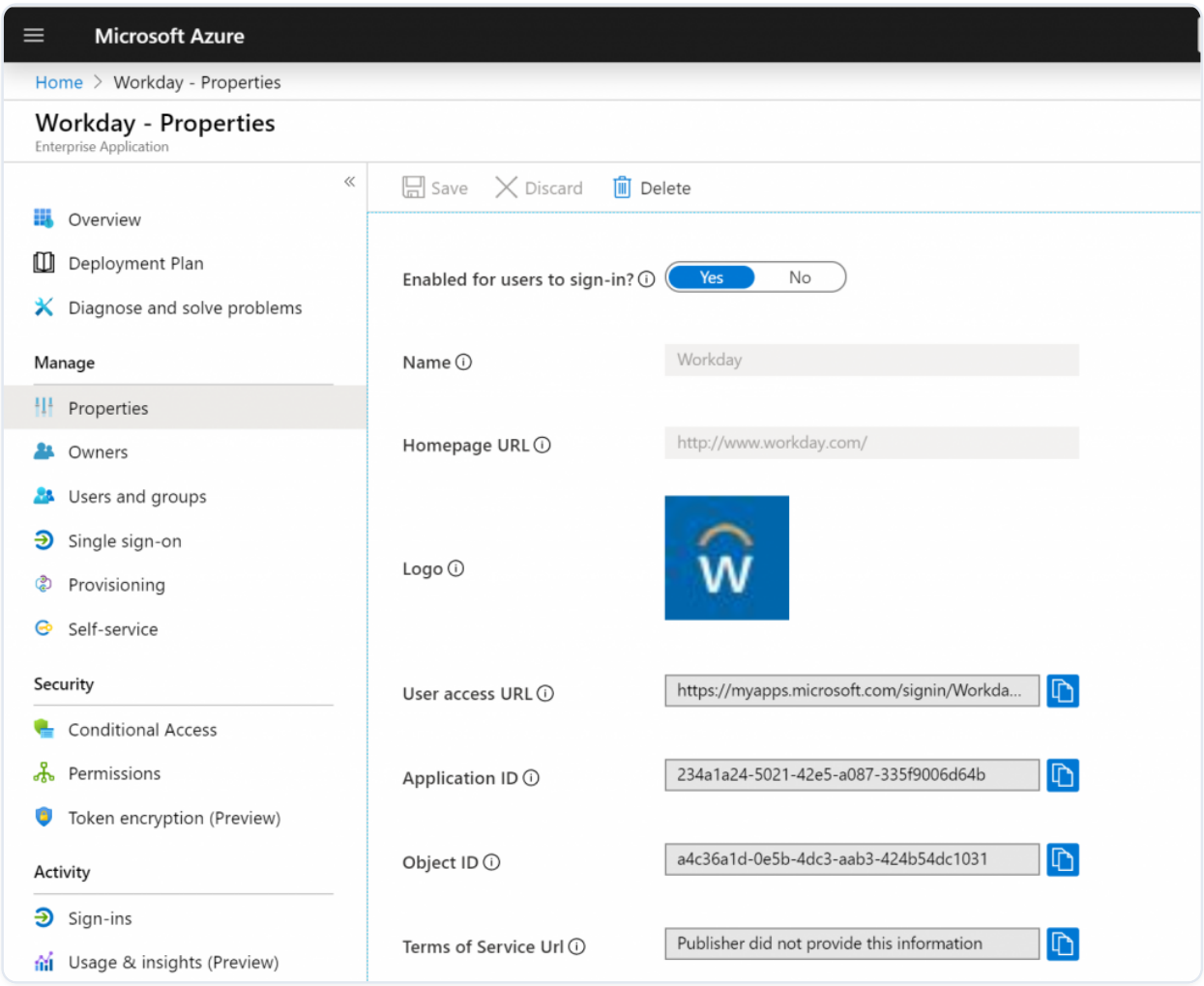


3. 选择 **企业应用程序**，然后选择要为其生成智能链接的应用程序。



4. 选择 **属性** 并复制用户访问 URL。

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



5. 将 `whr` 附加到 URL 后，`whr` 参数将按示例 URL 中所示显示。

   示例 URL: `https://myapps.microsoft.com/signin/Workday/12345678912345678912345678896d64b&whr=ctxnsqa.net`

   注意： 将 `whr` 附加到 URL，以便 Microsoft Entra ID 知道根据联合设置使用哪个 IdP 来验证用户，并自动重定向到该 IdP。

6. 设置增强的安全控制。
7. 配置 SSO。

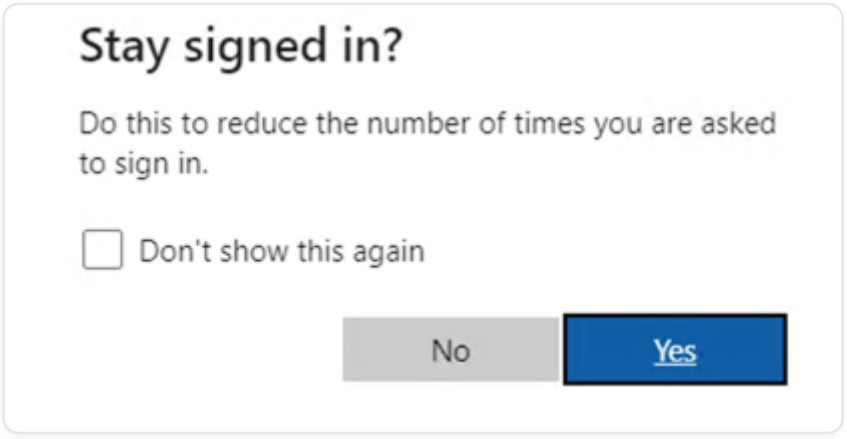
   - 名称 ID = AD GUID
   - 启用 SP 发起的复选框
   - 断言 URL = 登录 URL

     当您执行 IdP 发起的流程时，用户会被重定向到 Microsoft Entra ID 门户页面。如果您想直接进入应用程序页面，则需要 SP 发起的流程，因为它会在 SAML 断言中发送正确的 relay state。

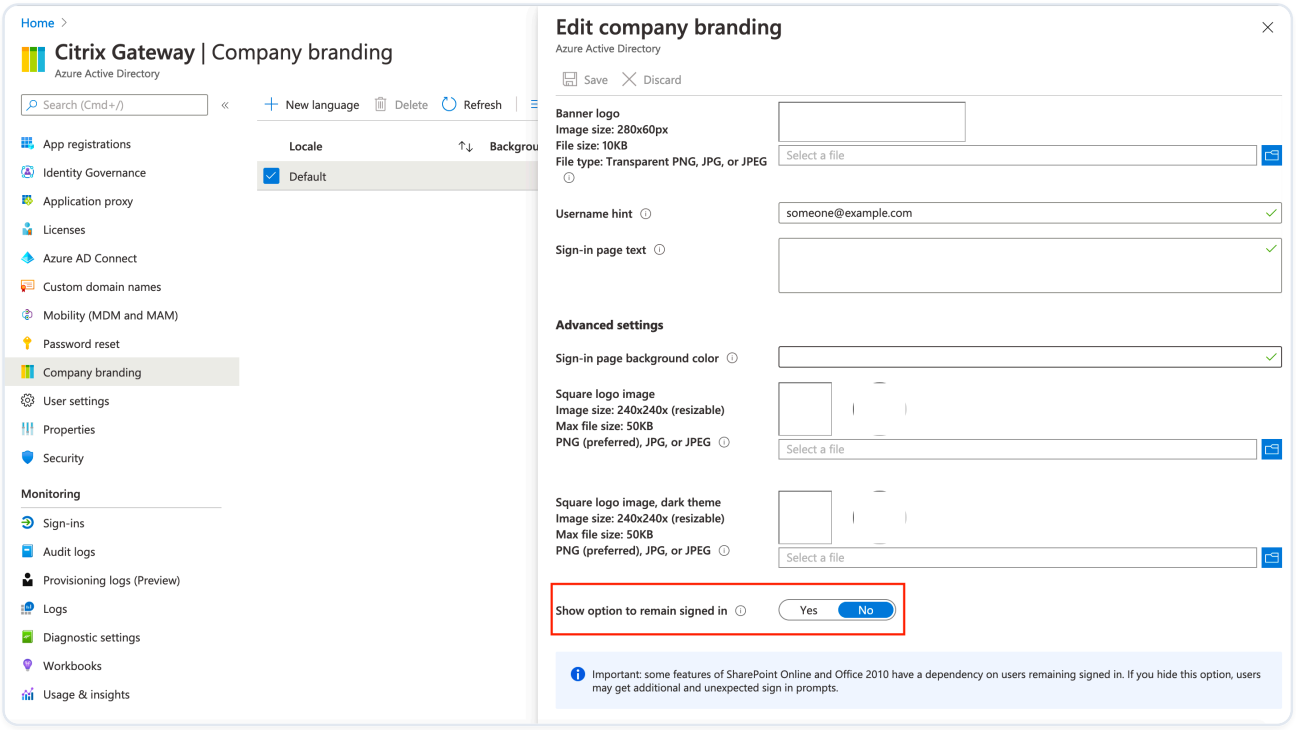
© 1997–2026 Citrix Systems, Inc. All rights reserved.

注意：

- 当启用主域的联合时，所有 Microsoft Entra ID 用户在对任何 Office 365 应用程序进行身份验证时都会被重定向到 Citrix Workspace。如果未理解其影响就执行此操作，可能会导致客户出现中断/事件。
- 如果用户使用 Microsoft Entra ID 登录 Citrix Workspace，则用于登录的用户主域不得联合到 Citrix Gateway 服务。这会导致循环。在这种情况下，请使用与用户登录 Microsoft Entra ID 的域不同的另一个域来联合到 Citrix Secure Private Access 服务。
- 如果主域联合到 Citrix Secure Private Access 服务，则 Microsoft Entra ID 中该域上的所有用户登录都将重定向到 Citrix Secure Private Access 服务。对于概念验证 (POC)，如果需要，您可以在联合主域之前联合一个测试域。
- 如果 Microsoft Entra ID 启用了位置策略，则用户必须仅来自公司网络允许的 IP 地址列表。在这种情况下，您可以将 O365 应用程序发布为 Web 应用程序，并通过 Connector Appliance 路由其流量。
- 登录 Microsoft Entra ID 时，如果您想避免出现“**保持登录状态？**”提示，可以使用 Microsoft Entra ID 更改此设置。请注意更改设置时出现的重要消息，并在必要时恢复。



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



参考链接

Azure PowerShell 模块参考

在 Microsoft Azure 中部署 Office 365 目录同步

配置 ERP Cloud

以下部分提供了有关配置 ERP Cloud 的更多信息。

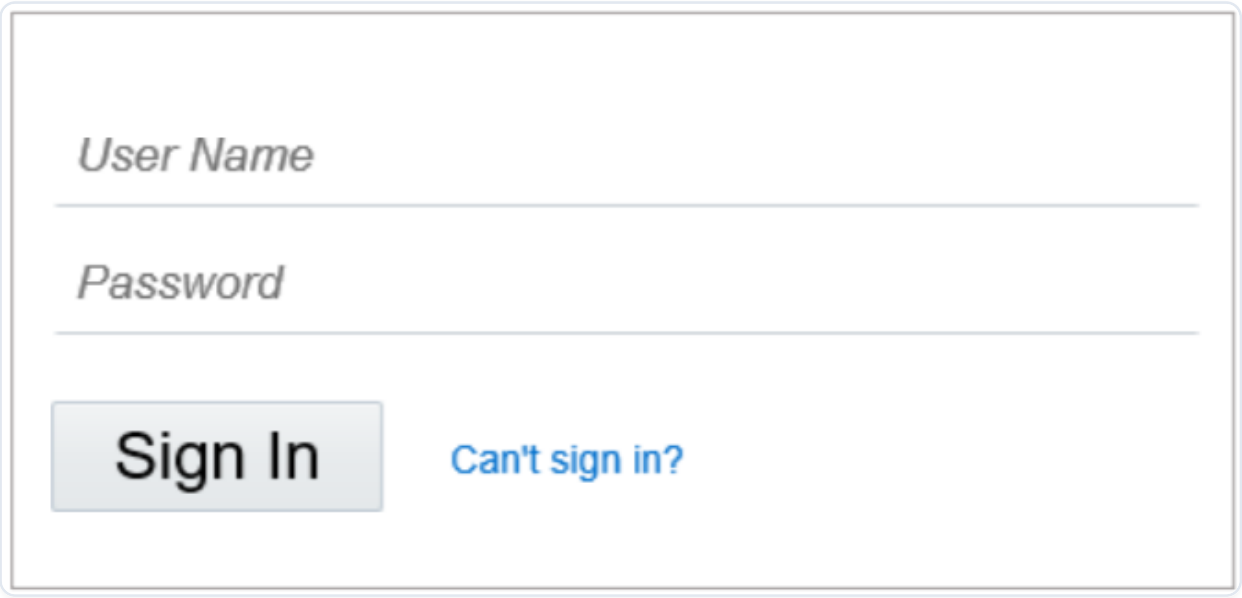
Citrix Gateway SaaS 应用程序

用户可以使用其企业凭据安全地登录 ERP Cloud。

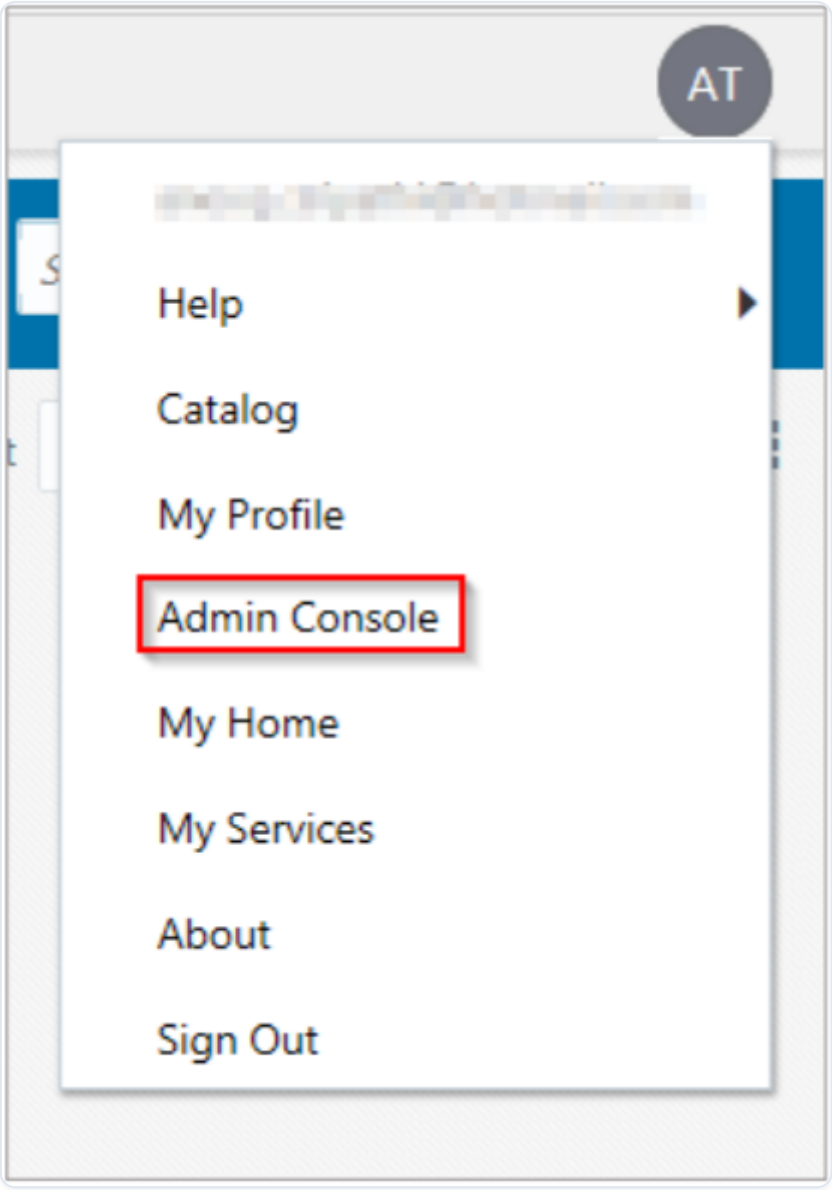
要通过 SAML 为 SSO 配置 ERP Cloud，请执行以下操作：

1. 在浏览器中，键入：`https://<organizationid>.identity.oraclecloud.com/ui/v1/adminconsole/?root=security&security=external-idp`，然后按 Enter。
2. 登录您的 ERP Cloud 帐户。

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



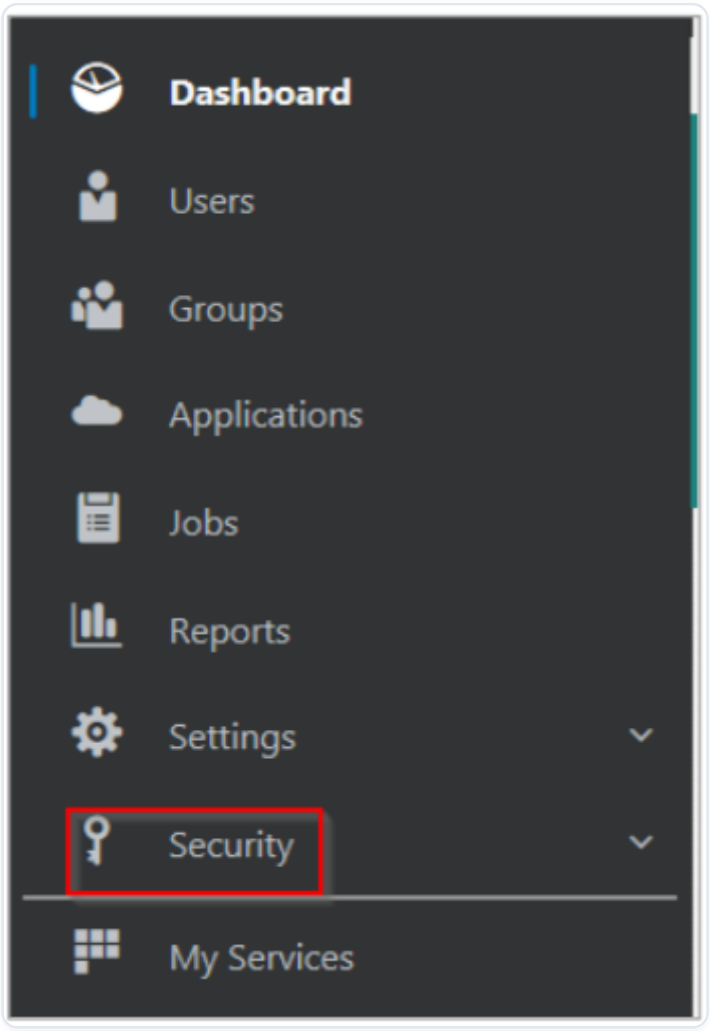
3. 在主页右上角，单击您的个人资料首字母，然后单击“Admin Console”。



4. 在左上角，单击省略号。

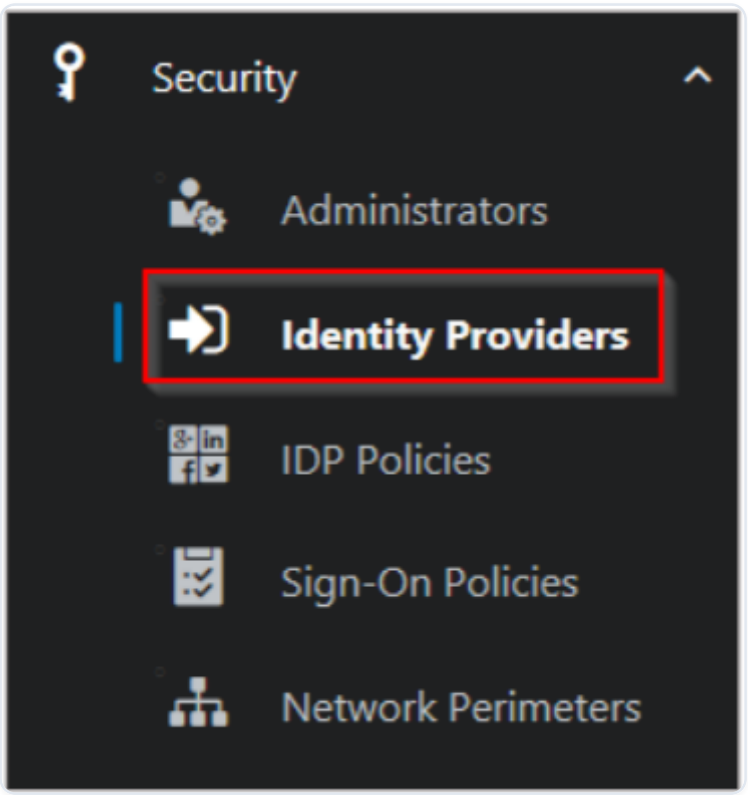
© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. 单击“安全”。

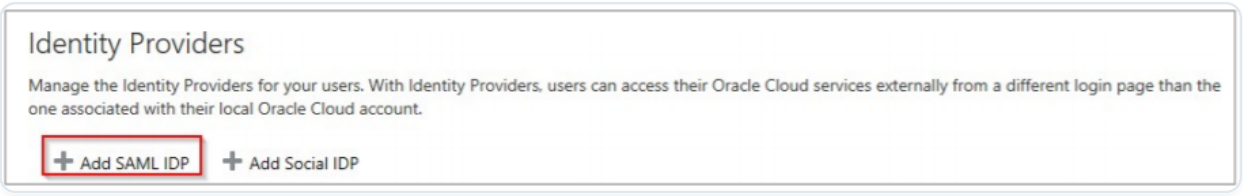


6. 单击“身份提供程序”。

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

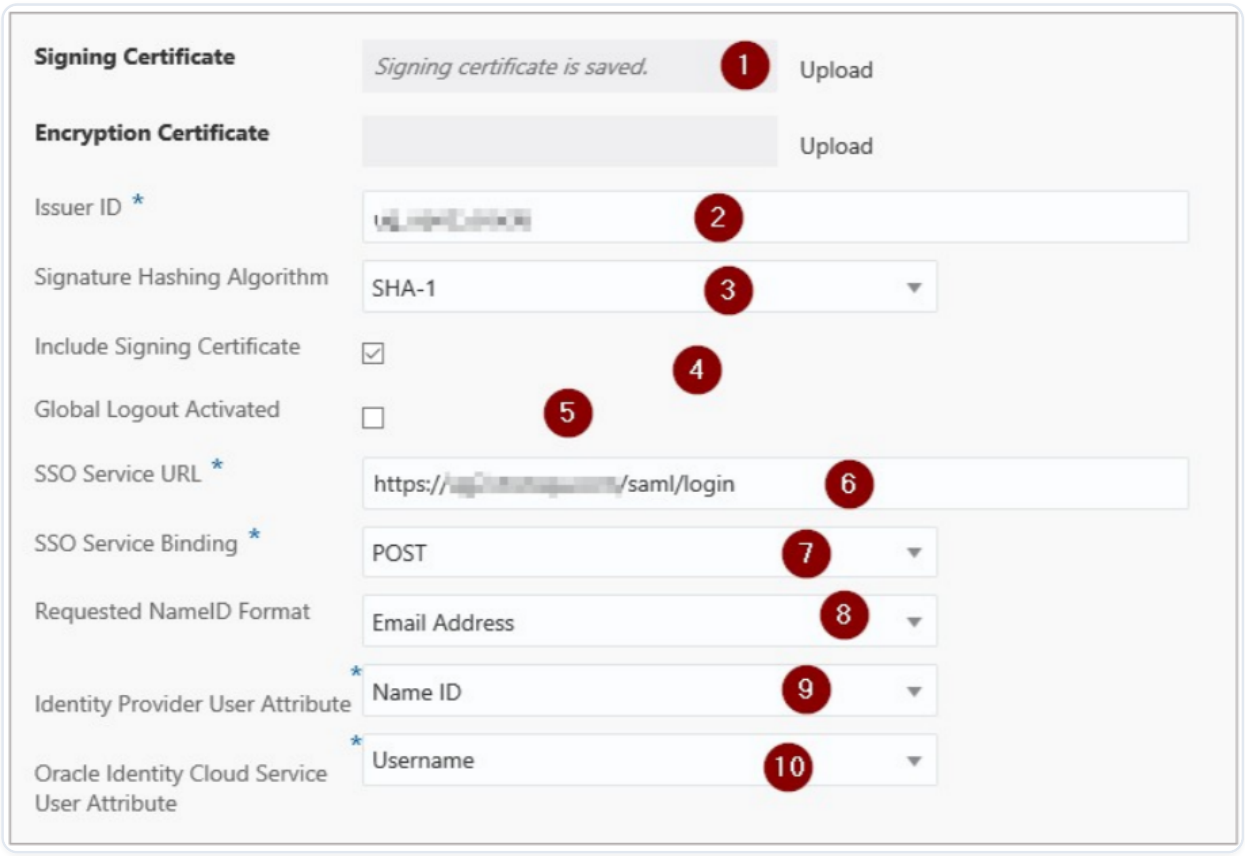


7. 在“身份提供程序”页面上，单击“添加 SAML IdP”。



8. 在“身份提供程序”页面上，指定以下信息：

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



a. 签名证书 – 粘贴 PEM 证书。

要获取 IdP 证书，请执行以下操作：

- 使用 PuTTY 远程访问您的 NetScaler® 实例。
- 导航到 /nsconfig/ssl 文件夹（使用 shell 命令 `cd` /nsconfig/ssl），然后按 Enter。
- 键入 cat `<certificate-name>`，然后按 Enter。
- 复制从 -----BEGIN CERTIFICATE----- 到 -----ENDCERTIFICATE----- 的文本。
- 将文本粘贴到文本编辑器中，并以适当的格式（例如 `your organization name`.pem）保存文件。

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



b. 颁发者 ID – 键入一个唯一的名称。

c. 签名哈希算法 – 选择用于签署 SAML 消息的哈希算法。

d. 包含签名证书 - 如果要包含签名证书以验证 IdP 消息的签名，请选中此复选框。

e. 全局注销已激活 - 如果要激活 SAML 全局注销，请选中此复选框。

f. SSO 服务 URL – 输入 IdP URL，后跟 /saml/ login。例如：`https://<netscalerinstance>.com/saml/ login`

g. SSO 服务绑定 – 单击相应选项以发送身份验证请求。

h. 请求的 NameID 格式 – 单击相应格式，用于将 IdP 中用户的属性值映射到 Oracle Identity CloudService 中的相应属性。

i. 身份提供程序用户属性 – 单击从 IdP 接收到的相应属性值，以唯一标识用户。

j. Oracle Identity Cloud Service 用户属性 – 单击用于映射从 IdP 接收到的属性的相应属性。

9. 单击“保存更改”。

配置 ServiceNow

用户可以使用其企业凭据安全登录 ServiceNow。

要通过 SAML 为 SSO 配置 ServiceNow，请执行以下操作：

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

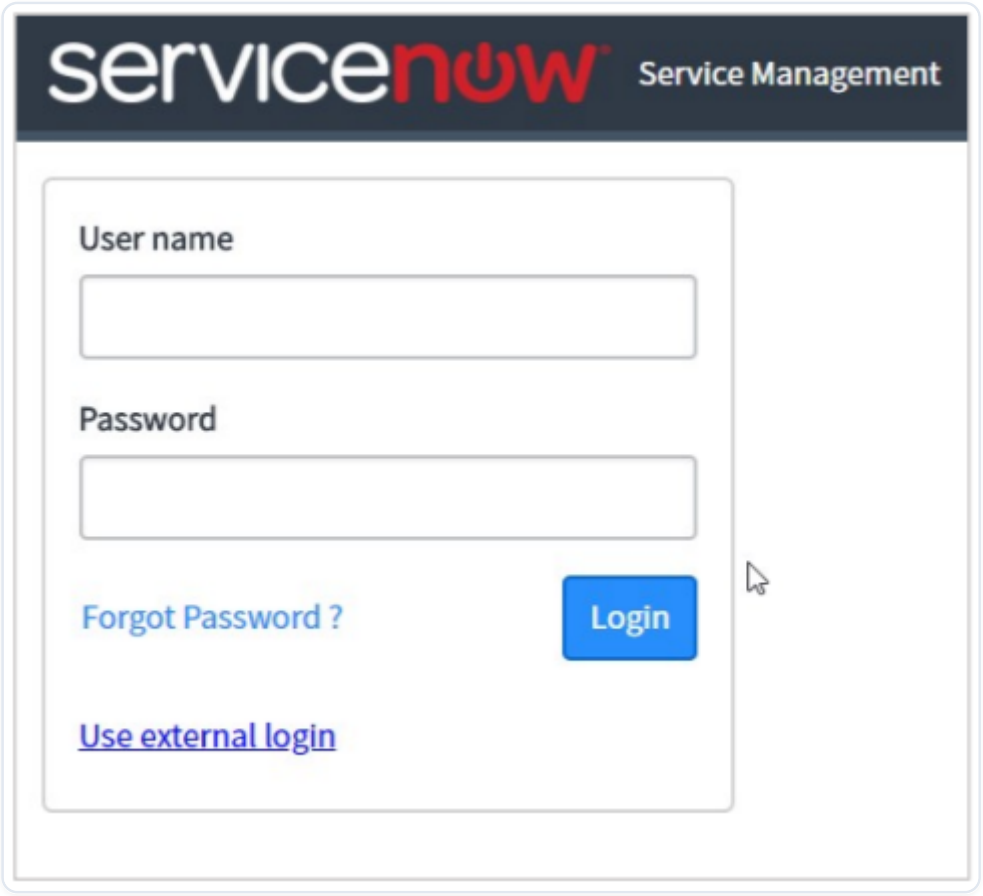
1. 在浏览器中，键入 `https://<your-organization>.service-now.com/`，然后按 **Enter**。

   例如，如果您用于访问 ServiceNow 的 URL 是 `https://myserver.servicenow.com`，则必须将 `<your-organization>` 替换为 `myserver`。

   注意：

   - 添加 ServiceNow 应用程序时，请确保在 Citrix Gateway 服务用户界面中提供以下详细信息。
     - 断言 URL: `https://<your-organizaton>.service-now.com/navpage.do`
     - 中继状态: `https://<your-organizaton>.service-now.com/`
     - 受众: `https://<your-organizaton>.service-now.com/`
     - 名称 ID 格式: 选择“电子邮件地址”
     - 名称 ID: 选择“用户主体名称 (UPN)”
   - 名称 ID 格式和名称 ID 属性取决于为 ServiceNow 选择的身份验证方法。

2. 以管理员身份登录您的 ServiceNow 帐户。

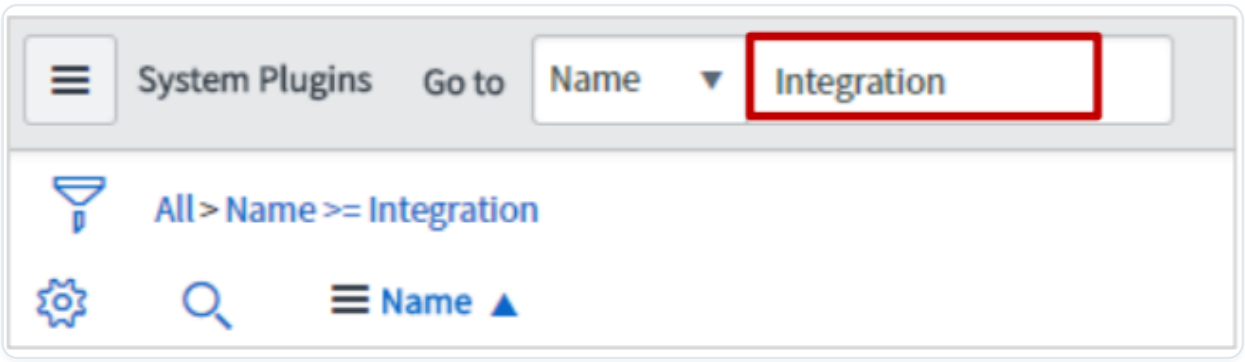


3. 在左上角，使用筛选导航器搜索插件，并在搜索结果中点击 **Plugins**。

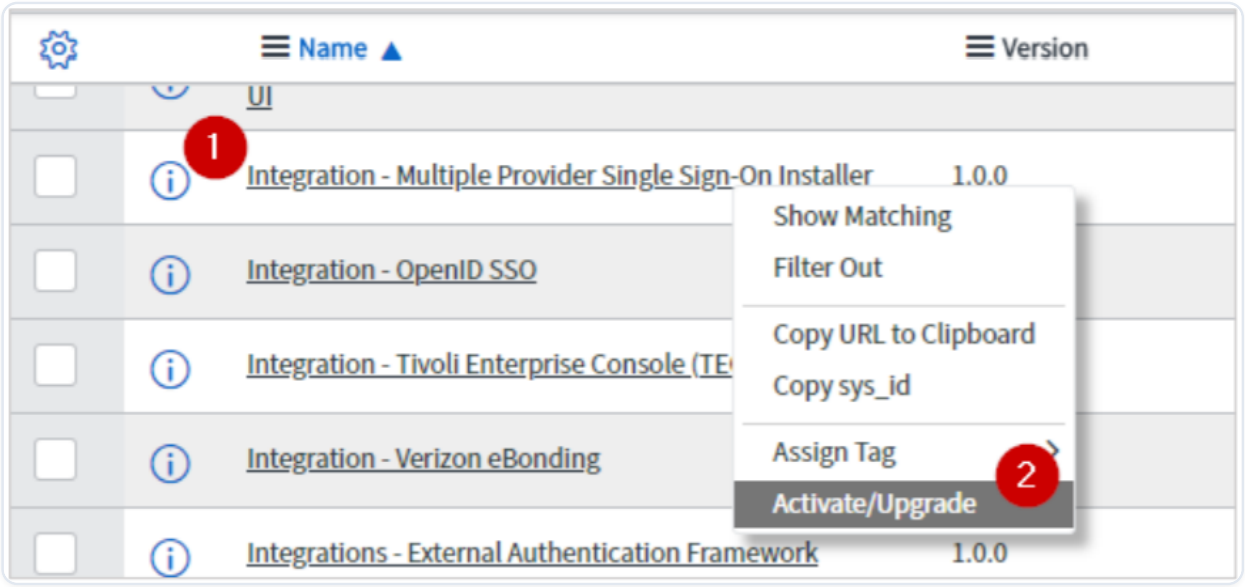
© 1997–2026 Citrix Systems, Inc. All rights reserved.



4. 在右侧窗格中，在“**系统插件**”部分中搜索集成。



5. 在搜索结果中，右键单击 **Integration - Multiple Provider Single Sign-OnInstaller** 并点击 **Activate/Upgrade**。

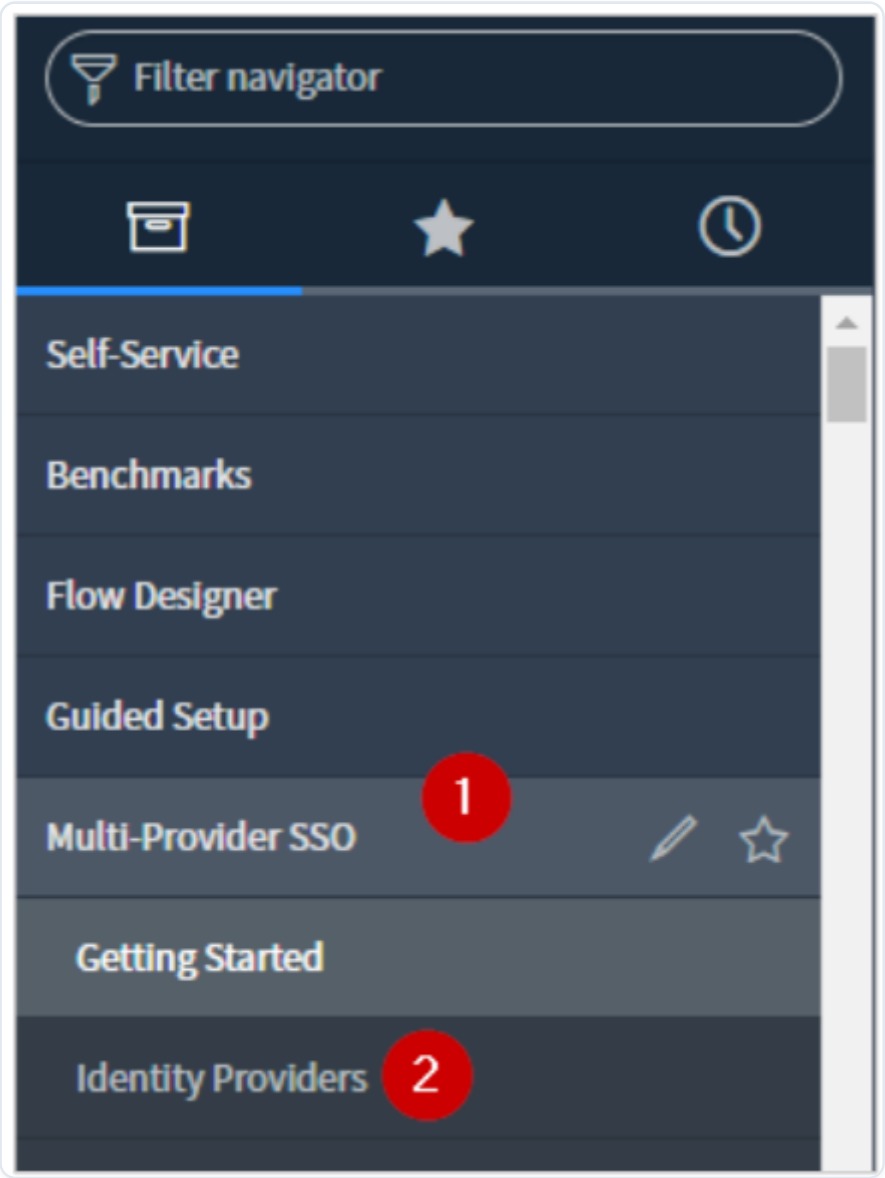


6. 点击 **Activate**。

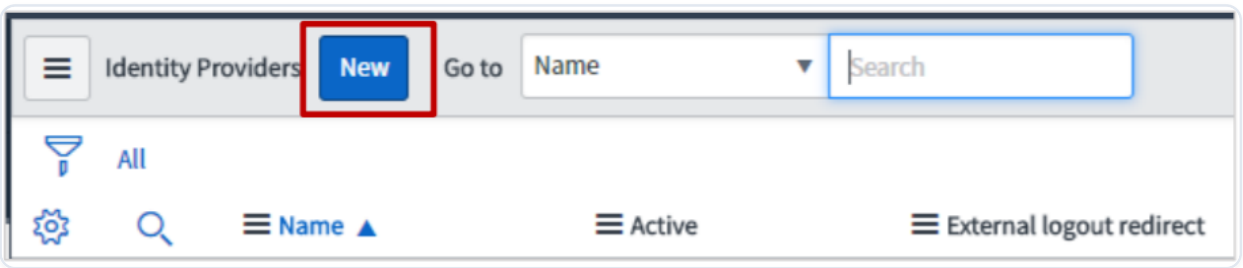
   进度条指示激活过程的完成。

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

7. 在左侧窗格中，向下滚动到“多提供商 SSO”部分，然后点击 **Multi-ProviderSSO > Identity Providers**。

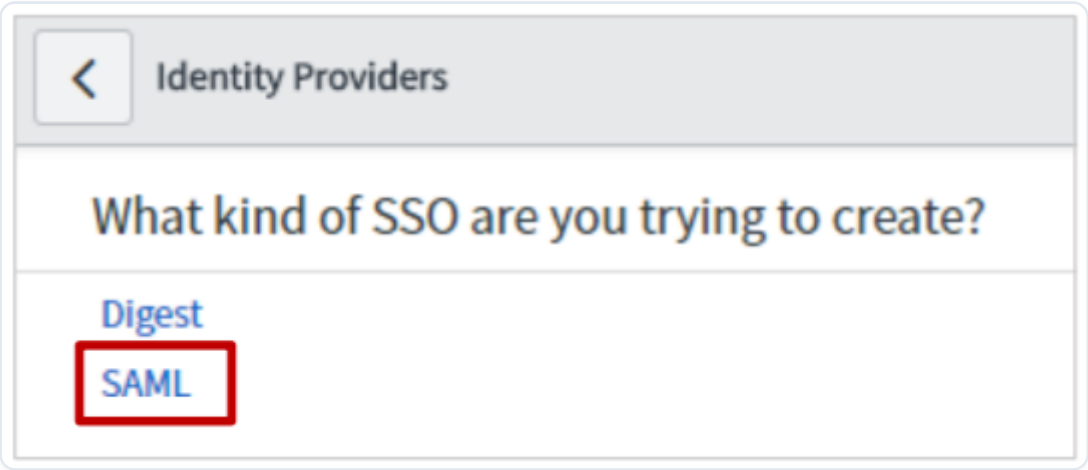


8. 在右侧窗格中，点击 **New**。



9. 点击 **SAML**。

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

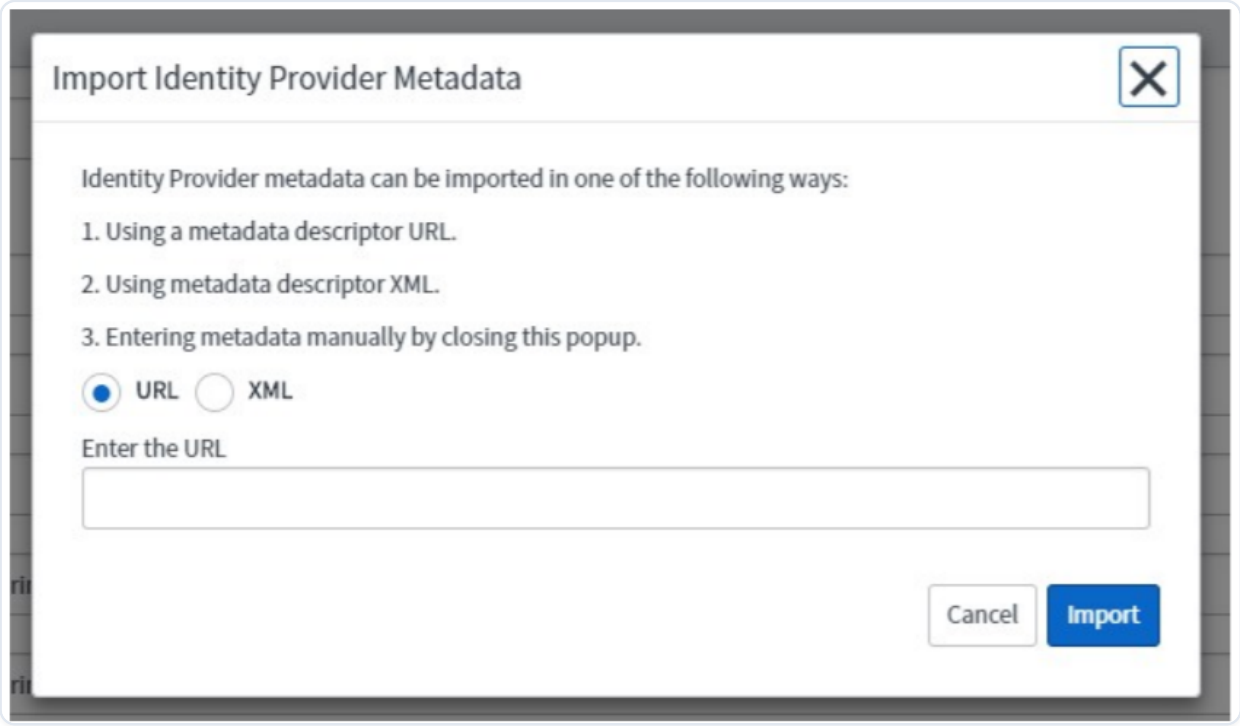


10. 如果您有元数据 URL，请在“**身份提供商新记录**”部分中，在“**导入身份提供商元数据**”弹出窗口中，点击 **URL**，然后输入元数据 URL 并点击 **Import**。

    身份提供商记录字段的值会自动填充。

    如果您有元数据 XML 文件，请单击 XML。复制身份提供商元数据 XML 数据并粘贴到框中。单击“**导入**”。

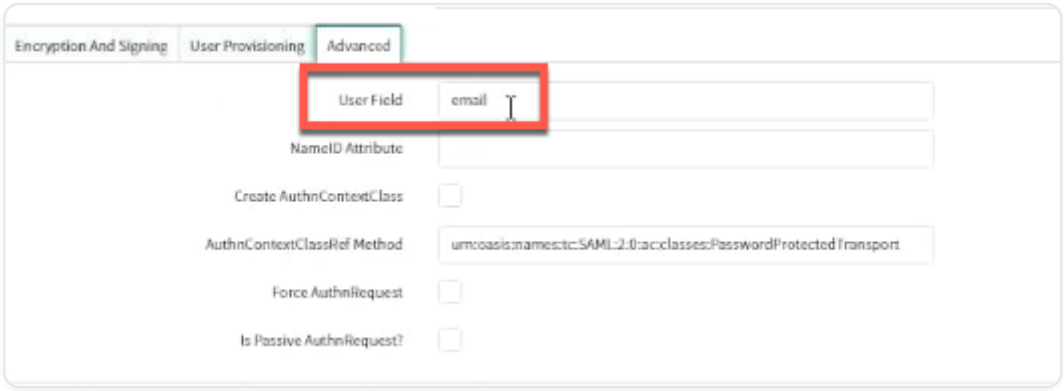
    身份提供商记录字段的值会自动填充。如有必要，您可以更新这些值。



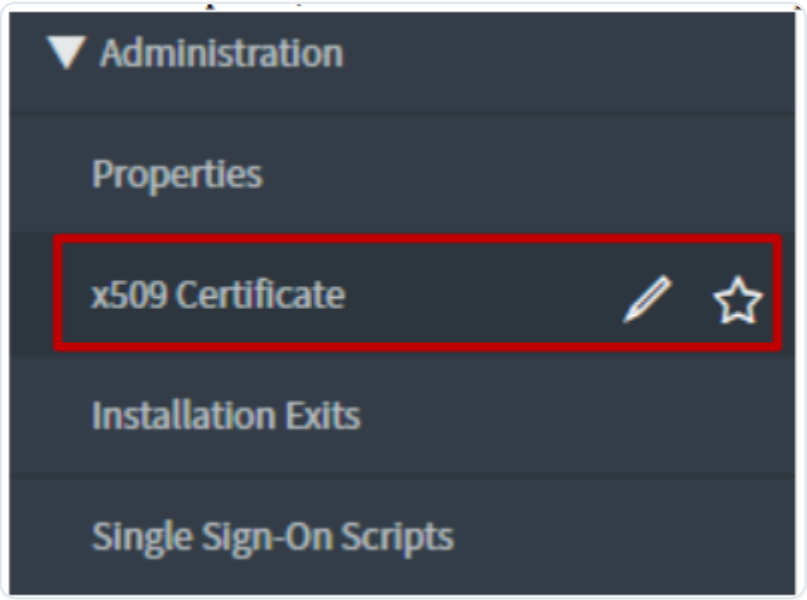
© 1997–2026 Citrix Systems, Inc. All rights reserved.

重要提示：

- Citrix 建议您导入元数据 XML 文件，而不是手动配置。您可以从 Citrix Cloud 向导（**Citrix Gateway Service > 添加 Web/SaaS 应用程序 > 单点登录 > SAML 元数据**）导入元数据 XML 文件。
- 在“**高级**”选项卡中配置参数时，请确保“**用户字段**”值与 Citrix Gateway 服务用户界面中为“**名称 ID**”字段配置的值匹配。

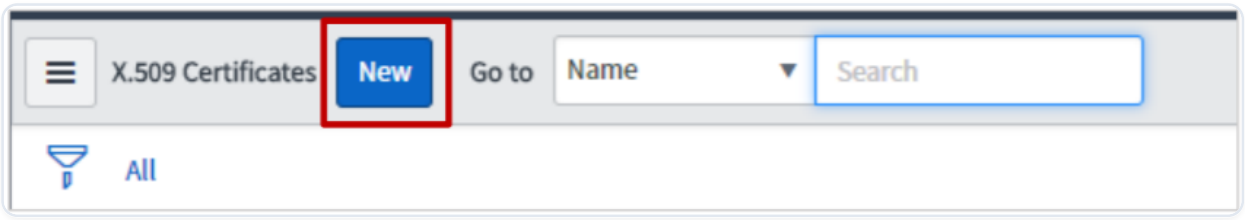


11. 单击“**提交**”。
12. 在左侧窗格中，单击 x509 证书以上传 x509 证书。

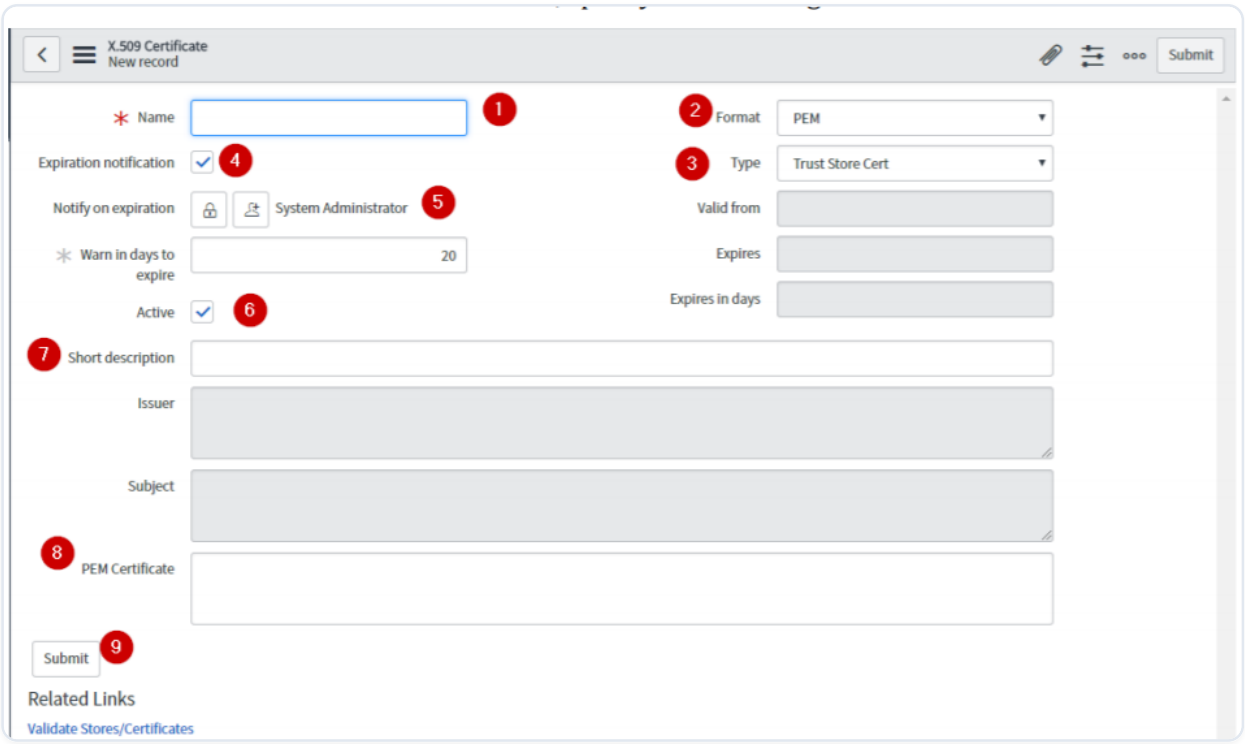


13. 在右侧窗格中，单击“**新建**”。

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



14. 在 X.509 证书新建记录部分中，指定以下信息：



名称 – 输入证书名称。

- 格式 – 单击相应的格式：例如 PEM。
- 到期通知 – 选中该复选框。
- 类型 – 单击相应的类型。
- 到期时通知 – 单击“添加我”图标以获取通知。单击“解锁到期时通知”以添加更多用户。
- 活动 – 选中该复选框。
- 简短描述 – 输入证书的描述。
- PEM 证书 – 粘贴 PEM 证书。
  - 从 **Citrix Cloud 向导 (Citrix Gateway Service > 添加 Web/SaaS 应用程序 > 单点登录 > 证书)** 下载证书。
  - 复制从 —–BEGIN CERTIFICATE—– 到 —–ENDCERTIFICATE—– 的文本
  - 将文本粘贴到文本编辑器中，并以适当的格式保存文件，例如 `<your organization name>.`.

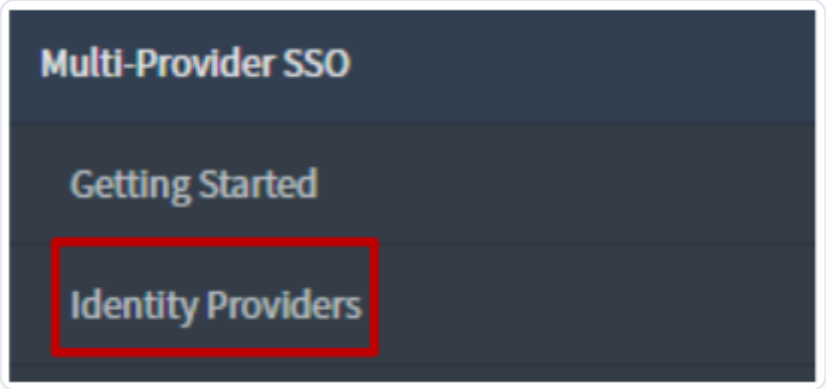
© 1997–2026 Citrix Systems, Inc. All rights reserved.

注意： 如果您已使用 XML 文件配置 IdP，则无需配置证书。

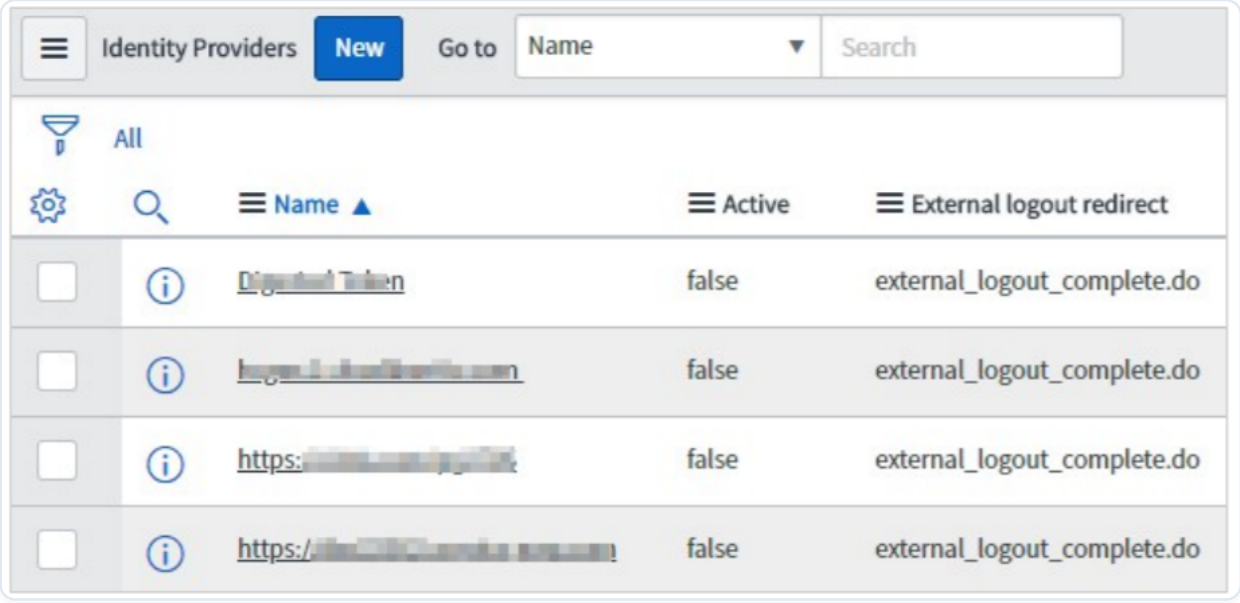


单击 **提交**。

15. 在左侧窗格中，单击 **身份提供程序**。

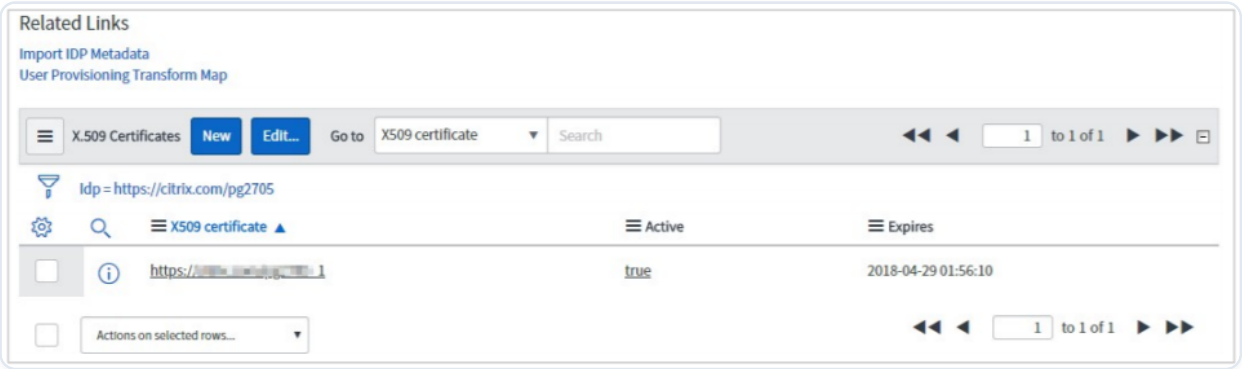


16. 单击您已添加的身份提供程序。



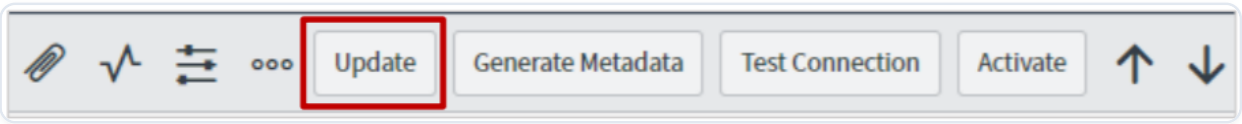
© 1997–2026 Citrix Systems, Inc. All rights reserved.

17. 在身份提供程序详细信息页面上，向下滚动到“相关链接”部分。在 X.509 证书行中，搜索 X.509 证书，然后单击“**编辑**”为身份提供程序添加相应的证书。



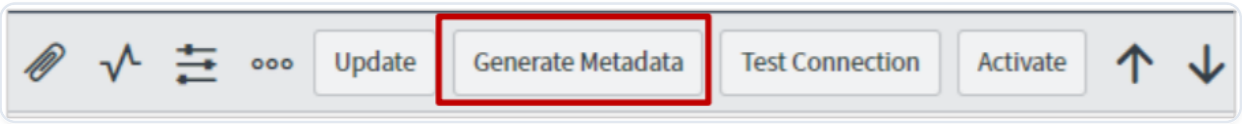
要添加新的 X.509 证书，请单击“**新建**”；要添加或删除证书，请单击“**编辑**”。

18. 在身份提供程序详细信息页面上，单击“**更新**”以保存更改。

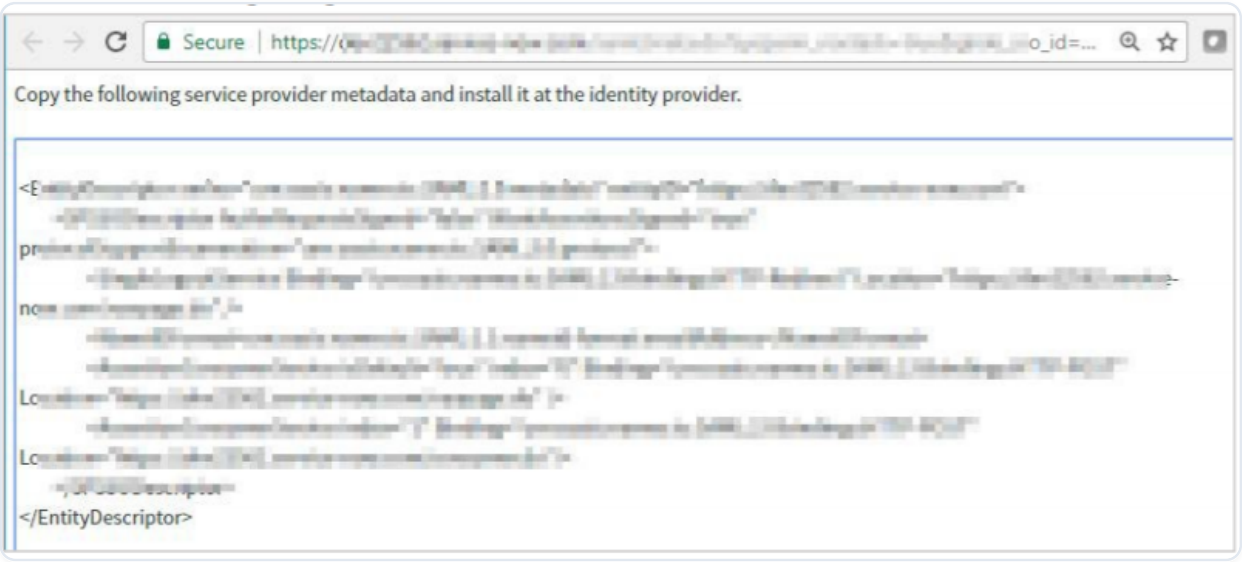


19. 要获取用于 IdP 配置的元数据，请单击“**生成元数据**”。

注意： 您必须单击“**生成元数据**”才能完成更新。



服务提供程序元数据将显示在新窗口中。您可以使用元数据来验证 SP 和 IdP 之间的实体。



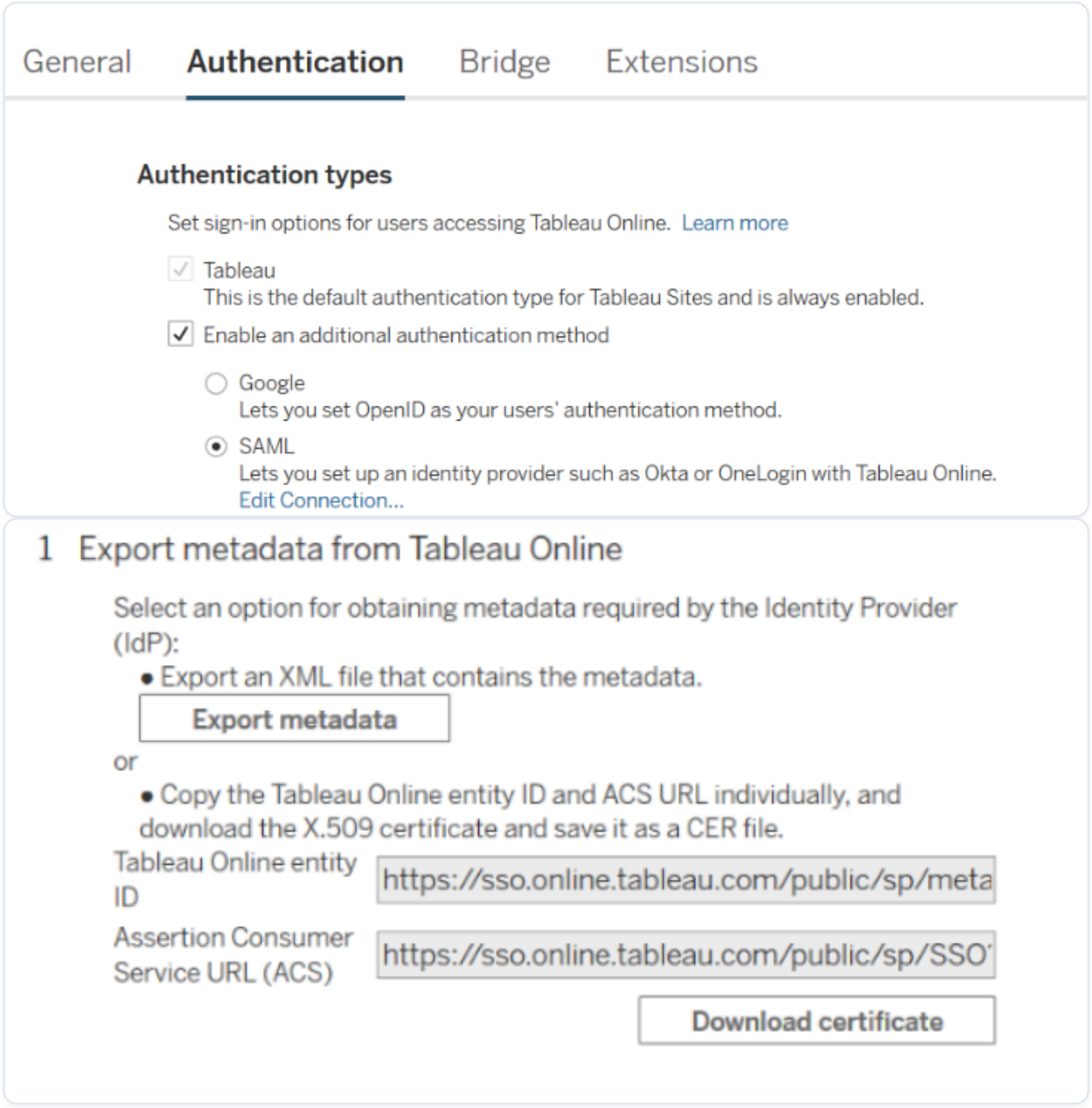
配置 Tableau

用户可以使用其企业凭据安全登录 Tableau。

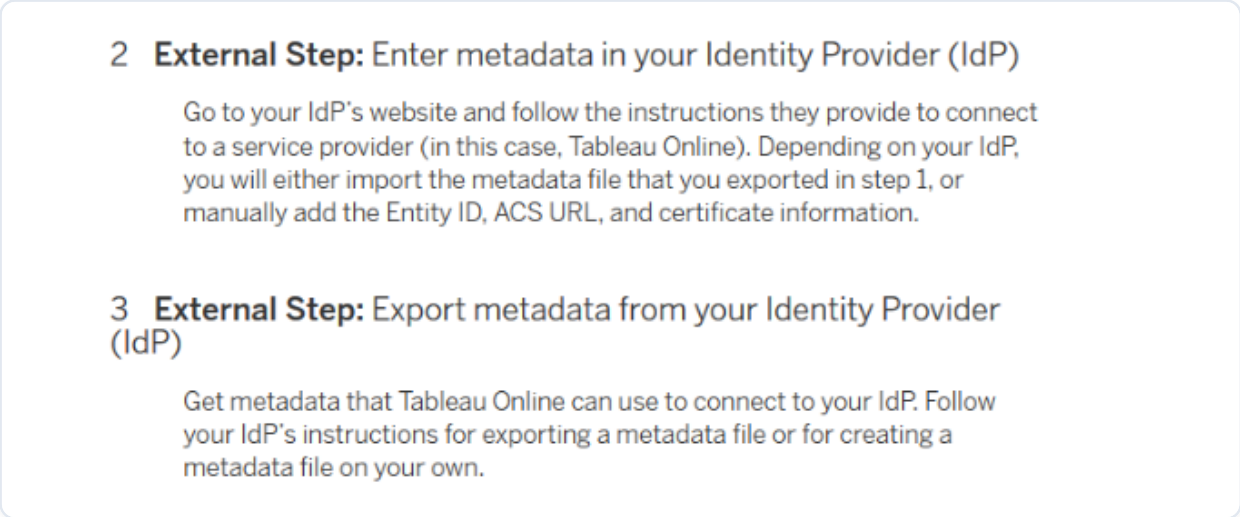
© 1997–2026 Citrix Systems, Inc. All rights reserved.

要配置 Tableau 以通过 SAML 进行 SSO，请执行以下操作：

1. 以管理员身份登录 Tableau。
2. 在菜单栏中单击**设置**。
3. 单击**身份验证**。
4. 在身份验证类型中，选择 **SAML**，然后单击**编辑连接**。



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



5. 从 Citrix Cloud 向导下载元数据文件 (**Citrix Gateway Service > 添加 Web/SaaS 应用程序 > 单点登录 > SAML 元数据**)。

   注意：

   - Citrix® 建议您导入元数据 XML 文件，而不是手动配置它。
   - 您可以从 Citrix Cloud 向导下载证书 (**Citrix Gateway Service > 添加 Web/SaaS 应用程序 > 单点登录 > 证书**)。

6. 将 IdP 元数据文件导入 **Tableau Online**。

   导入元数据(/en-us/citrix-secure-private-access/media/tableau-saml-3.png)

7. 输入格式为 `https://citrix.com/<customerID>` 的 IdP 实体 ID。
8. 单击 **测试连接**。
9. 将您的 IdP 属性与 Tableau 属性匹配，然后单击 **应用**。

   匹配属性(/en-us/citrix-secure-private-access/media/tableau-saml-4.png)

10. 向下滚动并选择 **SAML** 作为嵌入式视图的默认身份验证类型。

    添加选定用户(/en-us/citrix-secure-private-access/media/tableau-saml-5.png)

11. 根据需要添加或选择用于 SSO 的用户。

    - 要添加新用户，请单击 **添加用户** 并输入电子邮件地址。
    - 对于现有用户，请单击 **选择用户** 并根据需要进行更改。

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

配置 Workday

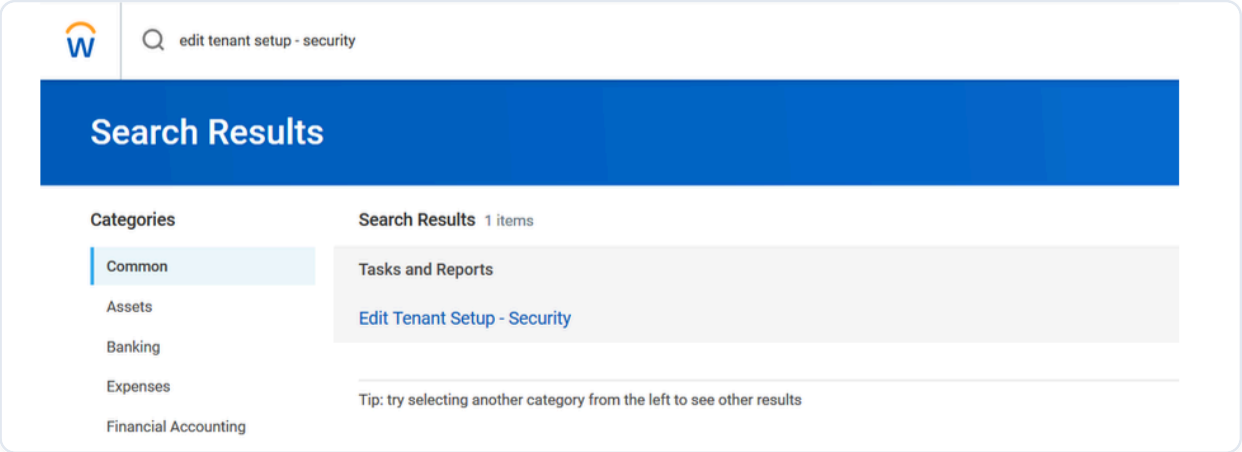
以下部分提供了有关配置 Workday 的更多信息。

Citrix Gateway SaaS 应用程序

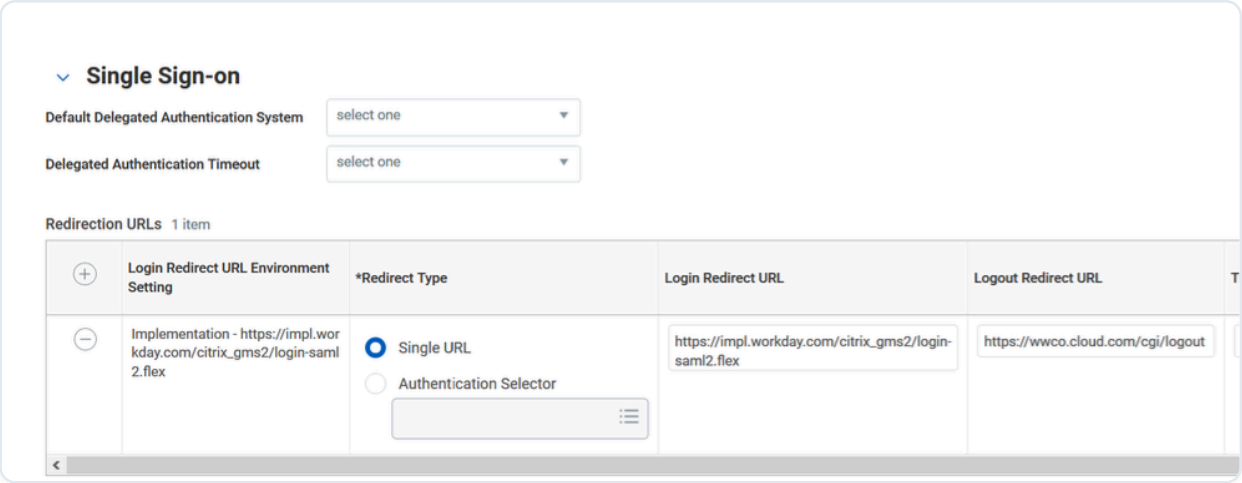
用户可以使用其企业凭据安全地登录 Workday。

要通过 SAML 为 SSO 配置 Workday，请执行以下操作：

1. 以管理员身份登录 Workday。
2. 导航到 **编辑租户设置 - 安全**，然后单击 **编辑租户设置**。

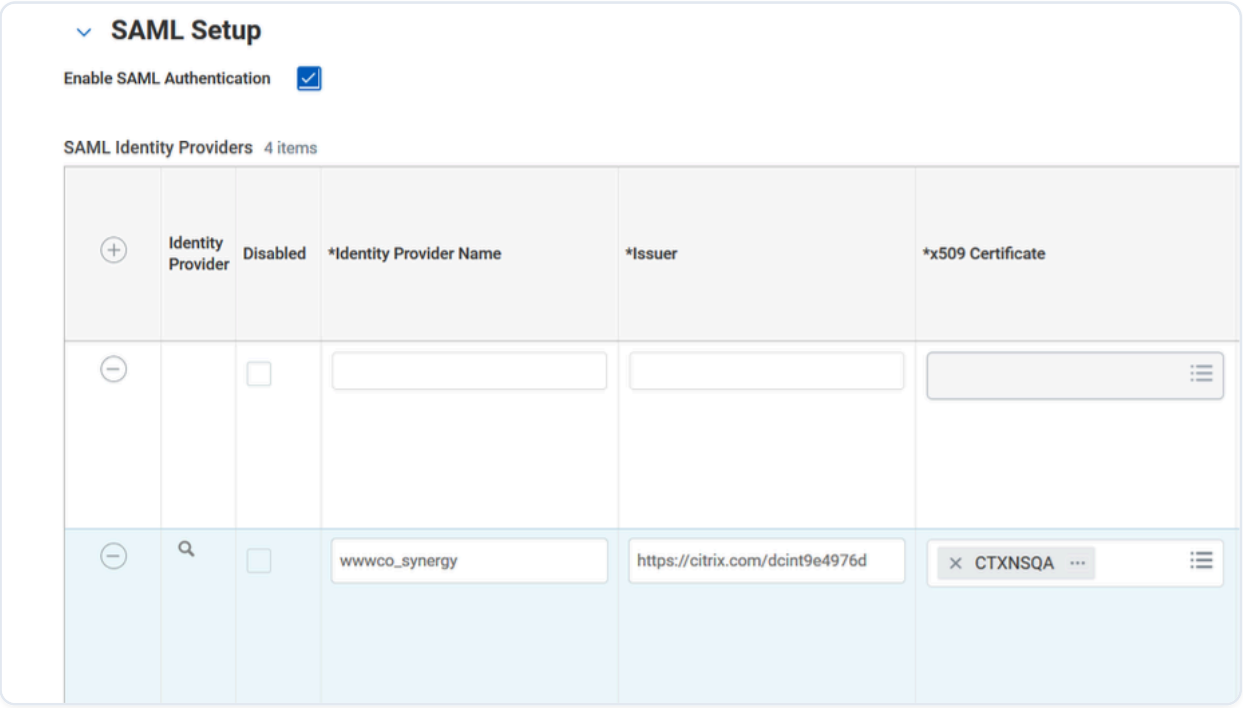


3. 单击 **单一登录**。

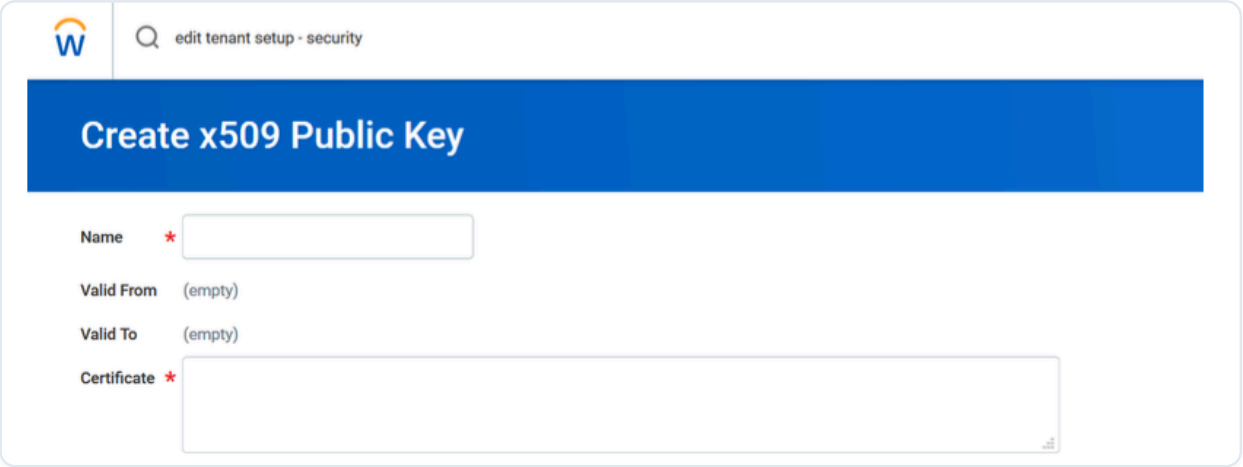


4. 单击“重定向 URL”表中的加号图标。
5. 在 **登录重定向 URL** 中，输入格式为 `https://impl.workday.com/<customer>/login-saml2.flex` 的 URL。
6. 单击 **启用 SAML 身份验证**。

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



7. 单击 SAML 身份提供程序下的加号 (+) 图标以添加一行，并指定以下信息：
   a. **身份提供商名称** - 输入 Citrix Gateway。
   b. **颁发者** - 输入一个唯一的颁发者名称。
8. 在 **x509 证书**中，单击 X509 证书图标，然后单击 **创建 x509 公钥**。
9. 从 Citrix Cloud 向导下载证书 (**Citrix Gateway 服务 > 添加 Web/SaaS 应用程序 > 单点登录 > 证书**)。



10. 复制证书中从 ——BEGIN CERTIFICATE—— 到 ——ENDCERTIFICATE 的文本，并将证书粘贴到“证书”字段中。
11. 单击 **确定**。

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

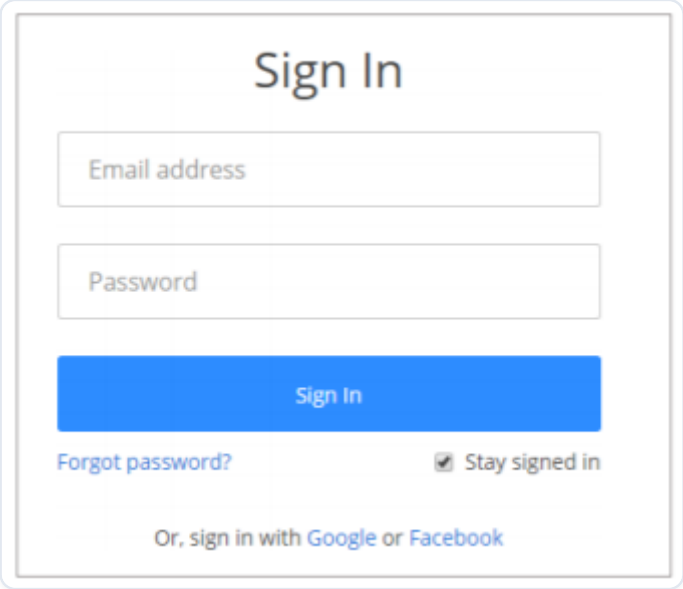
配置 Zoom

以下部分提供了有关配置 Zoom 的更多信息。

Citrix Gateway SaaS 应用程序

为 SSO 配置 Zoom 使管理员能够使用 NetScaler 管理其用户。 用户可以使用其企业凭据安全登录 Zoom。

1. 在浏览器中，键入 `https://zoom.us/signin`，然后按 Enter 键。
2. 登录您的 Zoom 帐户



3. 在“**我的个人资料**”页面上，在左侧窗格的“**高级**”部分下，单击“**单点登录**”。



4. 在 SAML 选项卡中，复制“自定义 URL”框中显示的 URL。NetScaler 配置需要此 URL。

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

5. 在“登录页面 URL”框中，输入您的 NetScaler 应用程序的 IdP URL：`https://<NetscalerGateway FQDN>/saml/login`
6. 在“注销页面 URL”框中，输入 https:< NetScaler Gateway FQDN >.com/cgi/tmlogout。
7. 在“身份提供商证书”框中，您必须粘贴身份提供商证书。
8. 要上传您的 IdP 证书，请执行以下操作：
   - 使用 PuTTY 远程访问您的 NetScaler 实例。
   - 导航到 /nsconfig/ssl 文件夹 (cd/nsconfig/ssl) 并按 Enter 键。
   - 键入 cat certifcate-name.pem 并按 Enter 键。

     注意： 这是您的 SAML IdP 签名证书。
   - 复制 -----BEGIN CERTIFICATE----- 和 -----ENDCERTIFICATE----- 之间的文本

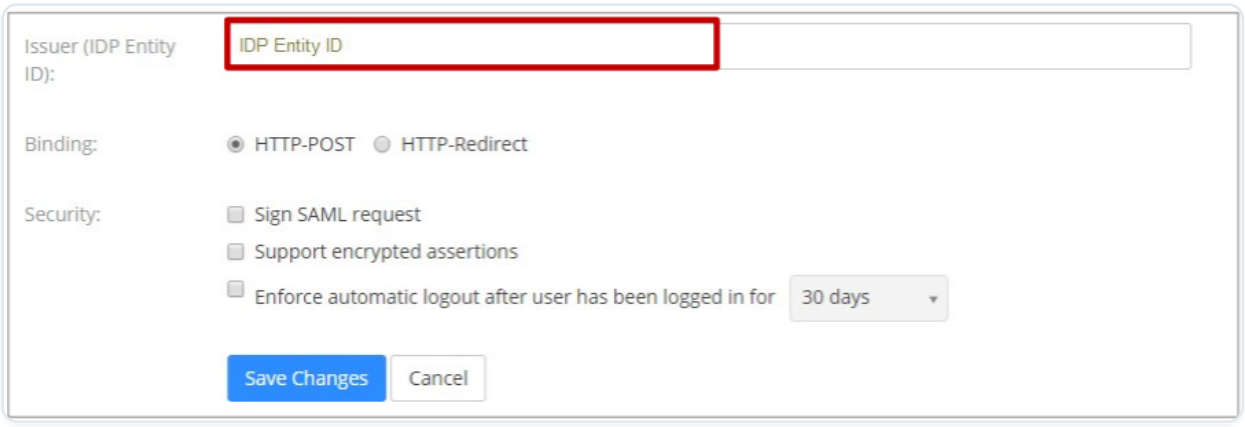


9. 复制服务提供商 (SP) 实体 ID 框中显示的 URL。



10. 在颁发者 (IdP 实体 ID) 框中，键入唯一的颁发者 ID，然后单击 SaveChanges。

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



基于访问模式的策略实施

基于访问模式的策略实施允许管理员限制用户连接应用程序的方式。连接可以通过基于浏览器的客户端或 Citrix Secure Access 客户端进行。以前，Secure Private Access 无法根据客户端发起会话的方式来限制访问。访问模式增加了此功能。

例如，管理员可以配置 SSH 和 RDP 应用程序只能通过浏览器（例如 Chrome Enterprise Premium）访问，而不能通过 Citrix Secure Access 客户端进行隧道连接。这确保了基于浏览器的安全控制始终适用。

注意：

访问模式仅是一种限制条件。它可以缩小访问范围，但不能自行授予访问权限。策略中的所有其他条件仍将进行评估。

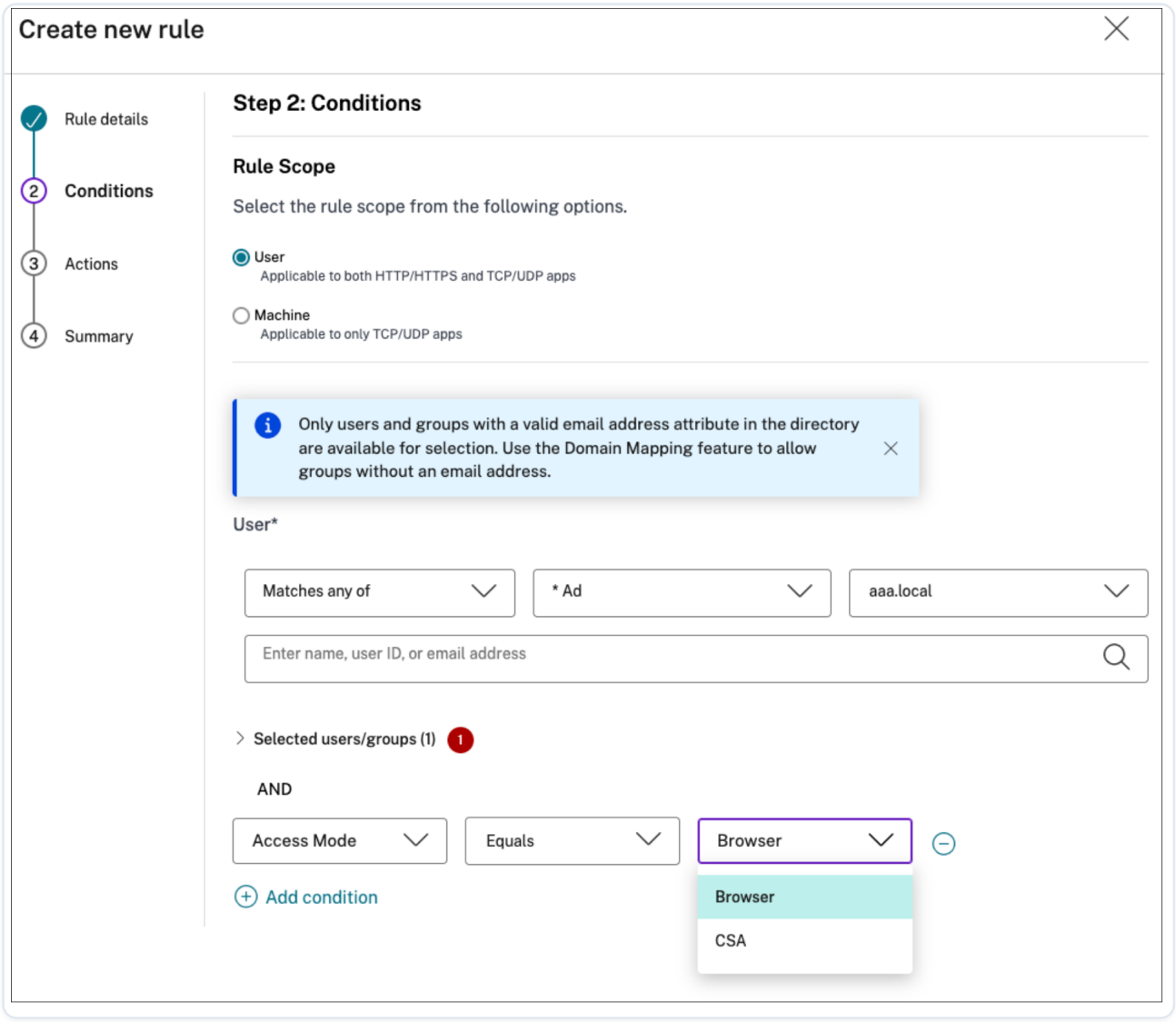
工作原理

访问模式在 Secure Private Access 管理控制台中配置，可以添加到三种策略类型中的任何一种规则中。

- 自适应访问策略
- 会话策略
- 浏览器策略

下图显示了一个示例访问策略规则条件。

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



最终用户体验

根据访问模式，应用程序的枚举和启动要么被允许，要么被限制。

- **匹配客户端** — 应用程序被枚举并正常启动。
- **不匹配的客户端** — 在枚举期间，应用程序不会显示在应用程序列表中，并且启动尝试被阻止。用户将被发送到标准的访问拒绝页面。不会引入新的拒绝消息。
- **无法确定的会话** — 当无法确定访问模式时（例如，某些移动安全访问会话），访问模式条件将被跳过，并且会话不受影响。所有其他条件仍然适用。

支持服务器到客户端连接 - 预览

在传统的客户端-服务器设置中，远程用户可以使用 HTTP、TCP 和 UDP 连接访问客户资源位置中的资源。然而，在某些场景中，服务器或后端系统需要与远程客户端设备（例如笔记本电脑、智能手机、平板电脑）发起连接，以执行推送配置、远程协助、应用程序访问或应用程序安装等任务，

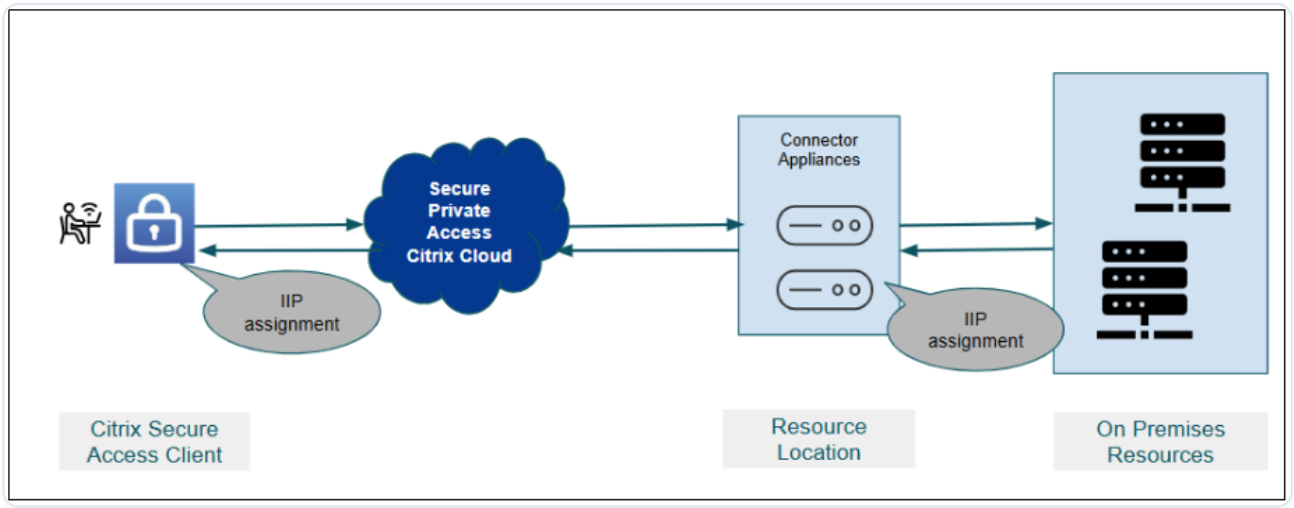
© 1997–2026 Citrix Systems, Inc. All rights reserved.

同时保护用户隐私和安全。Secure Private Access 支持服务器到客户端连接，其中客户资源位置中的服务器可以与远程客户端建立 TCP/UDP 连接。

- 为了启用服务器到客户端连接，Secure Private Access 引入了服务器到客户端应用程序。此应用程序可以配置客户端详细信息（端口、协议）和后端服务器的 IP CIDR 范围。
- 创建服务器到客户端应用程序类型后，必须为这些应用程序配置适当的访问策略，以启用服务器到客户端连接。

服务器到客户端连接的工作原理

下图显示了一个服务器到客户端连接架构示例。



以下步骤说明了服务器到客户端连接工作流：

1. 当用户登录到 Citrix Secure Access™ 客户端时，用户会从指定的客户端内部 IP 地址池中分配到一个内部 IP 地址。此分配基于 IP 地址池配置中配置的资源位置、IP CIDR 和用户上下文。
2. 然后，此分配的 IP 地址将与配置的资源位置和 IP 池中的特定连接器设备关联。此连接器设备拥有并管理与此 IP 地址相关的连接，用于后端客户资源位置。
3. 后端服务器使用分配的客户端内部 IP 地址，通过服务器到客户端应用程序配置中指定的客户端应用程序端口，向远程客户端发起 TCP/UDP 连接。
4. 连接器与 Secure Private Access 通信，以与客户端建立连接。
5. Secure Private Access 验证后端服务器是否已在服务器到客户端应用程序中配置，然后评估相关的访问策略，以确定是允许还是阻止访问客户端计算机。
6. 如果策略允许访问，则 Secure Private Access 连接到远程客户端计算机。如果客户端计算机已加入域，则该计算机的 FQDN 将注册到 IIP 地址。可以通过 FQDN 或内部 IP 地址访问该计算机。
7. 当用户注销时，分配的内部 IP 地址将从连接器设备和活动会话中释放。如果同一用户在 15 天内再次登录，用户将获得相同的 IP 地址，否则该地址将被释放供其他用户使用。

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

创建服务器到客户端应用程序

以下部分提供了有关创建服务器到客户端应用程序的详细信息。

先决条件

- 客户端内部 IP 地址池已创建。IP 地址池对于为用户及其关联设备分配唯一 IP 地址至关重要。有关详细信息，请参阅客户端内部 IP 地址池。
- 客户管理员必须为资源位置网络分配一个空闲的内网 IP CIDR 子网。此 IP CIDR 不得与其他资源 IP 地址冲突。
- 客户管理员必须确定哪些组/上下文用户从哪个资源位置分配内网 IP 地址。建议保持用户与 IP 地址的比例为 1:3。也就是说，如果登录用户数为 1000，建议在客户端 IP 池中分配 3000 个 IP 地址。
- 空闲的 IIP 子网和连接器的主 IP 地址必须属于同一网络和子网。
- 必须在资源位置之间保持互连，以允许其他位置（未在 IP 池中配置）的服务器连接到客户端。
- 确保您使用的 Citrix Secure Access 客户端版本支持服务器到客户端应用程序。
  - Windows 24.11.1.17 及更高版本
  - macOS 25.01.1 及更高版本
  - Linux 25.2.2 及更高版本

执行以下步骤配置服务器到客户端 TCP/UDP 应用程序

1. 登录 Citrix 云 并选择 **安全私有访问**。
2. 单击 **应用程序 > 应用配置**，然后单击 **添加应用**。
3. 在“**选择模板**”部分，单击“**跳过**”。模板仅适用于 SaaS 应用程序。

   创建客户端-服务器应用程序(/en-us/citrix-secure-private-access/media/spa-server-client-app-details1.png)
4. 选择位置“**在我的公司网络中**”。
5. 输入以下详细信息：
   - “**应用程序类型**” – 选择“**TCP/UDP - 服务器到客户端**”。
   - “**应用程序名称**” – 应用程序的名称。
   - “**应用程序描述**” – 您正在添加的应用程序的描述。此字段是可选的。
   - “**服务器**” - 可与客户端计算机建立连接的后端服务器的 IP 地址范围。这可确保只有 IP 地址在此范围内的服务器才能访问客户端的端口。

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

- “**端口**” – 后端服务器可发起连接的客户端计算机的端口号。
- “**协议**” – TCP 或 UDP。

6. 单击“**添加**”以添加更多服务器和端口。
7. 单击“**保存**”。应用程序将添加到“**应用程序配置**”页面。

配置应用程序后，您可以从“应用程序”页面编辑或删除应用程序。为此，请单击应用程序行中的省略号按钮并相应地选择操作。

创建服务器到客户端应用程序后，根据要求创建访问策略。

“

注意：

”.

所有现有的访问策略都支持服务器到客户端应用程序。服务器到客户端的访问权限仅授予那些其上下文在配置的访问策略中被评估为“允许”的用户。

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