Citrix Cloud™

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

Contents

思杰云™ 36

试用 Citrix Cloud 36

全新现代 Citrix Cloud™ 主页和统一导航体验 36

主要功能 37

服务访问 38

近期活动 38

快速链接 39

平台路线图 40

即将举行的活动 40

资源 40

反馈 41

Citrix Cloud 服务文档 41

架构和部署资源 41

教育资源 41

Citrix Cloud™ 中的新增功能 42

2026 年 5 月 42

2026 年 4 月 42

2026 年 1 月 42

2024 年 12 月 42

2024 年 9 月 42

2024 年 6 月 43

2024 年 4 月 43

2024 年 3 月 43

2024 年 1 月 43

服务级别协议 43

各项服务的可用性衡量标准 45

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

服务承诺和补救措施 46
第三方通知 46
如何获取帮助和支持 48
创建帐户 48
登录 Citrix 网站和 Citrix Cloud 48
我无法设置 MFA，或者在登录 Citrix 帐户时无法通过 MFA 进行身份验证 48
如何查找我的 Citrix 帐户用户名或重置我的 Citrix 密码? 49
我无法登录 Citrix Cloud 49
Citrix 电子邮件未出现在我的收件箱中 50
Citrix 和 Citrix Cloud 帐户的多重身份验证 50
帐户恢复 51
更新您的 MFA 设置 52
更改密码 53
云服务运行状况 54
Citrix Cloud 支持论坛 54
支持文章和文档 54
Citrix 支持知识中心 54
Citrix 技术专区 55
用户帮助中心 55
如何在线提交客户服务案例 55
通过实时支持提交离线案例 59
Citrix Cloud™ 服务运行状况 59
查看运行状况和维护状态 61
查看服务事件详细信息 62
事件通知频率 63
订阅通知 64
订阅某个区域中的特定服务 64
订阅特定服务组 66

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

取消订阅通知 66
更改服务通知 68
系统和连接要求 69
系统要求 69
支持的 Web 浏览器 69
传输层安全性要求 69
Citrix Cloud 管理控制台 70
代理配置 70
防火墙配置 70
控制台通知 70
会话超时 71
可配置的控制台不活动超时 71
许可证服务器与 Citrix Cloud 的连接 72
Citrix 云连接器™ 72
Cloud Connector 常见服务连接要求 72
Cloud Connector 允许的 FQDN 73
本地主机缓存（高可用性服务） 73
自适应身份验证 73
连接器允许列表 API 74
网关服务存在点 76
证书验证 76
SSL 解密 76
适用于云服务的 Citrix Connector™ 设备 76
网络要求 77
Citrix Analytics 服务连接 77
NetScaler® Console 服务连接 77
Citrix DaaS 连接 77
Cloud Connectors 到 DaaS 的连接 77

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

连接到 DaaS 管理控制台 78

Citrix DaaS 远程 PowerShell SDK 78

使用 Rendezvous 协议时的 VDA 连接 79

本地主机缓存要求 79

VDA 升级要求 79

Endpoint Management 服务连接 80

Citrix Gateway 服务连接 80

Cloud Connector 连接到 Citrix Gateway 服务 80

客户端连接到 Citrix Gateway Service 81

SD-WAN Orchestrator 服务连接 81

远程浏览器隔离（原安全浏览器）服务 81

Cloud Connector 连接到远程浏览器隔离服务 81

连接到管理控制台 81

客户端连接到 Citrix Secure Private Access™ 82

客户端连接到全局应用配置服务 82

最终用户与应用商店的连接 82

应用商店 URL 82

身份验证 82

存储图形界面资产 83

个性化、通知和功能发布 83

品牌图片 84

个人资料图片 84

应用程序图标 85

潘多 85

Citrix 分析服务 85

其他服务 85

Citrix 联合身份验证服务 (FAS) 85

工作区环境管理™ 服务连接 86

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

规划您的部署 87
服务试用和订阅 87
区域和服务存在 87
部署资源 87
迁移资源 87
更多信息 88
Citrix Cloud™ 服务试用 88
服务试用概述 88
请求服务试用 89
服务试用期 89
购买服务订阅 89
适用于 Azure 的 Citrix DaaS Standard 89
请求服务演示 90
请求服务试用 90
购买 Citrix Cloud 服务 90
更多信息 91
延长 Citrix Cloud™ 服务订阅 91
到期前 91
到期后：服务阻止和数据保留 92
客户管理的 Azure 订阅 92
购买服务扩展 92
地理考量 93
选择区域 93
每个区域的服务部署情况 94
使用 Console Advisory Connect 低接触式载入 NetScaler Console 实例 98
Endpoint Management 服务位置 98
Secure Private Access 服务接入点 98
Pendo 数据驻留和区域注意事项 98

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

Citrix 的其他云平台 99
Citrix Cloud 政府版 99
Citrix Cloud 日本 99
Citrix Cloud™ 平台安全部署指南 99
服务的技术安全概述 99
管理员指南 100
密码合规性 100
加密和密钥管理 101
数据主权 101
安全问题洞察 102
Citrix 云连接器™ 102
安装云连接器 102
配置云连接器 102
登录到托管 Cloud Connector 的计算机 102
在 Cloud Connector 机器上安装其他软件 103
入站和出站端口配置 103
监视出站通信 104
查看 Cloud Connector 日志 104
SSL/TLS 配置 105
安全合规性 105
适用于云服务的 Citrix Connector™ 设备 105
安装 Connector 设备 105
登录到托管 Connector 设备的主机管理程序 106
入站和出站端口配置 106
监视出站通信 107
查看 Connector Appliance 日志 107
SSL/TLS 配置 107
安全合规性 108

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

处理受损帐户的指南 108

适用于 Citrix DaaS™ 的本地 StoreFront™ 身份验证参考架构 108

维护本地 StoreFront 的原因 108

作为资源域的父子域 109

连接工作流 109

外部信任域到资源域 110

连接工作流 111

林信任/快捷方式信任到资源域 111

创建 Citrix Cloud™ 帐户 112

Citrix 新客户的注册流程 112

什么是 Citrix 帐户? 112

什么是 OrgID? 112

什么是 Citrix Cloud 帐户? 113

多重身份验证 114

步骤 1：访问 Citrix Cloud 网站 114

如果帐户已在使用中，会发生什么情况? 115

步骤 2：设置多重身份验证 115

电子邮件作为身份验证方法 116

MFA 要求 116

注册多重身份验证 116

管理您的MFA注册 119

步骤3：验证您的OrgID 119

后续步骤 121

更多信息 121

验证您的 Citrix Cloud™ 电子邮件 122

常见问题 122

我多久会被要求验证一次? 122

我的帐户是否发生了什么问题? 122

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

我没有收到验证电子邮件。我该怎么办? 122

联系 Citrix 支持 123

连接到 Citrix Cloud™ 124

资源位置 124

资源位置部署示例 124

查看和管理资源位置 124

创建资源位置 125

资源类型 126

使用 Citrix Cloud Connector 的服务 126

使用 Connector Appliance 的服务 127

资源位置限制 127

命名限制 127

主资源位置 128

网关 128

思杰云连接器™ 128

需要 Cloud Connector 的服务 129

云连接器功能 129

云连接器通信 129

Cloud Connector 可用性和负载管理 129

在何处获取 Cloud Connector 130

我需要多少个 Cloud Connector? 130

在何处安装 Cloud Connector 130

Citrix Cloud Connector 系统要求 131

主机资源要求 131

操作系统 131

.NET 要求 131

服务器要求 132

Windows 更新指南 132

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

防病毒配置 133
证书验证要求 133
Active Directory 的要求 137
网络要求 138
联邦信息处理标准 (FIPS) 支持 138
Citrix Cloud Connector™ 技术详细信息 138
系统要求 138
Cloud Connector 已安装的服务 138
Active Directory 中 Cloud Connector 的部署方案 140
查看 Cloud Connector 的运行状况 143
故障排除 145
云连接器代理和防火墙配置 145
连接要求 145
检查 Cloud Connector 连接 146
安装程序 146
运行时服务 146
云连接器安装 147
安装前需要查看的信息 148
部署后指南 148
交互式安装 149
命令行安装 154
HTTPS 配置 155
后续步骤 157
安装问题疑难解答 157
Cloud Connector 高级连接检查 159
Cloud Connector 安装程序高级连接检查 159
Citrix Cloud Services 连接测试工具 161
数据包捕获 163

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

Cloud Connector 高级健康检查 - 已弃用 163
查看 Connector 健康检查数据 164
查看服务详细信息 165
连接器通知 165
云连接器 166
Citrix Cloud Connector™ 的日志收集 168
步骤 1：重现问题 168
步骤 2：收集 CDF 跟踪 168
步骤 3：将数据提交给 Citrix 169
选择主资源位置 170
选择主资源位置 170
选择不同的主资源位置 171
重置主资源位置 171
适用于云服务的连接器设备 171
连接器设备功能 171
Connector Appliance 可用性和负载管理 172
连接器设备 更新 172
连接器设备 通信 173
Internet 连接要求 174
网络要求 174
系统要求 174
获取连接器设备 175
在您的虚拟机管理程序上安装 Connector Appliance 177
XenServer 177
威睿 ESXi 178
海伯-V 179
诺坦尼克斯 AHV 181
微软 Azure 182

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

AWS 184

Google Cloud 平台 191

将您的 Connector Appliance 注册到 Citrix Cloud 194

注册您的连接器设备后 199

Connector Appliance 连接性检查 199

生成诊断报告 200

验证您的网络连接 201

网络连接探测工具 201

将活动目录连接到 Citrix Cloud 201

验证您的 Kerberos 配置 201

您的连接器设备的网络设置 203

在连接器设备管理页面上配置网络设置 204

使用 Connector Appliance 控制台设置网络配置 204

更改 Connector Appliance 的管理员用户密码 205

替换服务器证书 206

查看当前服务器证书 206

替换服务器证书 207

替换证书的步骤 208

证书格式要求 209

错误处理 209

恢复为自签名证书 211

使用连接器设备的活动目录 211

要求 211

支持的 Active Directory 功能级别 212

使用连接器设备将 Active Directory 域连接到 Citrix Cloud 213

后续步骤 219

查看您的 Active Directory 配置 219

从连接器设备中移除活动目录域 219

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

更改已加入的 Active Directory 域的域控制器首选项 220

设置林首选连接器类型 220

用于将连接器设备与 Active Directory 结合使用的部署场景 221

连接器设备网络连接探测器 222

指定代理 223

允许的网络目标 224

数据包捕获 224

网络探测结果 225

解释基于 HTTP 的探测结果 225

连接器更新 226

首选时间 226

首选星期几 226

8 天等待期示例 227

13 天等待期的示例 227

更新通知和按需更新 227

选择更新计划 227

重新启动更新 228

延迟更新 229

未计划的更新 229

比较 Cloud Connector 版本 229

解决更新失败问题 230

身份和访问管理 231

身份提供程序 231

Citrix 身份提供程序 231

删除 Citrix 身份提供程序 232

Citrix 联邦身份验证服务 232

管理员 233

多重身份验证 233

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

添加新管理员 233

重置密码 234

删除管理员 234

最终用户 234

管理最终用户使用情况 235

主要资源位置 235

更多信息 235

管理管理员对 Citrix Cloud 的访问 236

添加新管理员 236

邀请单个管理员 236

邀请管理员 237

重新发送邀请 239

使用新的登录链接重新发送邀请 239

接受管理员邀请 239

添加管理员组 239

批准加入 Citrix Cloud 的请求 240

更改您的电子邮件地址 240

修改管理员权限 241

控制台权限 244

管理您的主要 MFA 方法 244

更改 MFA 设备 245

更改您的 MFA 方法 247

管理您的 MFA 恢复方法 247

添加或更改您的恢复电子邮件 248

生成新的备用代码 248

更改您的恢复电话号码 249

管理管理员组 249

AD 先决条件 249

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

Microsoft Entra ID 先决条件 249
验证您与 Microsoft Entra ID 的连接 250
重新连接到 Microsoft Entra ID 250
Google 云身份 251
支持的权限 251
限制 251
具有 Citrix®、AD、Microsoft Entra ID 和 Google Cloud 身份的管理员的最终权限 252
管理员的登录体验 254
已知问题 254
限制 255
多个组对应用程序性能的影响 255
多个组对身份验证的影响 255
由于分配的角色/范围对过多，添加组失败 255
将管理员组添加到 Citrix Cloud 255
修改管理员组的服务权限 255
删除管理员组 256
在多个 Citrix Cloud 帐户之间切换 256
链接 Citrix Cloud 帐户 258
取消链接 Citrix Cloud 帐户 259
将本地产品注册到 Citrix Cloud™ 260
注册产品 261
移除产品注册 261
条件身份验证 262
常见用例 262
先决条件 262
多 IdP 262
配置条件身份验证 263
条件身份验证概念 265

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

条件身份验证配置文件 265

条件身份验证策略 265

条件身份验证预身份验证页面 266

登录自动填充 266

用户名提示文本 268

策略条件类型 269

商店 URL 270

使用商店 URL 或自定义 URL 访问商店 270

AD 用户组成员身份 272

UPN 后缀 273

域向下兼容登录名 273

网络位置名称 274

为条件身份验证配置文件设置自定义错误消息 277

使用 Citrix 监视器集成进行故障排除 279

云原生条件身份验证与基于 NetScaler 的自适应身份验证的比较 280

已知问题和限制 281

身份提供程序 282

将活动目录连接到 Citrix Cloud™ 282

连接活动目录 282

通过连接器设备连接 Active Directory 282

通过云连接器连接 Active Directory 283

将您的 Active Directory 连接到 Citrix Cloud 283

启用 Active Directory 加令牌身份验证 284

更多信息 285

建立 微软 Entra ID 与 Citrix Cloud™ 的连接 286

Microsoft Entra ID 应用程序和权限 286

使用多个 Citrix Cloud 帐户进行身份验证 286

准备您的 活动目录 和 微软 Entra ID 287

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

使用 Microsoft Entra ID Connect 同步帐户 287

将 思杰云 连接到 Microsoft Entra 标识 287

备用连接方法 288

从 Microsoft Entra ID 将管理员添加到 Citrix Cloud 288

使用 Microsoft Entra 标识 登录 思杰云 289

为应用商店启用 Microsoft Entra ID 身份验证 289

启用高级 Microsoft Entra ID 功能 289

重新连接到 Microsoft Entra ID 以使用更新的应用程序 289

要求 290

重新连接 Microsoft Entra ID 290

Citrix Cloud™ 的 微软 Entra ID 权限 291

企业应用程序 291

权限 292

商店最终用户登录 293

Microsoft Entra ID 与 Citrix Cloud 之间的默认连接 294

管理员邀请和登录 294

Microsoft Entra ID 与 Citrix Cloud（含 Endpoint Management）之间的默认连接 295

Microsoft Entra ID 与 Citrix Cloud 和 Endpoint Management 之间的旧版连接 295

将本地 Citrix Gateway 作为身份提供程序连接到 Citrix Cloud™ 296

支持的版本 296

先决条件 296

云连接器 296

活动目录 297

要求 298

Citrix Gateway 高级策略 298

签名证书 298

时钟同步 298

任务概述 298

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

为最终用户启用 Citrix Gateway 身份验证 298
故障排除 301
全局编录服务器 301
使用 Kerberos 或 IdP 链进行单点登录的 AD 搜索 301
用于多重身份验证的默认密码 303
更多信息 303
将 Google Cloud Identity 作为身份提供程序连接到 Citrix Cloud™ 303
已加入域和未加入域配置的要求 303
使用多个 Citrix Cloud 帐户进行身份验证 305
准备活动目录和 Citrix Cloud 连接器 305
将活动目录与 Google Cloud 身份同步 305
将您的 AD 与 Google Cloud 同步 306
创建服务帐户 307
创建服务帐号密钥 307
配置域范围委派 307
添加只读 API 用户帐户 308
将谷歌云身份连接到 Citrix 云 309
将管理员添加到 Citrix Cloud 309
为商店身份验证启用 Google Cloud Identity 309
将 Okta 作为身份提供商连接到 Citrix Cloud™ 310
先决条件 310
云连接器或连接器设备 310
Okta 域 310
Okta OIDC Web 应用程序 311
应用商店 URL 311
Okta API 令牌 311
使用 Okta AD 代理将 Active Directory 帐户同步到 Okta 312
创建 Okta OIDC Web 应用程序集成 313

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

配置 Okta OIDC Web 应用程序 314
创建 Okta API 令牌 319
将 Citrix Cloud 连接到您的 Okta 组织 319
为应用商店启用 Okta 身份验证 320
更多信息 320
故障排除 320
将 SAML 作为身份提供程序连接到 Citrix Cloud™ 323
关于本文 323
Citrix SAML 登录用例 323
为您的用例选择正确的 SAML 流程 324
支持的 SAML 提供程序 324
支持范围限定的实体 ID 325
管理员使用 SAML 2.0 进行身份验证 325
使用现有 SAML 连接进行管理员身份验证 325
设置新 SAML 连接的任务概述 325
为 Citrix Cloud 管理员使用现有 SAML 连接的任务概述 326
创建和映射自定义 SAML 属性 326
配置管理员登录 URL 328
配置 SAML 提供程序元数据 328
创建 SAML 连接器应用程序 328
将 SAML 提供程序元数据添加到 Citrix Cloud 329
从 AD 将管理员添加到 Citrix Cloud 332
为应用商店启用 SAML 身份验证 332
在身份和访问管理中克隆现有 SAML 连接 332
先决条件 333
云连接器 334
Active Directory (默认 AD 身份 SAML 流程) 334
EntraID 目录 (EntraID 身份 SAML 流程) 334

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

SAML 与 Active Directory 集成 335
如何选择 SAML 绑定机制? 336
SAML 绑定支持 336
服务提供商发起的 SSO 与 身份提供商发起的 SSO 337
身份提供商发起的 SSO 可以与商店或 Citrix Cloud 一起使用? 337
将 SAML 提供程序直接连接到 Citrix Cloud 与 IDP 链 337
IDP 链是否支持 SAML 登录到商店或 Citrix Cloud? 337
IDP 链示例 337
如果我正在使用 IDP 链，在调试 SAML 问题时能否获得 Citrix 的协助和支持? 338
是否应尽可能避免 IDP 链? 338
SAML 注销注意事项 338
商店会话不活动超时行为 339
使用元数据 URL 模式创建 SAML 连接 340
为什么元数据 URL 模式是创建 Citrix Cloud SAML 连接的推荐方式? 341
当使用元数据 URL 模式时，Citrix Cloud 如何处理 IdP 证书轮换? 341
使用您的 IdP 元数据 URL 配置 Citrix Cloud SAML 连接 341
使用元数据文件模式创建 SAML 连接 344
元数据文件模式与元数据 URL 模式有何不同? 344
元数据文件模式为何不如元数据 URL 模式有用? 345
使用 IdP 元数据文件配置 Citrix Cloud SAML 连接 345
使用手动模式创建 SAML 连接 349
故障排除 353
当我开启 SAML 支持案例时，需要向 Citrix 支持和工程团队提供哪些信息? 353
为 Citrix 支持和工程团队捕获 SAML 跟踪 354
如何从我的浏览器收集 HAR 文件并发送给 Citrix 支持和工程团队? 355
有用的第三方 SAML 调试工具 355
属性错误 356
意外错误 357

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

在 Citrix Cloud™ 中配置具有范围实体 ID 的 SAML 应用程序 357
什么是实体 ID? 358
按区域划分的通用和范围限定的 SP 实体 ID 359
为新的和现有的 SAML 连接生成唯一的 SP 实体 ID 359
关于范围限定实体 ID 的常见问题 360
受影响的 SAML 提供商 360
受影响的用例 361
使用范围限定的实体 ID 配置主 SAML 连接 362
使用通用实体 ID 配置主 SAML 连接 362
使用 Citrix® StoreFront Cloud 自定义域配置 SAML 连接 362
具有范围限定的实体 ID 的 SAML 提供商配置 364
故障排除 365
使用多个自定义 URL 通过 SAML 登录到应用商店 367
常见问题 368
迁移旧版自定义 URL 和 SAML 配置 372
我需要做什么才能从我当前的 1x SAML 应用程序自定义 URL 解决方案迁移到新的更简单的解决方案? 377
旧版自定义 URL SAML 配置 378
1x SAML 应用程序配置（旧版 SAML 配置） 379
2 个 SAML 应用程序配置（旧版 SAML 配置） 383
更新服务提供商 SAML 签名证书 389
服务提供商签名证书 390
常见问题 390
使用元数据交换自动使用最新的 Citrix Cloud SP SAML 签名证书更新 SAML 提供程序 396
手动使用最新的 Citrix Cloud SP SAML 签名证书更新 SAML 提供程序 397
将替换的 Citrix Cloud SAML 签名证书上传到您的 Microsoft Entra ID SAML 应用程序 401
更新身份提供商 SAML 签名证书 405
常见问题 405

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

高级 SAML 场景以及在 SAML 断言中正确使用 cip_forest 和 cip_domain 419
先决条件 419
常见问题 421
将 ADFS 配置为商店身份验证的 SAML 提供程序 426
先决条件 426
为 Citrix Cloud 配置信赖方信任 426
使用 PowerShell 修改 Citrix Cloud 信赖方信任 431
使用 PowerShell 更新信赖方信任的 SAML 签名设置 432
Citrix Cloud 中的 SAML 配置 433
将 Duo 配置为商店身份验证的 SAML 提供程序 434
先决条件 434
配置 Active Directory 同步到您的 Duo 租户 434
为 SAML 配置 Duo 身份验证代理配置文件 437
配置用于商店的 Duo SAML 应用程序 438
配置 Citrix Cloud SAML 连接 441
Duo SAML 注销行为 442
使用 Entra ID 和 AD 身份进行商店身份验证的 SAML 444
功能范围 444
AD 身份与 Entra ID 身份：最佳选择? 444
配置自定义 Entra ID 企业 SAML 应用程序 445
故障排除 447
配置 Citrix Cloud SAML 连接 448
使用 Entra ID 和 Entra ID 身份进行商店身份验证的 SAML 450
功能范围 450
AD 身份与 Entra ID 身份：最佳选择? 451
更多信息 452
要求 452
配置自定义 Entra ID 企业 SAML 应用程序 453

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

故障排除 458
配置 Citrix Cloud SAML 连接 459
使用 Entra ID 的 SAML，用于访客和 B2B 身份进行商店身份验证 461
先决条件 461
常见问题 461
为外部访客账户配置 Entra ID 中的 B2B SAML 应用程序 466
配置 Citrix Cloud B2B SAML 连接 470
配置 AD 影子帐户资源位置和连接器 471
在后端 AD 林中配置 FAS 471
在 AD 域中配置备用 UPN 后缀 472
在后端 AD 林中配置 AD 影子账户 473
配置来宾 Entra ID 用户 UPN 以匹配 AD 影子帐户 UPN 474
测试 B2B SAML 解决方案 477
B2B SAML 解决方案故障排除 478
配置 Citrix Cloud SAML 连接 479
将 Okta 配置为商店身份验证的 SAML 提供程序 481
先决条件 481
要求 482
为商店身份验证配置 Okta SAML 应用程序 483
配置 Citrix Cloud SAML 连接 488
将本地 PingFederate 服务器配置为商店和 Citrix Cloud™ 的 SAML 提供程序 490
先决条件 490
使用 PingFederate 中的数据存储配置到 AD 域的 Active Directory 连接 491
上传 Citrix Cloud SAML 签名证书 492
上传 Citrix Cloud 元数据 493
在 PingFederate 中配置密码凭据验证器 494
在 PingFederate 中配置 IDP 适配器 496
配置服务提供商连接 (SAML 应用程序) 以用于 Citrix Cloud 或 Workspaces 498

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

配置 Citrix Cloud SAML 连接 508

Citrix Cloud™ 许可 511

企业客户许可 511

本地部署许可 511

Citrix 服务提供商 (CSP) 许可 511

监控云服务的许可证和活动使用情况 512

支持的区域和云服务 514

Citrix DaaS™ 的多类型许可 514

许可证分配 514

许可摘要和详细信息 514

使用趋势和许可证活动 515

释放已分配的许可证 515

常见问题 515

监控 Citrix DaaS (用户/设备) 的许可证和活跃使用情况 516

许可证分配 516

域名截断 517

许可摘要 518

计算分配的许可证和活跃使用情况 519

使用趋势 519

许可证活动 520

释放已分配许可证 521

许可证自动切换 523

监控 Citrix DaaS™ 的许可证和峰值使用情况（并发用户） 523

许可证分配 523

许可摘要 523

使用趋势和许可证活动 525

用户和设备的许可证活动 526

释放许可证 526

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

监控 Citrix DaaS Standard for Azure 的许可证和使用情况 526
思杰 Azure 消费基金（仅限用户/设备） 526
许可证分配 526
域名截断 527
许可摘要 528
使用趋势 529
用户和设备的许可证活动 531
释放用户/设备许可证 532
释放并发用户许可证 534
监控 Endpoint Management 的许可证和活动使用情况 534
许可证分配 534
许可摘要和详细信息 534
使用趋势 534
许可证活动 535
查看注册设备 536
自动释放分配的许可证 536
监控 Gateway 服务带宽使用情况 536
使用情况摘要 537
使用详情 539
使用趋势 540
许可证活动 540
监控 Secure Private Access 的许可证和使用情况 543
许可证分配 543
许可摘要 543
已使用的许可证和带宽 544
使用趋势 544
许可证活动 546
释放已分配的许可证 547

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

监控适用于 Citrix DaaS™ 的 Citrix 管理的 Azure 资源消耗 547
支持的产品 548
消费摘要 548
消费详情 549
使用报告 549
使用趋势和消耗活动 550
释放已分配的许可证 553
监控本地部署的许可证和使用情况 553
支持的产品 553
先决条件 554
连接要求 554
连接到 Citrix Cloud 555
查看本地产品许可证使用情况 555
查看许可证服务器状态 556
许可证服务器状态对许可证使用情况视图的影响 556
许可证使用情况 557
每个许可证服务器的使用情况 557
并发许可模型的峰值许可证使用情况 558
解释许可证使用情况的注意事项 559
删除许可证服务器注册 559
删除使用数据 559
Citrix 服务提供商的许可 560
其他信息 560
开始使用许可证使用情况洞察 561
支持的 Citrix® 产品 561
要求 561
步骤 1：更新 Citrix License Server 561
步骤 2：使用 My Citrix 凭据登录 Citrix Cloud™ 561

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

步骤 3（可选）：通过许可证服务器匿名化用户名 562
步骤 4：使用 License Usage Insights 服务 563
更多详细信息 563
帮助和支持 563
常见问题 564
管理产品使用情况、许可证服务器和通知 564
产品选择 564
客户通知 565
许可证服务器状态 566
上传中包含的许可证服务器信息 566
使用情况收集 567
历史趋势 570
导出使用情况和分配数据 570
使用 API 访问许可数据 570
分销商对 API 的访问权限 570
Citrix 服务提供商的云服务许可证使用情况和报告 571
支持的服务 572
许可证摘要 572
查看和导出每月使用情况 574
客户许可证和使用情况监控（适用于 Citrix DaaS™） 574
许可证分配 575
许可摘要 576
使用趋势 576
已授权用户 577
每月许可证发布 577
查看每月许可证历史记录 577
导出许可证详细信息 577
Citrix Platform Flex 的授权许可 578

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

功能 578

可用服务 578

概念和术语 579

Flex 点数 579

角色 579

服务 585

平台 Flex 积分消耗和报告 585

按服务计算消耗量 585

附加条款 586

管理 Citrix Cloud 587

Citrix Cloud™ 账户管理 587

创建 Citrix Cloud 账户 587

许可证管理 590

许可证分配 590

许可证解除分配 594

已知问题 595

自定义登录页面 596

配置自定义登录页面 597

如何删除 Citrix Cloud™ 帐户并重新加入 598

先决条件 599

步骤 599

网络位置 601

查看网络位置 601

添加网络位置 602

编辑网络位置 603

删除网络位置 604

使用 PowerShell 管理网络位置 604

下载 PowerShell 模块 604

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

创建服务主体 605

配置网络位置 607

修改网络位置 608

删除网络位置 608

示例脚本 608

通知 610

查看通知 610

关闭通知 610

接收电子邮件通知 610

为自己启用电子邮件通知 611

为非管理员启用电子邮件通知 611

修改通知设置 612

修改非管理员的通知 612

禁用电子邮件通知 612

删除非管理员联系人 612

系统日志 613

记录的事件 614

导出事件 615

检索特定时间段的事件 616

SystemLog API 616

数据保留 616

系统日志事件参考 616

生成事件的云组件和服务 616

事件数据说明 617

适用于 Citrix Cloud™ 平台的系统日志事件 618

微软 Entra ID 租户 618

Citrix Cloud 管理员和服务主体 619

Citrix Cloud 服务主体 620

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

Active Directory Plus 令牌的设备重置 621
域管理 622
网络位置 622
资源位置 622
账户名称和徽标更改 623
连接器的系统日志事件 623
连接器注册 623
连接器更新 624
连接器公钥 624
Citrix Cloud™ 中许可的系统日志事件 625
本地许可证服务器 625
云服务许可 625
适用于 Citrix 服务提供商的许可证使用情况洞察 626
云服务和本地产品的许可证使用情况 626
Secure Private Access 的系统日志事件 627
Web 和 SaaS 应用程序 627
用户和组订阅 627
上下文策略 628
应用程序域 629
浏览器扩展设置 630
网站 URL 列表和筛选类别 630
网站筛选类别预设 633
已阻止的网站 URL 列表和筛选类别 633
允许的网站 URL 列表和筛选类别 635
重定向到远程浏览器隔离（以前称为 Secure Browser）网站 URL 列表和筛选类别 637
Citrix® StoreFront Cloud 的系统日志事件 639
商店 URL 639
StoreFront 身份验证 640

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

Citrix 联合身份验证服务 640
收藏夹 641
更改密码 641
长期令牌 642
Web 不活动超时 643
功能发布 643
SDK 和 API 645
服务主体 645
云许可 API 646
SystemLog API 646
资源位置 API 646
服务授权 API 647
通知 API 647
其他服务的 SDK 和 API 647
更多信息 647
Citrix Cloud™ 面向合作伙伴 648
合作伙伴身份识别 648
客户控制板 650
谁可以查看客户控制板? 651
合作伙伴与客户的连接 651
与多个合作伙伴或客户的连接 651
连接通知 651
合作伙伴对服务授权的可见性 652
添加新客户 652
激活已添加的客户 656
将云租户设为多租户 DaaS 客户 656
将云租户设为单租户客户 657
与客户建立连接 660

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

删除合作伙伴或客户连接 662

删除与客户的连接 662

删除与合作伙伴的连接 662

许可趋势 662

带宽使用情况 665

Citrix 服务提供商的客户许可和使用情况 666

合作伙伴对客户通知的可见性 667

Citrix 服务提供商的联合域 668

Citrix 服务提供商的应用商店外观选项 668

云服务 669

Citrix® 服务 669

NetScaler® 服务 670

Virtual Apps and Desktops Essentials 671

Citrix 虚拟应用精简版™ 671

部署架构 671

部署摘要 672

新增功能 673

系统要求 674

微软 Azure 674

思杰云 674

虚拟应用基本版控制台 674

已知问题 674

如何购买服务 675

准备 Azure 订阅 676

链接您的 Azure 订阅 677

准备和上传主映像 678

过程摘要 678

在 Azure 中创建主映像 VM 679

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

在主映像上安装应用程序 680

在主映像上安装 VDA 681

上传主映像 681

在 Virtual Apps Essentials 中准备主映像 682

部署目录、发布应用程序和桌面以及分配最终用户 682

创建目录 683

发布应用程序并为目录分配最终用户 689

测试并共享应用商店链接 693

更新主映像和目录 693

更新主映像 693

使用新映像更新目录 694

更新目录中的 VDA 数量 694

监视计算机状态 694

监视服务 696

会话信息 696

使用情况信息 696

配置文件管理 697

配置用户配置文件管理 697

配置 Microsoft RDS 许可证服务器 698

使用组策略设置配置 RDS 许可证服务器 698

配置 RDS 许可证服务器 698

连接用户 698

店面体验 698

思杰网关服务 699

取消虚拟应用精简版 699

在 Azure 中取消 虚拟应用 Essentials 699

删除由 Virtual Apps Essentials 创建的 Azure 资源 700

合作伙伴资源 700

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

获取帮助 701
更多信息 701
升级到适用于 Azure 的 Citrix DaaS 标准版 701
Citrix 虚拟桌面基础版™ 701
新增功能 702
如何购买虚拟桌面基础版 703
系统要求、先决条件和兼容性 703
微软 Azure 703
思杰云连接器™ 704
思杰云 704
已知问题 704
步骤 1：将您的 Azure 订阅连接到 Virtual Desktops Essentials 705
步骤 2：创建主机连接 705
选项 1：创建连接 706
选项 2：使用现有主机连接 706
步骤 3：创建 Windows 10 桌面池 707
在基础映像上安装 VDA 707
创建存储帐户 708
为 Citrix Virtual Desktops Essentials 创建计算机目录 709
在 Microsoft Azure 中识别映像名称 710
步骤 4：将 Windows 10 桌面分配给您的用户 710
通过 Studio 在交付组中添加或删除用户 711
通过 Studio 更改交付组中的用户设置 711
通过 Citrix Cloud 添加用户访问权限 711
步骤 5：在 Azure 中配置 NetScaler Console VPX（可选） 712
配置 Citrix Gateway 设置以实现安全访问 712
在 Citrix 网关中配置 Citrix 虚拟桌面精简版设置 712
配置 Citrix Gateway 以实现高可用性和负载平衡 712

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

步骤 6：连接用户 713
使用 NetScaler Console VPX 进行远程访问 713
合作伙伴资源 713
升级到适用于 Azure 的 Citrix DaaS Standard 714
微软 CSP 对 Citrix Essentials 的启用 714
新增功能 714
要求 714
过程摘要 714
为客户创建 Citrix Cloud 帐户 715
结果 717
为客户创建 Azure 订阅 717
结果 721
为客户购买 Citrix Essentials 721
Citrix Cloud 文档历史记录 723
index 739
远程浏览器隔离 739
与 Citrix Secure Private Access™ 结合的远程浏览器隔离服务 740
参考文章 740
相关产品中的新增功能 740

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

思杰云™

注意：

Citrix Virtual Apps Essentials 和 Citrix Virtual Desktops Essentials 已达到销售终止 (End of Sales) 和生命周期终止 (End of Life) 阶段。有关详细信息，请参阅 CTX583004。

Citrix Cloud 是一个托管和管理 Citrix 云服务的平台。它通过您选择的任何云或基础设施（本地、公有云、私有云或混合云）上的 连接器 连接到您的资源。它允许您通过单个控制台创建、管理和向最终用户部署包含应用程序和数据的应用商店。

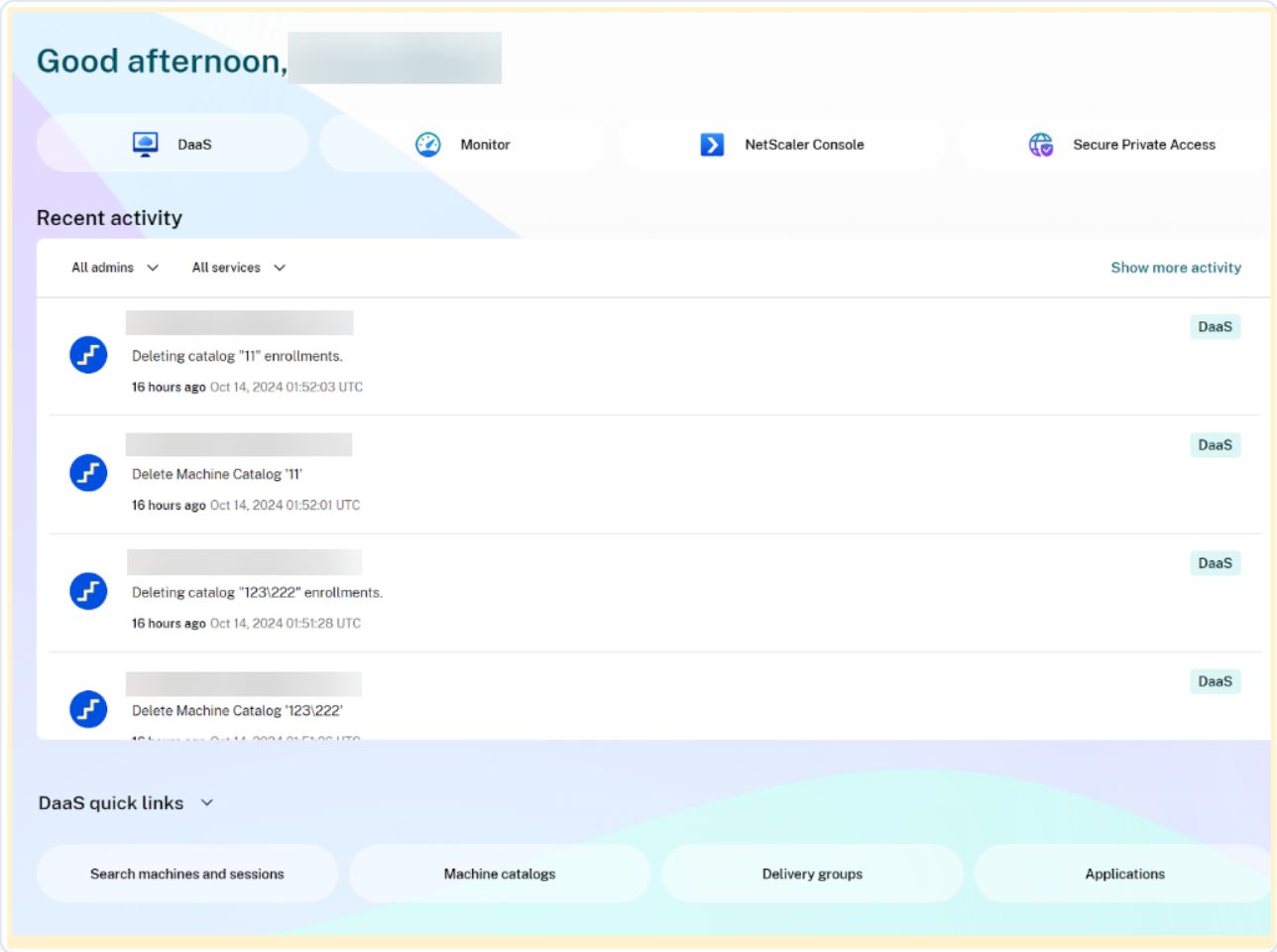
试用 Citrix Cloud

在概念验证中体验一个或多个 Citrix Cloud 服务的完整生产环境。在 注册 Citrix Cloud 后，您可以直接在控制台中请求服务试用。试用期结束后，您可以转换为生产环境，从而保留所有配置。有关详细信息，请参阅 Citrix Cloud 服务试用。

全新现代 Citrix Cloud™ 主页和统一导航体验

随着 Citrix 平台的推出，我们承诺提供一个简化的统一平台，为您提供零信任访问、一流的应用程序和桌面虚拟化以及具有全面安全性的高性能应用程序交付。 作为此承诺的一部分，我们正在推出全新设计的 Citrix Cloud 主页和统一导航体验，以提升管理员管理和使用其环境的方式。

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

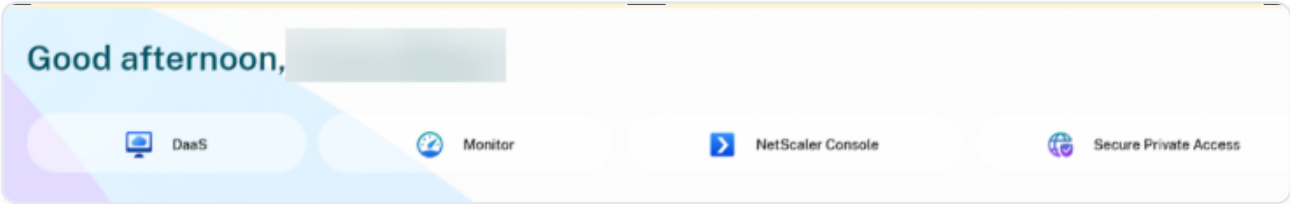


主要功能

- 运营效率
  - 直接访问关键服务
  - 一目了然地查看近期活动
  - 产品内操作的快速链接
- 教育中心
  - Citrix 路线图
  - 即将举行的活动
  - 培训、社区资源和技术文档的快速链接
- 改进的导航
  - 所有 Citrix 解决方案之间一致的外观和体验
  - 带有面包屑和页面路径的简化导航
  - 可自定义的功能，例如固定

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

服务访问



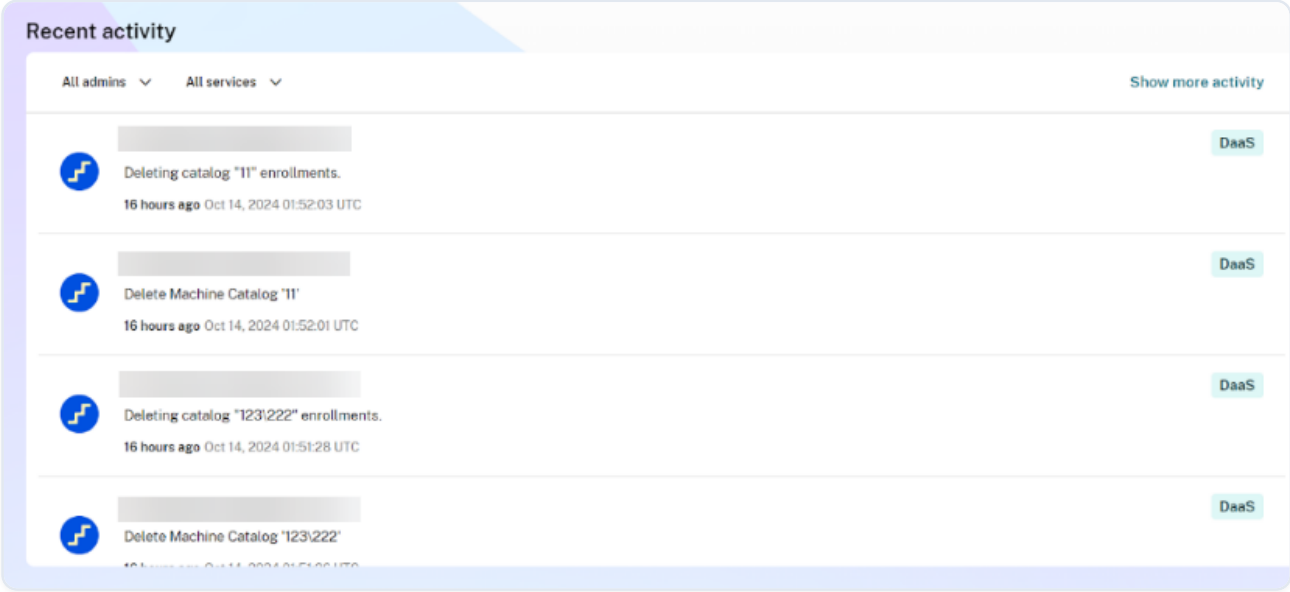
您可以通过这些选项访问所有关键服务。

- DaaS
- 监控
- NetScaler® 控制台
- 安全私有访问

注意：

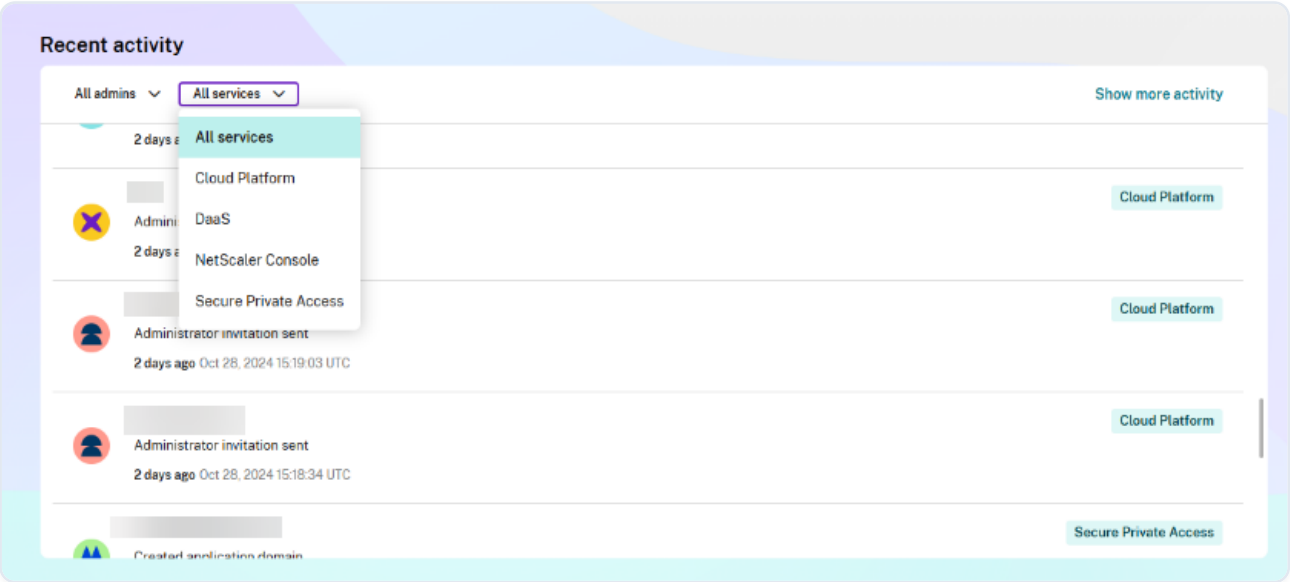
其他服务可以通过左上角的九宫格菜单访问。

近期活动

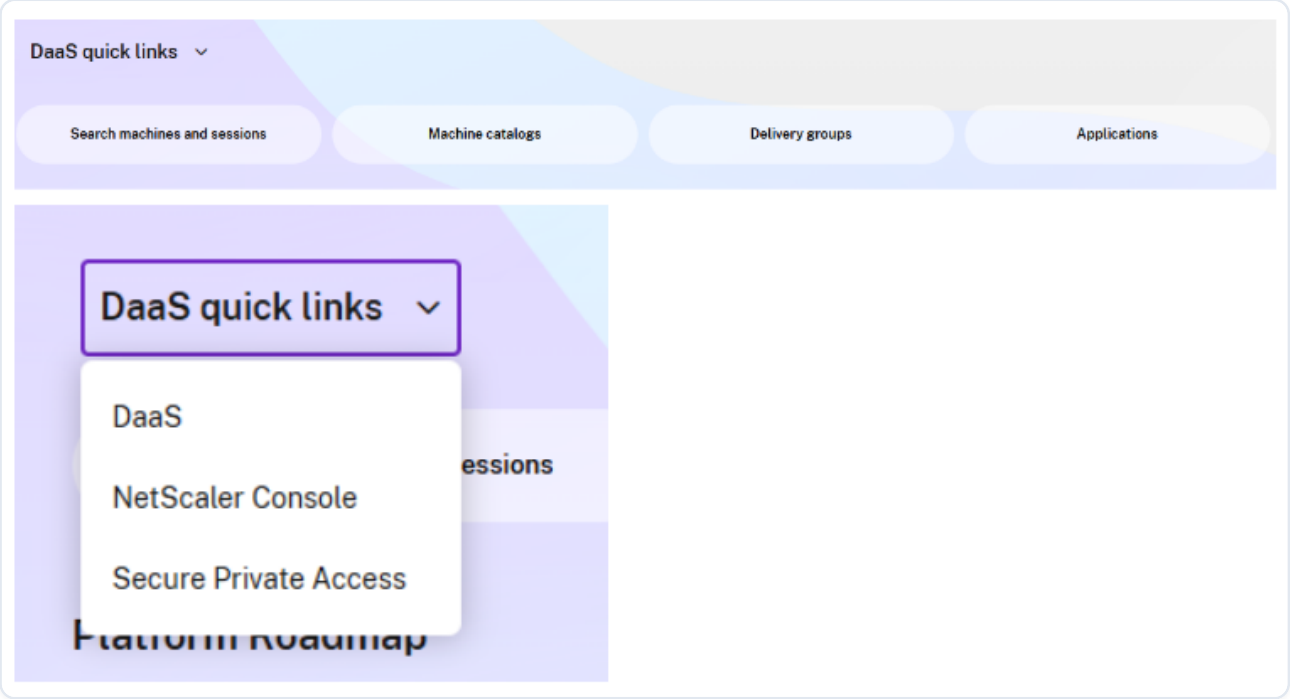


近期活动显示了平台中针对 DaaS、NetScaler Console、Secure Private Access 和 Citrix Cloud 等服务所做的配置更改，提供快速概览。您可以按服务筛选活动，并选择查看所有管理员或仅您自己所做的更改。在小组件右上角选择“显示更多活动”可查看多达 100 条日志。有关更多信息，您可以单击服务以获取详细日志。

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



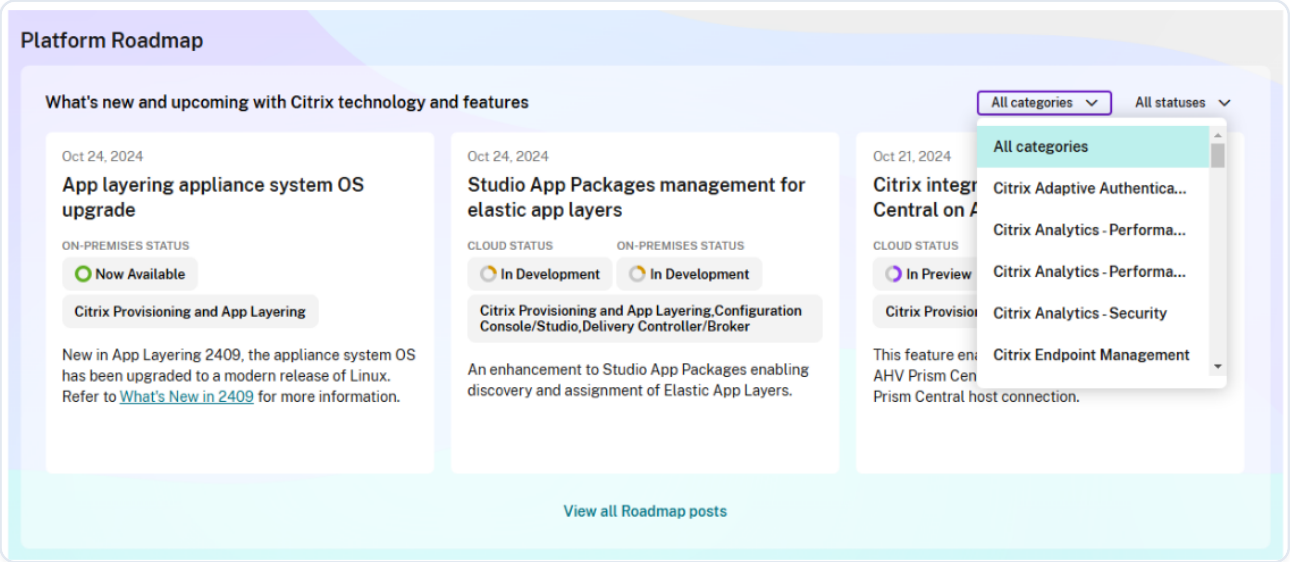
快速链接



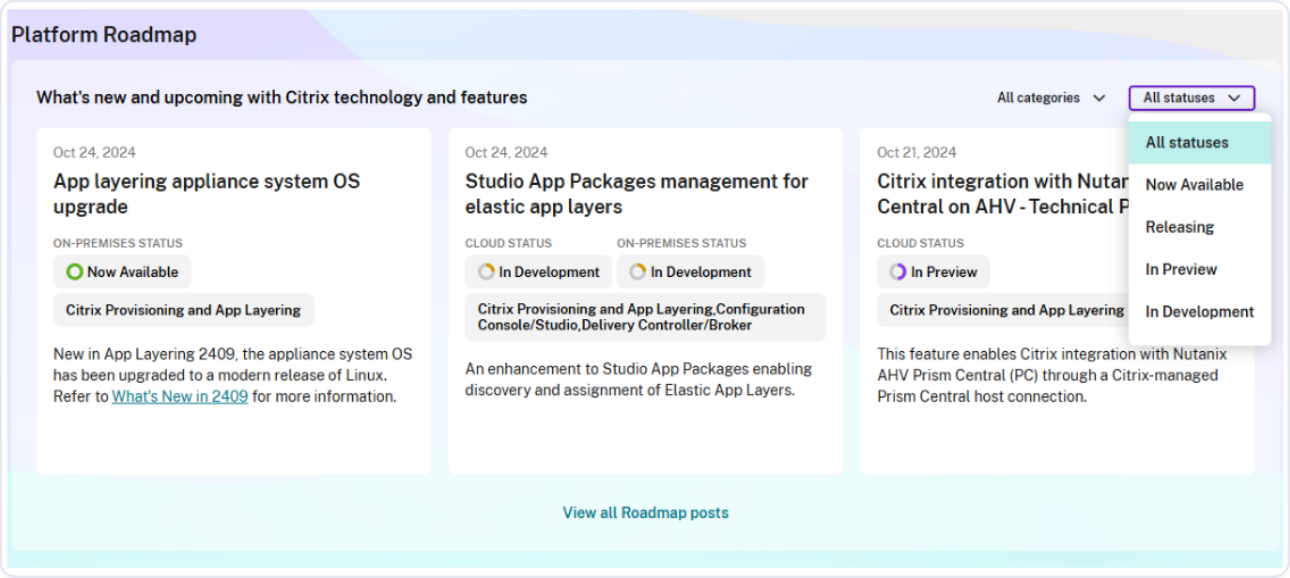
快速链接旨在帮助您更高效地工作，让您只需更少的点击即可直接导航到特定的服务部分。选择您希望访问的服务的快速链接，例如 **DaaS**、**NetScaler Console** 或 **Secure Private Access**。

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

平台路线图



查看所有当前正在进行、发布中、技术预览中或已全面上市 (GA) 的项目。您可以按类别（例如预配、安全私有访问）和/或按发布状态进行筛选。要查看完整列表，请单击“查看所有路线图帖子”。



即将举行的活动

及时了解最新活动，并通过点击“**查看全部**”访问完整列表，这会将您定向到 Citrix 社区页面：Citrix 活动。

资源

以下是一些重要资源，可帮助您充分利用该平台：

- **Citrix 社区**：访问讨论论坛、视频和即将举行的活动。
- **培训**：查找全面的培训资源，包括 Pluralsight 课程。
- **自动化**：探索平台上的 SDK、REST API、迁移工具等。

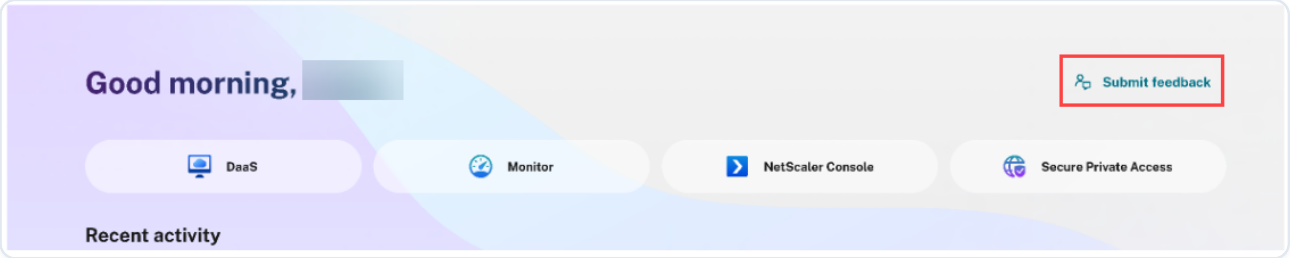
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Techwire**：我们的月度平台新闻通讯，包含更新和最热门的发布功能。

通过这些更新，Citrix Cloud 现在提供完全集成的高性能体验，为可访问性、可用性和生产力设定了新标准。

反馈

单击屏幕右上角的“**提交反馈**”以分享有关错误、增强功能和您的整体满意度的反馈。



Citrix Cloud 服务文档

正在寻找有关设置或管理 Citrix Cloud 服务的信息？请访问 (/zh-cn/citrix-cloud/services.html) 以查找所有云服务的产品文档链接。

架构和部署资源

(/zh-cn/tech-zone.html) 包含大量信息，可帮助您了解有关 Citrix Cloud 和其他 Citrix 产品的更多信息。在这里，您将找到参考架构、图表和技术白皮书，它们为设计、构建和部署 Citrix 技术提供了见解。

要了解有关 Citrix Cloud 中关键服务组件的更多信息，请参阅以下资源：

- Citrix® StoreFront Cloud 概念图：概述了身份、商店智能和单点登录等关键领域。
- 参考架构：提供全面的指南，用于规划您的 StoreFront Cloud 实施，包括用例、建议和相关资源。
- Citrix DaaS 参考架构：提供深入指导，用于部署 Citrix DaaS（以前称为 Virtual Apps and Desktops 服务）及相关服务。

教育资源

Citrix Cloud 学习系列门户 提供教育模块，帮助您快速上手 Citrix Cloud 及其服务。您可以按顺序查看所有模块，从概述到规划和构建服务。通过以下课程开始您的云之旅：

- Citrix Cloud 基础知识

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

- Citrix 身份和身份验证简介

Citrix 教育视频库 提供在线视频课程，引导您完成关键部署任务以及对与 Citrix Cloud 服务一起使用的组件进行故障排除。了解更多关于安装 Cloud Connectors 和注册 VDA 等任务，以及这些组件的故障排除。

Citrix Cloud™ 中的新增功能

本文介绍了 Citrix Cloud 版本中的新增功能、增强功能和修复。

2026 年 5 月

- **Citrix Platform Flex 许可**。Citrix Platform Flex 是一个托管式云交付平台，旨在跨云提供安全、弹性且灵活的数字商店和平台服务。有关详细信息，请参阅：
  - 针对 Citrix Platform Flex 的许可
  - Flex Credit 消耗和报告

2026 年 4 月

- **控制台可配置的非活动超时**。完全访问权限的管理员现在可以配置 Citrix Cloud 控制台上的非活动持续时间，超过该持续时间后管理员将自动注销。可配置的非活动超时范围为 10 分钟到 12 小时，默认值为 60 分钟。有关详细信息，请参阅 系统和连接要求。
- **条件身份验证增强功能**。条件身份验证现在支持其他身份提供程序和策略条件。有关详细信息，请参阅 条件身份验证。

2026 年 1 月

- **使用 Entra ID 对访客和 B2B 身份进行 SAML 身份验证**。Citrix Cloud 现在支持使用 Entra ID 作为 SAML 提供程序对访客和 B2B 用户身份进行商店身份验证。有关详细信息，请参阅 使用 Entra ID 对访客和 B2B 身份进行商店身份验证的 SAML 身份验证。

2024 年 12 月

- **条件身份验证**。Citrix Cloud 现在支持条件身份验证，使管理员能够强制执行上下文感知访问策略。有关详细信息，请参阅 条件身份验证。

2024 年 9 月

- **为合作伙伴引入新客户**。Citrix 合作伙伴现在可以直接从 Citrix Cloud 控制台引入新客户。有关详细信息，请参阅 引入新客户。

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

- **账户管理更新**。账户管理中的许可证管理部分已更新。有关详细信息，请参阅账户管理。

2024 年 6 月

- **将 Microsoft Entra ID 用于访客和 B2B 身份的 SAML**。Citrix Cloud 现在支持访客和 B2B 用户身份的商店身份验证。有关详细信息，请参阅将 Microsoft Entra ID 用于访客和 B2B 身份的 SAML 以进行商店身份验证。

2024 年 4 月

- **SAML 签名证书**。您现在可以更新服务提供商和身份提供商 SAML 签名证书。有关详细信息，请参阅：
  - 更新服务提供商 SAML 签名证书
  - 更新身份提供商 SAML 签名证书

2024 年 3 月

- **自定义登录页面**。管理员现在可以为 Citrix Cloud 配置自定义登录页面。有关详细信息，请参阅自定义登录页面。
- **与 PingFederate 结合使用的 SAML**。Citrix Cloud 现在支持将本地 PingFederate 服务器配置为 SAML 提供商。有关详细信息，请参阅使用 PingFederate 的 SAML。

2024 年 1 月

- **Citrix 身份提供商支持**。在身份和访问管理中添加了 Citrix 身份提供商支持。有关详细信息，请参阅身份和访问管理。
- **License Usage Insights 作为一项新服务**。License Usage Insights 现已作为一项新服务在支持的服务中提供。

服务级别协议

生效日期：October 30, 2020

Citrix Cloud™ 采用行业最佳实践设计，以实现高度的服务可用性。

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

注意：

- 有关 Citrix Cloud Government 的 SLA 信息，请参阅服务级别协议。
- 有关 Citrix Platform Flex 的 SLA 信息，请参阅服务级别协议。

本服务级别协议 (SLA) 描述了 Citrix 对 Citrix Cloud 服务可用性的承诺。本 SLA 是 Cloud Software Group 涵盖服务（“服务”）的最终用户协议 (EULA) 的一部分。

Citrix 的服务承诺（“服务承诺”）是在服务上保持至少 99.9% 的月度正常运行时间（“月度正常运行时间”）。月度正常运行时间是通过从 100% 中减去服务实例在一个完整月份内处于“不可用”状态的分钟百分比来计算的。服务以及每个服务的可用性衡量标准如下表所示。月度正常运行时间百分比测量不包括因以下原因造成的停机时间：

- 定期计划的维护窗口。
- 客户未能遵循 https://docs.citrix.com 上记录的服务配置要求，或滥用行为，或错误输入。
- Citrix® 建议客户修改其服务使用方式后，如果客户未修改使用方式，则客户对服务的使用。
- 由非 Citrix 管理的任何组件引起，包括但不限于客户控制的物理和虚拟机、客户安装和维护的操作系统、客户安装和控制的软件、网络设备或其他硬件；客户定义和控制的安全设置、组策略和其他配置策略；公共云提供商故障、互联网服务提供商故障；或 Citrix 控制范围之外的其他客户支持因素。
- 客户的员工、代理、承包商或供应商，或任何通过客户密码或设备获得访问权限的人，或因客户未能遵循适当的安全实践而导致的任何其他情况。
- 客户尝试执行超出服务权利的操作。
- 因不可抗力导致的服务中断，包括但不限于自然灾害、战争或恐怖主义行为，或政府行为。

任何 Citrix 试用版、技术预览版、实验室或 Beta 服务均不提供服务承诺。

Citrix 向符合以下条件的客户提供服务承诺：

- 已通过基于期限的订阅（最少 1 年订阅期）购买服务。
- 在索赔期内，根据适用于服务的许可模型，至少拥有 100 个单元的订阅（Citrix 服务提供商最少 1,000 个）。

Citrix 服务提供商 (CSPs) 于 October 1, 2018 起符合条件。

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

各项服务的可用性衡量标准

服务	月度正常运行时间衡量标准
思杰性能分析™	用户可以访问和改进应用程序和桌面性能的时间。
思杰安全分析™	用户可以检测和缓解用户访问和活动风险的时间。
NetScaler® Console 服务	服务在所有 POP 中可用的平均时间。
思杰端点管理™	用户可以通过服务访问其 Citrix 交付的移动应用程序和注册设备的时间。
适用于 HDX™ 代理的 Citrix Gateway 服务	用户可以通过服务访问其应用程序或桌面会话的时间。
NetScaler SD-WAN 编排器	用户可以通过服务访问其 SD-WAN Orchestrator 帐户并管理其 SD-WAN 网络的时间。
Citrix 安全私有访问™	用户可以通过服务访问其 SaaS 或内部 Web 应用程序的时间。
思杰 DaaS™	用户可以通过服务访问其应用程序或桌面会话的时间。
思杰® StoreFront 云	与上述组件服务相同，但包括每个组件的可用性。如果索赔涉及的组件少于所有组件，则积分可能会按比例分配。
许可证激活服务 (LAS)	产品激活可供客户使用的时间。

注意：

Citrix DaaS 是以下各项的新名称：Citrix Virtual Apps 服务、Citrix Virtual Desktops 服务以及 Citrix Virtual Apps and Desktops™ 服务。

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

服务承诺和补救措施

如果 Citrix 在 SLA 生效日期或之后，在任意连续 5 个月中的至少 3 个月内未能履行服务承诺，则唯一的补救措施是按月计算的 10% 服务抵扣金，适用于 Citrix 未能履行服务承诺的月份，并应用于客户在紧随其后的续订期内，针对受影响的相同服务和相同数量单元的下一次年度服务续订。

- 月度正常运行时间百分比：> 99.9%
- 服务抵扣金：适用月份可享受 10% 折扣（以凭证形式提供给客户）

要获得上述补救措施，客户必须遵守 EULA，并且必须在提出抵扣金索赔的连续五个月期间的最后一个月结束后的三十 (30) 天内报告故障。有关报告此 SLA 可能违规行为的说明，请参阅 CTX237141。

请求必须指明服务，定义不可用性的日期、时间和持续时间，以及证实不可用性的支持日志或记录，并指明受影响的用户及其位置，以及任何请求的技术支持或已实施的补救措施。每项服务只发放一份服务抵扣金，适用于相应月份数，续订期内所有月份最多可获得一份 10% 的服务抵扣金。客户必须在购买续订时出示凭证。

如果您通过经销商购买续订，您将通过经销商获得抵扣金。我们为直接购买应用或为间接购买转交给您的经销商的抵扣金，将基于相同数量单元的续订的按比例计算的混合建议零售价。Citrix 不控制转售定价或转售抵扣金。抵扣金不包括抵销因 Citrix 或经销商而产生的付款的权利。Citrix 将不时更新这些条款。更新时，Citrix 还将修订服务级别协议顶部的发布日期。任何更改仅适用于您在当前发布日期或之后的新服务购买或服务续订。

第三方通知

- Citrix Cloud 第三方通知 (PDF)
- Citrix Analytics Service 第三方通知 (PDF)
- Citrix DaaS 第三方通知 (PDF)
- 适用于 Azure 的 Citrix DaaS Standard 第三方通知 (PDF)
- 远程浏览器隔离（以前称为 Secure Browser） (PDF)
- Citrix Endpoint Management 第三方通知 (PDF)
- Citrix Cloud Linux VDA 映像服务第三方通知 (PDF)
- 适用于云服务的连接器设备第三方通知 (PDF)
- Citrix Gateway Service 第三方通知 (PDF)
- Citrix Device Posture Service 第三方通知 (PDF)
- Citrix Secure Private Access 第三方通知 (PDF)

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

注意：

Citrix DaaS 以前称为 Citrix Virtual Apps and Desktops 服务。适用于 Azure 的 Citrix DaaS Standard 以前称为适用于 Azure 的 Citrix Virtual Apps and Desktops Standard。

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

如何获取帮助和支持

本文介绍了在创建帐户或登录 Citrix Cloud™ 或其他 Citrix 网站时遇到问题时，如何进行故障排除和获取帮助。本文还包括其他自助资源和引导式支持选项。

重要提示：

如果您在登录 Citrix 网站或注册多重身份验证 (MFA) 时遇到问题，请首先查阅本文以获取故障排除资源。如果这些资源无法帮助您解决问题，请通过 https://www.citrix.com/contact/customer-service.html 联系 Citrix 客户服务。

创建帐户

访问 Citrix 网站上的某些资源（例如 Citrix 讨论论坛、培训课程、某些产品下载和 Citrix 技术支持）需要 Citrix 帐户。

要为您的公司创建新的 Citrix 帐户，请通过以下方法之一联系 Citrix：

- 联系 Citrix 客户服务。
- 联系您所在地区的 Citrix 合作伙伴 或 Citrix 销售办事处。

如果您已有 Citrix 帐户，可以通过完成 创建 Citrix Cloud 帐户 中所述的任务来创建 Citrix Cloud 帐户并完成入职流程。

如果您在注册 Citrix Cloud 时遇到问题，请联系 Citrix 客户服务。

登录 Citrix 网站和 Citrix Cloud

如果您在使用 Citrix 帐户登录 Citrix 网站时遇到问题，请使用以下资源进行故障排除：

- CTX228792: 解决 Citrix 网站上的登录问题

我无法设置 MFA，或者在登录 Citrix 帐户时无法通过 MFA 进行身份验证

请参阅以下文章以获取故障排除信息：

- CTX461297: 如何注册多重身份验证 (MFA)

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

- CIX463758: 如何使用恢复电子邮件地址或备用代码重置 Citrix MFA

如果您仍然无法使用 MFA 登录，请通过 https://www.citrix.com/contact/customer-service.html 联系 Citrix 客户服务。

如何查找我的 Citrix 帐户用户名或重置我的 Citrix 密码?

请按照以下步骤验证您的 Citrix 帐户用户名并重置密码。

1. 访问 https://www.citrix.com/welcome/request-password.html。
2. 要验证您的 Citrix 帐户用户名：
   a. 在 **通过以下方式查找我的帐户** 下，选择 **电子邮件**。
   b. 输入与您的 Citrix 帐户关联的电子邮件地址。
3. 要重置您的 Citrix 帐户密码：
   a. 在 **通过以下方式查找我的帐户** 下，选择 **用户名**。
   b. 输入您的 Citrix 帐户用户名。
4. 单击 **查找我的帐户**。

如果 Citrix 使用您的电子邮件地址找到您的帐户，Citrix 会向您发送一封电子邮件，其中包含与您的电子邮件地址关联的用户名和公司名称。如果 Citrix 使用您的 Citrix 用户名找到您的帐户，Citrix 会向您发送一封包含重置密码说明的电子邮件。

如果几分钟后您仍未收到电子邮件，请参阅本文中的“(#citrix-emails-arent-appearing-in-my-email-inbox)”。

我无法登录 Citrix Cloud

- 确保您使用正确的帐户凭据登录。要验证您的帐户用户名，请访问 https://citrix.cloud.com/，选择 **Forgot your username?**（忘记用户名？），然后输入您的电子邮件地址。Citrix 会向您发送一封包含您的帐户用户名的电子邮件。
- 您可能需要重置密码。如果您最近未登录或密码不够强，Citrix Cloud 会提示您更改密码。有关详细信息，请参阅本文中的“(#changing-your-password)”。
- 您可能需要使用自定义登录 URL 登录。如果您的 Citrix Cloud 帐户使用 (/zh-cn/citrix-cloud/citrix-cloud-management/identity-access-management/connect-azure-ad.html)、(/zh-cn/citrix-cloud/citrix-cloud-management/identity-access-management/google-identity) 或 (/zh-cn/citrix-cloud/citrix-cloud-management/identity-access-management/saml-identity.html) 对管理员进行身份验证，请选择 **Sign in with my company credentials**（使用我的公司凭据登录）并输入您

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

公司的登录 URL。然后，您可以输入公司凭据以访问您公司的 Citrix Cloud 帐户。如果您不知道公司的登录 URL，请联系您公司的管理员寻求帮助。

如果您仍然无法登录 Citrix Cloud，请联系 Citrix 客户服务。

Citrix 电子邮件未出现在我的收件箱中

当 Citrix 向您发送电子邮件以验证您的 MFA 身份、查找您的 Citrix 帐户或更改密码时，电子邮件通常会在几分钟内送达。如果您未收到这些电子邮件，请执行以下操作：

- 检查您 Citrix 帐户注册的电子邮件地址，并验证其是否正确。如果您最近更改了电子邮件地址，验证电子邮件可能会发送到您的旧地址。
- 电子邮件可能被意外过滤。检查电子邮件客户端中的垃圾邮件和废纸篓文件夹。您还可以搜索电子邮件帐户中来自 `donotreplynotifications@citrix.com` 或 `cloud@citrix.com` 的电子邮件。
- 您的防火墙可能已阻止该电子邮件。确保以下地址被列为受信任的发件人：
  - `donotreplynotifications@citrix.com`
  - `cloud@citrix.com`
  - `CustomerService@citrix.com`

如果几分钟后您仍未收到电子邮件，或者您遇到其他登录问题，请联系 Citrix 客户服务。

Citrix 和 Citrix Cloud 帐户的多重身份验证

Citrix 客户需要使用 MFA 登录其 Citrix 帐户和 Citrix Cloud。在以下情况下会注册 MFA：

- 新客户首次登录其 Citrix 帐户。
- Citrix 客户(/zh-cn/citrix-cloud/overview/signing-up-for-citrix-cloud/signing-up-for-citrix-cloud.html)，但尚未注册 MFA。
- 新管理员(/zh-cn/citrix-cloud/citrix-cloud-management/identity-access-management/add-admins.html)。

如果您在登录 Citrix 帐户或 Citrix Cloud 时收到注册 MFA 的提示，请按照CTX461297: How to Enroll into Multi Factor Authentication (MFA)中的步骤操作。

有关 Citrix 帐户 MFA 的更多信息，请参阅 CTX463482：在 Citrix 属性上设置多重身份验证 (MFA) 时的常见问题。

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

帐户恢复

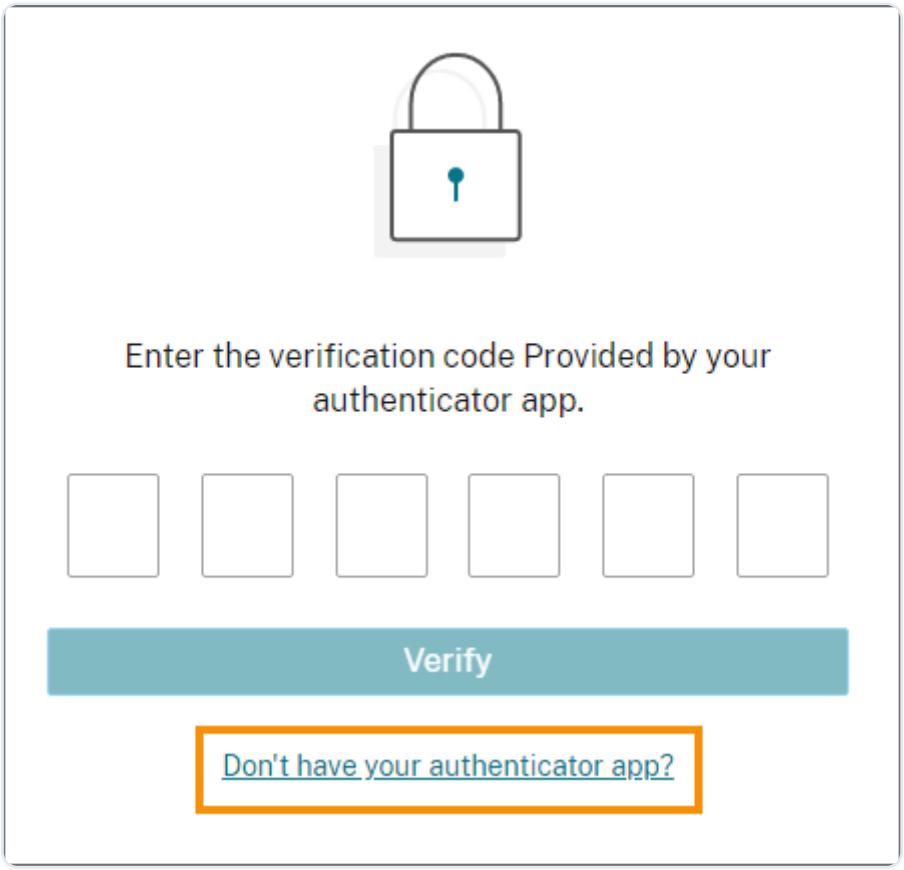
如果您需要帮助恢复 Citrix 帐户凭据，请参阅本文中的(#how-do-i-find-my-citrix-account-user-name-or-reset-my-citrix-password)。

如果您需要帮助恢复对 Citrix Cloud 帐户的访问权限，可以使用在注册 MFA 时配置的恢复方法。这些恢复方法包括：

- Citrix 发送到您的恢复电子邮件地址的一次性代码。
- 在 MFA 注册期间生成的列表中的备份代码。
- Citrix 支持部门致电您的恢复电话号码，以验证您的身份并帮助您访问帐户。在 MFA 注册期间需要设置恢复电话号码。

要使用恢复方法登录：

1. 从 Citrix 帐户 或 Citrix Cloud 登录页面，输入您的用户名和密码，然后选择**登录**。
2. 当系统提示您输入主要 MFA 方法的代码时，选择 **使用恢复方法**。



3. 如果适用，选择您要使用的恢复方法。如果您除了恢复电话号码之外只配置了另一种恢复方法，Citrix 会自动提示您使用该方法。
4. 如果使用您的恢复电子邮件地址，请输入 Citrix 发送的一次性代码，然后选择 **验证**。如果一段时间内未收到代码，请选择 **重新发送电子邮件**。验证后，Citrix Cloud 会将您登录。

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

5. 如果使用备用代码，请在出现提示时输入代码，然后选择 **验证并继续**。Citrix Cloud 会将您登录，并向您发送一封电子邮件，通知您已使用备用代码以及剩余有效备用代码的数量。记下或删除已使用的备用代码，以确保您不会再次使用它。
6. 如果您无法使用恢复电子邮件或备用代码：
   a. 选择 **联系 Citrix 支持**。
   b. 填写表格，提供您问题的详细信息。Citrix 支持代表将使用您的恢复电话号码与您联系以验证您的身份。之后，代表会向您发送一个可用于登录的恢复代码。
   c. 返回 Citrix Cloud 登录页面，并使用您的 Citrix Cloud 凭据登录。
   d. 当系统提示您输入代码时，请输入您从 Citrix 支持收到的恢复代码，然后选择 **验证**。

登录后，请务必更新您的帐户恢复方法，以避免将来登录延迟。

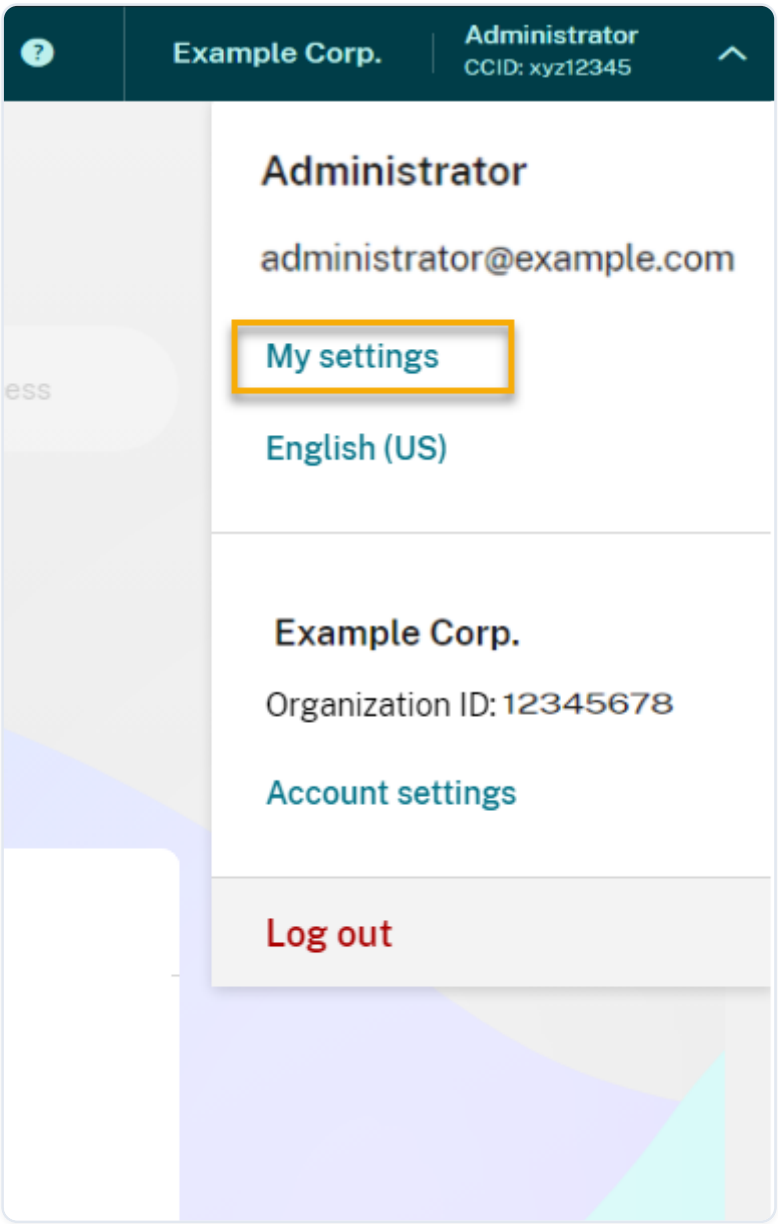
更新您的 MFA 设置

您可以通过“**我的设置**”页面更新您的 MFA 访问和恢复设置。您可以通过 Citrix 帐户或 Citrix Cloud 访问此页面。

要访问您的“**我的设置**”页面：

1. 登录您的 Citrix 帐户或 Citrix Cloud。
2. 从您的 Citrix 帐户，访问 https://accounts.cloud.com/core/profile。
3. 在 Citrix Cloud 中，从右上角菜单中选择 **我的设置**。

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



要更改您的 MFA 设置，请参阅以下部分：

- 管理您的主要 MFA 方法
- 管理您的 MFA 恢复方法

更改密码

如果您忘记了帐户密码，请选择 **忘记密码？** 并在出现提示时输入您的帐户用户名。Citrix 会向您帐户上的电子邮件地址发送一封电子邮件，其中包含用于设置新密码的链接。如果几分钟后您仍未收到此电子邮件，或者您需要进一步帮助，请联系 Citrix 客户服务。

当您尝试登录时，Citrix Cloud 可能会提示您重置密码。出现此提示的原因如下：

- 您的密码不符合 Citrix Cloud 的复杂性要求。

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

- 您的密码包含字典词。
- 您的密码列在已知泄露密码数据库中。
- 您在过去 60 天内未登录 Citrix Cloud。

密码长度必须介于 8 到 128 个字符之间，并且包含：

- 至少一个数字
- 至少一个大写字母
- 至少一个符号：! @ # $ % \^ * ? + = -

出现提示时，选择 **重置密码** 以创建您的帐户的新强密码。

云服务运行状况

Citrix Cloud 运行状况仪表板 https://status.cloud.com 提供了 Citrix Cloud 平台和各项服务在每个地理区域的实时可用性概览。如果您在使用 Citrix Cloud 时遇到任何问题，请查看 Cloud 运行状况仪表板，以验证 Citrix Cloud 或特定服务是否正常运行。

有关 Cloud 运行状况仪表板的更多信息，请参阅服务运行状况。

Citrix Cloud 支持论坛

在Citrix Cloud 支持论坛上，您可以获得帮助、提供反馈和改进建议、查看其他用户的对话或开始您自己的主题。

Citrix 支持人员会跟踪这些论坛，并随时准备回答您的问题。其他 Citrix Cloud 社区成员也可以提供帮助或加入讨论。

您无需登录即可阅读论坛主题。但是，您必须登录才能发布或回复主题。要登录，请使用您现有的 Citrix 帐户凭据，或使用您在创建 Citrix Cloud 帐户时提供的电子邮件地址和密码。

支持文章和文档

Citrix 提供了大量产品和支持内容，可帮助您充分利用 Citrix Cloud 并解决您在使用 Citrix 产品时可能遇到的问题。

Citrix 支持知识中心

知识中心提供故障排除内容以及所有 Citrix 产品的安全公告和软件更新通知。只需输入搜索字符串即可查找相关内容。您可以根据产品和文章类型筛选结果。

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

Citrix 技术专区

Citrix Tech Zone 包含有助于您了解 Citrix Cloud 和其他 Citrix 产品的更多信息。在此处，您可以找到参考架构、图表、视频和技术论文，这些内容为设计、构建和部署 Citrix 技术提供了见解。

用户帮助中心

Citrix 用户帮助中心 提供了专门面向您组织中最终用户的 Citrix 产品文档。用户帮助中心以易于阅读的格式提供了面向最终用户产品的说明，例如 Citrix Workspace 应用程序和 Citrix SSO。有关 ShareFile 的最终用户文档，请参阅 ShareFile 产品文档网站上的 Citrix Files 应用程序。

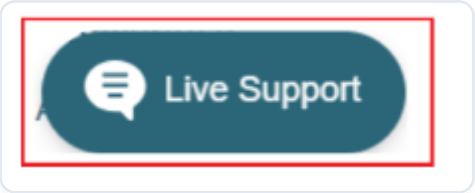
如何在线提交客户服务案例

注意：

只有符合遥测要求并拥有有效、活跃授权的客户或合作伙伴才能提交客户服务案例。 如果“创建案例”按钮不再可用，客户必须使用聊天联系支持。顾问可以提供帮助或启动 Web-to-Case 来创建支持案例。

要创建新案例，请按照以下步骤操作：

1. 访问 Citrix 支持站点。
2. 使用您的 Citrix 凭据登录。
3. 如果您在使用 Citrix 帐户登录 Citrix 网站时遇到问题，请参阅文章 CTX228792: 解决 Citrix 网站上的登录问题
4. 单击 **Live Support** 以启动虚拟助理流程。



5. 选择相应的“案例类型”，然后从可用选项中选择“**相关问题**”。

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

6. 如果您要跟进现有案例，请选择“**我的支持案例**”并按照提示继续。机器人会显示与您问题相关的文章或文档。

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

7. 如果有帮助，请单击“**是**”。系统会提示您返回主菜单或结束聊天。
8. 如果文章没有帮助，请单击“**否**”。机器人会要求您再次描述问题，并尝试根据您的新输入提供更相关的文章。
9. 如果第二篇文章仍然没有帮助，请再次单击“**否**”以联系支持人员。
10. 单击“**获取支持**”以继续。

11. 单击“**新建案例**”以开始创建案例。

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

12. 从下拉列表中选择“**帐户**”。
13. 从可用选项中选择您的**首选语言**。

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

14. 系统会提示您以下消息：“**您希望在创建案例后联系实时座席吗？**”?
15. 选择“**是**”以与实时座席发起聊天。将创建一个案例，并且您将连接到可用的顾问。
16. 如果选择“**否**”，机器人会要求提供其他信息并创建一个离线案例。

通过实时支持提交离线案例

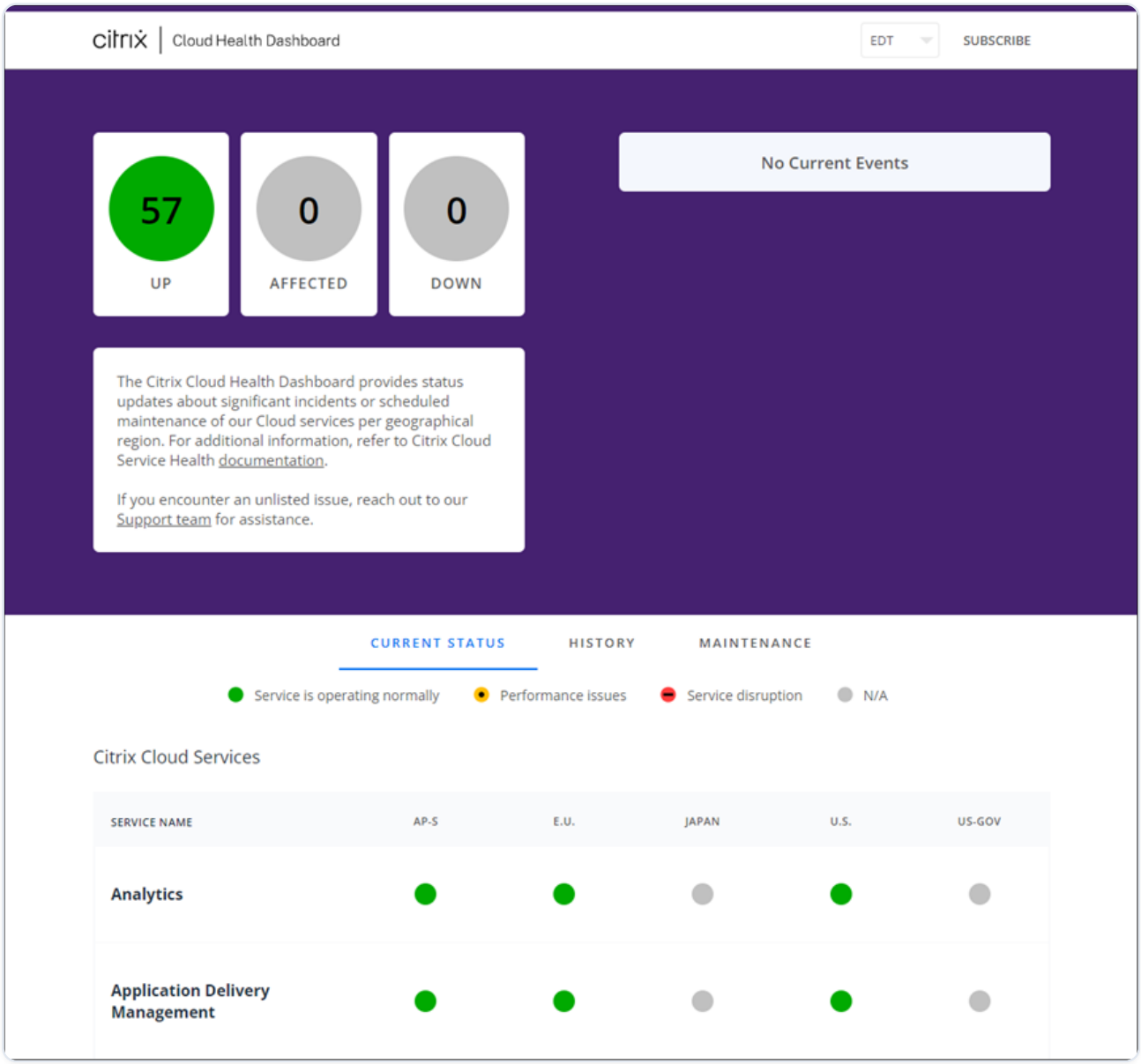
如果虚拟助手无法解决您的问题，系统可能会提示您提供更多详细信息，以便创建离线案例。

1. **用不超过 10 个字描述问题**：提供问题或请求的简要摘要。
2. **请输入首选回拨号码**：提供一个有效的电话号码，以便 Citrix 客户服务顾问可以联系到您。
3. 提交所需信息后。系统会生成一个离线案例并将其通过电子邮件发送给聊天发起人。客户服务顾问会在两小时内联系客户。

Citrix Cloud™ 服务运行状况

Citrix Cloud Health Dashboard 提供了 Citrix Cloud 平台和各项服务在每个地理区域的实时可用性概览。如果您遇到任何 Citrix Cloud 问题，请查看 Cloud Health Dashboard 以验证 Citrix Cloud 或特定服务是否正常运行。

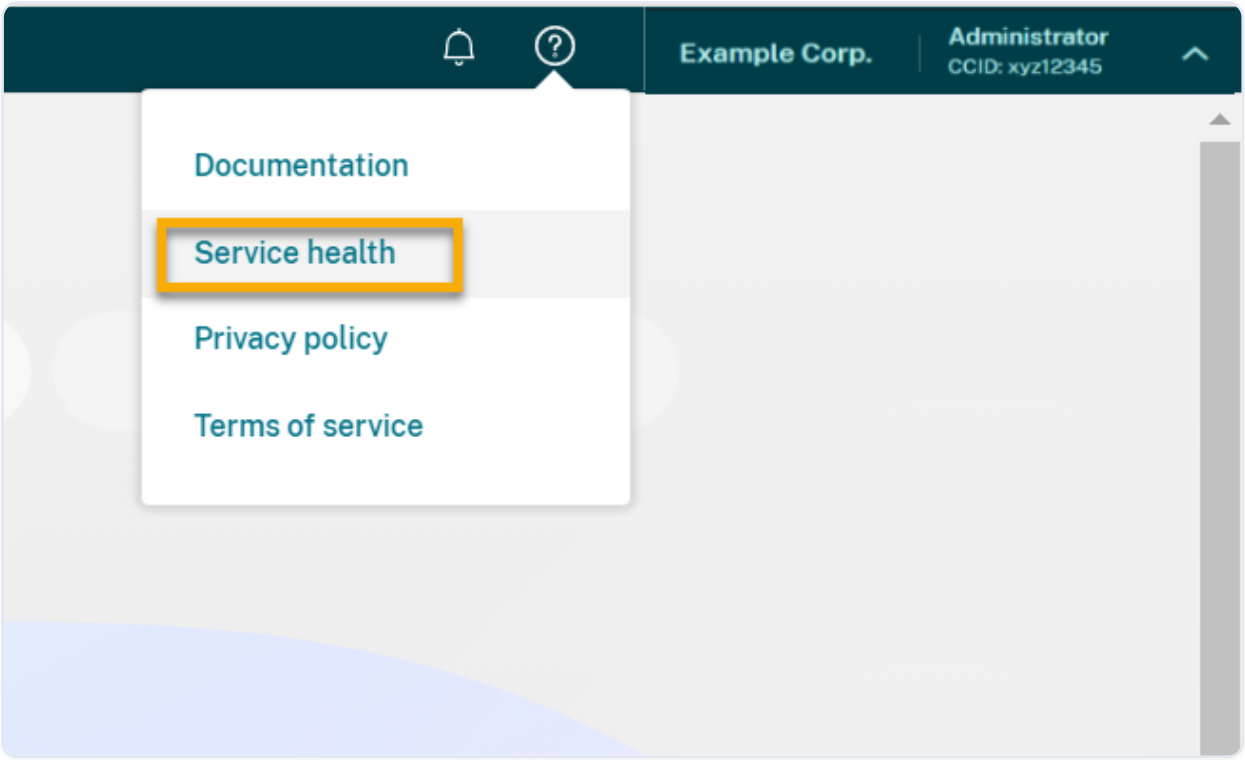
© 1997–2026 Citrix Systems, Inc. All rights reserved.



您可以使用以下方法访问 Cloud Health Dashboard：

- 通过您的 Web 浏览器导航到 https://status.cloud.com。
- 从 Citrix Cloud 的“帮助”菜单中选择“**服务运行状况**”。

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



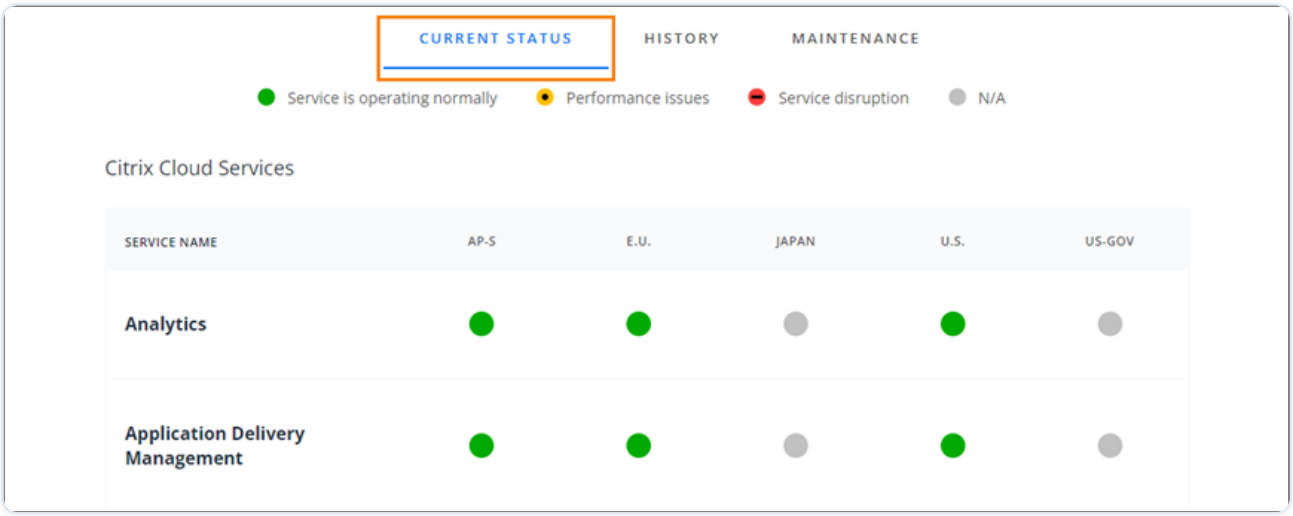
使用仪表板了解以下情况：

- 所有 Citrix Cloud 服务的当前运行状况，按地理区域分组
- 过去七天内各项服务的运行状况历史记录
- 特定服务的维护时段

您还可以订阅有关维护时段和服务事件等事件的通知。

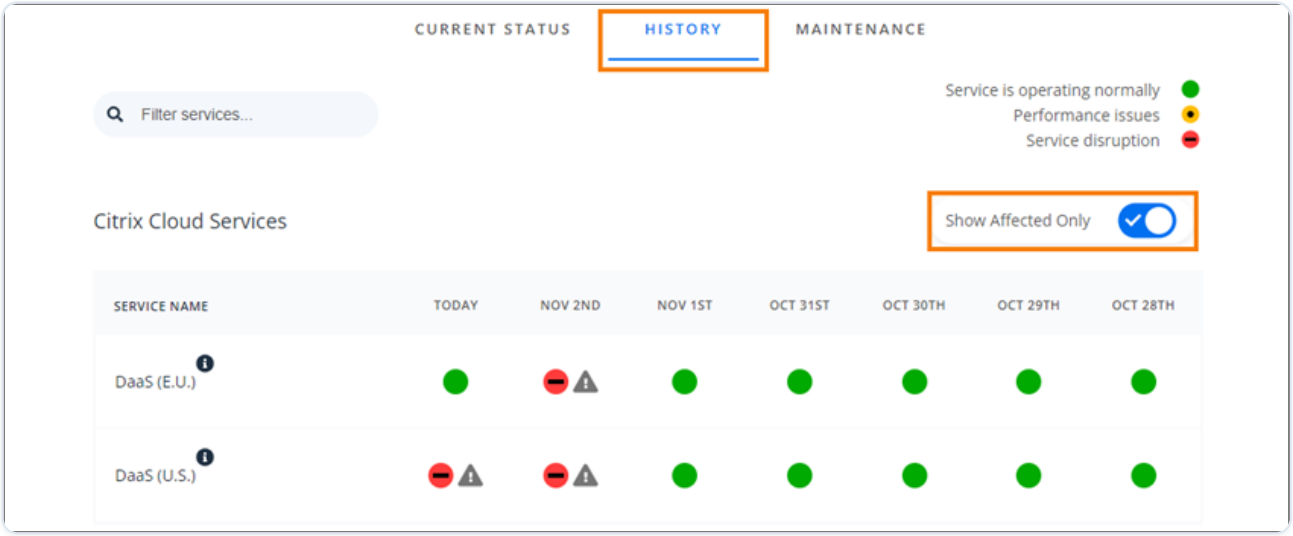
查看运行状况和维护状态

选择“**当前状态**”以显示所有 Citrix Cloud 服务和平台组件在每个地理区域的当前运行状况。

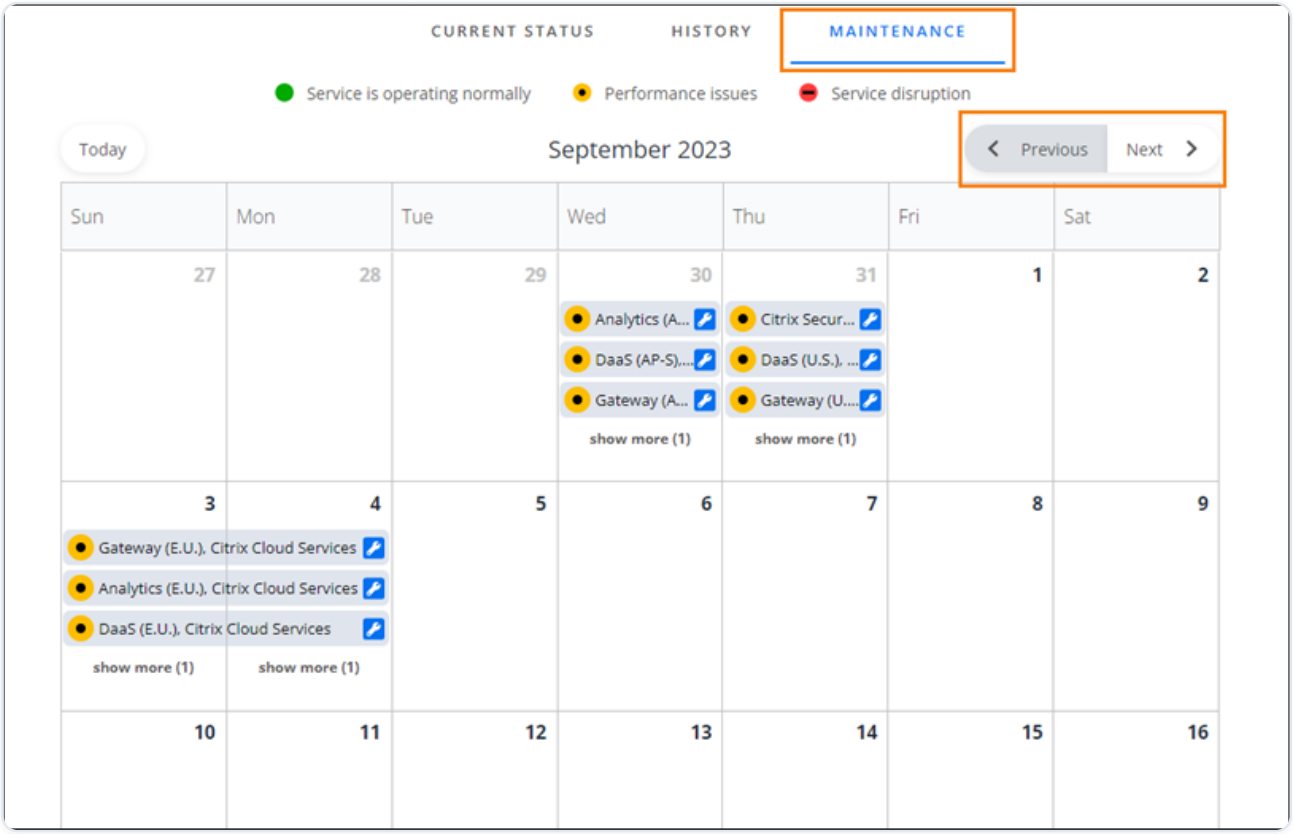


选择“**历史记录**”以显示过去七天所有 Citrix Cloud 服务和平台组件的运行状况。选择“**仅显示受影响的服务**”以仅显示过去七天内发生过维护或运行状况事件的服务。

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



选择“**维护**”以日历视图显示服务维护窗口。选择“**下一页**”以查看计划在未来几个月进行的维护事件。选择“**上一页**”以返回到当月的事件。

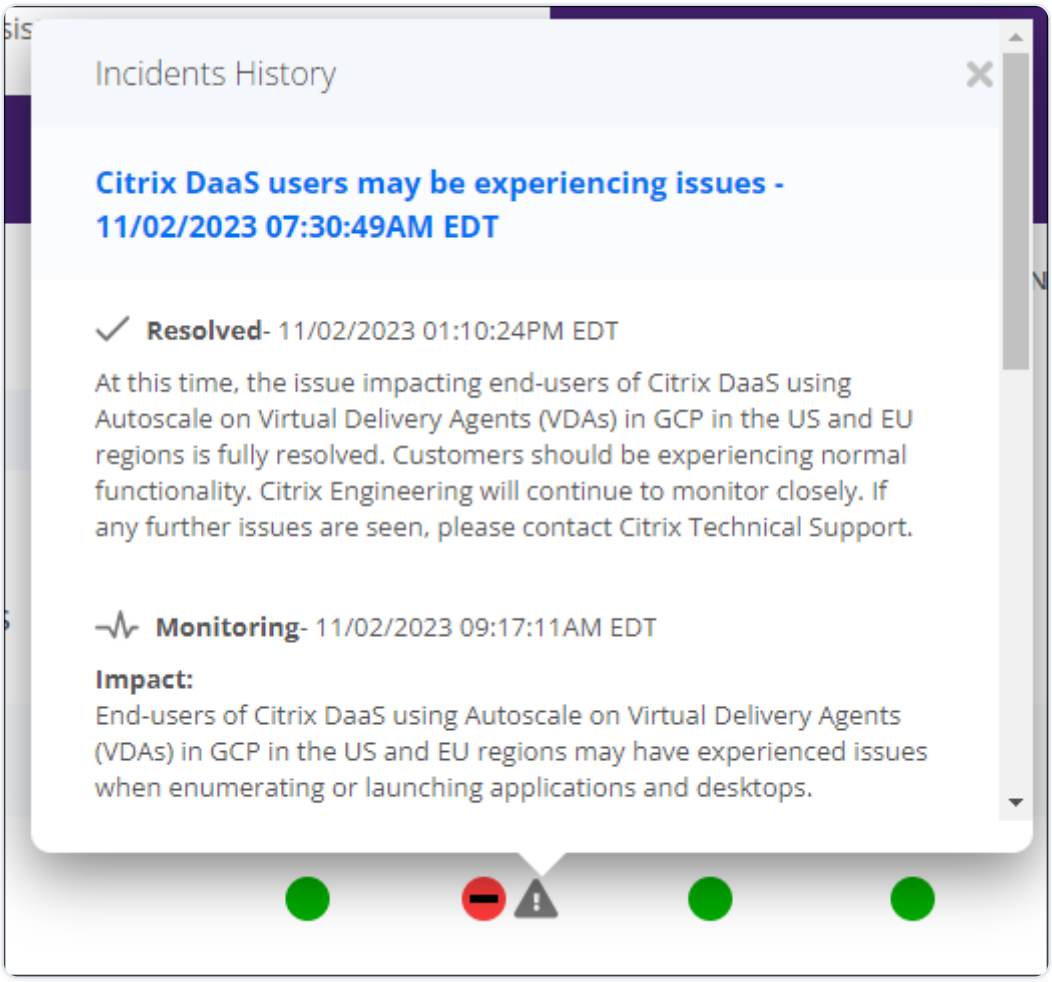


查看服务事件详细信息

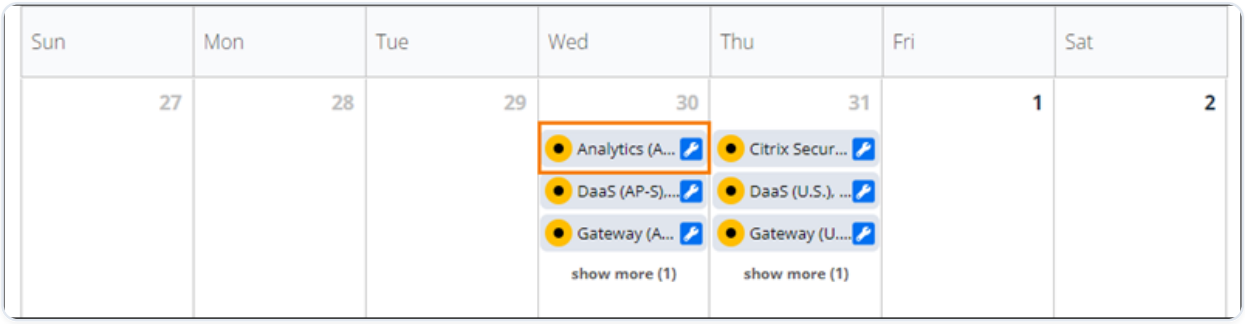
要查看受影响服务的服务运行状况事件的更多详细信息：

- 在“历史记录”视图中，单击服务指示器旁边的图标以查看有关服务运行状况事件的更多详细信息。

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



- 在“维护”视图中，单击服务条目以查看计划维护窗口的状态页面。



事件通知频率

如果发生服务运行状况事件，Citrix 在发布到 status.cloud.com 时会考虑以下特征：

- 影响持续时间
- 影响频率

在处理事件时，Citrix® 会将以下类型的通知发布到云运行状况控制板：

- **正在调查：** 此通知表示 Citrix 已将此问题确定为紧急问题，并正在调查此问题。
- **正在监控：** 此通知表示 Citrix 已确定根本原因并正在缓解此问题。

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

- **已解决：** 此通知表示 Citrix 已解决此问题，并且服务已恢复到正常状态。

在调查和监控事件期间，Citrix 会以 60 到 120 分钟的间隔发布更新。这些更新可能包括以下信息：

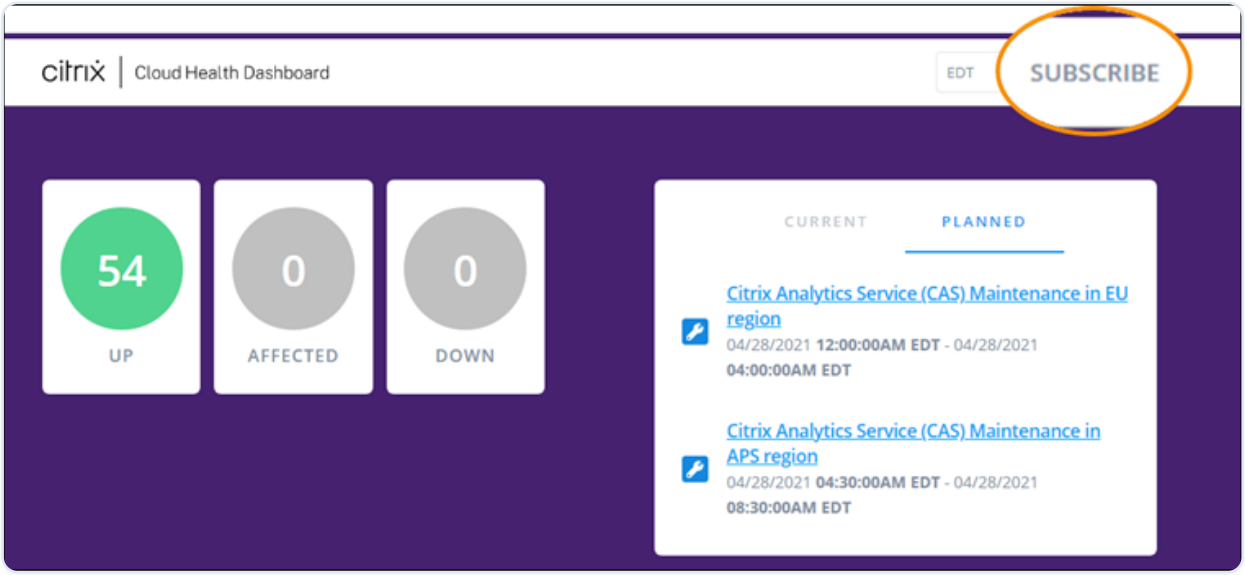
- 有关事件的其他详细信息。
- Citrix 为解决事件而采取的措施说明。
- 指示自上次更新以来未发生任何新更改。

事件解决后，Citrix 会发布最终更新。此更新可能表明事件已解决，并且服务已恢复到正常状态。

订阅通知

您可以使用以下方法接收有关服务运行状况事件的通知：

- 选择仪表板右上角的“**订阅**”，然后选择要使用的通知方法。您可以从多种方法中进行选择，包括电子邮件和电话（短信）。



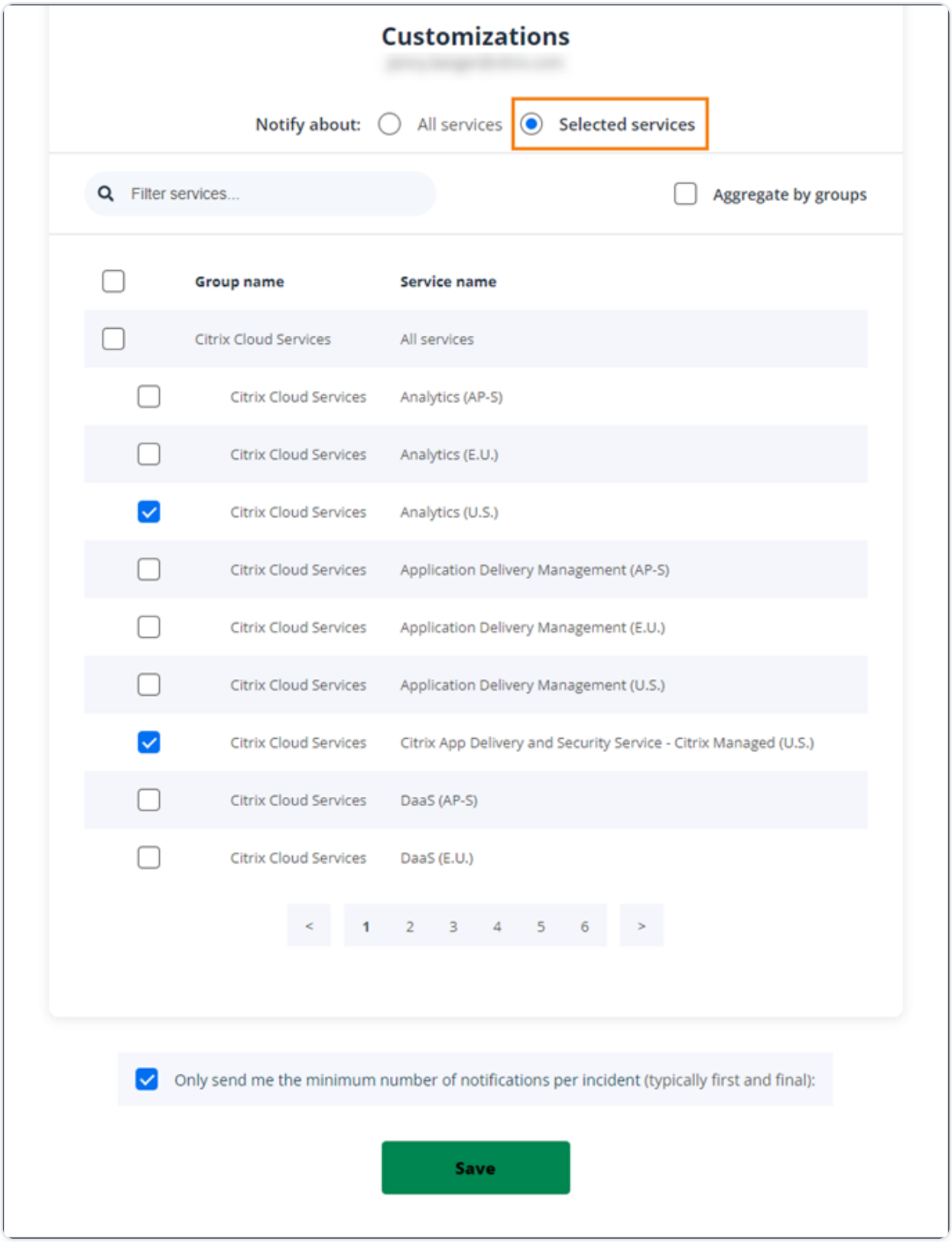
- 在您的 RSS 阅读器中输入以下 URL 以订阅 Citrix Cloud Health RSS 源：
  - 要在单个源中接收服务事件和维护通知，请订阅 `https://status.cloud.com/?format=atom`。
  - 要仅接收服务事件通知，请订阅 `https://status.cloud.com/atom/incidents`。
  - 若要仅接收维护通知，请订阅 `https://status.cloud.com/atom/maintenances`。

订阅某个区域中的特定服务

1. 在控制板的右上角选择 **Subscribe**，然后选择要使用的通知方法。
2. 输入所选订阅方法的联系方式或 URL，然后选择 **I accept terms & services**。选择 **Next**。此时将显示 **Customizations** 页面，其中默认选中 **Selected services**。

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

3. 在 **Customizations** 页面上，从多页列表中选择所需区域中的服务。



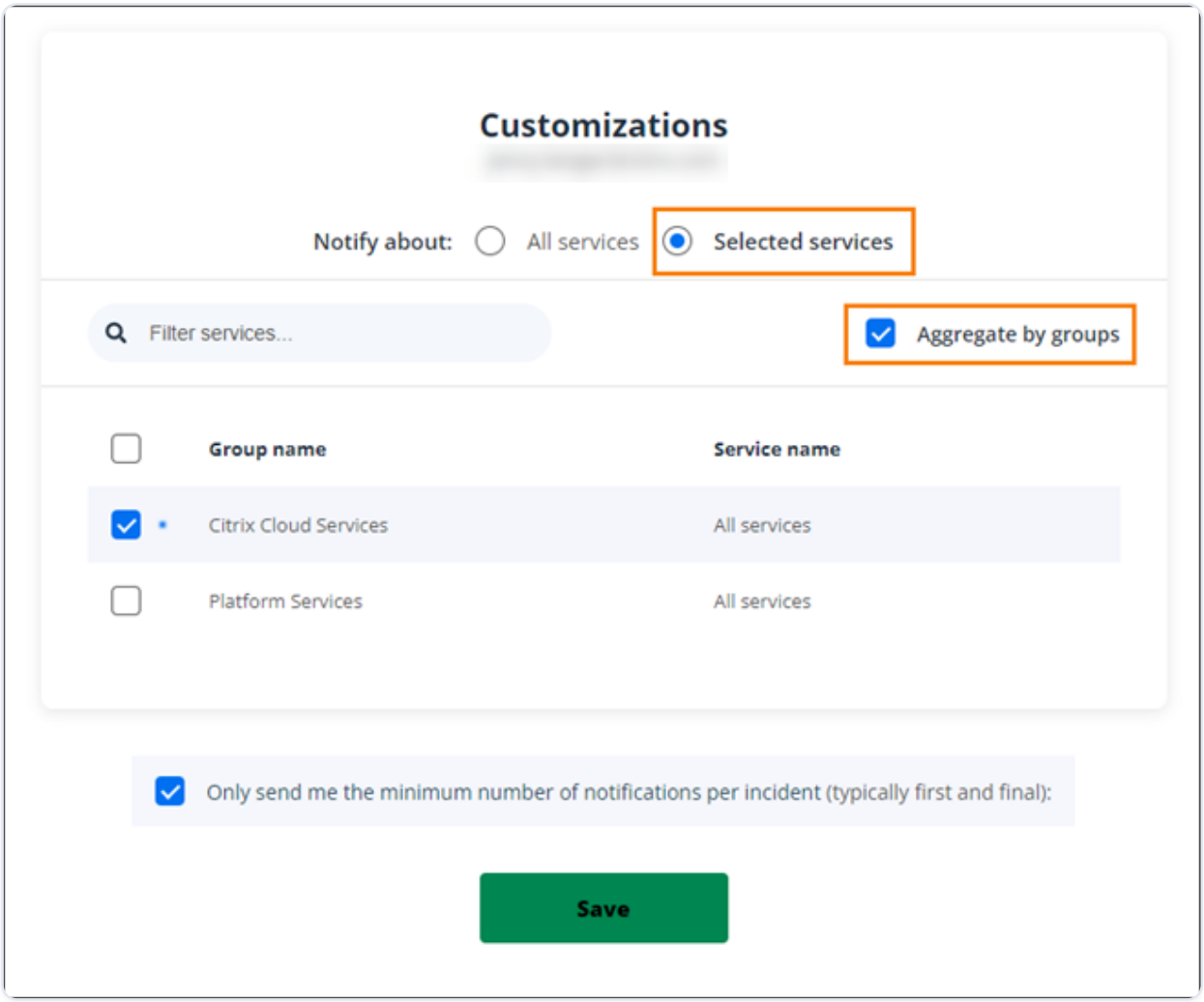
4. 若要仅接收每个事件的第一个和最后一个通知，请选择 **Only send me the minimum number of notifications per incident**。
5. 单击 **Save**。

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

订阅特定服务组

您可以订阅所有区域中所有云服务（例如，Analytics 和 DaaS）或所有平台服务（例如，控制平面和云 API）的通知。

1. 在控制板的右上角选择 **Subscribe**，然后选择要使用的通知方法。
2. 输入所选订阅方法的联系方式或 URL，然后选择 **I accept terms & services**。选择 **Next**。此时将显示 **Customizations** 页面，其中默认选中 **Selected services**。
3. 在 **Customizations** 页面上，选择 **Aggregate by groups**。
4. 选择 **Citrix 云服务** 或 **平台服务**。



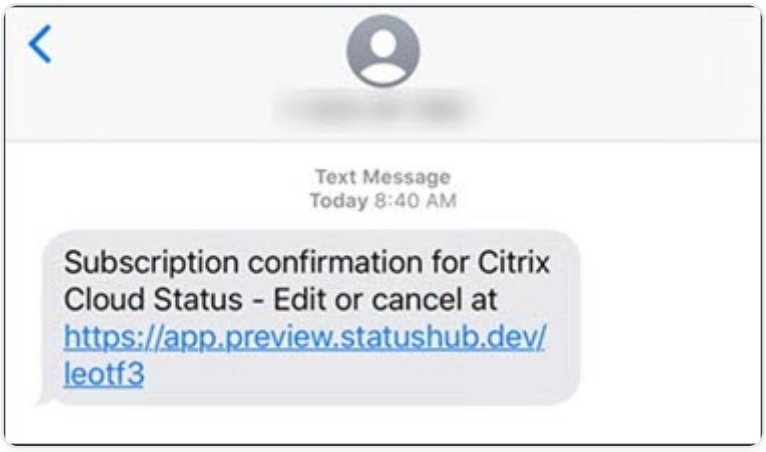
5. 要仅接收每个事件的首次和末次通知，请选择**仅向我发送每个事件的最低数量通知**。
6. 单击**保存**。

取消订阅通知

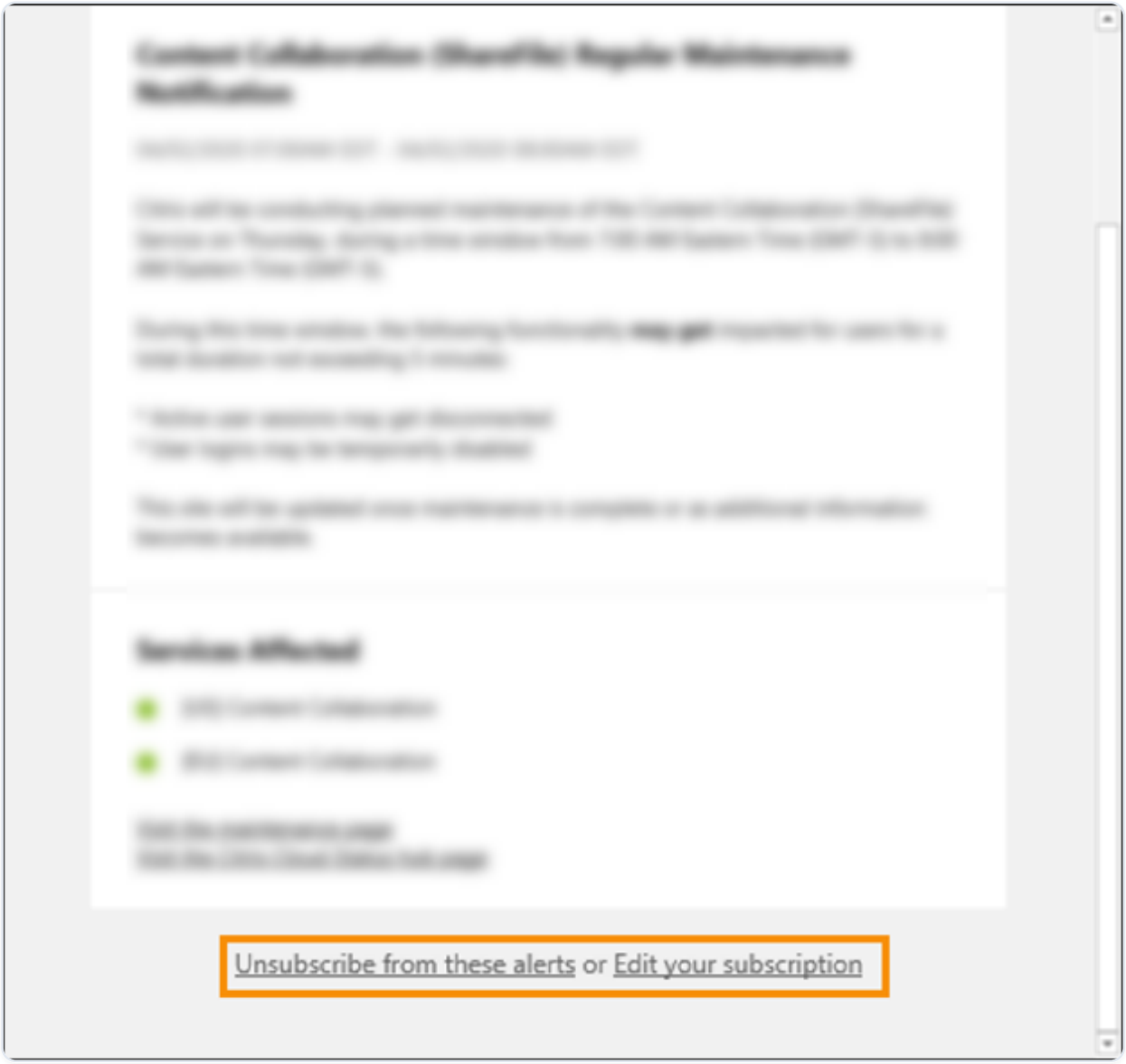
根据订阅方法，取消订阅或更改订阅的链接包含在您收到的确认消息中（例如，订阅电话通知时）或每条通知消息中（例如，订阅电子邮件通知时）。例如：

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

- 包含订阅选项的电话通知：



- 包含订阅选项的通知电子邮件



要取消订阅所有通知并删除所有订阅方法：

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

1. 找到您的订阅确认消息或现有通知，然后选择取消订阅链接。某些订阅方法可能提供一个用于编辑或取消订阅的链接。
2. 根据您的订阅方法，在**编辑订阅**页面上使用以下选项之一：
   - 选择**删除所有订阅**。
   - 选择**取消订阅**。在**取消订阅方法**页面上，选择**删除所有订阅**。

要取消订阅特定订阅方法的所有通知：

1. 找到您的订阅确认消息或现有通知，然后选择取消订阅链接。某些订阅方法可能提供一个用于编辑或取消订阅的链接。
2. 根据您的订阅方法，在“**编辑订阅**”页面上使用以下选项之一：
   - 选择您要删除的订阅方法。您的订阅将立即删除。
   - 选择“**取消订阅**”。在“**取消订阅方法**”页面上，选择您要删除的订阅方法。您的订阅将立即删除。

更改服务通知

1. 找到您的订阅确认消息或现有通知，然后选择链接以编辑您的订阅。某些订阅方法可能提供一个用于编辑或取消订阅的单个链接。
2. 在“**编辑订阅**”页面上，选择您要管理的订阅方法。
3. 在“**自定义**”页面上，选择您希望收到通知的服务，或根据需要清除您不再希望收到通知的服务。
4. 选择“**保存**”。

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

系统和连接要求

Citrix Cloud™ 提供管理功能（通过 Web 浏览器）和操作请求（来自其他已安装组件），这些功能和请求连接到部署中的资源。本文介绍了系统要求、所需的可联系 Internet 地址以及在您的资源和 Citrix Cloud 之间建立连接的注意事项。

系统要求

Citrix Cloud 需要以下最低配置：

- 一个 Active Directory 域
- 两台物理或虚拟机，加入您的域，用于 Citrix Cloud Connector。有关详细信息，请参阅 Cloud Connector 系统要求。
- 物理或虚拟机，加入您的域，用于托管工作负载和其他组件（例如 StoreFront）。有关特定服务的系统要求的详细信息，请参阅每个服务的 Citrix® 文档。

有关规模和大小要求的信息，请参阅 Cloud Connector 的规模和大小注意事项。

支持的 Web 浏览器

- 最新版本的 Google Chrome
- 最新版本的 Mozilla Firefox
- 最新版本的 Microsoft Edge
- 最新版本的 Apple Safari

传输层安全性要求

Citrix Cloud 支持传输层安全性 (TLS) 1.2，用于组件之间基于 TCP 的连接。Citrix Cloud 不允许通过 TLS 1.0 或 TLS 1.1 进行通信。

要访问 Citrix Cloud，您必须使用支持 TLS 1.2 并配置了接受的密码套件的浏览器。有关详细信息，请参阅加密和密钥管理。

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

Citrix Cloud 管理控制台

Citrix Cloud 管理控制台是一个基于 Web 的控制台，您可以在 https://citrix.cloud.com 登录后访问。构成控制台的网页可能需要在登录时或稍后执行特定操作时访问 Internet 上的其他资源。

代理配置

如果您通过代理服务器连接，管理控制台将使用应用于您的 Web 浏览器的相同配置运行。控制台在用户上下文中运行，因此任何需要用户身份验证的代理服务器配置都应按预期工作。

防火墙配置

为了使管理控制台正常运行，您必须打开端口 443 以进行出站连接。您可以通过在控制台内导航来测试常规连接。有关所需端口的更多信息，请参阅入站和出站端口配置。

控制台通知

管理控制台使用 Pendo 显示关键警报、新功能通知以及某些功能和服务的内产品指南。

为确保您可以在管理控制台中查看 Pendo 内容，Citrix 建议以下地址可访问：

- `https://citrix-cloud-content.customer.pendo.io/`
- `https://citrix-cloud-data.customer.pendo.io/`

如果对 Pendo 服务的连接受限，则产品内指南、通知和相关用户体验功能可能会受到限制或不可用。Pendo 服务托管在美国 (US)，Pendo 收集的数据在此区域内处理。有关详细信息，请参阅地理考量。

注意：

这两个 URL 都需要才能完全启用消息传递功能，包括中断通知、新功能公告和客户反馈调查。

显示 Pendo 内容的服务包括：

- Citrix Cloud 管理控制台
- Citrix DaaS™（包括 工作区环境管理™、Web Studio 和 会话录制）
- Citrix Studio（本地部署）
- Citrix Director 和 监控
- NetScaler (ADC)

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

- NetScaler Console (ADM) 和 NetScaler Console 服务
- 安全开发人员空间
- Citrix® StoreFront Cloud（桌面、移动设备和平板电脑 – 仅限云部署），包括原生 iOS 和 Android 应用程序

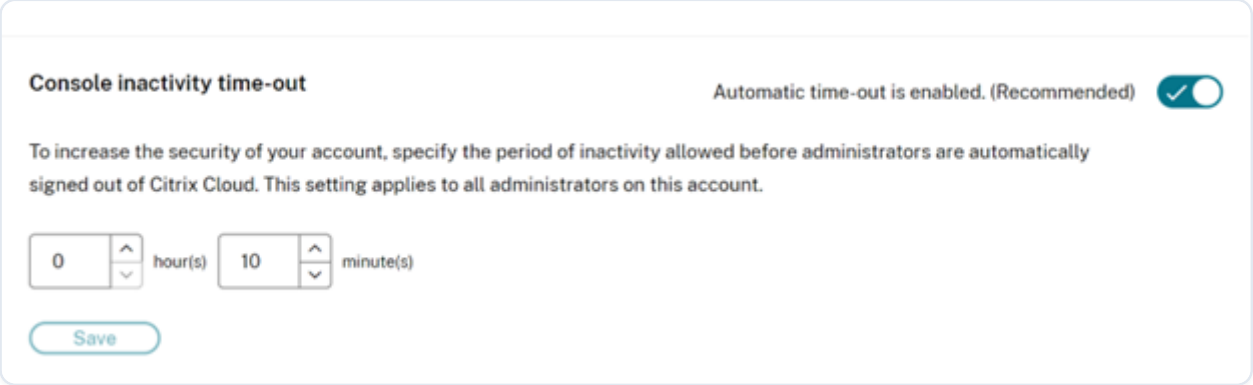
Pendo 是 Citrix 用于向 Citrix 客户提供云和支持服务的第三方子处理器。有关这些子处理器的完整列表，请参阅 Citrix Cloud 和支持服务以及 Citrix 关联公司的子处理器。

会话超时

管理员登录 Citrix Cloud 后，管理控制台会话将在 72 小时后超时。无论控制台活动如何，都会发生此超时。

可配置的控制台不活动超时

作为完全访问权限管理员，您可以配置 Citrix Cloud 控制台上的不活动持续时间，在此持续时间之后管理员将自动注销。配置后，指定的超时期限将应用于 Citrix Cloud 帐户的所有管理员。



当此功能启用时，管理员将在配置的不活动期限后注销，并且会话超时将在每次后续登录时重置。

当此功能禁用时，没有不活动计时器，管理员只会在达到 72 小时会话限制时注销。

注意：

- 默认情况下，此功能处于禁用状态。
- 可配置的不活动超时时间为 10 分钟到 12 小时。
- 默认不活动超时时间为 60 分钟。

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

许可证服务器与 Citrix Cloud 的连接

如果您要将本地 Citrix 许可证服务器注册到 Citrix Cloud 以 (/zh-cn/citrix-cloud/citrix-cloud-management/citrix-cloud-on-premises-license-usage.html)，请确保以下地址可访问：

- `https://trust.citrixnetworkapi.net`（用于检索代码）
- `https://trust.citrixworkspacesapi.net/`（用于确认许可证服务器已注册）
- `https://cis.citrix.com`（用于数据上传）
- `https://core.citrixworkspacesapi.net`
- `ocsp.digicert.com port 80`
- `crl3.digicert.com port 80`
- `crl4.digicert.com port 80`
- `ocsp.entrust.net port 80`
- `crl.entrust.net port 80`

如果您正在将代理服务器与 Citrix License Server 配合使用，请确保按照许可产品文档中 配置代理服务器 所述配置代理服务器。

Citrix 云连接器™

Citrix Cloud Connector 是一个软件包，它部署了一组在 Microsoft Windows 服务器上运行的服务。托管 Cloud Connector 的计算机位于您与 Citrix Cloud 配合使用的资源所在的网络中。Cloud Connector 连接到 Citrix Cloud，使其能够根据需要操作和管理您的资源。

有关安装 Cloud Connector 的要求，请参阅 系统要求。要运行，Cloud Connector 需要在端口 443 上进行出站连接。安装后，Cloud Connector 可能有额外的访问要求，具体取决于其所使用的 Citrix Cloud 服务。

托管 Cloud Connector 的计算机必须与 Citrix Cloud 具有稳定的网络连接。网络组件必须支持 HTTPS 和持久安全 Web 套接字。如果在网络组件中配置了超时，则超时必须大于 2 分钟。

有关排查 Cloud Connector 和 Citrix Cloud 之间连接问题的帮助，请使用 Cloud Connector 高级连接检查

Cloud Connector 常见服务连接要求

从您的数据中心连接到 Internet 需要打开端口 443 以进行出站连接。但是，要在包含 Internet 代理服务器或防火墙限制的环境中运行，可能需要进一步配置。有关详细信息，请参阅 Cloud Connector 代理和防火墙配置。

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

本文中每个服务的地址都必须可访问，才能正常运行和使用该服务。以下列表包含大多数 Citrix Cloud 服务通用的地址：

- `https://*.citrixworkspacesapi.net`（提供对服务使用的 Citrix Cloud API 的访问）
- `https://*.cloud.com`（提供对 Citrix Cloud 登录界面的访问）
- `https://*.blob.core.windows.net`（提供对 Azure Blob 存储的访问，该存储用于存储 Citrix Cloud Connector 的更新）
- `https://*.servicebus.windows.net`（提供对 Azure Service Bus 的访问，该服务用于日志记录和 Active Directory 代理）

这些地址仅以域名形式提供，因为 Citrix Cloud 服务是动态的，其 IP 地址会定期更改。

最佳实践是使用组策略来配置和管理这些地址。此外，仅配置适用于您和您的最终用户正在使用的服务的地址。

如果您将 Citrix Cloud 与 Citrix License Server 结合使用来 (/zh-cn/citrix-cloud/citrix-cloud-management/citrix-cloud-on-premises-registration.html)，请参阅本文中的 (#license-server-connectivity-to-citrix-cloud) 以获取其他必需的可联系地址。

Cloud Connector 允许的 FQDN

为帮助您确保所有必需的完全限定域名 (FQDN) 都通过防火墙，Citrix 提供了以下资源：

- 连接器允许列表 API
- (/zh-cn/citrix-gateway-service/pops-citrix-gateway-service)

配置防火墙时，请查阅这两个资源，以验证您的服务部署所需的 FQDN 是否已获允许。

本地主机缓存（高可用性服务）

在连接器中使用本地主机缓存 (LHC) 时，请确保连接器可以访问资源位置中所有其他连接器的选举端点。选举端点位于端口 80，可通过以下 URL 访问：`http://<FQDN_OR_IP_OF_PEER_CONNECTOR>/Citrix/CdsController/ISecondaryBrokerElection`。

如果连接器无法在此地址进行通信，则在 LHC 事件期间会选举多个代理，这可能导致间歇性的虚拟应用程序和桌面启动失败。有关详细信息，请参阅 (/zh-cn/citrix-daas/manage-deployment/local-host-cache.html#resource-locations-with-multiple-cloud-connectors)。

自适应身份验证

当使用 Cloud Connector 连接到自适应身份验证服务时，您必须允许 Citrix Cloud Connector 访问您为自适应身份验证实例保留的域或 URL。例如，允许 `https://aauth.xyz.com`。有关详细信息，

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

请参阅 (/zh-cn/adaptive-authentication/configure-the-adaptive-authentication-service#prerequisites)。

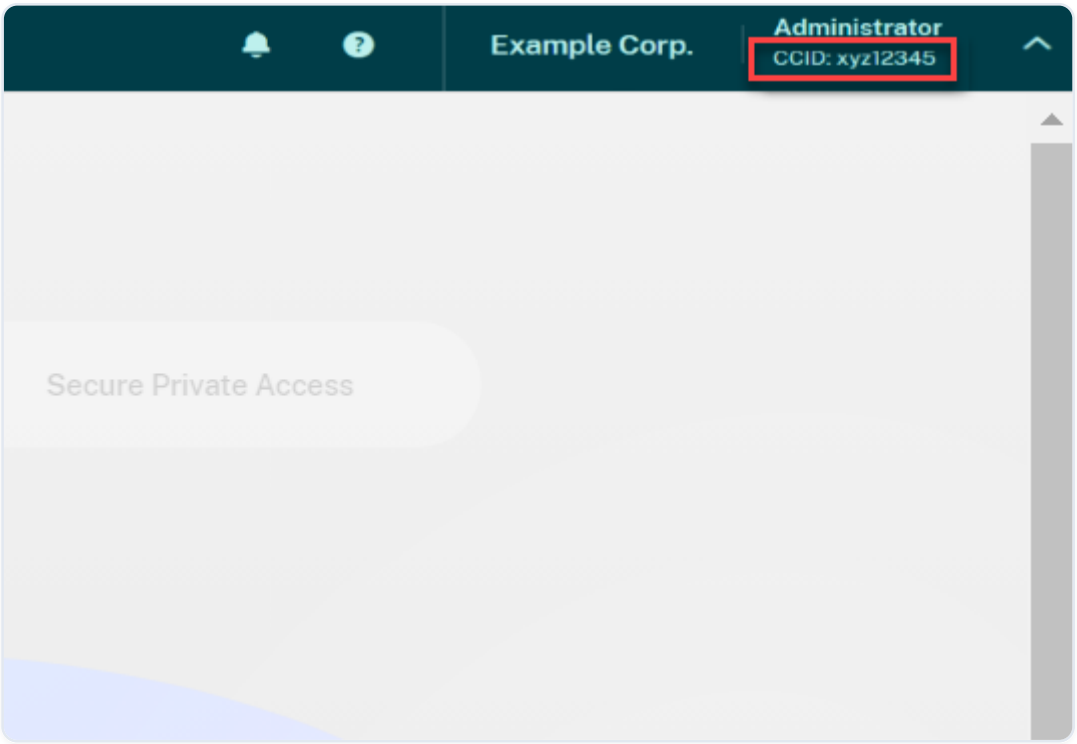
连接器允许列表 API

在可能的情况下，请使用 (/zh-cn/citrix-cloud/overview/requirements/internet-connectivity-requirements.html#cloud-connector-common-service-connectivity-requirements) 部分中的通配符地址。如果您的环境不允许使用通配符，请使用连接器允许列表 API 检索所需的 FQDN 的当前列表。

从以下位置检索列表: `https://api.cloud.com/connectivity/v2/allowlist?customerId=<CUSTOMER_ID>`

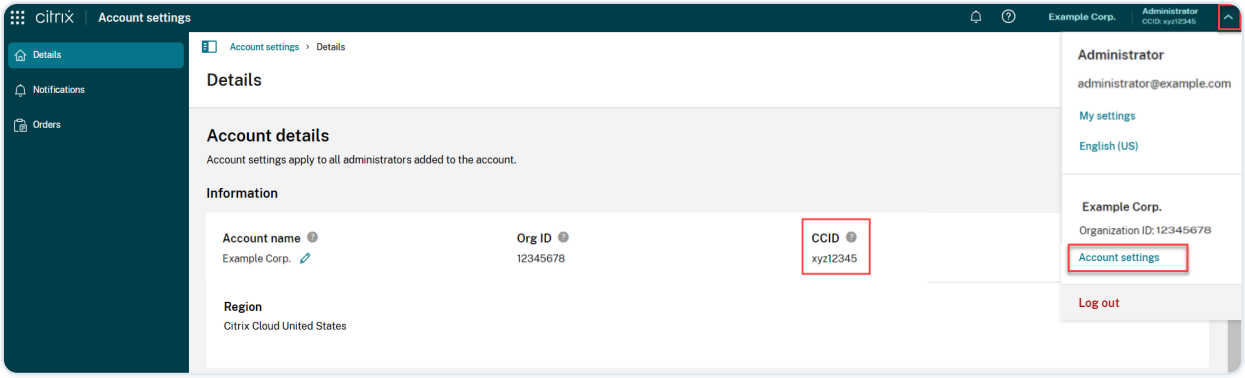
将 `<CUSTOMER_ID>` 替换为您的 Citrix Cloud 客户 ID (CCID)。您可以在 Citrix Cloud 控制台的以下位置找到您的 CCID：

- 控制台右上角，客户名称下方。



- 在“帐户设置”页面上，**Citrix Cloud 客户 ID (CCID)** 下方。

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



查询参数

通过使用 `&` 分隔每个名称-值对，将查询参数添加到端点。例如，要检索欧盟地理区域的出站 FQDN，请使用以下 URL：

`https://api.cloud.com/connectivity/v2/allowlist?customerId=<CCUSTOMER_ID>&direction=outbound&geo=EU`

v2 API 支持以下查询参数：

- **CustomerId**：您的 Citrix Cloud 客户 ID (CCID)。当您传递 customerId 时，API 会在返回列表之前替换返回的 FQDN 中的 `<CUSTOMER_ID>` 占位符（例如，`<CUSTOMER_ID>.xendesktop.net` 变为 `abc123.xendesktop.net`）。您不再需要在下载文件后手动替换每个条目中的 CCID，就像您使用以前的 allowlist.json 文件时那样。
- **Format**：在 `json`（默认）或 `zscaler` 之间选择。如果省略，响应将以 json（默认）格式返回。将 format=zscaler 设置为接收预格式化的响应，以便导入到 Zscaler 配置中。
- **Geo**：如果省略，则默认为 `all` 并返回所有 Citrix Cloud 地理区域的 FQDN。要将响应范围限定为您资源位置所服务的单个地理区域，请将 `geo` 设置为 `us`、`eu` 或 `ap-s` 之一。范围限定会生成一个更短、更有针对性的列表，并避免允许您的部署无法到达的区域。
- **Direction**：如果省略，则默认为 `all` 并返回入站和出站 FQDN。将 `direction=outbound` 设置为仅检索 Cloud Connector 需要访问的 FQDN（典型的防火墙出站用例），或将 `direction=inbound` 设置为 Citrix Cloud 联系您环境的 FQDN。

注意：

位于 `https://fqdnallowlistsa.blob.core.windows.net/fqdnallowlist-commercial/allowlist.json` 的旧允许列表文件在有限的过渡期内仍然可用，但已弃用供客户使用。请迁移到上面的 API 端点。Blob URL 仅暂时保留用于内部连接器连接检查，并将在未来版本中删除。

v2 API 端点目前可供 Citrix Cloud 商业客户使用。

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

网关服务存在点

allowlist.json 文件中包含的一些 FQDN 也包含在 Citrix Gateway Service -- Points of Presence (PoPs) 中。但是，Citrix Gateway Service -- Points of Presence (PoPs) 也包含客户端访问的 FQDN，例如：

- 全球网关服务点：global-s.g.nssvc.net
- Azure网关服务点：azure-s.g.nssvc.net

证书验证

Cloud Connector 二进制文件和 Cloud Connector 联系的端点受 X.509 证书保护，这些证书在软件安装时进行验证。为了验证这些证书，每台 Cloud Connector 计算机都必须满足某些要求。有关这些要求的完整列表，请参阅 证书验证要求。

SSL 解密

在某些代理上启用 SSL 解密可能会阻止 Cloud Connector 成功连接到 Citrix Cloud。有关解决此问题的更多信息，请参阅 CTX221535。

适用于云服务的 Citrix Connector™ 设备

Connector Appliance 是一种可以在您的虚拟机管理程序中部署的设备。托管 Connector Appliance 的虚拟机管理程序位于您与 Citrix Cloud 配合使用的资源所在的网络中。Connector Appliance 连接到 Citrix Cloud，使其能够根据需要操作和管理您的资源。

有关安装 Connector Appliance 的要求，请参阅 系统要求。

为了运行，Connector Appliance 需要在端口 443 上进行出站连接。但是，要在包含 Internet 代理服务器或防火墙限制的环境中运行，可能需要进一步配置。

为了正常运行和使用 Citrix Cloud 服务，必须能够访问以下地址：

- `https://*.cloud.com`
- `https://*.citrixworkspacesapi.net`
- `https://*.citrixnetworkapi.net`
- `https://*.*.nssvc.net`

  无法启用所有子域的客户可以使用以下地址

  - `https://*.g.nssvc.net`

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

  - `https://*.c.nssvc.net`

- `https://*.servicebus.windows.net`
- `https://ctxccopspacrconnappprod.azurecr.io`
- `https://ctxccopspacrconnappprod.eastus.data.azurecr.io`

网络要求

确保您的 Connector Appliance 环境具有以下配置：

- 网络允许 Connector Appliance 使用 DHCP 获取 DNS 和 NTP 服务器、IP 地址、主机名和域名，或者您可以在 Connector Appliance 控制台 中手动设置网络设置。
- 网络未配置为使用链路本地 IP 范围 169.254.0.1/24、169.254.64.0/18 或 169.254.192.0/18，这些范围由 Connector Appliance 内部使用。
- 虚拟机管理程序时钟设置为协调世界时 (UTC) 并与时间服务器同步，或者 DHCP 向 Connector Appliance 提供 NTP 服务器信息。
- 如果您将代理与 Connector Appliance 结合使用，则该代理必须未经身份验证或使用基本身份验证。

Citrix Analytics 服务连接

- 对于产品内消息（包括新功能、重要通信和客户调查），必须能够访问以下地址：
  - `https://citrix-cloud-content.customer.pendo.io/`
  - `https://citrix-cloud-data.customer.pendo.io/`
- 其他要求：先决条件

有关将数据源载入服务的更多信息，请参阅支持的数据源。

NetScaler® Console 服务连接

有关完整的 Internet 连接要求，请参阅 NetScaler 产品文档中的支持的端口。

Citrix DaaS 连接

Cloud Connectors 到 DaaS 的连接

除了Cloud Connector 常见服务连接要求之外，当与 DaaS 结合使用时，Cloud Connectors 还需要连接到以下各项：

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

- `https://[customerid].xendesktop.net`，其中 `[customerid]` 是 Citrix Cloud 管理控制台的**服务主体**选项卡（**身份和访问管理 > API 访问 > 服务主体**）上显示的客户 ID 参数。
- 使用 快速部署 安装 Citrix DaaS 的客户需要使这些附加地址可访问：
  - `https://*.apps.cloud.com`
  - 此 `AzureCloud` 服务标签
- `https://*.*.nssvc.net`
  - 无法启用所有子域的客户可以使用以下地址代替：
    - `https://*.g.nssvc.net`
    - `https://*.c.nssvc.net`

有关 Cloud Connector 如何与服务通信的概述，请参阅 Citrix Tech Zone 网站上的 Citrix DaaS 图。

连接到 DaaS 管理控制台

要管理 DaaS，除了 Citrix Cloud 管理控制台，您还必须能够连接到以下各项：

- `https://*.citrixworkspacesapi.net` (Rendezvous 协议不需要)
- `https://*.citrixnetworkapi.net` (Rendezvous 协议不需要)
- `https://*.cloud.com` (Rendezvous 协议不需要)
- `https://[customerid].xendesktop.net`，其中 `[customerid]` 是显示在 Citrix Cloud 管理控制台的**服务主体**选项卡（**身份和访问管理 > API 访问 > 服务主体**）上的客户 ID 参数。
- `https://*.*.nssvc.net` (不适用于 思杰 DaaS 标准版（适用于 Azure）)
  - 无法启用所有子域的客户可以使用以下地址代替：
    - `https://*.g.nssvc.net`
    - `https://*.c.nssvc.net`
- 对于产品内消息（包括新功能、重要通信和客户调查），必须能够联系以下地址：
  - `https://citrix-cloud-content.customer.pendo.io/`
  - `https://citrix-cloud-data.customer.pendo.io/`

Citrix DaaS 远程 PowerShell SDK

要使用 Citrix DaaS 远程 PowerShell SDK，请将以下 URL 列入白名单：

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

- `https://*.cloud.com`
- `https://*.citrixworkspacesapi.net/[customerid]`
- `https://[customerid].xendesktop.net:443`

使用 Rendezvous 协议时的 VDA 连接

使用 Citrix Gateway Service 时，Rendezvous 协议允许 VDA 绕过 Citrix Cloud Connectors，直接安全地连接到 Citrix Cloud 控制平面。

无论您使用的是哪个协议版本，VDA 都必须能够联系上面列出的管理控制台地址，除非另有说明。有关 Rendezvous 协议要求的完整列表，请参阅 Citrix DaaS 产品文档的以下部分：

- Rendezvous 版本1
- Rendezvous 版本2

本地主机缓存要求

如果您的防火墙执行数据包检测并且您想使用本地主机缓存功能，请确保您的防火墙接受 XML 和 SOAP 流量。此功能需要下载 MDF 文件的能力，这在 Cloud Connector 将配置数据与 Citrix Cloud 同步时发生。这些文件通过 XML 和 SOAP 流量传送到 Cloud Connector。如果防火墙阻止此流量，则 Cloud Connector 和 Citrix Cloud 之间的同步将失败。如果发生中断，用户将无法继续工作，因为 Cloud Connector 上的配置数据已过期。

有关此功能的更多信息，请参阅 Citrix DaaS 产品文档中的本地主机缓存。

VDA 升级要求

使用 Citrix DaaS 的完整配置界面，您可以按目录或按计算机升级 VDA。您可以立即升级它们，也可以在预定时间升级。有关 VDA 升级功能的更多信息，请参阅使用完整配置界面升级 VDA。

使用此功能时，请确保满足以下连接要求：

- 以下 Azure CDN URL 已添加到允许列表。此功能从 Azure CDN 端点下载 VDA 安装程序。
  - 生产 - 美国 (US)：`https://prod-us-vus-storage-endpoint.azureedge.net/*`
  - 生产 - 欧盟 (EU)：`https://prod-eu-vus-storage-endpoint.azureedge.net/*`
  - 生产 - 亚太南部 (APS)：`https://prod-aps-vus-storage-endpoint.azureedge.net/*`
  - 生产 - 日本 (JP)：`https://prod-jp-vus-storage-endpoint.azureedge.net/*`
- 此功能验证 VDA 安装程序是否由有效证书签名。请确保以下 URL 已添加到允许列表，以进行证书有效性和吊销检查：

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

  - `http://crl3.digicert.com/*`
  - `http://crl4.digicert.com/*`
  - `http://ocsp.digicert.com/*`
  - `http://cacerts.digicert.com/*`
- 此功能需要 VDA 升级代理才能工作。在 VDA 上运行的 VDA 升级代理与 Citrix DaaS 通信。请确保以下 URL 已添加到允许列表中：
  - `https://[customerId].xendesktop.net/citrix/VdaUpdateService/*`，其中 `[customerid]` 是在 Citrix Cloud 管理控制台的“**服务主体**”选项卡（**身份和访问管理 > API 访问 > 服务主体**）上显示的客户 ID 参数。
  - `http://xendesktop.net/citrix/VdaUpdateService/*`

Endpoint Management 服务连接

Citrix 资源位置 / Cloud Connector：

- Cloud Connector 常见服务连接要求
- 其他要求：/zh-cn/citrix-endpoint-management/endpoint-management.html

管理控制台：

- `https://*.citrix.com`
- `https://*.citrixworkspacesapi.net`
- `https://*.cloud.com`
- `https://*.blob.core.windows.net`
- 其他要求：/zh-cn/citrix-endpoint-management/endpoint-management.html

Citrix Gateway 服务连接

Cloud Connector 连接到 Citrix Gateway 服务

当通过 Cloud Connector 使用 Citrix Gateway Service（即不使用 Rendezvous v2）时，除了 (/zh-cn/citrix-cloud/overview/requirements/internet-connectivity-requirements.html#cloud-connector-common-service-connectivity-requirements) 之外，Cloud Connector 还需要访问：

- `https://*.*.nssvc.net`

无法启用所有子域的客户可以使用以下地址：

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

- `https://*.g.nssvc.net`
- `https://*.c.nssvc.net`

重要提示：

无法对 Citrix Gateway 地址执行 SSL 拦截。在某些代理上启用 SSL 拦截可能会阻止 Cloud Connector 成功连接到 Citrix Cloud。

客户端连接到 Citrix Gateway Service

要使用 Citrix Gateway Service，客户端设备需要访问：

- `https://*.*.nssvc.net`

无法启用所有子域的客户可以使用以下地址：

- `https://*.g.nssvc.net`
- `https://*.c.nssvc.net`

SD-WAN Orchestrator 服务连接

有关完整的 Internet 连接要求，请参阅 Citrix SD-WAN Orchestrator 服务使用先决条件。

远程浏览器隔离（原安全浏览器）服务

Cloud Connector 连接到远程浏览器隔离服务

Cloud Connector 除了 (#cloud-connector-common-service-connectivity-requirements) 之外，不需要任何额外的连接。

连接到管理控制台

- `https://*.cloud.com`
- `https://*.citrixworkspacesapi.net`
- `https://browser-release-a.azureedge.net`
- `https://browser-release-b.azureedge.net`

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

客户端连接到 Citrix Secure Private Access™

- `https://*.netscalergateway.net`
- `https://*.*.nssvc.net`
  - 无法启用所有子域的客户可以使用以下地址：
    - `https://*.g.nssvc.net`
    - `https://*.c.nssvc.net`

客户端连接到全局应用配置服务

`https://discovery.cem.cloud.us`

有关此服务的更多信息，请参阅 自定义 Workspace 应用程序设置。

最终用户与应用商店的连接

本节列出了客户端在使用 Citrix Workspace 应用程序或 Web 浏览器访问其云应用商店时必须能够访问的 URL。

应用商店 URL

用户通过云 URL（例如 `https://<customername>.cloud.com`）或自定义 URL 访问应用商店。有关详细信息，请参阅 配置对应用商店的访问。

身份验证

思杰云：

- `https://accounts.cloud.com`
- `https://accounts-dsauthweb.cloud.com`
- `https://accounts-webassets.cloud.com` - 用于图形界面资产
- `https://login.cloud.com` - 仅当您使用 Active Directory 或 Active Directory + 令牌作为身份提供程序时才需要

Citrix 云 日本：

- `https://accounts.citrixcloud.jp`
- `https://accounts-dsauthweb.citrixcloud.jp`

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

- `https://accounts-webassets.citrixcloud.jp` - 用于图形界面资产
- `https://login.citrixcloud.jp` - 仅当您使用 Active Directory 或 Active Directory + 令牌作为身份提供程序时才需要

Citrix 政府云：

- `https://accounts.cloud.us`
- `https://accounts-dsauthweb.cloud.us`
- `https://login.cloud.us` - 仅当您使用 Active Directory 或 Active Directory + 令牌作为身份提供程序时才需要

`https://accounts-webassets.cloud.us` 对于 Citrix Cloud Government 不是必需的。`https://accounts.cloud.us` 用于图形界面资产。

如果您使用的是第三方身份提供程序，请联系供应商以获取所需的 URL。

存储图形界面资产

- `https://ctx-ws-assets.cloud.com`

对于 Citrix Cloud Government，这在将来可能会更改为 `https://ctx-ws-assets.cloud.us`。

个性化、通知和功能发布

当使用 Citrix Workspace 应用程序而非 Web 浏览器时，根据您组织的区域，需要以下 URL。

美国：

- `https://customer-interface-personalization.us.wsp.cloud.com`
- `https://user-personalization.us.wsp.cloud.com`
- `https://admin-notification.us.wsp.cloud.com`
- `https://feature-rollout.us.wsp.cloud.com`

欧盟：

- `https://customer-interface-personalization.eu.wsp.cloud.com`
- `https://user-personalization.eu.wsp.cloud.com`
- `https://admin-notification.eu.wsp.cloud.com`
- `https://feature-rollout.eu.wsp.cloud.com`

亚太南部：

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

- `https://customer-interface-personalization.ap-s.wsp.cloud.com`
- `https://user-personalization.ap-s.wsp.cloud.com`
- `https://admin-notification.ap-s.wsp.cloud.com`
- `https://feature-rollout.ap-s.wsp.cloud.com`

Citrix Cloud 日本：

- `https://customer-interface-personalization.jp.wsp.citrixcloud.jp`
- `https://user-personalization.jp.wsp.citrixcloud.jp`
- `https://admin-notification.jp.wsp.citrixcloud.jp`
- `https://feature-rollout.jp.wsp.citrixcloud.jp`

Citrix Cloud 政府版：

- `https://customer-interface-personalization.us.wsp.cloud.us`
- `https://user-personalization.us.wsp.cloud.us`
- `https://admin-notification.us.wsp.cloud.us`
- `https://feature-rollout.us.wsp.cloud.us`

品牌图片

- 美国：`https://cips-iws-prod-eus2-cip-cdn.azureedge.net`
- 欧盟：`https://cips-iws-prod-weu-cip-cdn.azureedge.net`
- AP-S `https://cips-iws-prod-aue-cip-cdn.azureedge.net`
- Citrix Cloud 日本版 `https://cips-wspjp-prod-jpe-cip-cdn.azureedge.net`
- Citrix Cloud 政府版 `https://cips-wspgov-prod-usgv-cip-cdn.azureedge.us`

个人资料图片

如果用户上传个人资料图片，则需要访问以下 URL：

- 美国：`https://wups-us-iws-cloud.azureedge.net`
- 欧盟：`https://wups-eu-iws-cloud.azureedge.net`
- 亚太南部：`https://wups-ap-s-iws-cloud.azureedge.net`
- Citrix Cloud 日本：`https://wups-wspjp-jp-production.azureedge.net`

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

应用程序图标

思杰云：

- `https://wscs-cdn.wsp.cloud.com/icons`

Citrix Cloud 日本：

- `https://wscs-cdn.wsp.citrixcloud.jp/icons`

思杰政府云：

- `https://wscs-cdn.wsp.cloud.us/icons`

潘多

用于产品内消息，包括新功能和重要通知。

- `https://citrix-cloud-content.customer.pendo.io`

Citrix 分析服务

- `locus.analytics.cloud.com`

根据租户的地理位置，启用对以下列表中相应 URL 的访问：

- 美国：`citrixanalyticseh.servicebus.windows.net`
- 欧盟：`citrixanalyticseheu.servicebus.windows.net`
- 亚太南部：`citrixanalyticsehaps.servicebus.windows.net`

其他服务

对于客户端可能需要连接的其他服务，请参阅：

- 客户端连接到 Citrix Gateway 服务
- 客户端连接到 Citrix Secure Private Access 服务
- 客户端连接到 Global App Configuration 服务

Citrix 联合身份验证服务 (FAS)

请参阅 Citrix 联合身份验证服务与 Citrix Cloud 之间的连接。

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

工作区环境管理™ 服务连接

Citrix 资源位置 / Cloud Connector / 代理：

`https://*.wem.cloud.com`

有关完整要求，请参阅 Workspace Environment Management 服务文档中的连接先决条件。

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

规划您的部署

本文概述了规划 Citrix Cloud™ 部署的关键注意事项。它提供了服务试用、云订阅、区域以及部署和迁移资源的概述。

服务试用和订阅

Citrix Cloud 为大多数云服务提供试用。试用版具有与付费服务相同的功能，因此适用于概念验证或试点部署。有关详细信息，请参阅 Citrix Cloud 服务试用。

通常，付费服务授权可以是每月、每年或有期限的。当授权即将到期时，Citrix Cloud 会发送提醒，以便您可以在不造成不必要服务中断的情况下续订授权。有关续订授权的更多信息，请参阅 延长 Citrix Cloud 服务订阅。

区域和服务存在

Citrix Cloud 在三个区域提供服务：美国、欧盟和亚太南部。注册 Citrix Cloud 时，您必须选择最适合您的性能和业务需求的区域。

要了解有关选择区域以及每个区域中可用服务的更多信息，请参阅 地理注意事项。

部署资源

- Citrix Cloud 弹性
- Tech Zone 概念验证指南
- Tech Zone 参考架构
- Cloud Connector 的规模和大小注意事项
- 本地主机缓存的规模和大小注意事项
- Citrix DaaS 的本地 StoreFront 身份验证参考架构

迁移资源

- 概念验证：自动化配置工具
- 将本地 Citrix 虚拟应用和桌面 迁移到 Citrix 云

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

- 将 Citrix 虚拟应用和桌面 从 VMware vSphere 迁移到 Microsoft Azure 上的 Citrix DaaS
- 使用 Citrix Endpoint Management 从 Android 设备管理员迁移到 Android Enterprise

更多信息

- Citrix Discussions: Citrix Cloud：Citrix Cloud 和 Citrix 云服务的社区支持论坛
- Citrix 培训：
  - Citrix Cloud 基础知识
  - Citrix 身份和身份验证简介

Citrix Cloud™ 服务试用

针对单个 Citrix Cloud 服务的试用通过 Citrix Cloud 管理控制台提供。服务试用版的功能与购买的服务相同，因此它们适用于概念验证 (POC) 或试点部署。

当您准备购买 Citrix Cloud 服务时，您的试用版将转换为生产服务。无需重新配置任何内容或创建单独的生产帐户。

服务试用概述

本节中的信息适用于大多数 Citrix Cloud 服务试用版。具有不同试用条款的服务将在单独的部分中介绍。

	CITRIX CLOUD 试用
允许的最终用户数量	25
试用期最长持续时间	60 个日历日
数据保留期限	试用期满后 90 个日历日
可用性	受限可用性
资源位置	客户提供和配置
用户会话时长	无限制
本地 微软 活动目录 集成	是
资源位置选择	是

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

	CITRIX CLOUD 试用
部署到本地	是
Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops™ 服务）	完整功能集
端点管理	完整功能集
可自定义	是

请求服务试用

Citrix Cloud 试用访问权限是按服务管理的。对于某些服务，您可以按照本文中的 请求服务试用 所述请求试用。对于其他服务，您必须先请求演示，然后才能获得试用访问权限，如本文中的 请求服务演示 所述。

服务试用期

对于大多数服务，在您的试用请求获得批准后，您有 60 天的时间试用该服务。您只能为一项服务请求一次试用。

购买服务订阅

您可以在试用期间或数据保留期间随时购买服务订阅。有关详细信息，请参阅 购买 Citrix Cloud 服务。

购买订阅后，您的试用版将转换为生产服务。管理员和用户可以访问该服务，并且您在试用期间添加的任何数据都将保持不变。

适用于 Azure 的 Citrix DaaS Standard

本节介绍适用于 Azure 的 Citrix DaaS Standard（以前称为适用于 Azure 的 Citrix Virtual Apps and Desktops Standard）的以下试用类型：

- **自动批准试用：** 在您通过 Citrix Cloud 管理控制台 请求试用 后，试用将自动获得批准并可供使用。
- **销售批准试用：** 在您联系 Citrix® 销售代表请求试用后，销售代表会批准该试用。批准后，试用即可使用。

	自动批准试用	销售批准试用
最长试用期	7 个日历日	14 个日历日

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

	自动批准试用	销售批准试用
数据保留期	试用期结束后 30 个日历日	试用期结束后 90 个日历日

根据试用类型，您有 7 天或 14 天的时间使用该服务。您只能为该服务申请一次试用。

根据试用类型，Citrix 会在试用期结束后 30 天或 90 天内保留您添加到服务中的任何数据。如果您在此保留期内购买了该服务的订阅，管理员和用户可以访问该服务，并且您的数据将保持完整。

您可以通过 Azure Marketplace 或 联系您的 Citrix 销售代表 购买该服务的订阅。

请求服务演示

对于某些服务，您必须先向 Citrix 销售代表请求演示，然后才能试用该服务。请求演示可让您与 Citrix 销售代表讨论您组织的云服务需求。此外，销售代表会确保您拥有成功使用该服务所需的所有信息。

1. 登录您的 Citrix Cloud 帐户。
2. 在管理控制台中，选择您所需服务的“**请求演示**”。将显示该服务的演示请求页面。
3. 填写并提交表单。Citrix 销售代表将与您联系，提供更多信息并指导您使用该服务。

请求服务试用

1. 登录您的 Citrix Cloud 帐户。
2. 在管理控制台中，选择您要试用服务的“**请求试用**”。

当您的试用获得批准并准备就绪时，Citrix 会向您发送电子邮件通知。

注意：

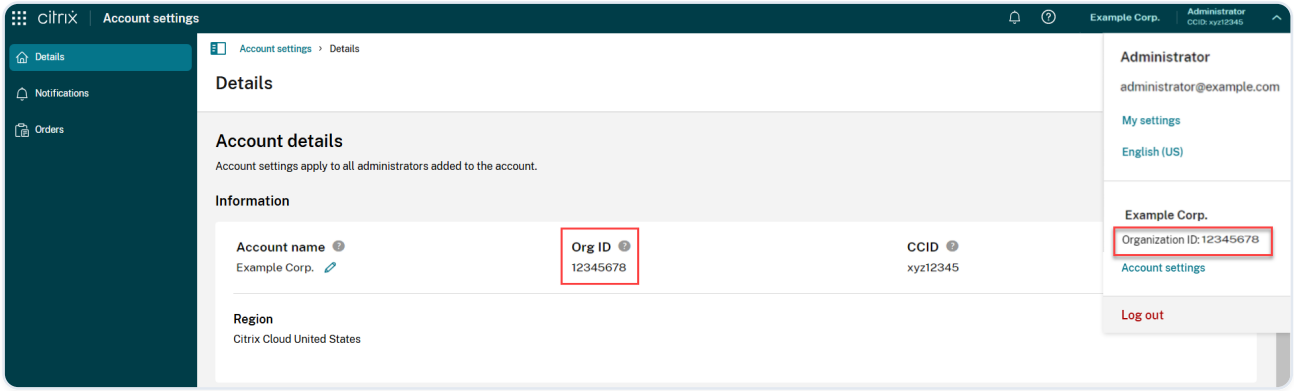
为提供最佳客户体验，Citrix 保留随时批准有限数量参与者试用的权利。

购买 Citrix Cloud 服务

当您准备好将试用版转换为生产服务时，请访问 https://www.citrix.com/buy/ 查找本地 Citrix 合作伙伴。

要购买此服务，您需要您的组织 ID (OrgID)。您的 OrgID 显示在 Citrix Cloud 管理控制台右上角的客户菜单中。您的 OrgID 也显示在“**帐户设置**”页面上。

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



更多信息

- Citrix Cloud 服务的服务条款
- Citrix Cloud 基础知识 课程包含一个简短视频，指导您如何申请试用。完整课程还涵盖 Citrix Cloud 平台的组件及其服务。

延长 Citrix Cloud™ 服务订阅

本文介绍了 Citrix Cloud 服务的已购买订阅如何到期以及如何延长您的订阅。

在本文中，*月度订阅* 指按月购买的服务。*年度订阅* 指按年购买的服务。*多年订阅* 指按多年购买的服务。

注意：

Citrix 服务提供商 (CSP) 可以通过向其 CSP 分销商提交零美元采购订单来延长其订阅。有关 CSP 产品续订和许可的更多信息，请参阅可通过 Citrix Partner Central 网站获取的《*Citrix Cloud 的 Citrix 服务提供商许可指南*》。

到期前

对于月度订阅，Citrix Cloud 不会在到期前发送通知。

对于年度和多年订阅，当您现有订阅即将到期时，Citrix Cloud 会在特定时间间隔通知您。这些通知会提醒您延长订阅并避免服务中断。以下通知会显示在 Citrix Cloud 管理控制台中：

- 到期前 90 天：将显示一个黄色横幅，其中显示需要延长的服务及其到期日期。此通知每七天显示在控制台中，直到服务延长。
- 到期前七天：将显示一个红色横幅，其中显示需要延长的服务及其到期日期。此通知显示在控制台中，直到服务延长。

您可以在这些通知出现时将其关闭；但是，它们会在七天后重新出现。

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

Citrix® 还会向您发送一封电子邮件通知，其中包含需要延长的服务列表及其到期日期。Citrix 会在以下时间间隔发送此通知：

- 到期前 90 天
- 到期前 60 天
- 到期前 30 天
- 到期前七天
- 到期前一天

管理控制台和最终用户会收到额外的警告，以提醒他们订阅的到期状态。当订阅中的所有许可证都已到期（通常在 12 个月期限结束后）时，会触发这些消息。

- 管理员警告：在订阅到期前 30 天开始，Studio 控制台中会出现警告，提醒管理员即将到期。
- 最终用户警告：订阅到期后，最终用户在启动会话时会收到警告消息。
  - 消息文本："Citrix Virtual Apps and Desktops 警告：您的企业 Citrix 环境目前不受支持。请联系您的 IT 部门解决此问题。"

到期后：服务阻止和数据保留

- 合同到期后，对 Citrix Cloud 服务的访问将立即暂停。
- 要恢复服务，客户必须联系其专属 Citrix 代表或客户团队以启动续订流程。

客户管理的 Azure 订阅

如果您将自己的 Azure 订阅与 Citrix Cloud 服务结合使用，则当您将 Azure 订阅连接到该服务时，该服务会安装一个应用程序。如果您不延长 Citrix Cloud 服务订阅，Citrix 不会在 90 天保留期结束后从您的 Azure 订阅中删除此应用程序。您必须删除此应用程序才能将服务从您的 Azure 订阅中完全删除。您可以使用以下方法之一删除该应用程序：

- 如果管理员尚未被阻止访问该服务，请从服务内部删除此应用程序。
- 如果管理员被阻止访问该服务，请从 Azure 门户内部删除此应用程序。

购买服务扩展

要延长您的 Citrix Cloud 服务订阅，请联系您的 Citrix 销售代表。要查找您的销售代表，请执行以下步骤：

1. 登录您的 Citrix 帐户。

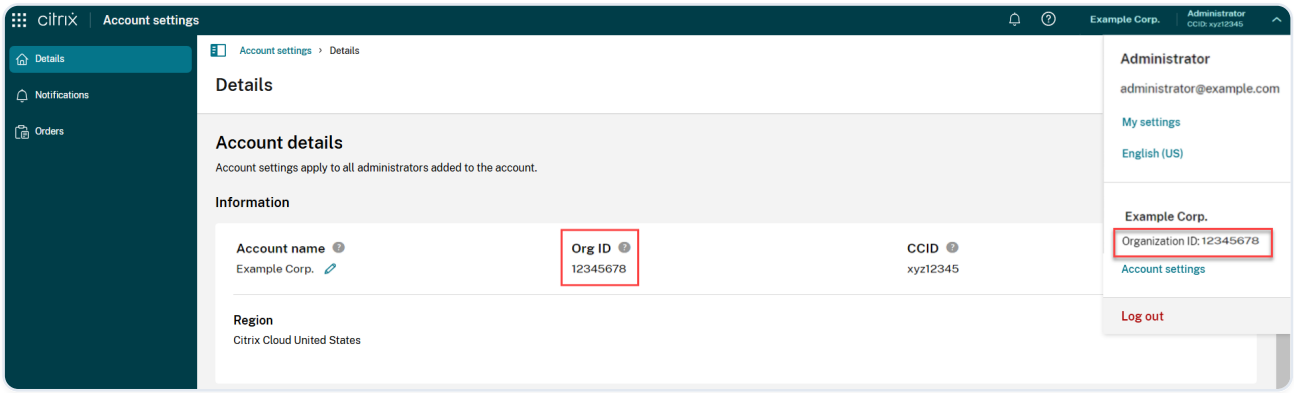
© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. 选择 **Quoting (DOTI)**，然后选择 **Transactions**。您的销售代表及其电子邮件地址显示在此视图的顶部附近。

或者，访问 Citrix 客户服务 页面，获取您所在地理区域的联系信息。

要完成购买，您的销售代表需要您的 Citrix Cloud 帐户的组织 ID。要查找您的组织 ID，请登录您的 Citrix Cloud 帐户。您的组织 ID 显示在以下位置：

- 在 Citrix Cloud 控制台右上角的客户菜单中。
- 在 **帐户设置** 页面上。



地理考量

本文讨论了 Citrix Cloud™ 使用的商业区域以及 Citrix Cloud 商业服务在每个区域的部署情况。

有关 Citrix 公共部门和专用云平台的地理区域和服务部署情况的更多信息，请参阅 Citrix 的其他云平台。

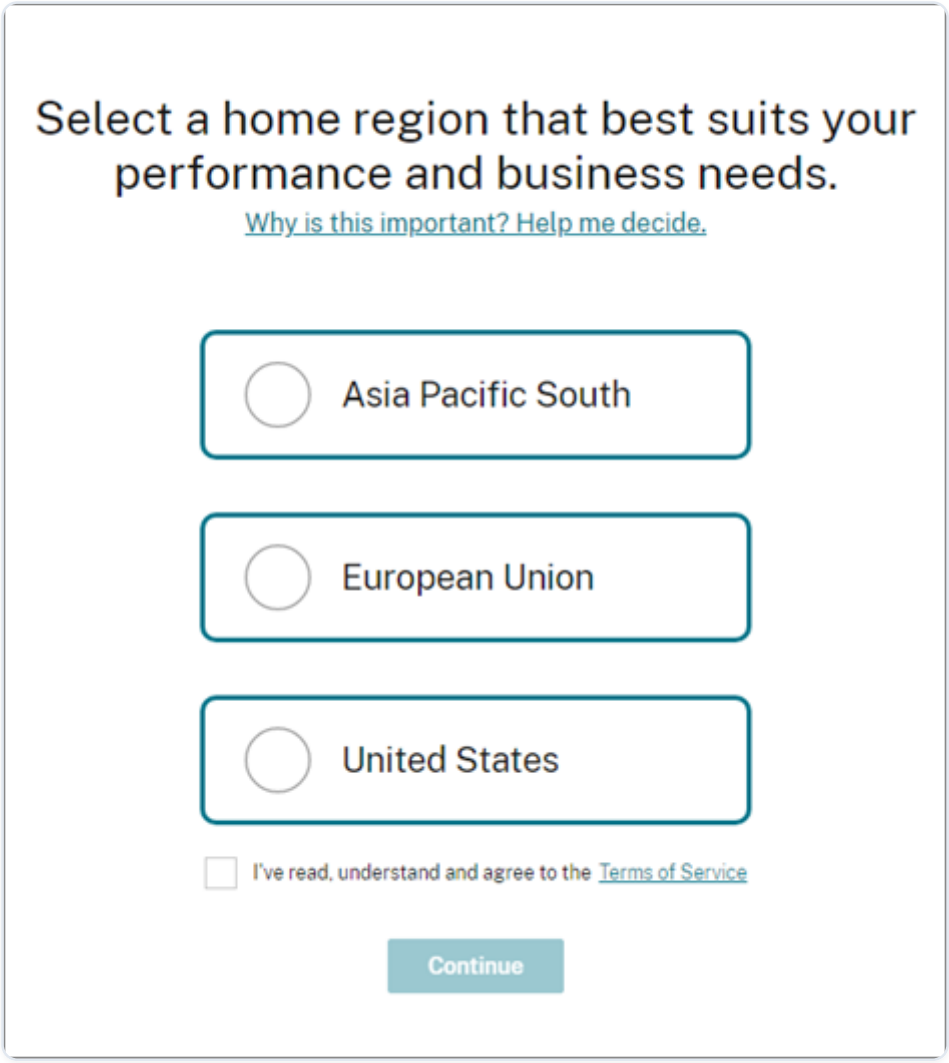
选择区域

当您的组织加入 Citrix Cloud 并且您首次登录时，系统会要求您选择以下区域之一：

- 美国
- 欧盟
- 亚太南部

当您选择一个区域时，在可能的情况下，该地理区域中托管的服务将用于与组织相关的操作。请选择一个与您大多数用户和资源所在位置相对应的区域。

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



重要说明：

- 您只能在组织加入时选择一次区域。以后无法更改区域。
- 如果您位于一个区域并使用另一个区域的服务，任何性能影响都将是最小的。Citrix Cloud 服务旨在全球范围内使用。例如，在美国拥有用户和连接器但在澳大利亚的客户，其延迟影响将是最小的。
- 如果您的区域不支持 Citrix Cloud，请选择一个最接近您大多数用户和资源所在位置的区域。

每个区域的服务部署情况

大多数 Citrix Cloud 服务都是全球复制的。您选择的区域表示连接应建立的首选位置。但是，连接仍可能建立到其他地理区域。当服务在全球复制时，该服务的所有数据都存储在所有区域中。

同样，您的数据可能由 Citrix 关联公司或子处理器 在全球范围内处理，以执行必要的服务。

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

某些服务具有专用的区域实例。某些服务仅具有基于美国的实例。在这些情况下，连接和数据都包含在该地理区域内。

如果您为组织选择的区域中没有可用的服务，则某些信息（例如身份验证数据）可能会根据需要跨区域传输。

服务	美国	欧盟	亚太南部	备注
Citrix Cloud 控制平面	是	是	是	
思杰安全分析™	是	是	是	
Citrix Analytics 性能分析™	是	是	是	
NetScaler® Console（以前称为应用程序交付管理）	是	是	是	请参阅本文中的使用 Console Advisory Connect 轻松载入 NetScaler 实例。 有关控制台本地遥测程序，请参阅(https://docs.netscaler.com/zh-cn/netscaler-application-delivery-management-software/130-adm-0443.html)。
Citrix DaaS™（以前称为 Virtual Apps and Desktops 服务）	是	是	是	服务使用 Citrix Cloud 区域。

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

服务	美国	欧盟	亚太南部	备注
适用于 Azure 的 Citrix DaaS Standard（以前称为适用于 Azure 的 Virtual Apps and Desktops Standard）	是	是	是	服务使用 Citrix Cloud 区域。
适用于 Google Cloud 的 Citrix DaaS Standard（以前称为适用于 Google Cloud 的 Virtual Apps and Desktops Standard）	是	否（使用美国区域）	否（使用美国区域）	
适用于 Google Cloud 的 Citrix DaaS Premium（以前称为适用于 Google Cloud 的 Virtual Apps and Desktops Premium）	是	否（使用美国区域）	否（使用美国区域）	
Citrix 端点管理™	是	是	是	可从多个区域的多个位置中选择。请参阅本文中的Endpoint Management 服务位置。
远程浏览器隔离服务	是	是	是	服务使用 Citrix Cloud 区域。
SD-WAN 编排器	是	是	是	

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

服务	美国	欧盟	亚太南部	备注
Citrix 安全私有访问™	全球复制	全球复制	全球复制	请参阅本文中的 Secure Private Access 存在点。
会话录制服务	是	是	是	
Citrix 虚拟应用基础版™	是	是	是	服务使用 Citrix Cloud 区域。
思杰虚拟桌面精简版™	是	是	是	服务使用 Citrix Cloud 区域。
Web 应用防火墙	是	是	否（使用美国区域）	
工作区环境管理™；思杰优化包	是	是	是	
网络服务	是	否（使用美国区域）	否（使用美国区域）	
许可证使用情况洞察（仅限 CSP）	全球复制	全球复制	全球复制	
思杰网关服务访问节点/POP	多个全球节点；根据需要路由流量以确保最佳体验	多个全球节点；根据需要路由流量以确保最佳体验	多个全球节点；根据需要路由流量以确保最佳体验	您可以配置资源位置以启用用户流量路由到特定区域。有关更多信息，请参阅地理位置路由 - 预览
许可证激活服务	是	是	是	

注意：

某些区域服务可能随附如上表其他部分所述的非区域组件服务，并可由客户自行选择使用。

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

Citrix Cloud 服务使用客户指定的区域来存储客户内容和日志，但由 Citrix 子处理器收集的特定日志除外，或为了服务性能需要非区域存储的情况除外，包括用于支持或故障排除、监控性能、安全性、审计以及实现跨区域身份验证（例如，当欧盟的支持工程师需要访问美国环境时）。客户内容和日志可在全球范围内访问，以执行所需服务。
有关各个服务存储的数据的更多信息，请参阅每个服务的技术安全概述。

使用 Console Advisory Connect 低接触式载入 NetScaler Console 实例

作为基于 Console Advisory Connect 的 Console 实例低接触式载入 的一部分：

- 如果您是现有的 Citrix Cloud 客户，Console 服务租户将在您创建 Citrix Cloud 帐户时选择的同一地理区域中创建。
- 如果您不是现有的 Citrix Cloud 客户，则会引用 Citrix.com 门户中为该客户提及的地址。将在与此引用地址区域对应的地理区域中创建一个占位符 Console 服务租户。如果您将来选择载入 Citrix Cloud，则会在您创建 Citrix Cloud 帐户时选择的同一区域中创建一个新的 Console 服务租户。此外，数据将从占位符 Console 服务租户迁移到新的 Console 服务租户。

Endpoint Management 服务位置

您可以从您的主区域中选择以下 Endpoint Management 服务位置之一：

- 美国东部
- 美国西部
- 欧盟西部
- 东南亚
- 悉尼

Secure Private Access 服务接入点

有关 Secure Private Access 用于确保客户服务连续性和质量的存在点 (PoP) 列表，请参阅 Secure Private Access 服务文档中的所有 Secure Private Access PoP 位置有哪些？。

Pendo 数据驻留和区域注意事项

Citrix 使用 Pendo 在各种产品和服务中提供产品内指导、功能公告和重要通知。Pendo 收集的所有数据均仅在美国 (US) 区域内处理和存储。

此数据驻留仅适用于以下 Citrix 产品和服务的 **Pendo 处理数据**：

- Citrix Cloud 管理控制台

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

- Citrix DaaS（包括工作区环境管理、Web Studio 和会话录制）
- Citrix Studio（本地部署）
- Citrix Director 和 监控工具
- NetScaler (ADC)
- NetScaler Console (ADM) 和 NetScaler Console 服务
- 安全开发者空间
- Citrix Workspace 应用程序（桌面、移动和平板电脑 – 仅限云部署）
- 适用于 iOS 的 Citrix Workspace 应用程序（原生）
- 适用于 Android 的 Citrix Workspace 应用程序（原生）

Citrix 的其他云平台

除了 Citrix Cloud 之外，Citrix 还提供其他与 Citrix Cloud 隔离且独立的云。

Citrix Cloud 政府版

Citrix Cloud Government 允许美国政府机构和美国其他公共部门客户根据法规和合规性要求使用 Citrix 云服务。Citrix Cloud Government 是 Citrix 运营、存储和复制服务及数据以交付 Citrix Cloud Government 服务的地理边界。Citrix 可能会使用位于美国一个或多个州的多个公共或私有云来提供服务。

Citrix Cloud Government 及其提供的服务仅在美国地区可用。

有关更多信息，请参阅 Citrix Cloud Government 产品文档。

Citrix Cloud 日本

Citrix Cloud Japan 允许日本客户在专用的 Citrix 管理环境中使用某些 Citrix Cloud 服务。Citrix Cloud Japan 及其提供的服务仅在日本可用。

有关更多信息，请参阅 Citrix Cloud Japan 产品文档。

Citrix Cloud™ 平台安全部署指南

Citrix Cloud 安全部署指南概述了使用 Citrix Cloud 时的安全最佳实践，并描述了 Citrix Cloud 收集和管理的信息。

服务的技术安全概述

有关 Citrix 云服务中数据安全的更多信息，请参阅以下文章：

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

- 分析技术安全概述
- Endpoint Management 技术安全概述
- 远程浏览器隔离技术安全概述
- Citrix DaaS 技术安全概述
- 适用于 Azure 的 Citrix DaaS Standard 技术安全概述

管理员指南

- 使用强密码并定期更改密码。
- 客户帐户中的所有管理员都可以添加和删除其他管理员。请确保只有受信任的管理员才能访问 Citrix Cloud。
- 默认情况下，客户的管理员拥有对所有服务的完全访问权限。某些服务提供限制管理员访问权限的功能。有关更多信息，请查阅各服务的文档。
- Citrix Cloud 管理员的双因素身份验证通过默认的 Citrix 身份提供程序实现。当管理员注册 Citrix Cloud 或受邀加入 Citrix Cloud 帐户时，他们需要注册多重身份验证 (MFA)。如果客户使用 Microsoft Azure 对 Citrix Cloud 管理员进行身份验证，则可以按照 Microsoft 网站上 配置 Microsoft Entra ID 多重身份验证设置 中所述配置多重身份验证。
- 默认情况下，无论控制台活动如何，Citrix Cloud 都会在 72 小时后自动终止管理员会话。此超时时间无法更改。
- 管理员帐户最多可关联 100 个客户帐户。如果管理员需要管理 100 个以上的客户帐户，他们必须使用不同的电子邮件地址创建单独的管理员帐户来管理额外的客户帐户。或者，他们可以从不再需要管理的客户帐户中移除其管理员身份。

密码合规性

如果存在以下任一情况，Citrix Cloud 会提示管理员更改其密码：

- 当前密码已超过 60 天未使用。
- 当前密码已列入已知泄露密码数据库。

新密码必须满足以下所有条件：

- 至少 8 个字符长（最多 128 个字符）
- 包含至少一个大写字母和一个小写字母
- 包含至少一个数字
- 包含至少一个特殊字符：! @ # $ % \^ * ? + = -

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

更改密码的规则：

- 当前密码不能用作新密码。
- 不能重复使用前 5 个密码。
- 新密码不能与帐户用户名相似。
- 新密码不得列入已知泄露密码数据库。Citrix Cloud 使用 https://haveibeenpwned.com/ 提供的列表来确定新密码是否违反此条件。

加密和密钥管理

Citrix Cloud 控制平面不存储敏感客户信息。相反，Citrix Cloud 会按需检索信息，例如管理员密码（通过明确提示管理员）。

对于静态数据，Citrix Cloud 存储使用 AES-256 位或更高加密强度的密钥进行加密。这些密钥由 Citrix 管理。

对于传输中的数据，Citrix 使用行业标准 TLS 1.2 和最强的密码套件。客户无法控制正在使用的 TLS 证书，因为 Citrix Cloud 托管在 Citrix 拥有的 cloud.com 域上。要访问 Citrix Cloud，客户必须使用支持 TLS 1.2 的浏览器，并且必须配置已接受的密码套件。

建议使用以下强密码：TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384, TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

注意：

虽然需要 TLS 1.2，但某些服务可以协商 TLS 1.3 以增强安全性和性能。建议客户允许其客户端协商 TLS 1.2 和 TLS 1.3。建议使用以下强密码：

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

有关 Citrix Cloud 服务数据如何受到保护的更多信息，请参阅 Citrix 网站上的Citrix Cloud 服务数据保护概述。

有关每个云服务中加密和密钥管理的更多信息，请查阅该服务的文档。

数据主权

Citrix Cloud 控制平面托管在美国、欧盟和澳大利亚。客户对此没有控制权。

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

客户拥有并管理其与 Citrix Cloud 配合使用的资源位置。资源位置可以在客户所需的任何数据中心、云、位置或地理区域中创建。所有关键业务数据（例如文档、电子表格等）都存储在资源位置并由客户控制。

其他服务可能提供在不同区域存储数据的选项。请查阅每个服务的地理注意事项主题或技术安全概述（本文开头列出）。

安全问题洞察

网站 status.cloud.com 提供有关持续影响客户的安全问题的透明度。该站点记录状态和正常运行时间信息。可以选择订阅平台或单个服务的更新。

Citrix 云连接器™

安装云连接器

出于安全和性能原因，Citrix® 建议客户不要在域控制器上安装 Cloud Connector 软件。

此外，Citrix 强烈建议安装 Cloud Connector 软件的计算机位于客户的专用网络中，而不是位于 DMZ 中。有关网络和系统要求以及安装 Cloud Connector 的说明，请参阅 Citrix Cloud Connector 。

配置云连接器

客户负责使安装了 Cloud Connector 的计算机保持最新的 Windows 安全更新。

客户可以在 Cloud Connector 旁边使用防病毒软件。Citrix 支持使用行业标准 AV 产品的客户。

在客户的 Active Directory (AD) 中，Citrix 强烈建议将 Cloud Connector 的计算机帐户限制为只读访问。这是 Active Directory 中的默认配置。此外，客户可以在 Cloud Connector 的计算机帐户上启用 AD 日志记录和审计，以监视任何 AD 访问活动。

登录到托管 Cloud Connector 的计算机

Cloud Connector 允许敏感安全信息传递到 Citrix Cloud 服务中的其他平台组件，但也会存储以下敏感信息：

- 用于与 Citrix Cloud 通信的服务密钥
- 用于 Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops™ 服务）中电源管理的虚拟机管理程序服务凭据

此敏感信息使用托管 Cloud Connector 的 Windows 服务器上的数据保护 API (DPAPI) 进行加密。Citrix 强烈建议只允许权限最高的管理员登录到 Cloud Connector 计算机（例如，执行维护操作）。

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

通常，管理员无需登录这些计算机来管理任何 Citrix 产品。Cloud Connector 在这方面是自我管理的。

不允许最终用户登录到托管 Cloud Connector 的机器。

在 Cloud Connector 机器上安装其他软件

客户可以在安装了 Cloud Connector 的机器上安装防病毒软件和虚拟机管理程序工具（如果安装在虚拟机上）。但是，Citrix 建议客户不要在这些机器上安装任何其他软件。其他软件会产生可能的安全攻击向量，并可能降低整个 Citrix Cloud 解决方案的安全性。

入站和出站端口配置

Cloud Connector 需要开放出站端口 443 以访问互联网。Citrix 强烈建议 Cloud Connector 没有可从互联网访问的入站端口。

客户可以将 Cloud Connector 放置在 Web 代理后面，以监控其出站互联网通信。但是，该 Web 代理必须支持 SSL/TLS 加密通信。

Cloud Connector 可能有其他可访问互联网的出站端口。如果其他端口可用，Cloud Connector 会通过广泛的端口进行协商，以优化网络带宽和性能。

Cloud Connector 必须在内部网络中开放广泛的入站和出站端口。下表列出了所需的基本开放端口集。

客户端端口	服务器端口	服务
49152 -65535/UDP	123/UDP	W32时间
49152 -65535/TCP	135/TCP	RPC 端点映射器
49152 -65535/TCP	464/TCP/UDP	Kerberos 密码更改
49152 -65535/TCP	49152-65535/TCP	LSA、SAM、Netlogon 的远程过程调用 (*)
49152 -65535/TCP/UDP	389/TCP/UDP	LDAP
49152 -65535/TCP	3268/TCP	LDAP GC
53, 49152 -65535/TCP/UDP	53/TCP/UDP	DNS
49152 -65535/TCP	49152 -65535/TCP	FRS RPC (*)

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

客户端端口	服务器端口	服务
49152 -65535/TCP/UDP	88/TCP/UDP	科尔贝罗斯
49152 -65535/TCP/UDP	445/TCP	SMB

Cloud Connector 使用 LDAP 签名和密封来保护与域控制器的连接。这意味着不需要通过 SSL 的 LDAP (LDAPS)。有关 LDAP 签名的更多信息，请参阅 如何在 Windows Server 中启用 LDAP 签名和 Microsoft 启用 LDAP 通道绑定和 LDAP 签名的指南。

Citrix Cloud 中使用的每项服务都会扩展所需的开放端口列表。有关更多信息，请查阅以下资源：

- 技术安全概述 针对每项服务（本文开头列出）
- 适用于 Citrix Cloud 服务的 Internet 连接要求
- 控制台服务端口要求
- Endpoint Management 端口要求

监视出站通信

Cloud Connector 通过端口 443 出站与 Internet 通信，包括与 Citrix Cloud 服务器和 Microsoft Azure Service Bus 服务器通信。

Cloud Connector 与本地网络上的域控制器通信，这些域控制器位于托管 Cloud Connector 的计算机所在的 Active Directory 林中。

在正常运行期间，Cloud Connector 仅与 Citrix Cloud 用户界面中**身份和访问管理**页面上未禁用的域中的域控制器通信。

Citrix Cloud 中的每项服务都会扩展 Cloud Connector 在正常运行期间可能联系的服务器和内部资源列表。此外，客户无法控制 Cloud Connector 发送给 Citrix 的数据。有关服务的内部资源以及发送给 Citrix 的数据的更多信息，请查阅以下资源：

- 每项服务的技术安全概述（本文开头列出）
- 适用于 Citrix Cloud 服务的Internet 连接要求

查看 Cloud Connector 日志

与管理员相关或可供管理员操作的任何信息都可在 Cloud Connector 计算机上的 Windows 事件日志中找到。

在以下目录中查看 Cloud Connector 的安装日志：

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

- %AppData%\\Local\\Temp\\CitrixLogs\\CloudServicesSetup
- %windir%\\Temp\\CitrixLogs\\CloudServicesSetup

Cloud Connector 发送到云的日志位于 %ProgramData%\\Citrix\\WorkspaceCloud\\Logs 中。

当 WorkspaceCloud\\Logs 目录中的日志超过指定大小阈值时，这些日志将被删除。管理员可以通过调整注册表项 HKEY_LOCAL_MACHINE\\SOFTWARE\\Citrix\\CloudServices\\AgentAdministration\\MaximumLogSpaceMegabytes 的值来控制此大小阈值。

SSL/TLS 配置

托管 Cloud Connector 的 Windows Server 必须启用 (#encryption-and-key-management) 中详述的密码。

Cloud Connector 必须信任 Citrix Cloud SSL/TLS 证书和 Microsoft Azure Service Bus SSL/TLS 证书所使用的证书颁发机构 (CA)。Citrix 和 Microsoft 将来可能会更改证书和 CA，但始终使用属于标准 Windows 受信任发布者列表的 CA。

Citrix Cloud 中的每项服务可能具有不同的 SSL 配置要求。有关详细信息，请查阅每项服务的 (#technical-security-overviews-for-services)（本文开头列出）。

安全合规性

为确保安全合规性，Cloud Connector 会自行管理。请勿禁用重新启动或对 Cloud Connector 施加其他限制。这些操作会阻止 Cloud Connector 在有关键更新时自行更新。

客户无需采取任何其他措施来应对安全问题。Cloud Connector 会自动应用任何安全修复。

适用于云服务的 Citrix Connector™ 设备

安装 Connector 设备

Connector 设备托管在管理程序上。此管理程序必须位于您的专用网络中，而不能位于 DMZ 中。

确保 Connector 设备位于默认阻止访问的防火墙内。使用允许列表仅允许来自 Connector 设备的预期流量。

确保托管 Connector 设备的管理程序已安装最新的安全更新。

有关网络和系统要求以及安装 Connector 设备的说明，请参阅 (/zh-cn/citrix-cloud/citrix-cloud-resource-locations/connector-appliance.html)。

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

登录到托管 Connector 设备的主机管理程序

Connector Appliance 包含用于与 Citrix Cloud 通信的服务密钥。仅允许权限最高的管理员登录到托管 Connector Appliance 的虚拟机管理程序（例如，执行维护操作）。通常，管理员无需登录这些虚拟机管理程序来管理任何 Citrix 产品。Connector Appliance 是自我管理的。

入站和出站端口配置

Connector Appliance 需要打开出站端口 443 以访问互联网。Citrix 强烈建议 Connector Appliance 没有可从互联网访问的入站端口。

您可以将 Connector Appliance 放置在 Web 代理后面，以监控其出站互联网通信。但是，Web 代理必须支持 SSL/TLS 加密通信。

Connector Appliance 可能有其他可访问互联网的出站端口。如果有其他端口可用，Connector Appliance 会通过广泛的端口进行协商，以优化网络带宽和性能。

Connector Appliance 必须在内部网络中打开广泛的入站和出站端口。下表列出了所需的基本开放端口集。

连接方向	连接器设备端口	外部端口	服务
入站	443/TCP	任意	本地 Web UI
出站	49152-65535/UDP	123/UDP	NTP
出站	53, 49152-65535/TCP/UDP	53/TCP/UDP	DNS
出站	67/UDP	68/UDP	DHCP 和广播
出站	49152 -65535/UDP	123/UDP	W32Time 服务
出站	49152 -65535/TCP	464/TCP/UDP	Kerberos 密码更改
出站	49152 -65535/TCP/UDP	389/TCP/UDP	LDAP
出站	49152 -65535/TCP	3268/TCP	LDAP GC
出站	49152 -65535/TCP/UDP	88/TCP/UDP	Kerberos 协议

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

连接方向	连接器设备端口	外部端口	服务
出站	49152 -65535/TCP/UDP	445/TCP	SMB
出站	137/UDP	137/UDP	NetBIOS 名称服务
出站	138/UDP	138/UDP	NetBIOS 数据报
出站	139/TCP	139/TCP	NetBIOS 会话

Citrix Cloud 中使用的每项服务都会扩展所需的开放端口列表。有关更多信息，请查阅以下资源：

- 技术安全概述（针对每项服务，列于本文开头）
- Citrix Cloud 服务的系统和连接要求

监视出站通信

Connector Appliance 通过端口 443 与 Citrix Cloud 服务器进行出站 Internet 通信。

Citrix Cloud 中的每项服务都会扩展 Connector Appliance 在正常运行期间可能联系的服务器和内部资源列表。此外，客户无法控制 Connector Appliance 发送给 Citrix 的数据。有关服务的内部资源以及发送给 Citrix 的数据的更多信息，请查阅以下资源：

- 技术安全概述（针对每项服务，列于本文开头）
- Citrix Cloud 服务的系统和连接要求

查看 Connector Appliance 日志

您可以下载包含各种日志文件的 Connector Appliance 诊断报告。有关获取此报告的更多信息，请参阅适用于云服务的 Connector Appliance。

SSL/TLS 配置

Connector Appliance 不需要任何特殊的 SSL/TLS 配置。

Connector Appliance 信任 Citrix Cloud SSL/TLS 证书使用的证书颁发机构 (CA)。Citrix 将来可能会更改证书和 CA，但始终会使用 Connector Appliance 信任的 CA。

Citrix Cloud 中的每项服务可能具有不同的 SSL 配置要求。有关更多信息，请查阅每项服务的 技术安全概述（本文开头列出）。

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

安全合规性

为确保安全合规性，Connector Appliance 会自行管理，您无法通过控制台登录它。

您无需采取任何其他措施来应对连接器安全问题。Connector Appliance 会自动应用所有安全修复程序。

确保托管 Connector Appliance 的虚拟机管理程序已安装最新的安全更新。

在您的 Active Directory (AD) 中，我们建议将 Connector Appliance 计算机帐户限制为只读访问。这是 Active Directory 中的默认配置。此外，客户可以在 Connector Appliance 计算机帐户上启用 AD 日志记录和审计，以监控任何 AD 访问活动。

处理受损帐户的指南

- 审计 Citrix Cloud 中的管理员列表，并删除任何不受信任的管理员。
- 禁用公司 Active Directory 中任何受损的帐户。
- 联系 Citrix 并请求轮换为客户所有 Cloud Connector 存储的授权密钥。根据泄露的严重程度，采取以下措施：
  - **低风险：** Citrix 可以随着时间推移轮换密钥。Cloud Connector 将继续正常运行。旧的授权密钥将在 2-4 周内失效。在此期间监控 Cloud Connector，以确保没有意外操作。
  - **持续高风险：** Citrix 可以撤销所有旧密钥。现有的 Cloud Connector 将不再运行。要恢复正常操作，客户必须在所有适用的计算机上卸载并重新安装 Cloud Connector。

适用于 Citrix DaaS™ 的本地 StoreFront™ 身份验证参考架构

尽管 Citrix® StoreFront Cloud 可以满足大多数 Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops™ 服务）用例的需求，但仍有一些用例和要求需要将 StoreFront 托管在客户的数据中心或资源位置。本文介绍了高级架构以及组件如何与 Active Directory 设计支持的各种身份验证场景进行交互。本文假设 StoreFront 和 Gateway 组件在每个数据中心共同托管。

维护本地 StoreFront 的原因

- 支持不具备互联网连接的客户端。
- 启用本地主机缓存功能以提高弹性。
- 域直通和智能卡身份验证。
- 深度自定义，例如商店插件。
- 托管具有不同配置的多个 StoreFront 商店。

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

作为资源域的父子域

父子域作为资源域(/en-us/citrix-cloud/media/adv-concepts-parent-child-resource-domain.png)

在此场景中，子域充当虚拟桌面代理 (VDA) 和 StoreFront 实例的资源域。父域包含将访问子域中资源的用户。

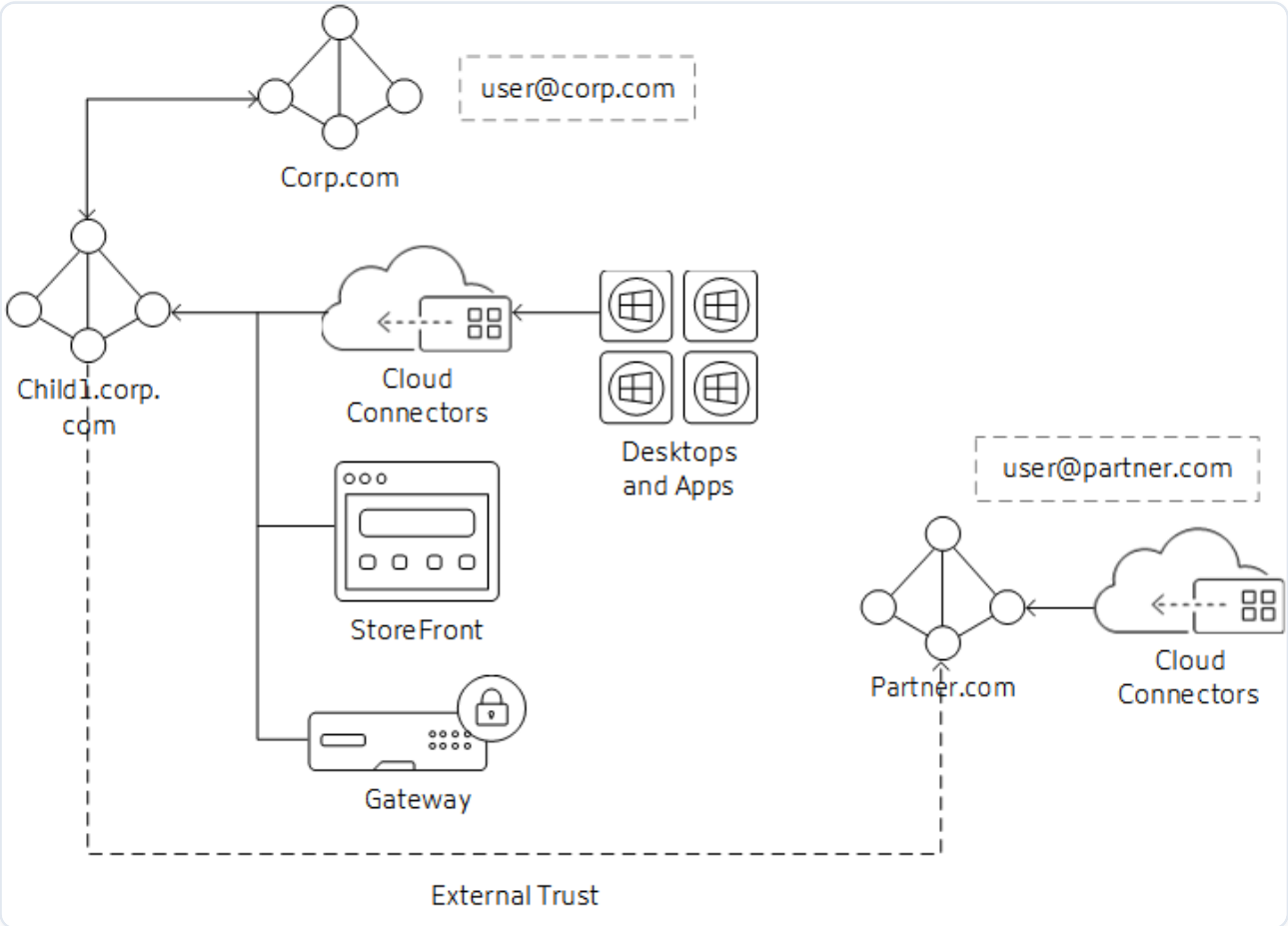
1. Cloud Connector 仅加入子域。子域和父域之间的双向可传递信任允许 Cloud Connector 与父域中的全局编录进行通信。
2. StoreFront 已加入子域。商店配置为支持用户名/密码和 Citrix Gateway 直通身份验证。用户名/密码身份验证配置为信任任何域。
3. Citrix Gateway 身份验证配置文件配置为父域使用 UPN 作为主要登录方法。如果有用户需要从子域进行身份验证，则子域的 LDAP 身份验证配置文件和策略也必须绑定到 Gateway vServer。
4. 编辑 Citrix Gateway 会话操作系统和 Web 配置文件，并将“已发布的应用程序/单点登录域”设置留空（可能需要设置覆盖设置）。

连接工作流

1. mailto:User@corp.com 登录到 Citrix Gateway。Gateway 通过身份验证配置文件查找用户并匹配策略操作。
2. 凭据传递给 StoreFront。StoreFront 接受凭据并将其传递给 Cloud Connectors。
3. Cloud Connectors 查找 Citrix Cloud 所需的用户对象详细信息。
4. Cloud Connectors 将身份信息传递给 Citrix Cloud，身份令牌对用户进行身份验证并枚举分配给用户的资源。
5. Cloud Connectors 将分配的资源返回给 StoreFront 以进行用户枚举。
6. 当用户启动应用程序或桌面时，Citrix Gateway 使用配置的 Cloud Connectors 生成 STA 票证请求。
7. Citrix Cloud 代理管理资源域 Cloud Connectors 与在该资源位置注册的 VDA 之间的会话。
8. 客户端、Citrix Gateway 和已解析的 VDA 之间建立会话。

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

外部信任域到资源域



在此场景中，业务合作伙伴需要访问发布给公司用户的资源。公司域是 corp.com，合作伙伴域是 partner.com。

1. 公司域对合作伙伴域具有出站外部信任。来自合作伙伴域的用户可以对加入公司域的资源进行身份验证。
2. Citrix Cloud 客户需要两个资源位置：一个用于 corp.com Cloud Connectors，另一个用于 partner.com Cloud Connectors。partner.com Cloud Connectors 仅用于对域进行身份验证和身份调用；它们不用于代理 VDA 或会话。
3. StoreFront 服务器已加入 corp.com 域。商店配置了一个站点，该站点列出了 corp.com 域中的 Cloud Connectors。商店配置为支持用户名/密码和从 Citrix Gateway 身份验证直通。用户名/密码身份验证配置为信任任何域。
4. Citrix Gateway 身份验证配置文件配置为 corp.com 域使用 UPN 作为主要登录方法。为 partner.com 域配置第二个配置文件和策略以使用 UPN，并将其绑定到与 corp.com 域相同的 Gateway vServer。
5. 编辑 Citrix Gateway 会话操作系统和 Web 配置文件，并将“已发布的应用程序/单一登录域”设置留空（可能需要设置覆盖设置）。

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

注意：

根据外部受信任域的位置，外部域用户可能会比资源域或父域用户遇到更长的启动时间。

连接工作流

1. mailto:User@partner.com 登录到 Citrix Gateway。Gateway 通过与 UPN 查找匹配的身份验证配置文件查找用户，并匹配策略操作。
2. 凭据传递给 StoreFront。StoreFront 接受凭据并将其传递给 Cloud Connectors。
3. Cloud Connectors 执行 Citrix Cloud 所需的用户对象详细信息查找。
4. Cloud Connectors 将身份信息传递给 Citrix Cloud，身份令牌对用户进行身份验证并枚举分配给用户的资源。
5. Cloud Connectors 将分配的资源返回给 StoreFront 以进行用户枚举。
6. 当用户启动应用程序或桌面时，Citrix Gateway 使用配置的 Cloud Connectors 生成 STA 票证请求，在本例中来自 child1.corp.com。
7. Citrix Cloud 代理管理资源域 Cloud Connectors 与在该资源位置注册的 VDA 之间的会话。
8. 会话在客户端、Citrix Gateway 和已解析的 VDA 之间建立。

林信任/快捷方式信任到资源域

仅当林信任和快捷方式信任域被视为与资源域的外部域信任关系时才受支持。对于林信任，您可以遵循 外部受信任域到资源域 部分中描述的相同步骤。此部分将来可能会根据用户域和资源域/林之间本机林信任的支持情况而改变。

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

创建 Citrix Cloud™ 帐户

本文将引导您完成创建 Citrix Cloud 帐户以及成功完成帐户入职所需任务的过程。

与 Citrix® 建立了现有关系但首次使用 Citrix 云服务的客户可以使用本文中的任务来完成入职流程。

Citrix 新客户的注册流程

如果您是 Citrix 和 Citrix Cloud 的新用户，则必须联系 Citrix 为您的公司创建新的 Citrix 帐户。请使用以下联系方式之一：

- 联系 Citrix 客户服务。
- 联系您所在地区的 Citrix 合作伙伴 或 Citrix 销售办事处。

联系 Citrix 时，您可以与 Citrix 代表讨论您的业务需求。代表将帮助您完成注册过程并为您提供 Citrix 登录凭据。

收到 Citrix 帐户凭据后，您可以使用本文中的任务登录并开始使用 Citrix Cloud。

什么是 Citrix 帐户?

Citrix 帐户（也称为 Citrix.com 帐户或 My Citrix 帐户）使您能够管理对所购买许可证的访问。您的 Citrix 帐户使用组织 ID (OrgID) 作为唯一标识符。如果您的帐户已关联用户名（也称为 Web 登录）或电子邮件地址，您可以通过登录 https://www.citrix.com 访问您的 Citrix 帐户。

重要提示：

一个用户名映射到一个唯一的 Citrix 帐户，但一个电子邮件地址可以映射到多个 Citrix 帐户。

什么是 OrgID?

OrgID 是分配给您的 Citrix 帐户的唯一标识符。您的 OrgID 与物理站点地址（通常是您公司的营业地址）相关联。公司通常只有一个 OrgID。但是，在某些情况下，例如拥有不同的分支机构或不同的部门单独管理其资产，Citrix 可能会允许一家公司拥有多个 OrgID。

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

Citrix 定期清理某些 OrgID，在某些情况下会合并重复项。如果您的公司拥有您希望与有效且活动的 OrgID 合并的 OrgID，您可以联系 Citrix 客户支持并提供您希望合并的 OrgID。

注意：

公司已根据其管理资产的方式设置了 OrgID，因此如果您不知道需要使用哪个 OrgID 或拥有多少个 OrgID，请联系您公司的 IT 部门或 Citrix 管理员。如果您需要帮助，请通过 https://www.citrix.com/support/ 联系 Citrix 客户服务以查找您的 OrgID。

什么是 Citrix Cloud 帐户？

Citrix Cloud 帐户使您能够使用一个或多个 Citrix 云服务来安全地交付您的应用程序和数据。Citrix Cloud 帐户由客户 ID 标识，并与 OrgID 关联。一个 OrgID 可以与多个 Citrix Cloud 客户 ID 关联，但一个客户 ID 只能与一个 OrgID 关联。

根据您的组织设置 OrgID 的方式，使用正确的 Citrix Cloud 帐户非常重要，这样您的购买和管理员访问权限才能在相同的 OrgID 上继续。例如，如果一家公司使用 OrgID 1234 的设计部门一直在使用本地 Virtual Apps and Desktops 并希望试用 Citrix Cloud，则 OrgID 1234 的其中一位管理员可以使用其 Citrix 帐户登录凭据或与该 OrgID 关联的电子邮件地址在该 OrgID 上注册 Citrix Cloud。当公司决定购买 Citrix DaaS™ 订阅时，订单可以正确地放置在 OrgID 1234 上。

重要提示：

拥有特定 Citrix 帐户访问权限的用户不会自动拥有与该 Citrix 帐户的 OrgID 关联的 Citrix Cloud 帐户的访问权限。由于 Citrix Cloud 访问权限可能允许用户影响服务，因此控制谁访问 Citrix Cloud 帐户非常重要。

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

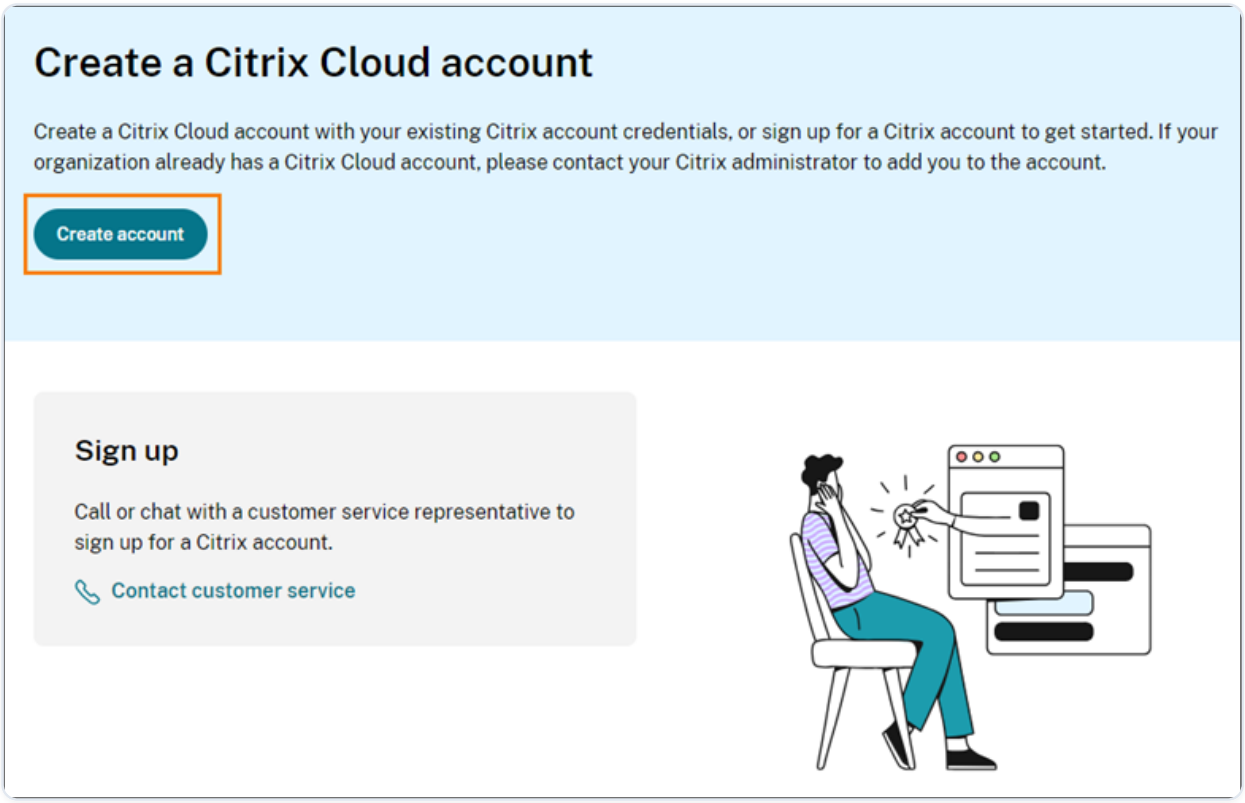
多重身份验证

为确保您的 Citrix Cloud 帐户安全可靠，Citrix 要求所有客户注册多重身份验证 (MFA)。要注册，您只需要一个设备（例如计算机或移动设备）以及一个已安装的身份验证器应用程序（例如 Citrix SSO）。如果无法使用带有身份验证器应用程序的设备，则可以使用电子邮件地址代替。

如果您尚未注册 MFA，Citrix 会在您使用 Citrix 帐户凭据登录时提示您注册。有关要求和说明，请参阅本文中的步骤 2：设置多重身份验证。

步骤 1：访问 Citrix Cloud 网站

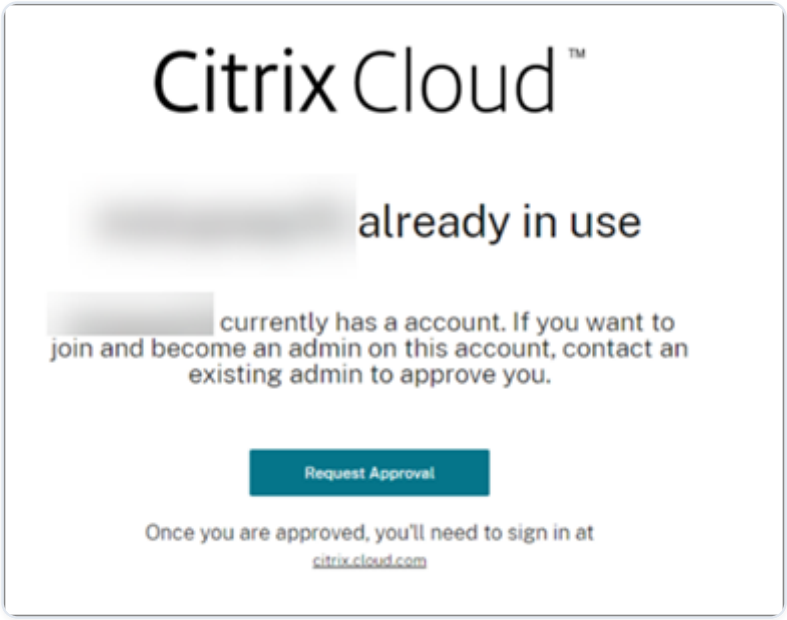
1. 使用 Web 浏览器访问 https://onboarding.cloud.com。
2. 选择 **创建帐户**。



3. 输入您的用户名和密码，或与您的 Citrix.com 帐户关联的电子邮件地址和密码。

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

如果帐户已在使用中，会发生什么情况?



如果您看到一条消息，指示您的组织已在使用 Citrix Cloud 帐户，则表示您的 Citrix 帐户中的另一位管理员已创建了 Citrix Cloud 帐户。在您访问该帐户之前，现有管理员需要邀请您成为管理员，即使您已经是 Citrix 帐户的成员。

由于 Citrix Cloud 帐户允许管理员对服务进行更大的控制，我们希望创建 Citrix Cloud 帐户的第一位管理员必须明确授予其他管理员访问权限，即使其他管理员已经是 Citrix 帐户的成员。

要请求加入 Citrix Cloud 帐户的邀请，请选择 **请求批准**。帐户上的所有现有管理员都会收到一封电子邮件，通知他们您的请求。如果现有管理员已不在您的组织中，请联系 Citrix 支持。

当管理员收到您的批准请求时，他们会邀请您成为管理员，如邀请个人管理员中所述。

收到邀请电子邮件后，单击**登录**链接接受邀请。浏览器打开后，Citrix Cloud 会提示您创建密码并登录 Citrix Cloud 帐户。

步骤 2：设置多重身份验证

如果您未注册 MFA，Citrix Cloud 会在您登录前提示您注册。您可以选择使用身份验证器应用（推荐）或您的电子邮件地址注册 MFA。

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

注意：

- 只有 Citrix 身份提供商下的管理员才能通过 Citrix Cloud 设置 MFA。如果您使用 Microsoft Entra ID 管理 Citrix Cloud 管理员，则可以使用 Azure 门户配置 MFA。有关详细信息，请参阅 Microsoft 网站上的配置 Azure 多重身份验证设置。
- 完成设置过程后，MFA 将用于您在 Citrix Cloud 中所属的所有客户组织。完成设置过程后，您无法禁用 MFA。
- 您只能注册一台设备。如果您以后注册其他设备，Citrix Cloud 将删除当前设备注册并替换为新设备。有关详细信息，请参阅管理您的主要 MFA 方法。

电子邮件作为身份验证方法

如果您无法使用身份验证器应用访问 Citrix Cloud，则使用电子邮件进行 MFA 是一种便捷的替代方法。但是，Citrix 强烈建议您采取预防措施，以确保您的电子邮件地址访问安全。

MFA 要求

要使用身份验证器应用设置 MFA，您必须在设备（例如智能手机或台式计算机）上安装遵循 基于时间的一次性密码 标准的应用。根据您注册的设备，该应用可能需要访问设备的摄像头才能扫描 QR 码。如果您的设备没有摄像头，您可以输入 Citrix Cloud 提供的密钥。

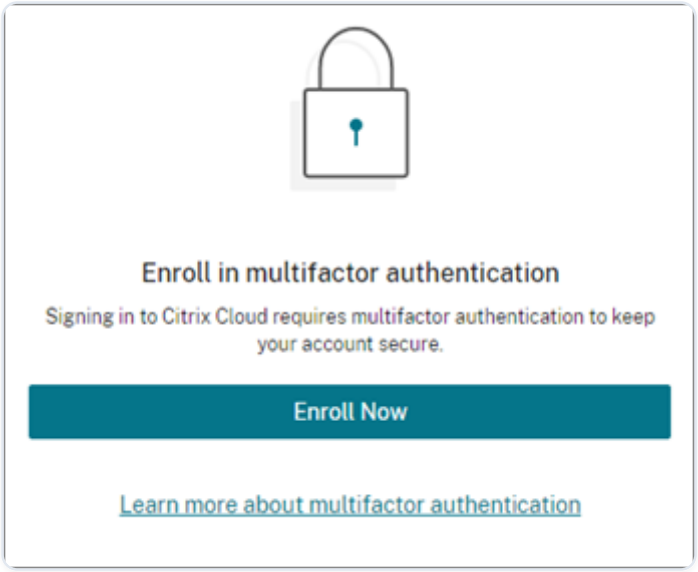
要使用电子邮件地址设置 MFA，您必须使用满足以下要求的电子邮件地址：

- 该电子邮件地址与您用于 Citrix 帐户的电子邮件地址不同。
- 该电子邮件地址是您可以访问以接收来自 Citrix 的验证电子邮件的地址。

注册多重身份验证

1. 当系统提示您注册 MFA 时，选择 **立即注册**。

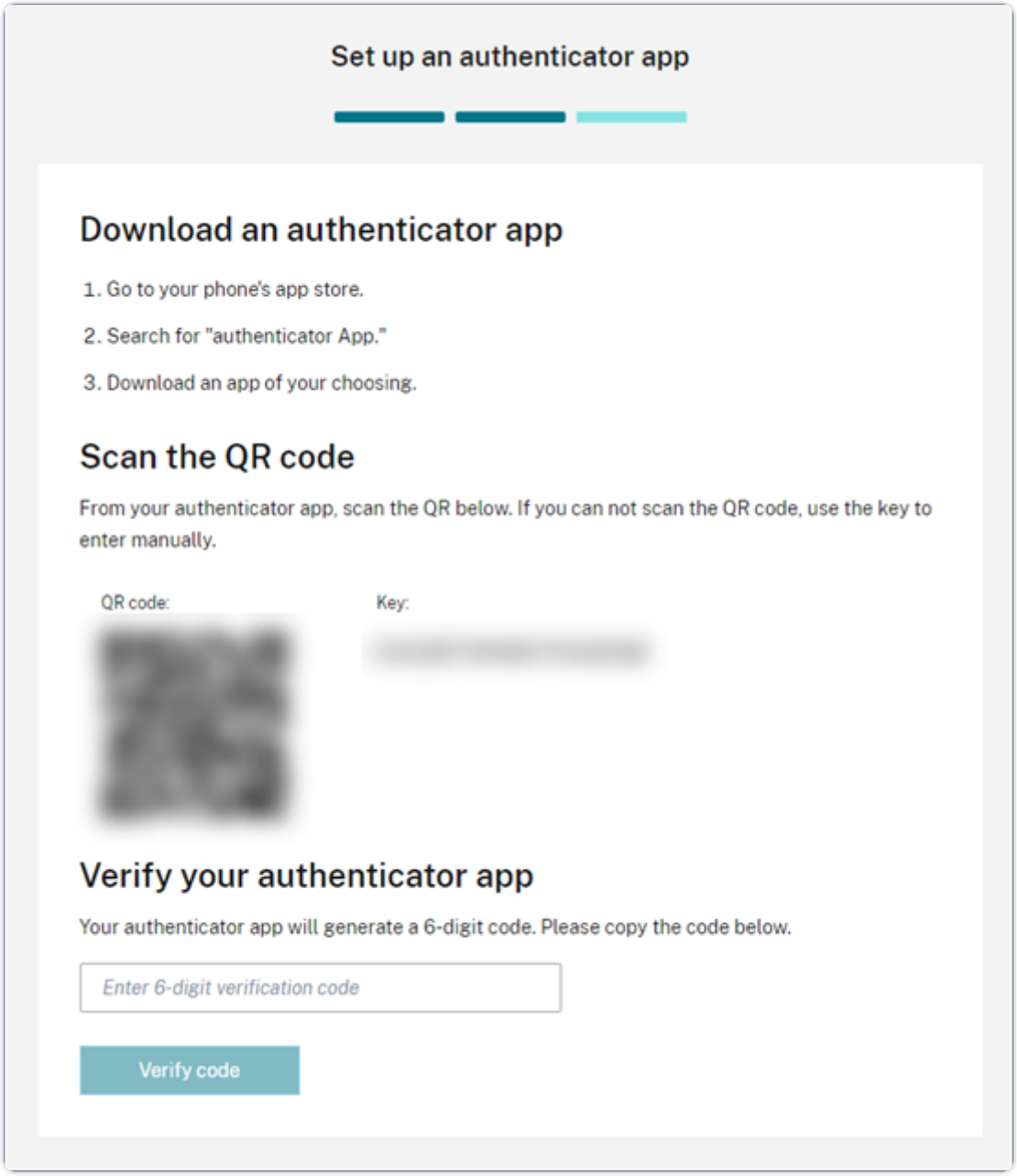
© 1997–2026 Citrix Systems, Inc. All rights reserved.



2. 出现提示时，输入您的电子邮件地址并选择 **发送电子邮件**。Citrix Cloud 会向您发送一封包含验证码的电子邮件。
3. 输入电子邮件中的验证码和您的 Citrix 帐户密码。单击 **验证并继续**。
4. 选择您要使用的身份验证方法，可以是身份验证器应用或电子邮件。
5. 如果您选择了 **身份验证器应用**，请执行以下操作：

   a. 在您的身份验证器应用中，扫描 QR 码或手动输入密钥。您的身份验证器应用会显示 Citrix Cloud 的条目并生成一个 6 位数代码。

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



b. 在“**验证您的身份验证器应用**”下，输入身份验证器应用中的代码，然后选择“**验证代码**”。

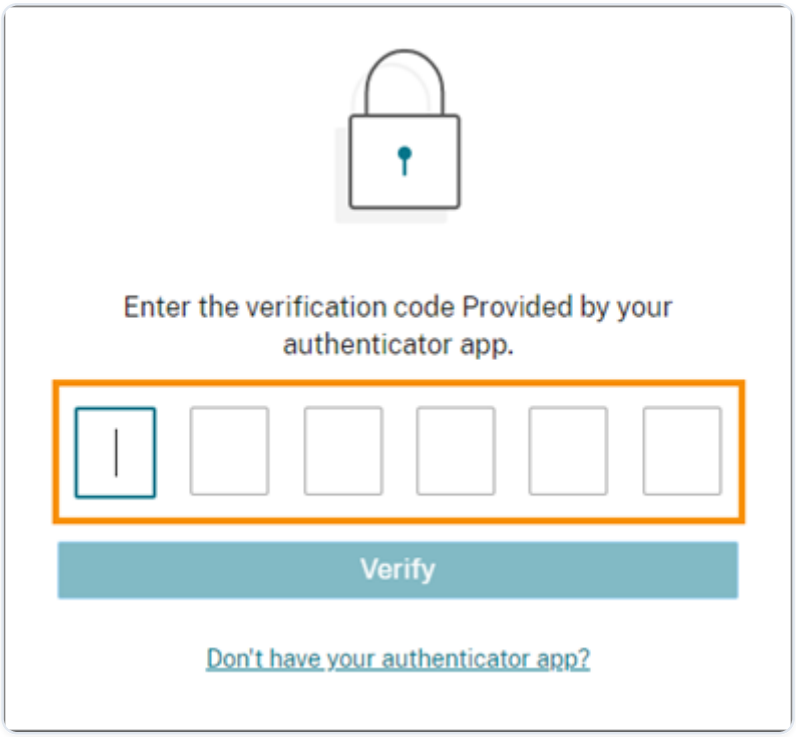
6. 单击“**下一步：恢复方法**”。
7. 选择“**添加恢复电话**”，然后输入一个Citrix支持人员可以用来呼叫您并验证您身份的恢复电话号码。Citrix建议使用座机电话号码。完成后，单击“**保存恢复电话号码**”。
8. 选择“**下一步**”。
9. 选择“**添加恢复电子邮件**”，然后输入一个您可以访问的电子邮件地址，该地址与您用于Citrix Cloud的地址不同。Citrix使用此地址向您发送验证码以验证您的身份。

   如果您没有其他电子邮件地址，请选择“**没有恢复电子邮件？**”以生成备用代码列表。不建议使用备用代码，因为它们很容易丢失。如果您选择此选项，请下载代码并将其保存在需要时可以访问的位置。

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

10. 选择“**完成**”以完成注册。

下次您使用Citrix Cloud管理员凭据登录时，Citrix Cloud会提示您输入所选MFA方法中的验证码。



管理您的MFA注册

要更改您的设备、切换到不同的MFA方法或更新您的恢复方法，请参阅以下文章：

- 管理您的主要MFA方法
- 管理您的MFA恢复方法

步骤3：验证您的OrgID

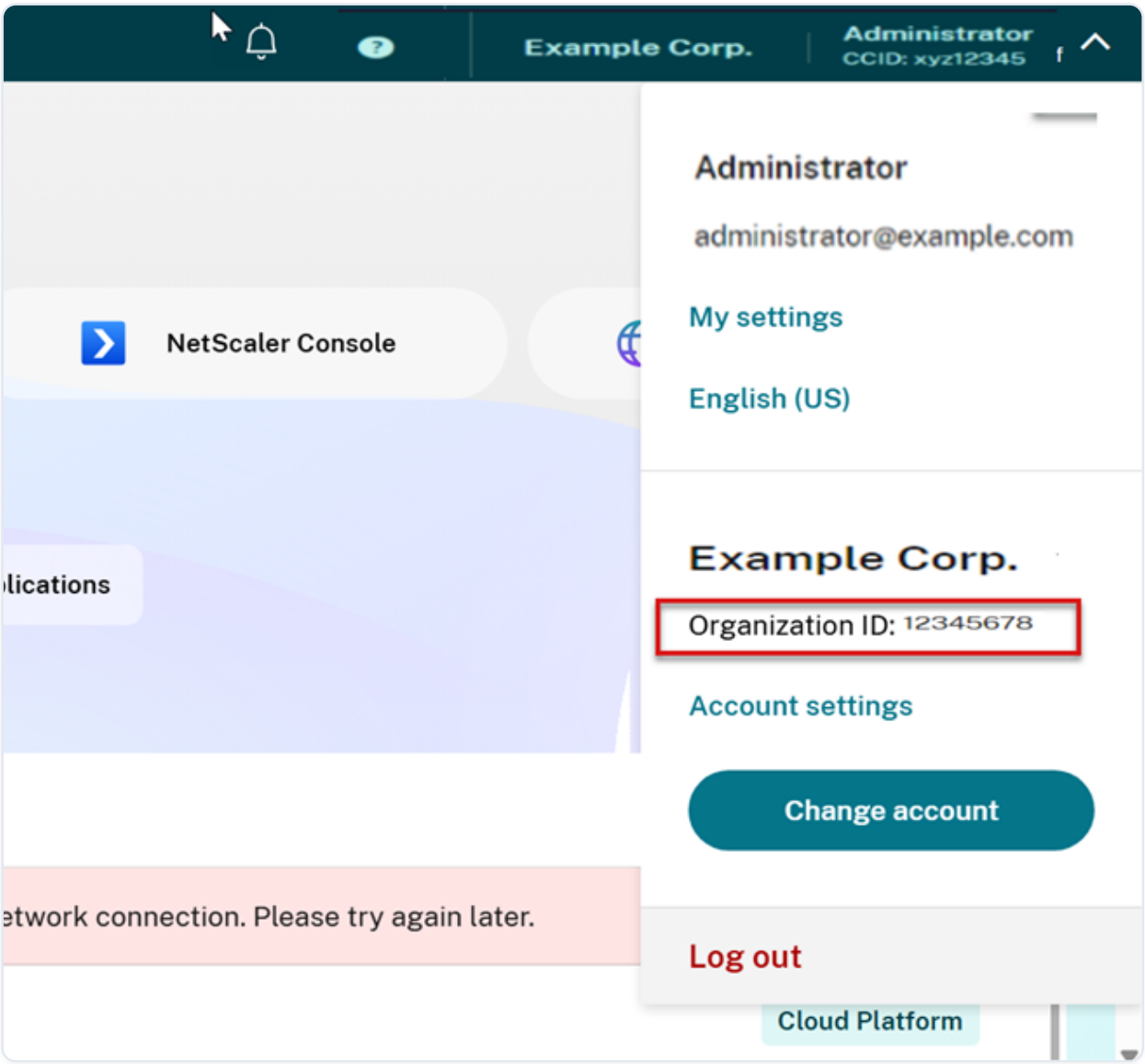
在使用 Citrix Cloud 之前，请花点时间验证您的 OrgID。

请确保您的帐户 OrgID 与您用于下订单的 OrgID 匹配。Citrix Cloud 的优势之一是，如果您试用某项服务并决定购买，那么您在试用版中进行的所有配置都将保留在购买的服务中，因为购买发生在同一帐户中。因此，确保试用版从正确的 OrgID 开始，可以在您决定购买时节省精力。

您的 OrgID 出现在管理控制台的以下位置：

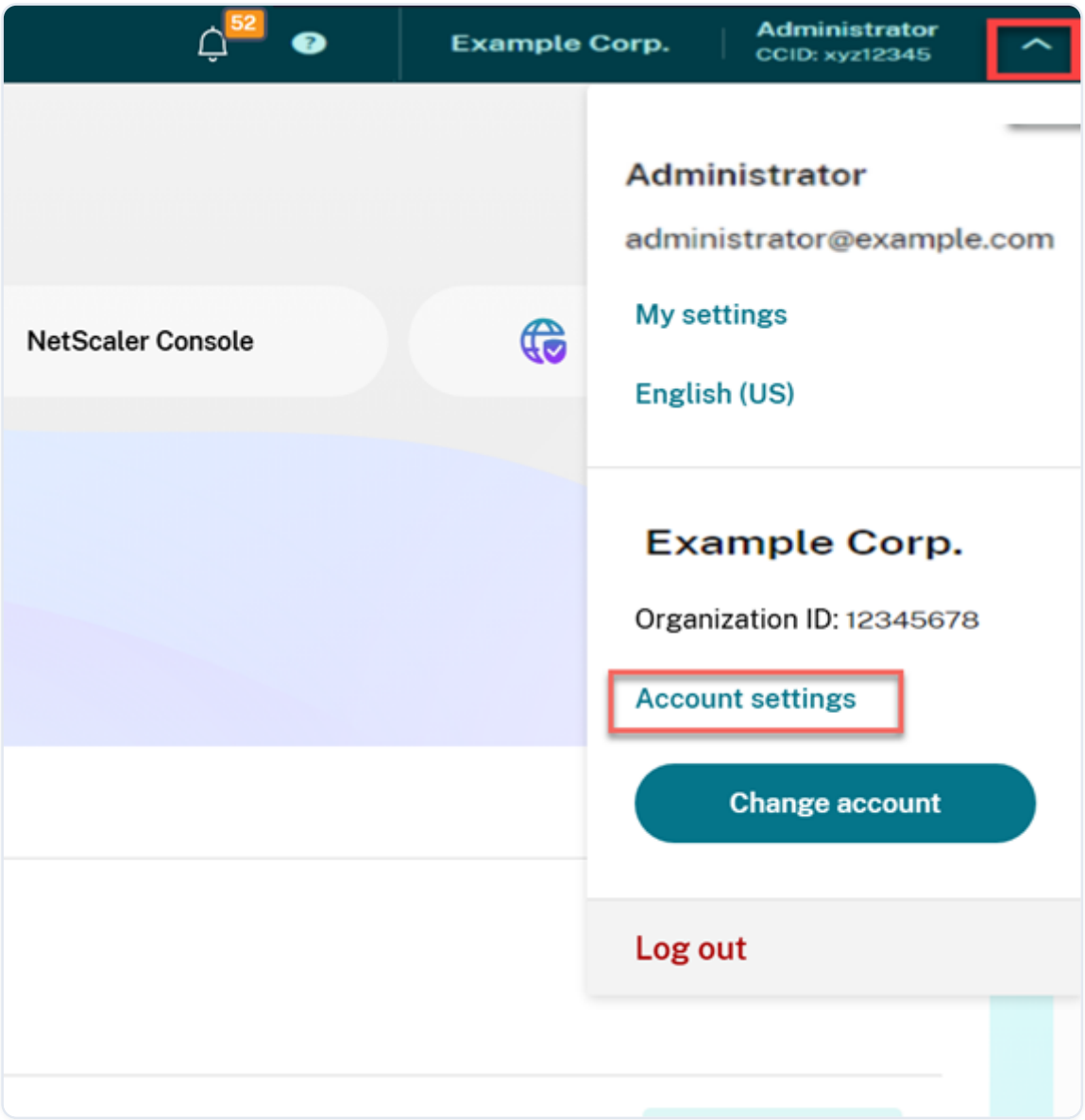
- 在您的客户名称下方的菜单中。单击右上角的客户名称以显示菜单。

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



- 在您的**帐户设置**页面上。从客户菜单中选择**帐户设置**。

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



后续步骤

完成入门后，您可以继续执行以下任务：

- 添加身份提供程序 以验证管理员或最终用户。
- 将管理员添加到您的 Citrix Cloud 帐户。即使您的其他管理员有权访问 Citrix.com 上的 Citrix 帐户，您仍然需要将他们添加到您的 Citrix Cloud 帐户。
- 请求云服务试用版。试用版旨在与您选择的本地基础架构或公共云、您的应用程序以及您的 Microsoft Active Directory 进行测试。
- 将许可证分配给帐户。此过程可帮助您将许可证分配给用户。

更多信息

- Citrix 培训：Citrix Cloud 基础知识

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

- YouTube 上的 Citrix 频道：Citrix Cloud 大师班

验证您的 Citrix Cloud™ 电子邮件

Citrix 可能会不时要求您验证您的 Citrix Cloud 帐户。您可能需要验证电子邮件的一些原因如下：

- 您有一段时间未登录 Citrix Cloud。
- 您更改了电子邮件地址。
- 您为 Citrix Cloud 帐户添加了新的管理员。
- 由于 Citrix Cloud 的安全系统更新，您需要重新验证您的 Citrix Cloud 帐户。

常见问题

我多久会被要求验证一次?

验证您的帐户是一次性事件。Citrix Cloud 不会在您每次登录或帐户发生更改时要求您进行验证。如果您被频繁要求验证，请联系 Citrix 技术支持。

我的帐户是否发生了什么问题?

不，被要求验证您的帐户并不意味着您的帐户或任何 Citrix Cloud 服务出现问题。这只是 Citrix 保护您的信息安全的一种方式。

我没有收到验证电子邮件。我该怎么办?

执行以下步骤：

1. 在收件箱中搜索来自“Citrix”的验证电子邮件。验证电子邮件在 24 小时后过期。要触发新的验证电子邮件，请再次登录 Citrix Cloud。这是每次 Web 登录的一次性过程。
2. 如果不在收件箱中，请检查您的文件夹。如果垃圾邮件过滤器或电子邮件规则移动了该电子邮件，它可能位于您的垃圾邮件或废纸篓文件夹中。检查所有防火墙。
3. 确保您正在检查正确的电子邮件帐户。Citrix 会将验证电子邮件发送到您帐户中当前存档的电子邮件地址。通常，这是您最初注册 Citrix Cloud 时使用的电子邮件地址，或者是您受邀加入 Citrix Cloud 帐户时使用的电子邮件地址。
4. 通过在 https://www.citrix.com/account 登录您的 Citrix 帐户，确认记录中的电子邮件地址有效。如果电子邮件无效，请更新您的电子邮件地址并再次登录 Citrix Cloud 以触发新的验证电子邮件。有关更多信息，请参阅 Citrix 支持知识中心中的 CTX120355。
5. 如果您仍未收到验证电子邮件，请联系 Citrix Support 以开立支持案例。对于教育站点（请参阅 **Partner Services Delivery > eLearning > Citrix Training**），请与教育团队开立案例以进行进一步调查。要开立案例，请在 Contact Us 页面上请求 **General Support**。

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

如果您已成功验证电子邮件但仍无法登录 Citrix Cloud，请参阅 Citrix 网站登录问题疑难解答。

联系 Citrix 支持

如果您遇到此处未涵盖的问题，请联系 Citrix 支持部门 以开立支持案例。

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

连接到 Citrix Cloud™

将您的资源连接到 Citrix Cloud 涉及在您的环境中部署连接器并创建 *资源位置*。

资源位置

资源位置包含向最终用户交付云服务所需的资源。资源位置包含不同的资源，具体取决于您正在使用的 Citrix Cloud 服务以及您希望向用户提供的服务。

您的资源位置是您的资源所在的任何地方，无论是公共云、私有云、分支机构还是数据中心。如果您已经在自己的云或数据中心拥有资源，您的资源将保留在原地。无需将它们移动到其他地方即可与 Citrix Cloud 配合使用。

您的位置选择可能会受到以下因素的影响：

- 靠近最终用户
- 靠近数据
- 规模要求
- 安全属性

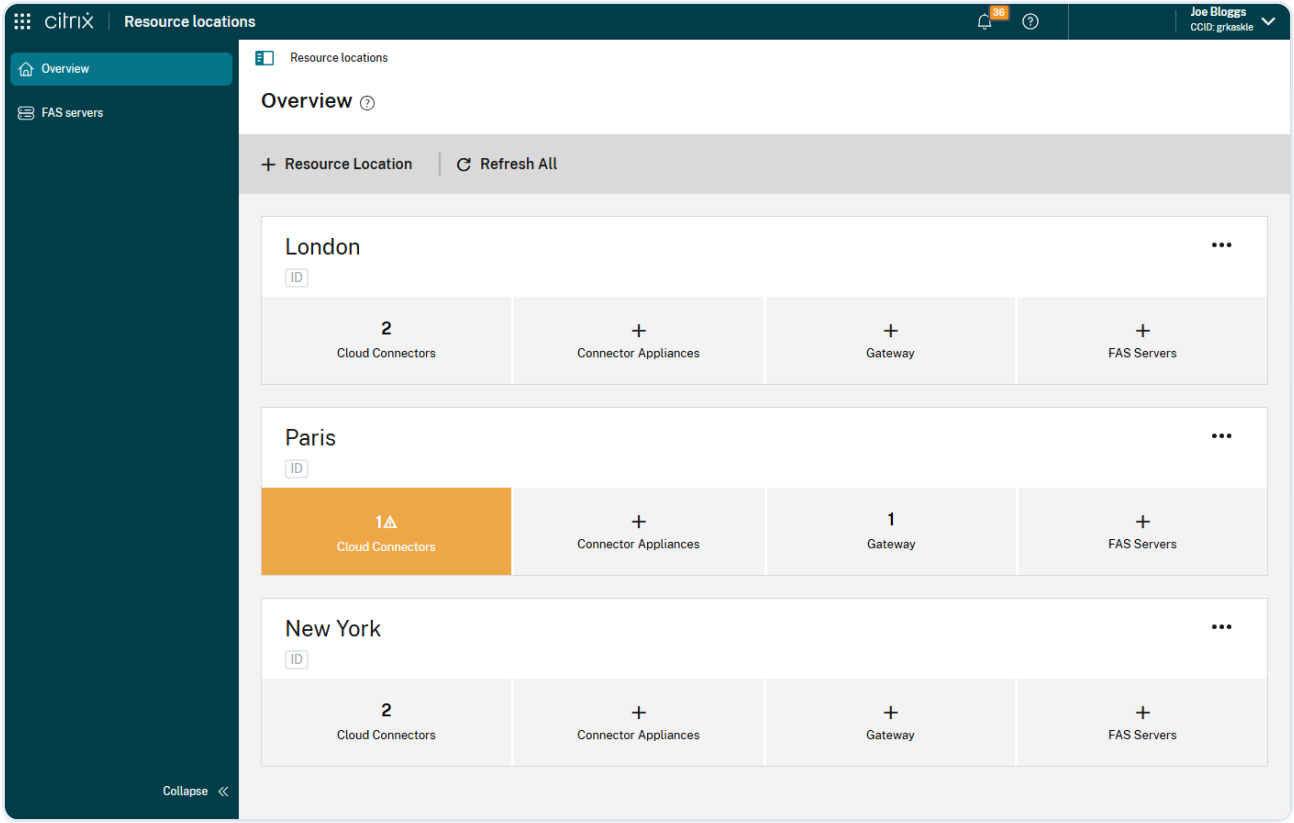
资源位置部署示例

- 根据需要靠近数据的用户和应用程序，在数据中心为总部构建您的第一个资源位置。
- 在公共云中为您的全球用户添加第二个资源位置。或者，在分支机构中构建单独的资源位置，以提供最适合靠近分支机构员工的应用程序。
- 在提供受限应用程序的单独网络上添加另一个资源位置。这为其他资源和用户提供了受限的可见性，而无需调整其他资源位置。

查看和管理资源位置

要管理资源位置，请登录到 Citrix Cloud 并从主菜单中选择**资源位置**。

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



对于每个资源位置，您可以添加：

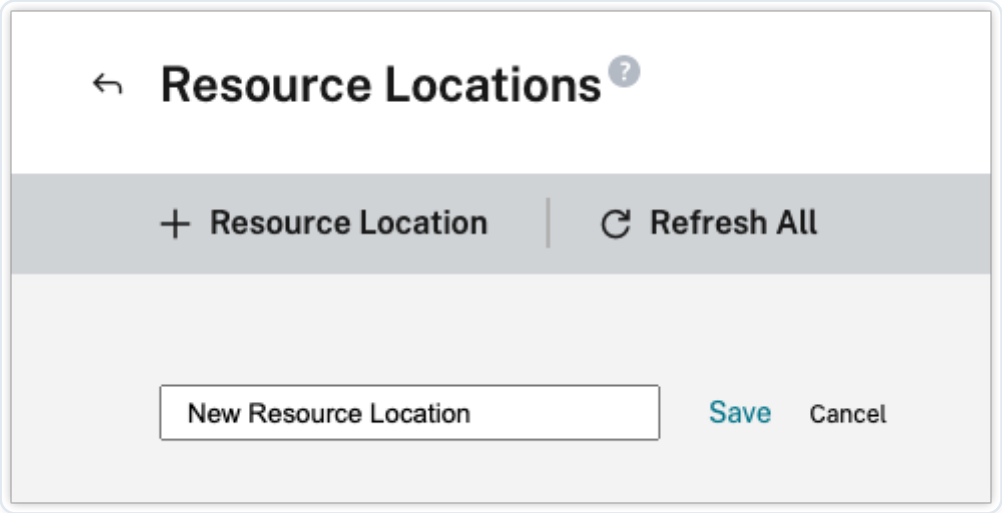
- 云连接器
- 连接器设备
- Citrix 网关
- FAS 服务器

创建资源位置

要创建资源位置：

1. 选择**+ 资源位置**

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



2. 输入资源位置的名称。请参阅命名限制。
3. 按**保存**。将创建新的资源位置。

4. 在资源位置中安装至少两个连接器。根据您使用的云服务，需要云连接器或连接器设备才能在 Citrix Cloud 与您的资源之间建立通信。有关选择相应连接器的详细信息，请参阅资源类型。要部署连接器，请参阅以下文章：
   - 云连接器安装
   - 适用于云服务的 Connector Appliance

资源类型

资源位置包含不同的资源，具体取决于您正在使用的 Citrix Cloud 服务以及您希望提供给最终用户的服务。不同的资源使用不同类型的连接器。大多数服务使用 Citrix Cloud Connector™，但某些特定服务需要 Connector Appliance。

使用 Citrix Cloud Connector 的服务

- **Citrix DaaS**（以前称为 Citrix Virtual Apps and Desktops 服务）需要 Cloud Connector 才能在您的资源位置发布应用程序和桌面以及预配计算机目录。有关 Cloud Connector 如何与此服务通信的概述，请参阅 Citrix Tech Zone 中的 Citrix DaaS 图表。
- **适用于 Azure 的 Citrix DaaS Standard**（以前称为适用于 Azure 的 Citrix Virtual Apps and Desktops Standard）需要 Cloud Connector 才能从多会话计算机交付 Citrix 托管的 Azure 虚拟桌面和应用程序。

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

- **Endpoint Management** 需要 Cloud Connector 才能管理应用程序和设备策略以及向用户交付应用程序。

使用 Connector Appliance 的服务

- **映像可移植性服务**简化了跨平台映像的管理。此功能对于管理本地资源位置和公有云中的资源位置之间的映像很有用。Citrix Virtual Apps and Desktops™ REST API 可用于自动化 Citrix Virtual Apps and Desktops 站点内的资源管理。

  当您使用 Citrix Cloud 启动映像从本地位置到公有云订阅的迁移时，映像可移植性工作流即开始。准备好映像后，映像可移植性服务会帮助您将映像传输到您的公有云订阅并准备运行。最后，Citrix Provisioning 或 Machine Creation Services™ 在您的公有云订阅中预配映像。

  有关详细信息，请参阅 映像可移植性服务。

- **Citrix Secure Private Access** 使管理员能够提供无缝体验，将单点登录、远程访问和内容检查集成到一个解决方案中，以实现端到端访问控制。有关详细信息，请参阅 借助 Connector Appliance 实现安全私有访问。

可能还有其他预览版服务也依赖于 Connector Appliance。

资源位置限制

您的 Citrix Cloud 帐户中最多可以有 50 个资源位置。

命名限制

您分配给资源位置的名称必须符合以下限制：

- 最大长度：64 个字符
- 不允许使用的字符：
  - `#`、`$`、`%`、`\^`、`&`、`?`、`+`
  - 大括号：`[]`、`{}`
  - 管道符 (`|`)
  - 小于号 (`<`) 和大于号 (`>`)
  - 正斜杠和反斜杠 (`/`、`\`)
- 不得与 Citrix Cloud 帐户中的任何其他资源位置名称（不区分大小写）匹配

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

主资源位置

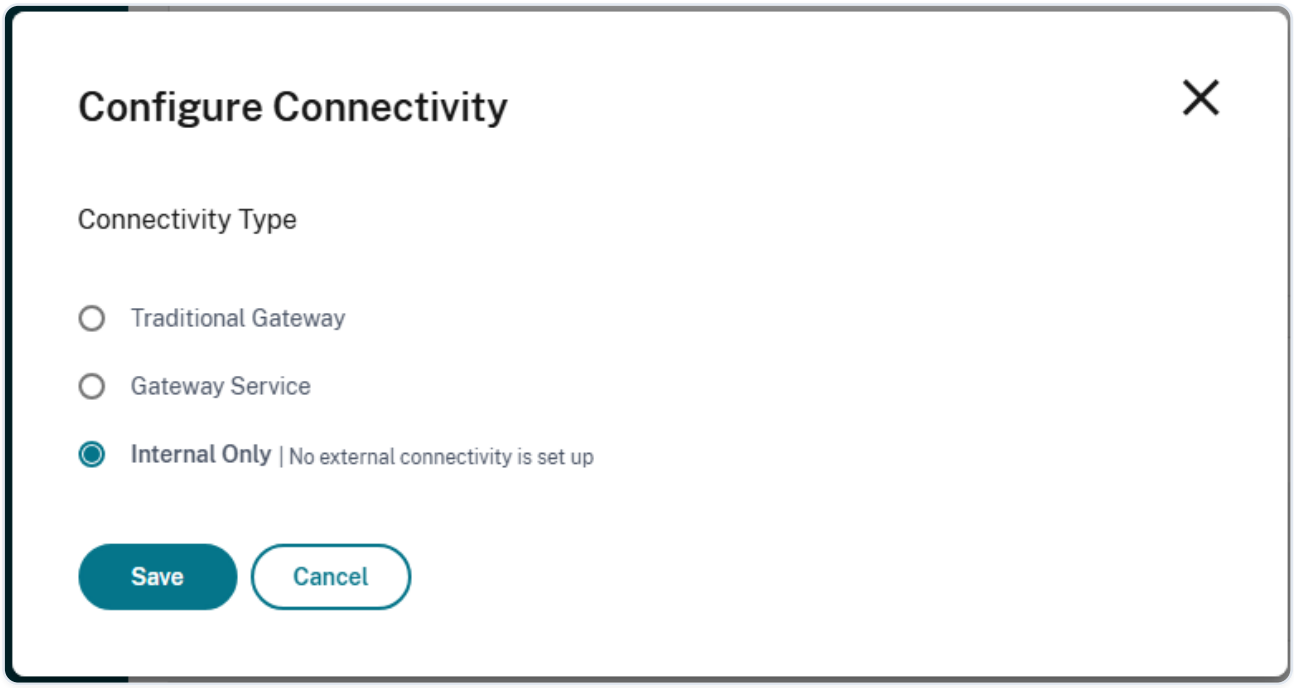
主资源位置是您指定为在您的域和 Citrix Cloud 之间进行某些通信时“最优先”的资源位置。主资源位置中的 Cloud Connector 用于用户登录和预配操作。您选择为“主”的资源位置应具有与您的域具有最佳性能和连接性的 Cloud Connector。这使您的用户能够快速登录 Citrix Cloud。

有关详细信息，请参阅选择主资源位置。

网关

默认情况下，客户端必须能够直接访问托管您的虚拟应用程序和桌面的计算机。您可以使用网关启用远程访问。您可以选择使用 Citrix Gateway Service 或使用您自己的 NetScaler® 网关。

要配置远程访问，请选择资源位置的 **Gateway** 磁贴。



或者，您可以从 **StoreFront Cloud** 访问相同的配置屏幕。

有关配置网关的更多信息，请参阅 配置对应用商店的访问 - 外部连接。

思杰云连接器™

Citrix Cloud™ Connector 是一个 Citrix 组件，它在 Citrix Cloud 与您的资源位置之间充当通信通道，无需复杂的网络或基础架构配置即可实现云管理。这消除了管理交付基础架构的所有麻烦。它使您能够管理并专注于为用户提供价值的资源。

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

注意：

请勿在 Citrix Cloud Connector 计算机上安装 Citrix DaaS 远程 PowerShell SDK。它可以安装在同一资源位置内的任何已加入域的计算机上。

Citrix® 建议您不要在 Cloud Connector 上运行此 SDK 的 cmdlet。SDK 的操作不涉及 Cloud Connector。

需要 Cloud Connector 的服务

Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops 服务）需要 Cloud Connector。有关 Cloud Connector 如何与服务通信的概述，请参阅 Tech Zone 中的 Citrix DaaS 图表。

Citrix Endpoint Management™ 需要 Cloud Connector 才能实现企业连接到 Endpoint Management 服务。远程浏览器隔离服务需要 Cloud Connector 才能用于经过身份验证的外部 Web 应用程序。

云连接器功能

- **Active Directory (AD)**：启用 AD 管理，允许在您的资源位置内使用 AD 林和域。它消除了添加任何额外 AD 信任的需要。
- **虚拟应用程序和桌面发布**：启用从您的资源位置中的资源发布 Citrix DaaS™。
- **Endpoint Management**：启用移动设备管理 (MDM) 和移动应用程序管理 (MAM) 环境，用于管理设备和应用程序策略以及向用户交付应用程序。
- **计算机目录预配**：启用将计算机直接预配到您的资源位置。

云连接器通信

Cloud Connector 对 Citrix Cloud 与您的资源位置之间的所有通信进行身份验证和加密。安装后，Cloud Connector 通过出站连接启动与 Citrix Cloud 的通信。所有连接都使用标准 HTTPS 端口 (443) 和 TCP 协议从 Cloud Connector 建立到云。不接受来自公共互联网的任何入站连接。

Cloud Connector 可用性和负载管理

为了持续可用性和管理负载，请在每个资源位置安装多个 Cloud Connector。每个资源位置至少需要两个 Cloud Connector，以确保与 Citrix Cloud 建立高可用性连接。如果一个 Cloud Connector 在任何时间段内不可用，其他 Cloud Connector 可以维持连接。由于每个 Cloud Connector 都是无状态的，因此负载可以分布到所有可用的 Cloud Connector 上。无需配置此负载平衡功能。它是完全自动化的。

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

只要有一个 Cloud Connector 可用，与 Citrix Cloud 的通信就不会中断。在可能的情况下，最终用户与资源位置中资源的连接不依赖于与 Citrix Cloud 的连接。这使得资源位置能够为用户提供对其资源的访问，而无论与 Citrix Cloud 的连接是否可用。

在何处获取 Cloud Connector

您可以从 Citrix Cloud 中下载 Cloud Connector 软件。

1. 登录到 Citrix Cloud。
2. 从屏幕左上角的菜单中，选择 **Resource Locations**。
3. 如果您没有现有资源位置，请在“资源位置”页面上单击 **Download**。出现提示时，保存 **cwcconnector.exe** 文件。
4. 如果您有资源位置但其中未安装 Cloud Connector，请单击 Cloud Connectors 栏，然后单击 **Download**。出现提示时，保存 **cwcconnector.exe** 文件。

我需要多少个 Cloud Connector?

至少需要两个 (2) Cloud Connector 才能在 Citrix Cloud 和您的资源位置之间建立高可用性连接。根据您的环境和支持的工作负载，您可能需要更多 Cloud Connector 来确保为用户提供最佳体验。

作为最佳实践，Citrix 建议在确定需要部署的 Cloud Connector 数量时使用 N+1 冗余模型。根据您的环境、工作负载、Active Directory 配置和服务，确定您在资源位置中需要的 Cloud Connector 数量。在此数量的基础上，至少再添加一个 Cloud Connector 以提供弹性。例如，如果您确定需要五个 Cloud Connector，则在此总数上再添加一个，并在您的资源位置中安装六个 Cloud Connector。

有关其他规模和大小调整准则，请参阅 Scale and size considerations for Cloud Connectors。

在何处安装 Cloud Connector

将 Cloud Connector 安装在已加入您的域并能够与您希望从 Citrix Cloud 管理的资源通信的专用计算机上。有关详细信息，请参阅 system requirements。

有关更多部署信息，请参阅以下文章：

- Active Directory 中 Cloud Connector 的部署方案
- 云连接器安装

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

Citrix Cloud Connector 系统要求

托管 Citrix Cloud Connector™ 的计算机必须满足以下要求。对于生产环境，每个资源位置至少需要两个 Cloud Connector 以确保高可用性。作为最佳实践，Citrix® 建议在部署 Cloud Connector 时使用 N+1 冗余模型，以保持与 Citrix Cloud 的高可用性连接。

主机资源要求

每个 Cloud Connector 最低要求：

- 2 个 vCPU
- 4 GB 内存
- 20 GB 磁盘空间

对于将用于 本地主机缓存 的 Cloud Connector，Citrix 建议 Cloud Connector 至少配备 4 个 vCPU 和 6 GB 内存。

更多的 vCPU 内存使 Cloud Connector 能够为更大的站点进行扩展。有关推荐配置，请参阅 Cloud Connector 的规模和大小注意事项。

操作系统

支持以下操作系统：

- Windows Server 2025 服务器
- Windows Server 2022 服务器
- Windows Server 2019 服务器
- Windows Server 2016 服务器

Cloud Connector 不支持与 Windows Server Core 一起使用。

.NET 要求

您必须在每台服务器上安装以下两项。

- Microsoft .NET Framework 4.7.2 或更高版本。此版本在 Windows Server 2019 及更高版本上已默认安装。在 Windows Server 2016 上，下载最新版本 从 Microsoft 网站。
- Microsoft .NET 8.0。从 Microsoft 网站下载最新版本。

Citrix 强烈建议将 Windows Update 配置为“接收其他 Microsoft 产品的更新”，以确保这些软件包保持最新。

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

服务器要求

如果您将 Cloud Connector 与 Citrix DaaS™（以前称为 Citrix Virtual Apps and Desktops 服务）结合使用，请参阅(/zh-cn/citrix-virtual-apps-desktops-service/install-configure/resource-location/cc-scale-and-size.html)以获取计算机配置指南。

以下要求适用于安装了 Cloud Connector 的所有计算机：

- 使用专用计算机托管 Cloud Connector。请勿将其与任何其他 Citrix 产品或其他应用程序安装在同一台计算机上。
- 服务器不是 Active Directory 域控制器或对您的资源位置基础结构至关重要的任何其他计算机。Cloud Connector 上的(/zh-cn/citrix-cloud/citrix-cloud-resource-locations/connector-updates.html)会执行可能导致这些额外资源中断的计算机操作。
- 服务器时钟设置为正确的 UTC 时间。
- 如果您使用图形安装程序，则必须安装浏览器并设置默认系统浏览器。
- Cloud Connector 安装程序是从 Citrix Cloud 下载的，因此您的浏览器必须允许下载可执行文件。

Windows 更新指南

Citrix 强烈建议在所有托管 Cloud Connector 的计算机上启用 Windows Update，包括“安装其他 Microsoft 产品的更新”策略。Cloud Connector 每五分钟执行一次定期检查，以查找待处理的重新启动，这些重新启动可能由各种因素触发，包括 Windows 更新。任何检测到的重新启动都会立即执行，无论在资源位置设置的首选日期计划如何。这种主动方法可确保 Cloud Connector 不会长时间处于待更新状态，从而保持系统稳定性。

Citrix Cloud 管理重新启动以保持可用性，每次只允许一个 Cloud Connector 重新启动。设置 Windows Update 时，请确保 Windows 设置为在非工作时间自动下载并安装更新。但是，自动重新启动至少在四小时内不允许，以使 Cloud Connector 有充足的时间管理重新启动过程。此外，您可以使用组策略或系统管理工具建立一个备用重新启动机制，以应对更新后必须重新启动计算机的情况。有关更多信息，请参阅管理更新后设备重启。

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

注意：

- 如果客户不希望其 Cloud Connector 在工作时间重新启动，我们建议客户相应地在非工作时间安排 Windows 更新。
- 每个 Cloud Connector 大约需要 10 分钟才能重新启动，这包括与 Citrix Cloud 平台同步所需的时间，以确保在任何给定时间点只有一个 Cloud Connector 重新启动。因此，如前所述，建议的自动重新启动最短延迟时间为四小时，可以根据租户中 Cloud Connector 的数量相应地调整为更短或更长的时间。

防病毒配置

本文 技术白皮书：端点安全、防病毒和反恶意软件最佳实践 提供了指导，可帮助您确定环境中 Cloud Connector 的安全性与性能之间的适当平衡。Citrix 强烈建议与您组织的防病毒和安全团队一起审查这些指南，并在将其应用于生产环境之前进行严格的实验室测试。

证书验证要求

Cloud Connector 依赖 X.509 证书来验证其安装的软件包以及其联系的 Citrix Cloud 端点的完整性。这些证书由广受尊敬的企业证书颁发机构 (CA) 颁发。

为执行此验证，Cloud Connector 具有以下要求：

- 根证书必须存在于主机证书存储中。
- 中间证书必须存在于主机证书存储中。
- Cloud Connector 必须能够验证证书的证书吊销列表 (CRL)。

有关下载和安装证书的完整说明，请参阅 CTX223828。

根证书要求

以下根证书必须安装在 Cloud Connector 主机上：

- `https://cacerts.digicert.com/DigiCertGlobalRootG3.crt`
- `https://cacerts.digicert.com/DigiCertGlobalRootG2.crt`
- `https://cacerts.digicert.com/DigiCertGlobalRootCA.crt`
- `https://cacerts.digicert.com/DigiCertTrustedRootG4.crt`
- `https://cacerts.digicert.com/BaltimoreCyberTrustRoot.crt`
- `https://www.d-trust.net/cgi-bin/D-TRUST_Root_Class_3_CA_2_2009.crt`

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

- `https://www.microsoft.com/pkiops/certs/Microsoft%20RSA%20Root%20Certificate%20Authority%202017.crt`
- `https://www.microsoft.com/pkiops/certs/Microsoft%20EV%20ECC%20Root%20Certificate%20Authority%202017.crt`
- `https://www.microsoft.com/pkiops/certs/Microsoft%20ECC%20Root%20Certificate%20Authority%202017.crt`

根证书通常作为操作系统的一部分打包，或由 Windows 根证书计划，除非：

- 关闭自动根证书更新 组策略已启用以阻止根证书更新；并且
- Connector 主机服务器到 Internet 的连接受限，导致无法下载更新

如果缺少任何证书，Cloud Connector 安装程序将尝试从 `http://cacerts.digicert.com` 下载。

如果无法做到这一点，则需要在所有 Cloud Connector 主机上手动安装根证书。

中间证书要求

以下中间证书必须安装在 Cloud Connector 主机上：

- `https://cacerts.digicert.com/DigiCertTrustedG4CodeSigningRSA4096SHA3842021CA1.crt`

当服务器收到由中间机构颁发的证书，且该证书在 Windows 证书存储中缺失时，中间证书通常会按需下载。

如果连接器主机服务器到 Internet 的连接受限，则可能无法进行此下载。在这种情况下，需要手动将中间证书安装到所有 Cloud Connector 主机上。

证书吊销列表 (CRL) 要求

验证用于验证组件的证书是否未受损非常重要。这通过证书吊销列表 (CRL) 实现。当客户端使用证书验证文件或端点的完整性时，客户端会检查它是否信任颁发证书的 CA 以及证书是否已被吊销。如果证书在 CRL 上，则该证书已被吊销且不可信。

CRL 服务器使用端口 80 上的 HTTP，而不是端口 443 上的 HTTPS。Cloud Connector 组件本身不通过外部端口 80 进行通信。对外部端口 80 的需求是操作系统执行的证书验证过程的副产品。

Cloud Connector 必须能够通过 HTTP 端口 80 访问以下 CRL 端点：

- `http://cacerts.digicert.com/`
- `http://dl.cacerts.digicert.com/`
- `http://crl3.digicert.com`

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

- `http://crl4.digicert.com`
- `http://ocsp.digicert.com`
- `http://www.d-trust.net`
- `http://root-c3-ca2-2009.ocsp.d-trust.net`
- `http://crl.microsoft.com`
- `http://oneocsp.microsoft.com`
- `http://ocsp.msocsp.com`

有关如何测试 CRL 和 OCSP 连接的更多信息，请参阅 https://www.digicert.com/kb/util/utility-test-ocsp-and-crl-access-from-a-server.htm。

客户管理的证书

除了与 Citrix Cloud 服务通信所需的 Citrix 管理证书之外，客户还可以在 Cloud Connector 上部署其他证书，以保护与本地其他组件的通信。这些证书将由客户管理，需要由客户进行监控和续订。

下表总结了可以使用客户管理的证书保护的通信流。

组件	来自连接器的流量流	更多文档
StoreFront	入站	HTTPS 配置
NetScaler® 网关	入站	HTTPS 配置(/zh-cn/citrix-cloud/citrix-cloud-resource-locations/citrix-cloud-connector/installation.html#https-configuration)
管理程序	出站	保护与 VMware 环境的连接(/zh-cn/citrix-daas/install-configure/connections/connection-vmware-virtualization-environments.html#securing-connections-to-the-vmware-environment)

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

思杰 DaaS

将 Cloud Connector 用于连接 DaaS 资源需要安装额外的证书，并授予对扩展 PKI 基础设施的访问权限。每台 Cloud Connector 计算机都必须满足以下要求：

- HTTP 端口 80 对以下地址开放：
  - `crl.*.amazontrust.com`
  - `ocsp.*.amazontrust.com`
  - `*.ss2.us`
- 与以下地址的通信已启用
  - `https://*.amazontrust.com`
  - `https://*.ss2.us`
- 已安装以下根证书：
  - `https://www.amazontrust.com/repository/AmazonRootCA1.cer`
  - `https://www.amazontrust.com/repository/AmazonRootCA2.cer`
  - `https://www.amazontrust.com/repository/AmazonRootCA3.cer`
  - `https://www.amazontrust.com/repository/AmazonRootCA4.cer`
  - `https://www.amazontrust.com/repository/SFSRootCAG2.cer`
- 已安装以下中间证书：
  - `https://www.amazontrust.com/repository/G2-RootCA4.orig.cer`
  - `https://www.amazontrust.com/repository/R3-ServerCA3A.cer`
  - `https://www.amazontrust.com/repository/SFC2CA-SFSRootCAG2.cer`
  - `https://www.amazontrust.com/repository/SFC2CA-SFSRootCAG2.v2.cer`
  - `https://www.amazontrust.com/repository/G2-RootCA1.orig.cer`
  - `https://www.amazontrust.com/repository/R1-ServerCA1A.cer`
  - `https://www.amazontrust.com/repository/G2-RootCA3.cer`
  - `https://www.amazontrust.com/repository/R3-ServerCA3A.orig.cer`
  - `https://www.amazontrust.com/repository/G2-RootCA2.orig.cer`
  - `https://www.amazontrust.com/repository/G2-RootCA4.cer`
  - `https://www.amazontrust.com/repository/R2-ServerCA2A.cer`

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

- `https://www.amazontrust.com/repository/R4-ServerCA4A.cer`
- `https://www.amazontrust.com/repository/R1-ServerCA1A.orig.cer`
- `https://www.amazontrust.com/repository/G2-RootCA1.cer`
- `https://www.amazontrust.com/repository/G2-RootCA2.cer`
- `https://www.amazontrust.com/repository/G2-RootCA3.orig.cer`
- `https://www.amazontrust.com/repository/R4-ServerCA4A.orig.cer`
- `https://www.amazontrust.com/repository/G2-ServerCA0A.cer`
- `https://www.amazontrust.com/repository/G2-ServerCA0A.orig.cer`
- `https://www.amazontrust.com/repository/SFSRootCA-SFSRootCAG2.cer`

如果缺少任何证书，Cloud Connector 将从 `<https://www.amazontrust.com>` 下载。

有关下载和安装证书的完整说明，请参阅 CTX223828。

Active Directory 的要求

- 服务器必须加入包含您用于为用户创建产品的资源和用户的 Active Directory 域。对于多域环境，请参阅 Active Directory 中 Cloud Connector 的部署方案。
- 您计划与 Citrix Cloud 配合使用的每个 Active Directory 林必须始终可通过两个 Cloud Connector 访问。
- Cloud Connector 必须能够访问林根域和您打算与 Citrix Cloud 配合使用的域中的域控制器。有关详细信息，请参阅以下 Microsoft 支持文章：
  - 如何配置域和信任
  - Windows 的服务概述和网络端口要求 中的“系统服务端口”部分
- 使用通用安全组而不是全局安全组。此配置可确保可以从林中的任何域控制器获取用户组成员身份。

支持的 Active Directory 功能级别

Cloud Connector 支持 当前支持的 Microsoft 版本和功能级别。

注意：

Windows Server 2025 功能级别仅在禁用数据库 32k 页的情况下受支持。

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

网络要求

- 连接到可联系您在资源位置中使用的资源的网络。有关详细信息，请参阅 Cloud Connector 代理和防火墙配置。
- 连接到 Internet。有关详细信息，请参阅 系统和连接要求 中的以下部分：
  - Cloud Connector 常见服务连接要求
  - Cloud Connector 允许的 FQDN

联邦信息处理标准 (FIPS) 支持

Cloud Connector 支持在启用 FIPS 的计算机上使用的 FIPS 验证加密算法。

Citrix Cloud Connector™ 技术详细信息

Citrix Cloud™ Connector 是一个组件，用于在 Citrix Cloud 与您的资源位置之间建立连接。本文介绍了部署要求和场景、Active Directory 和 FIPS 支持以及故障排除选项。

系统要求

请参阅系统要求。

Cloud Connector 已安装的服务

本节介绍随 Cloud Connector 安装的服务及其系统权限。

在安装过程中，Citrix Cloud Connector 可执行文件会安装必要的服务配置并将其设置为正常运行所需的默认设置。如果手动更改了默认配置，Cloud Connector 可能无法按预期运行。在这种情况下，当下次 Cloud Connector 更新发生时（假设处理更新过程的服务仍能正常运行），配置将重置为默认状态。有时，服务会以“禁用”状态发布，以支持添加或删除服务。

Citrix Cloud Agent System 负责促进其他 Cloud Connector 服务正常运行所需的所有提升调用，并且不直接在网络上通信。当 Cloud Connector 上的服务需要执行需要本地系统权限的操作时，它会通过 Citrix Cloud Agent System 可以执行的一组预定义操作来完成。

服务名称	说明	运行身份
思杰云代理系统	处理本地代理所需的系统调用。包括安装、重新启动和注册表访问。只能由 Citrix Cloud Services Agent WatchDog 调用。	本地系统

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

服务名称	说明	运行身份
思杰云服务代理看门狗	监控并升级本地代理（常青）。	网络服务
Citrix Cloud Services 代理日志记录器	为 Citrix Cloud Connector 服务提供支持日志记录框架。	网络服务
Citrix Cloud Services AD 提供程序	使 Citrix Cloud 能够促进管理与其安装所在的 Active Directory 域帐户关联的资源。	网络服务
Citrix Cloud Services 代理发现	使 Citrix Cloud 能够促进管理 XenApp 和 XenDesktop® 旧版本地 Citrix 产品。	网络服务
Citrix Cloud Services 凭据提供程序	处理加密数据的存储和检索。	网络服务
Citrix Cloud Services WebRelay 提供程序	允许从 WebRelay 云服务接收的 HTTP 请求转发到本地 Web 服务器。	网络服务
Citrix CDF 捕获服务	捕获所有已配置产品和组件的 CDF 跟踪。	网络服务
Citrix 配置同步服务	在本地复制代理配置以实现高可用性模式。	网络服务
Citrix 连接租约交换服务	允许 Workspace 应用程序和 Cloud Connector 之间交换连接租约文件，以实现 Citrix® StoreFront Cloud 的服务连续性。	网络服务
Citrix 高可用性服务	在中心站点中断期间提供服务连续性。	网络服务
Citrix ITSM 适配器提供程序	自动化虚拟应用和桌面的预配和管理。	网络服务

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

服务名称	说明	运行身份
思杰 NetScaler® 云网关	为本地桌面和应用程序提供互联网连接，无需打开入站防火墙规则或在 DMZ 中部署组件。	网络服务
思杰远程代理提供程序	允许本地 VDA 和 StoreFront™ 服务器与远程 Broker Service 进行通信。	网络服务
思杰远程 HCL 服务器	代理 Delivery Controller™ 与 Hypervisor 之间的通信。	网络服务
思杰 WEM 云身份验证服务	为 Citrix WEM 代理提供身份验证服务，以便连接到云基础设施服务器。	网络服务
思杰 WEM 云消息传递服务	为 Citrix WEM 云服务提供服务，以接收来自云基础设施服务器的消息。	网络服务
Citrix 安全私有访问™	对所有企业应用程序的零信任网络访问	网络服务
Citrix Cloud Services 消息代理	处理 Citrix Cloud 提供商与 Citrix Cloud 服务之间的消息	网络服务
Citrix 安全票证颁发机构服务	为 Citrix Cloud 服务提供安全票证颁发机构	网络服务
Citrix 监控服务	使 Citrix Monitor 云服务能够监视本地 Citrix 组件并与之通信	网络服务

Active Directory 中 Cloud Connector 的部署方案

您可以使用 Cloud Connector 和 Connector Appliance 连接到 Active Directory 控制器。要使用的连接器类型取决于您的部署。

有关将 Connector Appliance 与 Active Directory 结合使用的更多信息，请参阅 Active Directory 中 Connector Appliance 的部署方案

在您安全的内部网络中安装 Cloud Connector。

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

如果您在单个林中拥有单个域，则只需在该域中安装 Cloud Connector 即可建立资源位置。如果您的环境中存在多个域，则必须考虑在何处安装 Cloud Connector，以便用户可以访问您提供的资源。

如果域之间的信任不是父/子关系，您可能需要为每个单独的域或林安装 Cloud Connector。当使用安全组分配资源或注册来自任一域的 VDA 时，可能需要此配置来处理资源枚举。

注意：

以下资源位置构成了一个蓝图，您可能需要根据资源的托管位置在其他物理位置重复此蓝图。

单个林中的单个域，带有一组 Cloud Connector

在此方案中，单个域包含所有资源和用户对象 (forest1.local)。一组 Cloud Connector 部署在单个资源位置中，并加入 forest1.local 域。

- 信任关系：无 - 单个域
- **身份和访问管理**中列出的域：forest1.local
- 用户登录到云存储：所有用户均支持
- 用户登录到本地存储：所有用户均支持

注意：

如果您在单独的域中拥有管理程序实例，只要管理程序实例和 Cloud Connector 可以通过同一网络访问，您仍然可以部署一组 Cloud Connector。Citrix Cloud 使用托管连接和可用网络与管理程序建立通信。因此，即使管理程序位于不同的域中，您也无需在该域中部署另一组 Cloud Connector 来确保 Citrix Cloud 可以与管理程序通信。

单一林中的父域和子域，带有一组 Cloud Connector

在此场景中，父域 (forest1.local) 及其子域 (user.forest1.local) 位于单个林中。父域充当资源域，子域是用户域。一组 Cloud Connector 部署在单个资源位置中，并加入到 forest1.local 域。

- 信任关系：父/子域信任
- 在 **身份和访问管理** 中列出的域：forest1.local, user.forest1.local
- 用户登录到云存储：所有用户均支持
- 用户登录到本地存储：所有用户均支持

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

注意：

您可能需要重新启动 Cloud Connector，以确保 Citrix Cloud 注册子域。

独立林中的用户和资源（带信任），带有一组 Cloud Connector

在此场景中，一个林 (forest1.local) 包含您的资源域，另一个林 (forest2.local) 包含您的用户域。存在单向信任，其中包含资源域的林信任包含用户域的林。一组 Cloud Connector 部署在单个资源位置中，并加入到 forest1.local 域。

- 信任关系：单向林信任
- 在 **身份和访问管理** 中列出的域：forest1.local
- 用户登录到云存储：仅支持 forest1.local 用户
- 用户登录到本地存储：所有用户均支持

注意：

两个林之间的信任关系需要允许用户林中的用户能够登录到资源林中的机器。

由于 Cloud Connector 无法遍历林级信任，因此 forest2.local 域不会显示在 Citrix Cloud 控制台的 **身份和访问管理** 页面上，也无法被任何云端功能使用。这会带来以下限制：

- 资源只能发布给 Citrix Cloud 中 forest1.local 的用户和组。但是，如果您使用本地存储，forest2.local 用户可以嵌套到 forest1.local 安全组中以缓解此问题。
- 云存储无法验证来自 forest2.local 域的用户。
- Citrix DaaS 中的 Monitor 控制台无法枚举来自 forest2.local 域的用户。

要解决这些限制，请按照 (#users-and-resources-in-separate-forests-with-trust-with-a-set-of-cloud-connectors-in-each-forest) 中所述部署 Cloud Connector。

具有信任关系的独立林中的用户和资源，每个林中都有一组 Cloud Connector

在此场景中，一个林 (forest1.local) 包含您的资源域，另一个林 (forest2.local) 包含您的用户域。存在单向信任关系，其中包含资源域的林信任包含用户域的林。一组 Cloud Connector 部署在 forest1.local 域中，第二组部署在 forest2.local 域中。

- 信任关系：单向林信任
- **身份和访问管理** 中列出的域：forest1.local, forest2.local
- 用户登录到云存储：所有用户均支持

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

- 用户登录到本地存储：所有用户均支持

在此场景中，可以在没有资源的用户林中使用 Connector Appliance 代替 Cloud Connector，以降低成本和管理开销，尤其是在存在多个用户林的情况下。有关更多信息，请参阅 (/zh-cn/citrix-cloud/citrix-cloud-resource-locations/connector-appliance/active-directory.html#users-and-resources-in-separate-forests-with-trust-with-a-single-set-of-connector-appliances-for-all-forests)。

查看 Cloud Connector 的运行状况

Citrix Cloud 中的“资源位置”页面显示您的资源位置中所有 Cloud Connector 的运行状况。您还可以查看每个 Cloud Connector 的高级运行状况检查数据。有关更多信息，请参阅 (/zh-cn/citrix-cloud/citrix-cloud-resource-locations/citrix-cloud-connector/connector-advanced-health-checks.html)。

Windows 事件日志

云连接器会生成某些 Windows 事件日志，您可以通过 Windows 事件查看器查看这些日志。如果您希望启用首选监控软件来查找这些日志，可以将其下载为 ZIP 存档。ZIP 下载包含以下 XML 文件中的这些日志：

- Citrix.CloudServices.Agent.Core.dll.xml（连接器代理提供程序）
- Citrix.CloudServices.AgentWatchDog.Core.dll.xml（连接器 AgentWatchDog 提供程序）

CITRIX.CLOUDSERIVCES.AGENTWATCHDOG

在正常操作期间，可能会发生以下事件：

事件 ID	事件	描述
10000	ConnectedToMessagingService	当连接器与 Citrix Cloud 建立持久的出站 WebSocket 连接时，会引发此事件，从而允许与 Citrix Cloud 进行双向通信。
10001	ConnectedToMessagingServiceWithWebProxy	通过地址为“{0}”的 Web 代理连接到消息服务。WebSocket 连接是使用配置的代理设置的。
10002	UnableToConnectToMessagingService	无法连接到消息服务“{0}”。Cloud Connector 无法建立其到 Citrix Cloud 的 WebSocket 连接。

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

事件 ID	事件	描述
10003	UnableToConnectToMessagingServiceWithWebProxy	无法通过地址为“{0}”的 Web 代理连接到消息服务。Cloud Connector 在使用配置的代理时无法建立其到 Citrix Cloud 的 WebSocket 连接。
10004	ClockOutOfSyncError	与 Citrix Cloud 通信时出现问题。请确保此计算机上的时钟具有正确的时间和时区 (UTC)。您可能需要重新启动计算机以解决此问题。
10005	ConnectivityCheckHealthyToFailedStatus	Cloud Connector 的每小时健康检查在之前健康的情况下报告失败。
10006	ConnectivityCheckFailedStatus	Cloud Connector 的每小时健康检查报告失败，过去也曾出现过故障。
10007	ConnectivityCheckFailedToHealthyStatus	Cloud Connector 的每小时健康检查在之前出现故障后报告了健康状态。
10008	ConnectivityCheckHealthyStatus	Cloud Connector 的每小时健康检查在之前处于健康状态后报告了健康状态。

CITRIX.CLOUDSERVICES.AGENT

在正常操作期间，可能会发生以下事件：

10100	ConnectedToForest	连接到具有域控制器的林。
10101	UnableToConnectToForest	无法连接到林。请确保主机已加入域并具有网络连接。
10102	UnableToConnectToForestWithDomainName	无法连接到与该域关联的林。

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

10103	ClockOutOfSyncError	与 Citrix Cloud 通信时出现问题。请确保此计算机上的时钟具有正确的时间和时区 (UTC)。您可能需要重新启动计算机以解决此问题。

有关 Broker 或 LHC 事件日志的更多信息，请参阅 事件日志

下载 Cloud Connector 事件消息。

Connector 日志文件

默认情况下，事件日志位于托管 Cloud Connector 的计算机的 `C:\ProgramData\Citrix\WorkspaceCloud\Logs` 目录中。

故障排除

诊断 Cloud Connector 任何问题的第一步是检查事件消息和事件日志。如果您在资源位置中没有看到 Cloud Connector 或其处于“未联系”状态，事件日志会提供一些初始信息。

Cloud Connector 连接性

如果 Cloud Connector 处于“已断开连接”状态，Cloud Connector 高级连接检查工具可以帮助验证 Cloud Connector 是否可以访问 Citrix Cloud 及其相关服务。

有关详细信息，请参阅 Cloud Connector 高级连接检查工具。

安装

如果 Cloud Connector 处于“错误”状态，则 Cloud Connector 的托管可能存在问题。请在新计算机上安装 Cloud Connector。如果问题仍然存在，请联系 Citrix 支持。要解决安装或使用 Cloud Connector 时的常见问题，请参阅 CTX221535。

云连接器代理和防火墙配置

云连接器支持通过未经身份验证的 Web 代理服务器连接到 Internet。安装程序及其安装的服务都需要连接到 Citrix Cloud。 在这两个点都需要有 Internet 访问权限。

连接要求

对 HTTP 流量使用端口 443，仅出站。有关所需可联系地址的列表，请参阅以下资源：

- 系统和连接要求
- 云连接器常见服务连接要求

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

Citrix Cloud 所需的可联系地址指定为域名，而非 IP 地址。由于 IP 地址可能会更改，允许使用域名可确保与 Citrix Cloud 的连接保持稳定。

有关所需端口的列表，请参阅 入站和出站端口配置。

重要提示：

- 在某些代理上启用 SSL 拦截可能会阻止云连接器成功连接到 Citrix Cloud。
- 无法在 Citrix Gateway 地址上执行 SSL 拦截。有关详细信息，请参阅 Citrix Gateway Services 连接要求。
- SSL 拦截不得影响网络连接或稳定性。有关详细信息，请参阅 Citrix Cloud Connector
- 如果您正在使用代理，以下流量必须绕过代理：
  - 连接器之间的通信（例如，在 LHC 事件期间）。
  - 连接器与 VDA 之间的通信（WCF 连接）。
  - 连接器与域控制器之间的通信（AD 请求）。

此外，需要注意的是，连接器使用 WinHTTP 代理设置。有关配置设置，请参阅 CTX222727。

检查 Cloud Connector 连接

Cloud Connector 高级连接检查工具可以通过一系列连接检查来帮助验证 Cloud Connector 与 Citrix Cloud 之间的连接。

有关详细信息，请参阅 Cloud Connector 高级连接检查工具。

安装程序

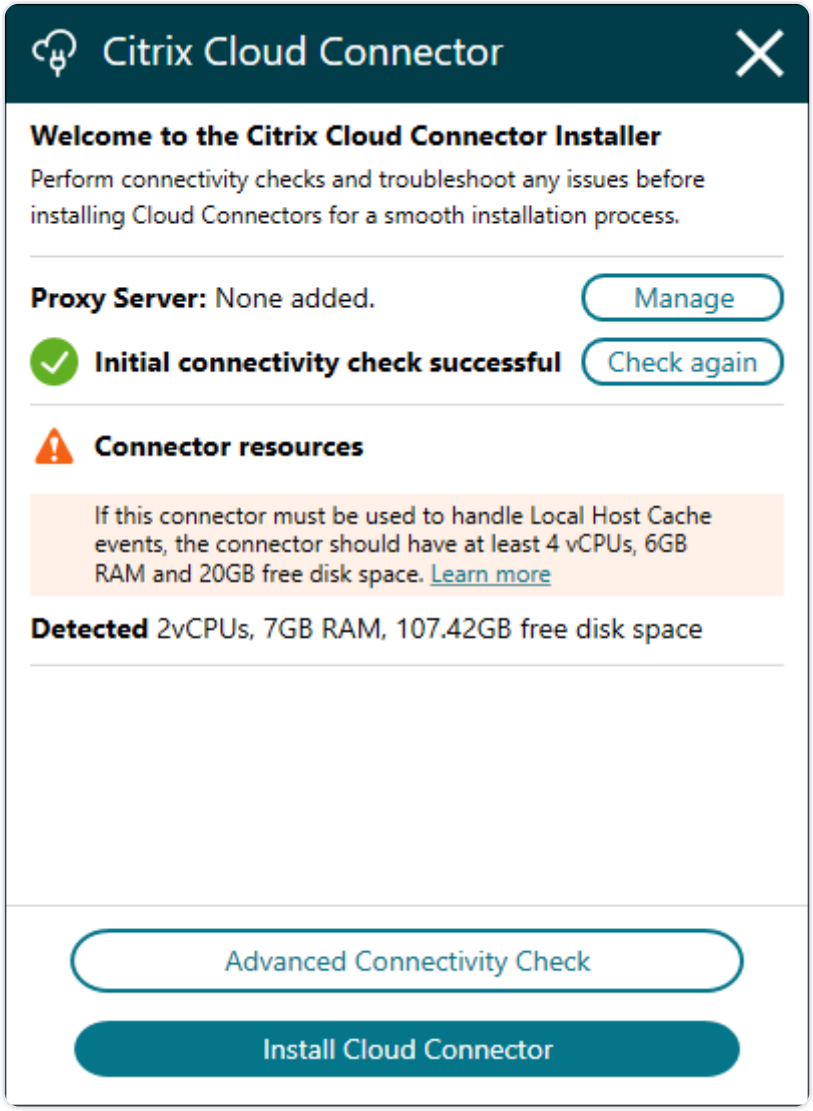
安装程序使用为 Internet 连接配置的设置。如果您可以从计算机浏览 Internet，则安装程序也应该可以正常运行。

运行时服务

运行时服务在本地服务的上下文中运行。它不使用为用户定义的设置（如上所述）。

您可以在安装过程中配置代理设置。

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



安装程序启动后，在登录 Citrix Cloud 之前，单击**配置代理**。系统会提示您添加代理信息和要绕过代理的地址。指定绕过地址时，支持完全限定域名 (FQDN) 和通配符地址。

注意：

如果您正在使用代理服务器，则必须使用手动代理设置。不支持通过自动检测或 PAC/设置脚本进行的自动代理设置。

云连接器安装

您可以交互式地或使用命令行安装 Cloud Connector 软件。

安装以启动安装的用户的权限进行。Cloud Connector 需要访问云以执行以下操作：

- 验证执行安装的用户
- 验证安装程序的权限
- 下载并配置 Cloud Connector 服务

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

安装前需要查看的信息

安装前请查看系统要求。

部署后指南

安装后，请保持所有 Cloud Connector 持续通电，以确保与 Citrix Cloud 的始终在线连接。

升级

升级通常由 Citrix Cloud 自动管理。要手动升级，请先卸载旧的 Cloud Connector，然后再安装新版本。请勿使用较新版本升级以前安装的 Cloud Connector。请勿单独升级 Cloud Connector 的各个组件。

重命名计算机

安装后，请勿重命名托管 Cloud Connector 的计算机。如果以后需要更改服务器名称，请执行以下任务：

1. 从资源位置中移除计算机：
   a. 从 Citrix Cloud 菜单中，选择 **资源位置**。
   b. 找到要管理的资源位置，然后选择 **Cloud Connectors** 磁贴。
   c. 找到要管理的计算机，然后单击省略号菜单。选择 **删除连接器**。
2. 卸载 Cloud Connector 软件。
3. 重命名计算机。
4. 按照本文所述安装最新版本的 Cloud Connector 软件。

将计算机移动到其他域

安装后，请勿将托管 Cloud Connector 的计算机移动到其他域。如果以后需要将计算机加入其他域，请执行以下任务：

1. 从资源位置中移除计算机。
2. 卸载 Cloud Connector 软件。
3. 将计算机从当前域中取消加入，然后将其重新加入新域。
4. 按照本文所述安装最新版本的 Cloud Connector 软件。

克隆计算机的注意事项

每台托管 Cloud Connector 的计算机都必须具有唯一的 SID 和连接器 ID，以便 Citrix Cloud 能够与资源位置中的计算机可靠地通信。如果您打算在资源位置中的多台计算机上托管 Cloud Connector 并希望使用克隆计算机，请执行以下步骤：

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

1. 根据您的环境要求准备计算机模板。
2. 预置您打算用作 Cloud Connector 的计算机数量。
3. 在每台计算机上安装 Cloud Connector，手动安装或使用静默安装模式均可。

不支持在计算机模板（克隆之前）上安装 Cloud Connector。如果您克隆了已安装 Cloud Connector 的计算机，则 Cloud Connector 服务将无法运行，并且该计算机无法连接到 Citrix Cloud。

服务的注意事项

本文中的安装步骤介绍了部署 Cloud Connector 的过程，无论它们用于何种服务。

为 Citrix DaaS 部署 Cloud Connector 时，请验证连接器所在的 AD 域是否处于活动状态，并且在 Citrix Cloud 控制台中未显示为“未使用”。如果在 Citrix DaaS 中设置计算机目录时指定了未使用的域，则可能会发生错误。有关详细信息，请参阅 Citrix DaaS 产品文档中的 在 Citrix Cloud 中添加资源类型或激活未使用的域。

有关其他服务的其他注意事项，请查阅该服务的文档。

默认资源位置

如果您的 Citrix Cloud 帐户中没有资源位置，并且您在域中安装 Cloud Connector，则 Citrix Cloud 创建的资源位置将成为默认资源位置。您的帐户中只能有一个默认资源位置。如果需要，您可以在 Citrix Cloud 中 创建其他资源位置，然后在其他域中安装 Cloud Connector 时选择所需的资源位置。

或者，您可以在域中安装 Cloud Connector 之前，先在控制台中创建所需的资源位置。Cloud Connector 安装程序会在安装过程中提示您选择所需的资源位置。

交互式安装

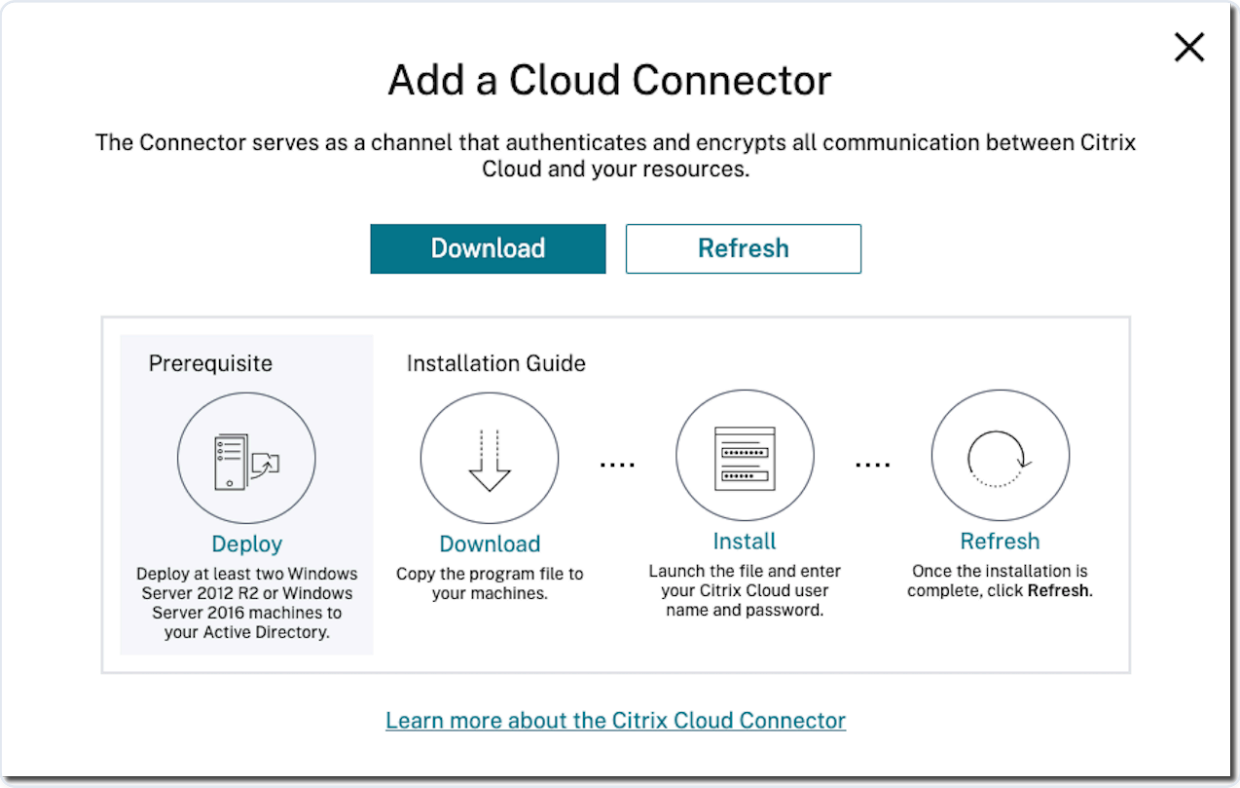
您可以使用图形安装程序界面下载并安装 Cloud Connector。在此之前，您必须在 Citrix Cloud 管理控制台中创建一个或多个资源位置，以便在其上部署 Cloud Connector。有关资源位置的详细信息，请参阅 资源位置。

下载 Citrix Cloud Connector™ 软件

1. 以 Windows 管理员身份登录到您打算安装 Citrix Cloud Connector 的计算机。
2. 访问 https://citrix.cloud.com 并登录您的管理员帐户。
3. 在 Citrix Cloud 控制台中，从主菜单导航到**资源位置**。
4. 如果您还没有资源位置，请单击加号图标 (+) 或选择**添加资源位置**。有关详细信息，请参阅创建资源位置。
5. 找到您要管理的资源位置，然后选择**+ Cloud Connectors**。

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

6. 在打开的窗口中选择**下载**。将 **cwcconnector.exe** 文件保存到连接器计算机上的本地文件位置。

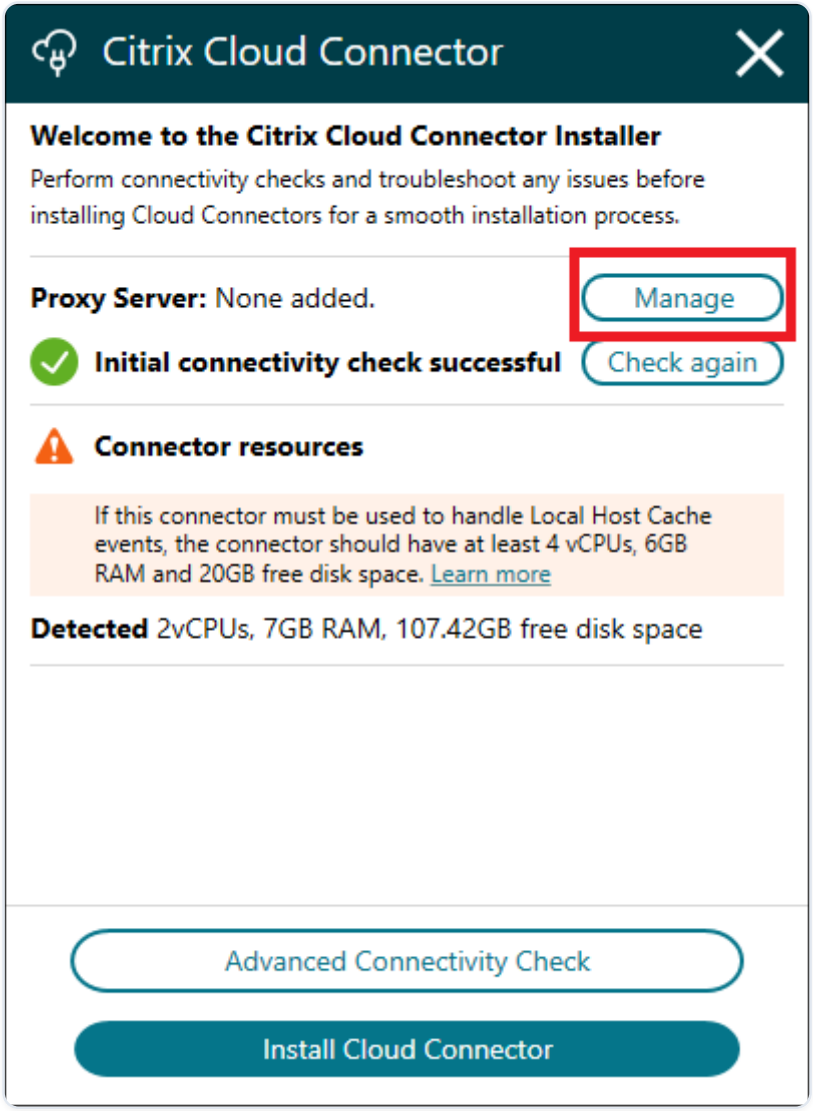


安装 Citrix Cloud Connector 软件

先决条件

1. 右键单击 `cwcconnector.exe` 安装程序文件，然后选择**以管理员身份运行**。安装程序会执行初始连接检查，以确保您在安装 Cloud Connector 之前可以连接到 Citrix Cloud。
2. 单击**管理**以更新代理服务器。

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

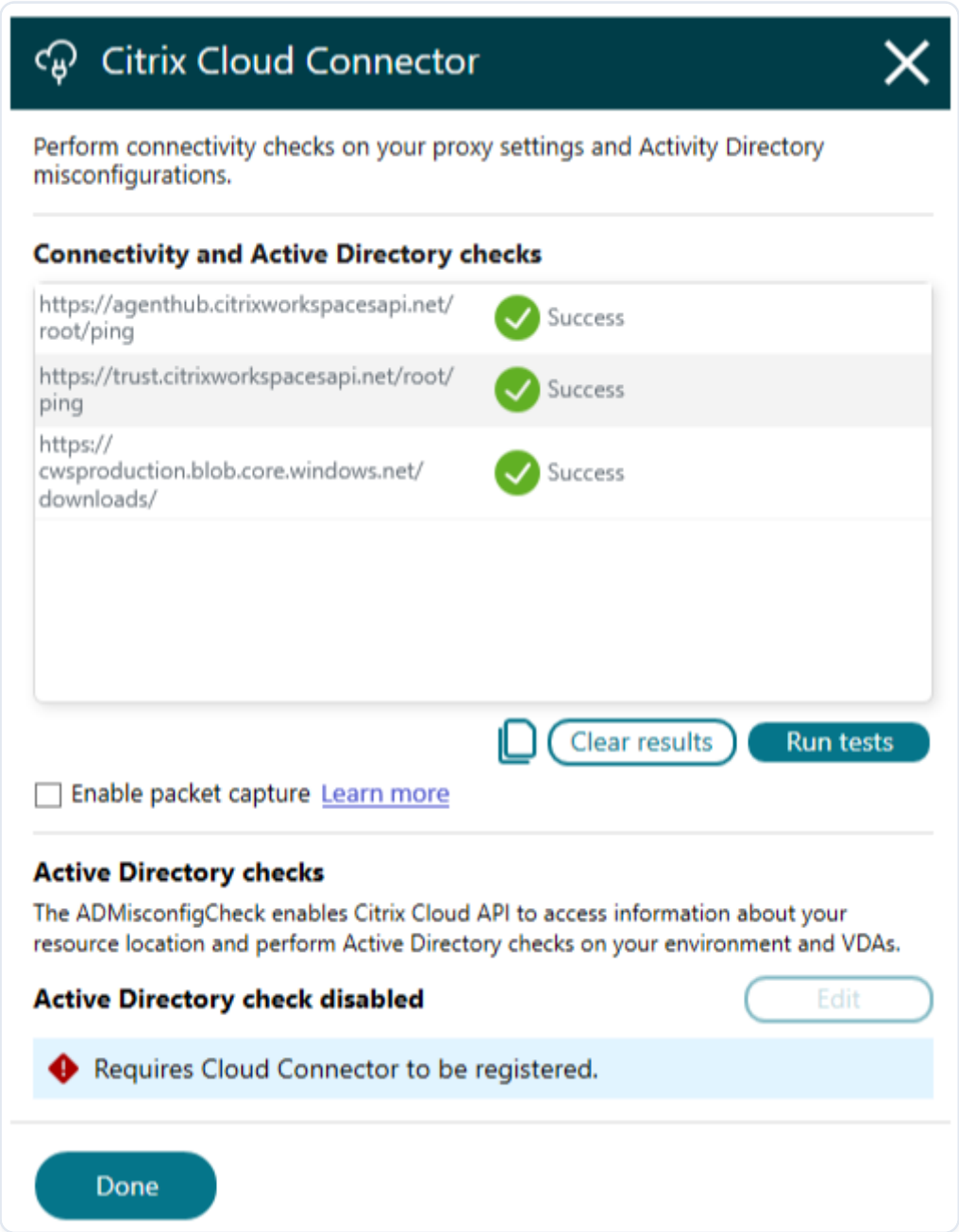


注意：

由于 Microsoft WinHTTP 的限制，仅支持一个代理服务器。有关详细信息，请参阅WinHTTP 中的自动代理问题

1. 单击**高级连接检查**以运行详细检查，确保计算机满足连接器安装的基本连接要求。

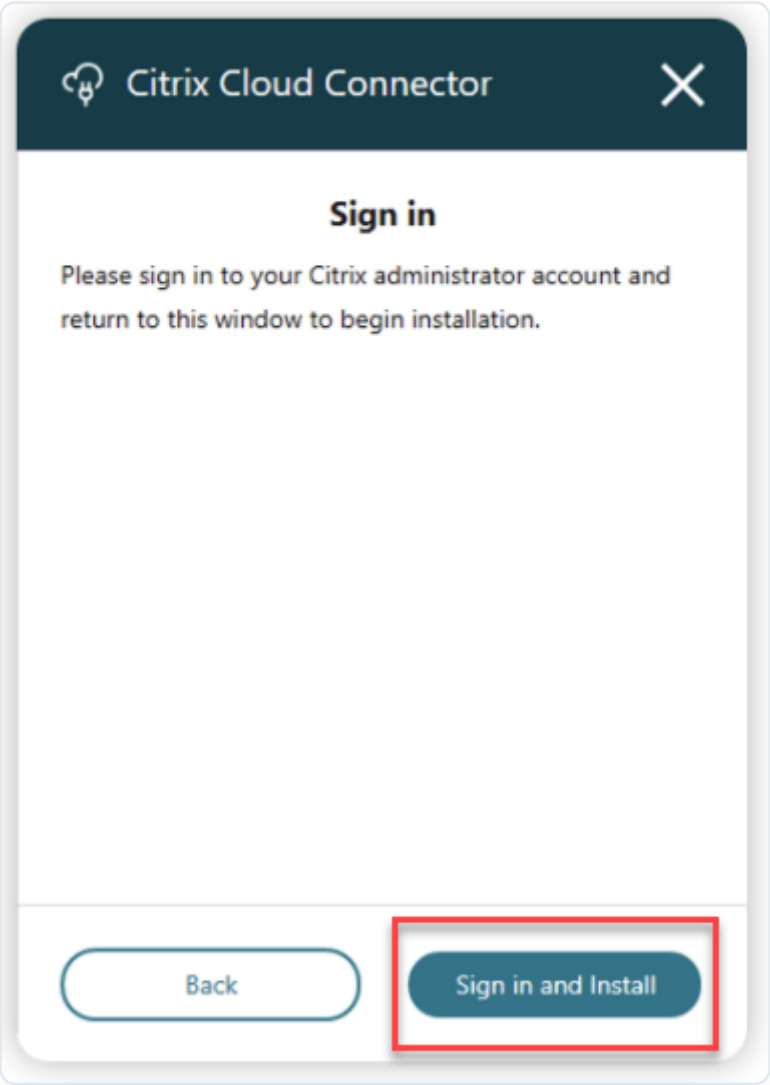
© 1997–2026 Citrix Systems, Inc. All rights reserved.



初始升级和测试

1. 更新 **代理服务器** 并检查 **高级连接检查** 后，单击 **安装 Cloud Connector**。
2. 在 **登录** 页面上，单击 **登录并安装**。

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



3. 此时将显示 **Citrix Cloud 连接测试** 窗口，其中包含初始升级和测试的状态以及事件日志。

   正在进行的初始测试 (/en-us/citrix-cloud/media/initial-tests-in-progress.png)

4. 单击 **查看日志** 以打开包含所有连接检查调试日志的目录 `(C:\ProgramData\Citrix\WorkspaceCloud\InstallLogs)`。
5. 初始升级和测试完成后，您将看到 Citrix Cloud 连接测试 **成功**，如以下图像所示。连接检查结果在首次升级后显示在事件日志框中。

   初始测试完成 (/en-us/citrix-cloud/media/initial-tests-complete.png)

激活未使用的域

如果您正在为 Citrix DaaS™ 创建资源位置并部署 Cloud Connector，请验证您与 Citrix DaaS 配合使用的 AD 域是否处于活动状态且未被视为未使用。如果在 Citrix DaaS 中设置计算机目录时指定了未使用的域，则可能会发生错误。

有关详细信息，请参阅 Citrix DaaS 产品文档中的 在 Citrix Cloud 中添加资源类型或激活未使用的域。

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

创建其他资源位置

1. 在 Citrix Cloud 管理控制台中，单击菜单按钮并选择 **资源位置**。
2. 单击 **+ 资源位置** 并输入一个有意义的名称。
3. 点击“**保存**”。Citrix Cloud 会显示新资源位置的磁贴。
4. 点击“**Cloud Connectors**”，然后点击“**下载**”以获取 Cloud Connector 软件。
5. 在每台准备好的计算机上，使用安装向导或命令行安装安装 Cloud Connector 软件。Citrix Cloud 会提示您选择要与 Cloud Connector 关联的资源位置。

针对多个客户和现有资源位置的安装

如果您是多个客户帐户的管理员，Citrix Cloud 会提示您选择要与 Cloud Connector 关联的客户帐户。

如果您的客户帐户已存在多个资源位置，Citrix Cloud 会提示您选择要与 Cloud Connector 关联的资源位置。

命令行安装

支持静默或自动化安装。但是，连接器安装程序会定期更新，因此建议每次安装都下载最新的安装程序。从 Citrix Cloud 控制台的“资源位置”页面下载新的 Cloud Connector 安装程序。

要求

要将命令行安装与 Citrix Cloud 结合使用，您需要提供以下信息：

- 您正在为其安装 Cloud Connector 的 Citrix Cloud 帐户的客户 ID。此 ID 显示在“**身份和访问管理**”中的“**API 访问**”选项卡顶部。
- 您要用于安装 Cloud Connector 的服务主体的 ID 和密钥。要获取这些值，您必须首先创建一个服务主体。服务主体必须以“完全访问”权限创建。有关创建服务主体的更多信息，请参阅创建服务主体。获得服务主体的 ID 和密钥后，即可继续进行 Cloud Connector 安装。
- 您要与 Cloud Connector 关联的资源位置的资源位置 ID。要检索此值，请在“**资源位置**”页面上资源位置名称下方选择“**ID**”按钮。如果您不提供此值，Citrix Cloud 将使用默认资源位置的 ID。

支持的参数

为确保服务主体 ID 和密钥的安全性，必须向安装程序提供 JSON 配置文件。此文件必须在安装完成后删除。配置文件的支持值包括：

- **customerName** 必需。Citrix Cloud 控制台（在“身份和访问管理”中）的“API 访问”页面上显示的客户 ID。
- **clientId** 必需。管理员可以在“API 访问”页面上创建的服务主体 ID。

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

- **clientSecret** 必需。创建服务主体后可以下载的服务主体密钥。位于“API 访问”页面上。
- **resourceLocationId** 建议。现有资源位置的唯一标识符。在 Citrix Cloud 控制台的“资源位置”页面上选择“ID”按钮以检索资源位置 ID。如果未指定任何值，Citrix Cloud 将使用帐户中第一个资源位置的 ID。
- **acceptTermsOfService** 必需。必须设置为 **true**。

示例配置文件

```
{

"customerName": "CustomerID",

"clientId": "clientID",

"clientSecret": "ClientSecret",

"resourceLocationId": "ResourceLocationId",

"acceptTermsOfService": "true"

}
```

示例命令

以下命令使用 JSON 配置文件以静默方式安装 Cloud Connector 软件：

```
CWCConnector.exe /q /ParametersFilePath:c:
\cwcconnector_install_params.json
```

使用 `/q` 指定静默安装。

使用 **Start /Wait CWCConnector.exe /ParametersFilePath:value** 检查故障情况下的潜在错误代码。安装完成后，您可以使用运行 **echo %ErrorLevel%** 的标准机制。

HTTPS 配置

为了允许 StoreFront™ 和 NetScaler Gateway 设备安全地连接到 Cloud Connector 并加密所有数据，强烈建议您启用 HTTPS。这需要 SSL 证书。

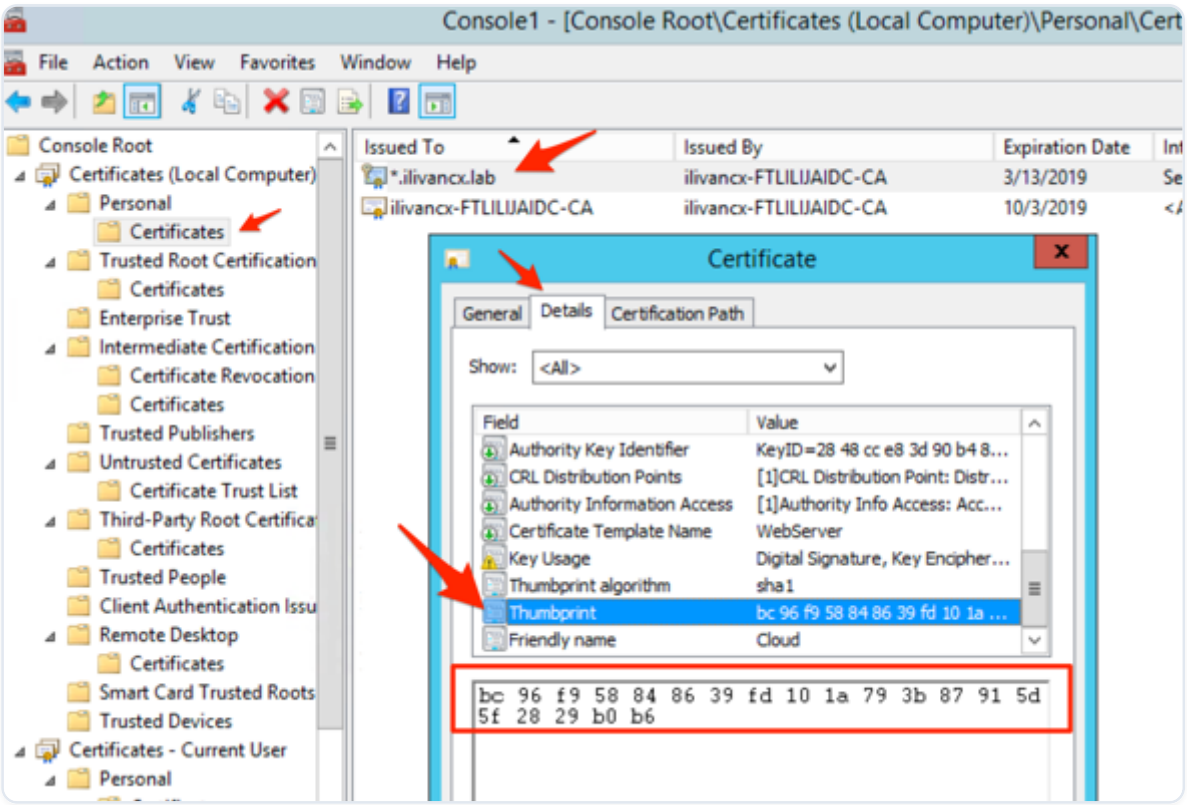
- 证书必须包含用于访问连接器的 FQDN 作为公用名或主题备用名称。如果您在连接器前面部署了负载平衡器，则使用负载平衡器的 FQDN。
- 证书可以由企业 CA 或公共 CA 签名。

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

- 连接到 Cloud Connector 的任何 StoreFront 和网关服务器都必须信任该证书。

要启用 HTTPS：

1. 打开 证书 MMC 管理单元。
2. 在个人证书存储中创建或导入合适的证书。有关管理证书的更多信息，请参阅 管理证书。
3. 打开证书，转到**详细信息**选项卡，记下**指纹**，忽略所有空格。



4. 确定要将证书绑定到哪个 IP 地址。通常，您可以使用 `0.0.0.0` 的 IP 地址应用于所有 IPv4 地址。如果启用了 IPv6，则使用 `[::]` 应用于所有 IPv6 地址。如果您只想将更改应用于特定的网络适配器，请记下该网络适配器的 IP 地址。
5. 在提升的命令提示符下运行

```
netsh http add sslcert ipport=<IP address>:<Port number>
certhash=<Certificate Hash Number> appid={Any GUID}
```

您可以为 AppId 使用任何有效的 GUID。其目的是记录哪个应用程序添加了绑定。但是，该绑定适用于使用该端口的所有应用程序。

例如：

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

```
C:\> netsh http add sslcert ipport=0.0.0.0:443
certhash=BC96F958848639FD101A793B87915D5F2829B0B6 appid={6DE9BEFD-
F4CB-4D63-8681-E88012D6F5F1}



SSL Certificate successfully added
```

6. 要禁用 HTTP，请在注册表中转到 `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\DesktopServer` 并创建名称为 `XMLServicesEnableNonSSL` 且值为 0 的 `DWORD`。

后续步骤

1. 设置 Citrix Cloud Connector 更新计划。有关 Citrix Cloud Connector 更新和管理更新计划的信息，请访问 连接器更新。
2. 如果您正在使用 StoreFront，请配置 StoreFront，使其可以使用连接器访问 DaaS 以枚举和启动资源。如果这是新 DaaS 部署中的第一个连接器，则创建新的资源源。如果这是附加连接器，则建议为了弹性，将所有 Cloud Connector 添加到现有 DaaS 资源源的服务器列表中。有关更多信息，请参阅 管理商店中可用的资源。
3. 如果您正在将 StoreFront 与 NetScaler 网关结合使用，则可以使用连接器访问 Citrix Cloud Secure Ticket Authority (STA)。有关更多信息，请参阅 配置 Citrix 网关。
4. 如果这是特定 Active Directory 域上的第一个连接器，则可以将该域连接到 Citrix Cloud。有关更多信息，请参阅 将 Active Directory 连接到 Citrix Cloud。

安装问题疑难解答

本节详细介绍了诊断和修复安装过程中可能遇到的一些问题的方法。有关安装问题疑难解答的更多指导，请参阅Citrix Cloud Connector 疑难解答指南。

安装日志

您可以通过首先查阅可用的日志文件来排查安装过程中遇到的问题。

安装期间发生的事件可在 **Windows 事件查看器**中找到。您还可以查看 Cloud Connector 安装日志，这些日志位于 **%LOCALAPPDATA%\Temp\CitrixLogs\CloudServicesSetup**。 安装后，日志还会添加到 **%ProgramData%\Citrix\WorkspaceCloud\InstallLogs**。

退出代码

根据安装过程的成功或失败，可能会返回以下退出代码：

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

- 1603 - 发生意外错误
- 2 - 先决条件检查失败
- 0 - 安装成功完成

安装错误

如果您通过双击安装程序来安装 Citrix Cloud Connector 软件，则可能会收到以下错误消息：

`Can't reach this page.`.

即使您以管理员身份登录计算机来安装 Citrix Cloud Connector，也可能会发生此错误。为避免此错误，请右键单击安装程序并选择“以管理员身份运行”，以管理员身份运行 Citrix Cloud Connector 软件。

连接失败

为确保 Cloud Connector 可以与 Citrix Cloud 通信，请确认以下 Citrix 服务处于 **已启动** 状态：

- Citrix Cloud AD 提供程序
- Citrix Cloud 代理记录器
- Citrix Cloud 代理系统
- Citrix Cloud 代理看门狗
- Citrix Cloud 凭据提供程序
- Citrix 配置同步器服务
- Citrix 高可用性服务
- 思杰 NetScaler® CloudGateway
- Citrix 远程代理提供程序
- Citrix 远程 HCL 服务器
- Citrix 会话管理器代理

有关这些服务的更多信息，请参阅已安装的服务。

Cloud Connector 高级连接检查工具可以帮助验证 Cloud Connector 是否可以访问 Citrix Cloud 及其相关服务。

有关详细信息，请参阅Cloud Connector 高级连接检查工具。

有关如何解决连接检查失败的更多信息，请参阅 CTX224133: Cloud Connector 连接检查失败。

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

Cloud Connector 高级连接检查

Cloud Connector 包含两个工具，可帮助管理员诊断和解决连接问题。它们是 Cloud Connector 安装程序中提供的 `Advanced Connectivity Checks`，以及与 Cloud Connector 软件一同安装的 `Citrix Cloud Services Connectivity Test Tool`。

这两个工具都包含以下测试：

- 代理和防火墙配置符合 Cloud Connector 连接要求
- 证书要求符合 证书验证要求

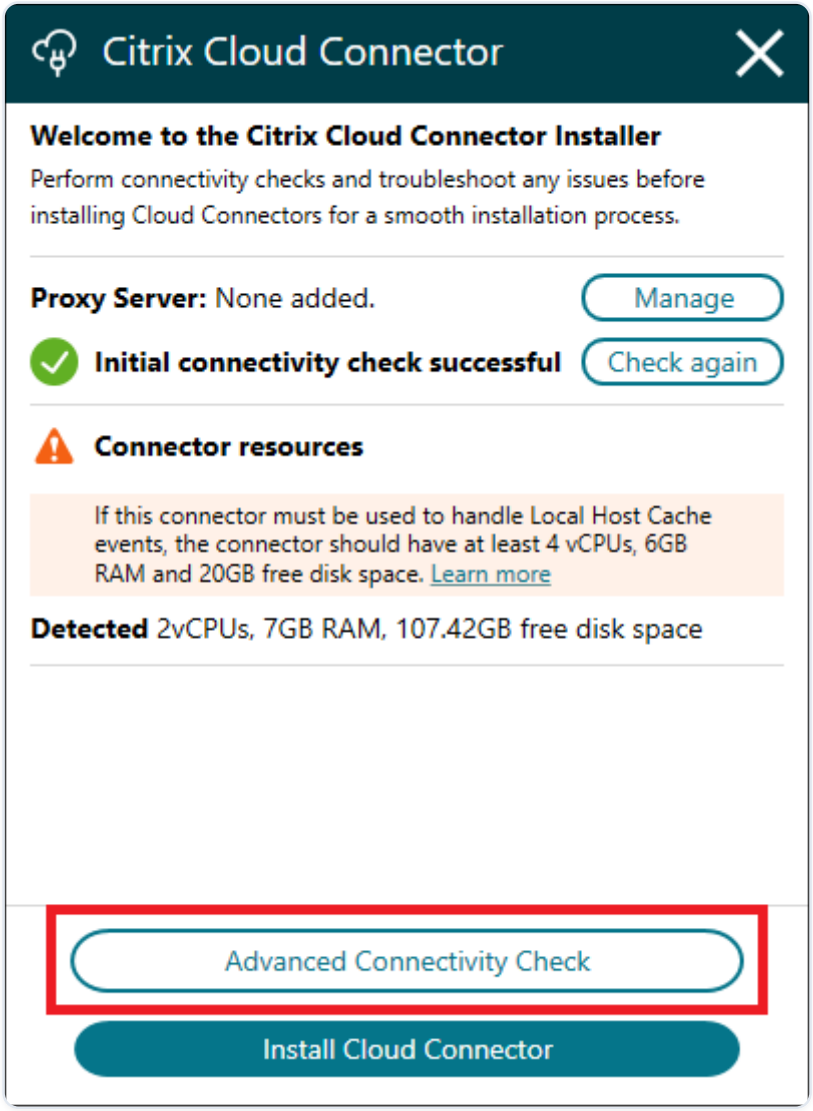
这些工具还可以用于执行网络数据包捕获，以帮助诊断和解决连接问题。

Cloud Connector 安装程序高级连接检查

`Advanced Connectivity Checks` 包含在 Cloud Clonnecter `cwcconnector.exe` 安装程序中。

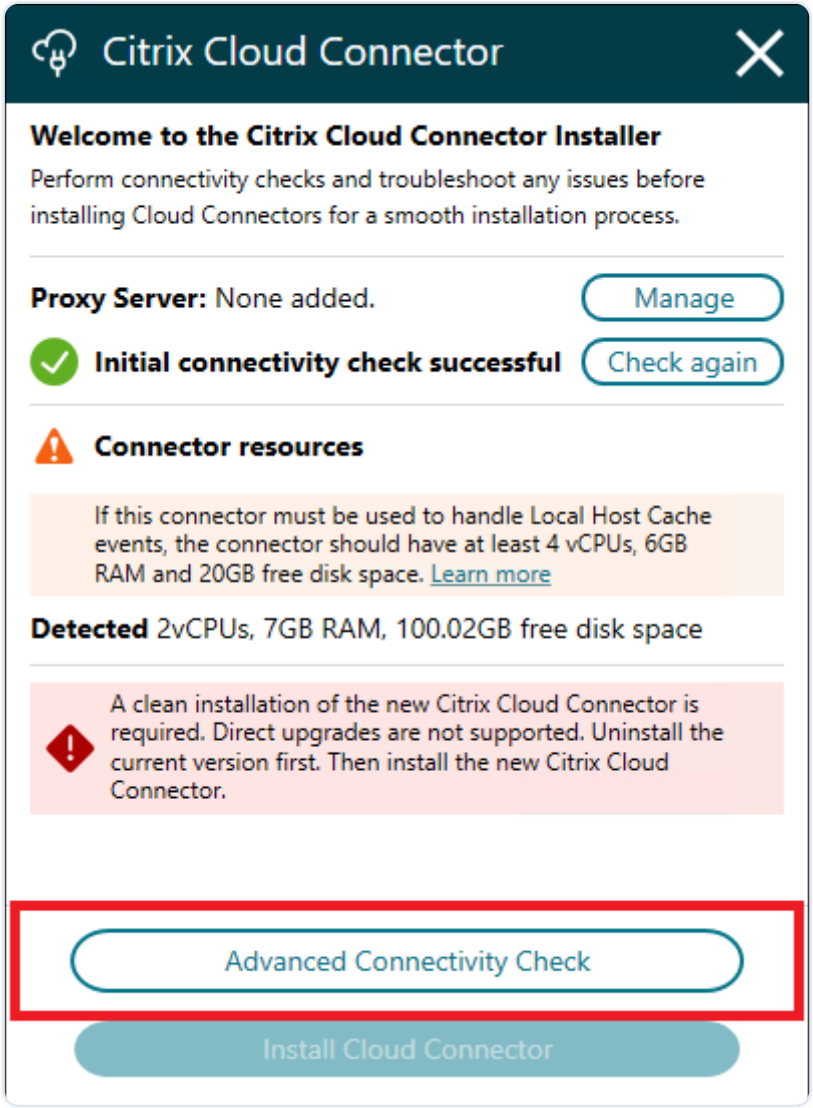
要访问这些检查，请右键单击 `cwcconnector.exe` 安装程序文件并选择“以管理员身份运行”。然后可以通过单击“高级连接检查”来访问高级连接检查工具。

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



如果 Cloud Connector 软件已安装在主机上，则会出现警告，并且 `Install Cloud Connector` 选项将被禁用，但是“高级连接检查”选项仍将可用。

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



安装程序高级连接检查执行的检查

高级连接检查工具执行的检查分为三类。

- **初始检查：** 这些是安装和注册 Cloud Connector 所需的平台服务检查。它们涵盖了与 Cloud Connector 编排、身份验证和升级相关的服务的连接。
- **证书检查：** 这些测试验证必要的根证书和中间证书是否存在，以验证与 Citrix Cloud 的安全连接（TLS 证书）并检查升级包的完整性（代码签名证书）。有关 Cloud Connector 证书要求的更多信息，请参阅证书验证要求。
- **FQDN 检查：** 这些检查涵盖了与在Cloud Connector 常见服务要求中发布的完全限定域名 (FQDN) AllowList.json 中描述的其余服务的连接。

Citrix Cloud Services 连接测试工具

`Citrix Cloud Services Connectivity Test Tool` 仅在已安装 Cloud Connector 软件的主机上可用。可以通过导航到 `Start Menu > Citrix > Citrix Cloud Services Connectivity Test Tool` 来访问它。

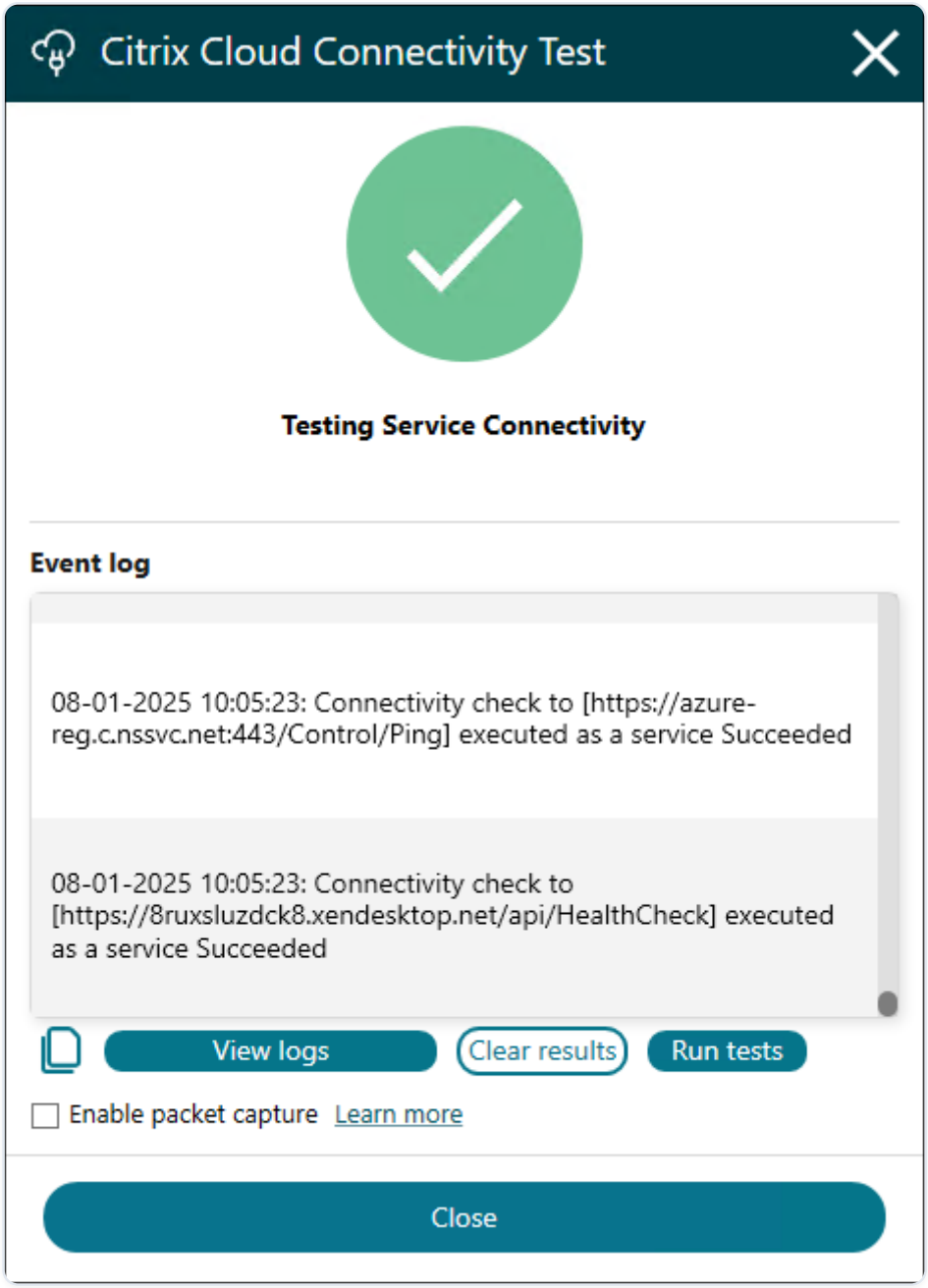
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix Cloud Services 连接测试工具执行的检查

独立的 `Citrix Cloud Services Connectivity Test Tool` 执行与上述相同的初始、证书和 FQDN 检查。此外，它还执行一组额外的特定于用例的测试。

Citrix Cloud Connector™ 会安装许多与其每个用例相关的服务。每个服务都实现了一组与其特定用例相关的连接检查。Citrix Cloud Services 连接测试工具通过查询每个服务来执行为其特定用例实现的测试。

这些测试的详细信息可以通过运行该工具找到。也可以访问包含相同内容的日志文件。

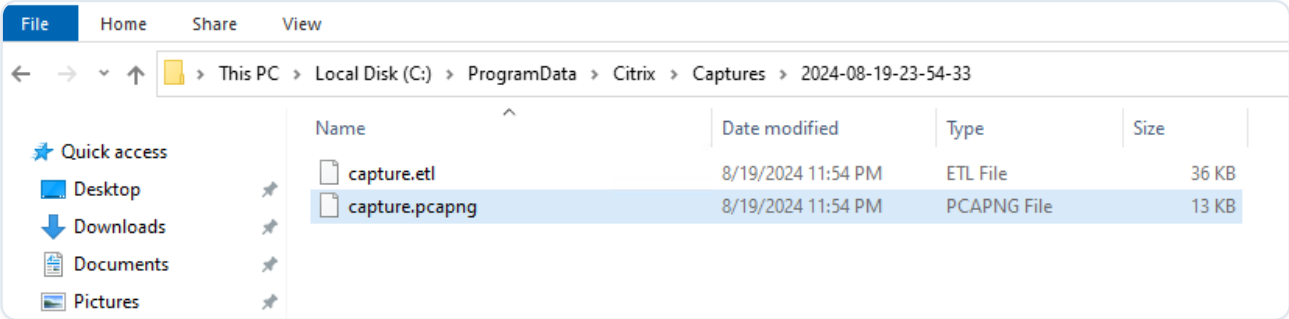


© 1997–2026 Citrix Systems, Inc. All rights reserved.

数据包捕获

`Advanced Connectivity Checks` 和 `Citrix Cloud Services Connectivity Test Tool` 都包含在执行连接检查的同时执行数据包捕获的功能。默认情况下，此复选框未选中，因此除非明确启用，否则不会执行数据包捕获。

激活后，此功能会利用 Windows 上内置的 `pktmon` 实用程序在连接检查期间捕获网络流量。检查完成后，捕获的数据将保存在本地 `C:\ProgramData\Citrix\Captures` 下的一个带时间戳的子目录中。文件将以 .etl 和 .pcapng 两种格式存储。.pcapng 是与 Wireshark 等工具兼容的广泛使用的格式。这些文件保留在您的本地计算机上，不会上传到 Citrix Cloud。



对于需要额外帮助的客户，可以将这些数据包捕获共享给我们的支持团队，以帮助诊断连接问题。

注意：

当在安装程序的“高级连接检查”屏幕或 Citrix Cloud 连接测试工具中激活数据包捕获功能时，在连接检查期间发生的所有网络流量都将被记录。这不仅包括由连接检查及其相关的 Cloud Connector 组件生成的流量，还包括 Cloud Connector VM 上的任何其他网络活动。例如，在连接检查期间发生的任何未加密的 HTTP 流量（例如登录尝试）也将被捕获到生成的数据包捕获文件中。

Cloud Connector 高级健康检查 - 已弃用

注意：

Cloud Connector 健康指标和警报已添加到 Citrix DaaS™ 基础设施监控中。这应该是主动分析和排查您的基础设施相关问题的主要位置。

有关详细信息，请参阅基础设施监控。
在更新之前和之后，Cloud Connector 执行健康检查，以确保更新不会给提供商造成不必要的停机。您可以查看 Connector 以及 Connector 上每个服务或提供商的连接和健康状态。

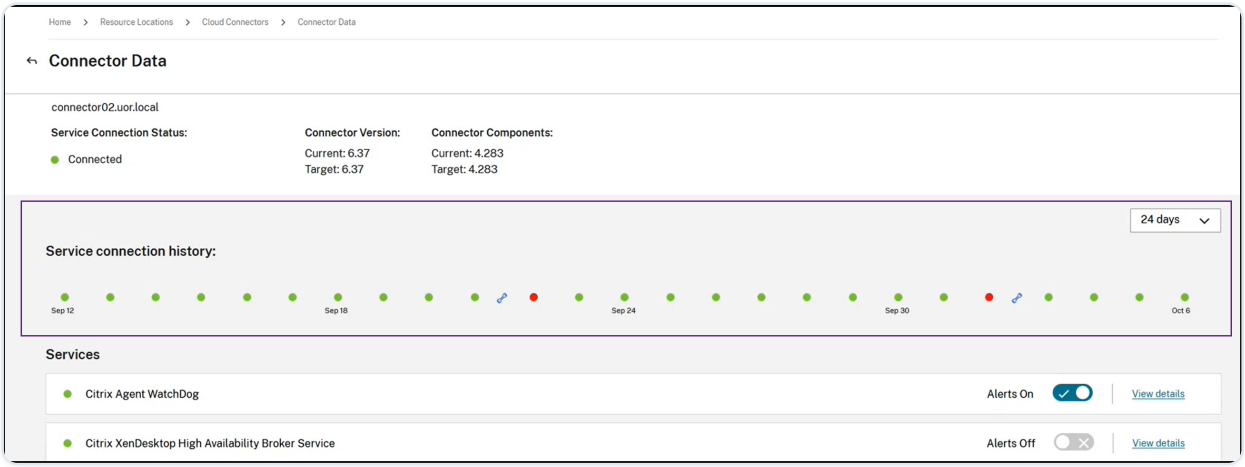
© 1997–2026 Citrix Systems, Inc. All rights reserved.

查看 Connector 健康检查数据

1. 从 Citrix Cloud™ 菜单中，选择**资源位置**。
2. 选择要查看其健康检查数据的 Connector。
3. 在“Connectors”页面上，转到 Connector 旁边的省略号菜单，然后选择**查看 Connector 数据**。

将显示“Connector 数据”页面，其中显示以下信息。

- **服务连接状态**。“Connector 数据”页面的此区域显示：
  - 您的 Connector 是否已连接到云
  - 对于 Connector 及其组件，当前安装的版本以及下次更新中要安装的目标版本
- **服务连接历史记录**。24 个状态指示器显示 Connector 随时间的健康状态。默认情况下，服务连接历史记录以一小时为间隔显示过去 24 小时的状态。要查看更多历史记录，请从下拉菜单中选择**24 天**。该视图以一天为间隔显示过去 24 天的状态。
  - 绿点表示在此时间间隔内的健康状态。
  - 红点表示在该时间间隔内出现故障或异常状态。将鼠标悬停在点上可获取更多信息。
  - 扳手图标表示在该时间间隔内发生了更新。将鼠标悬停在扳手图标上可获取更多信息。
  - 灰点表示在该时间间隔内未收到任何运行状况信息。



- **服务**。此区域列出了在连接器上运行的每个服务。
  - 每个服务旁边的点表示服务的当前状态。
  - 使用“**警报开启**”和“**警报关闭**”来控制是否接收来自服务的警报通知。如果警报设置为“开启”，则服务中的故障会导致整体连接器连接状态失败。
  - 选择“**查看详细信息**”以查看服务随时间的运行状况详细信息。

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

- **连接器指标**。此区域显示连接器在过去 24 小时或 24 天内的内存使用情况、CPU、网络数据和磁盘空间使用情况。使用“**服务连接历史记录**”区域中的下拉菜单来控制显示的时间段。

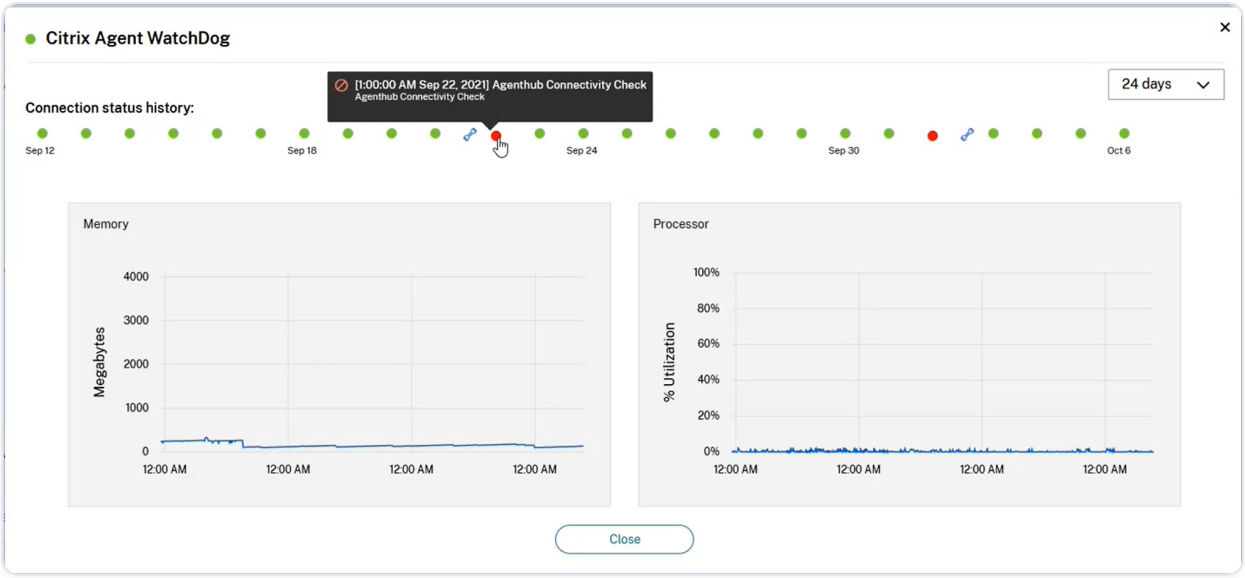
查看服务详细信息

要查看每个服务的连接状态历史记录和指标：

1. 使用“**服务连接历史记录**”部分中的下拉菜单选择时间段。您可以按一小时间隔查看过去 24 小时，或按一天间隔查看过去 24 天。
2. 在“连接器数据”页面上，选择服务旁边的“**查看详细信息**”。

出现的页面显示：

- 24 个状态指示器，显示服务随时间的运行状况。
  - 绿点表示在此时间间隔内状态正常。
  - 红点表示在此时间间隔内出现故障或异常状态。将鼠标悬停在点上可获取更多信息。
  - 扳手图标表示在此时间间隔内发生了更新。将鼠标悬停在扳手图标上可获取更多信息。
  - 灰点表示在此时间间隔内未收到任何运行状况信息。
- 显示服务在指定时间段内的内存和处理器使用情况的图表。



连接器通知

您的连接器会在出现警告或错误情况后的 2 小时内生成通知。您可以在 Citrix Cloud™ 标头中的铃铛图标上看到新通知。

单击此图标可查看通知，或从控制台菜单中选择**通知**。

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

有关详细信息，请参阅通知。

注意：

当为 Cloud Connector 发出通知时，务必在重新安装 Cloud Connector 软件之前了解根本原因。否则可能会导致问题再次发生。

如果需要重新安装，务必确保资源位置中的其他 Cloud Connector 运行状况良好，并且在第一个 Cloud Connector 移除后不会受到问题的影响。否则可能会导致服务中断。

云连接器

下表列出了 Cloud Connector 可以发出的通知：

警报消息	警报类型	详细信息	解决方案
连接器 *CONNECTOR_NAME* 处于脱机状态且已过期，因为未能执行定期维护。过期的连接器将影响服务可用性并阻止维护。	错误	如果连接器长时间处于离线状态，之后又重新上线，它可能是一个无法更新到最新版本的旧版本。过时的连接器无法执行维护，并可能影响环境中其他连接器的维护过程。	在卸载过时的 Cloud Connector 之前，请安装一个新的 Cloud Connector。
连接器 *CONNECTOR_NAME* 未与 UTC 时间同步。处于此状态的连接器可能会影响服务可用性、功能或性能。	错误		如何同步 Cloud Connector 时间
连接器 *CONNECTOR_NAME* 的维护失败。此连接器上的维护失败将阻止环境中其他连接器的维护。维护失败的连接器可能会影响	错误	此连接器上的连接器升级或其他维护操作失败。	如何解决 Cloud Connector 维护失败问题

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

警报消息	警报类型	详细信息	解决方案
服务可用性、功能或性能。			
连接器 *CONNECTOR_NAME* 已离线 *NUMBER* 小时或更长时间。离线连接器将影响服务可用性并阻止维护。	警告	如果连接器在一定小时数内无法联系，则被视为离线。	如何将离线 Cloud Connector 恢复到在线状态
连接器 *CONNECTOR_NAME* 最近的连接性检查失败。连接性检查失败可能会影响服务可用性或功能。	警告	连接性检查失败，错误代码为 *HEALTH_CHECK_CODE*。此连接器无法联系通知消息中列出的某些 Web 或 IP 地址。	Cloud Connector 连接性检查失败
连接器 *CONNECTOR_NAME* 的 CPU 利用率过高。资源受限的连接器可能会影响服务可用性、功能或性能。	警告	此连接器在一小时采样期内 CPU 利用率已超过 80%。	如何解决 Cloud Connector 资源可用性警报
连接器 *CONNECTOR_NAME* 的可用磁盘空间不足。磁盘空间受限的连接器将影响服务性能和维护。	警告	此连接器的可用磁盘空间不足 2 GB。	如何解决 Cloud Connector 资源可用性警报
连接器 *CONNECTOR_NAME* 检测到关键进程或服务已停止运行。此状态可能会影响服务可用性、功能或性能。	警告		

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

Citrix Cloud Connector™ 的日志收集

CDF 日志用于 Citrix 产品中的故障排除。Citrix 支持人员使用 CDF 跟踪来识别应用程序和桌面代理、用户身份验证、虚拟投递代理 (VDA) 注册方面的问题。本文讨论如何捕获 Cloud Connector 数据，这些数据可用于排查和解决您在环境中可能遇到的问题。

重要说明：

- 在资源位置中的所有 Cloud Connector 计算机上启用日志记录。
- 为确保捕获完整的数据范围，Citrix 建议使用 VDA 上的 CDFControl 捕获工具。有关详细信息，请参阅 Citrix 支持知识中心中的 CTX111961。有关 Citrix Workspace 应用程序的日志收集的更多信息，请参阅 CTX141751。
- 要向 Citrix 提交 CDF 跟踪，您必须有一个开放的 Citrix 支持案例。Citrix 支持技术人员无法审查未附加到现有支持案例的 CDF 跟踪。

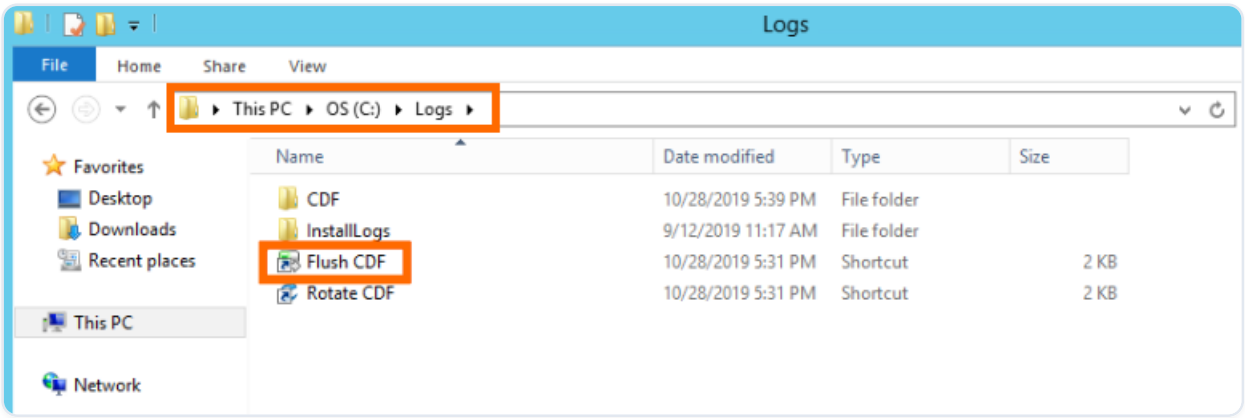
步骤 1：重现问题

在此步骤中，重现您在环境中遇到的问题。如果问题与应用程序启动或代理相关，请重现启动失败。如果问题与 VDA 注册相关，请通过在 VDA 计算机上手动重新启动 Citrix Desktop Service 来重现 VDA 注册尝试。

步骤 2：收集 CDF 跟踪

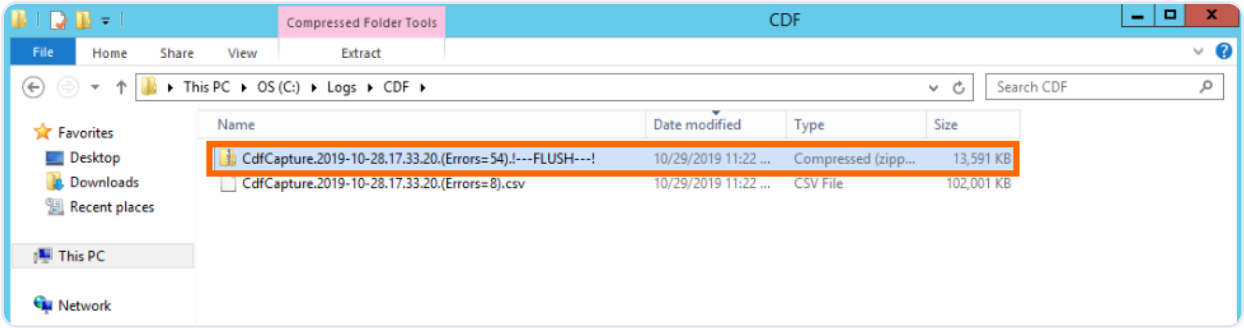
在此步骤中，您将从资源位置中的每个 Cloud Connector 收集 CDF 刷新跟踪。

1. 使用域管理员或本地管理员帐户启动 RDP 连接，访问 Cloud Connector 计算机。
2. 在 Cloud Connector 计算机上，打开文件资源管理器并导航到 `C:\logs`。



3. 运行 **Flush CDF**。一个图标会在 Cloud Connector 计算机的任务栏上短暂出现，然后消失。
4. 在文件资源管理器中，导航到 C:\logs\CDF 并找到以 **!--FLUSH--!** 结尾的最新文件夹。

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

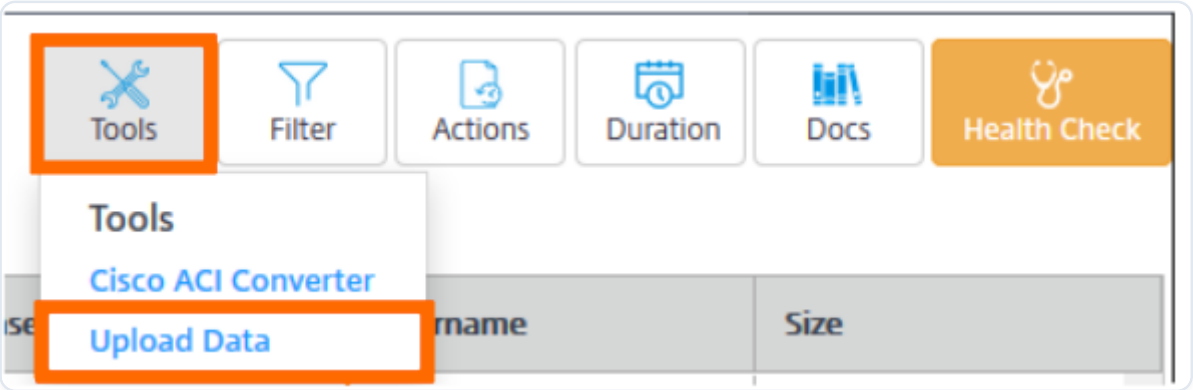


5. 在资源位置中的每台 Cloud Connector 计算机上执行步骤 1-5，并将所有 Cloud Connector 刷新跟踪合并到一个 ZIP 存档中。如果您不创建所有 Cloud Connector 计算机的刷新跟踪的 ZIP 存档，则需要逐个提交给 Citrix。

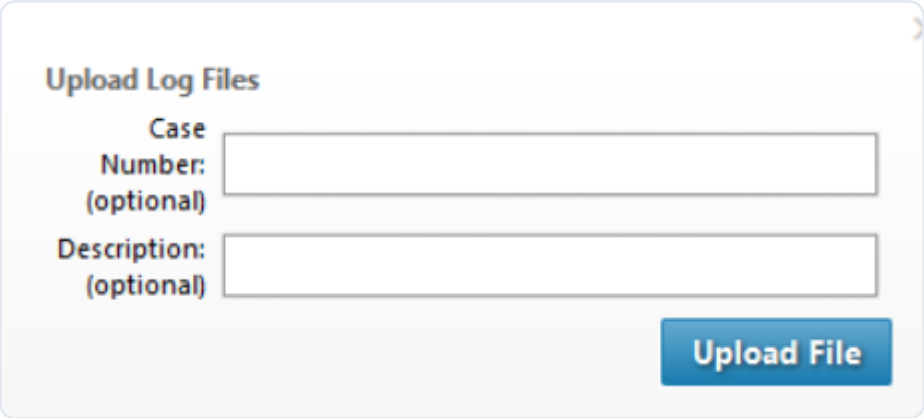
步骤 3：将数据提交给 Citrix

在此步骤中，您将跟踪文件附加到您的 Citrix 支持案例并提交以供审查。

1. 访问 https://cis.citrix.com/ 并使用您的 Citrix.com 凭据登录。
2. 选择 **诊断**。
3. 选择 **工具**，然后选择 **上传数据**。



4. 在 **案例编号** 中，输入现有支持案例的 Citrix 支持案例编号。如果没有附加到数据上传的案例编号，Citrix 支持技术人员无法正确审查 CDF 跟踪。



5. 在 **描述**（可选）中，您可以输入简要描述或将此字段留空。

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

6. 选择 **上传文件** 并选择您之前创建的 ZIP 存档。如果您没有从所有 Cloud Connector 计算机创建刷新跟踪的 ZIP 存档，请重复步骤 3-6 以附加您要提交的每个刷新跟踪。

提交刷新跟踪后，Citrix Insight Services 会对其进行处理并将其附加到您指定的支持案例。此过程可能需要长达 24 小时，具体取决于文件大小。

选择主资源位置

如果您的域中有多个资源位置，您可以选择其中一个作为 Citrix Cloud 的“主”或“首选”位置。主资源位置在 Citrix Cloud 和您的域之间提供最佳性能和连接，使用户能够快速登录。

当您选择主资源位置时，该资源位置中的 Cloud Connector 将尽可能用于用户登录和预配操作。如果主资源位置中的 Cloud Connector 不可用，则这些操作将使用域中的另一个 Cloud Connector 执行。使用用户主体名称 (UPN) 的登录可能不包含域名，并且可能不使用主资源位置。

注意：

为确保 Cloud Connector 在任何资源位置始终可用，请在每个资源位置至少安装两个 Cloud Connector。

要决定将哪个资源位置用作主资源位置，请考虑以下因素：

- 该资源位置是否与您的域具有最佳连接？
- 该资源位置是否最接近您使用 Citrix Cloud 管理控制台的地理区域？例如，如果您的 Citrix Cloud 控制台位于 https://us.cloud.com，则您选择的资源位置将是距离美国区域最近的一个。

选择主资源位置

1. 在 Citrix Cloud 管理控制台中，单击菜单按钮并选择**身份和访问管理**。
2. 单击**域**，然后展开包含您要使用的资源位置的域。
3. 单击**设置主资源位置**，然后选择要指定为主的资源位置。
4. 单击**保存**。Citrix Cloud 会在您选择的资源位置旁边显示“主”。

注意：

在展开其他域之前，请务必在一个域中保存您的选择。当您展开一个域然后展开另一个域时，之前展开的域会折叠并丢弃任何未保存的选择。

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

选择不同的主资源位置

1. 在 Citrix Cloud 管理控制台中，单击菜单按钮并选择 **身份和访问管理**。
2. 单击 **域**，然后展开包含要更改的主资源位置的域。
3. 单击 **更改主资源位置**，然后选择要使用的资源位置。
4. 单击 **保存**。

重置主资源位置

重置主资源位置允许您从资源位置中删除“主”指定，而无需选择其他资源位置。当您删除“主”指定时，域中的任何 Cloud Connector 都可以处理用户登录操作。因此，某些用户可能会遇到登录速度变慢的情况。

1. 在 Citrix Cloud 管理控制台中，单击菜单按钮并选择 **身份和访问管理**。
2. 选择 **域**，然后展开包含要更改的主资源位置的域。
3. 选择 **更改主资源位置**，然后选择 **重置**。将出现一条通知，警告您登录性能可能会受到影响。
4. 选择 **我了解对最终用户的潜在影响**，然后单击 **确认重置**。

适用于云服务的连接器设备

连接器设备是托管在您的虚拟机管理程序或云提供商中的 Citrix 组件。它充当 Citrix Cloud™ 与您的资源位置之间的通信通道，无需任何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。

注意：

连接器设备不能用于 VDA 注册、Storefront XML 流量、Netscaler STA 流量、MCS 的虚拟机管理程序管理或与 DaaS 资源相关的任何其他用例。对于这些用例，请使用 Cloud Connector。

连接器设备功能

- **将 Active Directory 连接到 Citrix Cloud** 可实现 AD 管理，允许在您的资源位置中使用 AD 林和域。它消除了添加任何额外 AD 信任的需要。与 Cloud Connector 不同，单个连接器设备可用于为多个 Active Directory 域提供连接。有关详细信息，请参阅 使用连接器设备的 Active Directory。

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

- **映像可移植性服务** 简化了跨平台映像的管理。此功能对于管理本地资源位置与公有云中的资源位置之间的映像非常有用。Citrix Virtual Apps and Desktops™ REST API 可用于自动执行 Citrix Virtual Apps and Desktops 站点中资源的管理。

  映像可移植性工作流在您使用 Citrix Cloud 启动将映像从本地位置迁移到公有云订阅时开始。准备好映像后，映像可移植性服务可帮助您将映像传输到公有云订阅并准备运行。最后，Citrix Provisioning 或 Machine Creation Services™ 在您的公有云订阅中预配映像。

  有关详细信息，请参阅 映像可移植性服务。

- **Citrix Secure Private Access** 使管理员能够提供一种内聚的体验，将单点登录、远程访问和内容检查集成到一个解决方案中，以实现端到端访问控制。有关详细信息，请参阅 使用连接器设备的 Secure Private Access。

可能还有其他预览版服务也依赖于连接器设备。

连接器设备平台是 Citrix Cloud Platform 和 Citrix Identity Platform 的一部分，可以处理数据，包括以下信息：

- IP 地址或 FQDN
- 设备、用户和资源位置标识符
- 时间戳
- 事件数据
- 来自 Active Directory 的用户和组详细信息（例如，用于身份验证和搜索用户和组）

Connector Appliance 处理的特定信息详细信息可在 Citrix Cloud Services Data Protection Overview 中的 *Data Collected by Citrix Cloud Platform* 表中找到。

Connector Appliance 可用性和负载管理

为了实现持续可用性和管理负载，请在每个资源位置安装多个 Connector Appliance。Citrix 建议在每个资源位置至少安装两个 Connector Appliance。如果一个 Connector Appliance 在任何时候不可用，其他 Connector Appliance 可以保持连接。由于每个 Connector Appliance 都是无状态的，因此负载可以分布到所有可用的 Connector Appliance 上。无需配置此负载平衡功能。它是自动化的。如果至少有一个 Connector Appliance 可用，则与 Citrix Cloud 的通信不会中断。

如果您的资源位置只配置了一个连接器，Citrix Cloud 会在**资源位置**页面上显示警告。

连接器设备 更新

Connector Appliance 会自动更新。您无需执行任何操作来更新连接器。

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

您可以将资源位置配置为在更新可用时立即应用更新，或者在预定时间之后应用更新。

有关配置更新的详细信息，请参阅 连接器更新

作为更新的一部分，Connector Appliance 会暂时不可用。更新一次只应用于租户中的一个 Connector Appliance。因此，请在每个资源位置注册至少两个 Connector Appliance，以确保始终至少有一个 Connector Appliance 可用。

连接器设备 通信

Connector Appliance 对 Citrix Cloud 与您的资源位置之间的所有通信进行身份验证和加密。安装后，Connector Appliance 通过出站连接启动与 Citrix Cloud 的通信。所有连接都使用标准 HTTPS 端口 (443) 和 TCP 协议从 Connector Appliance 建立到云。不允许任何入站连接。

下表列出了 Connector Appliance 需要访问的端口：

服务	端口	支持的域协议	配置详细信息
DNS	53	TCP/UDP	此端口必须对本地设置开放
NTP	123	UDP	此端口必须对本地设置开放
HTTPS	443	TCP	连接器设备需要对此端口进行出站访问

要配置 Connector Appliance，IT 管理员必须能够通过 Connector Appliance 的 443 端口 (HTTPS) 访问管理界面。

注意：

要访问管理界面，您必须在 IP 地址的开头包含 `https://` 。

Connector Appliance 可以与资源位置中的本地系统以及外部系统进行通信。如果您在 Connector Appliance 管理界面上定义了一个或多个 Web 代理，则只有从 Connector Appliance 到外部系统的流量会通过此 Web 代理路由。如果您的本地系统位于专用地址空间中，则从 Connector Appliance 到此系统的流量不会通过 Web 代理路由。

Connector Appliance 将以下 IPv4 地址范围定义为专用地址空间：

- 10.0.0.0 – 10.255.255.255

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

- 172.16.0.0 – 172.31.255.255
- 192.168.0.0 – 192.168.255.255

Internet 连接要求

从数据中心连接到 Internet 需要打开 443 端口以进行出站连接。但是，要在包含 Internet 代理服务器或防火墙限制的环境中运行，可能需要进一步配置。

为了正常运行和使用 Citrix Cloud 服务，必须能够通过未修改的 HTTPS 连接访问以下地址：

- `https://*.cloud.com`
- `https://*.citrixworkspacesapi.net`
- `https://*.citrixnetworkapi.net`
- `https://*.nssvc.net`
  - 无法启用所有子域的客户可以使用以下地址：
    - `https://*.g.nssvc.net`
    - `https://*.c.nssvc.net`
- `https://*.servicebus.windows.net`
- `https://ctxccopspacrconnappprod.azurecr.io`
- `https://ctxccopspacrconnappprod.eastus.data.azurecr.io`

网络要求

确保您的环境具有以下配置：

- 网络允许 Connector Appliance 使用 DHCP 获取 DNS 和 NTP 服务器、IP 地址、主机名和域名，或者您可以在 Connector Appliance 控制台 中手动设置网络设置。
- 网络未配置为使用链路本地 IP 范围 169.254.0.1/24、169.254.64.0/18 或 169.254.192.0/18，这些范围由 Connector Appliance 内部使用。
- 虚拟机管理程序时钟设置为协调世界时 (UTC) 并与时间服务器同步，或者 DHCP 向 Connector Appliance 提供 NTP 服务器信息。
- 如果您将代理与 Connector Appliance 结合使用，则该代理必须未经身份验证或使用基本身份验证。

系统要求

Connector Appliance 支持以下虚拟机管理程序：

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

- VMware ESXi 版本 7 更新 2
- VMware ESXi 版本 8
- 在 Windows Server 2016、Windows Server 2019、Windows Server 2022 或 Windows Server 2025 上运行的 Hyper-V。
- Nutanix AHV
- 微软 Azure
- AWS
- 谷歌云平台
- XenServer® 8.4
- XenServer® 9

您的管理程序必须提供以下最低功能：

- 20 GB 根磁盘
- 2 个 vCPU
- 4 GB 内存
- 一个 IPv4 网络

您可以在同一管理程序主机上托管多个 Connector Appliance。同一主机上的 Connector Appliance 数量仅受管理程序和硬件限制。

注意：

克隆、暂停和拍摄 Connector Appliance VM 的快照不受支持。

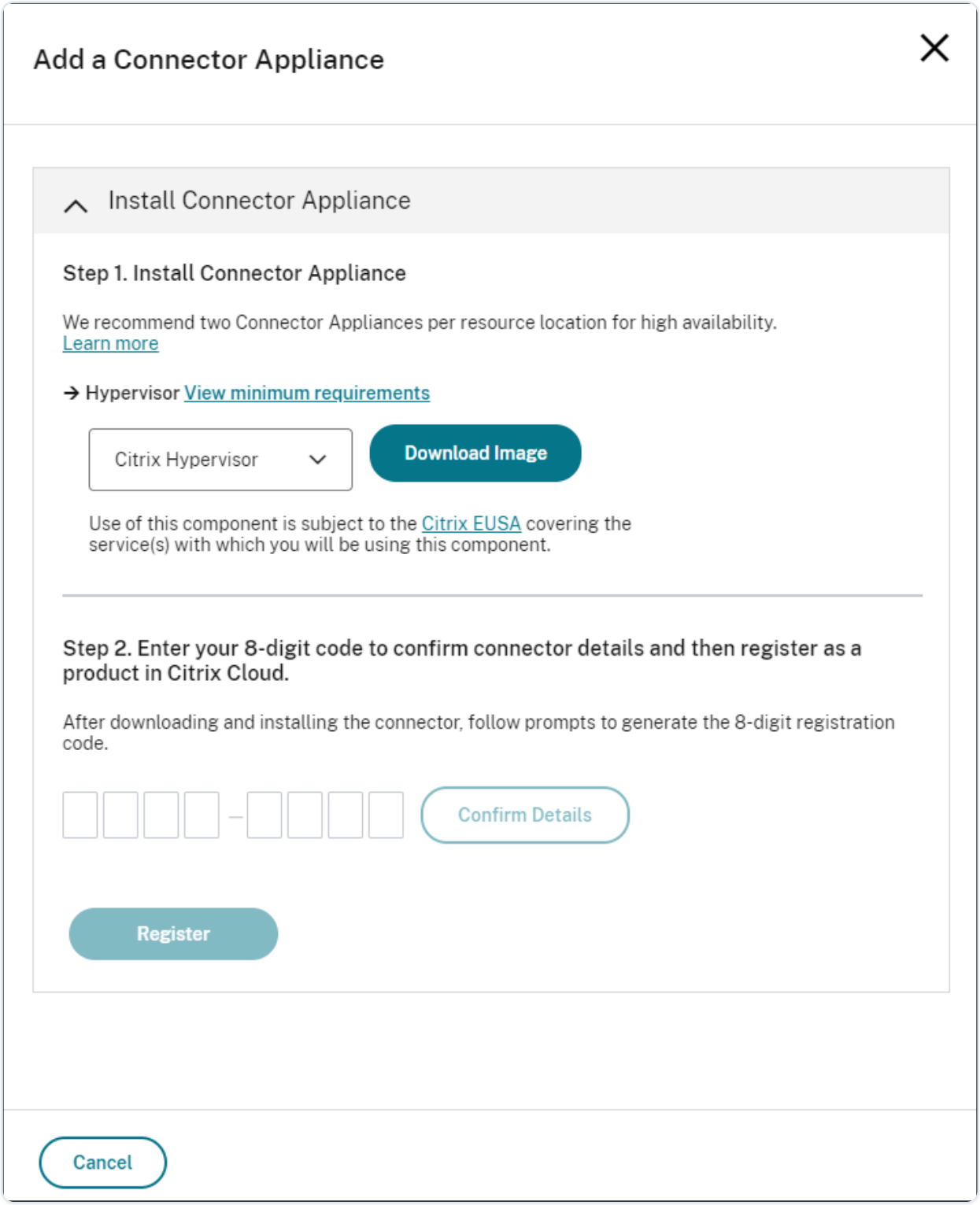
获取连接器设备

从 Citrix Cloud 中下载 Connector Appliance 软件。

1. 登录 Citrix Cloud。
2. 从屏幕左上角的菜单中，选择 **资源位置**。
3. 如果您还没有资源位置，请单击加号图标 (+) 或选择 **添加资源位置**。有关详细信息，请参阅 创建资源位置。
4. 在要注册 Connector Appliance 的资源位置中，单击 **Connector Appliances** 加号图标 (+)。

   添加 Connector Appliance 任务打开。

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



5. 在 **步骤 1** 中的 **管理程序** 列表中，选择用于托管 Connector Appliance 的管理程序或云提供商类型。

   - 对于本地管理程序和云环境，您可以在 Citrix Cloud 中下载 Connector Appliance：

     a. 单击 **下载映像**。

     b. 查看 Citrix 最终用户服务协议，如果您同意，请选择 **同意并继续**。

     c. 出现提示时，保存提供的 Connector Appliance 文件。

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

Connector Appliance 文件的文件扩展名取决于您选择的管理程序。

- 对于某些云环境，您可以从市场获取 Connector Appliance：
  - AWS
  - 微软 Azure
  - 谷歌云

6. 保持“**安装 Connector Appliance**”任务处于打开状态。安装 Connector Appliance 后，将注册码输入到“**步骤 2**”中。

您也可以从“**连接器**”页面访问“**安装 Connector Appliance**”任务。选择加号图标 (+) 以添加连接器，然后选择添加 Connector Appliance。

在您的虚拟机管理程序上安装 Connector Appliance

- XenServer™
- 威睿 ESXi
- 海珀-V
- 努坦尼克斯 AHV
- 微软 Azure
- 谷歌云平台
- AWS

XenServer

本节介绍如何使用 XenCenter 将 Connector Appliance 导入到 XenServer 主机。

1. 在可以访问已下载的 Connector Appliance XVA 文件的系统上，使用 XenCenter 连接到您的 XenServer 主机或池。
2. 选择 **文件** > **导入**。
3. 指定或浏览到 Connector Appliance XVA 文件所在的路径。单击 **下一步**。
4. 选择要托管 Connector Appliance 的 XenServer 主机。或者，您可以选择要托管 Connector Appliance 的池，XenServer 将选择一个合适的可用服务器。单击 **下一步**。
5. 指定用于 Connector Appliance 的存储库。单击 **导入**。
6. 单击 **添加** 以添加虚拟网络接口。从 **网络** 列表中，选择 Connector Appliance 要使用的网络。单击 **下一步**。

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

7. 查看用于部署 Connector Appliance 的选项。如果任何选项不正确，请使用 **上一步** 更改这些选项。
8. 确保选中 **导入完成后自动启动新虚拟机**。单击 **完成**。

Connector Appliance 部署并成功启动后，其控制台会显示一个包含 Connector Appliance IP 地址的登录页面。使用此 IP 地址连接到 Connector Appliance 管理页面并完成注册过程。

默认情况下，Connector Appliance 使用 DHCP 设置其网络配置。如果您的环境中没有 DHCP，则必须在 Connector Appliance 控制台上设置网络配置，然后才能访问 Connector Appliance 管理控制台。有关详细信息，请参阅 使用 Connector Appliance 控制台设置网络配置。

下一步：将您的 Connector Appliance 注册到 Citrix Cloud。

威睿 ESXi

本节介绍如何使用 VMware vSphere Client 在 VMware ESXi 主机上部署 Connector Appliance。

1. 在可以访问已下载的 Connector Appliance OVA 文件的系统上，使用 vSphere Client 连接到您的 ESXi 主机。
2. 选择 **文件** > **部署 OVF 模板...**。
3. 指定或浏览到 Connector Appliance OVA 文件所在的路径。单击 **下一步**。
4. 查看模板详细信息。单击 **下一步**。
5. 您可以为 Connector Appliance 实例指定一个唯一的名称。默认情况下，名称设置为 **Connector Appliance**。请确保选择一个能够将此 Connector Appliance 实例与此 ESXi 主机上托管的其他实例区分开来的名称。单击 **下一步**。
6. 指定 Connector Appliance 的目标存储。单击 **下一步**。
7. 选择存储虚拟磁盘的格式。单击 **下一步**。
8. 查看用于部署 Connector Appliance 的选项。如果任何选项不正确，请使用 **返回** 更改这些选项。
9. 选择 **部署后开机**。单击 **完成**。

Connector Appliance 部署并成功启动后，其控制台会显示一个包含 Connector Appliance IP 地址的登录页面。使用此 IP 地址连接到 Connector Appliance 管理页面并完成注册过程。

默认情况下，Connector Appliance 使用 DHCP 设置其网络配置。如果您的环境中没有 DHCP，则必须在 Connector Appliance 控制台上设置网络配置，然后才能访问 Connector Appliance UI。有关详细信息，请参阅使用 Connector Appliance 控制台设置网络配置。

下一步：将您的 Connector Appliance 注册到 Citrix Cloud。

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

海伯-V

本节介绍如何在 Hyper-V 主机上部署 Connector Appliance。您可以使用 Hyper-V 管理器或使用随附的 PowerShell 脚本部署 VM。

使用 Hyper-V 管理器部署 Connector Appliance

1. 连接到您的 Hyper-V 主机。
2. 将 Connector Appliance ZIP 文件复制或下载到 Hyper-V 主机。
3. 解压 ZIP 文件的内容。ZIP 文件包含一个 PowerShell 脚本和 connector-appliance.vhdx 文件。
4. 将 VHDX 文件复制到您希望存储 VM 磁盘的位置。例如，`C:\ConnectorApplianceVMs`。
5. 打开 Hyper-V 管理器。
6. 右键单击您的服务器名称，然后选择 **新建 > 虚拟机**。
7. 在**新建虚拟机向导**的**指定名称和位置**面板上，输入一个唯一名称以标识您的 Connector Appliance。单击**下一步**。
8. 在**指定代数**面板上，选择**第 1 代**。单击**下一步**。
9. 在**分配内存**面板上，配置以下设置，然后单击**下一步**：
   a. 分配 4 GB RAM。
   b. 禁用动态内存。
10. 在**配置网络**面板上，从列表中选择一个交换机（例如，默认交换机）。单击**下一步**。
11. 在**连接虚拟硬盘**面板上，选择**使用现有虚拟硬盘**。
12. 浏览到 connector-appliance.vhdx 文件的位置并选择它。单击**下一步**。
13. 在**摘要**面板上，查看您选择的值，然后单击**完成**以创建 VM。
14. 在**虚拟机**面板上，右键单击 Connector Appliance VM 并选择**设置**。
15. 在“**设置**”窗口中，选择“**硬件 > 处理器**”，然后执行以下操作：
    a. 在“**虚拟处理器数量**”中，将值更改为 **2**。
    b. 单击“**应用**”。
    c. 单击“**确定**”。
16. 在“**虚拟机**”面板上，右键单击 Connector Appliance VM，然后选择“**启动**”。
17. 右键单击 Connector Appliance VM，然后选择“**连接**”以打开控制台。

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

Connector Appliance 部署并成功启动后，使用 Hyper-V 管理器连接到控制台。控制台会显示一个包含 Connector Appliance IP 地址的登录页面。使用此 IP 地址连接到 Connector Appliance 管理页面并完成注册过程。

默认情况下，Connector Appliance 使用 DHCP 设置其网络配置。如果您的环境中没有可用的 DHCP，您必须在 Connector Appliance 控制台中设置网络配置，然后才能访问 Connector Appliance UI。有关详细信息，请参阅使用 Connector Appliance 控制台设置网络配置。

下一步：将 Connector Appliance 注册到 Citrix Cloud。

使用 PowerShell 脚本部署 Connector Appliance

connector-appliance.zip 文件包含一个 PowerShell 脚本，用于创建和启动新的 VM。

注意：

要运行此未签名的 PowerShell 脚本，您可能需要更改 Hyper-V 系统上的执行策略。有关详细信息，请参阅 `<https://go.microsoft.com/fwlink/?LinkID=135170>`。或者，您可以使用提供的脚本作为基础来创建或修改自己的本地脚本。

1. 连接到您的 Hyper-V 主机。
2. 将 Connector Appliance ZIP 文件复制或下载到 Hyper-V 主机。
3. 提取 ZIP 文件的内容：一个 PowerShell 脚本和一个 VHDX 文件。
4. 在 PowerShell 控制台中，将当前目录更改为 ZIP 文件内容所在的目录，然后运行以下命令：

```
.\connector-appliance-install.ps1
```

5. 出现提示时，键入 VM 的名称，或选择 **Enter** 接受默认值 **Connector Appliance**。
6. 出现提示时，键入根磁盘的目标位置，或按 Enter 键使用 VHD 的系统默认目录。
7. 出现提示时，键入根磁盘的文件名，或选择 **Enter** 接受默认值 connector-appliance.vhdx。
8. 出现提示时，选择要使用的交换机。选择 **Enter**。
9. 查看 VM 导入信息的摘要。如果信息正确，请选择 **Enter** 继续。脚本将创建并启动 Connector Appliance VM。

Connector Appliance 部署并成功启动后，其控制台会显示一个包含 Connector Appliance IP 地址的登录页面。使用此 IP 地址连接到 Connector Appliance 并完成注册过程。

下一步：向 Citrix Cloud 注册您的 Connector Appliance。

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

诺坦尼克斯 AHV

本节介绍如何使用 Nutanix Prism Web 控制台将 Connector Appliance 从 `connector-appliance.vhdx` 文件部署到 Nutanix AHV 主机。

1. 在 Nutanix Prism Web 控制台的主菜单上，选择“**存储**”视图。
2. 单击“**+ 存储容器**”以创建存储容器来保存 Connector Appliance 映像文件。或者，您可以使用现有存储容器。
3. 将 `connector-appliance.vhdx` 文件上传到您的存储容器。
   a. 在 Web 控制台的主菜单上，选择“**设置**”。
   b. 选择**映像配置**选项卡，然后单击**+ 上传映像**
   c. 在**创建映像**中，为您的映像指定一个**名称**。
   d. 从**映像类型**列表中，选择**DISK**。
   e. 从**存储容器**列表中，选择您创建的存储容器。
   f. 选择**上传文件**。
   g. 单击**选择文件**，然后导航到本地系统上的 `connector-appliance.vhdx` 文件。
   h. 单击**保存**。
4. 等待映像创建完成，并且其状态在**映像配置**页面中显示为**ACTIVE**。
5. 选择**网络配置**选项卡。
6. 单击**+ 创建网络**，为 Connector Appliance 创建一个网络以供使用。
7. 在**创建网络**页面中，指定以下信息：
   - 网络名称。
   - 网络 VLAN ID。
8. 在 Web 控制台的主菜单上，选择**VM**视图。
9. 单击**+ 创建 VM**，以创建 Connector Appliance 实例。
10. 在 **创建 VM** 中，指定以下信息：
    - VM 名称
    - vCPU 数量
    - 以 GiB 为单位的内存量
11. 选择使用 **Legacy BIOS**。

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

12. 单击 **+ 添加新磁盘** 以将磁盘添加到 VM。
13. 在 **添加磁盘** 中，填写以下信息：
    a. 对于 **类型**，选择 **DISK**。
    b. 对于 **操作**，选择 **从映像服务克隆**。
    c. 对于 **总线类型**，选择 **SCSI**
    d. 对于 **映像**，选择您上传 Connector Appliance 文件时创建的映像。
14. 单击 **添加** 以完成磁盘添加。
15. 在 **创建 VM** 中，单击 **+ 添加新网卡**。
16. 在 **创建网卡** 中，选择要将 VM 添加到的网络。
17. 对于 **网络连接状态**，选择 **已连接**。
18. 单击**添加**以完成添加 NIC。
19. 单击**保存**以创建 VM。

    默认情况下，新 VM 已关闭电源。
20. 在**VM**视图中，选择 VM 并单击**开机**。
21. 等待 VM 启动。此过程可能需要几分钟。

部署并成功启动 Connector Appliance 后，您可以在以下位置之一找到 Connector Appliance IP 地址：

- 在 Nutanix Prism Web 控制台的**VM**视图中。
- 在 Connector Appliance 控制台中。

使用此 IP 地址连接到 Connector Appliance 管理页面并完成注册过程。

下一步：将您的 Connector Appliance 注册到 Citrix Cloud。

微软 Azure

本节介绍如何在 Microsoft Azure 中部署 Connector Appliance。您可以从 Azure Marketplace 或通过使用随附的 PowerShell 脚本从下载的磁盘映像部署 Connector Appliance。

从 Azure Marketplace 部署连接器设备

要从 Azure Marketplace 部署 Connector Appliance，请完成以下步骤：

1. 前往 Azure 市场中的连接器设备。(Azure 市场)

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

此外，您可以在市场搜索中搜索“Connector Appliance for Cloud Services”。

2. 单击**立即获取**，然后单击**创建**。
3. 在**创建 Citrix Connector™ Appliance for Cloud Services** 页面上，填写以下信息：
   - 选择要使用的**订阅**。
   - 选择要使用的**资源组**。
   - 选择 Connector Appliance 所在的**区域**。
   - 指定一个 **VM 名称**。
   - 选择一个**虚拟网络**以添加 Connector Appliance。此网络用于访问 Citrix Cloud、本地资源和 Connector Appliance 管理页面。此网络以后无法更改。
   - 为**子网**指定一个值。

   单击**下一步：标记 >**。
4. 在**标记**选项卡上，如果需要，添加所需的标记。

   单击**下一步：审核 + 创建 >**。
5. 审核部署详细信息后，单击**创建**。

Connector Appliance 部署并成功启动后，其控制台会显示一个包含 Connector Appliance IP 地址的登录页面。使用此 IP 地址连接到 Connector Appliance 管理页面并完成注册过程。

下一步：将您的 Connector Appliance 注册到 Citrix Cloud。

使用 PowerShell 脚本部署 Connector Appliance VM

`connector-appliance-azure.zip` 文件包含一个 PowerShell 脚本，用于创建和启动新的 VM。您可以使用提供的脚本作为基础来创建或修改您自己的本地脚本。

在运行脚本之前，请确保您具备以下先决条件：

- 将 Az PowerShell 模块安装到您的本地 PowerShell 环境中。
- 在 VHD 文件所在的目录中运行 PowerShell 脚本。

完成以下步骤：

1. 将 Connector Appliance ZIP 文件复制或下载到您的 Windows 系统。
2. 解压 ZIP 文件的内容：一个 PowerShell 脚本和一个 VHD 文件。
3. 以管理员身份打开 PowerShell 控制台。
4. 将当前目录更改为 ZIP 文件内容所在的目录，然后运行以下命令：

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

```
.\connector-appliance-upload-Azure.ps1
```

5. 将出现一个对话框，提示您登录 Microsoft Azure。输入您的凭据。
6. 当 PowerShell 脚本提示时，选择要使用的订阅。按 Enter。
7. 按照脚本中的提示操作，这些提示将指导您上传映像并创建虚拟机。
8. 创建第一个 VM 后，脚本会询问您是否要从上传的映像创建另一个 VM。
   - 键入 `y` 以创建另一个 VM。
   - 输入 `n` 退出脚本。

Connector Appliance 部署并成功启动后，其控制台会显示一个包含 Connector Appliance IP 地址的登录页面。使用此 IP 地址连接到 Connector Appliance 管理页面并完成注册过程。

下一步：将您的 Connector Appliance 注册到 Citrix Cloud。

AWS

本节介绍如何在 AWS 中部署 Connector Appliance。Connector Appliance 在 AWS Marketplace 中以 AMI 形式提供，我们建议您从 AMI 安装 Connector Appliance。或者，您可以使用 AWS UI 或随附的 PowerShell 脚本部署下载的磁盘映像。

网络先决条件

要在 AWS 上部署 Connector Appliance，请确保您可以从创建 Connector Appliance 的子网访问 Citrix Cloud。

我们建议为设备使用私有 IP 地址，这需要特定的配置才能提供对 Citrix Cloud 的访问。要实现此配置，请在 **AWSManagement Console** 中完成以下步骤：

1. 创建 NAT 网关。
   a. 在顶部导航栏中，选择 **Services > VPC > NAT Gateways**。
   b. 在右上角，单击 **Create NAT Gateway**。输入以下信息：
      - 输入 **Name**。
      - 从列表中选择 **subnet**。
      - 将 **Connectivity type** 设置为 **Public**。
      - 从列表中选择一个 **Elastic IP allocation ID**。如果没有可用的弹性 IP，请单击 **Allocate Elastic IP** 并按照说明创建一个。

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

   c. 单击**创建 NAT 网关**。

2. 创建包含 NAT 网关的路由表条目。

   a. 在顶部导航栏中，选择**服务 > VPC > 路由表**。
   b. 在右上角，单击**创建路由表**。输入以下信息：

      - 输入**名称**。
      - 从列表中，选择包含您在创建 NAT 网关时所选子网的 VPC。

   c. 单击**创建路由表**。
   d. 在您创建的路由表的**路由**选项卡中，单击**编辑路由 > 添加路由**。
   e. 输入新路由条目的**目标**和**靶标**。

      - 将目标设置为 0.0.0.0/0。
      - 对于靶标，从列表中选择您创建的**NAT 网关**。

   f. 单击**保存更改**。

3. 将用于 Connector Appliance 的子网附加到此路由表。

   a. 在顶部导航栏中，**选择服务 > VPC > 路由表**。
   b. 选择包含 NAT 网关的路由表。
   c. 在显示页面中，转到“**子网关联**”选项卡。
   d. 单击“**编辑子网关联**”。
   e. 选择要附加到路由表的子网或多个子网。
   f. 单击“**保存关联**”。

从 AWS Marketplace 部署连接器设备

开始之前，请确保满足以下先决条件：

- 您拥有操作 EC2 资源的权限。
- 您已完成 (#networking-prerequisites) 中的配置。
- （可选）您可以创建一个安全组，限制允许哪些 IP 地址访问您的 Connector Appliance。

完成以下步骤：

1. 登录到 **AWS 管理控制台**。
2. 在 AWS Marketplace 中查找 Connector Appliance AMI。您可以通过以下任一方式执行此操作：

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

- 按照 Citrix Cloud 中提供的 Marketplace 链接操作。 (AWS Marketplace)
- 在 AWS 管理控制台中搜索 AMI：

  a. 转到“**服务 > 计算 > EC2 > AMI**”

  b. 确保您位于美国东部（俄亥俄州）区域。

  c. 在 **公共映像** 中，搜索“Citrix Connector Appliance”或 AMI ID“ami-026eaf9b3b232577f”。

3. 通过检查 AMI ID (ami-026eaf9b3b232577f) 和所有者 ID (414337923189) 来验证您是否拥有正确的 AMI。
4. 将 AMI 复制到您的订阅：

   a. 转到 **操作 > 复制 AMI**。

   b. 在 **复制 AMI** 对话框中，您可以选择所需的 **目标区域**。

   c. 单击 **复制 AMI**

5. 在您复制的 AMI 摘要页面中，单击 **从 AMI 启动实例**。
6. 在 **启动实例** 对话框中，完成以下步骤：

   a. 选择要创建的实例数量。为了实现弹性，我们建议您在每个资源位置部署两个或更多 Connector Appliance。

   b. 为实例指定名称。

   c. 对于 **实例类型**，选择 **t2.medium**。实例类型必须至少具有 4 GB 内存和 2 个 CPU。

   d. 对于 **密钥对（登录）**，选择 **不使用密钥对继续**。不允许通过 SSH 登录 Connector Appliance，因此不需要密钥对。

   e. 对于 **网络设置**，在 **防火墙（安全组）** 部分中，配置以下设置：

      i. 选择是 **创建安全组** 还是 **选择现有安全组**。

      ii. 取消选择 **允许来自互联网的 SSH 流量**

      iii. 选择 **允许来自互联网的 HTTPS 流量**

      iv. 选择 **允许来自互联网的 HTTP 流量**

   单击 **启动实例**。

7. 实例创建后，在**成功**部分中，单击实例 ID 链接以查看您的 Connector Appliance 实例。

   或者，您可以单击此页面上的**查看所有实例**按钮，或转到 AWS 管理控制台中的**服务 > EC2 > 实例**以查看您的实例列表。

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

8. 当您的**实例状态**变为**正在运行**时，进入实例详细信息并使用**私有 IPv4 地址**连接到 Connector Appliance 管理页面并完成注册过程。

您可能需要使用堡垒主机从浏览器访问内部 IP 地址处的 Connector Appliance 管理页面并完成注册过程。

默认情况下，Connector Appliance 使用 DHCP 设置其网络配置。您可以使用 Connector Appliance Web 界面编辑此网络配置。有关详细信息，请参阅在 Connector Appliance 管理页面上配置网络设置。

下一步：向 Citrix Cloud 注册您的 Connector Appliance。

使用 AWS UI 部署 Connector Appliance

开始之前，请确保满足以下先决条件：

- 您拥有操作 S3 和 EC2 资源的权限。
- 您已创建具有 VM 导入访问权限的服务角色和策略。有关详细信息，请参阅 `<https://docs.aws.amazon.com/vm-import/latest/userguide/required-permissions.html#vmimport-role>`。

  > **注意：**
  >
  > 要创建服务角色，您必须创建一个 S3 存储桶。创建策略时，请将您创建的 S3 存储桶设置为具有 VM 导入访问权限。

- 您有权访问 AWS CloudShell。它仅在某些区域可用。有关支持 AWS CloudShell 的区域列表，请参阅 `<https://docs.aws.amazon.com/cloudshell/latest/userguide/supported-aws-regions.html>`。
- 您已完成 网络先决条件 中的配置。

完成以下步骤：

1. 在本地系统上，提取 `connector-appliance-aws.zip` 的内容。
2. 登录到 **AWS 管理控制台**。
3. 通过完成以下步骤创建存储桶。（或者，您可以跳过这些步骤并使用现有存储桶。）

   a. 在顶部导航栏中，选择 **服务** > **S3** > **创建存储桶**。

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

b. 为您的存储桶输入一个唯一的名称。有关 Amazon S3 中存储桶的命名约定，请参阅 `<https://docs.aws.amazon.com/AmazonS3/latest/userguide/bucketnamingrules.html>`。

c. 选择存储桶的区域。请确保选择与您的 AWS 区域相同的区域，因为如果这些区域不同，您将无法使用存储桶中的文件。

d. 保持其余设置不变，然后单击 **创建存储桶**。

4. 单击您已创建的存储桶的名称。单击 **上传** > **添加文件**，然后选择 `connector-appliance.vhd` 文件。保持其余设置不变，然后单击 **上传**。
5. 单击您上传的文件。单击 **复制 S3 URI**。
6. 单击顶部导航栏中的 **AWS CloudShell 图标** 并运行以下命令：

   a. 创建任务以将 VHD 文件转换为快照：

   ```
   aws ec2 import-snapshot --disk-container
   Format=VHD,Url="&lt;S3_URI>"
   ```

   将占位符值替换为您从上一步复制的 S3 URI。例如，`aws ec2 import-snapshot --disk-container Format=VHD,Url="s3://my-aws-bucket/connector-appliance.vhd"`。

   当以下命令返回包含 `"Status": "completed"` 的 JSON 字符串时，此命令完成。记下 JSON 输出中的 `ImportTaskId` 值。

   b. 运行以下命令：

   ```
   aws ec2 describe-import-snapshot-tasks --import-task-ids
   &lt;ImportTaskId>
   ```

   将占位符值替换为您从上一步复制的 `ImportTaskId`。例如，`aws ec2 describe-import-snapshot-tasks --import-task-ids import-snap-0273h2836153itg5`。

7. 在 **AWSManagement Console** 的顶部导航栏中，选择 **Services** > **EC2**。
8. 在屏幕左侧的菜单中，单击 **Snapshots**。
9. 右键单击您创建的快照，然后单击 **Create Image**。
10. 在打开的窗格中，完成以下步骤：

    a. 输入您的 AMI 名称。

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

   b. 选择 **硬件辅助虚拟化**。

   单击 **Create**。

11. 在屏幕左侧的菜单中，单击 **AMIs**。
12. 右键单击您创建的 AMI，然后单击 **Launch**。
13. 在打开的窗格中，完成以下步骤：

   a. 选择实例类型。
   b. (可选) 在**配置实例**选项卡上自定义网络。
   c. (可选) 在**添加存储**选项卡上附加另一个卷。
   d. 在**配置安全组**选项卡上设置安全组规则。

   查看实例启动后，单击**审核并启动**。

部署并成功启动 Connector Appliance 后，转到**服务** > **EC2** > **实例**，然后选择您创建的实例。使用**私有 IPv4 地址**连接到 Connector Appliance 管理页面并完成注册过程。您可能需要使用堡垒主机从浏览器访问内部 IP 地址处的 Connector Appliance 管理页面，以继续安装过程。

默认情况下，Connector Appliance 使用 DHCP 设置其网络配置。您可以使用 Connector Appliance Web 界面编辑此网络配置。有关详细信息，请参阅在 Connector Appliance 管理页面上配置网络设置。

下一步：将您的 Connector Appliance 注册到 Citrix Cloud。

使用 PowerShell 脚本部署 Connector Appliance

`connector-appliance-aws.zip` 文件包含一个 PowerShell 脚本，用于创建和启动新的 VM。在运行脚本之前，请确保您满足以下先决条件：

- 您的系统上已安装 AWS.Tools、AWSPowerShell.NetCore 或 AWSPowerShell。有关详细信息，请参阅 `<https://docs.aws.amazon.com/powershell/latest/userguide/pstools-getting-set-up.html>`。
- 您已创建具有 VM 导入访问权限的服务角色和策略。为了使此 PowerShell 脚本正常工作，服务角色和策略都必须命名为 `vmimport`。有关详细信息，请参阅 `<https://docs.aws.amazon.com/vm-import/latest/userguide/required-permissions.html#vmimport-role>`。

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

> **注意：**
>
> 要创建服务角色，您必须创建一个 S3 存储桶。创建策略时，请将您创建的 S3 存储桶设置为具有 VM 导入访问权限。

- 您已创建 Amazon EC2 安全组。
- 您具有 S3 权限和 API 访问权限。
- 您已完成 (#networking-prerequisites) 中的配置。

完成以下步骤：

1. 在本地系统上，将 `connector-appliance-aws.zip` 的内容提取到一个文件夹中。
2. 在 PowerShell 中，运行以下命令：

   a. 要在本地环境中运行 AWS cmdlet，请运行以下命令将新配置文件添加到 AWS SDK 存储中：

   ```
   Set-AWSCredential -AccessKey &lt;access_key_ID> -SecretKey
   &lt;secret_key> -StoreAs MyProfile
   ```

   将占位符值替换为您的访问密钥和秘密密钥。提供一个唯一的配置文件名称。在我们提供的示例中，它是 `MyProfile`。

   b. 将配置文件设置为默认值：

   ```
   Initialize-AWSDefaultConfiguration -ProfileName MyProfile
   ```

   c. 将当前目录更改为提取文件所在的文件夹，然后运行以下命令：

   ```
   .\connector-appliance-upload-aws.ps1
   ```

3. 按照脚本中的提示操作，这些提示将指导您选择 Connector Appliance 部署的区域、将映像上传到所选存储桶以及输入 VM 的名称。

   - 您必须使用之前创建的具有 VM 导入访问权限的存储桶。
   - 当要求选择要使用的 VPC 时，请选择配置了 NAT 网关和路由表的 VPC。
   - 当要求选择要使用的子网时，请选择连接到包含 NAT 网关的路由表的子网。

   有关详细信息，请参阅 (#networking-prerequisites)。

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

Connector Appliance 部署并成功启动后，脚本会显示 Connector Appliance 的私有 IP 地址。您可能需要使用堡垒主机从浏览器访问内部 IP 地址处的 Connector Appliance 管理页面，并完成注册过程。

默认情况下，Connector Appliance 使用 DHCP 设置其网络配置。您可以使用 Connector Appliance Web 界面编辑此网络配置。有关详细信息，请参阅 (#configuring-network-settings-on-the-connector-appliance-administration-page)。

下一步：将您的 Connector Appliance 注册到 Citrix Cloud(#register-your-connector-appliance-with-citrix-cloud)。

Google Cloud 平台

本节介绍如何在 Google Cloud Platform 上部署 Connector Appliance。您可以从 Google Cloud Marketplace 安装 Connector Appliance。或者，您可以使用 Google Cloud Platform Console 或随附的 PowerShell 脚本部署下载的磁盘映像。

文件 `connector-appliance-gcp.zip` 包含：

- `connector-appliance.tar.gz`，它是 Connector Appliance 的磁盘映像
- `connector-appliance-upload-gcp.ps1`，这是一个可用于自动部署 Connector Appliance 的 PowerShell 脚本

从 Google Cloud 市场部署连接器设备

1. 登录您的 Google 帐户。
2. 按照 Citrix Cloud 中提供的 Marketplace 链接操作。(Google Cloud Marketplace)

   或者，您可以在 Marketplace 搜索中搜索“适用于云服务的 Connector Appliance”。
3. 单击 **Launch**。
4. 在“**New Citrix Connector Appliance for Cloud Services deployment**”页面上，填写以下信息：

   - 为部署作业指定一个 **Deployment name**。
   - 选择用于放置 Connector Appliance 的 **Zone**。
   - 选择要使用的 **Machine family**、**Series** 和 **Machine type**。
   - 选择要使用的**启动磁盘类型**和**启动磁盘大小（GB）**。
   - 在**网络**部分，指定连接器设备要使用的网络接口。如果您希望能够从公共网络连接到管理页面，请指定一个**外部 IP**。

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

单击**部署**。您将被定向到**部署管理器**页面。

> **注意：**
>
> 连接器设备部署并成功启动后，您将收到一封电子邮件，确认连接器设备已部署在 Google Cloud Platform 上。

5. 在**部署管理器**页面上，单击实例名称。或者，您可以在**Compute Engine**中搜索您创建的连接器设备实例。
6. 如果您在为连接器设备设置网络接口时曾指定**外部 IP**，请在**详细信息**选项卡的**网络接口**部分复制**外部 IP 地址**。使用此 IP 地址连接到连接器设备管理页面并完成注册过程。或者，您可以使用**主内部 IP 地址**从与您的连接器设备位于同一子网中的另一台计算机访问连接器设备管理页面。

下一步：将您的连接器设备注册到 Citrix Cloud。

使用 Google Cloud Platform 控制台部署连接器设备

1. 在本地系统上，提取 `connector-appliance-gcp.zip` 的内容。
2. 在您的 Google Cloud Platform 项目中，创建一个存储桶。（或者，您可以使用现有的存储桶。）
   a. 从主菜单中，选择**Cloud Storage**。
   b. 在主窗格中，选择**创建存储桶**。
   c. 为您的存储桶指定一个名称。
   d. 配置所需的数据存储和访问设置。您可以将这些设置保留为默认值。
   e. 点击 **Create**。
3. 在您的存储桶中，选择 **Upload files** 并选择文件 `connector-appliance.tar.gz`。等待文件上传完成。
4. 选择已上传的文件以查看其详细信息。将 **gsutil URI** 的值复制到剪贴板。
5. 通过点击标题栏中的 **Activate Cloud Shell** 图标打开 Cloud Shell。
6. 在您的 Cloud Shell 中，运行以下命令以创建映像：

```
gcloud compute images create "Image name" --guest-os-
features=MULTI_IP_SUBNET --source-uri="gsutil URI of uploaded
connector-appliance.tar.gz file"
```

7. 从主菜单中，选择 **Compute Engine** > **VM Instances**。

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

8. 选择 **Create Instance**。在打开的窗格中，指定以下信息：
   a. 在 **Name** 字段中，为 Connector Appliance 实例指定一个名称。
   b. 选择一个区域以部署 Connector Appliance。
   c. 选择机器配置。
   d. 在 **Boot disk** 部分中，点击 **Change**。
   e. 在打开的部分中，转到 **Custom images** 选项卡。
   f. 从 **Image** 列表中，选择您创建的映像。
   g. 点击 **Select**。
   h. 在 **Firewall** 部分中，启用 HTTPS 流量以允许访问 Connector Appliance 管理页面。
   i. 指定任何所需的额外配置。例如，您可能不想使用默认的网络配置。

   单击 **创建**。
9. 在 **VM 实例** 部分中，选择您新创建的 VM 以查看其详细信息。

Connector Appliance 部署并成功启动后，**VM 实例** 部分将显示 Connector Appliance 的 IP 地址。

如果 Connector Appliance 具有外部 IP 地址，您可以使用此 IP 地址从浏览器访问 Connector Appliance 管理页面并完成注册过程。

如果 Connector Appliance 只有内部 IP 地址，请使用堡垒主机从浏览器访问 Connector Appliance 管理页面并完成注册过程。有关详细信息，请参阅 `<https://cloud.google.com/compute/docs/connect/ssh-using-bastion-host>`。

下一步：将您的 Connector Appliance 注册到 Citrix Cloud。

使用 PowerShell 脚本部署 Connector Appliance

要使用提供的 PowerShell 脚本部署 Connector Appliance，您的系统上必须安装 Google Cloud SDK。

1. 在本地系统上，将 `connector-appliance-gcp.zip` 的内容解压到一个文件夹中。
2. 在 PowerShell 中，将目录更改为解压文件所在的文件夹。
3. 运行命令 `.\connector-appliance-upload-GCP.ps1`。
4. 在打开的浏览器窗口中，使用有权访问您要部署 Connector Appliance 的项目的帐户通过 Google Cloud SDK 进行身份验证。
5. 在 Google Cloud Tools for PowerShell 中，当 PowerShell 脚本提示时，选择要使用的项目。按 Enter。

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

6. 按照脚本中的提示操作，这些提示将指导您完成上传磁盘、创建映像和创建虚拟机。
7. 创建第一个虚拟机后，脚本会询问您是否要从上传的映像创建另一个虚拟机。
    - 键入 `y` 以创建另一个虚拟机。
    - 键入 `n` 以退出脚本。

Connector Appliance 部署并成功启动后，脚本会显示 Connector Appliance 的内部 IP 地址。或者，您可以转到 Google Cloud Platform 控制台查找 Connector Appliance 内部 IP 地址。“**Compute Engine**”>“**VM Instances**”部分显示 Connector Appliance IP 地址。

使用堡垒主机从浏览器访问内部 IP 地址处的 Connector Appliance 管理页面，并完成注册过程。有关详细信息，请参阅 `<https://cloud.google.com/compute/docs/connect/ssh-using-bastion-host>`。

下一步：将您的 Connector Appliance 注册到 Citrix Cloud。

将您的 Connector Appliance 注册到 Citrix Cloud

将 Connector Appliance 注册到 Citrix Cloud，以便为 Citrix Cloud 与您的资源位置之间的通信提供通道。

在管理程序上安装并启动 Connector Appliance 后，控制台会显示 Connector Appliance 的 IP 地址。控制台还会显示一个 SSL 指纹，您可以使用该指纹验证与 Connector Appliance UI 的连接。

1. 将 Connector Appliance IP 地址复制到浏览器地址栏。

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

注意：

您可能需要在 IP 地址的开头包含 `https://`。

Connector Appliance UI 使用自签名证书，有效期为五年。因此，您可能会看到一条关于连接不安全的消息。要验证与 Connector Appliance 的连接，您可以将控制台中的 SSL 指纹与浏览器从网页接收到的指纹进行比较。

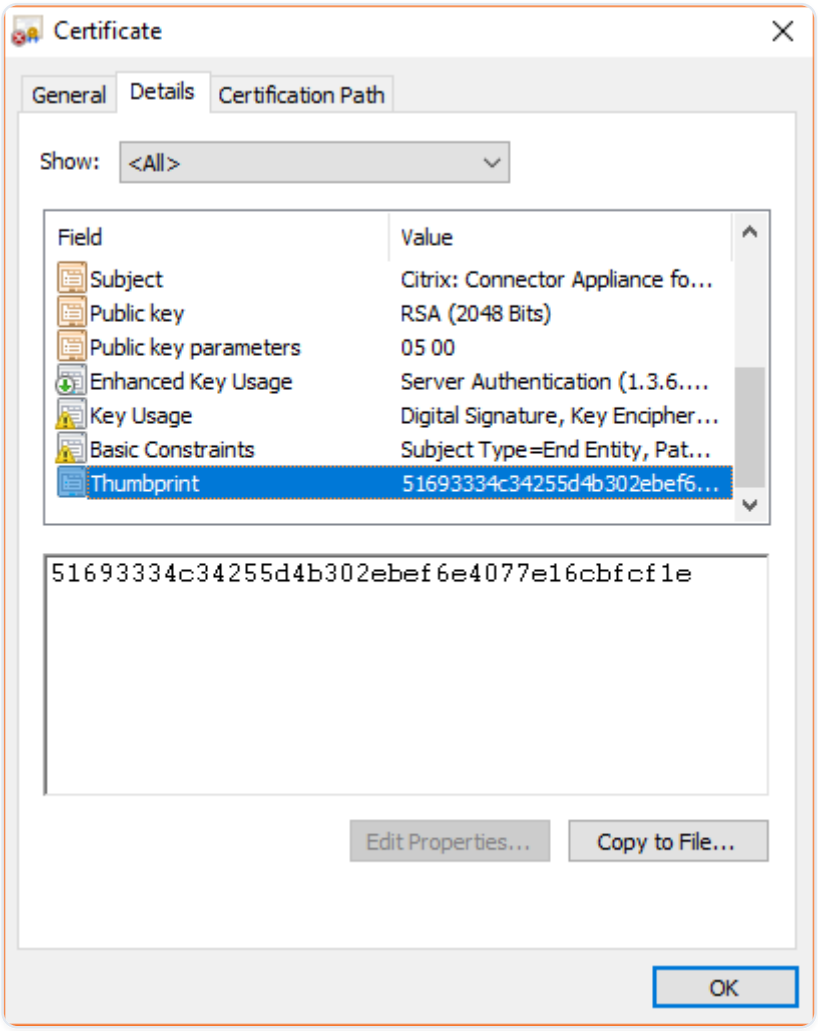
例如，在 Google Chrome 浏览器中，完成以下步骤：

a. 点击地址栏旁边的**不安全**标记。

b. 选择**证书**。**证书**窗口打开。

c. 转到**详细信息**选项卡并找到**指纹**字段。

   如果**指纹**字段的值与控制台中提供的 SSL 指纹匹配，您可以确认您的浏览器正在直接连接到 Connector Appliance UI。



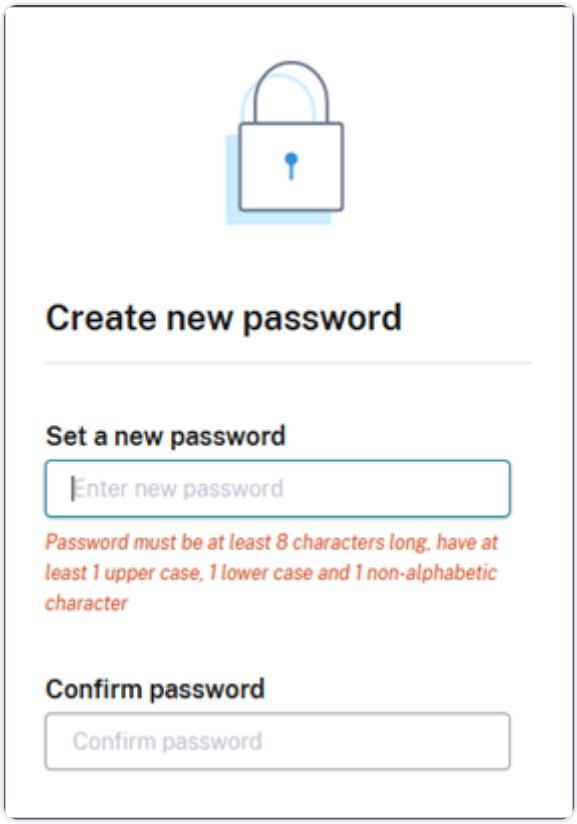
© 1997–2026 Citrix Systems, Inc. All rights reserved.

您可以将此自签名证书替换为您自己的证书，该证书由您的组织签名或使用您组织的信任链生成。有关详细信息，请参阅管理证书。

2. 如果您的浏览器需要额外步骤来确认您要继续访问该站点，请立即完成此步骤。

   创建新密码网页打开。

3. 为您的 Connector Appliance UI 创建密码，然后点击**设置密码**。



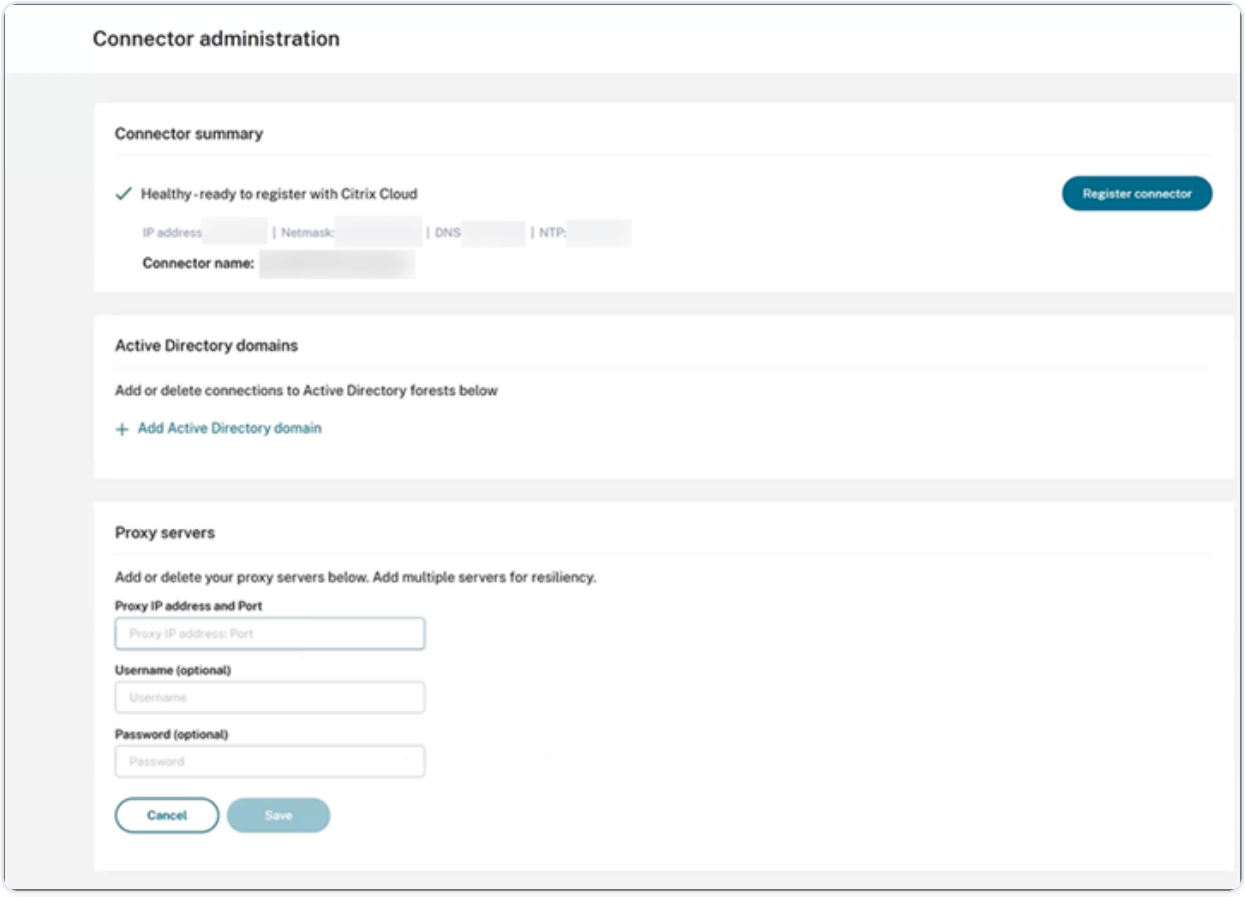
   您设置的密码必须满足以下要求：

   - 8 个或更多字符长
   - 包含大小写字母
   - 包含至少一个非字母字符

   请确保将此密码存储在安全位置以备将来使用。

4. 使用您设置的密码登录。**连接器管理**页面将打开。

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



5. (可选) 如果您使用一个或多个 Web 代理，可以在**代理服务器**部分添加代理地址。支持未经身份验证和经过身份验证的代理。要添加未经身份验证的代理，请提供有效的**代理 IP 地址和端口**。要添加经过身份验证的代理，还需要提供有效的**用户名**和**密码**。

> **注意：**
>
> 仅支持基本代理身份验证。不支持其他形式的身份验证。

只有流向外部系统的流量才通过 Web 代理路由。有关详细信息，请参阅连接器设备通信。

6. (可选) 如果您的网络使用 TLS 拦截 Web 代理访问互联网，您可能需要您的连接器信任其根证书颁发机构才能成功与云通信。

   a. 在**根证书颁发机构**下，选择**添加证书**。

   b. 以 PEM 格式复制证书内容：

```
-----BEGIN CERTIFICATE-----

<certificate-base64-bytes>
```

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

```
-----END CERTIFICATE-----
```

c. 在**完整证书详细信息**中，粘贴证书内容。

d. 选择**添加证书**。

要使用连接器设备 API 添加 RootCA，请参阅 Citrix Developer 文档中的管理根证书颁发机构。

> **注意：**
>
> 已过期或将在未来 30 天内过期的证书将显示警告。

7. 单击**注册连接器**以打开注册任务。
8. 为您的 Connector Appliance 选择一个名称。此名称可帮助您区分资源位置中存在的各种 Connector Appliance。注册 Connector Appliance 后，名称无法更改。

   在“**Connector Appliance 名称**”字段中输入名称，然后单击“**下一步**”。

   命名连接器设备。(/en-us/citrix-cloud/media/connector-appliance-rename.png)

   网页提供了一个用于向 Citrix Cloud 注册的代码。此代码将在 15 分钟后过期。

   用于连接到 Citrix Cloud 的生成代码(/en-us/citrix-cloud/media/connector-appliance-code.png)
9. 使用“**复制**”按钮将代码复制到剪贴板。
10. 返回“**资源位置**”网页。
11. 将代码粘贴到“**安装 Connector Appliance**”任务的“**步骤 2**”中。单击“**确认详细信息**”。

    Citrix Cloud 验证 Connector Appliance 是否存在且可联系。如果注册代码已过期，系统会提示您生成新代码。

    步骤 2 显示连接器已准备好注册。(/en-us/citrix-cloud/media/connector-appliance-step-2.png)
12. 单击“**注册**”。

    页面显示注册是否成功。如果注册失败，系统会提示您重试。
13. 单击“**关闭**”。

“**Connector Appliance 管理页面**”还允许您下载 Connector Appliance 的诊断报告。有关详细信息，请参阅生成诊断报告。

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

注册您的连接器设备后

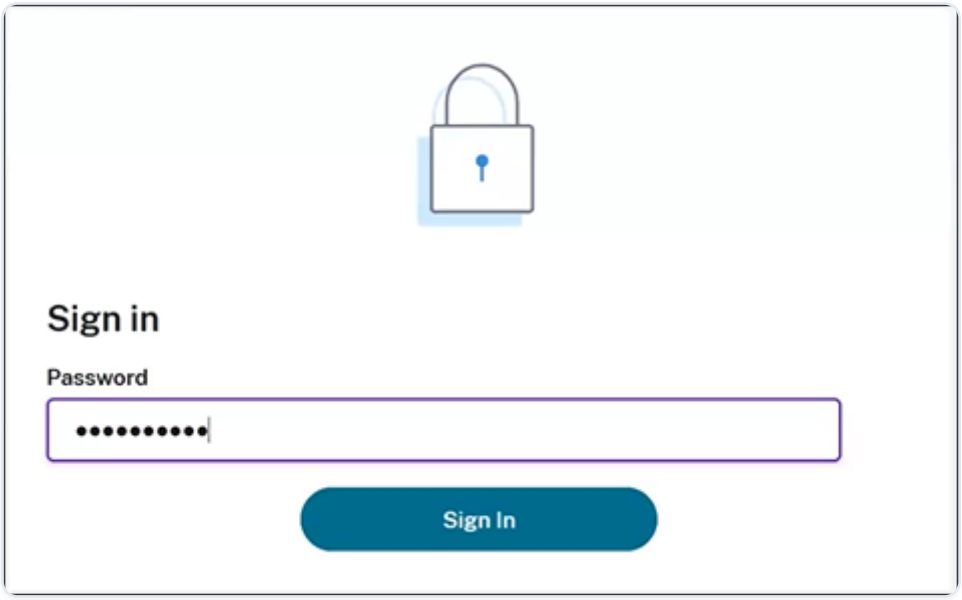
对于每个资源位置，我们建议您安装并注册两个或更多 Connector Appliance。此配置可确保持续可用性，并使连接器能够平衡负载。

您无法直接管理您的 Connector Appliance。

Connector Appliance 会自动更新。您无需执行任何操作来更新连接器。您可以指定希望在资源位置应用 Connector Appliance 更新的时间和日期。有关详细信息，请参阅连接器更新。

请勿克隆、暂停或创建 Connector Appliance VM 的快照。不支持这些操作。

首次连接到 Connector Appliance UI 时，只会显示“**创建新密码**”页面。请务必将此密码存储在安全位置以备将来使用。此密码无法重置。如果您忘记密码，则必须重新安装 Connector Appliance。后续连接到 UI 时，系统会要求您输入注册 Connector Appliance 时设置的密码。



Connector Appliance 连接性检查

Connector Appliance 实施了一组自动连接性检查，以确保满足 Connector Appliance 连接的所有要求。有关连接性要求的更多信息，请参阅Internet 连接要求。

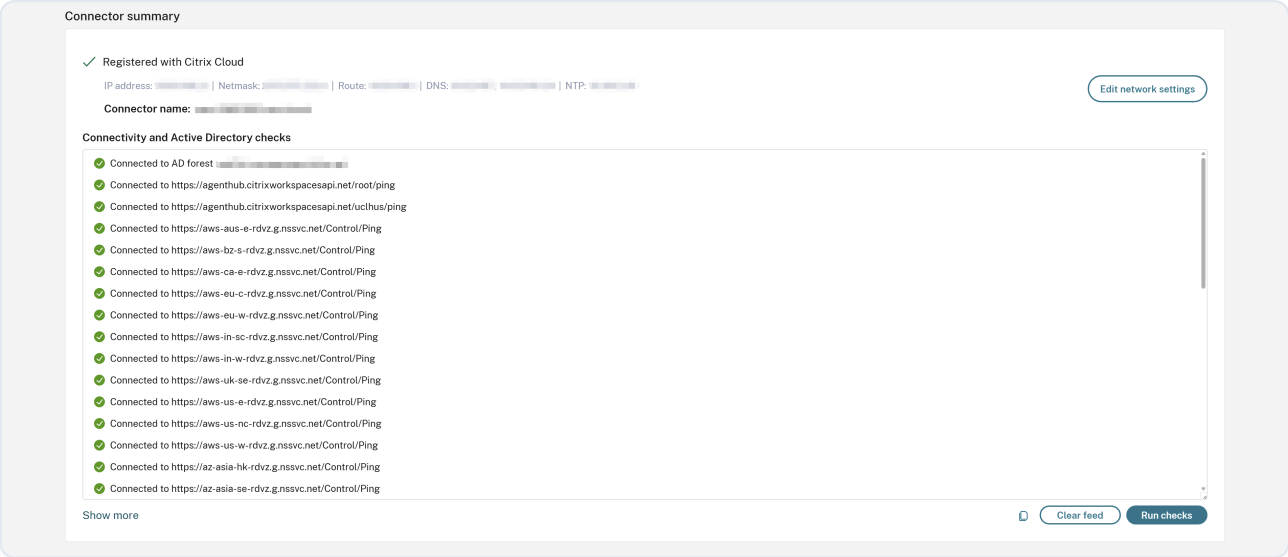
这些检查可以手动触发，并且可以从 Connector Appliance 管理员用户界面查看结果。

访问和运行连接性检查的步骤

1. 在您的虚拟机管理程序中的 Connector Appliance 控制台中，将 IP 地址复制到浏览器的地址栏中。
2. 输入您注册 Connector Appliance 时设置的密码。
3. 加载页面后，测试会自动运行。

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

4. 要重新运行测试，请单击“**运行检查**”。
5. 要将结果复制到剪贴板，请单击“**复制**”图标。



活动目录检查

与 Active Directory 相关的检查按域分组。如果设备未加入任何域，则不会运行 Active Directory 测试。

对于每个已加入的域，将运行以下检查：

- 域连接
- 与域的查询时间同步
- 验证处理来自 Citrix Cloud 的域请求的能力

网关服务提供商

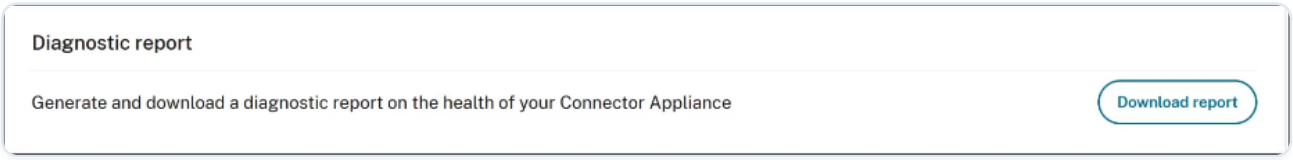
对于网关服务，连接器查询存在点列表并验证连接。

核心连接器服务

对于核心连接器服务，连接器设备向一系列用作核心功能一部分的云服务执行 HTTP GET 请求。设备还会测试与 Azure 容器注册表 (ACR) 的连接，该注册表用于下载新版本的连接器。

生成诊断报告

您可以从 **连接器设备管理页面** 生成并下载诊断报告。



1. 从虚拟机管理程序中的连接器设备控制台，将 IP 地址复制到浏览器地址栏。

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

2. 输入您在注册 Connector Appliance 时设置的密码。
3. 在页面的“**诊断报告**”部分，单击“**下载报告**”。

诊断报告以 `.zip` 文件的形式提供。

验证您的网络连接

您可以使用“**TCP 捕获**”诊断检查，从“**Connector Appliance 管理页面**”检查您的网络连接。

1. 在“**Connector Appliance 管理页面**”上，单击标题栏中的帐户名，然后选择“**网络诊断**”。
2. （可选）在“**TCP 捕获**”部分，输入目标 IP 地址、主机名或端口以限制 TCP 捕获。
3. 从“**跟踪持续时间**”菜单中，选择您希望跟踪运行的持续时间。
4. （可选）启用“**数据包跟踪**”以捕获数据包内容。

   禁用数据包跟踪时，TCP 捕获功能会尽力捕获标头以进行诊断。这种尽力而为的方法会捕获每个数据包的前 512 字节。但是，由于标头不是固定大小，因此此方法可能无法捕获所有标头。
5. 单击“**开始跟踪**”。
6. 等待跟踪完成。跟踪完成后，您可以下载跟踪报告或开始新的跟踪。
   - 单击“**下载**”以下载跟踪报告。跟踪报告以 `.pcap` 文件的形式提供。
   - 单击“**开始新跟踪**”以开始另一个跟踪。

网络连接探测工具

Connector Appliance 网络连接探测器提供了一种按需方式，可以使用多种协议测试到支持的网络目标的连接，并可选择代理和数据包捕获。有关支持的协议、代理行为、允许的目标以及如何解释探测结果的详细信息，请参阅Connector Appliance 网络连接探测页面。

将活动目录连接到 Citrix Cloud

您可以使用 Connector Appliance 将资源位置连接到不包含 Citrix Virtual Apps and Desktops 资源的林。例如，对于 Citrix Secure Private Access™ 客户或某些林仅用于用户身份验证的 Citrix Virtual Apps and Desktops 客户。

有关详细信息，请参阅使用 Connector Appliance 的 Active Directory。

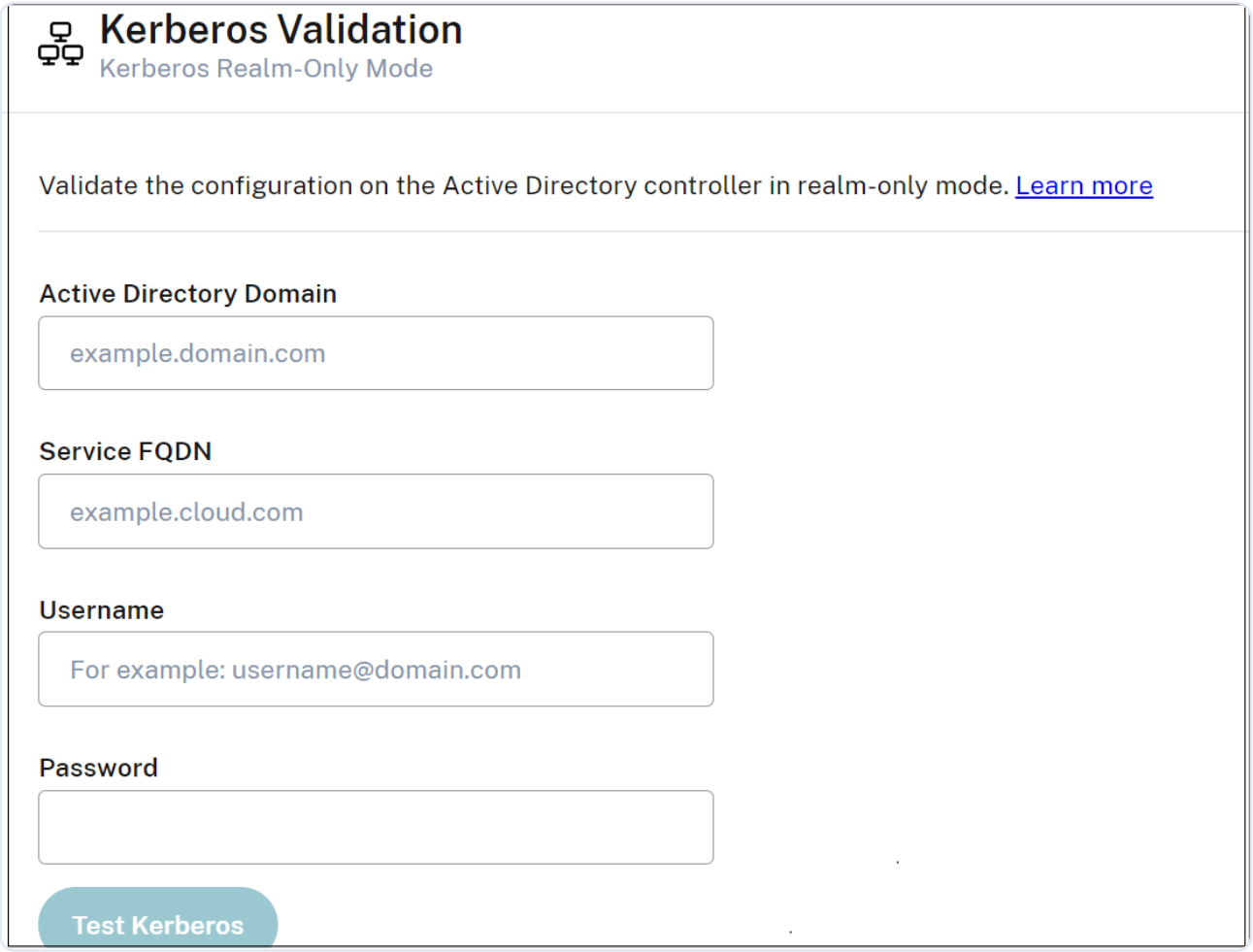
验证您的 Kerberos 配置

如果您使用 Kerberos 进行单点登录，则可以从**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 仅限领域模式配置或 Kerberos 约束委派 (KCD) 模式配置。

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

验证 Kerberos 仅限领域配置：

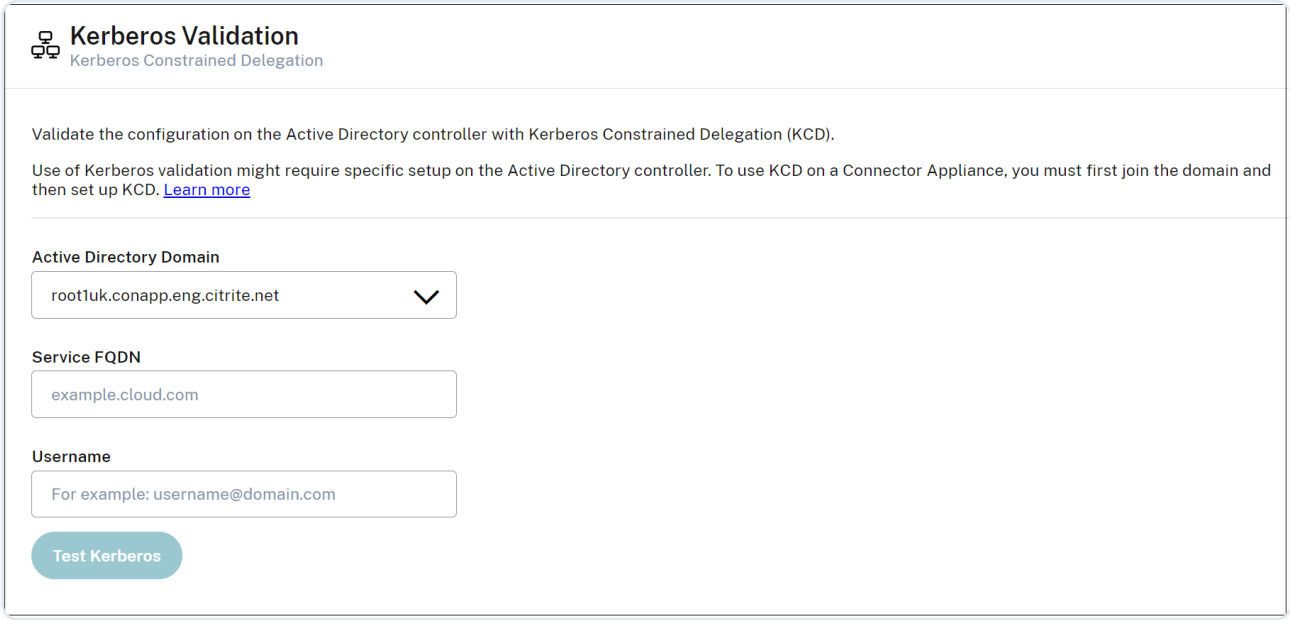
1. 转到**Connector Appliance 管理**页面。
2. 从您的虚拟机管理程序中的 Connector Appliance 控制台，将 IP 地址复制到浏览器地址栏。
3. 输入您注册 Connector Appliance 时设置的密码。
4. 要验证您的仅限领域 Kerberos 配置，请在**Active Directory 域**部分中选择**Kerberos 验证（仅限领域）**。
5. 指定 **Active Directory 域**。
   - 如果您正在验证 Kerberos 仅限领域模式配置，则可以指定任何 Active Directory 域。此模式不依赖于加入域。
6. 指定**服务 FQDN**。默认服务名称假定为“https”。如果您指定“computer.example.com”，则此值被视为与“`<https://computer.example.com>`”相同。
7. 指定**用户名**。
8. 指定**密码**。
9. 单击**测试 Kerberos**。



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

验证 Kerberos 约束委派 (KCD) 配置：

1. 转到**Connector Appliance 管理**页面。
2. 要验证已加入 Connector Appliance 的域的**Kerberos 约束委派 (KCD)** 模式，请从相关域的省略号菜单 (...) 中选择**Kerberos 验证**。
3. 指定**Active Directory 域**。
   - 如果您正在验证 Kerberos 约束委派配置，则必须从已加入的域列表中进行选择。
4. 指定**服务 FQDN**。默认服务名称假定为“https”。例如，指定“computer.example.com”，此值被视为与“`<https://computer.example.com”>`。
5. 指定**用户名**。
   - 对于 Kerberos 约束委派模式，您还可以通过选择**服务帐户**选项卡来使用服务帐户验证 Kerberos 设置。
6. 单击**测试 Kerberos**。



如果 Kerberos 配置正确，您将看到消息“Kerberos 设置已成功验证”。如果 Kerberos 配置不正确，您将看到一条错误消息，其中提供有关验证失败方式的信息。

有关 Kerberos 的更多信息，请参阅 Microsoft 文档。

您的连接器设备的网络设置

默认情况下，您的连接器设备的 IP 地址和网络设置通过 DHCP 自动分配。

通过 DHCP 注册连接器设备后，您可以在**连接器设备管理页面**中编辑其网络设置。

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

但是，如果您的环境中没有 DHCP，或者您无法访问**连接器设备管理页面**，则可以直接在连接器设备控制台上设置网络配置。

在连接器设备管理页面上配置网络设置

通过 DHCP 注册连接器设备后，您可以在**连接器设备管理页面**中编辑其网络设置。

要手动配置网络设置，请执行以下操作：

1. 在**连接器摘要**部分中，选择**编辑网络设置**。
2. 在**网络设置**对话框中，选择**配置您自己的网络设置**。
3. 输入 **IP 地址**、**子网掩码**和**默认网关**。
4. 添加一个或多个 **DNS 服务器**。
5. 添加一个或多个 **NTP 服务器**。
6. 单击**保存**。

保存对网络设置的更改后，连接器设备将重新启动。在重新启动期间，连接器设备将暂时不可用。您将从**连接器设备管理页面**注销，并且此页面的 URL 会更改。您可以在连接器设备控制台中或通过查看管理程序中的网络信息来查找新的 URL。

要将网络配置更改为使用自动分配的值，请执行以下操作：

1. 在“**连接器摘要**”部分中，选择“**编辑网络设置**”。
2. 在“**网络设置**”对话框中，选择“**自动获取 IP 地址**”。
3. 单击“**保存**”。

保存对网络设置的更改后，Connector Appliance 将重新启动。在重新启动期间，Connector Appliance 将暂时不可用。您将从“**Connector Appliance 管理页面**”注销，并且此页面的 URL 会更改。您可以在 Connector Appliance 控制台中或通过查看管理程序中的网络信息来查找新的 URL。

使用 Connector Appliance 控制台设置网络配置

默认情况下，Connector Appliance 的 IP 地址和网络设置通过 DHCP 自动分配。但是，如果您的环境中没有 DHCP，或者您无法访问“**Connector Appliance 管理页面**”，则可以直接在 Connector Appliance 控制台上设置网络配置。

要设置网络配置：

1. 在您的管理程序中，重新启动 Connector Appliance。
2. 在 Connector Appliance 启动时，在控制台中查找消息 `Welcome to GRUB!`。

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

3. 看到此消息时，按 **Esc** 进入 GRUB 菜单。
4. 要编辑启动参数，请按 **e**。

   您会看到一个类似于下图的视图：

5. 编辑以 `linux` 开头的行，以包含所需的网络配置。
   - 要指定 DHCP 网络，请将 `network=dhcp` 附加到行的末尾。
   - 要指定静态网络，请将以下参数附加到行尾：

     ```
     network=static:ip=<static_ip_address>:netmask=<netmask>:route=<defau
     lt_gateway>:dns=<dns_server_1>,<dns_server_2>:ntp=<ntp_server_1>,<nt
     p_server_2>
     ```

     将占位符值替换为您的配置值。
6. 按 **Ctrl+X** 以新配置启动 Connector Appliance。

更改 Connector Appliance 的管理员用户密码

1. 在控制台右上角的用户菜单中，选择 **更改密码**。

   显示更改密码页面。

2. 输入您的当前密码，然后输入并确认新密码。您设置的新密码必须满足以下要求：

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

- 长度为 8 个或更多字符
- 包含大小写字母
- 包含至少一个非字母字符
- 不得与当前密码相同

3. 选择 **更改密码** 以保存您的更改。

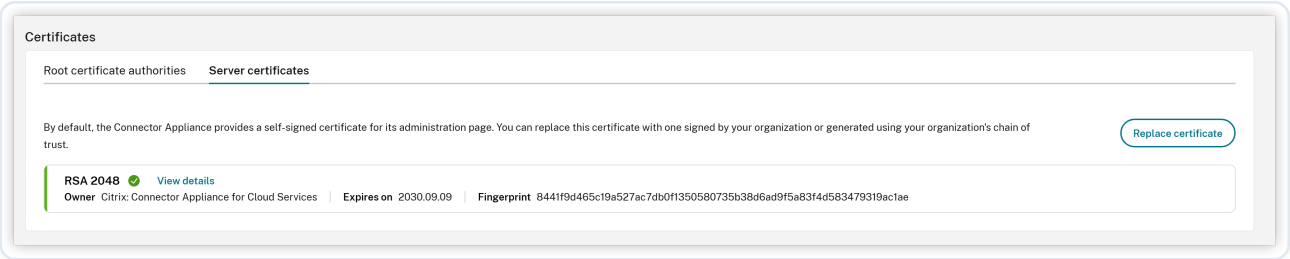
Citrix Cloud 会自动将您注销并重定向到登录页面。

替换服务器证书

Connector Appliance 允许管理员替换其管理 Web 界面使用的默认自签名 SSL 或 TLS 证书。管理员可以使用由其组织签名或使用其组织的信任链生成的自定义证书。

要访问服务器证书管理界面，请转到 Connector Appliance 管理员界面。导航到 **Certificates**（证书）并选择 **Server certificates**（服务器证书）选项卡。

默认情况下，Connector Appliance 使用自签名证书。将其替换为自定义证书后，必须由受信任的证书颁发机构颁发该证书，浏览器才能信任管理页面。



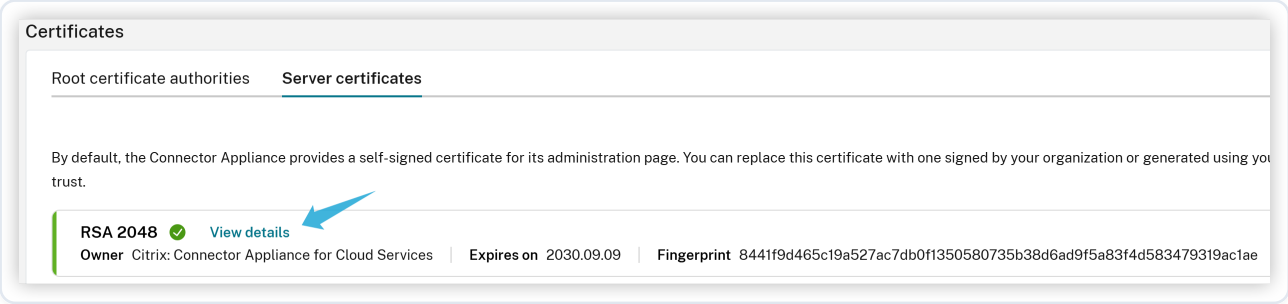
查看当前服务器证书

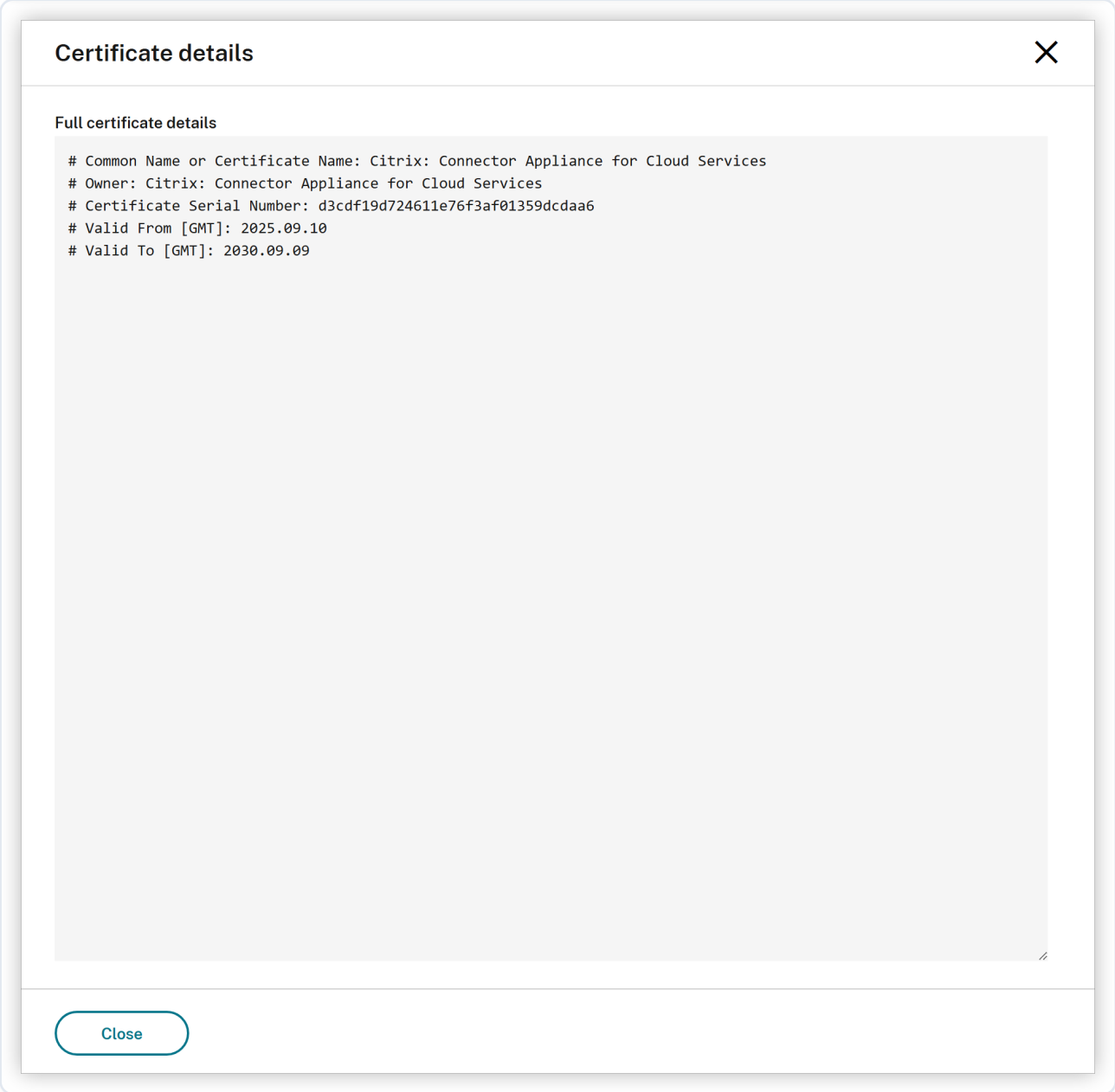
Server certificates（服务器证书）选项卡显示一个卡片，其中包含有关当前证书的信息：

- **Subject**（主题）— 证书算法和密钥长度（例如，RSA 2048）。
- **Owner**（所有者）— 证书颁发者或所有者（如果可用）。
- **Expires on**（过期日期）— 证书过期日期。
- **Fingerprint**（指纹）— 证书的 SHA-256 指纹。

要查看完整的证书详细信息，请单击证书卡上的 **View details**（查看详细信息）链接。此时会打开一个侧面板，显示完整的已解析证书信息。单击 **Close**（关闭）以关闭详细信息面板。

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





替换服务器证书

您可以使用由您的组织签名的自定义证书替换服务器证书。

先决条件：在替换证书之前，请确保您拥有以下各项

- **PEM 格式**的证书文件。该证书应由访问 Connector Appliance 管理页面的浏览器信任的证书颁发机构颁发。

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

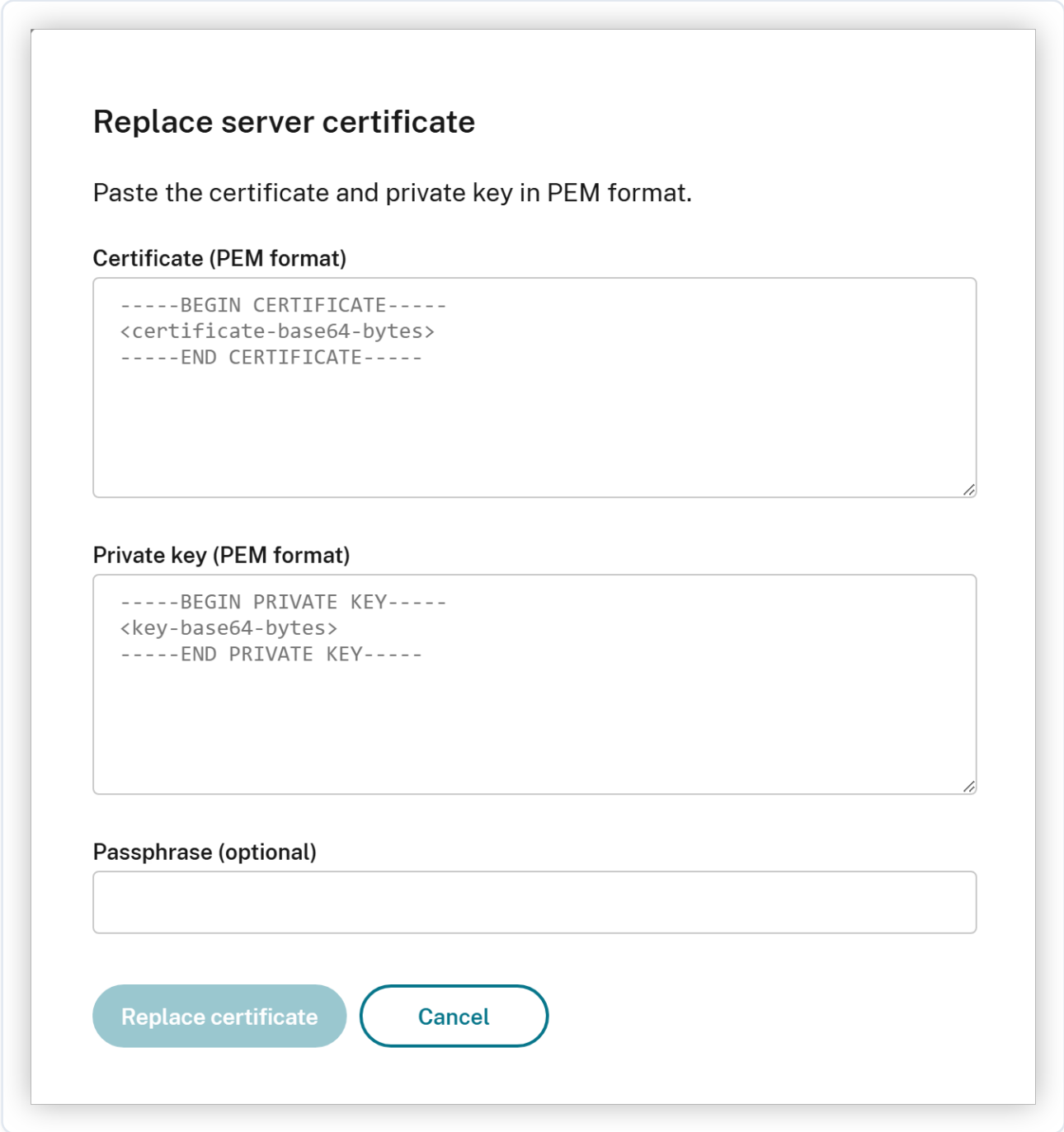
- 相应的 **PEM 格式**的**私钥**。
- 私钥的**密码**（如果密钥已加密）（可选）。

替换证书的步骤

1. 在您的虚拟机管理程序中的 Connector Appliance 控制台中，复制 IP 地址并将其粘贴到浏览器的地址栏中。
2. 输入您在注册 Connector Appliance 时设置的密码。
3. 导航到左侧菜单中的**证书**。
4. 选择**服务器证书**选项卡。
5. 单击**替换证书**按钮。
6. 在“替换服务器证书”对话框中：
   - 将 PEM 格式的证书内容粘贴到**证书 (PEM 格式)**字段中。证书应以 `-----BEGIN CERTIFICATE-----` 开头，并以 `-----END CERTIFICATE-----` 结尾。
   - 将 PEM 格式的私钥粘贴到**私钥 (PEM 格式)**字段中。密钥应以 `-----BEGIN PRIVATE KEY-----` 开头，并以 `-----END PRIVATE KEY-----` 结尾。
   - （可选）如果私钥已加密，请在**密码（可选）**字段中输入密码。
7. 单击**替换证书**以提交。

如果替换成功，系统将显示成功消息，并使用新的证书信息更新证书卡。

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



证书格式要求

- 证书和私钥都必须采用**PEM 格式**。
- 证书字段支持完整的证书链。如果中间 CA 签署了您的证书，请粘贴完整的链（服务器证书后跟中间证书）。
- 支持的密钥类型为**RSA**和**ECDSA**。

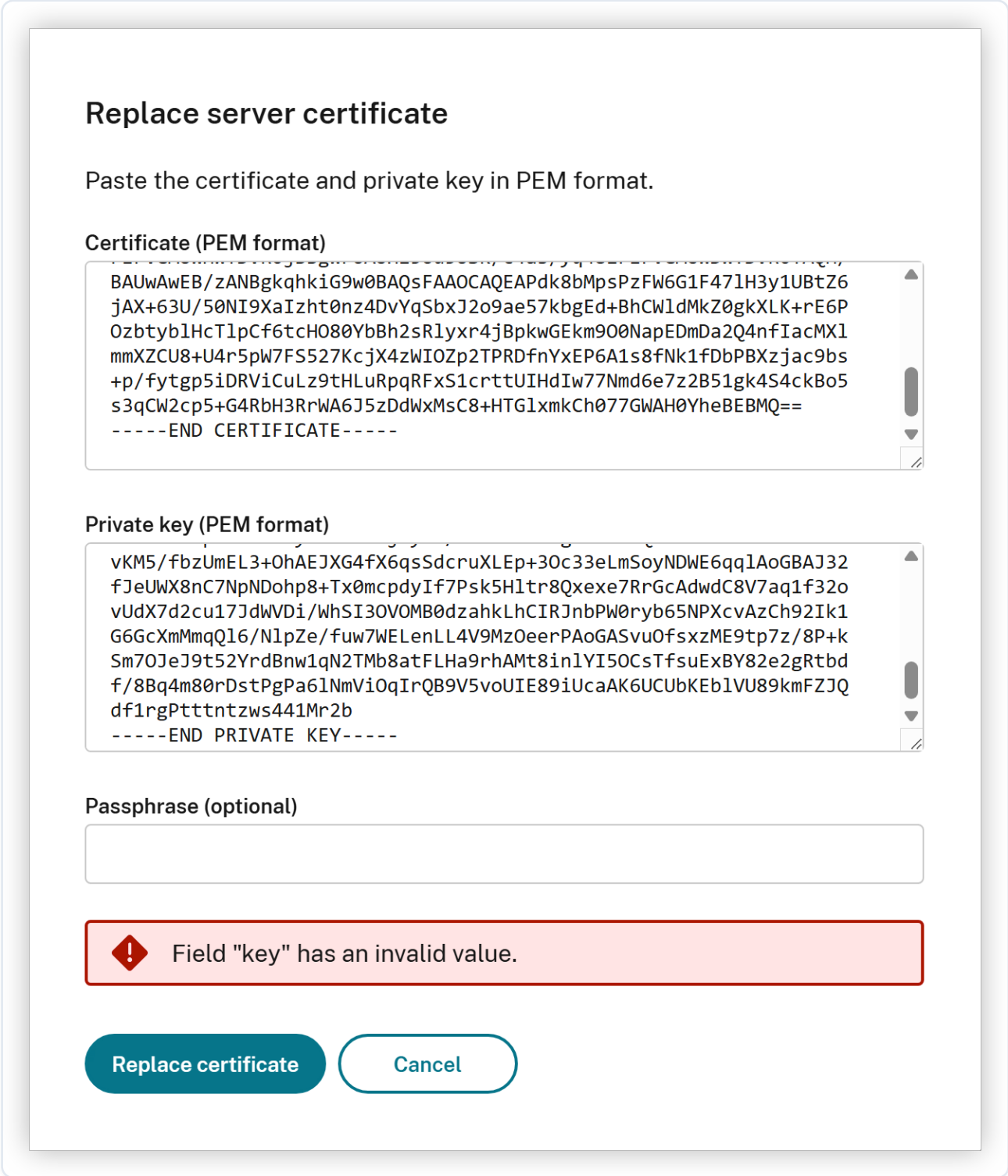
错误处理

如果证书替换失败，对话框将显示错误消息。常见的失败原因包括：

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

- 证书和私钥不匹配。
- 证书或私钥不是有效的 PEM 格式。
- 私钥密码不正确。

查看错误消息，更正问题，然后重试。单击**取消**以关闭对话框而不进行更改。



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

恢复为自签名证书

要恢复到默认的自签名证书，您必须重新部署连接器设备。目前无法独立恢复证书。

注意

- 更换证书后，连接器设备管理页面将对所有后续 HTTPS 连接使用新证书。
- “**服务器证书**”选项卡上显示的证书信息每 30 秒自动刷新一次。
- 证书更换操作要求您使用有效的会话令牌登录。

使用连接器设备的活动目录

您可以使用 Connector Appliance 将资源位置连接到不包含 Citrix Virtual Apps and Desktops™ 资源的林。例如，对于 Citrix Secure Private Access 客户，或者对于某些林仅用于用户身份验证的 Citrix Virtual Apps and Desktops 客户。

将多域 Active Directory 与 Connector Appliance 结合使用时，适用以下限制：

- 在包含 VDA 的林中，Connector Appliance 不能替代 Cloud Connectors 使用。

要求

活动目录要求

- 加入包含您用于为用户创建服务的资源和用户的 Active Directory 域。有关详细信息，请参阅本文中的 Active Directory 中 Connector Appliance 的部署方案。
- 您计划与 Citrix Cloud™ 配合使用的每个 Active Directory 林必须始终可通过两个 Connector Appliance 访问。
- Connector Appliance 必须能够访问林根域和您打算与 Citrix Cloud 配合使用的域中的域控制器。有关详细信息，请参阅以下 Microsoft 支持文章：
  - 如何配置域和信任
  - Windows 的服务概述和网络端口要求 中的“系统服务端口”部分
- 使用通用安全组而不是全局安全组。此配置可确保可以从林中的任何域控制器获取用户组成员身份。

网络要求

- 连接到可以联系您在资源位置中使用的资源的网络。

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

- 连接到 Internet。有关详细信息，请参阅 系统和连接要求。

除了(/zh-cn/citrix-cloud/citrix-cloud-resource-locations/connector-appliance.html#connector-appliance-communication)中列出的连接器设备通信端口之外，连接器设备还需要通过以下端口与 Active Directory 域建立出站连接：

服务	端口	支持的域协议
科尔贝罗斯	88	TCP/UDP
NetBIOS 名称服务	137	UDP
NetBIOS 数据报	138	UDP
NetBIOS 会话	139	TCP
LDAP	389	TCP/UDP
基于 TCP 的 SMB	445	TCP
科尔贝罗斯 kpasswd	464	TCP/UDP
全局编录	3268	TCP
动态 RPC 端口	49152–65535	TCP

连接器设备使用 LDAP 签名来保护与域控制器的连接。这意味着不需要通过 SSL 的 LDAP (LDAPS)。有关 LDAP 签名的更多信息，请参阅 如何在 Windows Server 中启用 LDAP 签名 和 Microsoft 关于启用 LDAP 通道绑定和 LDAP 签名的指南。

支持的 Active Directory 功能级别

连接器设备已经过测试，并支持 Active Directory 中的以下林和域功能级别。

林功能级别	域功能级别	支持的域控制器
Windows Server 2016 服务器	Windows Server 2016 服务器	Windows Server 2019 服务器

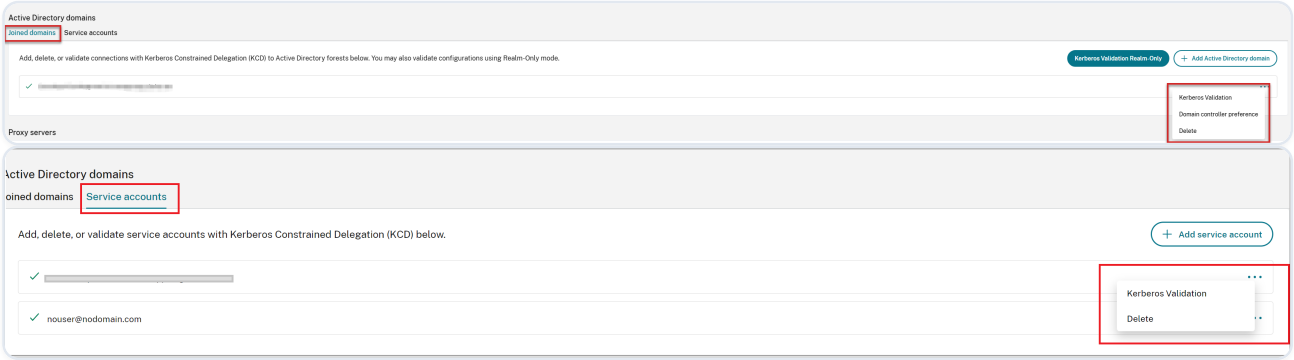
域控制器、林功能级别和域功能级别的其他组合尚未与连接器设备进行测试。但是，这些组合预计可以工作，并且也受支持。

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

使用连接器设备将 Active Directory 域连接到 Citrix Cloud

当您连接到连接器设备管理网页时，“**Active Directory 域**”部分显示两个选项卡。

- **已加入的域** – 用于通过在域中为设备创建计算机帐户，将连接器设备加入 AD 域。可以通过单击已加入域右侧的省略号菜单来验证 Kerberos。域中需要存在计算机帐户。
- **服务帐户** – 用作安全专用访问 (SPA) 解决方案的一部分，以使用服务帐户而不是通过加入域创建的计算机帐户来实现 Kerberos SSO。可以通过单击服务帐户右侧的省略号菜单来验证 Kerberos。机器关联特定域并非强制要求。但是，即使连接器设备未连接到域，它仍然可以连接到域控制器。



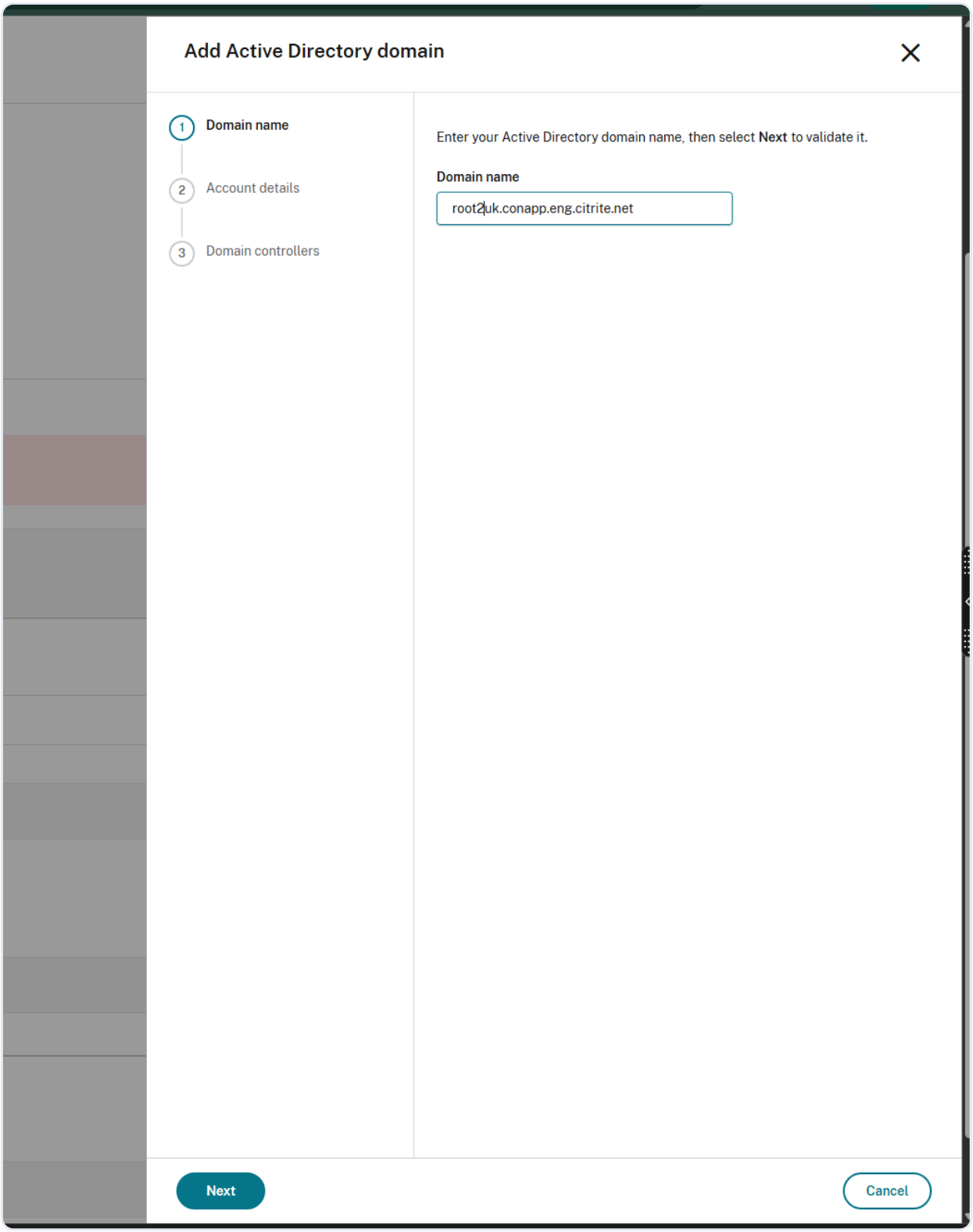
要通过 Connector Appliance 将 Active Directory 配置为连接到 Citrix Cloud，请完成以下步骤。

1. 在您的资源位置安装 **Connector Appliance**。

   您可以按照 Connector Appliance 产品文档 中的信息进行操作。

2. 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。
3. 在“**Active Directory 域**”部分中，导航到“**已加入的域**”选项卡。
4. 单击“**+ 添加 Active Directory 域**”，将显示一个新弹出窗口以输入域名。
5. 在“**域名**”步骤中，输入 Active Directory 域名，然后单击“**下一步**”。**Connector Appliance** 将检查该域。如果检查成功，向导将进入下一步。

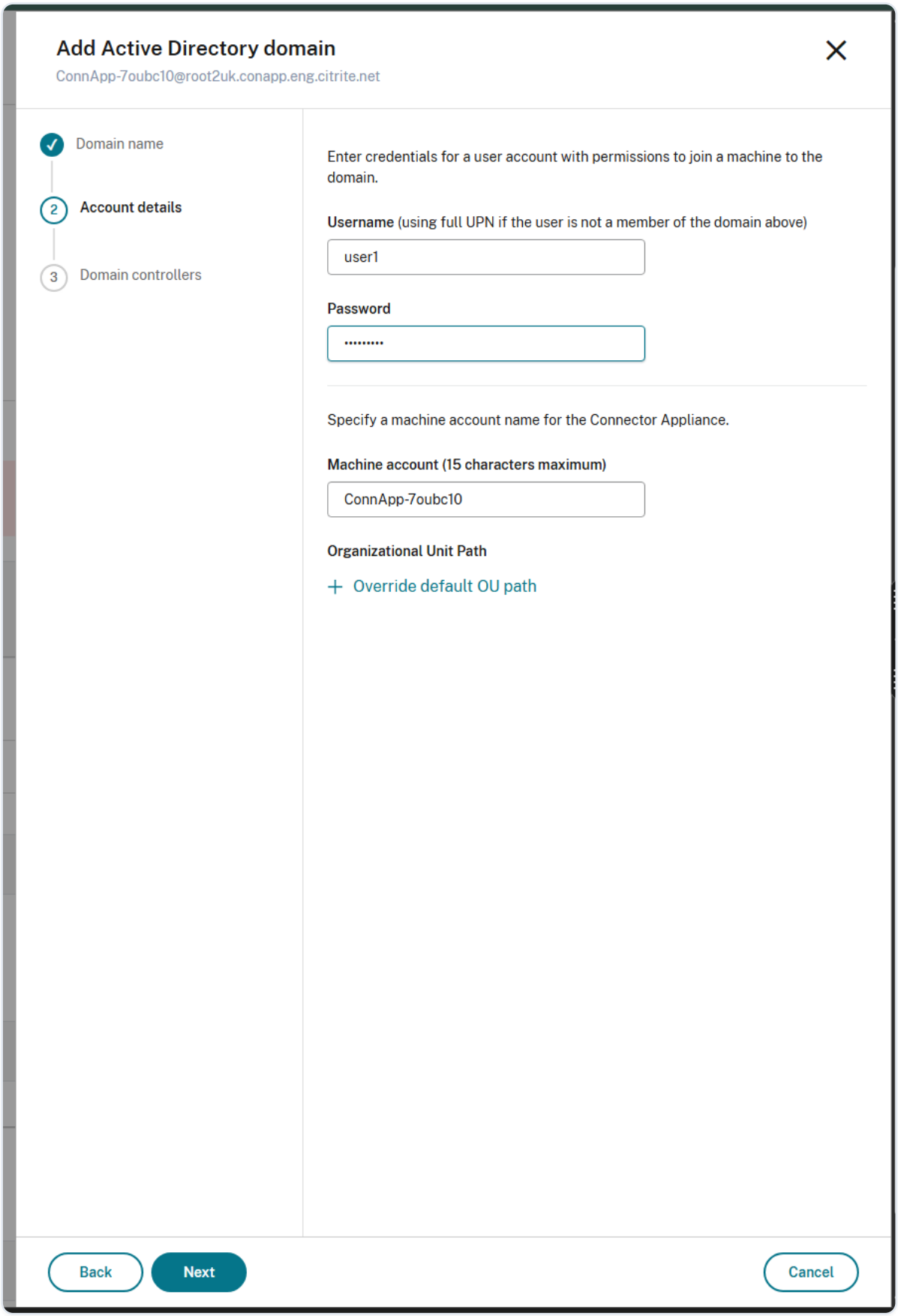
© 1997–2026 Citrix Systems, Inc. All rights reserved.



6. 在“**帐户详细信息**”步骤中，提供以下信息，然后单击“**下一步**”：

   - 具有加入域权限的 Active Directory 用户的用户名和密码。
   - 计算机名称。**Connector Appliance** 会建议一个计算机名称；您可以将其替换为自己的计算机名称，最多 15 个字符。当 **Connector Appliance** 加入 Active Directory 域时，将在该域中创建此计算机名称。

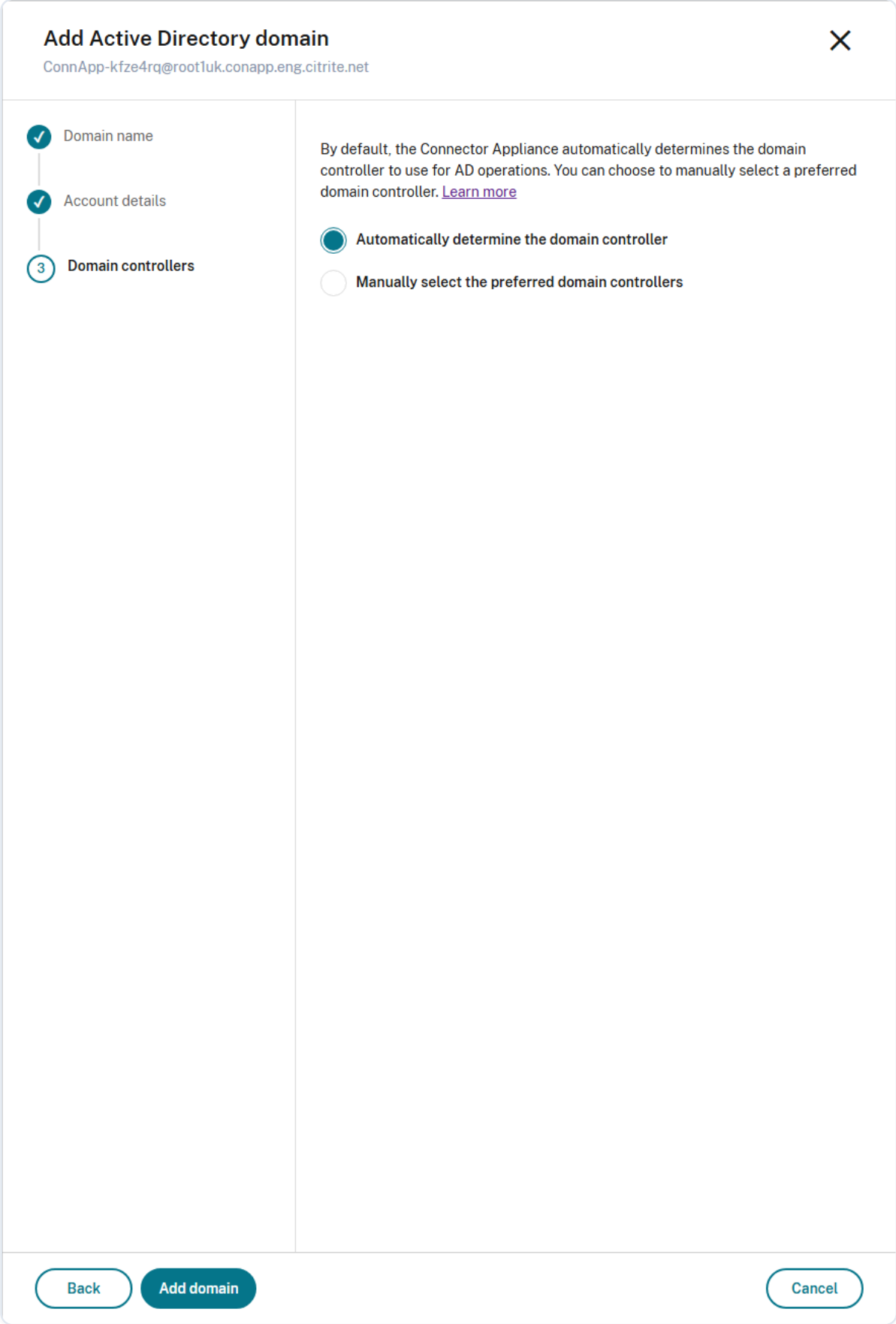
© 1997–2026 Citrix Systems, Inc. All rights reserved.



7. 在“**域控制器**”步骤中，选择以下选项之一，以确定 **Connector Appliance** 如何选择此域的域控制器：

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

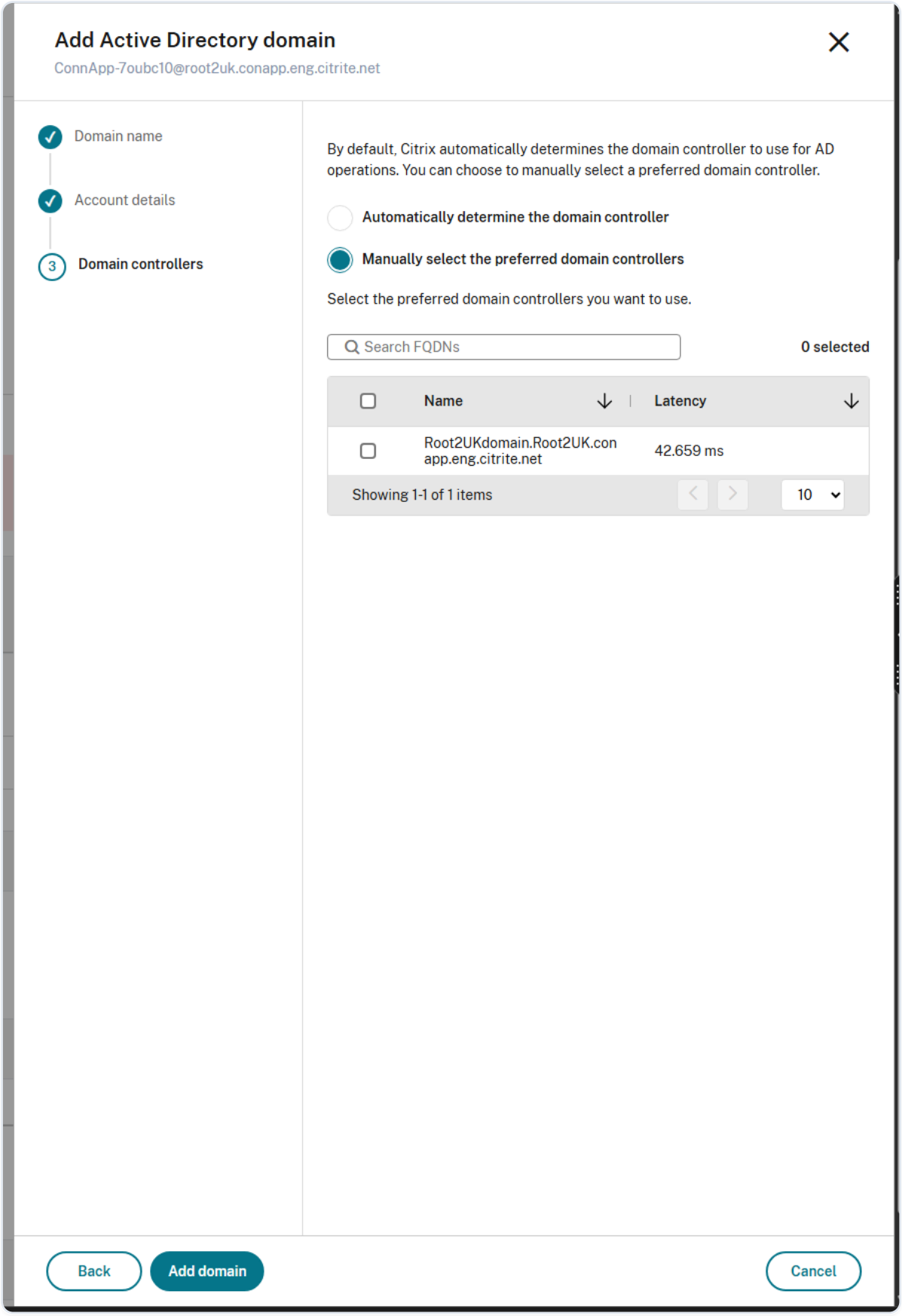
- **自动确定域控制器**（默认）– Connector Appliance 自动确定用于 Active Directory 操作的域控制器，并定期重新评估此选择。



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

- **手动选择首选域控制器** — **Connector Appliance** 仅使用您选择的域控制器。可搜索的表格列出了可用的域控制器及其测量的**延迟**（以毫秒为单位）。使用搜索框按名称筛选，或按**名称**或**延迟**排序，然后选中要使用的域控制器的复选框。如果您未选择任何域控制器，**Connector Appliance** 将回退到自动选择。

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



8. 点击“**添加域**”。该域现在列在 **Connector Appliance** UI 的“**Active Directory 域**”部分中。

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

后续步骤

- 您可以将更多域添加到此 Connector Appliance。

> **注意：**
>
> Connector Appliance 经过测试，最多支持 10 个林。

- 为了提高弹性，请在每个资源位置将每个域添加到多个 Connector Appliance。

查看您的 Active Directory 配置

您可以在以下位置查看资源位置中 Active Directory 域和 Connector Appliance 的配置：

- 在 Citrix Cloud 中：
  a. 在菜单中，转到“**身份和访问管理**”页面。
  b. 转到“**域**”选项卡。

     您的 Active Directory 域将与它们所属的资源位置一起列出。
- 在 Connector Appliance 网页中：
  a. 使用 Connector Appliance 控制台中提供的 IP 地址连接到 Connector Appliance 网页。
  b. 使用您首次注册时创建的密码登录。
  c. 在页面的“**Active Directory 域**”部分，您可以看到此 Connector Appliance 已加入的 Active Directory 域列表。

从连接器设备中移除活动目录域

要离开 Active Directory 域，请完成以下步骤：

1. 使用 Connector Appliance 控制台中提供的 IP 地址连接到 Connector Appliance 网页。
2. 使用您首次注册时创建的密码登录。
3. 在页面的“**Active Directory 域**”部分，在已加入的 Active Directory 域列表中找到您要离开的域。
4. 记下您的 Connector Appliance 创建的计算机帐户的名称。
5. 单击域旁边的删除图标（垃圾桶）。将出现一个确认对话框。
6. 单击“**继续**”以确认操作。
7. 转到您的 Active Directory 控制器。
8. 从控制器中删除您的 Connector Appliance 创建的计算机帐户。

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

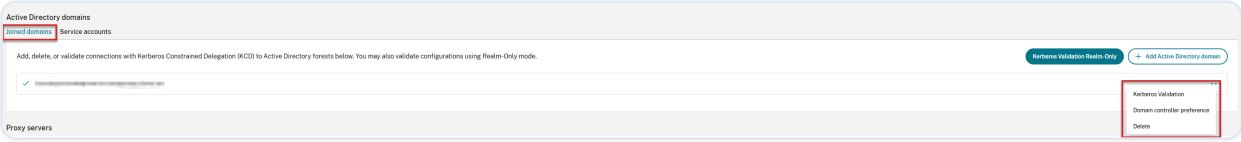
更改已加入的 Active Directory 域的域控制器首选项

加入 Active Directory 域后，您可以随时更改 **Connector Appliance** 用于该域的域控制器。默认情况下，**Connector Appliance** 会自动确定域控制器并定期重新评估选择；如果您在具有大量域控制器的环境中观察到性能不一致，则可以切换到手动选择一个或多个首选域控制器。

要更改已加入域的域控制器首选项，请完成以下步骤：

1. 使用 **Connector Appliance** 控制台中提供的 IP 地址连接到 **Connector Appliance** 管理网页。
2. 使用您首次注册时创建的密码登录。
3. 在“**Active Directory 域**”部分中，在“**已加入的域**”选项卡上，找到要更新的域。
4. 单击域旁边的省略号 (**...**) 菜单，然后选择“**域控制器首选项**”。

   “**域控制器首选项**”边栏随即打开。



5. 选择 **Connector Appliance** 如何为此域选择域控制器：

   - “**自动确定域控制器**” – **Connector Appliance** 自动确定要用于 Active Directory 操作的域控制器，并定期重新评估此选择。
   - **手动选择首选域控制器** – **Connector Appliance** 仅使用您选择的域控制器。可搜索的 表格列出了可用的域控制器及其测量的毫秒级 **延迟**。使用搜索框按名称筛选，或 按**名称**或**延迟**排序，然后选中要使用的 域控制器的复选框。

   注意：

   如果您选择“**手动选择首选域控制器**”但未选择任何域控制器，则 **Connector Appliance** 将回退到自动选择。

6. 单击“**保存**”以应用更改。

设置林首选连接器类型

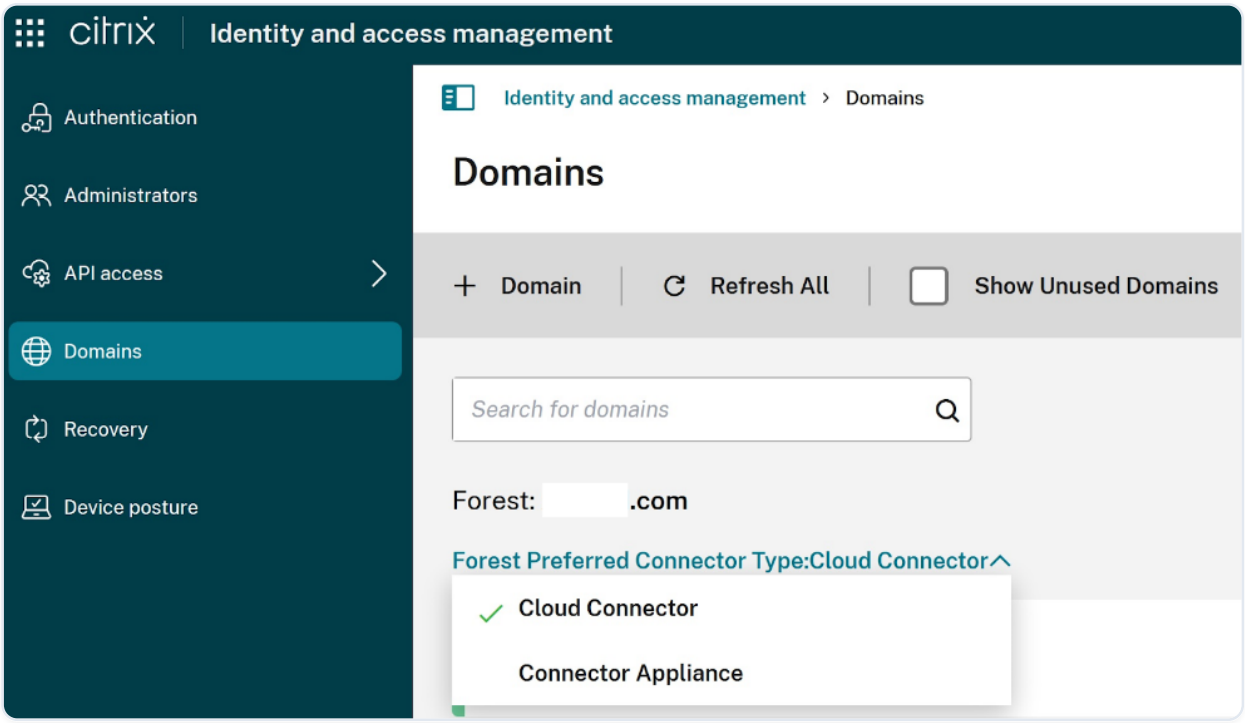
当 Citrix Cloud 租户同时拥有已加入同一 AD 林的 Windows 连接器和连接器设备时，可以设置首选连接器类型。

要为特定的 Active Directory 林设置首选连接器类型，请完成以下步骤：

1. 导航到“**身份和访问管理 > 域**”，然后单击要为其设置首选连接器类型的 AD 林上的向下箭头。

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

2. 选择 **林首选连接器类型**。



用于将连接器设备与 Active Directory 结合使用的部署场景

您可以使用 Cloud Connector 和连接器设备连接到 Active Directory 控制器。要使用的连接器类型取决于您的部署。

有关将 Cloud Connector 与 Active Directory 结合使用的更多信息，请参阅 Active Directory 中 Cloud Connector 的部署场景

在以下情况下，使用连接器设备将您的资源位置连接到 Active Directory 林：

- 您正在设置安全专用访问。有关更多信息，请参阅 使用连接器设备的安全专用访问。
- 您有一个或多个仅用于用户身份验证的林
- 您希望减少支持多个林所需的连接器数量
- 您需要连接器设备用于其他用例

仅一个或多个林中的用户，所有林共用一套连接器设备

此场景适用于标准客户或使用连接器设备进行安全专用访问的客户。

在此场景中，有多个林仅包含用户对象 (`forest1.local`, `forest2.local`)。这些林不包含资源。一套连接器设备部署在资源位置内，并加入到这些林中的每个域。

- 信任关系：无
- 列在 **身份和访问管理** 中的域：`forest1.local`, `forest2.local`

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

- 用户登录到云商店：所有用户均支持
- 用户登录到本地商店：所有用户均支持

用户和资源位于不同的林中（带信任），所有林使用一套连接器设备

此方案适用于拥有多个林的 Citrix Virtual Apps and Desktops 客户。

在此方案中，某些林 (`resourceforest1.local` , `resourceforest2.local`) 包含您的资源（例如 VDA），而某些林 (`userforest1.local` , `userforest2.local`) 仅包含您的用户。这些林之间存在信任关系，允许用户登录到资源。

一套 Cloud Connector 部署在 `resourceforest1.local` 林中。另一套 Cloud Connector 部署在 `resourceforest2.local` 林中。

一套连接器设备部署在 `userforest1.local` 林中，同一套设备也部署在 `userforest2.local` 林中。

- 信任关系：双向林信任，或从资源林到用户林的单向信任
- **Identity and Access Management** 中列出的域： `resourceforest1.local` , `resourceforest2.local` , `userforest1.local` , `userforest2.local`
- 用户登录到 Citrix® StoreFront Cloud：所有用户均支持
- 用户登录到本地 StoreFront：所有用户均支持

连接器设备网络连接探测器

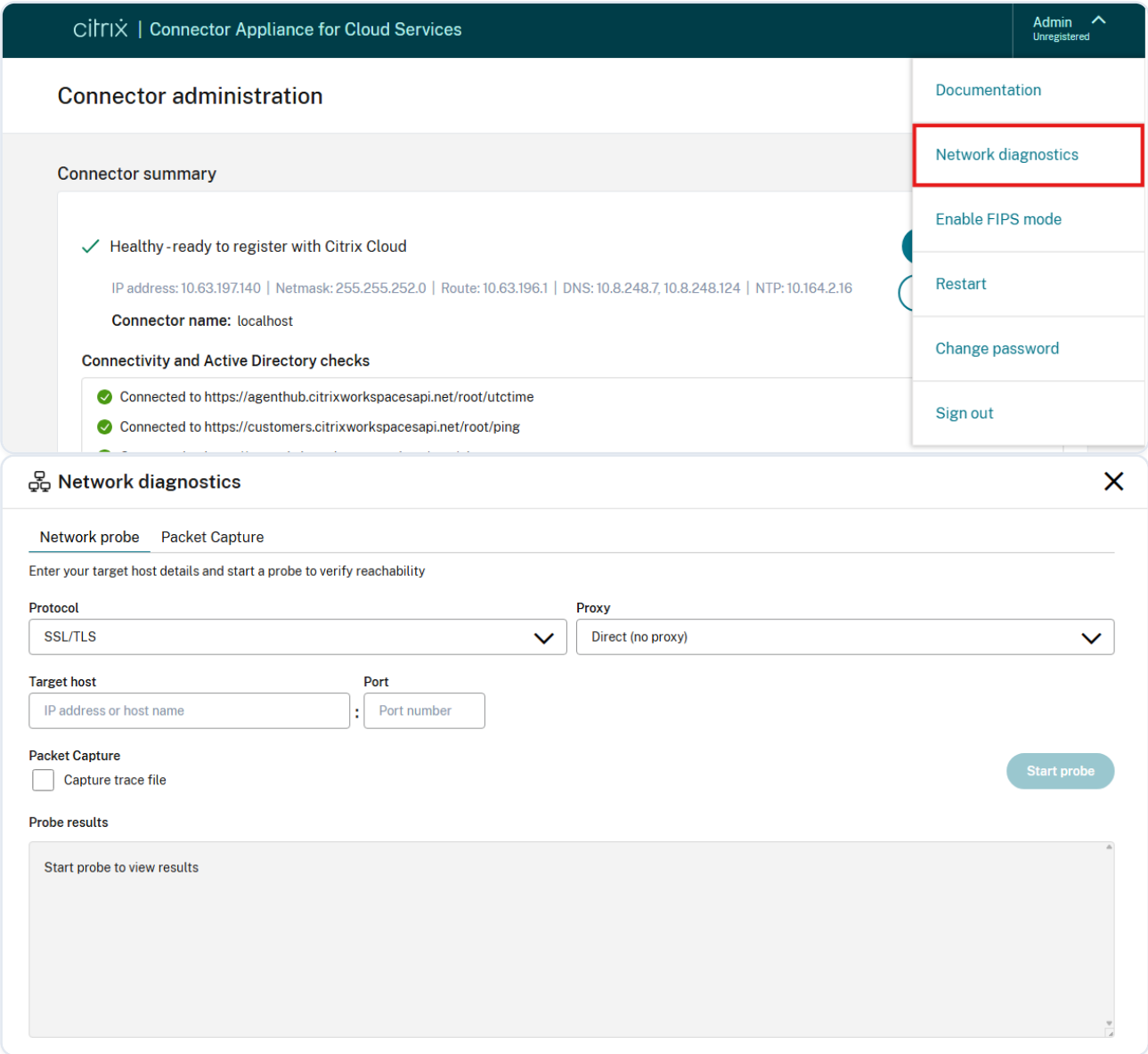
连接器设备网络连接探测器允许用户对网络目标执行按需连接性检查。

可以通过导航到右上角菜单中的**网络诊断**，从连接器设备管理员界面访问网络探测器用户界面。

支持以下协议：

- ICMP（发送 ping 请求）
- TCP
- TLS
- HTTP
- HTTPS

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



指定代理

默认情况下，网络探测器将直接连接到指定目标，不使用代理。

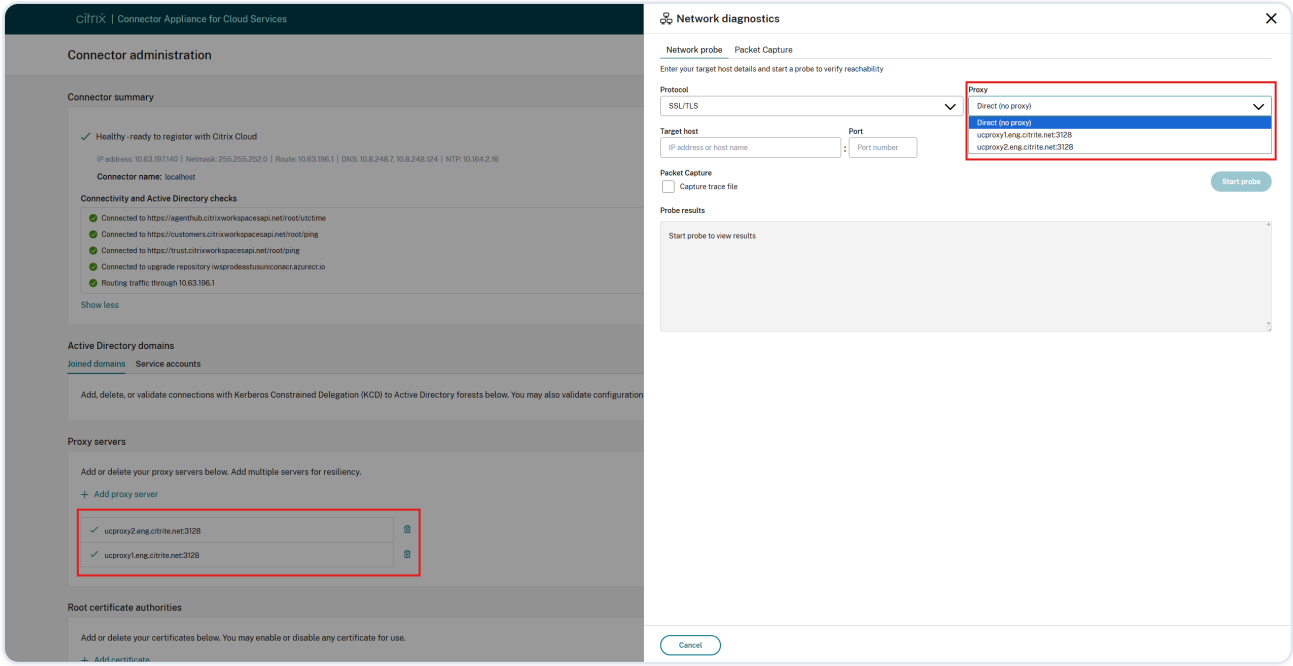
ICMP 网络探测器从不使用代理。

对于其他协议，可以使用**代理**下拉菜单为网络探测器选择连接器设备上配置的代理之一。网络探测器将通过选定的代理执行。

对于 TCP、TLS 和 HTTPS 协议，代理将用作 HTTPS 代理，网络探测将向所选代理发送 HTTP CONNECT 请求，以建立与指定网络目标的连接。

如果选择了 HTTP 协议，网络探测将把代理用作纯 HTTP 代理。

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



允许的网络目标

允许探测所有 私有网络目标。对于外部公共网络目标，只允许 Internet 连接要求 部分下列出的域。这些域中的每一个都由 Citrix 拥有，或者属于 Connector Appliance 运行所需的服务。

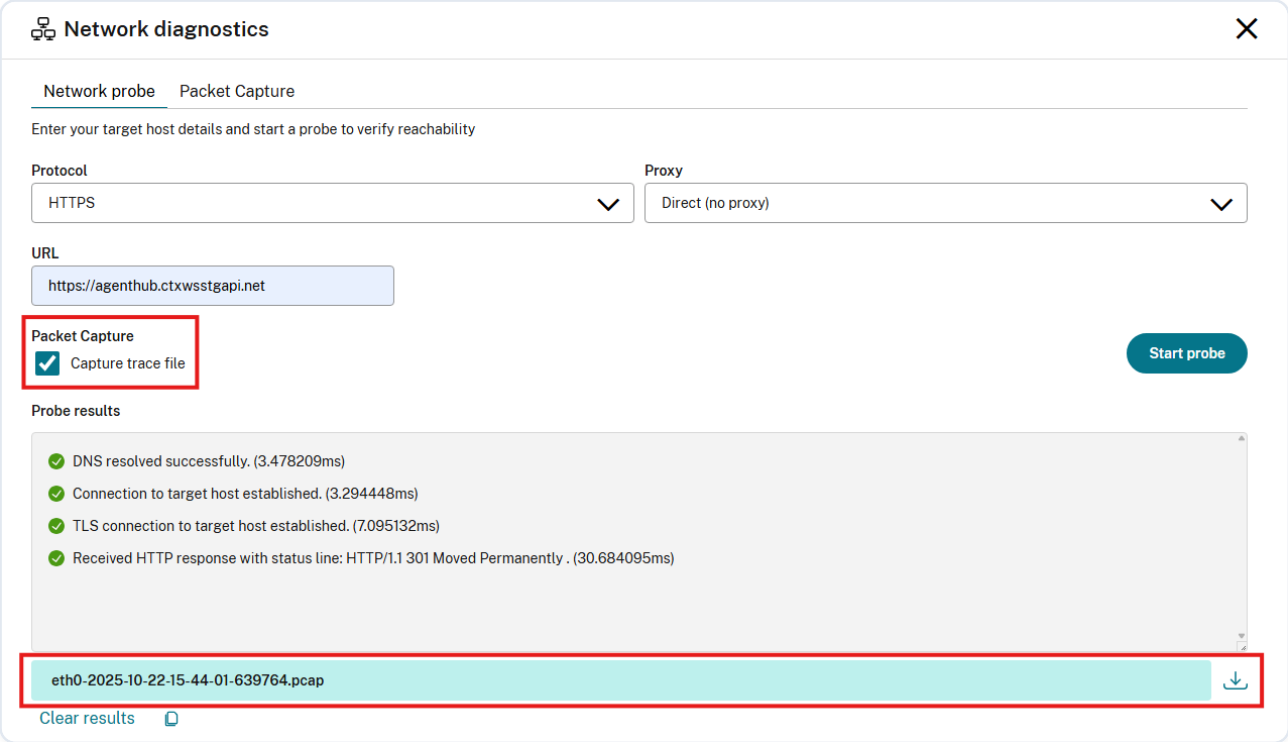
数据包捕获

勾选“**捕获跟踪文件**”复选框，可以在网络探测期间启用数据包跟踪。探测完成后，数据包捕获的链接将显示在探测的“**探测结果**”下。此数据包跟踪文件有助于进一步诊断网络探测结果。

注意：

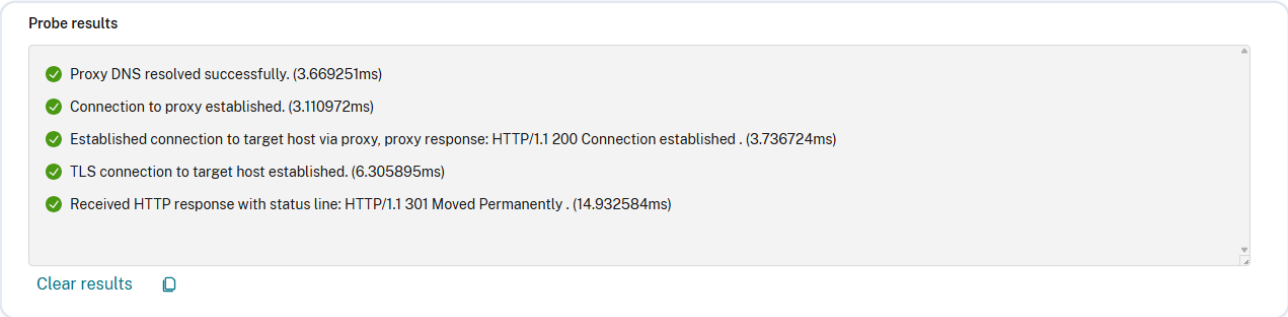
数据包跟踪捕获的是 Connector Appliance 在网络探测期间的所有流量，而不仅仅是网络探测本身的流量。这可能包括敏感数据或凭据。

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



网络探测结果

单击“**开始探测**”按钮后，“**探测结果**”框将显示网络探测的进度。将显示网络探测的每个步骤的信息，例如 DNS 解析、TCP 连接等。随着网络探测的进行，每个网络探测阶段旁边的图标将指示其是正在进行、已完成还是失败，并且将显示每个步骤的计时信息和错误详细信息。



解释基于 HTTP 的探测结果

只要从目标 URL 收到 HTTP 响应，HTTP 和 HTTPS 网络探测就会被标记为成功，无论返回的 HTTP 状态代码是什么。响应的 HTTP 状态行（包括 HTTP 响应状态代码）将显示在“**探测结果**”中。

当选择了代理时，纯 HTTP 网络探测也是如此。在这种情况下，所选代理将用作纯 HTTP 代理，并且只要代理返回 HTTP 响应，探测就会被视为成功。在 **探测结果** 中显示的带有错误状态码的 HTTP 状态行可能表示代理错误或目标 URL 错误。

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

连接器更新

Citrix® 会定期发布更新，以提高 Cloud Connector 或 Connector Appliance 的性能、安全性和可靠性。

当新的连接器版本可供 Citrix Cloud 租户使用时，默认行为是租户中的每个连接器立即以随机顺序逐个安装更新。如果任何连接器未能执行更新，它将阻止所有后续连接器开始更新。这是为了防止租户中的所有连接器都发生更新失败。一旦更新失败的连接器成功更新或被移除，后续连接器将立即继续其更新。有关详细信息，请参阅 故障排除更新失败

为确保及时安装更新，而不会过度影响用户的 Citrix Cloud™ 体验，您可以按如下方式控制连接器更新：

- 将更新的开始时间安排在首选的一天中的时间和一周中的首选日期。
- 执行一次性延迟，以便您指定的连接器在计划时间后两周更新。
- 如果更新因主机问题而失败，请在解决问题后重新启动更新。

此外，您可以通过将资源位置中的当前连接器版本与 Citrix Cloud 中的目标版本进行比较来验证您的连接器是否为最新版本。

注意：

本文介绍了如何使用 Citrix Cloud 管理控制台安排连接器更新。有关使用 Citrix Cloud API 配置连接器更新的首选时间和星期几的信息，请参阅 Citrix Developer 文档中的 Citrix Cloud - 维护计划。

首选时间

当您指定首选时间时，Citrix Cloud 会在更新可用 24 小时后，在您的首选时间开始安装更新。例如，如果您的首选时间是美国太平洋时间凌晨 2:00，并且更新在星期二可用，Citrix Cloud 会等待 24 小时，然后在第二天凌晨 2:00 开始安装更新。

首选星期几

当您指定首选星期几时，Citrix Cloud 会等待七天，然后才在您的首选日期开始安装更新。这个七天的等待期为您提供了足够的时间来选择是按需安装更新，还是等待 Citrix Cloud 在您的首选日期开始安装。根据您选择的星期几和更新可用的日期，Citrix Cloud 最多可能需要等待 13 天才能开始安装更新。

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

8 天等待期示例

在周一，您将周二下午 6:00 配置为首选更新日期。当天晚些时候，Citrix Cloud 会通知您有可用更新，并显示**更新**按钮。如果您未启动更新，Citrix Cloud 将等待七天，然后在第二天（即周二下午 6:00）开始安装更新。

13 天等待期的示例

您将周一晚上 6:00 配置为首选更新时间。在周二，Citrix Cloud 会通知您有可用更新，并显示**更新**按钮。如果您未启动更新，Citrix Cloud 将等待七天，然后在六天后（即周一晚上 6:00）开始安装更新。

注意：

更新计划指示连接器开始尝试更新的时间。由于更新是逐个安装在每个连接器上的，因此实际更新可能会晚于计划时间。例如，如果资源位置中第一个要更新的连接器在更新过程中遇到问题，导致更新需要 4 小时才能完成，则资源位置中的后续连接器将不会在计划时间后至少 4 小时内开始更新。

由于此行为，在重新启动失败连接器上的更新或从 Citrix Cloud 中移除已失败更新的连接器之前，请务必注意，其余连接器可能会立即启动更新，并且此更新可能在工作时间发生。

更新通知和按需更新

当有可用更新时，Citrix Cloud 会通过您的通知中的警报通知您。此外，每个连接器都会显示更新的安装日期和时间。

在 Citrix Cloud 通知您有可用更新后，每个连接器都会显示一个**更新**按钮，以便您可以比首选时间或日期更早地安装更新。在您为每个连接器选择**更新**后，Citrix Cloud 会将更新排队并逐个安装。启动更新后，您无法取消更新。

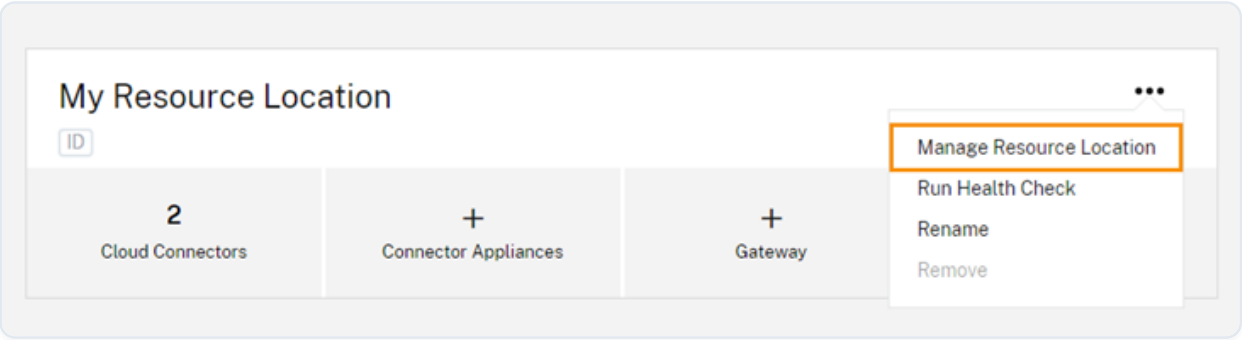
更新完成后，Citrix Cloud 会显示上次更新的日期。如果某些更新无法完成，则会发送通知告知您。

选择更新计划

使用本节中的步骤通过 Citrix Cloud 管理控制台安排连接器更新。有关使用 Citrix Cloud API 安排更新的信息，请参阅 Citrix Developer 文档中的Citrix Cloud - 维护计划。

1. 从 Citrix Cloud 菜单中，选择**资源位置**。
2. 找到要修改的资源位置，然后从省略号菜单中选择**管理资源位置**。

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



3. 在“**选择您的更新方法**”下，选择“**设置维护开始时间**”，然后选择安装更新的首选日期、时间及时间区域。

   - 要仅指定首选时间，请选择您希望安装更新的小时和时区。Citrix Cloud 会在更新可用 24 小时后，在您首选的时间安装更新。
   - 要指定首选星期几，请选择小时、日期和时区。Citrix Cloud 会在更新可用七天后，在您首选的日期安装更新。

配置更新计划后，Citrix Cloud 会在资源位置名称旁边显示该计划。

突出显示更新计划的资源位置(/en-us/citrix-cloud/media/connector-update-schedule.png)

您选择的开始时间将应用于所有连接器，无论它们位于哪个时区。如果您在不同的时区有连接器，Citrix Cloud 会在您选择的时间和时区安装更新。例如，如果您将更新安排在美国太平洋时区凌晨 2:00，并且您在伦敦有连接器，Citrix Cloud 将在太平洋时间凌晨 2:00 开始在这些连接器上安装更新。

注意：

更新计划指示连接器将开始尝试更新的时间。由于更新是逐个连接器安装的，因此实际更新可能会晚于计划时间。例如，如果资源位置中第一个要更新的连接器在更新期间遇到问题，导致更新需要 4 小时才能完成，则资源位置中的后续连接器将不会在计划时间后至少 4 小时内开始更新。

由于此行为，在重新启动失败连接器上的更新或从 Citrix Cloud 中删除已失败更新的连接器之前，请务必注意，其余连接器可能会立即启动更新，并且此更新可能会在工作时间发生。

重新启动更新

如果连接器在更新安装期间遇到问题，安装将暂停，直到问题解决。由于更新是逐个连接器安装的，因此一个连接器上暂停的更新可能会阻止 Citrix Cloud 帐户中所有剩余的 Cloud Connector 进行更新。问题解决后，您可以重新启动更新。

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

1. 从 Citrix Cloud 菜单中，选择“**资源位置**”。
2. 找到要管理的资源位置，然后选择“**Cloud Connector**”或“**Connector Appliance**”磁贴。
3. 找到要管理的连接器，然后选择“**重新启动更新**”。

   突出显示“重新启动更新”的连接器磁贴(/en-us/citrix-cloud/media/connector-update-restart-button.png)

延迟更新

您可以将计划更新延迟两周，使其在您指定的连接器上发生。您只能延迟一次计划更新。延迟更新一次后，您不能再次延迟。此外，您不能更改默认的两周期限。

1. 在 Citrix Cloud 菜单中，选择 **资源位置**。
2. 找到要管理的资源位置，然后选择 **Cloud Connectors** 或 **Connector Appliances** 磁贴。
3. 找到要管理的连接器，然后选择 **延迟更新**。

   突出显示了“延迟更新”按钮的连接器磁贴(/en-us/citrix-cloud/media/connector-update-delay-button.png)

   计划日期将更改为比原定计划日期晚两周的日期。

未计划的更新

即使您将更新安排在以后的日期和时间，Citrix Cloud 仍可能在更新可用后尽快安装。未计划的更新在以下情况下发生：

- 更新在其可用后的 48 小时内无法在首选时间安装。例如，如果您的首选时间是凌晨 2:00，并且连接器在更新发布后离线三天，则当连接器重新联机时，Citrix Cloud 会立即安装更新。
- 更新包含针对关键安全或功能问题的修复。

比较 Cloud Connector 版本

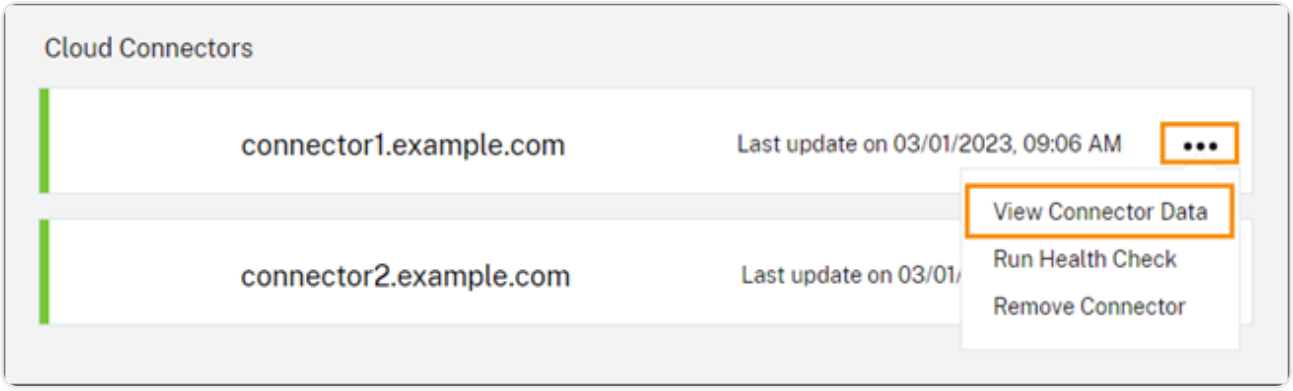
您可以检查您的资源位置中运行的 Cloud Connector 版本以及它是否是最新版本。此信息可帮助您验证 Cloud Connector 是否成功更新。

注意：

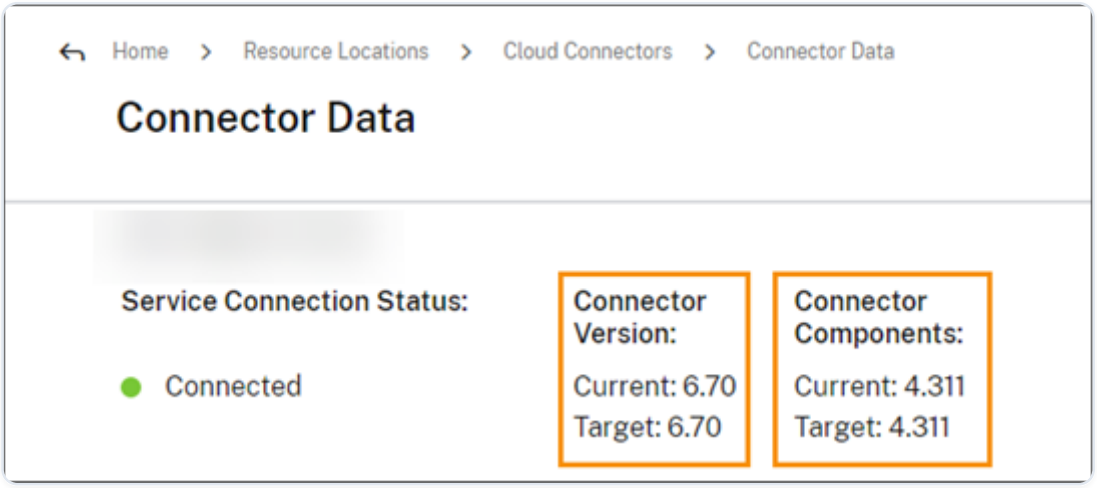
此信息不适用于 Connector Appliances。

从“**资源位置**”页面，选择要管理的资源位置的“**云连接器**”磁贴。找到要检查的云连接器，然后从省略号菜单中选择“**查看连接器数据**”。

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



“**当前**”版本号是云连接器计算机上当前运行的云连接器软件的版本。“**目标**”版本号是 Citrix 发布的最新云连接器软件版本。如果计算机已成功更新，则当前版本号和目标版本号将匹配。



解决更新失败问题

云连接器计算机上安装的冲突软件或维护期间发生的意外错误可能导致云连接器更新失败和服务中断。有关在云连接器维护后处理更新失败的信息，请访问 解决云连接器维护失败问题。

如果云连接器未成功更新，您可以通过验证以下条件来开始排查问题：

- 云连接器已开机并使用 云连接器高级连接检查 连接到 Citrix Cloud。
- 代理和防火墙配置正确。
- 所需的 Windows 服务处于“已启动”状态。
- 云连接器上已启用高级日志记录。

有关排查云连接器更新失败的说明，请参阅 Citrix 支持知识中心中的 CTX270718。

如需故障排除协助，您可以将 Citrix Cloud Connector 日志发送给 Citrix。有关详细信息，请参阅 Citrix Cloud Connector 日志收集。

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

身份和访问管理

身份和访问管理定义了用于 Citrix Cloud™ 管理员和最终用户的身份提供程序和帐户。

身份提供程序

Citrix Cloud 支持的身份提供程序可用于验证 Citrix Cloud 管理员、最终用户或两者。

身份提供程序	管理员身份验证	最终用户身份验证
Citrix® 身份提供程序	是	否
本地活动目录	否	是
Active Directory 加令牌	否	是
微软 Entra ID	是	是
思杰网关	否	是
谷歌云身份	是	是
奥克塔	否	是
SAML 2.0	是	是

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。Citrix 身份提供程序仅对 Citrix Cloud 管理员进行身份验证。

Citrix 身份提供程序

Citrix Cloud 包含内置的 Citrix 身份提供程序，用于在管理员登录时对其进行身份验证。在 Citrix Cloud 控制台中，Citrix 身份提供程序标记为 Citrix Identity。 如果您使用不同的身份提供程序进行管理员身份验证，Citrix 建议在 **Citrix 身份提供程序**下至少有一个完全访问权限的管理员。此条件可确保：

- 如果您的主身份提供程序不可用，您将不会被锁定在 Citrix Cloud 帐户之外。

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

- 您可以访问您的 Citrix Cloud 帐户，以执行在其他身份提供程序（例如 Microsoft Entra ID）下登录时无法完成的某些操作。例如，如果 Microsoft Entra ID 是您选择的身份提供程序，并且您需要重新初始化 Microsoft Entra ID 与 Citrix Cloud 之间的连接，则可以在使用 Citrix 身份提供程序登录后执行此任务。

删除 Citrix 身份提供程序

对于所有新的 Citrix Cloud 帐户，Citrix 身份提供程序默认处于连接状态。如果您选择不使用 Citrix 身份提供程序，则可以在需要时删除连接。例如，您可能选择删除此连接以符合您组织的安全和管理员管理策略。

删除此连接会禁用 Citrix 身份提供程序，因此无法用于对 Citrix Cloud 管理员进行身份验证。

在删除 Citrix 身份提供程序连接之前，您必须在 Citrix Cloud 中配置另一个身份提供程序。如果没有其他已配置的身份提供程序，Citrix Cloud 不允许您删除此连接。

重要

如果您无法访问所选的身份提供程序，您必须联系 Citrix 支持部门以恢复您的 Citrix Cloud 帐户。此过程可能需要几天才能完成。

要删除 Citrix 身份提供程序连接：

1. 在 Citrix Cloud 菜单中，选择 **身份和访问管理**。
2. 在 **身份验证** 选项卡上，找到 Citrix 身份提供程序。
3. 单击省略号菜单并选择 **删除身份提供程序**。

4. 当系统提示确认删除时，选择 **我了解删除此身份提供程序也会删除 Citrix Cloud 中此身份提供程序的配置数据**。
5. 单击 **删除身份提供程序**。

Citrix 联邦身份验证服务

Citrix Cloud 还支持使用 Citrix 联邦身份验证服务为最终用户提供单点登录访问。有关详细信息，请参阅以下文章：

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

- 将 FAS 连接到 Citrix Cloud：为使用 Citrix 联邦身份验证服务的应用商店启用单点登录
- Citrix 技术专区：
  - 参考体系结构：联邦身份验证服务
  - 技术洞察：联邦身份验证服务

管理员

管理员使用其身份访问 Citrix Cloud、执行管理活动以及安装 Citrix Cloud Connector。

Citrix 身份机制使用电子邮件地址和密码为管理员提供身份验证。管理员还可以使用其 My Citrix 凭据登录 Citrix Cloud。

多重身份验证

Citrix Cloud 为管理员和最终用户提供多重身份验证方法。

对于管理员，登录 Citrix Cloud 时需要多重身份验证。管理员可以在加入其 Citrix Cloud 帐户时或接受其他管理员的邀请后注册其设备。有关更多信息，请参阅以下文章：

- 设置多重身份验证
- 管理您的主要 MFA 方法
- 管理您的 MFA 恢复方法

对于最终用户，当管理员配置 Active Directory 加令牌身份验证方法时，将启用多重身份验证。Active Directory 加令牌是 Citrix® StoreFront Cloud 的默认身份提供程序。配置后，最终用户为其设备注册多重身份验证。有关更多信息，请参阅以下文章：

- 启用 Active Directory 加令牌身份验证
- 注册设备以进行双因素身份验证
- 重新注册设备

或者，您可以将 Microsoft Entra ID 多重身份验证用于 Citrix Cloud 管理员和最终用户。有关部署方法的更多信息，请参阅Microsoft Azure MFA 部署方法。

添加新管理员

在帐户加入过程中，会创建一个初始管理员。作为初始管理员，您可以将其他管理员添加到您的 Citrix Cloud 帐户。这些新管理员可以使用其现有的 Citrix 帐户凭据，或者在需要时设置新帐户。您

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

还可以微调所添加管理员的访问权限。设置这些权限可让您根据管理员在组织中的角色调整访问级别。

有关添加管理员和设置访问权限的更多信息，请参阅管理管理员访问权限。

重置密码

如果您忘记或想要重置密码，请在 Citrix Cloud 登录页面上单击**忘记您的用户名或密码？**。输入您的电子邮件地址或用户名以查找您的帐户后，Citrix 会向您发送一封包含重置密码链接的电子邮件。

Citrix 要求您在某些条件下重置密码，以帮助您确保帐户密码的安全。有关这些条件的更多信息，请参阅更改密码。

注意：

将 mailto:customerservice@citrix.com 添加到您的允许电子邮件地址列表中，以确保 Citrix Cloud 电子邮件不会进入您的垃圾邮件或废纸篓文件夹。

删除管理员

您可以在“**管理员**”选项卡上从您的 Citrix Cloud 帐户中删除管理员。删除管理员后，他们将无法再登录 Citrix Cloud。

如果管理员在您删除帐户时已登录，则该管理员最多保持活动状态一分钟。之后，将拒绝访问 Citrix Cloud。

注意：

- 如果帐户中只有一个管理员，则无法删除该管理员。Citrix Cloud 要求每个客户帐户至少有一名管理员。
- Citrix Cloud Connectors 不与管理员帐户关联。因此，即使您删除了安装它们的管理员，Cloud Connectors 也会继续运行。

最终用户

最终用户的身份定义了他们在 Citrix Cloud 中有权访问的服务。此身份来自资源位置内域提供的 Active Directory 域帐户。将最终用户分配给 Library 产品授权最终用户访问该产品。

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

管理员可以在“**域**”选项卡上控制用于提供这些身份的域。如果您计划使用来自多个林的域，请在每个林中安装至少两个 Citrix Cloud Connectors。Citrix 建议至少使用两个 Citrix Cloud Connectors 以维护高可用性环境。有关在 Active Directory 中部署 Cloud Connectors 的更多信息，请参阅在 Active Directory 中部署 Cloud Connectors 的方案。

注意：

- 禁用域仅阻止选择新身份。它不会阻止最终用户使用已分配的身份。
- 每个 Citrix Cloud Connector 都可以枚举和使用其安装所在单个林中的所有域。

管理最终用户使用情况

您可以使用个人帐户或 Active Directory 组将最终用户添加到产品/服务中。使用 Active Directory 组后，无需通过 Citrix Cloud 进行管理，即可将该组分配给产品/服务。

当管理员从产品/服务中删除单个最终用户或最终用户组时，这些最终用户将无法再访问该服务。有关从特定服务中删除最终用户的更多信息，请参阅 Citrix 产品文档 网站上的服务文档。

主要资源位置

主要资源位置是您指定为您的域与 Citrix Cloud 之间通信“最优先”的资源位置。对于您的主要资源位置，请选择具有 Citrix Cloud Connector 且与您的域具有最佳性能和连接性的资源位置。将此资源位置设为您的主要资源位置可让您的用户快速登录 Citrix Cloud。

有关详细信息，请参阅 选择主要资源位置。

更多信息

- 通过 Citrix 培训网站上的 Citrix 身份和身份验证简介 培训课程，了解有关受支持的身份提供程序的更多信息。
- 思杰技术专区：
  - 技术简报：Workspace 身份
  - 技术简报：Workspace 单点登录
  - 技术洞察：移动 SSO

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

管理管理员对 Citrix Cloud 的访问

管理员通过 Citrix Cloud 控制台进行管理。根据您用于验证管理员身份的身份提供程序，您可以单独添加管理员或使用组添加管理员。

所有管理员在登录 Citrix Cloud 时都必须使用令牌作为第二重身份验证因素。添加管理员后，他们可以将设备注册到多重身份验证中，并使用任何遵循 基于时间的一次性密码 标准的应用程序（例如 Citrix SSO）生成令牌。

添加新管理员

Citrix Cloud 支持以下身份提供程序用于验证管理员身份：

- Citrix 身份提供程序：Citrix Cloud 中的默认身份提供程序。仅支持添加单个管理员。
- Microsoft Entra ID：支持单独添加管理员以及通过 ME-ID 组添加管理员。有关详细信息，请参阅 (/zh-cn/citrix-cloud/citrix-cloud-management/identity-access-management/administrator-groups.html)。
- SAML 2.0：支持单独添加管理员以及通过 AD 组添加管理员。有关详细信息，请参阅 (/zh-cn/citrix-cloud/citrix-cloud-management/identity-access-management/saml-identity.html)
- Google：支持单独添加管理员以及通过 Google 组添加管理员。有关详细信息，请参阅 (/zh-cn/citrix-cloud/citrix-cloud-management/identity-access-management/google-identity)

添加新管理员使用以下工作流程：

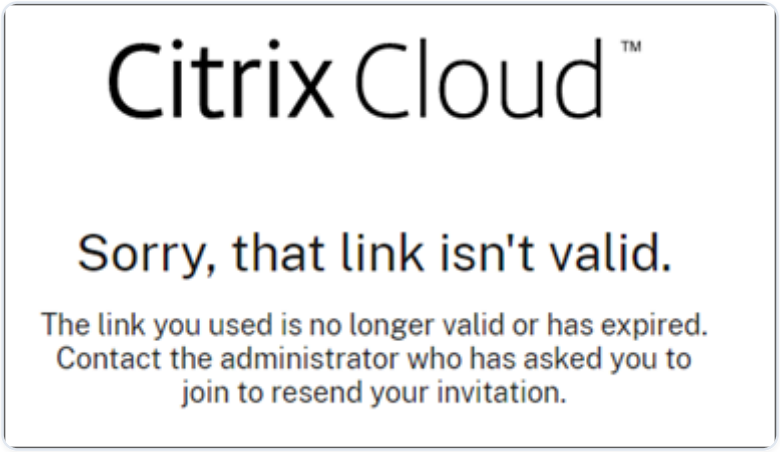
1. 选择您要用于验证管理员身份的身份提供程序。
2. 根据身份提供程序，邀请单个管理员或选择管理员所属的组。
3. 指定与管理员在组织中的角色相符的访问权限。有关详细信息，请参阅本文中的 (#modify-administrator-permissions)。

邀请单个管理员

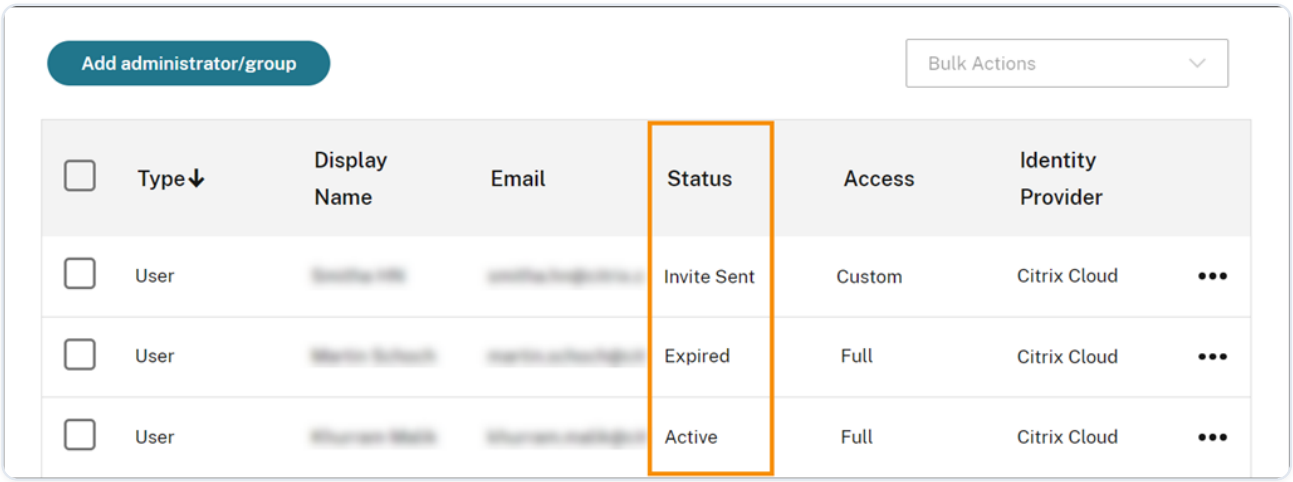
添加单个管理员需要邀请他们加入您的 Citrix Cloud 帐户。当您添加管理员时，Citrix 会向他们发送一封邀请电子邮件。管理员必须接受邀请才能登录。通过组添加的管理员不会收到邀请，并且在您添加他们后可以立即登录。

邀请电子邮件从 `cloud@citrix.com` 发送，并说明如何访问帐户。邀请自发送之日起连续五天有效。五天后，邀请链接将过期。如果受邀管理员使用过期链接，Citrix Cloud 将显示一条消息，指示该链接无效。

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



Citrix Cloud 还会显示邀请状态，以便您查看管理员是否已接受邀请并登录到 Citrix Cloud。



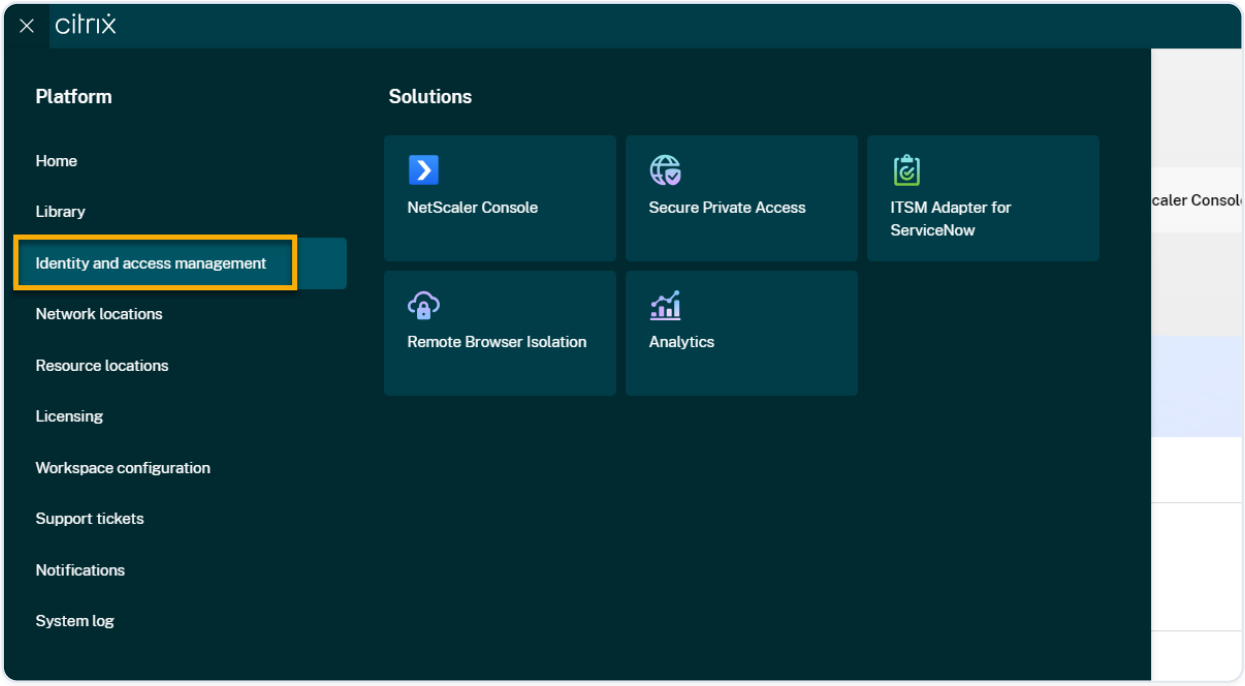
注意

管理员帐户最多可与 100 个客户帐户关联。如果管理员需要管理 100 多个客户帐户，则必须使用不同的电子邮件地址创建单独的管理员帐户来管理其他客户。或者，您可以将管理员从他们不再需要管理的客户帐户中删除。

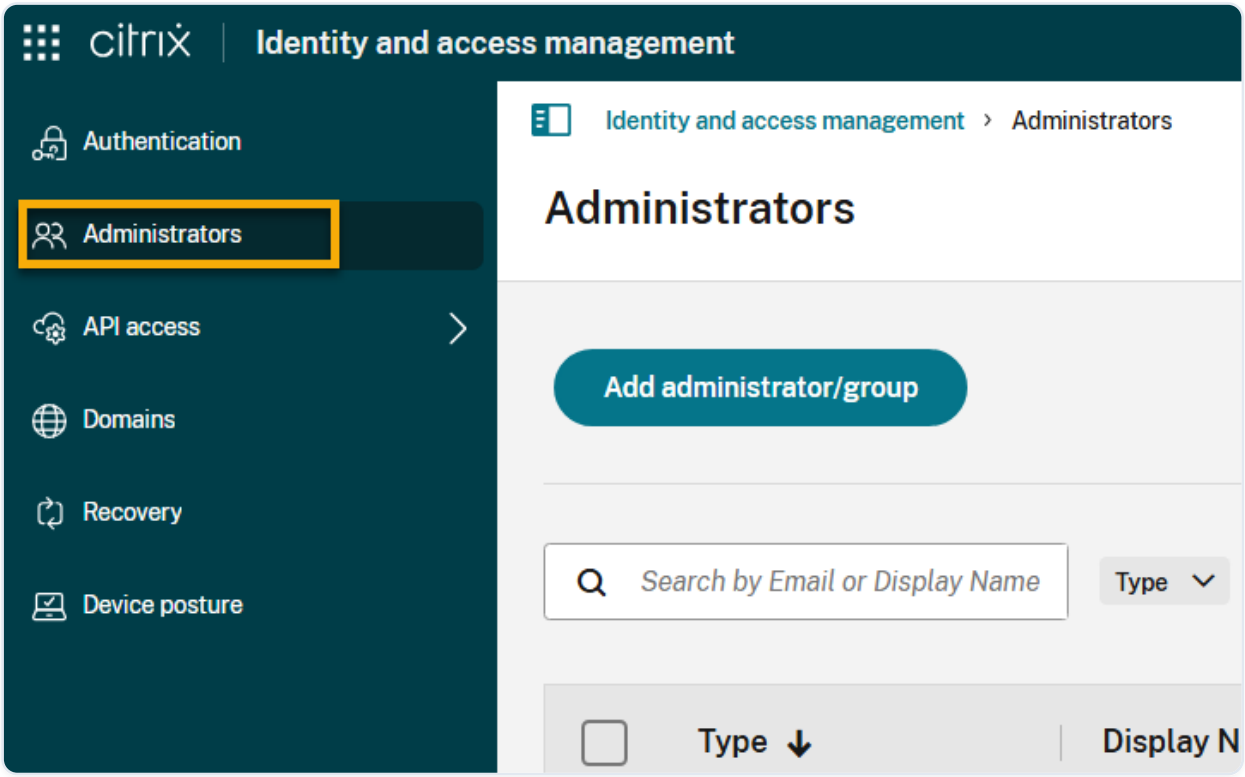
邀请管理员

1. 登录到 Citrix Cloud，然后从菜单中选择 **身份和访问管理**。

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



2. 在 **身份和访问管理** 页面上，选择 **管理员**。控制台显示帐户中的所有当前管理员。



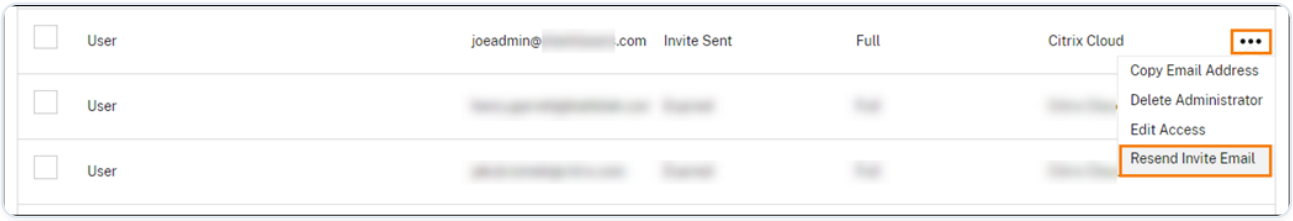
3. 选择 **添加管理员/组**。
4. 在 **管理员详细信息** 中，选择要使用的身份提供程序。如果使用 Microsoft Entra ID，Citrix Cloud 可能会提示您先登录。
5. 如果选择了 **Citrix Identity**，请输入用户的电子邮件地址，然后选择 **下一步**。
6. 如果选择了 **Microsoft Entra ID**，请键入要添加的用户的名称，然后单击 **下一步**。不支持邀请 ME-ID 访客用户。

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

7. 在“**设置访问权限**”中，配置管理员的相应权限。“**完全访问权限**”（默认选中）允许控制所有 Citrix Cloud 功能和订阅服务。“**自定义访问权限**”允许控制您选择的功能和服务。
8. 查看管理员详细信息。选择“**返回**”以进行任何更改。
9. 选择“**发送邀请**”。Citrix Cloud 会向您指定的用户发送邀请，并将管理员添加到列表中。

重新发送邀请

要重新发送邀请，请从控制台最右侧的省略号菜单中选择“**重新发送邀请电子邮件**”。重新发送邀请不会影响邀请过期前的五天时间限制。



使用新的登录链接重新发送邀请

如果原始邀请电子邮件过期，您可以向管理员发送一封新邮件。执行以下步骤：

1. 从 Citrix Cloud 中删除管理员：在“**管理员**”页面上，在列表中找到该管理员，然后从省略号菜单中选择“**删除管理员**”。
2. 等待几分钟，确保 Citrix Cloud 完成删除。在某些情况下，删除后立即再次邀请管理员可能会导致发送带有故障登录链接的邀请。
3. 再次邀请管理员，如 邀请管理员 中所述。

接受管理员邀请

如果您受邀加入 Citrix Cloud 帐户，Citrix 会向您发送一封电子邮件，其中包含该帐户的组织 ID 和客户名称。

要接受邀请，请单击“**登录**”。之后，将打开一个浏览器窗口。如果您还没有 Citrix Cloud 帐户，浏览器会显示一个页面，您可以在其中创建密码。如果您已有帐户，Citrix Cloud 会提示您使用现有密码登录。

登录期间，系统可能会提示您注册多重身份验证。有关注册说明，请参阅 设置多重身份验证。

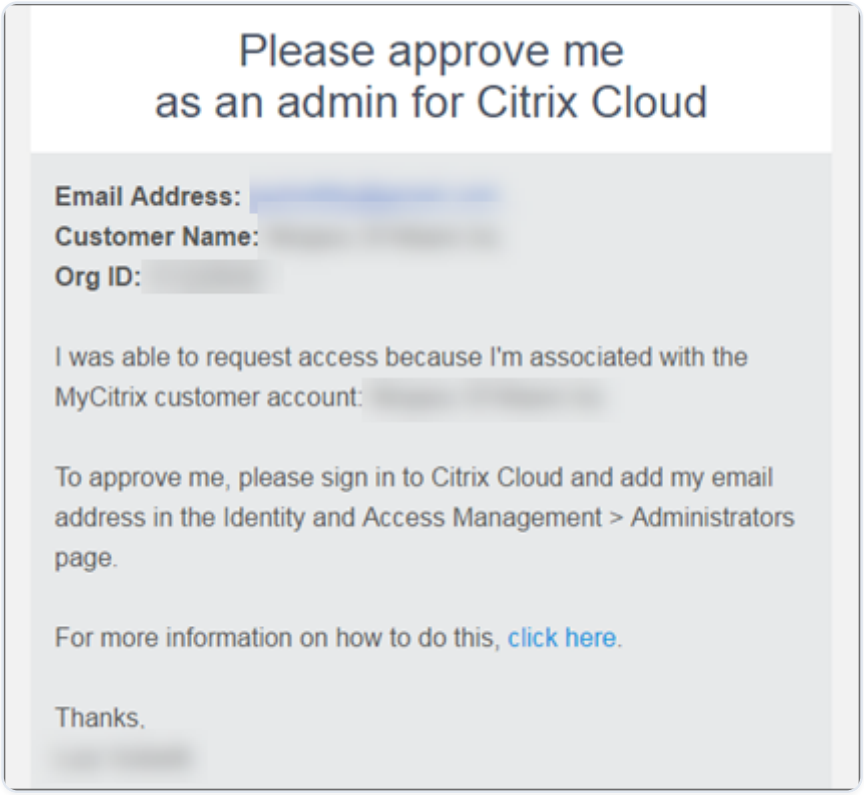
添加管理员组

您可以使用 AD 组（用于 SAML 身份验证）、Microsoft Entra ID 组（用于 Microsoft Entra ID 身份验证）或 Google 组（用于 Google 身份验证）添加管理员。有关详细信息，请参阅管理管理员组。

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

批准加入 Citrix Cloud 的请求

您可能会不时收到来自 Citrix Cloud 的批准请求，该请求代表您组织中希望以管理员身份加入您的 Citrix Cloud 帐户的某人。


Please approve me
as an admin for Citrix Cloud

Email Address:
Customer Name:
Org ID:

I was able to request access because I'm associated with the MyCitrix customer account:

To approve me, please sign in to Citrix Cloud and add my email address in the Identity and Access Management > Administrators page.

For more information on how to do this, click here.

Thanks,

要批准这些请求，您需要邀请请求访问的人员成为管理员，如本文中的邀请个人管理员所述。您必须使用批准请求电子邮件中显示的相同电子邮件地址。

收到邀请后，请求访问的人员会单击“**登录**”链接以接受邀请。然后，该人员可以为 Citrix Cloud 创建密码并登录到您的帐户。

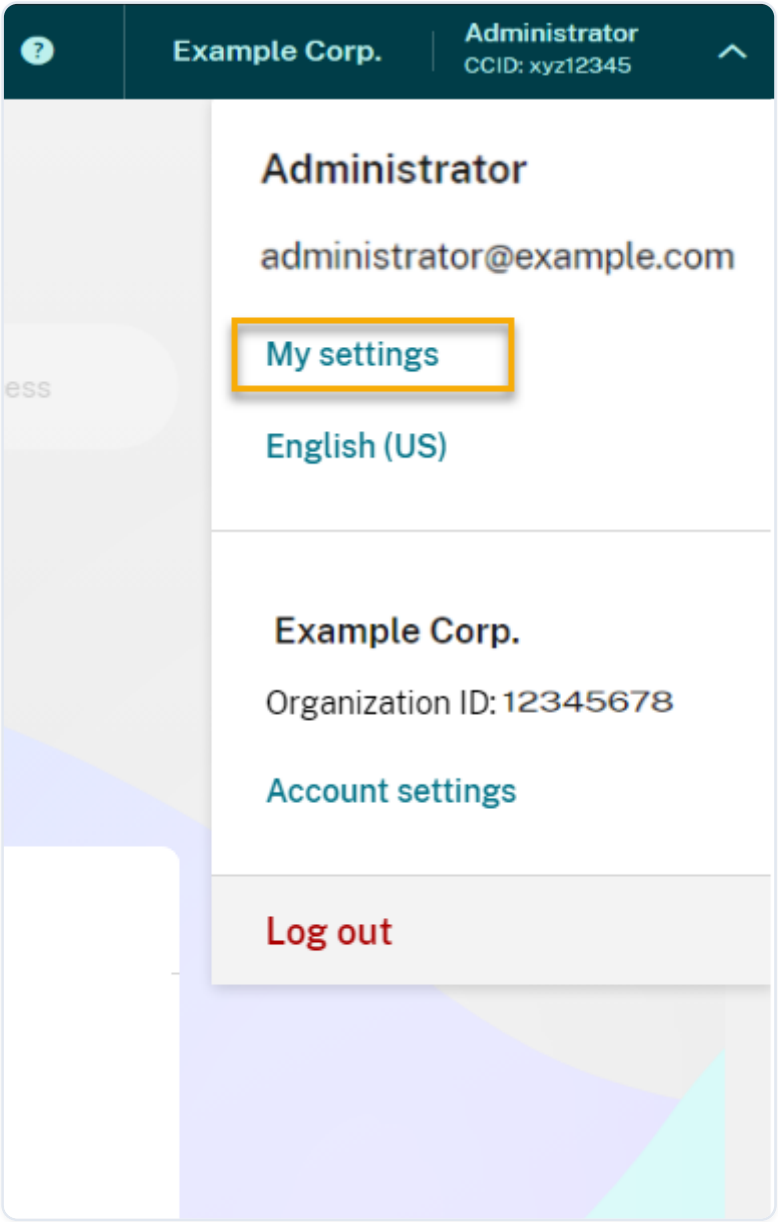
有关如何生成批准请求的更多信息，请参阅如果帐户已在使用中会发生什么？。

更改您的电子邮件地址

您可以在 Citrix Cloud 中更改自己的电子邮件地址。您的新地址必须与您的多重身份验证 (MFA) 恢复电子邮件地址不同。更改电子邮件地址时，Citrix Cloud 会向新地址发送验证电子邮件。验证后，Citrix Cloud 会将您注销，以便完成更改。几分钟后，您可以使用新电子邮件地址再次登录。

1. 从右上角菜单中，选择“**我的设置**”。

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



2. 在“**电子邮件地址**”中，选择“**更改电子邮件**”。
3. 输入新的电子邮件地址，然后选择“**发送验证电子邮件**”。
4. 输入电子邮件中的 6 位验证码，然后选择“**验证并完成**”。
5. 选择 **是，更改我的电子邮件地址** 以确认更改。

确认更改后，Citrix Cloud 会将您注销。几分钟后，您可以使用新的电子邮件地址再次登录。

修改管理员权限

When you add administrators to your Citrix Cloud account, you define the administrator permissions that are appropriate for their role in your organization. By default, new administrators are assigned *full access permissions* to all Citrix Cloud account functions and available services. If

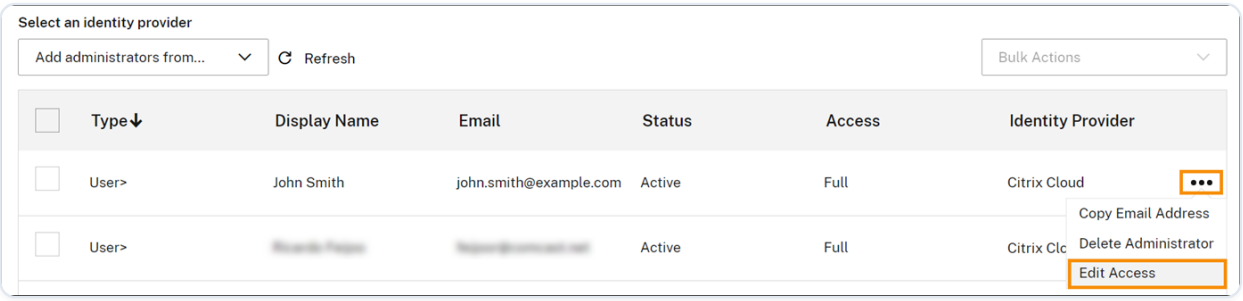
© 1997–2026 Citrix Systems, Inc. All rights reserved.

you want to limit access to certain areas of the management console or specific services, you can define *custom access permissions*.

只有具有完全访问权限的 Citrix Cloud 管理员才能为其他管理员定义权限。

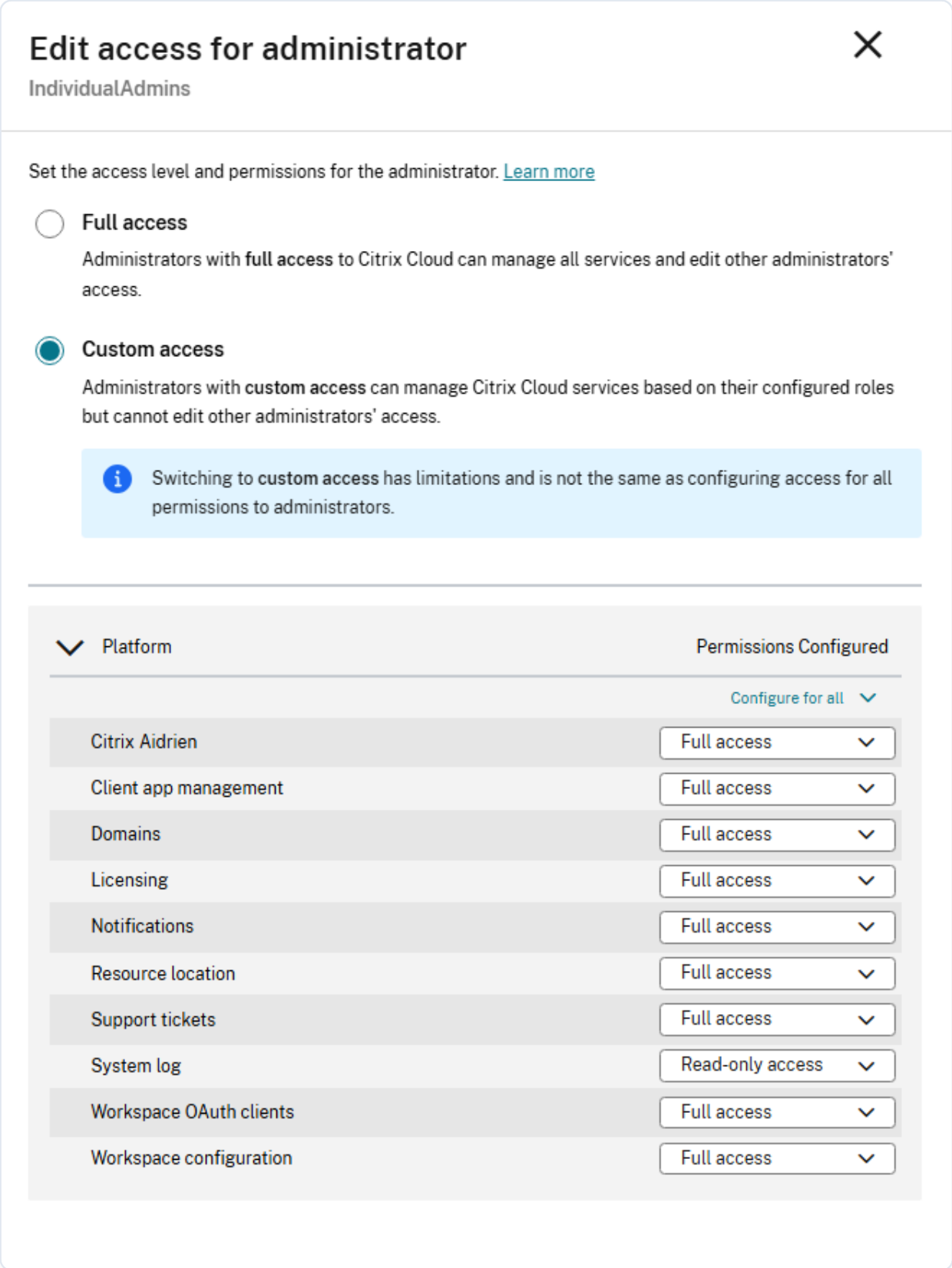
要更改现有管理员权限：

1. 登录 Citrix Cloud：https://citrix.cloud.com。
2. 从 Citrix Cloud 菜单中，选择 **身份和访问管理**，然后选择 **管理员**。
3. 选择要管理的身份提供程序：Citrix Identity（默认）、Active Directory（如果使用 SAML 作为身份提供程序）或 Microsoft Entra ID（如果已连接）。
4. 找到要管理的管理员或组，单击省略号按钮，然后选择 **编辑访问权限**。



5. 要允许或禁止特定权限，请选择 **自定义访问权限**。要允许访问所有 Citrix Cloud 功能，请选择 **完全访问权限**。
6. 要快速查找服务权限，请在搜索框中开始键入。Citrix Cloud 会在您键入时显示匹配的权限。例如，如果您开始键入“read only”，则会显示标题中包含“read only”的权限。权限搜索不区分大小写。
7. 要为 Citrix Cloud 管理控制台定义自定义访问权限，请展开 **常规**。

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



8. 要为特定服务定义自定义访问权限，请展开该服务。
9. 对于每个权限，根据需要选中或清除复选标记。
10. 选择 **保存**。

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

控制台权限

本节介绍 Citrix Cloud 管理控制台可用的自定义访问权限。有关特定服务的自定义访问权限的更多信息，请查阅该服务的文档。大多数平台角色支持**只读**访问，但某些角色仅限于**只读**或**完全访问**（见下文）：

- **客户控制板：** 仅适用于 Citrix 服务提供商 (CSP)。授予对 客户控制板 的查看权限。（仅限只读）
- **域：** 授予对 **身份和访问管理 > 域** 选项卡的访问权限。管理员可以通过从此选项卡下载 Citrix Cloud Connector™ 软件并将其安装到域中的服务器上来添加 Active Directory 域。
- **许可：** 授予对 **许可** 控制台页面的 **云服务** 和 **许可部署** 选项卡的访问权限。（仅限只读）
- **通知：** 授予对 **通知** 控制台页面的访问权限。管理员可以查看和关闭 Citrix Cloud 通知。
- **资源位置：** 授予对 **资源位置** 控制台页面的访问权限。管理员可以添加新的资源位置并添加用于单点登录的 FAS 服务器。他们还可以管理连接器更新。
- **支持票证：** 授予对 **支持票证** 控制台菜单选项和 **打开票证** 帮助菜单选项的访问权限。选择其中任一选项会将管理员发送到 我的支持 门户。有关详细信息，请参阅 技术支持。（仅限完全访问）
- **系统日志：** 授予对 **系统日志** 控制台页面的访问权限。管理员可以查看系统日志事件 并将事件导出到 CSV 文件。（仅限只读）
- **StoreFront Cloud：** 授予对 **StoreFront Cloud** 控制台页面的访问权限。管理员可以更改身份验证方法、自定义应用商店外观和行为、启用和禁用服务以及配置站点聚合。有关详细信息，请参阅 Citrix® StoreFront Cloud 产品文档。（仅限完全访问）
- **应用商店 OAuth 客户端（预览版）：** 授予对 **身份和访问管理 > API 访问 > 应用商店 API** 选项卡的访问权限。管理员可以创建和管理自己的 OAuth 客户端，以与 StoreFront Cloud 平台 API 交互。OAuth 客户端专门用于应用商店 API，并包含创建自动过期私有客户端的选项。

注意：

建议谨慎分配 **Store OAuth clients** 自定义角色。与此角色关联的访问权限可能允许管理员访问商店平台上的最终用户资源（VDA 或应用程序）。同样重要的是要注意，具有 **完全访问权限** 的管理员将自动拥有与具有 **Store OAuth clients** 权限的管理员等效的访问权限。

管理您的主要 MFA 方法

要使用多重身份验证 (MFA) 登录 Citrix Cloud，您可以使用身份验证器应用程序或您的电子邮件地址。本节介绍如何更改 MFA 的设备注册或切换到不同的 MFA 方法。

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

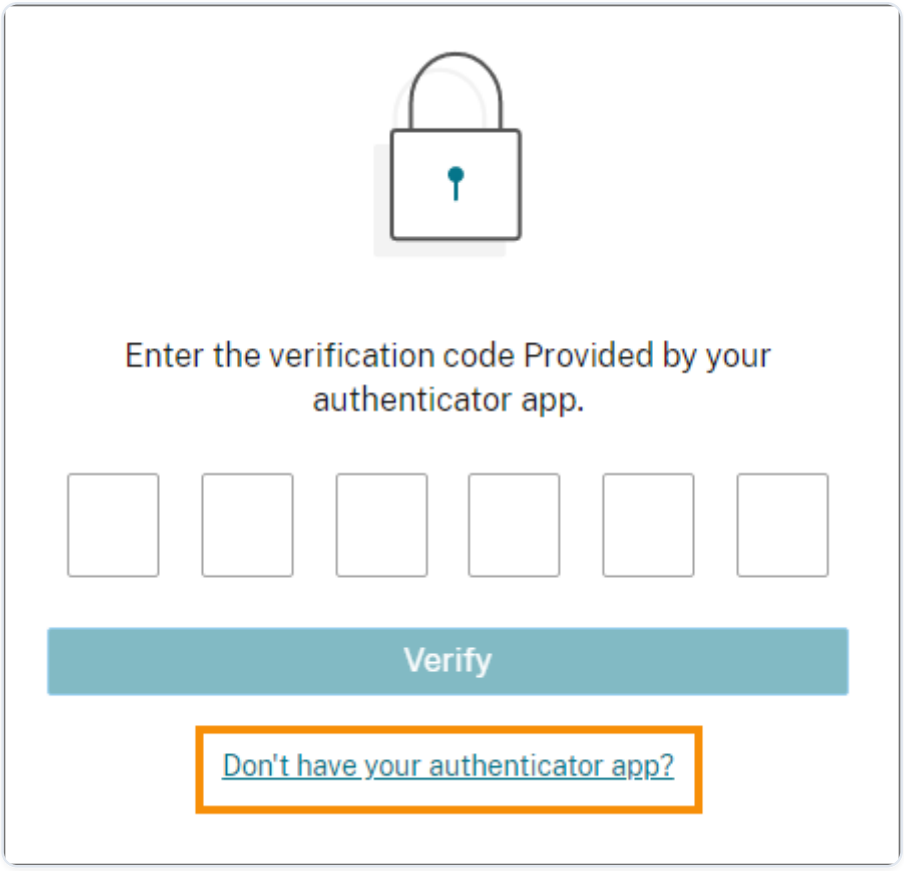
更改 MFA 设备

如果您丢失了已注册的设备、想在 Citrix Cloud 中使用其他设备或重置身份验证器应用程序，您可以重新注册 Citrix Cloud MFA。

注意

- 更改设备会删除当前设备注册并生成新的身份验证器应用程序密钥。
- 如果您使用与原始注册相同的身份验证器应用程序重新注册，请在重新注册之前从身份验证器应用程序中删除 Citrix Cloud 条目。完成重新注册后，此条目中显示的代码将不再有效。如果您在重新注册之前或之后未删除此条目，您的身份验证器应用程序将显示两个具有不同代码的 Citrix Cloud 条目，这可能会在登录 Citrix Cloud 时造成混淆。
- 如果您正在使用新设备重新注册但没有身份验证器应用程序，请从设备的应用程序商店下载并安装一个。为了获得更流畅的体验，Citrix 建议您在重新注册设备之前安装身份验证器应用程序。

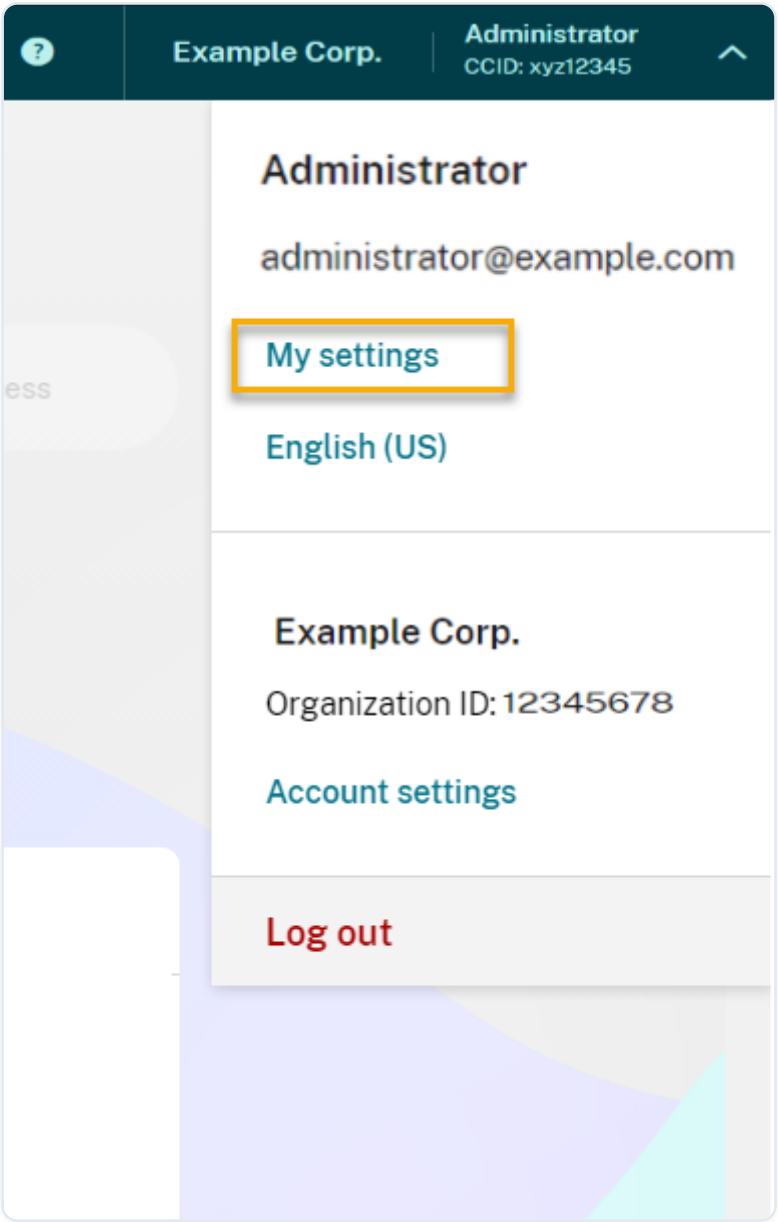
1. 登录 Citrix Cloud 并输入身份验证器应用程序中的代码。



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

如果您没有身份验证器应用程序，请单击 **没有您的身份验证器应用程序？** 并选择一种恢复方法以帮助您登录。根据所选的恢复方法，输入您收到的恢复代码或未使用的备份代码，然后选择**验证**。

2. 如果您是多个客户组织的管理员，请选择任意客户组织。
3. 从右上角菜单中，选择 **我的设置**。



4. 在**身份验证器应用**中，选择**添加新设备**。

   突出显示“更改设备”的登录安全部分(/en-us/citrix-cloud/media/admin-mfa-change-device-link.png)

5. 当系统提示您确认更改设备时，选择**是，更改我的设备**。

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

6. 通过输入身份验证器应用中的验证码来验证您的身份。如果您没有身份验证器应用，请选择**使用恢复方法**以使用您选择的恢复方法验证您的身份。根据您选择的恢复方法，输入您收到的验证码或恢复代码，或未使用的备份代码。选择**验证并继续**。
7. 如果您正在使用最初注册的设备和原始身份验证器应用，请从您的身份验证器应用中删除现有的 Citrix Cloud 条目。
8. 如果您正在注册新设备但没有身份验证器应用，请从设备的应用程序商店下载一个。
9. 在您的身份验证器应用中，使用您的设备扫描二维码或手动输入密钥。
10. 输入身份验证器应用中的 6 位验证码并选择**验证代码**。

更改设备后，Citrix 强烈建议检查“我的个人资料”页面中的验证方法是否为最新。

更改您的 MFA 方法

如果您使用身份验证器应用注册了 MFA 并希望切换为使用电子邮件地址，请注意，更改身份验证方法会删除您的设备注册。如果您想重新使用身份验证器应用进行 MFA，则需要重新注册您的设备。

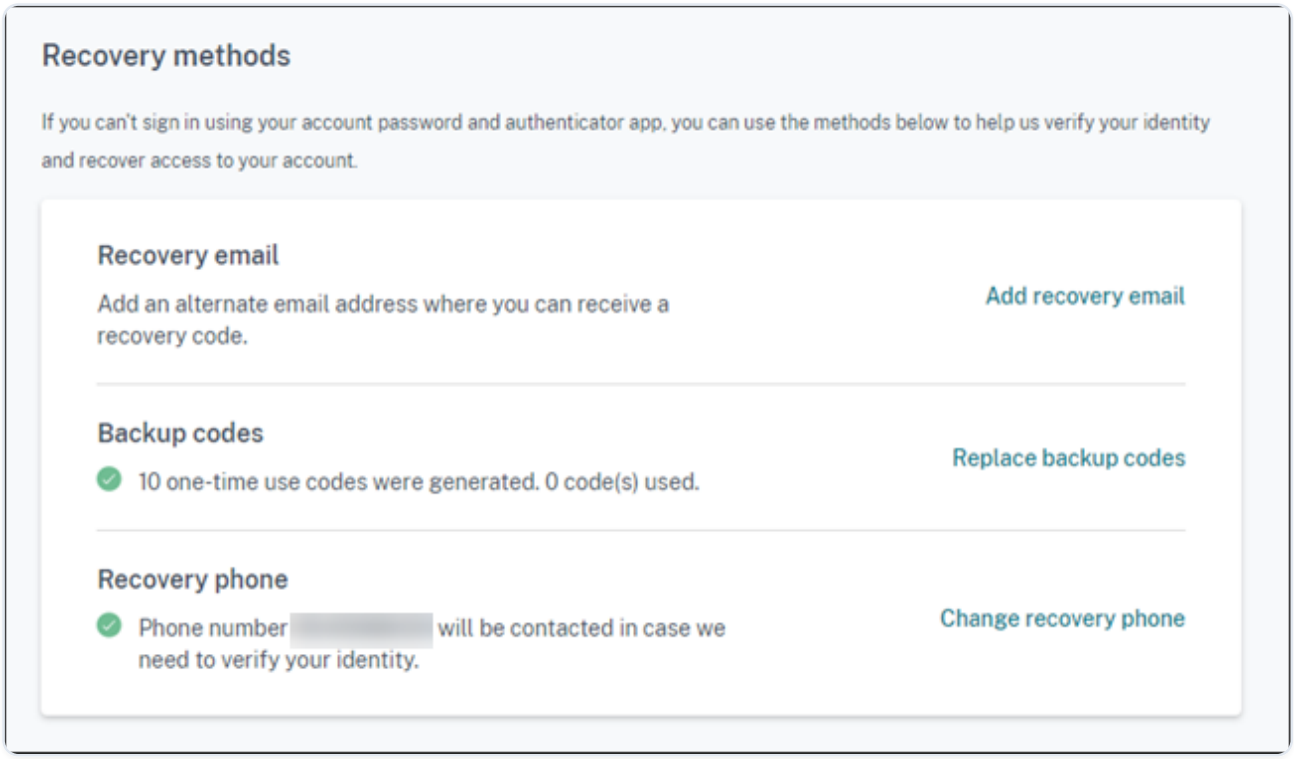
1. 在 Citrix Cloud 控制台的右上角菜单中，选择**我的设置**。
2. 在**多重身份验证 (MFA)** 下，选择您要切换到的身份验证方法。
3. 如果切换到电子邮件 MFA：
   a. 选择**是，更改为电子邮件**以确认您要更改 MFA 方法。
   b. 输入身份验证器应用中的代码，或使用恢复方法确认您的身份。
   c. 选择 **验证并继续** 以完成更改。
4. 如果切换到身份验证器应用：
   a. 出现提示时，输入 Citrix Cloud 发送到您电子邮件地址的验证码，然后选择 **验证并继续**。或者，使用恢复方法确认您的身份。
   b. 使用您的身份验证器应用，用设备的摄像头扫描二维码或输入字母数字密钥。
   c. 在 **验证您的身份验证器应用** 下，输入身份验证器应用中的 6 位数代码。
   d. 单击 **验证代码** 以完成设备注册。

管理您的 MFA 恢复方法

重要提示：

为确保您的 Citrix Cloud 帐户安全，请使您的验证方法保持最新且信息准确。如果您无法访问身份验证器应用或 MFA 电子邮件地址，这些验证方法是您恢复帐户访问权限的唯一方式。

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



添加或更改您的恢复电子邮件

1. 从右上角菜单中，选择 **我的设置**。
2. 在 **恢复方法** 下的 **恢复电子邮件** 中，如果您尚未添加恢复电子邮件地址，请选择 **添加恢复电子邮件**。如果您已添加恢复电子邮件地址，请选择 **更改恢复电子邮件**。
3. 出现提示时，输入身份验证器应用中的验证码或发送到您电子邮件地址的代码。
4. 输入您要使用的新电子邮件地址，然后选择 **发送验证电子邮件**。此电子邮件地址必须与您用于 Citrix Cloud 帐户的电子邮件地址不同。Citrix Cloud 会向您输入的电子邮件地址发送一封验证电子邮件。
5. 输入验证电子邮件中的代码，然后单击 **验证代码并完成**。

生成新的备用代码

您可以随时生成一组新的备用代码。当您使用备用代码时，Citrix Cloud 会在您的“我的配置文件”页面中记录已使用的数量。

生成新的备用代码后，请务必将其存储在安全的地方。

1. 从右上角菜单中，选择 **我的设置**。
2. 在 **恢复方法** 下的 **备用代码** 中，如果您之前未生成备用代码，请选择 **生成新的备用代码**。如果您之前已生成备用代码，请选择 **替换备用代码**。
3. 当系统提示您替换备用代码时，选择 **是，替换我的代码**。
4. 通过输入身份验证器应用中的验证码或发送到您电子邮件地址的代码来验证您的身份。

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

5. 选择 **验证并继续**。Citrix Cloud 会生成并显示一组新的备用代码。
6. 选择 **下载代码** 将新代码下载为文本文件。然后，选择 **我已存储我的备用代码**。
7. 选择 **我已存储我的备用代码** 以完成替换备用代码。

更改您的恢复电话号码

1. 从右上角菜单中，选择 **我的设置**。
2. 在 **恢复方法** 下的 **恢复电话** 中，选择 **更改恢复电话**。
3. 输入来自身份验证器应用或发送到您电子邮件地址的验证码。选择 **验证并继续**。
4. 输入您要使用的新电话号码。然后，重新输入电话号码以确认。
5. 选择 **保存恢复电话号码**。

注意：

您只能在管理员接受了管理员邀请并点击了 CEM 磁贴上的 **管理** 之后，才能修改 Citrix Endpoint Management™ (CEM) 管理员的权限。与所有 Citrix Cloud 管理员一样，CEM 管理员默认拥有完全访问权限。

管理管理员组

您可以使用 Active Directory、Microsoft Entra ID (ME-ID) 或 Google Cloud Identity 中的组将管理员添加到您的 Citrix Cloud™ 帐户。然后，您可以管理组中所有管理员的服务访问权限。

AD 先决条件

Citrix Cloud 通过 SAML 2.0 支持 AD 组身份验证。在将 AD 管理员组的成员添加到 Citrix Cloud 之前，您需要配置 Citrix Cloud 与 SAML 提供商之间的连接。有关详细信息，请参阅 将 SAML 连接为 Citrix Cloud 的身份提供商。

如果您在 Citrix Cloud 中已有 SAML 连接，则在添加 AD 管理员组之前，必须将您的 SAML 提供商重新连接到 Citrix Cloud。如果您不重新连接 SAML，添加 AD 管理员组可能会失败。有关详细信息，请参阅 将现有 SAML 连接用于管理员身份验证。

Microsoft Entra ID 先决条件

使用 Microsoft Entra ID 组身份验证需要最新版本的 Microsoft Entra ID 应用程序，以便将其连接到 Citrix Cloud。当您首次连接 Microsoft Entra ID 时，Citrix Cloud 获取了此应用程序。如果您在 2019 年 5 月之前将 Microsoft Entra ID 连接到 Citrix Cloud，则 Citrix Cloud 可能未使用最新的应用程序与

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

其连接。如果您的帐户未使用最新的应用程序，Citrix Cloud 将无法显示您的 Microsoft Entra ID 组。

在 Citrix Cloud 中使用 Microsoft Entra ID 组之前，请执行以下任务：

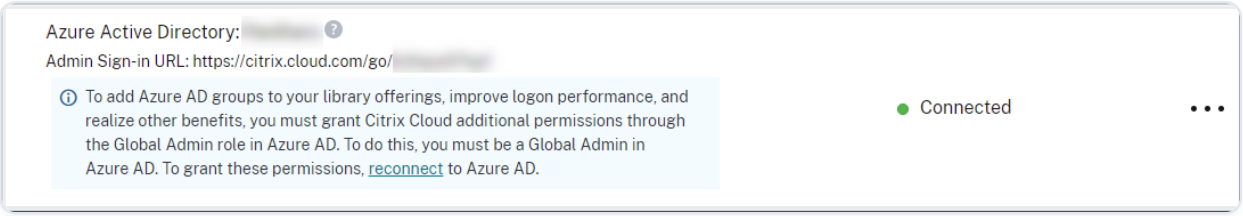
1. 验证您是否正在使用最新应用程序进行 Microsoft Entra ID 连接。如果您未使用最新的应用程序，Citrix Cloud 将显示通知。
2. 如果应用程序必须更新，请将您的 Microsoft Entra ID 重新连接到 Citrix Cloud。通过重新连接到您的 Microsoft Entra ID，您将授予 Citrix Cloud 应用程序级别的只读权限，并允许 Citrix Cloud 代表您重新连接到您的 Microsoft Entra ID。在重新连接期间，将显示这些权限的列表供您审阅。有关 Citrix Cloud 请求的权限的更多信息，请参阅 Citrix Cloud 的 Microsoft Entra ID 权限。

重要提示：

要完成此任务，您必须是 Microsoft Entra ID 中的全局管理员。此外，您必须使用 Citrix 身份提供商下的完全访问权限管理员帐户登录到 Citrix Cloud。如果您使用 Microsoft Entra ID 凭据登录，则重新连接将失败。如果您没有任何使用 Citrix 身份提供商的管理员，您可以暂时添加一个以执行此任务，然后将其删除。

验证您与 Microsoft Entra ID 的连接

1. 使用 Citrix 身份提供商下的完全访问权限管理员帐户登录到 Citrix Cloud。
2. 从 Citrix Cloud 菜单中，选择 **身份和访问管理**，然后选择 **身份验证**。
3. 找到 **Microsoft Entra ID**。如果 Citrix Cloud 必须更新您的 Microsoft Entra ID 连接的应用程序，则会出现通知。



如果 Citrix Cloud 已经在使用最新应用程序，则不会出现通知。

重新连接到 Microsoft Entra ID

1. 在 Citrix Cloud 控制台中的 Microsoft Entra ID 通知中，单击**重新连接**链接。将显示请求的 Azure 权限列表。
2. 查看权限，然后选择**接受**。

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

Google 云身份

Citrix Cloud 支持通过 Google Cloud Identity 进行管理员组身份验证。在将管理员组添加到 Citrix Cloud 之前，您必须配置 Citrix Cloud 与 Google Cloud Identity 之间的连接。有关详细信息，请参阅将 Google Cloud Identity 作为身份提供程序连接到 Citrix Cloud。

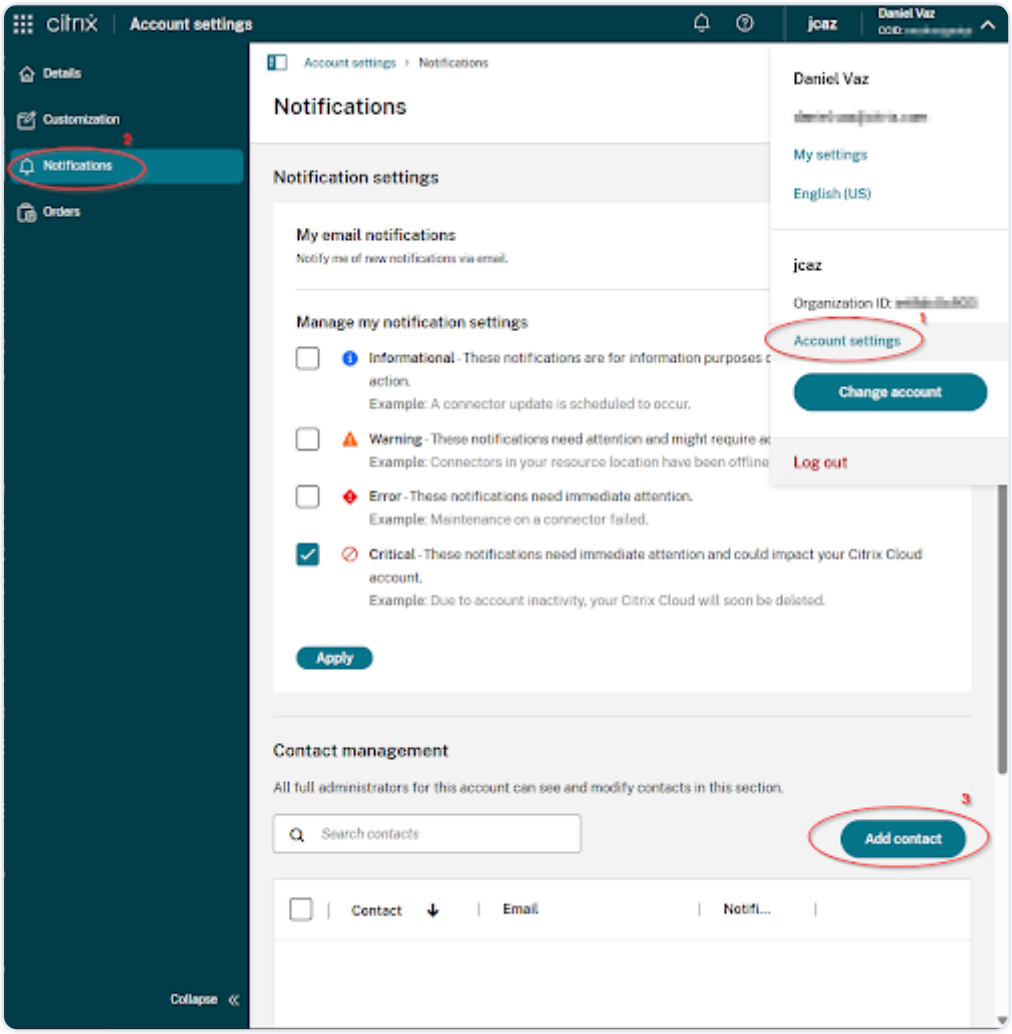
支持的权限

在此处查看支持的权限说明，控制台权限。

限制

管理员组成员无法使用通知功能的自定义访问权限。

您可以在“通知联系人管理”下为组成员添加通知联系人，如下图所示：



依赖于 Citrix Cloud 平台功能的 Citrix DaaS™ 功能（例如快速部署用户分配）不可用。

管理员组成员的权限更改，如果该成员已登录，则只有在该成员注销并重新登录后才会生效。

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

具有 Citrix®、AD、Microsoft Entra ID 和 Google Cloud 身份的管理员的最终权限

当管理员登录到 Citrix Cloud 时，如果管理员同时拥有 Citrix 身份（Citrix Cloud 中的默认身份提供程序）以及通过 AD、Microsoft Entra ID 或 Google Cloud Identity 获得的单用户或基于组的身份，则可能只有某些权限可用。本节中的表格描述了这些身份的每种组合可用的权限。

单用户身份 指的是通过个人帐户授予管理员的 AD、Microsoft Entra ID 或 Google Cloud Identity 权限。*基于组的身份* 指的是作为组成员授予的 AD、Microsoft Entra ID 或 Google Cloud Identity 权限。

CITRIX 身份	单用户 AD 或 MICROSOFT ENTRA ID 身份	基于组的 AD 或 MICROSOFT ENTRA ID 身份	单用户或基于组的 GOOGLE CLOUD IDENTITY	身份验证后可用的权限
X	X			管理员在使用 Citrix 身份、AD 身份或 Microsoft Entra ID 身份成功进行身份验证后，将拥有这两种身份的累积权限。
X		X		每个身份都被视为一个独立的实体。可用权限取决于管理员是使用 Citrix 身份还是 Microsoft Entra ID 身份进行身份验证。
X			X	每个身份都被视为一个独立的实体。可用权限取决于管理员是使用 Citrix 身份还是 Google Cloud 身份进行身份验证。

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

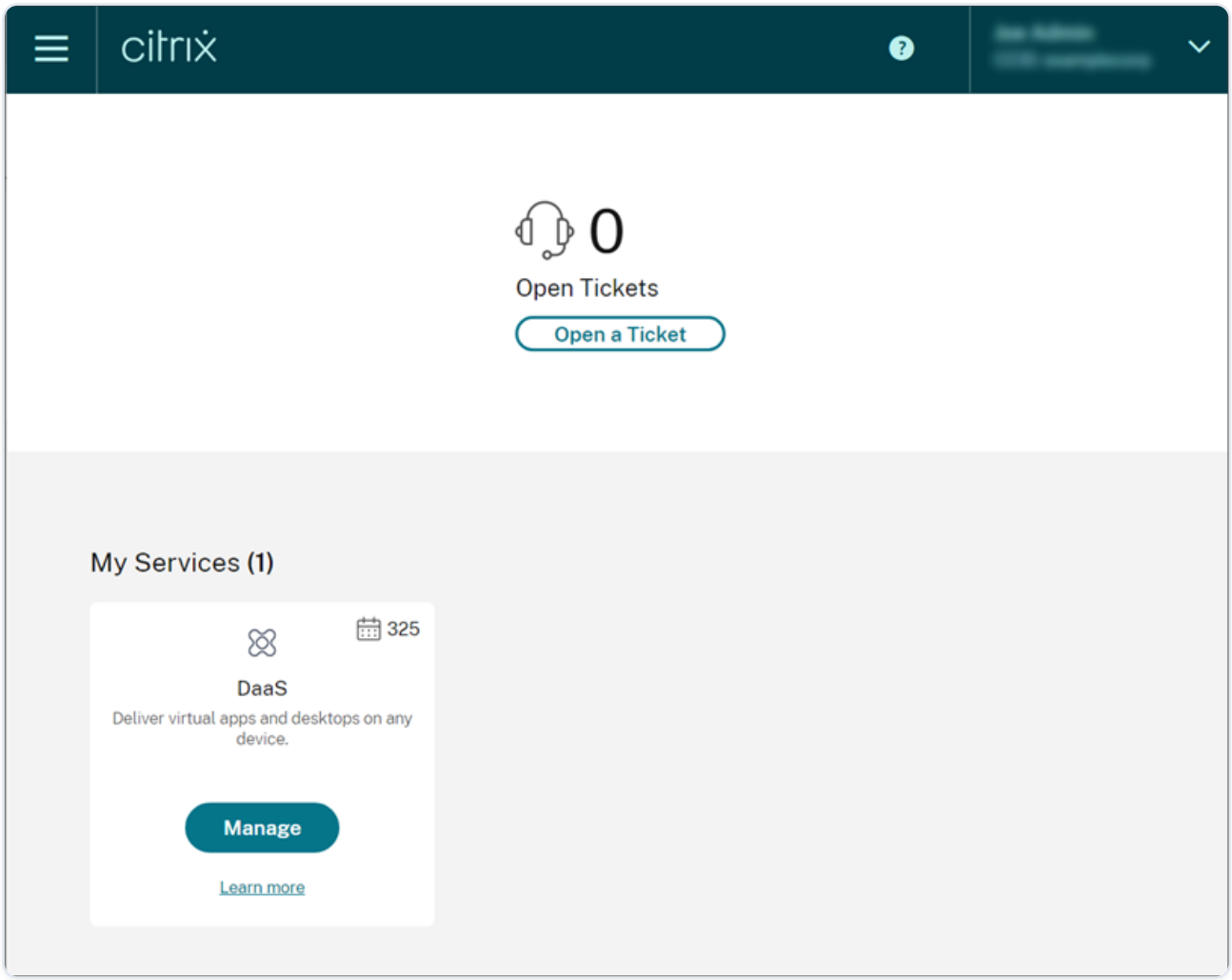
CITRIX 身份	单用户 AD 或 MICROSOFT ENTRA ID 身份	基于组的 AD 或 MICROSOFT ENTRA ID 身份	单用户或基于组的 GOOGLE CLOUD IDENTITY	身份验证后可用的权限
	X	X		当使用 AD 或 Microsoft Entra ID 验证到 Citrix Cloud 时，管理员拥有这两种身份的累积权限。
	X		X	每个身份都被视为一个独立的实体。可用权限取决于管理员是使用 Citrix 身份还是 Google Cloud 身份进行身份验证。
		X	X	每个身份都被视为一个独立的实体。可用权限取决于管理员是使用 Citrix 身份还是 Google Cloud 身份进行身份验证。
X	X	X		当使用其 Citrix 身份进行身份验证时，管理员拥有 Citrix 身份和单用户 Microsoft Entra ID 身份的累积权限。当使用 Microsoft Entra ID 进行身份验证时，管理员拥有所有三种身份的累积权限。

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

管理员的登录体验

将组添加到 Citrix Cloud 并定义服务权限后，组中的管理员只需在 Citrix Cloud 登录页面上选择**使用我的公司凭据登录**，然后输入其帐户的登录 URL（例如 `https://citrix.cloud.com/go/mycompany`）即可登录。与添加单个管理员不同，组中的管理员不会收到明确邀请，因此他们不会收到任何接受成为 Citrix Cloud 管理员邀请的电子邮件。

登录后，管理员从服务磁贴中选择**管理**以访问服务的管理控制台。



仅作为组成员获得权限的管理员可以使用 Citrix Cloud 帐户的登录 URL 访问 Citrix Cloud 帐户。

通过个人帐户和作为组成员获得权限的管理员可以选择他们想要访问的 Citrix Cloud 帐户。如果管理员是多个 Citrix Cloud 帐户的成员，他们可以在成功进行身份验证后从客户选择器中选择一个 Citrix Cloud 帐户。

已知问题

在 Active Directory 中重命名组后，新名称可能不会显示。解决方法是，在 **Citrix Identity and Access Management** 中删除旧组并添加重命名后的组。

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

限制

多个组对应用程序性能的影响

Citrix 建议单个管理员所属的已添加到 Citrix Cloud 的组不超过 20 个。所属组数量过多可能会导致应用程序性能下降。

多个组对身份验证的影响

如果基于组的管理员在 AD 或 Microsoft Entra ID 中被分配到多个组，则身份验证可能会失败，因为组的数量过多。此问题是由于 Citrix Cloud 与 AD 和 Microsoft Entra ID 集成中的限制所致。当管理员尝试登录时，Citrix Cloud 会尝试压缩检索到的组数量。如果 Citrix Cloud 无法成功应用压缩，则无法检索所有组，并且身份验证失败。

此问题也可能影响通过 AD 或 Microsoft Entra ID 对云存储进行身份验证的用户。如果用户属于多个组，则身份验证可能会失败，因为组的数量过多。

为解决此问题，请检查管理员或用户帐户，并验证他们是否仅属于其在组织中担任角色所需的组。

由于分配的角色/范围对过多，添加组失败

添加具有多个角色/范围对的组时，可能会出现指示无法创建该组的错误。发生此错误的原因是分配给该组的角色/范围对数量过多。要解决此错误，请将角色/范围对分配给两个或更多组，并将管理员分配给这些组。

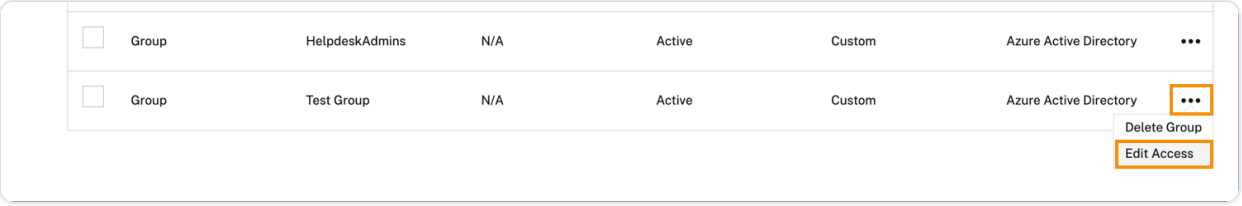
将管理员组添加到 Citrix Cloud

1. 从 Citrix Cloud 菜单中，选择 **身份和访问管理**，然后选择 **管理员**。
2. 选择 **添加管理员/组**。
3. 在 **管理员详细信息** 中，选择要使用的身份提供程序。如果选择了 Microsoft Entra ID，请根据需要登录到 Azure。选择 **下一步**。
4. 如果需要，选择要使用的域。
5. 搜索要添加的组并选择该组。
6. 在 **设置访问权限** 中，选择要分配给该组的角色。您必须至少选择一个角色。
7. 完成后，选择 **保存**。

修改管理员组的服务权限

1. 从 Citrix Cloud 菜单中，选择 **身份和访问管理**，然后选择 **管理员**。
2. 找到要管理的管理员组，然后从省略号菜单中选择 **编辑访问权限**。

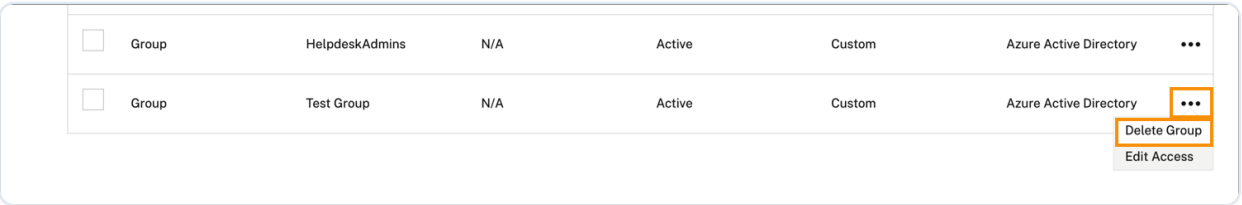
© 1997–2026 Citrix Systems, Inc. All rights reserved.



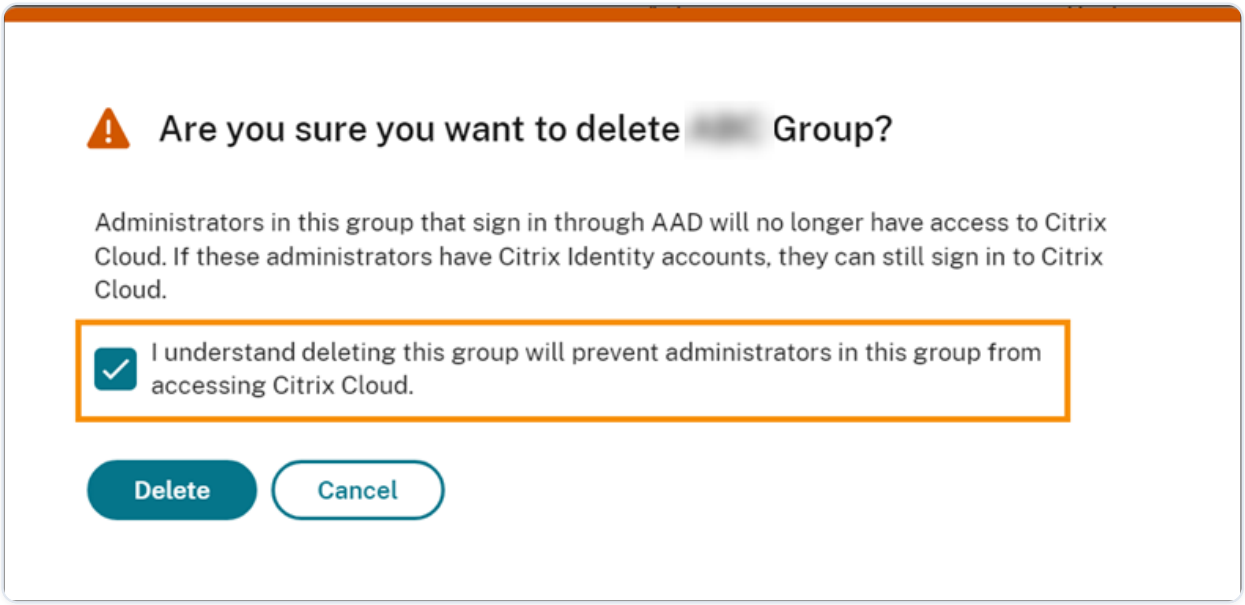
3. 根据需要选择或清除一个或多个角色和范围对旁边的复选标记。
4. 完成后，选择 **保存**。

删除管理员组

1. 从 Citrix Cloud 菜单中，选择 **身份和访问管理**，然后选择 **管理员**。
2. 找到要管理的管理员组，然后从省略号菜单中选择 **删除组**。



将显示确认消息。



3. 选择 **我了解删除此组将阻止组中的管理员访问 Citrix Cloud。** 以确认您了解删除该组的影响。
4. 选择 **删除**。

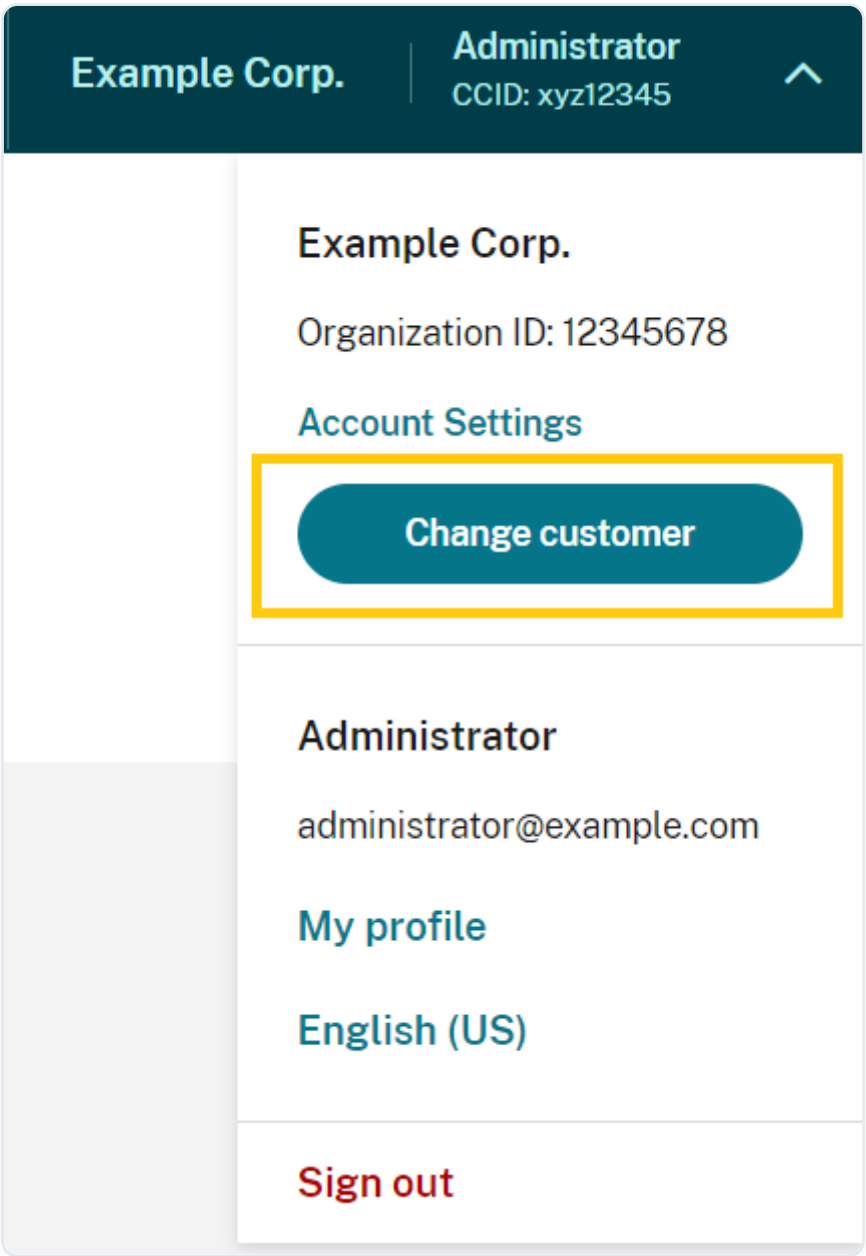
在多个 Citrix Cloud 帐户之间切换

注意：

本节介绍了一种情况，该情况仅影响 Microsoft Entra ID 管理员组的成员。

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

默认情况下，Microsoft Entra ID 管理员组的成员无法在他们可以访问的其他 Citrix Cloud 帐户之间切换。对于这些管理员，Citrix Cloud 用户菜单中不显示下图所示的 **更改客户** 选项。



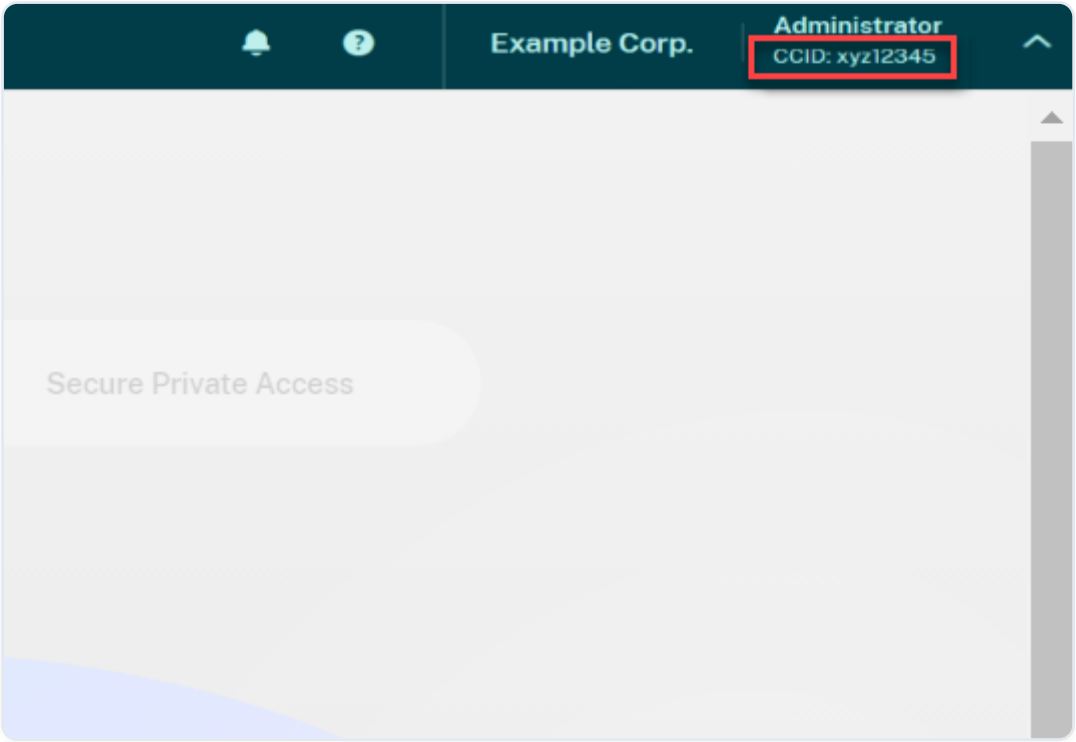
要启用此菜单选项并允许 Microsoft Entra ID 组成员在其他 Citrix Cloud 帐户之间切换，您必须链接要切换的帐户。

链接 Citrix Cloud 帐户涉及采用中心辐射型方法。在链接帐户之前，请确定哪个 Citrix Cloud 帐户将作为访问其他帐户的帐户（“中心”），以及您希望在客户选择器中列出哪些帐户（“辐射”）。

在链接帐户之前，请确保满足以下要求：

- 您在 Citrix Cloud 中拥有完全访问权限。
- 您可以访问 Windows PowerShell 集成脚本环境 (ISE)。
- 您拥有要链接的 Citrix Cloud 帐户的客户 ID。客户 ID 显示在每个帐户的管理控制台的右上角。

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



- 您拥有要作为中心帐户链接的 Citrix Cloud 帐户的 Citrix CWSAuth 持有者令牌。要检索此持有者令牌，请按照 CTX330675 中的说明进行操作。链接 Citrix Cloud 帐户时，您需要提供此信息。

链接 Citrix Cloud 帐户

1. 打开 PowerShell ISE 并将以下脚本粘贴到工作窗格中：

```
$headers = @{}

$headers.Add("Accept","application/json")

$headers.Add("Content-Type","application/json")

$headers.Add("Authorization","CWSAuth bearer=XXXXXXX")



$uri = "https://trust.citrixworkspacesapi.net/HubCustomerID/links"



$resp = Invoke-RestMethod -Method Get -Uri $uri -Headers $headers

$allLinks = $resp.linkedCustomers + @("SpokeCustomerID")
```

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

```
$body = @{"customers"=$allLinks}

$bodyjson = $body | ConvertTo-Json



$resp = Invoke-WebRequest -Method Post -Uri $uri -Headers $headers
-Body $bodyjson -ContentType 'application/json'

Write-Host "Citrix Cloud Status Code: $($resp.RawContent)"
```

2. 在第 4 行，将 `CWSAuth bearer=XXXXXXX` 替换为您的 CWSAuth 值（例如，`CWSAuth bearer=AbCdef123Ghik…`）。此值是一个类似于证书密钥的长哈希。
3. 在第 6 行，将 `HubCustomerID` 替换为中心帐户的客户 ID。
4. 在第 9 行，将 `SpokeCustomerID` 替换为分支帐户的客户 ID。
5. 运行脚本。
6. 重复步骤 3-5 以将其他帐户链接为分支帐户。

取消链接 Citrix Cloud 帐户

1. 打开 PowerShell ISE。如果 PowerShell ISE 已打开，请清除工作窗格。
2. 将以下脚本粘贴到工作窗格中：

```
$headers = @{}

$headers.Add("Accept","application/json")

$headers.Add("Content-Type","application/json")

$headers.Add("Authorization","CWSAuth bearer=XXXXXXX")



$uri = "https://trust.citrixworkspacesapi.net/HubCustomerID/links/
SpokeCustomerID"



$resp = Invoke-WebRequest -Method Delete -Uri $uri -Headers $headers
```

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

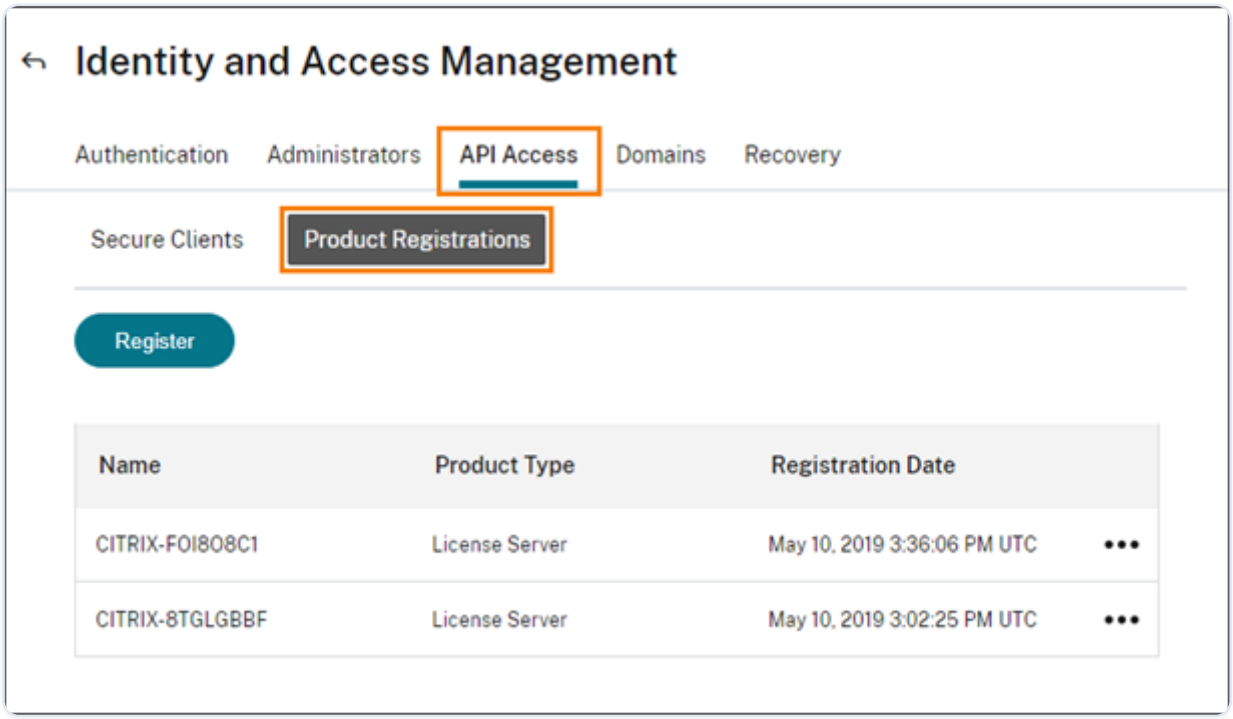
```
Write-Host "Response: $($resp.RawContent)"
```

3. 在第 4 行，将 `CWSAuth bearer=xxxxxxx1` 替换为您的 CWSAuth 值（例如，`CWSAuth bearer=AbCdef123Ghik…`）。此值是一个类似于证书密钥的长哈希。
4. 在第 6 行，将 `HubCustomerID` 替换为中心帐户的客户 ID。
5. 在第 6 行，将 `SpokeCustomerID` 替换为分支帐户的客户 ID。
6. 运行脚本。
7. 重复步骤 4-6 以取消关联其他帐户。

将本地产品注册到 Citrix Cloud™

您可以通过 Citrix Cloud 使用短代码激活轻松注册您的本地 Citrix 产品。根据您的产品，此 8 位代码可能在产品安装过程中生成，或者在您运行产品的管理控制台时生成。当产品提示您注册时，它会从 Citrix Cloud 请求代码并显示该代码。然后，您可以复制并粘贴此代码，或在 Citrix Cloud 中手动输入。

注册后，产品注册页面 (**身份和访问管理 > API 访问 > 产品注册**) 会显示您的注册产品所在的服务器。



您可以注册到 Citrix Cloud 的本地产品包括：

- Citrix Connector™ Appliance 用于云服务
- Citrix 联合身份验证服务

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

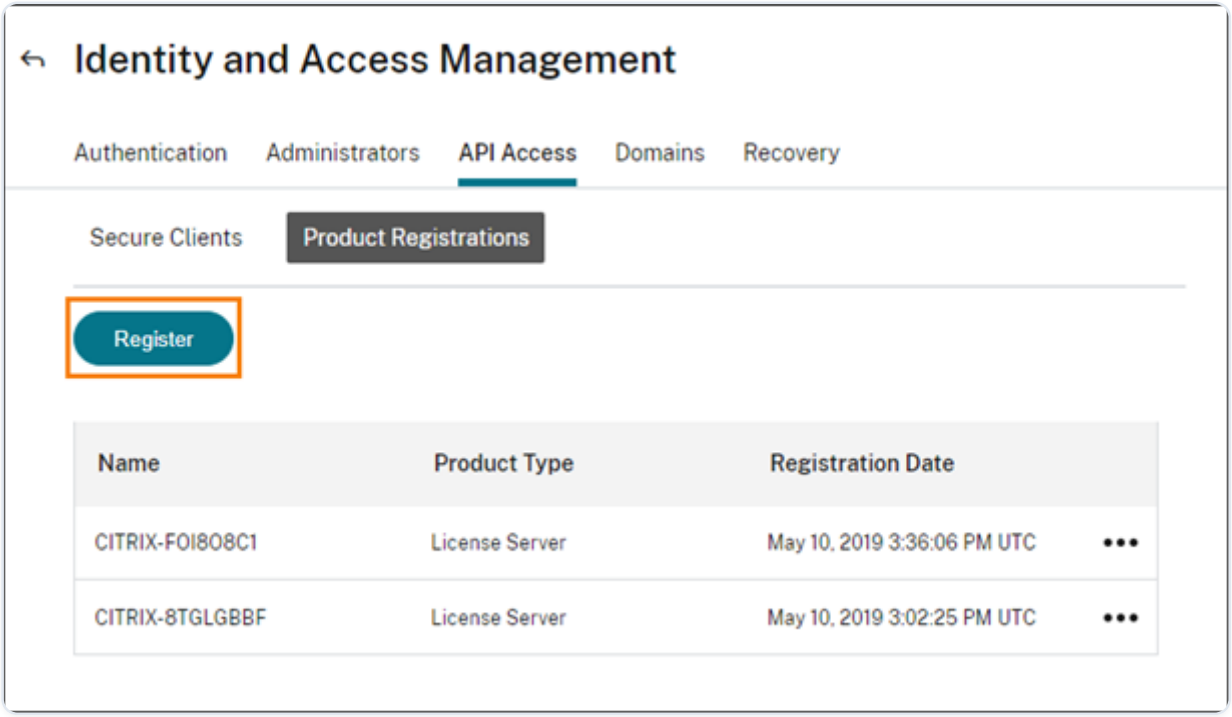
- Citrix 许可证服务器
- Citrix 虚拟应用和桌面，当使用 Citrix Analytics for Performance™ 注册站点时

注意：

本文介绍了将本地产品注册到 Citrix Cloud 的步骤。有关特定于产品的要求，请参阅该产品的文档。

注册产品

1. 从 Citrix Cloud 菜单中，选择 **身份和访问管理**。
2. 选择 **API 访问 > 产品注册**，然后选择 **注册**。



3. 输入您的 Citrix 产品的 8 位字母数字代码，然后单击 **继续**。
4. 审查注册详细信息，然后单击 **注册**。

移除产品注册

如果您从环境中移除运行已注册 Citrix 产品的服务器，则“产品注册”页面仍会显示这些服务器。请按照以下步骤从 Citrix Cloud 中移除这些服务器。如果需要，您以后可以再次注册产品，以便在“产品注册”页面上显示这些服务器。

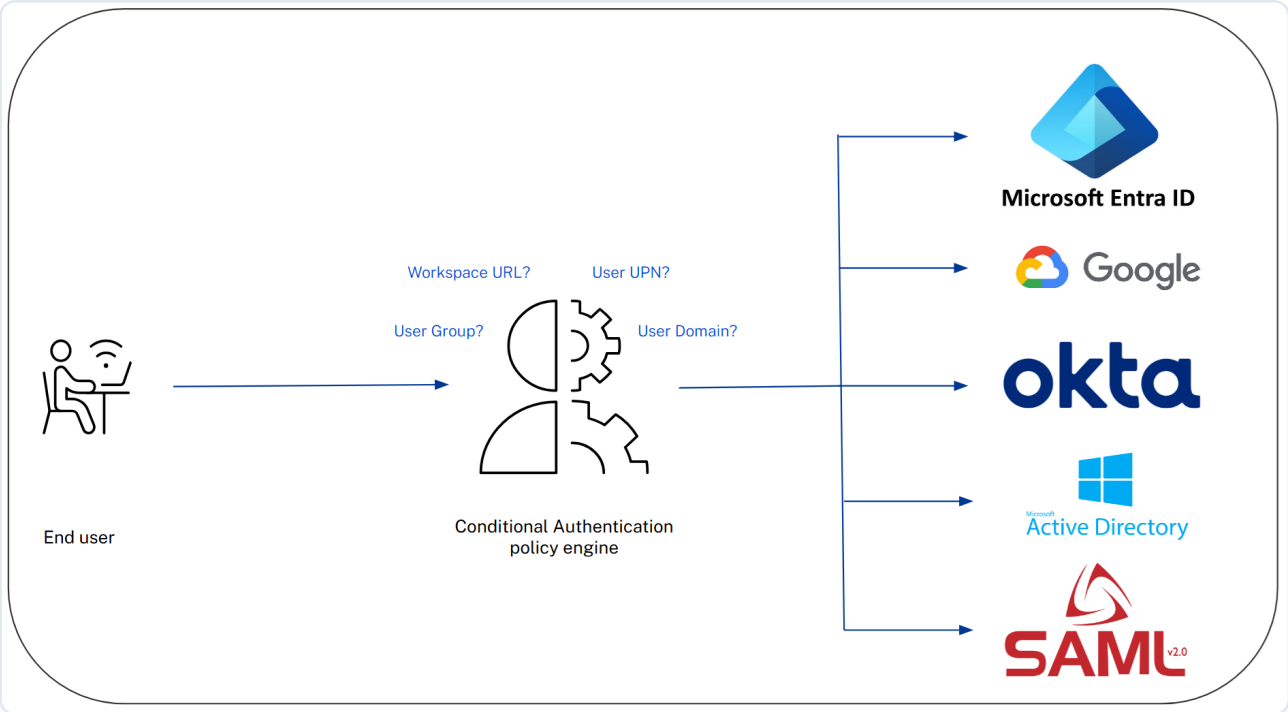
1. 在“产品注册”页面上，找到要移除的服务器。
2. 单击省略号按钮并选择 **移除注册**。 (/en-us/citrix-cloud/media/prod-reg-remove-registration.png)
3. 出现提示时，选择 **移除**。

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

条件身份验证

条件身份验证是一项新的安全功能，有助于进一步增强您的零信任框架。条件身份验证允许 Citrix Cloud™ 管理员根据您设置的策略条件，在应用商店登录流程中将最终用户定向到不同的 IdP。因此，不同的最终用户将根据管理员建立的风险因素拥有不同级别的访问验证。

在撰写本文时，支持五种不同的切换条件，这些条件将根据您定义的策略将最终用户定向到不同的 IdP 实例。



常见用例

- 合并与收购，其中大型母公司包含多个正在合并中的小型公司。
- 通过将第三方用户和承包商定向到专用 IdP、OIDC 应用程序或 SAML 应用程序来授予他们应用商店访问权限，这与您组织内的全职员工通常被授权使用的不同。
- 拥有多个分支机构或部门的大型组织，需要不同的身份验证机制。

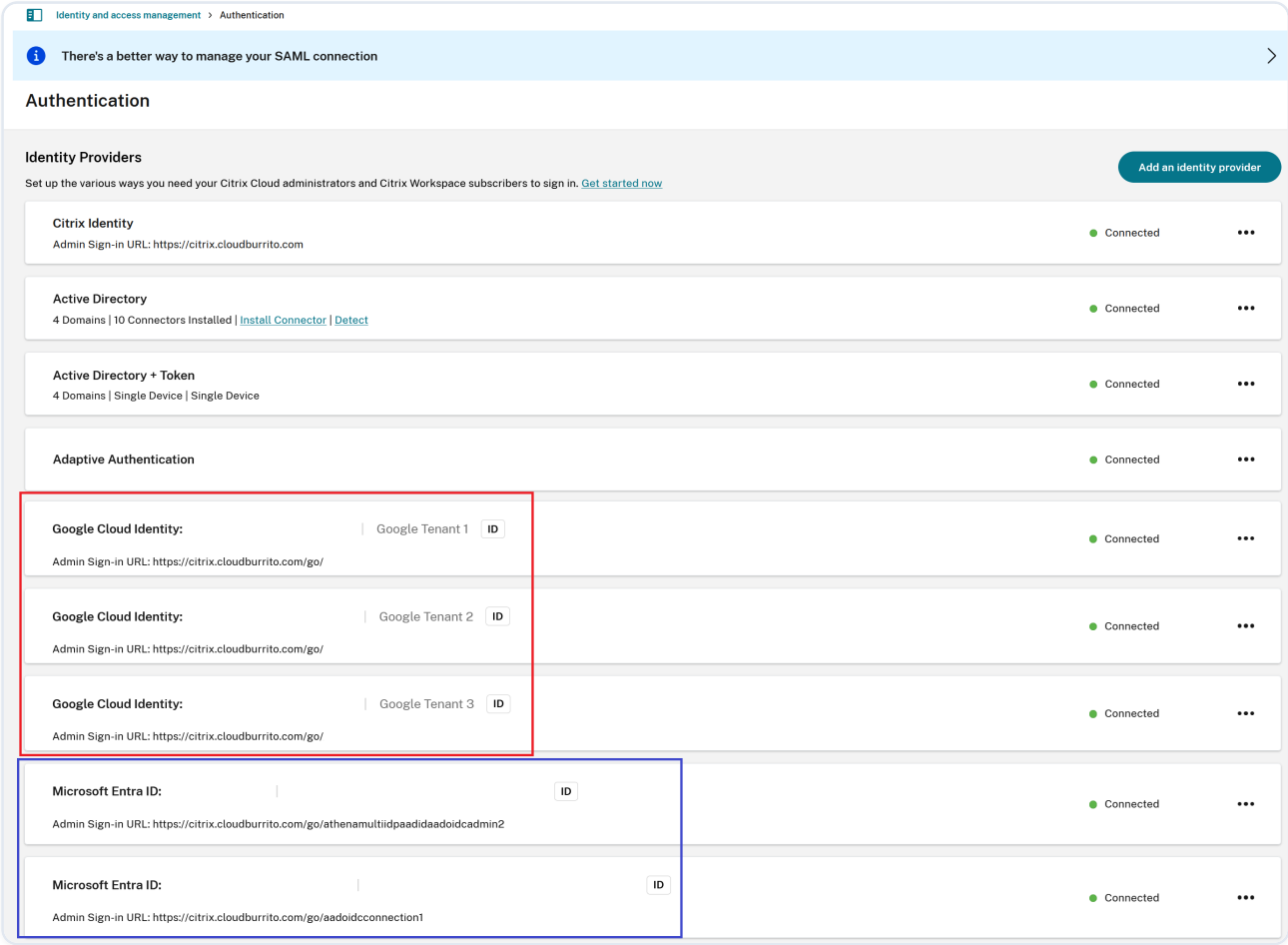
先决条件

- 在Citrix Cloud 身份和访问管理页面中创建两个或更多身份提供商

多 IdP

过去，只允许单个身份类型实例。Citrix Cloud® 现在支持添加同一身份提供商类型的多个实例。例如，现在可以在“身份和访问管理”选项卡下添加多个 EntraID IdP、Google IdP 或 Okta IdP 连接，每个连接都指向**不同**的 IdP 租户。

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

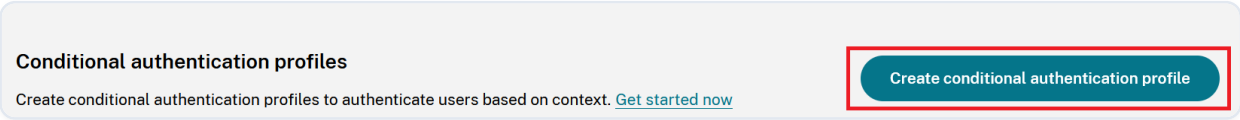


重要提示：

虽然 DaaS 和 SPA 目前支持多个 IdP，但某些服务仍在努力实施此功能，并将很快推出。

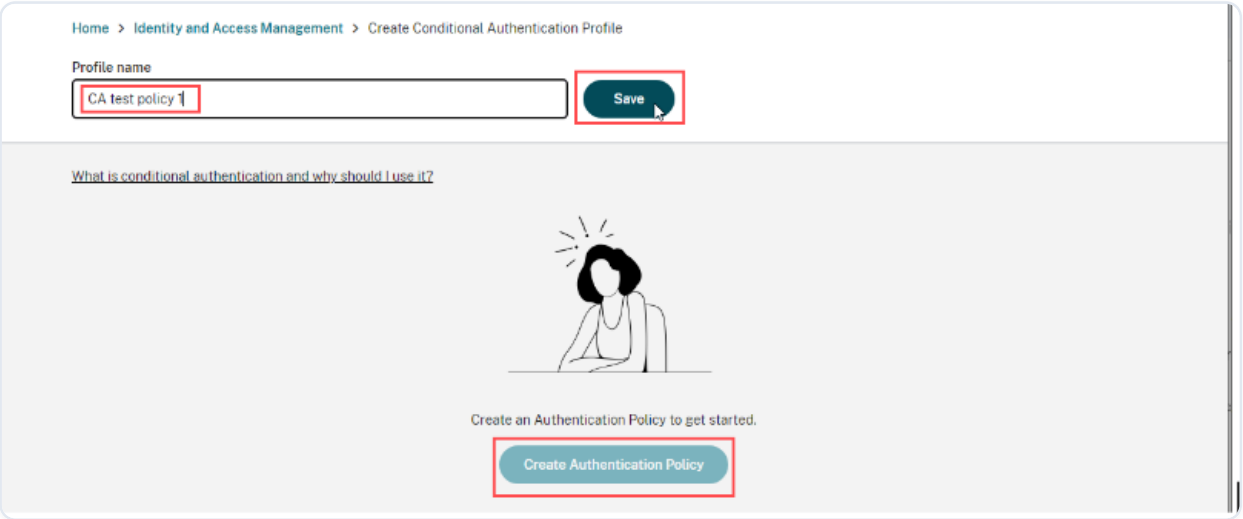
配置条件身份验证

1. 单击“**创建条件身份验证配置文件**”。

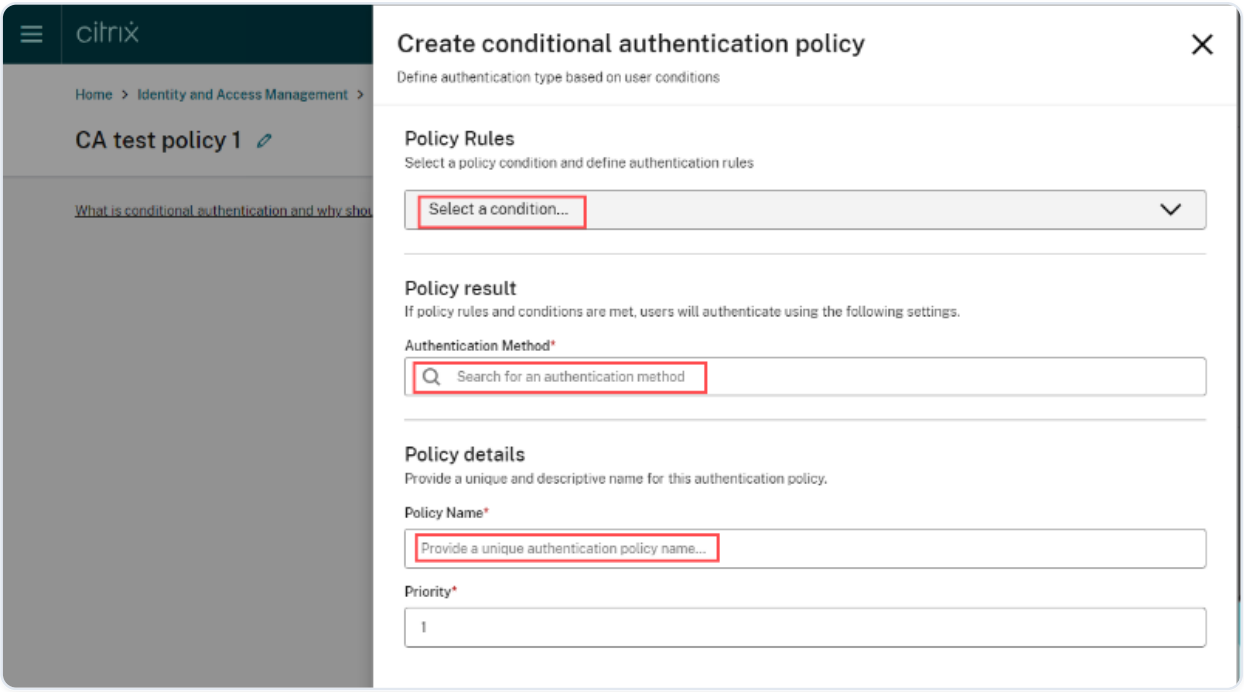


2. 输入配置文件的名称，然后单击“**创建身份验证策略**”。

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

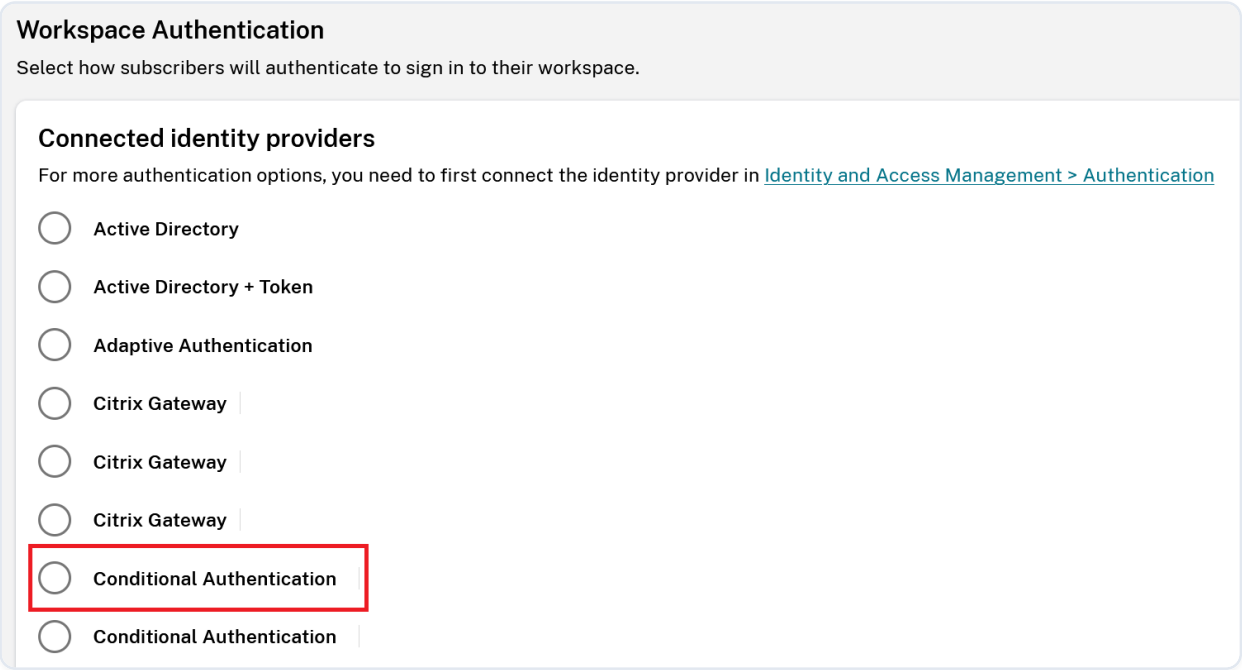


3. 根据需要选择要应用于策略的条件，然后单击“**保存**”。



4. 导航到“**StoreFront Cloud**”，然后单击“**身份验证**”以选择您的身份提供程序或条件身份验证配置文件。

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



条件身份验证概念

条件身份验证配置文件

条件身份验证配置文件由多个条件身份验证策略组成，这些策略根据您定义的条件控制最终用户如何向商店进行身份验证。此配置文件允许策略优先级排序和重新排序，使您能够指定应评估策略的顺序。

条件身份验证策略

条件身份验证策略是包含一个或多个条件的策略。当使用 AND 逻辑满足这些条件时，它们会将最终用户的登录过程引导至特定的目标 IdP 实例，例如 Okta OIDC、SAML 或 Gateway IDP 连接。可以克隆单个策略，以便根据需要进行修改和重命名。

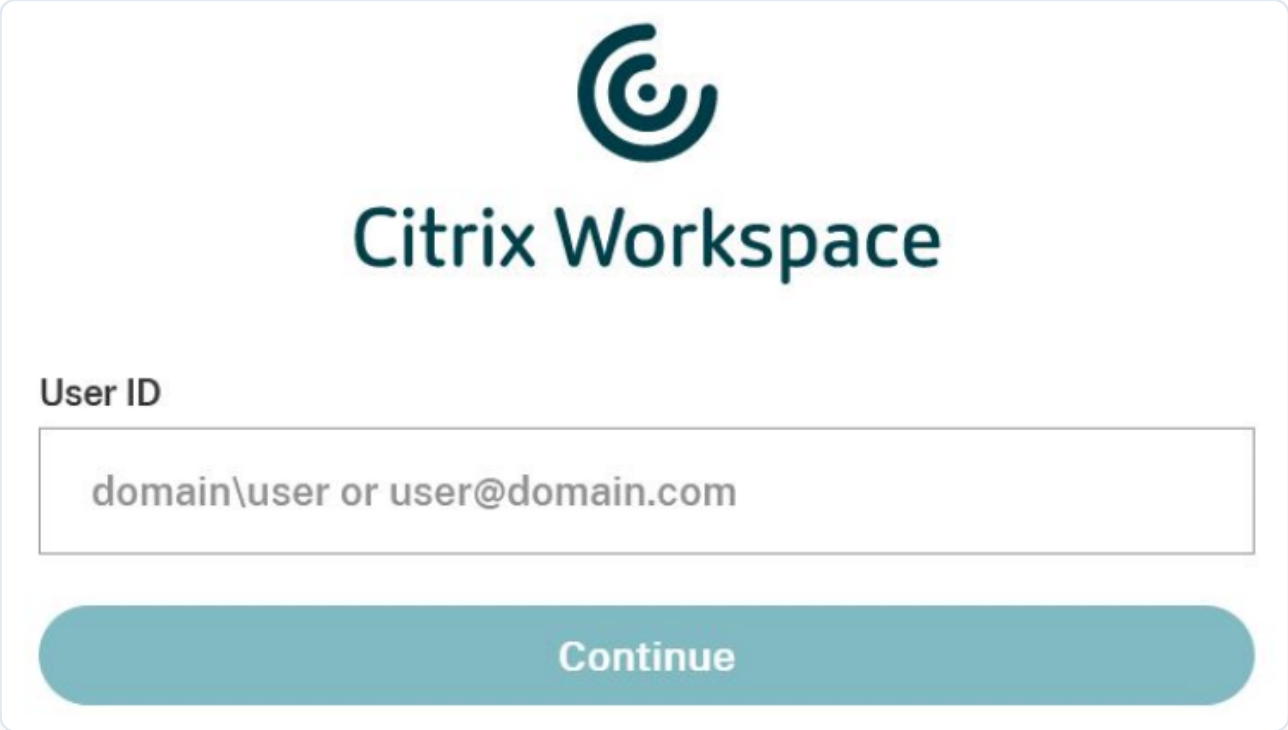
每个条件身份验证策略包含以下数据：

- **策略规则**，即一个或多个必须满足的条件，才能将最终用户定向到特定的 IdP 实例。例如，使用商店 URL 1 并且用户是 AD Group1 的成员。
- **策略结果 IdP**，即用户在登录过程中被定向到的目标 IdP 实例。例如，`store URL 1 is used AND user is a member of AD Group1 → EntraID SAML IDP Instance`。
- **策略名称**，这是一个管理员友好的名称，用于识别和描述策略。 例如，`store URL 1 AND Group1 - EntraID SAML`。
- **策略优先级**，它决定了策略的评估顺序。优先级按降序评估。例如：优先级 1 高于优先级 2。

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

条件身份验证预身份验证页面

根据您的商店配置方式以及条件身份验证配置文件中设置的条件，您的商店用户在登录过程中可能会遇到预身份验证页面。此页面对于捕获商店用户的用户名格式至关重要，而用户名格式对于根据条件身份验证策略做出决策至关重要。它确保用户的登录流程被定向到适当的 IdP 实例。

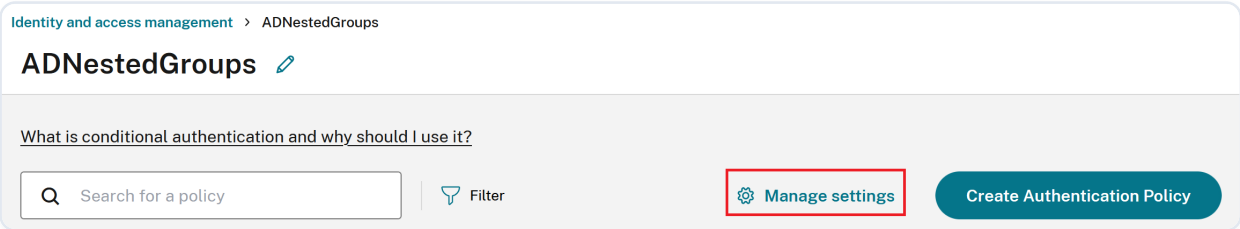


登录自动填充

当需要预身份验证页面时，我们引入了登录自动填充功能，该功能会自动使用用户在预身份验证页面中的输入填充登录页面上的用户名字段。这消除了用户两次输入用户名的需要。

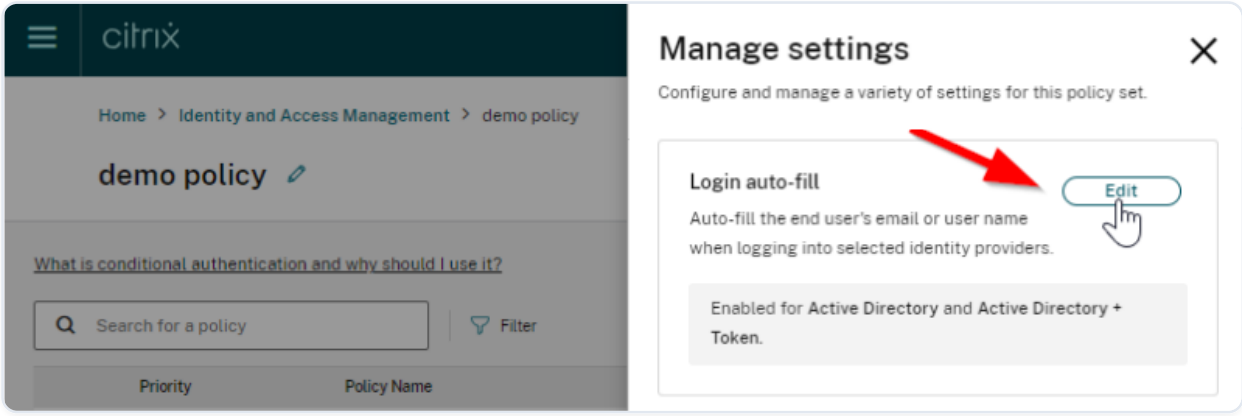
登录自动填充功能由管理员在条件身份验证配置文件设置中进行管理和配置，如下所示：

1. 在条件身份验证配置文件页面中，单击**管理设置**。

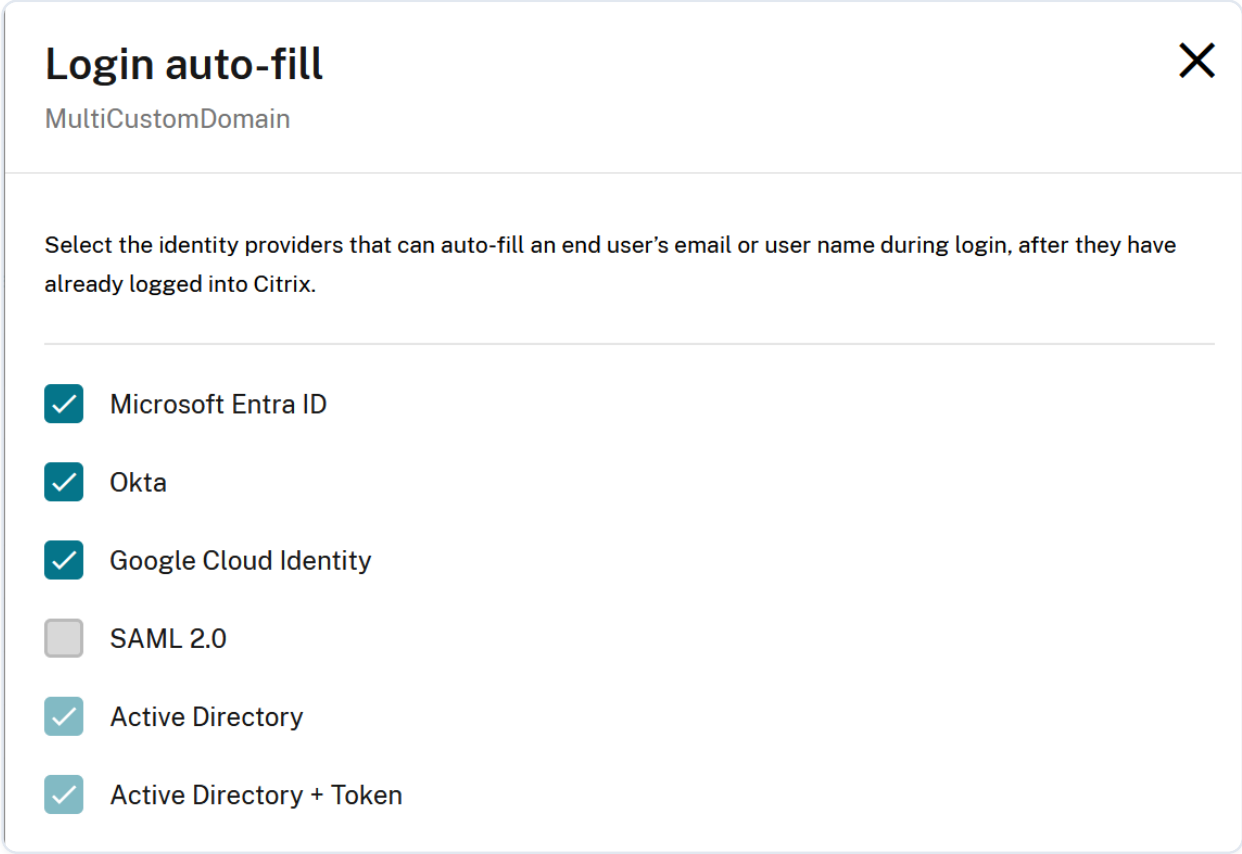


2. 单击**编辑**

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



3. 选择您要为其启用登录自动填充的 IdP。



重要提示：

登录自动填充仅适用于支持它的 IdP，并且默认情况下会为 AD 和 AD+TOTP 启用并强制执行（有关默认设置，请参见上面的屏幕截图）。

某些 IdP 需要特定的登录格式，有些可以支持多种用户名格式。例如，Google Cloud Identity 要求用户使用其电子邮件地址 (`user.name@domain.com`) 登录，这有时可能与他们的 UPN (`username@domain.com`) 不同。如果商店最终用户在预身份验证页面中输入了下级登录名 (domain\username)，该下级登录名将预填充到 IdP 登录页面的用户名字段中，并在用户尝试登录时

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

导致错误。管理员在配置登录自动填充功能之前，应考虑最合适的 IdP 切换策略条件以及特定 IdP 在登录过程中期望接收的用户名格式。

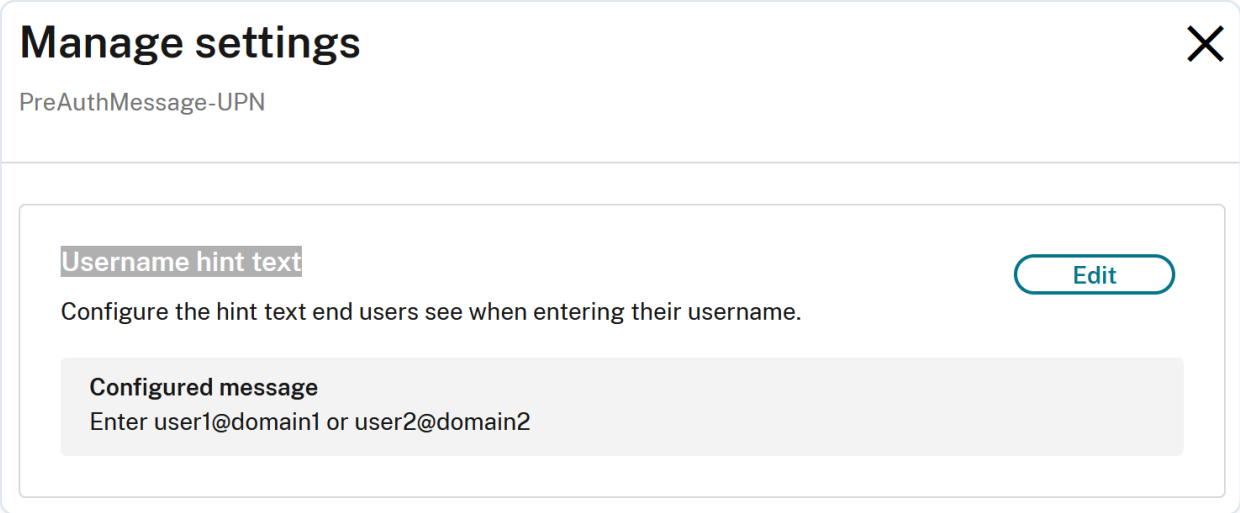
用户名提示文本

当条件身份验证需要额外的 AD 域或 AD 组用户上下文来做出 IdP 切换决策时，在登录流程中会向最终用户显示一个预身份验证页面。如果用户以不符合任何已配置 CA 策略的意外或不正确格式输入用户名，将阻止用户登录。可以自定义预身份验证对话框中显示的用户名提示文本，以便为最终用户提供指导，使其以正确且预期的格式输入用户名。

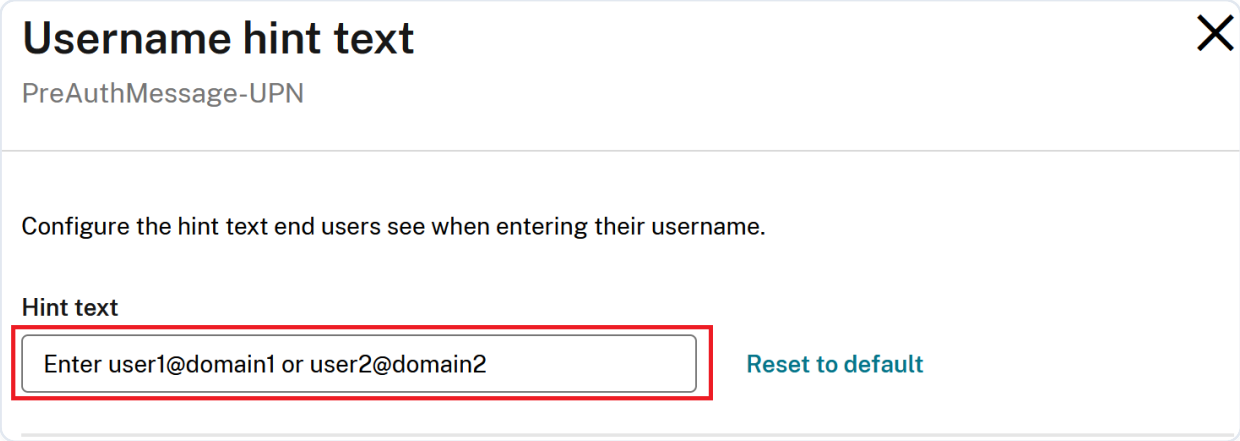
重要提示：

请谨慎使用用户名提示文本功能，以避免泄露有关您的 Citrix 环境、AD 域和用户详细信息的敏感信息。建议使用通用用户名示例。

1. 在条件身份验证配置文件页面中，单击“**管理设置**”。
2. 单击“**用户名提示文本**”上的“**编辑**”。

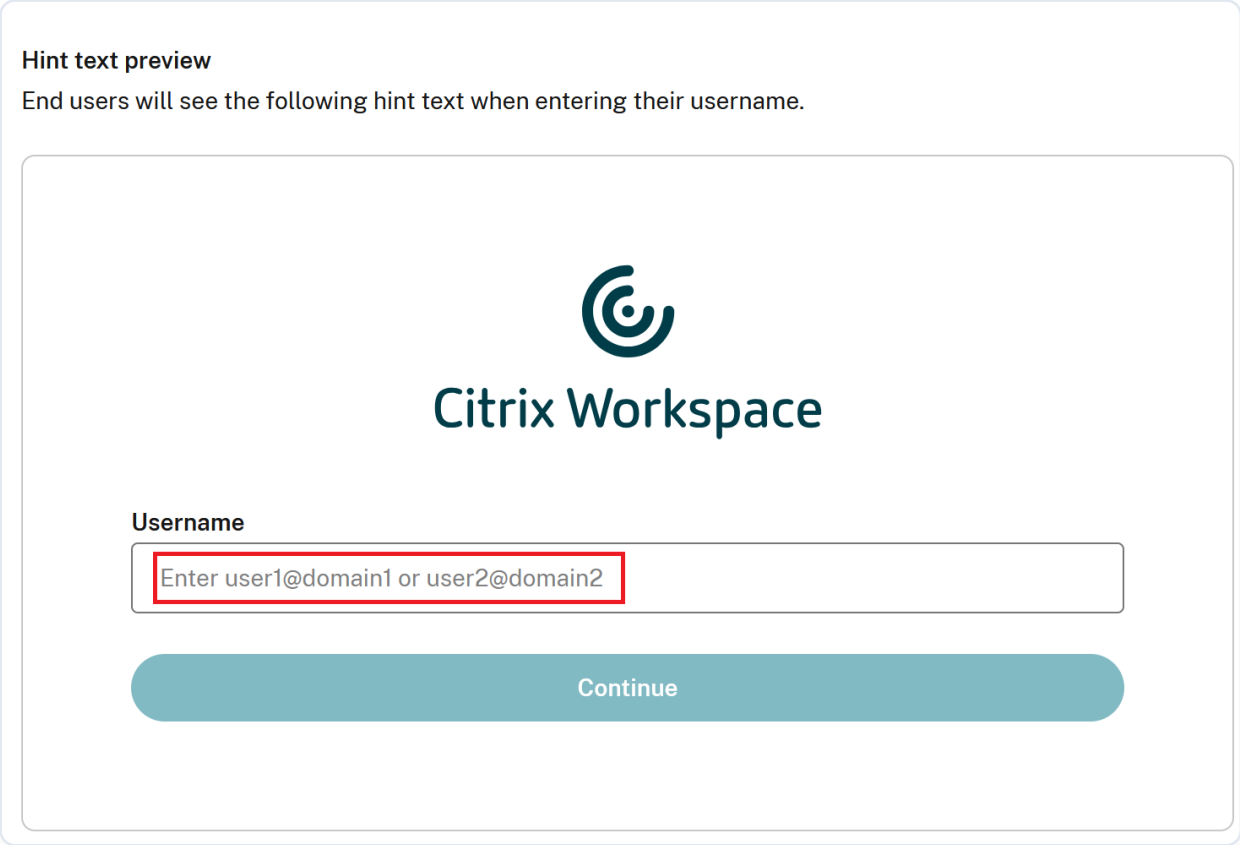


3. 设置您希望在条件身份验证登录流程期间，在预身份验证对话框中显示的“**登录提示文本**”。

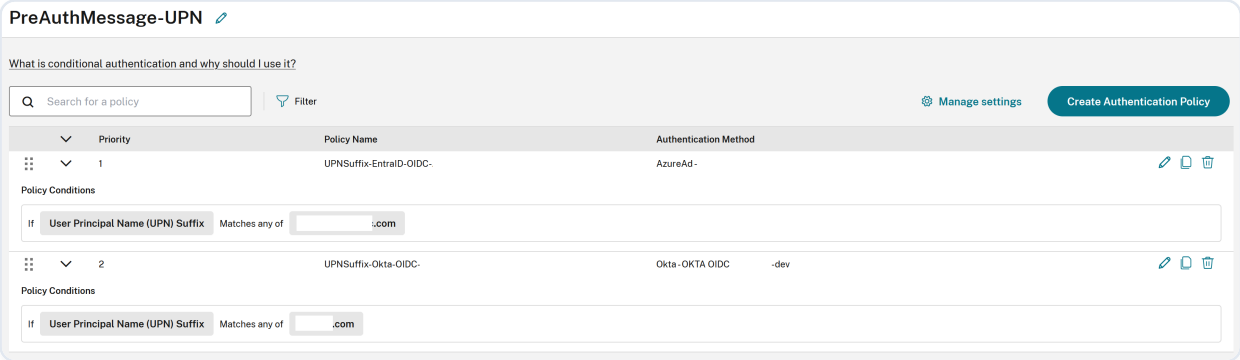


4. 查看预览图像，以了解登录提示文本将如何向最终用户显示。

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



上面显示的示例适用于基于 UPN 的不同 IdP 之间的切换。



5. 单击“**保存**”。

策略条件类型

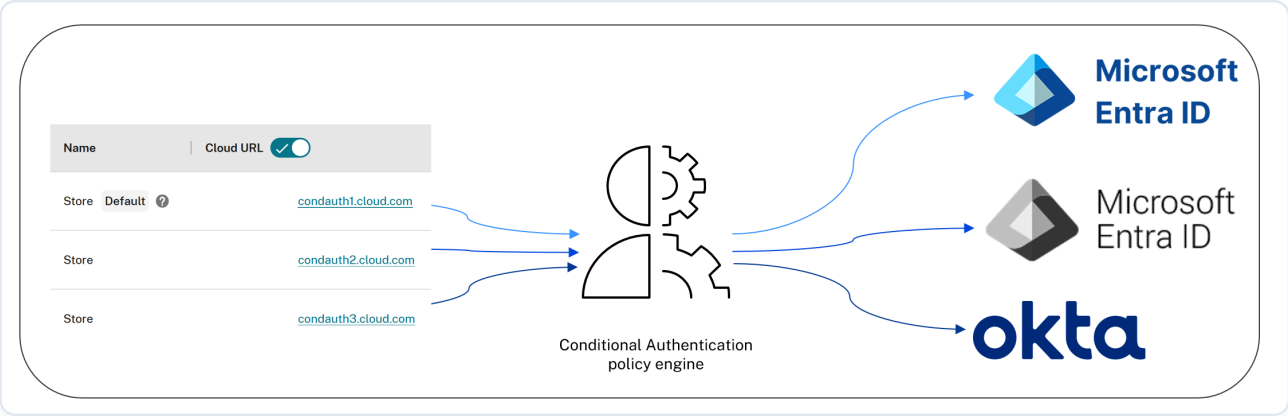
注意：

如果条件身份验证配置文件仅包含商店 URL 条件类型或网络位置名称条件类型的策略，则不会显示预身份验证页面，用户将直接重定向到 IdP。如果配置文件包含任何其他策略条件类型，则会向最终用户显示预身份验证页面。即使匹配策略是商店 URL 或网络位置名称类型，情况也是如此。

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

商店 URL

在 **StoreFront Cloud** > **访问**中，每个商店 URL 都可以链接到不同的 IdP 实例。此外，多个商店 URL 可以与同一策略关联，从而将您的最终用户定向到同一 IdP 实例。



使用商店 URL 或自定义 URL 访问商店

您的最终用户可以根据他们在浏览器中输入的商店 URL 或自定义 URL，或者他们在 Citrix Workspace 应用程序中配置的商店，切换到不同的结果 IdP。

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

Name	Cloud URL	Custom URL
Store Default	1.cloud.com	1. .com
Store	2.cloud.com	2. .com
Store	3.cloud.com	3. .com
Store	4.cloud.com	4. .com
Store	5.cloud.com	5. .com
Store	6.cloud.com	6. .com
Store	7.cloud.com	7. .com
Store	8.cloud.com	8. .com
Store	9.cloud.com	9. .com
Store	10.cloud.com	10. .com

最终用户可以使用这些 URL 之一访问特定的条件身份验证策略结果 IdP 实例。Citrix Cloud 管理员必须向其最终用户提供正确的商店 URL。

`https://workspaces1.cloud.com` URL

或者，

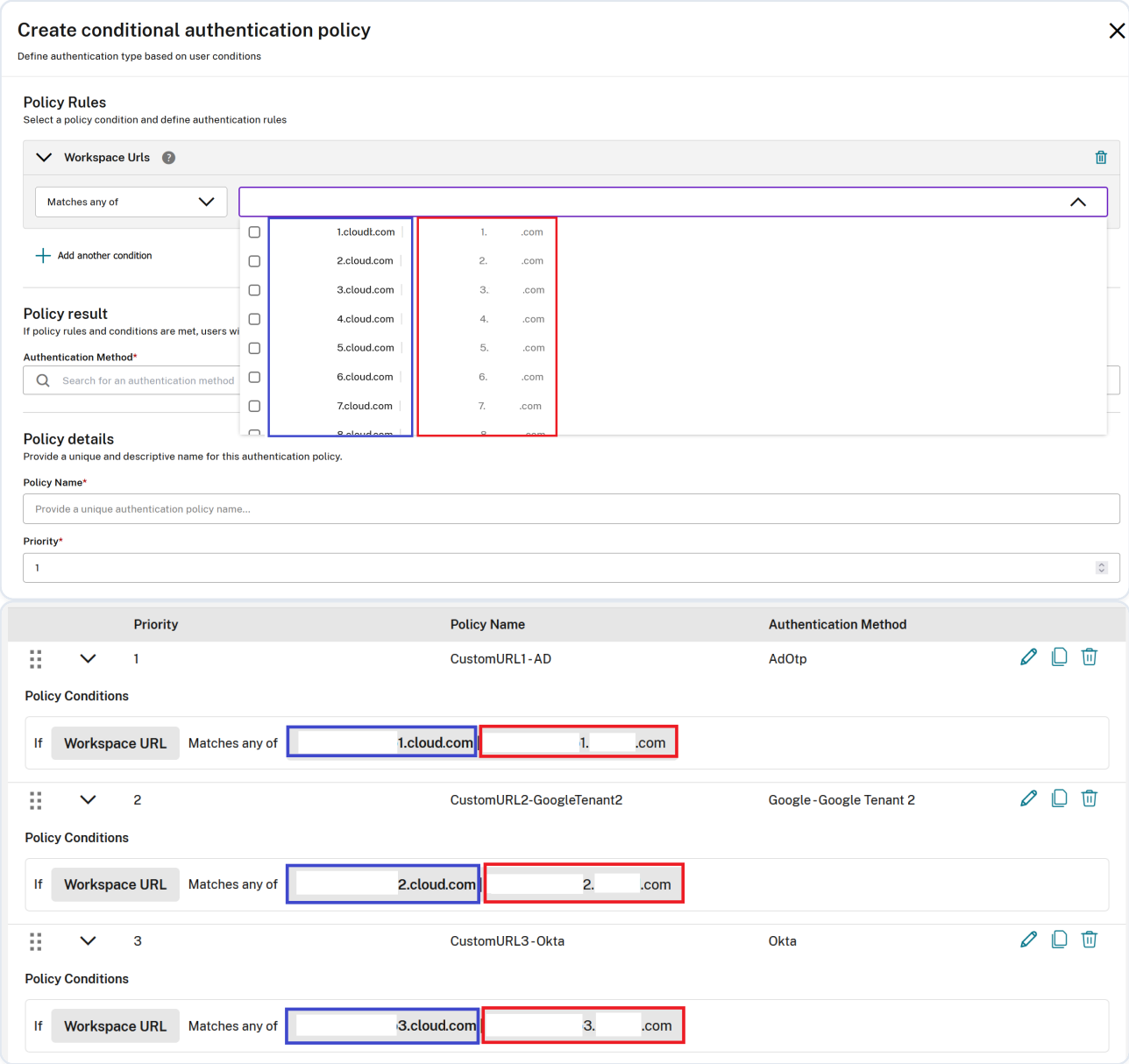
`https://workspaces1.mycompany.com` 自定义 URL

通过使用下拉列表选择一对 URL 来配置条件身份验证策略。

- 以**蓝色**显示的商店 URL，例如 `https://workspaces1.cloud.com`
- 以**红色**显示的自定义 URL，例如 `https://workspaces1.mycompany.com`

使用 URL 对配置条件身份验证策略：

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



重要提示：

未迁移的旧版自定义域不能用于通过条件身份验证访问应用商店。在向最终用户提供自定义 URL 之前，请先迁移这些旧版自定义 URL。如果您的条件身份验证策略解析为 SAML IdP 实例，则还需要考虑其他因素。

有关如何使用 SAML 和自定义 URL 配置条件身份验证的详细说明，请参阅使用自定义域通过 SAML 登录应用商店。

AD 用户组成员身份

AD 用户组成员身份允许您根据 Active Directory 用户的组成员身份，为特定组的 Active Directory 用户指定一个 IdP 实例。

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

UPN 后缀或域向下级别登录名是两个互斥的策略条件。 这些条件决定了最终用户必须在预身份验证页面中输入的所需用户名格式。您不能在同一策略中同时使用这两个条件。

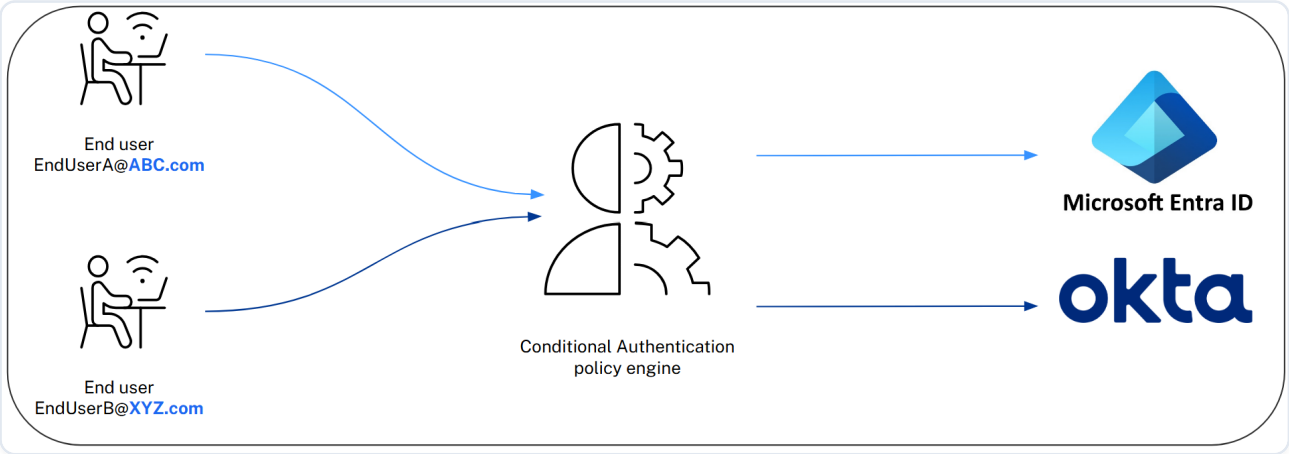
支持直接 AD 组成员身份（推荐）和嵌套 AD 组成员身份。

要求：

- 仅支持**通用** AD 组。
- Citrix Cloud 连接器已加入所需的 AD 林域，以检查用户是哪些 AD 组的成员。
- 对于 AD 组条件，当用户输入其 UPN 时，用户的 UPN 后缀决定了用于执行 AD 组成员身份查找的域上下文。

  \> **重要提示：**

  唯一的 UPN 后缀必须仅在一个连接的 AD 林中定义。不支持在连接到同一 Citrix Cloud 租户的两个或更多 AD 林中出现的模糊 UPN 后缀。



UPN 后缀

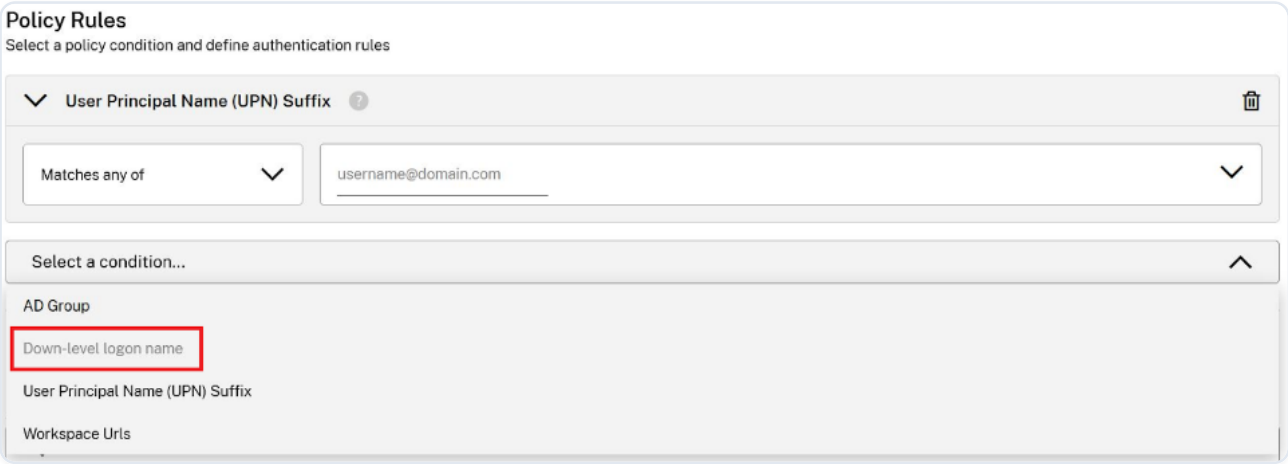
为一个或多个 UPN 后缀配置 IdP 实例，例如 `username1@domain.com` 或 `username2@domain.net`。

域向下兼容登录名

将 IdP 实例分配给一个或多个域名，例如 `DOMAIN1\username1` 或 `DOMAIN1.COM\username1`。

当选择两个互斥条件中的一个时，另一个条件的下拉菜单选项将被禁用，以防止其被添加到同一策略中。

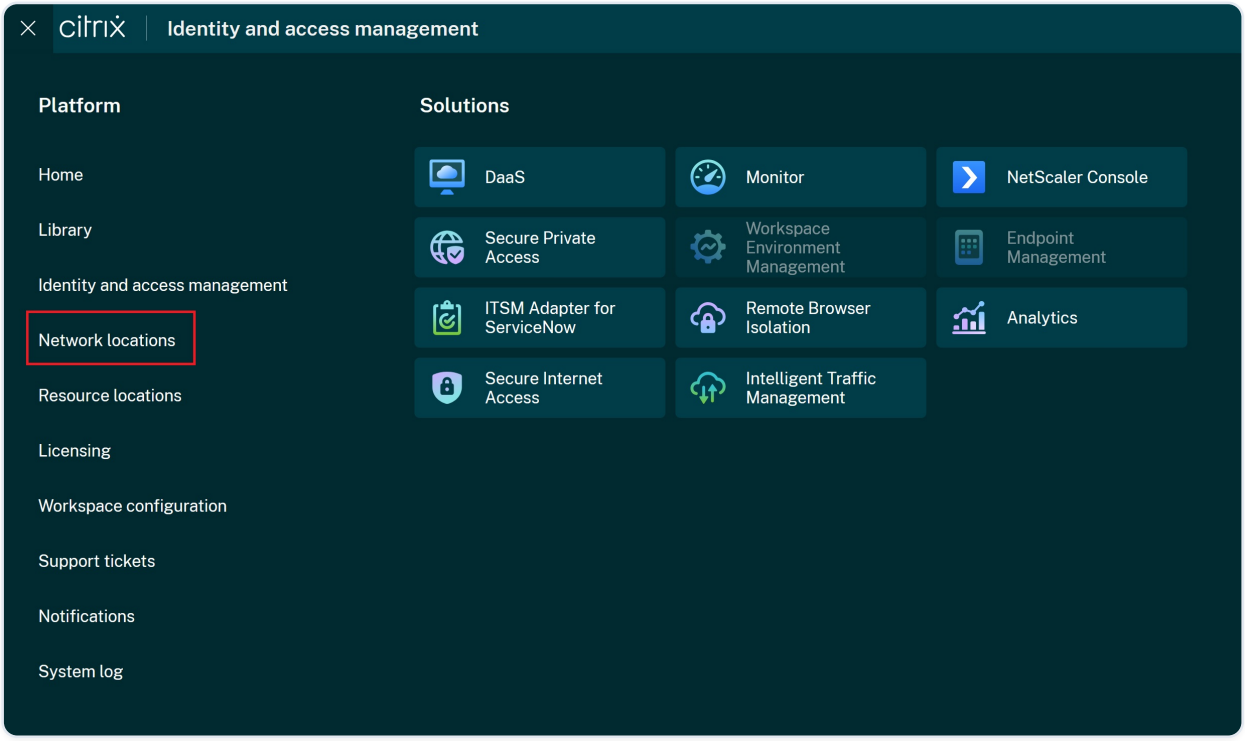
© 1997–2026 Citrix Systems, Inc. All rights reserved.



网络位置名称

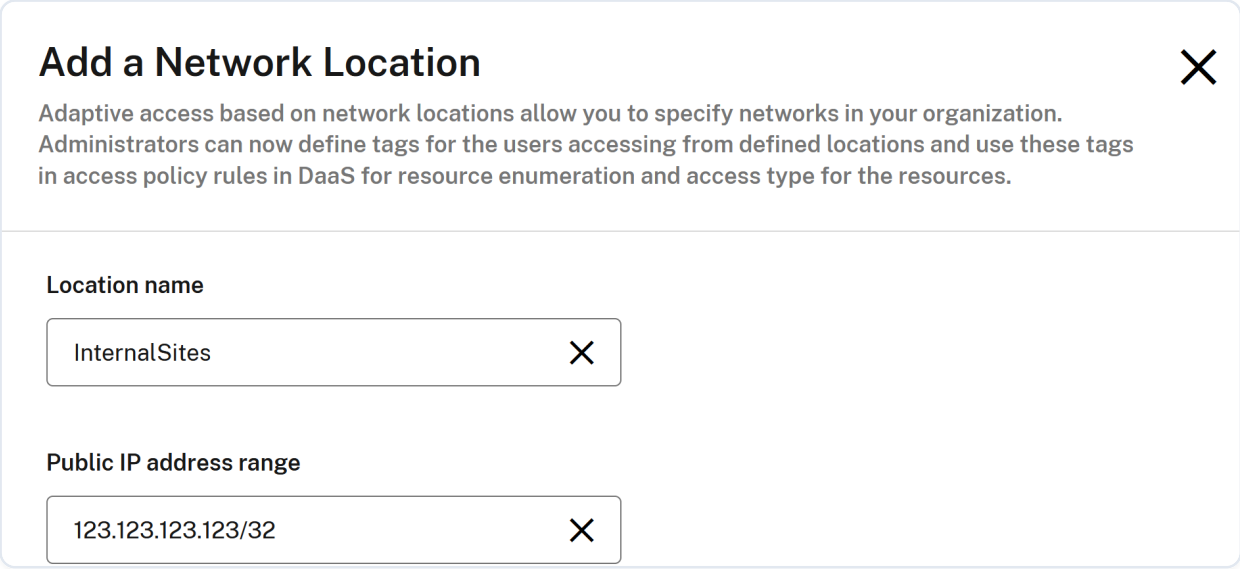
根据客户端公共出站 IP 和网络位置名称分配 IdP 实例。

1. 在“网络位置”下创建您的公共 IP 地址范围。

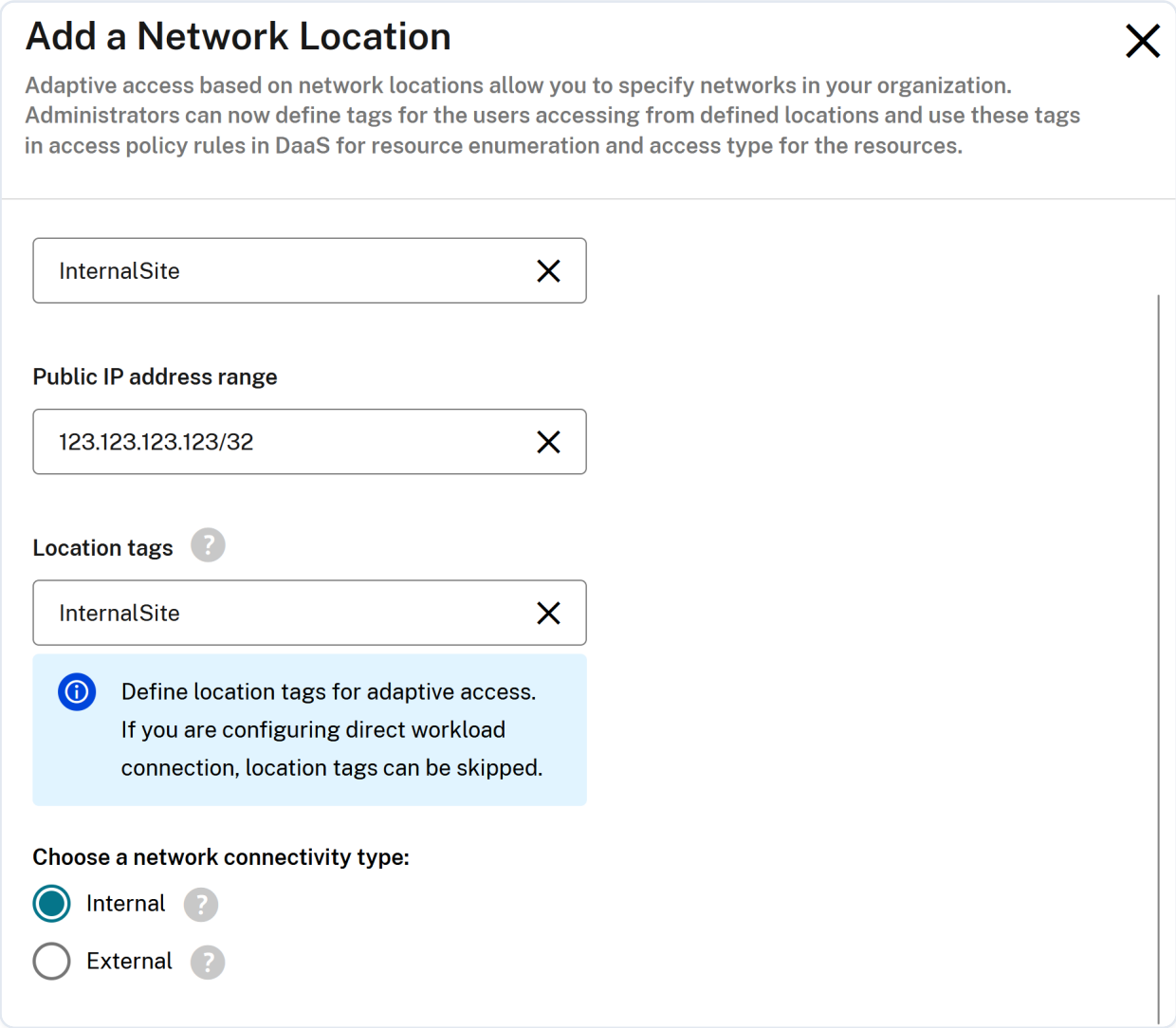


2. 单击“添加网络位置”，输入名称和公共 IP 地址范围（CIDR 表示法）

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

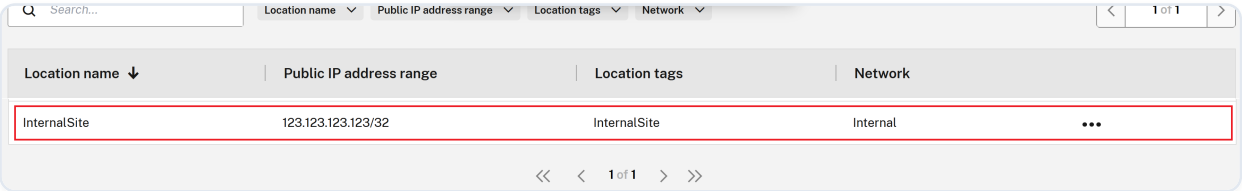


或者，当 Citrix Cloud 租户上启用了智能访问标记时

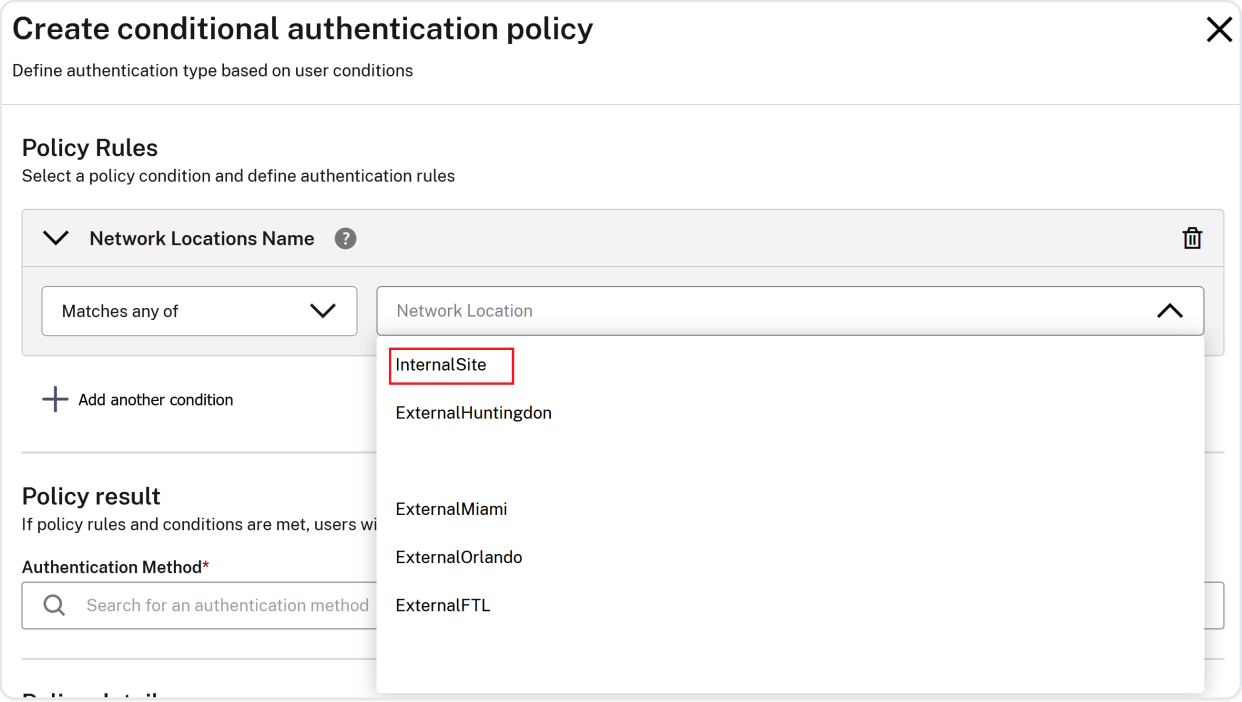


3. 确认网络位置已正确添加。

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



4. 在您的条件身份验证配置文件中，位置名称将预填充。选择所需的位置名称并分配目标 IdP。



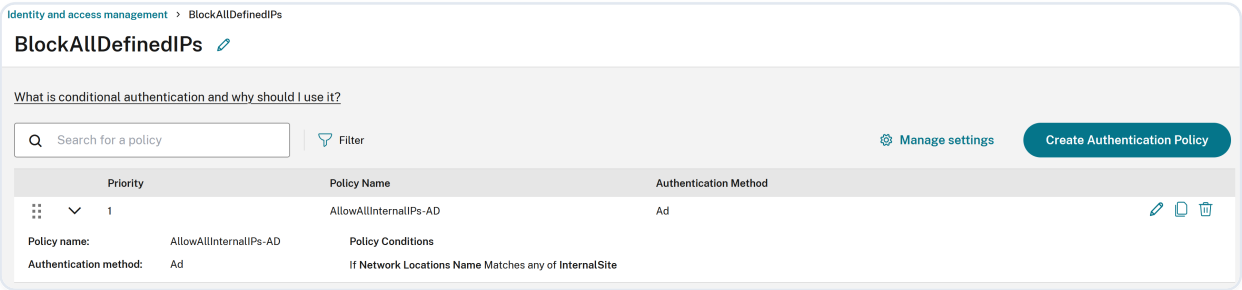
重要提示：

任何未在网络位置站点中明确定义且未被网络位置名称策略引用的客户端出站 IP 都归类为“未定义”。

常见 NLS 用例/配置：

1. **NLS 场景 1**：阻止外部（未定义）IP 进行身份验证和访问商店。

   策略 1：只有在 AllInternalIPs NLS 站点中定义了出站 IP 的内部客户端才能使用 AD 登录商店。

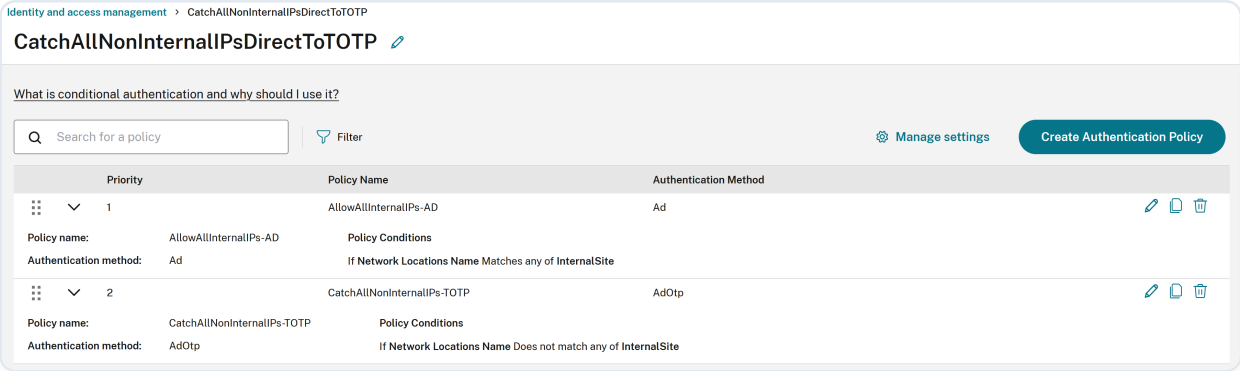


© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. **NLS 场景 2**：将所有“未定义”的出站 IP 定向到“全捕获 IdP 实例”，并增加额外的身份验证因素和/或提高安全性。使用“不匹配任何”和所有内部 NLS 站点的列表来定义一个“捕获所有未定义出站 IP”策略。

   策略 1：只有在 AllInternalIPs NLS 站点中定义了出站 IP 的内部客户端才能使用 AD 登录商店。

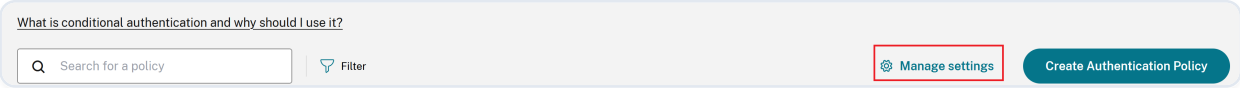
   策略 2：任何未在 AllInternalIPs NLS 站点中定义的外部出站 IP 必须使用 TOTP 登录商店。



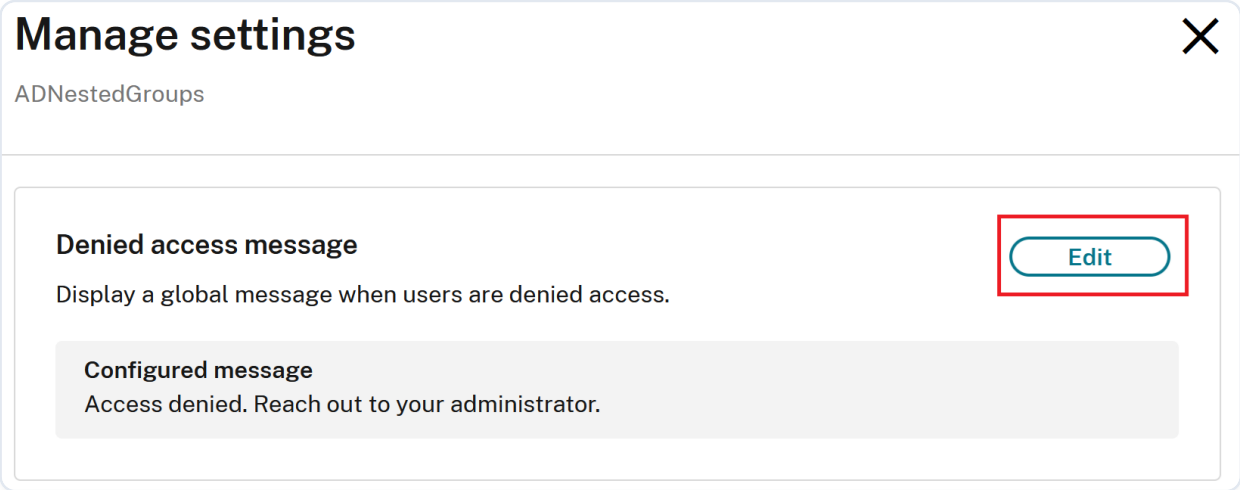
为条件身份验证配置文件设置自定义错误消息

可以配置用户友好的错误消息，当用户的输入与任何策略条件都不匹配时，这些消息将显示给商店最终用户。

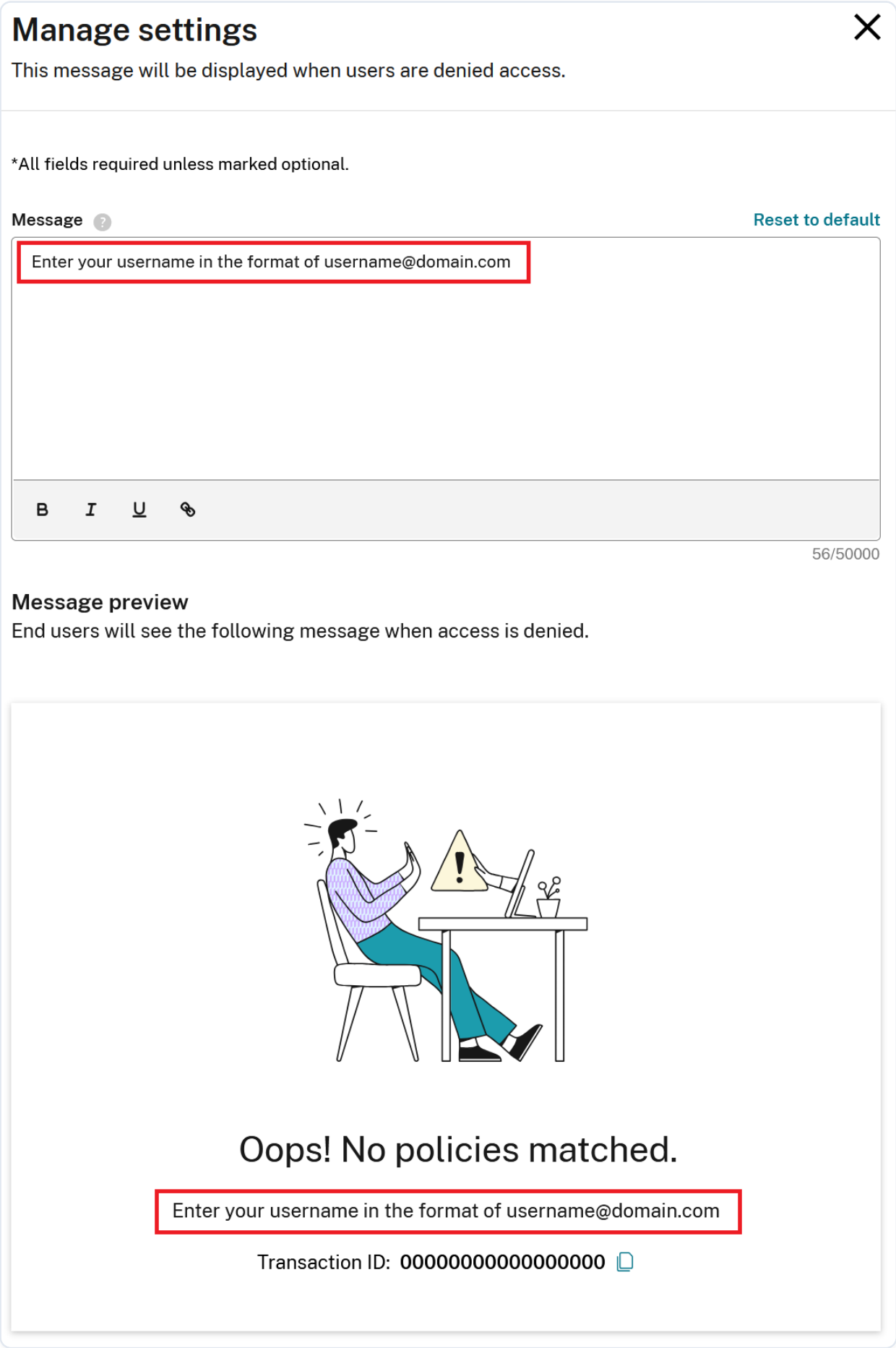
1. 在您的条件身份验证配置文件中，选择 **管理设置**。



2. 编辑将显示给最终用户的默认错误消息。



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



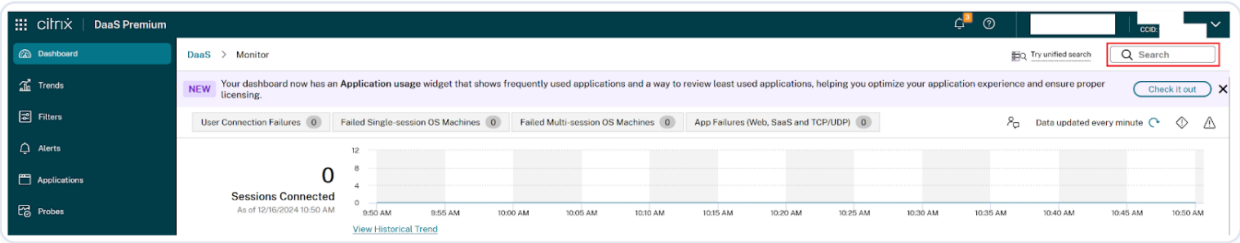
© 1997–2026 Citrix Systems, Inc. All rights reserved.

使用 Citrix 监视器集成进行故障排除

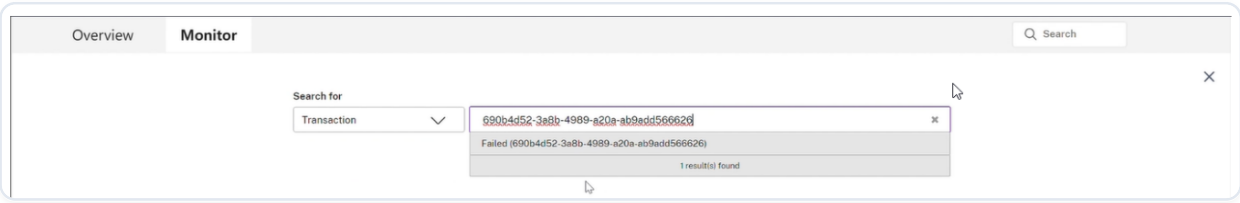
如果用户的登录尝试因缺少匹配策略而失败，将显示一个错误页面，其中包含一个事务 ID。用户可以将此事务 ID 提供给其 Citrix Cloud 管理员以获得进一步帮助。

Citrix Cloud 管理员可以将商店最终用户提供的事务 ID 粘贴到 Citrix Monitor 中，以访问有关策略、输入的用户名以及关联的条件身份验证策略的详细信息。此信息有助于管理员更高效地排查和解决条件身份验证问题。

1. 选择 **监视器**，然后单击右上角的搜索框。

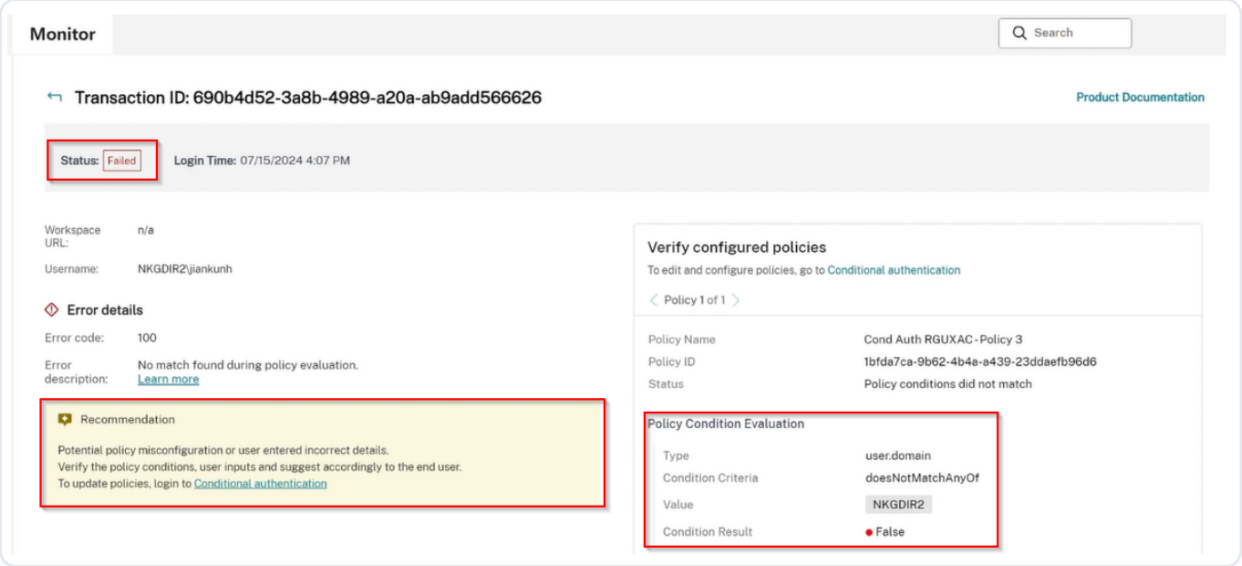


2. 从下拉列表中选择事务 ID。仅提供过去 3 天的事务。



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

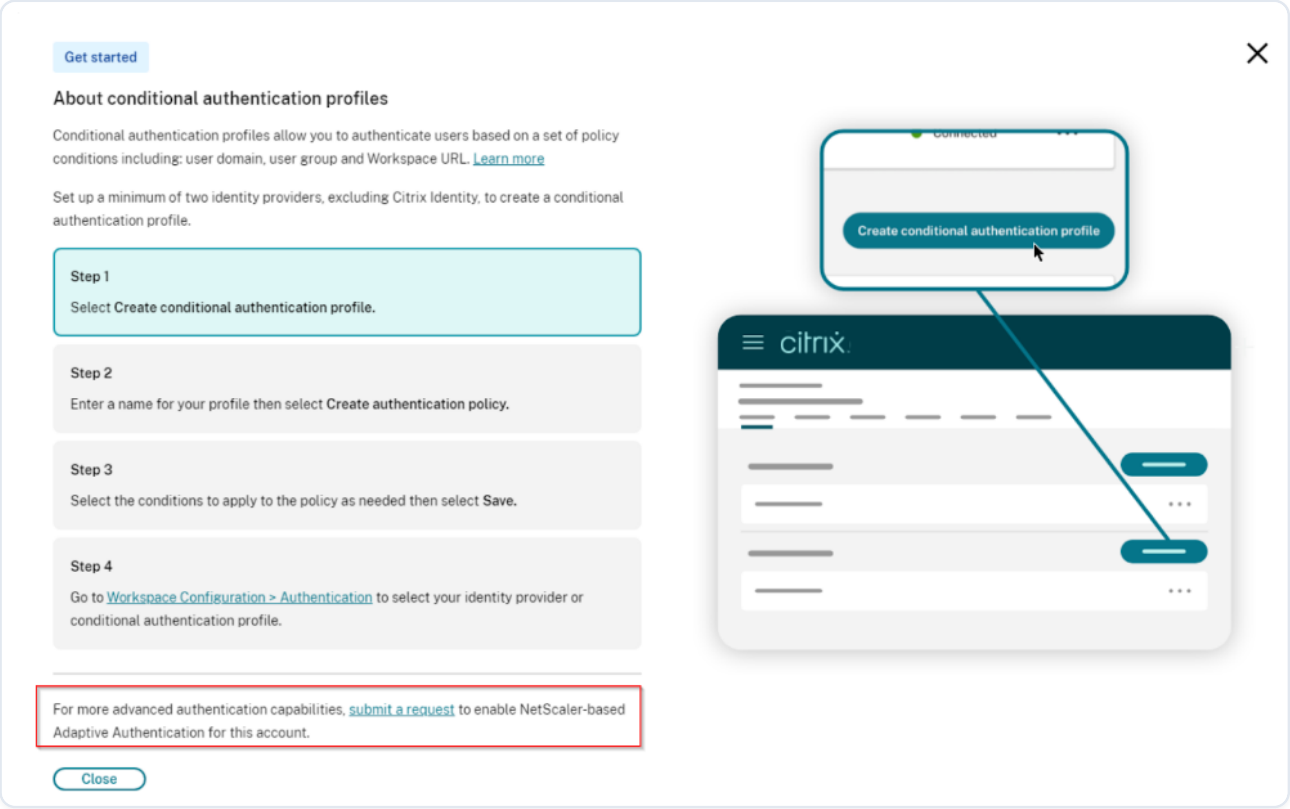
3. 查看最终用户的失败事务，以及已评估的条件身份验证策略的详细信息。您可以单击 V 形按钮来浏览所有已评估的策略，例如最终用户的 <Policy 1 of 3>。



云原生条件身份验证与基于 NetScaler 的自适应身份验证的比较

云原生条件身份验证功能旨在涵盖大多数条件身份验证用例。但是，对于更高级的身份验证功能，可以使用基于 NetScaler 的自适应身份验证。

要使用基于 NetScaler 的自适应身份验证，请通过 Citrix Cloud 的“**身份和访问管理**”页面 >“**条件身份验证配置文件**”部分提交请求。



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

已知问题和限制

- 为策略设置负优先级未按预期运行。将在未来的更新中解决。
- 目前，组条件仅支持 Active Directory。原生的 Entra Id 组条件将在未来添加。

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

身份提供程序

将活动目录连接到 Citrix Cloud™

Citrix Cloud 支持使用您的本地 Active Directory (AD) 来验证最终用户。此外，某些应用商店身份验证方法要求您的 AD 与 Citrix Cloud 之间建立连接。有关详细信息，请参阅 选择或更改身份验证方法。

Citrix Cloud 还支持使用令牌作为通过 Active Directory 登录其应用商店的最终用户的第二重身份验证因素。最终用户可以使用任何遵循 基于时间的一次性密码 标准的应用程序（例如 Citrix SSO）生成令牌。

有关使用 Active Directory 加令牌验证最终用户的详细信息，请参阅 Active Directory 加令牌。

提示：

通过 Citrix 身份和身份验证简介 培训课程了解有关受支持的身份提供程序的更多信息。“规划 Citrix 身份和访问管理”模块包含短视频，可指导您将此身份提供程序连接到 Citrix Cloud 并为 Citrix® StoreFront Cloud 启用身份验证。

连接活动目录

将 Active Directory 连接到 Citrix Cloud 涉及在您的域中安装连接器。您可以选择使用 Cloud Connector 或 Connector Appliance 作为 Active Directory 的连接器。要选择适合您环境的连接器类型，请参阅以下文章：

- Active Directory 中 Cloud Connector 的部署方案
- Active Directory 中 Connector Appliance 的部署方案

通过连接器设备连接 Active Directory

您可以使用 Connector Appliance 将资源位置连接到不包含 Citrix Virtual Apps and Desktops™ 资源的林。例如，对于 Citrix Secure Private Access 客户或 Citrix Virtual Apps and Desktops 客户，某些林仅用于用户身份验证。

有关详细信息，请参阅 带有 Connector Appliance 的 Active Directory

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

通过云连接器连接 Active Directory

至少需要两个 Cloud Connector 才能确保与 Citrix Cloud 的高可用性连接。有关详细信息，请参阅以下文章：

- Cloud Connector 系统要求。
- Cloud Connector 技术详细信息：有关部署建议。
- Cloud Connector 安装：有关使用图形界面或命令行进行安装的说明。

将您的 Active Directory 连接到 Citrix Cloud 涉及以下任务：

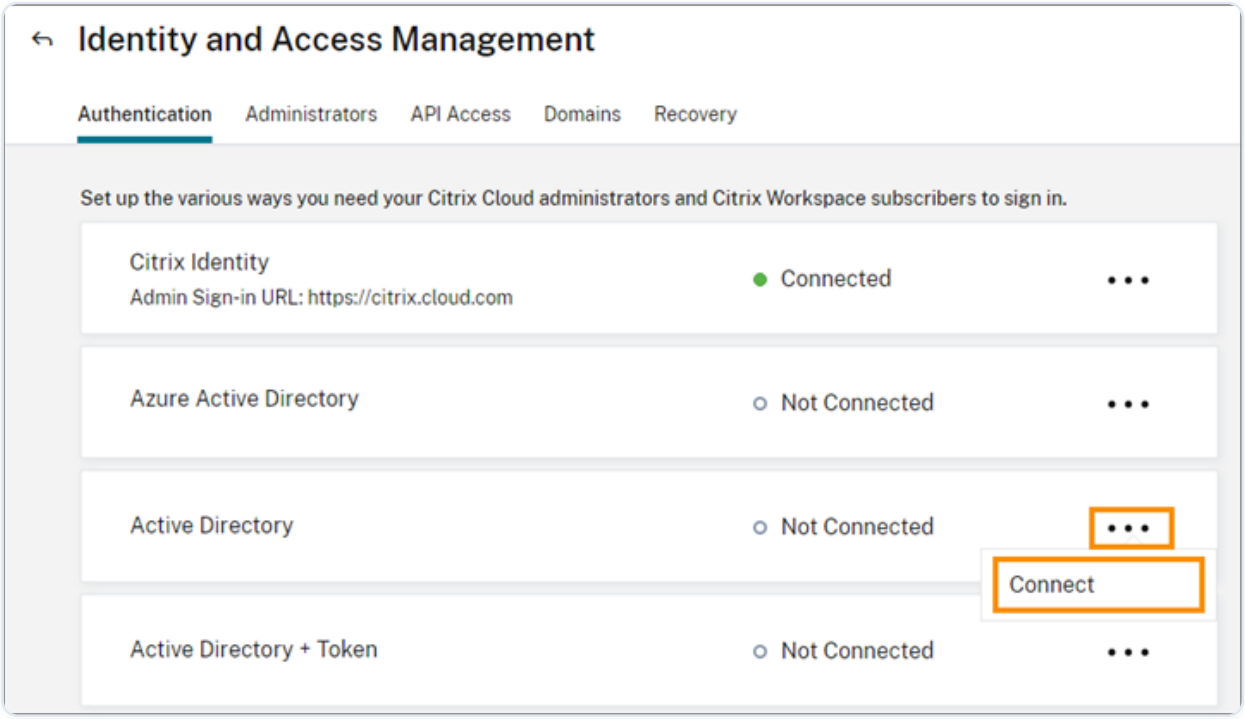
1. 安装 Cloud Connector 在您的域中。Citrix 建议安装两个 Cloud Connector 以实现高可用性。
2. 如果适用，为用户设备启用令牌。最终用户一次只能注册一台设备。

重要提示：

如果您正在部署 Cloud Connector 以与 Citrix DaaS 配合使用，则可能需要执行其他步骤以确保您的 AD 域在 Cloud Connector 部署后已注册并处于活动状态。验证您的 AD 域在 Citrix Cloud 中处于活动状态可确保计算机目录设置顺利进行。有关 Citrix DaaS 部署后步骤的更多信息，请参阅 Citrix DaaS 产品文档中的 在 Citrix Cloud 中添加资源类型或激活未使用的域。

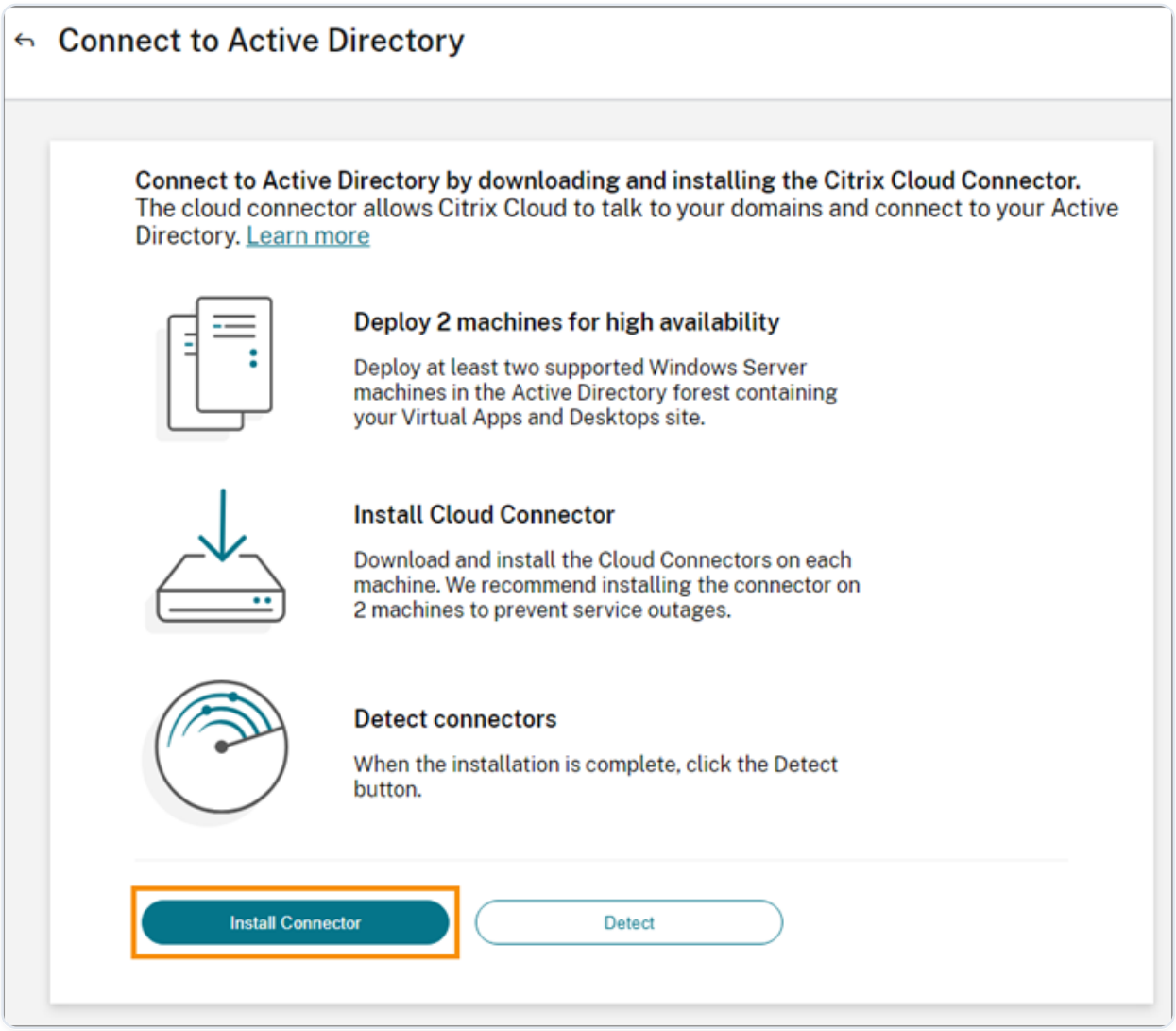
将您的 Active Directory 连接到 Citrix Cloud

1. 在 Citrix Cloud 菜单中，选择 **身份和访问管理**。
2. 在 **身份验证** 选项卡中，在 **Active Directory** 下，单击省略号菜单并选择 **连接**。



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

3. 单击 **安装连接器** 以下载 Cloud Connector 软件。



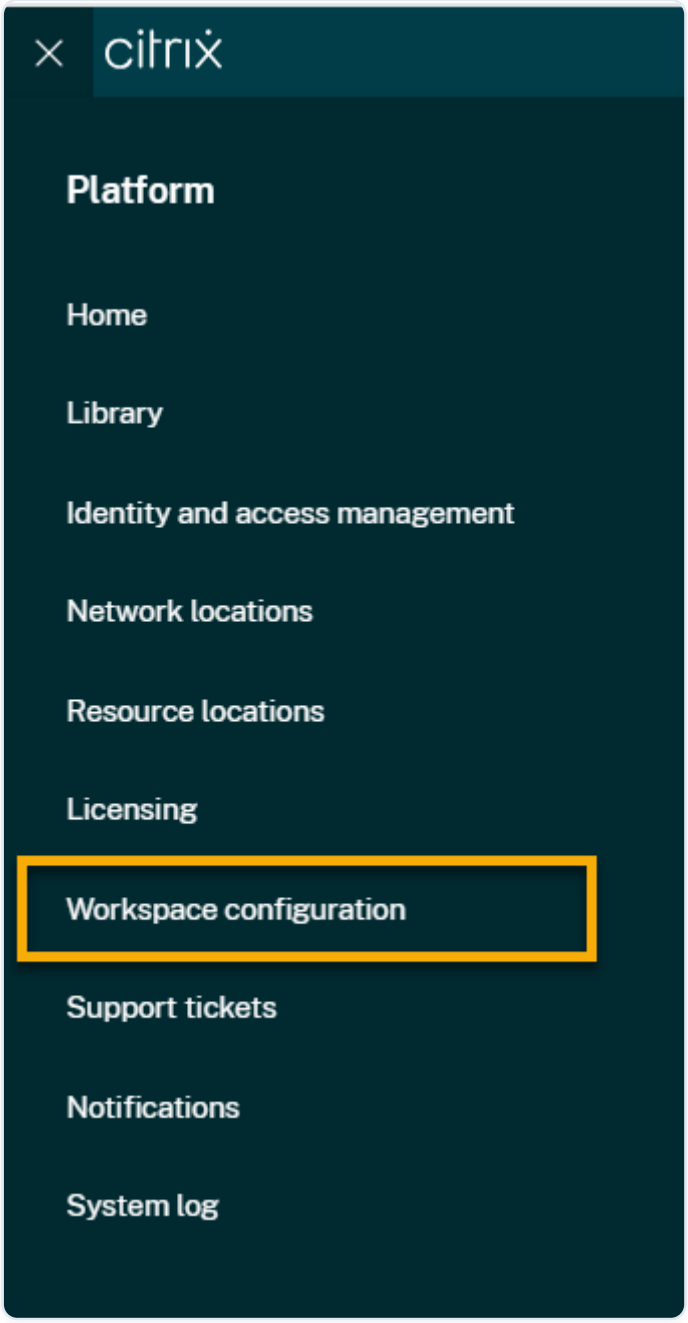
4. 启动 Cloud Connector 安装程序并按照安装向导进行操作。
5. 在 **连接到 Active Directory** 页面上，单击 **检测**。验证后，Citrix Cloud 将显示一条消息，指示您的 Active Directory 已连接。
6. 单击 **返回身份验证**。在 **身份验证** 选项卡上，**Active Directory** 条目标记为 **已启用**。

启用 Active Directory 加令牌身份验证

1. 使用连接器设备或云连接器将 Active Directory 连接到 Citrix Cloud。
2. 在 Citrix Cloud 的“**身份和访问管理**”部分中，在“**身份验证**”选项卡上，检查“**Active Directory**”条目是否标记为“**已启用**”。
3. 单击“**下一步**”。将显示“**配置令牌**”页面，并且默认选中“**单个设备**”选项。
4. 单击“**保存并完成**”以完成配置。在“**身份验证**”选项卡上，“**Active Directory + 令牌**”条目标记为“**已启用**”。
5. 为应用商店启用令牌身份验证：

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

a. 从 Citrix Cloud 菜单中，选择“**StoreFront Cloud**”。



b. 在“**身份验证**”选项卡上，选择“**Active Directory + 令牌**”。

启用 Active Directory 加令牌身份验证后，最终用户可以注册其设备并使用身份验证器应用程序生成令牌。最终用户一次只能注册一台设备。有关注册最终用户设备的说明，请参阅双因素身份验证（可选）。

有关重新注册最终用户设备的选项，请参阅重新注册设备。

更多信息

Citrix 技术区：

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

- 技术洞察：身份验证 - TOTP
- 技术洞察：身份验证 - 推送

建立 微软 Entra ID 与 Citrix Cloud™ 的连接

Citrix Cloud 支持使用 Microsoft Entra ID (ME-ID) 对 Citrix Cloud 管理员和最终用户进行身份验证。

通过将 Microsoft Entra ID 与 Citrix Cloud 结合使用，您可以：

- 利用您自己的 Active Directory，以便您可以控制审计、密码策略，并在需要时轻松禁用帐户。
- 配置多重身份验证，以获得更高级别的安全性，防止登录凭据被盗。
- 使用品牌登录页面，以便您的用户知道他们正在正确的位置登录。
- 使用联合身份验证连接到您选择的身份提供程序，包括 ADFS、Okta 和 Ping 等。

Microsoft Entra ID 应用程序和权限

Citrix Cloud 包含一个 Microsoft Entra ID 应用程序，该应用程序允许 Citrix Cloud 连接到 Microsoft Entra ID，而无需您登录到活动的 Microsoft Entra ID 会话。自此应用程序推出以来，Citrix 发布了更新，以提高性能并支持新功能和权限。

如果您已有一个到 Citrix Cloud 的现有 Microsoft Entra ID 连接，并希望使用最新更新的应用程序，您需要在 Citrix Cloud 中更新您的 Microsoft Entra ID 连接。有关详细信息，请参阅本文中的 重新连接到 Microsoft Entra ID 以使用更新的应用程序。如果您选择不更新应用程序，则现有连接将继续正常运行。

有关 Citrix Cloud 用于连接您的 Microsoft Entra ID 的 Microsoft Entra ID 应用程序和权限的详细信息，请参阅 Citrix Cloud 的 Microsoft Entra ID 权限。

提示：

通过 Citrix 身份和身份验证简介 教育课程了解有关受支持的身份提供程序的更多信息。“规划 Citrix 身份和访问管理”模块包含简短视频，可指导您将此身份提供程序连接到 Citrix Cloud 并为 Citrix® StoreFront Cloud 启用身份验证。

使用多个 Citrix Cloud 帐户进行身份验证

本文介绍了如何将您的 Microsoft Entra ID 作为身份提供程序连接到单个 Citrix Cloud 帐户。如果您有多个 Citrix Cloud 帐户，可以将每个帐户连接到同一个 Microsoft Entra ID 租户。执行以下任务：

1. 登录您的 Citrix Cloud 帐户，并从客户选择器中选择相应的客户 ID。

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

2. 如果所选客户是您首次连接到 Microsoft Entra ID 的客户，请按照本文中的所有步骤同步您的 AD 和 Microsoft Entra ID，将客户连接到 Citrix Cloud，并添加管理员。
3. 要连接其他客户，请单击 Citrix Cloud 控制台右上角的用户菜单，选择 **更改客户**，然后选择要连接的下一个客户 ID。
4. 按照本文中 (#connect-citrix-cloud-to-microsoft-entra-id) 所述，将客户连接到您的 Microsoft Entra ID。
5. 对每个客户 ID 重复步骤 3 和 4。

准备您的 活动目录 和 微软 Entra ID

在使用 Microsoft Entra ID 之前，请确保满足以下要求：

- 您拥有一个 Microsoft Azure 帐户。每个 Azure 帐户都免费附带 Microsoft Entra ID。如果您没有 Azure 帐户，请在 https://azure.microsoft.com/zh-cn/free/?v=17.36 注册。
- 您在 Microsoft Entra ID 中拥有全局管理员角色。此角色是 Citrix Cloud 连接到 Microsoft Entra ID 所需的同意。
- 管理员帐户在 Microsoft Entra ID 中配置了“邮件”属性。为此，您可以使用 Microsoft 的 Microsoft Entra ID Connect 工具将本地 Active Directory 中的帐户同步到 Microsoft Entra ID。或者，您可以为未同步的 Microsoft Entra ID 帐户配置 Office 365 电子邮件。

使用 Microsoft Entra ID Connect 同步帐户

1. 确保 Active Directory 帐户已配置“电子邮件”用户属性：
   a. 打开 Active Directory 用户和计算机。
   b. 在 **用户** 文件夹中，找到要检查的帐户，右键单击并选择 **属性**。在 **常规** 选项卡上，验证 **电子邮件** 字段是否包含有效条目。Citrix Cloud 要求从 Microsoft Entra ID 添加的管理员具有与使用 Citrix 托管身份登录的管理员不同的电子邮件地址。
2. 安装并配置 Microsoft Entra ID Connect。有关完整说明，请参阅 Microsoft Azure 网站上的 使用快速设置开始使用 Microsoft Entra ID Connect。

将 思杰云 连接到 Microsoft Entra 标识

当您将 Citrix Cloud 帐户连接到 Microsoft Entra ID 时，Citrix Cloud 需要权限才能访问您的用户配置文件（或已登录用户的配置文件），以及 Microsoft Entra ID 中用户的基本配置文件。Citrix 请求此权限是为了获取您的姓名和电子邮件地址（作为管理员），并使您能够浏览其他用户并稍后将其添加为管理员。有关 Citrix Cloud 请求的应用程序权限的更多信息，请参阅 Citrix Cloud 的 Microsoft Entra ID 权限。

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

重要提示：

您必须是 Microsoft Entra ID 中的全局管理员才能完成此任务，或者要求任何全局管理员在登录 Citrix Cloud 之前执行先决条件。

1. 单击页面左上角的“**菜单**”，然后选择“**身份和访问管理**”。
2. 找到 Microsoft Entra ID，然后从省略号菜单中选择“**连接**”。
3. 出现提示时，为您的公司输入一个简短的、URL 友好的标识符，然后单击“**连接**”。您选择的标识符在 Citrix Cloud 中必须是全局唯一的。
4. 出现提示时，登录到您要连接的 Azure 帐户。Azure 会显示 Citrix Cloud 访问该帐户并获取连接所需信息的权限。这些权限大多数是只读的，允许 Citrix Cloud 从您的 Microsoft Graph 收集基本信息，例如组和用户配置文件。如果您将 Citrix Endpoint Management 或 XenMobile Server 与 Microsoft Intune 集成，则必须授予与 Microsoft Intune 相关的读写权限。有关更多信息，请参阅 Citrix Cloud 的 Microsoft Entra ID 权限。
5. 单击“**接受**”以接受权限请求。

备用连接方法

您可以将连接流程分为以下两个阶段：

1. 在 Azure 中创建 Microsoft Entra ID 应用程序。
2. Citrix Cloud 连接到 Citrix Cloud 中的 Microsoft Entra ID 应用程序。

首先，您需要构建一个 URL，全局管理员可以使用该 URL 将企业应用程序添加到租户中。有关更多信息，请参阅 构建用于授予租户范围管理员同意的 URL。

以下是所构建 URL 的说明。 `https://login.microsoftonline.com/<tenant url>/adminconsent?client_id=f9c0e999-22e7-409f-bb5e-956986abdf02&redirect_uri=https://portal.azure.com`

其中： `tenant url` 是您的租户 URL 或 ID。 `f9c0e999-22e7-409f-bb5e-956986abdf02` 是 Citrix Cloud 的客户端 ID。

从 Microsoft Entra ID 将管理员添加到 Citrix Cloud

Citrix Cloud 支持单独添加管理员或以 Microsoft Entra ID 组的形式添加管理员。

要从 Microsoft Entra ID 添加单个管理员，请参阅管理管理员访问权限。

要将 Microsoft Entra ID 管理员组添加到 Citrix Cloud，请参阅管理管理员组。

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

使用 Microsoft Entra 标识 登录 思杰云

连接 Microsoft Entra ID 用户帐户后，用户可以使用以下方法之一登录 Citrix Cloud：

- 导航到您在首次连接公司的 Microsoft Entra ID 身份提供程序时配置的管理员登录 URL。示例：`https://citrix.cloud.com/go/mycompany`
- 在 Citrix Cloud 登录页面上，单击**使用我的公司凭据登录**，键入您在首次连接 Microsoft Entra ID 时创建的标识符（例如，“mycompany”），然后单击**继续**。

为应用商店启用 Microsoft Entra ID 身份验证

将 Microsoft Entra ID 连接到 Citrix Cloud 后，您可以允许最终用户通过 Microsoft Entra ID 对其应用商店进行身份验证。

重要提示：

在启用 Microsoft Entra ID 应用商店身份验证之前，请查看Microsoft Entra ID 部分，了解将 Microsoft Entra ID 与应用商店结合使用的注意事项。

1. 在 Citrix Cloud 中，单击左上角的菜单按钮，然后选择 **StoreFront Cloud**。
2. 在**身份验证**选项卡中，选择 **Microsoft Entra ID**。
3. 点击 **确认** 以接受在启用 Microsoft Entra ID 身份验证时将发生的商店体验更改。

启用高级 Microsoft Entra ID 功能

Microsoft Entra ID 提供高级多重身份验证、世界一流的安全功能、与 20 个不同身份提供程序的联合，以及自助式密码更改和重置等诸多功能。为您的 Microsoft Entra ID 用户启用这些功能后，Citrix Cloud 将能够自动利用这些功能。

要比较 Microsoft Entra ID 服务级别功能和定价，请参阅 https://azure.microsoft.com/zh-cn/pricing/details/active-directory/。

重新连接到 Microsoft Entra ID 以使用更新的应用程序

Citrix Cloud 包含一个 Microsoft Entra ID 应用程序，该应用程序允许 Citrix Cloud 连接到 Microsoft Entra ID，而无需您登录到活动的 Microsoft Entra ID 会话。自此应用程序推出以来，Citrix 已按如下方式更新了该应用程序：

- 2018 年 8 月，该应用程序已更新，以提高性能并让您为将来的版本做好准备。

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

- 2019 年 5 月，该应用程序已更新以支持将 Microsoft Entra ID 管理员组 (/zh-cn/citrix-cloud/citrix-cloud-management/identity-access-management/administrator-groups.html) 添加到 Citrix Cloud。
- 2022 年 4 月，该应用程序已更新，以使用 GroupMember.Read.All 权限，该权限取代了 Group.Read.All 权限。

如果您在这些更新发布之前将 Microsoft Entra ID 连接到 Citrix Cloud，并且想要使用最新的更新应用程序，则需要断开 Microsoft Entra ID 与 Citrix Cloud 的连接，然后重新连接。使用最新应用程序是可选的。如果您选择不更新应用程序，则现有连接仍可正常运行。

要求

在重新连接 Microsoft Entra ID 之前，请验证您是否满足以下要求：

- 您必须是默认 Citrix 身份提供程序下具有完全访问权限的管理员。如果您使用 Microsoft Entra ID 凭据登录到 Citrix Cloud，则重新连接将失败。如果您的帐户中没有任何使用 Citrix 身份提供程序的管理员，您可以暂时添加一个，并在重新连接 Microsoft Entra ID 后将其删除。有关说明，请参阅 (/zh-cn/citrix-cloud/citrix-cloud-management/identity-access-management/add-admins.html#invite-individual-administrators)。
- 如果您正在使用 Microsoft Entra ID 对最终用户进行身份验证，请暂时选择其他身份提供程序。如果 Microsoft Entra ID 也用作 StoreFront Cloud 的身份验证方法，Citrix Cloud 不允许您断开其连接。有关详细信息，请参阅 StoreFront Cloud 文档中的 (/zh-cn/citrix-workspace/secure.html#choose-or-change-authentication-methods)。

重新连接 Microsoft Entra ID

1. 以在 Citrix 身份提供商下具有完全访问权限的管理员身份登录 Citrix Cloud。
2. 从 Citrix Cloud 菜单中，选择 **身份和访问管理**，然后选择 **身份验证**。
3. 找到 **Microsoft Entra ID**，然后从页面最右侧的省略号菜单中选择 **断开连接**。
4. 从省略号菜单中，选择 **连接**。

注意：

如果您按照步骤 3 中所述断开 Microsoft Entra ID 的连接，Citrix Cloud 会要求管理员删除此身份提供商下的所有管理员配置文件。 为避免此操作，管理员可以按照以下步骤重新连接 Microsoft Entra ID 身份提供商。

1. 作为全局管理员，导航到 Azure 并删除应用程序。

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

2. 登录 Citrix Cloud 并导航到 **身份和访问管理**，然后单击 **身份验证**。在 **身份验证** 选项卡中，您会注意到 Microsoft Entra ID 仍处于连接状态。
3. 在 Citrix Cloud 中为 Microsoft Entra ID 添加新的管理员。

这将触发应用程序的重新创建和重新连接，而无需删除管理员。

Citrix Cloud™ 的 微软 Entra ID 权限

本文介绍了 Citrix Cloud 在连接和使用 Microsoft Entra ID (ME-ID) 时请求的权限。根据 Microsoft Entra ID 与 Citrix Cloud 帐户的使用方式，目标 Microsoft Entra ID 租户中可能会创建一个或多个企业应用程序。您可以将多个 Citrix Cloud 帐户连接到一个 Microsoft Entra ID 租户，并使用相同的企业应用程序，而无需为每个帐户创建一组应用程序。

注意：

截至 2022 年 4 月，Citrix Cloud 用于连接您的 Microsoft Entra ID 的 Microsoft Entra ID 应用程序已更新为使用 GroupMember.Read.All 权限，而不是 Group.Read.All 权限。如果您有现有的 Microsoft Entra ID 连接（2022 年 4 月之前），并且希望应用程序使用新权限，则必须断开连接，然后将您的 Microsoft Entra ID 重新连接到 Citrix Cloud。此操作可确保您的帐户在 Citrix Cloud 中使用最新的 Microsoft Entra ID 应用程序。有关详细信息，请参阅重新连接到 Microsoft Entra ID 以获取升级后的应用程序。

如果您选择不更新应用程序，则现有连接仍可正常运行。

企业应用程序

下表列出了 Citrix Cloud 在连接和使用 Microsoft Entra ID 时使用的 Microsoft Entra ID 企业应用程序，以及每个应用程序的用途。

名称	应用程序 ID	用途
思杰云	e95c4605-aeab-48d9-9c36-1a262ef8048e	商店最终用户登录
思杰云	f9c0e999-22e7-409f-bb5e-956986abdf02	Microsoft Entra ID 与 Citrix Cloud 之间的默认连接 (#default-connection-between-microsoft-entra-id-and-citrix-cloud)

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

名称	应用程序 ID	用途
思杰云	1b32f261-b20c-4399-8368-c8f0092b4470	管理员邀请和登录(#administrator-invitations-and-logins)
思杰云	5c913119-2257-4316-9994-5e8f3832265b	Microsoft Entra ID 与 Citrix Cloud 之间通过 Citrix Endpoint Management™ 的默认连接(#default-connection-between-microsoft-entra-id-and-citrix-cloud-with-endpoint-management)
思杰云	e067934c-b52d-4e92-b1ca-70700bd1124e	Microsoft Entra ID 与 Citrix Cloud 之间通过 Citrix Endpoint Management 的旧版连接(#legacy-connection-between-microsoft-entra-id-and-citrix-cloud-with-endpoint-management)

权限

Citrix Cloud 企业应用程序中的权限允许 Citrix Cloud 访问您的 Microsoft Entra ID 租户中的某些数据。Citrix Cloud 使用这些数据来执行特定功能，例如连接到您的 Microsoft Entra ID 租户、使管理员能够使用专用登录 URL 登录 Citrix Cloud，以及将您的 Microsoft Entra ID 租户与 Endpoint Management 连接。Citrix Cloud 只能在您同意的情况下访问这些数据。这些权限代表了 Citrix Cloud 与您的 Microsoft Entra ID 配合使用所需的最低权限。有关 Microsoft Entra ID 权限和同意的更多信息，请参阅 Microsoft Azure 文档网站上的 Microsoft 身份平台中的权限和同意。

在本文中，每组 Microsoft Entra ID 应用程序权限都包含以下信息：

- **API 名称：** Citrix Cloud 请求权限的资源应用程序。这些应用程序是 Microsoft Graph 和 Windows Microsoft Entra ID。Citrix Cloud 从这两个资源应用程序请求相同的权限。
- **类型：** Citrix Cloud 为给定权限请求的访问级别。给定企业应用程序中的权限可以具有以下访问级别之一：
  - **委派权限**用于代表已登录用户执行操作，例如查询用户配置文件时。

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

  - **应用程序权限**用于应用程序在用户不在场的情况下执行操作时，例如查询特定组中的用户。此权限类型需要 Microsoft Entra ID 中全局管理员的同意。

- **声明值：** Microsoft Entra ID 分配给给定权限的信息字符串。给定企业应用程序中的权限可以具有以下声明值之一：

  - **User.Read：** 允许 Citrix Cloud 管理员将来自已连接 Microsoft Entra ID 的用户添加为 Citrix Cloud 帐户上的管理员。
  - **User.ReadBasic.All：** 从用户配置文件收集基本信息。它是 User.Read.All 的一个子集，但该权限本身保留用于向后兼容。
  - **User.Read.All：** Citrix Cloud 调用 Microsoft Graph 中的 列出用户，以启用从客户已连接的 Microsoft Entra ID 浏览和选择用户。例如，可以授予来自 Microsoft Entra ID 的用户对具有商店的 Citrix DaaS 资源的访问权限。Citrix Cloud 无法使用 `User.ReadBasic.All`，因为 Citrix Cloud 需要访问基本配置文件之外的属性，例如 `onPremisesSecurityIdentifier`。
  - **GroupMember.Read.All：** Citrix Cloud 调用 Microsoft Graph 中的 列出组，以允许从客户已连接的 Microsoft Entra ID 浏览和选择组。例如，也可以授予来自 Microsoft Entra ID 的组对 Citrix DaaS 应用程序的访问权限。
  - **Directory.Read.All：** Citrix Cloud 调用 Microsoft Graph 中的 列出 memberOf 以获取用户的组成员身份，因为 `Groups.Read.All` 不足。
  - **DeviceManagementApps.ReadWrite.All：** 允许 Citrix Cloud 读取和写入由 Microsoft Intune 管理的属性、组分配、应用程序状态、应用程序配置和应用程序保护策略。
  - **Directory.AccessAsUser.All：** 允许 Citrix Cloud 拥有与已登录用户相同的目录信息访问权限。

注意：

Directory.Read.All 仅适用于 Microsoft Entra ID 与 Citrix Cloud 之间与 Endpoint Management 的默认连接。

商店最终用户登录

此 Citrix Cloud 应用程序 (ID: e95c4605-aeab-48d9-9c36-1a262ef8048e) 使用以下权限：

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

API 名称	声明值	权限名称	类型
微软图形	User.Read	登录并读取用户配置文件	委派

Microsoft Entra ID 与 Citrix Cloud 之间的默认连接

此 Citrix Cloud 应用程序（ID：f9c0e999-22e7-409f-bb5e-956986abdf02）使用以下权限：

API 名称	声明值	权限	类型
微软图形	GroupMember.Read.All	读取所有组	委派
微软图形	User.ReadBasic.All	读取所有用户的基本配置文件	委派
微软图形	User.Read.All	读取所有用户的完整配置文件	委派
微软图形	User.Read	登录并读取用户配置文件	委派
微软图形	GroupMember.Read.All	读取所有组	应用程序
微软 Graph	User.Read.All	读取所有用户的完整配置文件	应用程序

管理员邀请和登录

此 Citrix Cloud 应用程序（ID：1b32f261-b20c-4399-8368-c8f0092b4470）使用以下权限：

API 名称	声明值	权限名称	类型
微软 Graph	User.Read	登录并读取用户配置文件	委派
微软图形	User.ReadBasic.All	读取所有用户的基本配置文件	委派

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

Microsoft Entra ID 与 Citrix Cloud（含 Endpoint Management）之间的默认连接

此 Citrix Cloud 应用程序（ID：5c913119-2257-4316-9994-5e8f3832265b）使用以下权限：

API 名称	声明值	权限名称	类型
微软图形	GroupMember.Read.All	读取所有组	委派
微软 Graph	User.ReadBasic.All	读取所有用户的基本配置文件	委派
微软 Graph	User.Read	登录并读取用户配置文件	委派
微软 Graph	Directory.Read.All	读取目录数据	应用程序
微软 Graph	Directory.Read.All	读取目录数据	委托
微软图形	DeviceManagementApps.ReadWrite.All	读取和写入 Microsoft Intune 应用	委托
微软图形	Directory.AccessAsUser.All	以登录用户身份访问目录	委托

Microsoft Entra ID 与 Citrix Cloud 和 Endpoint Management 之间的旧版连接

此 Citrix Cloud 应用程序（ID: e067934c-b52d-4e92-b1ca-70700bd1124e）使用以下权限：

API 名称	声明值	权限名称	类型
微软图形	GroupMember.Read.All	读取所有组	委派
微软图形	User.ReadBasic.All	读取所有用户的基本配置文件	委派
微软图形	User.Read	登录并读取用户配置文件	委派

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

API 名称	声明值	权限名称	类型
微软图形	DeviceManagementApps.ReadWrite.All	读取和写入 Microsoft Intune 应用	委派
微软图形	Directory.AccessAsUser.All	以登录用户身份访问目录	委派

将本地 Citrix Gateway 作为身份提供程序连接到 Citrix Cloud™

Citrix Cloud 支持使用本地 Citrix Gateway 作为身份提供程序，对登录其应用商店的最终用户进行身份验证。

通过使用 Citrix Gateway 身份验证，您可以：

- 继续通过现有 Citrix Gateway 对用户进行身份验证，以便他们可以通过 Citrix® StoreFront Cloud 访问本地 Virtual Apps and Desktops 部署中的资源。
- 将 Citrix Gateway 的身份验证、授权和审计 (AAA) 功能 与 StoreFront Cloud 结合使用。
- 在通过 StoreFront Cloud 为用户提供所需资源访问权限的同时，使用直通身份验证、智能卡、安全令牌、条件访问策略、联合等功能。

提示：

通过Citrix 身份和身份验证简介 培训课程了解有关受支持的身份提供程序的更多信息。“规划 Citrix 身份和访问管理”模块包含简短视频，可指导您将此身份提供程序连接到 Citrix Cloud 并为 StoreFront Cloud 启用身份验证。

支持的版本

Citrix Gateway 身份验证支持与以下本地产品版本结合使用：

- Citrix Gateway 12.1 54.13 Advanced 版或更高版本
- Citrix Gateway 13.0 41.20 Advanced 版或更高版本

先决条件

云连接器

您需要至少两 (2) 台服务器来安装 Citrix Cloud Connector™ 软件。这些服务器必须满足以下要求：

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

- 满足 Cloud Connector 系统要求 中所述的系统要求。
- 未安装任何其他 Citrix 组件，不是 Active Directory 域控制器，也不是对您的资源位置基础结构至关重要的计算机。
- 已加入您的站点所在的域。如果用户访问您的站点在多个域中的应用程序，则必须在每个域中安装至少两个 Cloud Connector。
- 连接到可以联系您的站点的网络。
- 已连接到 Internet。有关详细信息，请参阅 系统和连接要求。
- 需要至少两个 Cloud Connector 以确保与 Citrix Cloud 的高可用性连接。安装后，Cloud Connector 允许 Citrix Cloud 定位您的站点并与之通信。

有关安装 Cloud Connector 的详细信息，请参阅 Cloud Connector 安装。

活动目录

在启用 Citrix Gateway 身份验证之前，请执行以下任务：

- 验证您的最终用户在 Active Directory (AD) 中拥有用户帐户。没有 AD 帐户的最终用户无法成功登录其应用商店。
- 确保最终用户的 AD 帐户中的用户属性已填充。Citrix Cloud 需要这些属性才能在最终用户登录时建立用户上下文。如果这些属性未填充，最终用户将无法登录其应用商店。这些属性包括：
  - 电子邮件地址
  - 显示名称
  - 通用名称
  - SAM 帐户名
  - 用户主体名称
  - OID
  - SID
- 将您的 Active Directory (AD) 连接到您的 Citrix Cloud 帐户。在此任务中，您将在准备好的服务器上安装 Cloud Connector 软件，如 (#cloud-connectors) 部分所述。Cloud Connector 使 Citrix Cloud 能够与您的本地环境通信。有关说明，请参阅 (/zh-cn/citrix-cloud/citrix-cloud-management/identity-access-management/connect-ad.html#to-connect-your-active-directory-to-citrix-cloud)。
- 如果您正在使用 Citrix Gateway 身份验证执行联合，请将您的 AD 用户同步到联合提供程序。Citrix Cloud 需要您的最终用户的 AD 用户属性，以便他们能够成功登录。

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

要求

Citrix Gateway 高级策略

由于经典策略已弃用，Citrix Gateway 身份验证要求在本地 Gateway 上使用高级策略。高级策略支持 Citrix Cloud 的多重身份验证 (MFA)，包括身份提供程序链等选项。如果您当前使用经典策略，则必须创建新的高级策略才能在 Citrix Cloud 中使用 Citrix Gateway 身份验证。创建高级策略时，可以重用经典策略的 Action 部分。

签名证书

在配置 Gateway 以对最终用户进行 StoreFront Cloud 身份验证时，Gateway 充当 OpenID Connect 提供程序。Citrix Cloud 和 Gateway 之间的消息符合 OIDC 协议，该协议涉及数字签名令牌。因此，您必须配置一个用于签署这些令牌的证书。此证书必须由公共证书颁发机构 (CA) 颁发。不支持使用由私有 CA 颁发的证书，因为无法向 Citrix Cloud 提供私有根 CA 证书。因此，无法建立信任链。如果您配置了多个用于签名的证书，则这些密钥会针对每条消息进行轮换。

密钥必须绑定到 **vpn global**。如果没有这些密钥，最终用户在登录后将无法成功访问其应用商店。

时钟同步

由于 OIDC 中的数字签名消息带有时间戳，因此 Gateway 必须与 NTP 时间同步。如果时钟未同步，Citrix Cloud 在检查令牌有效性时会假定令牌已过期。

任务概述

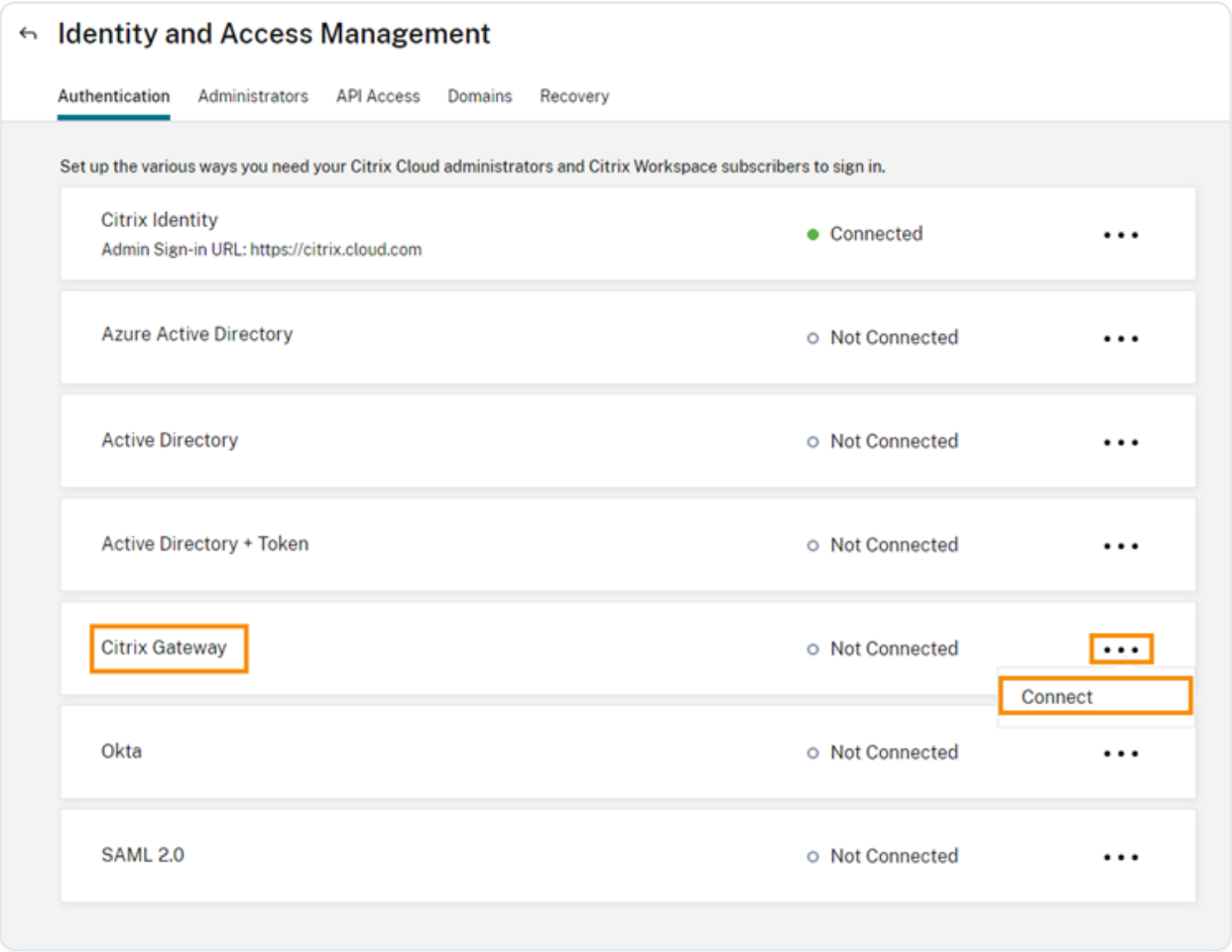
要设置 Citrix Gateway 身份验证，请执行以下任务：

1. 在**身份和访问管理**中，开始配置与网关的连接。在此步骤中，您将为网关生成客户端 ID、密钥和重定向 URL。
2. 在网关上，使用从 Citrix Cloud 生成的信息创建 OAuth IdP 高级策略。这使 Citrix Cloud 能够连接到您的本地网关。有关说明，请参阅以下文章：
   - Citrix Gateway 12.1: 将本地 Citrix Gateway 用作 Citrix Cloud 的身份提供程序
   - Citrix Gateway 13.0: 将本地 Citrix Gateway 用作 Citrix Cloud 的身份提供程序
3. 在 **StoreFront Cloud** 中，为最终用户启用 Citrix Gateway 身份验证。

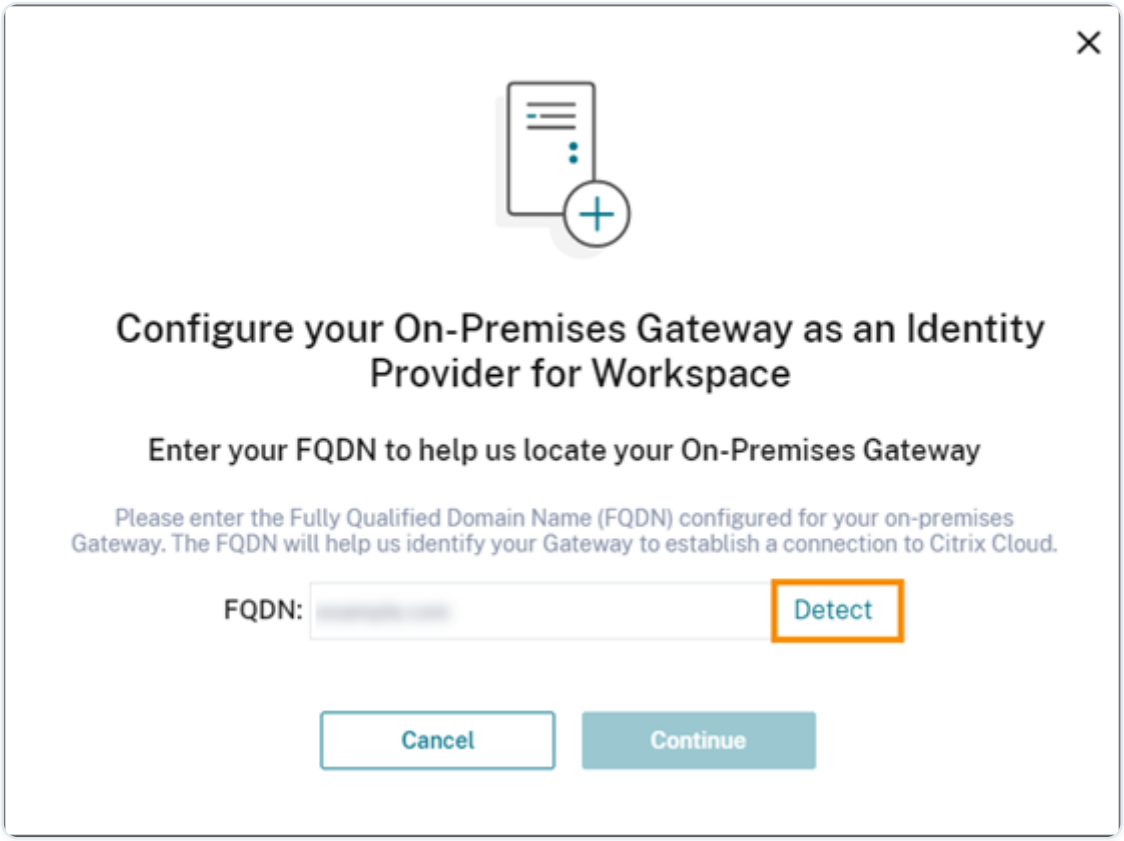
为最终用户启用 Citrix Gateway 身份验证

1. 从 Citrix Cloud 菜单中，选择**身份和访问管理**。
2. 在**身份验证**选项卡中，在 **Citrix Gateway** 下，单击省略号菜单并选择**连接**。

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



3. 输入本地网关的 FQDN，然后单击**检测**。

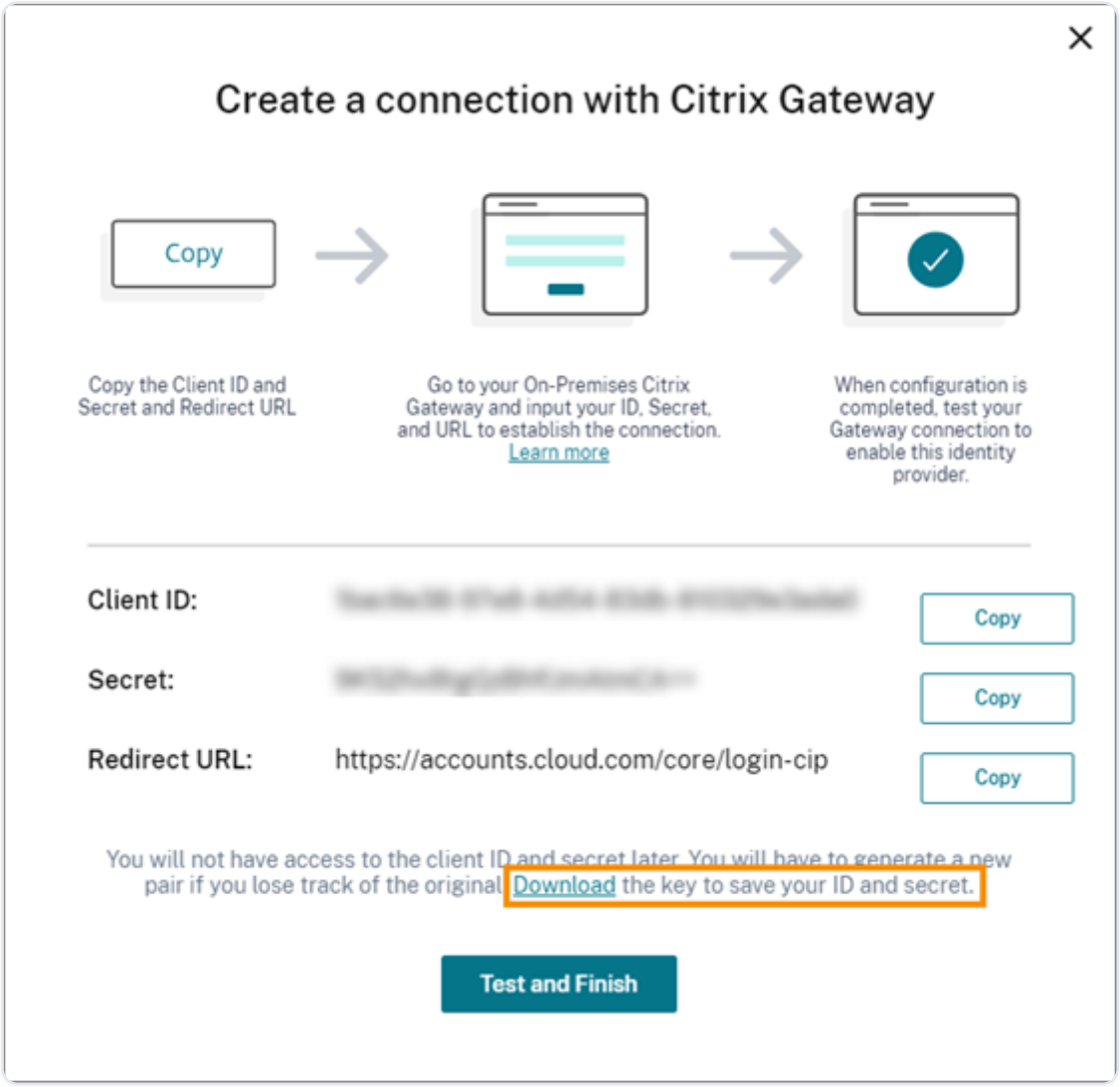


Citrix Cloud 成功检测到它后，单击**继续**。

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

4. 创建与本地网关的连接：

   a. 复制 Citrix Cloud 显示的客户端 ID、密钥和重定向 URL。



   此外，下载此信息的副本并将其安全地离线保存以供参考。此信息生成后，在 Citrix Cloud 中将不可用。

   b. 在网关上，使用 Citrix Cloud 中的客户端 ID、密钥和重定向 URL 创建 OAuth IdP 高级策略。有关说明，请参阅以下文章：

      - 对于 Citrix Gateway 12.1: 将本地 Citrix Gateway 用作 Citrix Cloud 的身份提供程序
      - 对于 Citrix Gateway 13.0: 将本地 Citrix Gateway 用作 Citrix Cloud 的身份提供程序

   c. 单击**测试并完成**。Citrix Cloud 会验证您的网关是否可访问且配置正确。

5. 为商店启用 Citrix Gateway 身份验证：

   a. 从 Citrix Cloud 菜单中，选择 **StoreFront Cloud**。

   b. 在“**身份验证**”选项卡中，选择“**Citrix Gateway**”。

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

c. 选择“**我了解这对最终用户体验的影响**”，然后单击“**保存**”。

故障排除

首先，请查看本文中的先决条件和要求部分。验证您的本地环境中是否具备所有必需的组件，并且已完成所有必需的配置。如果缺少或错误配置了其中任何一项，则使用 Citrix Gateway 的商店身份验证将无法工作。

如果您在 Citrix Cloud 与本地 Gateway 之间建立连接时遇到问题，请验证以下各项：

- Gateway FQDN 可从 Internet 访问。
- 您已在 Citrix Cloud 中正确输入 Gateway FQDN。
- 您已在 OAuth IdP 策略的 `-issuer` 参数中正确输入 Gateway URL。示例：`-issuer https://GatewayFQDN.com`。`issuer` 参数区分大小写。
- Citrix Cloud 中的客户端 ID、密钥和重定向 URL 值已正确输入到 OAuth IdP 策略的“客户端 ID”、“客户端密钥”、“重定向 URL”和“受众”字段中。验证是否已在策略的“受众”字段中输入了正确的客户端 ID。
- OAuth IdP 身份验证策略配置正确。有关说明，请参阅以下文章：
  - Citrix Gateway 12.1：将本地 Citrix Gateway 用作 Citrix Cloud 的身份提供程序
  - Citrix Gateway 13.0：将本地 Citrix Gateway 用作 Citrix Cloud 的身份提供程序
- 验证策略是否已按照绑定身份验证策略中的说明正确绑定到 AAA 身份验证服务器。

全局编录服务器

除了检索用户帐户详细信息之外，Gateway 还会检索用户的域名、AD NETBIOS 名称和根 AD 域名。要检索 AD NETBIOS 名称，Gateway 会搜索用户帐户所在的 AD。NETBIOS 名称不会在全球编录服务器上复制。

如果您在 AD 环境中使用全局编录服务器，则在此类服务器上配置的 LDAP 操作不适用于 Citrix Cloud。相反，您必须在 LDAP 操作中配置各个 AD。如果您有多个域或林，则可以配置多个 LDAP 策略。

使用 Kerberos 或 IdP 链进行单点登录的 AD 搜索

如果您使用 Kerberos 或使用 SAML 或 OIDC 协议进行最终用户登录的外部身份提供程序，请验证是否已配置 AD 查找。Gateway 需要 AD 查找来检索最终用户的 AD 用户属性和 AD 配置属性。

即使身份验证由第三方服务器处理，也要确保已配置 LDAP 策略。要配置这些策略，您可以通过执行以下任务向现有登录架构配置文件添加第二个身份验证因素：

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

1. 创建一个仅从 Active Directory 执行属性和组提取的 LDAP 身份验证服务器。
2. 创建一个 LDAP 高级身份验证策略。
3. 创建一个身份验证策略标签。
4. 将身份验证策略标签定义为主要身份提供程序之后的下一个因素。

将 LDAP 添加为第二个身份验证因素

1. 创建 LDAP 身份验证服务器：
   a. 选择 **系统 > 身份验证 > 基本策略 > LDAP > 服务器 > 添加**。
   b. 在“**创建身份验证 LDAP 服务器**”页面上，输入以下信息：
      - 在“**选择服务器类型**”中，选择“**LDAP**”。
      - 在 **名称** 中，输入服务器的友好名称。
      - 选择 **服务器 IP**，然后输入 LDAP 服务器的 IP 地址。
      - 在 **安全类型** 中，选择所需的 LDAP 安全类型。
      - 在 **服务器类型** 中，选择 **AD**。
      - 在 **身份验证** 中，不要选中此复选框。必须清除此复选框，因为此身份验证服务器仅用于从 Active Directory 提取用户属性和组，而非用于身份验证。
   c. 在 **其他设置** 下，输入以下信息：
      - 在 **服务器登录名属性** 中，输入 **UserPrincipalName**。
      - 在 **组属性** 中，选择 **memberOf**。
      - 在 **子属性名称** 中，选择 **cn**。
2. 创建 LDAP 高级身份验证策略：
   a. 选择 **安全 > AAA - 应用程序流量 > 策略 > 身份验证 > 高级策略 > 策略 > 添加**。
   b. 在 **创建身份验证策略** 页面上，输入以下信息：
      - 在 **名称** 中，输入策略的友好名称。
      - 在 **操作类型** 中，选择 **LDAP**。
      - 在 **操作** 中，选择之前创建的 LDAP 身份验证服务器。
      - 在 **表达式** 中，输入 **TRUE**。
   c. 单击 **创建** 以保存配置。
3. 创建身份验证策略标签：

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

a. 选择 **安全 > AAA – 应用程序流量 > 策略 > 身份验证 > 高级策略 > 策略标签 > 添加**。
b. 在 **名称** 中，输入身份验证策略标签的友好名称。
c. 在登录架构中，选择 **LSCHEMA_INT**。
d. 在 **策略绑定** 下，在 **选择策略** 中，选择您之前创建的 LDAP 高级身份验证策略。
e. 在 **GoTo 表达式** 中，选择 **END**。
f. 单击 **绑定** 以完成配置。

4. 将 LDAP 身份验证策略标签定义为下一个因素，在主身份提供程序之后：

a. 选择 **系统 > 安全 > AAA - 应用程序流量 > 虚拟服务器**。
b. 选择包含主身份提供程序绑定的虚拟服务器，然后选择 **编辑**。
c. 在 **高级身份验证策略** 下，选择现有的 **身份验证策略** 绑定。
d. 选择主身份提供程序的绑定，然后选择 **编辑绑定**。
e. 在 **策略绑定** 页面上，在 **选择下一个因素** 中，选择您之前创建的 LDAP 身份验证策略标签。
f. 单击 **绑定** 以保存配置。

用于多重身份验证的默认密码

如果您为最终用户使用多重身份验证 (MFA)，Gateway 会将最后一个因素的密码用作单点登录的默认密码。当最终用户登录其应用商店时，此密码将发送到 Citrix Cloud。如果您的环境中 LDAP 身份验证之后是另一个因素，您必须将 LDAP 密码配置为发送到 Citrix Cloud 的默认密码。在与 LDAP 因素对应的登录架构上启用 **SSOCredentials**。

更多信息

Citrix Tech Zone：技术洞察：身份验证 - Gateway

将 Google Cloud Identity 作为身份提供程序连接到 Citrix Cloud™

Citrix Cloud 支持使用 Google Cloud Identity 作为身份提供程序，对登录其商店的最终用户进行身份验证。通过将您组织的 Google 帐户连接到 Citrix Cloud，您可以为访问 Citrix® StoreFront Cloud 和 Google 资源提供统一的登录体验。

已加入域和未加入域配置的要求

您可以使用已加入域或未加入域的计算机，在 Citrix Cloud 中将 Google Cloud Identity 配置为身份提供程序。

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

- 已加入域表示计算机已加入本地 Active Directory (AD) 中的域，并且身份验证使用存储在该域中的用户配置文件。
- 未加入域表示计算机未加入 AD 域，并且身份验证使用存储在您的 Google Workspace 目录中的用户配置文件（也称为 Google 原生用户）。

下表列出了每种配置类型的要求。

要求	已加入域	未加入域	更多信息
本地 AD	是	否	请参阅本文中的准备 Active Directory 和 Citrix Cloud Connector。
在您的资源位置部署的 Citrix Cloud Connector	是	否；访问非域加入的计算机不需要 Cloud Connector。	请参阅本文中的 准备 Active Directory 和 Citrix Cloud Connector。
AD 与 Google Cloud 同步	仅在使用 Gateway 服务且不使用其他服务时为可选。否则，此任务是必需的。	否	请参阅本文中的 将 Active Directory 与 Google Cloud Identity 同步。
具有 Google Cloud Platform 控制台访问权限的开发者帐户。用于创建服务帐户和密钥，以及启用 Admin SDK API。	是	是	请参阅本文中的 创建服务帐户、创建服务帐户密钥 和 配置域范围委派。
具有 Google Workspace 管理控制台访问权限的管理员帐户。用于配置域范围委派和只读 API 用户帐户。	是	是	请参阅本文中的 (#configure-domain-wide-delegation) 和 (#add-a-read-only-api-user-account)。

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

使用多个 Citrix Cloud 帐户进行身份验证

本文介绍了如何将 Google Cloud Identity 作为身份提供程序连接到单个 Citrix Cloud 帐户。如果您有多个 Citrix Cloud 帐户，则可以使用相同的服务帐户和只读 API 用户帐户将每个帐户连接到同一个 Google Cloud 帐户。只需登录 Citrix Cloud 并从客户选择器中选择相应的客户 ID 即可。

准备活动目录和 Citrix Cloud 连接器

如果您将 Google Cloud Identity 与**已加入域**的计算机结合使用，请使用本节准备您的本地 AD。如果您使用的是未加入域的计算机，请跳过此任务并继续阅读本文中的 (#create-a-service-account)。

您需要在 Active Directory 域中至少有两 (2) 台服务器来安装 Citrix Cloud Connector 软件。Cloud Connector 是实现 Citrix Cloud 与您的 (/zh-cn/citrix-cloud/citrix-cloud-resource-locations/resource-locations.html) 之间通信所必需的。至少需要两个 Cloud Connector 才能确保与 Citrix Cloud 的高可用性连接。这些服务器必须满足以下要求：

- 满足 (/zh-cn/citrix-cloud/citrix-cloud-resource-locations/citrix-cloud-connector/system-requirements.html) 中描述的要求。
- 未安装任何其他 Citrix® 组件，不是 Active Directory 域控制器，并且不是对您的资源位置基础结构至关重要的计算机。
- 已加入您的 Active Directory (AD) 域。如果您的存储资源和用户位于多个域中，则必须在每个域中安装至少两个 Cloud Connector。有关详细信息，请参阅 (/zh-cn/citrix-cloud/citrix-cloud-resource-locations/citrix-cloud-connector/technical-details.html#deployment-scenarios-for-cloud-connectors-in-active-directory)。
- 连接到可以联系用户通过云存储访问的资源的网络。
- 连接到 Internet。有关详细信息，请参阅 (/zh-cn/citrix-cloud/overview/requirements/internet-connectivity-requirements.html)。

有关安装 Cloud Connector 的详细信息，请参阅 (/zh-cn/citrix-cloud/citrix-cloud-resource-locations/citrix-cloud-connector/installation.html)。

将活动目录与 Google Cloud 身份同步

如果您将 Google Cloud Identity 与**已加入域**的计算机结合使用，请使用本节准备您的本地 AD。如果您使用的是未加入域的计算机，请跳过此任务并继续阅读本文中的 (#create-a-service-account)。

如果您仅使用 Citrix Gateway 服务且未启用其他服务，则将 AD 与 Google Cloud Identity 同步是可选的。对于这些服务，您可以直接使用 Google 原生用户，而无需与 AD 同步。

如果您正在使用其他 Citrix Cloud 服务，则需要将您的 AD 与 Google Cloud Identity 同步。Google Cloud 必须将以下 AD 用户属性传递给 Citrix Cloud：

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

- SecurityIDentifier (SID)
- objectGUID
- userPrincipalName (UPN)

将您的 AD 与 Google Cloud 同步

1. 从 Google 网站下载并安装 Google Cloud Directory Sync 实用程序。有关此实用程序的更多信息，请参阅 Google 网站上的 Google Cloud Directory Sync 文档。
2. 安装该实用程序后，启动配置管理器 (**开始 > 配置管理器**)。
3. 按照实用程序文档中 使用配置管理器设置同步 的说明，指定 Google 域设置和 LDAP 设置。
4. 在**常规设置**中，选择**自定义架构**。保持默认选择不变。
5. 配置自定义架构以应用于所有用户帐户。使用本节中指定的精确大小写和拼写输入所需信息。

   a. 选择**自定义架构**选项卡，然后选择**添加架构**。

   b. 选择**使用“用户帐户”中定义的规则**。

   c. 在**架构名称**中，输入 **citrix-schema**。

   d. 选择**添加字段**，然后输入以下信息：

      - 在**架构字段模板**下，在**架构字段**中，选择 **userPrincipalName**。
      - 在 **Google 字段详细信息**下，在 **字段名称**中，输入 **UPN**。

   e. 重复步骤 4 以创建以下字段：

      - objectGUID: 在 **架构字段模板**下，选择 **objectGUID**。在 **Google 字段详细信息**下，输入 **objectGUID**。
      - SID: 在 **架构字段模板**下，选择 **自定义**。在 **Google 字段详细信息**下，输入 **SID**。
      - objectSID: 在 **架构字段模板**下，选择 **自定义**。在 **Google 字段详细信息**下，输入 **objectSID**。

   f. 选择 **确定** 以保存您的条目。

6. 完成为您的组织配置所有剩余设置，并验证同步设置，如实用程序文档中的 使用 Configuration Manager 设置同步 中所述。
7. 选择 **同步并应用更改** 以将您的 Active Directory 与您的 Google 帐户同步。

同步完成后，Google Cloud 中的“用户信息”部分将显示用户的 Active Directory 信息。

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

创建服务帐户

要完成此任务，您需要一个 Google Cloud Platform 开发者帐户。

1. 登录 https://console.cloud.google.com。
2. 从仪表板侧边栏中，选择 **IAM 和管理**，然后选择 **服务帐户**。
3. 选择 **创建服务帐户**。
4. 在 **服务帐户详细信息**下，输入服务帐户名称和服务帐户 ID。
5. 选择 **完成**。

创建服务帐号密钥

1. 在 **服务帐号** 页面上，选择您刚刚创建的服务帐号。
2. 选择 **密钥** 选项卡，然后选择 **添加密钥 > 创建新密钥**。
3. 保留默认的 JSON 密钥类型选项处于选中状态。
4. 选择 **创建**。将密钥保存到以后可以访问的安全位置。将 Google Cloud Identity 连接为身份提供程序时，您将在 Citrix Cloud 控制台中输入私钥。

配置域范围委派

1. 启用 Admin SDK API：
   a. 在 Google Cloud Platform 菜单中，选择 **API 和服务 > 已启用的 API 和服务**。
   b. 选择控制台顶部附近的 **启用 API 和服务**。API 库主页随即显示。
   c. 搜索 **Admin SDK API**，然后从结果列表中选择它。
   d. 选择 **启用**。
2. 为服务帐号创建 API 客户端：
   a. 在 Google Cloud Platform 菜单中，选择 **IAM 和管理 > 服务帐号**，然后选择您之前创建的服务帐号。
   b. 在服务帐号的 **详细信息** 选项卡中，展开 **高级设置**。
   c. 在 **Domain-wide Delegation** 下，复制客户端 ID，然后选择 **View Google Workspace Admin Console**。
   d. 如果适用，选择您要使用的 Google Workspace 管理员帐户。Google 管理控制台随即显示。
   e. 在 Google 管理侧边栏中，选择 **Security > Access and data control > API controls**。
   f. 在 **域范围委派** 下，单击 **管理域范围委派**。

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

g. 选择 **Add new**。

h. 在 **Client ID** 中，粘贴您在步骤 C 中复制的服务帐户的客户端 ID。

i. 在 **OAuth scopes** 中，以逗号分隔的单行形式输入以下范围：

```
https://www.googleapis.com/auth/
admin.directory.user.readonly,https://www.googleapis.com/auth/
admin.directory.group.readonly,https://www.googleapis.com/auth/
admin.directory.domain.readonly
```

j. 选择 **Authorize**。

添加只读 API 用户帐户

在此任务中，您将创建一个具有 Citrix Cloud 只读 API 访问权限的 Google Workspace 用户帐户。此帐户不用于任何其他目的，也没有其他特权。

1. 在 Google 管理菜单中，选择 **Directory > Users**。
2. 选择 **Add new user** 并输入相应的用户信息。
3. 选择 **Add new user** 以保存帐户信息。
4. 为只读用户帐户创建自定义角色：

   a. 在 Google 管理菜单中，选择 **Account > Admin roles**。

   b. 选择 **创建新角色**。

   c. 输入新角色的名称。示例：API-ReadOnly

   d. 选择 **继续**。

   e. 在 **管理员 API 权限** 下，选择以下权限：

      - 用户 > 读取
      - 群组 > 读取
      - 域管理

   f. 选择 **继续**，然后选择 **创建角色**。

5. 将自定义角色分配给您之前创建的只读用户帐户：

   a. 在自定义角色详细信息页面中，在 **管理员** 窗格中，选择 **分配用户**。

   b. 开始键入只读用户帐户的名称，并从用户列表中选择它。

   c. 选择 **分配角色**。

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

d. 要验证角色分配，请返回到“用户”页面 (**目录 > 用户**) 并选择只读用户帐户。自定义角色分配显示在 **管理员角色和权限** 下。

将谷歌云身份连接到 Citrix 云

1. 登录到 Citrix Cloud，网址为 https://citrix.cloud.com。
2. 从 Citrix Cloud 菜单中，选择 **身份和访问管理**。
3. 找到 **Google Cloud Identity**，然后从省略号菜单中选择 **连接**。
4. 出现提示时，为您的公司输入一个简短的、URL 友好的标识符，然后选择 **保存并继续**。您选择的标识符在 Citrix Cloud 中必须是全局唯一的。
5. 选择 **导入文件**，然后选择您在 为服务帐户创建密钥时 保存的 JSON 文件。此操作将导入您的私钥以及您创建的 Google Cloud 服务帐户的电子邮件地址。
6. 在 **模拟用户** 中，输入只读 API 用户帐户的名称。
7. 选择 **下一步**。Citrix Cloud 将验证您的 Google 帐户详细信息并测试连接。
8. 查看列出的关联域。如果正确，请选择 **确认** 以保存您的配置。

将管理员添加到 Citrix Cloud

您可以通过 Google Cloud 添加单个 Citrix Cloud 管理员和管理员组。有关详细信息，请参阅以下文章：

- 对于单个管理员：管理对 Citrix Cloud 的管理员访问权限
- 对于管理员组：管理管理员组

将管理员添加到 Citrix Cloud 后，他们可以使用以下方法之一登录：

- 导航到您在最初将 Google Cloud 配置为身份提供程序时配置的管理员登录 URL。示例：`https://citrix.cloud.com/go/mycompany`
- 在 Citrix Cloud 登录页面上，选择 **使用我的公司凭据登录**，输入您公司的唯一标识符（例如，“mycompany”），然后单击 **继续**。

为商店身份验证启用 Google Cloud Identity

1. 从 Citrix Cloud 菜单中，选择 **StoreFront Cloud > Authentication**。
2. 选择 **Google Cloud Identity**。出现提示时，选择 **我了解这对最终用户体验的影响**，然后单击 **保存**。

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

将 Okta 作为身份提供商连接到 Citrix Cloud™

Citrix Cloud 支持使用 Okta 作为身份提供商对登录其商店的最终用户进行身份验证。通过将您的 Okta 组织连接到 Citrix Cloud，您可以为最终用户提供统一的登录体验，以访问 Citrix® StoreFront Cloud 中的资源。

在 StoreFront Cloud 中启用 Okta 身份验证后，最终用户将获得不同的登录体验。选择 Okta 身份验证提供的是联合登录，而不是单点登录。最终用户从 Okta 登录页面登录商店，但当他们从 Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops 服务）打开应用程序或桌面时，可能需要再次进行身份验证。要启用单点登录并防止第二次登录提示，您需要将 Citrix Federated Authentication Service 与 Citrix Cloud 结合使用。有关详细信息，请参阅将 Citrix Federated Authentication Service 连接到 Citrix Cloud。

先决条件

云连接器或连接器设备

Cloud Connector 或 Connector Appliance 是实现 Citrix Cloud 与您的 (/zh-cn/citrix-cloud/citrix-cloud-resource-locations/resource-locations.html) 之间通信所必需的。至少需要两个 Cloud Connector 或 Connector Appliance，以确保与 Citrix Cloud 建立高可用性连接。您需要至少两个已加入 Active Directory 域的 Connector。这些可以是 (/zh-cn/citrix-cloud/citrix-cloud-resource-locations/citrix-cloud-connector.html) 或 (/zh-cn/citrix-cloud/citrix-cloud-resource-locations/connector-appliance.html)。

连接器必须满足以下要求：

- 满足其各自文档中描述的要求
- 已加入您的 Active Directory (AD) 域。如果您的商店用户位于多个域中，可以使用 (/zh-cn/citrix-cloud/citrix-cloud-resource-locations/connector-appliance/active-directory.html) 加入多个域。
- 连接到可以联系用户通过云商店访问的资源的网络。
- 连接到 Internet。有关详细信息，请参阅 (/zh-cn/citrix-cloud/overview/requirements/internet-connectivity-requirements.html)。

有关安装 Cloud Connector 的详细信息，请参阅 (/zh-cn/citrix-cloud/citrix-cloud-resource-locations/citrix-cloud-connector/installation.html)。 有关安装 Connector Appliance 的详细信息，请参阅 (/zh-cn/citrix-cloud/citrix-cloud-resource-locations/connector-appliance.html#obtain-the-connector-appliance)。

Okta 域

将 Okta 连接到 Citrix Cloud 时，您必须提供您组织的 Okta 域。Citrix 支持以下 Okta 域：

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

- okta.com
- okta-eu.com
- oktapreview.com

您也可以将 Okta 自定义域与 Citrix Cloud 结合使用。请查看 Okta 网站上关于使用自定义域的重要注意事项，具体请参阅 自定义 Okta URL 域。

有关查找组织的自定义域的更多信息，请参阅 Okta 网站上的查找您的 Okta 域。

Okta OIDC Web 应用程序

要将 Okta 用作身份提供程序，您必须首先创建一个 Okta OIDC Web 应用程序，其中包含可与 Citrix Cloud 结合使用的客户端凭据。创建并配置应用程序后，请记下客户端 ID 和客户端密钥。连接 Okta 组织时，您需要向 Citrix Cloud 提供这些值。

要创建和配置此应用程序，请参阅本文中的以下部分：

- (#create-an-okta-oidc-web-app-integration)
- (#configure-the-okta-oidc-web-application)

应用商店 URL

创建 Okta 应用程序时，您必须提供 Citrix Cloud 中的应用商店 URL。要找到应用商店 URL，请从 Citrix Cloud 菜单中选择 **StoreFront Cloud**。应用商店 URL 显示在 **访问** 选项卡上。

重要提示：

如果您稍后修改商店 URL，则必须使用新的 URL 更新 Okta 应用程序配置。否则，您的最终用户在从其商店注销时可能会遇到问题。

Okta API 令牌

将 Okta 用作 Citrix Cloud 的身份提供程序需要为您的 Okta 组织提供一个 API 令牌。使用 Okta 组织中的只读管理员帐户创建此令牌。此令牌必须能够读取 Okta 组织中的用户和组。

要创建 API 令牌，请参阅本文中的 创建 Okta API 令牌。有关 API 令牌的更多信息，请参阅 Okta 网站上的 创建 API 令牌。

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

重要提示：

创建 API 令牌时，请记下令牌值（例如，将该值暂时复制到纯文本文档中）。Okta 只显示此值一次，因此您可以在执行 将 Citrix Cloud 连接到您的 Okta 组织 中的步骤之前创建令牌。

使用 Okta AD 代理将 Active Directory 帐户同步到 Okta

要将 Okta 用作身份提供商，您必须首先将本地 AD 与 Okta 集成。为此，您需要在域中安装 Okta AD 代理，并将您的 AD 添加到您的 Okta 组织。有关部署 Okta AD 代理的指导，请参阅 Okta 网站上的 Active Directory 集成入门。

之后，将您的 AD 用户和组导入 Okta。导入时，请包含与您的 AD 帐户关联的以下值：

- 电子邮件
- SID
- UPN
- OID

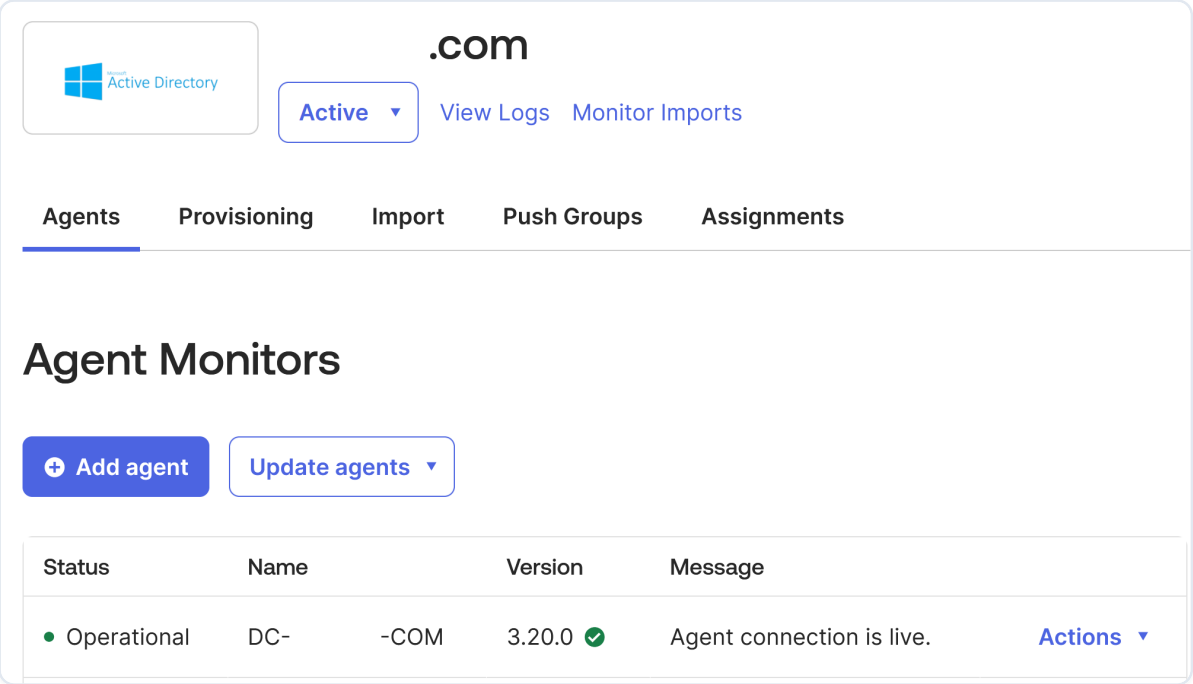
注意：

如果您将 Citrix Gateway 服务与 Store 结合使用，则无需将 AD 帐户与 Okta 组织同步。

要将 AD 用户和组与 Okta 组织同步：

1. 安装并配置 Okta AD 代理。有关完整说明，请参阅 Okta 网站上的以下文章：
    - 安装 Okta Active Directory 代理
    - 配置 Active Directory 导入和帐户设置
    - 配置 Active Directory 预配设置

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



2. 通过手动导入或自动导入将您的 AD 用户和组添加到 Okta。有关 Okta 导入方法和说明的更多信息，请参阅 Okta 网站上的管理 Active Directory 用户和组。

创建 Okta OIDC Web 应用程序集成

1. 在 Okta 管理控制台中，在 **Applications** 下，选择 **Applications**。
2. 选择 **创建应用程序集成**。
3. 在 **Sign in method** 中，选择 **OIDC - OpenID Connect**。
4. 在 **Application type** 中，选择 **Web Application**。选择 **Next**。
5. 在 **App Integration Name** 中，输入应用程序集成的友好名称。
6. 在 **Grant type** 中，选择 **Authorization Code**（默认选中）。
7. 在 **Sign-in redirect URIs** 中，输入 `https://accounts.cloud.com/core/login-okta`。
   - 如果您的 Citrix Cloud 客户位于欧盟、美国或亚太南部地区，请输入 `https://accounts.cloud.com/core/login-okta`。
   - 如果您的 Citrix Cloud 客户位于日本地区，请输入 `https://accounts.citrixcloud.jp/core/login-okta`。
   - 如果您的 Citrix Cloud 客户位于 Citrix Cloud Government 地区，请输入 `https://accounts.cloud.us/core/login-okta`。
8. 在 **注销重定向 URI** 中，输入您的 Citrix Cloud 应用商店 URL。
9. 如果您还使用应用商店自定义域，则也需要输入此项。例如

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

- `https://workspaceurl1.cloud.com`
- `https://workspaceurl2.cloud.com`
- `https://workspaceurl1.mycustomdomain.com`

10. 在 **分配** 下的 **受控访问** 中，选择是将应用程序集成分配给组织中的所有人、仅分配给您指定的组，还是稍后分配访问权限。
11. 选择 **保存**。保存应用程序集成后，控制台将显示应用程序配置页面。
12. 在 **客户端凭据** 部分，复制 **客户端 ID** 和 **客户端密钥** 值。当您将 Citrix Cloud 连接到您的 Okta 组织时，将使用这些值。

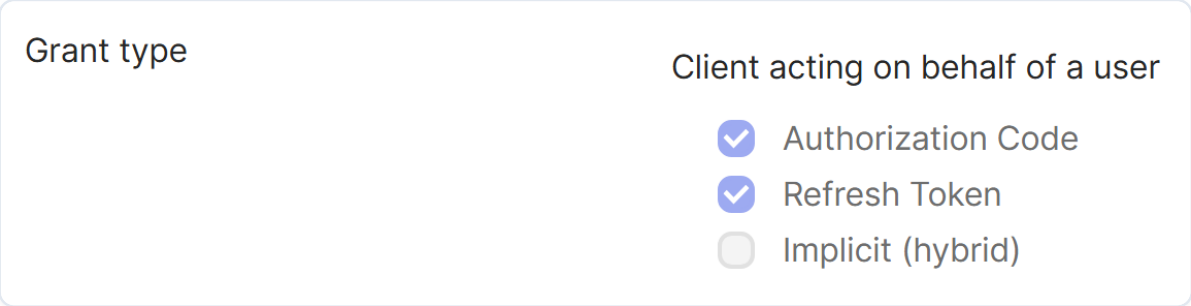
配置 Okta OIDC Web 应用程序

在此步骤中，您将使用 Citrix Cloud 所需的设置配置 Okta OIDC Web 应用程序。Citrix Cloud 需要这些设置，以便在最终用户登录其应用商店时通过 Okta 对其进行身份验证。

1. （可选）更新隐式授权类型的客户端权限。如果您希望为此授权类型授予最少权限，则可以选择执行此步骤。

   a. 在 Okta 应用程序配置页面上，在 **常规** 选项卡中，滚动到 **常规设置** 部分并选择 **编辑**。

   b. 在 **应用程序** 部分的 **授权类型** 中，在 **代表用户操作的客户端** 下，清除 **允许使用隐式授权类型访问令牌** 设置。

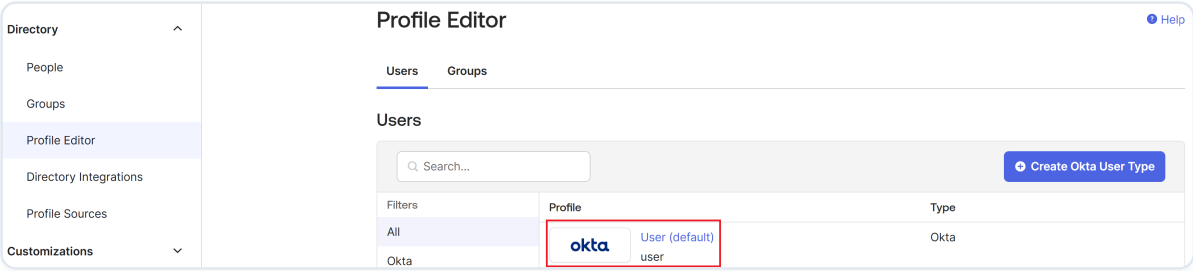
   c. 选择 **保存**。

2. 添加应用程序属性。这些属性区分大小写。

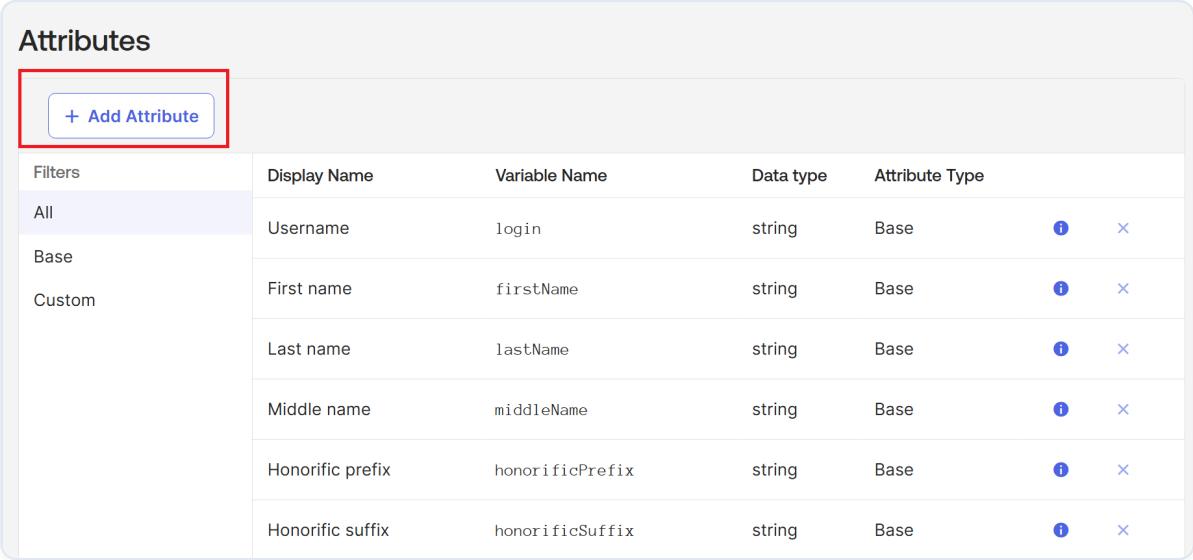
   a. 在 Okta 控制台菜单中，选择 **Directory > Profile Editor**。

   b. 选择 Okta **User (default)** 配置文件。Okta 显示 **User** 配置文件页面。

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



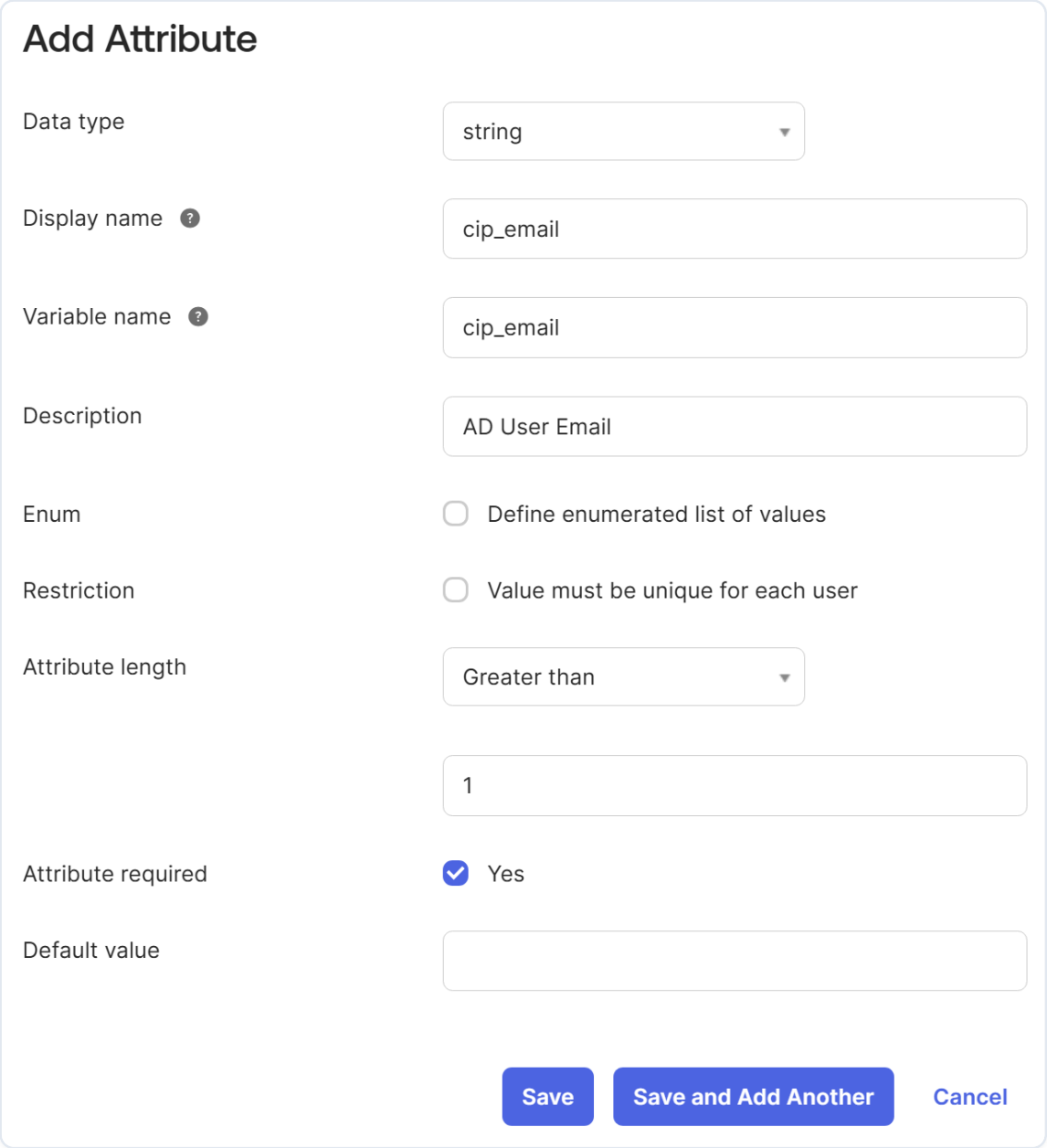
c. 在 **Attributes** 下，选择 **Add attribute**。



d. 输入以下信息：

- 显示名称：cip_email
- 变量名称：cip_email
- 描述：AD User Email
- 属性长度：选择 **Greater than**，然后输入 **1**。
- 属性必填：是

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



e. 选择 **保存并添加另一个**。

f. 输入以下信息：

- 显示名称: cip_sid
- 变量名称: cip_sid
- 描述: AD 用户安全标识符
- 属性长度: 选择“**大于**”，然后输入“**1**”。
- 属性必填: 是

g. 选择“**保存并添加另一个**”。

h. 输入以下信息:

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

- 显示名称: cip_upn
- 变量名称: cip_upn
- 描述: AD 用户主体名称
- 属性长度: 选择“**大于**”，然后输入“**1**”。
- 属性必填: 是

i. 选择“**保存并添加另一个**”。

j. 输入以下信息:

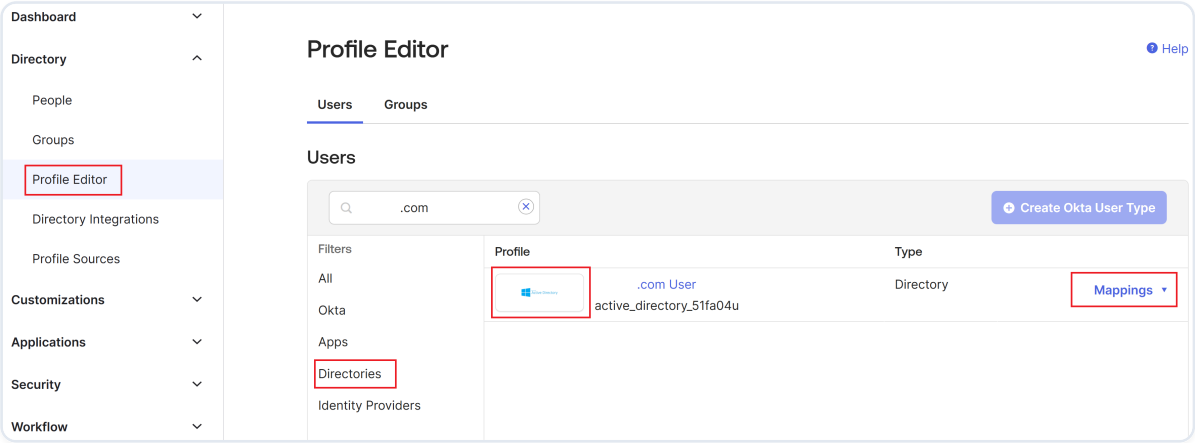
- 显示名称: cip_oid
- 变量名称: cip_oid
- 描述: AD User GUID
- 属性长度: 选择 **大于**，然后输入 **1**。
- 必需属性: 是

k. 选择 **保存**。

3. 编辑应用程序的属性映射:

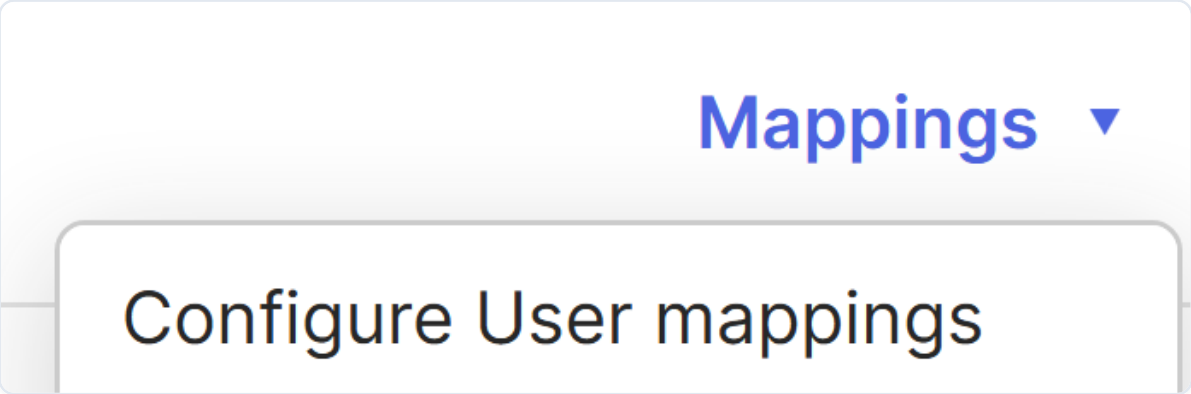
a. 在 Okta 控制台中，选择 **Directory > Profile Editor > Directories**。

b. 找到您的 AD 的 **active_directory** 配置文件。此配置文件可能使用 `myDomain User` 格式标记，其中 `myDomain` 是您的集成 AD 域的名称。

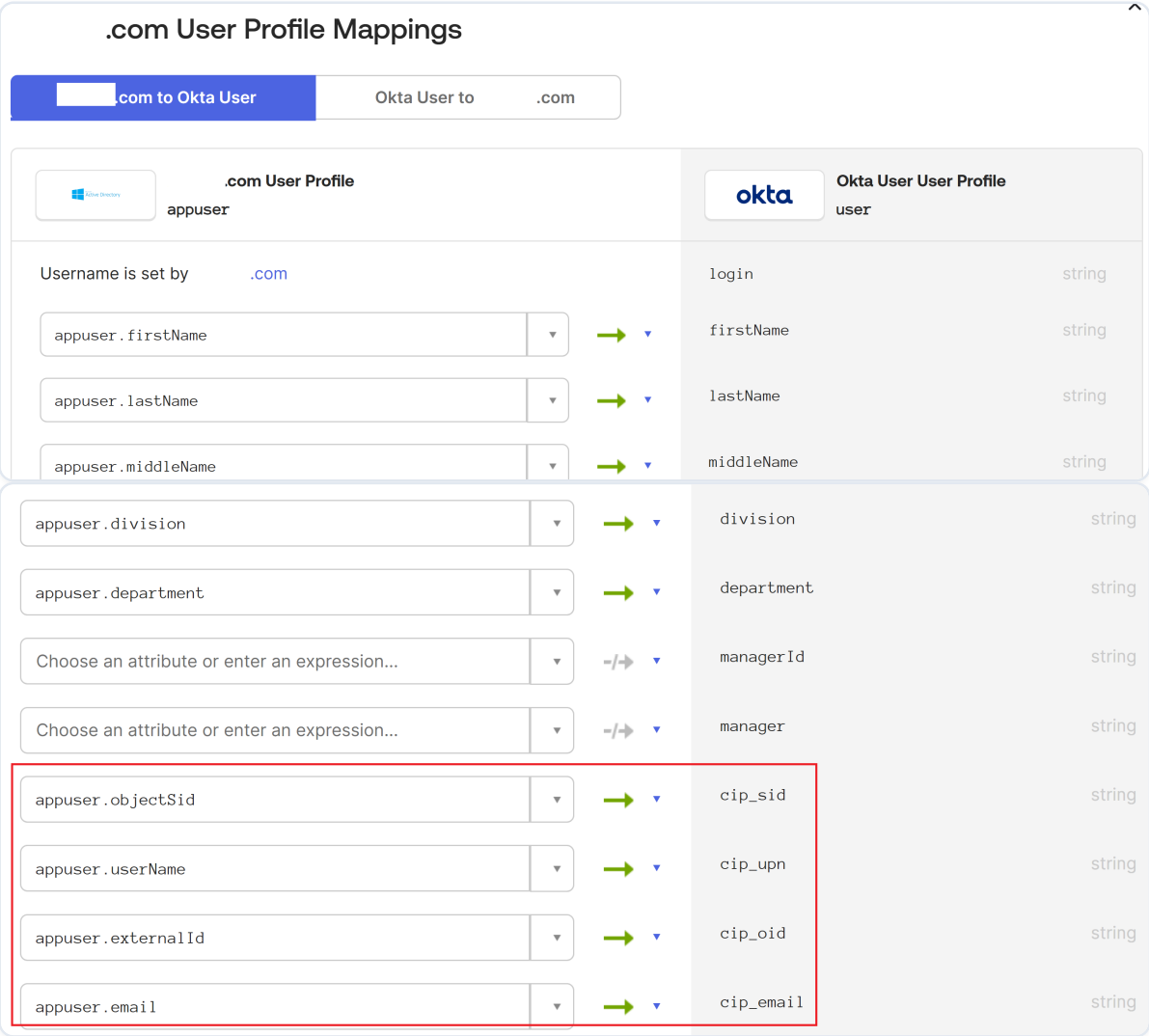


c. 选择 **Mappings**。将显示您的 AD 域的用户配置文件映射页面，并选中了用于将 AD 映射到 Okta 用户的选项卡。

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



d. 在 **Okta User User Profile** 列中，找到您在步骤 2 中创建的属性，并按如下方式映射:



- 对于 `cip_email`，从您的域的用户配置文件列中选择 `email`。选中后，映射显示为 `appuser.email`。
- 对于 `cip_sid`，从您的域的用户配置文件列中选择 `objectSid`。选中后，映射显示为 `appuser.objectSid`。
- 对于 `cip_upn`，从您的域的用户配置文件列中选择 `userName`。选中后，映射显示为 `appuser.userName`。

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

- 对于 `cip_oid`，从您的域的用户配置文件列中选择 `externalId`。选中后，映射显示为 `appuser.externalId`。

e. 选择 **保存映射**。

f. 选择 **立即应用更新**。Okta 会启动一个作业来应用这些映射。

g. 将 Okta 与您的 AD 同步。

   i. 在 Okta 控制台中，选择 **目录 > 目录集成**。

   ii. 选择您集成的 AD。

   iii. 选择**预配**选项卡。

   iv. 在**设置**下，选择**到 Okta**。

   v. 滚动到**Okta 属性映射**部分，然后选择**强制同步**。

创建 Okta API 令牌

1. 使用只读管理员帐户登录 Okta 控制台。
2. 从 Okta 控制台菜单中，选择 **安全 > API**。
3. 选择**令牌**选项卡，然后选择**创建令牌**。
4. 输入令牌的名称。
5. 选择 **创建令牌**。
6. 复制令牌值。将 Okta 组织连接到 Citrix Cloud 时，需要提供此值。

将 Citrix Cloud 连接到您的 Okta 组织

1. 在 https://citrix.cloud.com 登录 Citrix Cloud。
2. 从 Citrix Cloud 菜单中，选择 **身份和访问管理**。
3. 找到 **Okta**，然后从省略号菜单中选择 **连接**。
4. 在 **Okta URL** 中，输入您的 Okta 域。
5. 在 **Okta API 令牌** 中，输入您的 Okta 组织的 API 令牌。
6. 在 **客户端 ID** 和 **客户端密钥** 中，输入您之前创建的 OIDC Web 应用程序集成中的客户端 ID 和密钥。要从 Okta 控制台复制这些值，请选择 **应用程序** 并找到您的 Okta 应用程序。在 **客户端凭据** 下，使用每个值的 **复制到剪贴板** 按钮。
7. 单击 **测试并完成**。Citrix Cloud 将验证您的 Okta 详细信息并测试连接。

成功验证连接后，您可以为最终用户启用 Okta 身份验证。

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

为应用商店启用 Okta 身份验证

1. 从 Citrix Cloud 菜单中，选择 **StoreFront Cloud > 身份验证**。
2. 选择 **Okta**。
3. 当出现提示时，选择 **我了解这对最终用户体验的影响**。
4. 选择 **保存**。

切换到 Okta 身份验证后，Citrix Cloud 会暂时禁用商店几分钟。商店重新启用后，您的最终用户可以使用 Okta 登录。

更多信息

- Citrix 技术专区：
  - 技术洞察：身份验证 - Okta
  - 技术简报：Workspace 身份
  - 技术简报：Workspace SSO

故障排除

问题 1

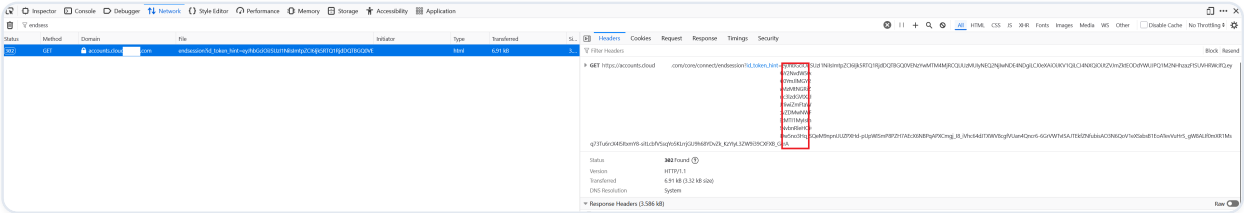
Okta OIDC 对商店的身份验证成功，但最终用户在商店中看不到 DaaS 资源。这可能是由于缺少诸如“ctx_user.sid”之类的声明未发送到 DaaS 造成的。

调试步骤 1

1. 使用浏览器捕获 HAR 文件，并使用 Okta OIDC 身份验证登录商店，然后从商店注销。
2. 当用户从商店执行显式注销操作时，在浏览器开发人员工具中找到以下调用

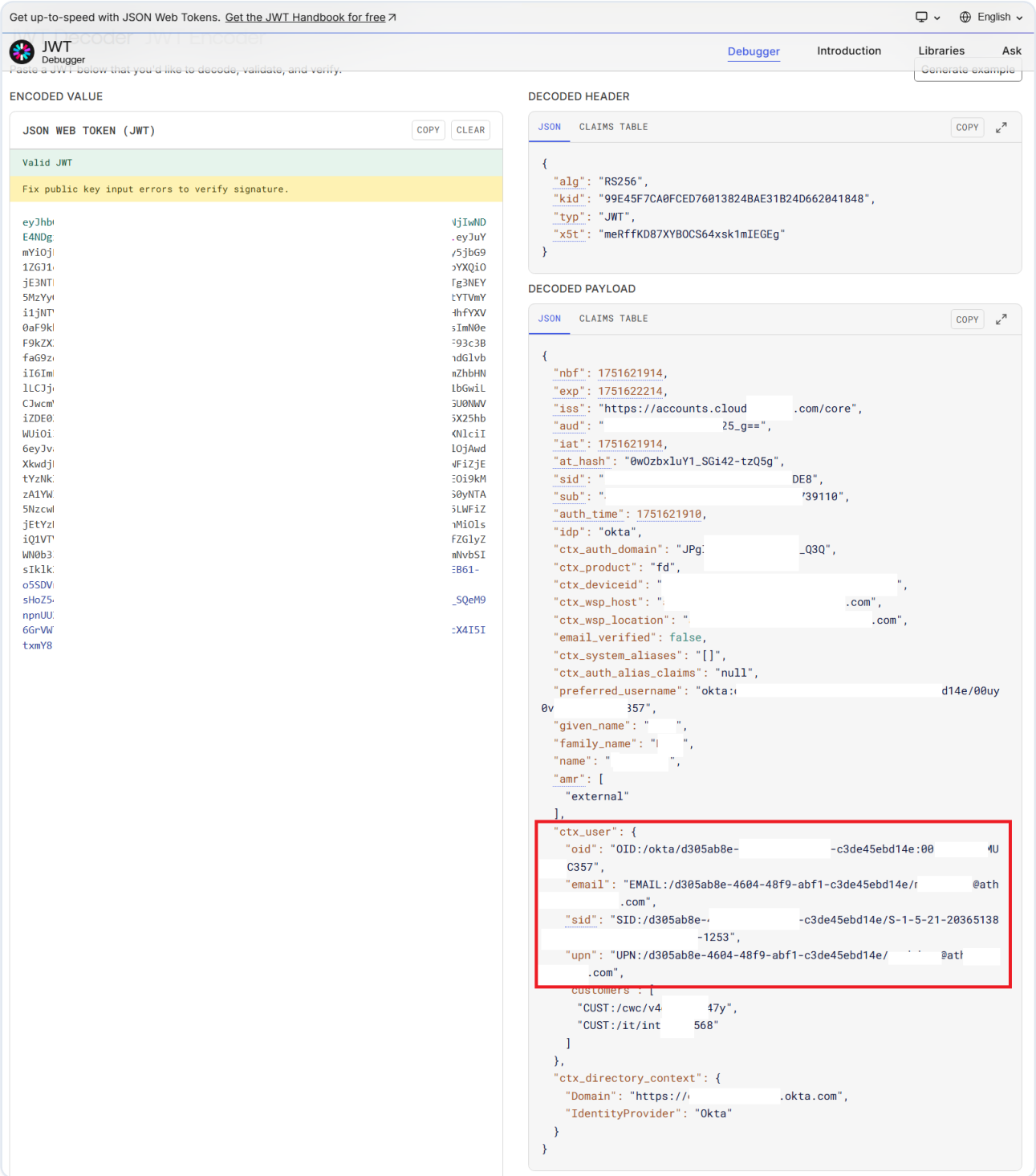
   GET `https://accounts.cloud.com/core/connect/endsession?id_token_hint=<base64string>`

3. 复制 `?id_token_hint=` 之后的 base64 字符串，其中包含一个 JWT。示例取自 FireFox 开发工具。



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

将此 base64 字符串粘贴到 `https://jwt.io` 中的“Encoded Value JSON WEB TOKEN (JWT)”字段，以检查 Citrix Cloud 从您的 Okta OIDC 应用程序收到的声明。 验证 `"ctx_user": {}` 中是否存在所有必需的声明，并且每个声明都包含登录到商店的用户的正确用户数据。确保 `"ctx_user": {}` 中有四个名为 `"oid", "email", "sid", and "upn"` 的声明。已解码 JWT 的示例。



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

原因 1

您的 Okta OIDC 应用程序未发送所有四个必需的 cip_* 声明，或者您的 Okta 用户配置文件不包含必需的属性。

解决方案 1

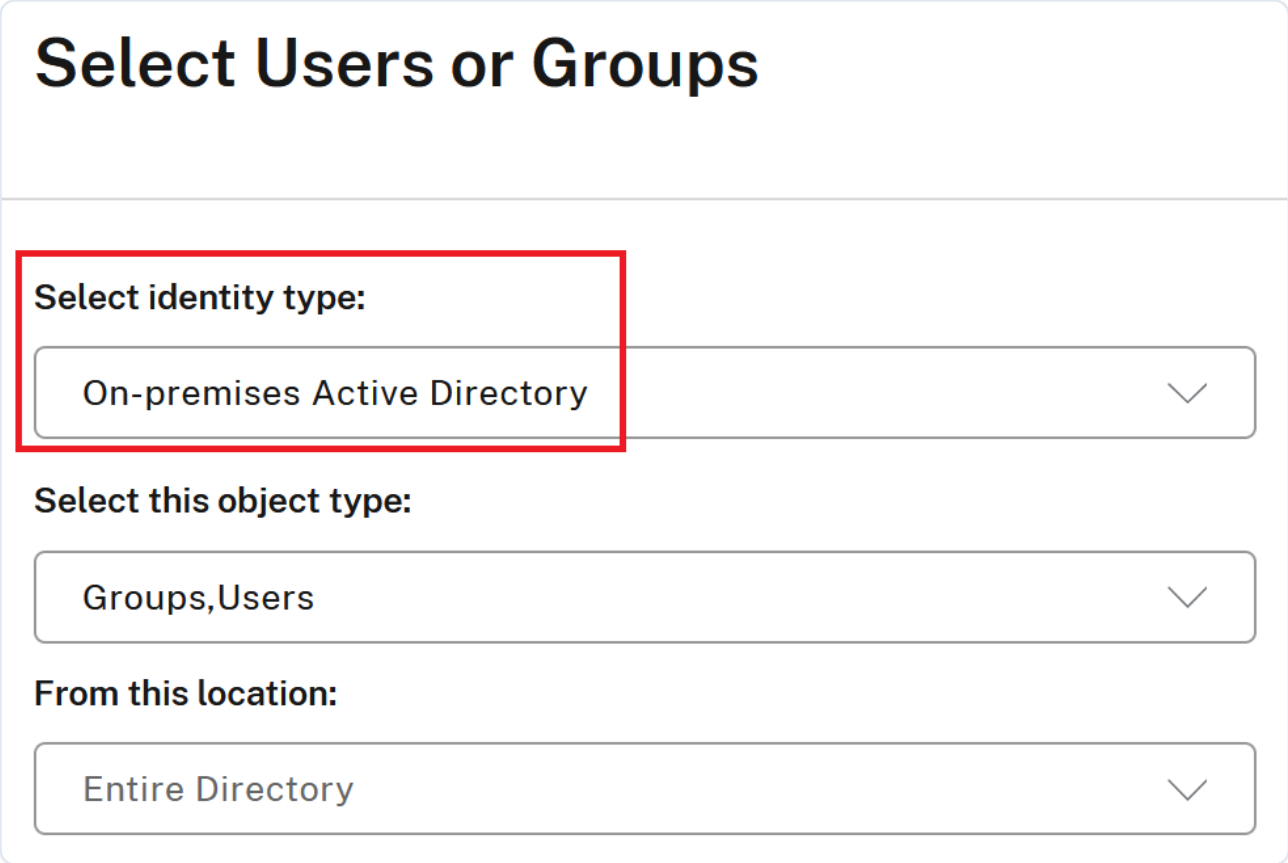
检查您的 Okta OIDC 应用程序配置和 Okta 用户配置文件属性映射。确保您的 Okta OIDC 应用程序正在发送正确的声明。使用声明名称 `cip_upn, cip_email, cip_sid, and cip_oid`。所有声明名称都必须是小写。

原因 2

您错误地配置了 DaaS 交付组，并将资源映射到 **Okta** 身份而不是 **Active Directory** 身份。

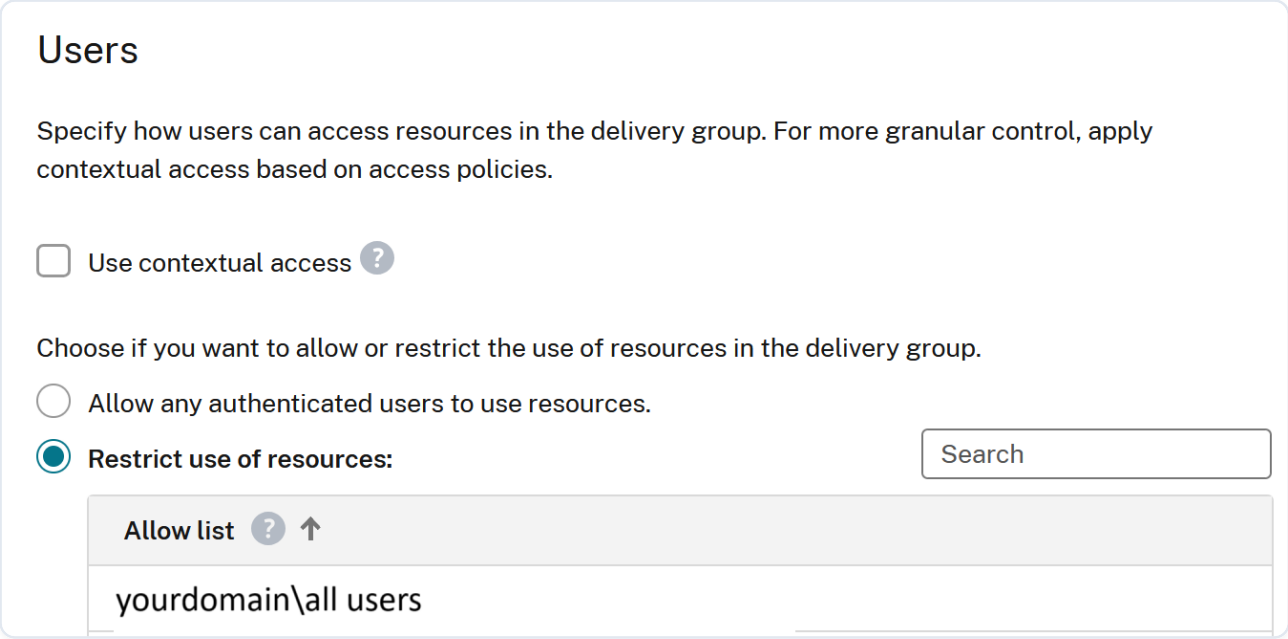
解决方案 2

将加入 AD 域的交付组和 VDA 映射到 **Active Directory** 身份，而不是 **Okta** 身份。仅将 **Okta** 身份用于启动**未加入域**的资源。



将交付组配置为根据 AD 用户和组**限制资源使用**。

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



原因 3

您未按照 Citrix Cloud 的要求使用 **AD 通用组**，或者您的 Citrix Cloud Connector 未加入正确的 AD 域级别。有关详细信息，请参阅本文：Citrix Cloud Connector 系统要求

解决方案 3

在将用户分配给 DaaS 资源时使用通用组

或者，

将商店用户直接分配到交付组。

将 SAML 作为身份提供程序连接到 Citrix Cloud™

Citrix Cloud 支持使用 SAML（安全断言标记语言）作为身份提供程序，以对登录其商店的 Citrix Cloud 管理员和最终用户进行身份验证。您可以将您选择的 SAML 2.0 提供程序与本地 Active Directory (AD) 结合使用。

关于本文

本文介绍了配置 Citrix Cloud 与 SAML 提供程序之间连接所需的步骤。其中一些步骤描述了您在 SAML 提供程序的管理控制台中执行的操作。您用于执行这些操作的具体命令可能与本文中描述的命令有所不同，具体取决于您选择的 SAML 提供程序。这些 SAML 提供程序命令仅作为示例提供。有关您的 SAML 提供程序的相应命令的更多信息，请参阅您的 SAML 提供程序的文档。

Citrix SAML 登录用例

- 最终用户登录商店。

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

- 最终用户使用商店自定义域登录商店。
- 管理员用户登录 Citrix Cloud。

为您的用例选择正确的 SAML 流程

- **AD 支持的身份**，导入到您的 SAML 提供程序中。这些身份包含本地用户属性，例如 objectSIDs 和 objectGUIDs。这些不需要 AD 影子帐户，因为与这些导入用户对应的 AD 帐户已存在于 Active Directory 中。
- **本机身份**，仅存在于 SAML 提供程序目录中，例如 Entra ID 或 Okta 用户。这些身份在 AD 中没有对应的身份，如果使用 AD 域加入的 VDA 和 DaaS 目录，则需要 AD 影子帐户。这些用户没有嵌入的 objectSIDs。
- **Entra ID 访客/B2B 用户**，他们从其他 Entra ID 租户或使用访客电子邮件地址被邀请到 Entra ID。这些身份在 AD 中没有对应的身份，如果使用 AD 域加入的 VDA 和 DaaS 目录，则需要 AD 影子帐户。这些用户可能没有嵌入的 objectSIDs。某些用户在错误的 Active Directory 中可能具有不正确的 objectSIDs。

支持的 SAML 提供程序

支持官方 SAML 2.0 规范的 SAML 提供程序均可与 Citrix Cloud 结合使用。

Citrix 已测试以下 SAML 提供程序，用于对 Citrix Cloud 管理员进行身份验证，以及使用单点登录 (SSO) 和单点注销 (SLO) 对 Citrix® StoreFront Cloud 最终用户进行身份验证。未在此列表中出现的 SAML 提供程序也受支持。

- 微软 ADFS
- 微软 Entra ID
- Duo
- 奥克塔
- PingFederate

在测试这些提供商时，Citrix 使用了以下设置在 Citrix Cloud 控制台中配置 SAML 连接：

CITRIX CLOUD 中的此字段	输入此值
实体 ID	`https://entityid.com`
签署身份验证请求	是
SSO 服务 URL	`https://yoursamlprovider/sso/saml2`

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

CITRIX CLOUD 中的此字段	输入此值
SSO 绑定机制	HTTP 提交
SAML 响应	签署响应或断言
身份验证上下文	未指定，精确
注销 URL	`https://yoursamlprovider/slo/saml2`
签署注销请求	是
SLO 绑定机制	HTTP 提交

有关这些设置的更多信息，请参阅本文中的将 SAML 提供程序元数据添加到 Citrix Cloud。

支持范围限定的实体 ID

本文介绍了如何使用单个 SAML 应用程序和 Citrix Cloud 的默认通用实体 ID 配置 SAML 身份验证。

如果您的 SAML 身份验证要求包括在单个 SAML 提供程序中使用多个 SAML 应用程序，请参阅在 Citrix Cloud 中配置具有范围限定实体 ID 的 SAML 应用程序。

管理员使用 SAML 2.0 进行身份验证

Citrix Cloud 支持使用 SAML 2.0 对 AD 中的单个管理员和管理员组的成员进行身份验证。有关将管理员组添加到 Citrix Cloud 的更多信息，请参阅管理管理员组。

使用现有 SAML 连接进行管理员身份验证

如果您在 Citrix Cloud 中已有 SAML 2.0 连接并希望使用它来验证管理员，则必须首先在**身份和访问管理**中断开 SAML 2.0，然后重新配置连接。如果您正在使用 SAML 连接来验证 StoreFront Cloud 最终用户，则还必须在 **StoreFront Cloud** 中禁用 SAML 身份验证方法。重新配置 SAML 连接后，您可以将单个管理员或管理员组添加到 Citrix Cloud。

如果您尝试在未首先断开并重新连接 SAML 2.0 的情况下添加单个管理员或管理员组，则将管理员组添加到 Citrix Cloud 中所述的 **Active Directory** 身份选项将不会出现。

设置新 SAML 连接的任务概述

要在 Citrix Cloud 中设置新的 SAML 2.0 连接，请执行以下任务：

1. 在**身份和访问管理**中，按照将 Active Directory 连接到 Citrix Cloud 中所述，将您的本地 AD 连接到 Citrix Cloud。

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

2. 按照本文中SAML 与 Active Directory 集成 中所述，将您的 SAML 提供程序与您的本地 AD 集成。
3. 配置登录 URL，管理员可以使用该 URL 登录 Citrix Cloud。
4. 在**身份和访问管理**中，配置 Citrix Cloud 中的 SAML 身份验证。此任务涉及使用 Citrix Cloud 中的 SAML 元数据配置您的 SAML 提供程序，然后使用您的 SAML 提供程序中的元数据配置 Citrix Cloud 以创建 SAML 连接。

为 Citrix Cloud 管理员使用现有 SAML 连接的任务概述

如果您在 Citrix Cloud 中已有 SAML 2.0 连接并希望将其用于管理员身份验证，请执行以下任务：

1. 如果适用，禁用 SAML 2.0 存储身份验证：在 **StoreFront Cloud > 身份验证**中，选择其他身份验证方法，然后在出现提示时选择**确认**。
2. 断开现有 SAML 2.0 连接：在**身份和访问管理 > 身份验证**中，找到 SAML 连接。从最右侧的省略号菜单中，选择**断开连接**。选择**是，断开连接**以确认操作。
3. 重新连接 SAML 2.0 并配置连接：从 **SAML 2.0** 的省略号菜单中，选择 **连接**。
4. 出现提示时，为管理员将用于登录的 登录 URL 输入一个唯一标识符。
5. 按照本文中 配置 SAML 身份提供商元数据 所述配置 SAML 连接。

配置 SAML 连接后，您可以按照 管理管理员组 所述将 AD 管理员组添加到 Citrix Cloud。您还可以按照本文所述 为最终用户重新启用 SAML。

创建和映射自定义 SAML 属性

如果您的 SAML 身份提供商中已配置 SID、UPN、OID、电子邮件和 displayName 属性的自定义属性，则无需执行此任务。请继续执行 创建 SAML 连接器应用程序 并在步骤 5 中使用您现有的自定义 SAML 属性。

注意：

本节中的步骤描述了您在 SAML 身份提供商的管理控制台中执行的操作。根据您选择的 SAML 身份提供商，用于执行这些操作的具体命令可能与本节中描述的命令有所不同。本节中的 SAML 身份提供商命令仅作为示例提供。有关您的 SAML 身份提供商的相应命令的更多信息，请参阅您的 SAML 身份提供商的文档。

1. 登录到您的 SAML 身份提供商的管理控制台，然后选择用于创建自定义用户属性的选项。例如，根据您的 SAML 身份提供商的控制台，您可能会选择 **用户 > 自定义用户字段 > 新建用户字段**。

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

2. 为以下 AD 属性添加属性。使用所示的默认值命名属性。

AD 属性	必需或可选	默认值
userPrincipalName	如果未添加 SID 属性（推荐），则为必需。	`cip_upn`
objectSID	如果未添加 UPN 属性，则为必需项。	`cip_sid`
objectGUID	身份验证可选	`cip_oid`
邮件	身份验证可选	`cip_email`
displayName	应用商店 UI 必需	`displayName`
givenName	应用商店 UI 必需	`firstName`
sn	商店 UI 所需	`lastName`
AD 域林	身份验证可选	`cip_forest`
AD 域	身份验证可选	`cip_domain`

3. 选择您已连接到 Citrix Cloud 的 AD。例如，根据您的 SAML 提供商控制台，您可能会选择 **用户 > 目录**。
4. 选择添加目录属性的选项。例如，根据您的 SAML 提供商控制台，您可能会选择 **目录属性**。
5. 选择添加属性的选项，并将以下 AD 属性映射到您在步骤 2 中创建的自定义用户属性：
   - 如果您在步骤 2 中添加了 SID 属性（例如，`cip_sid`），请选择 **objectSid** 并映射到您创建的属性。
   - 如果您在步骤 2 中添加了 UPN 属性（例如，`cip_upn`），请选择 **userPrincipalName** 并映射到您创建的属性。
   - 如果您在步骤 2 中添加了 ObjectGUID 属性（例如，`cip_oid`），请选择 **ObjectGUID** 并映射到您创建的属性。
   - 如果您在步骤 2 中添加了 Mail 属性（例如，`cip_email`），请选择 **mail** 并映射到您创建的属性。
   - 如果您在步骤 2 中添加了 Display Name 属性（例如，`displayName`），请选择 **displayName** 并映射到您创建的属性。

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

配置管理员登录 URL

1. 在 https://citrix.cloud.com 登录 Citrix Cloud。
2. 从 Citrix Cloud 菜单中，选择 **身份和访问管理**。
3. 找到 **SAML 2.0**，然后从省略号菜单中选择 **Connect**。
4. 出现提示时，为您的公司输入一个简短的、URL 友好的标识符，然后选择 **Save and continue**。将显示 **Configure SAML** 页面。
5. 继续下一部分以配置与 Citrix Cloud 的 SAML 连接。

配置 SAML 提供程序元数据

在此任务中，您将使用 Citrix Cloud 中的 SAML 元数据创建连接器应用程序。配置 SAML 应用程序后，您将使用连接器应用程序中的 SAML 元数据来配置与 Citrix Cloud 的 SAML 连接。

注意：

本节中的某些步骤描述了您在 SAML 提供程序的管理控制台中执行的操作。根据您选择的 SAML 提供程序，用于执行这些操作的具体命令可能与本节中描述的命令有所不同。本节中的 SAML 提供程序命令仅作为示例提供。有关您的 SAML 提供程序的相应命令的更多信息，请参阅您的 SAML 提供程序的文档。

创建 SAML 连接器应用程序

1. 在 SAML 提供程序的管理控制台中，为具有属性和签名响应的身份提供程序添加应用程序。例如，根据您的提供程序的控制台，您可能选择 **Applications > Applications > Add App**，然后选择 **SAML Test Connector (IdP w/ attr w/ sign response)**。
2. 如果适用，输入显示名称并保存应用程序。
3. 在 Citrix Cloud 的“**配置 SAML**”屏幕中，在“**SAML 元数据**”中，选择“**下载**”。元数据 XML 文件将显示在另一个浏览器选项卡中。

   注意：

   如果需要，您也可以从 `https://saml.cloud.com/saml/metadata.xml` 下载此文件。在导入和监控 SAML 身份提供商元数据时，此端点可能对某些身份提供商更友好。

4. 输入连接器应用程序的以下详细信息：

   - 在“**受众**”字段中，输入 `https://saml.cloud.com`。

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

- 在“**收件人**”字段中，输入 `https://saml.cloud.com/saml/acs`。
- 在 ACS URL 验证器字段中，输入 `https://saml.cloud.com/saml/acs`。
- 在 ACS URL 字段中，输入 `https://saml.cloud.com/saml/acs`。

5. 将您的自定义 SAML 属性添加为应用程序中的参数值：

创建此字段	分配此自定义属性
cip_sid	您为 SID 创建的自定义属性。示例：cip_sid
cip_upn	您为 UPN 创建的自定义属性。示例：cip_upn
cip_oid	您为 ObjectGUID 创建的自定义属性。示例：cip_oid
cip_email	您为 Mail 创建的自定义属性。示例：cip_email
displayName	您为 Display Name 创建的自定义属性。示例：displayName

6. 将您的最终用户添加为用户，以允许他们访问应用程序。

将 SAML 提供程序元数据添加到 Citrix Cloud

1. 从您的 SAML 提供程序获取 SAML 元数据。下图是此文件可能的外观示例：

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

```
<?xml version="1.0"?>
<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata" entityID="
https://app.[redacted].com/saml/metadata/8c733cbd-c579-41d4-b4e1-4ff034893d19">
  <IDPSSODescriptor xmlns:ds="http://www.w3.org/2000/09/xmldsig#" protocolSupportEnumeration=
  "urn:oasis:names:tc:SAML:2.0:protocol">
    <KeyDescriptor use="signing">
      <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:X509Data>
          <ds:X509Certificate>MIID2DCCA[redacted]
[redacted]+w3PpA==</ds:X509Certificate>
        </ds:X509Data>
      </ds:KeyInfo>
    </KeyDescriptor>
    <SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="
    https://citrixidentity-dev.[redacted].com/trust/saml2/http-redirect/slo/1097253"/>

      <NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</NameIDFormat>

    <SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="
    https://citrixidentity-dev.[redacted].com/trust/saml2/http-redirect/sso/8c733cbd-c579-41d4-b4e1-4ff034893d19"/>
    <SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="
    https://citrixidentity-dev.[redacted].com/trust/saml2/http-post/sso/8c733cbd-c579-41d4-b4e1-4ff034893d19"/>
    <SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP" Location=
    "https://citrixidentity-dev.[redacted].com/trust/saml2/soap/sso/8c733cbd-c579-41d4-b4e1-4ff034893d19"/>
  </IDPSSODescriptor>
</EntityDescriptor>
```


2. 在 Citrix Cloud 的**配置 SAML** 屏幕中，输入 SAML 提供程序的元数据文件中的以下值：

   - 在**身份提供程序实体 ID** 中，输入元数据中 **EntityDescriptor** 元素中的 **entityID** 值。

     ```
     <EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata" entityID="
     https://app.[redacted].com/saml/metadata/8c733cbd-c579-41d4-b4e1-4ff034893d19">
     ```

   - 在**签署身份验证请求**中，选择**是**以允许 Citrix Cloud 签署身份验证请求，证明它们来自 Citrix Cloud 而非恶意行为者。如果您希望将 Citrix ACS URL 添加到 SAML 提供程序用于安全发布 SAML 响应的允许列表中，请选择**否**。

   - 在 **SSO 服务 URL** 中，输入您要使用的绑定机制的 URL。您可以使用 HTTP-POST 或 HTTP-Redirect 绑定。在元数据文件中，找到绑定值为 **HTTP-POST** 或 **HTTP-Redirect** 的 **SingleSignOnService** 元素。

     ```
     <SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="
     https://citrixidentity-dev.[redacted]/trust/saml2/http-redirect/sso/8c733cbd-c579-41d4-b4e1-4ff034893d19"/>
     <SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="
     https://citrixidentity-dev.[redacted].com/trust/saml2/http-post/sso/8c733cbd-c579-41d4-b4e1-4ff034893d19"/>
     ```

   - 在 **绑定机制** 中，选择与您从元数据文件中选择的 SSO 服务 URL 的绑定匹配的机制。默认情况下，选择 **HTTP Post**。

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

- 在 **SAML 响应** 中，选择您的 SAML 提供程序用于 SAML 响应和 SAML 断言的签名方法。默认情况下，选择 **签名响应或断言**。Citrix Cloud 将拒绝任何未按此字段中指定签名方式签名的响应。

3. 在您的 SAML 提供程序的管理控制台中，执行以下操作：

   - 为 SAML 签名算法选择 **SHA-256**。
   - 将 X.509 证书下载为 Base64 编码的 PEM、CRT 或 CER 文件。

4. 在 Citrix Cloud 的 **配置 SAML** 页面上，在 **X.509 证书** 中，选择 **上传文件** 并选择您在上一步中下载的证书文件。
5. 选择 **继续** 以完成上传。
6. 在 **身份验证上下文** 中，选择您要使用的上下文以及您希望 Citrix Cloud 强制执行此上下文的严格程度。选择 **最小** 以在选定的上下文中请求身份验证，而不强制执行该上下文的身份验证。选择 **精确** 以在选定的上下文中请求身份验证，并且仅在该上下文中强制执行身份验证。如果您的 SAML 提供程序不支持身份验证上下文或您选择不使用它们，请选择 **未指定** 和 **最小**。默认情况下，选择 **未指定** 和 **精确**。
7. 对于 **注销 URL**（可选），决定您是否希望用户在注销其商店或 Citrix Cloud 后，也注销他们之前通过 SAML 提供程序登录的所有 Web 应用程序。

   - 如果您希望用户在注销其商店或 Citrix Cloud 后仍保持登录其 Web 应用程序，请将 **注销 URL** 字段留空。
   - 如果您希望用户在注销其商店或 Citrix Cloud 后注销所有 Web 应用程序，请输入您的 SAML 提供程序的 SingleLogout (SLO) 端点。如果您使用 Microsoft ADFS 或 Microsoft Entra ID 作为 SAML 提供程序，则 SLO 端点与单点登录 (SSO) 端点相同。

8. 验证 Citrix Cloud 中的以下默认属性值是否与您的 SAML 提供程序中配置的相应属性值匹配。为了让 Citrix Cloud 在 SAML 断言中找到这些属性，此处输入的值必须与您的 SAML 提供程序中的值匹配。如果您未在 SAML 提供程序中配置某个属性，则可以使用 Citrix Cloud 中的默认值或将该字段留空，除非另有说明。

   - **用户显示名称的属性名称**：默认值为 `displayName`。
   - **用户名的属性名称**：默认值为 `firstName`。

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

- **用户姓氏的属性名称**：默认值为 `lastName`。
- **安全标识符 (SID) 的属性名称**：如果您没有为 UPN 创建属性，则必须从 SAML 提供程序输入此属性名称。默认值为 `cip_sid`。
- **用户主体名称 (UPN) 的属性名称**：如果您没有为 SID 创建属性，则必须从 SAML 提供程序输入此属性名称。默认值为 `cip_upn`。
- **电子邮件的属性名称**：默认值为 `cip_email`。
- **AD 对象标识符 (OID) 的属性名称**：默认值为 `cip_oid`。
- **AD 林的属性名称**：默认值为 `cip_forest`。
- **AD 域的属性名称**：默认值为 `cip_domain`。

9. 选择 **测试并完成** 以验证您是否已成功配置连接。

从 AD 将管理员添加到 Citrix Cloud

有关在 Citrix Cloud 中添加和管理 AD 组的说明，请参阅 管理管理员组。

为应用商店启用 SAML 身份验证

1. 从 Citrix Cloud 菜单中，选择 **StoreFront Cloud**。
2. 选择 **身份验证** 选项卡
3. 选择 **SAML 2.0**。

在身份和访问管理中克隆现有 SAML 连接

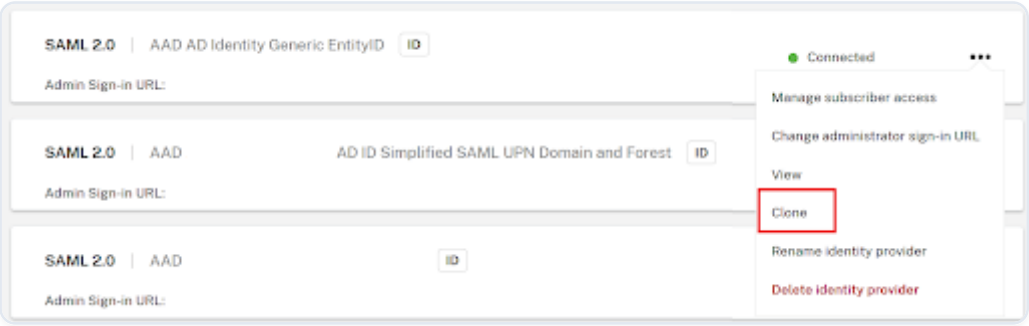
重要提示：

克隆 SAML 连接不会克隆现有的范围实体 ID。如果您在克隆过程中添加范围实体 ID 或生成新的实体 ID，则可能需要更新您的 SAML 应用程序配置。

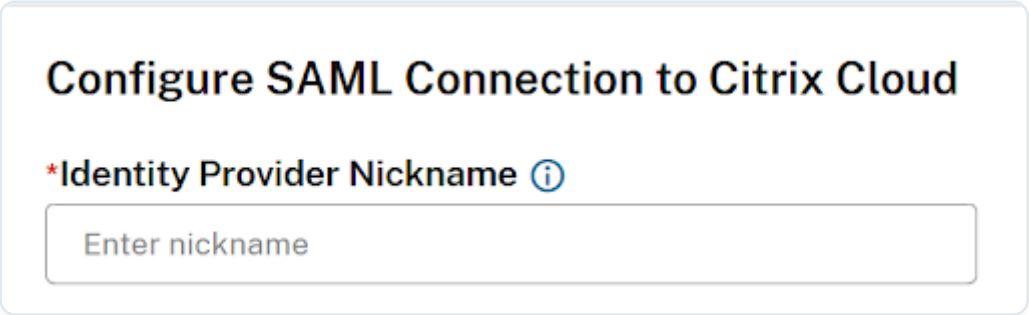
要克隆现有 SAML 连接，请按照以下步骤操作：

1. 选择现有 SAML 连接右侧的三个点，然后从操作列表中选择 **克隆**。

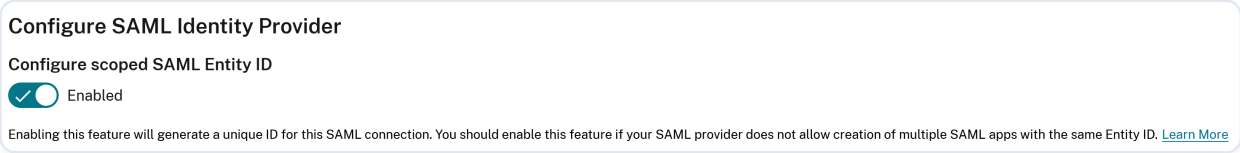
© 1997–2026 Citrix Systems, Inc. All rights reserved.



2. 为新的 SAML 连接输入一个新的唯一 GO URL。如果需要，以后可以更改此项。
3. 为新的 SAML 连接输入一个新的唯一昵称。



4. 更新连接中的任何设置，例如启用范围实体 ID、需要启用签名、添加缺失的注销 URL，或更新最近已过期的 SAML 提供程序证书.....
5. 单击“测试并完成”以保存新的 SAML 连接。
6. 切换商店以在 **StoreFront Cloud -> 身份验证** 中使用新的 SAML 连接。
7. 使用新的范围实体 ID 更新您的 SAML 应用程序配置（并非总是必需）



先决条件

将 SAML 身份验证与 Citrix Cloud 结合使用有以下要求：

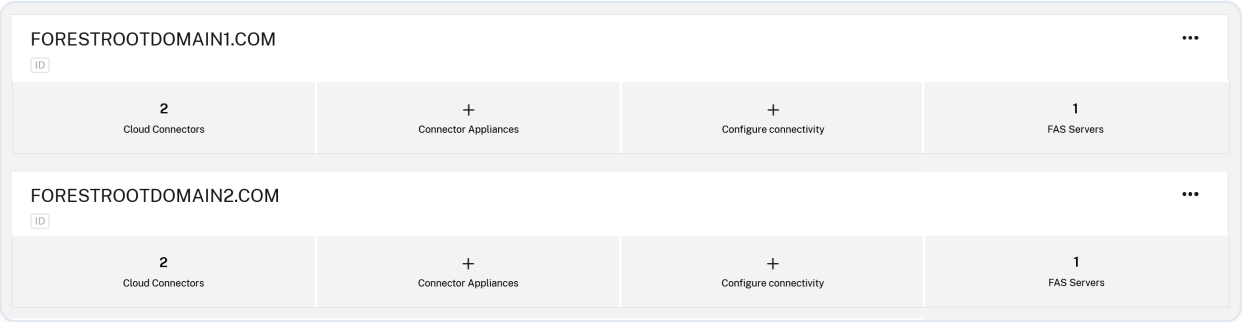
- 支持 SAML 2.0 的 SAML 提供程序。
- 本地 AD 域。
- 两个 Cloud Connector 部署到资源位置并加入您的本地 AD 域。Cloud Connector 用于确保 Citrix Cloud 可以与您的资源位置通信。
- AD 与您的 SAML 提供程序集成。

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

云连接器

您需要至少两 (2) 台服务器来安装 Citrix Cloud Connector™ 软件。Citrix 建议至少两台服务器以实现 Cloud Connector 高可用性。这些服务器必须满足以下要求：

- 满足 Cloud Connector 系统要求 中描述的系统要求。
- 未安装任何其他 Citrix® 组件，不是 AD 域控制器，也不是对您的资源位置基础结构至关重要的计算机。
- 加入到您的 AD 用户和资源所在的 AD 域。如果用户访问多个域中的资源，您需要在每个域中安装至少两个 Cloud Connector。



- 连接到可以联系最终用户通过其商店访问的资源的网络。
- 连接到 Internet。有关更多信息，请参阅 系统和连接要求。

有关安装 Cloud Connector 的更多信息，请参阅 Cloud Connector 安装。

Active Directory (默认 AD 身份 SAML 流程)

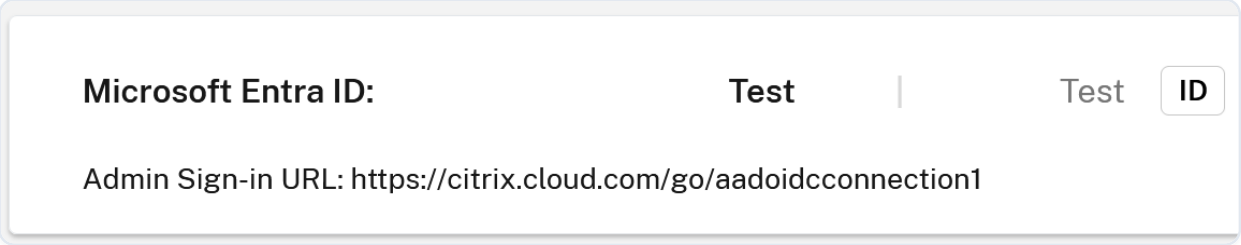
- 验证您的最终用户在您的 AD 中拥有用户帐户。当配置了 SAML 身份验证时，没有 AD 帐户的最终用户无法成功登录其商店。
- 通过在您的本地 AD 中部署 Cloud Connector，将您的 AD 连接到您的 Citrix Cloud 帐户。
- 将您的 AD 用户同步到 SAML 提供程序。Citrix Cloud 需要最终用户的 AD 用户属性，以便他们能够成功登录。
- 只能使用通用 AD 组。
- 您必须在 Active Directory 中定义您的 SAML 用户配置使用的任何 UPN 后缀。Citrix Cloud 连接器不能使用未定义或模糊的 UPN 后缀来确定 Active Directory 域上下文。
- 默认 SAML 流程不需要 EntraID OIDC IdP 连接，因为这使用 AD 身份。

EntraID 目录 (EntraID 身份 SAML 流程)

- EntraID B2B 和外部用户支持需要具有与 EntraID 内部前端用户匹配的 UPN 的 AD 影子帐户。

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

- 如果使用 SAML with Entra ID identities 中所述的 Entra ID 身份 SAML 流程，那么您还必须在 **身份和访问管理 > 身份验证** 中连接正确的 EntraID 租户。



AD 用户属性

所有 Active Directory 用户对象都需要以下属性，并且必须填充：

- 通用名称
- SAM 帐户名
- 用户主体名称 (UPN)
- 对象 GUID
- SID

Citrix Cloud 使用您的 AD 中的对象 GUID 和 SID 属性，在最终用户登录其商店时建立用户上下文。如果这些属性中的任何一个未填充，最终用户将无法登录。

以下属性并非使用 SAML 身份验证与 Citrix Cloud 集成的必需属性，但 Citrix 建议填充它们以确保最佳用户体验：

- 电子邮件地址
- 显示名称

Citrix Cloud 使用显示名称属性在其商店中正确显示最终用户的名称。如果此属性未填充，最终用户仍然可以登录，但其名称可能无法按预期显示。

SAML 与 Active Directory 集成

在启用 SAML 身份验证之前，您必须将本地 AD 与 SAML 提供程序集成。此集成允许 SAML 提供程序在 SAML 断言中将以下必需的 AD 用户属性传递给 Citrix Cloud：

- objectSID (SID)
- objectGUID (OID)
- userPrincipalName (UPN)
- Mail (电子邮件)

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

- 显示名称 (displayName)

您可以配置这些属性的一个子集，前提是 SAML 断言中包含 SID 或 UPN 属性。Citrix Cloud 会根据需要从您的 AD 中检索其他属性。

注意：

为确保最佳性能，Citrix 建议配置本节中提及的所有属性。

尽管不同 SAML 提供商的集成步骤各不相同，但集成过程通常包括以下任务：

1. 在您的 AD 域中安装同步代理，以在您的域和 SAML 提供商之间建立连接。如果您使用 ADFS 作为 SAML 提供商，则不需要此步骤。
2. 创建自定义属性并将其映射到本节前面提到的所需 AD 用户属性。有关参考，此任务的一般步骤在本文的创建和映射自定义 SAML 属性中进行了描述。
3. 将您的 AD 用户同步到您的 SAML 提供商。

有关将 AD 与 SAML 提供商集成的更多信息，请查阅您的 SAML 提供商的产品文档。

如何选择 SAML 绑定机制?

对于 SSO 和 SLO，是使用 HTTP POST 还是 HTTP Redirect 取决于您的 SAML IdP 支持的 SAML 绑定。如果您的 SAML 提供程序支持多种绑定机制，Citrix 建议您选择 HTTP Post 而不是 HTTP Redirect 作为 SAML 绑定。如果您的 SAML 提供程序同时支持这两种机制，则无需同时启用它们。建议您为 SSO 和 SLO 选择单一的 SAML 绑定类型。

SAML 绑定支持

SAML 绑定	CITRIX CLOUD 支持
HTTP POST	推荐。
HTTP 重定向	支持。
SAML Artifact 绑定	不支持。
SOAP	不支持。

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

重要提示：

HTTP Post 是 SSO 和 SLO 请求的推荐绑定机制，原因有二。

HTTP Post 在SAML连接双方都启用了签名强制时更易于调试，因为SAML XML包含易于识别的段，这些段显示了所使用的签名和证书。这比签名数据嵌入到需要URL解码的非常长的重定向URI中，更容易让人查看和调试。
HTTP Redirect URI可能会变得非常长并超过关键阈值，这会导致SAML身份验证期间出现错误，并可能导致登录或注销失败。GET绑定类型限制为最多**2,048个字符**，减去实际路径中的字符数。POST方法不受用于提交名称和值对的URL大小的限制。

服务提供商发起的 SSO 与 身份提供商发起的 SSO

SP 发起的 SSO - 最终用户直接从 Web 应用程序 (SP)（例如商店和/或 Citrix Cloud）登录，然后该应用程序将其重定向到 SAML IdP 进行身份验证，如果身份验证成功，则将最终用户重定向回 Web 应用程序 (SP) 并登录。

IdP 发起的 SSO - 最终用户首先登录其 SAML IdP，然后从 IdP 门户选择他们想要启动的应用程序 (SP)。

身份提供商发起的 SSO 可以与商店或 Citrix Cloud 一起使用?

否。商店和 Citrix Cloud 都只支持 SAML **服务提供商发起的 SSO** 登录。所有登录流程都必须通过商店 URL（用于最终用户访问）或 Citrix Cloud GO URL（用于 Citrix Cloud 管理员访问）启动。

将 SAML 提供程序直接连接到 Citrix Cloud 与 IDP 链

IDP 链是否支持 SAML 登录到商店或 Citrix Cloud?

只要 IDP 链中最接近的 SAML IDP 配置正确，并将来自 Citrix Cloud 的 SAML 请求转发到 IDP 链的后续环节，并且 IDP 链向 Citrix Cloud 返回正确的 SAML 响应，就支持 IDP 链。

IDP 链示例

- Citrix Cloud → F5（作为 SAML 提供程序直接连接到 Citrix Cloud） → 联合到 Entra ID
- Citrix Cloud → Entra ID（作为 SAML 提供程序直接连接到 Citrix Cloud） → 联合到 ADFS
- Citrix Cloud → Entra ID（作为 SAML 提供程序直接连接到 Citrix Cloud） → 联合到 PingFederate
- Citrix Cloud → Entra ID（作为 SAML 提供程序直接连接到 Citrix Cloud） → 联合到 Okta

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

如果我正在使用 IDP 链，在调试 SAML 问题时能否获得 Citrix 的协助和支持?

Citrix 支持和 Citrix 工程部门只能调试 Citrix Cloud 与链中最接近的 SAML IDP 之间的直接 SAML 连接。

重要提示：

Citrix 不负责调试直接连接的 SAML 提供程序上游的复杂 IDP 链中的问题。

是否应尽可能避免 IDP 链?

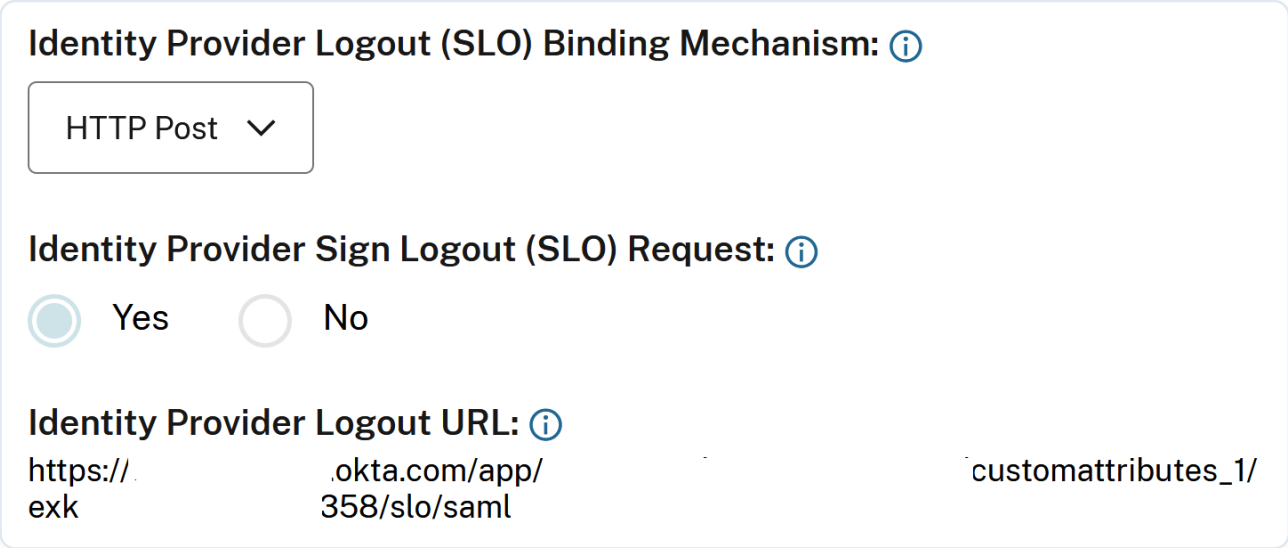
Citrix 建议将您的 SAML IDP 直接连接到 Citrix Cloud，因为这可以大大降低配置和调试的复杂性，并最大程度地减少最终用户登录延迟，这种延迟可能在 Citrix Cloud 等待复杂 IDP 链响应时产生。当多个 IDP 链接在一起时，特别是在 IDP 链中不同 IDP 使用不同的 SAML 绑定时，SSO 和 SLO 都可能出现许多问题。直接连接的 SAML 提供程序将始终比依赖上游 IDP 的提供程序更容易调试且性能更高。

SAML 注销注意事项

对于身份提供程序注销 URL (SLO)，请根据您希望连接到 Citrix Cloud 的 SAML 应用程序是否也由其他服务提供商 (SP) 共享，来决定最适合您组织的 SAML 注销行为。

Citrix 建议在您的 SAML 提供程序中创建一个新的专用 SAML 应用程序，该应用程序仅供商店和/或 Citrix Cloud 使用。如果您已遵循 Citrix 的 SAML 应用程序设置指南之一，并且正在为商店和/或 Citrix Cloud 使用专用 SAML 应用程序，那么配置注销 URL 始终是正确的做法。

选项 1：已配置 SLO（推荐）：从商店和/或 Citrix Cloud 注销的用户也会从连接的 SAML IDP 注销。



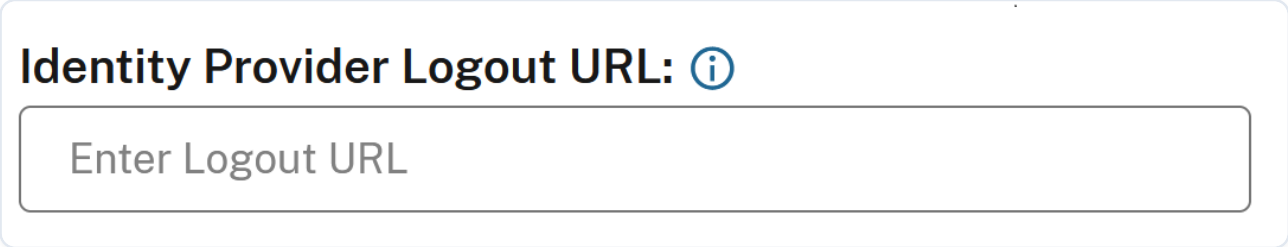
© 1997–2026 Citrix Systems, Inc. All rights reserved.

重要提示：

要使 SAML SLO 成功，您必须配置 SAML 连接的两端以支持它。Citrix Cloud 期望从 SAML 应用程序接收 SLO 响应，指示注销成功且用户已从 SAML IDP 注销。请确保您的 SAML 应用程序配置为使用此 SAML 注销端点 `https://saml.cloud.com/saml/logout/callback` 将 SLO 响应发送回 Citrix Cloud。

或

选项 2：未配置 SLO：如果您希望用户在从商店和/或 Citrix Cloud 注销后仍保持登录到您的 SAML 应用程序，请将 Citrix Cloud SAML 连接中的“注销 URL”字段留空。当最终用户在商店或 Citrix Cloud UI 中执行显式注销时，这只会将用户从商店或 Citrix Cloud 注销。用户不会从 SAML IDP 注销，并且不会从 Citrix Cloud 向 SAML 应用程序发送 SLO 请求。



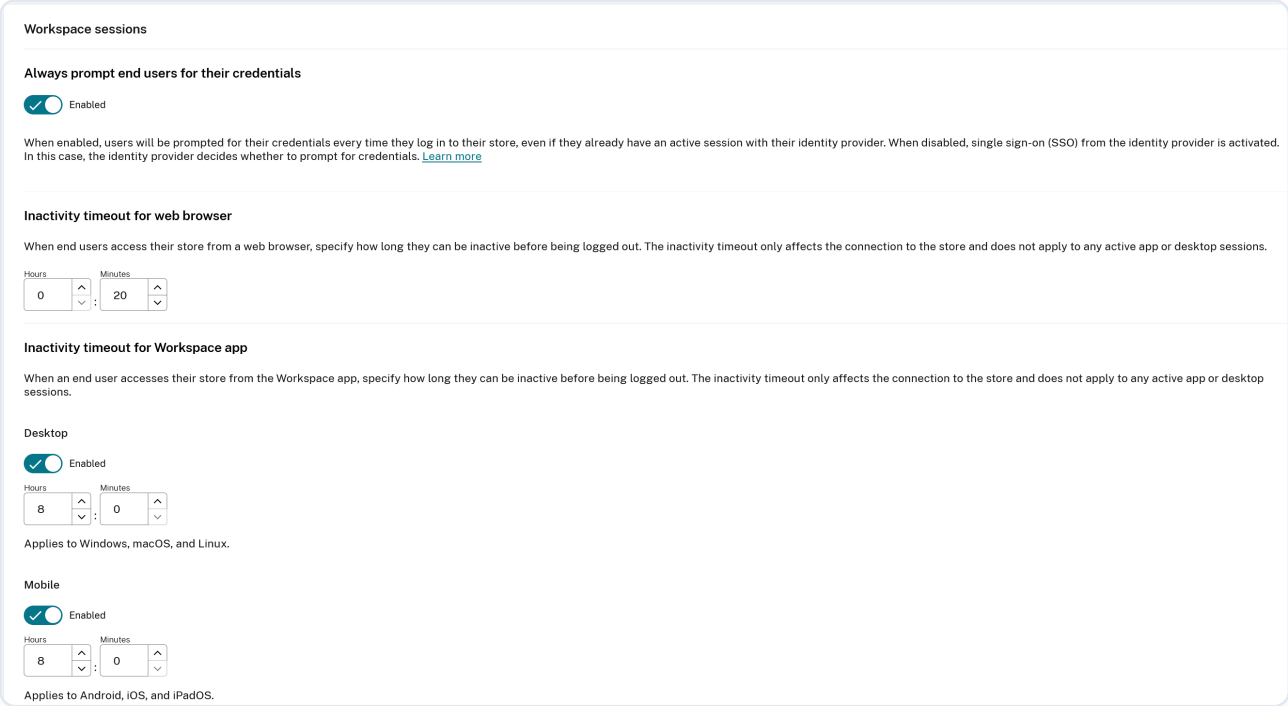
重要提示：

仅当连接到 Citrix Cloud 的 SAML 应用程序由其他非 Citrix 服务提供商 (SP) 共享时，才建议使用此未配置注销 URL 的 SAML 连接配置。

商店会话不活动超时行为

当最终用户在商店中未执行任何操作时，会话不活动超时将触发从商店注销。商店不活动超时在 **StoreFront Cloud** → **自定义** → **首选项** → **商店会话**中定义。

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



商店不活动超时不会触发 SLO 请求，以将最终用户从 SAML IdP 注销。SAML IdP 空闲会话超时可能与商店中设置的值不同。建议您尽可能将它们设置为相同的持续时间。

在 **toreFront Cloud** → **自定义** → **首选项**中，将**始终提示最终用户输入其凭据**设置为**已启用**，以确保最终用户始终被提示重新进行身份验证，即使用户的 SAML 提供程序会话仍然存在。

将**始终提示最终用户输入其凭据**设置为**已启用**，也会在 SAML 请求中将 **ForceAuthn** 设置为 **True**。

使用元数据 URL 模式创建 SAML 连接

Citrix 建议所有新的 SAML 连接都使用元数据 URL 模式创建。从您的 IdP 中获取 SAML 应用程序的元数据 URL。Citrix Cloud 可以使用 SAML IdP 元数据自动配置 SAML 连接。

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

为什么元数据 URL 模式是创建 Citrix Cloud SAML 连接的推荐方式?

简单性。 Citrix Cloud 中的 SAML 连接是使用默认连接设置值和从元数据中获取的值组合自动设置的。

IdP 元数据包含在 Citrix Cloud 中设置 SAML 连接所需的所有以下信息：

- SAML 实体 ID
- SSO 端点
- SLO 端点（如果 IdP 中已配置）
- 支持的 SAML 绑定
- 公钥和签名证书

减少维护。 自动处理 SAML IdP 内部所做的更改和 IdP 证书轮换。

当使用元数据 URL 模式时，Citrix Cloud 如何处理 IdP 证书轮换?

自动。 当您的 SAML IdP 管理员更新 SAML 应用程序以包含新的 IdP 签名证书或替换现有证书时，Citrix Cloud 会隐式信任 IdP 元数据中提供的所有 SAML 签名证书。元数据 URL 模式消除了在 Citrix Cloud 中手动进行 IdP 证书轮换的需要。IdP 管理员所做的任何更改都会自动检测到。在每次 SAML 登录期间，都会使用您的 SAML 应用程序的元数据 URL 来获取您的 SAML 应用程序签名证书的最新副本。

使用您的 IdP 元数据 URL 配置 Citrix Cloud SAML 连接

1. 获取您的 SAML 应用程序元数据的链接，并将其输入浏览器以证明其可访问，并且没有防火墙规则阻止 Citrix Cloud 访问它。

   示例：

   `https://tenant.okta.com/app/zxv1r8qo70l2q5LNT359/sso/saml/metadata`

2. 当您到达 SAML 向导的**第 4 节服务提供商**部分时，在此处输入您的 SAML 应用程序的元数据 URL，然后单击**验证**。

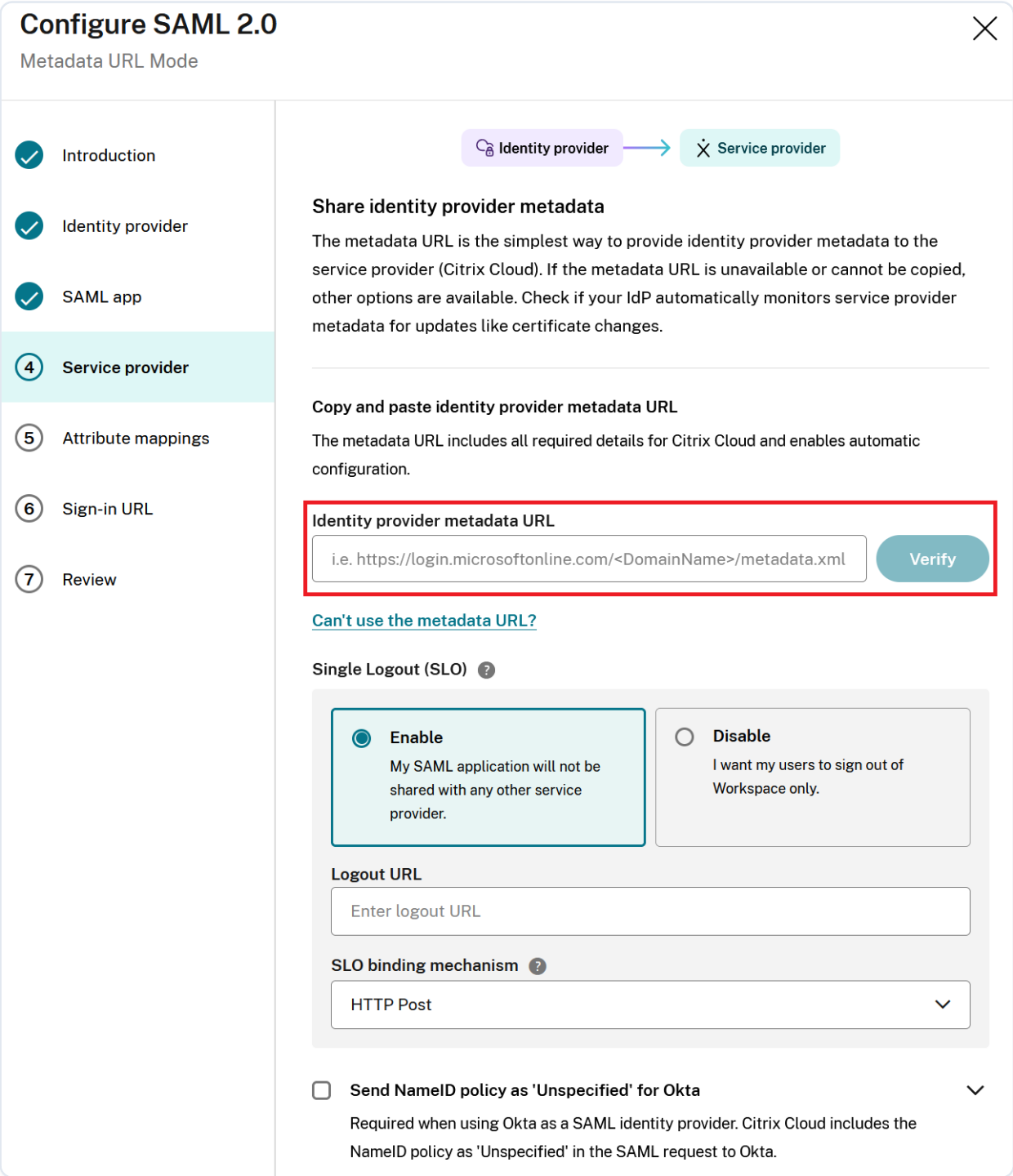
   重要提示：

   \> 如果您的 SAML 应用程序存在于本地服务器（例如 ADFS 或 PingFederate 服务器）上，并且 SAML IdP 元数据 URL 无法验证，请检查您的防火墙规则。验证您的元数据 URL 可以从组织外部的任何客户端在浏览器中访问。

3. Citrix Cloud 解析元数据 URL 后，您应该会看到此成功消息和“重新验证”。

   以下是 Okta 成功导入元数据连接的示例。

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



4. 通过启用或禁用 SLO 来配置您想要的 SAML 注销行为。

   有关注销注意事项，请参阅这篇深入文章。

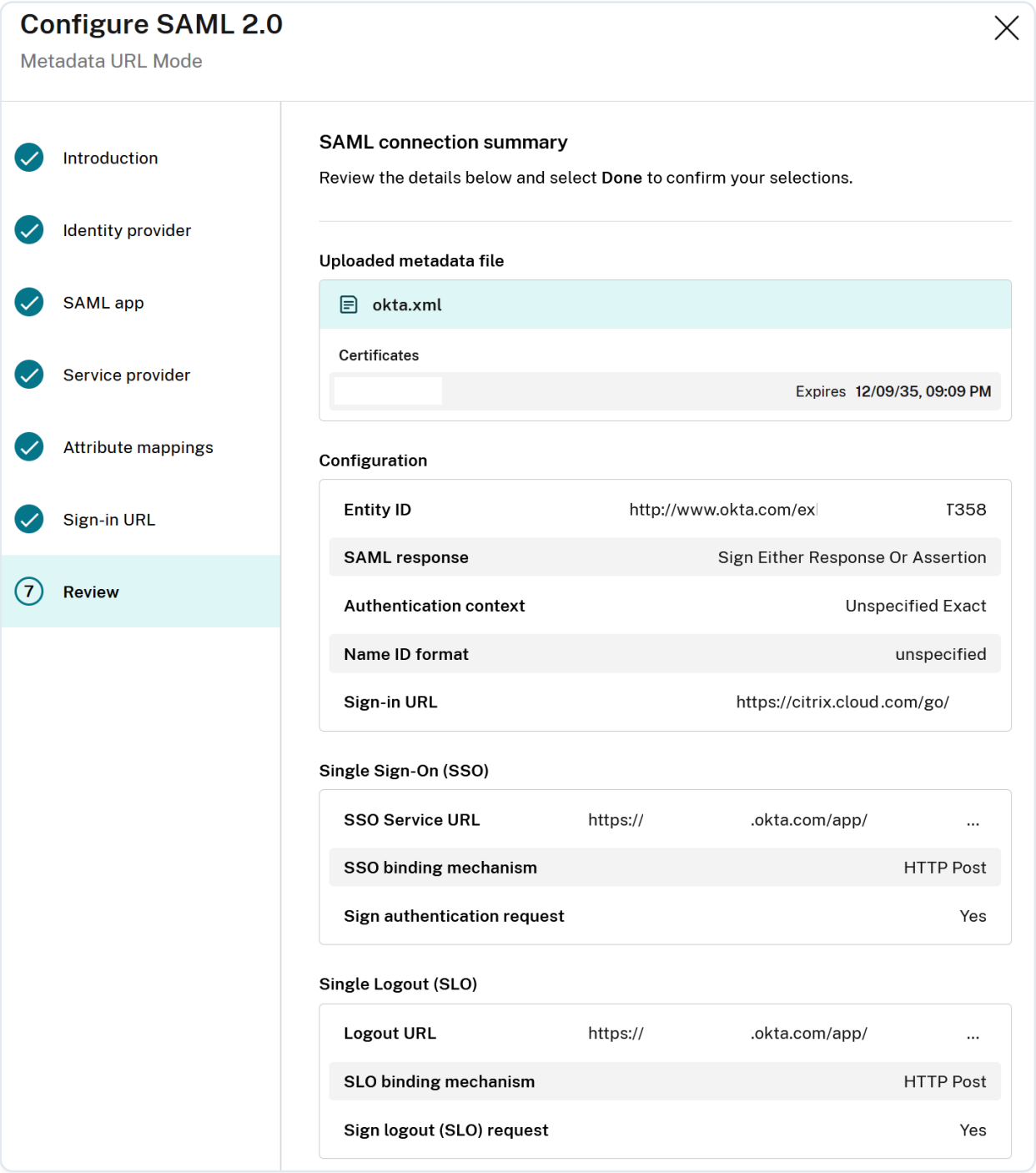
© 1997–2026 Citrix Systems, Inc. All rights reserved.

重要提示：

仅限 Okta SAML 连接。如果元数据 URL 包含 SSO 端点和包含“okta”的 DNS 域字符串，则“将 NameID 策略作为未指定发送给 Okta”将自动启用。使用 Okta 自定义域（例如 mytenant.domain.com）的 Okta SAML 应用程序无法自动检测，并且 Citrix 管理员必须通过单击复选框手动启用“将 NameID 策略作为未指定发送给 Okta”。

5. 接受默认属性映射。
6. 配置您的 Citrix Cloud 管理员登录 URL。
7. 检查“审核”部分中的 SAML 向导摘要，并验证 SAML 配置在解析 IdP 元数据 URL 后是否符合您的预期。

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



使用元数据文件模式创建 SAML 连接

元数据文件模式与元数据 URL 模式有何不同?

本地 SAML IdP（例如 ADFS 或 PingFederate 服务器）可能存在限制，阻止公共访问其 SAML 元数据 URL 端点，因此无法使用元数据 URL 模式。如果 Citrix Cloud 管理员获得从 SAML IdP 导出的 metadata.xml 文件，他们仍然可以从 Citrix Cloud SAML 连接的自动配置中受益。Citrix Cloud 管理员仍然可以在 SAML 连接创建向导中上传此文件。

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

元数据文件模式为何不如元数据 URL 模式有用?

元数据文件模式是存储在 Citrix Cloud 中的静态配置。使用元数据文件模式创建的 Citrix Cloud SAML 连接在上传到 Citrix Cloud 后，无法检测 SAML 应用程序中的更改。

元数据 URL 模式是按需获取的动态配置。元数据 URL 模式会持续轮询您的 SAML IdP，并可以在 SAML 应用程序配置中进行更改后立即检测到这些更改。

使用 IdP 元数据文件配置 Citrix Cloud SAML 连接

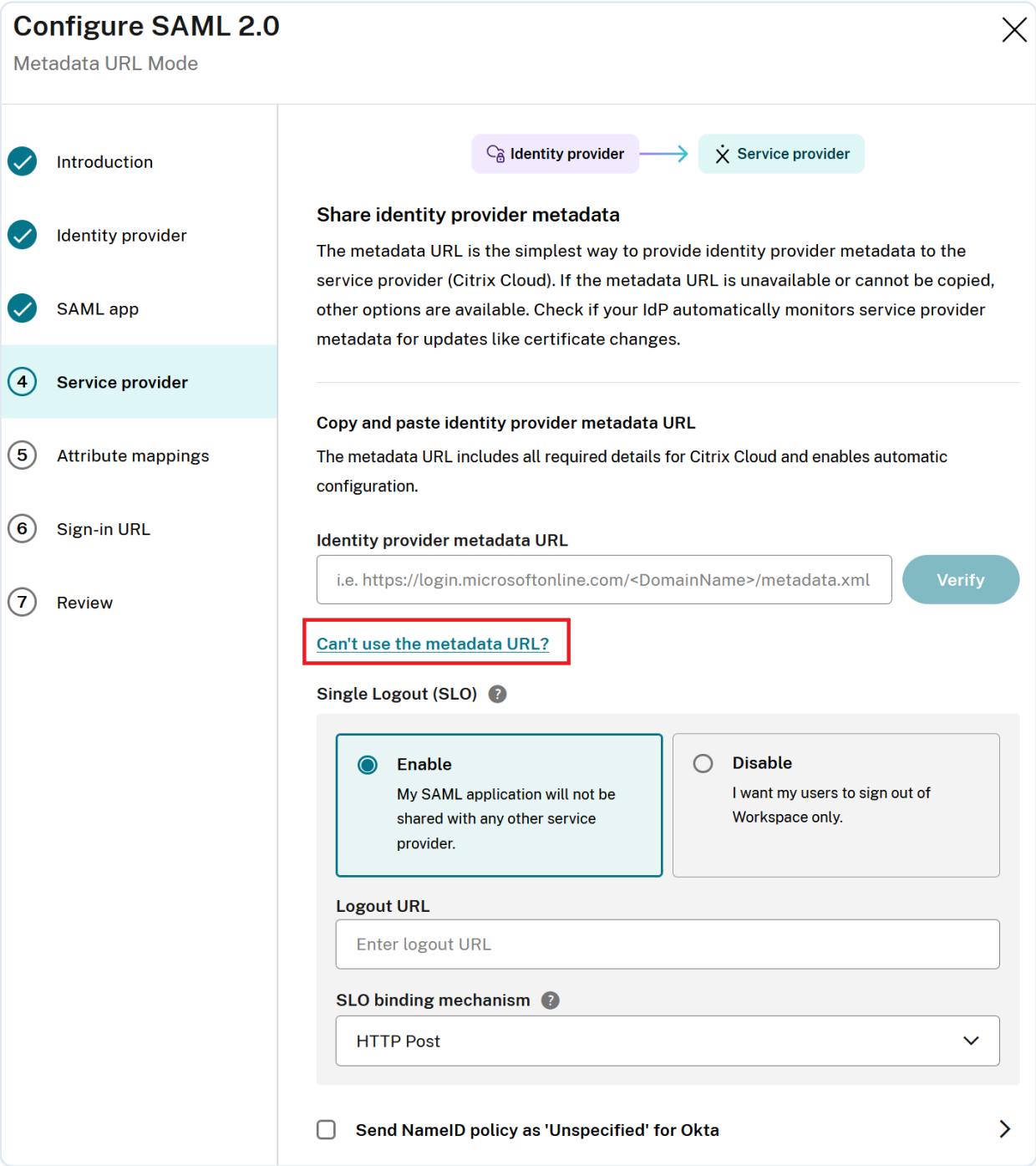
1. 从您希望在 Citrix Cloud 中配置为新 SAML IdP 连接的 SAML 应用程序下载 metadata.xml 文件。
2. 将文件保存到磁盘为 `<filename>.xml`，并且不要对其 XML 格式或内容进行任何更改。建议您使用从 SAML IdP 导出后直接获取的、完全未更改且未格式化的 metadata.xml 文件。

   重要提示：

   metadata.xml 文件通常由 IdP 签名以防止篡改。对 metadata.xml 文件内的数据进行的任何更改，例如使用 XML 美化工具重新格式化，都将使嵌入式签名失效，并导致 metadata.xml 上传和解析失败。

3. 当您到达 SAML 向导的**第 4 节 服务提供商**部分时，选择 *无法使用元数据 URL ?*。

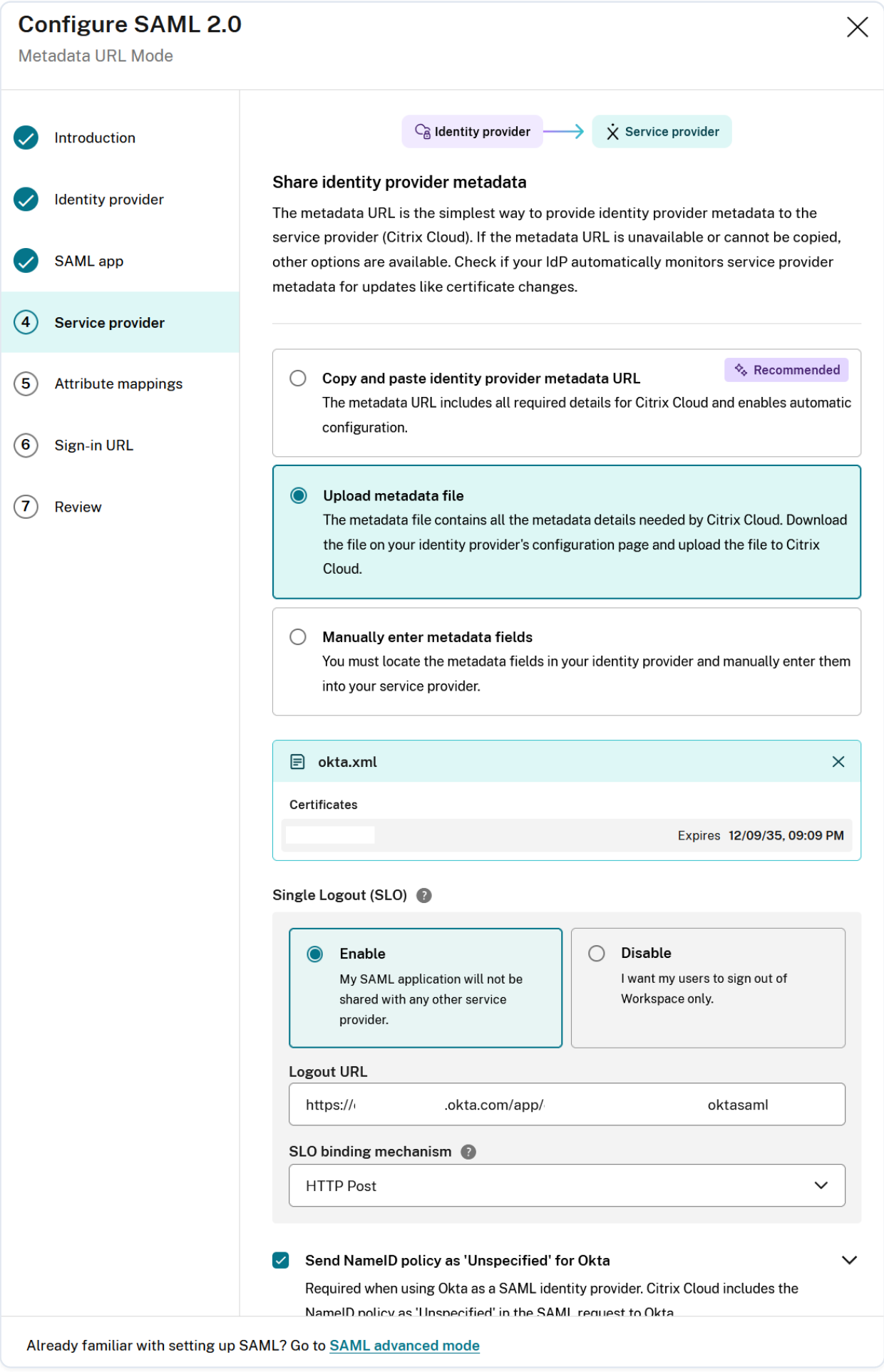
© 1997–2026 Citrix Systems, Inc. All rights reserved.



4. 选择“上传元数据文件”，然后将 metadata.xml 文件拖放到文件上传对话框中，或浏览到磁盘上的 metadata.xml 文件。

   以下是成功导入元数据文件的 **Okta** 示例。

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



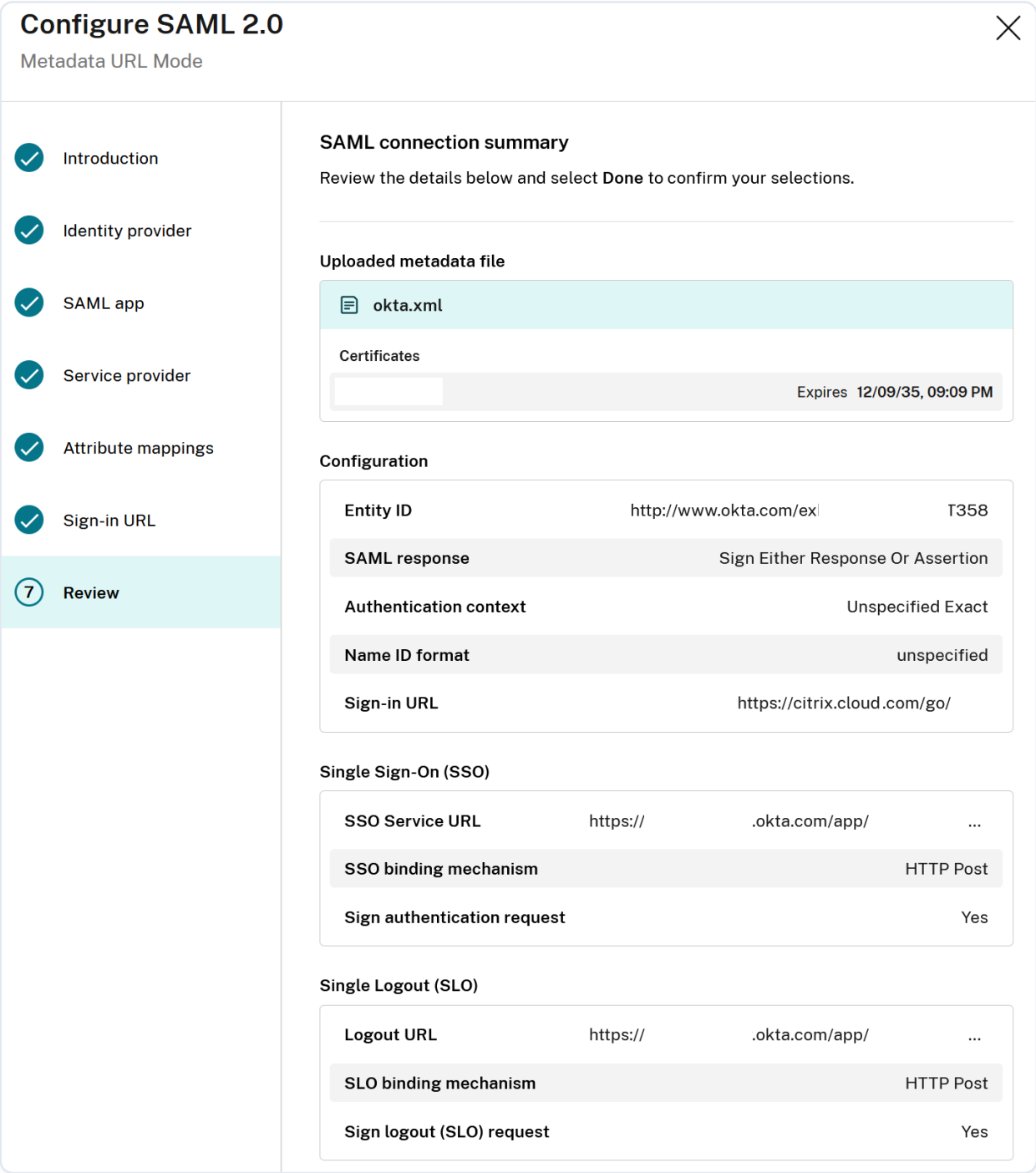
© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. 通过启用或禁用 SLO 来配置所需的 SAML 注销行为。

   有关注销注意事项，请参阅这篇深度文章。

6. 仅限 Okta SAML 连接。如果元数据文件包含 SSO 端点和包含“okta”的 DNS 域字符串，则将自动启用**将 NameID 策略作为 Okta 的未指定策略发送**。使用 Okta 自定义域（例如 mytenant.domain.com）的 Okta SAML 应用程序无法自动检测，并且 Citrix 管理员必须通过单击复选框手动启用**将 NameID 策略作为 Okta 的未指定策略发送**。
7. 接受默认属性映射。
8. 配置您的 Citrix Cloud 管理员登录 URL。
9. 检查“审核”部分中的 SAML 向导摘要，并验证 SAML 配置在解析 IdP 元数据文件后是否符合您的预期。

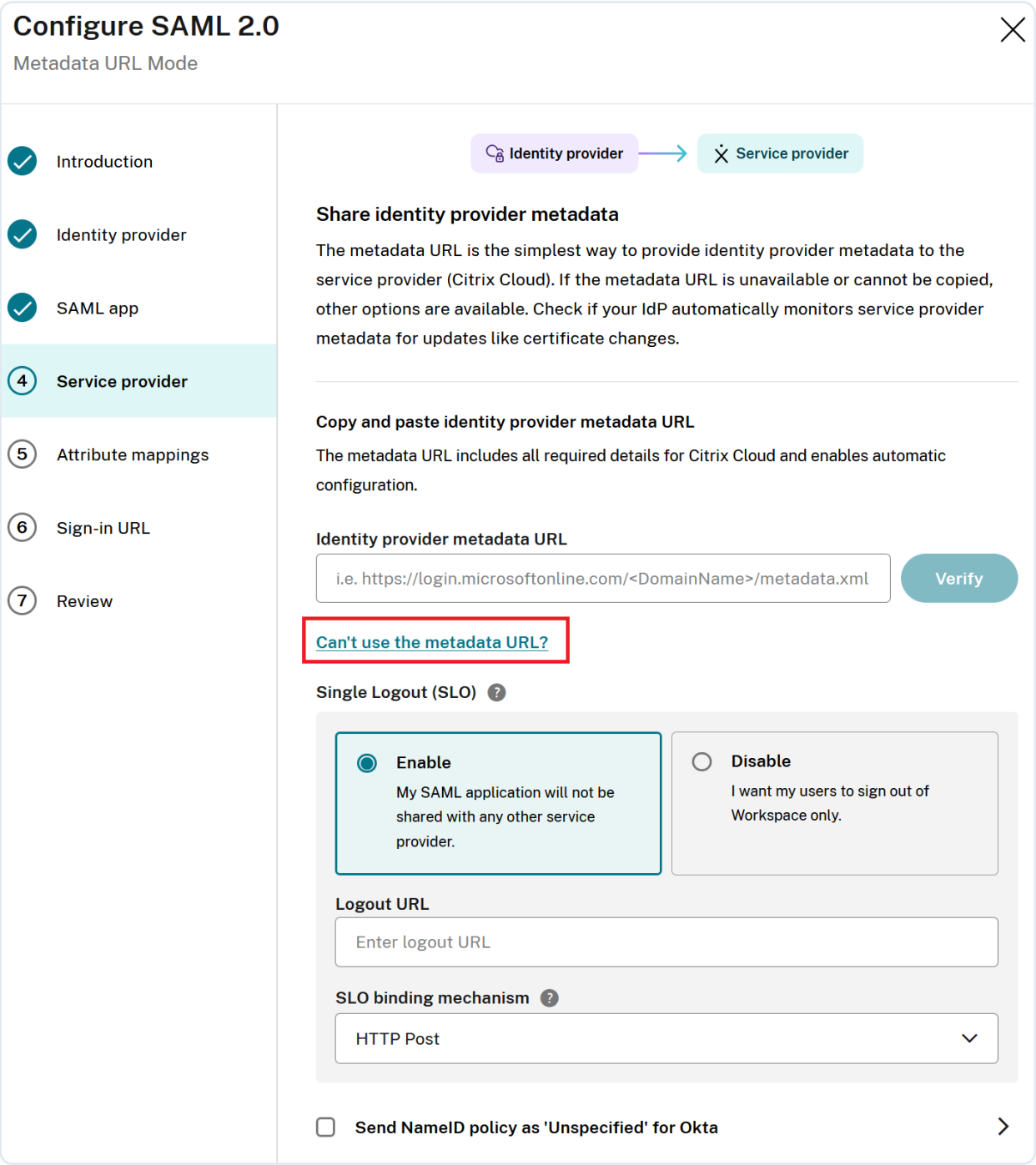
© 1997–2026 Citrix Systems, Inc. All rights reserved.



使用手动模式创建 SAML 连接

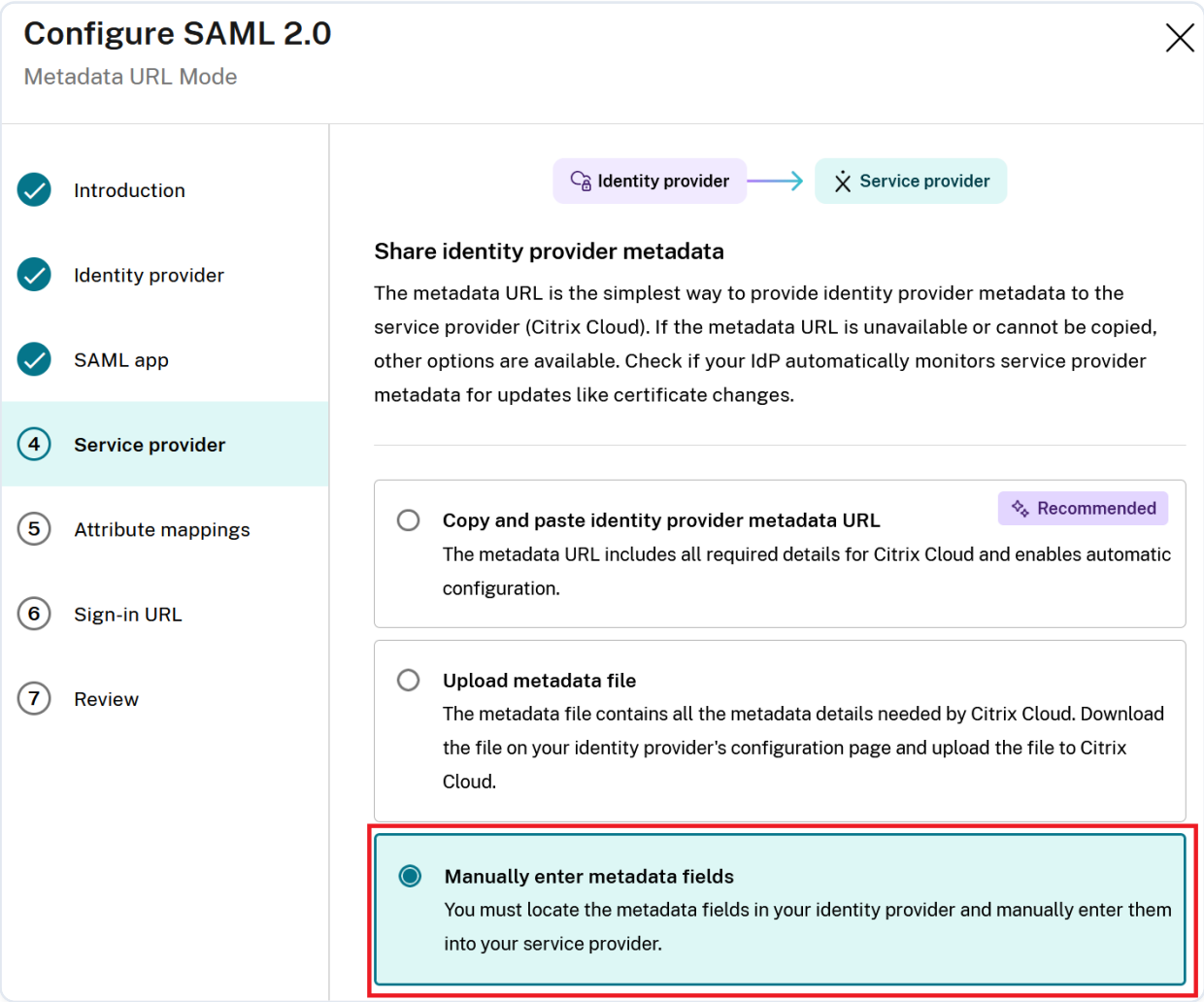
1. 获取您的 SAML 应用程序及其 SAML 端点的详细信息。
2. 从您的 SAML 应用程序下载 SAML 签名证书。
3. 当您到达 SAML 向导的**第 4 节 服务提供商部分**时，选择*无法使用元数据 URL？*

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

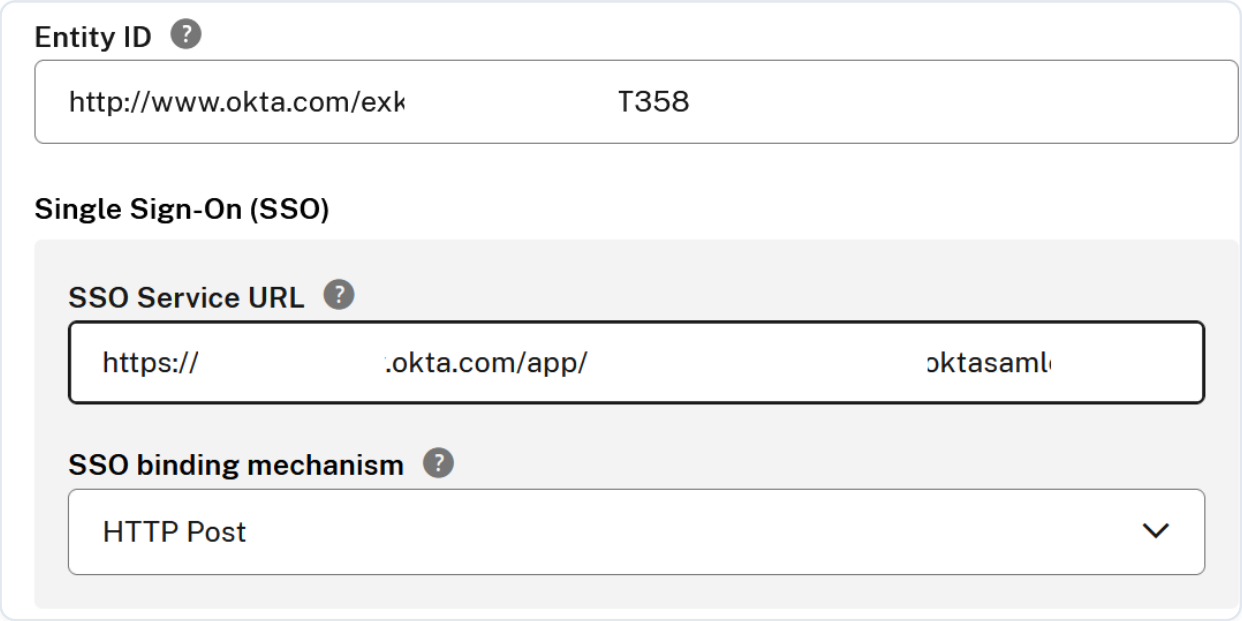


4. 选择**手动输入元数据字段**。

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



5. 输入您的 SAML 应用程序的实体 ID 和 SSO URL。

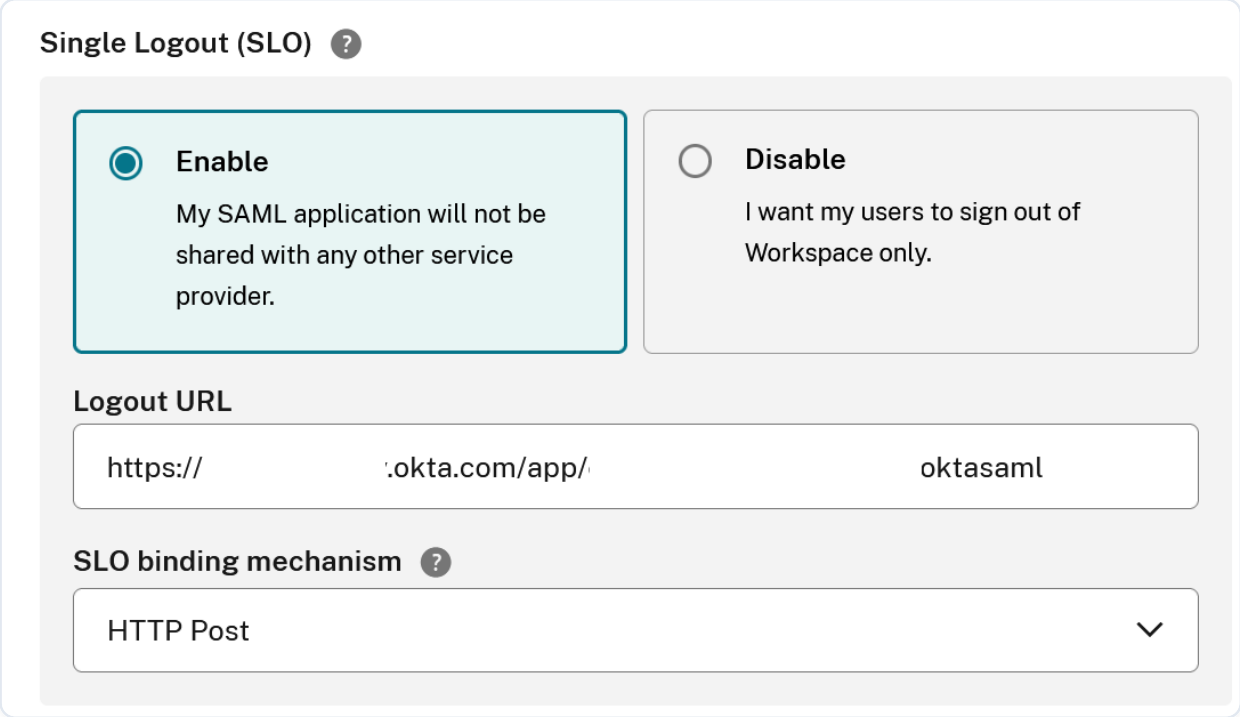


6. 通过将文件拖放到文件上传对话框中，或浏览到磁盘上的 samlapp.cer 文件，上传您的 SAML 应用程序的签名证书。

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

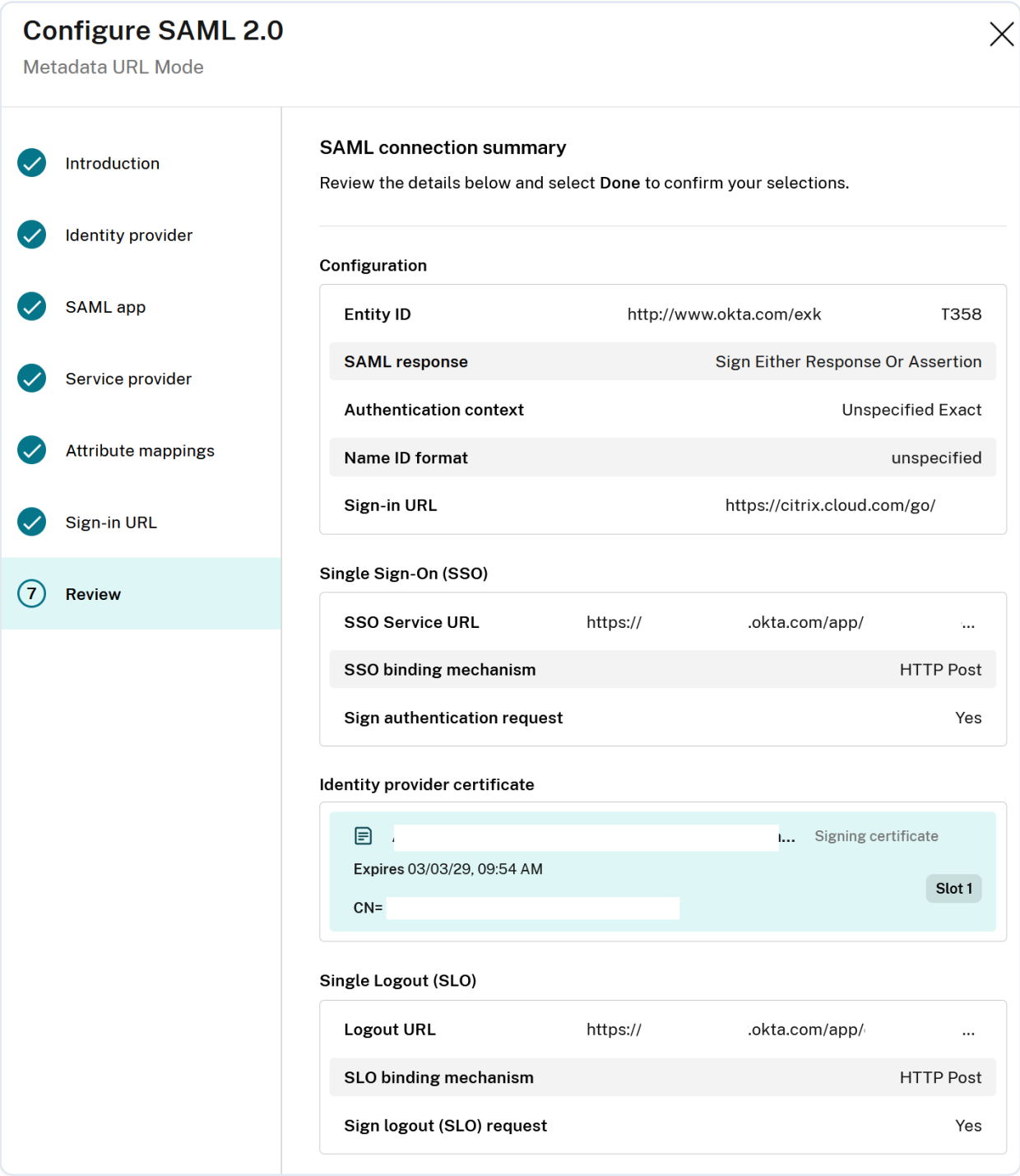
7. 通过启用或禁用 SLO 来配置您想要的 SAML 注销行为。有关详细信息，请参阅这篇深入文章：注销注意事项。

   输入您的 SAML 应用程序的 SLO URL（推荐）。



8. 仅限 Okta SAML 连接。如果输入的 SSO URL 包含带有“okta”的 DNS 域字符串，则**将 NameID 策略作为未指定发送给 Okta**将自动启用。使用 Okta 自定义域（例如 mytenant.domain.com）的 Okta SAML 应用程序无法自动检测，并且 Citrix 管理员必须通过单击复选框手动启用**将 NameID 策略作为未指定发送给 Okta**。
9. 接受默认属性映射。
10. 配置您的 Citrix Cloud 管理员登录 URL。
11. 检查“审核”部分中的 SAML 向导摘要，并验证手动配置连接后 SAML 配置是否符合您的预期。

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



故障排除

当我开启 SAML 支持案例时，需要向 Citrix 支持和工程团队提供哪些信息?

如果您需要 SAML 相关问题的帮助，Citrix 支持和工程团队需要以下信息：

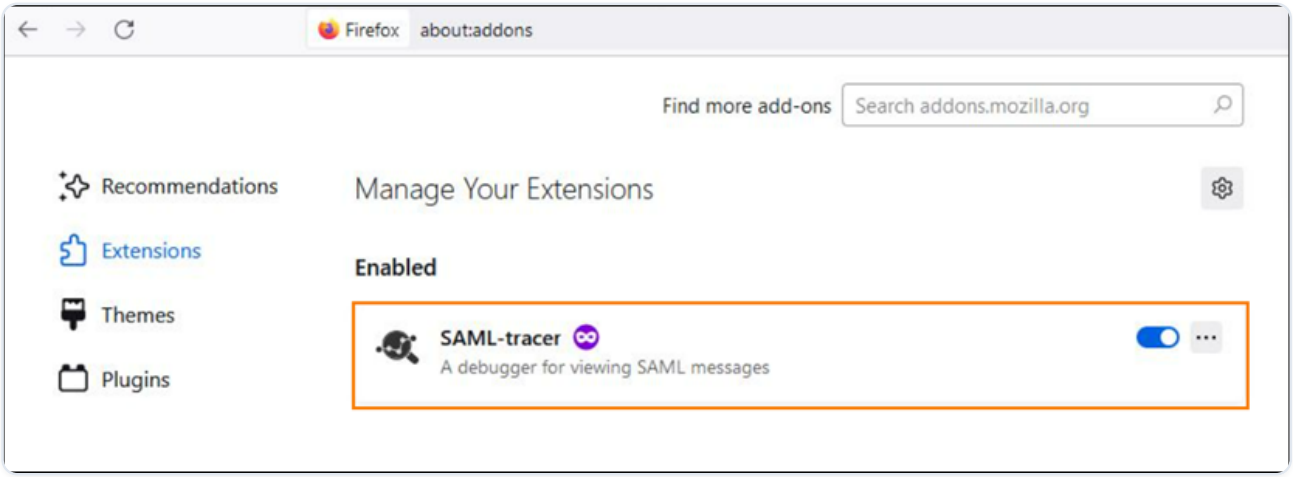
- 提供足够的上下文，并描述您的登录场景以及 Citrix 或 Active Directory 环境。
- 您在初始配置期间遵循了哪些 Citrix eDocs。
- 您的 IdP 中 SAML 应用程序的屏幕截图和详细信息。

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

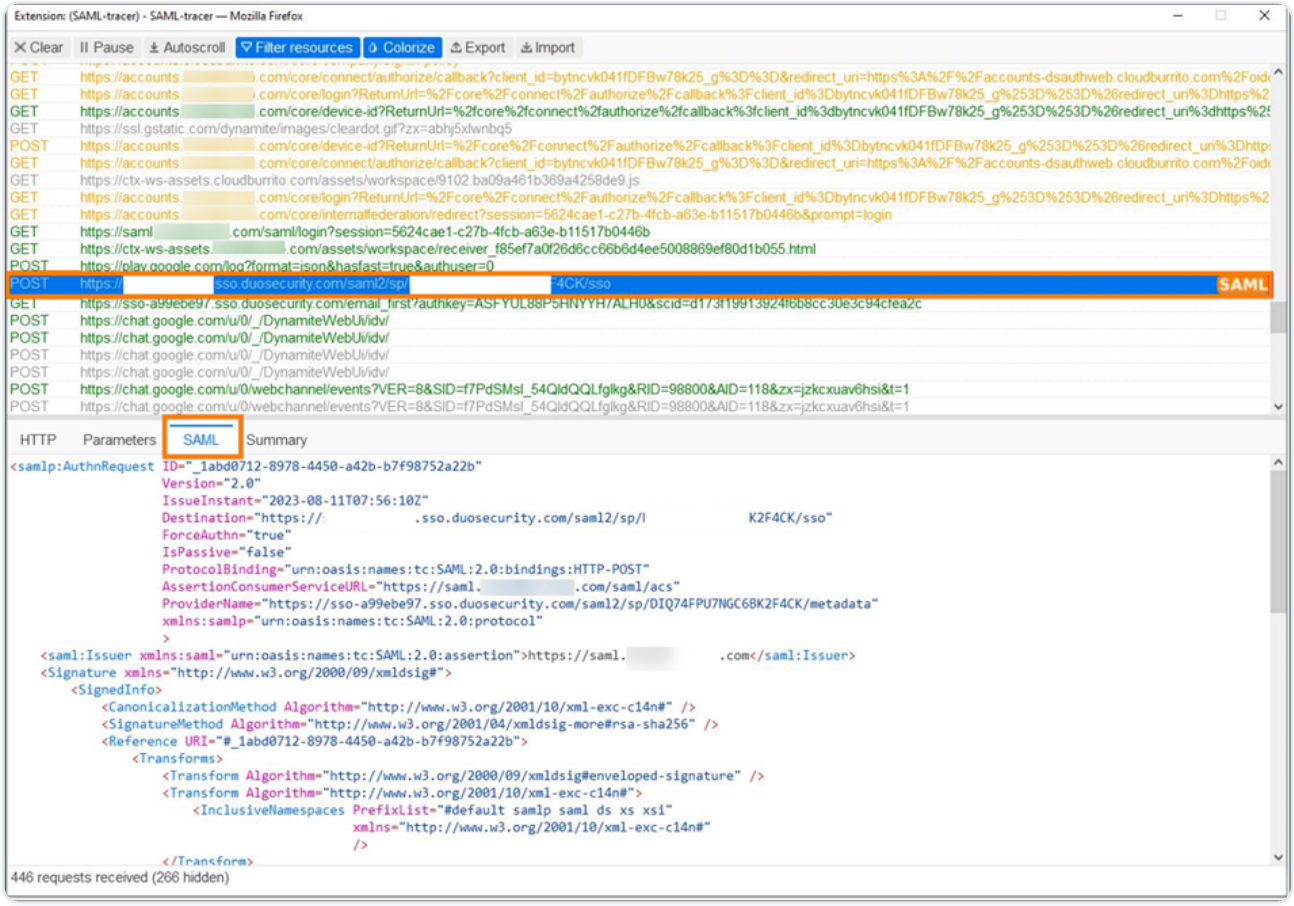
- 您的 Active Directory 详细信息。
- 来自 SAML 跟踪器浏览器扩展的 SAML 跟踪器文件 (`.json`)。
- 来自浏览器开发工具的 HAR 文件 (`.har`)。
- 正常工作和出现故障的最终用户或 Citrix Cloud 管理员用户的详细信息。
- 执行 SAML 登录到 Store 或 Citrix Cloud 的计算机的公共调用方 IP。

为 Citrix 支持和工程团队捕获 SAML 跟踪

Citrix 工程和支持团队建议使用 SAML 跟踪器浏览器扩展进行所有 SAML 调试，以及使用浏览器开发工具生成的 `.HAR` 文件。此扩展适用于大多数常用 Web 浏览器，并可导出 `.JSON` 文件。该扩展将 SAML 请求和响应解码为 XML，使其易于阅读，更易于理解和调试。



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



如何从我的浏览器收集 HAR 文件并发送给 Citrix 支持和工程团队?

有关更多信息，请参阅文章 收集 HAR 文件

有用的第三方 SAML 调试工具

重要提示：

当使用第三方工具进行调试时，Citrix 不承担任何责任。使用和访问第三方工具和网站的风险由您自行承担。

工具	用途
https://www.samltool.io/	解码 base 64 SAML 请求和响应
https://www.sslshopper.com/certificate-decoder.html	解码证书数据
https://www.rcfed.com/SAMLWSFed/MetadataCertificateExtract	从 SAML 元数据中提取签名和加密证书文件

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

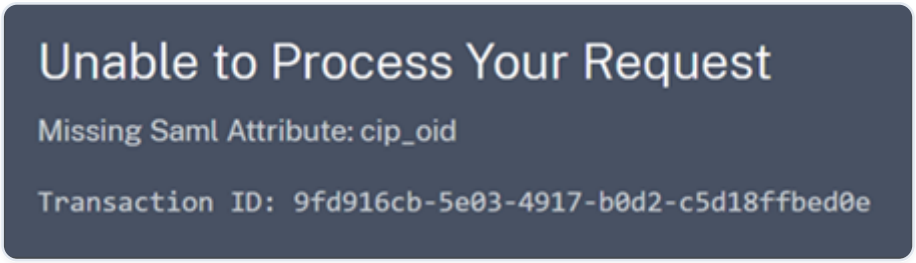
工具	用途
https://www.whatismyip.com/	提供尝试 SAML 登录的客户端的调用方 IP。

属性错误

属性错误可能在以下任何一种情况下发生：

- SAML 配置中所需的属性编码不正确。
- `cip_sid` 和 `cip_upn` 属性在 SAML 断言中缺失。
- `cip_sid` 或 `cip_oid` 属性在 SAML 断言中缺失，并且由于连接问题，Citrix Cloud 无法从 Active Directory 中检索它们。

当发生属性错误时，Citrix Cloud 会显示一条错误消息，其中包含有问题的属性。



要解决此类错误：

1. 确保您的 SAML 提供程序以正确的编码发送所需的属性，如以下表格所示。至少必须包含 SID 或 UPN 属性之一。

属性	编码	必需
cip_email	必须是字符串格式 (`user@domain`)	
cip_oid	必须采用 Base64 或字符串格式	
cip_sid	必须采用 Base64 或字符串格式	是，如果未使用 `cip_upn`
cip_upn	必须采用字符串格式 (`user@domain`)	是，如果未使用 `cip_sid`

2. 验证 Cloud Connector 在线且运行状况良好，以便 Citrix Cloud 可以检索其所需的任何缺失属性。有关详细信息，请参阅Cloud Connector 高级运行状况检查。

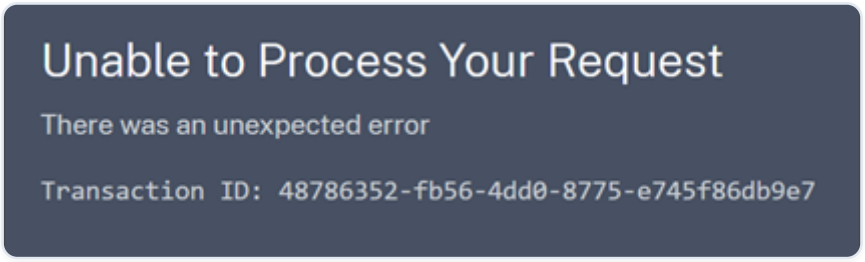
© 1997–2026 Citrix Systems, Inc. All rights reserved.

意外错误

在以下情况下，Citrix Cloud 可能会遇到意外错误：

- 用户使用 IDP 发起的流程启动 SAML 请求。例如，通过身份提供程序的应用程序门户选择磁贴而不是直接导航到应用商店 URL (`customer.cloud.com`) 来发出请求。
- SAML 证书无效或已过期。
- 身份验证上下文无效。
- SAML 断言和响应签名不匹配。

发生此错误时，Citrix Cloud 会显示一条通用错误消息。



如果此错误是由于通过身份提供商的应用程序门户导航到 Citrix Cloud 而导致的，您可以使用以下变通方法：

1. 在身份提供商的应用程序门户中创建一个书签应用程序，该应用程序引用您的应用商店 URL（例如，`https://customer.cloud.com`）。
2. 将用户分配给 SAML 应用程序和书签应用程序。
3. 更改 SAML 应用程序和书签应用程序的可见性设置，以便书签应用程序可见，而 SAML 应用程序在应用程序门户中隐藏。
4. 在 Citrix® StoreFront Cloud 中禁用**始终提示最终用户输入其凭据**设置，以移除额外的密码提示。有关说明，请参阅始终提示最终用户输入其凭据。

在 Citrix Cloud™ 中配置具有范围实体 ID 的 SAML 应用程序

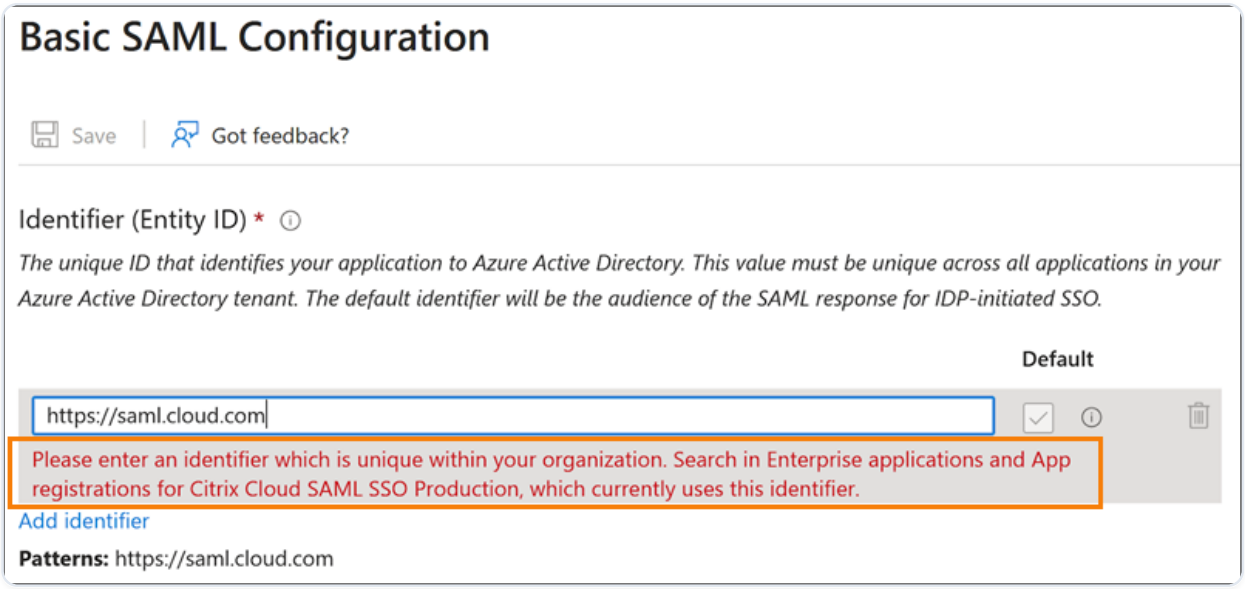
本文介绍如何在同一 SAML 提供程序中预配多个 SAML 应用程序。

某些 SAML 提供程序（例如 Microsoft Entra ID (ME-ID)、Active Directory 联合身份验证服务 (ADFS)、PingFederate 和 PingSSO）禁止在多个 SAML 应用程序中重复使用相同的服务提供程序 (SP) 实体 ID。因此，在同一 SAML 提供程序中创建两个或更多不同 SAML 应用程序的管理员无法将其链接到相同或不同的 Citrix Cloud 租户。尝试创建第二个 SAML 应用程序时，如果使用相同的 SP 实体 ID（例如 `https:\\saml.cloud.com`），而现有 SAML 应用程序已在使用该 ID，则会在 SAML 提供程序处触发错误，指示实体 ID 已在使用中。

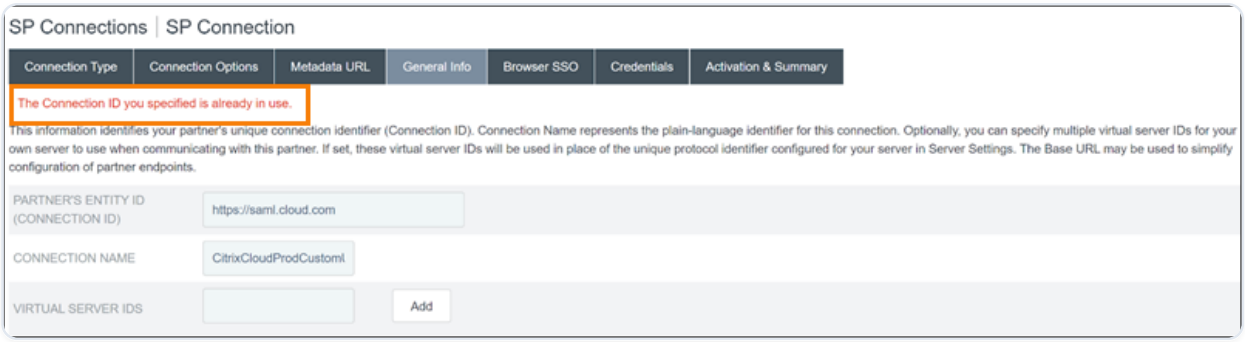
以下图像说明了此错误：

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

- 在 Microsoft Entra ID 内部：



- 在 PingFederate 中：



Citrix Cloud 中的范围实体 ID 功能解决了此限制，因此您可以在 SAML 提供程序（例如 Microsoft Entra ID 租户）中创建多个 SAML 应用程序，并将其链接到单个 Citrix Cloud 租户。

什么是实体 ID?

SAML 实体 ID 是一个唯一标识符，用于在 SAML 身份验证和授权协议中标识特定实体。通常，实体 ID 是分配给实体的 URL 或 URI，并用于 SAML 消息和元数据中。您在 SAML 提供程序中创建的每个 SAML 应用程序都被视为一个唯一实体。

例如，在 Citrix Cloud 和 Microsoft Entra ID 之间的 SAML 连接中，Citrix Cloud 是服务提供程序 (SP)，Microsoft Entra ID 是 SAML 提供程序。两者都有一个实体 ID，必须在 SAML 连接的另一端进行配置。这意味着 Citrix Cloud 的实体 ID 必须在 Microsoft Entra ID 中配置，而 Microsoft Entra ID 的实体 ID 必须在 Citrix Cloud 中配置。

以下实体 ID 是 Citrix Cloud 中通用实体 ID 和范围实体 ID 的示例：

- 通用：`https://saml.cloud.com`

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

- 范围：`https://saml.cloud.com/67338f11-4996-4980-8339-535f76d0c8fb`

按区域划分的通用和范围限定的 SP 实体 ID

Citrix Cloud 中现有的 SAML 连接（在 2023 年 11 月之前创建）对每个 SAML 连接和 Citrix Cloud 租户使用相同的通用实体 ID。只有新的 Citrix Cloud SAML 连接才提供使用范围限定实体 ID 的选项。

如果您选择为新连接使用范围限定实体 ID，则任何现有 SAML 连接将继续使用其原始通用实体 ID 运行。

下表列出了每个 Citrix Cloud 区域的通用和范围限定 SP 实体 ID：

CITRIX CLOUD 区域	通用 SP 实体 ID	范围限定实体 ID
美国、欧盟、亚太南部	`https://saml.cloud.com`	`https://saml.cloud.com/67338f11-4996-4980-8339-535f76d0c8fb`
日本	`https://saml.citrixcloud.jp`	`https://saml.citrixcloud.jp/db642d4c-ad2c-4304-adcf-f96b6aa16c29`
政府	`https://saml.cloud.us`	`https://saml.cloud.us/20f1cf66-cfe9-4dd3-865c-9c59a6710820`

为新的和现有的 SAML 连接生成唯一的 SP 实体 ID

当您创建新的 SAML 连接时，Citrix Cloud 会生成一个唯一 ID (GUID)。要生成范围限定的实体 ID，您需要在创建新连接时启用**配置范围限定的 SAML 实体 ID**设置。

如果您想更新现有 SAML 连接以使用范围限定的实体 ID，您必须在 Citrix Cloud 的**身份和访问管理 > 身份验证**页面中断开连接，然后重新连接您的 SAML 提供程序。Citrix Cloud 不允许您直接编辑现有 SAML 连接。但是，您可以克隆配置并修改克隆。

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

重要提示：

在完成 SAML 连接过程之前关闭它会丢弃 Citrix Cloud 自动生成的实体 ID。当您重新启动 SAML 连接过程时，Citrix Cloud 会生成一个新的范围限定的实体 ID GUID。在配置 SAML 提供程序时，请使用此新的范围限定的实体 ID。如果您正在更新现有 SAML 连接以使用范围限定的实体 ID，则必须使用 Citrix Cloud 生成的范围限定的实体 ID 更新该连接的 SAML 应用程序。

关于范围限定实体 ID 的常见问题

我可以在同一个 Microsoft Entra ID 租户中创建多个 Microsoft Entra ID SAML 应用程序并将其链接到一个或多个 Citrix Cloud 租户吗?

Citrix Cloud 的范围限定实体 ID 功能解决了某些 SAML 提供程序施加的防止重复实体 ID 的限制。借助此功能，您可以在 Microsoft Entra ID 租户中预配多个 SAML 应用程序，并为每个应用程序配置来自单个 Citrix Cloud 租户的范围限定实体 ID。

我仍然可以将同一个 Microsoft Entra ID SAML 应用程序链接到多个 Citrix Cloud 租户?

这种情况在 Citrix Cloud 客户中很常见，Citrix 将继续支持它。要实现此场景，您必须满足以下要求：

- 使用通用实体 ID，例如 `https://saml.cloud.com`。
- 不要为您的 SAML 连接启用范围限定的实体 ID。

我如何决定是否在我的 SAML 提供程序中使用范围限定的实体 ID?

Citrix Cloud 中的范围限定实体 ID 提供了使用通用或范围限定实体 ID 的灵活性，具体取决于您的要求。请考虑您需要的 SAML 应用程序数量以及您拥有的 Citrix Cloud 租户数量。此外，还要考虑每个租户是否可能共享现有 SAML 应用程序或需要其自己的范围限定 SAML 应用程序。

重要：

如果您的 SAML 提供商已允许您创建具有相同实体 ID 的多个 SAML 应用程序（例如 `https://saml.cloud.com`），则无需启用范围实体 ID 或对现有 SAML 配置进行任何更改。您也无需更新 Citrix Cloud 或 SAML 应用程序中的任何设置。

受影响的 SAML 提供商

下表列出了允许或限制使用重复实体 ID 的 SAML 提供商。

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

SAML 提供商	支持重复实体 ID
微软 恩特拉 身份 (云)	否
ADFS（本地）	否
PingFederate（本地）	否
PingOneSSO（云）	否
Okta（云）	是
Duo（云）	是
OneLogin（云）	是

受影响的用例

下表指明了是支持通用实体 ID 还是范围实体 ID，具体取决于您的用例所需的 SAML 应用程序以及您的 SAML 提供程序是否支持重复的实体 ID。

用例要求	SAML 提供程序是否支持重复的实体 ID？	支持的配置
只有一个 SAML 应用程序	是	通用或范围实体 ID
只有一个 SAML 应用程序	否	通用或范围限定的实体 ID
两个或更多 SAML 应用程序	是	通用或范围限定的实体 ID
两个或更多 SAML 应用程序	否	范围限定的实体 ID
存储自定义 URL 和 SAML 应用程序对	是	通用或范围限定的实体 ID
存储自定义 URL 和 SAML 应用程序对	否	范围限定的实体 ID
将相同的 SAML 应用程序链接到多个 Citrix Cloud 租户	是	通用实体 ID
将同一个 SAML 应用程序链接到多个 Citrix Cloud 租户	否	通用实体 ID

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

使用范围限定的实体 ID 配置主 SAML 连接

在此任务中，您将使用主 SAML 应用程序 (SAML App 1) 的范围限定实体 ID 在 Citrix Cloud 中创建 SAML 连接。

1. 从 Citrix Cloud 菜单中，选择 **身份和访问管理**。
2. 在“**身份验证**”选项卡上，找到 **SAML 2.0**，然后从省略号菜单中选择“**连接**”。
3. 当系统提示您创建唯一的登录 URL 时，请输入一个简短的、对 URL 友好的公司标识符（例如，`https://citrix.cloud.com/go/mycompany`），然后选择“**保存并继续**”。此标识符在整个 Citrix Cloud 中必须是唯一的。
4. 在“**配置 SAML 身份提供程序**”下，选择“**配置范围限定的 SAML 实体 ID**”。Citrix Cloud 会自动生成范围限定的实体 ID，并填充实体 ID、断言使用者服务和注销 URL 字段。
5. 在“**配置到 Citrix Cloud 的 SAML 连接**”下，输入 SAML 提供程序的连接详细信息。
6. 接受默认的 SAML 属性映射。
7. 选择“**测试并完成**”。

使用通用实体 ID 配置主 SAML 连接

在此任务中，您将使用主 SAML 应用程序 (SAML App 1) 的默认通用实体 ID 在 Citrix Cloud 中创建 SAML 连接。

1. 从 Citrix Cloud 菜单中，选择 **身份和访问管理**。
2. 在 **身份验证** 选项卡上，找到 **SAML 2.0** 并从省略号菜单中选择 **连接**。
3. 当提示您创建唯一的登录 URL 时，为您的公司输入一个简短的、URL 友好的标识符（例如，`https://citrix.cloud.com/go/mycompany`），然后选择 **保存并继续**。此标识符在整个 Citrix Cloud 中必须是唯一的。
4. 在 **配置 SAML 身份提供程序** 下，验证 **配置范围限定的 SAML 实体 ID** 是否已禁用。
5. 在 **配置到 Citrix Cloud 的 SAML 连接** 下，输入您的 SAML 提供程序提供的连接详细信息。
6. 在 **服务提供商 SAML 元数据** 中，如果需要，单击 **下载** 以获取通用 SAML 元数据的副本。
7. 接受默认的 SAML 属性映射。
8. 选择 **测试并完成**。

使用 Citrix® StoreFront Cloud 自定义域配置 SAML 连接

本节介绍如何使用自定义应用商店 URL 配置 SAML 连接，该 URL 具有范围限定的或通用的实体 ID。

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

本节中的任务仅适用于您拥有正在与 SAML 结合使用的现有自定义应用商店 URL 的情况。如果您没有将自定义应用商店 URL 与 SAML 身份验证结合使用，则可以跳过本节中的任务。

有关详细信息，请参阅以下文章：

- 配置自定义域
- 使用自定义域通过 SAML 登录应用商店

使用应用商店自定义 URL 和通用实体 ID 配置 SAML 连接

在此任务中，**配置范围实体 ID** 设置已禁用。

1. 从 Citrix Cloud 菜单中，选择 **Store Authentication**。
2. 在 **Custom store URL** 中，从省略号菜单中选择 **Edit**。
3. 选择 **同时使用 .cloud.com URL 和自定义域 URL**。
4. 输入 SAML App 2 的通用实体 ID、SSO URL 和可选的 SLO URL，然后上传您之前从 SAML 提供商下载的签名证书。
5. 如果需要，在 **Service Provider SAML Metadata for custom domain** 中，单击 **Download** 以获取商店自定义 URL SAML 应用程序的通用 SAML 元数据副本。
6. 单击 **Save**。

配置具有商店自定义 URL 和范围实体 ID 的 SAML 连接

在此任务中，**配置范围实体 ID** 设置已启用。

1. 从 Citrix Cloud 菜单中，选择 **Store Authentication**。
2. 在 **Custom store URL** 中，从省略号菜单中选择 **Edit**。
3. 选择 **同时使用 .cloud.com URL 和自定义域 URL**。
4. 输入 SAML App 2 的范围实体 ID、SSO URL 和可选的 SLO URL，然后上传您之前从 SAML 提供商下载的 SAML 签名证书。
5. 单击 **Save**。

保存配置后，Citrix Cloud 会生成包含正确 GUID 的范围 SAML 元数据。如果需要，您可以获取商店自定义 URL SAML 应用程序的范围元数据副本。

1. 在“**身份和访问管理**”页面上，找到 SAML 连接，然后从省略号菜单中选择“**查看**”。
2. 在“**自定义域的服务提供商 SAML 元数据**”中，单击“**下载**”。

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

查看主 SAML 应用程序和自定义应用商店 URL SAML 应用程序的 SAML 配置

查看范围限定的 SAML 连接的配置详细信息时，Citrix Cloud 会显示主 SAML 应用程序和应用商店自定义域 SAML 应用程序的范围限定的实体 ID 设置。

例如，当启用范围限定的实体 ID 时，“**服务提供商实体 ID**”和“**自定义域的服务提供商实体 ID**”字段包含 Citrix Cloud 生成的范围限定的实体 ID。

启用了范围限定的实体 ID 的 SAML 配置(/en-us/citrix-cloud/media/saml-entity-id-scoped-custom-domain-example.png)

当禁用范围限定的实体 ID 时，“**服务提供商实体 ID**”和“**自定义域的服务提供商实体 ID**”字段包含通用实体 ID。

具有通用实体 ID 的 SAML 配置(/en-us/citrix-cloud/media/saml-entity-id-generic-custom-domain-example.png)

您可以通过将范围限定的实体 ID 附加到现有实体 ID 值来更新 SAML 提供商中的现有 SAML 应用程序。

具有范围限定的实体 ID 的 SAML 提供商配置

在 Citrix Cloud 中使用范围限定的实体 ID 配置 SAML 连接后，您可以将范围限定的实体 ID 添加到您的 SAML 提供商。

本节包含 Microsoft Entra ID 和 PingFederate 的配置示例。

具有范围限定的实体 ID 的 Microsoft Entra ID SAML 配置

在此示例中，Citrix Cloud 中的范围限定的实体 ID 输入到 Microsoft Entra ID 的“**标识符**”字段中。

Microsoft Entra ID 中突出显示实体 ID 的 SAML 应用程序配置(/en-us/citrix-cloud/media/saml-entity-id-aad-example-config.png)

PingFederate SAML 配置，带范围限定的实体 ID

在此示例中，来自 Citrix Cloud 的范围限定实体 ID 和通用实体 ID 分别填充在“**合作伙伴实体 ID**”字段和“**基本 URL**”字段中。

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

Summary	
SP Connection	
Connection Type	
Connection Role	SP
Browser SSO Profiles	true
Protocol	SAML 2.0
Connection Template	No Template
WS-Trust STS	false
Outbound Provisioning	false
Connection Options	
Browser SSO	true
IdP Discovery	false
Attribute Query	false
General Info	
Partner's Entity ID (Connection ID)	https://saml.cloud.com/dea0781e-be43-4056-994f-f356ec486981
Connection Name	CitrixCloudProdScopedEntityID
Base URL	https://saml.cloud.com

故障排除

Citrix 建议使用 SAML-tracer 浏览器扩展来排查 SAML 配置中的任何问题。此扩展将 Base64 编码的请求和响应解码为 SAML XML，使信息易于阅读。您可以使用 SAML-tracer 扩展来检查 Citrix Cloud（服务提供商）生成并发送到您的 SAML 提供商（身份提供商）的 SSO 和 SLO SAML 请求。该扩展可以显示实体 ID 范围 (GUID) 是否包含在这两个请求中。

1. 在 Web 浏览器的“扩展”面板中，安装并启用 SAML-tracer 扩展。
2. 执行 SAML 登录和注销操作，并使用 SAML-tracer 扩展捕获整个流程。
3. 在 SAML SSO 请求或 SLO 请求中找到以下行。

```
<saml:Issuer
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">https://
saml.cloud.com/cfee4a86-97a8-49cf-9bb6-fd15ab075b92</saml:Issuer>
```

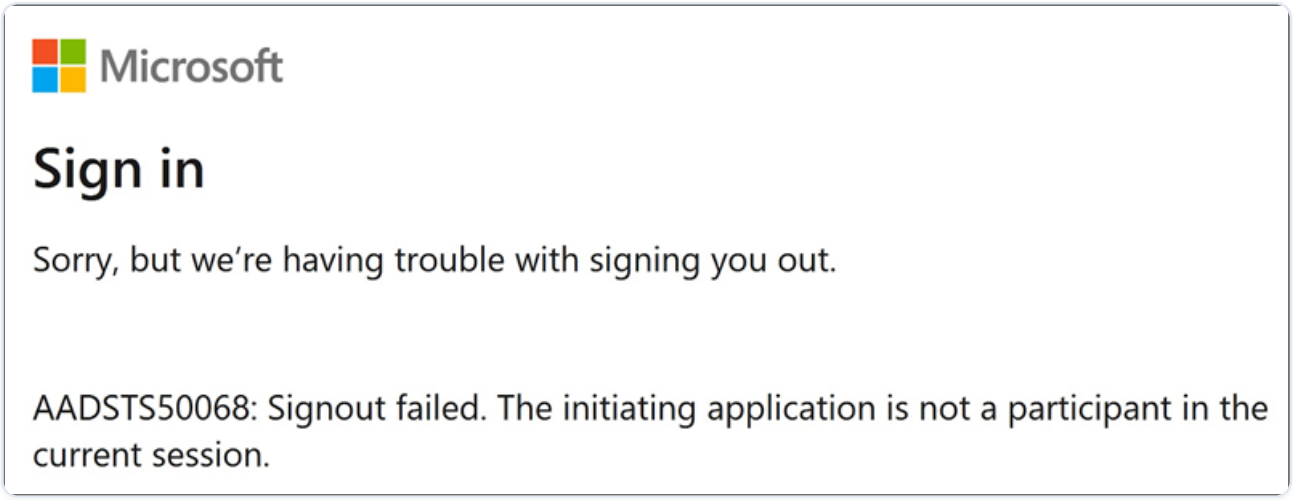
4. 验证实体 ID 是否与 SAML 提供商应用程序中配置的实体 ID 匹配。
5. 验证范围限定的实体 ID 是否存在于“**颁发者**”字段中，并验证其在 SAML 提供商中是否配置正确。

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

6. 导出并保存 SAML-tracer JSON 输出。如果您正在与 Citrix 支持部门合作解决问题，请将输出上传到您的 Citrix 支持案例。

Microsoft Entra ID 故障排除

问题： 配置 SLO 后，从 Microsoft Entra ID 注销失败。Microsoft Entra ID 向用户显示以下错误：



如果 Citrix Cloud 中 SAML 连接启用了范围限定实体 ID，则必须在 SSO 和 SLO 请求中发送范围限定实体 ID。

原因： 范围实体已配置，但 SLO 请求中缺少实体 ID。请验证 SAML-tracer 输出中 SLO 请求中是否存在范围实体 ID。

本地 PingFederate 故障排除

问题： 启用范围实体 ID 设置后，登录或注销 PingFederate 失败。

原因： PingFederate 管理员将范围实体 ID 添加到了 SP 连接基本 URL。

要解决此问题，请仅将范围实体 ID 添加到 **Partner's EntityID** 字段。将范围实体 ID 添加到基本 URL 会导致 SAML 端点格式错误。如果 Citrix Cloud 基本 URL 更新不正确，则所有其他从基本 URL 派生的 SAML 端点相对 URL 都会导致登录失败。

以下端点是可能出现在 SAML-tracer 输出中的格式错误的 Citrix Cloud SAML 端点示例：

- `https://saml.cloud.com/<GUID>/saml/acs`
- `https://saml.cloud.com/<GUID>/saml/logout/callback`

下图显示了一个配置错误的 PingFederate SAML 应用程序。正确配置的字段显示为绿色。配置错误的字段显示为红色。

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

Summary	
SP Connection	
Connection Type	
Connection Role	SP
Browser SSO Profiles	true
Protocol	SAML 2.0
Connection Template	No Template
WS-Trust STS	false
Outbound Provisioning	false
Connection Options	
Browser SSO	true
IdP Discovery	false
Attribute Query	false
General Info	
Partner's Entity ID (Connection ID)	https://saml.cloud.com/dea0781e-be43-4056-994f-f356ec486981
Connection Name	CitrixCloudProdScopedEntityID
Base URL	https://saml.cloud.com/dea0781e-be43-4056-994f-f356ec486981

使用多个自定义 URL 通过 SAML 登录到应用商店

支持使用应用商店自定义 URL 的 SAML 架构已简化和更新，现在只需在 SAML IdP 中配置**一个 SAML 应用程序**即可支持多个自定义域。Citrix Cloud 的身份验证平台和应用商店自定义 URL 服务已进行更改，以支持多达 10 个带有 SAML 和条件身份验证的自定义 URL。过去，需要配置一个带有 `cloud.com` SAML 端点的 SAML 应用程序，以及另一个带有包含自定义 URL 的 SAML 端点的 SAML 应用程序。现在不再需要创建和维护多个不同的 SAML 应用程序来支持所有 SAML 用例。

支持多个自定义 URL 的新架构的优势。

只需创建 1 个 SAML 应用程序，其中包含与您的 Citrix Cloud 区域匹配的 Citrix Cloud SAML 端点，例如 `saml.cloud.com`（美国、欧盟和亚太地区）、`saml.citrixcloud.jp`（日本）或 `saml.cloud.us`（政府）。

SAML 应用程序端点示例：

- 实体 ID `https://saml.cloud.com` 或 `https://saml.cloud.com/<guid>`
- 断言消费者服务 (SSO)：`https://saml.cloud.com/saml/acs`
- 注销 (SLO)：`https://saml.cloud.com/saml/logout/callback`

支持的 SAML 登录用例：

- 使用单个 SAML 应用程序通过您的任一应用商店 URL 登录到应用商店 `store.cloud.com` 或 `store.mycustomer.com`
- 使用 SAML 登录 Citrix Cloud 进行管理员访问也使用相同的通用 SAML 应用程序。

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

- 您的 IdP 中的单个 SAML 应用程序现在可以支持多达 10 个应用商店自定义 URL，而无需创建和维护多个不同的 SAML 应用程序。Citrix Cloud 不再需要带有自定义 URL SAML 端点的额外 SAML 应用程序来支持所有 SAML 用例。

常见问题

应用商店中的多自定义 URL 功能是什么?

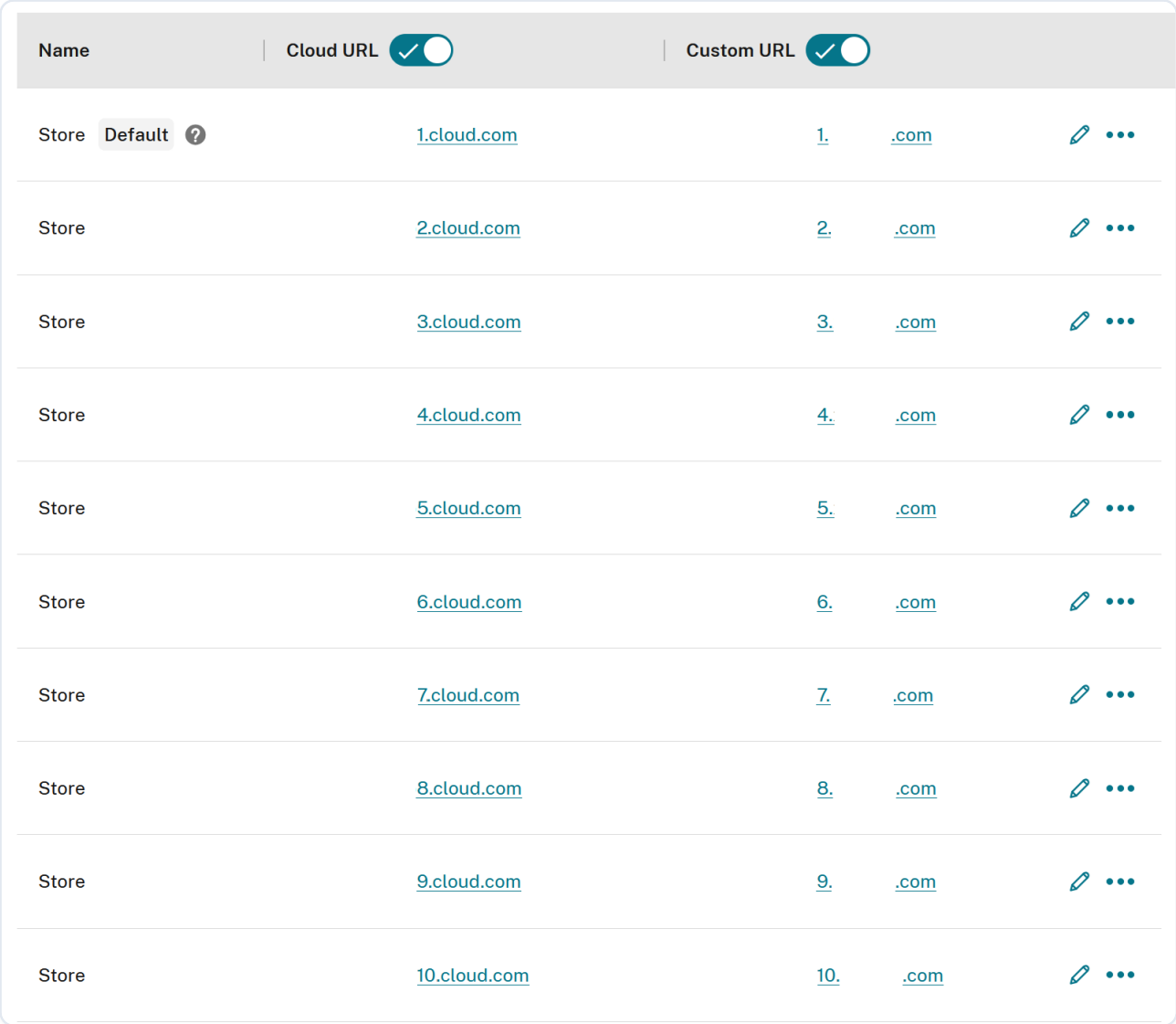
过去，Citrix Cloud 仅支持与第一个应用商店 `cloud.com` URL 关联的单个自定义 URL。现在，可以为您的每个应用商店 `cloud.com` URL 配置一个自定义 URL，最多可达 10 个。这些 URL 形成对，其中每个自定义 URL 是其相应 `cloud.com` URL 的 DNS 中的 CNAME。

在多自定义 URL 发布之前，**StoreFront Cloud > 访问**中仅支持与主要 `cloud.com` 商店 URL 关联的 1 个自定义 URL。

Store	https://	1.cloud.com	Default	.com	Enabled	•••
Store	https://	2.cloud.com			Enabled	•••
Store	https://	3.cloud.com			Enabled	•••
Store	https://	4.cloud.com			Enabled	•••
Store	https://	5.cloud .com			Enabled	•••
Store	https://	6.cloud.com			Enabled	•••
Store	https://	7.cloud.com			Enabled	•••
Store	https://	8.cloud.com			Enabled	•••
Store	https://	9.cloud.com			Enabled	•••
Store	https://	10.cloud.com			Enabled	•••

在多自定义 URL 发布后，**StoreFront Cloud > 访问**。现在支持 1 – 10 个自定义 URL。

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



我如何决定是否需要迁移我的自定义 URL?

这取决于您希望在 Citrix Cloud 和商店中使用的身份验证功能组合、您当前的登录场景以及您当前的 SAML 解决方案。请参阅下表以获取指导。

SAML 登录场景	未迁移的自定义 URL	已迁移的自定义 URL
使用 1 个带有**自定义 URL 端点**的 SAML 应用程序登录到商店	支持（1 个自定义 URL）	不支持（1–10 个自定义 URL）
使用 2 个 SAML 应用程序登录到商店	支持（1 个自定义 URL）	支持（1–10 个自定义 URL）
Citrix Cloud 管理员使用 SAML 1x 应用程序登录，并带有 `cloud.com` **URL 端点**	支持	支持

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

SAML 登录场景	未迁移的自定义 URL	已迁移的自定义 URL
Citrix Cloud 管理员使用 2x SAML 应用程序登录	支持	支持
Citrix Cloud 管理员使用 SAML 1x 应用程序登录，并带有 **自定义 URL 端点**	不支持	不支持
使用应用商店 URL 和 SAML 的条件身份验证策略	支持	支持
最终用户在浏览器或 Citrix Workspace 应用程序中输入 `cloud.com` **URL**		
使用商店 URL 和 SAML 的条件身份验证策略	不支持（1 个自定义 URL）	支持（1–10 个 URL）
最终用户在浏览器或 Citrix Workspace 应用程序中输入**自定义 URL**		

为什么 SAML 和自定义 URL 架构需要更改以支持多个自定义 URL?

可扩展性。在 Citrix Cloud 中引入多个自定义 URL 意味着，每个自定义 URL 需要一个 SAML 应用程序的传统架构无法扩展，并且对于 Citrix Cloud 和 IdP 管理员来说都不切实际。

传统 SAML 自定义 URL 要求：

- 1 个 `cloud.com` SAML 应用程序，用于使用 SAML 进行 Citrix Cloud 管理员登录。
- 每个自定义 URL 1 个 SAML 应用程序。

IdP 配置复杂性。每个 SAML 应用程序除了其 SAML 端点外，都需要进行相同的配置，这导致您的 SAML IdP 中增加了额外的工作。这增加了部署和配置的复杂性。新的多自定义域架构消除了这种需求，您的 IdP 中只需要一个 SAML 应用程序即可支持 1 – 10 个自定义 URL。

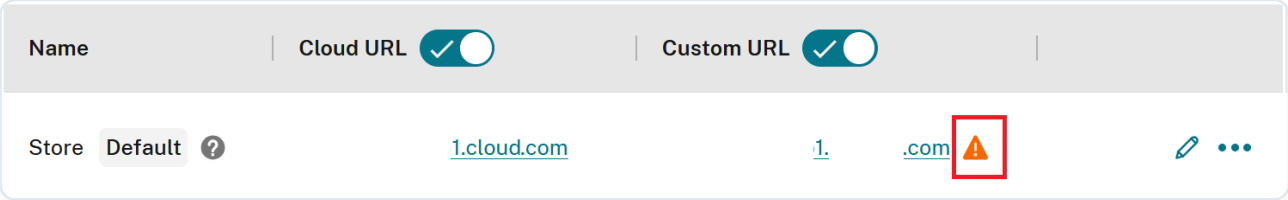
持续的 IdP 维护任务。配置和维护多个 SAML 应用程序，并需要在多个 SAML 应用程序上执行持续的年度证书轮换任务，这对于 Citrix Cloud 和 IdP 管理员来说都是劳动密集型且不理想的。随着添加更多自定义域和需要更多 SAML 应用程序，此问题对管理员而言只会增加。新架构消除了此维护问题，因为所有 SAML 和自定义 URL 用例只需要一个 SAML 应用程序。

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

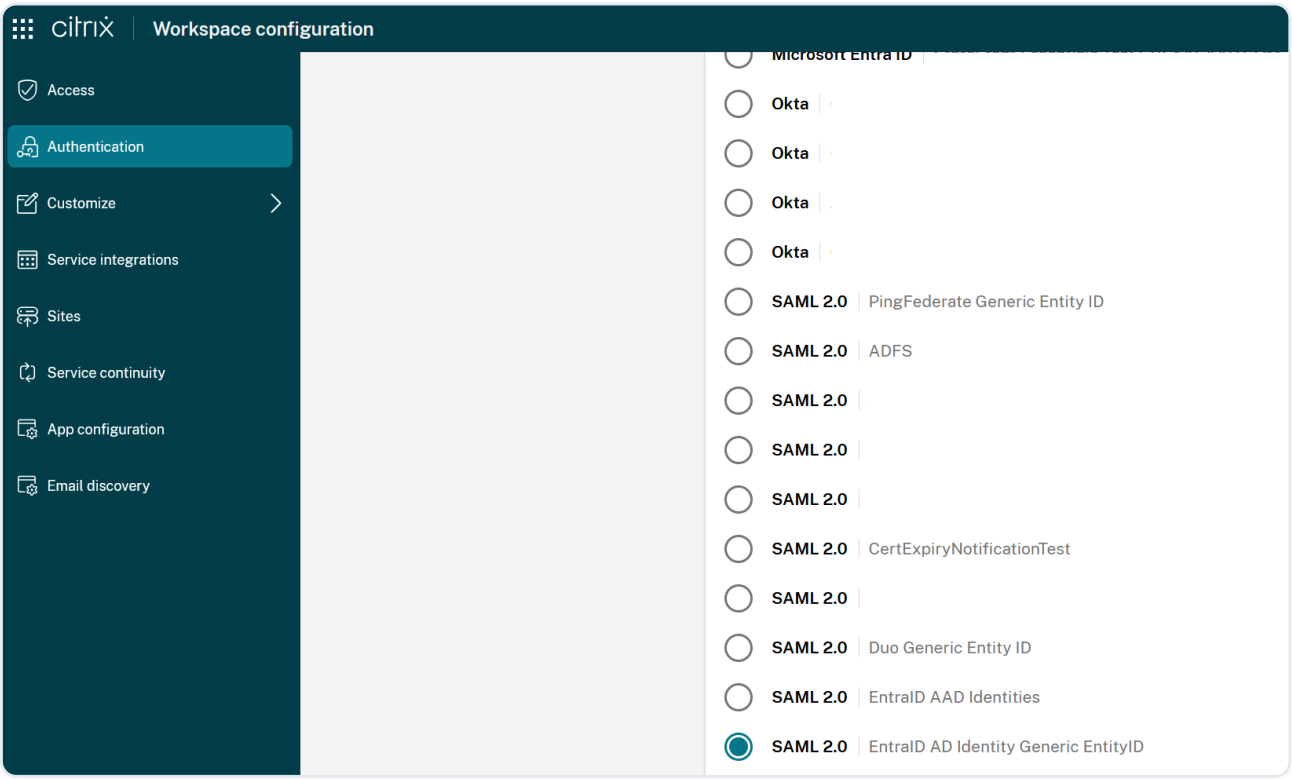
为什么 Citrix 要求我从当前的自定义 URL SAML 解决方案迁移到新的更简单的解决方案?

同时使用多自定义 URL 功能和带自定义 URL 的条件身份验证功能，需要更新和迁移旧版 1x 和 2x SAML 应用程序配置。本文档包含有关如何为使用旧版 1x 或 2x SAML 应用程序解决方案的客户执行迁移的说明。

此警告位于 **StoreFront Cloud > Access** 中，表示您有一个或多个自定义 URL 需要迁移。



仅当您在 **StoreFront Cloud > Authentication** 中启用了 SAML 或条件身份验证时，才会出现此警告。



SAML IdP 配置是否相同，以支持我所有最多 10 个新的自定义 URL?

是的。如果您打算使用一个或多个自定义 URL 来访问商店，请以相同方式配置您的 SAML 应用程序。

条件身份验证现在是否支持多个 SAML 应用程序和多个自定义域?

是的。这是许多大型企业希望使用的常见场景。一直以来，都可以创建条件身份验证策略，这些策略使用您的 1-10 个 `cloud.com` URL 中的任何一个解析为不同的 SAML 应用程序。现在，您的每个 `cloud.com` URL 都可以拥有自己的自定义 URL（URL 对）。

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

有关根据最终用户使用的商店 URL 在不同 IdP 之间切换的详细说明，请参阅本文 条件身份验证文章。

旧版未迁移 SAML 连接在不使用多个自定义 URL 或条件身份验证时的功能?

是的。将保持与现有旧版 1x 和 2x SAML 应用程序解决方案的向后兼容性，并且现有 SAML 应用程序解决方案将继续运行并得到支持。如果您的任何自定义 URL 仍处于未迁移状态，您将无法将自定义 URL 与 SAML 或条件身份验证结合使用。

多自定义 URL 功能发布后新 URL 的迁移?

不需要。在多自定义 URL 功能发布后，所有新引入的自定义域都将支持新架构，无需迁移。迁移仅适用于在多自定义 URL 功能发布之前创建的自定义 URL 配置。这通常是指您在 Citrix Cloud 租户中配置的第一个也是唯一一个自定义 URL，它在引入对多个自定义 URL 的支持之前就已经存在。

迁移旧版自定义 URL 和 SAML 配置

在执行任何迁移操作之前，您需要阅读整个 旧版自定义 URL SAML 配置 部分，以便了解您当前的自定义 URL 和 SAML 配置，以及您当前是否正在使用 **1x 或 2x SAML 应用程序**解决方案。迁移操作应在计划的维护窗口中进行，并在迁移后进行测试，以确保 SAML 登录未受影响，然后才能从 IdP 中删除任何过时的 SAML 应用程序。

重要提示：

如果您的 Citrix Cloud 和 SAML IdP 中的传统 SAML 配置与本文档“传统自定义 URL SAML 配置”部分中描述的 1x 或 2x SAML 应用程序解决方案不完全匹配，则您处于不受支持的状态。

我需要做些什么才能从当前的 2x SAML 应用程序自定义 URL 解决方案迁移到新的更简单的解决方案?

1. Citrix Cloud 管理员必须与 IdP 管理员协调，以便在 Citrix Cloud 的自定义 URL 服务和您的 SAML IdP 中进行必要的更改。
2. 在您的 SAML IdP 中，验证主要和辅助 SAML 应用程序的存在和配置。这对于每个 SAML IdP（例如 EntraID、Okta、Duo、PingFederate 等）都不同。
3. 请勿更改现有的主要 SAML 应用程序 Citrix Cloud SAML 端点。这是出现在 **身份和访问管理 > 身份验证** 中的 SAML 应用程序，在自定义 URL 迁移后将用于所有 SAML 登录用例。

   来自 Citrix Cloud 商业版美国、欧盟和亚太地区的主要应用程序示例

   - 实体 ID: `https://saml.cloud.com` 或 `https://saml.cloud.com/<guid>`
   - 断言消费者服务 (SSO): `https://saml.cloud.com/saml/acs`

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

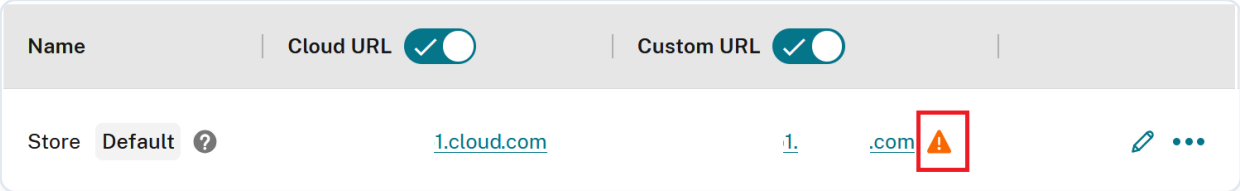
- 注销 (SLO): `https://saml.cloud.com/saml/logout/callback`

4. 识别此过时的辅助 SAML 应用程序。此 SAML 应用程序的配置在 **StoreFront Cloud > 访问** 菜单中指定。

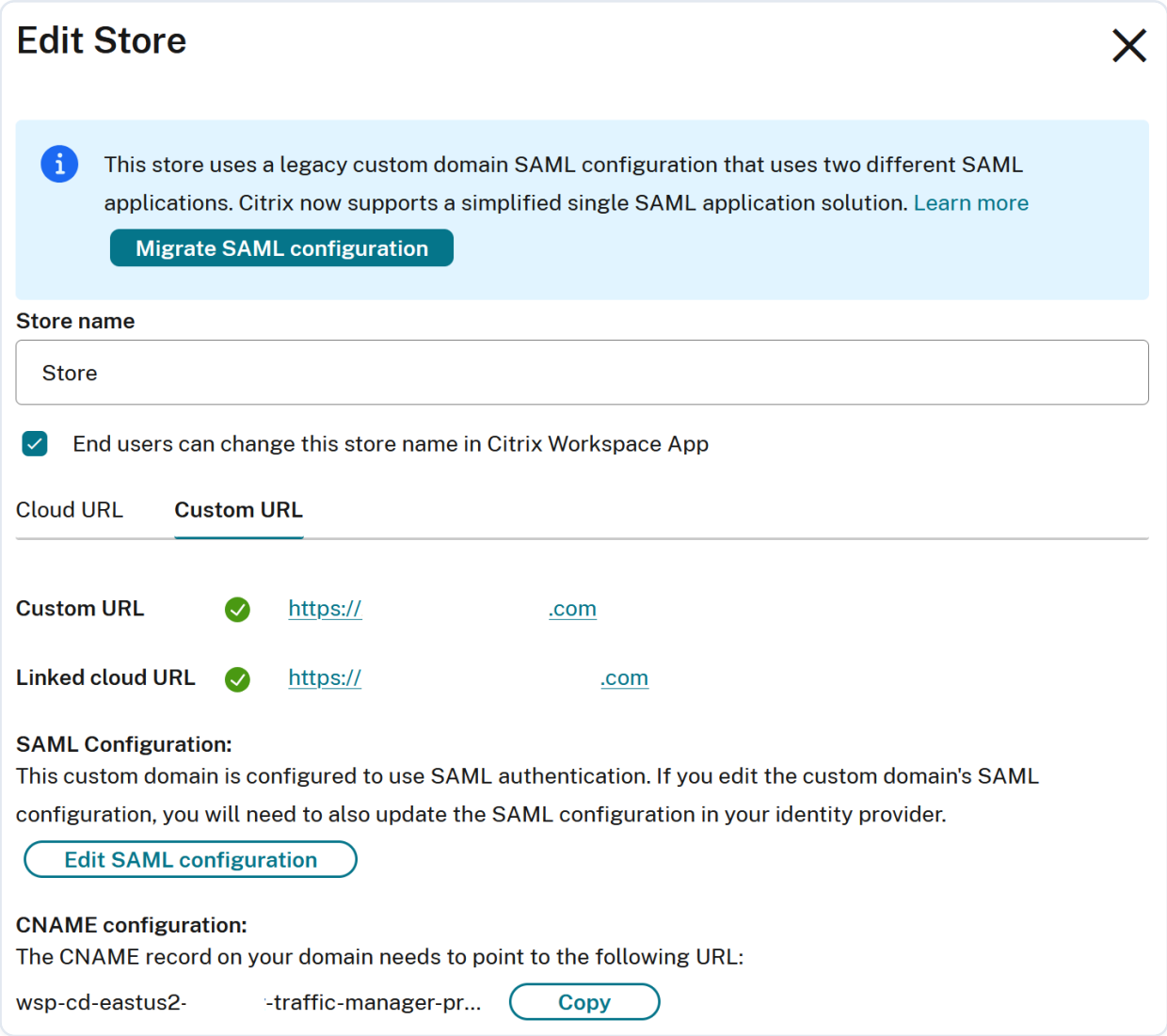
   辅助应用程序示例

   - 实体 ID: `https://saml.cloud.com` 或 `https://saml.cloud.com/<guid>`
   - 断言消费者服务 (SSO): `https://workspaces.mycompany.com/saml/acs`
   - 注销 (SLO): `https://workspaces.mycompany.com/saml/logout/callback`

5. 导航到 **StoreFront Cloud > 访问**，然后点击**警告图标**以打开迁移 UI。

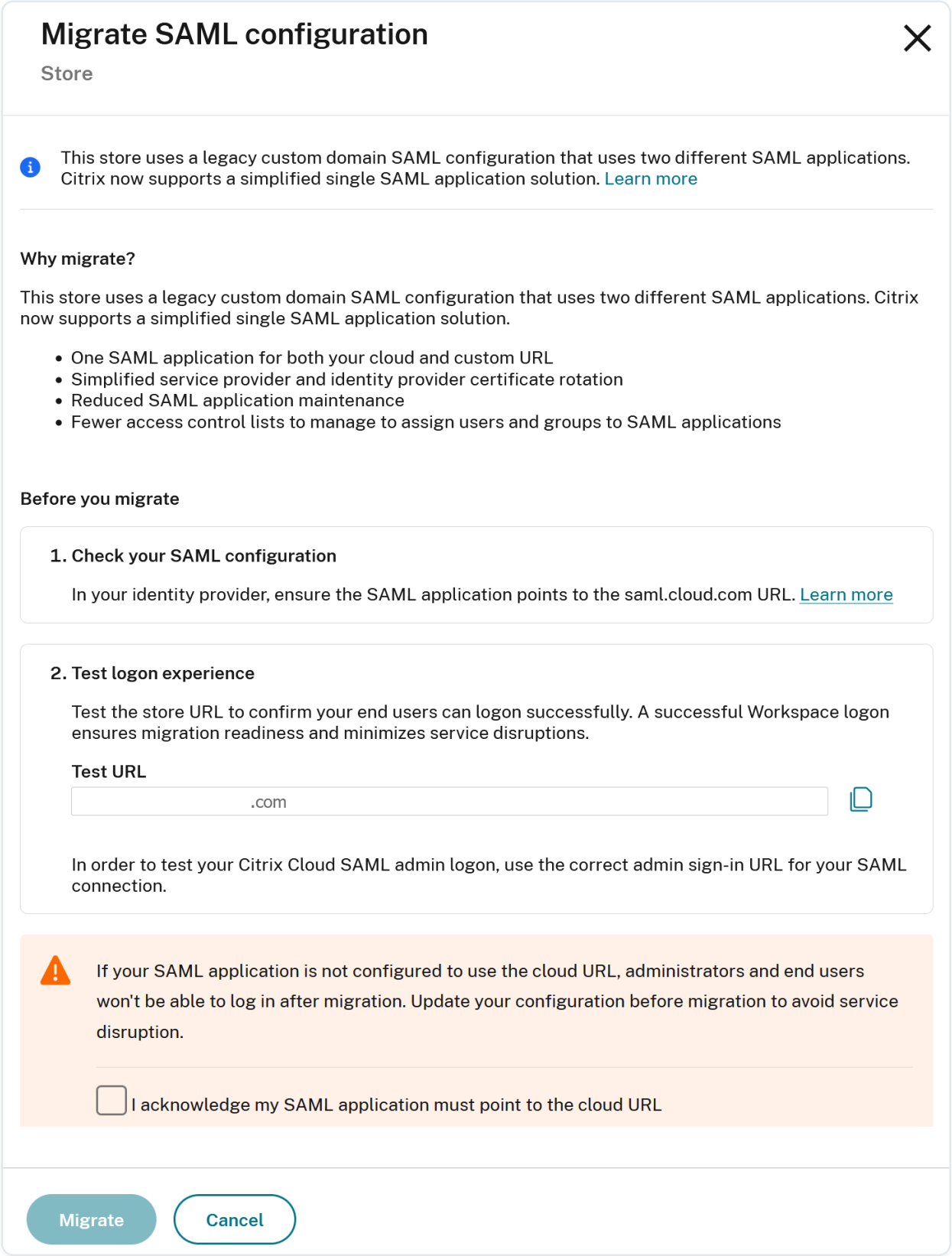


6. 点击下方所示的**迁移 SAML 配置**按钮。



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

7. 接受警告并在此 UI 中执行迁移。



8. 点击**迁移**。

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

重要提示：

迁移会更新商店自定义 URL 服务中的旧后端数据。这是对商店自定义 URL 服务记录的不可逆操作，一旦执行就无法恢复。

9. 迁移成功后，步骤 4 中自定义 URL 旁边的警告图标应会消失。这表示商店自定义 URL 服务中的后端数据已更新。

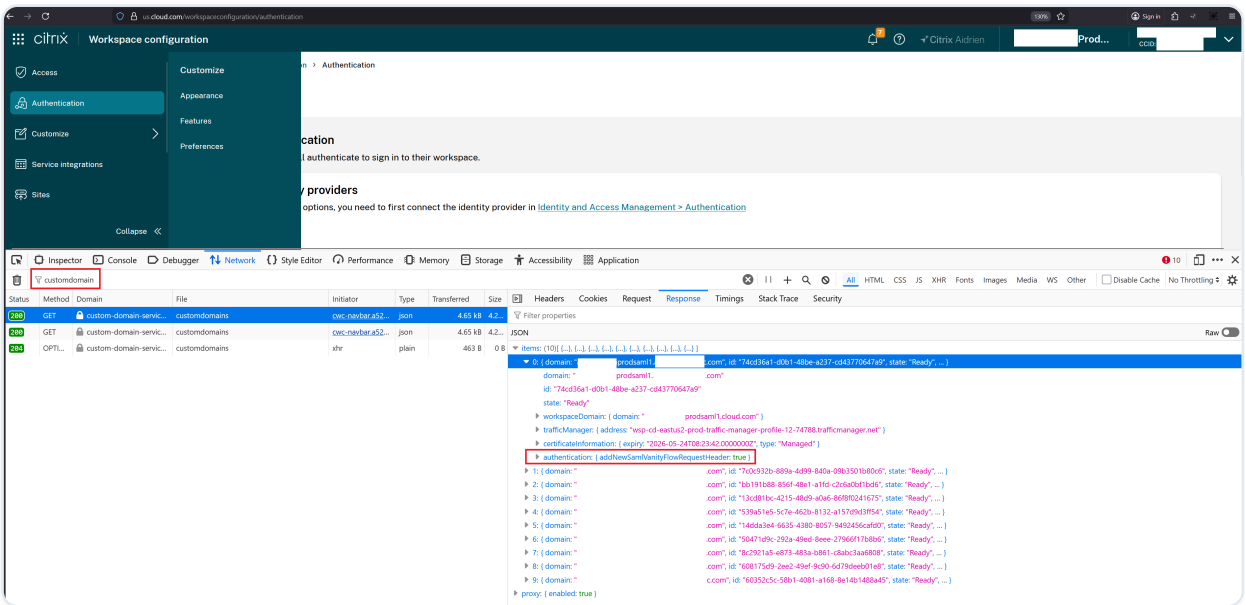
   验证所有 SAML 登录用例在迁移后仍然成功。

   - 使用任何 `cloud.com` URL 测试 SAML 登录到商店。这使用主 SAML 应用程序。
   - 使用所有自定义 URL 测试 SAML 登录到商店。这在迁移**之前**曾使用辅助 SAML 应用程序，但现在使用未更改的主 SAML 应用程序。
   - 使用您的管理员登录 URL，并使用在迁移前配置的任何 AD 管理员用户和组，测试 SAML 登录到 Citrix Cloud。这使用主 SAML 应用程序。

10. 验证后端商店自定义 URL 服务数据已成功更新。

    例如，使用 FireFox 开发者工具。

    在键盘上按 F12 打开浏览器上的开发者工具，然后从 Citrix Cloud UI 中已运行开发者工具的任何其他页面导航到 **StoreFront Cloud > 访问**。这将捕获 Citrix Cloud 控制台发出的所有 REST API 调用，以返回自定义 URL 列表。



    在网络搜索对话框中输入 `customdomain` 以筛选出正确的 REST API 调用。

    找到此 REST API 调用：

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

`GET https://custom-domain-service.us.wsp.cloud.com/services/custom-domain-service/customers/<CCID>/stores/<storeID>/customdomains`

迁移的自定义 URL 对象将包含此附加数据。

`"addNewSamlVanityFlowRequestHeader":true`

自定义 URL 对象示例：

```
"items": [

    {

        "domain": "stores.mycompany.com",

        "id": "74cd36a1-d0b1-48be-a237-cd43770647a9",

        "state": "Ready",

        "workspaceDomain": {

            "domain": "stores.cloud.com"

        },

        "trafficManager": {

            "address": "wsp-cd-eastus2-prod-traffic-manager-
profile-12-74788.trafficmanager.net"

        },

        "certificateInformation": {

            "expiry": "2026-05-24T08:23:42.0000000Z",

            "type": "Managed"

        },

        "authentication": {

            "addNewSamlVanityFlowRequestHeader": true
```

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

```
        }

    }

]
```

11. 从使用自定义 URL SAML 端点的 SAML IdP 中删除辅助应用程序。在 SAML 登录流程中不再使用辅助 SAML 应用程序。

> **重要提示：**
>
> 仅当您已证明迁移成功且所有必需的 SAML 登录场景均已测试通过后，才能删除辅助 SAML 应用程序。

我需要做什么才能从我当前的 1x SAML 应用程序自定义 URL 解决方案迁移到新的更简单的解决方案?

1. Citrix Cloud 管理员必须与 IdP 管理员协调，以便在 Citrix Cloud 的自定义 URL 服务和您的 SAML IdP 中进行必要的更改。
2. 在您的 SAML IdP 中验证自定义 URL SAML 应用程序的存在和配置。您的 SAML IdP 中应该只配置一个 SAML 应用程序。这对于每个 SAML IdP（例如 EntraID、Okta、Duo、PingFederate 等）都不同。

   您现有的主 SAML 应用程序的 Citrix Cloud SAML 端点应如下例所示。

   主应用程序示例

   - 实体 ID：`https://saml.cloud.com` 或 `https://saml.cloud.com/<guid>`
   - 断言消费者服务 (SSO)：`https://workspaces.mycompany.com/saml/acs`
   - 注销 (SLO)：`https://workspaces.mycompany.com/saml/logout/callback`
3. 提出支持案例并联系 Citrix 支持和工程团队，以安排协助迁移您的自定义域。Citrix 工程团队将在审查您的 SAML 配置后，代表您迁移您的自定义 URL。
4. 在安全地更改 SAML 应用程序之前，必须完成步骤 3。更新现有**主 SAML 应用程序**的 Citrix Cloud SAML 端点，使其与此示例类似。

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

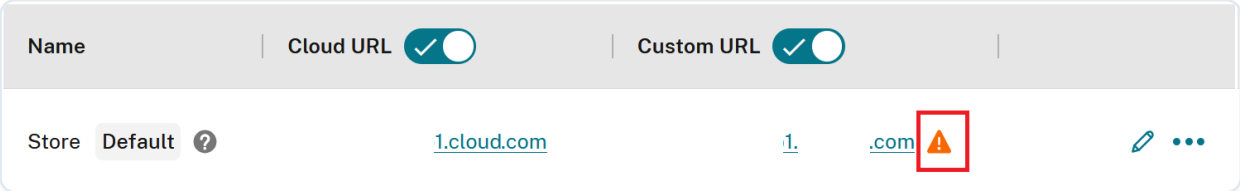
重要提示：

请勿更新或更改**主** SAML 应用程序上现有的 EntityID SAML 端点。无需更改此项。只需更新 ACS 和注销 SAML 端点。

主应用程序示例

- 实体 ID：`https://saml.cloud.com` 或 `https://saml.cloud.com/<guid>`（请勿更改）
- 断言消费者服务 (SSO)：`https://saml.cloud.com/saml/acs`（更新）
- 注销 (SLO)：`https://saml.cloud.com/saml/logout/callback`（更新）

5. 导航到 **StoreFront Cloud > 访问**，然后单击**警告图标**以打开迁移 UI。



6. 一旦 Citrix 支持和工程团队完成迁移，步骤 4 中自定义 URL 旁显示的警告图标应会消失。这表示商店自定义 URL 服务中的后端数据已成功更新。
7. 使用所有自定义 URL 测试 SAML 登录到商店（迁移前曾使用辅助 SAML 应用程序）。
   - 使用任何 `cloud.com` URL 测试 SAML 登录到商店（继续使用主 SAML 应用程序）。
   - 使用所有自定义 URL 测试 SAML 登录到商店（迁移前曾使用辅助 SAML 应用程序）。

旧版自定义 URL SAML 配置

要确定您是否在 Citrix Cloud 环境中部署了 **1x 或 2x SAML 应用程序**解决方案，请确定您当前使用的 SAML 登录方案组合，并检查 SAML 身份提供商中的当前 SAML 应用程序。

默认情况下，以下登录方案共享相同的 SAML 应用程序（SAML App 1）：

- SAML 身份验证，其中您所在区域的商店登录 URL (`cloud.com`, `citrixcloud.jp`, `cloud.us`) 在您的 SAML 提供商中配置为 SP 实体 ID。
- 使用您的唯一登录 URL（例如，`https://citrix.cloud.com/go/mycompany`）对 Citrix Cloud 进行 SAML 身份验证。在此方案中，管理员根据其 Active Directory (AD) 组成员身份，使用 SAML 对 Citrix Cloud 进行身份验证。

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

通过您在 Citrix® StoreFront Cloud 中配置的自定义域（例如，`https://workspaces.mycompany.com`）为用户添加 SAML 身份验证需要第二个 SAML 应用程序（SAML App 2）。

注意：

添加自定义 URL 并配置 SAML 在 Citrix Cloud 中预配最多需要 24 小时。

下表列出了支持的 SAML 登录方案组合以及所需的 SAML 应用程序。

使用商店 URL 登录商店	使用自定义域 URL 登录商店	使用 SAML 登录 URL 登录 CITRIX CLOUD	需要 SAML APP 1 吗？	需要 SAML APP 2 吗？
是	否	否	是 - 使用 cloud.com SAML 端点	否
否	是	否	是 - 使用自定义域 SAML 端点	否
否	否	是	是 - 使用 cloud.com SAML 端点	否
是	否	是	是 - 使用 cloud.com SAML 端点	否
否	否	是	是 - 使用 cloud.com SAML 端点	是 - 使用自定义域 SAML 端点
是	是	是	是 - 使用 cloud.com SAML 端点	是 - 使用自定义域 SAML 端点

1x SAML 应用程序配置（旧版 SAML 配置）

1. 在 Citrix Cloud 中，您在 **StoreFront Cloud > 访问**中配置了自定义 URL。
2. 在您的 SAML 提供商的管理控制台中，您使用商店自定义 URL 作为 SP 端点配置了 **1 个 SAML 应用程序**。

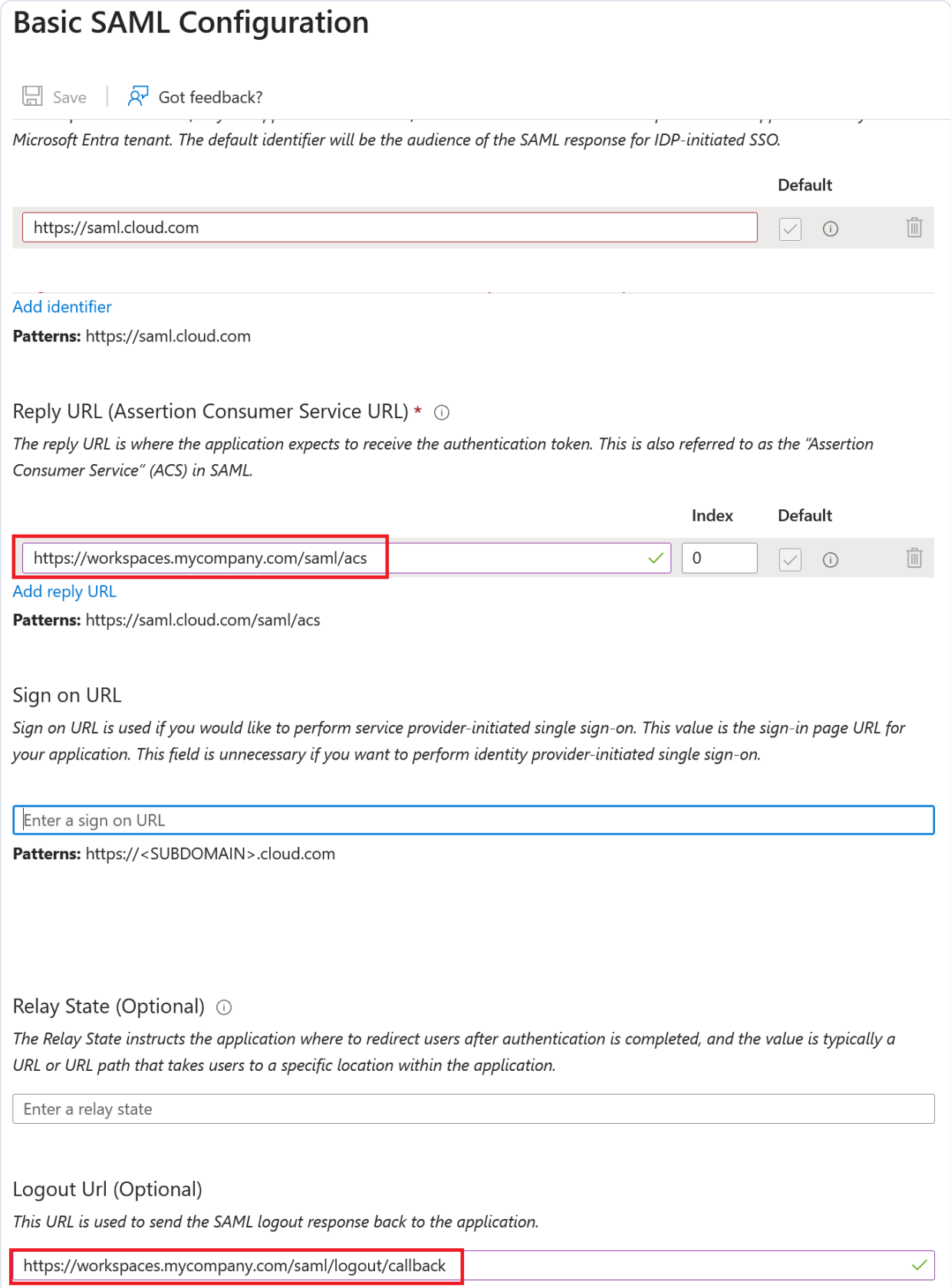
© 1997–2026 Citrix Systems, Inc. All rights reserved.

旧版自定义 URL SAML 应用程序端点示例

- 实体 ID: `https://saml.cloud.com` 或 `https://saml.cloud.com/<guid>`
- 断言消费者服务 (SSO): `https://workspaces.mycompany.com/saml/acs`
- 注销 (SLO): `https://workspaces.mycompany.com/saml/logout/callback`

以下示例说明了 Entra ID 的自定义 URL SAML 端点配置：

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

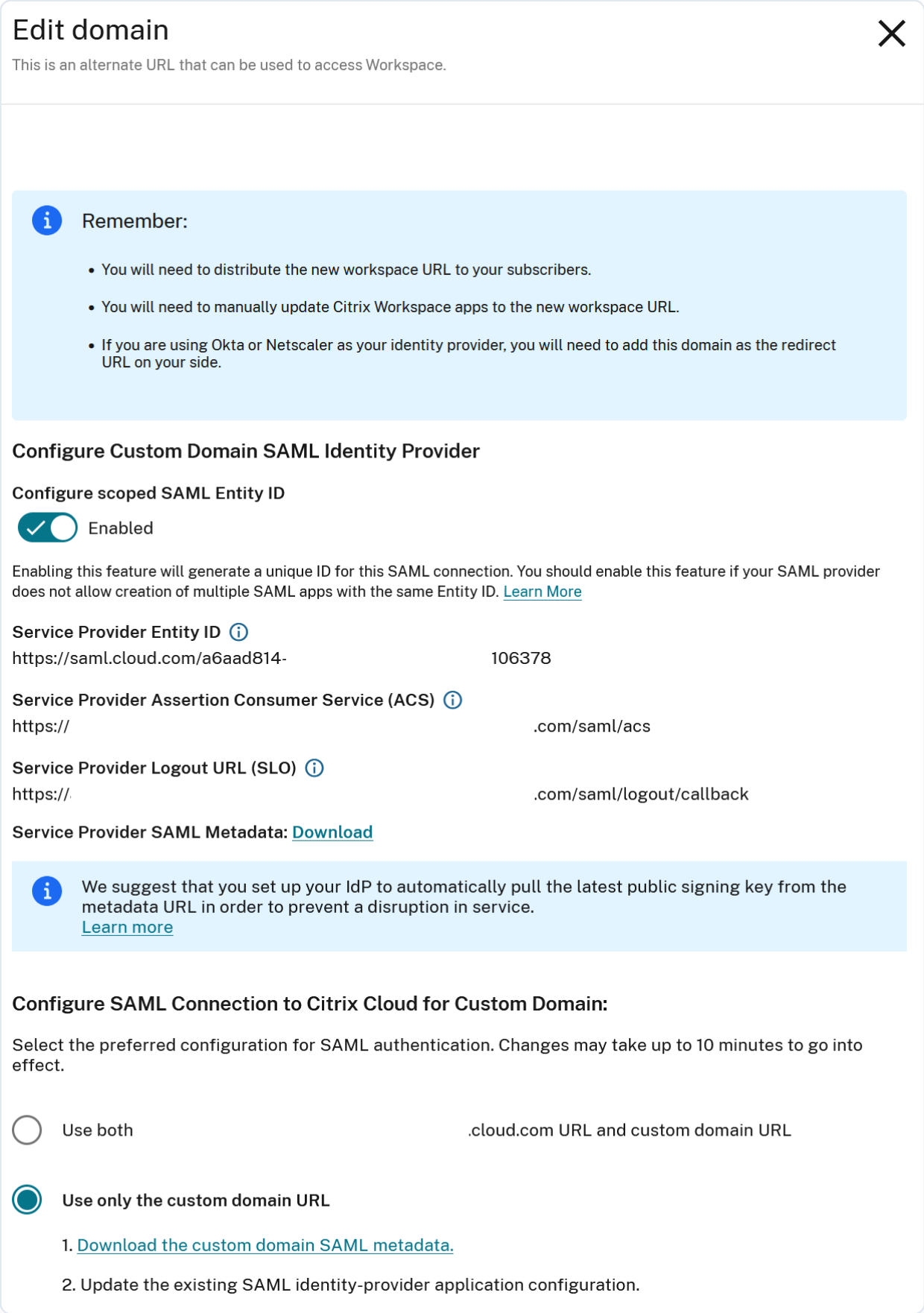


以下示例说明了 Okta 的自定义 URL SAML 端点配置，其中“受众限制”包含“实体 ID”值：

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

3. 您在 **StoreFront Cloud > 访问 > 编辑** 中选择了 **仅使用自定义域**。

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



2 个 SAML 应用程序配置（旧版 SAML 配置）

1. 在 Citrix Cloud 中，您在 **StoreFront Cloud > 访问** 中配置了一个自定义域。

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

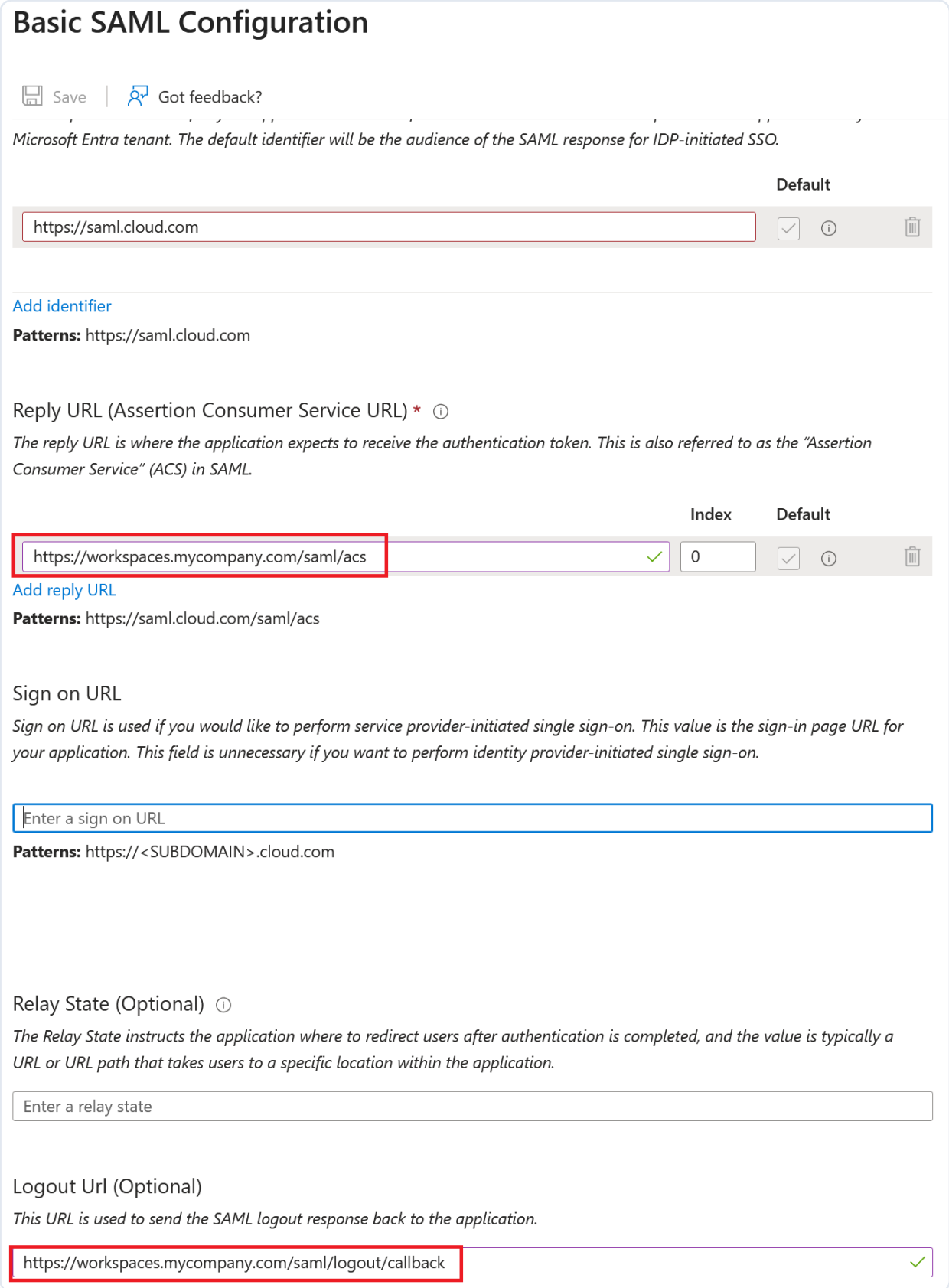
2. 在您的 SAML 提供商的管理控制台中，您配置了 **2 个 SAML 应用程序**。
3. 在**主 SAML 应用程序**中，您配置了以下 cloud.com SP 端点：

   - 实体 ID: `https://saml.cloud.com` 或 `https://saml.cloud.com/<guid>`
   - 断言消费者服务 (SSO): `https://saml.cloud.com/saml/acs`
   - 注销 (SLO): `https://saml.cloud.com/saml/logout/callback`

   以下示例显示了 Okta 管理控制台中的此端点配置：

   以下示例显示了 Entra ID 管理控制台中的此服务提供商端点配置：

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



4. 在**辅助 SAML 应用程序**中，您配置了以下商店自定义域 SP 端点。

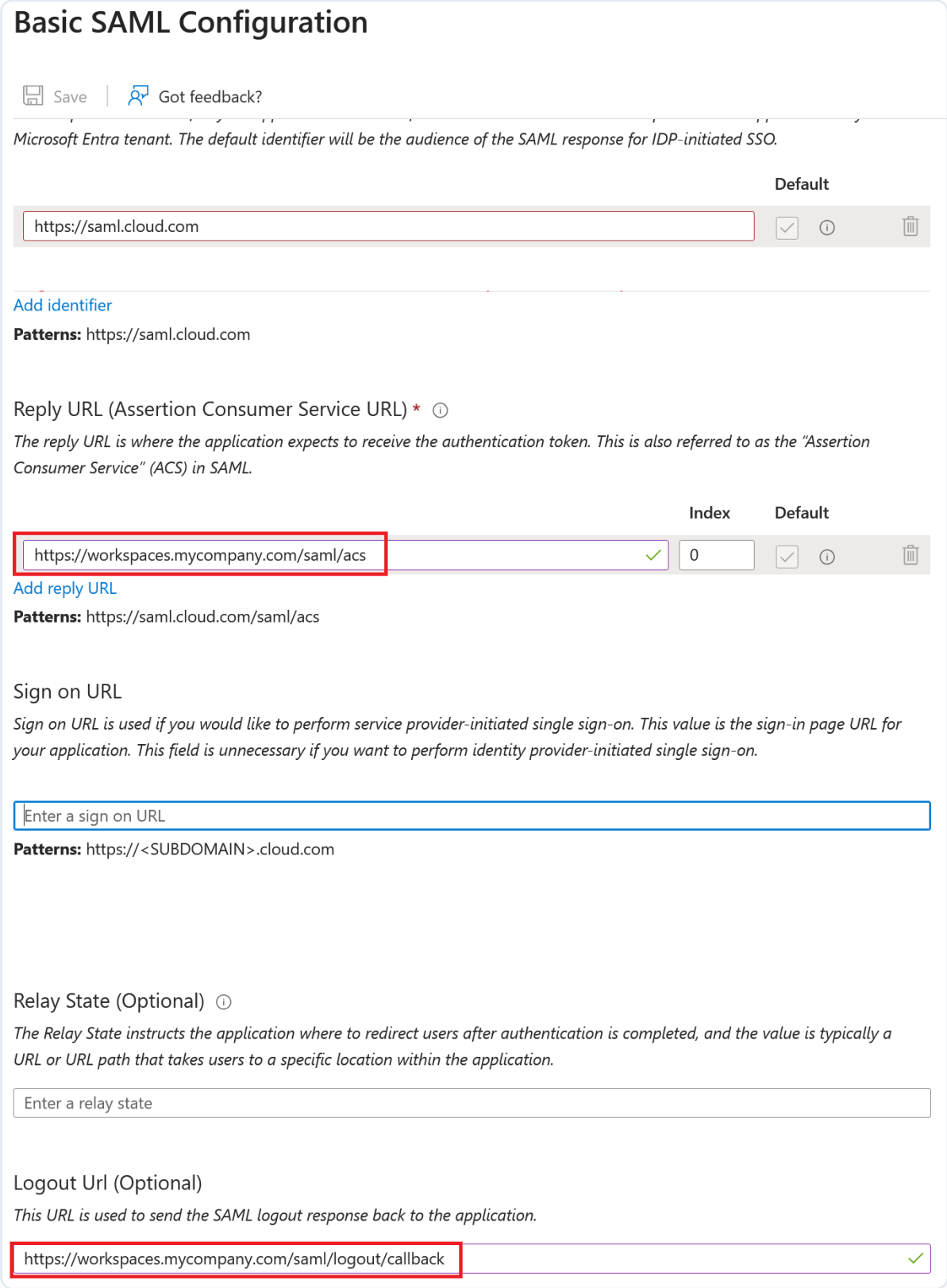
   - 实体 ID: `https://saml.cloud.com`
   - 断言消费者服务 (SSO): `https://workspaces.mycompany.com/saml/acs`

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

- 注销 (SLO): `https://workspaces.mycompany.com/saml/logout/callback` 以下示例显示了 Okta 控制台中的此服务提供商端点配置。

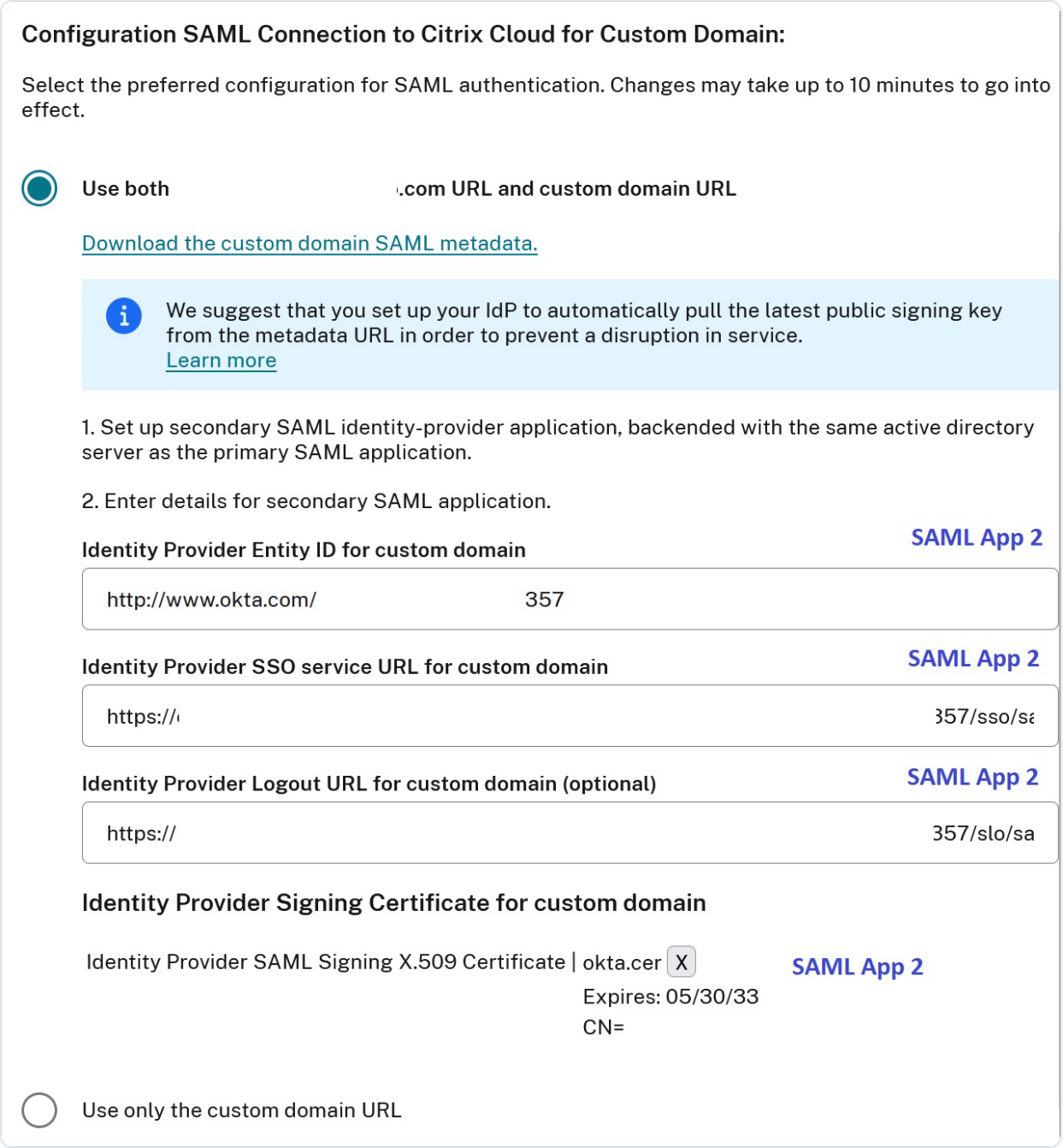
- 以下示例显示了 **Entra ID** 控制台中的此服务提供商端点配置。

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



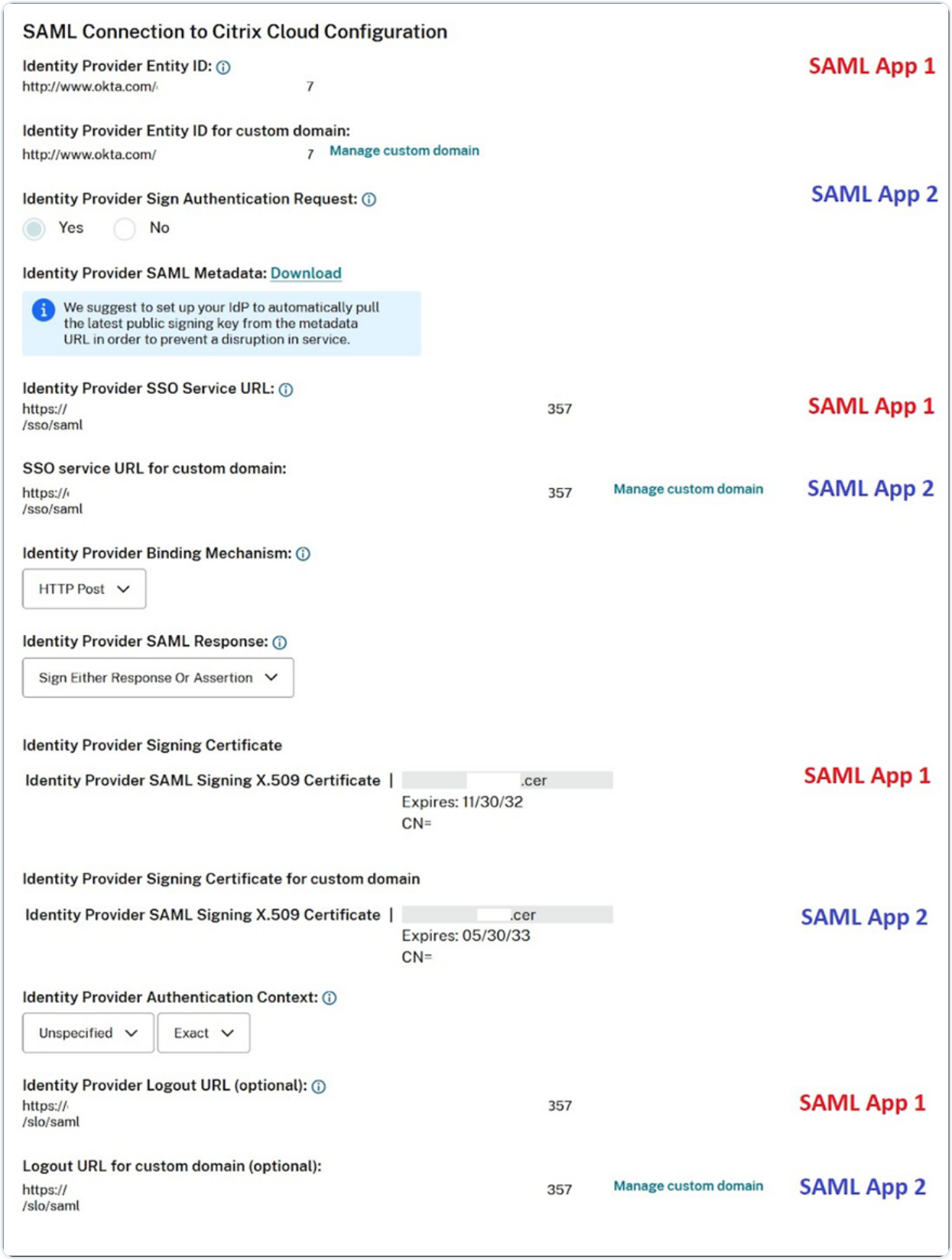
5. 您在 **StoreFront Cloud > 访问 > 编辑**中选择了**同时使用** `customer.cloud.com` **URL 和自定义 URL**。

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



6. 在**身份和访问管理 > 身份验证**中，从省略号菜单中选择**选择 SAML 提供程序 > 查看**。SAML 配置页面应显示为实体 ID、SSO URL 和注销 URL 配置的 SAML 端点对。

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



更新服务提供商 SAML 签名证书

使用签名请求和响应的 SAML 连接依赖于两个不同的 SAML 签名证书。SAML 连接的每一侧各一个。

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

服务提供商签名证书

此证书由 Citrix 通过 Citrix Cloud™ SAML 元数据提供，并在 SP 签名证书轮换的通告阶段进行更新。这至少每年发生一次。

SAML 签名证书需要在其到期日期之前进行轮换，以便为 Citrix Cloud 管理员提供准备部署的时间。服务提供商和身份提供商都需要进行证书轮换，以确保一致性并防止任何停机。

如果所选的 SAML 提供商不支持 SP SAML 签名证书的自动轮换，则必须在您的 SAML 提供商中手动轮换 SAML 签名证书，以替换即将到期的证书。

重要提示：

本 SAML 电子文档部分中的所有现有指南都包含有关如何在 SAML 连接的两侧配置签名的详细信息。Citrix® 仅推荐签名 SAML 配置，因为这些配置更安全，并且某些 SAML 提供商要求它们才能成功注销 (SLO)。

常见问题

什么是 SAML 签名?

SAML 协议使用消息来请求身份验证并发送身份断言。这些消息的安全性取决于传输和消息级别的安全性。这些消息是根据 XML 签名语法 签名的 XML 文档。这既提供了消息的完整性保证，又通过证明发送方持有私钥来验证发送方身份。信任模型由 SAML 安全和隐私注意事项 描述。用于定义哪些私钥受信任的公钥可以以任何合适的格式分发。思杰使用 X.509 证书作为分发和使用密钥的合适容器。

什么是 SAML 签名请求强制执行?

Just because Citrix Cloud is configured to send signed requests within the SAML connection this does not guarantee that the SAML provider will enforce the use of signatures and reject any unsigned incoming SAML requests. Most SAML IdPs have an option to enforce signed requests. If an unsigned request to log into the SAML provider is received then the SAML logon will fail. Some SAML IdPs like Duo do not even offer this option. It is the responsibility of the SAML IdP admin to check the status of the SAML IdP configuration. Citrix support does not control or have any visibility of whether signed requests are enforced within your SAML application.

Citrix 多久轮换一次其服务提供商 SAML 签名证书?

为了确保活动的服务提供商签名证书与新颁发的证书之间有足够的重叠时间，Citrix 大约每 11 个月轮换一次服务提供商签名证书。这是为了确保在新证书激活前 30 天，有效的证书可供 Citrix Cloud 客户使用。

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

什么是服务提供商 SAML 签名证书通告阶段?

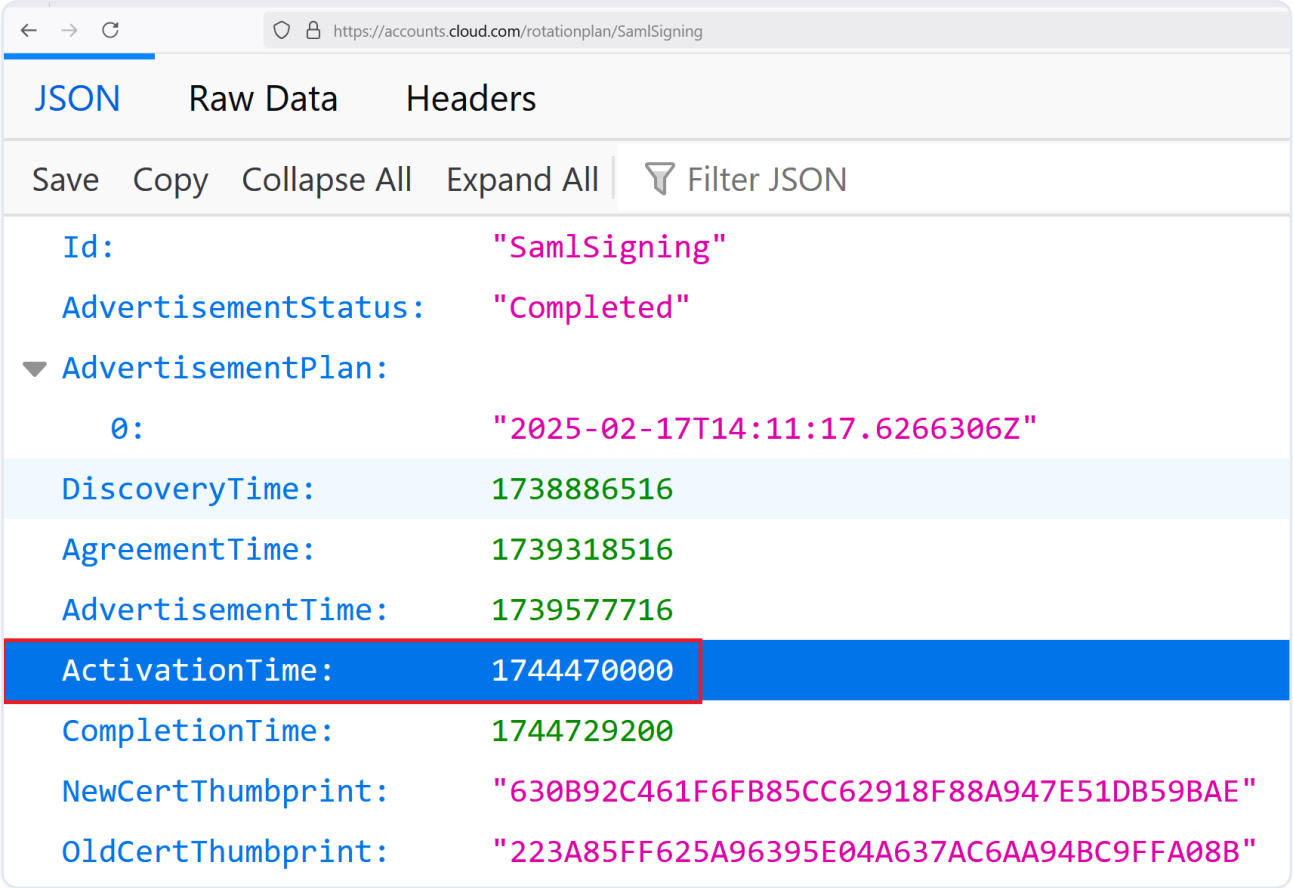
在通告阶段，当前和替换的 SAML 签名证书将存在于 Citrix Cloud 元数据中。在轮换日期和时间之前，只有活动证书可用于 SAML 请求验证。这是 Citrix Cloud 电子邮件和 Citrix Cloud 控制台通知中指定的日期和时间。

重要提示：

签名证书的到期日期与激活日期不同。Citrix 和 IdP 管理员需要关注的是激活日期，而不是证书的到期日期。Citrix Cloud 签名证书总会在到期前进行轮换。

您可以使用此链接 轮换计划 查看通告和激活日期和时间。

日期和时间以 Unix 纪元时间戳的形式提供，用于服务提供商签名证书轮换过程中的每个事件。



使用 纪元转换器 将 Unix 纪元时间戳转换为人类可读的日期和时间格式。

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

Citrix 为何决定使用自签名 Citrix Cloud SAML 签名证书，而不是由 Digitcert 等公共证书颁发机构签名的证书?

在您应上传到 SAML 应用程序的最新版 SAML 签名证书中，**颁发者**：现在是“samlsigning.cloud.com, Citrix Systems Inc.”，而不是 Digicert 等公共证书颁发机构。使用自签名 SP 签名证书是为了缓解外部颁发证书中已知的 SAML 漏洞，该漏洞被称为“Silver SAML”。

我为何通过电子邮件和 Citrix Cloud 控制台收到通知，指出当前的 Citrix Cloud SAML 签名证书即将到期且必须更换?

SAML 提供商 (IdP) 需要有效且在有效期内的证书来验证来自服务提供商（例如 Store 和 Citrix Cloud 控制台）的传入 SAML 请求的签名。将联系使用 SAML 进行 Store 或 Citrix Cloud 控制台登录的 Citrix Cloud 客户，告知他们即将进行的 SAML 签名证书轮换。

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

citrix

Hi [redacted]

Customer name: [redacted]
Organization ID:

Source: Citrix Cloud
Type: Critical

Final notice: Service Provider SAML certificate rotation on 2026-08-13 18:07:44 UTC

This notice is about an impending Citrix Cloud Service Provider (SP) SAML signing certificate rotation.

If your identity provider can't retrieve the latest public signing key automatically from the Citrix Cloud metadata, you must follow these manual steps to avoid service interruptions:

1. Determine if your SAML IDP supports Signing Enforcement.
2. Determine if your SAML app is already configured to enforce signed incoming SAML requests from Citrix Cloud and already has a copy of the existing Citrix Cloud certificate configured within it. Complete steps 3-5 only if both are true.
3. Download the new Citrix Cloud SP signing certificate from the Citrix Cloud SAML UI.
4. Upload it into your IDP's SAML application as an additional signing verification certificate before **2026-08-13 18:07:44 UTC**.
5. Remove the old Citrix Cloud certificate after **2026-08-13 18:07:44 UTC**. Do not remove it before this time.

You are advised to read the details on how to Update the Service Provider SAML Signing Certificate.

Certificate rotation time: **2026-08-13 18:07:44 UTC**.

View all notifications

To stop receiving Citrix Cloud notification, Manage Preferences from Account Settings and turn off email notifications.

xae2sfstg | Org ID: int65bff83c | Citrix Cloud Customer ID: xae2sfstg

© 2026 Citrix Systems, Inc. All rights reserved. Citrix, the Citrix logo, Citrix Cloud, and other proprietary Citrix marks appearing herein are trademarks of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered in the U.S. Patent and Trademark Office and in other countries. All other marks appearing in this piece are the property of their respective owners. Privacy and terms

Citrix Cloud
Sep 22, 2026 7:08:11 PM

Service Provider SAML certificate rotation on 2026-08-13 18:07:44 UTC

This notice is about an impending Citrix Cloud Service Provider (SP) SAML signing certificate rotation.

If your identity provider can't retrieve the latest public signing key automatically from the Citrix Cloud metadata, you must follow these manual steps to avoid service interruptions:

1. Determine if your SAML IDP supports Signing Enforcement.
2. Determine if your SAML app is already configured to enforce signed incoming SAML requests from Citrix Cloud and already has a copy of the existing Citrix Cloud certificate configured within it. Complete steps 3-5 only if both are true.
3. Download the new Citrix Cloud SP signing certificate from the Citrix Cloud SAML UI.
4. Upload it into your IDP's SAML application as an additional signing verification certificate before **2026-08-13 18:07:44 UTC**.
5. Remove the old Citrix Cloud certificate after **2026-08-13 18:07:44 UTC**. Do not remove it before this time.

You are advised to read the details on how to Update the Service Provider SAML Signing Certificate.

Certificate rotation time: **2026-08-13 18:07:44 UTC**.

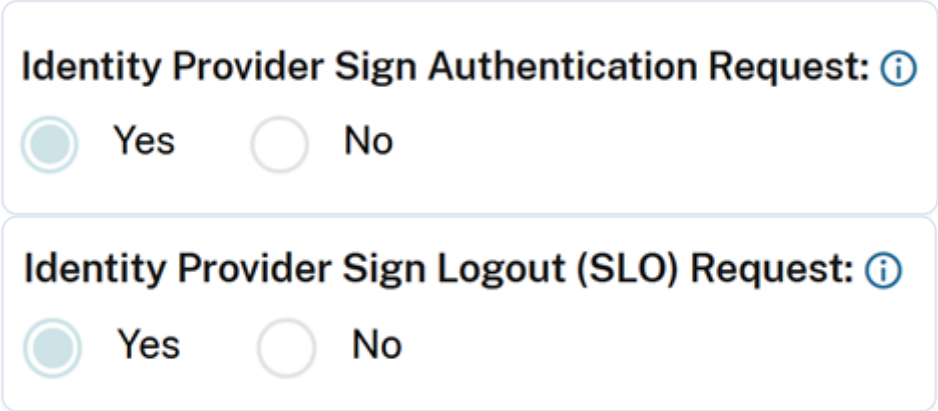
我如何知道我的 Citrix Cloud 客户是否受到 Citrix Cloud SAML 签名证书轮换的影响?

这将影响具有以下 SAML 配置的 Citrix Cloud 客户。

- 您的 Citrix Cloud 中的 SAML 连接配置为 **Sign Authentication Requests = Yes**
- 您已将 SAML 提供程序（例如 Microsoft Entra ID、ADFS 或 Okta）配置为拒绝未签名的 SAML 请求（签名强制）。
- 您已在 Citrix Cloud SAML 连接和 SAML 提供程序中配置了单点注销 (SLO)。作为安全最佳实践的一部分，SLO 请求需要签名。

如何检查我的 Citrix Cloud SAML 连接的签名配置?

导航到 **Identity and Access Management** > **SAML 2.0** > **Edit**，检查您的 Citrix Cloud SAML 连接中是否启用了 **Sign Authentication Requests**。Citrix Cloud 中的所有新 SAML 连接都将默认设置为 **Identity Provider Sign Authentication/Logout Requests = Yes**，用于登录 (SSO) 和注销 (SLO)。

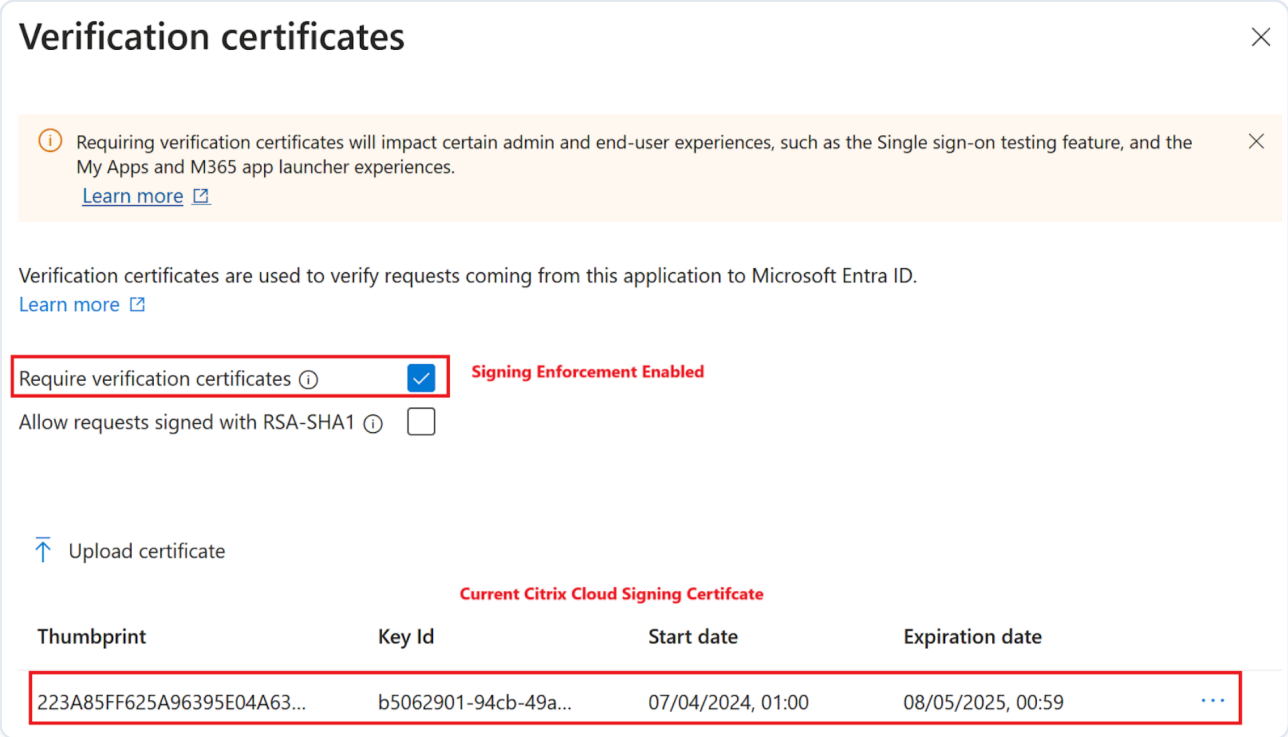


如何检查我的 SAML 应用程序中是否配置了签名强制?

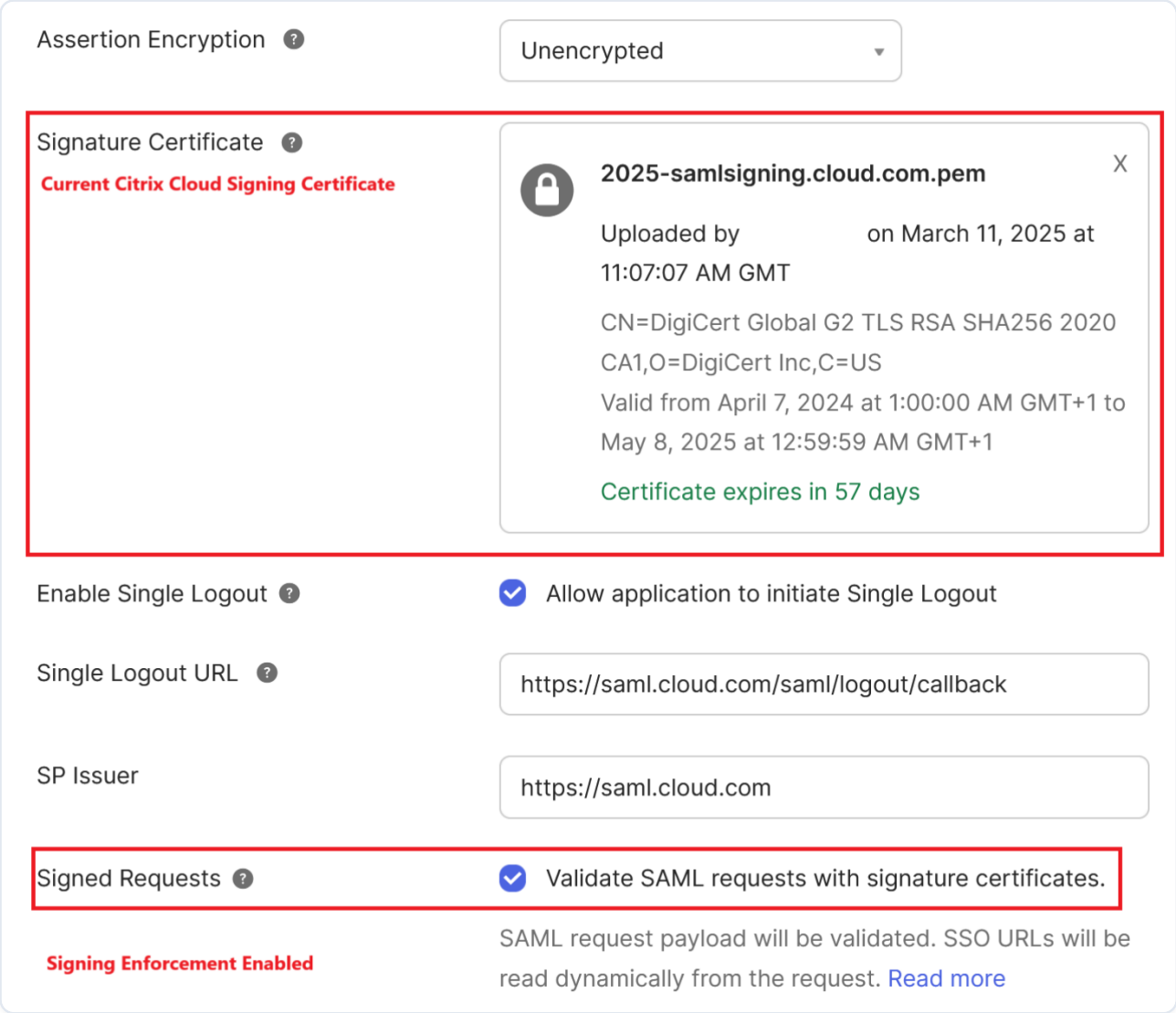
这取决于您使用的 SAML 提供程序。所有 Citrix 文档中记载的 SAML 解决方案都包含启用签名强制的步骤，作为安全最佳实践的一部分。

EntraID 签名强制示例：

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



Okta 签名强制示例：



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

在哪里可以获取最新服务提供商 (SP) 签名证书的副本?

此证书由 Citrix 通过 Citrix Cloud SAML 元数据提供，并在 SP 签名证书轮换的通告阶段定期更新。这至少每年发生一次。

美国、欧盟和亚太南部：`<https://saml.cloud.com/saml/metadata>`

日本：`<https://saml.citrixcloud.jp/saml/>`

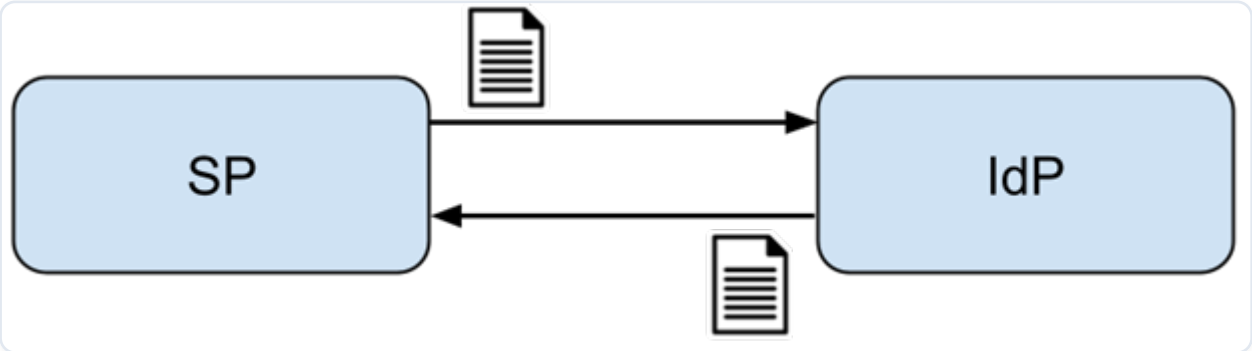
政府：`<https://saml.cloud.us/saml/metadata>`

如果我的 SAML 应用程序支持多个验证证书，何时可以安全地删除旧的 Citrix Cloud SAML 签名证书?

仅在电子邮件和 Citrix Cloud 控制台通知中给出的证书激活日期和时间之后，才能从 SAML 应用程序中删除旧的 Citrix Cloud 签名证书。某些 SAML IdP（例如 Okta）一次只允许上传一个签名证书。在这种情况下，别无选择，只能在激活日期和时间之后用新证书覆盖当前证书。这不应在激活日期和时间之前完成。

使用元数据交换自动使用最新的 Citrix Cloud SP SAML 签名证书更新 SAML 提供程序

通过 SAML 元数据交换，SAML 提供程序通过监视元数据 URL（例如 `<https://saml.cloud.com/saml/metadata>`）自动使用 Citrix Cloud SAML 元数据。如果您的 SAML 提供程序支持 SAML 元数据交换，则 SP 签名证书可能已自动更新。 验证您的 SAML 提供程序是否支持元数据交换。之后，您可以在当前 SAML 签名证书过期之前验证更新是否已发生。



重要

每个第三方 SAML 提供程序支持的 SAML 功能存在很大差异。Citrix Cloud 管理员有责任了解和理解所用 SAML 提供程序的功能和要求。这对于确保 Citrix Cloud SAML 连接配置 (SP) 和 SAML 提供程序 (IdP) 配置匹配是必要的。请参阅您的 SAML 提供程序的文档，以确定它是否支持签名验证以及 SAML 请求和响应是否需要签名。

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

手动使用最新的 Citrix Cloud SP SAML 签名证书更新 SAML 提供程序

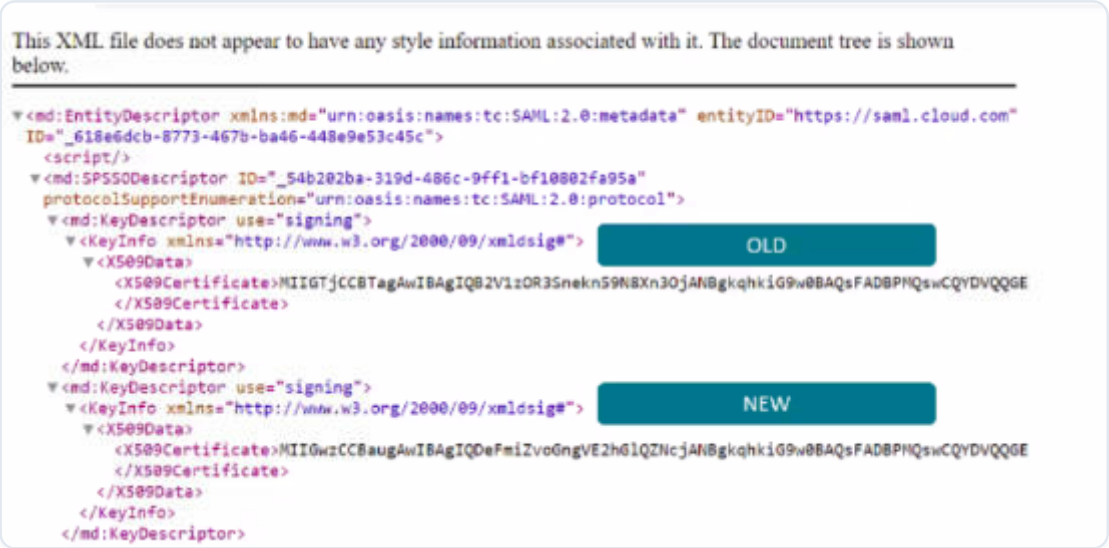
重要

每次从 Citrix Cloud 发布新证书时都必须进行 SP 证书轮换，否则 SAML 登录将受到影响，并且您将遭受停机。

从 Citrix Cloud 元数据中获取未来服务提供商证书的副本

1. 通过在**身份和访问管理**中查看您当前的 SAML 连接，单击**身份验证**，选择**SAML 连接**并单击**查看**，从 Citrix Cloud 获取最新的 SAML 元数据。 下图显示了此文件在 Citrix Cloud 区域（例如美国、欧盟和亚太地区）中的示例外观：

   `<https://saml.cloud.com/saml/metadata>`

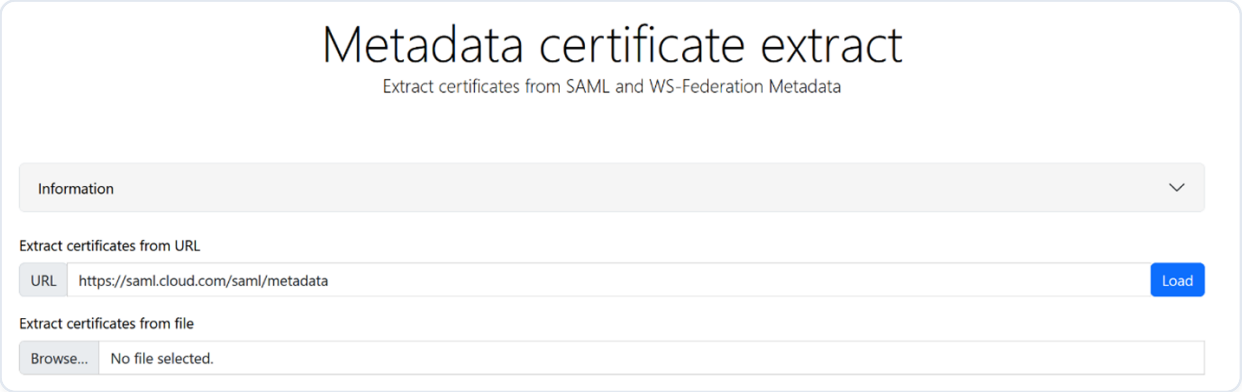
   

   在此元数据 XML 文件示例中，有两个 x.509 Citrix Cloud SAML 签名证书。

2. 可以通过将 XML 文件上传到第三方工具或提供元数据 URL，从元数据中提取 x.509 证书。
3. 导航到 `<https://www.rcfed.com/SAMLWSFed/MetadataCertificateExtract>`
4. 输入与您的 Citrix Cloud 客户区域相对应的 SAML 元数据 URL：

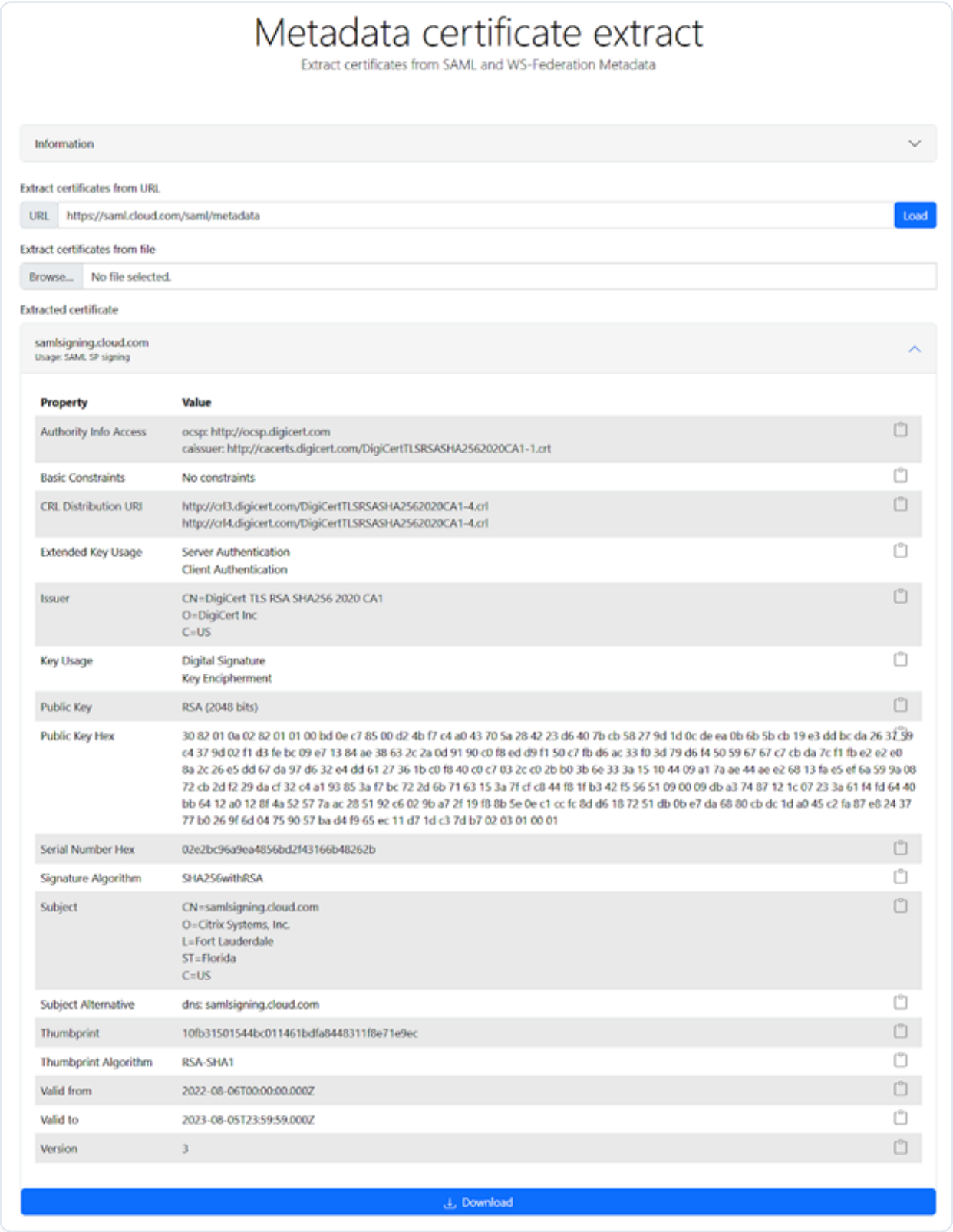
   - 美国、欧盟和亚太地区：`<https://saml.cloud.com/saml/metadata>`
   - 日本：`<https://saml.citrixcloud.jp/saml/metadata>`
   - 政府：`<https://saml.cloud.us/saml/metadata>`

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



从 `<https://www.rcfed.com/SAMLWSFed/MetadataCertificateExtract>` 下载 SAML 签名证书。

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



5. 将新提取的 Citrix Cloud SP SAML 证书上传到您的 SAML 提供商。此过程对于每个 SAML 提供商都不同。请使用您的特定 SAML 提供商文档验证正确的 SP 签名证书轮换过程。

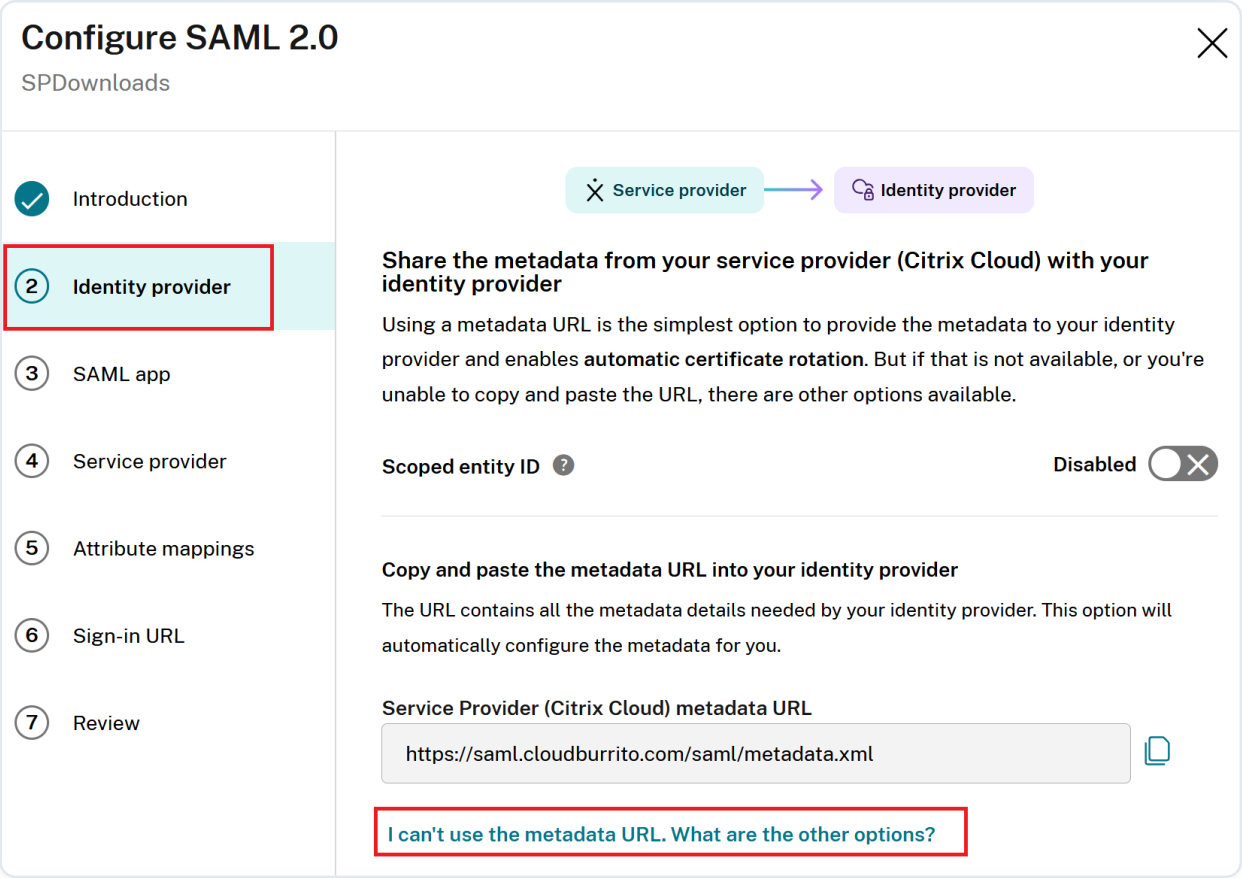
   根据您的 SAML 提供商，现有的 SAML 签名证书可能需要替换为新证书。在某些情况下，SAML 提供商可能同时支持多个 SP 签名证书，因此只需上传新证书即可。建议您在旧证书过期后将其删除。

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

或者，

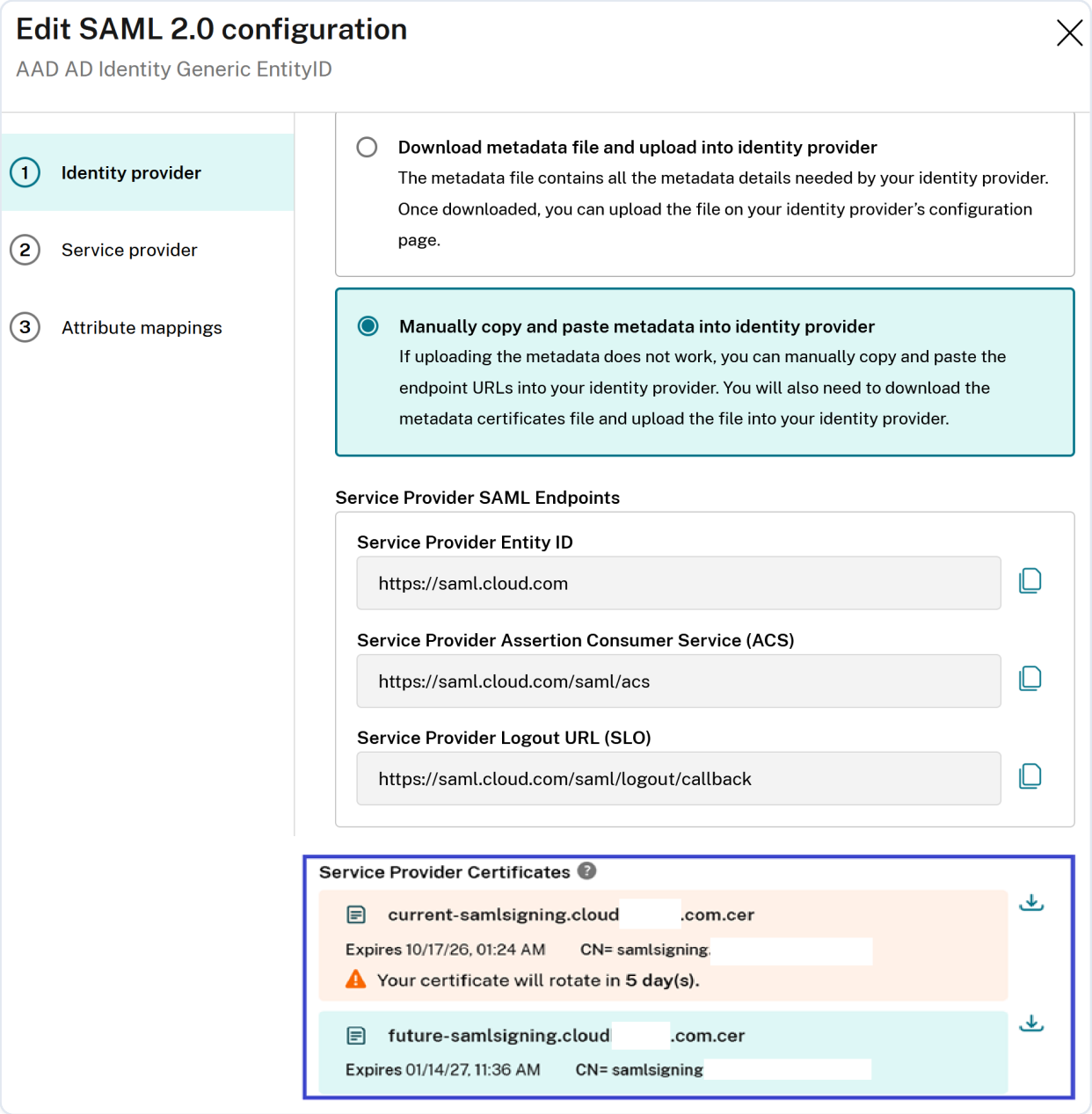
从 Citrix Cloud UI 内部获取未来服务提供商证书的副本

1. 在新手动创建的连接的“配置 SAML 2.0”向导中。
2. 在向导流程中导航到“**身份提供商**”页面。
3. 选择“**我无法使用元数据 URL。还有其他选项吗？**”?



4. 选择“**手动输入元数据字段**”并导航到“**服务提供商证书**”部分。
5. 下载未来版本的 Citrix Cloud 签名证书。

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

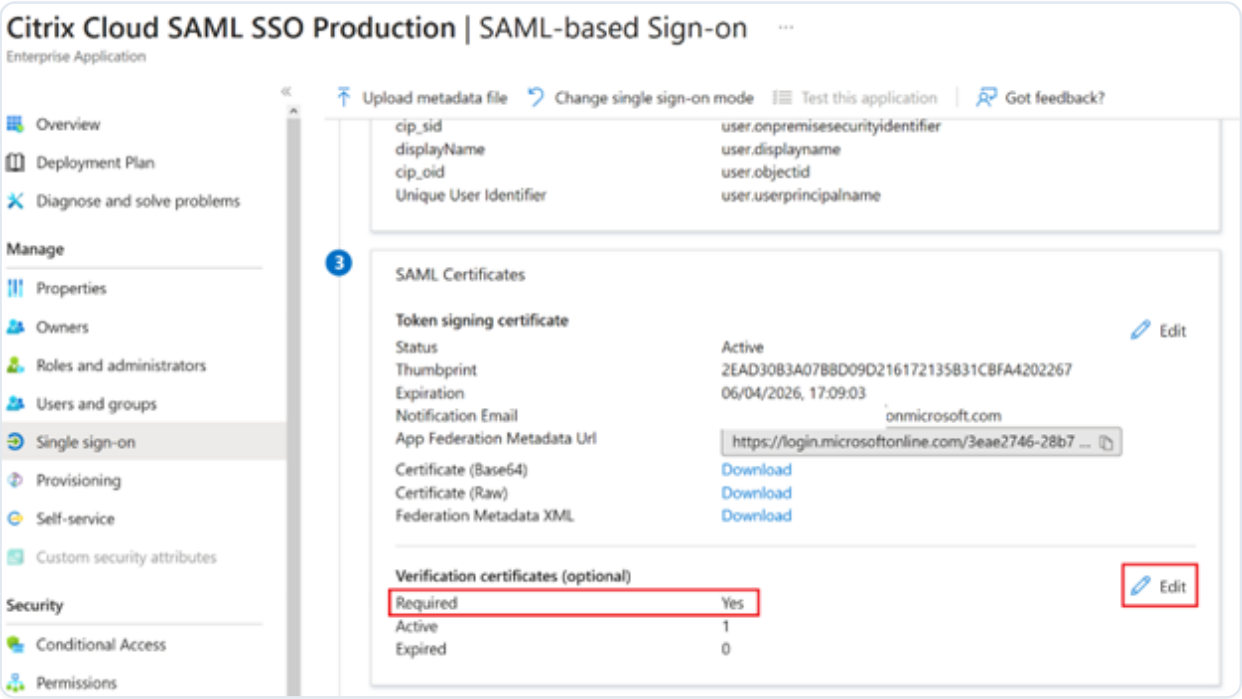


将替换的 Citrix Cloud SAML 签名证书上传到您的 Microsoft Entra ID SAML 应用程序

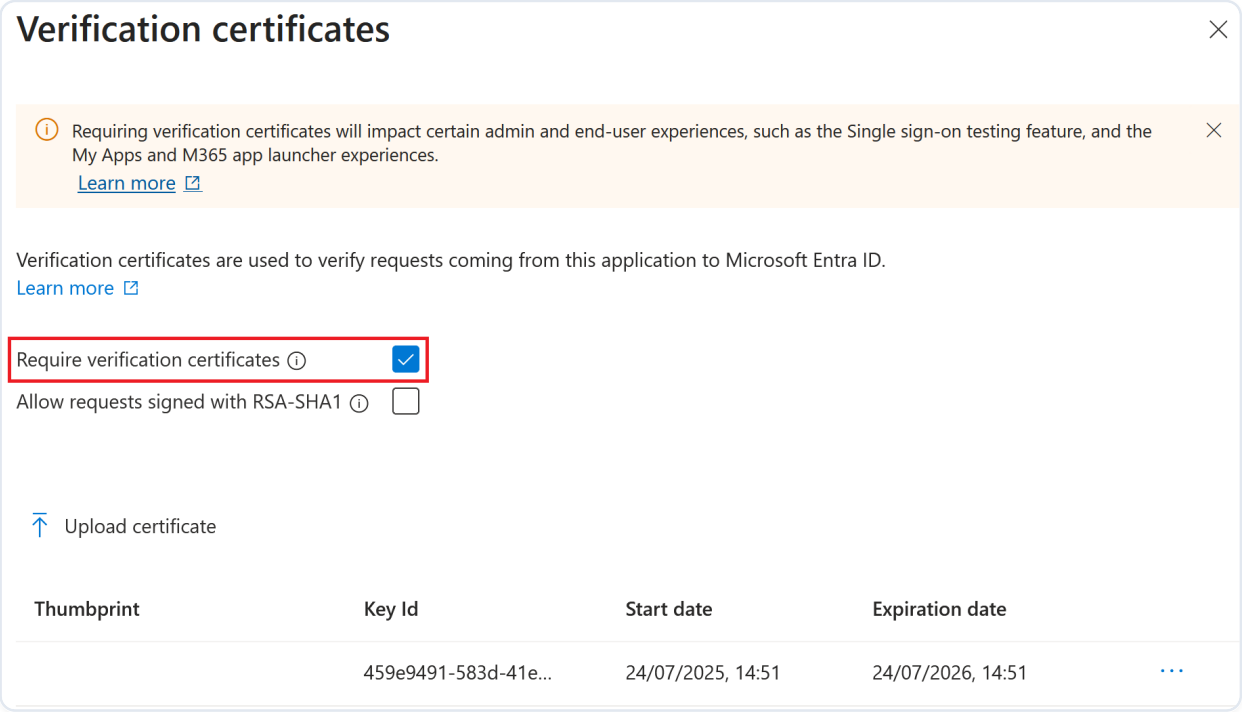
在配置 Microsoft Entra ID SAML 应用程序之前，请参阅SAML 请求签名验证以获取更多信息。

1. 导航到“**Microsoft Entra ID**”，选择“**企业应用程序**”，然后单击“您的 SAML 应用程序”。
2. 在 SAML 应用程序中找到 SAML 证书部分。

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



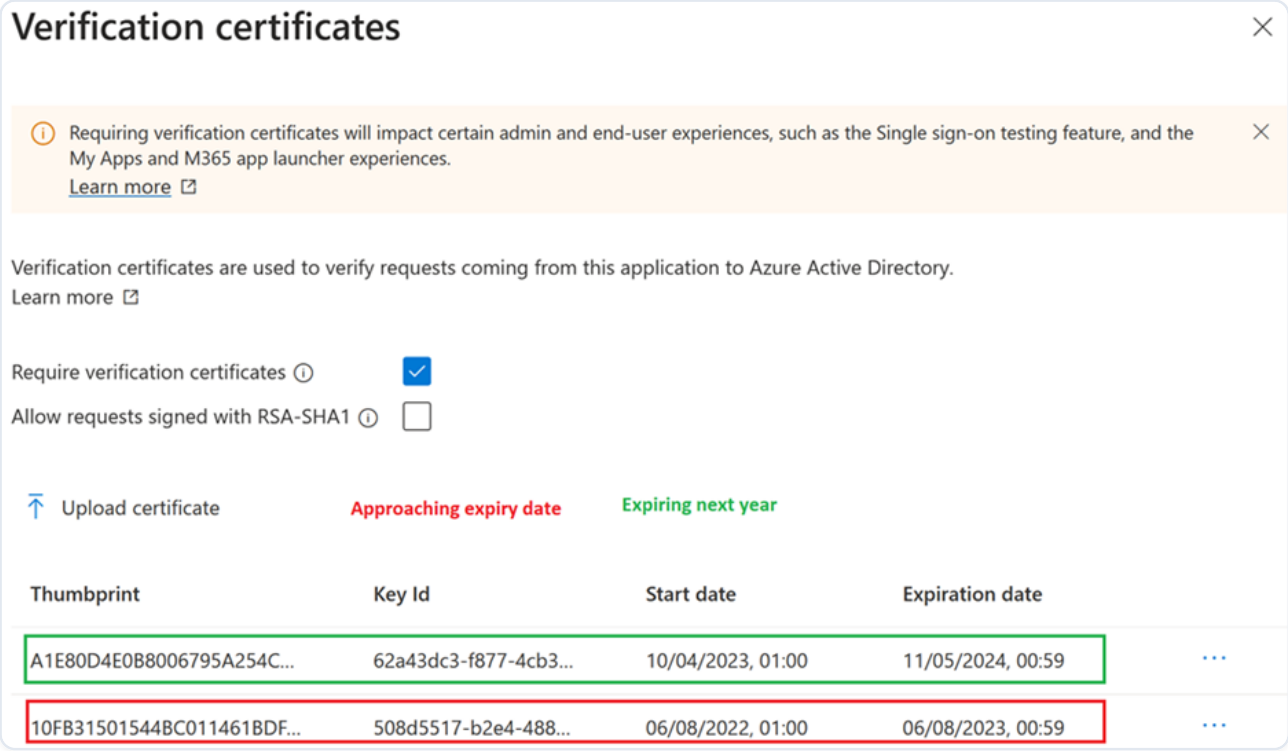
3. 选择 **上传证书** 并上传从 SAML 元数据中获取的替换 Citrix Cloud SAML 签名证书。



注意：

Microsoft Entra ID SAML 应用程序可以配置多个签名验证证书，因此可以在当前证书过期很久之前上传替换证书。以下屏幕截图显示了两个有效证书。其中一个证书即将在不久的将来过期。只要上传的证书中至少有一个有效且尚未过期，SAML 登录到商店或 Citrix Cloud 将继续成功，并且您不会遇到服务中断。

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



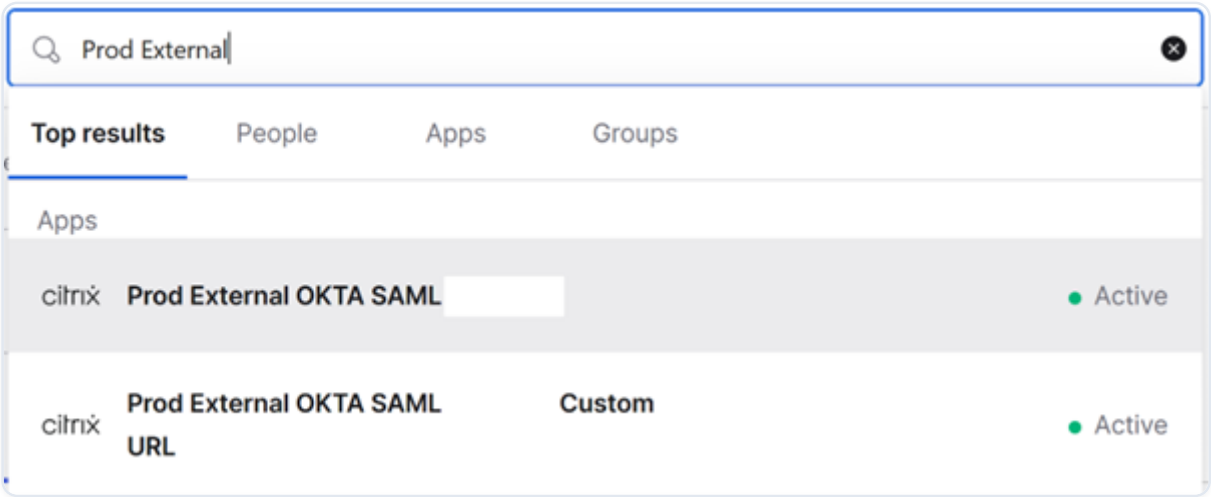
重要提示：

在电子邮件和 Citrix Cloud 控制台通知中给出的 SAML 轮换日期和时间过去之前，请勿删除现有验证证书。新的 Citrix Cloud 证书仅在两次通知中给出的日期和时间生效。

将替换的 Citrix Cloud SAML 签名证书上传到您的 Okta SAML 应用程序

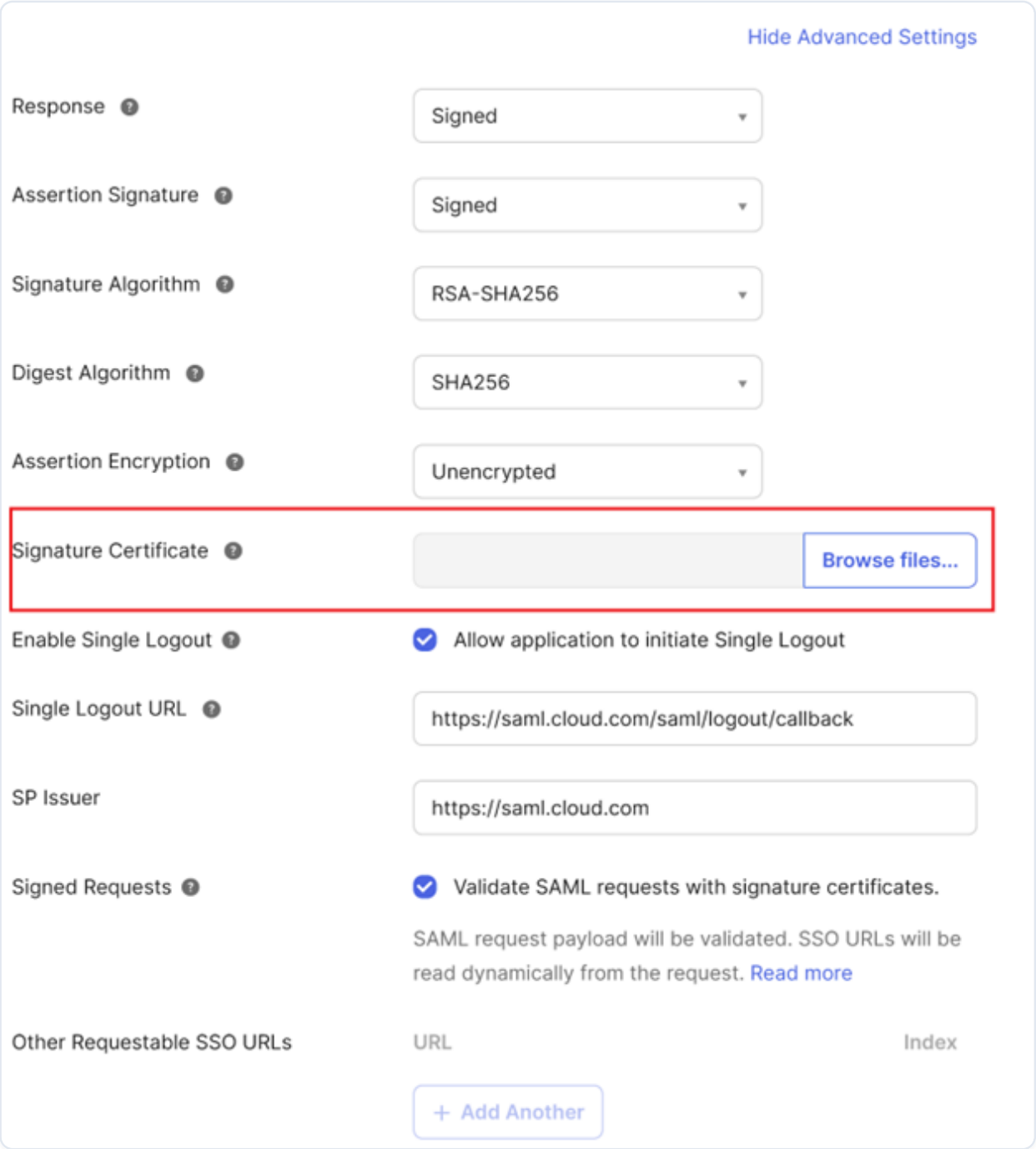
Okta 不支持同时使用多个 SP SAML 签名证书。您别无选择，只能用新证书覆盖当前正在使用的现有 Citrix Cloud SP 签名证书。建议您在计划的维护窗口中执行此操作。

1. 导航到 **应用程序**，选择 **应用程序** 并搜索您的 Okta SAML 应用程序



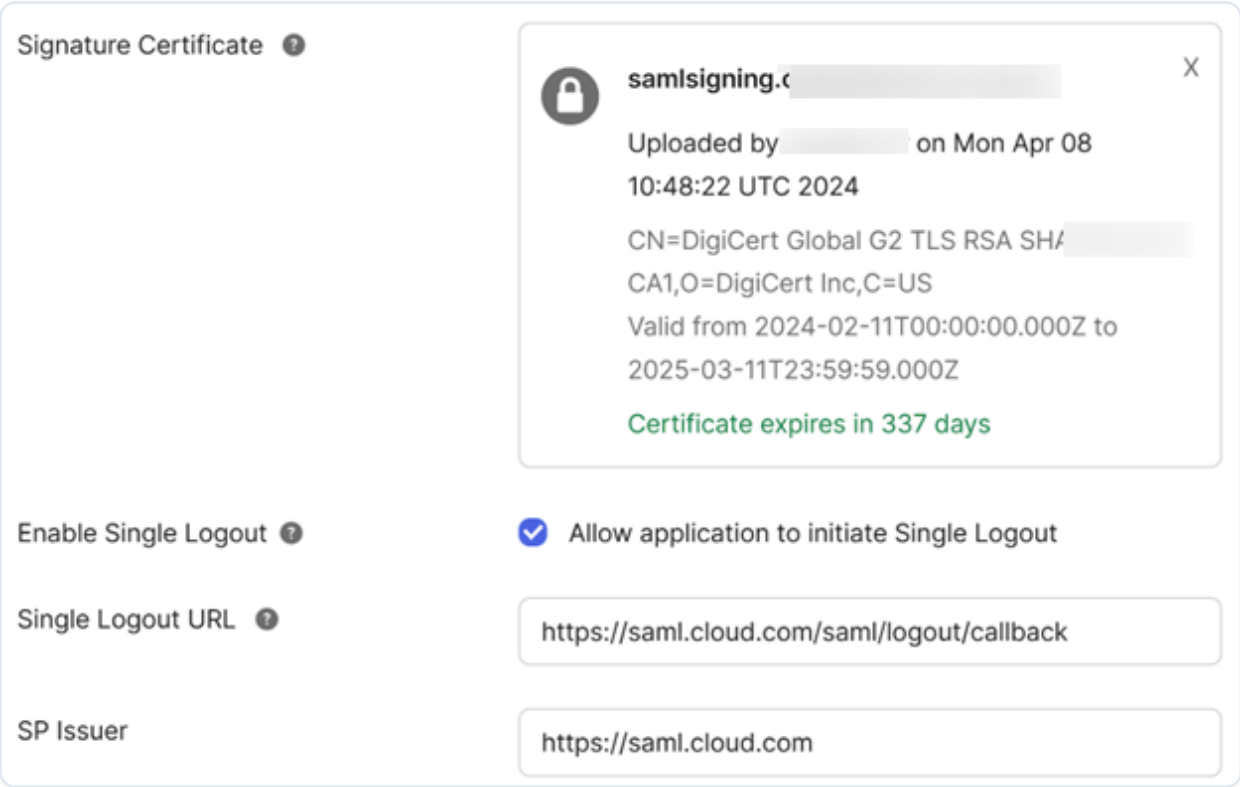
© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. 从 **常规** 导航到 **SAML 设置**，单击 **编辑**，选择 **配置 SAML**，选择 **显示高级设置**，然后单击 **签名证书** 以便上传替换证书。Okta 不会在上传 UI 中显示当前的 Citrix Cloud SAML 签名证书。它只会在上传替换证书后显示该证书。



3. 选择 **签名证书**，单击 **浏览文件** 并上传从 Citrix Cloud SAML 元数据中获取的替换 Citrix Cloud SAML 签名证书。

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



重要

在电子邮件和 Citrix Cloud 控制台通知中给出的 SAML 轮换日期和时间之前，请勿覆盖现有的验证证书。新的 Citrix Cloud 证书仅在这些通知中给出的日期和时间生效。

更新身份提供商 SAML 签名证书

使用签名请求和响应的 SAML 连接依赖于两种不同的 SAML 签名证书。SAML 连接的每一侧各一个。**IdP 证书轮换**过程不应与所有 Citrix Cloud 客户使用的 `samlsigning.cloud.com` 证书的 **服务提供商** 年度轮换混淆。Citrix 不控制您的 SAML 应用程序的 IDP 证书的轮换。您的 Citrix Cloud 和 IdP 管理员控制此过程。

常见问题

SAML 应用程序的签名证书用于什么?

当您首次创建 SAML 连接时，您的 SAML 应用程序的签名证书会上传到 Citrix Cloud。在初始 SAML 连接创建过程中，只需提供一个 IdP 签名证书。IdP 证书从您的 SAML 提供商（例如 Microsoft Entra ID、Okta、PingFederate 或 ADFS）中获取。Citrix Cloud 使用 IdP 签名证书来验证在 SAML 身份验证过程中从您的 SAML 应用程序发送到 Citrix Cloud 的 SAML 响应的签名。IdP 证书将受到 Citrix Cloud 的信任，直到其到期日期。

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

什么是 SAML 应用程序签名证书轮换?

IdP 签名证书轮换是一项计划性维护任务，当您的 SAML 应用程序的签名证书即将到期时需要执行。管理员需要关注 Citrix Cloud 中 SAML 连接使用的 IdP 签名证书。当证书在 30 天内即将到期时，请将有效的替换证书上传到您的 Citrix Cloud SAML 连接中。在当前证书到期之前完成此替换。

我需要多久轮换一次 SAML 应用程序的签名证书?

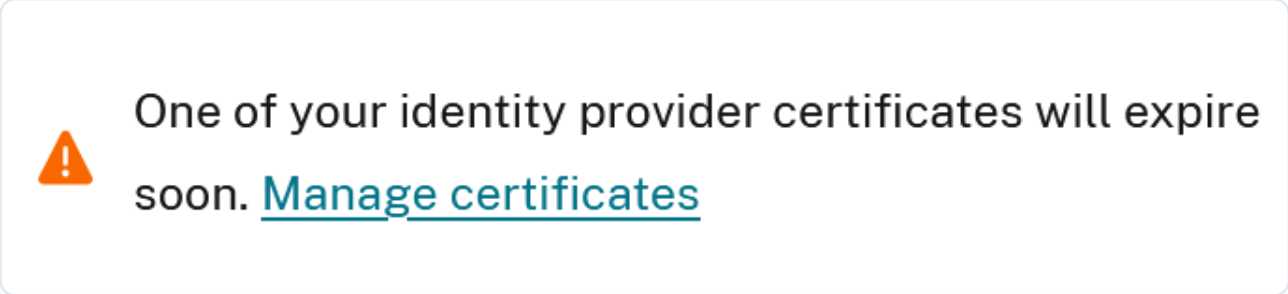
云 SAML 应用程序证书通常具有很长的生命周期，例如 Duo 为 16 年，Okta 为 10 年，Entra ID SAML 应用程序为 3 年。本地 SAML IdP（例如 PingFederate 或 ADFS）中使用的证书像您环境中的任何其他 x509 证书一样创建和维护，因此通常由 Digicert 等商业证书颁发机构每年替换。

我如何知道我的 SAML 应用程序的签名证书是否即将到期?

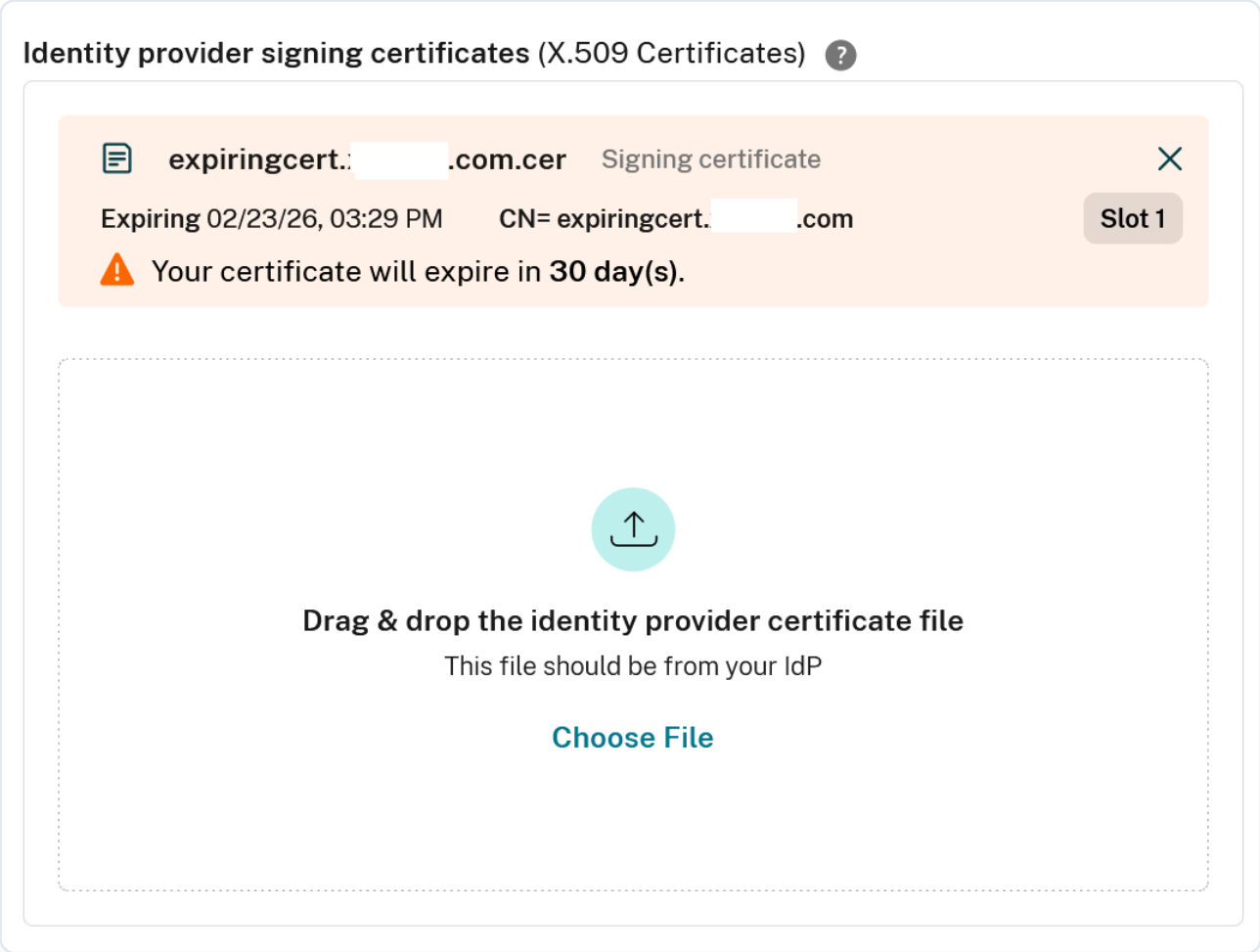
您需要检查您的 IdP 的 SAML 应用程序中当前活动的证书的到期日期。

在您的 SAML 应用程序签名证书到期前 30 天，Citrix Cloud 将在 **身份和访问管理 > 身份验证** 中的 SAML 连接上显示警告。

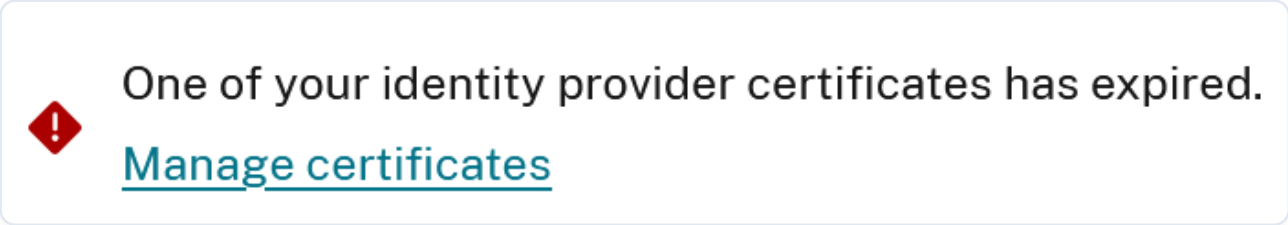
单击 **管理证书** 将重定向到 **查看 > SAML 连接** 页面，您可以在其中上传新证书或删除已过期证书。



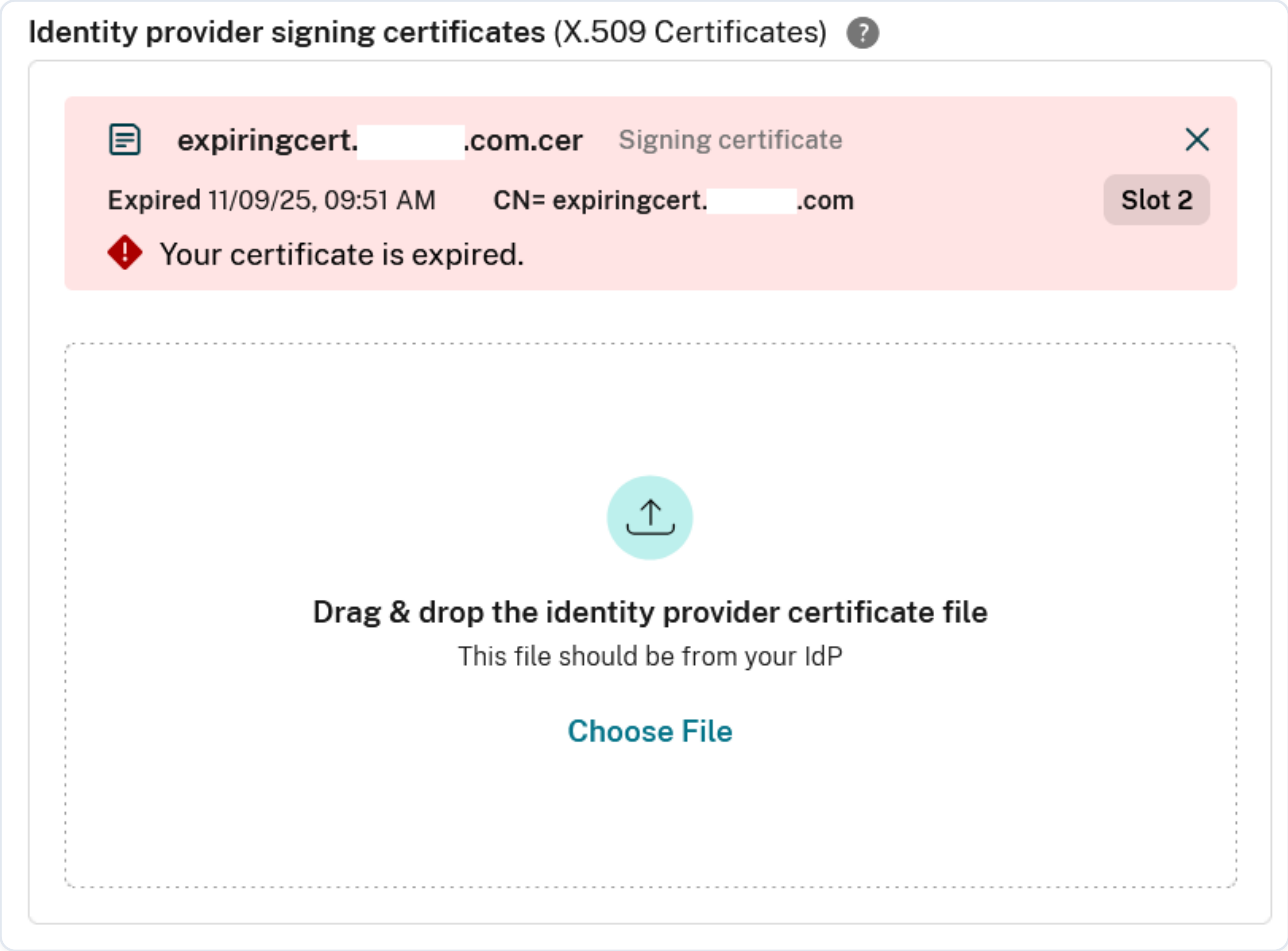
© 1997–2026 Citrix Systems, Inc. All rights reserved.



如果 IdP 证书实际上已过期，Citrix Cloud 也会在 SAML 连接上显示错误，如下所示。过期的 IdP 证书会使 SAML 连接无法使用，直到证书被替换。



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



当我的 SAML 应用程序的签名证书即将过期时，我将收到 Citrix Cloud 的哪些通知?

如果 Citrix Cloud 管理员有一个或多个 IdP 证书将在**未来 30 天内**过期的 SAML 连接，他们将收到**严重通知**。Citrix Cloud 会监控所有 SAML 连接，并检测任何包含将在未来 30 天内过期的证书的连接。除了来自 Citrix Cloud 租户的通知外，您还可能收到来自 SAML IdP 的关于即将过期的 SAML 应用程序证书的通知。

重要提示：

如果您的 Citrix Cloud 管理员选择禁用所有电子邮件和 Citrix Cloud 控制台通知，您可能会错过这些关键警告，因为您的 SAML IdP 证书即将到期。您的 Citrix Cloud 管理员有责任确保至少有一名或多名活跃管理员用户可以接收这些关键通知。请参阅本文，了解 Citrix Cloud 管理员如何管理其通知

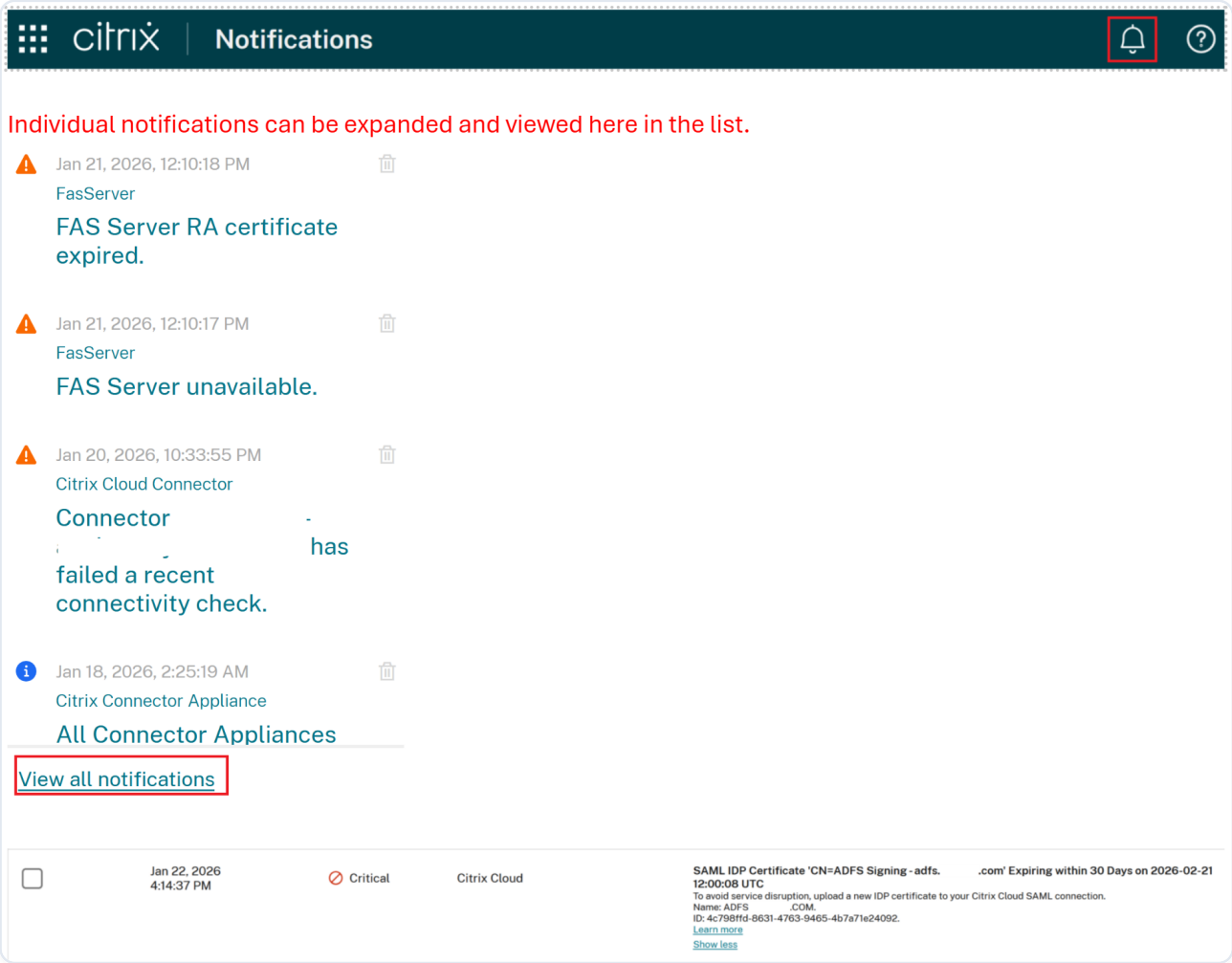
每个 IdP 证书过期通知都包含详细信息，可帮助您识别 Citrix Cloud 中的 SAML 连接以及身份提供商中即将过期的 IdP 证书。导航至**身份和访问管理 > 身份验证**。

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

- SAML 连接昵称：`ExpiringIdPCert`
- SAML 连接 ID：`e65e3d1d-f4fa-40f4-a53e-de84a270011c`
- 证书通用名称：`CN=expiringcert.domain.com`
- 过期日期：`2025-12-27`

CITRIX CLOUD 门户中的管理员通知

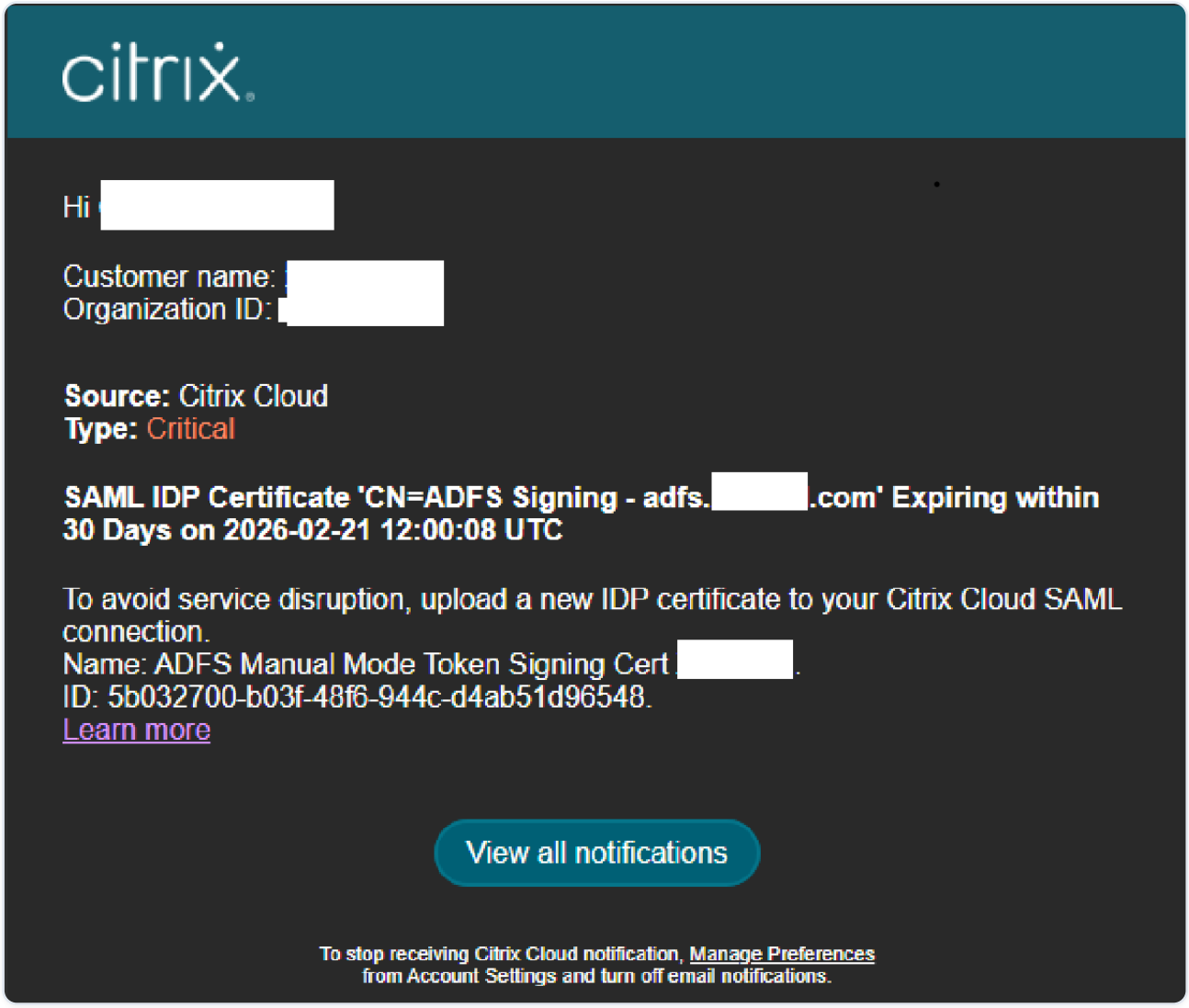
导航到 Citrix Cloud 主页，单击铃铛图标并选择“查看所有通知”。查找指示将在未来 30 天内过期的证书和 SAML 连接的关键警报。



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

电子邮件通知

一旦 IdP 证书过期通知已**发送一次**，它将不会再次发送。这是为了防止不必要的电子邮件垃圾邮件，并确保 Citrix Cloud 管理员只收到一次通知电子邮件，而不是在到期临近的整个 30 天内每天都收到另一封电子邮件。如果 Citrix Cloud 通知被关闭，它将不会被重新发送。



在不触发中断的情况下，我是否可以在仍使用 Citrix Cloud SAML 连接的同时更新 SAML IdP 证书?

是的。在 SAML IdP 连接中引入第二个 IdP 证书，可以实现无缝的 SAML 应用程序证书滚动更新。请在当前证书过期前**至少 24 小时上传新证书。如果正确遵循本文，您的最终用户或 Citrix Cloud 管理员用户将不会受到影响。**

如何从 SAML 应用程序获取最新的身份提供商 (IdP) 签名证书副本?

本地 SAML IdP（例如 PingFederate）中使用的证书可从组织内部的私有证书颁发机构或 Digicert 等商业证书颁发机构获取。基于云的 SAML IdP SAML 应用程序可以在 SAML 应用程序 UI 中随时按需生成新的 IdP 证书。新的 IdP 签名证书可以随时生成并设置为“非活动”状态。

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

Citrix Cloud 能否同时信任两个不同的 IdP 签名证书?

是的。无缝 IdP 证书滚动更新依赖于此。 Citrix Cloud SAML 连接信任 SAML 响应。这些响应必须使用已上传到 SAML 连接的两个受信任 IdP 签名证书中的任何一个进行签名。如果其中一个证书已过期，Citrix Cloud 将不再信任它，并且您的 SAML 应用程序也不应再使用它。

Citrix Cloud SAML 连接可以存储一个或两个 SAML 应用程序证书。

Slot1： 包含您在首次创建 Citrix Cloud SAML 连接时上传的证书。此证书需要在过期前更换，以防止中断。

Slot2： 在您的 SAML 连接创建后始终为空，但可以在 **Slot1** 中的证书过期前用于上传新的 SAML 应用程序证书。它旨在提供一个替代的受信任证书，以接替即将过期的 **Slot1** 签名证书。

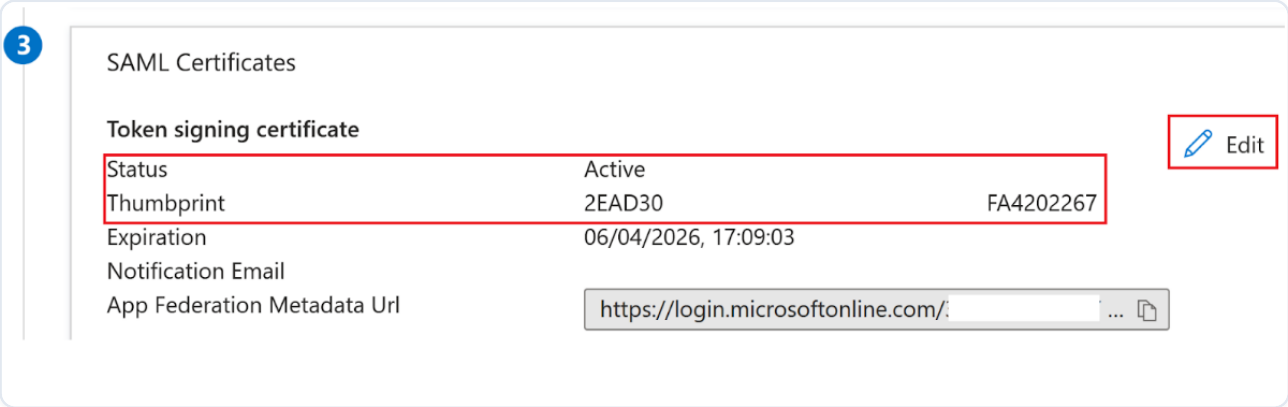
我应该何时从 Citrix Cloud 中的 SAML 连接中删除“旧”身份提供商 (IdP) 签名证书?

只有在您已证明“新”签名证书已在您的 SAML 应用程序中**激活**，并且您已成功使用它登录到商店和/或 Citrix Cloud **之后**，才能从 Citrix Cloud SAML 连接中删除**旧**身份提供商 (IdP) 签名证书。如果两个 IdP 证书都仍在 Citrix Cloud 连接中，则回滚失败的 IdP 证书轮换维护任务会更容易。只要两个证书都仍在有效期内，Citrix Cloud 就可以信任它们。如果 IdP 证书已过期，则无法回滚到该证书。

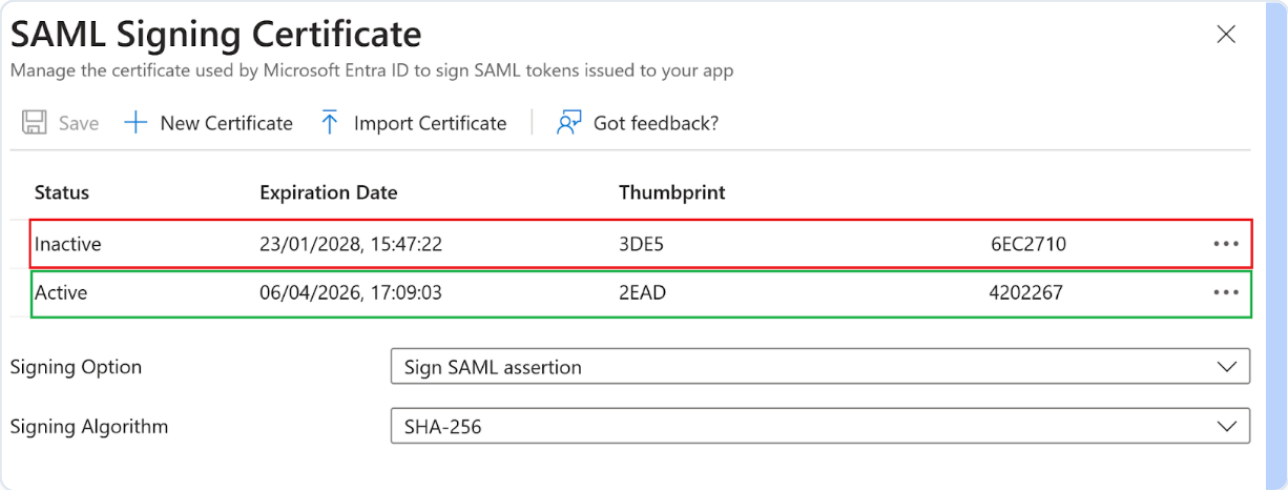
我如何知道我的 SAML 应用程序当前正在使用哪个 IdP 签名证书来签署 SAML 响应?

您的 SAML 应用程序一次只使用一个证书来签署 SAML 响应。它使用当前在您的 SAML 应用程序中设置为**活动**的证书。**活动**的 IdP 签名证书也存在于 SAML 应用程序元数据中。

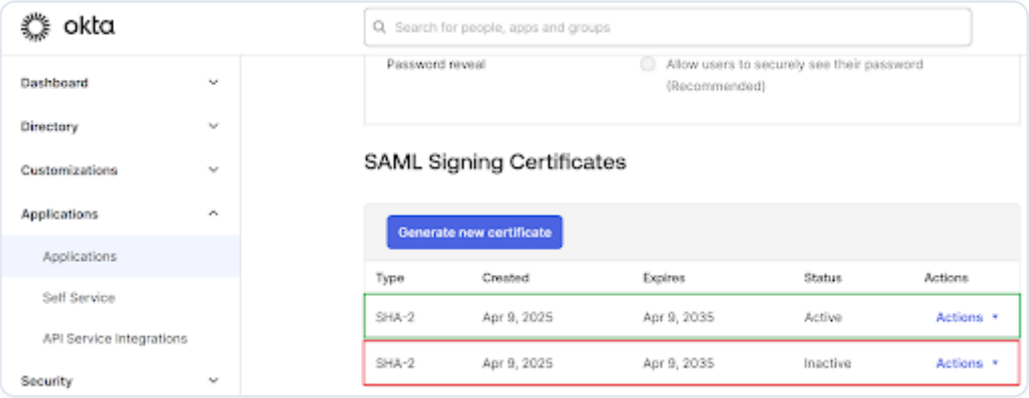
以下屏幕截图显示了 Entra ID 的示例。



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



以下屏幕截图显示了 Okta 的示例。



将 SAML 应用程序 IdP 证书轮换作为计划维护任务执行

重要提示：

您的 SAML 连接中至少有一个 IdP 证书必须在有效期内并在您的 IdP 中处于活动状态，以防止中断。如果您在 Citrix Cloud 证书中只配置了一个 IdP 证书，并且该证书过期，您的用户将遇到中断，并且您的 SAML 登录将失败。这种情况会影响商店用户和/或 Citrix Cloud 管理员用户，具体取决于您的 SAML 连接的使用方式。

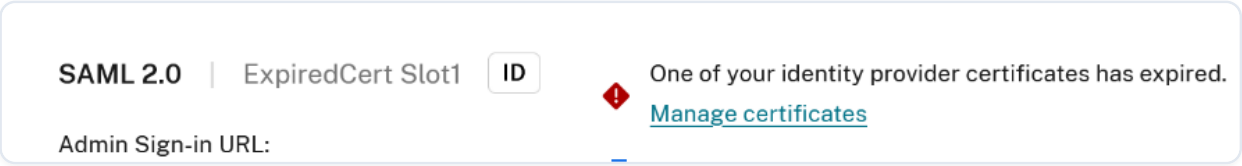
1. 计划在当前证书到期日期前几天执行 IdP 证书轮换。
2. 从您要轮换到的 SAML 应用程序中获取替换 IdP 证书的副本。确保 IdP 证书为 PEM、CER 或 CRT 格式，以便上传到您的 Citrix Cloud SAML 连接中。
3. 在您希望触发 SAML 应用程序中证书轮换之前，至少提前 24 小时将替换 IdP 证书上传到您的 Citrix SAML 连接中。

   导航到**身份和访问管理 > 身份验证**中的 SAML 连接。选择证书在未来 30 天内到期的 SAML 连接上的三个点，然后单击**查看**。

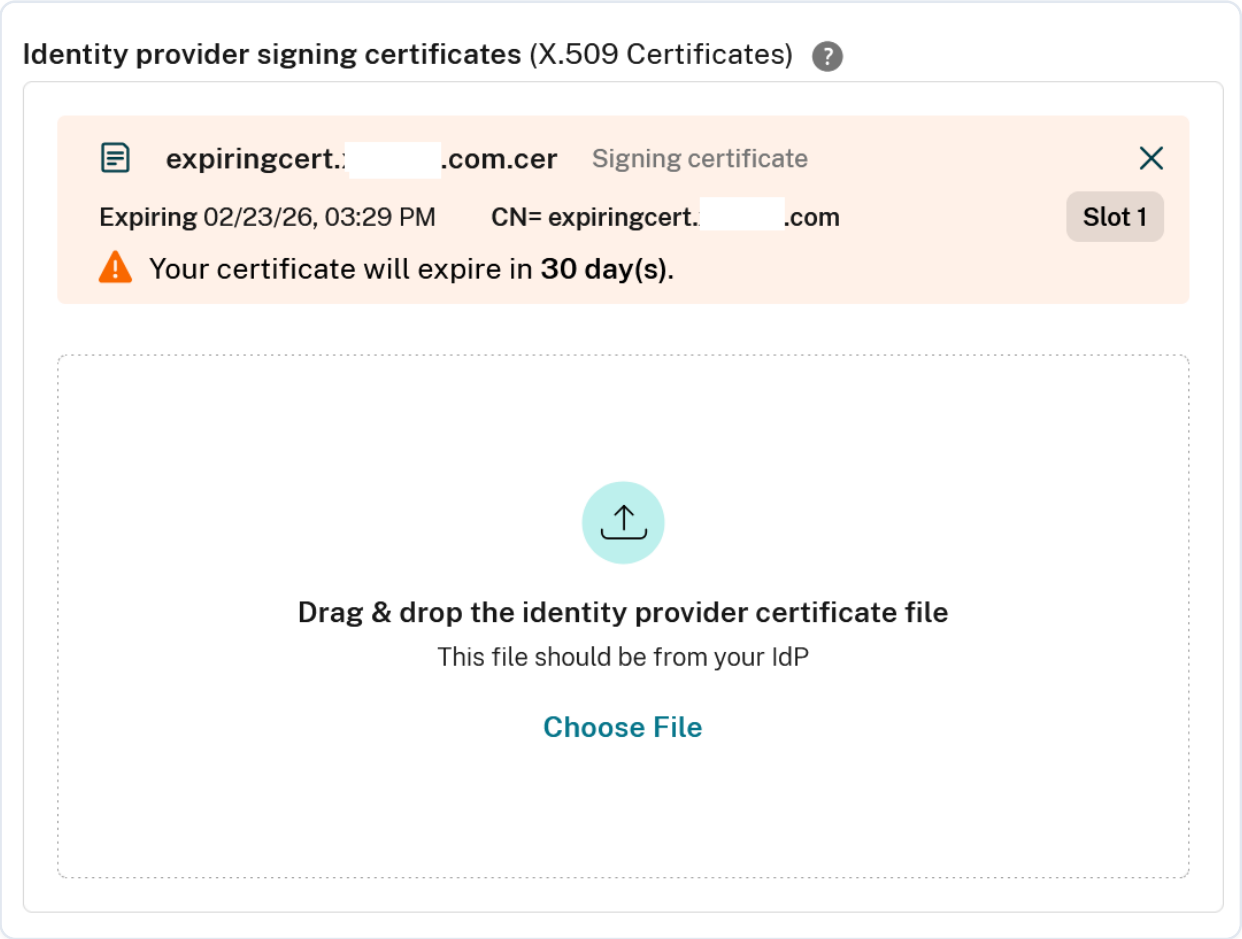
© 1997–2026 Citrix Systems, Inc. All rights reserved.

或者，

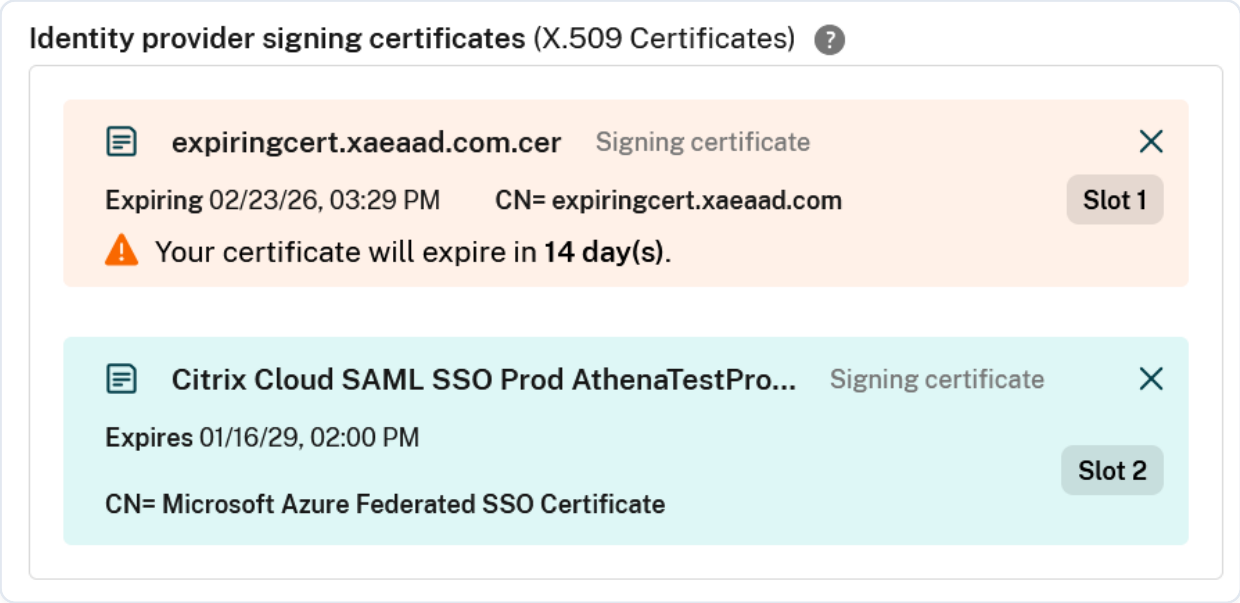
单击**管理证书**。



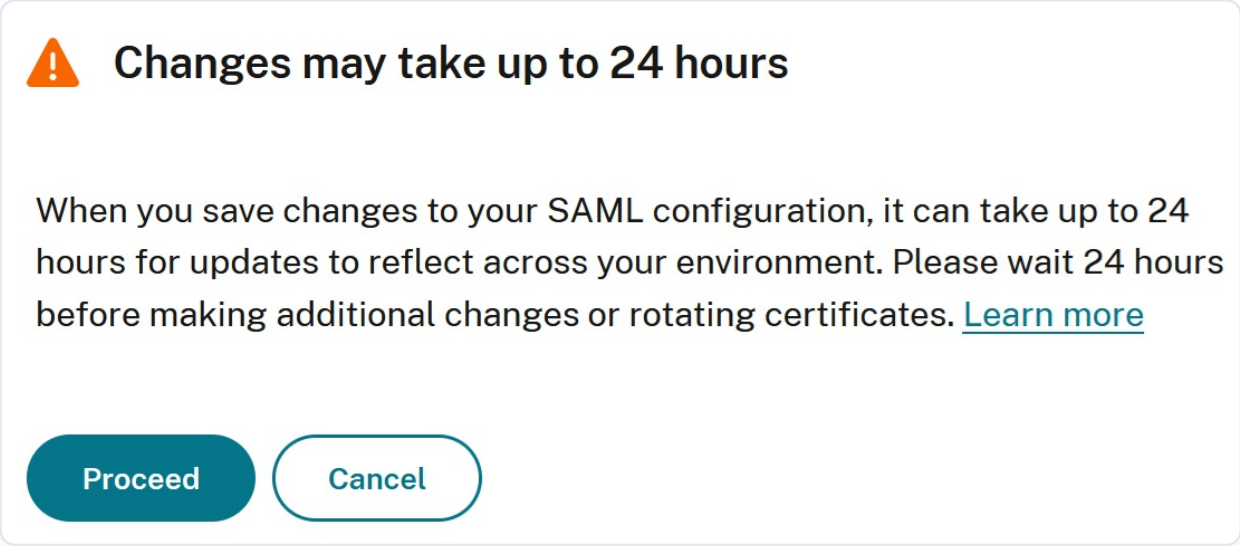
4. 使用 Citrix Cloud SAML 连接中的 **Slot2** 上传选项上传第二个 IdP 证书。



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



5. 上传新证书后，保存 SAML 连接。

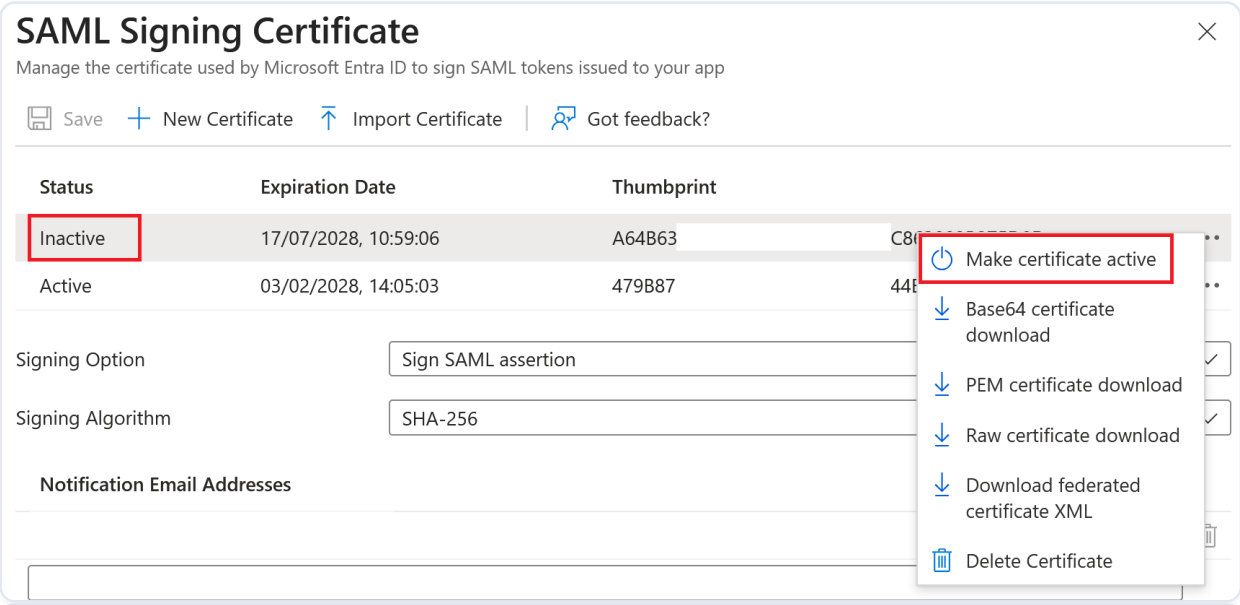


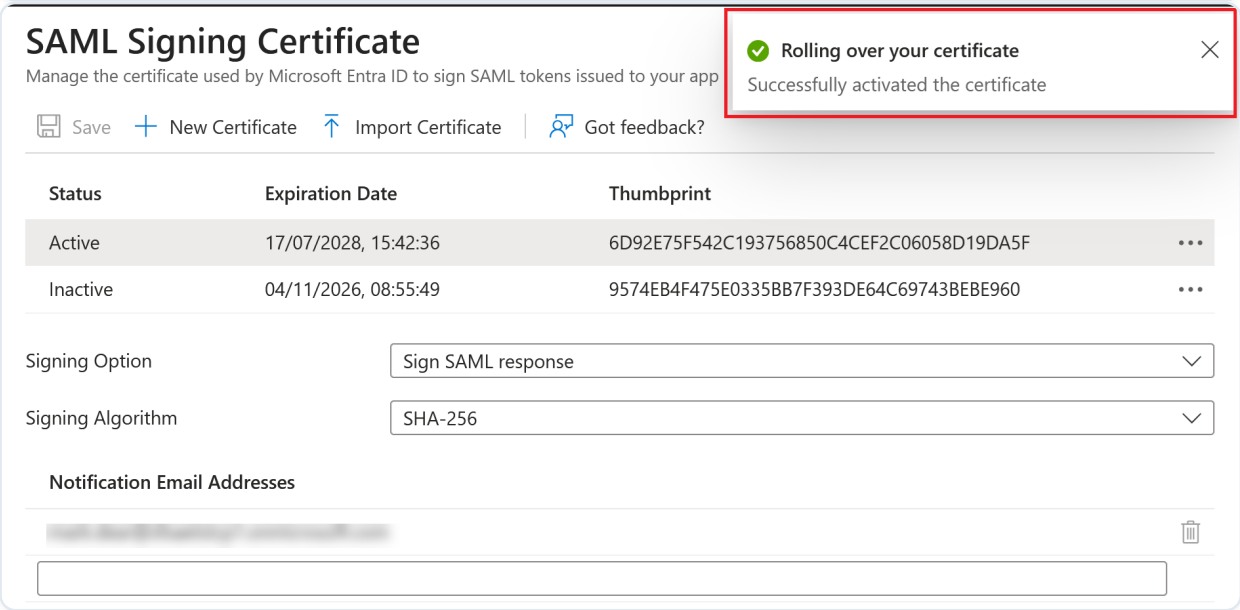
6. **等待大约 24 小时**，然后在您的 IdP 中执行**滚动更新操作**，并将辅助 IdP 证书设置为**活动**状态。每个 SAML IdP 滚动更新证书的方法都不同。

> **重要提示：**
>
> 出于弹性与性能考虑，Citrix 的身份验证平台会对所有 IDP 设置进行缓存。由于缓存值的原因，您无法将替换证书上传到 Citrix Cloud，然后立即在 SAML 应用程序中轮换证书。在新证书上传和在 SAML 应用程序中激活新证书之间需要一个延迟。此延迟允许 Citrix 身份验证缓存使用新上传的证书进行更新。24 小时的延迟比缓存的 TTL 值更长。此持续时间可确保当 SAML 应用程序在第二天切换使用新证书时，新证书可用。

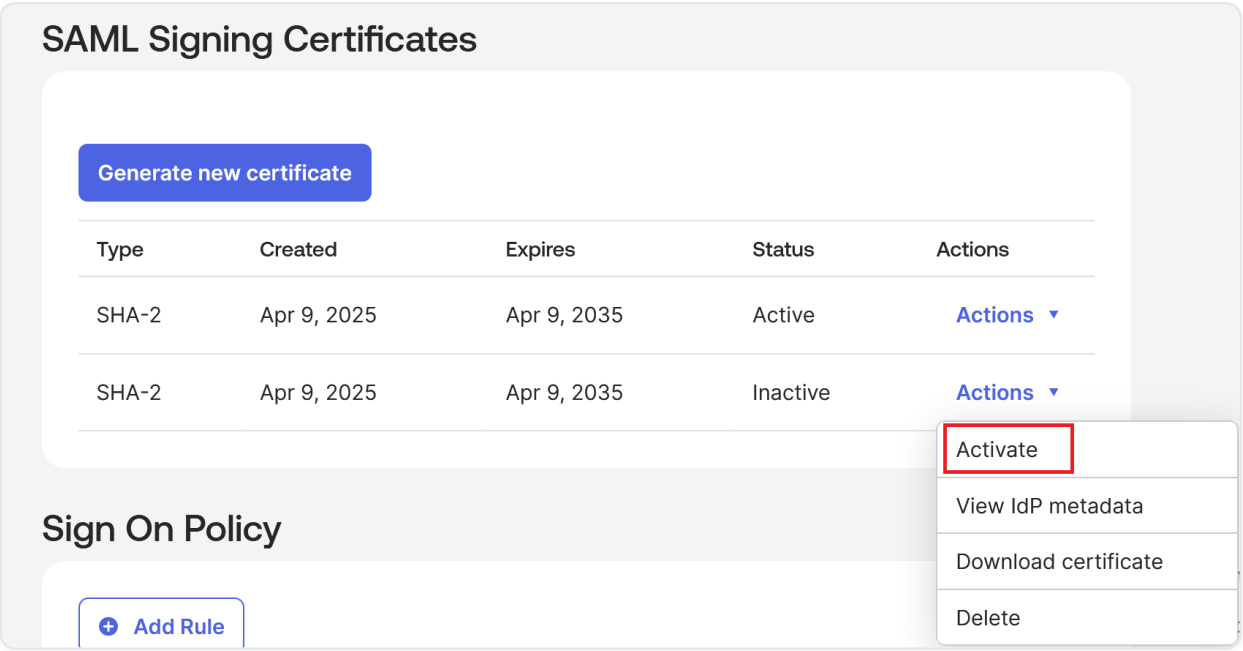
Entra ID SAML 应用程序：

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





Okta SAML 应用程序：



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

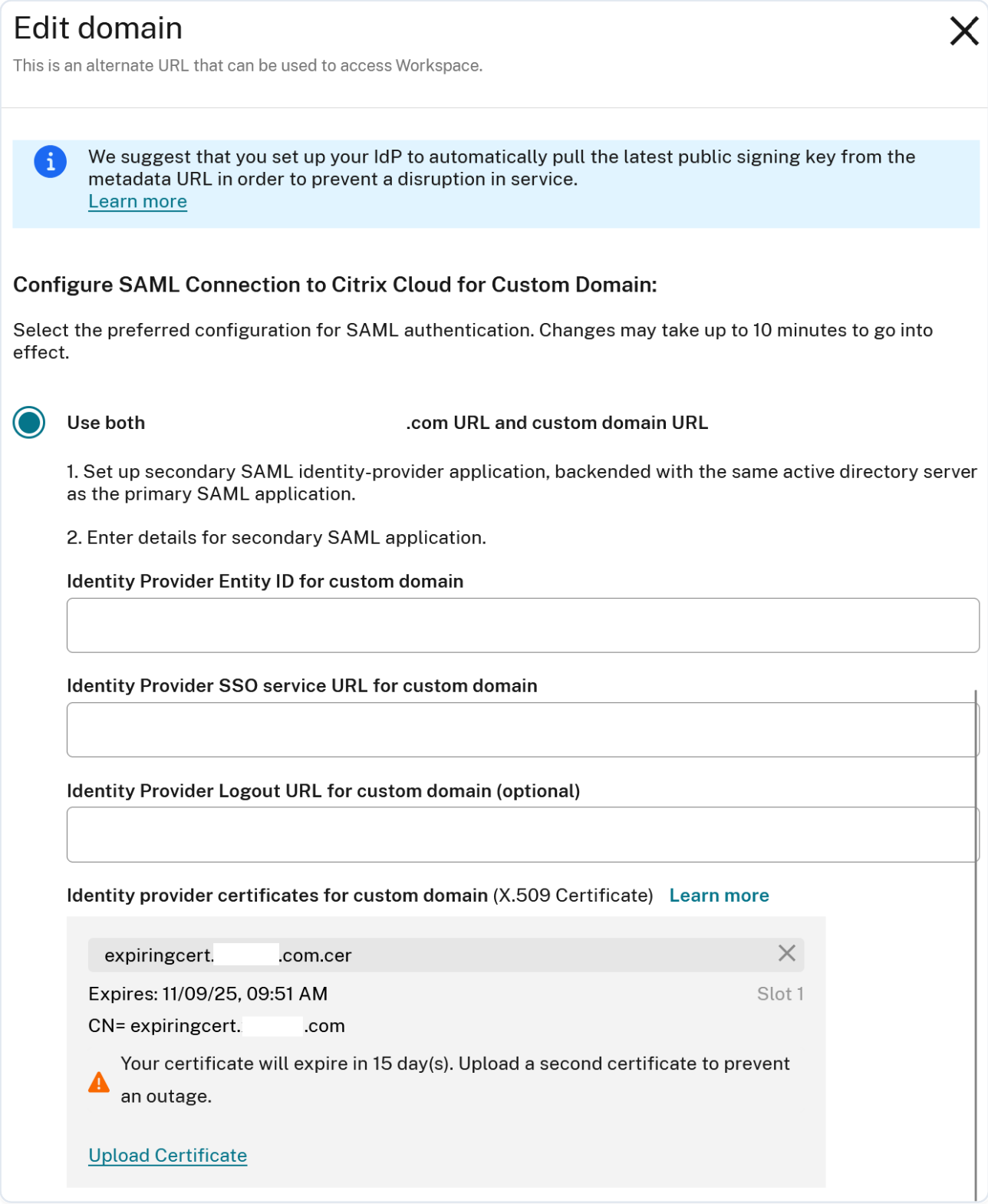
7. 测试 SAML 登录是否成功，可以使用您的商店 URL 和/或 Citrix Cloud SAML 登录 URL，并检查 SAML 断言中签名证书的值。

将辅助 SAML IdP 证书上传到现有商店自定义域 SAML 连接?

如果您需要更新由配置为支持商店自定义域的辅助 SAML 应用程序使用的 IDP 证书，请遵循上述文档中的相同步骤。

1. 导航到 **StoreFront Cloud > 访问 > 自定义商店 URL > 选择 3 个点 > 编辑**。

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



IDP 签名证书轮换故障排除

如果在执行 IdP 证书轮换后遇到任何 SAML 登录问题，请收集 SAML 跟踪器文件并检查 SAML 响应中的证书 base64 数据。

1. 在浏览器中输入商店 URL 或 Citrix Cloud GO URL **之前**开始 SAML 跟踪器捕获。确保从头到尾捕获整个身份验证过程。

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

2. 使用您的 IdP 执行 SAML 登录到商店或 Citrix Cloud，并在系统提示您输入凭据时完成身份验证步骤。
3. 找到您的 IdP 发送到 Citrix Cloud SAML 端点的 SAML 响应 `https://saml.cloud.com/saml/acs` 以及 SAML 跟踪器文件中的条目。

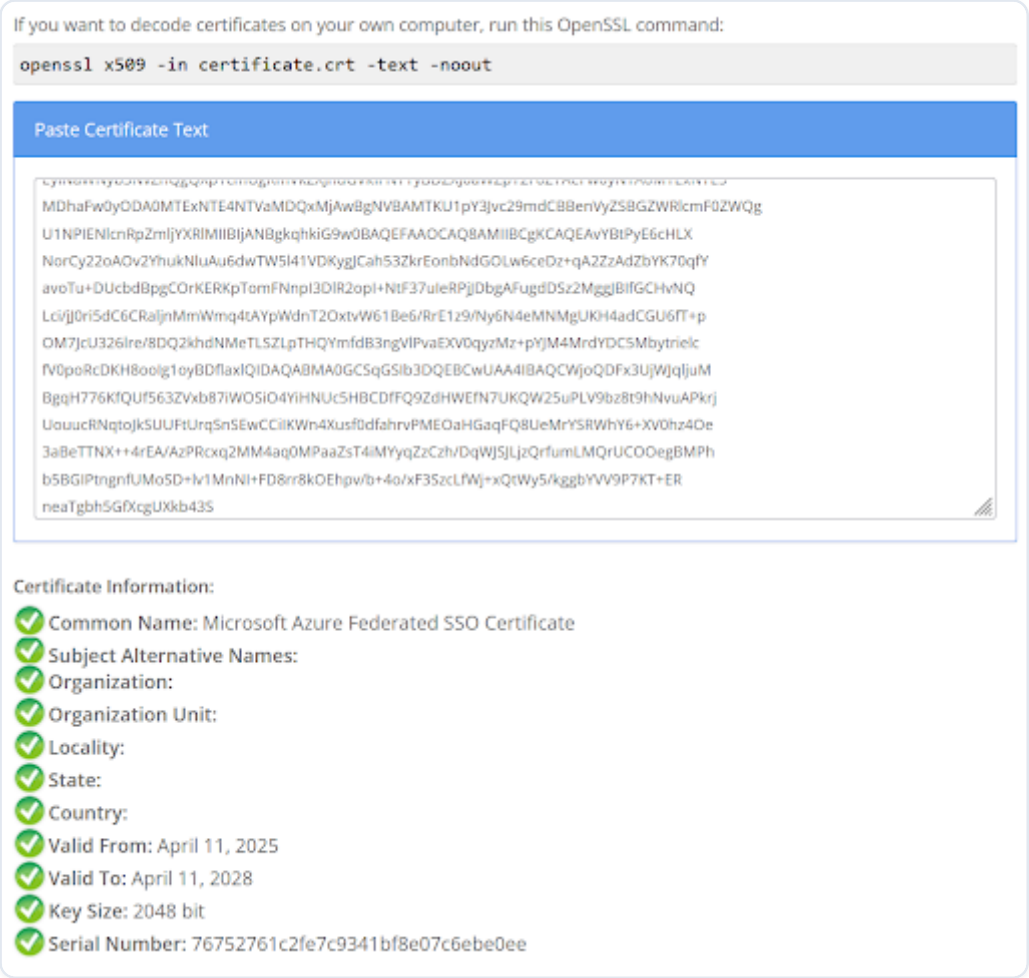
4. 在 SAML XML 中找到证书部分，并将 IDP 签名证书的 base64 数据复制到合适的工具进行解码。

重要提示：

此步骤假设您已遵循 Citrix 的 SAML 推荐配置，并在您的 Citrix Cloud SAML 连接中使用了 HTTP POST 作为 SAML 绑定。

5. 从其base64数据解码证书，并检查它是否与SAML IdP中的活动证书相对应，具有正确的日期和时间。

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



6. 如果从步骤 4 和 5 中的 SAML 响应获得的证书不符合预期，请在您的 IdP 中激活正确的证书。检查您的 SAML 应用程序中的活动证书。此证书包含在 SAML 响应中。

高级 SAML 场景以及在 SAML 断言中正确使用 cip_forest 和 cip_domain

本文介绍了涉及多个连接的 Active Directory 林和域的 Citrix Cloud 或 Storefront 高级 SAML 配置。本文适用于具有复杂 AD 部署的大型企业，应由架构师级别的 Citrix Cloud、IdP 和 AD 管理员实施。此高级 SAML 配置最常见的用途是在并购场景中，其中大型企业由许多具有不同 AD 基础架构、多个林以及具有不同 UPN 的不同 AD 后端用户群体的较小组织组成。在并购场景中，通常还需要条件身份验证。

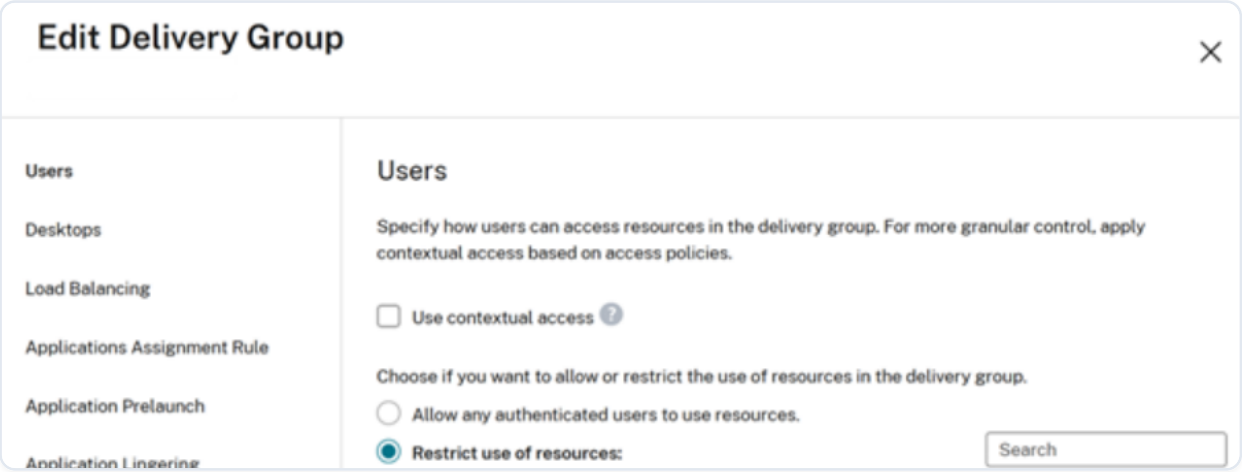
可选的 cip_forest 和 cip_domain 声明使 Citrix Cloud 管理员能够更好地控制在 SAML 身份验证期间使用哪些 Citrix Cloud Connector 来查找 AD 后端用户帐户。Citrix Cloud 与 SAML 支持许多高级帐户映射用例，而其他 Citrix Cloud 联合 OIDC 身份验证方法（例如 Okta IdP 或 Entra ID IdP）无法实现这些用例。

先决条件

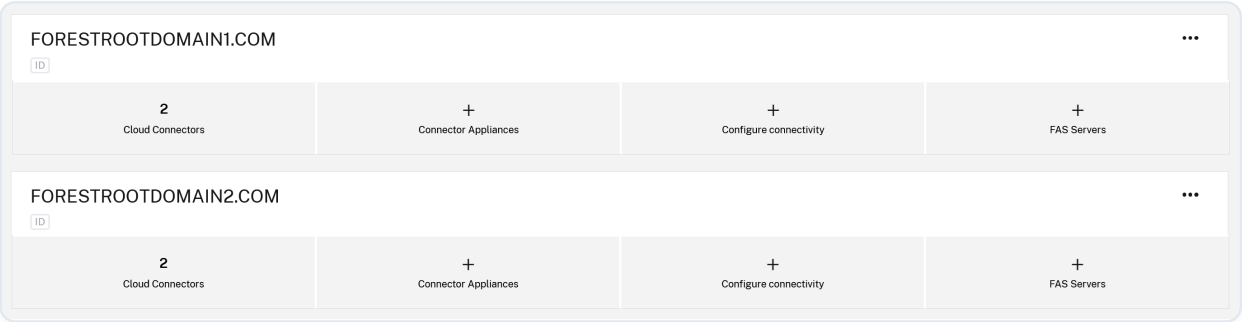
- 使用默认的 Citrix Cloud SAML 流程，该流程使用 AD 身份验证最终用户。
- 全面了解您的 AD 林或域基础架构以及您的 Storefront 最终用户身份所在的位置。

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

- Citrix Cloud Connector 已加入正确的 AD 林和域，并已在正确的 AD 域级别加入。
- 了解您的 Citrix Cloud 租户中已配置的现有资源位置和 Citrix Cloud Connector。
- 连接到 Citrix Cloud 的多个 AD 林之间不应存在任何 Active Directory 信任关系。
- 了解前端（Entra ID、Okta、Duo）和后端用户 (AD) 身份的含义。
- 前端和后端用户身份必须通过匹配的 UPN 进行链接。不支持链接一对 UPN 不匹配的前端和后端用户身份。
- 了解每个 UPN 后缀在 Active Directory 中的位置，以及特定 UPN 后缀是否模糊不清并存在于多个连接的 AD 林中。
- DaaS VDA 应加入 AD 域。
- DaaS 应用程序和桌面应发布到 AD 身份。
- 在 DaaS 中将交付组资源映射到 AD 组时，通用 AD 组是强制性的。
- DaaS 交付组必须设置为“限制资源使用”，并且应分配给正确的通用 AD 组。DaaS 交付组中不支持使用“允许任何经过身份验证的用户使用资源”。



- FAS 服务器已加入正确的 AD 林，并在正确的 AD 级别加入域。在 DaaS 启动期间，SSON 到已加入 AD 域的 VDA 需要 FAS 服务器。



- 如果您有多个 SAML 应用程序，并且每个连接的 AD 林需要一个 SAML 应用程序，则可能还需要实施条件身份验证。在并购场景中，每个 SAML 应用程序可能需要为 cip_forest 和 cip_domain 提供一组不同的值。

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

常见问题

如果我在 SAML 断言中发送 cip_sid，是否还需要发送 cip_forest 和 cip_domain 可选声明?

不需要。如果您的 SAML 应用程序配置为发送 cip_sid 声明并将其包含在 SAML 断言中，那么 Citrix Cloud 将始终能够正确识别 AD 后端用户所在的林和域。cip_forest 和 cip_domain 不是必需的。

重要提示：

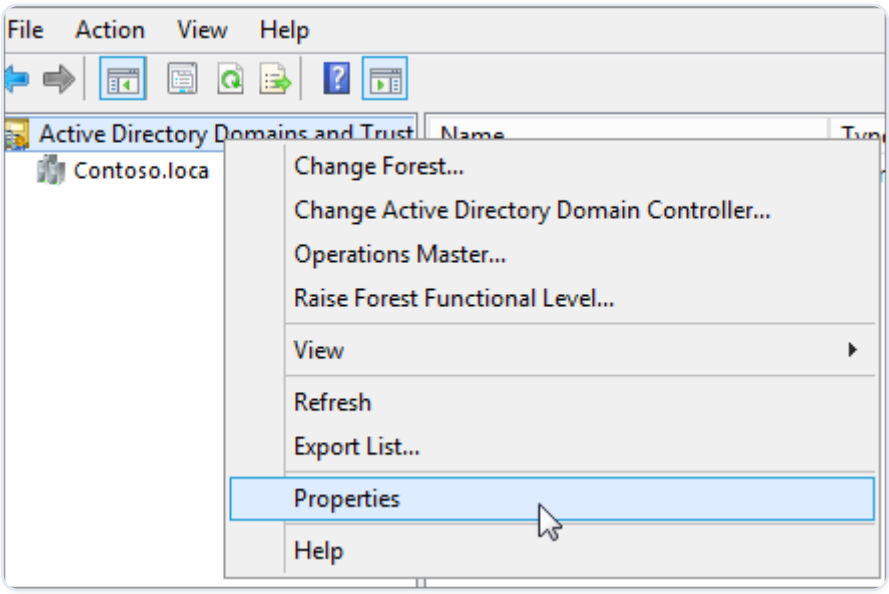
- 在 SAML 断言中无法发送 cip_sid 的 SAML 场景，可能需要改用 cip_forest 和 cip_domain。
- 包含不正确 SID 的前端用户，该 SID 与 DaaS 交付组中映射的后端 AD 用户的 SID 不匹配。
- 根本没有嵌入 SID 的前端用户，例如未通过 AD 导入工具在 IdP 内部创建的本机 Okta、Entra ID 或 Duo 用户。

什么是 AD 隐式 UPN 后缀?

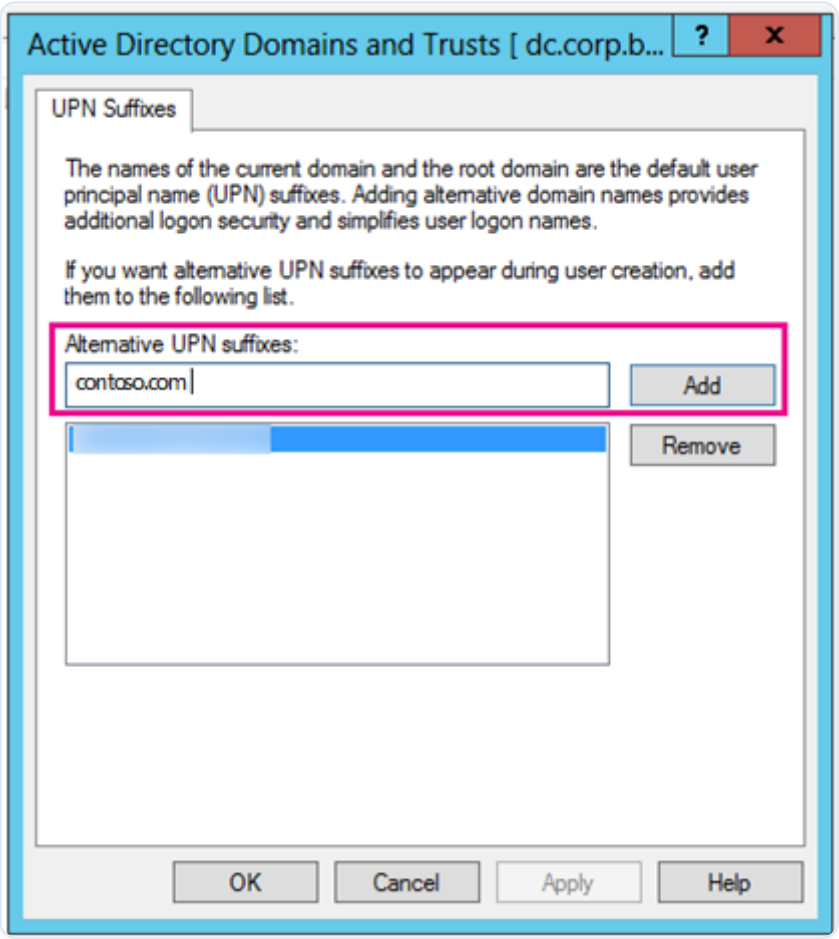
隐式 UPN 由 Active Directory 自动创建，并基于用户的 sAMAccountName 和林的 DNS 名称。隐式 UPN 在 AD 林中始终是唯一的，因为它们派生自 sAMAccountName 和域的 DNS 名称，而这些在 AD 林中是唯一的。例如 `@rootforestdomain.local`

什么是 AD 显式 (ALT) UPN 后缀?

显式 UPN 后缀是 AD 管理员在 Active Directory 域和信任中添加的自定义域名。例如 `@rootforestdomain.local`



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



重要提示：

Windows AD PowerShell 允许您创建具有任何指定 UPN 后缀的 AD 用户，即使该 UPN 后缀不存在于您的 AD 林中。您要使用的备用 UPN 后缀必须存在于 AD 林中，因为 Citrix Cloud Connector 依赖此列表来查找后端帐户用户。如果备用 UPN 后缀未按上述屏幕截图所示在 AD 林中配置，则 Citrix Cloud 将无法将您的前端身份与适当的后端 AD 帐户匹配。

什么是 UPN 歧义？为什么它会给 Citrix Cloud 和 DaaS 带来问题?

UPN 歧义是指当 `duplicateuser@domain.com` 存在于连接到 Citrix Cloud 的 2 个或更多 AD 林中时可能出现的情况。当存在两个版本的 `duplicateuser@domain.com` 时，仅凭 UPN 后缀 @domain.com 无法确定正确的 AD 后端用户。这可能导致 DaaS 资源完全无法枚举，或者使用已加入 AD 域的 VDA 发布的错误 DaaS 资源可能会显示在商店中。

为什么通用 AD 组是必需的?

通用 AD 组存储在全局编录 (GC) 中，使其对整个林中的所有域控制器可见。这使得它们可以用于向同一林中任何域中的资源分配权限。

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

重要提示：

使用 AD 通用组是所有 SAML 配置的要求，而不仅仅是涉及 cip_forest 和 cip_domain 的高级配置。使用其他 AD 组类型（例如全局组）可能导致商店中的资源枚举失败。

建议您阅读这篇关于 AD 组范围的 Microsoft 文章。

为什么不建议在 DaaS 交付组中使用“允许任何经过身份验证的用户使用资源”?

配置**允许任何经过身份验证的用户使用资源**将导致使用已加入 AD 域的 VDA 发布的资源在商店中显示给不在同一域和林中的 AD 用户身份。使用林 1 中的商店 AD 最终用户身份从林 2 中已加入域的 VDA 启动资源将不会成功。

在 SAML 断言中单独发送 cip_forest 或 cip_domain?

不。如果您想为后端用户查找指定特定的 AD 林和域上下文，则必须在 SAML 断言中提供这两个可选声明。

为 cip_forest 指定值时应使用的 UPN 后缀?

应使用 AD 林的隐式 UPN 后缀。请勿在 cip_forest 声明中指定已添加到 AD 林的 ALT UPN 后缀的值。这是因为在某些 AD 拓扑中，相同的 ALT UPN 后缀可能已添加到连接到 Citrix Cloud 的多个 AD 林中。隐式 UPN 后缀和 DN 对 Citrix Cloud 来说永远不会模棱两可，除非两个具有相同 DN（例如 DC=duplicate,DC=com）的不同 AD 林连接到 Citrix Cloud（这种情况不太可能发生）。

cip_forest 和 cip_domain 的值何时应该相同或不同?

场景 1： 您的 Citrix Cloud Connector 在林根级别加入域，并且后端 AD 帐户用户位于连接的 AD 林中的根域内。

cip_domain 和 cip_forest 应具有相同的值。

cip_forest = "forestrootdomain.com"

cip_domain = "forestrootdomain.com"

场景 2： 您的 Citrix Cloud Connector 加入了 AD 林层次结构中的子域。后端 AD 用户存在于您的 AD 林中的“childdomain.forestrootdomain.com”内。

cip_domain 和 cip_forest 应具有不同的值。

cip_forest = "forestrootdomain.com"

cip_domain = "childdomain.forestrootdomain.com"

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

我可以在 SAML 断言中硬编码 cip_forest 和 cip_domain 的值吗?

可以，但前提是所有映射到 DaaS 资源的后端 AD 用户都位于同一个 AD 林中。硬编码 cip_forest 和 cip_domain 的值要求每个前端用户在同一个 AD 林和域中拥有其对应的后端 AD 帐户。

我可以在 SAML 断言中动态指定 cip_forest 和 cip_domain 的不同值?

可以，如果您的 SAML 提供程序通过声明转换规则允许这样做。如果您有不同 UPN 后端用户群，则可以使用组员身份等切换条件动态指定 cip_forest 和 cip_domain 的值。这在 Entra ID SAML 应用程序中是可能的，在支持声明转换规则的其他 SAML IdP 中也可能实现。

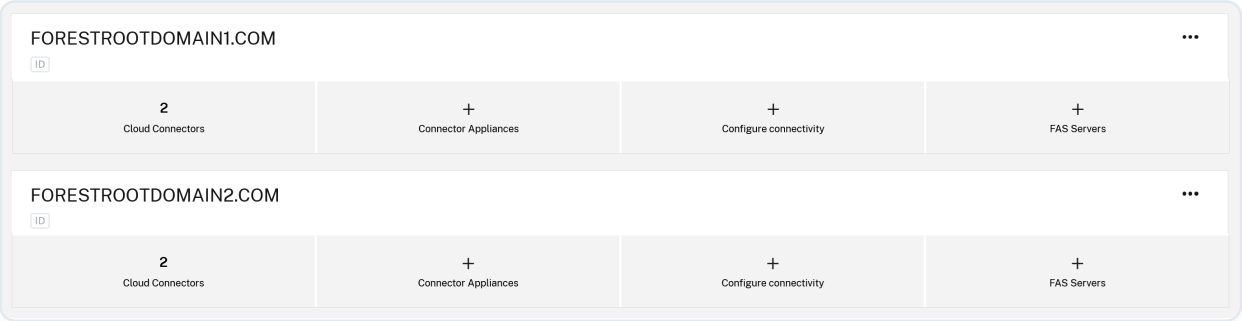
我应该将 FAS 服务器放在哪里，才能成功启动到已加入 AD 域的 VDA 的 SSON?

FAS 服务器应加入域，并在后端 AD 帐户所在的每个后端 AD 林中进行配置。建议您在 AD 林根域级别将 FAS 服务器加入域。

在 SAML 断言中需要 cip_forest 和 cip_domain 的 AD 拓扑

场景 1：SAML 最终用户的 UPN 模糊不清，并且存在于连接到 Citrix Cloud 的多个 AD 林中

- Citrix Cloud 租户有两个或更多资源位置，以及连接到 Citrix Cloud 的多个 AD 林或域。



- ResourceLocation1 包含 Citrix Cloud Connector，这些连接器已在根林级别加入 AD forestrootdomain1.com 域。
- ResourceLocation2 包含 Citrix Cloud Connector，这些连接器已在根林级别加入 AD forestrootdomain2.com 域。
- forestrootdomain1.com 和 forestrootdomain2.com 都具有相同的 UPN @domain.com 后缀。
- forestrootdomain1.com 和 forestrootdomain2.com 内部也可能存在具有相同 UPN `duplicateuser@domain.com` 但 SID 和 OID 值不同的重复用户。

问题：由于 UPN 模糊性，尝试使用 `username@duplicatesuffix.com` 查找正确的后端 AD 帐户并不总是返回正确的 AD 后端用户。Citrix Cloud 无法确定要使用哪个 AD 林和 Citrix Cloud Connector，因此商店中可能会显示错误的 DaaS 资源，或者根本不返回任何 DaaS 资源。

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

解决方案：配置两个不同的 SAML 应用程序，每个连接的 AD 林一个，并在 SAML 断言中包含正确 AD 林的相应 cip_domain 和 cip_forest 值。这为 Citrix Cloud 提供了额外的林和域上下文，以确保当 `username@duplicatesuffix.com` 存在于多个连接的林中时，能够“查找”到正确的后端 AD 用户。

SAML 应用程序 1 forestrootdomain1.com：

2

Attributes & Claims

cip_upn	user.localuserprincipalname
displayName	user.displayname
givenName	user.givenname
familyName	user.surname
cip_domain	"forestrootdomain1.com"
cip_forest	"forestrootdomain1.com"
Unique User Identifier	user.userprincipalname

SAML App 2 forestrootdomain2.com：

2

Attributes & Claims

cip_upn	user.localuserprincipalname
displayName	user.displayname
givenName	user.givenname
familyName	user.surname
cip_domain	"forestrootdomain2.com"
cip_forest	"forestrootdomain2.com"
Unique User Identifier	user.userprincipalname

使用正确的 AD 后端组正确映射两个 DaaS 交付组。

场景 2：云连接器在子域级别加入，并将用户存储在子域级别

Citrix Cloud 租户有一个资源位置，其中包含两个 Citrix Cloud Connector，它们在“childdomain.forestrootdomain.com”级别而不是推荐的“forestrootdomain.com”级别加入域。存储用户存在于 childdomain.forestrootdomain.com 子域中。用户配置为使用根域 UPN 后缀，例如 `username@forestrootdomain.com`。

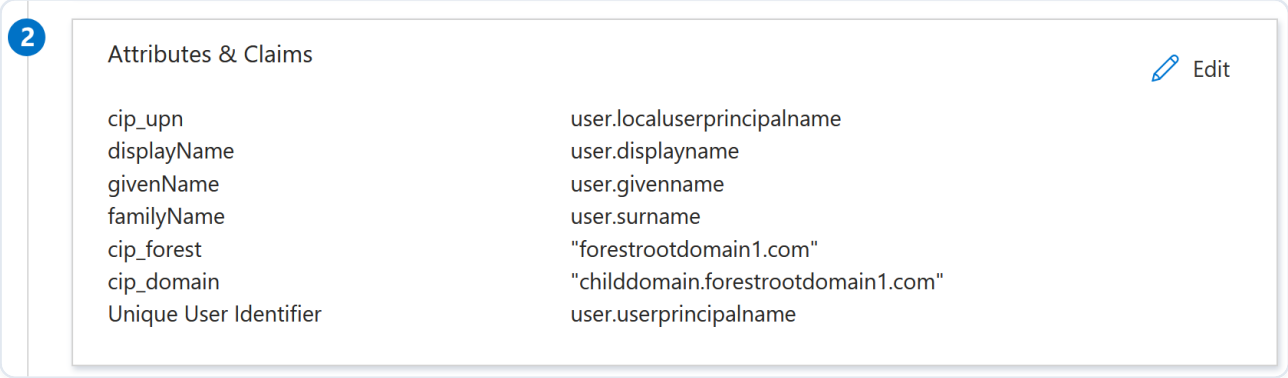
问题： Citrix Cloud 使用“forestrootdomain.com”执行 AD 帐户查找，但这与连接的 AD 域不匹配。

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

解决方案： 在 SAML 断言中指定子域上下文，以便从正确的 AD 子域和林上下文“查找”AD 帐户用户。

cip_forest = `forestrootdomain.com`

cip_domain = `childdomain.forestrootdomain.com`



将 ADFS 配置为商店身份验证的 SAML 提供程序

本文介绍如何配置 Citrix Cloud™ 使用 SAML 登录商店或 Citrix Cloud 所需的信赖方信任。

完成本文中的步骤后，您可以按照 (/zh-cn/citrix-cloud/citrix-cloud-management/identity-access-management/saml-identity.html) 中所述，配置 ADFS 服务器与 Citrix Cloud 之间的 SAML 连接。有关为 SAML 连接输入正确的 ADFS 值的指导，请参阅本文中的 (#saml-configuration-in-citrix-cloud)。

先决条件

本文中的说明假定您的环境中已部署运行中的 ADFS 服务器，并集成了 Citrix FAS。Citrix FAS 是在会话启动期间向 VDA 提供单点登录所必需的。

有关详细信息，请参阅以下文章：

- Citrix FAS 文档：
  - (/zh-cn/federated-authentication-service/current-release/install-configure.html)
  - (/zh-cn/federated-authentication-service/current-release/deployment-architectures/adfs)
- Citrix 技术专区：参考架构：联合身份验证服务

为 Citrix Cloud 配置信赖方信任

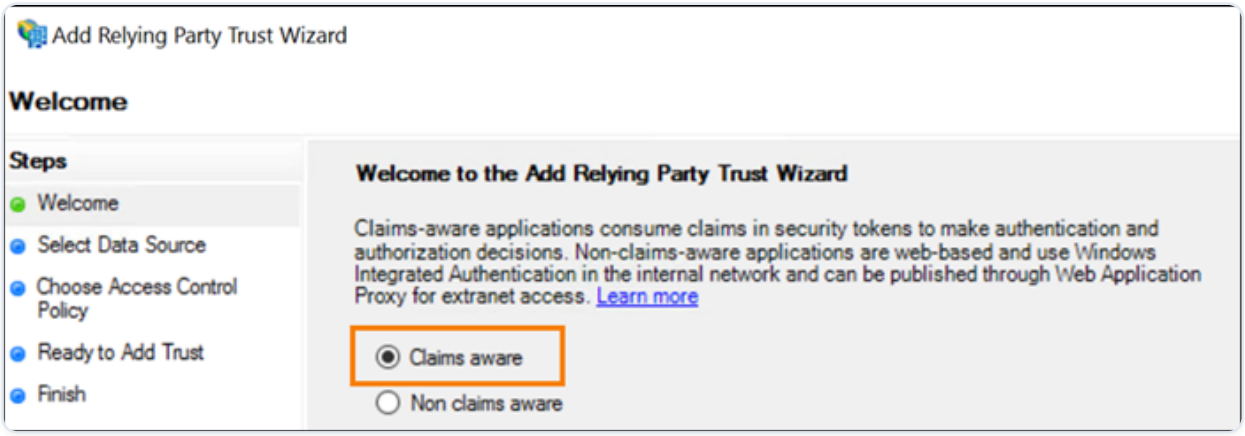
1. 在 AD FS 管理控制台中，展开左侧窗格中的 **AD FS** 节点。
2. 右键单击 **Relying Party Trust**，然后选择 **Add Relying Party Trust**。

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

(/en-us/citrix-cloud/media/saml-adfs-add-relying-party-trust-menu.png)

此时将显示“添加信赖方信任”向导。

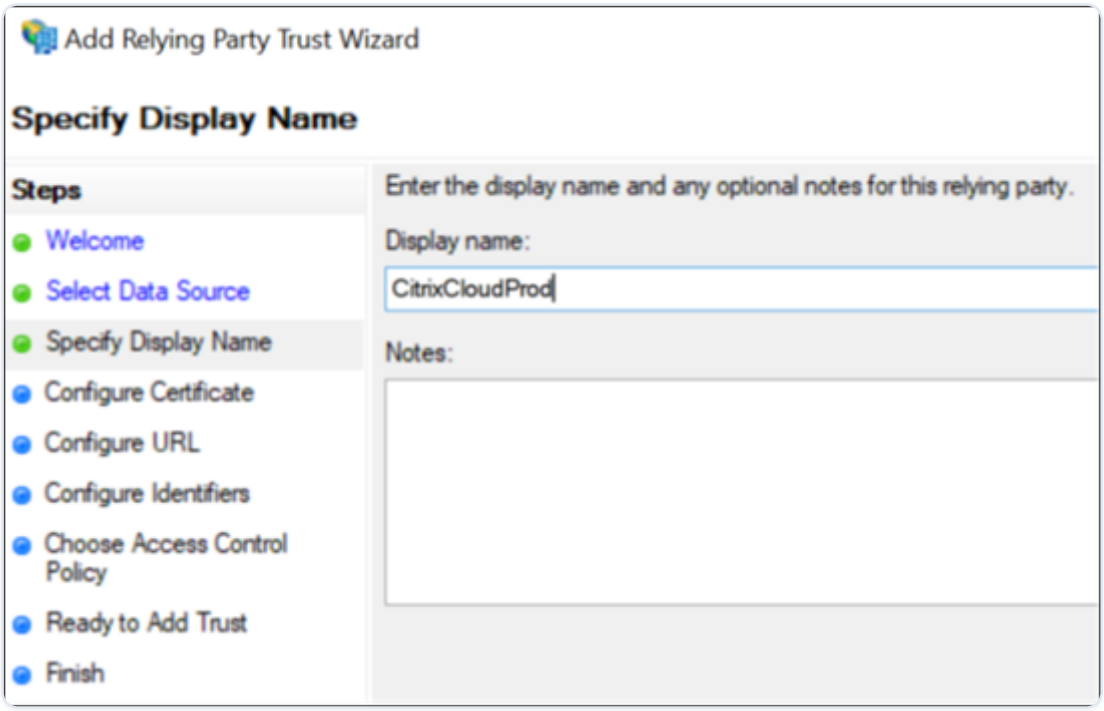
3. 选择 **声明感知**，然后选择 **下一步**。



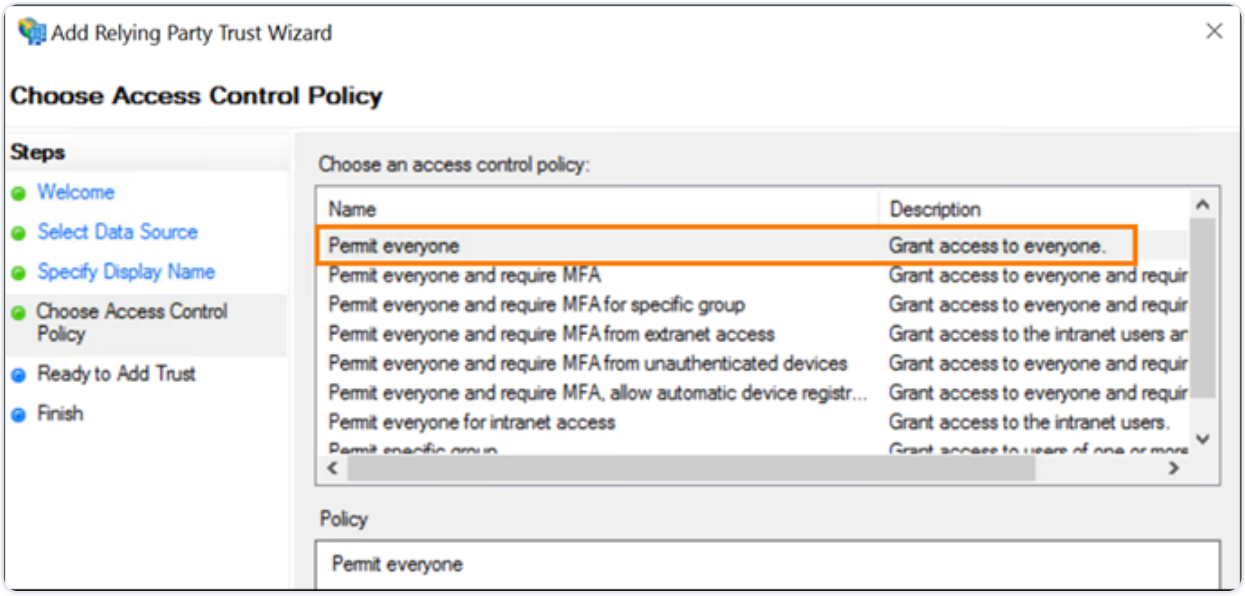
4. 在 **联合元数据地址** 中，输入 `https://saml.cloud.com/saml/metadata.xml`。选择 **下一步**。

5. 对于显示名称，输入 `CitrixCloudProd`。选择 **下一步**。

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

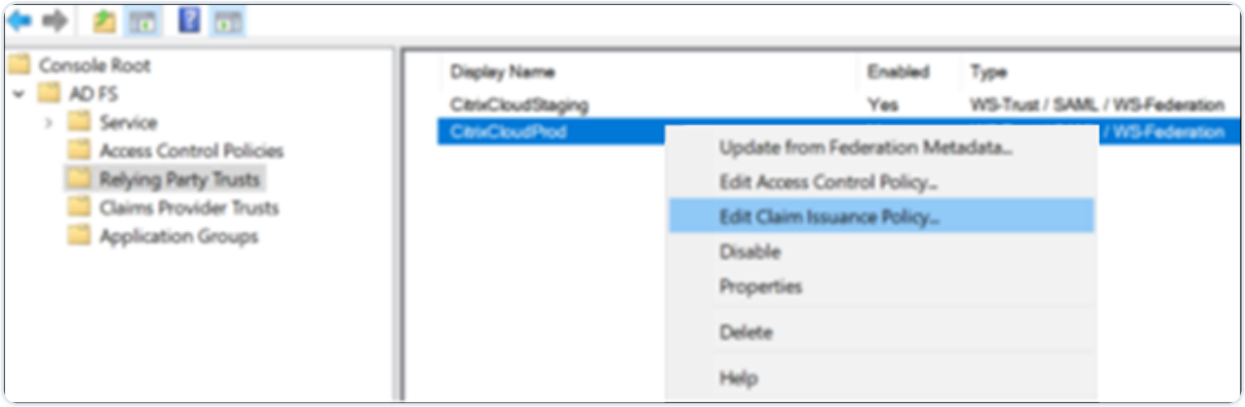


6. 对于访问控制策略，选择 **允许所有人**。选择 **下一步**。



7. 在 **准备添加信任** 屏幕上，选择 **下一步**。
8. 在 **完成** 屏幕上，选择 **为此应用程序配置声明颁发策略**。选择 **下一步**。

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



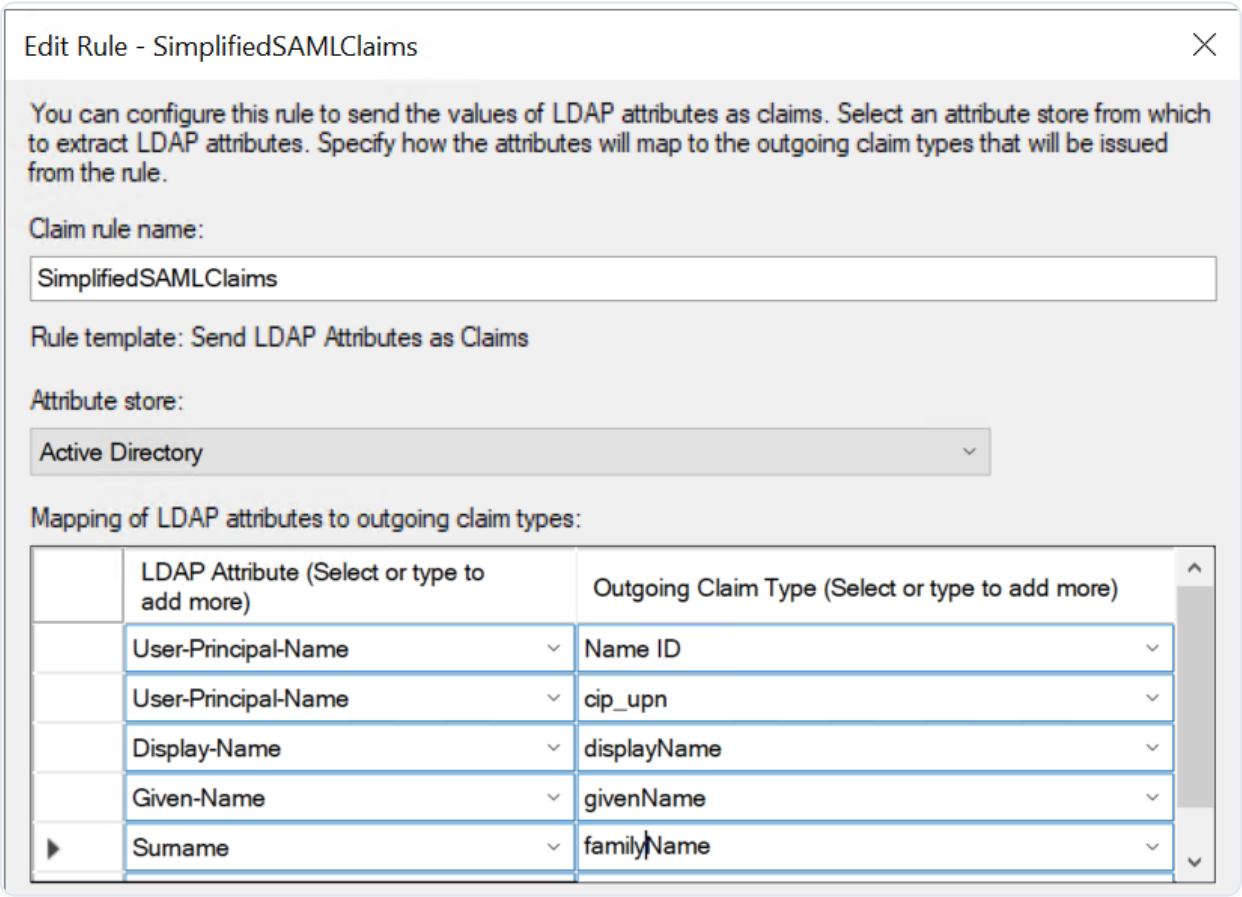
9. 右键单击新创建的信赖方信任，然后选择 **编辑声明颁发策略**。
10. 单击 **添加规则**，然后选择 **将 LDAP 属性作为声明发送**。选择 **下一步**。
11. 在 **声明规则名称** 中，输入 `CitrixCloud`。
12. 在 **属性存储** 中，选择 **活动目录**。
13. 在**将 LDAP 属性映射到传出声明类型**下，添加以下 LDAP 属性，请务必完全按照所示添加：

LDAP 属性	传出声明类型
用户主体名称	名称 ID
用户主体名称	cip_upn
显示名称	displayName
名字	givenName
姓氏	familyName

重要提示：

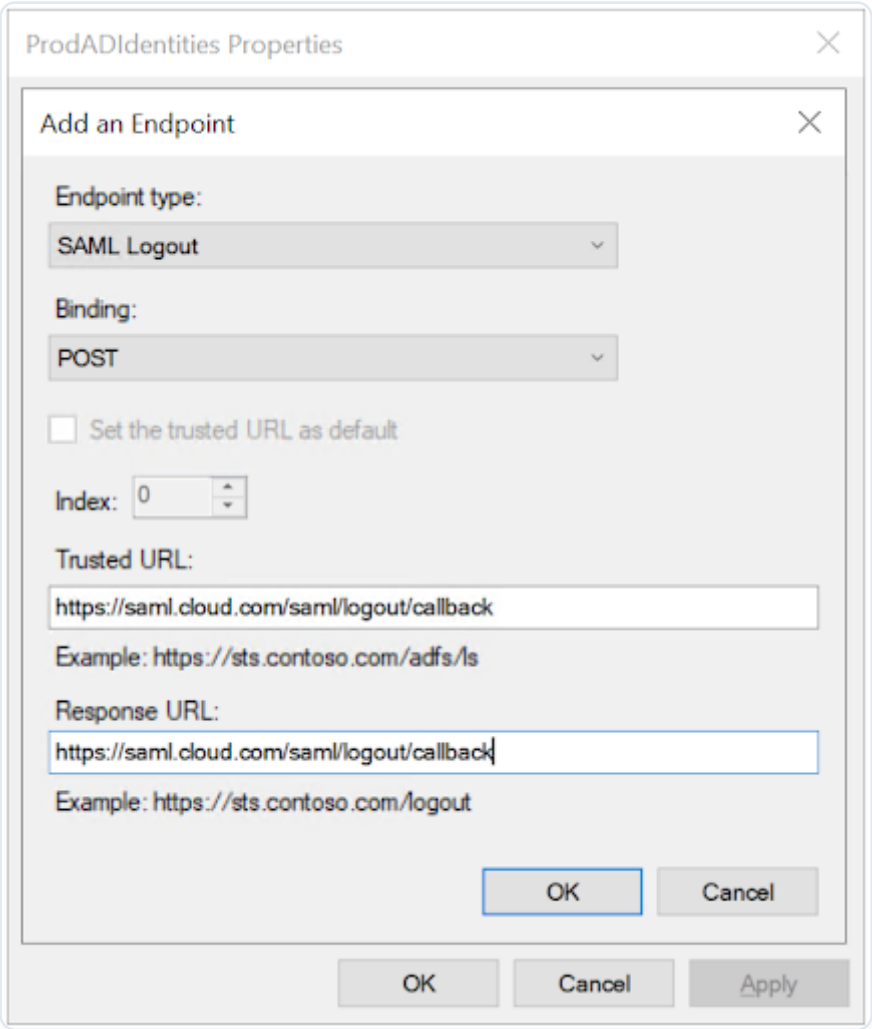
NameID 必须始终是添加到声明列表中的第一个声明，否则单一注销 (SLO) 将无法正常运行。

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



14. 选择 **完成**。
15. 右键单击新创建的名为“CitrixCloudProd”的信赖方信任，然后选择属性。
16. 选择 **端点** 选项卡，然后单击 **添加 SAML**。
17. 从端点类型下拉列表中选择 **SAML 注销**。
18. 从绑定下拉列表中选择 **POST**。
19. 在“受信任的 URL:”和“响应 URL:”中输入 `https://saml.cloud.com/saml/logout/callback>`:

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



20. 单击 **确定** 和 **应用**。

使用 PowerShell 修改 Citrix Cloud 信赖方信任

如果您使用默认的“开箱即用”配置配置了 ADFS 服务器，本节中的步骤可让您对其进行更新，使其符合 Citrix 推荐的配置。如果声明规则集中不包含 `nameidentifier` 属性，或者它不是声明规则集中的第一个 SAML 属性，则 Citrix Cloud 或商店中的 SAML 单点注销将失败，需要执行此任务来解决此问题。

注意：

如果您按照本文中 为 Citrix Cloud 配置信赖方信任 中的步骤创建了声明规则集，则无需执行此任务。

要完成此任务，您需要使用 PowerShell 将现有规则集替换为新的声明规则集。ADFS 管理控制台不支持此类操作。

1. 在 ADFS 服务器上，找到 PowerShell ISE。右键单击并选择 **以管理员身份运行**。

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

2. 备份您现有的 ADFS 声明规则到文本文件：

```
Get-ADFSRelyingPartyTrust -name "CitrixCloudProd" | Select-Object
-ExpandProperty IssuanceTransformRules | Out-File
"$env:USERPROFILE\desktop\claimrulesbackup.txt"
```

3. 下载 Citrix 在 https://github.com/citrix/sample-scripts/tree/master/citrix-cloud 提供的 claimrules.txt 文件。
4. 将 claimrules.txt 文件复制到您的桌面。
5. 使用 claimrules.txt 文件导入所需的声明规则：

```
Set-ADFSRelyingPartyTrust -Name "CitrixCloudProd" `

                       -MetadataUrl "https://saml.cloud.com/saml/
metadata" `

                       -AutoUpdateEnabled $True `

                       -IssuanceTransformRulesFile
"$env:USERPROFILE\desktop\claimrules.txt" `

                       -SignedSamlRequestsRequired $True `

                       -SamlResponseSignature "MessageAndAssertion" `

                       -Enabled $True
```

使用 PowerShell 更新信赖方信任的 SAML 签名设置

默认情况下，ADFS 信赖方信任具有以下设置：

- EncryptClaims: 真
- SignedSamlRequestsRequired: 假
- SamlResponseSignature: AssertionOnly

为了提高安全性，Citrix 建议对单点登录 (SSO) 和单点注销都使用已签名的 SAML 请求。本节介绍如何使用 PowerShell 更新现有信赖方信任的签名设置，使其符合 Citrix 推荐的配置。

1. 在您的 ADFS 服务器上获取当前的 RelyingPartyTrust 配置。

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

```
Get-ADFSRelyingPartyTrust -TargetName "CitrixCloudProd"
```

2. 更新 **CitrixCloudProd** 信赖方信任设置。

```
Set-ADFSRelyingPartyTrust -Name "CitrixCloudProd" `

                       -SignedSamlRequestsRequired $True `

                       -SamlResponseSignature "MessageAndAssertion"
```

Citrix Cloud 中的 SAML 配置

当您在 Citrix Cloud 中配置 SAML 连接时（如 (/zh-cn/citrix-cloud/citrix-cloud-management/identity-access-management/saml-identity.html#add-saml-provider-metadata-to-citrix-cloud) 中所述），您将按如下方式输入 ADFS 的值：

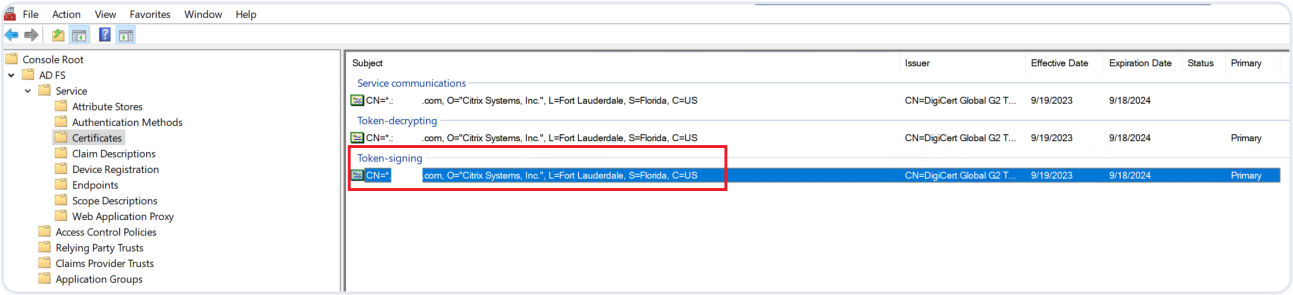
在 **Identity and Access Management > Authentication > Add an identity provider > SAML** 中使用 SAML 连接的默认推荐值。

在 CITRIX CLOUD 的此字段中	输入此值
实体 ID	`https://adfs.YourDomain.com/adfs/services/trust`，其中 `YourDomain.com` 是您的 ADFS 服务器域。
签署身份验证请求	是
SSO 服务 URL	`https://adfs.YourDomain.com/adfs/ls`，其中 `YourDomain.com` 是您的 ADFS 服务器域。
SSO 绑定机制	HTTP 提交
SAML 响应	签署响应或断言
身份验证上下文	未指定，精确
注销 URL	`https://adfs.YourDomain.com/adfs/ls`，其中 `YourDomain.com` 是您的 ADFS 服务器域。

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

在 CITRIX CLOUD 的此字段中	输入此值
注销请求签名	是
SLO 绑定机制	HTTP 提交

从 MMC ADFS 管理控制台中导出 ADFS 签名证书。请参阅下面的屏幕截图，了解 3 个证书中哪一个是正确的，以便在 SAML 连接中上传到 Citrix Cloud。



将 Duo 配置为商店身份验证的 SAML 提供程序

本文介绍了配置 Duo SAML 应用程序以及 Citrix Cloud™ 与您的 SAML 提供程序之间 SAML 连接所需的步骤。其中一些步骤描述了您在 Duo SAML 提供程序的管理控制台中执行的操作。

先决条件

在完成本文中的任务之前，请确保您已满足以下先决条件：

- 一个 Duo 云租户。
- 您的 AD 林中的 Duo 身份验证代理。
- 一个将您的 AD 用户同步到 Duo 的 Active Directory LDAPS 连接。

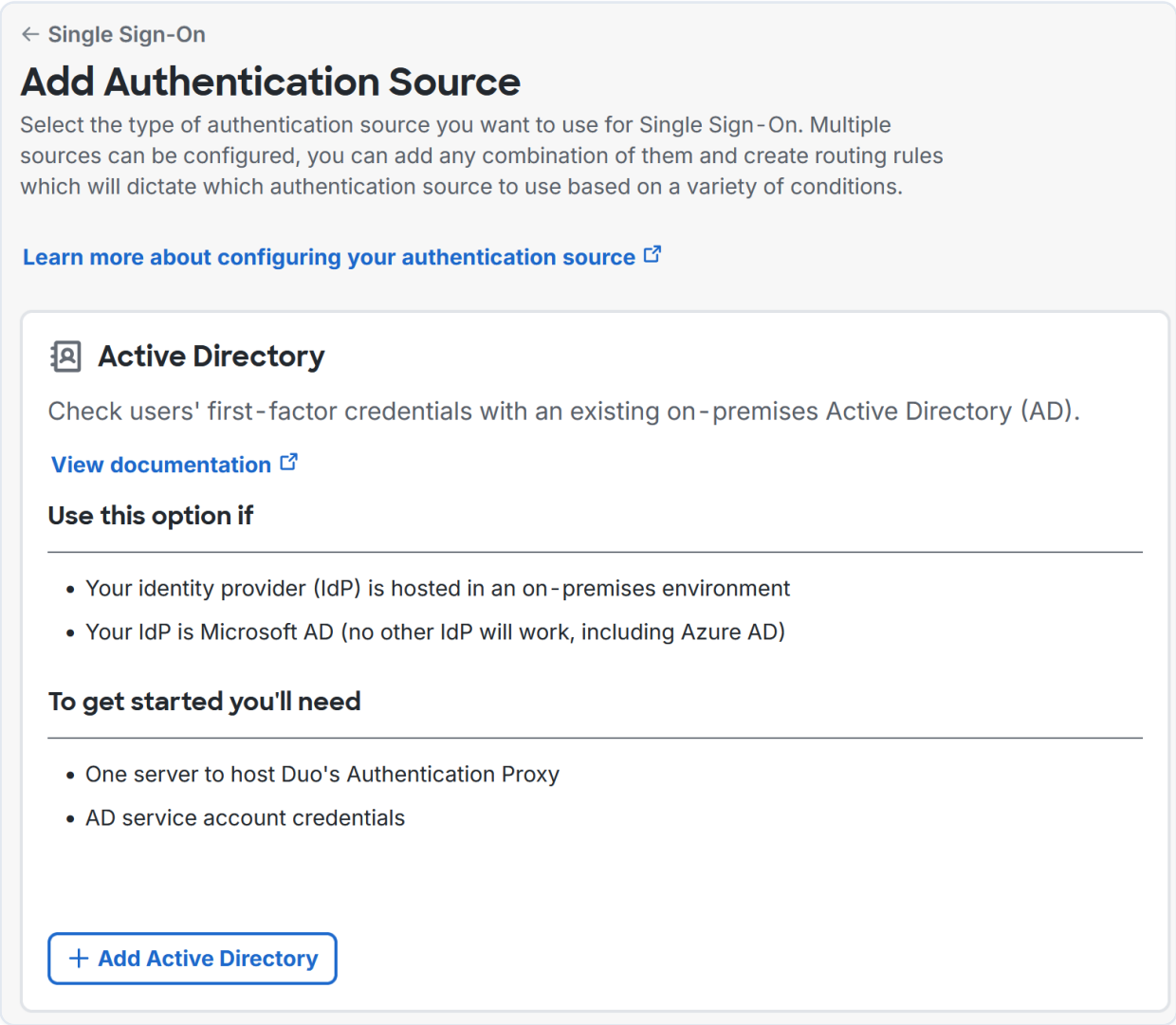
配置 Active Directory 同步到您的 Duo 租户

请遵循 Duo 文档中关于将本地 AD 连接到 Duo 并导入 SAML 用户 的说明。

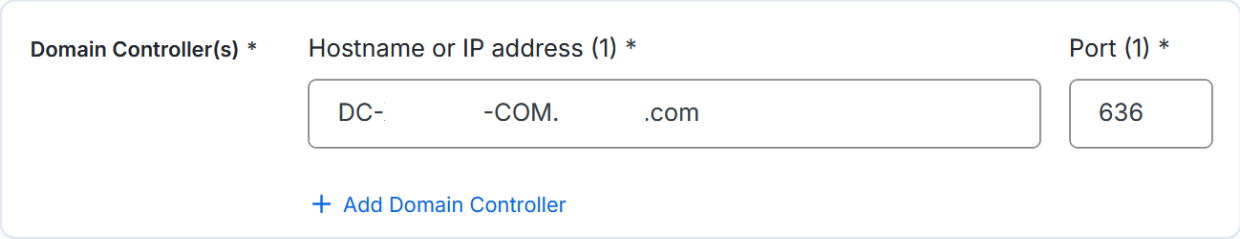
创建 Active Directory LDAPS 连接

1. 选择 **应用程序 > SSO 设置 > 添加源 > 活动目录 > 添加活动目录**。

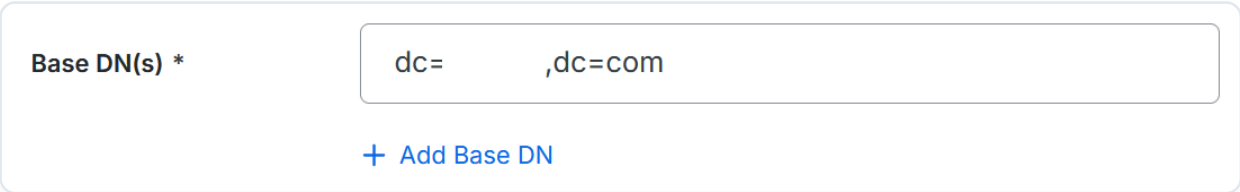
© 1997–2026 Citrix Systems, Inc. All rights reserved.



2. 输入您的 AD 林的 LDAPS 连接的显示名称。
3. 输入您的域控制器的 FQDN。

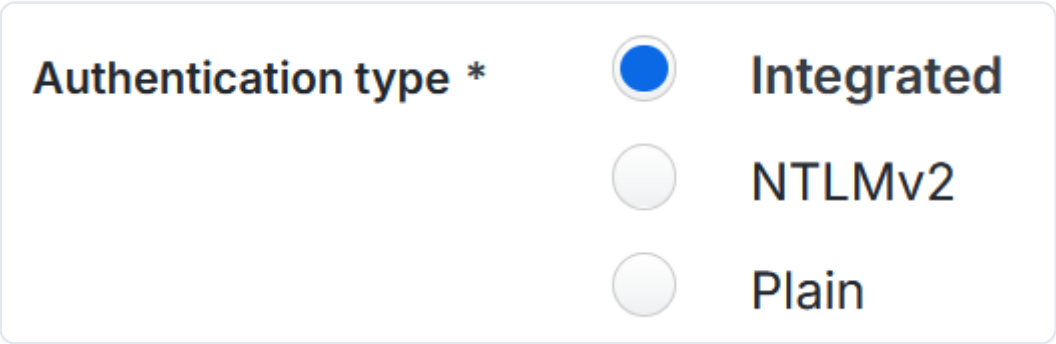


4. 配置您的 AD 域的基本 DN。

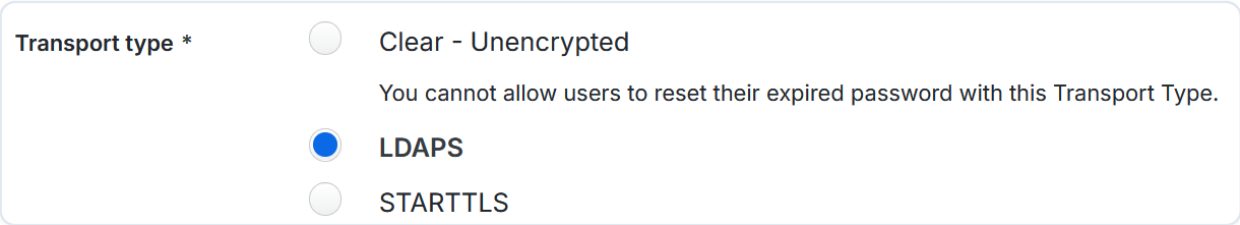


5. 选择“集成”作为身份验证类型。

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



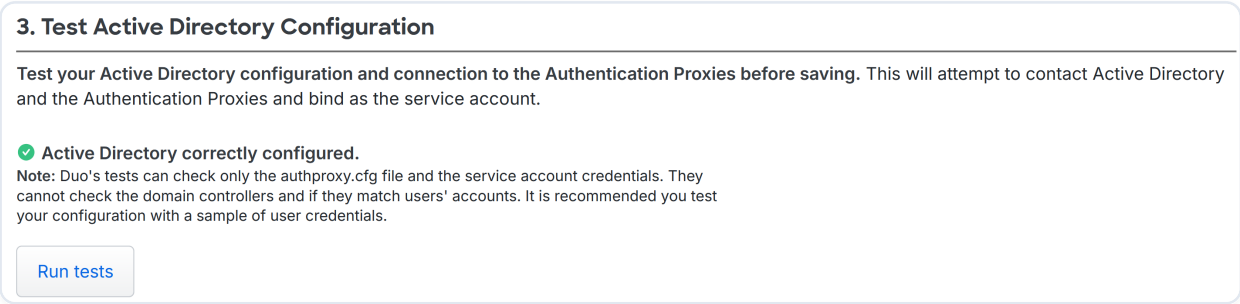
6. 选择 LDAPS 作为传输类型。



7. 勾选“SSL 验证主机名”。
8. 输入域控制器证书，然后输入用于签署域证书的私有企业证书颁发机构 CA 证书。
9. 按照以下示例输入 PEM 格式的证书

```
-----BEGIN CERTIFICATE-----

`<base64 Domain Controller Certificate>`

-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----

`<base64 Certificate Authority Certificate used to sign the Domain
Controller Certificate above>`

-----END CERTIFICATE-----
```

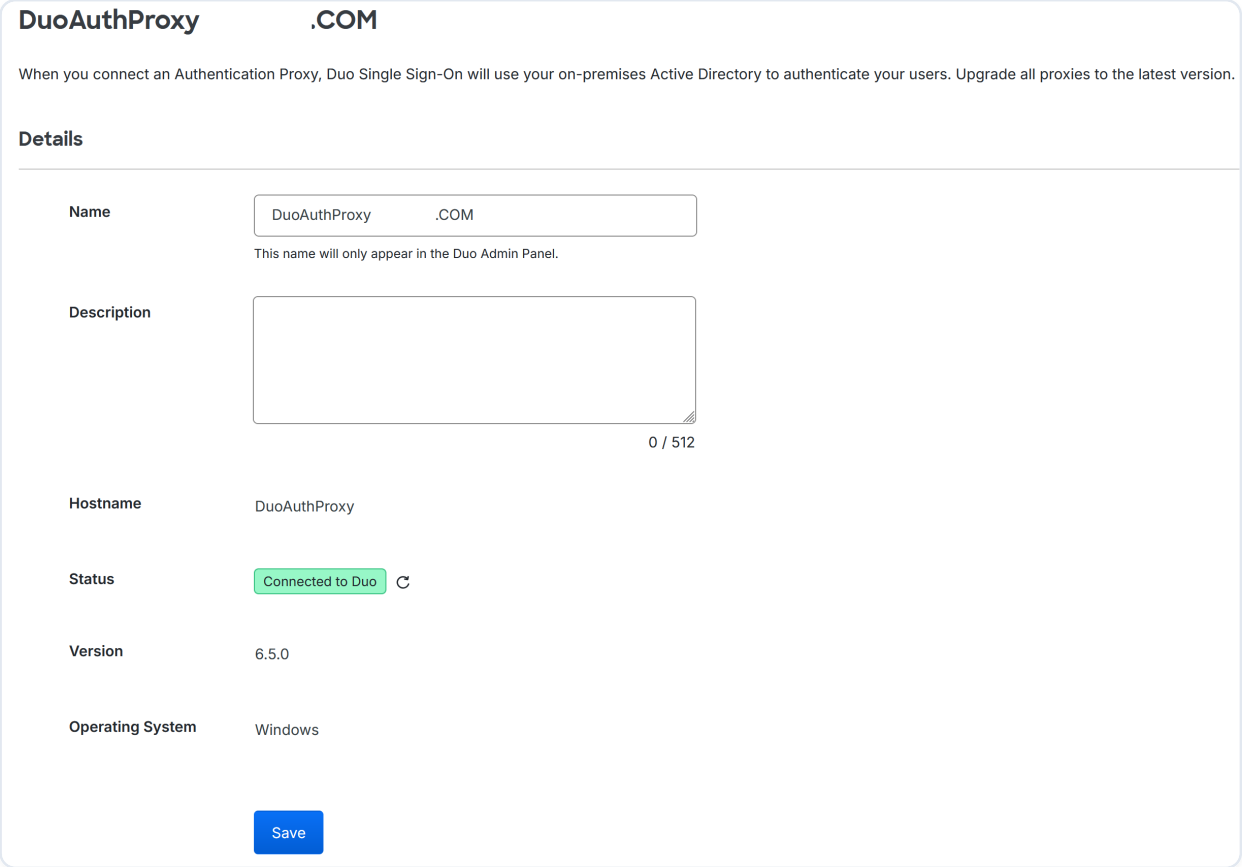
10. 测试您的 LDAPS 连接。



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

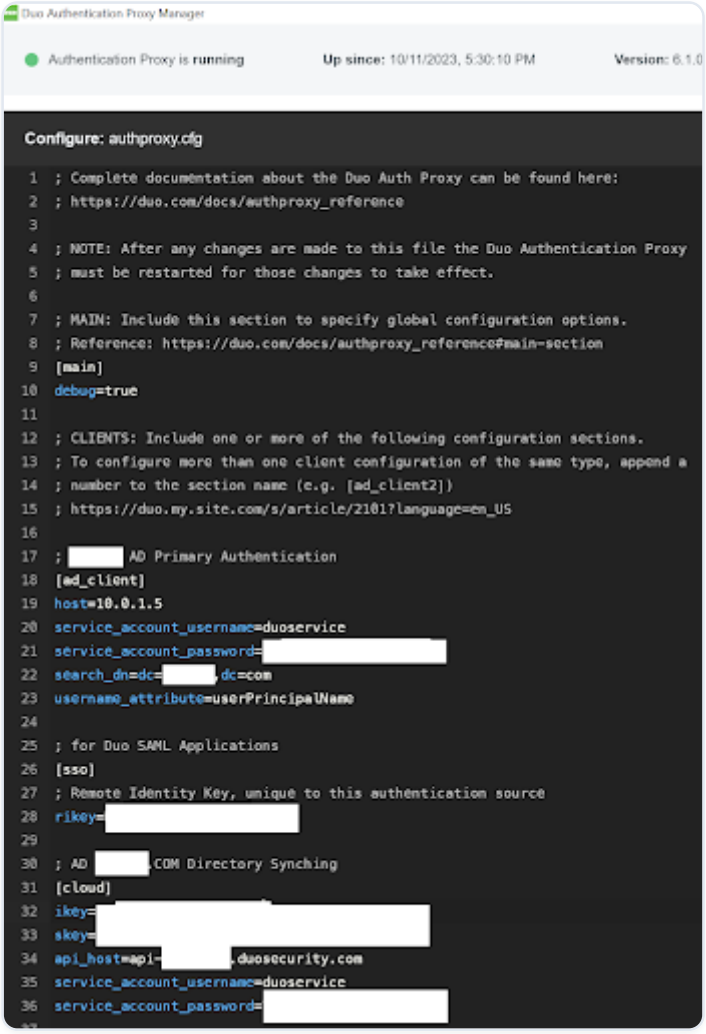
为 SAML 配置 Duo 身份验证代理配置文件

1. 检查您的 Duo 身份验证代理配置是否正常，并显示为“**已连接到 Duo**”。



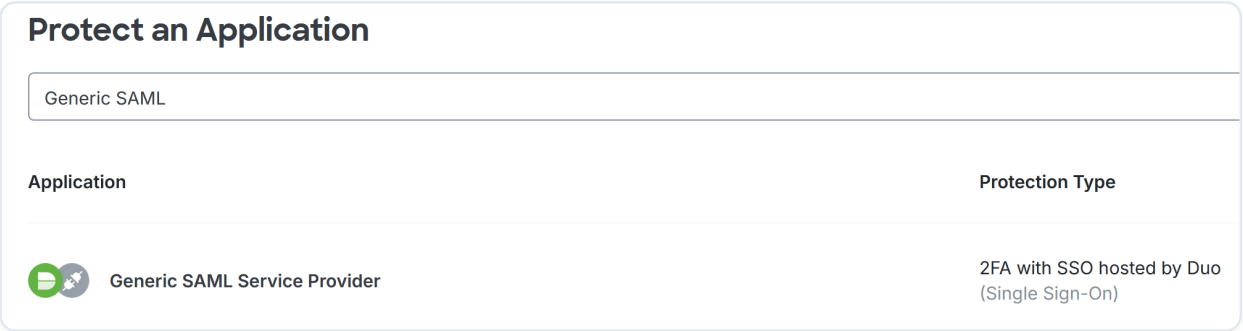
2. 登录到您的 Duo 身份验证代理，并使用 Duo 管理控制台提供的 **远程身份 (rikey)** 将 SAML 部分添加到其配置文件中。Duo 身份验证代理使用共享密钥与 Duo 云服务通信。此密钥在身份验证代理的初始安装或配置期间生成。

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



配置用于商店的 Duo SAML 应用程序

1. 选择 **应用程序 > 保护应用程序**。单击 **添加应用程序**。
2. 找到通用 SAML 服务提供商 Duo 应用程序模板的条目。Citrix® 推荐使用通用 SAML 服务提供商 Duo 模板，因为它最灵活，可让您根据需要配置不同的 SAML 属性组合和不同的 SAML 流。



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

重要提示：

不建议使用 Duo **Citrix Workspace** SAML 模板，因为它不灵活，并且仅支持使用 AD 身份的 SAML。Duo **Citrix Workspace** SAML 模板也不允许添加可选属性，例如 cip_domain 和 cip_forest，这些属性是某些高级并购 SAML 配置所必需的。它也不允许配置 Citrix Cloud 注销端点。

3. 为您的 SAML 应用程序指定一个**显示名称**，例如 **Citrix Cloud Prod**。
4. 指定**用户访问权限**，例如**为所有用户启用**。
5. 在**元数据发现**中选择**无（手动输入）**，然后输入以下 Citrix Cloud SAML 端点。
6. 根据您的 CC 租户所在的 Citrix Cloud 区域输入 **EntityID**。

URL	区域
`https://saml.cloud.com`	商业版（欧盟、美国和亚太南部）
`https://saml.citrixcloud.jp`	日本
`https://saml.cloud.us`	政府

7. 根据您的 CC 租户所在的 Citrix Cloud 区域配置**单点登录 URL (ACS URL)**。

URL	区域
`https://saml.cloud.com/saml/acs`	商业版欧盟、美国和亚太地区
`https://saml.citrixcloud.jp/saml/acs`	日本
`https://saml.cloud.us/saml/acs`	政府

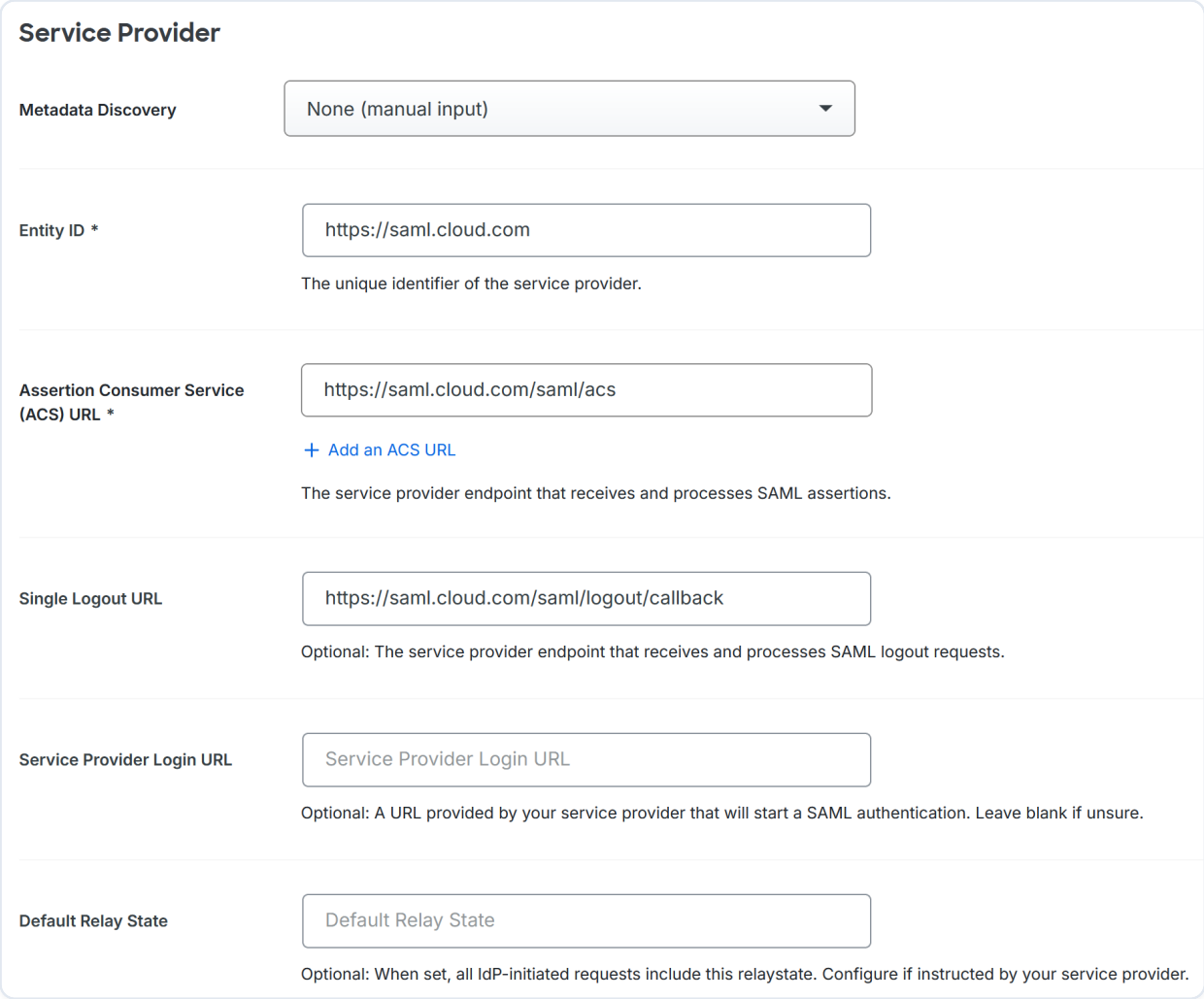
8. 根据您的 CC 租户所在的 Citrix Cloud 区域配置**单点注销 URL**。

URL	区域
`https://saml.cloud.com/saml/logout/callback`	商业版（欧盟、美国和亚太地区）
`https://saml.citrixcloud.jp/samllogout/callback`	日本

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

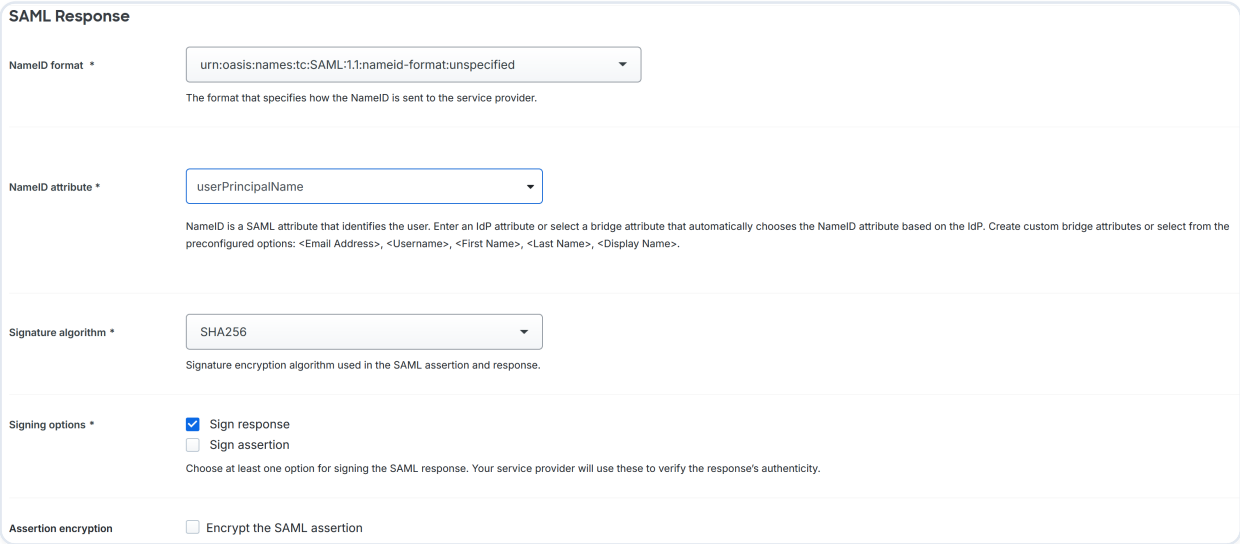
URL	区域
`https://saml.cloud.us/saml/samllogout/callback`	政府版

9. **服务提供商登录 URL** 不是必需的，可以留空。
10. **默认中继状态** 不是必需的，可以留空。

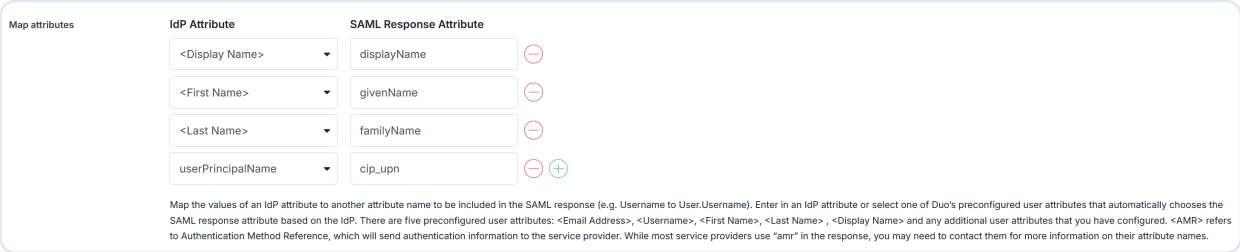


11. 将 **名称 ID 格式** 配置为 **未指定**。
12. 将 **名称 ID 属性** 配置为 **userPrincipalName**（区分大小写）。
13. 将 **签名算法** 配置为 **SHA256**。
14. 将 **签名选项** 配置为 **签名响应**。
15. 将 **断言加密** 配置为 **已禁用**。

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



16. 配置 **映射属性**，左侧为 Duo 桥接属性，右侧为 Citrix Cloud SAML 声明名称。



重要提示：

Duo 桥接属性（左侧）和 SAML 属性声明名称（右侧）区分大小写。右侧的声明名称必须与 Citrix Cloud SAML 连接中配置的名称匹配。

配置 Citrix Cloud SAML 连接

1. 所有 Citrix 登录流程都需要由服务提供商发起，使用应用商店 URL 或 Citrix Cloud GO URL。
2. 使用 **身份和访问管理 > 身份验证 > 添加身份提供商 > SAML** 中 SAML 连接的默认推荐值。
3. 通过访问 Duo Active Directory Sync 文档，从您的 Duo 门户获取 Duo SAML 应用程序的 SAML 端点，以输入到 Citrix Cloud SAML 连接中。

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

在 CITRIX CLOUD 的此字段中	输入此值
实体 ID	`https://sso-<id>.sso.duosecurity.com/saml2/sp/<samlappID>/metadata`
签署身份验证请求	是
SSO 服务 URL	`https://sso-<id>.sso.duosecurity.com/saml2/sp/<samlappID>/sso`
SSO 绑定机制	HTTP 提交
SAML 响应	签署响应或断言
身份验证上下文	未指定，精确
注销 URL	`https://sso-<id>.sso.duosecurity.com/saml2/sp/<samlappID>/slo`
签署注销请求	是
SLO 绑定机制	HTTP 提交

Duo SAML 注销行为

在撰写本文时，Duo SAML 尚不支持 SAML SLO，但可以配置 Duo 以在用户明确注销 StoreFront 和/或 Citrix Cloud 时终止 IDP 会话。建议您在选择配置 Duo SAML 应用程序的注销设置之前，阅读主 SAML 文章中的 SAML 注销注意事项部分 (/zh-cn/citrix-cloud/citrix-cloud-management/identity-access-management/saml-identity.html#saml-logout-considerations)。

重要提示：

摘自 Duo 文档 Duo SSO 注销行为和会话管理详情。

`Users that decide to log out and hit the SLO URL for Duo SSO will be logged out of Duo SSO and have their MFA remembered devices session deleted before redirecting them to the logout page`。

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

要在最终用户注销 StoreFront 和/或 Citrix Cloud 时配置 Duo IDP 会话的显式注销，请按照以下推荐步骤操作。

1. 在 Duo SAML 应用程序中配置 Citrix Cloud SAML 注销端点。

   (/en-us/citrix-cloud/media/saml-duo-cc-logout.png)

2. 在 Citrix Cloud SAML 连接中配置 Duo SLO 端点。

   重要提示：

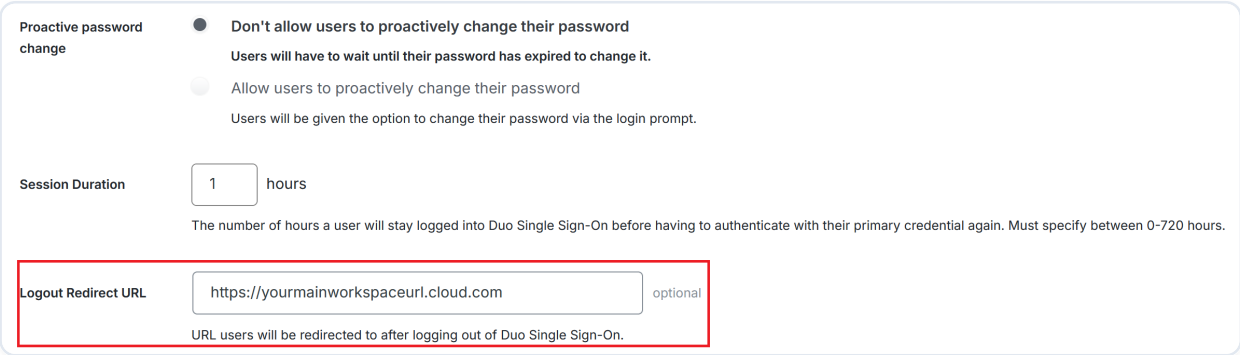
   如果您未使用 **Generic SAML Provider** Duo 应用程序模板，则无法完成此步骤，因为输入 Citrix Cloud 注销端点的选项将不可用。

   (/en-us/citrix-cloud/media/saml-duo-ccconnection-logout.png)

3. 当按照步骤 1 和 2 配置 SAML 连接的两端进行注销时，从 StoreFront 注销后，Duo 将显示以下 UI，表明 IDP 会话已终止。

   (/en-us/citrix-cloud/media/saml-duo-logout-ui.png)

4. **可选**：为了改善 StoreFront 最终用户的注销体验，可以为 Duo LDAPS 连接配置单个**注销重定向 URL**，该 URL 会将最终用户重定向回 StoreFront 登录页面。这在您的 AD 林 LDAPS 连接中完成。



   重要提示：

   上面显示的注销重定向 URL 字段只允许配置一个商店 URL。在 Citrix Cloud 租户中使用多个不同的商店 URL 无法在 Duo 的单个 Active Directory 林连接中进行配置。

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

使用 Entra ID 和 AD 身份进行商店身份验证的 SAML

本文介绍如何配置 SAML 以使用 Active Directory (AD) 身份进行商店身份验证。Citrix Cloud™ 和 SAML 对云商店或 Citrix Cloud 进行身份验证的默认行为（无论使用何种 SAML 提供程序）是针对 AD 用户身份进行断言。对于本文中描述的配置，需要使用 Entra ID Connect 将您的 AD 身份导入到您的 Entra ID。

重要提示：

确定适合最终用户的 SAML 流程至关重要，因为它直接影响他们的登录过程和资源可见性。所选身份会影响商店最终用户可访问的资源类型。 有一篇相关文章提供了有关使用 Entra ID 作为 SAML 提供程序，通过 ME-ID 身份对商店进行身份验证的说明。您可以在使用 Microsoft Entra ID 和 ME-ID 身份进行商店身份验证的 SAML 中找到详细说明。 通常，最终用户需要打开由加入 AD 域的 VDA 提供的应用程序和桌面。在决定最适合您组织的 SAML 流程之前，务必仔细查看两篇文章中概述的用例。如果不确定，Citrix® 建议使用 **AD SAML 流程**并遵循本文中的说明，因为它与最常见的 DaaS 场景一致。

功能范围

本文适用于使用以下 Citrix Cloud 和 Azure 功能组合的用户：

- 使用 AD 身份进行商店身份验证的 SAML
- 使用 AD 身份进行 Citrix Cloud 管理员登录的 SAML
- 使用加入 AD 域的 VDA 发布的资源的 Citrix DaaS™ 和 HDX 资源枚举
- 加入 AD 域的 VDA 资源枚举

AD 身份与 Entra ID 身份：最佳选择?

要确定您的商店用户应使用 SAML AD 还是 SAML Entra ID 身份进行身份验证：

1. 确定您打算在用户的商店中向他们提供哪些资源组合。
2. 使用下表确定哪种用户身份适用于每种资源类型。

资源类型 (VDA)	用户在登录商店时的身份	需要使用 ENTRA ID 的 SAML 身份吗？	FAS 是否为 VDA 提供单点登录 (SSO)？
已加入 AD	AD，从 AD 导入的 Entra ID（包含 SID）	否。使用默认 SAML。	是

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

配置自定义 Entra ID 企业 SAML 应用程序

默认情况下，SAML 登录商店的行为是针对 AD 用户身份进行断言。

1. 登录 Azure 门户。
2. 从门户菜单中，选择 **Entra ID**。
3. 在左侧窗格中，在 **管理** 下，选择 **企业应用程序**。
4. 在工作窗格的命令栏中，选择 **新建应用程序**。
5. 在命令栏中，选择 **创建自己的应用程序**。不要使用 Citrix Cloud SAML SSO 企业应用程序模板。该模板不允许您修改声明和 SAML 属性列表。
6. 输入应用程序名称，然后选择 **集成在库中找不到的任何其他应用程序（非库）**。单击 **创建**。应用程序概述页面随即出现。
7. 从左侧窗格中，选择 **单一登录**。从工作窗格中，选择 **SAML**。
8. 在 **基本 SAML 配置** 部分中，选择 **编辑** 并配置以下设置：

   a. 在 **标识符（实体 ID）** 部分中，选择 **添加标识符**，然后输入与您的 Citrix Cloud 租户所在区域关联的值：

      - 对于欧盟、美国和亚太南部地区，输入 `https://saml.cloud.com`。
      - 对于日本地区，输入 `https://saml.citrixcloud.jp`。
      - 对于 Citrix Cloud Government 地区，输入 `https://saml.cloud.us`。

   b. 在 **回复 URL（断言消费者服务 URL）** 部分中，选择 **添加回复 URL**，然后输入与您的 Citrix Cloud 租户所在区域关联的值：

      - 对于欧盟、美国和亚太南部地区，输入 `https://saml.cloud.com/saml/acs`。
      - 对于日本地区，输入 `https://saml.citrixcloud.jp/saml/acs`。
      - 对于 Citrix Cloud Government 地区，输入 `https://saml.cloud.us/saml/acs`。

   c. 在 **注销 URL（可选）** 部分中，输入与您的 Citrix Cloud 租户所在区域关联的值：

      - 对于欧盟、美国和亚太南部地区，输入 `https://saml.cloud.com/saml/logout/callback`。
      - 对于日本地区，输入 `https://saml.citrixcloud.jp/saml/logout/callback`。
      - 对于 Citrix Cloud Government 地区，输入 `https://saml.cloud.us/saml/logout/callback`。

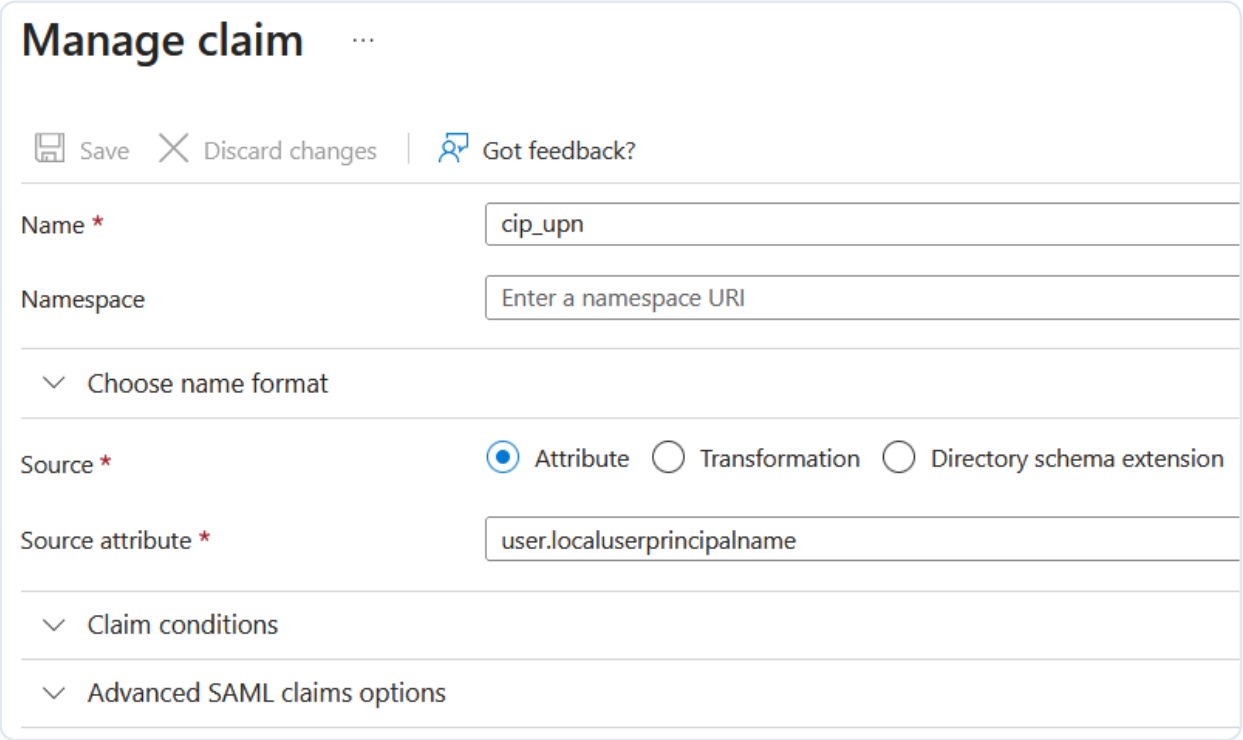
   d. 从命令栏中，选择 **保存**。

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

9. 在**属性和声明**部分中，单击**编辑**以配置以下声明。这些声明出现在 SAML 响应中的 SAML 断言中。创建 SAML 应用程序后，配置以下属性。

   a. 对于**唯一用户标识符 (名称 ID)** 声明，将默认值更新为 `user.localuserprincipalname`。

   b. 对于 **cip_upn** 声明，将默认值更新为 `user.localuserprincipalname`。



   a. 对于 **displayName**，保留默认值 `user.displayname`。

   b. 对于 **givenName** 声明，将默认值更新为 `user.givenname`。

   c. 对于 **familyName** 声明，将默认值更新为 `user.surname`。

   d. 在**附加声明**部分中，对于任何带有 `http://schemas.xmlsoap.org/ws/2005/05/identity/claims` 命名空间的剩余声明，单击省略号 (...) 按钮，然后单击**删除**。无需包含这些声明，因为它们是上述用户属性的重复项。

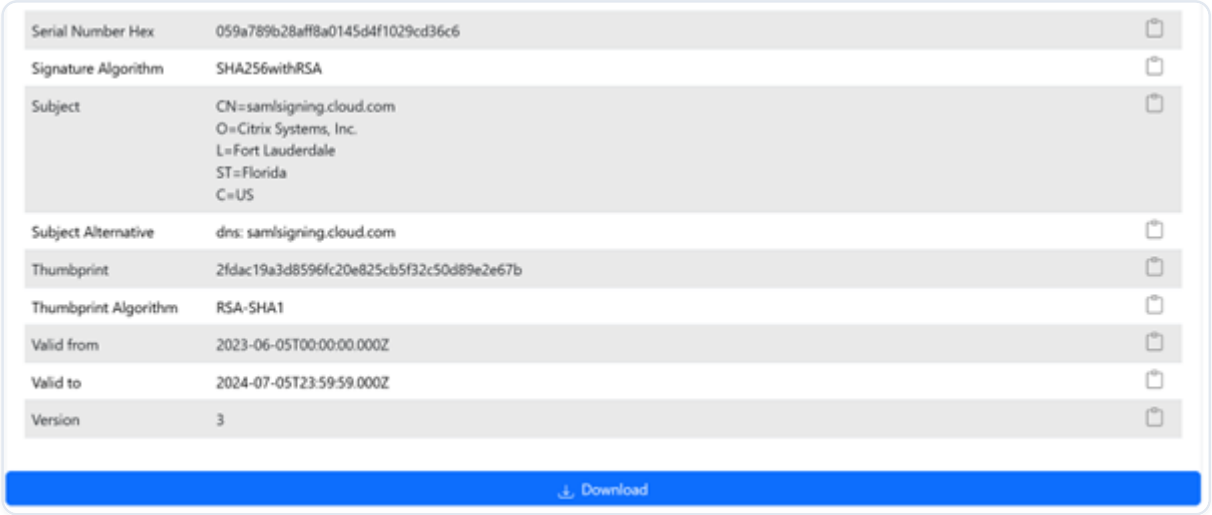
完成后，**属性和声明**部分显示如下：

10. 使用此第三方在线工具 获取 Citrix Cloud SAML 签名证书的副本。

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

a. 在 URL 字段中输入 `https://saml.cloud.com/saml/metadata`，然后单击**加载**。

a. 滚动到页面底部，然后单击**下载**。



下载证书(/en-us/citrix-cloud/media/certificate_download.png)

11. 配置 Entra ID SAML 应用程序的签名设置。

    a. 在 Entra ID SAML 应用程序中上传在步骤 9 中获得的生产 SAML 签名证书。

    b. 启用 **要求验证证书**。

    验证证书(/en-us/citrix-cloud/media/verification_cert.png)

    验证证书(/en-us/citrix-cloud/media/saml_certificate.png)

故障排除

1. 使用 SAML 网络工具（例如 SAML-tracer 浏览器扩展）验证您的 SAML 断言是否包含正确的用户属性。

SAML-tracer 浏览器扩展(/en-us/citrix-cloud/media/saml-tracer-browser-ext.png)

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

1. 找到以黄色显示的 SAML 响应，并与此示例进行比较：

   网络工具中的 SAML 响应示例(/en-us/citrix-cloud/media/saml-idp-aad-saml-tool-response.png)

2. 单击底部窗格中的 **SAML** 选项卡以解码 SAML 响应并以 XML 格式查看。
3. 滚动到响应底部，验证 SAML 断言是否包含正确的 SAML 属性和用户值。

   突出显示 SAML 断言值的 XML 文件(/en-us/citrix-cloud/media/saml-idp-aad-assertion-values.png)

如果您的最终用户仍然无法登录其商店或无法看到其 Citrix HDX™ Plus for Windows 365 桌面，请联系 Citrix 支持并提供以下信息：

- SAML-tracer 捕获
- 登录 Citrix® StoreFront Cloud 失败的日期和时间
- 受影响的用户名
- 用于登录其商店的客户端计算机的调用方 IP 地址。您可以使用 https://whatismyip.com 等工具获取此 IP 地址。

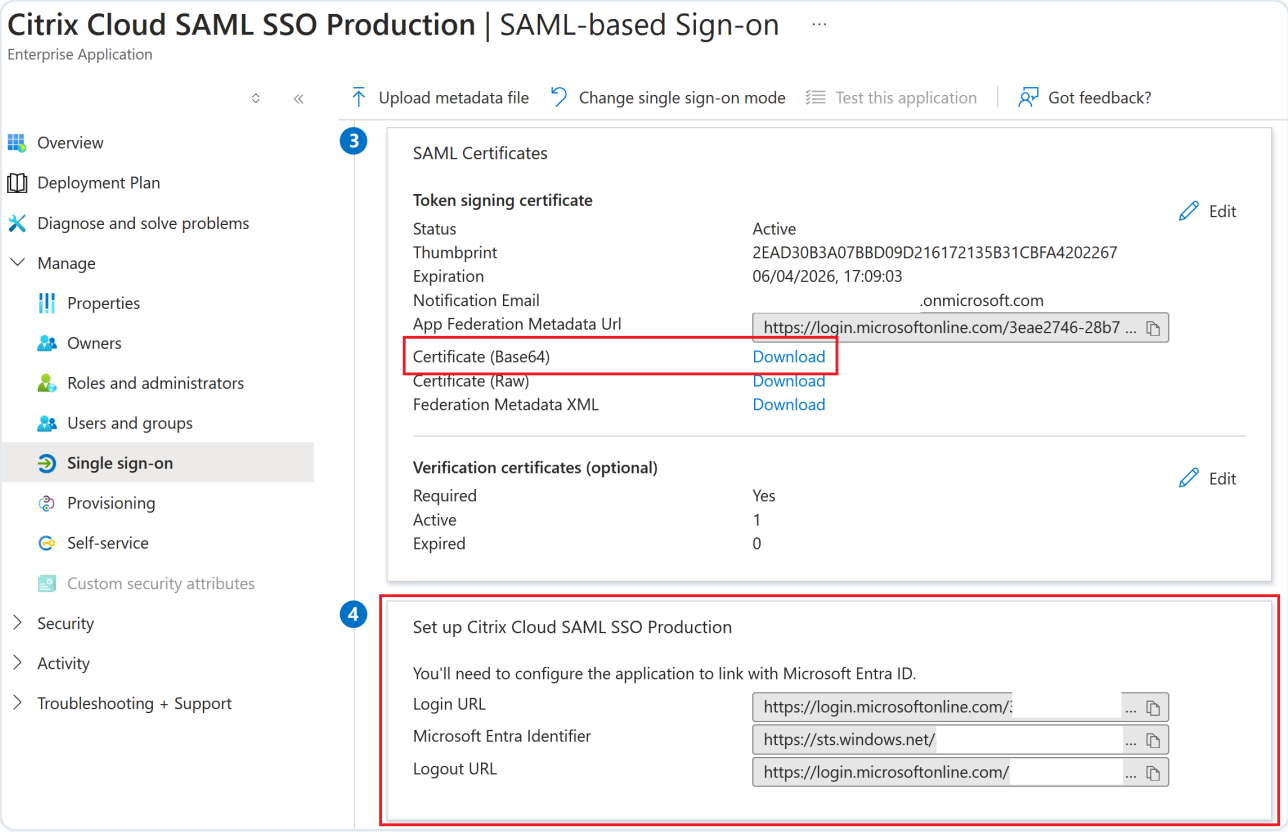
配置 Citrix Cloud SAML 连接

所有 Citrix 登录流程都需要由服务提供商使用商店 URL 或 Citrix Cloud GO URL 发起。

在 **身份和访问管理 > 身份验证 > 添加身份提供商 > SAML** 中，使用 SAML 连接的默认推荐值。

从您的 Entra ID 门户获取 Entra ID SAML 应用程序的 SAML 端点，以输入到 Citrix Cloud 中。

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



用于 Citrix Cloud SAML 连接的 Entra ID SAML 端点示例

重要提示：

EntraID SSO 和注销 SAML 端点是相同的 URL。

在 CITRIX CLOUD 的此字段中	输入此值
实体 ID	`https://sts.windows.net/<yourEntraIDTenantID>`
签署身份验证请求	是
SSO 服务 URL	`https://login.microsoftonline.com/<yourEntraIDTenantID>/saml2`
SSO 绑定机制	HTTP POST 请求
SAML 响应	签署响应或断言
身份验证上下文	未指定，精确

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

在 CITRIX CLOUD 的此字段中	输入此值
注销 URL	`https://login.microsoftonline.com/<yourEntraIDTenantID>/saml2`
签署注销请求	是
SLO 绑定机制	HTTP 提交

使用 Entra ID 和 Entra ID 身份进行商店身份验证的 SAML

本文介绍了如何配置 SAML 以使用 Entra ID 身份而不是 AD 身份进行商店身份验证。如果您的 Entra ID 用户在以默认 SAML 行为登录其商店后无法枚举 Windows 365 Cloud PC 或 Entra ID 域加入的 VDA，请使用此配置。完成配置后，您的用户可以使用 SAML 身份验证登录其商店，以通过 Citrix DaaS™ 访问 HDX 应用程序和桌面，并通过 Azure 访问 Windows 365 Cloud PC。

Citrix Cloud™ 和 SAML 对 Citrix® StoreFront Cloud 进行身份验证的默认行为是针对 AD 用户身份进行断言。对于本文中描述的配置，需要使用 Entra ID Connect 将您的 AD 身份导入到您的 Entra ID。AD 身份包含用户的 SID，StoreFront Cloud 可以将其发送到 Citrix DaaS，并允许枚举和启动 HDX 资源。由于使用了用户身份的 Entra ID 版本，用户还可以从 StoreFront Cloud 中枚举和启动 Azure 资源，例如 Windows 365 Cloud PC。

重要提示：

枚举是指用户登录其商店后看到的资源列表。给定用户被允许访问的资源取决于其用户身份以及在 Citrix DaaS 中与该身份关联的资源。有一篇相关文章提供了关于利用 Entra ID 和 AD 身份作为 SAML 提供程序进行商店身份验证的说明。您可以在使用 Entra ID 和 AD 身份进行商店身份验证的 SAML中找到详细说明。

功能范围

本文适用于使用以下 Citrix Cloud 和 Azure 功能组合的用户：

- 用于商店身份验证的 SAML
- Citrix DaaS 和 HDX™ 资源枚举，针对使用 AD 域加入的 VDA 发布的资源
- Entra ID 域加入的 VDA 资源枚举
- Azure 混合域加入的 VDA 资源枚举
- W365 Cloud PC 枚举和启动

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

重要提示：

请勿将此 ME-ID SAML 流程用于 Citrix Cloud 的 SAML 登录，因为这要求 Citrix Cloud 管理员用户是 AD 组的成员，因此应使用 AD 用户身份。您可以在使用 Entra ID 和 AD 身份进行商店身份验证的 SAML中找到详细说明。

AD 身份与 Entra ID 身份：最佳选择?

要确定您的商店用户应使用 SAML AD 身份还是 SAML Entra ID 身份进行身份验证：

1. 确定您打算在用户的商店中向他们提供哪些资源组合。
2. 使用下表确定哪种用户身份类型适用于每种资源类型。

资源类型 (VDA)	用户登录其商店时的身份	需要使用 ENTRA ID 的 SAML 身份吗？	FAS 是否为 VDA 提供单点登录 (SSO)？
已加入 AD	AD，从 AD 导入的 Entra ID（包含 SID）	否。使用默认 SAML。	是
混合加入	AD，从 AD 导入的 Entra ID（包含 SID）	否。使用默认 SAML。	是，对于作为身份提供程序的 AD。如果为 VDA 选择了 Entra ID，则不需要 FAS。
已加入 Entra	Entra ID 本机用户，从 AD 导入的 Entra ID（包含 SID）	是，通过 Entra ID 使用 SAML。	否
Windows 365 云电脑	Entra ID 本机用户，从 AD 导入的 Entra ID（包含 SID）	是，通过 Entra ID 使用 SAML。	否
已加入 AD，已加入 Entra ID，Windows 365 云电脑	从 AD 导入的 Entra ID（包含 SID）	是，通过 Entra ID 使用 SAML。	是，适用于已加入 AD。否，适用于已加入 Entra ID 和 Windows 365 云电脑。

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

更多信息

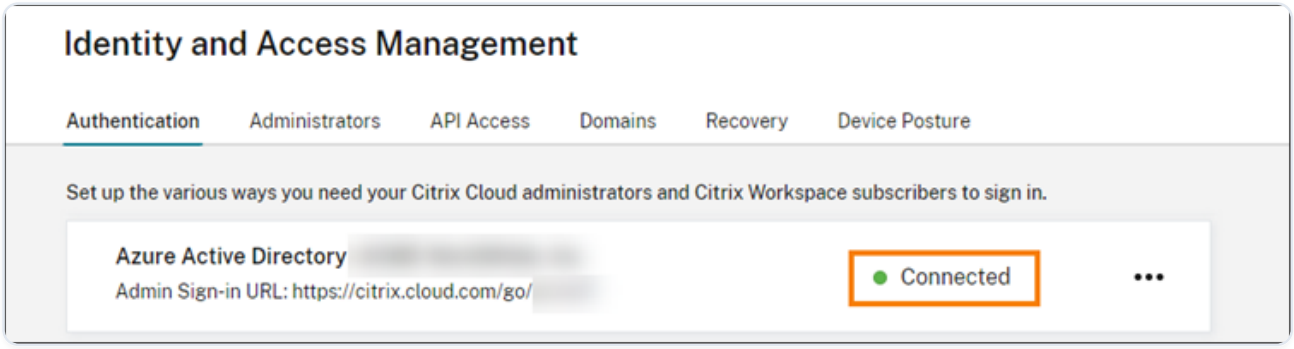
- Citrix DaaS 文档：
  - 计算机身份
  - 适用于 Windows 365 的 Citrix HDX Plus(/zh-cn/citrix-hdxplus-w365)
- Citrix FAS 文档：安装和配置
- Microsoft Azure 文档：什么是 Entra ID Connect？

要求

- 您的 Entra ID 租户必须连接到您的 Citrix Cloud 租户。在 Citrix Cloud 控制台中，您可以通过选择 **身份和访问管理 > 身份验证** 来查找现有的 Entra ID 连接。

或者，

您可以通过选择 **身份和访问管理 > 身份验证 --> 添加身份提供程序 --> 选择 Entra ID** 来创建新的 Entra ID 目录连接。



重要提示：

您必须连接您打算创建新 SAML 应用程序的同一个 Entra ID 租户，该应用程序将使用 ME-ID 身份。

- 商店身份验证方法必须设置为 **SAML 2.0**。请勿使用 Entra ID 作为身份验证方法。要更改商店身份验证方法，请在 Citrix Cloud 控制台中转到 **StoreFront Cloud > 身份验证**。
- UPN 后缀 `@yourdomain.com` 必须作为自定义域名导入并在 Entra ID 中进行验证。在 Azure 门户中，这位于 **Entra ID > 自定义域名** 下。
- Entra ID 用户身份必须使用 Microsoft Entra ID Connect 从 AD 导入。这可确保用户身份正确导入并具有正确的 UPN 后缀。不支持具有 `@yourtenant.onmicrosoft.com` UPN 后缀的 Entra ID 用户。

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

- Citrix FAS 必须部署并连接到 Citrix Cloud 租户和资源位置。FAS 为从 StoreFront Cloud 启动的 HDX 桌面和应用程序提供单点登录。您无需配置 AD 影子帐户，因为 AD 和 Entra ID 用户身份的 UPN `user@customerdomain` 必须匹配。FAS 会生成具有正确 UPN 的必要用户证书，并在启动 HDX 资源时执行智能卡登录。

配置自定义 Entra ID 企业 SAML 应用程序

默认情况下，SAML 登录到商店的行为是针对 AD 用户身份进行断言。**cip_directory** SAML 属性是一个硬编码字符串值，对所有最终用户都相同，并充当一个开关。Citrix Cloud 和 StoreFront Cloud 在登录期间检测到此属性，并触发 SAML 针对 Entra ID 版本的用户身份进行断言。将 **azuread** 参数与此属性一起使用会覆盖默认的 SAML 行为，这会导致商店用户使用其 Entra ID 身份而不是其 AD 身份进行身份验证。

尽管本节中的步骤适用于 Entra ID，但只要执行相同的任务，您就可以使用不同的 SAML 2.0 提供程序（例如 ADFS、Duo、Okta、OneLogin、PingOneSSO 等）创建类似的 SAML 应用程序。您的 SAML 提供程序必须允许您在 SAML 应用程序中配置硬编码的 SAML 属性 (cip_directory = azuread)。只需创建与本节中描述的相同的 SAML 属性映射即可。

1. 登录到 Azure 门户。
2. 从门户菜单中，选择 **Entra ID**。
3. 在左侧窗格的 **Manage**（管理）下，选择 **Enterprise Applications**（企业应用程序）。
4. 从工作窗格中的命令栏中，选择 **New Application**（新建应用程序）。
5. 从命令栏中，选择 **Create your own application**（创建您自己的应用程序）。请勿使用 Citrix Cloud SAML SSO 企业应用程序模板。该模板不允许您修改声明和 SAML 属性列表。
6. 输入应用程序的名称，然后选择 **Integrate any other application you don't find in the gallery (Non-gallery)**（集成库中未找到的任何其他应用程序（非库））。单击 **Create**（创建）。此时将显示应用程序概述页面。
7. 从左侧窗格中，选择 **Single sign-on**（单一登录）。从工作窗格中，选择 **SAML**。
8. 在 **Basic SAML Configuration**（基本 SAML 配置）部分中，选择 **Edit**（编辑）并配置以下设置：

   a. 在 **Identifier (Entity ID)**（标识符（实体 ID））部分中，选择 **Add identifier**（添加标识符），然后输入与您的 Citrix Cloud 租户所在区域关联的值：

      - 对于欧盟、美国和亚太南部区域，输入 `https://saml.cloud.com`。
      - 对于日本区域，输入 `https://saml.citrixcloud.jp`。
      - 对于 Citrix Cloud Government 区域，输入 `https://saml.cloud.us`。

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

b. 在 **Reply URL (Assertion Consumer Service URL)**（回复 URL（断言消费者服务 URL））部分中，选择 **Add reply URL**（添加回复 URL），然后输入与您的 Citrix Cloud 租户所在区域关联的值：

- 对于欧盟、美国和亚太南部地区，输入 `https://saml.cloud.com/saml/acs`。
- 对于日本地区，输入 `https://saml.citrixcloud.jp/saml/acs`。
- 对于 Citrix Cloud Government 地区，输入 `https://saml.cloud.us/saml/acs`。

c. 在“**注销 URL（可选）**”部分中，输入与您的 Citrix Cloud 租户所在区域关联的值：

- 对于欧盟、美国和亚太南部地区，输入 `https://saml.cloud.com/saml/logout/callback`。
- 对于日本地区，输入 `https://saml.citrixcloud.jp/saml/logout/callback`。
- 对于 Citrix Cloud Government 地区，输入 `https://saml.cloud.us/saml/logout/callback`。

d. 在命令栏中，选择“**保存**”。

9. 在“**属性和声明**”部分中，选择“**编辑**”以配置以下声明。这些声明将显示在 SAML 响应中的 SAML 断言内。

a. 对于“**唯一用户标识符 (名称 ID)**”声明，将默认值更新为 `user.localuserprincipalname`。

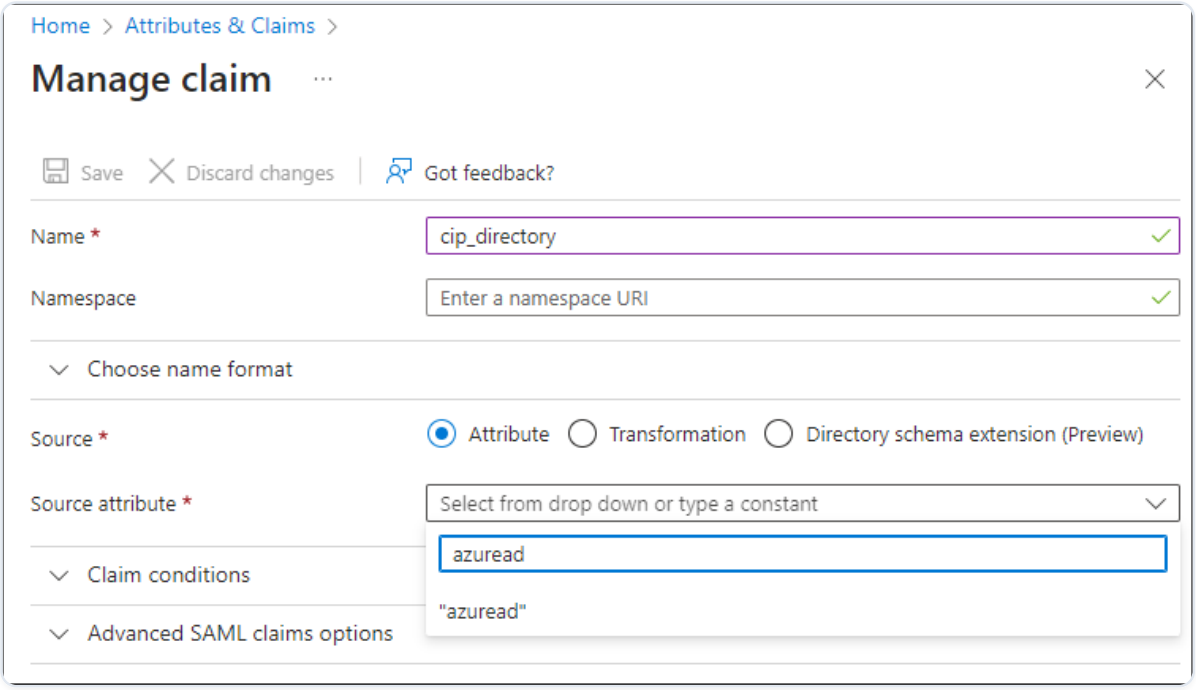
b. 在命令栏中，选择“**添加新声明**”。

c. 在“**名称**”中，输入 **cip_directory**。

d. 在“**源**”中，保持选中“**属性**”。

e. 在“**源属性**”中，输入 **azuread**。输入后，此值将显示在引号中。

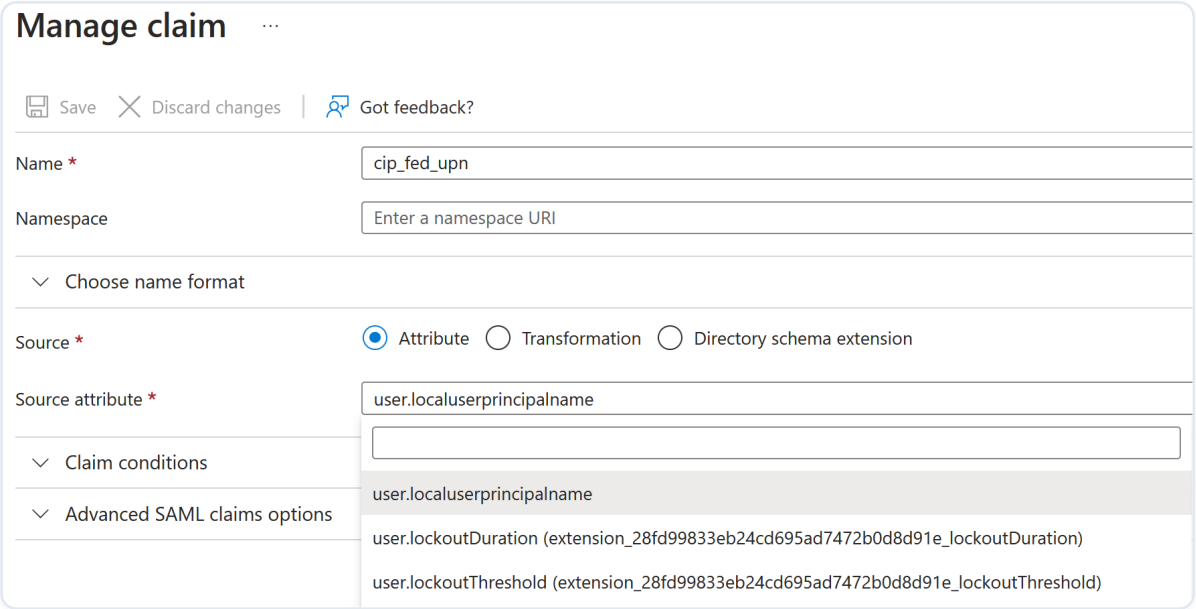
© 1997–2026 Citrix Systems, Inc. All rights reserved.



f. 从命令栏中，选择**保存**。

g. 在**名称**和**源属性**字段中，使用以下值创建其他声明：

名称	源属性
cip_fed_upn	user.localuserprincipalname
displayName	user.displayname
givenName	user.givenname
familyName	user.surname



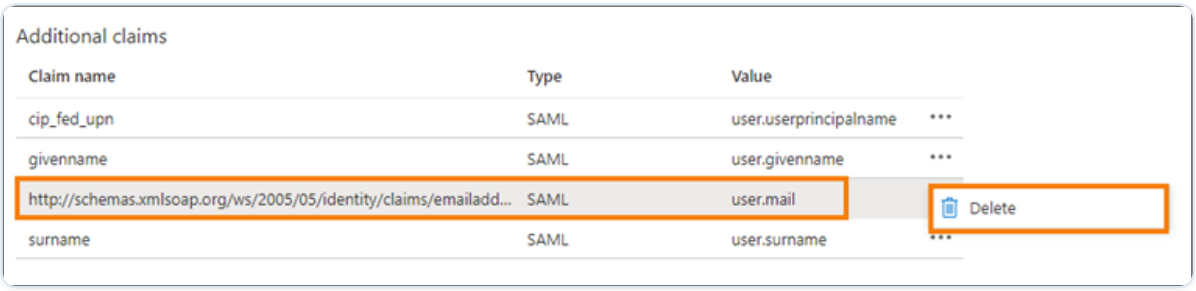
© 1997–2026 Citrix Systems, Inc. All rights reserved.

重要提示：

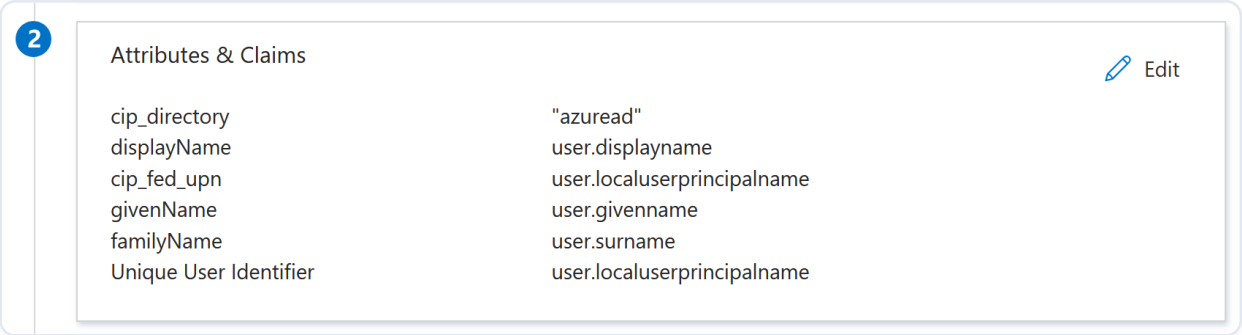
您可以通过为每个声明重复步骤 b-f，或者通过修改**附加声明**部分中已包含上表中列出的源属性的默认声明来创建这些附加声明。默认声明包含命名空间 `http://schemas.xmlsoap.org/ws/2005/05/identity/claims`。

如果您修改默认声明，则必须从每个声明中删除命名空间。如果您创建新声明，则必须删除包含命名空间的声明。如果生成的 SAML 断言中包含带有此命名空间的声明，则该断言将无效，并且将包含不正确的 SAML 属性名称。

h. 在“**附加声明**”部分中，对于任何带有 `http://schemas.xmlsoap.org/ws/2005/05/identity/claims` 命名空间的剩余声明，单击省略号 (...) 按钮，然后单击“**删除**”。

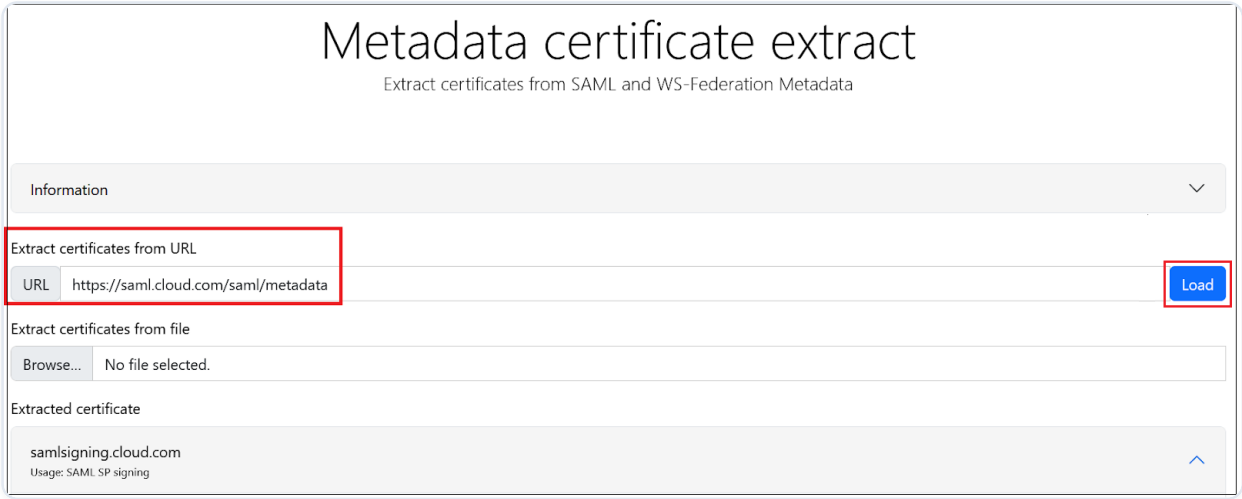


完成后，“**属性和声明**”部分将显示如下所示：

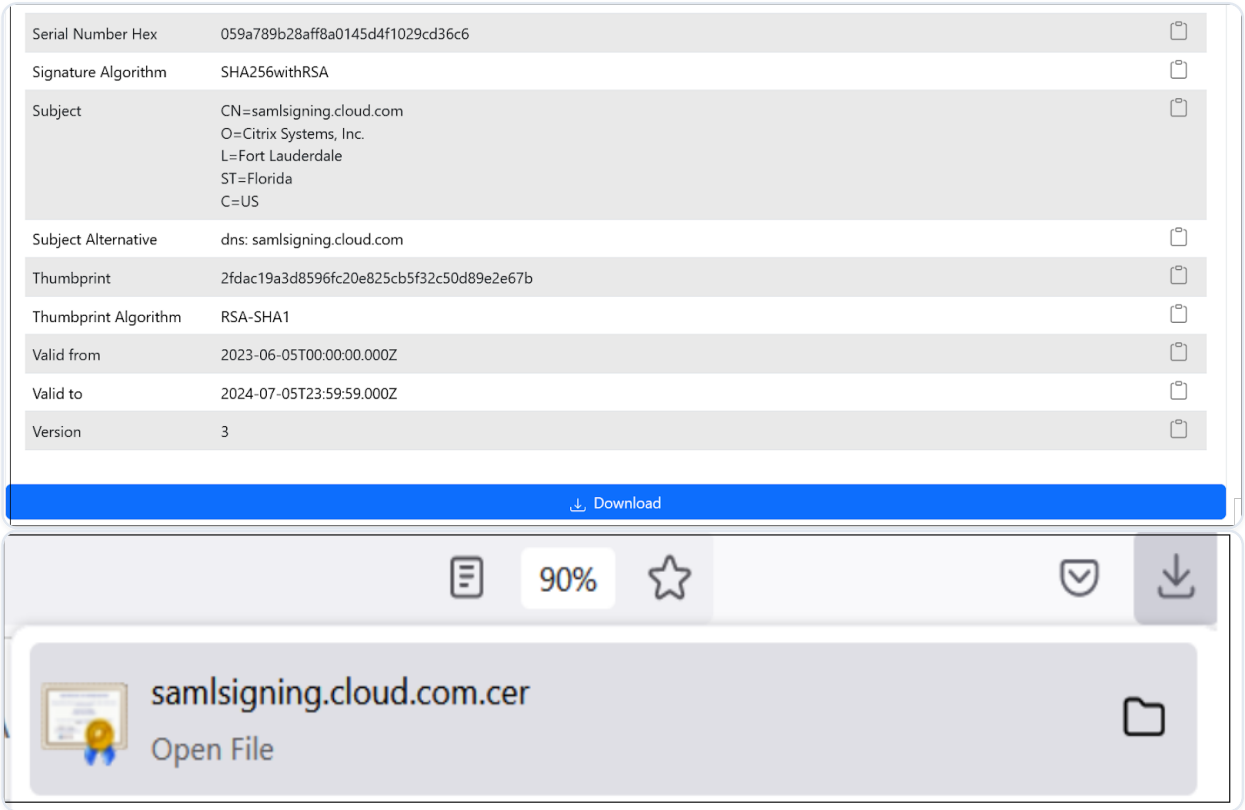


10. 使用此第三方在线工具获取 Citrix Cloud SAML 签名证书的副本。
11. 在 URL 字段中输入 `<https://saml.cloud.com/saml/metadata>`，然后单击“**加载**”。

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

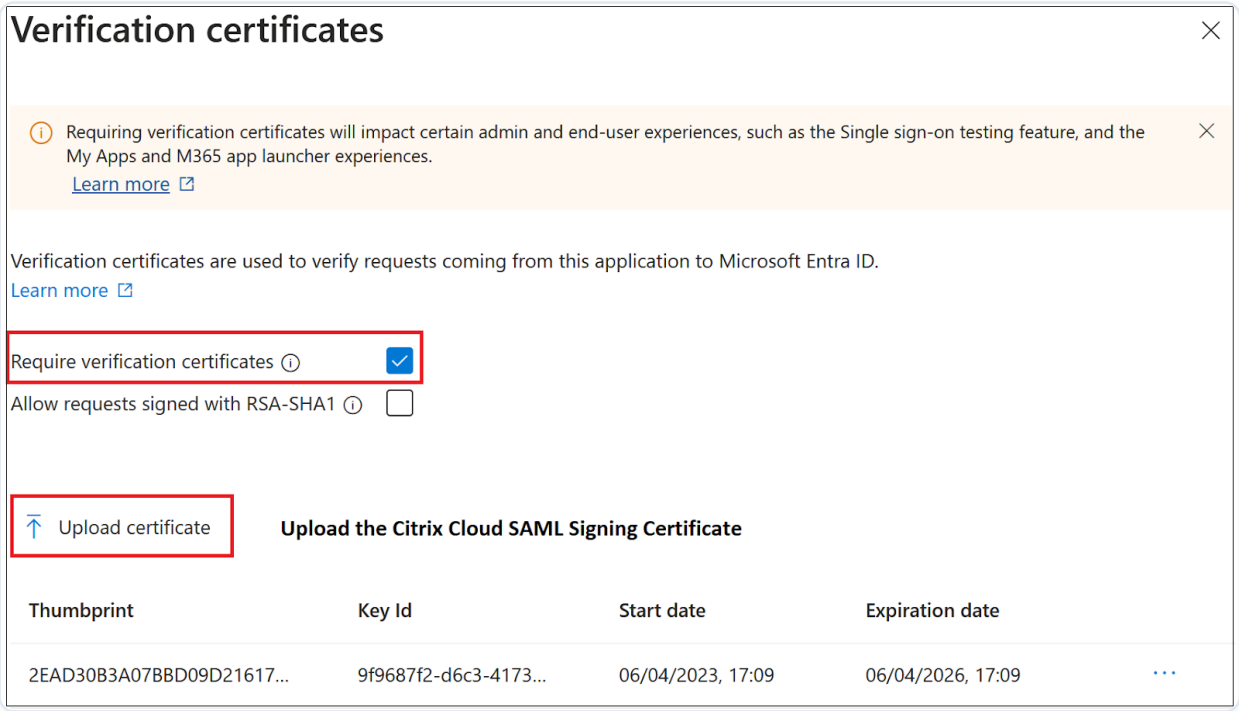


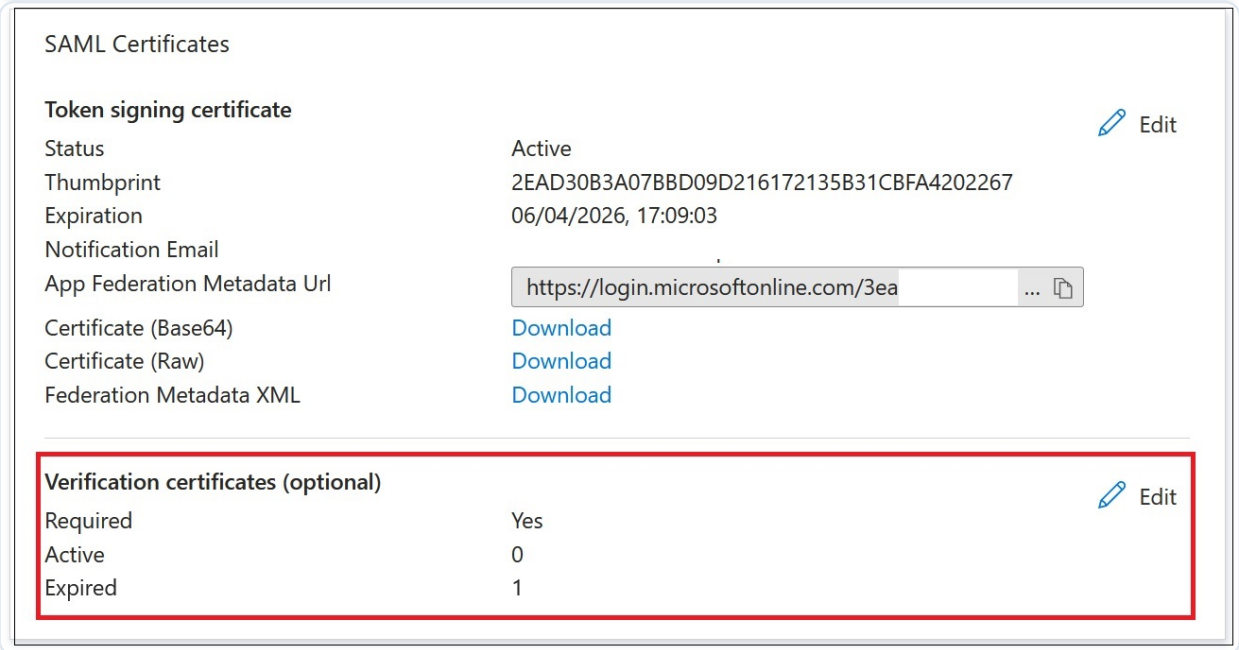
12. 滚动到页面底部，然后单击“**下载**”。



13. 配置 Entra ID SAML 应用程序签名设置。
14. 在 Entra ID SAML 应用程序中上传在步骤 10 中获得的生产 SAML 签名证书。
    - 启用“**需要验证证书**”。

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





故障排除

1. 验证您的 SAML 断言包含正确的用户属性，可以使用 SAML 网络工具，例如 SAML-tracer 浏览器扩展。
2. 找到以黄色显示的 SAML 响应，并与此示例进行比较：

3. 单击底部窗格中的 **SAML** 选项卡，以解码 SAML 响应并将其视为 XML。

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

4. 滚动到响应底部，并验证 SAML 断言包含正确的 SAML 属性和用户值。


```
HTTP    Parameters    SAML    Summary
        <Conditions NotBefore="2025-01-07T12:19:02.866Z"
                    NotOnOrAfter="2025-01-07T13:24:02.866Z"
                    >
            <AudienceRestriction>
                <Audience>https://saml.cloud       .com/                                    </Audience>
            </AudienceRestriction>
        </Conditions>
        <AttributeStatement>
            <Attribute Name="http://schemas.microsoft.com/identity/claims/tenantid"
                       NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
                       >
                <AttributeValue>                                    </AttributeValue>
            </Attribute>
            <Attribute Name="http://schemas.microsoft.com/identity/claims/objectidentifier"
                       NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
                       >
                <AttributeValue>                                    </AttributeValue>
            </Attribute>
            <Attribute Name="http://schemas.microsoft.com/identity/claims/identityprovider"
                       NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
                       >
                <AttributeValue>https://sts.windows.net/                                  /</AttributeValue>
            </Attribute>
            <Attribute Name="http://schemas.microsoft.com/claims/authnmethodsreferences"
                       NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
                       >
                <AttributeValue>http://schemas.microsoft.com/ws/2008/06/identity/authenticationmethod/password</AttributeValue>
            </Attribute>
            <Attribute Name="cip_directory">
                <AttributeValue>azuread</AttributeValue>
            </Attribute>
            <Attribute Name="displayName">
                <AttributeValue>         </AttributeValue>
            </Attribute>
            <Attribute Name="firstName">
                <AttributeValue>    </AttributeValue>
            </Attribute>
            <Attribute Name="lastName">
                <AttributeValue>    </AttributeValue>
            </Attribute>
            <Attribute Name="cip_fed_upn">
                <AttributeValue>        @      .com</AttributeValue>
            </Attribute>
        </AttributeStatement>
        <AuthnStatement AuthnInstant="2025-01-07T12:24:01.191Z"
                        SessionIndex="_c84f3c5d-94d1-4220-8da8-faa6c5125400"
                        >
            <AuthnContext>
                <AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:Password</AuthnContextClassRef>
            </AuthnContext>
        </AuthnStatement>
    </Assertion>
</samlp:Response>
```


如果您的最终用户仍然无法登录其应用商店，请联系 Citrix 支持并提供以下信息：

- SAML-tracer 捕获
- 登录应用商店失败的日期和时间
- 受影响的用户名
- 您用于登录应用商店的客户端计算机的调用方 IP 地址。您可以使用 https://whatismyip.com 等工具获取此 IP 地址。

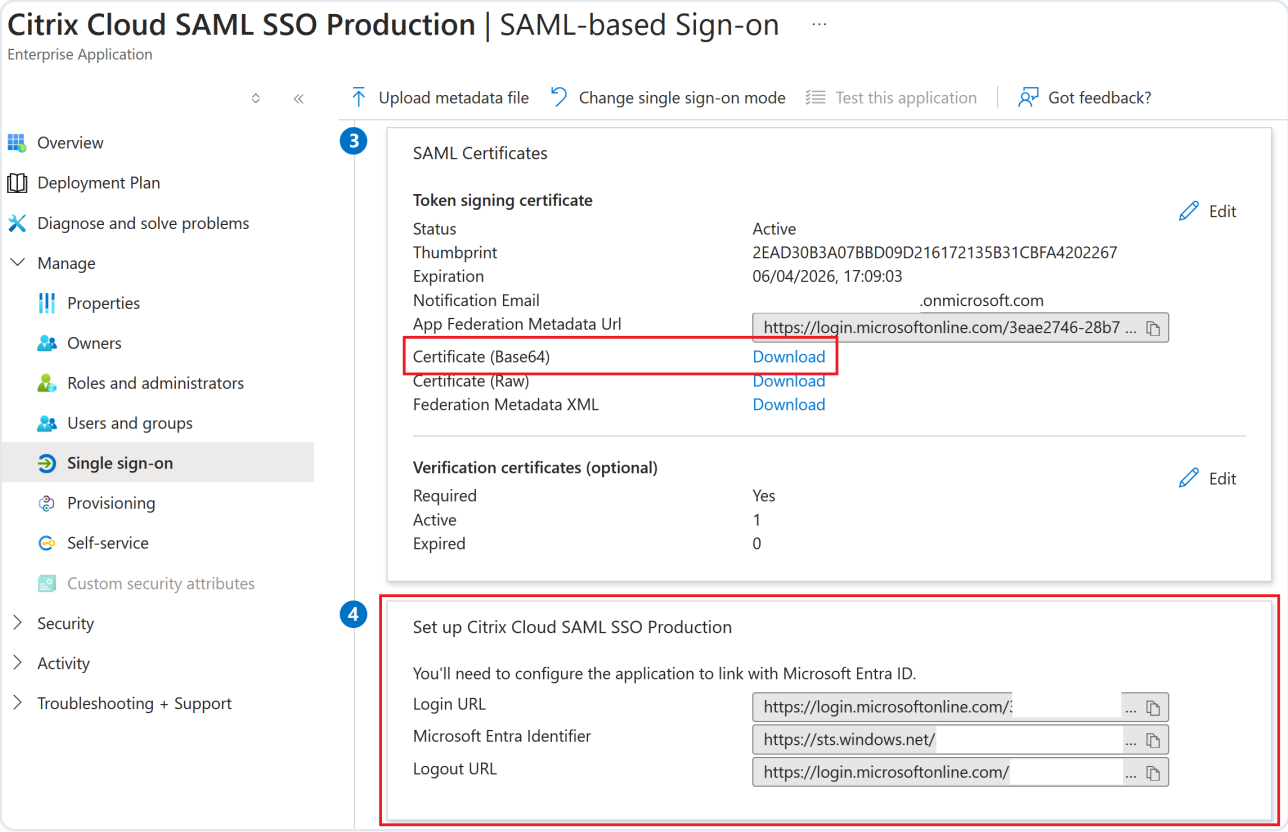
配置 Citrix Cloud SAML 连接

所有 Citrix 登录流程都需要由服务提供商发起，使用应用商店 URL 或 Citrix Cloud GO URL。

在**身份和访问管理 > 身份验证 > 添加身份提供程序 > SAML**中，使用 SAML 连接的默认推荐值。

从您的 Entra ID 门户获取 Entra ID SAML 应用程序的 SAML 端点，并将其输入到 Citrix Cloud 中。

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



在 Citrix Cloud SAML 连接中使用的 Entra ID SAML 端点示例

重要提示：

EntraID SSO 和注销 SAML 端点是相同的 URL。

在 CITRIX CLOUD 的此字段中	输入此值
实体 ID	`https://sts.windows.net/<yourEntraIDTenantID>`
签署身份验证请求	是
SSO 服务 URL	`https://login.microsoftonline.com/<yourEntraIDTenantID>/saml2`
SSO 绑定机制	HTTP 提交
SAML 响应	签署响应或断言
身份验证上下文	未指定，精确

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

在 CITRIX CLOUD 的此字段中	输入此值
注销 URL	`https://login.microsoftonline.com/<yourEntraIDTenantID>/saml2`
签署注销请求	是
SLO 绑定机制	HTTP 提交

使用 Entra ID 的 SAML，用于访客和 B2B 身份进行商店身份验证

在阅读本文之前，您必须了解 B2B SAML 是否适合您的身份验证用例。在决定实施此特定特殊情况的 SAML 解决方案之前，请仔细阅读用例描述和常见问题解答。在继续之前，请确保您完全理解 B2B SAML 适用的场景以及您需要使用的身份类型。

先决条件

- 一个专门配置用于 B2B SAML 的 SAML 应用程序，该应用程序仅在 SAML 断言中发送 **cip_upn** 进行身份验证。
- SAML 提供程序中的前端用户。
- 一个资源位置，其中包含一对连接到 AD 林和域的 Citrix Cloud™ 连接器，AD 影子帐户在此处创建。
- 使用隐式 UPN 或将备用 UPN 后缀添加到创建 AD 影子帐户的后端 AD 林。
- 具有匹配 UPN 的后端 AD 影子帐户。
- 映射到 AD 影子帐户用户的 DaaS 或 CVAD 资源。
- 一个或多个链接到同一资源位置的 FAS 服务器。

常见问题

我为什么要使用 B2B SAML?

大型组织邀请承包商和临时员工加入其身份平台的情况非常普遍。目标是使用用户现有身份（例如承包商电子邮件地址或组织外部的电子邮件地址）授予承包商对商店的临时访问权限。`B2B SAML` 允许使用在发布 DaaS 资源的 AD 域中不存在的本机或访客前端身份。

什么是 B2B SAML?

AD 属性	SAML 断言中的默认属性名称
userPrincipalName	cip_upn

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

AD 属性	SAML 断言中的默认属性名称
邮件	cip_email
objectSID	cip_sid
objectGUID	cip_oid

身份验证所需的其他三个 AD 用户属性 objectSID、objectGUID 和 mail 是通过连接到存在 AD 影子帐户的 AD 域的 Citrix Cloud 连接器获取的。在商店或 Citrix Cloud 的 SAML 登录流程中，它们不再需要包含在 SAML 断言中。

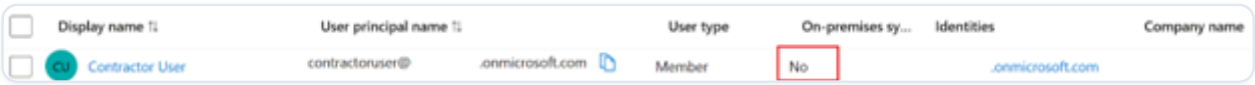
AD 属性	SAML 断言中的默认属性名称
userPrincipalName	cip_upn

重要提示：

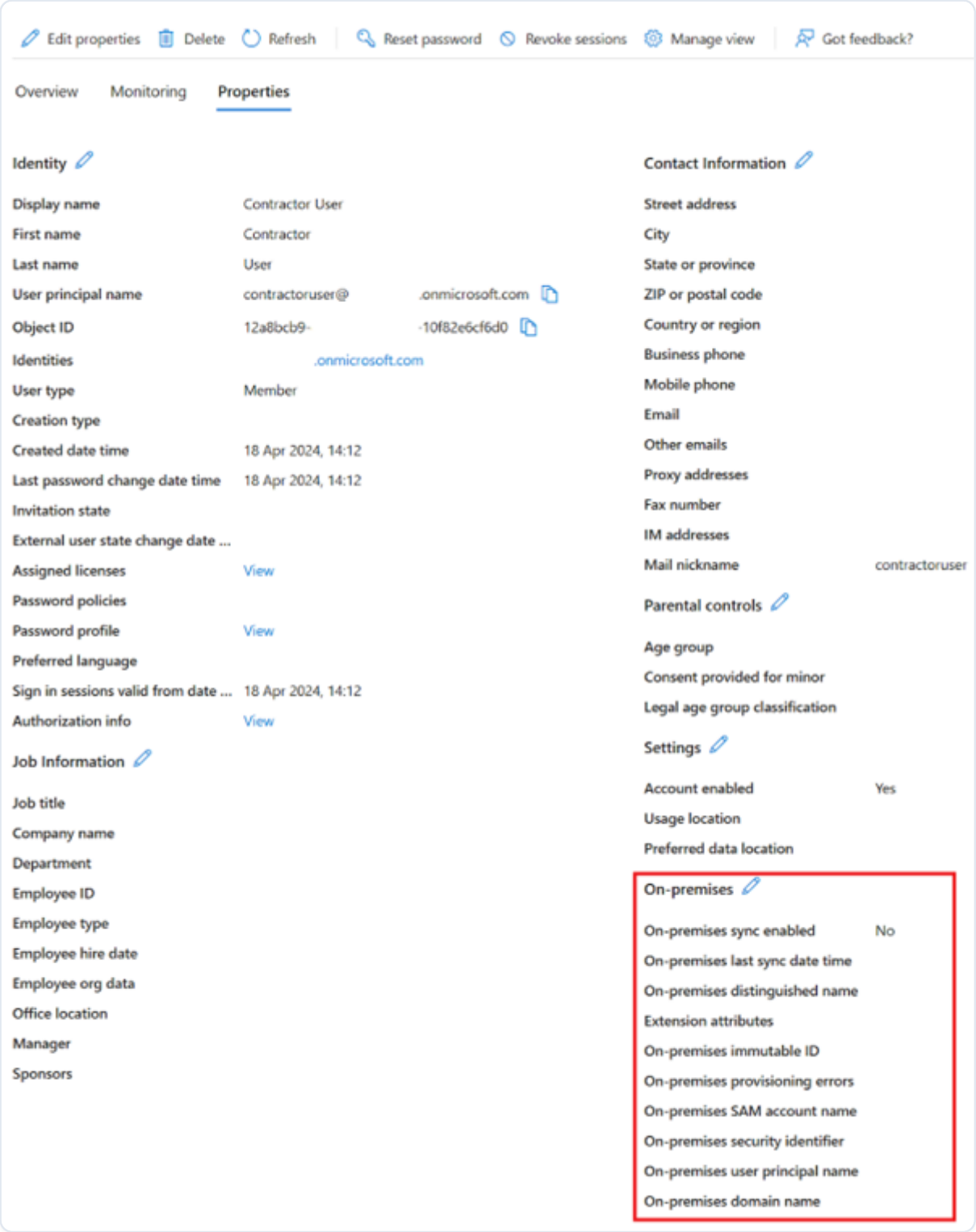
仍然需要为所有 SAML 流程（包括 `B2B SAML`）发送 **displayName**。商店 UI 需要 **displayName** 才能正确显示商店用户的全名。

什么是原生 SAML 用户身份?

原生 SAML 用户是一种仅存在于您的 SAML 提供商目录（例如 Entra ID 或 Okta）中的用户身份。这些身份不包含本地用户属性，因为它们不是通过 AD 同步工具（如 Entra ID Connect）创建的。它们需要匹配的 AD 后端影子帐户才能枚举和启动 DaaS 资源，原生 SAML 用户必须映射到 Active Directory 中的相应帐户。



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



什么是从其他 Entra ID 租户导入的 B2B 用户?

B2B 用户是 Entra ID 用户，它作为成员存在于 Entra ID 租户 1 中，并被邀请到其他 Entra ID 租户（例如 Entra ID 租户 2）作为访客用户。B2B SAML 应用程序在 Entra ID 租户 2 中配置，并作为 SAML IdP 连接到 Citrix Cloud。B2B 用户需要匹配的 AD 后端影子帐户才能枚举和启动 DaaS 资源。B2B 用户必须映射到 Active Directory 中的相应影子帐户。

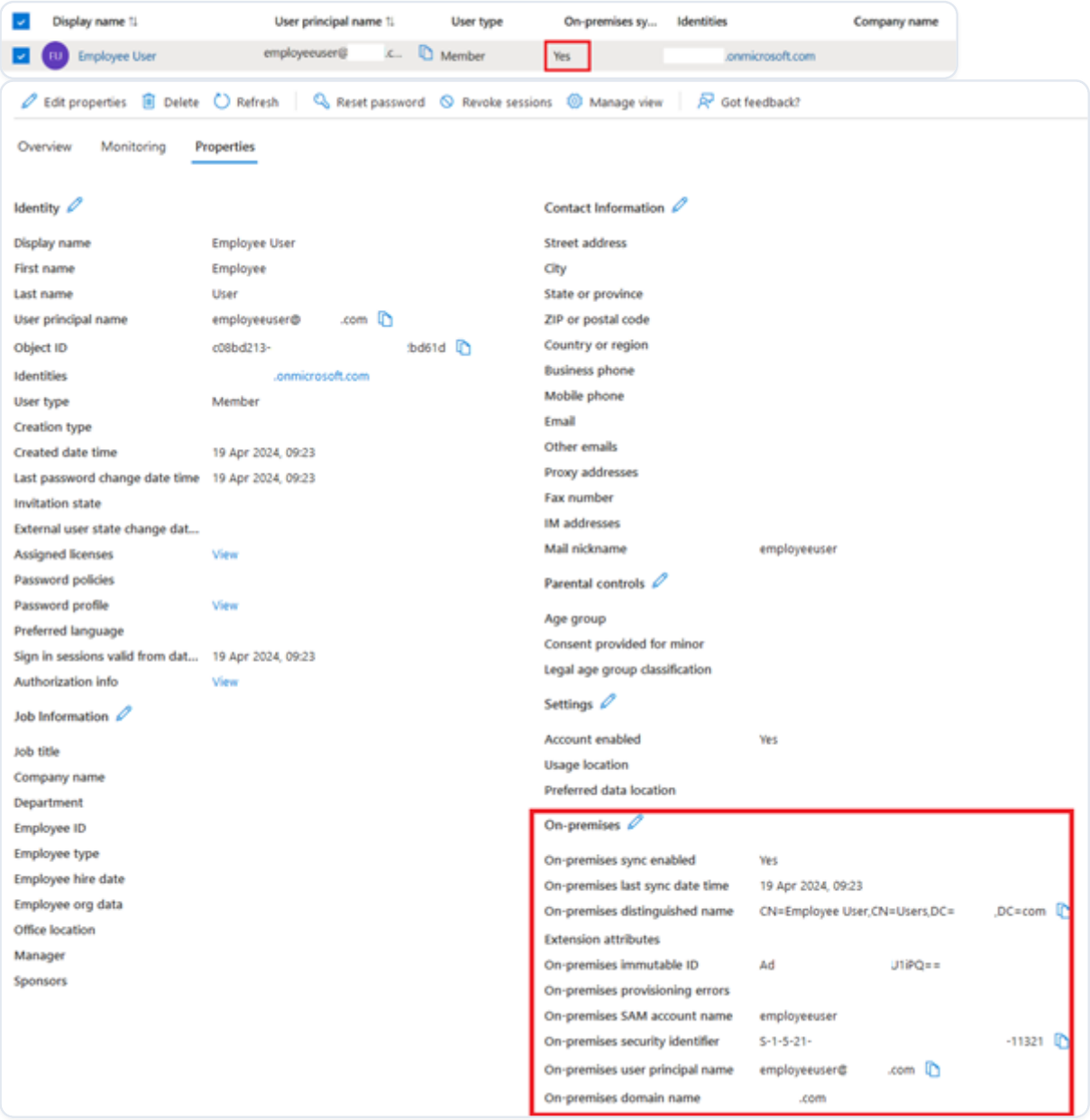
© 1997–2026 Citrix Systems, Inc. All rights reserved.

有关 B2B 用户以及如何将其他 Entra ID 租户的成员用户邀请到您的 Entra ID 租户作为访客用户的详细信息，请参阅 Microsoft 文档。

概述：与外部访客进行 B2B 协作以支持您的员工队伍 Microsoft Entra B2B 协作用户的属性

什么是 AD 支持的 SAML 用户身份?

AD 支持的 SAML 用户是一种用户身份，它存在于您的 SAML 提供商目录（如 Entra ID 或 Okta）中，也存在于您的本地 AD 林中。这些身份包含本地用户属性，因为它们是通过 AD 同步工具（如 Entra ID Connect）创建的。这些用户不需要 AD 后端影子帐户，因为它们包含本地 SID 和 OID，因此可以枚举和启动使用 AD 域加入的 VDA 发布的 DaaS 资源。



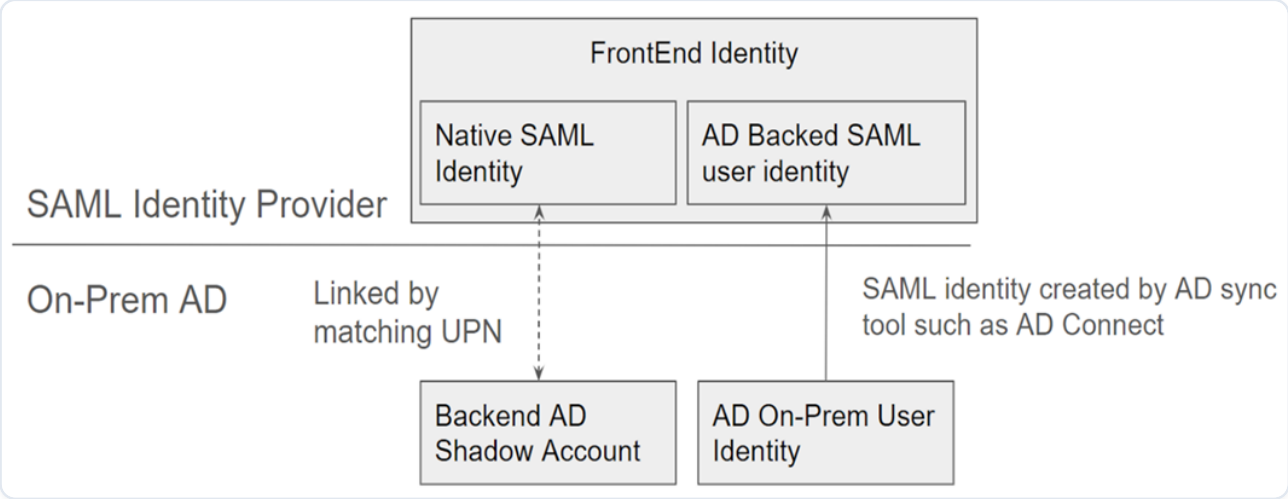
什么是前端身份?

前端身份是用于登录 SAML 提供商和商店的身份。前端身份具有不同的用户属性，具体取决于它们在 SAML 提供商中创建的方式。

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

1. 本机 SAML 用户身份
2. AD 支持的 SAML 用户身份

您的 SAML 提供商可能混合了这两种类型的身份。例如，如果您的身份平台中既有承包商也有正式员工，`B2B SAML` 将适用于这两种前端身份，但仅当您拥有某些属于本机 SAML 用户身份类型的帐户时才强制要求。



什么是后端 AD 影子帐户？

后端 AD 影子帐户是 DaaS 使用的 AD 帐户，它映射到 SAML 提供商中的相应前端身份。

为什么需要后端 AD 影子帐户？

为了枚举使用已加入 AD 域的 VDA 发布的 DaaS 或 CVAD 资源，需要 VDA 所加入的 Active Directory 林中的 AD 帐户。将 DaaS 交付组中的资源映射到影子帐户用户，以及映射到您将 VDA 加入的 AD 域中包含影子帐户的 AD 组。

重要：

只有没有 AD 域属性的本机 SAML 用户才需要匹配的 AD 影子帐户。如果您的前端身份是从 Active Directory 导入的，则无需使用 `B2B SAML`，并且无需创建后端 AD 影子帐户。

如何将前端身份链接到相应的后端 AD 影子帐户？

链接前端身份和后端身份的方法是使用匹配的 UPN。这两个链接的身份应具有相同的 UPN，以便商店可以识别它们代表需要登录商店并枚举和启动 DaaS 资源的同一最终用户。

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

重要

单个前端身份只能映射到单个 AD 林/域中的单个后端身份。DaaS 资源的枚举将仅使用从正确的 Citrix Cloud 连接器执行的 AD 影子帐户查找中获取的一个 SID 值。您不能使用与具有相同 UPN 后缀的多个 AD 影子帐户匹配的单个前端用户来创建一对多关系。后端 AD 影子帐户应仅存在于单个 AD 林/域中。

支持使用前端和后端身份之间明确的 UPN 匹配 前端用户 `(user@yourforest.com)` > AD 林 1 中的后端用户 `(UPN user@yourforest.com)`
不支持，因为在尝试将一个前端身份与一个后端身份匹配时存在 UPN 歧义 前端用户 `(user@yourforest1.com)` > AD 林 1 中的后端用户 `(UPN user@yourforest1.com)` > AD 林 2 中的后端用户 `(UPN user@yourforest1.com)`

B2B SAML 是否需要 Citrix FAS?

是的。当使用任何联合身份验证方法登录到商店时，在启动期间，FAS 是 VDA 单点登录 (SSON) 所必需的。

什么是“SID 不匹配问题”以及何时会发生?

当 SAML 断言包含前端用户的 SID，但该 SID 与 AD 影子账户用户的 SID 不匹配时，就会导致“SID 不匹配问题”。当登录到 SAML 提供程序的账户具有本地 SID，且该 SID 与影子账户用户的 SID 不同时，可能会发生这种情况。这仅在前端身份由 AD 同步工具（如 Entra ID Connect）预配，并且来自与创建影子账户不同的 AD 林时才会发生。

`B2B SAML` 阻止“SID 不匹配问题”的发生。通过连接到后端 AD 域的 Citrix Cloud 连接器，始终为影子账户用户获取正确的 SID。影子账户用户查找是使用前端用户的 UPN 执行的，然后将其匹配到其对应的后端影子账户用户。

SID 不匹配问题示例： **前端用户**由 Entra ID Connect 创建并从 **AD 林 1** 同步。
`S-1-5-21-000000000-0000000000-0000000001-0001`

后端影子账户用户在 **AD 林 2** 中创建并映射到 DaaS 资源
`S-1-5-21-000000000-0000000000-0000000002-0002`

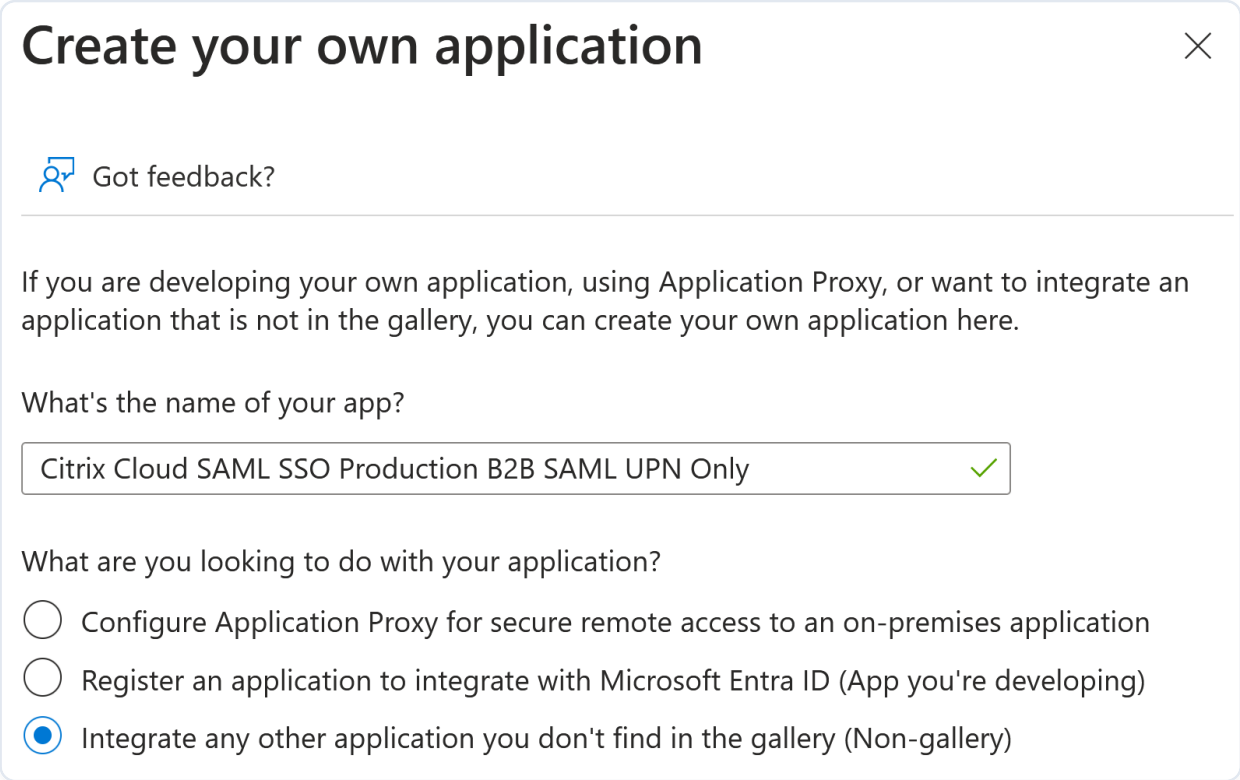
SAML 断言包含所有四个 cip_* 属性，并且 **cip_sid** 包含值 `S-1-5-21-000000000-0000000000-0000000001-0001`，该值与影子账户的 SID 不匹配并触发错误。

为外部访客账户配置 Entra ID 中的 B2B SAML 应用程序

1. 登录到 Azure 门户。

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

2. 从门户菜单中，选择 **Entra ID**。
3. 在左侧窗格的“**管理**”下，选择“**企业应用程序**”。
4. 选择“**创建自己的应用程序**”。
5. 为 SAML 应用程序输入一个合适的名称，例如 `Citrix Cloud SAML SSO Production B2B SAML UPN Only`。



6. 在左侧导航窗格中，选择**单一登录**，然后在工作窗格中，单击**SAML**。
7. 在**基本 SAML 配置**部分中，单击**编辑**并配置以下设置：

   a. 在**标识符（实体 ID）部分中，选择添加标识符**，然后输入与您的 Citrix Cloud 租户所在区域关联的值：

      - 对于欧洲、美国和亚太南部地区，请输入 `https://saml.cloud.com`。
      - 对于日本地区，请输入 `https://saml.citrixcloud.jp`。
      - 对于 Citrix Cloud Government 区域，请输入 `https://saml.cloud.us`。

   b. 在**回复 URL（断言消费者服务 URL）部分中，选择添加回复 URL**，然后输入与您的 Citrix Cloud 租户所在区域关联的值：

      - 对于欧洲、美国和亚太南部地区，请输入 `https://saml.cloud.com/saml/acs`。
      - 对于日本地区，请输入 `https://saml.citrixcloud.jp/saml/acs`。
      - 对于 Citrix Cloud Government 区域，请输入 `https://saml.cloud.us/saml/acs`。

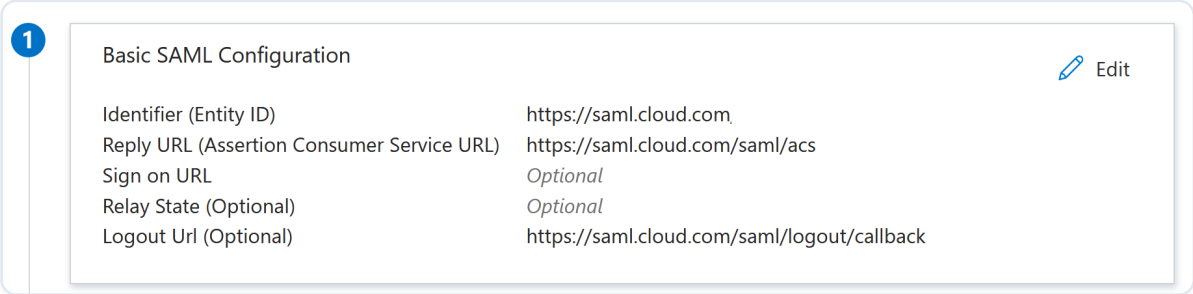
© 1997–2026 Citrix Systems, Inc. All rights reserved.

c. 在**登录 URL**部分中，输入您的商店 URL。

d. 在**注销 URL（可选）**部分中，输入与您的 Citrix Cloud 租户所在区域关联的值：

- 对于欧洲、美国和亚太南部地区，请输入 `https://saml.cloud.com/saml/logout/callback`。
- 对于日本地区，请输入 `https://saml.citrixcloud.jp/saml/logout/callback`。
- 对于 Citrix Cloud Government 区域，输入 `https://saml.cloud.us/saml/logout/callback`。

e. 在命令栏中，单击“**保存**”。“**基本 SAML 配置**”部分显示如下：



8. 在“**属性和声明**”部分中，单击“**编辑**”以配置以下声明。创建 SAML 应用程序后，配置以下属性。

a. 对于唯一用户标识符（名称 ID）声明，将名称标识符格式设置为未指定，并将其源属性设置为 `user.localuserprincipalname`。

b. 对于 **cip_upn** 声明，保留默认值 `user.localuserprincipalname`。

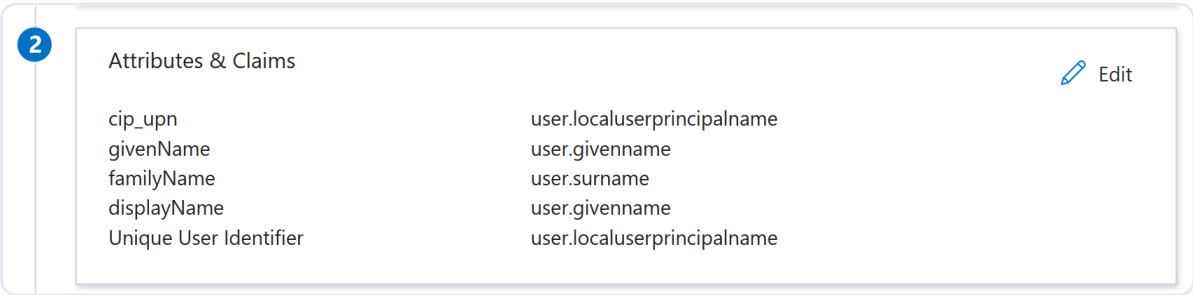
c. 对于 **displayName**，保留默认值 `user.displayname`。

d. 对于 **givenName** 声明，将默认值更新为 `user.givenname`。

e. 对于 **familyName** 声明，将默认值更新为 `user.surname`。

f. 在“**其他声明**”部分中，对于任何带有 `http://schemas.xmlsoap.org/ws/2005/05/identity/claims` 命名空间的剩余声明，单击省略号 (...) 按钮，然后单击“**删除**”。无需包含这些声明，因为它们是上述用户属性的重复项。

完成后，“**属性和声明**”部分显示如下所示：

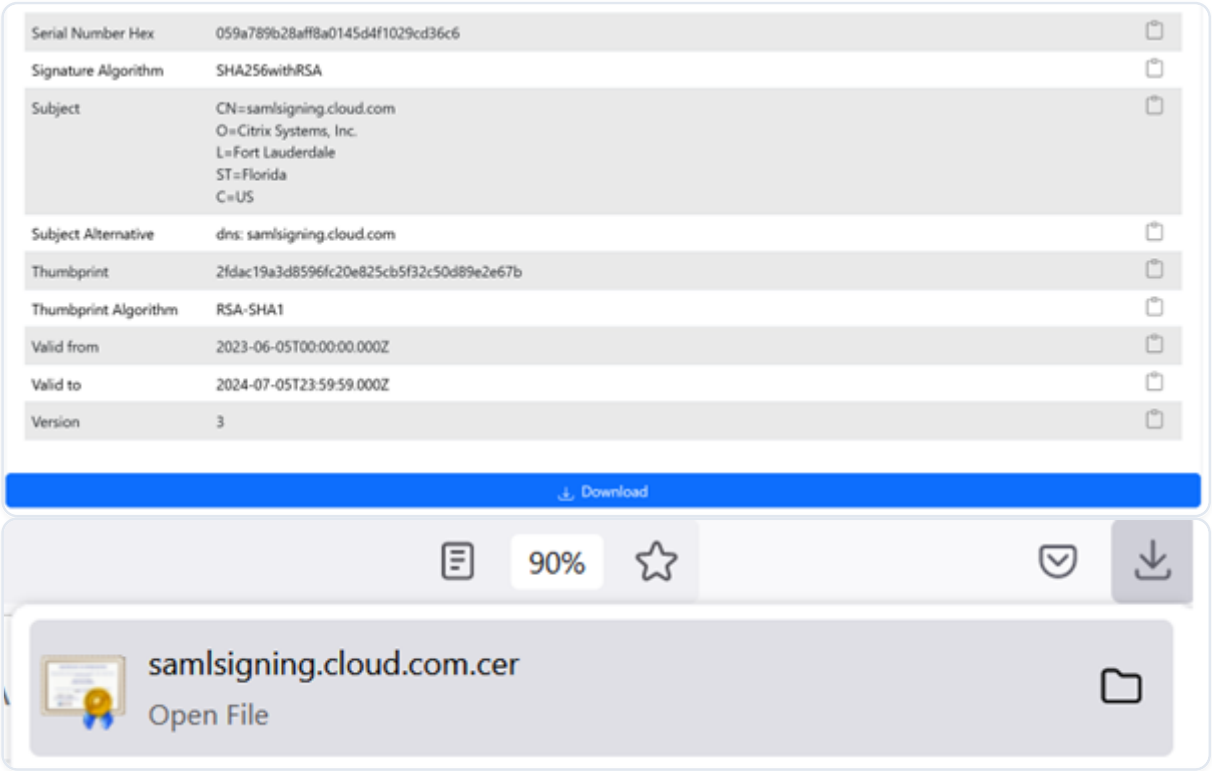


© 1997–2026 Citrix Systems, Inc. All rights reserved.

g. 使用此第三方在线工具 获取 Citrix Cloud SAML 签名证书的副本。

h. 在 URL 字段中输入 `https://saml.cloud.com/saml/metadata`，然后单击“**加载**”。

9. 滚动到页面底部，然后点击 **下载**。

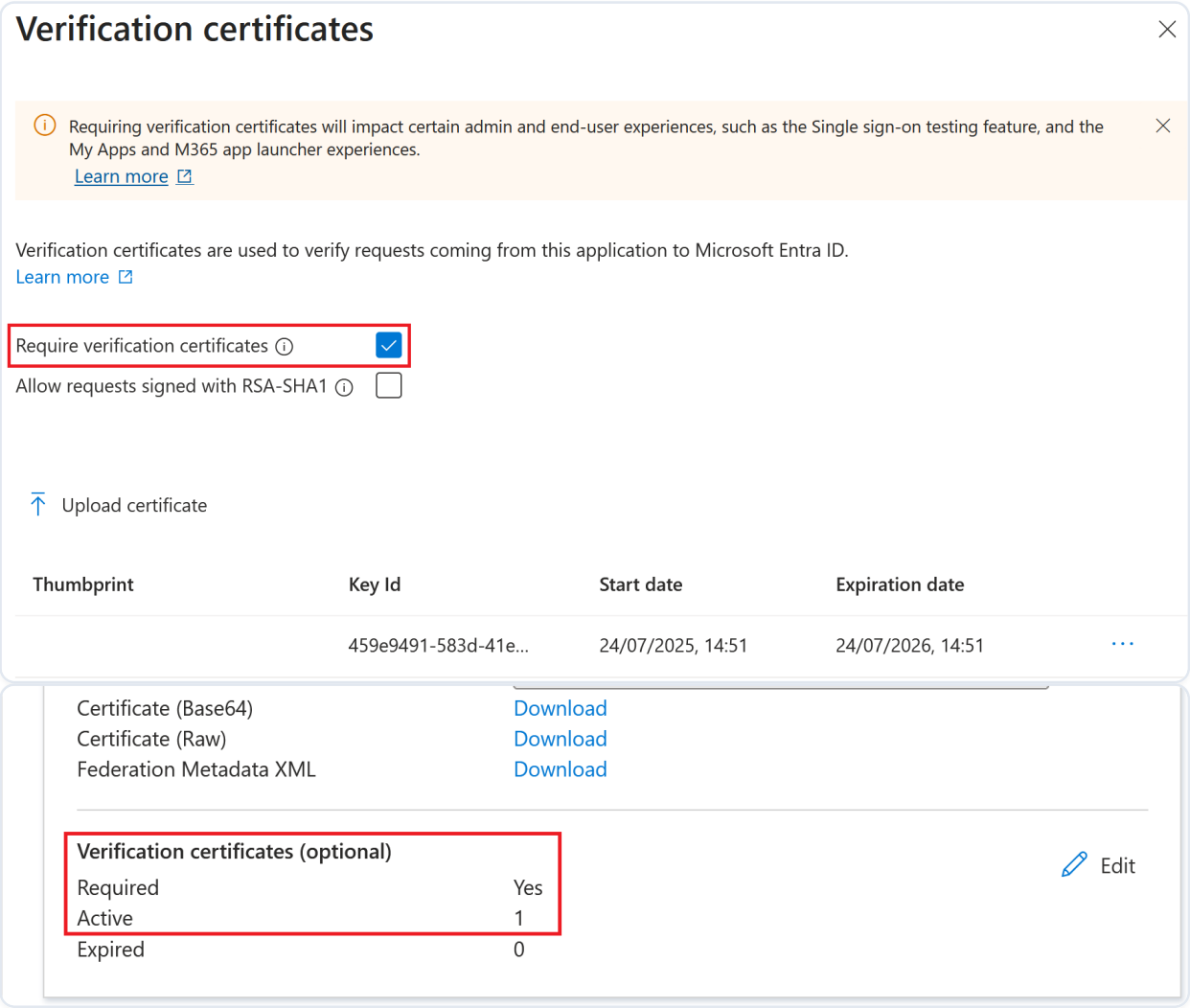


10. 配置 Entra ID SAML 应用程序的签名设置。

11. 在 Entra ID SAML 应用程序中上传在步骤 10 中获取的生产 SAML 签名证书

    a. 启用 **需要验证证书**。

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

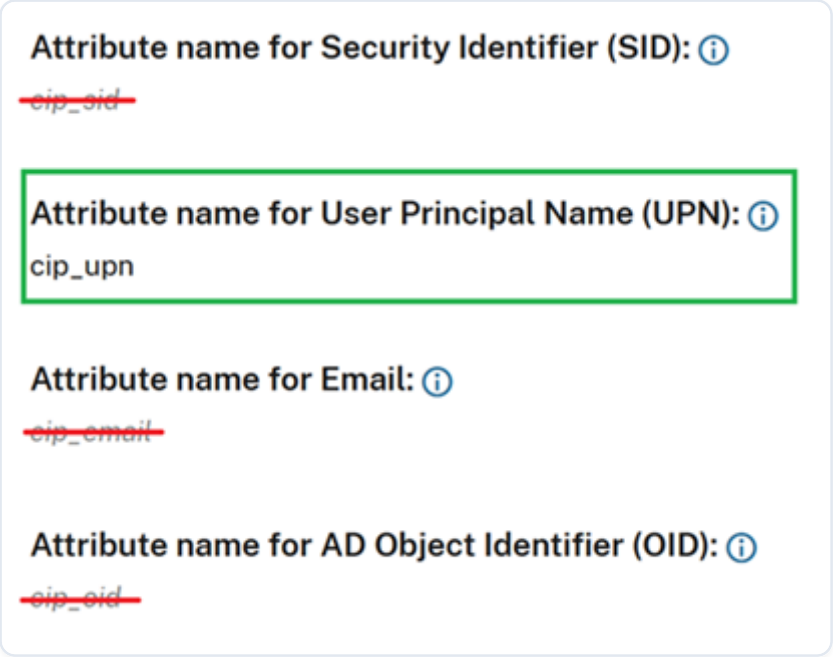


配置 Citrix Cloud B2B SAML 连接

默认情况下，Citrix Cloud 将要求 SAML 断言中存在 cip_upn、cip_email、cip_sid 和 cip_oid，如果未发送这些属性，SAML 登录将失败。为防止这种情况，在创建新的 SAML 连接时，请删除对这些属性的检查。

1. 使用默认设置创建新的 SAML 连接。
2. 导航到底部的 **SAML 属性映射配置** 部分，并在保存新的 SAML 配置之前进行更改。
3. 从 **cip_email**、**cip_sid** 和 **cip_oid** 字段中删除 SAML 属性名称。
4. 不要从 **cip_upn** 字段中删除它。
5. 不要从其他任何属性的相应字段中删除它们。商店 UI 仍然需要 **displayName**，不应更改。

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



配置 AD 影子帐户资源位置和连接器

后端影子帐户 AD 林中需要一个资源位置和连接器对。当 SAML 断言中仅直接提供 cip_upn 时，Citrix Cloud 需要此 AD 林中的连接器来查找影子帐户用户身份和属性，例如 cip_email、cip_sid 和 cip_oid。

1. 创建新的 **资源位置**，其中将包含已加入后端影子帐户 AD 林的 Citrix Cloud 连接器。

2. 命名资源位置以匹配包含您希望使用的后端 AD 影子帐户的 AD 林。
3. 在新创建的资源位置中配置一对 Citrix Cloud 连接器。

例如 `ccconnector1.shadowaccountforest.com` `ccconnector2.shadowaccountforest.com`

在后端 AD 林中配置 FAS

承包商前端用户肯定需要 FAS。在 DaaS 启动期间，承包商用户将无法手动输入 Windows 凭据来完成启动，因为他们可能不知道 AD 影子帐户密码。

1. 在创建影子帐户的后端 AD 林中配置一个或多个 FAS 服务器。
2. 将 FAS 服务器链接到包含一对 Citrix Cloud 连接器的同一资源位置，该连接器已加入创建影子帐户的后端 AD 林。

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

在 AD 域中配置备用 UPN 后缀

重要提示：

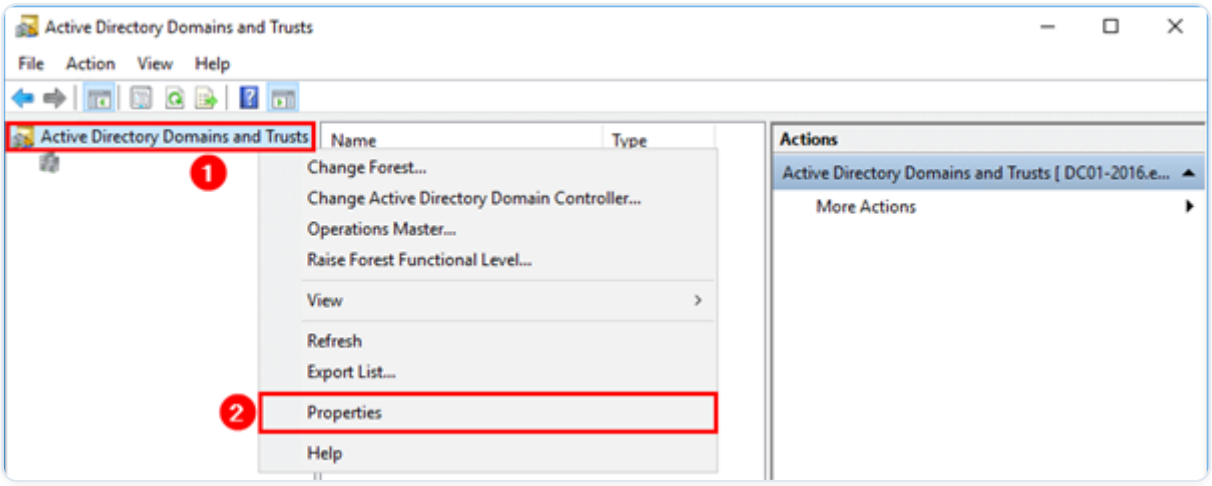
UPN 与用户的电子邮件地址不同。在许多情况下，为了方便使用，它们的值相同，但 UPN 和电子邮件通常可以具有不同的值，并且在不同的 Active Directory 属性和不同的 Entra ID 用户属性中定义。此解决方案依赖于前端和后端身份之间的 UPN 匹配，而不是电子邮件匹配。

如果您的域在 DNS 中可公开路由，您可以使用其隐式 UPN 后缀，或者为希望邀请到 Okta 或 Entra ID 租户中的每个外部前端用户添加一个匹配的备用 UPN 后缀。如果 AD 使用 `yourdomain.local` 作为隐式 UPN，您将必须选择一个备用 UPN 后缀，例如 `yourdomain.com`。Entra ID 不允许您在自定义域名中添加 `yourdomain.local`。

例如，如果您邀请外部用户 `contractoruser@hotmail.co.uk` 并希望将其与后端 AD 影子账户 `contractoruser@yourforest.com` 关联，则在您的 AD 林中添加 `yourforest.com` 作为备用 UPN 后缀。

使用 Active Directory 域和信任 UI 添加 Active Directory 中的备用 UPN 后缀

1. 登录到后端 AD 林中的域控制器。
2. 打开“**运行**”对话框，然后键入 `domain.msc`，再单击“**确定**”。
3. 在“Active Directory 域和信任”窗口中，右键单击“**Active Directory 域和信任**”，然后选择“**属性**”。
4. 在“**UPN 后缀**”选项卡上的“备用 UPN 后缀”框中，添加一个备用 UPN 后缀，然后选择“**添加**”。



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

5. 单击“**确定**”。

使用 PowerShell 管理后端 AD 林的 UPN 后缀

您可能需要向后端 AD 林添加大量新的 UPN 后缀，以创建必要的影子账户 UPN。您需要添加到后端 AD 林的备用 UPN 后缀数量将取决于您选择邀请到 SAML 提供程序租户中的外部用户数量。

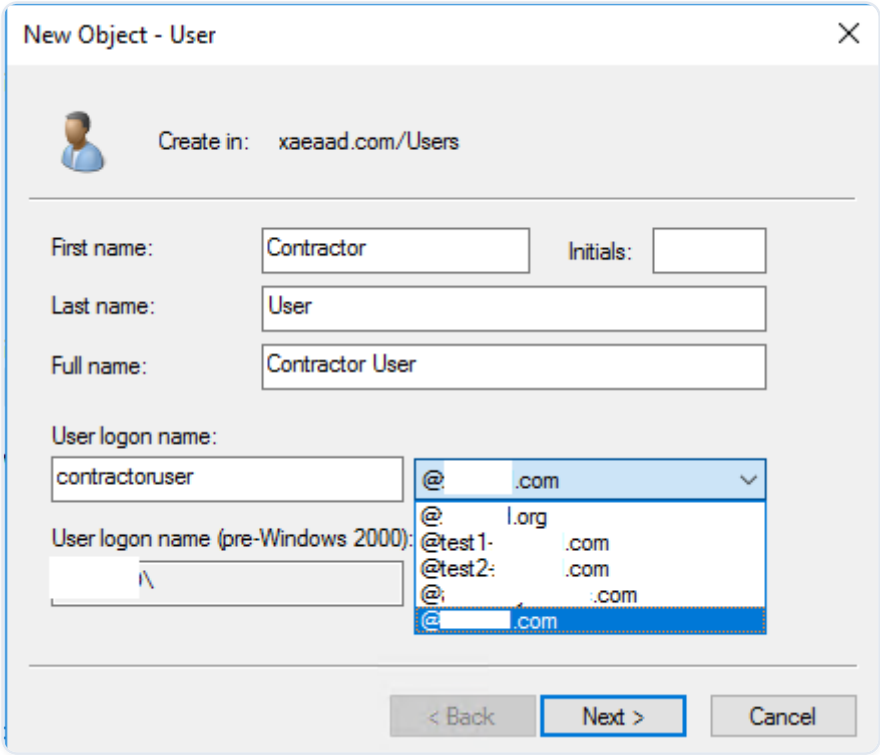
如果需要创建大量新的备用 UPN 后缀，以下是一些实现此目的的 PowerShell 命令。

```
# Get the list of existing ALT UPN suffixes within your AD Forest

(Get-ADForest).UPNSuffixes



# Add or remove ALT UPN Suffixes

$NewUPNSuffixes = @("yourforest.com","externalusers.com")



# Set action to "add" or "remove" depending on the operation you wish to
perform.

$Action = "add"

foreach($NewUPNSuffix in $NewUPNSuffixes)

{

    Get-ADForest | Set-ADForest -UPNSuffixes @{ $Action=$NewUPNSuffix }

}
```

在后端 AD 林中配置 AD 影子账户

1. 创建新的 AD 影子账户用户。
2. 默认情况下，为新的 AD 用户选择 AD 林隐式 UPN，例如 `yourforest.local`。选择您之前创建的适当的备用 UPN 后缀。例如，选择 `yourforest.com` 作为影子帐户用户的 UPN 后缀。

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



影子帐户用户的 UPN 也可以通过 PowerShell 更新。

```
Set-ADUser "contractoruser" -UserPrincipalName
"contractoruser@yourforest.com"
```

重要

Windows AD PowerShell 允许您创建具有任何指定 UPN 后缀的影子帐户用户，即使该 UPN 后缀在您的 AD 林中不存在。您希望使用的备用 UPN 后缀必须存在于 AD 林中，因为 Citrix Cloud 连接器依赖此列表来查找后端影子帐户用户。如果备用 UPN 后缀未按上述屏幕截图所示出现在 AD 林中，则 Citrix Cloud 将无法将您的前端身份与适当的后端 AD 影子帐户匹配。

3. 影子帐户用户的 UPN 应与外部前端身份用户的 UPN 完全匹配。
4. 测试前端用户登录到应用商店。
5. 验证登录成功后，应用商店中是否枚举了所有预期资源。应显示映射到 AD 影子帐户的资源。

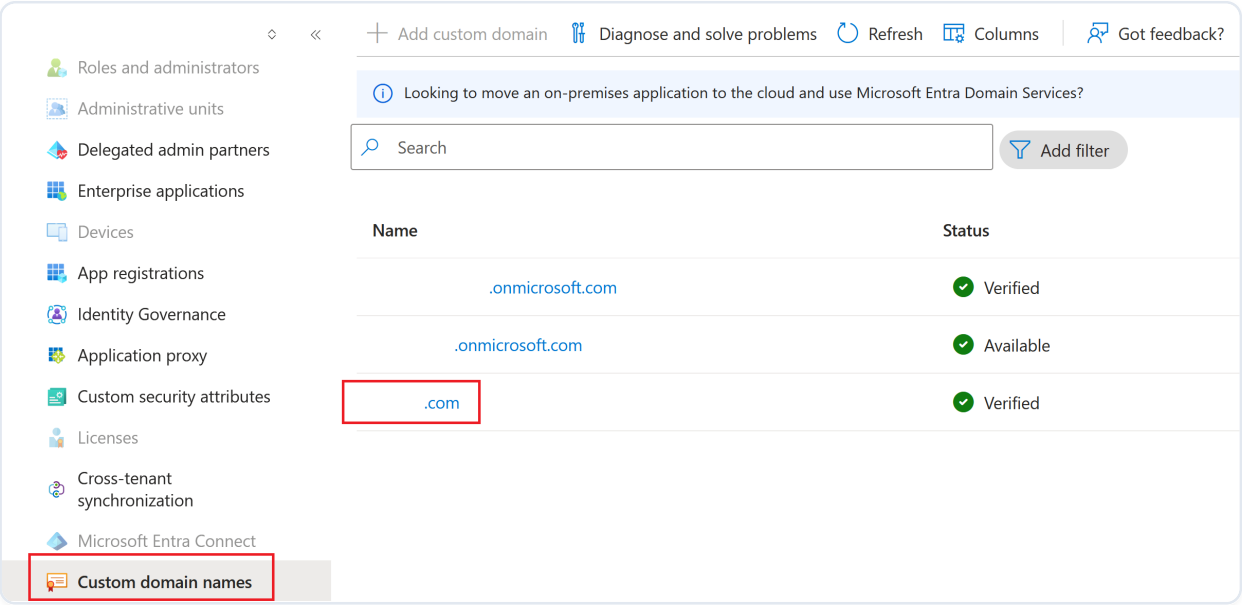
配置来宾 Entra ID 用户 UPN 以匹配 AD 影子帐户 UPN

当外部来宾用户被邀请到 Entra ID 租户时，会创建一个自动生成的 UPN，表明该用户是外部用户。外部 Entra ID 用户将自动分配 @Entra IDtenant.onmicrosoft.com UPN 后缀，这不适用于 B2B

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

SAML，并且与您的 AD 影子帐户不匹配。这需要更新以匹配 Entra ID 中导入的 DNS 域以及您在 AD 林中创建的备用 UPN 后缀。

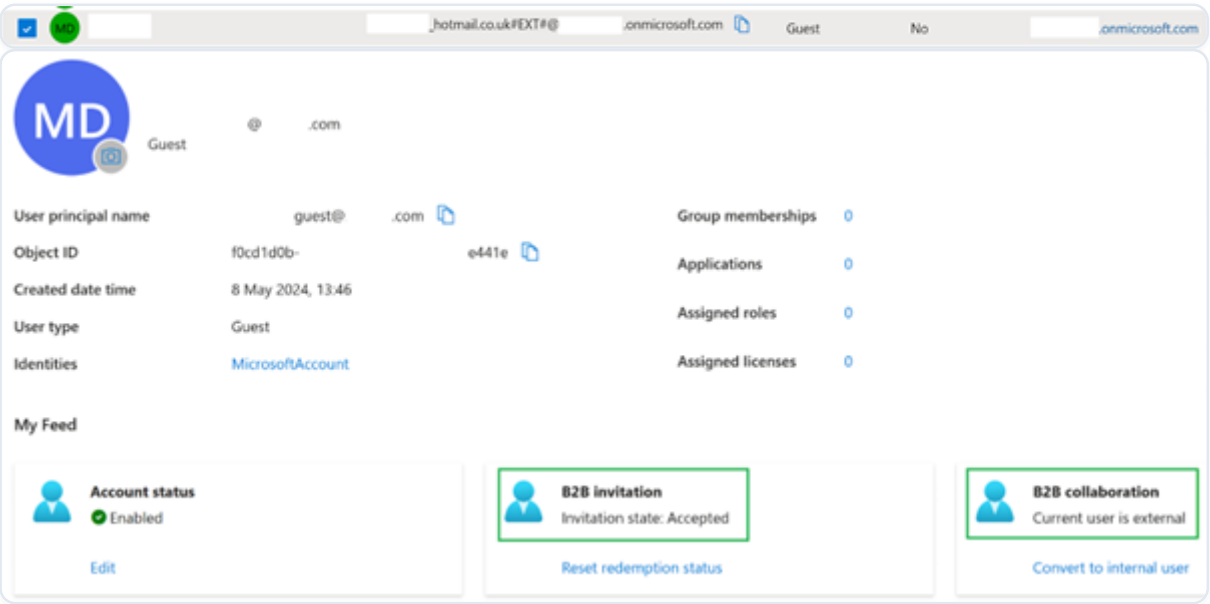
1. 将自定义域导入 Entra ID，该自定义域应与您添加到 AD 林中的备用 UPN 后缀匹配。



2. 邀请一位来宾用户，例如 `contractoruser@hotmail.co.uk`，并确保受邀的来宾用户接受 Microsoft 对 Entra ID 租户的邀请。

   Microsoft 生成的外部来宾用户 UPN 格式示例。

   `contractoruser_hotmail.co.uk#EXT#@yourEntra IDtenant.onmicrosoft.com`



重要提示：

Citrix Cloud 和 StoreFront 不能使用包含 # 字符的 UPN 进行 SAML 身份验证。

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

3. 安装必要的 Azure PowerShell Graph 模块，以便管理 Entra ID 用户。

```
Install-Module -Name "Microsoft.Graph" -Force

Get-InstalledModule -Name  "Microsoft.Graph"
```

4. 使用全局管理员帐户并以 `Directory.AccessAsUser.All` 范围登录到您的 Entra ID 租户。

重要提示：

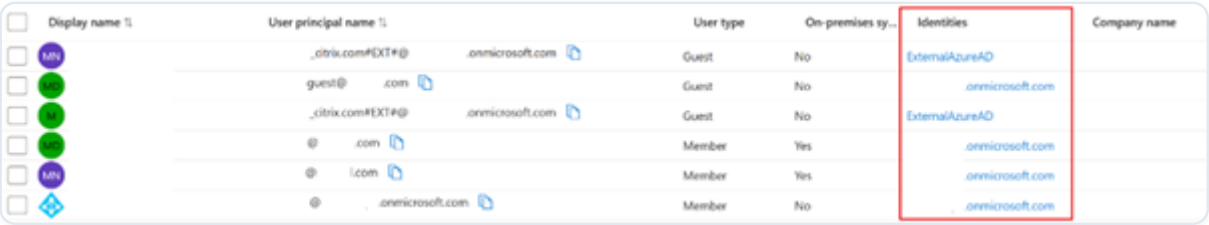
如果您使用权限较低的帐户或未指定 `Directory.AccessAsUser.All` 范围，则将无法完成步骤 4 并更新访客用户的 UPN。

```
Connect-MgGraph -Scopes Directory.AccessAsUser.All
```

5. 使用与为 AD 影子帐户配置的 UPN 匹配的 UPN 更新 Entra ID 用户。

```
$GuestUserId = (Get-MgUser -UserId
"contractoruser_hotmail.co.uk#EXT#@yourentraidtenant.onmicrosoft.com").
Id

Update-MgUser -UserId $GuestUserId -UserPrincipalName
"contractoruser@your.com"
```

6. 获取 Entra ID 租户中所有外部访客用户的列表（可选）。




```
Get-MgUser -filter "userType eq 'Guest'" | Select
Id,DisplayName,UserPrincipalName,Mail
```

7. 获取需要更新 UPN 的访客用户身份，然后更新其 UPN 后缀。

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

```
$GuestUserId = (Get-MgUser -UserId
"contractoruser_hotmail.co.uk#EXT#@yourEntra
IDtenant.onmicrosoft.com").Id



Update-MgUser -UserId $GuestUserId -UserPrincipalName
"contractoruser@yourforest.com"
```

8. 检查是否可以使用新更新的 UPN 找到访客用户身份。

```
Get-MgUser -UserId "contractoruser@yourforest.com"
```

测试 B2B SAML 解决方案

在 AD、Citrix Cloud 和 SAML 提供程序中完成所有记录的步骤后，您需要测试登录并验证 StoreFront 中是否为访客用户显示了正确的资源列表。

Citrix 建议使用 SAML-tracer 浏览器扩展进行所有 SAML 调试。此扩展适用于大多数常用 Web 浏览器。该扩展将 Base64 编码的请求和响应解码为 SAML XML，使其易于阅读。

SAML 跟踪器(/en-us/citrix-cloud/media/saml-tracer.png)

使用 SAML 跟踪器捕获的仅使用 cip_upn 进行身份验证的 B2B SAML 断言示例。

B2B SAML 示例(/en-us/citrix-cloud/media/example-simplified-saml.png)

测试前端(/en-us/citrix-cloud/media/testing-with-frontend-identities.png)

1. 将正确的 DaaS 资源映射到 AD 支持的用户和影子帐户用户或包含它们的组。
2. 启动 SAML 跟踪器浏览器扩展，并捕获整个登录和注销流程。
3. 使用表中为要测试的前端用户类型指定的属性登录到商店。

   来宾 Entra ID 用户登录： 您邀请到 Entra ID 租户作为来宾用户的承包商用户具有电子邮件地址 `contractoruser@hotmail.co.uk`。

   当 Entra ID 提示时，输入来宾用户的**电子邮件地址**。

   或

   AD 支持的 Entra ID 用户/本机 Entra ID 用户登录： 这些 Entra ID 用户的 UPN 格式为 `adbackeduser@yourforest.com` 或 `nativeuser@yourforest.com`。

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

当 Entra ID 提示时，输入用户的 **UPN**。

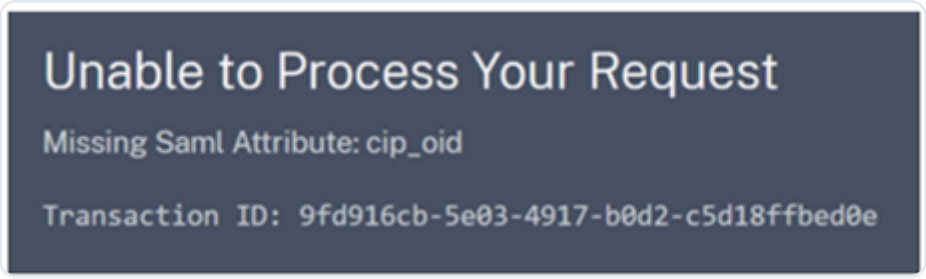
4. 检查断言是否仅包含用于身份验证的 **cip_upn** 属性，并且还包含商店 UI 所需的 **displayName** 属性。
5. 检查用户是否可以在 UI 中看到所需的 DaaS 资源。

B2B SAML 解决方案故障排除

SAML 断言中发送了错误的 UPN

原因：这仅适用于从 Entra ID 租户 1 导入到 Entra ID 租户 2 的 **B2B** 帐户。当使用从其他 Entra ID 租户导入的 **B2B** 用户时，SAML 断言中可能会发送错误的 UPN。如果使用 `user.userprincipalname` 并且最终用户使用从另一个 Entra ID 租户导入的 B2B 用户登录，则 SAML 断言中将发送错误的 **cip_upn** 值。SAML 断言中使用的 **cip_upn** 值将来自包含 B2B 用户作为**成员**的源 Entra ID 租户。使用 `user.localuserprincipalname` 可确保 **cip_upn** 值取自邀请 B2B 用户作为**访客**的 Entra ID 租户。

缺少 cip_* 属性错误



原因 1：SAML 断言中不存在 SAML 属性，但 Citrix Cloud 配置为期望接收它。您未能从 SAML 属性部分中 Citrix Cloud SAML 连接中删除不必要的 cip_* 属性。断开并重新连接 SAML 以删除对不必要的 cip_* 属性的引用。

原因 2：如果 Citrix Cloud 连接器在您的后端 AD 林中没有相应的 AD 影子帐户可供查找，也可能发生此错误。您可能已正确配置了前端身份，但具有匹配 UPN 的后端 AD 影子帐户身份不存在或无法找到。

登录成功，但用户登录到商店后未显示 DaaS 资源

原因：这很可能是由于前端到后端身份 UPN 映射不正确造成的。

确保前端和后端身份的两个 UPN 完全匹配，并代表登录到商店的同一最终用户。检查 DaaS 交付组是否包含到正确的 AD 影子帐户用户或包含它们的 AD 组的映射。

启动 DaaS 资源时，FAS SSON 到已加入 AD 域的 VDA 失败

尝试启动 DaaS 资源时，商店最终用户会在 GINA 中被提示输入其 Windows 凭据。此外，事件 ID 103 会出现在您的 FAS 服务器上的 Windows 事件日志中。

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

服务器 请求的 UPN `SID S-1-5-21-000000000-0000000000-0000000001-0001`，但查找返回 `SID S-1-5-21-000000000-0000000000-0000000001-0002`。

原因：您的 B2B SAML 部署存在“SID 不匹配问题”。您的前端身份包含来自与后端影子帐户 AD 林不同的 AD 林的 SID。

请勿在 SAML 断言中发送 **cip_sid**。

当多个连接的 AD 林中存在相同的 UPN 后缀时，AD 支持的用户登录失败

Citrix Cloud 具有多个资源位置和连接器，它们连接到不同的 AD 林。当从与影子帐户 AD 林不同的 AD 林导入到 Entra ID 的 AD 支持用户被使用时，登录失败。

AD 林 1 同步到 Entra ID 以创建具有 UPN（例如 `frontenduser@yourforest.com`）的前端用户。

AD 林 2 包含具有 UPN（例如 `frontenduser@yourforest.com`）的后端影子帐户。

原因：您的 B2B SAML 部署存在“UPN 歧义问题”。Citrix Cloud 无法确定使用哪个连接器来查找用户的后端身份。

请勿在 SAML 断言中发送 **cip_sid**。

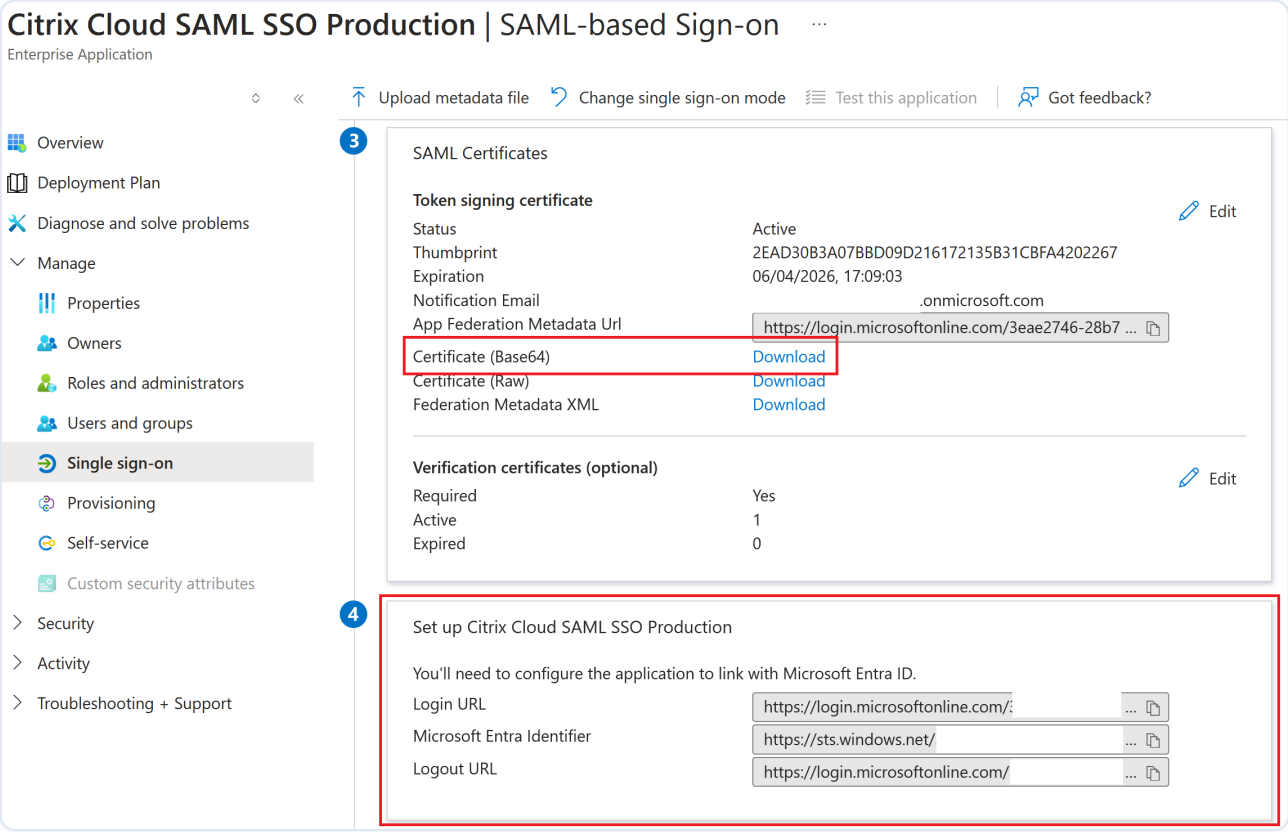
您的用户 UPN 存在于连接到 Citrix Cloud 的多个 AD 林中。

配置 Citrix Cloud SAML 连接

所有 Citrix 登录流程都需要使用商店 URL 或 Citrix Cloud GO URL 进行服务提供商启动。

从您的 Entra ID 门户获取 Entra ID SAML 应用程序 SAML 端点，并将其输入到 Citrix Cloud 中。

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



要在 Citrix Cloud SAML 连接中使用的 Entra ID SAML 端点示例

在 **身份和访问管理 > 身份验证 > 添加身份提供商 > SAML** 中，使用 SAML 连接的默认推荐值。

重要提示：

EntraID SSO 和注销 SAML 端点是相同的 URL。

在 CITRIX CLOUD 的此字段中	输入此值
实体 ID	`https://sts.windows.net/<yourEntraIDTenantID>`
签署身份验证请求	是
SSO 服务 URL	`https://login.microsoftonline.com/<yourEntraIDTenantID>/saml2`
SSO 绑定机制	HTTP 提交
SAML 响应	签署响应或断言
身份验证上下文	未指定，精确

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

在 CITRIX CLOUD 的此字段中	输入此值
注销 URL	`https://login.microsoftonline.com/<yourEntraIDTenantID>/saml2`
签署注销请求	是
SLO 绑定机制	HTTP 提交

将 Okta 配置为商店身份验证的 SAML 提供程序

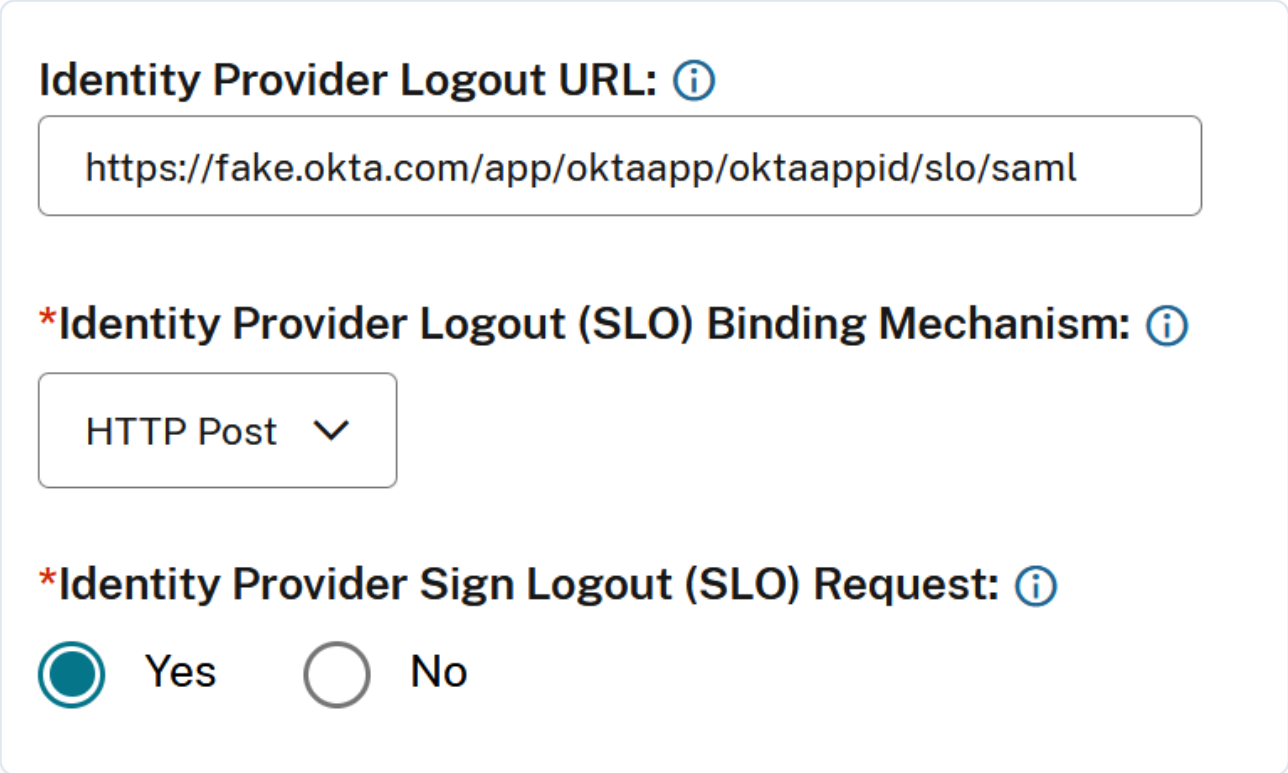
本文介绍了配置 Okta SAML 应用程序以及 Citrix Cloud™ 与您的 SAML 提供程序之间连接所需的步骤。其中一些步骤描述了您在 SAML 提供程序的管理控制台中执行的操作。

先决条件

在完成本文中的任务之前，请确保您已满足以下先决条件：

- Citrix 支持已在 Citrix Cloud 中启用 **SendNameIDPolicyInSAMLRequest** 功能。此功能按需启用。有关这些功能的更多信息，请参阅 使用 Okta 的 SAML 所需的云功能。
- 您有一个使用以下 Okta 域之一的 Okta 组织：
  - okta.com
  - 奥克塔-欧盟.com
  - oktapreview.com
- 您已将 Active Directory (AD) 与您的 Okta 组织同步。
- 您的 Okta 组织中已启用“**签署身份验证请求**”。
- Citrix Cloud 和 Okta SAML 应用程序中均配置了“**身份提供程序单点注销 (SLO)**”。配置 SLO 后，当最终用户从其商店注销时，他们也会从 Okta 以及所有共享 Okta SAML 应用程序的其他服务提供程序注销。
- Citrix Cloud 中已启用“**身份提供程序注销 (SLO) 请求**”。
- Citrix Cloud 中的“**身份提供程序注销绑定 (SLO)**”是 HTTPPost。

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



使用 Okta 的 SAML 所需的云功能

在完成本文中的任务之前，您必须联系 Citrix 支持部门以启用 **SendNameIDPolicyInSAMLRequest** 功能。此功能使 Citrix Cloud 能够在发送给 SAML 提供程序的 SAML 请求中将 **NameID** 策略指定为 **Unspecified**。此功能仅适用于 Okta。

您可以通过登录您的 Citrix 帐户并通过 Citrix 支持网站 提交支持请求来请求这些功能。

要求

本文包含一项任务，您将在其中 在 Okta 管理控制台中创建 SAML 应用程序。此应用程序需要适用于您的 Citrix Cloud 区域的 SAML 签名证书。

您可以使用提取工具（例如位于 https://www.rcfed.com/SAMLWSFed/MetadataCertificateExtract 的工具）从您的区域的 Citrix Cloud SAML 元数据中提取此证书。Citrix 建议您提前获取 Citrix Cloud SAML 证书，以便在需要时提供。

本节中的步骤介绍了如何使用位于 https://www.rcfed.com/SAMLWSFed/MetadataCertificateExtract 的提取工具获取签名证书。

要获取您的区域的 Citrix Cloud 元数据，请执行以下操作：

1. 在您选择的提取工具中，输入您的 Citrix Cloud 区域的元数据 URL：
   - 对于欧盟、美国和亚太南部区域，请输入 `https://saml.cloud.com/saml/metadata`。
   - 对于日本区域，请输入 `https://saml.citrixcloud.jp/saml/metadata`。

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

- 对于 Citrix Cloud Government 区域，请输入 `https://saml.cloud.us/saml/metadata`。

2. 单击 **Load**。提取的证书将显示在您输入的 URL 下方。
3. 单击 **Download** 以下载 PEM 格式的证书。

使用 Okta AD 代理同步帐户

要将 Okta 用作 SAML 提供程序，您必须首先将本地 AD 与 Okta 集成。为此，您需要在域中安装 Okta AD 代理，并将您的 AD 添加到 Okta 组织。有关部署 Okta AD 代理的指导，请参阅 Okta 网站上的开始使用 Active Directory 集成。

之后，将您的 AD 用户和组导入 Okta。导入时，请包含与您的 AD 帐户关联的以下值：

- 电子邮件
- SID
- UPN
- OID

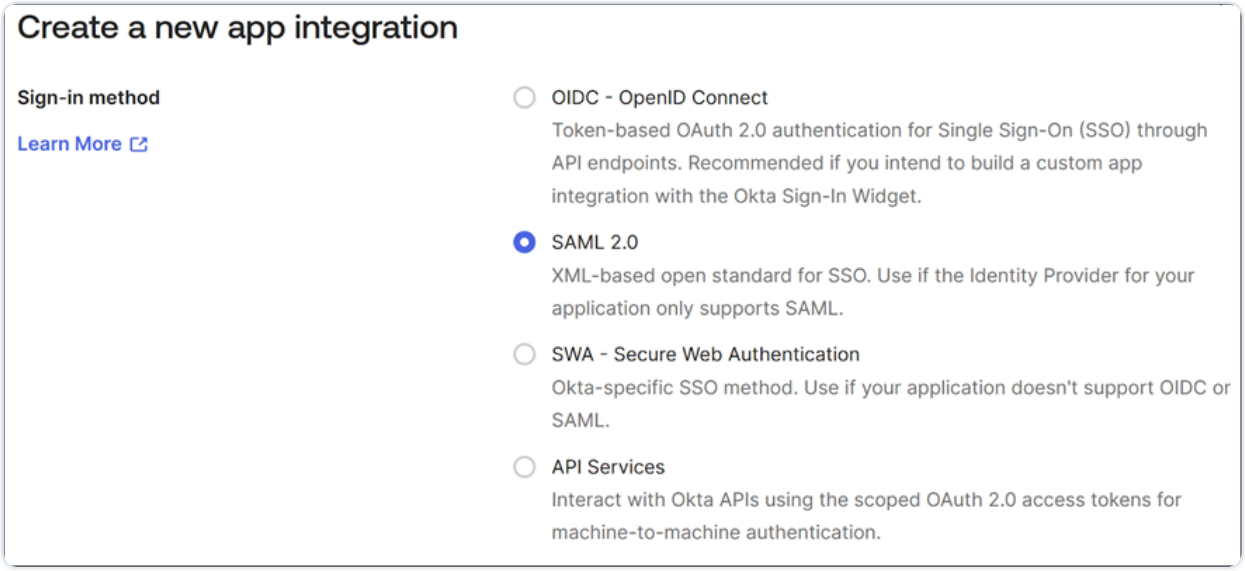
要将您的 AD 用户和组与 Okta 组织同步，请执行以下操作：

1. 安装并配置 Okta AD 代理。有关完整说明，请参阅 Okta 网站上的以下文章：
   - 安装 Okta Active Directory 代理
   - 配置 Active Directory 导入和帐户设置
   - 配置 Active Directory 预配设置
2. 通过手动导入或自动导入将您的 AD 用户和组添加到 Okta。有关 Okta 导入方法和说明的更多信息，请参阅 Okta 网站上的管理 Active Directory 用户和组。

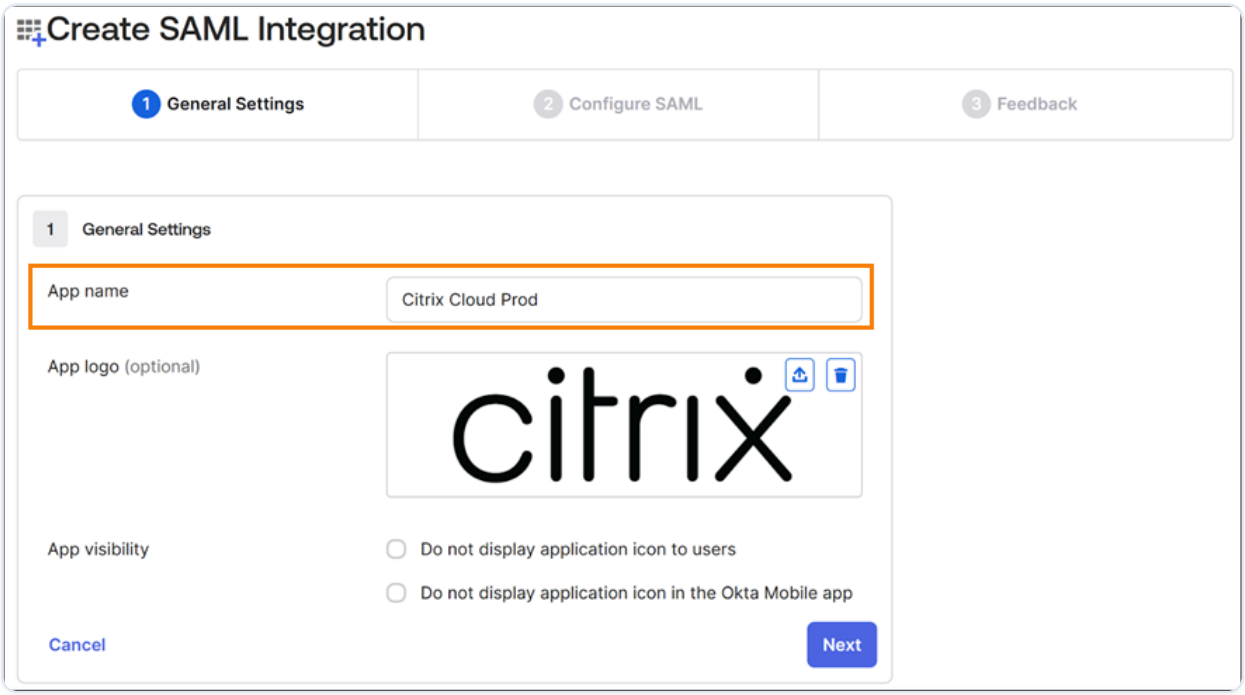
为商店身份验证配置 Okta SAML 应用程序

1. 使用具有添加和配置 SAML 应用程序权限的管理员帐户登录您的 Okta 组织。
2. 在管理控制台中，选择 **Applications（应用程序）> Applications（应用程序）> Create App Integration（创建应用程序集成）**，然后选择 **SAML 2.0**。选择**Next（下一步）**。

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



3. 在 **App Name** 中，输入应用程序的友好名称。选择 **Next**。



4. 在 **SAML Settings** 部分中，配置 Citrix Cloud 服务提供商 (SP) 连接：

   a. 在 **Single sign-on URL** 中，输入与您的 Citrix Cloud 客户的 Citrix Cloud 区域对应的 URL：

      - 如果您的客户 ID 位于欧盟、美国或亚太南部地区，请输入 `https://saml.cloud.com/saml/acs`。
      - 如果您的客户 ID 位于日本地区，请输入 `https://saml.citrixcloud.jp/saml/acs`。
      - 如果您的客户 ID 位于 Citrix Cloud Government 区域，请输入 `https://saml.cloud.us/saml/acs`。

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

b. 选择 **将此用于接收方和目标 URL**。

c. 在 **Audience URI (SP Entity ID)** 中，输入与您的 Citrix Cloud 客户的 Citrix Cloud 区域对应的 URL：

- 如果您的客户 ID 位于欧盟、美国或亚太南部地区，请输入 `https://saml.cloud.com`。
- 如果您的客户 ID 位于日本地区，请输入 `https://saml.citrixcloud.jp`。
- 如果您的客户 ID 位于 Citrix Cloud Government 区域，请输入 `https://saml.cloud.us`。

d. 在 **Name ID Format** 中，选择 **Unspecified**。Citrix Cloud 在 SAML 请求中发送的 NameID 策略必须与 Okta SAML 应用程序中指定的 NameID 格式匹配。如果这些项目不匹配，启用 **Sign Authentication Request** 将导致 Okta 报错。

e. 在 **应用程序用户名** 中，选择 **Okta 用户名**。

作为此配置的一个示例，下图说明了美国、欧盟和亚太南部地区的正确配置：

Okta 控制台中配置了设置的 SAML 设置(/en-us/citrix-cloud/media/saml-okta-console-app-configuration-complete.png)

> **重要提示：**
>
> **名称 ID** 设置必须配置为**未指定**。为此设置使用不同的值会导致 SAML 登录失败。

f. 单击**显示高级设置**并配置以下设置：

- 在**响应**中，选择**已签名**。
- 在**断言签名**中，选择**已签名**。
- 在**签名算法**中，选择 **RSA-SHA256**。
- 在**断言加密**中，选择**未加密**。

g. 在**签名证书**中，以上传 PEM 格式的 Citrix Cloud 区域的 SAML 签名证书。有关获取 SAML 签名证书的说明，请参阅本文中的要求。

h. 在**启用单点注销**中，选择**允许应用程序启动单点注销**。

i. 在**单点注销 URL** 中，输入与您的 Citrix Cloud 区域对应的 URL：

- 对于欧盟、美国和亚太南部地区，请输入 `https://saml.cloud.com/saml/logout/callback`。

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

- 对于日本地区，请输入 `https://saml.citrixcloud.jp/saml/saml/logout/callback`。
- 对于 Citrix Cloud Government，请输入 `https://saml.cloud.us/saml/logout/callback`。

j. 在 **SP Issuer** 中，输入您之前在 **Audience URI (SP Entity ID)** 中输入的值（此任务的第 4c 步）。

k. 在 **Signed Requests** 中，选择 **使用签名证书验证 SAML 请求**。

下图显示了美国、欧盟和亚太南部区域的正确配置：

Okta 控制台中已配置设置的高级 SAML 设置(/en-us/citrix-cloud/media/saml-okta-show-advanced-settings-console.png)

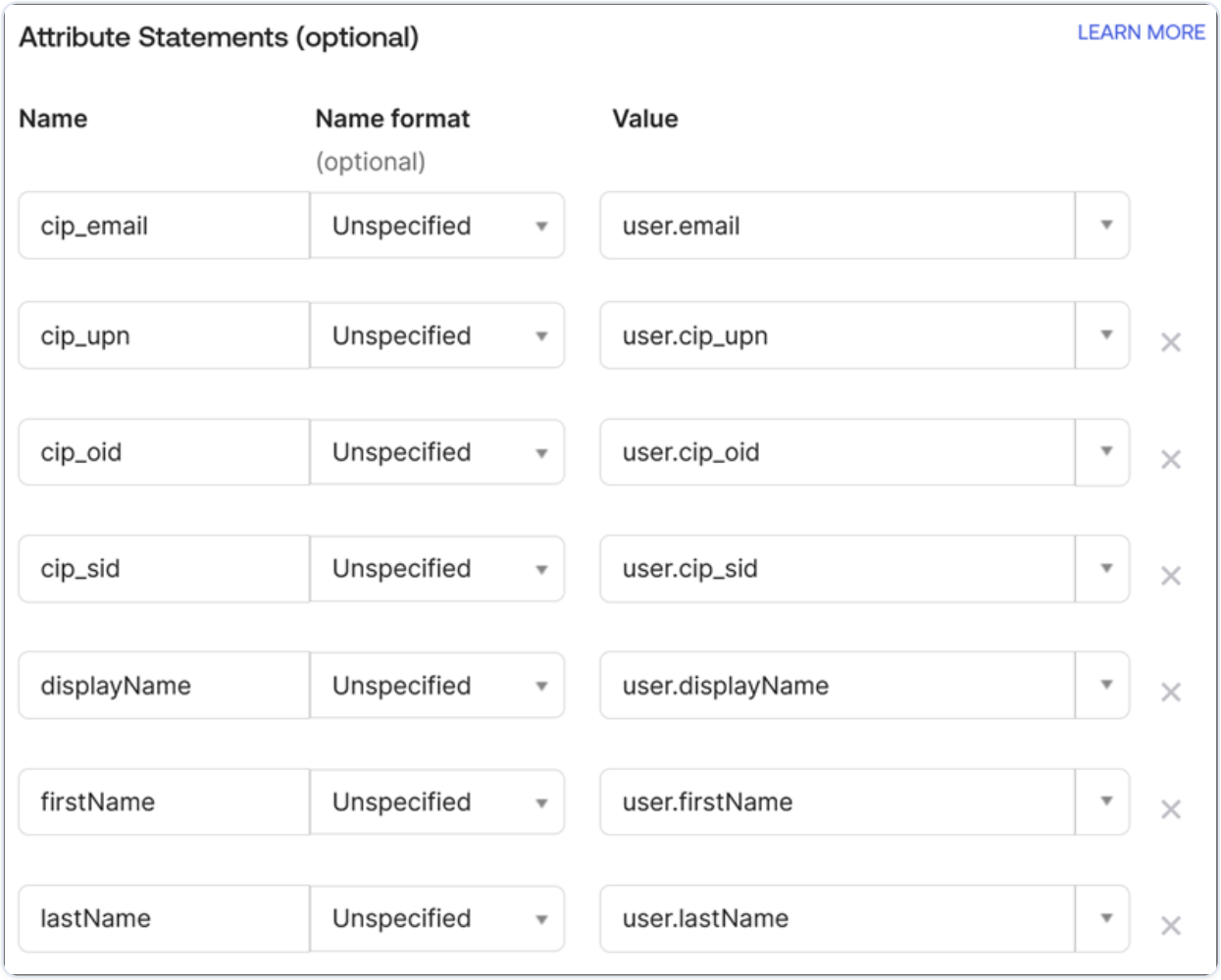
l. 对于所有剩余的高级设置，接受默认值。

Okta 控制台中具有默认值的高级设置(/en-us/citrix-cloud/media/saml-okta-default-advanced-settings.png)

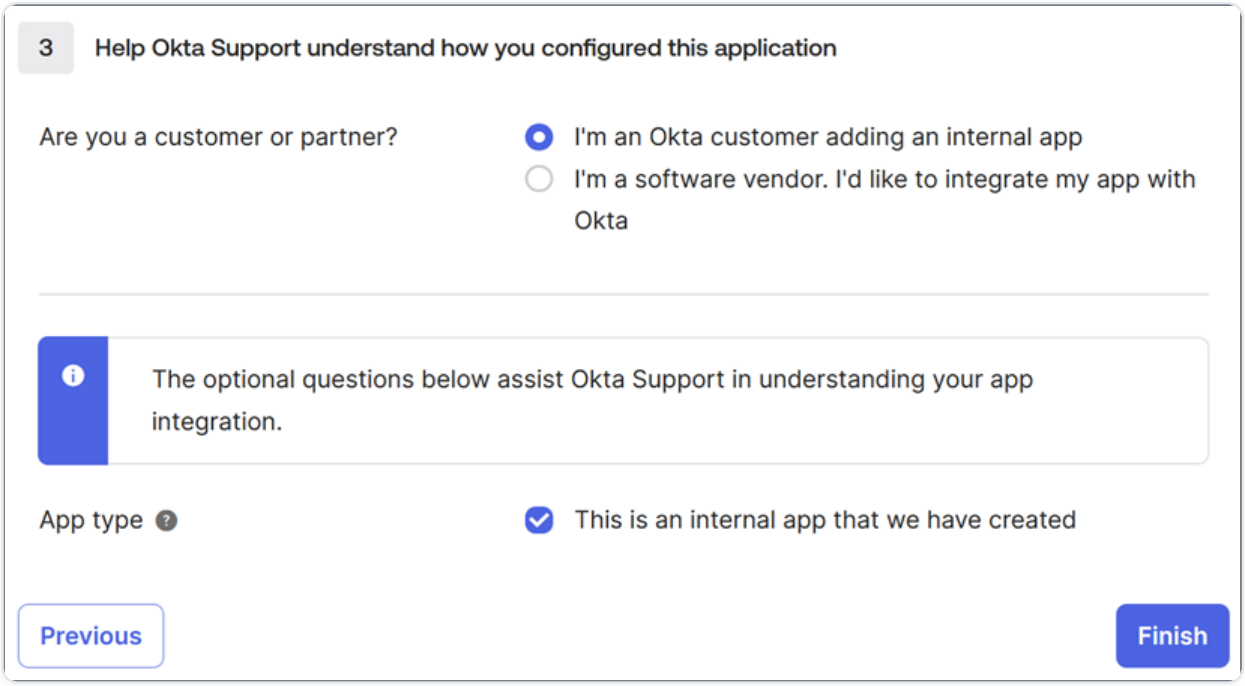
5. 在 **属性语句（可选）** 下，输入 **名称**、**名称格式** 和 **值** 的值，如下表所示：

名称	名称格式	值
cip_upn	未指定	user.cip_upn
displayName	未指定	user.displayName
firstName	未指定	user.givenName
lastName	未指定	user.familyName

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



6. 选择“**下一步**”。此时将显示 Okta 配置声明。



7. 在“**您是客户还是合作伙伴？**”中，选择“**我是 Okta 客户，正在添加内部应用程序**”。
8. 在“**应用程序类型**”中，选择“**这是我们创建的内部应用程序**”。

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

9. 选择“**完成**”以保存您的配置。此时将显示 SAML 应用程序的配置文件页面，并显示“**登录**”选项卡的内容。

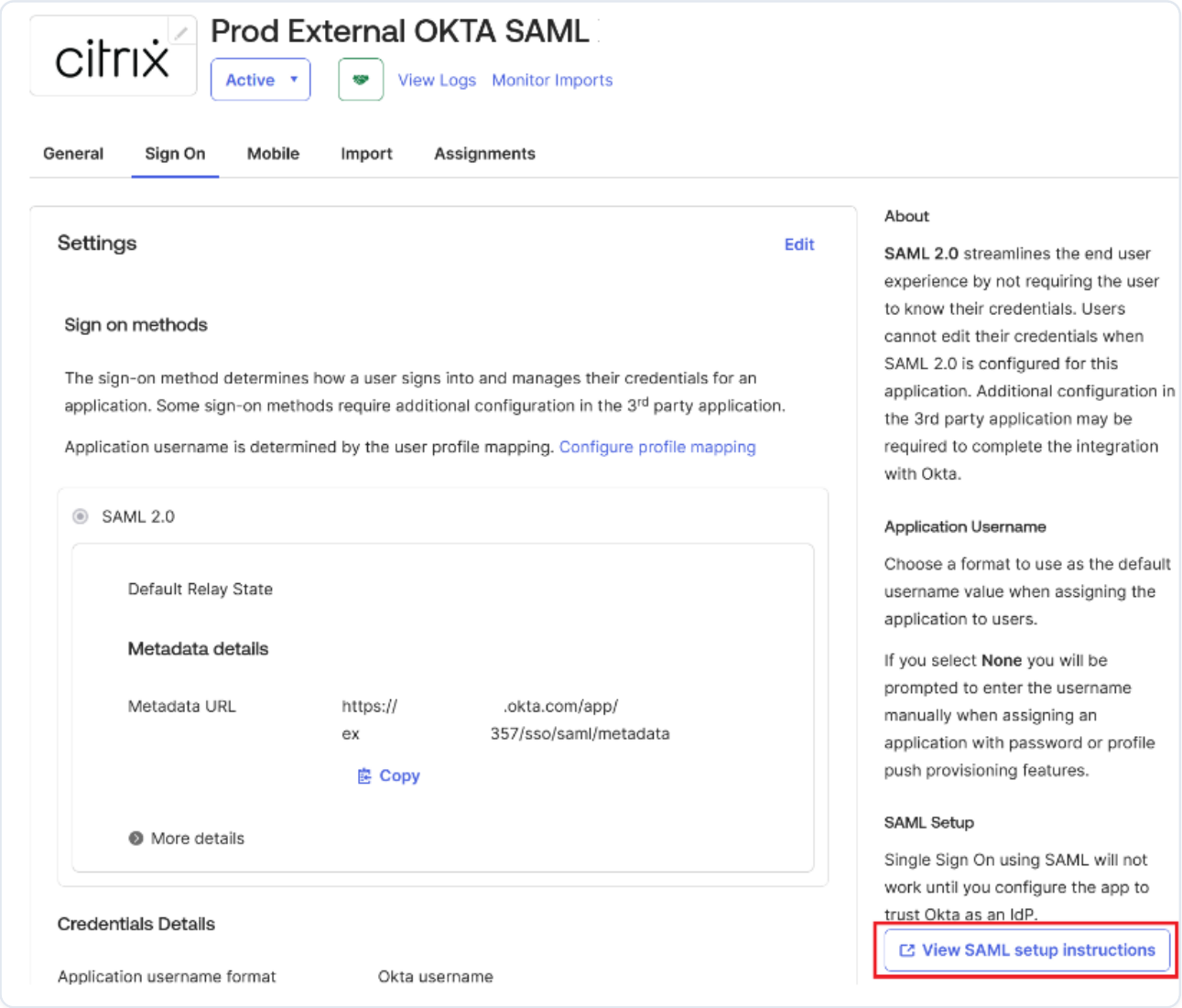
配置完成后，选择“**分配**”选项卡并将用户和组分配给 SAML 应用程序。

配置 Citrix Cloud SAML 连接

所有 Citrix 登录流程都需要使用商店 URL 或 Citrix Cloud GO URL 由服务提供商发起。

在 **身份和访问管理** → **身份验证** → **添加身份提供商** → **SAML** 中使用 SAML 连接的默认推荐值。

从您的 Okta 门户获取 Okta SAML 应用程序的 SAML 端点，以输入到 Citrix Cloud 中。



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

How to Configure SAML 2.0 for Prod External OKTA SAML Application

Note: These setup instructions include certificate information for this app's **most recently created** SAML signing certificate. For users to get access to the app using these instructions, that certificate must be active.

The following is needed to configure Prod External OKTA SAML

1. Identity Provider Single Sign-On URL:

```
https://[redacted].okta.com/app/citrix-[redacted]_1/exkp[redacted]HA357/sso/saml
```

2. Identity Provider Single Logout URL:

```
https://[redacted].okta.com/app/citrix-[redacted]_1/exkp[redacted]HA357/slo/saml
```

3. Identity Provider Issuer:

```
http://www.okta.com/ex[redacted]HA357
```

4. X.509 Certificate:


```
-----BEGIN CERTIFICATE-----
MIIDrDCCApSgAwIBAgIGAYXogrzaMA0GCSqGSIb3DQEBCwUAMIGWMQswCQYDVQQGEwJVUzETMBEG
A1UECAwKQ2FsaWZvcm5pYTEWMBQGA1UEBwwNU2FuIEZyYW5jaXNjbzENMAsGA1UECgwET2t0YTEU
[redacted]
aQRZmmwyqNuSGN2CHlKVSkYZvSxxgn9LFA7Y/EER9lp08/qXGE3BgFm93m0fS2zB9HYDWA0L5+3h
bN9bf95Eozn6kii4JO7LP4pJRCTpLu7zgGcSeNneu+A=
-----END CERTIFICATE-----
```


Download certificate

重要提示：

Okta 不需要范围实体 ID。本文档假定范围实体 ID 已禁用。有关范围实体 ID 的定义以及何时需要它，请参阅 Citrix 范围实体 ID 文档。使用默认的 Citrix Cloud SAML 连接设置，并保持 **范围实体 ID** 禁用。

SAML Identity Provider Configuration

SAML Application Scoped Entity ID

Disabled

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

CITRIX CLOUD 中的此字段	输入此值
实体 ID	`http://www.okta.com/<oktaSAMLappID>`
签署身份验证请求	是
SSO 服务 URL	`https://<youroktatenant>.okta.com/app/<oktatenantname>_<samlappname>/<samlappID>/sso/saml`
SSO 绑定机制	HTTP POST 方法
SAML 响应	签署响应或断言
身份验证上下文	未指定，精确
注销 URL	`https://<youroktatenant>.okta.com/app/<oktatenantname>_<samlappname>/<samlappID>/slo/saml`
签署注销请求	是
SLO 绑定机制	HTTP POST 方法

将本地 PingFederate 服务器配置为商店和 Citrix Cloud™ 的 SAML 提供程序

本文由 Citrix® 和 Ping 工程师合作撰写，并经双方审阅，以确保撰写时的技术准确性。有关如何预置、配置和许可本地 PingFederate 服务器以用作 SAML 提供程序的说明，请参阅 Ping 文档，因为这超出了本文的范围。

本文档使用 PingFederate 11.3 和 12 版本编写。

先决条件

本文专门讨论 SAML 配置，并确保满足以下条件。

- 您已在组织内预置了本地 PingFederate 服务器并获得了必要的许可证。有关详细信息，请参阅 PingFederate 安装。
- 您需要在 PingFederate 服务器上安装受支持的 Java 版本。有关受支持的 Java 版本，请参阅 Ping Identity 文档。有关详细信息，请参阅 Java PingFederate 要求。

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

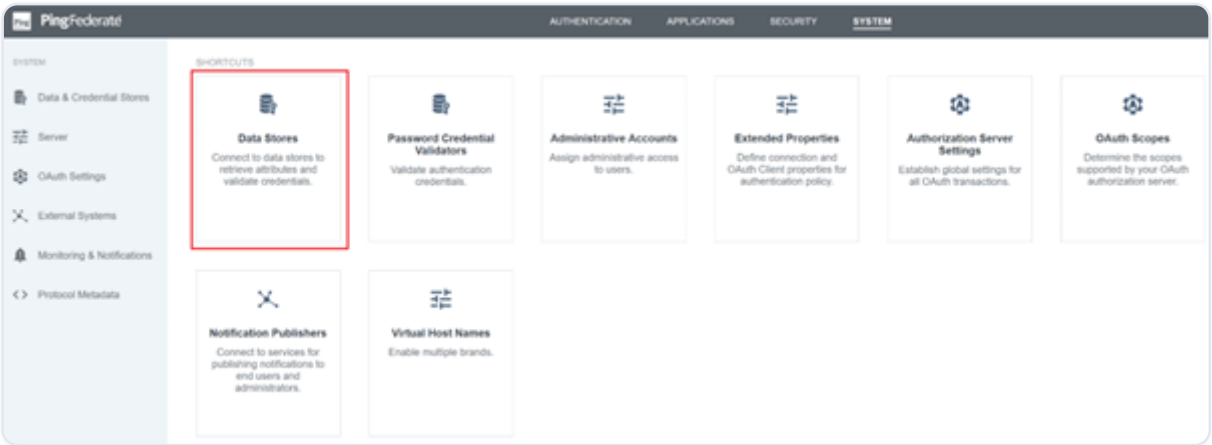
- 您已配置所需的网络和防火墙规则，以允许 Citrix Cloud 在商店/Citrix Cloud 管理控制台 SAML 登录过程中重定向到本地 PingFederate 服务器。有关详细信息，请参阅 PingFederate 网络要求。
- 您已将公共签名的 x509 证书导入到 PingFederate 服务器，该证书可用作 PingFederate 服务器的服务器证书。
- 您已将公共签名的 x509 证书导入到 PingFederate 服务器，该证书可用作 IdP 的 SAML 签名证书。此证书必须在 SAML 连接过程中上传到 Citrix Cloud。
- 您已将本地 Active Directory 连接到 PingFederate。有关详细信息，请参阅 PingFederate LDAP 数据存储

注意：

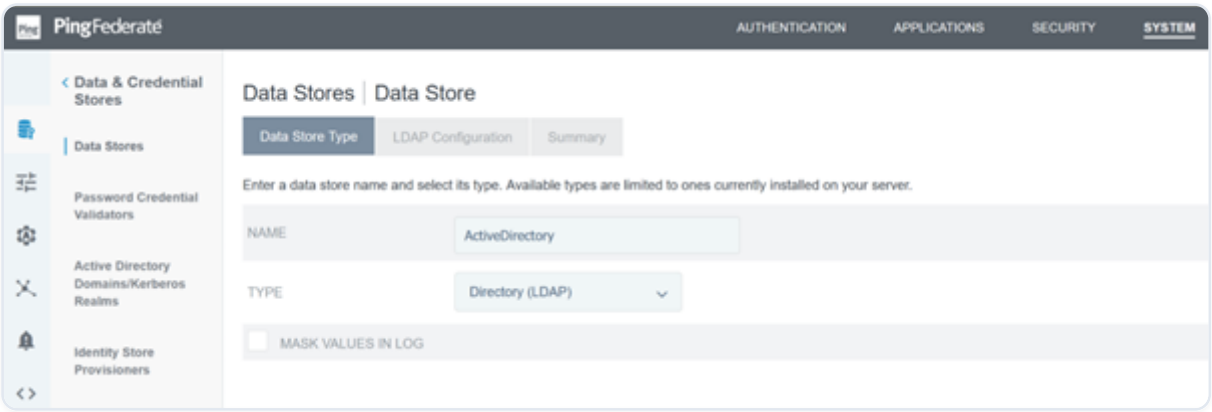
在配置 PingFederate 以与 Citrix Cloud 和商店配合使用时，请参阅 PingFederate 文档以了解各个 SAML 设置的作用，并帮助补充此处提供的说明。

使用 PingFederate 中的数据存储配置到 AD 域的 Active Directory 连接

1. 在数据存储中配置 Active Directory 连接。

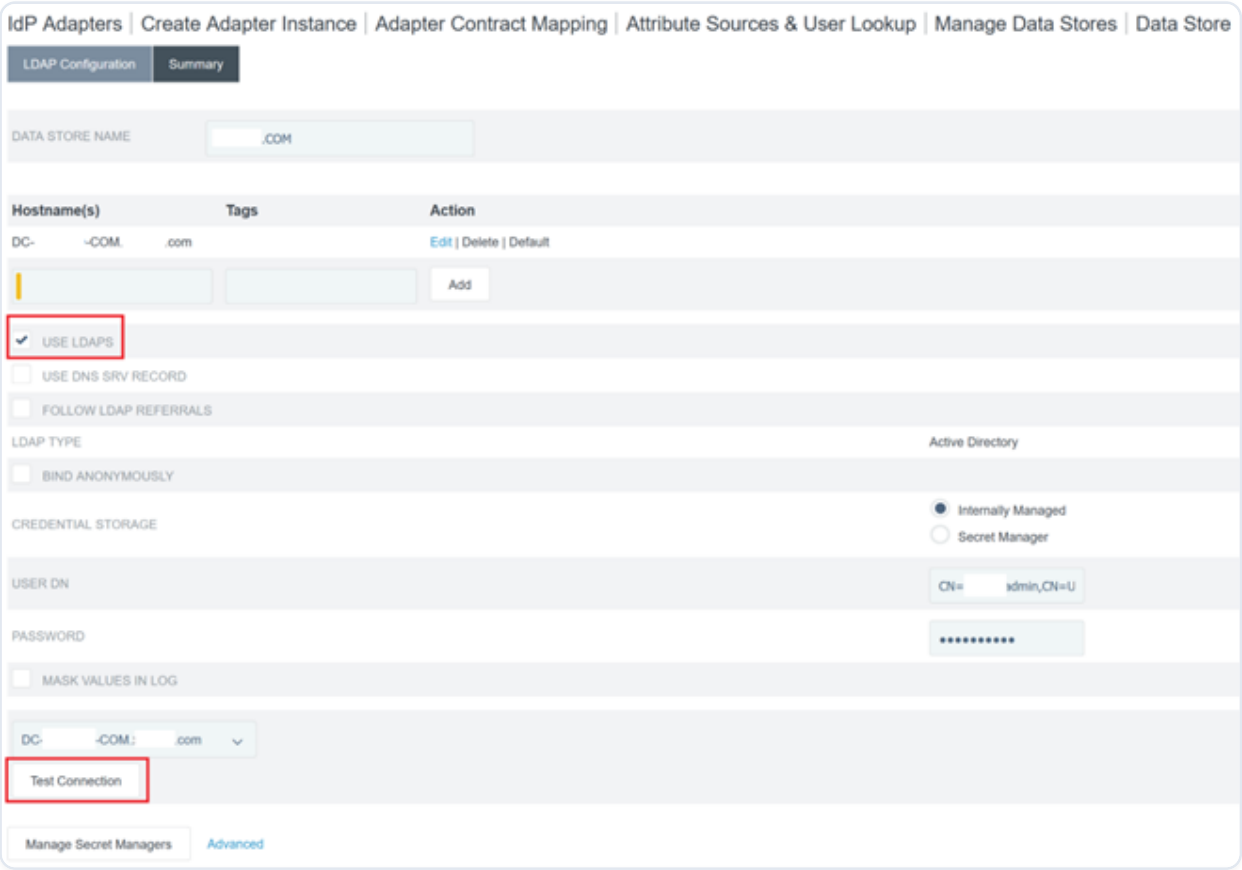


2. 将类型选择为 **目录 (LDAP)**。

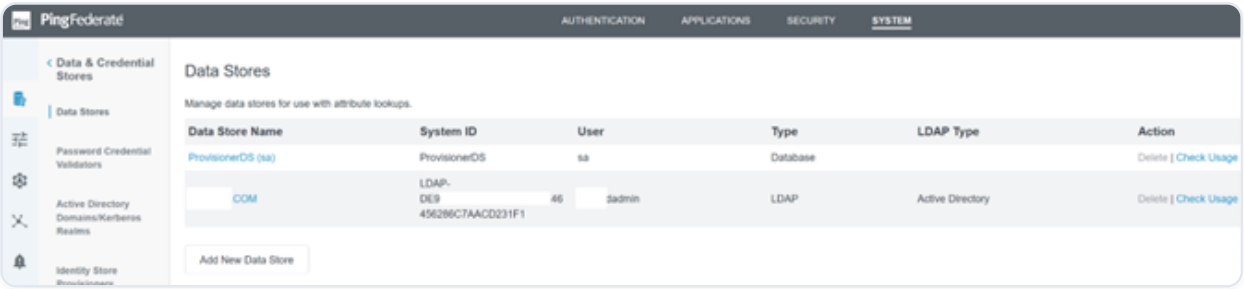


© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. 为 LDAPS 连接配置域控制器，并在主机名字段中添加域控制器 FQDN 列表。然后单击**测试连接**。

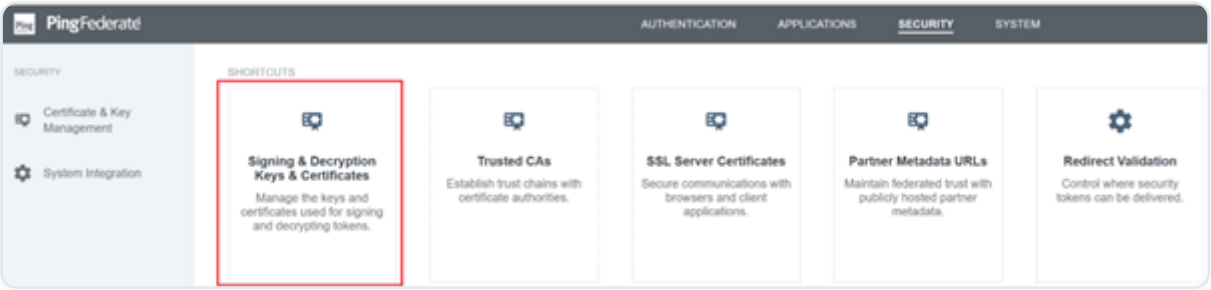


4. 配置完成后，Active Directory 连接应类似于以下示例：



上传 Citrix Cloud SAML 签名证书

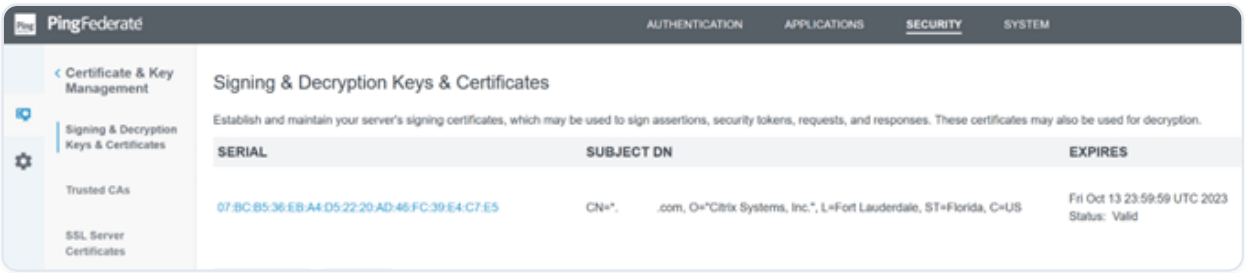
1. 单击**安全**选项卡
2. 在**签名和解密密钥与证书**中上传您希望 PingFederate 使用的 SAML 签名证书。



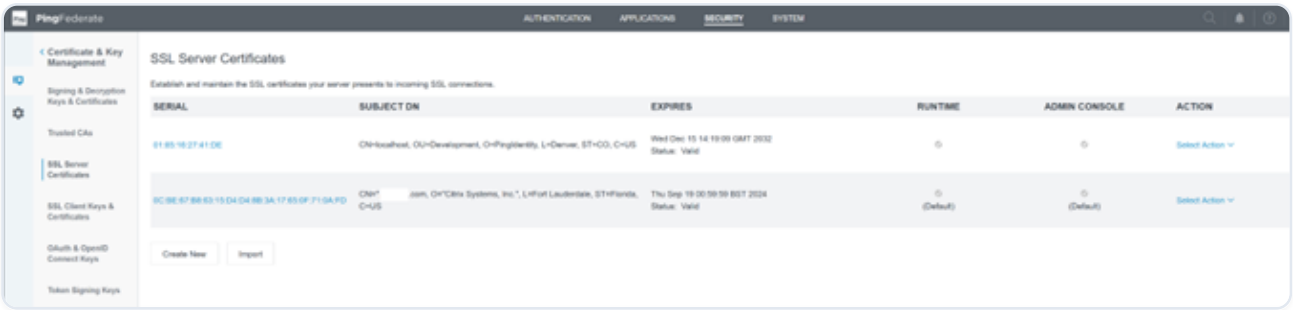
© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **注意：**
>
> 在此示例中，使用的证书是公开签名的 Digicert `pingfederateserver.domain.com` 证书。

3. 上传用于签署 PingFederate 服务器 SAML 签名证书的任何 CA 证书。



> **注意：**
>
> PingFederate 服务器证书和 SAML 签名证书可以是相同的 SSL 证书，也可以使用不同的 SSL 证书。配置 SAML 连接时，您需要向 Citrix Cloud 提供 SAML 签名证书的副本。

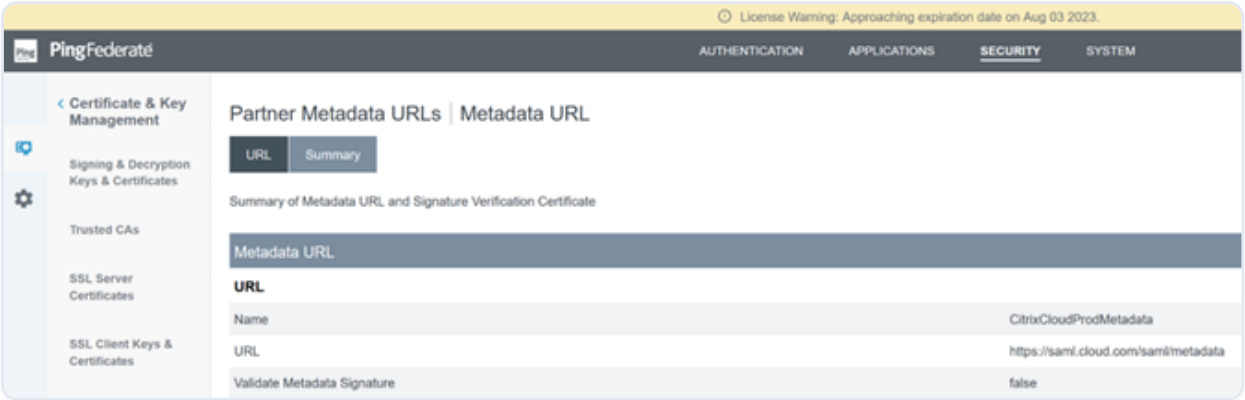


上传 Citrix Cloud 元数据

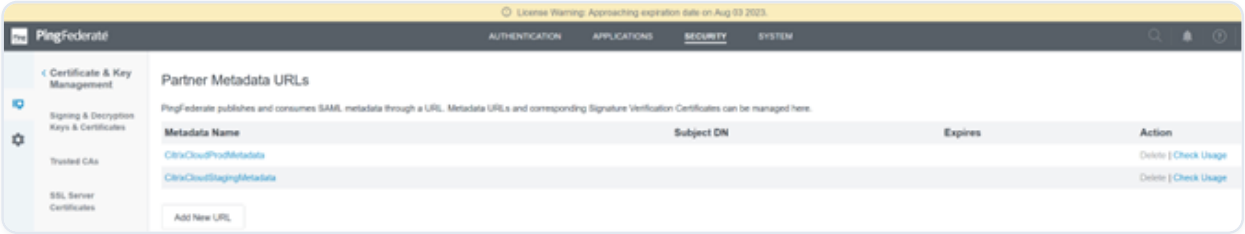
1. 为 Citrix Cloud 元数据提供一个名称，并输入与您的 Citrix Cloud 租户所在的 Citrix Cloud 区域对应的元数据 URL。

   - `<https://saml.cloud.com/saml/metadata>` - 商业版（欧盟、美国和亚太南部）
   - `<https://saml.citrixcloud.jp/saml/metadata>` - 日本
   - `<https://saml.cloud.us/saml/metadata>` - 政府版

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



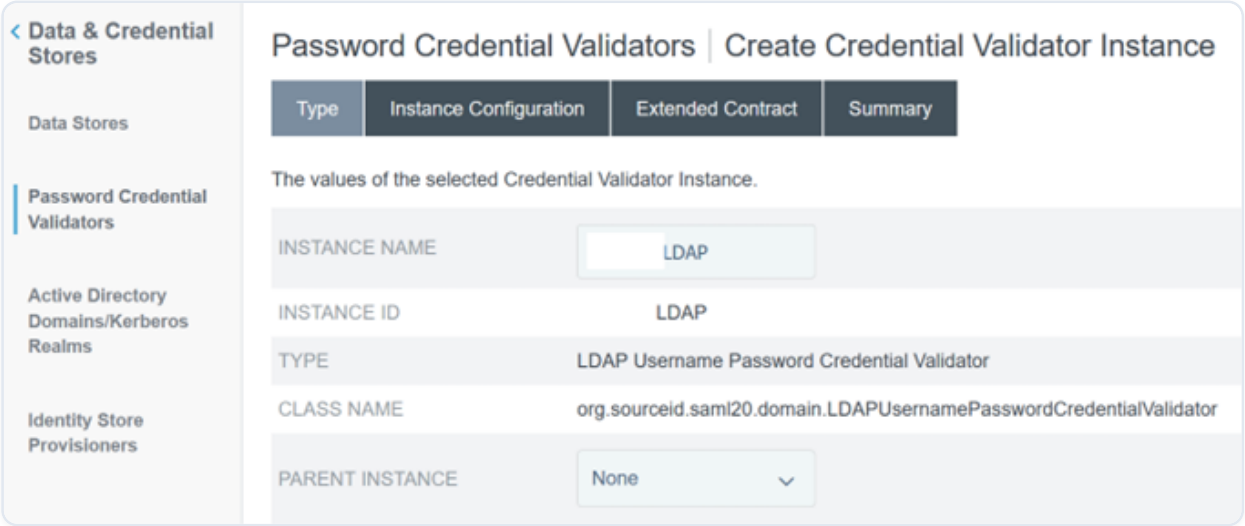
2. 配置完成后，Citrix Cloud 元数据配置应类似于以下示例。



在 PingFederate 中配置密码凭据验证器

有关详细信息，请参阅 PingFederate 密码凭据验证器

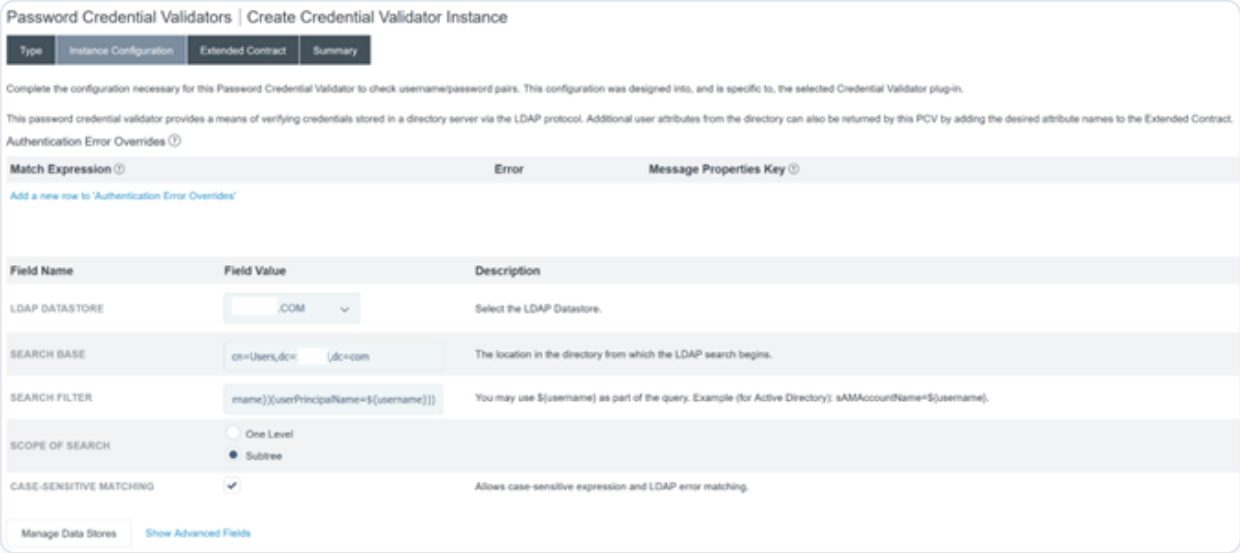
1. 将密码凭据验证器类型配置为 LDAP 用户名和密码。



2. 配置**实例配置**。选择您之前配置的 AD 域连接和数据存储 使用 PingFederate 中的 DataStore 配置到 AD 域的 Active Directory 连接。输入示例中所示的合适 LDAP 过滤器。

   `(((sAMAccountName=${username})(userPrincipalName=${username}))`

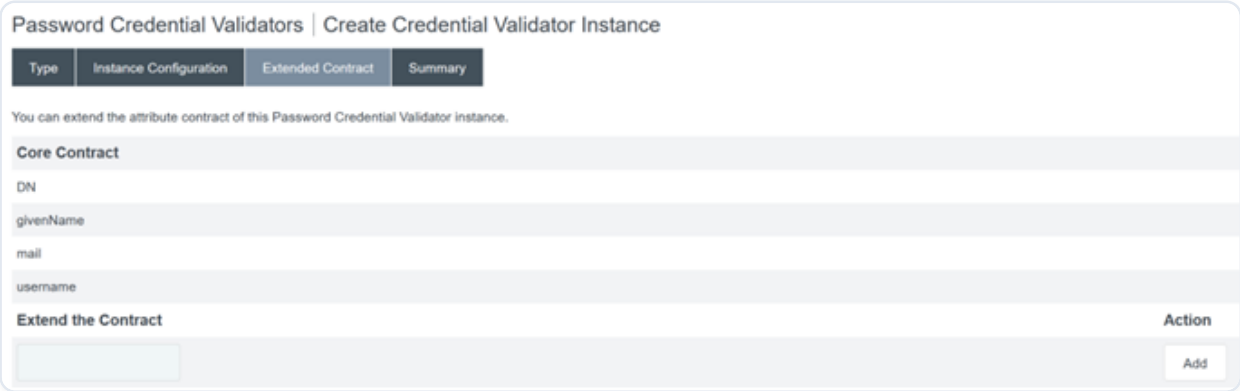
© 1997–2026 Citrix Systems, Inc. All rights reserved.



注意：

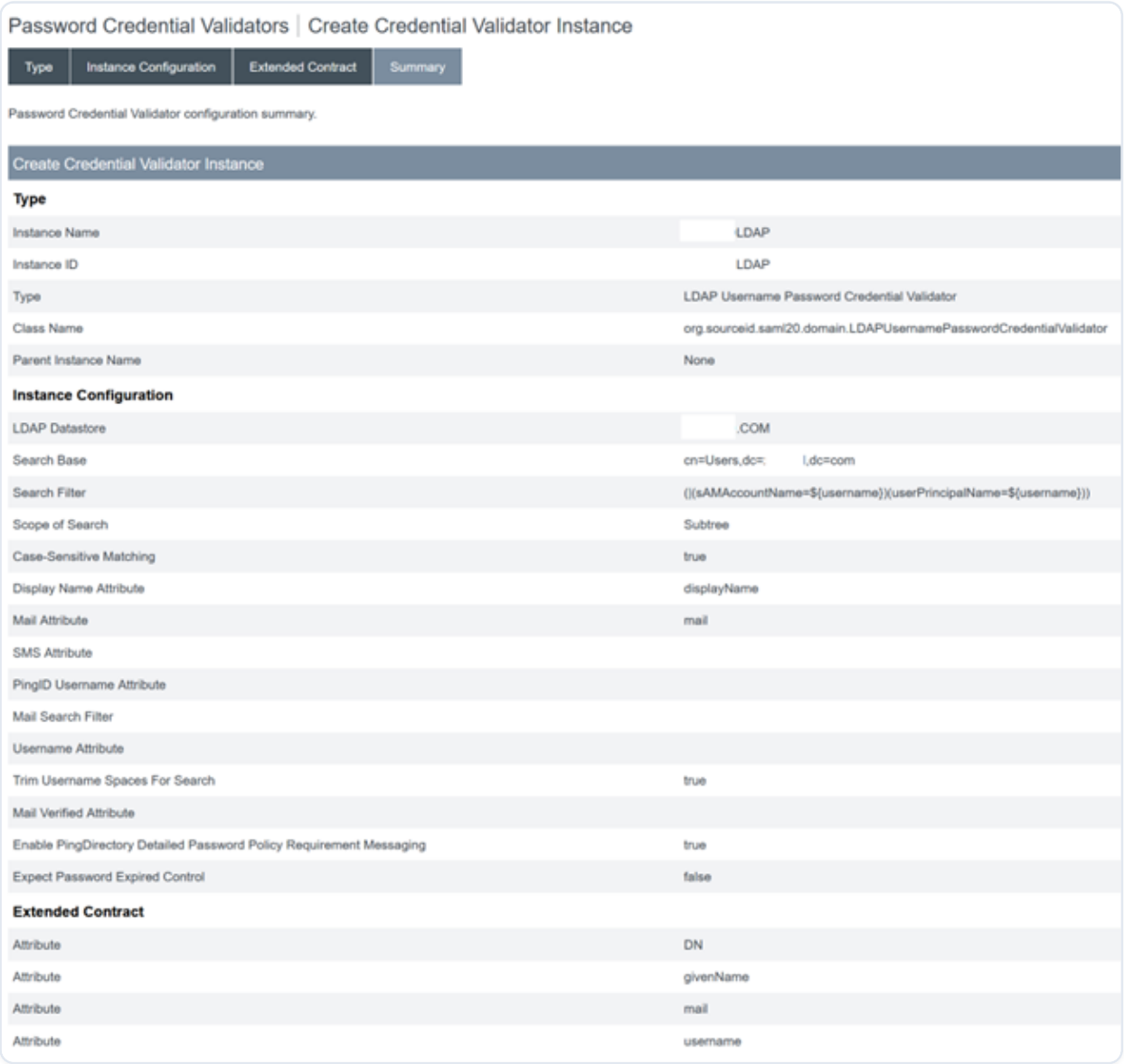
示例过滤器同时支持 sAMAccountName 和 userPrincipalName AD 用户名格式，允许最终用户使用其中任一格式登录到商店或 Citrix Cloud。

3. 配置**扩展协定**。



4. **密码凭据验证器**摘要应类似于此示例。

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



Password Credential Validators | Create Credential Validator Instance

Type | Instance Configuration | Extended Contract | Summary

Password Credential Validator configuration summary.

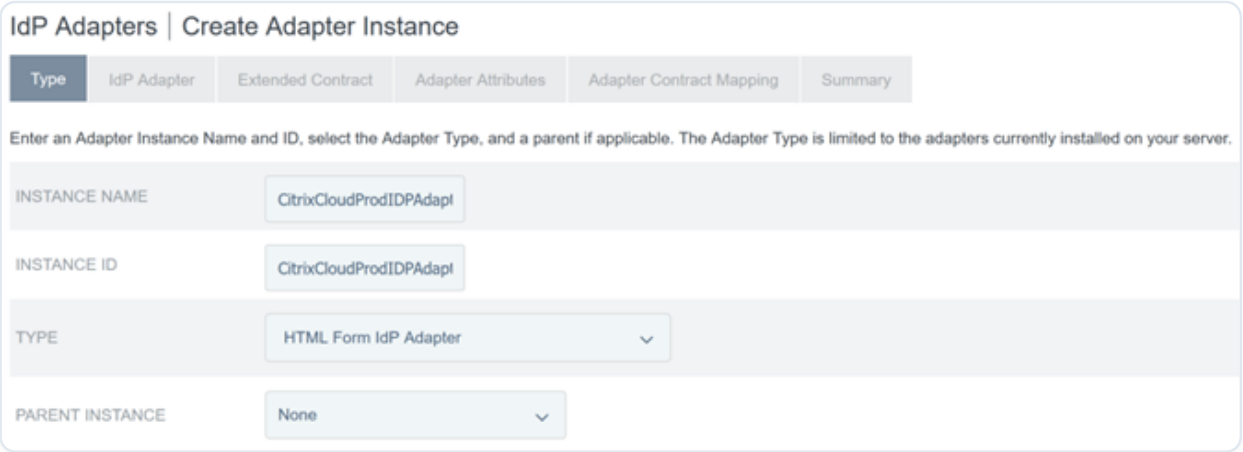
Create Credential Validator Instance

Type	
Instance Name	LDAP
Instance ID	LDAP
Type	LDAP Username Password Credential Validator
Class Name	org.sourceid.saml20.domain.LDAPUsernamePasswordCredentialValidator
Parent Instance Name	None
Instance Configuration	
LDAP Datastore	.COM
Search Base	cn=Users,dc= l,dc=com
Search Filter	(|(sAMAccountName=${username})(userPrincipalName=${username}))
Scope of Search	Subtree
Case-Sensitive Matching	true
Display Name Attribute	displayName
Mail Attribute	mail
SMS Attribute	
PingID Username Attribute	
Mail Search Filter	
Username Attribute	
Trim Username Spaces For Search	true
Mail Verified Attribute	
Enable PingDirectory Detailed Password Policy Requirement Messaging	true
Expect Password Expired Control	false
Extended Contract	
Attribute	DN
Attribute	givenName
Attribute	mail
Attribute	username

在 PingFederate 中配置 IDP 适配器

有关详细信息，请参阅 PingFederate HTML 表单适配器

1. 创建类型为 HTML 表单 IdP 适配器的新 IDP 适配器。



IdP Adapters | Create Adapter Instance

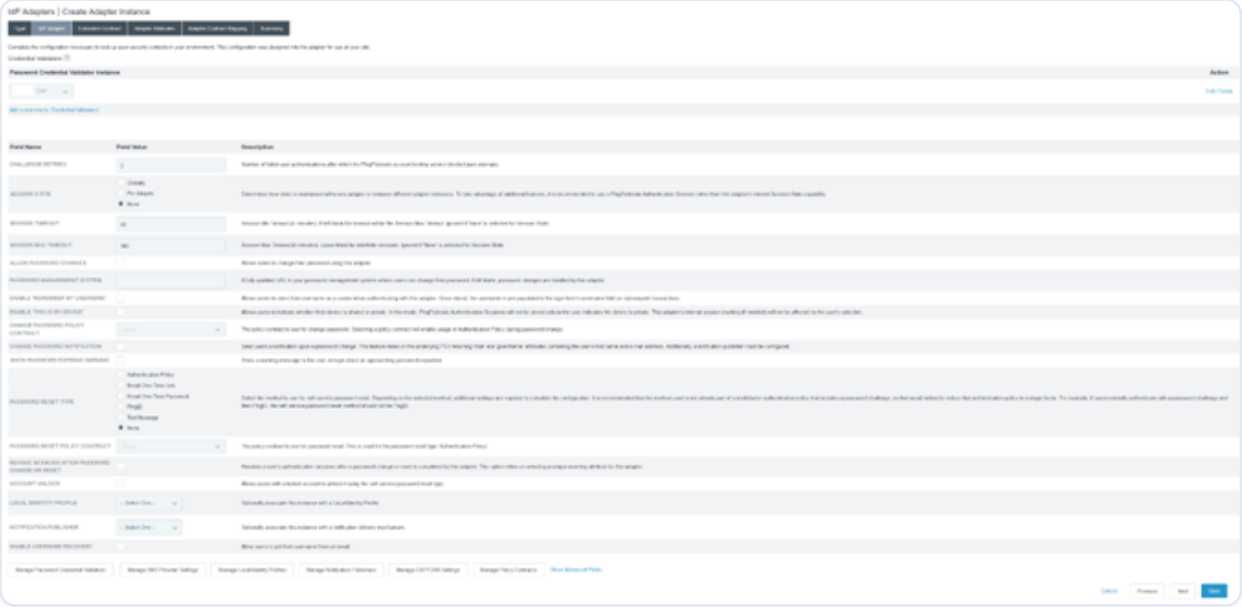
Type | IdP Adapter | Extended Contract | Adapter Attributes | Adapter Contract Mapping | Summary

Enter an Adapter Instance Name and ID, select the Adapter Type, and a parent if applicable. The Adapter Type is limited to the adapters currently installed on your server.

INSTANCE NAME	CitrixCloudProdIDPAdapt
INSTANCE ID	CitrixCloudProdIDPAdapt
TYPE	HTML Form IdP Adapter
PARENT INSTANCE	None

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

2. 选择您之前配置的现有**密码凭据验证器**并配置 IDP 适配器。有关详细信息，请参阅 在 PingFederate 中配置密码凭据验证器。



3. 配置**扩展协定**，其中包含在 SAML 登录期间传递给 Citrix Cloud 或商店的 SAML 属性。

   配置扩展合同 (/en-us/citrix-cloud/media/authentication-extended-contract.png)

4. 配置**适配器属性**。

   配置适配器属性 (/en-us/citrix-cloud/media/authentication-configure-adapter-attributes.png)

5. 配置**适配器合同映射**，其中 SAML 属性映射到 AD 身份的 LDAP 用户属性。单击**配置适配器合同**。

   设置 2 个二进制属性的编码。

   - objectGUID = base64 (已编码)
   - objectSid = SID (未编码)

   配置适配器属性编码 (/en-us/citrix-cloud/media/authentication-configure-adapter-attributes-encoding.png)

6. 配置**属性源和用户查找**。

   属性源和用户查找 (/en-us/citrix-cloud/media/attribute-sources.png)

7. 配置**适配器合同履行**。选择 **LDAP** 和您的活动目录数据存储名称作为用户属性数据的来源。值是用户的活动目录属性，例如 `objectGUID` 或 `objectSid`。

   配置适配器合同履行 (/en-us/citrix-cloud/media/adapter-contract-fulfillment.png)

8. 二进制属性编码应在**HTML 表单适配器**摘要中显示，如下图所示。

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

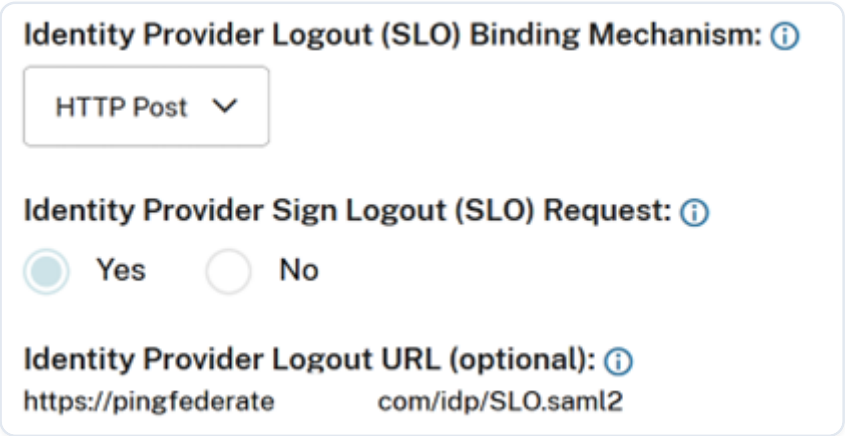
配置适配器摘要1 (/en-us/citrix-cloud/media/configure-adapter-summary1.png)

配置适配器摘要2 (/en-us/citrix-cloud/media/configure-adapter-summary2.png)

配置服务提供商连接 (SAML 应用程序) 以用于 Citrix Cloud 或 Workspaces

下面提供的 PingFederate 示例配置假定您的组织中存在以下 SAML 身份验证要求。

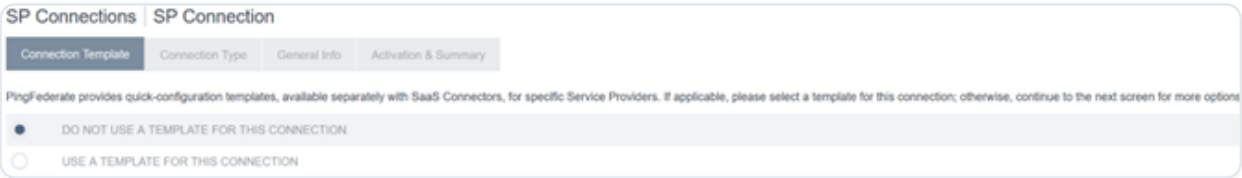
- 从商店/Citrix Cloud 管理控制台发送的 SAML 身份验证请求必须签名。
- SAML HTTP POST 绑定将用于 SSO 和 SLO 请求。
- 单点注销 (SLO) 是您组织中的一项要求。当最终用户从商店或 Citrix Cloud 管理控制台注销时，Citrix Cloud 会向 SAML 提供商 (IdP) 发送 SAML SLO 请求以注销用户。
- PingFederate 需要签名的 HTTP POST 请求才能启动注销。SAML 提供商需要签名的 SLO 请求。



有关详细信息，请参阅 PingFederate SP 管理

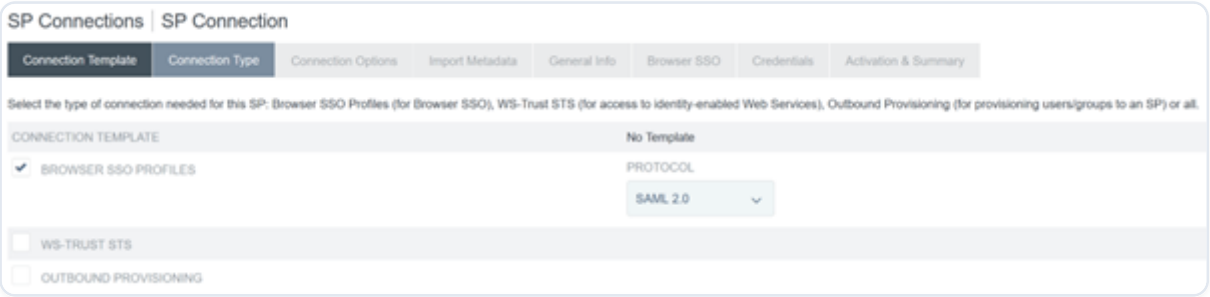
步骤

1. 配置 **连接模板**。

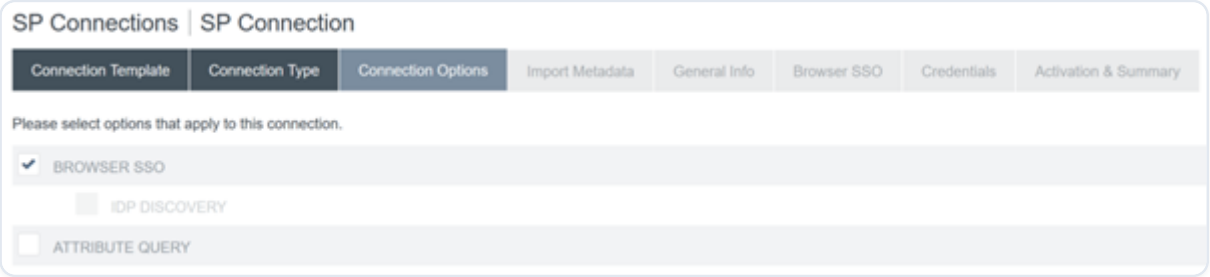


2. 配置 **连接类型** 并选择 **浏览器 SSO 配置文件和 SAML 2.0**。

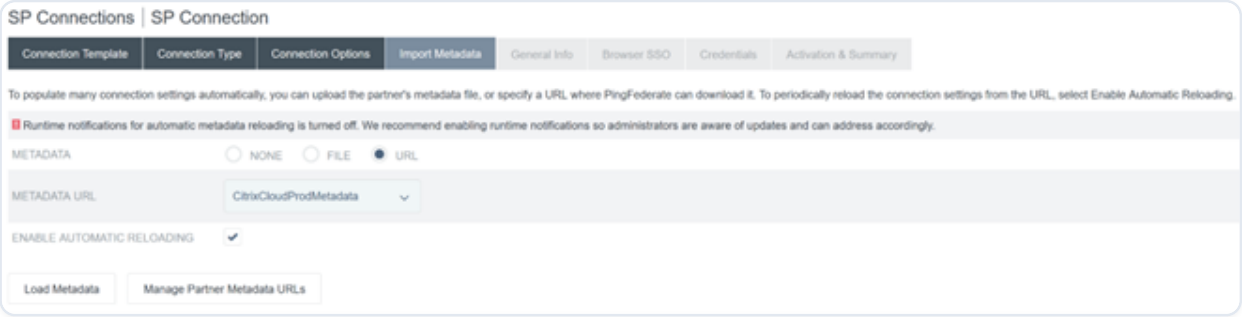
© 1997–2026 Citrix Systems, Inc. All rights reserved.



3. 配置 **连接选项**。



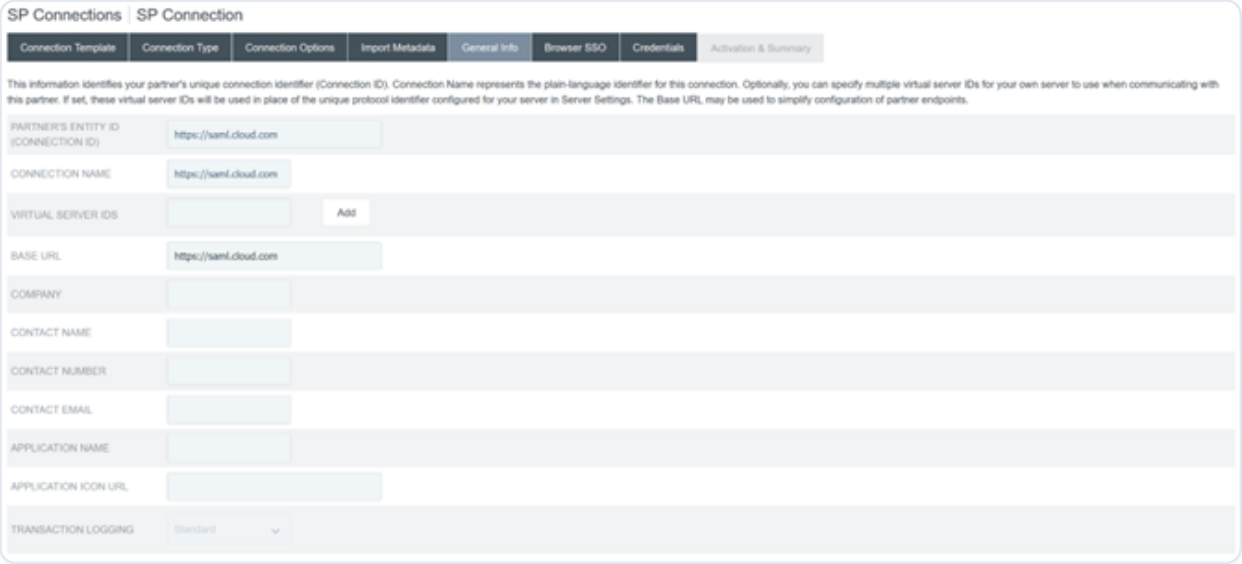
4. 导入 Citrix Cloud 元数据。选择 URL 和您之前创建的 `CitrixCloudProdMetadata` URL，然后单击“**加载元数据**”。



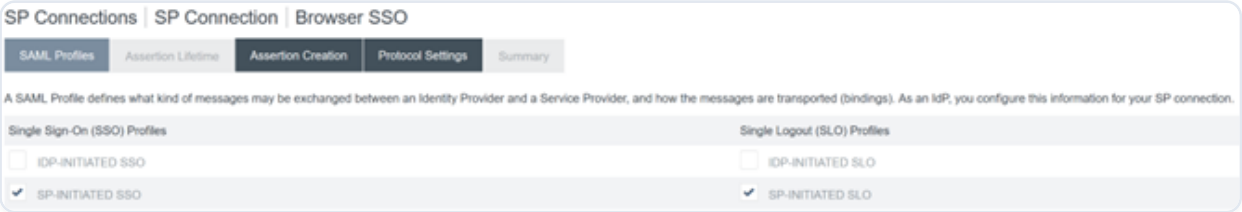
5. 配置“**常规信息**”。将服务提供商连接实体 ID、基本 URL 和连接名称设置为您的 Citrix Cloud 客户区域的 Citrix Cloud SAML 端点。

   - `<https://saml.cloud.com>` - 商业版（欧盟、美国和亚太地区）
   - `<https://saml.citrixcloud.jp>` - 日本
   - `<https://saml.cloud.us>` - 政府版

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



6. 配置“**协议设置**”。

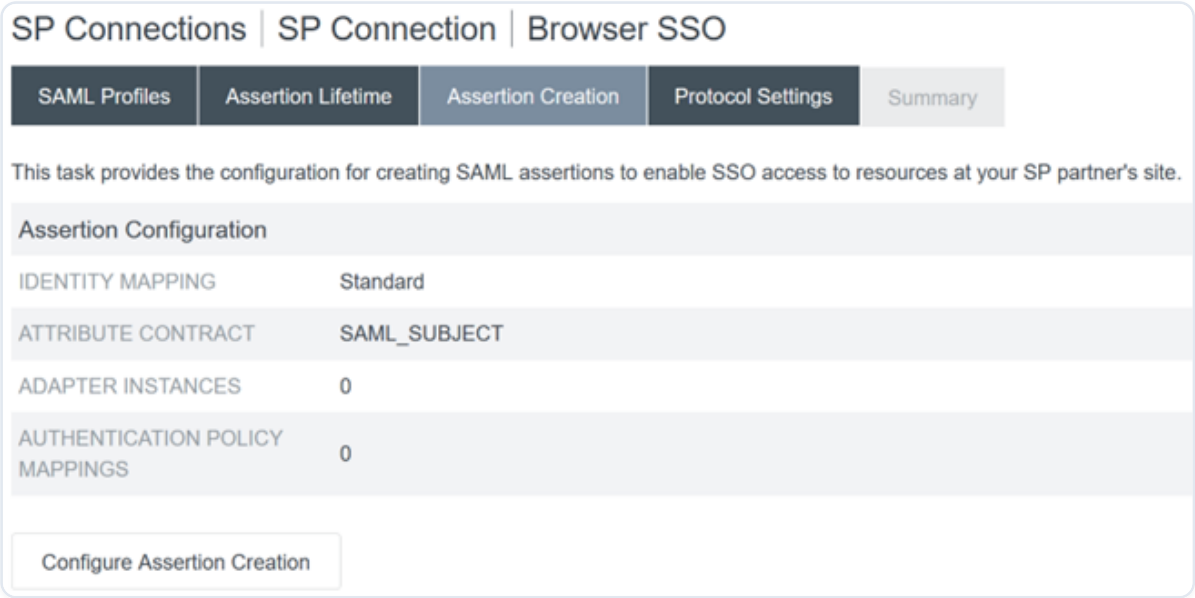


7. 使用默认的“**断言生存期**”设置。

8. 配置 SAML 断言创建。

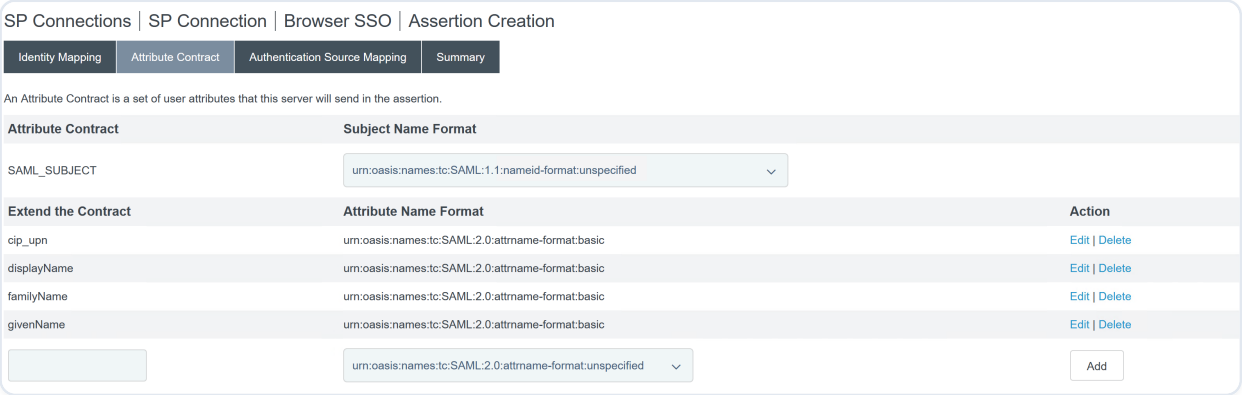
   a. 单击“**配置断言创建**”

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



b. 选择“**标准**”。

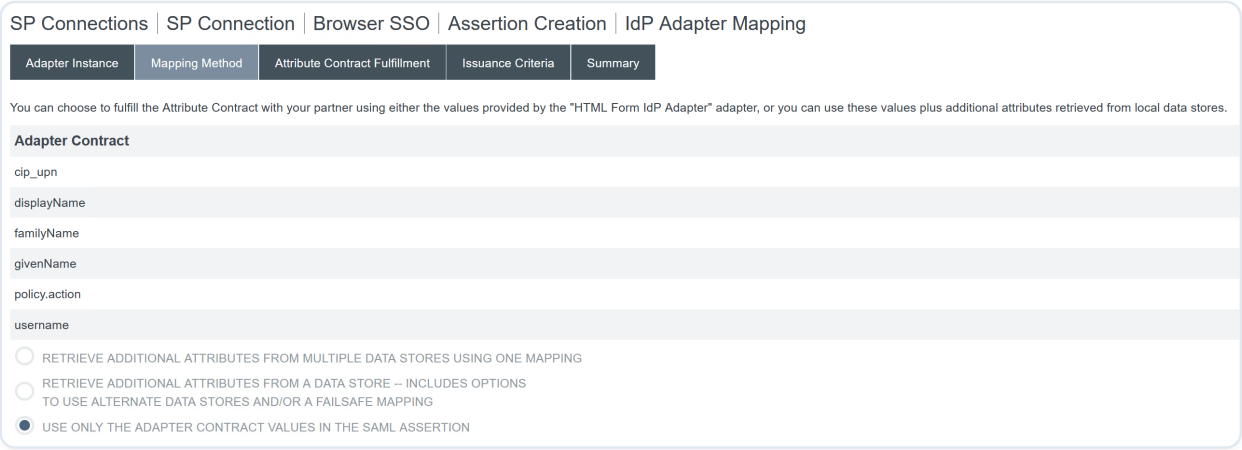
9. 配置 **属性协定**。



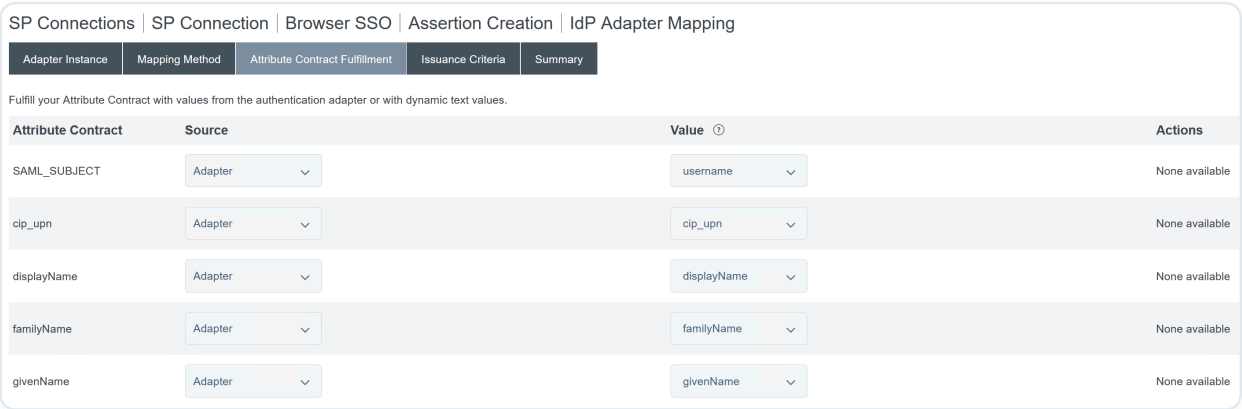
10. 配置 **适配器实例**。

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

11. 配置 **映射方法**。



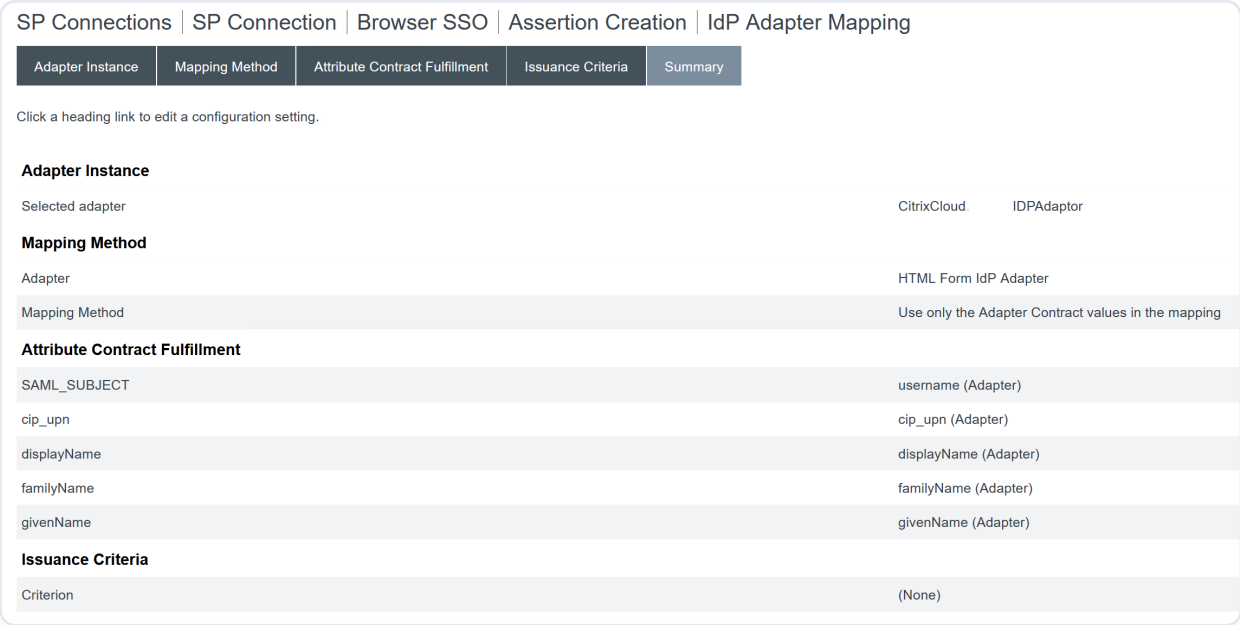
12. 配置 **属性协定履行**。



13. 配置 **颁发条件**，使用默认值且不带任何条件。

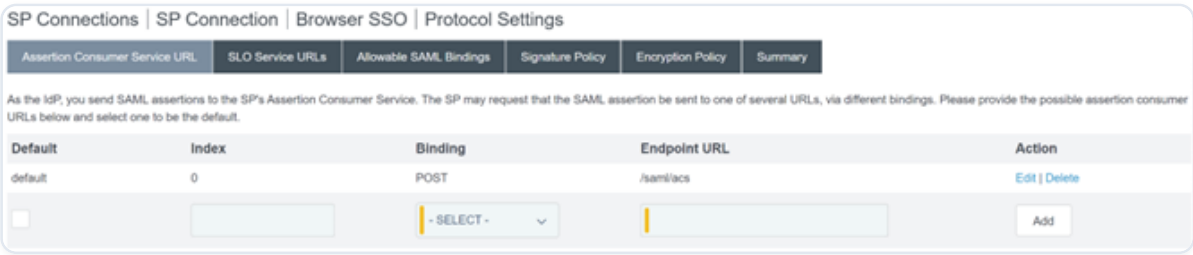
© 1997–2026 Citrix Systems, Inc. All rights reserved.

14. 已完成的 **IDP 适配器映射** 显示如下：



15. 配置 **协议设置**。Citrix Cloud 所需的 SAML 路径将附加到您的 PingFederate 服务器基本 URL。可以通过在端点 URL 字段中输入完整路径来覆盖基本 URL，但这通常是不必要且不推荐的。 基本 URL - `<https://youpingfederateserver.domain.com>`

    a. 配置断言消费者服务 URL，它将 SAML 路径附加到 PingFederate 服务器基本 URL。端点 URL - `/saml/acs`



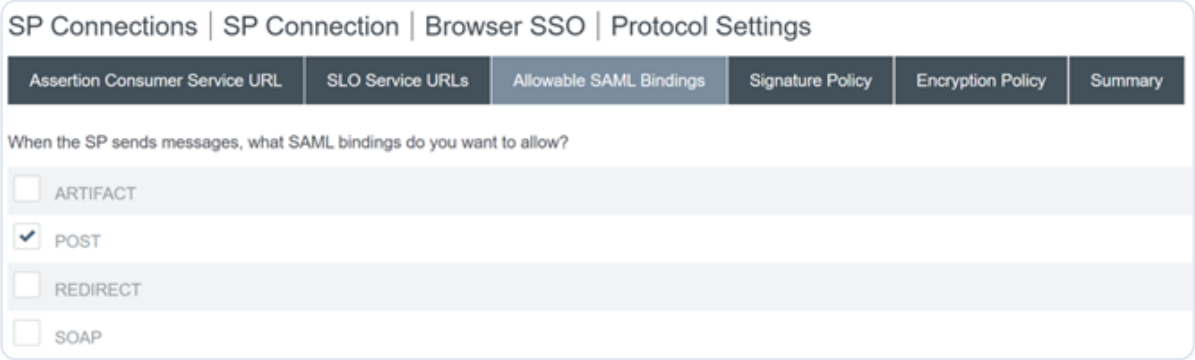
    b. 配置 **SLO 服务 URL**。端点 URL - `/saml/logout/callback`

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

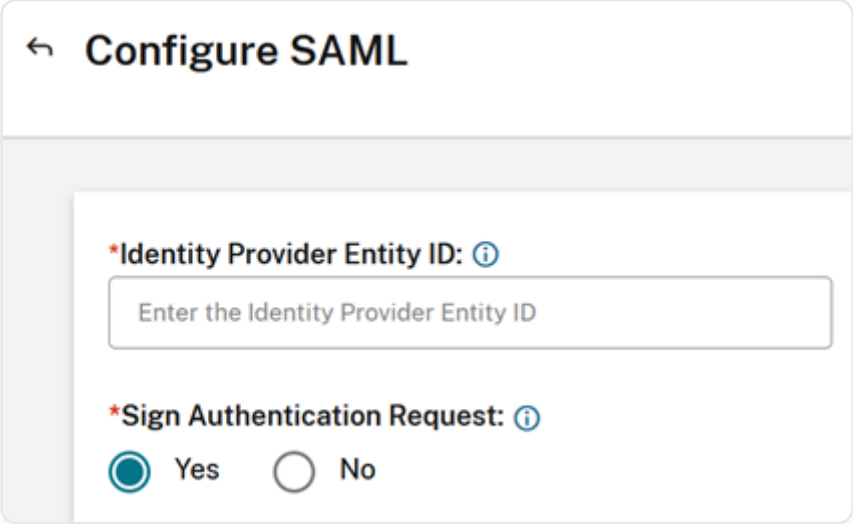
重要提示：

如果您希望在退出商店或 Citrix Cloud 时执行 SLO，则 Citrix Cloud SAML 连接需要配置 PingFederate 注销 URL 以匹配此项。如果未在 SAML 连接中配置注销 URL，则最终用户将仅从商店注销，而不会从 PingFederate 注销。

a. 配置 **允许的 SAML 绑定**。



b. 配置 **签名策略**。

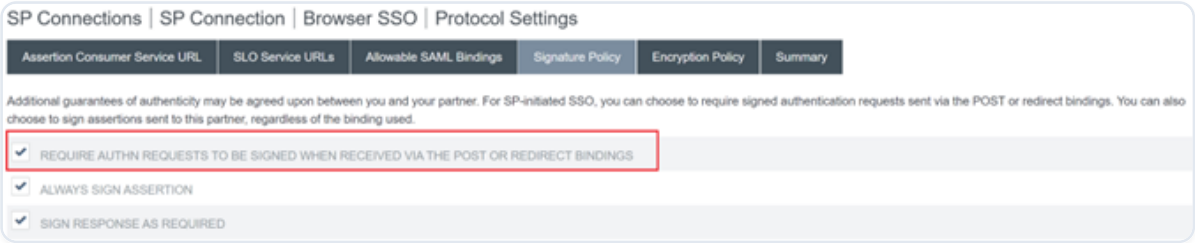


重要提示：

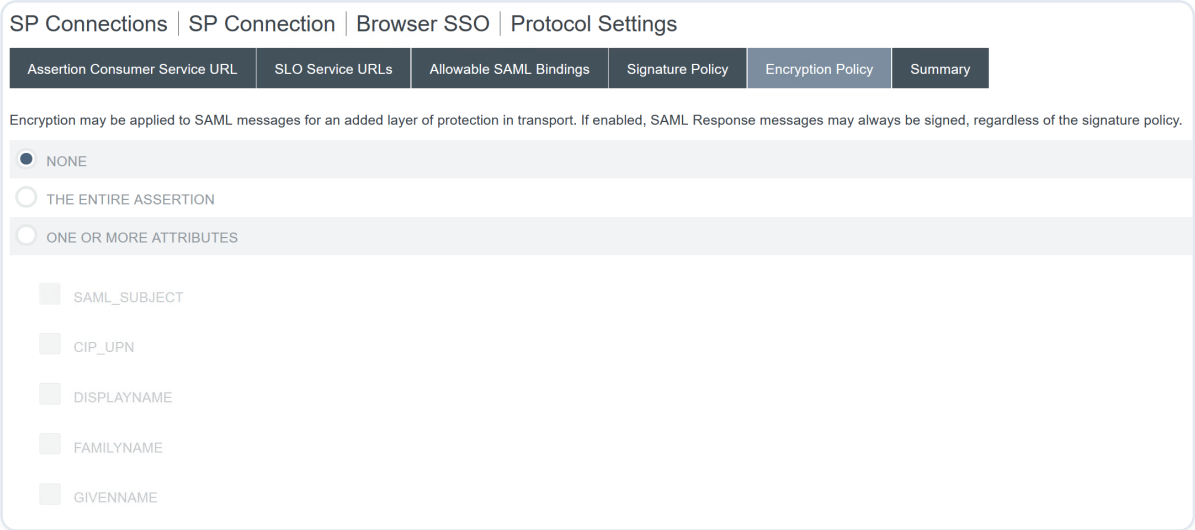
SAML 签名设置必须在 SAML 连接的两端保持一致配置。商店或 Citrix Cloud (SP) 必须配置为发送已签名的 SSO 和 SLO 请求。

a. 必须配置 PingFederate (IDP) 以使用 Citrix Cloud SAML 签名验证证书来强制执行已签名的请求。

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



b. 配置 **加密策略**。

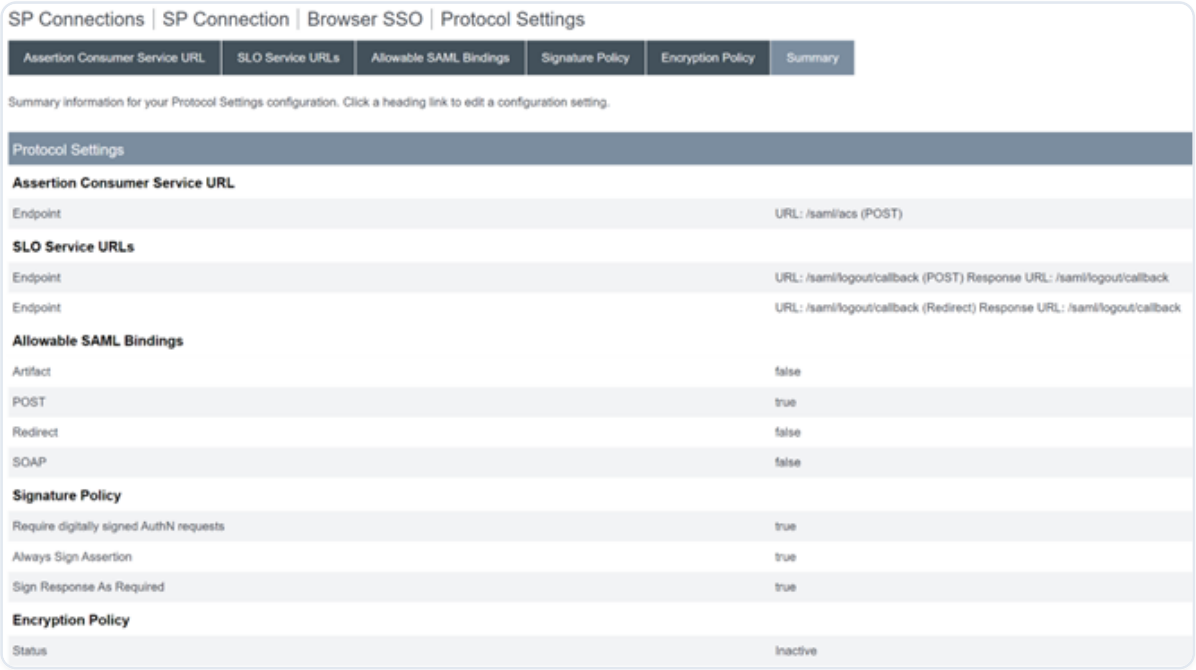


注意：

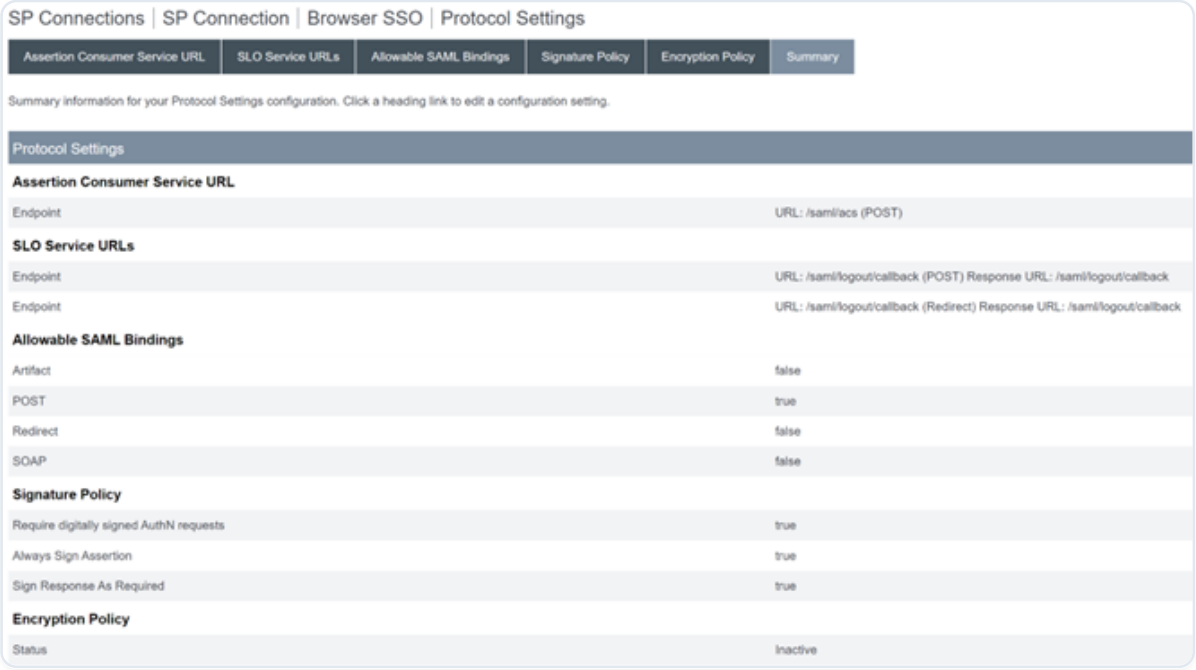
建议在初始设置和测试期间将加密设置为 **NONE**，以便您可以调试断言中缺少或不正确的 SAML 属性的任何问题。如果您需要加密断言，建议您在证明登录到商店或 Citrix Cloud 成功且所有资源都已成功枚举并可以启动后，再启用加密。如果您无法查看 SAML 断言的纯文本内容，则在启用加密的情况下调试 SAML 问题将是不可能的。

c. 查看**摘要**选项卡。

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



d. 查看 **Citrix Cloud 服务提供商 (SP) 连接**。配置 **Citrix Cloud SP 连接**后，它应如下例所示：



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

Browser SSO	
SAML Profiles	
IdP-Initiated SSO	false
IdP-Initiated SLO	false
SP-Initiated SSO	true
SP-Initiated SLO	true
Assertion Lifetime	
Valid Minutes Before	5
Valid Minutes After	5

Assertion Creation	
Identity Mapping	
Enable Standard Identifier	true
Attribute Contract	
Attribute	SAML_SUBJECT
Subject Name Format	urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified
Attribute	cip_upn
Attribute Name Format	urn:oasis:names:tc:SAML:2.0:attrname-format:basic
Attribute	displayName
Attribute Name Format	urn:oasis:names:tc:SAML:2.0:attrname-format:basic
Attribute	familyName
Attribute Name Format	urn:oasis:names:tc:SAML:2.0:attrname-format:basic
Attribute	givenName
Attribute Name Format	urn:oasis:names:tc:SAML:2.0:attrname-format:basic
Authentication Source Mapping	
Adapter instance name	CitrixCloudStagingIDPAdaptor
Adapter Instance	
Selected adapter	CitrixCloudStagingIDPAdaptor
Mapping Method	
Adapter	HTML Form IdP Adapter
Mapping Method	Use only the Adapter Contract values in the mapping
Attribute Contract Fulfillment	
SAML_SUBJECT	username (Adapter)
cip_upn	cip_upn (Adapter)
displayName	displayName (Adapter)
familyName	familyName (Adapter)
givenName	givenName (Adapter)

Protocol Settings	
Assertion Consumer Service URL	
Endpoint	URL: /saml/acs (POST)
SLO Service URLs	
Endpoint	URL: /saml/logout/callback (POST) Response URL: /saml/logout/callback
Endpoint	URL: /saml/logout/callback (Redirect) Response URL: /saml/logout/callback
Allowable SAML Bindings	
Artifact	false
POST	true
Redirect	false
SOAP	false
Signature Policy	
Require digitally signed AuthN requests	true
Always Sign Assertion	true
Sign Response As Required	true
Encryption Policy	
Status	Inactive
Credentials	
Digital Signature Settings	
Selected Certificate	CN=*.; .com, O="Citrix Systems, Inc.", L=Fort Lauderdale, ST=Florida, C=US (0C:BE:67:B8:63:15:D4:D4:8B:3A:17:65:0F:71:0A:FD | Exp: Sep 19, 2024)
Include Certificate in KeyInfo	false
Selected Signing Algorithm	RSA SHA256
Signature Verification	
Trust Model	
Trust Model	Unanchored
Signature Verification Certificate	
Active Certificate 1	CN=samlsigning.cloud .com, O="Citrix Systems, Inc.", L=Fort Lauderdale, ST=Florida, C=US (03:48:4A:61:BF:59:EB:13:9C:20:FE:F1:5B:3A:83:29 | Exp: May 11, 2024)
Active Certificate 2	CN=samlsigning.cloud .com, O="Citrix Systems, Inc.", L=Fort Lauderdale, ST=Florida, C=US (0B:5F:B5:43:89:16:B0:2F:98:45:58:D1:DA:D1:B1:1D | Exp: Mar 11, 2025)

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

> **有用提示：**
>
> 使用 SP 连接激活和摘要页面来查看您的 SAML 应用程序并进行调试，因为它允许快速轻松地进行配置更改。SP 连接激活和摘要页面允许您通过单击任何 SAML 配置子部分的标题来导航到该部分。单击任何以红色突出显示的标题以更新这些设置。

Protocol Settings	
Assertion Consumer Service URL	
Endpoint	URL: /saml/acs (POST)
SLO Service URLs	
Endpoint	URL: /saml/logout/callback (POST)
Allowable SAML Bindings	
Artifact	false
POST	true
Redirect	true
SOAP	false
Signature Policy	
Require digitally signed AuthN requests	false
Always Sign Assertion	true
Sign Response As Required	true

16. 已完成的 **Citrix Cloud SP 连接**应在列表中显示如下。

17. 可以将 SP 连接导出为 XML 文件。Citrix 建议您在与 Citrix Cloud 和商店测试 SP 连接后，对其进行备份。

配置 Citrix Cloud SAML 连接

所有 Citrix 登录流程都需要由服务提供商发起，使用商店 URL 或 Citrix Cloud GO URL。

使用 **身份和访问管理** → **身份验证** → **添加身份提供程序** → **SAML** 中 SAML 连接的默认推荐值。

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

CITRIX CLOUD 中的此字段	输入此值
实体 ID	`https://yourpingfedbaseurl.domain.com`，其中 `yourpingfedbaseurl.domain.com` 是您的 PingFederate 服务器域。
签署身份验证请求	是
SSO 服务 URL	`https://yourpingfedbaseurl.domain.com/idp/SSO.saml2`，其中 `yourpingfedbaseurl.domain.com` 是您的 PingFederate 服务器域。
SSO 绑定机制	HTTP 提交
SAML 响应	签署响应或断言
身份验证上下文	未指定，精确
注销 URL	`https://yourpingfedbaseurl.domain.com/idp/SLO.saml2`，其中 `yourpingfedbaseurl.domain.com` 是您的 PingFederate 服务器域。
签署注销请求	是
SLO 绑定机制	HTTP 提交

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

重要：

- 不支持使用不正确的 PingFederate IDP 发起的 SSO 端点 `https://yourpingfederateserver.domain.com/idp/startSSO.ping?PartnerSpId=https://saml.cloud.com`。Citrix Cloud 和商店不支持 IDP 发起的 SSO。
- 以下摘录自 PingFederate 文档： 这是用于启动非请求的 IdP 发起的单点登录 (SSO) 事务的路径，在此事务期间，包含断言的 SAML 响应将发送到服务提供商 (SP)。
- 已知使用不正确的 SAML 端点会导致 SAML 登录失败以及 Citrix Cloud 身份验证平台中出现以下错误。 `ExceptionMessage=An IdP-initiated SAML response from YourSAMLApp was received unexpectedly.`

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

Citrix Cloud™ 许可

Citrix Cloud 为某些云服务提供许可和使用情况监控。此外，对于已向 Citrix Cloud 注册 Citrix License Server 的本地部署，也提供许可和使用情况监控。

企业客户许可

企业客户可以通过从 Citrix Cloud 菜单中选择“**许可**”来监控受支持云服务的许可分配和使用情况。

Citrix Cloud 许可菜单(/en-us/citrix-cloud/media/lic-usage-menu-v3.png)

有关针对云服务的企业许可和使用情况监控的更多信息，请参阅监控云服务的许可和活动使用情况。

本地部署许可

拥有 Citrix Virtual Apps and Desktops 本地部署的企业客户可以使用 Citrix Cloud 随时了解用户/设备和并发许可模型的许可和使用情况。通过向 Citrix Cloud 注册 Citrix License Server，客户可以使用 Citrix Cloud 中的“**已许可部署**”页面执行以下任务：

- 监控已注册许可服务器的报告状态
- 查看使用用户/设备许可模型的部署的许可分配和使用趋势。
- 查看使用并发许可模型的部署的许可峰值使用趋势。

有关针对本地 Virtual Apps and Desktops 部署的许可和使用情况监控的更多信息，请参阅监控本地部署的许可和使用情况。

Citrix 服务提供商 (CSP) 许可

Citrix 服务提供商可以使用以下工具了解和报告产品许可和使用情况：

- License Usage Insights 是 Citrix Cloud 中的一项免费服务，用于收集和汇总针对单租户和多租户客户的产品使用情况信息。有关更多信息，请参阅Citrix 服务提供商许可。
- Citrix Cloud 中的许可功能使 CSP 的客户能够监控其支持的 Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops™ 服务）产品的许可证和使用情况。CSP 也可以在其客户的 Citrix Cloud 帐户下登录，以查看和导出此信息。有关更多信息，请参阅以下文章：

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

- Citrix DaaS 的客户许可证和使用情况监控(/zh-cn/citrix-cloud/license-usage-insights/virtual-apps-desktops-service-licensing-citrix-service-providers.html)

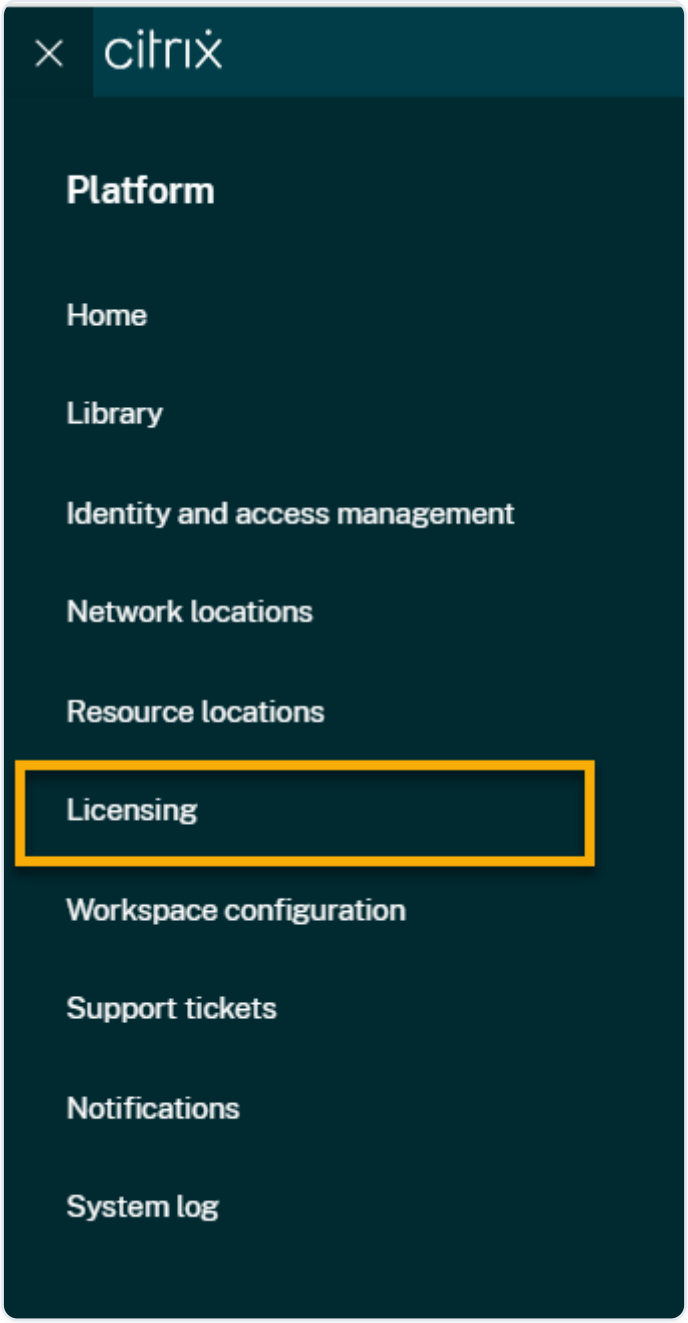
监控云服务的许可证和活动使用情况

Citrix Cloud™ 中的许可功能使您能够掌握所购买云服务的许可证消耗情况。通过使用摘要和详细报告，您可以：

- 概览许可证可用性和分配情况
- 查看适用云服务的每日和每月活动使用趋势
- 深入查看单个许可证分配详细信息和使用趋势
- 将许可证使用数据导出到 CSV

要查看云服务的许可数据，请从控制台菜单中选择“**许可**”。

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



注意：

本文介绍了所有受支持的 Citrix Cloud 服务通用的许可功能。许可的某些方面可能因服务而异（例如，许可证分配）。有关每项服务的许可证和使用情况的更多信息，请参阅以下文章：

- 监控 Citrix DaaS 的许可证和活动使用情况（用户/设备）
- 监控 Citrix DaaS 和 Citrix DaaS Standard for Azure 的许可证和峰值使用情况（并发）
- 监控 Citrix DaaS Standard for Azure 的许可证和活动使用情况（仅限用户/设备）
- 监控 Endpoint Management 服务的许可证和活动使用情况
- 监控 Gateway 服务的带宽使用情况

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

- 监控 Secure Private Access 的许可证和使用情况(/zh-cn/citrix-cloud/citrix-cloud-management/license-usage/secure-workspace-access-license-usage.html)

支持的区域和云服务

许可仅适用于美国、欧盟和亚太南部地区支持的服务。

许可支持以下云服务：

- Citrix DaaS（用户/设备和并发许可模式）- 以前称为 Citrix Virtual Apps and Desktops 服务
- 适用于 Azure 的 Citrix DaaS Standard（用户/设备许可模式）- 以前称为适用于 Azure 的 Citrix Virtual Apps and Desktops Standard
- 端点管理
- 网关
- 安全专用访问（以前称为 Secure Workspace Access）

Citrix DaaS™ 的多类型许可

Citrix Cloud 中的许可支持 Citrix DaaS 的多类型许可。如果用户/设备和并发许可模式都引入到单个 Citrix Cloud 帐户中，Citrix Cloud 会在“许可”控制台页面中显示每种许可模式下的许可证使用情况。

Citrix 建议在查看“许可”页面之前，在站点和交付组级别设置多类型许可。否则，可能不会显示正确的信息。有关说明，请参阅 Citrix DaaS 文档中的多类型许可。

如果成功使用 Web Studio 或 PowerShell 设置方法后，“许可”控制台页面未显示正确的多类型许可证使用情况，您可以选择以下选项：

- 等待 30 天并释放所有未使用的许可证。
- 联系Citrix 客户服务。

许可证分配

通常，用户在首次使用云服务时会被分配许可证。某些服务可能会根据其使用的许可模式以不同方式分配许可证。有关如何为每项服务分配许可证的更多信息，请参阅本文顶部引用的许可文章。

许可摘要和详细信息

许可摘要视图(/en-us/citrix-cloud/media/lic-usage-summary-view-v2.png)

许可摘要提供每个受支持服务的以下信息概览：

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

- 已分配的购买许可证总数的百分比。当百分比接近 100% 时，百分比颜色从绿色变为黄色。如果百分比超过 100%，百分比颜色变为红色。
- 已分配许可证与购买许可证的比率以及剩余可用许可证的数量。
- 云服务订阅到期前的剩余时间。如果订阅在未来 90 天内到期，将显示警告消息。

对于某些服务，此摘要可能包含其他信息，例如活动使用情况。有关服务特定详细信息的更多信息，请参阅本文顶部引用的许可文章。

使用趋势和许可证活动

要查看云服务许可证的详细信息，请单击 **查看使用情况详细信息**。然后，您可以查看使用趋势和云服务许可证使用者的细分。

许可证使用情况分配趋势图(/en-us/citrix-cloud/media/lic-usage-assignment-trends-v2.png)

此细分包含不同的信息，具体取决于云服务。有关服务特定的使用趋势和许可证活动的更多信息，请参阅本文顶部引用的许可文章。

释放已分配的许可证

通常，如果使用者连续 30 天未使用云服务，则已分配的许可证有资格被释放。释放许可证后，剩余许可证的数量会增加，而已分配许可证的数量会相应减少。

对于某些服务，根据所使用的许可模型，释放许可证的方式可能有所不同。有关释放特定服务许可证的更多信息，请参阅本文顶部引用的许可文章。

常见问题

- **如果分配的许可证超出购买的许可证，Citrix® 是否会阻止云服务使用？** 不会，如果您过度使用云许可证数量，Citrix 不会阻止任何服务启动。许可证使用情况提供有关了解云许可证使用情况的信息，因此 Citrix 希望您监控许可证分配并保持在购买的许可证数量范围内。如果在任何时候，您认为您将过度使用您的服务，Citrix 鼓励您联系您的销售代表讨论您的许可要求。
- **正在捕获哪些许可信息？** 目前，仅捕获与用户登录相关的许可信息。
- **Citrix DaaS 是否支持多类型许可（例如，同时使用用户/设备和并发用户模型）？** 是的。有关更多信息，请参阅本文中的多类型许可。
- **Citrix DaaS 是否支持多版本许可？例如，我可以在同一个 Citrix Cloud 帐户上同时使用 Premium 和 Advanced 版本吗？** 不支持此用例。一个 Citrix DaaS 站点只能获得一个版本的许可。如果您想在同一个 Citrix Cloud 帐户上使用多个 Citrix DaaS 实例，它们必须是相同的版本。

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

- **Monitor 报告（在 Director 中）与并发许可洞察之间有什么区别？** Monitor 报告和并发会话的解释提供了与正在使用的并发许可证度量不同的解释和指标。在大多数情况下，使用 Director 中并发会话的数量来表示或预测正在使用的峰值并发许可证会大大夸大所需的并发许可证数量。请勿使用 Director 中的 Monitor 报告来替代并发许可证使用情况报告。这两种报告工具之间的两个主要区别是：
  - **采样时长：** 许可具有五分钟的采样周期。每五分钟，Citrix Cloud 会统计当前连接到服务的唯一设备。所有五分钟的采样周期都会聚合，以确定 24 小时、每月和合同期内的峰值使用情况。Director 中的 Monitor 报告可以显示长达两小时的间隔，具体取决于报告的运行方式。
  - **唯一性：** 许可在会话启动时查找设备之间的唯一性。Monitor 报告不考虑唯一设备。
- **将用户迁移到云服务的新实例后（例如，我更改了组织的域名），为什么我的正在使用的许可证会为同一用户计算两次？*- Citrix Cloud 使用用户主体名称 (UPN) 来计算唯一用户。如果用户在迁移发生前后都访问了云服务，Citrix Cloud 会为该用户捕获两个唯一的 UPN，每个 UPN 具有不同的域名。因此，Citrix Cloud 会将同一用户计算两次。如果用户不再使用旧域名访问服务，您可以在 30 天后释放旧的许可证分配。如果您过度使用云许可证数量，Citrix 不会阻止任何服务启动。
- **为什么我看到同一用户或设备的重复许可证？*- 这是 Workspace app for HTML5 和本地安装的 Workspace app 的设计使然。通过 Workspace app for HTML5 启动会消耗一个用户/设备许可证。同样，通过本地安装的 Workspace app 启动也会消耗一个用户/设备许可证。因此，如果用户通过 Workspace app for HTML5 启动应用程序，然后稍后通过本地安装的 Workspace app 版本启动，Citrix Cloud 会显示该用户消耗了两个许可证。此行为不影响用户连接，但可能导致许可控制台中设备许可证使用报告虚高。如果您过度使用云许可证数量，Citrix 不会阻止任何服务启动。

监控 Citrix DaaS (用户/设备) 的许可证和活跃使用情况

本文介绍如何使用 Citrix Cloud 中的“许可”控制台管理云服务许可证分配和监控活跃使用情况。

如果您购买了 Citrix Azure 消耗基金以用于您的服务部署，请参阅 监控 Citrix DaaS 的 Citrix Managed Azure 资源消耗 了解更多信息。

许可证分配

当唯一用户或唯一设备首次启动应用程序或桌面时，Citrix Cloud 会分配一个许可证。

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

域名截断

如果您托管多个域并在这些域中拥有具有相似帐户的用户（例如，`johnsmith@company.com` 和 `johnsmith@mycompany.com`），您可以允许 Citrix Cloud 忽略帐户域，仅考虑帐户的用户名（例如，johnsmith）。此过程称为*域名截断*。默认情况下，域名截断处于禁用状态。

启用域名截断后，Citrix Cloud 对唯一用户的计算方式会发生变化。Citrix Cloud 不会将 `johnsmith@company.com` 和 `johnsmith@mycompany.com` 计为两个唯一用户，而是仅将 johnsmith 计为唯一用户。此计算更改会影响以下许可数据：

- 许可证分配
- 活跃使用情况
- 许可证使用趋势随时间变化
- 符合释放条件的许可证

从“许可”控制台将数据导出到 CSV 文件时，许可数据中的这些更改也会反映出来。

注意：

如果您托管多个域，并且这些域中具有用户名略有不同的相似帐户（例如，单个用户拥有帐户 `johnsmith@company.com` 和 `jsmith@newcompany.com`），域名截断对 Citrix Cloud 的计算没有影响。Citrix Cloud 仍将 johnsmith 和 jsmith 计为唯一用户，即使他们属于同一个人。

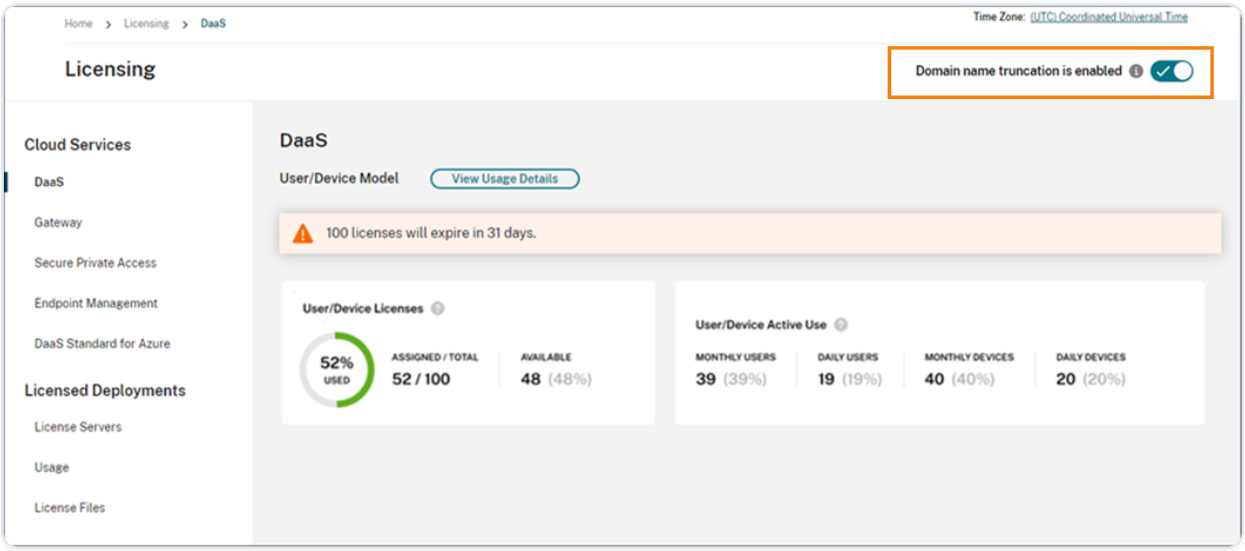
启用或禁用域名截断

默认情况下，域名截断处于禁用状态。域名截断会从您启用或禁用该功能的那一刻起影响您的用户/设备使用数据。例如，如果您在某个给定月份启用域名截断，Citrix Cloud 在该月份记录的数据将受到影响。但是，该功能禁用时前几个月的历史数据不受影响。同样，如果您在某个给定月份禁用域名截断，Citrix Cloud 在该月份记录的数据将受到影响。但是，该功能启用时的历史数据保持不变。

要启用或禁用域名截断：

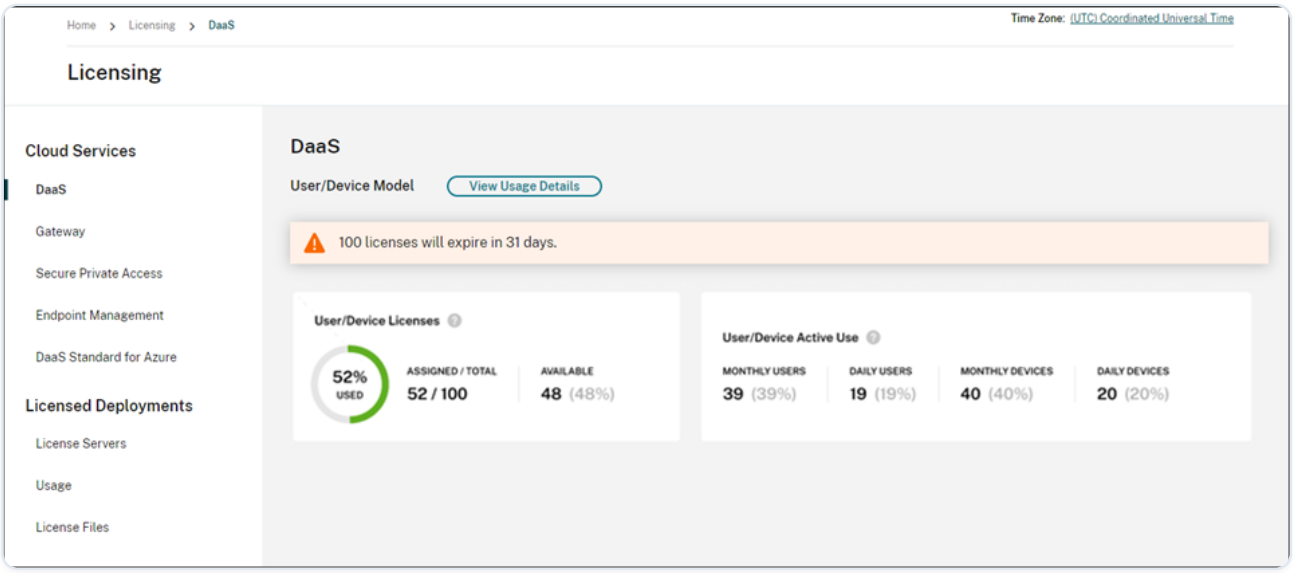
1. 单击许可控制台右上角附近的切换开关。

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



2. 当系统提示您确认操作时，选择 **是，我理解**。

许可摘要



许可摘要提供以下信息的一览视图：

- 已分配的已购买许可证总数的百分比。当百分比接近 100% 时，百分比从绿色变为黄色。如果百分比超过 100%，百分比将变为红色。

  已购买许可证的总数量是为使用用户/设备许可模型的 Citrix DaaS 版本购买的许可证的总和。
- 已分配许可证与已购买许可证的比率以及剩余可用许可证的数量。
- 每月和每日的活跃使用情况统计信息：
  - 每月活跃使用量是指过去 30 天内使用过服务的唯一用户或设备的数量。
  - 每日活跃使用量是指过去 24 小时内使用过服务的唯一用户或设备的数量。
- 云服务订阅到期前剩余的时间。如果订阅在未来 90 天内到期，将显示警告消息。

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

计算分配的许可证和活跃使用情况

为了准确反映 Citrix DaaS 的用户/设备许可模型，Citrix Cloud 会统计使用过服务的唯一用户和唯一设备的数量。为了衡量分配的许可证，Citrix Cloud 使用这些计数中较小的一个。为了衡量活跃使用情况，Citrix Cloud 将每个计数作为给定时期内活跃用户和活跃设备的数量。

计算分配许可证的示例

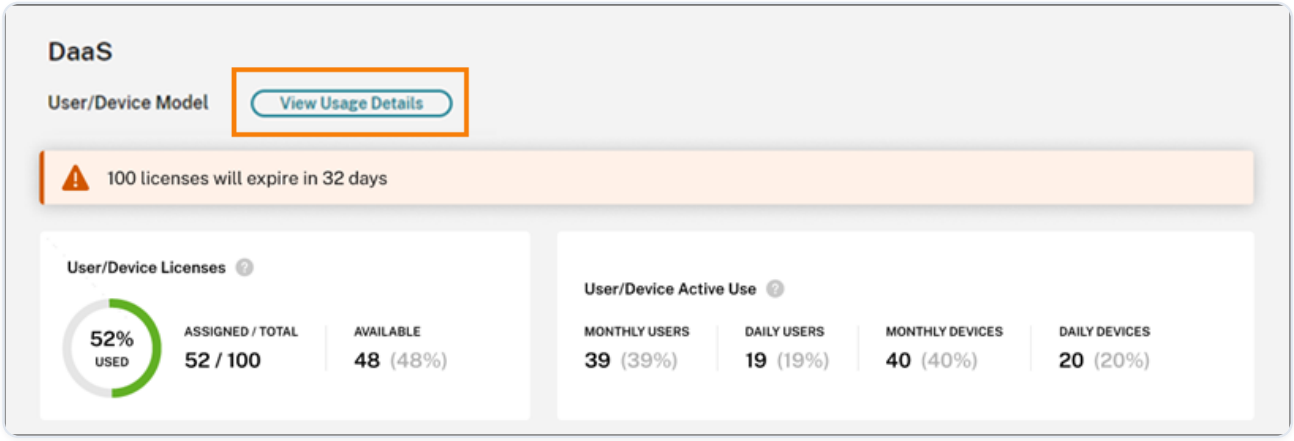
如果 100 个唯一用户和 50 个唯一设备使用了该服务，Citrix Cloud 会使用较小的数字 (50) 来确定分配的许可证数量。已使用的许可证百分比和可用许可证数量均基于这 50 个分配的许可证。

计算活跃使用情况的示例

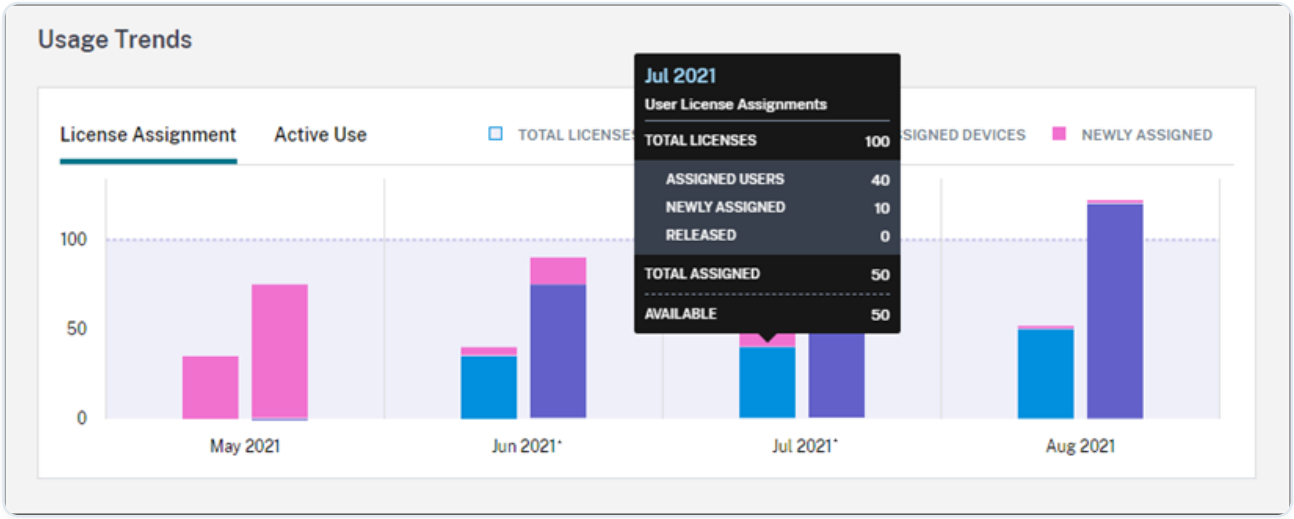
如果在过去 30 天内有 10 个唯一用户和 20 个唯一设备使用了该服务，Citrix Cloud 会确定每月活跃使用量包括 10 个活跃用户和 20 个活跃设备。同样，如果在过去 24 小时内统计到 30 个唯一用户和 15 个唯一设备，Citrix Cloud 会确定每日活跃使用量包括 30 个活跃用户和 15 个活跃设备。

使用趋势

要查看许可证的详细信息，请点击摘要最右侧的 **查看使用详情**。然后，您可以查看使用趋势以及正在使用云服务许可证的单个用户和设备的细分情况。



使用趋势 部分以图表形式显示此细分。

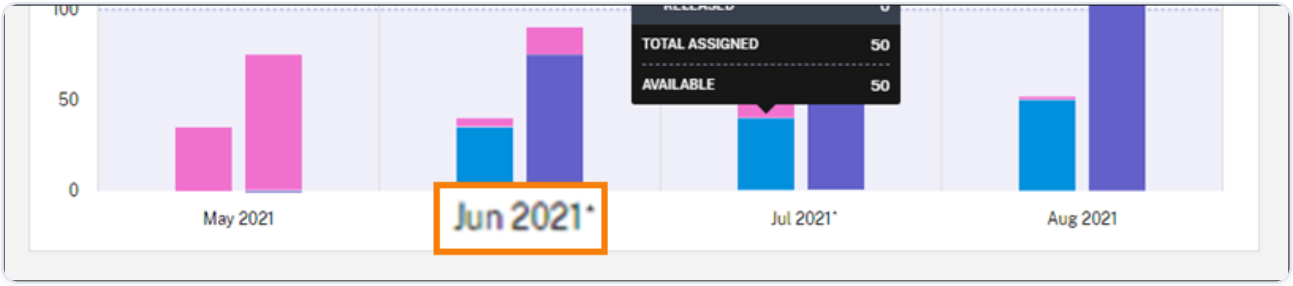


© 1997–2026 Citrix Systems, Inc. All rights reserved.

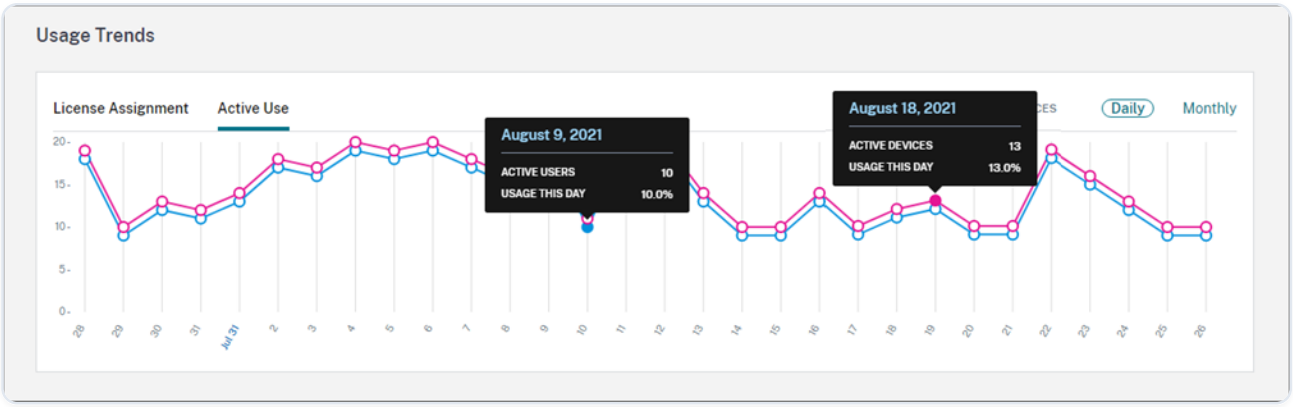
在 **许可证分配** 图表上，指向特定月份或日期的条形图会显示以下信息：

- **总许可证：** 您为云服务购买的所有授权的总许可证数量。
- **已分配用户：** 截至当前月份，分配给用户的累计许可证数量。
- **已分配设备：** 截至当月，已分配给设备的许可证累计数量。如果某个给定月份的此数字特别高，这可能是通过 Web 浏览器启动应用程序或桌面的结果。要降低此数字，Citrix® 建议使用本地安装的 Workspace 应用程序。
- **新分配：** 每个月分配的新许可证数量。例如，用户在 7 月首次访问云服务并获得许可证。此许可证在 7 月份被计为“新分配”。
- **已释放：** 每个月释放的符合条件的许可证数量。例如，如果有 20 个许可证符合释放条件，而您在 7 月释放了其中 10 个，则 7 月份显示的已释放许可证数量为 10。

启用域截断的时间间隔用星号标记。



在“**活动使用**”图表上，您可以分别查看上一个日历月和日历年的活动用户和设备。指向图表上的特定时间间隔会显示活动用户或设备的数量以及使用百分比。

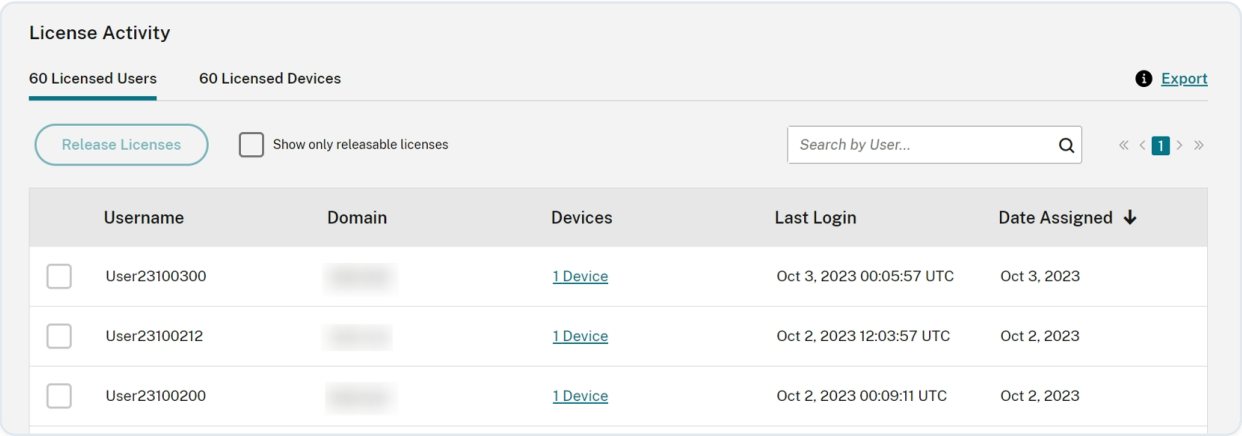


许可证活动

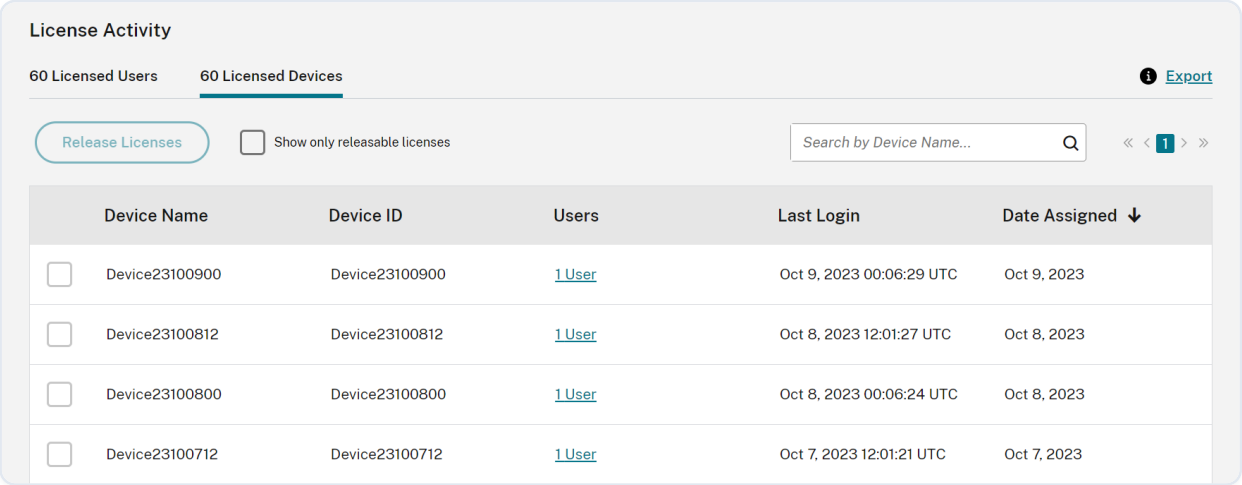
“**许可证活动**”部分显示以下信息：

- 已分配许可证的单个用户列表，包括关联设备。

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



- 已分配许可证的设备列表，包括关联用户。



- 许可证分配给用户或设备的日期。

您还可以筛选列表以仅显示符合释放条件的许可证。请参阅本文中的释放已分配许可证。

释放已分配许可证

分配许可证后，分配期为 90 天，并建立与服务的连接。如果用户或设备在 90 天内未启动应用程序或桌面，则这些许可证被视为未使用许可证，并将在 90 天后由 Citrix Cloud 释放。此过程是自动化的，无需管理员执行任何操作。

在分配期（90 天）之后，管理员仅在以下情况下才能手动释放许可证：

- 用户不再与公司关联。
- 用户正在长期休假。

管理员只能在设备停止服务时释放设备的许可证。

注意：

- 建议遵循自动释放许可证的流程。但是，如果管理员打算在 90 天期限之前释放许可证（除了上述原因），这可能会违反 Citrix EULA。在执行此操作之前，请联系 Citrix。

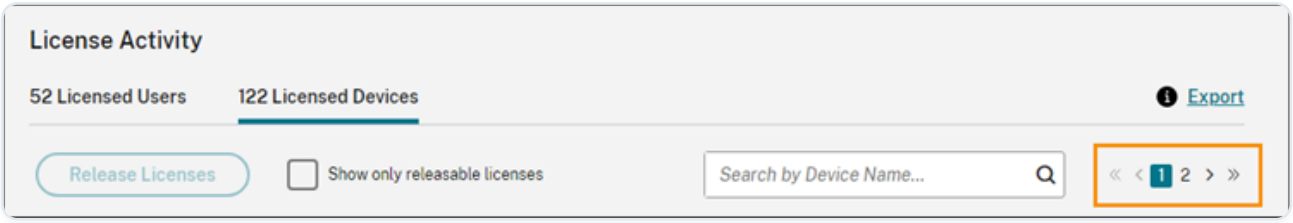
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 管理员可以通过 UI 手动释放单个许可证。或者，管理员可以选择使用云许可 API 释放许可证。有关更多信息，请参阅管理 Citrix 云许可的 API。

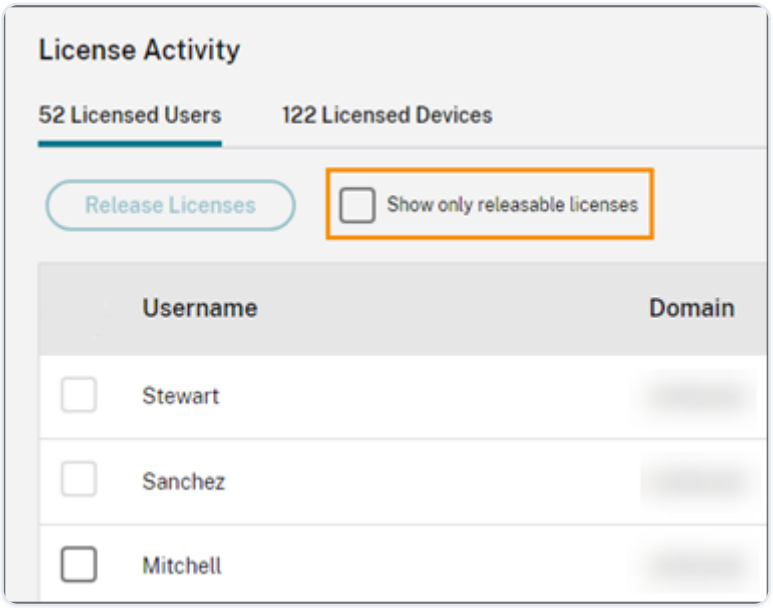
查找可释放的许可证

如果用户或设备在 30 天内未启动应用程序或桌面，Citrix Cloud 会将许可证置于可释放状态。可释放的许可证在“许可用户”或“许可设备”列表中显示为深灰色复选框，可以选中。不可释放的许可证显示为浅灰色复选框，表示无法选择该许可证。

“**许可证活动**”部分中显示的列表一次最多显示 100 个已分配的许可证。如果您有 100 多个许可证，请使用页面控件浏览列表。



要快速查找可释放的许可证，请单击“**释放许可证**”按钮旁边的“**仅显示可释放的许可证**”。此操作会隐藏尚未允许释放的已分配许可证。



选择可释放的许可证

选中每个许可证旁边的深灰色复选框以将其选中进行释放。当您从列表中选择许可证时，**释放许可证**按钮将变为活动状态。

您可以逐个选择所有可释放的许可证，然后单击**释放许可证**。

释放已分配的许可证

1. 在**许可证活动**下，单击**许可用户**或**许可设备**选项卡。

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

2. 如有需要，单击**显示可释放的许可证**以仅显示允许释放其许可证的用户。
3. 选择要管理的用户或设备，然后单击**释放许可证**。
4. 查看您已选择的用户或设备，然后单击**释放许可证**。

许可证自动切换

如果活动的“用户/设备”许可证过期，并且“并发”许可证是租户唯一活动的许可证类型，则站点许可证会自动切换到活动的“并发”许可证。这可以防止由于站点上缺少活动许可证而导致的任何中断。

监控 Citrix DaaS™ 的许可证和峰值使用情况（并发用户）

本文介绍了仅适用于 **Citrix DaaS** 的并发用户许可证管理体验。

有关 Citrix DaaS 的用户/设备许可信息，请参阅 监控 Citrix DaaS 的许可证和活动使用情况（用户/设备）。

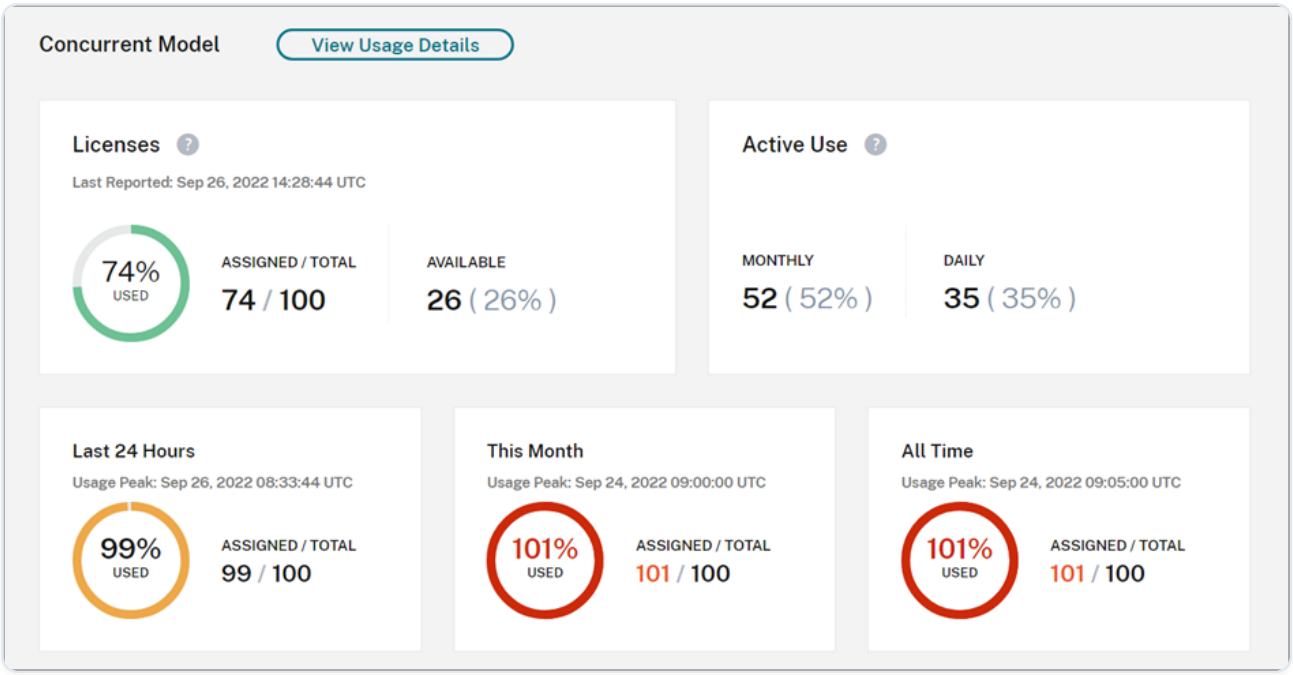
有关 Citrix DaaS Standard for Azure 的用户/设备和并发用户许可信息，请参阅 监控 Citrix DaaS Standard for Azure 的许可证和使用情况。

许可证分配

当用户在其设备上启动应用程序或桌面时，Citrix Cloud™ 会分配一个许可证。当用户注销或断开会话时，许可证将不再分配。因为许可证分配可能会根据在任何给定时间访问应用程序或桌面的设备数量而变化。

有关并发用户许可模型的更多信息，请参阅许可产品文档中的并发许可证。

许可摘要



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

许可摘要提供以下信息的一览视图：

- Citrix Cloud 上次评估正在使用的许可证时，当前正在使用的已购买许可证总数的百分比。已购买许可证总数是为使用并发用户许可模型的 Citrix DaaS 版本购买的许可证数量之和。
- 当前分配的许可证与已购买许可证总数的比率，以及剩余可用许可证的数量。此比率中显示的**总计**数字表示当前拥有的许可证总数（截至“上次报告”日期和时间）。
- 峰值使用情况统计。在计算峰值使用许可证时，Citrix Cloud 会检索以下时间段内使用的最大许可证数量：
  - **过去 24 小时：** 在过去 24 小时内一次性使用的最大许可证数量。
  - **本月：** 从当前日历月开始一次性使用的最大许可证数量。
  - **所有时间：** 从订阅开始以来，一次性使用的最大许可证数量。

  这些峰值使用期显示的**总计**数字表示当时拥有的许可证总数。如果拥有的许可证总数增加或减少，并且分配的许可证相应增加，则**总计**数字会随之更改，以反映当时拥有的新许可证数量。但是，如果没有相应的用量峰值，则**总计**数字不会更改。
- 活跃使用情况统计。Citrix Cloud 会显示以下时间段的唯一连接总数：
  - **每月：** 每月活跃使用量是指在过去 30 天内使用过服务的唯一用户或设备的数量。
  - **每日：** 每日活跃使用量是指在过去 24 小时内使用过服务的唯一用户或设备的数量。这些数字也表示为这些时间段内拥有的许可证总数的百分比。

计算正在使用的峰值许可证

为了准确反映并发用户许可模型，Citrix Cloud 会计算同时访问服务的唯一设备数量。如果此计数大于当前显示的峰值使用量，Citrix Cloud 会显示新的峰值使用量以及达到该峰值的日期和时间。如果此计数小于当前峰值使用量，则当前峰值使用量不会更改。

重要提示：

如果您在 Director 中使用 Monitor 来获取有关并发会话的信息，请注意 Monitor 报告对并发会话的解释不同，并且不能准确反映正在使用的并发用户许可证数量。有关 Monitor 报告和许可报告之间差异的更多信息，请参阅常见问题解答。

计算每月活跃使用量

在每个月初，Citrix Cloud 会对过去 30 天的数据进行快照。Citrix Cloud 会显示该日历月内发生的唯一连接总数。

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

计算每日活跃使用量

每天在同一时间，Citrix Cloud 会对过去 24 小时的数据进行快照。Citrix Cloud 会显示该 24 小时内发生的唯一连接总数。

使用趋势和许可证活动

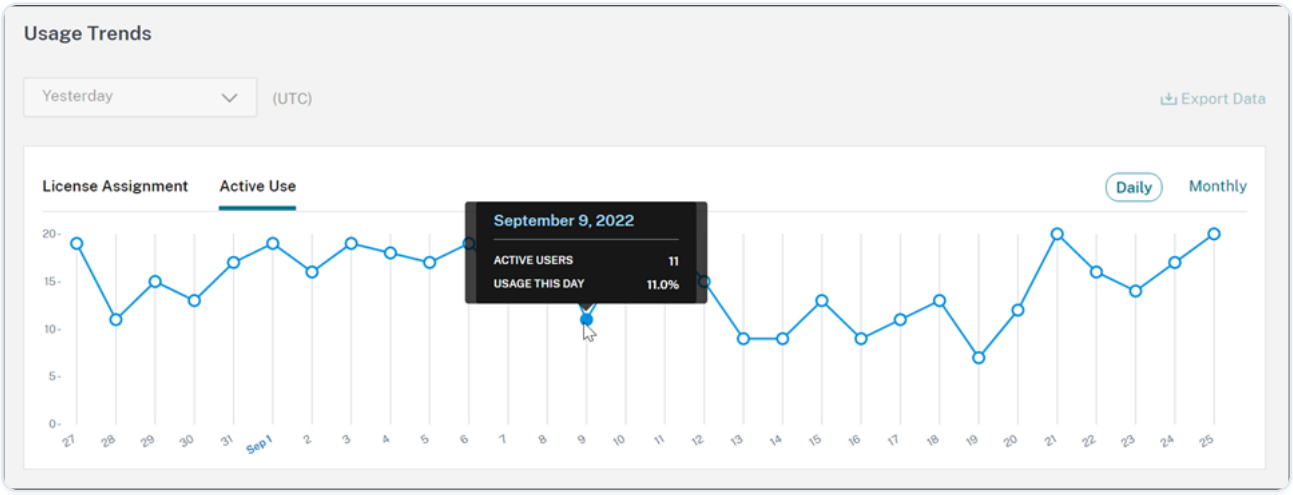
要查看许可证的历史记录，请单击**查看使用情况详细信息**。

“**使用趋势**”部分显示以下信息：

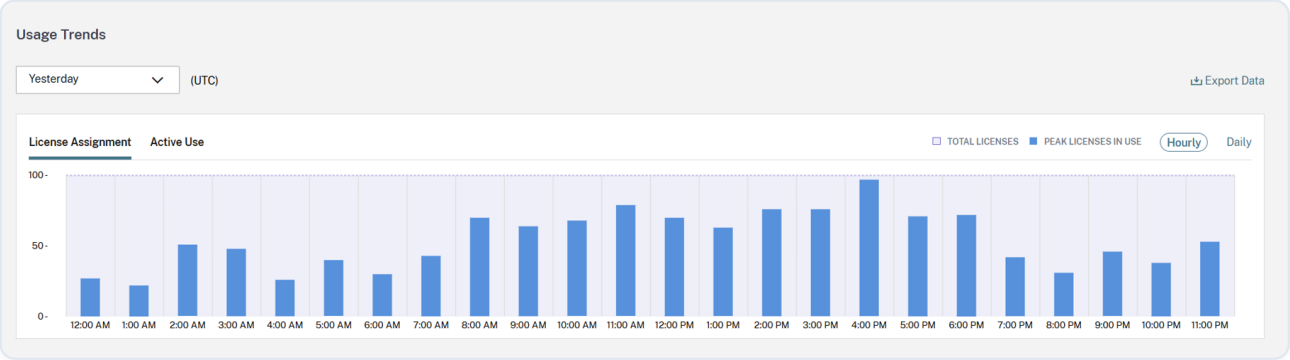
- **许可证分配**显示以下信息的图表：
  - **总许可证数：** 您购买的并发用户许可证总数。
  - **正在使用的峰值许可证数：** 您选择的日期范围内分配的最大许可证数。默认情况下，Citrix Cloud 会显示当前日历年中每个月的峰值使用情况。要深入查看每月或每小时的峰值使用情况，请从下拉菜单中选择要查看的日历月或日。

  如果您选择的日期范围尚未结束，Citrix Cloud 会显示最新时间间隔的当前峰值使用情况。例如，如果您深入查看仍在进行中的日历日，则会显示截至当前时间的每小时最大许可证数。如果最大许可证数在下一个计数间隔增加，Citrix Cloud 会更新当前小时的峰值使用情况。
- **活动使用情况**显示以下信息的图表：
  - **每日：** 过去 30 天内每天的总连接数。
  - **每月：** 过去日历年内每个月的总连接数。

指向**许可证分配**或**活动使用情况**图表上的某个时间间隔，会显示该时间间隔的详细信息。

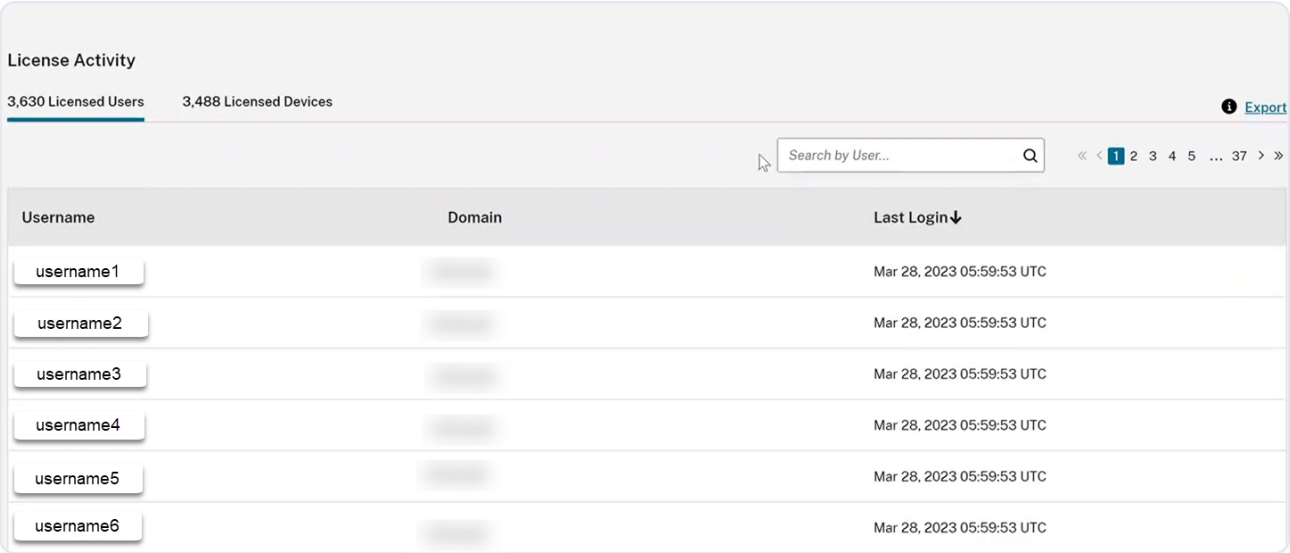


© 1997–2026 Citrix Systems, Inc. All rights reserved.



用户和设备的许可证活动

对于用户或设备许可证，**许可证活动**部分显示已分配许可证的各个用户列表，以及向用户分配许可证的日期。



释放许可证

并发用户许可证会在用户注销或断开其会话时自动释放。您无需手动释放这些许可证。

监控 Citrix DaaS Standard for Azure 的许可证和使用情况

本文介绍了管理用户/设备和并发用户许可模型许可证分配的经验。

思杰 Azure 消费基金（仅限用户/设备）

如果您购买了 Citrix Azure 消费基金以用于您的服务部署，请参阅 (/zh-cn/citrix-cloud/citrix-cloud-management/license-usage/managed-consumption.html) 以获取有关 Citrix 管理资源的消费报告的更多信息。

许可证分配

用户/设备许可模型： 当唯一用户或唯一设备首次启动桌面时，Citrix Cloud 会分配一个许可证。

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

并发用户许可模型： 当用户在其设备上启动桌面时，Citrix Cloud™ 会分配一个许可证。当用户注销或断开会话时，许可证将不再分配。由于许可证分配可能会根据在任何给定时间访问桌面的设备数量而变化，Citrix Cloud 每五分钟评估一次正在使用的许可证数量。

有关并发许可模型的更多信息，请参阅许可产品文档中的 (/zh-cn/licensing/current-release/legacy-licensing/license-types#concurrent-license)。

计算正在使用的峰值许可证

为了准确反映并发许可模型，Citrix Cloud 每五分钟计算一次同时访问服务的唯一设备数量。如果计数大于当前显示的峰值使用量，Citrix Cloud 将显示新的峰值使用量以及达到该峰值使用量的日期和时间。如果计数小于当前峰值使用量，则当前峰值使用量不会改变。

域名截断

此功能仅支持**用户/设备**许可模型。

如果您托管多个域并在这些域中拥有具有相似帐户的用户（例如，`johnsmith@company.com` 和 `johnsmith@mycompany.com`），您可以允许 Citrix Cloud 忽略帐户域，只考虑帐户的用户名（例如，johnsmith）。此过程称为*域名截断*。默认情况下，域名截断是禁用的。

启用域名截断后，Citrix Cloud 对唯一用户的计算会发生变化。Citrix Cloud 不会将 `johnsmith@company.com` 和 `johnsmith@mycompany.com` 计为两个唯一用户，而是只将 johnsmith 计为唯一用户。此计算更改会影响以下许可数据：

- 许可证分配
- 活动使用
- 许可证随时间的使用趋势
- 符合释放条件的许可证

当您从许可控制台将数据导出到 CSV 文件时，这些许可数据更改也会得到体现。

注意：

如果您托管多个具有相似帐户的域，其中用户名略有不同（例如，单个用户拥有帐户 `johnsmith@company.com` 和 `jsmith@newcompany.com`），则域名截断对 Citrix Cloud 的计算没有影响。即使 johnsmith 和 jsmith 属于同一个人，Citrix Cloud 仍将其视为唯一用户。

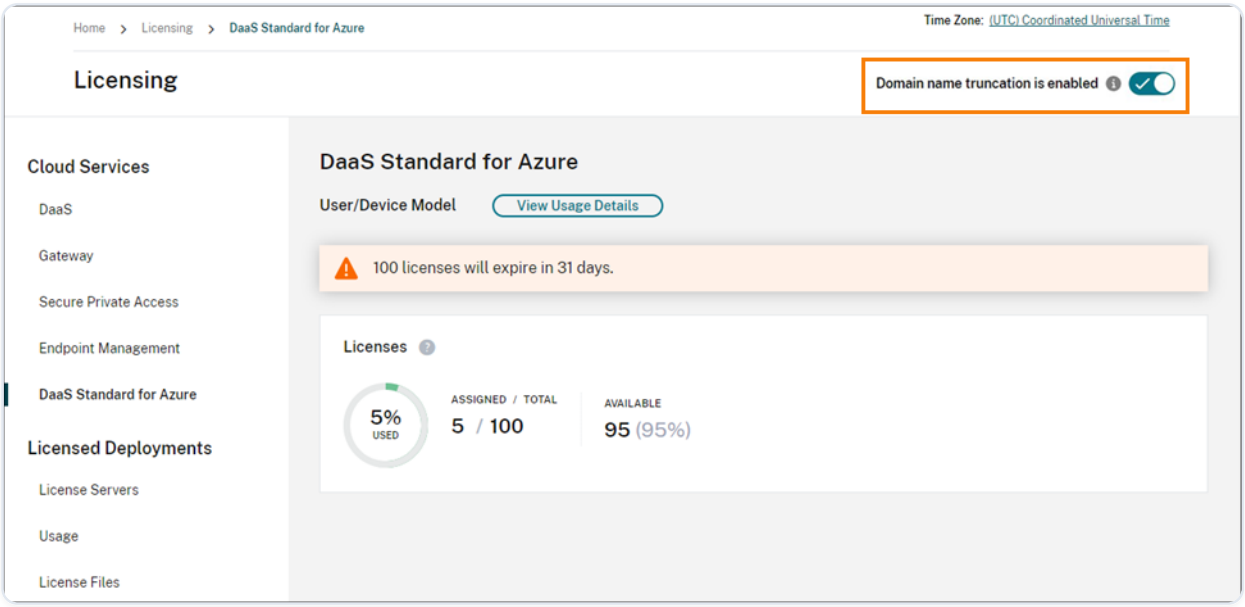
© 1997–2026 Citrix Systems, Inc. All rights reserved.

启用或禁用域名截断

默认情况下，域名截断处于禁用状态。从您启用或禁用该功能的那一刻起，域名截断就会影响您的用户/设备使用数据。例如，如果您在给定月份启用域名截断，则 Citrix Cloud 在该月份记录的数据会受到影响。但是，该功能禁用时前几个月的历史数据不受影响。同样，如果您在给定月份禁用域名截断，则 Citrix Cloud 在该月份记录的数据会受到影响。但是，该功能启用时的历史数据保持不变。

要启用或禁用域名截断：

1. 单击许可控制台右上角的切换开关。



2. 当系统提示您确认操作时，选择 **是，我理解**。

许可摘要

Citrix Cloud 会在用户/设备和并发用户许可模型下，显示正在使用的许可证的摘要视图。

用户和设备摘要

对于用户/设备模型，许可摘要显示了正在使用的许可证相对于您拥有的许可证总数。

用户/设备模型的许可证摘要视图(/en-us/citrix-cloud/media/lic-usage-summary-view-daas-azure.png)

当百分比接近 100% 时，百分比从绿色变为黄色。如果百分比超过 100%，百分比变为红色。

Citrix Cloud 还会显示已分配许可证与已购买许可证的比率以及剩余可用许可证的数量。

并发用户摘要

对于并发模型，许可摘要提供以下信息的一览视图：

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

并发模型的许可证摘要视图(/en-us/citrix-cloud/media/lic-usage-summary-view-daas-azure-concurrent.png)

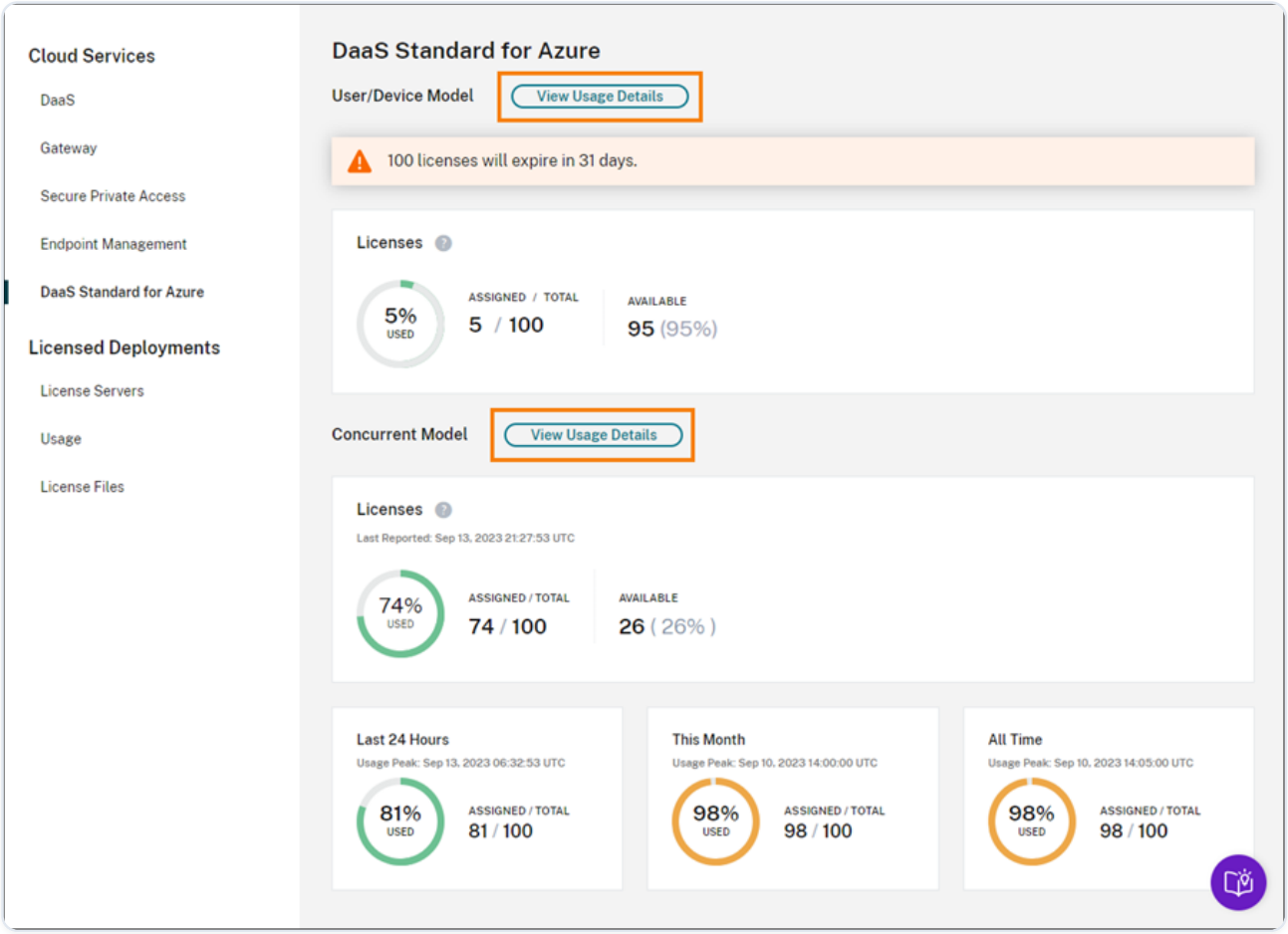
- Citrix Cloud 上次评估正在使用的许可证时，正在使用的已购买许可证总数的百分比。Citrix Cloud 每五分钟根据与服务具有活动连接的唯一设备计算此百分比。已购买许可证总数是为使用并发许可模型的 Citrix DaaS Standard for Azure 购买的许可证的总和。
- 当前已分配许可证与已购买许可证总数的比率以及剩余可用许可证的数量。此比率中显示的“**总计**”数字表示当前拥有的许可证总数（截至“上次报告”日期和时间）。
- 峰值使用情况统计信息。在计算正在使用的峰值许可证时，Citrix Cloud 会检索以下时间段内使用的最大许可证数量：
  - **过去 24 小时：** 过去 24 小时内一次性使用的最大许可证数量。
  - **本月：** 从当前日历月开始一次性使用的最大许可证数量。
  - **所有时间：** 从订阅开始一次性使用的最大许可证数量。

  这些峰值使用期显示的“**总计**”数字表示当时拥有的许可证总数。如果拥有的许可证总数增加或减少，并且已分配许可证也相应增加，则“**总计**”数字会随之更改，以反映该时间点拥有的新许可证数量。但是，如果没有相应的用量峰值，“**总计**”数字不会更改。

使用趋势

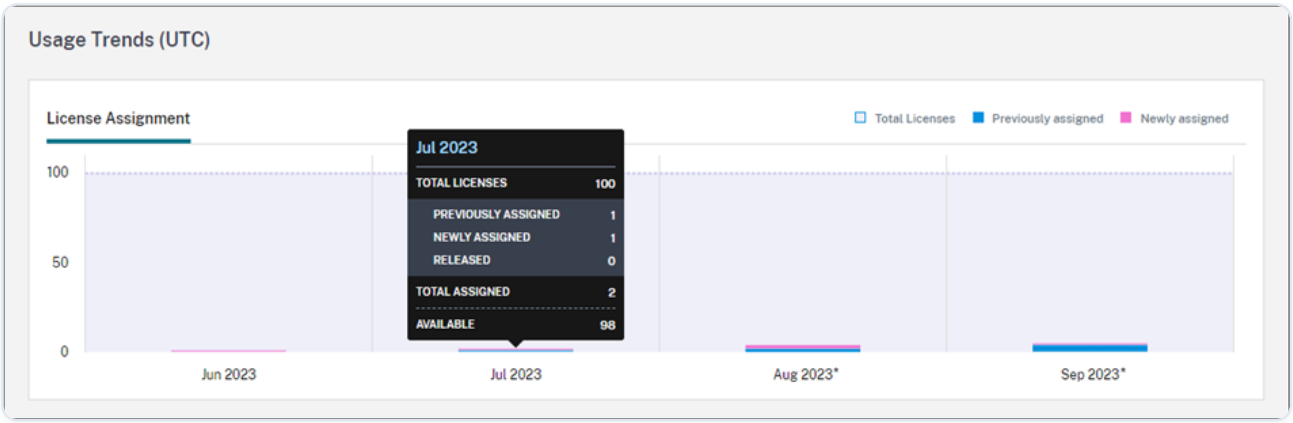
Citrix Cloud 显示用户/设备或并发用户许可证的使用趋势细分。要查看此细分，请从许可摘要页面中选择 **查看使用情况详细信息**。

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



用户和设备的趋势

对于用户/设备许可证，“**使用趋势**”部分以图表形式显示已分配许可证的细分。

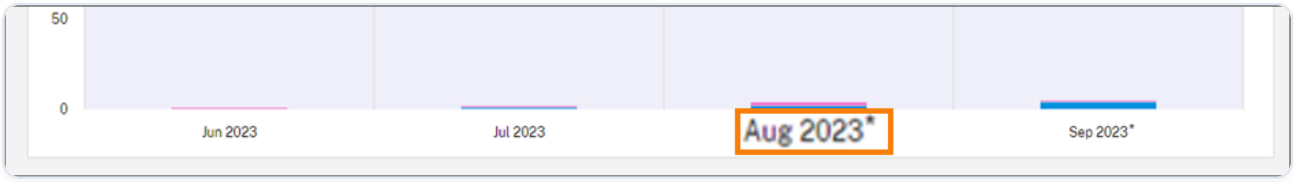


将鼠标指向图表上的某个时间间隔会显示以下信息：

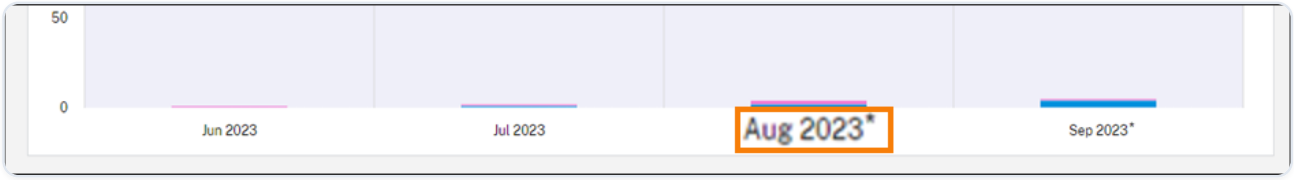
- **总许可证数：** 您为所有权利的云服务购买的许可证总数。
- **先前分配：** 上个月分配的许可证数量。例如，用户在 7 月首次访问云服务并获得许可证。此许可证在 7 月份计为“新分配”。在 8 月份，此许可证计为“先前分配”。
- **新分配：** 每个月分配的新许可证数量。例如，用户在 7 月首次访问云服务并获得许可证。此许可证在 7 月份计为“新分配”。

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

启用域截断的时间间隔用星号标记。



启用域截断的时间间隔用星号标记。



并发用户的趋势

对于并发用户许可证，“**使用趋势**”部分会显示以下信息：

- **总许可证：** 您购买的并发许可证总数。
- **峰值使用许可证：** 您选择的日期范围内分配的许可证最大数量。默认情况下，Citrix Cloud 会显示当前日历年中每个月的峰值使用情况。要深入查看每月或每小时的峰值使用情况，请从下拉菜单中选择要查看的日历月或日。

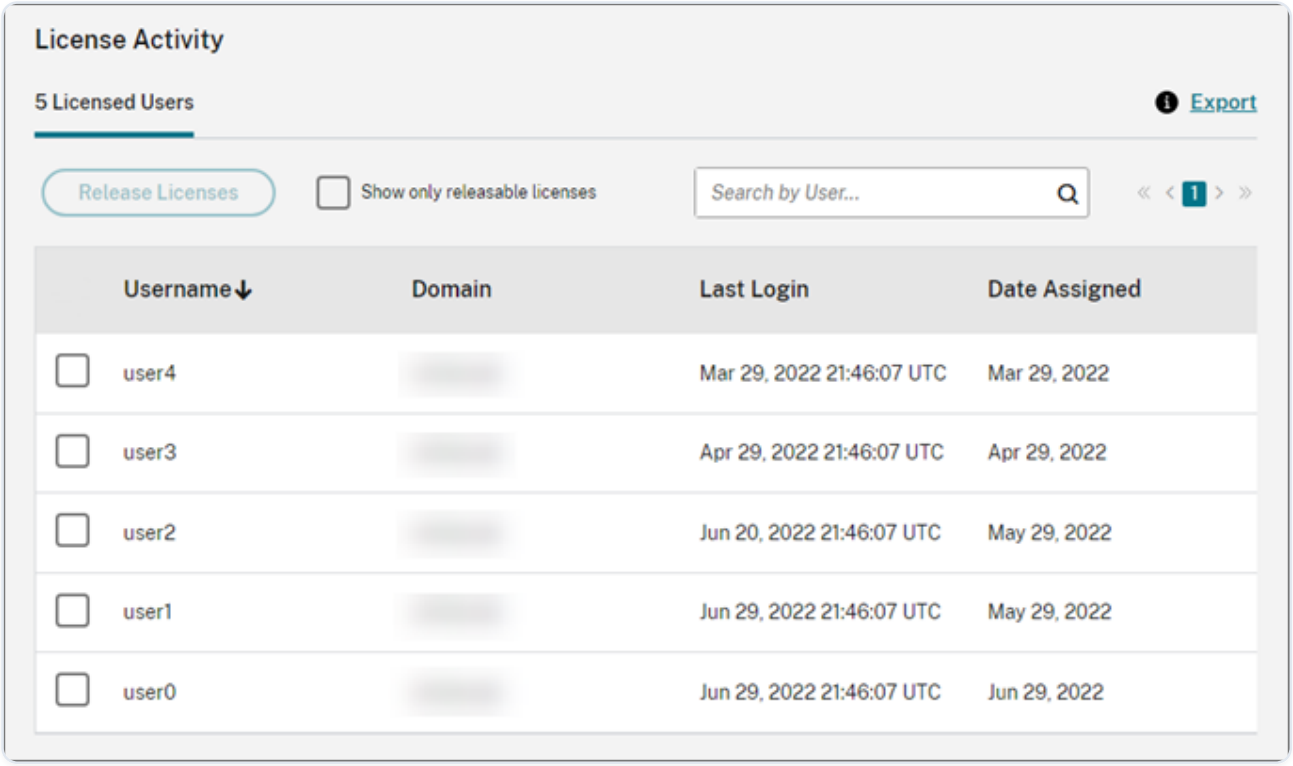
  如果您选择的日期范围尚未结束，Citrix Cloud 会显示最新时间间隔的当前峰值使用情况。例如，如果您深入查看仍在进行中的日历日，则会显示截至当前时刻每小时的最大许可证数量。如果最大许可证数量在下一个五分钟计数间隔增加，Citrix Cloud 会更新当前小时的峰值使用情况。

指向图表上的某个时间间隔，会显示该时间间隔内的总许可证数和峰值使用许可证数。

用户和设备的许可证活动

对于用户/设备许可证，**许可证活动**部分会显示已分配许可证的单个用户列表，以及向用户分配许可证的日期。此部分不适用于并发许可证。

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



您还可以筛选列表，仅显示符合释放条件的许可证。请参阅本文中的释放已分配许可证。

释放用户/设备许可证

释放符合条件的用户/设备许可证因服务订阅类型而异。

- **年度服务订阅：** 如果您有年度订阅，则可以释放过去 30 天内未启动应用程序或桌面的用户的许可证。您可以批量或单独释放多个许可证。
- **每月服务订阅：** 如果您有每月订阅，则可以在每个月的第一天释放许可证，无论不活动期如何。

分配许可证后，分配期为 90 天，并建立与服务的连接。如果用户或设备在 90 天内未启动应用程序或桌面，则这些许可证被视为未使用许可证，Citrix Cloud 会在 90 天后将其释放。此过程是自动化的，无需管理员执行任何操作。

在分配期（90 天）之后，管理员仅允许在以下情况下手动释放许可证：

- 用户不再与公司关联。
- 用户正在长期休假。

管理员只能在设备停止服务时释放设备的许可证。

注意：

- 建议遵循自动释放许可证的流程。但是，如果管理员打算在 90 天期限之前释放许可证（除了上述原因），这可能会违反 Citrix EULA。在执行此操作之前，请联系 Citrix。

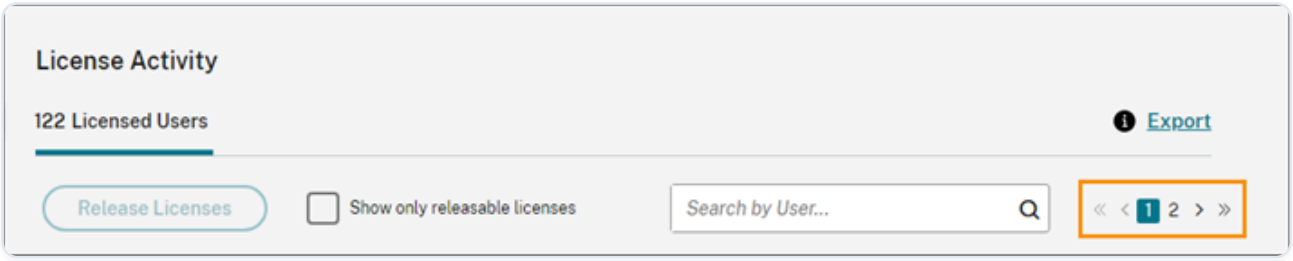
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 管理员可以通过 UI 手动释放单个许可证。或者，管理员可以选择使用云许可 API 释放许可证。有关详细信息，请参阅管理 Citrix 云许可的 API。

查找符合条件的许可证

如果用户或设备在 30 天内未启动应用程序或桌面，Citrix Cloud 会将许可证置于可释放状态。可释放的许可证在“许可用户”或“许可设备”列表中显示为深灰色复选框，可供选择。不可释放的许可证显示为浅灰色复选框，表示无法选择该许可证。

“**许可证活动**”部分中显示的列表一次最多显示 100 个已分配的许可证。如果您的许可证超过 100 个，请使用页面控件浏览列表。



要快速找到符合条件的许可证，请在“**释放许可证**”按钮旁边选择“**仅显示可释放的许可证**”。此操作会隐藏尚未符合释放条件的已分配许可证。

选择符合条件的许可证

选中每个许可证旁边的深灰色复选框以选择它进行释放。当您选择许可证时，“**释放许可证**”按钮将变为活动状态。

您可以逐一选择所有可释放的许可证，然后单击“**释放许可证**”。

释放已分配的许可证

1. 如果需要，单击 **显示可释放的许可证** 以仅显示允许释放许可证的用户。
2. 选择要管理的用户，然后单击 **释放许可证**。
3. 检查您已选择的用户，然后单击 **释放许可证**。

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

释放并发用户许可证

当用户注销或断开会话时，并发用户许可证会自动释放。您无需手动释放这些许可证。

监控 Endpoint Management 的许可证和活动使用情况

许可证分配

通常，用户在首次使用云服务时会获得许可证分配。对于 Endpoint Management，当用户注册设备时会分配许可证。设备注册后，会定期向 Citrix Cloud 报告。Citrix Cloud 随后使用此“签入脉冲”来计算每月使用情况，并帮助管理员了解用户最新的服务使用情况。

首次使用是指用户首次注册设备，或设备首次出现“签入脉冲”时。

许可证按用户分配。因此，如果两个用户注册并使用同一设备，则会分配两个许可证。

许可摘要和详细信息

许可证和使用情况摘要视图(/en-us/citrix-cloud/media/lic-usage-summary-view-cem.png)

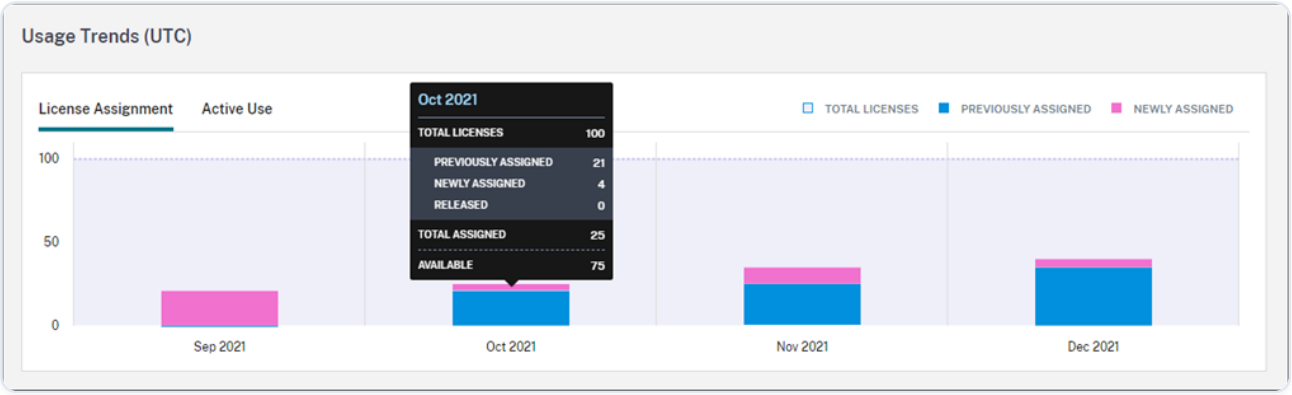
许可摘要提供适用于每个受支持服务的以下信息的概览：

- 已分配的购买许可证总数的百分比。当百分比接近 100% 时，颜色从绿色变为黄色。如果百分比超过 100%，则百分比变为红色。
- 已分配许可证与购买许可证的比率以及剩余可用许可证的数量。
- 按月和按日计算的活动使用情况统计信息：
  - 每月活动使用量是指过去 30 天内使用过服务的唯一用户数。
  - 每日活动使用量是指过去 24 小时内使用过服务的唯一用户数。
- 云服务订阅到期前的剩余时间。如果订阅在未来 90 天内到期，则会显示警告消息。

使用趋势

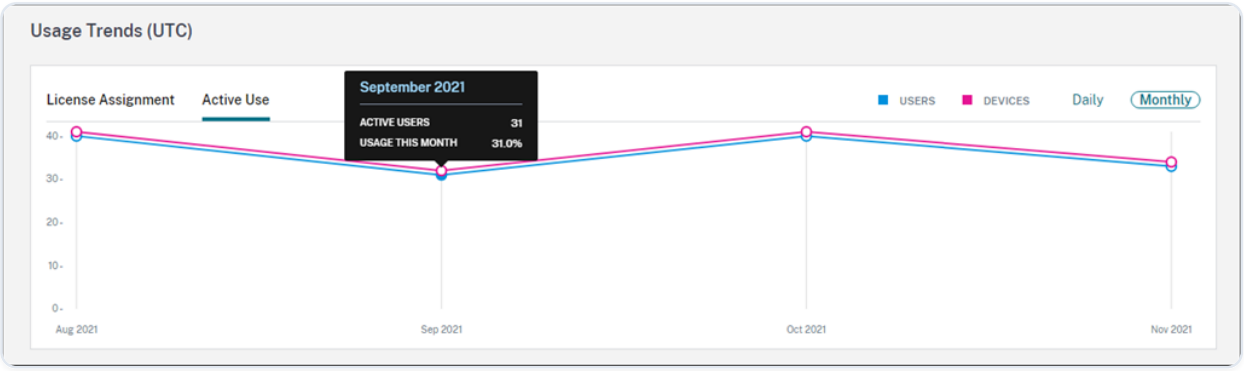
要详细查看您的许可证，请单击 **查看使用详情**。然后，您可以查看使用趋势以及正在使用云服务许可证的单个用户和设备的详细信息。

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



此详细信息显示以下信息：

- **总许可证数：** 您为所有授权的云服务购买的许可证总数。
- **先前已分配：** 每个月初已分配的云服务许可证。例如，如果用户在 7 月份分配了一个许可证，则该分配将计入 8 月份的“先前已分配”数量中。
- **新分配：** 每个月分配的云服务许可证数量。例如，首次在 7 月份访问云服务的用户会获得一个许可证。此许可证将计入 7 月份的“新分配”数量中。
- **活跃使用：** 分别显示上一个日历月和日历年的每日和每月活跃使用趋势。

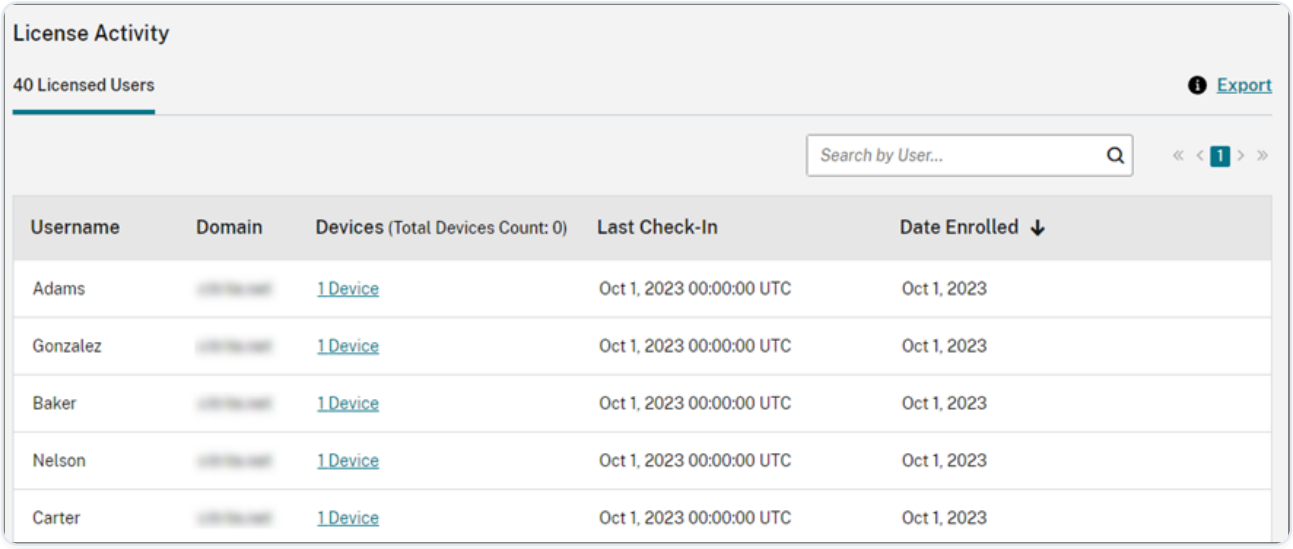


许可证活动

许可证活动部分显示包含以下信息的列表：

- 已分配许可证的单个使用者
- 许可证分配日期
- 每个用户的注册设备数量和上次签入日期

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



查看注册设备

要查看特定用户的注册设备数量，请单击**设备**列中的链接。

授权用户，“设备”链接已突出显示(/en-us/citrix-cloud/media/lic-usage-licensed-devices-select-cem.png)

Citrix Cloud 显示该用户的已注册设备列表以及每个设备的上次签入日期。

授权用户菜单，包含已注册设备详细信息(/en-us/citrix-cloud/media/lic-usage-licensed-devices-cem.png)

自动释放分配的许可证

Citrix Cloud 会自动释放过去 30 天内满足**所有**以下条件的用户许可证：

- 用户未注册新设备。
- 用户拥有现有设备，但该设备未向 Citrix Cloud 签入。

无需执行其他操作即可释放符合条件的许可证。

释放符合条件的许可证后，用户可以通过注册设备获取另一个许可证。

监控 Gateway 服务带宽使用情况

本文介绍了 Gateway 服务与 Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops™ 服务）和 Citrix® StoreFront Cloud 结合使用时的带宽使用情况。随 Virtual Apps Essentials 服务提供的 Gateway 服务的带宽消耗不会显示在 Citrix Cloud 管理控制台的“**许可**”页面上。

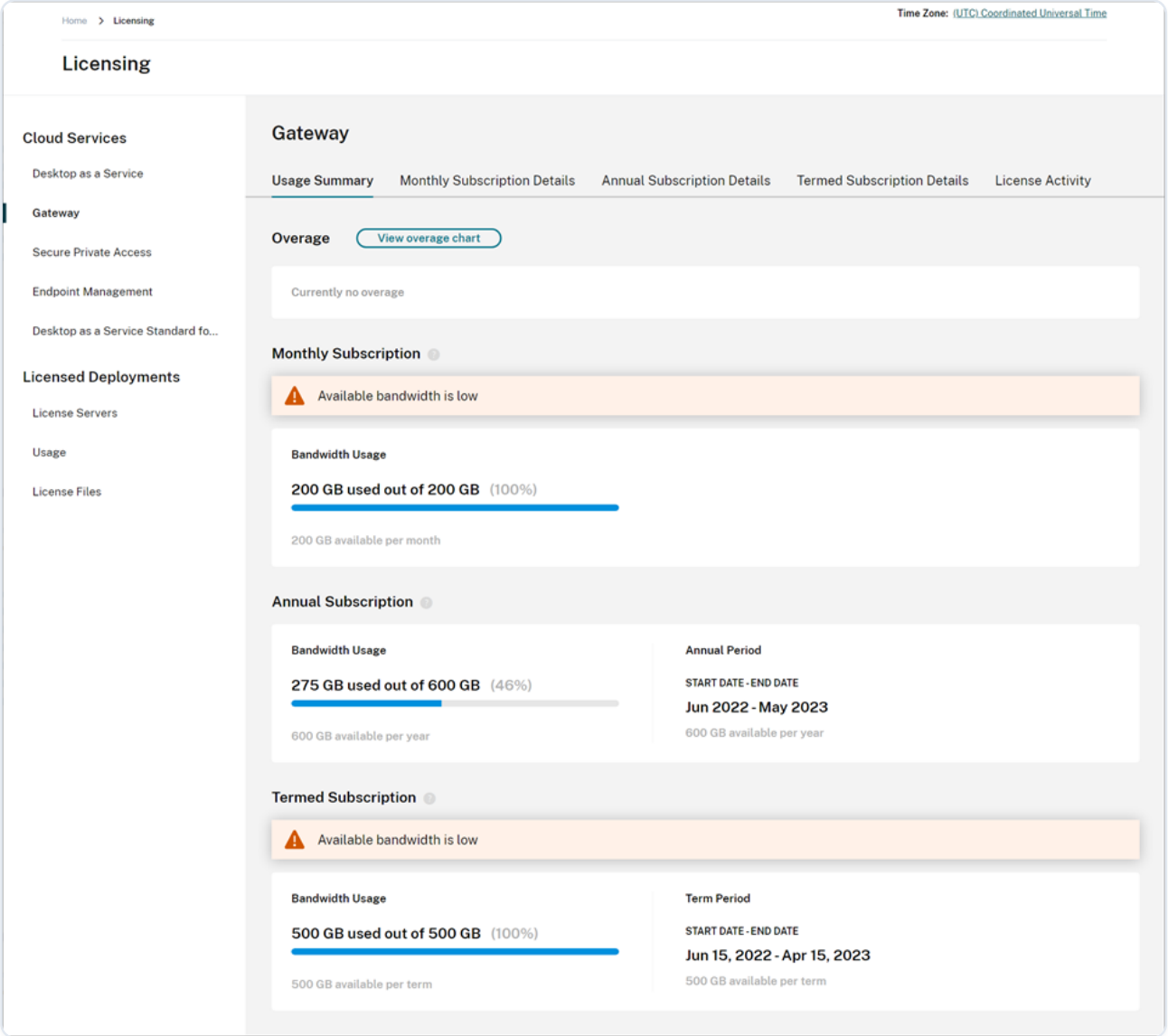
© 1997–2026 Citrix Systems, Inc. All rights reserved.

注意：

Gateway 服务的许可可帮助您了解与使用虚拟应用程序和桌面相关的带宽使用情况。Citrix® 不会在您的环境中强制执行带宽使用配额。如果您超出带宽配额，Citrix 不会干扰生产工作负载或服务的运行。如果 Citrix 更改 Gateway 服务和带宽使用策略的执行方式，Citrix 会在这些更改生效前通知您。

使用情况摘要

使用情况摘要可让您一目了然地查看每个 Gateway 服务订阅的带宽使用情况以及所有订阅（月度、年度和定期）的总超额使用量。



Citrix Cloud™ 显示每种订阅类型的总带宽量和已消耗的带宽量。

根据订阅类型，Citrix Cloud 还会显示订阅的计费周期：

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

- 月度订阅：Citrix Cloud 不显示当前计费周期。对于这些订阅，计费周期从每月的第一个日开始，到该月的最后一天结束。
- 年度订阅：Citrix Cloud 显示计费周期的开始日期和结束日期。对于这些订阅，计费周期为一年。
- 定期订阅：Citrix Cloud 显示计费周期的开始日期和结束日期。对于这些订阅，计费周期是购买订阅的时长。例如，如果购买了为期三年的定期订阅，则计费周期的开始日期和结束日期与该三年间隔相对应。

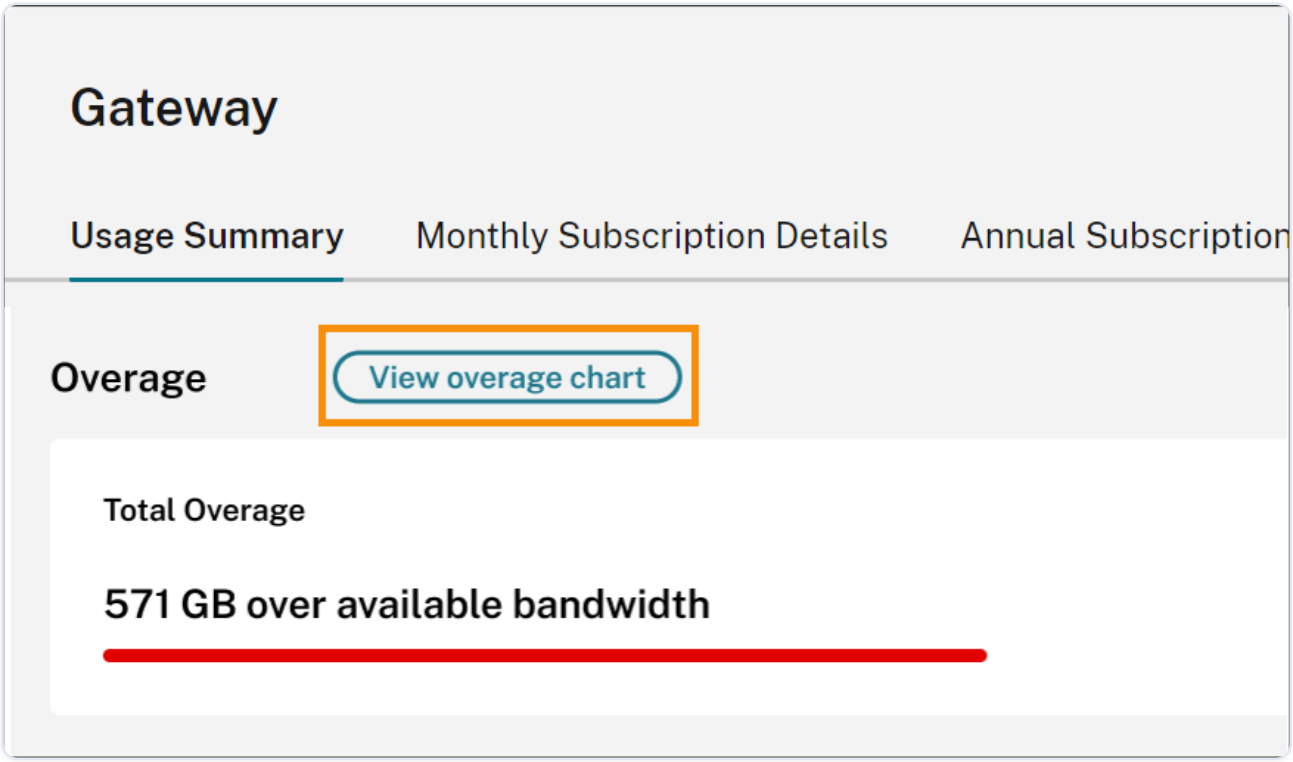
如果订阅在 90 天内到期，则会显示该订阅的警告消息。

超额使用

Citrix Cloud 会每月计算所有订阅的超额使用量。如果您消耗的带宽超出购买量，Citrix Cloud 会将超出部分显示为超额使用量。

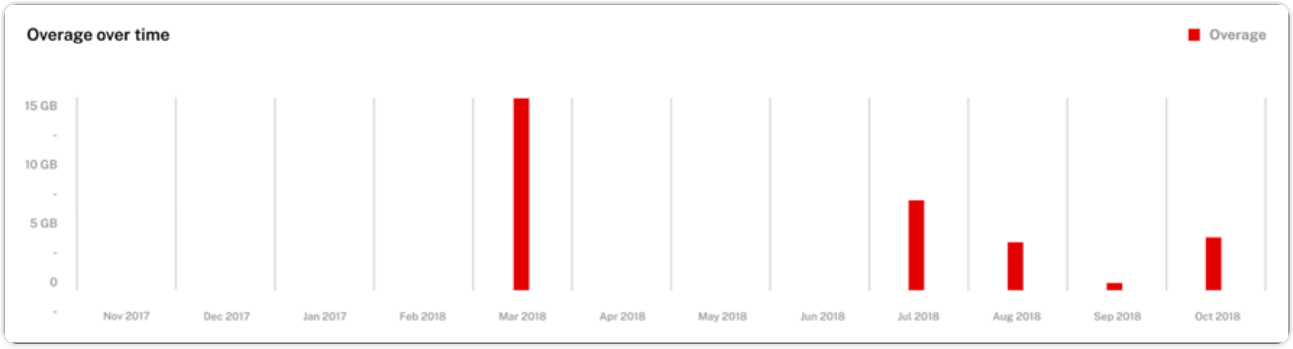
如果您有多个订阅，Citrix Cloud 会首先根据结束日期最早的订阅来衡量您的带宽使用情况。如果您用尽了该订阅中的带宽配额，Citrix Cloud 会根据下一个结束日期最早的订阅来衡量您的带宽使用情况。如果您用尽了所有订阅中的带宽配额，Citrix Cloud 会将超出部分显示为超额使用量。

“使用情况摘要”页面显示当月的总超额使用量。要查看随时间变化的超额使用量，请选择 **查看超额使用量图表**。



Citrix Cloud 会显示您过去 12 个月的总超额使用量图表。

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



当月的超额使用量不会结转到下个月。下个月开始时，总超额使用量将重置为零。

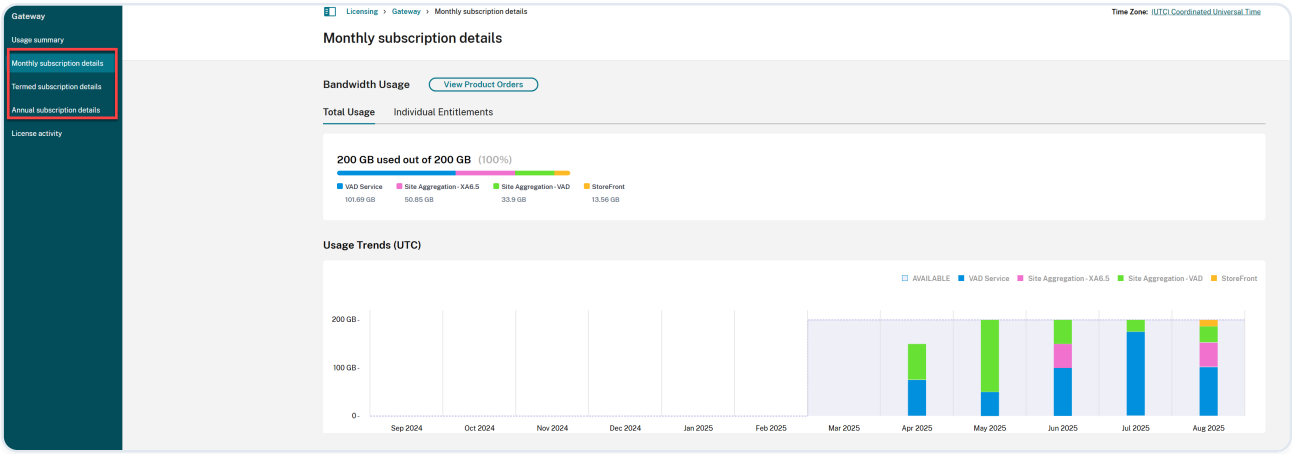
未使用的带宽

Citrix Cloud 会在下一个计费周期自动重置订阅的带宽使用情况。如果您在给定订阅期内没有用完所有带宽，Citrix Cloud 不会将任何未使用的带宽结转到下一个计费周期。

例如，如果您的月度订阅包含 150 GB 的总带宽，并且您在给定月份使用了 100 GB 的带宽，Citrix Cloud 会将使用量重置为零，并在下个月初将 150 GB 显示为您的总带宽量。未使用的带宽不会添加到您的总带宽配额中。

使用详情

要查看订阅的详细信息，请选择控制台顶部附近的月度、年度或定期订阅详细信息选项卡。



对于每种订阅类型，“详细信息”选项卡会显示以下信息：

- **总使用量：** 在给定类型的所有订阅中，已消耗的带宽量占可用总带宽量的比例。对于月度订阅，总使用量显示为当月。对于年度和定期订阅，总使用量是您所有年度或定期订阅的累计值。
- **个人权利：** 给定类型的每个订阅所消耗的带宽总量。例如，如果您有多个年度订阅，此选项卡会单独显示每个年度订阅的使用情况明细。

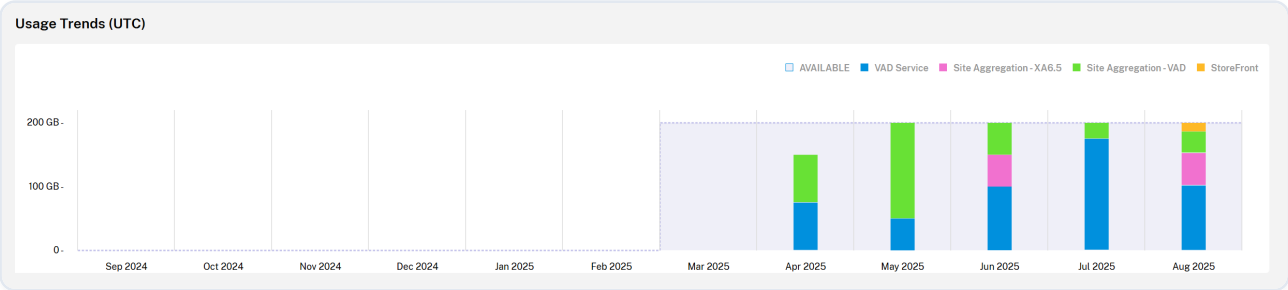
消耗的带宽量根据通过 Citrix DaaS (**VAD Service**) 的访问或通过使用 StoreFront Cloud 中的站点聚合 的本地 Virtual Apps and Desktops 部署进行细分。

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

使用趋势

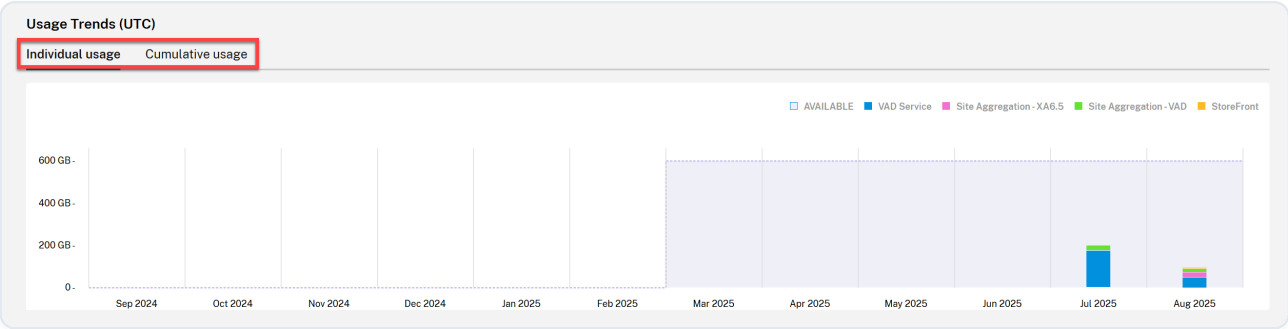
使用趋势部分显示了过去 12 个月的使用情况细分。

对于按月订阅，将显示每个使用月份的使用情况。

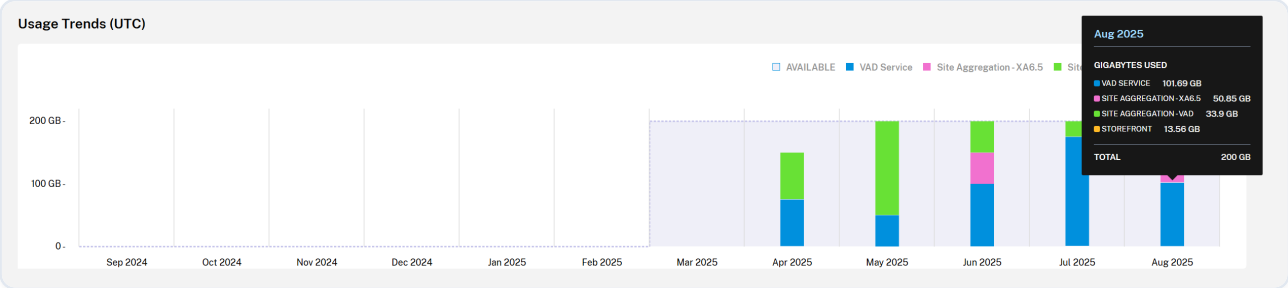


对于按年和定期订阅，本部分包括以下视图：

- **个人使用情况：** 当前计费周期内每个月的带宽使用情况。
- **累计使用情况：** 当前计费周期内每个月累计的带宽使用情况。



对于所有订阅类型，将鼠标指向“使用趋势”图表中的条形图会显示该时间点的带宽使用情况，并按访问类型细分。



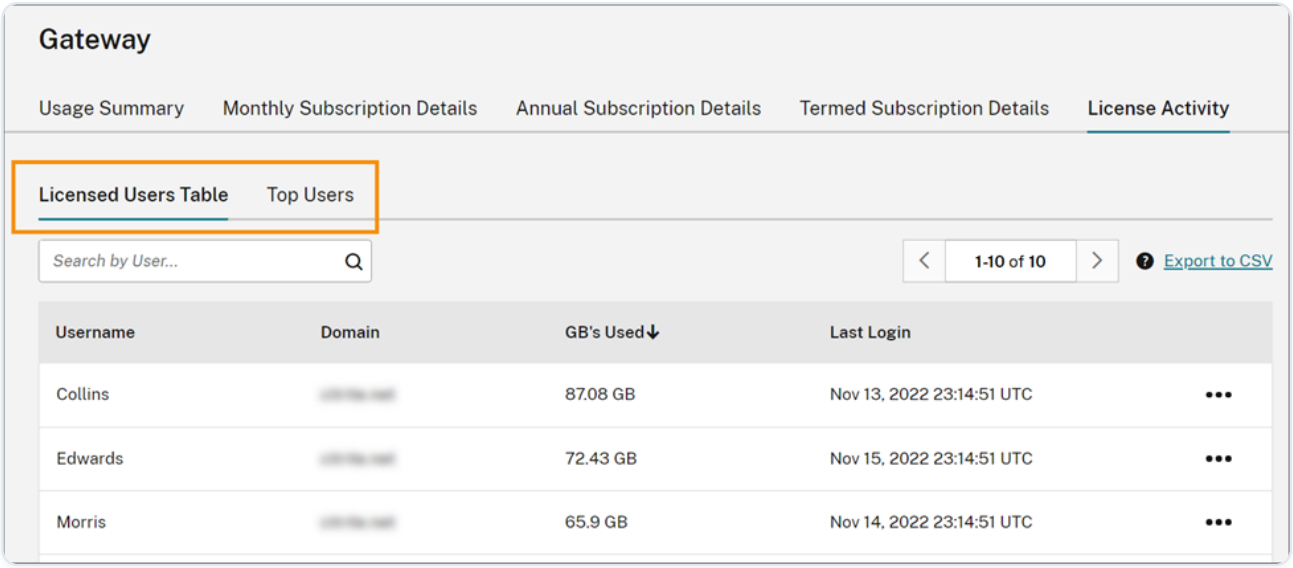
许可证活动

许可证活动部分提供了以下信息的视图：

- **许可用户：** 显示已分配许可证的个人用户列表。此列表包括每个用户所属的域、过去 30 天内使用的带宽量以及用户上次使用需要带宽的服务时的日期。

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

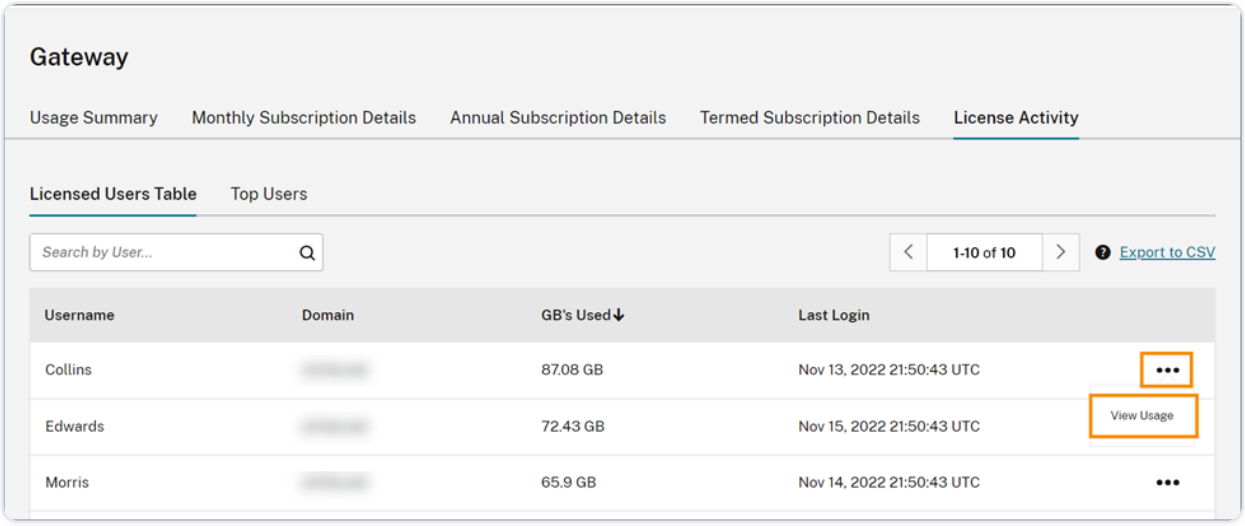
- **热门用户：** 显示根据带宽使用情况排名前 10 位的用户列表。此列表包括每个用户在过去 30 天内根据访问类型（Citrix DaaS™ 或通过站点聚合的本地 Virtual Apps and Desktops）的使用情况细分。



即使特定用户不再使用许可证，Citrix Cloud 也会显示该用户在过去 30 天内的带宽使用情况。当 Gateway 服务订阅过期时，Citrix Cloud 仍会显示单个用户在 30 天内消耗的带宽。

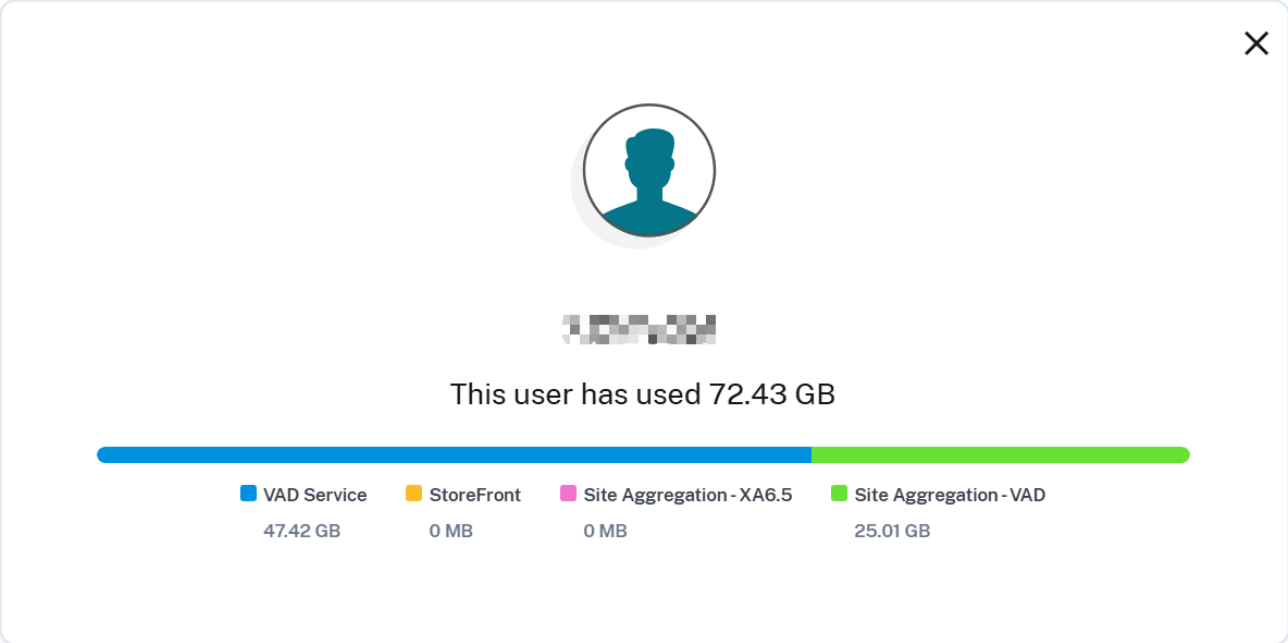
查看特定用户的用法详细信息

1. 选择 **许可用户表** 并在列表中找到要查看的用户。
2. 从页面最右侧的省略号菜单中选择 **查看用法**。



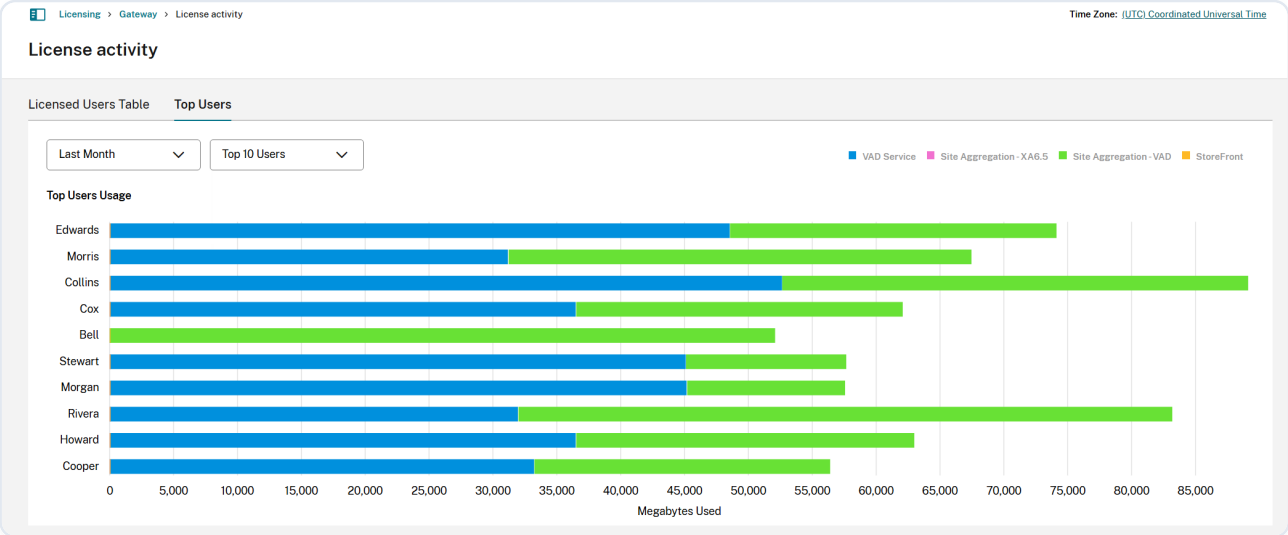
Citrix Cloud 显示按访问类型细分的用户带宽。

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



查看热门用户的用法详细信息

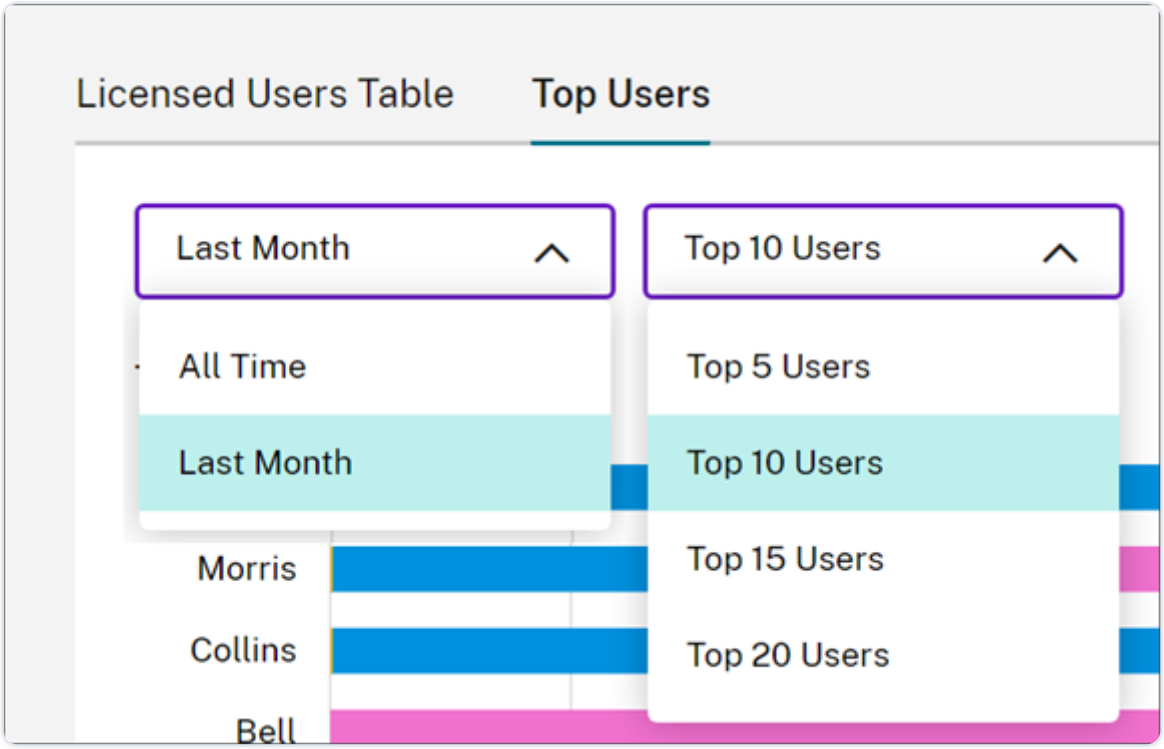
选择 **热门用户**。



Citrix Cloud 显示热门用户的带宽使用情况图表，按访问类型细分。

默认情况下，**热门用户** 图表显示在过去 30 天内使用带宽最多的前 10 位用户。您可以更改此视图以显示前五名、前 15 名或前 20 名用户。您还可以将持续时间更改为 **所有时间**，这将显示订阅生命周期内的热门用户。要更改此视图，请从每个菜单中选择一个选项。

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



监控 Secure Private Access 的许可证和使用情况

许可证分配

当唯一用户首次启动 Web 和 SaaS 应用程序或 TCP 和 UDP 应用程序时，将分配许可证。

许可摘要

许可摘要视图(/en-us/citrix-cloud/media/lic-usage-summary-view-swa.png)

许可摘要显示以下信息：

- 已分配的已购买许可证总数的百分比。
  - 当百分比接近 100% 时，颜色从绿色变为黄色。如果百分比超过 100%，则颜色变为红色。
- 已分配许可证与已购买许可证的比率以及可用于分配的许可证数量。
- 每月和每日的活跃使用情况统计信息：
  - 月活跃使用量是指在过去 30 天内使用过该服务的唯一用户数量。
  - 日活跃使用量是指在过去 24 小时内使用过该服务的唯一用户数量。
- 所有订阅的总带宽中已消耗的带宽量。
- 云服务订阅到期前的剩余时间。如果订阅将在未来 90 天内到期，则会出现警告消息。

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

已使用的许可证和带宽

在 Secure Private Access Advanced 订阅中，每位用户每月可获得 5 GB 带宽（每位用户每年 60 GB）。在 Secure Private Access Standard 订阅中，每位用户每月可获得 1 GB 带宽（每位用户每年 12 GB）。此带宽将根据许可证数量和订阅期进行汇总。

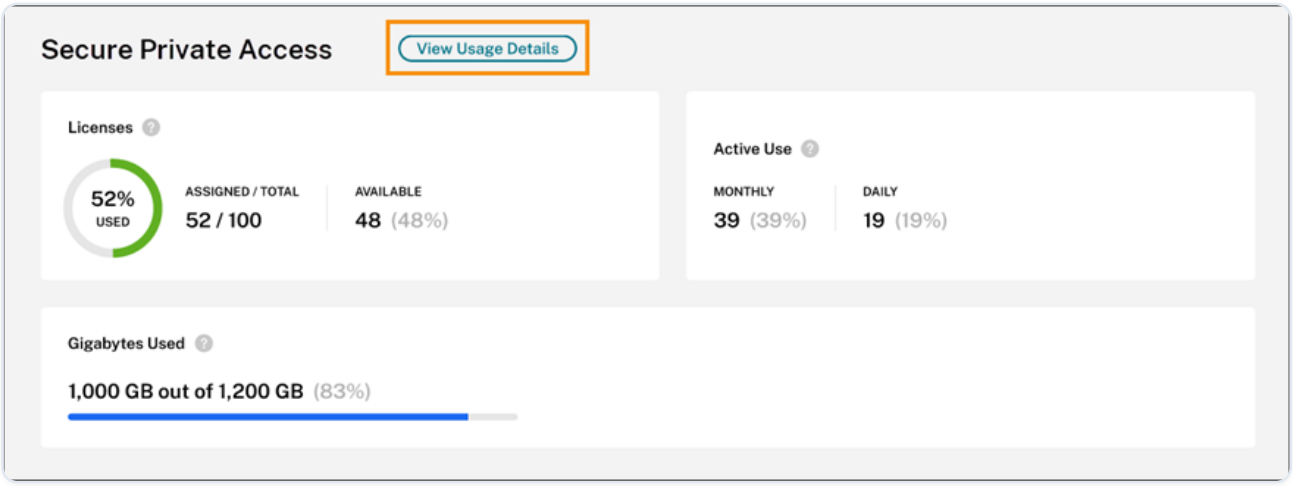
例如，如果您购买 100 个三年期许可证，则总带宽为 18000 GB（三年内每年 6000 GB）。此带宽在三年内分配给所有获得许可的用户。如果您购买更多订阅，Citrix Cloud™ 会显示所有订阅的许可证总数和总带宽。

如果在订阅期内未用完所有带宽，Citrix Cloud 在续订时不会结转任何未使用的带宽。当您使用的带宽超出购买量且订阅到期时，续订订阅后可用带宽量仍为零。

对于具有重叠期限的多个订阅，每个订阅到期时，与该订阅关联的带宽将从许可中移除。例如，如果您 购买了两个订阅，Citrix Cloud 会显示这两个订阅的总许可证和总带宽。当第一个订阅到期时，Citrix Cloud 仅显示与未到期订阅关联的带宽。

使用趋势

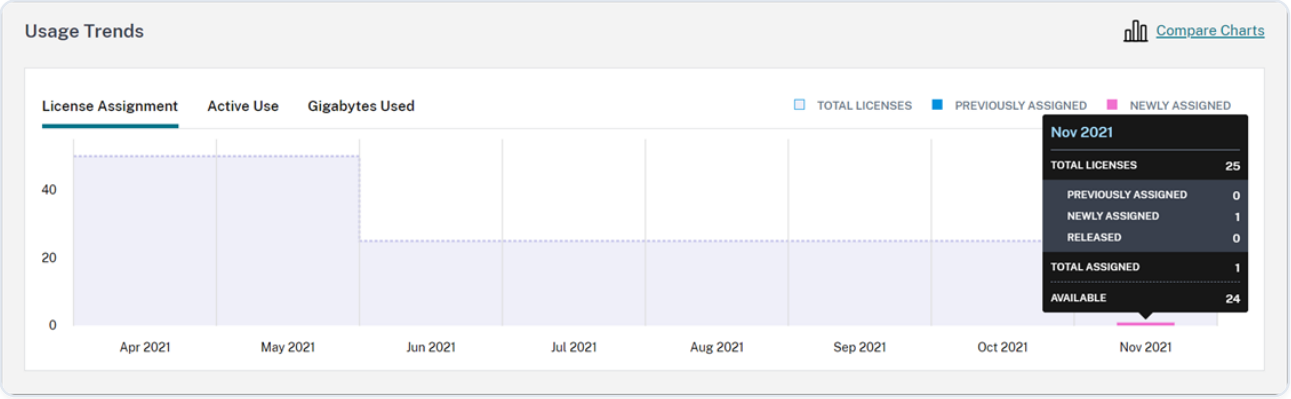
要查看带宽使用情况和许可证的详细信息，请单击 **View Usage Details**。



Citrix Cloud 根据用户有权访问的应用程序类型显示带宽消耗明细。

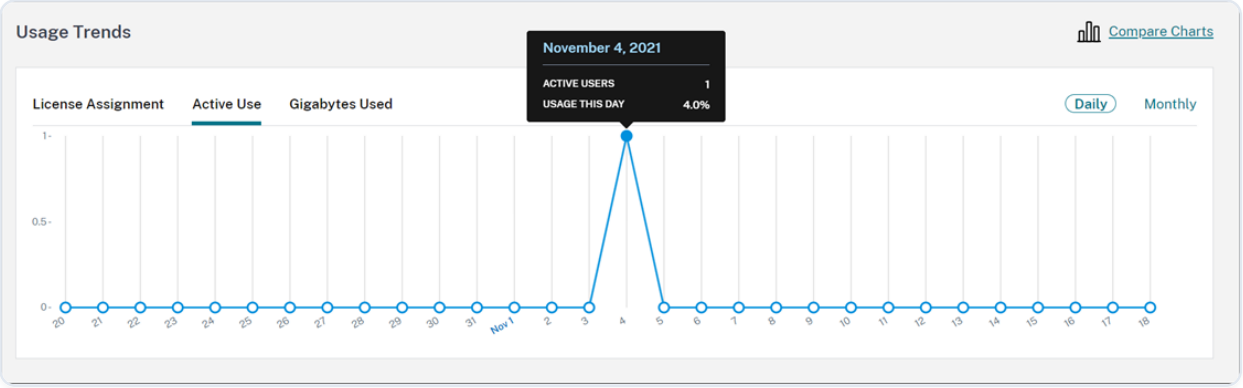
您还可以查看使用趋势明细以及正在消耗云服务许可证和带宽的单个用户。

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

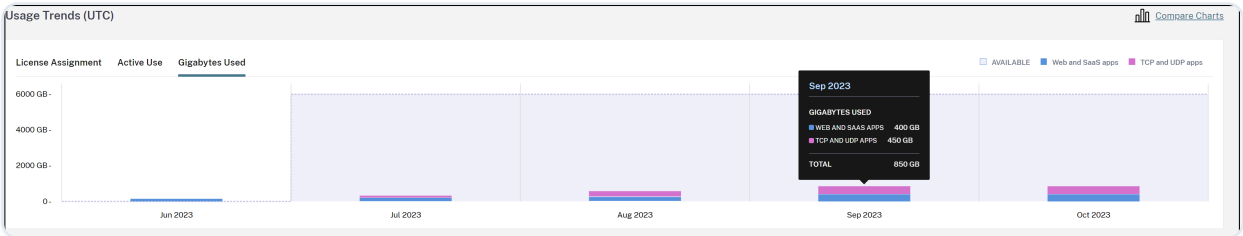


在 **Usage Trends** 下，此明细显示以下信息：

- 在 **License Assignment** 选项卡上：
  - **Total Licenses**（许可证总数）：您为所有授权的云服务购买的许可证总数。
  - **Previously Assigned**（先前已分配）：每个月初已分配的云服务许可证。例如，如果用户在 7 月分配了一个许可证，Citrix Cloud 会将该分配计入 8 月的“先前已分配”数量中。
  - **新分配：** 每个月分配的许可证数量。例如，当您在七月首次访问云服务并被分配许可证时，Citrix Cloud 会将该许可证计入七月的新分配数量中。
- 在**活跃使用**选项卡上：分别显示上一个日历月和日历年的每日和每月活跃使用趋势。



- 在**已用千兆字节**选项卡上：显示已用带宽量占可用总带宽量的比例。它显示按用户使用情况和按应用程序信息，例如 Web 和 SaaS 应用程序以及 TCP 和 UDP 应用程序。



要比较许可证分配、活跃使用和带宽使用趋势，请选择**比较图表**。

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

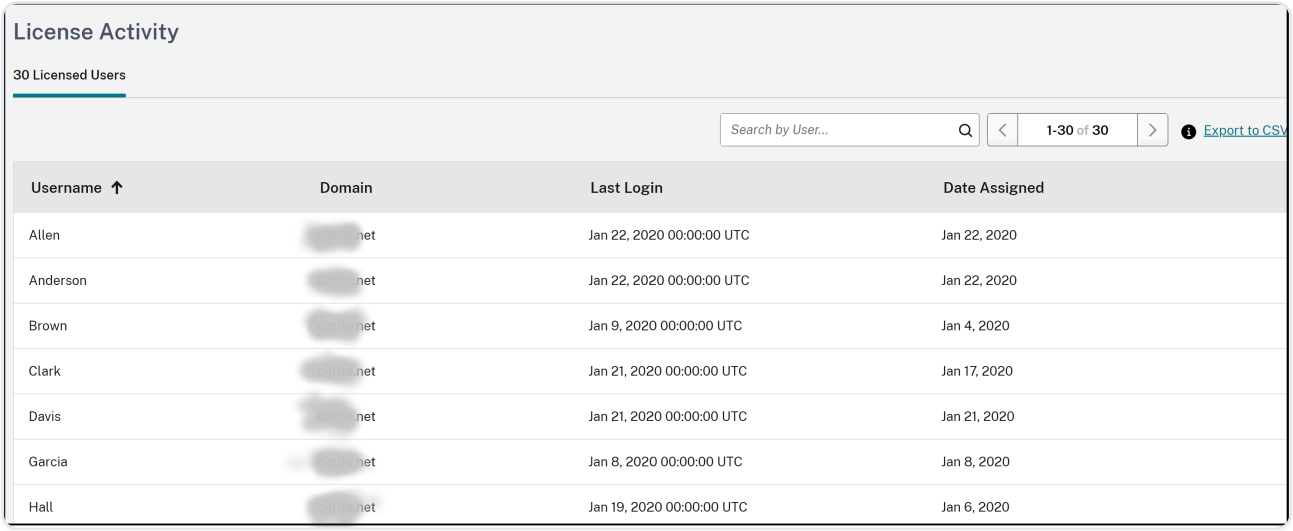
注意：

使用趋势在当前订阅期内是累积的。当您续订订阅时，使用趋势将在新订阅期开始时重置。

许可证活动

许可证活动部分还显示以下信息：

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



- 已分配许可证的单个用户列表。
- 用户所属的域。
- 用户上次使用服务的日期。
- 许可证分配给用户的日期。

释放已分配的许可证

如果您在过去 30 天内未使用该服务，Citrix Cloud 会自动释放许可证。Citrix 管理员无需执行任何操作即可释放许可证。

当许可证被释放时，剩余许可证的数量会增加，而已分配许可证的数量会相应减少。许可证释放后，您可以通过登录并使用云服务来获取另一个许可证。

监控适用于 Citrix DaaS™ 的 Citrix 管理的 Azure 资源消耗

当您购买 Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops™ 服务）的授权时，您还可以购买 Citrix Azure 消费基金，允许您在 Citrix 管理的 Azure 订阅中使用资源。您可以使用这些资源向用户交付应用程序和桌面，同时使用本地 VDA。

当您购买 Citrix Azure 消费基金时，您可以通过以下方法之一支付消费：

- 即用即付：对于您在给定月份使用的 Citrix 管理的 Azure 资源，Citrix 会在下个月向您收费。Citrix Cloud™ 会将您的使用量显示为超额。
- 预付费消费：您可以按月或按年（定期）预付消费。对于超出预付费消费的任何使用量，Citrix Cloud 会将其显示为超额。对于给定月份的任何超额，Citrix 会在下个月向您收费。

每个消费单位价值 1.00 美元。Citrix Cloud 中的许可控制台可帮助您跟踪所使用的单位。

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

要估算消费成本，请使用 Citrix 管理的 Azure 消费计算器。要估算 Citrix DaaS Standard for Azure（以前称为 Citrix Virtual Apps and Desktops Standard for Azure）的消费和许可成本，请使用 许可和消费计算器。

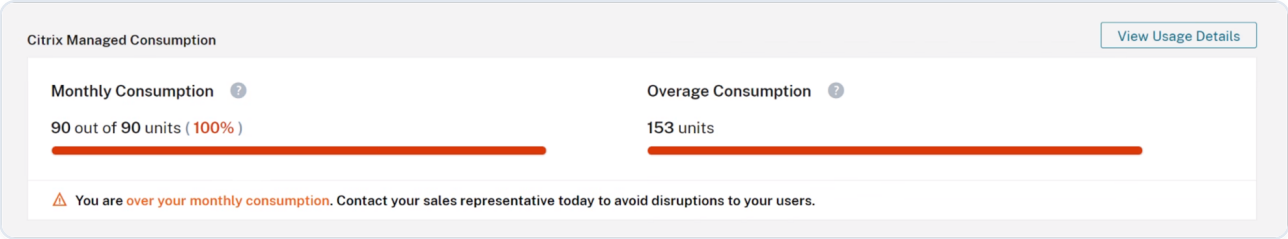
支持的产品

消费监控适用于以下 Citrix DaaS 版本：

- Citrix DaaS Advanced (以前称为 虚拟应用高级版)
- Citrix DaaS Premium (以前称为 虚拟应用尊享版)
- Citrix DaaS 高级增强版 (以前称为 Virtual Apps and Desktops 高级版)
- Citrix DaaS 高级版 (以前称为 Virtual Apps and Desktops 高级版)
- Citrix DaaS Azure 标准版（以前称为 Virtual Apps and Desktops Azure 标准版）

消费摘要

“Citrix 托管消费”部分显示了您在“消费基金”中使用的单位摘要。



月度消费显示了您在当月已使用的消费单位数量，该数量来自您购买的月度消费基金单位总数。月度消费每月重置。未使用的消费单位不会结转到下个月。

期限消费显示了您已使用的消费单位数量，该数量来自您购买的期限消费基金单位总数。与月度消费单位一样，未使用的期限消费单位不会结转到下一年。

超额消费显示了您使用的消费单位数量，该数量超出了您的 Azure 消费基金中的单位数量。如果您以即用即付方式使用 Citrix 托管 Azure 资源，则您的消费默认显示为超额。

超额如何衡量

如果您以即用即付方式使用 Azure 消费基金，Citrix Cloud 会将您当月使用的消费单位数量显示为超额。

如果您预付了按月或按年计算的消费，Citrix Cloud 会显示您在当月或当年使用的月度或期限消费单位数量。如果您消费的单位数量超出您购买的数量，Citrix Cloud 会将超出单位显示为超额。

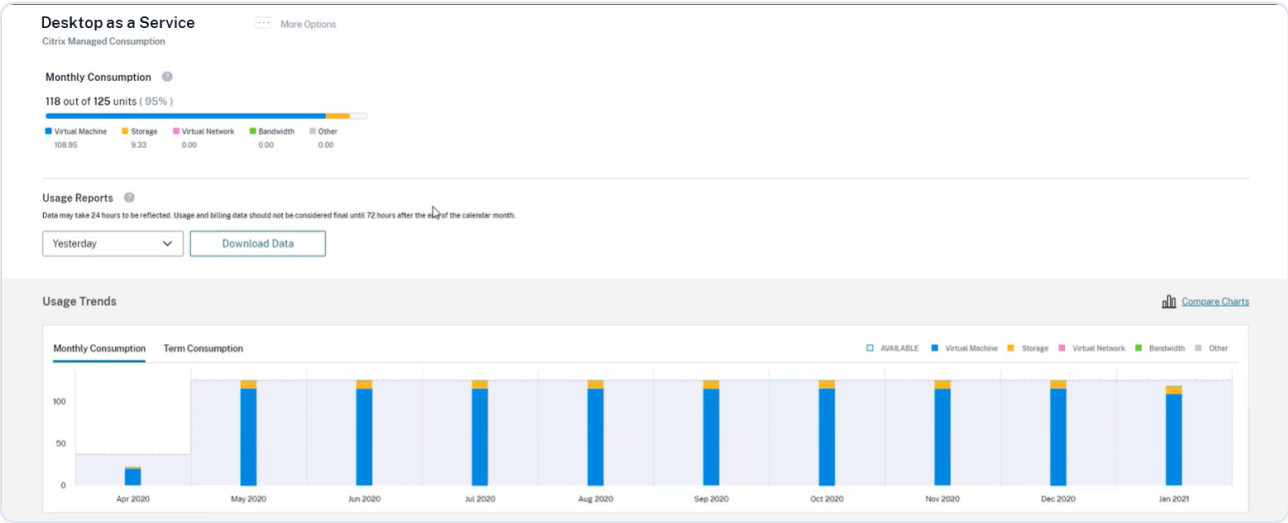
© 1997–2026 Citrix Systems, Inc. All rights reserved.

如果您同时预付了月度和年度消费，Citrix Cloud 会首先根据您购买的月度单位衡量您的消费。这些单位用完后，Citrix Cloud 会根据您的年度单位衡量您的消费。这些单位用完后，Citrix Cloud 会将您消费的任何超出单位显示为超额。

如果您购买了额外消费单位，并且您的帐户存在现有超额，则新的消费单位不会应用于超额。新的消费单位仅应用于购买这些单位之后发生的用量。

消费详情

要查看消费单位的详细信息，请单击摘要最右侧的**查看使用详情**。详细信息页面显示了您的消费和使用趋势的细分。



使用报告

您可以将指定时间间隔的使用信息下载为 CSV 文件。单击**下载数据**可生成 CSV 文件并下载到本地计算机。

数据可能需要长达 72 小时才能在一天或一个月结束后反映所有使用情况。

CSV 文件包含以下部分：

- 报告摘要，显示报告日期范围之前和之后可用的消耗单位、总使用费以及待处理的超额费用。

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

Data may take 24 hours to be reflected. Usage and billing data should not be considered final until 72 hours after the end of the calendar month.		
Org ID	51938754	
Report Date	12/3/2021	
Date Start	11/1/2021	
Date End	11/30/2021	
Report Summary		
	Credits	Debits
Monthly Consumption Units Available before 11/01/2021	$0	
Termed Consumption Units Available before 11/01/2021	$0	
Trial Consumption Units Available before 11/01/2021	$0	
Total Usage to Charge		$851.96
Expired Consumption Commitment		$0.00
Total	$0.00	$851.96
Monthly Consumption Units Available after 11/30/2021	$0	
Termed Consumption Units Available after 11/30/2021	$0	
Trial Consumption Units Available after 11/30/2021	$0	
Pending Overage by 11/30/2021	$0.00	

- 每日摘要，显示报告日期范围内的每天总使用费、剩余的每月和定期资金以及超额费用。

Daily Summary				
Date	Total Usage	Remaining Monthly Funds	Remaining Termed Funds	Overage Amount
11/1/2021	$28.40	$0	$0	$0
11/2/2021	$28.40	$0	$0	$0
11/3/2021	$28.40	$0	$0	$0
11/4/2021	$28.40	$0	$0	$0
11/5/2021	$28.39	$0	$0	$0
11/6/2021	$28.39	$0	$0	$0
11/7/2021	$28.40	$0	$0	$0
11/8/2021	$28.40	$0	$0	$0

- 报告日期范围内的每天 Azure VM、网络连接、Azure 存储和带宽的计量使用情况。

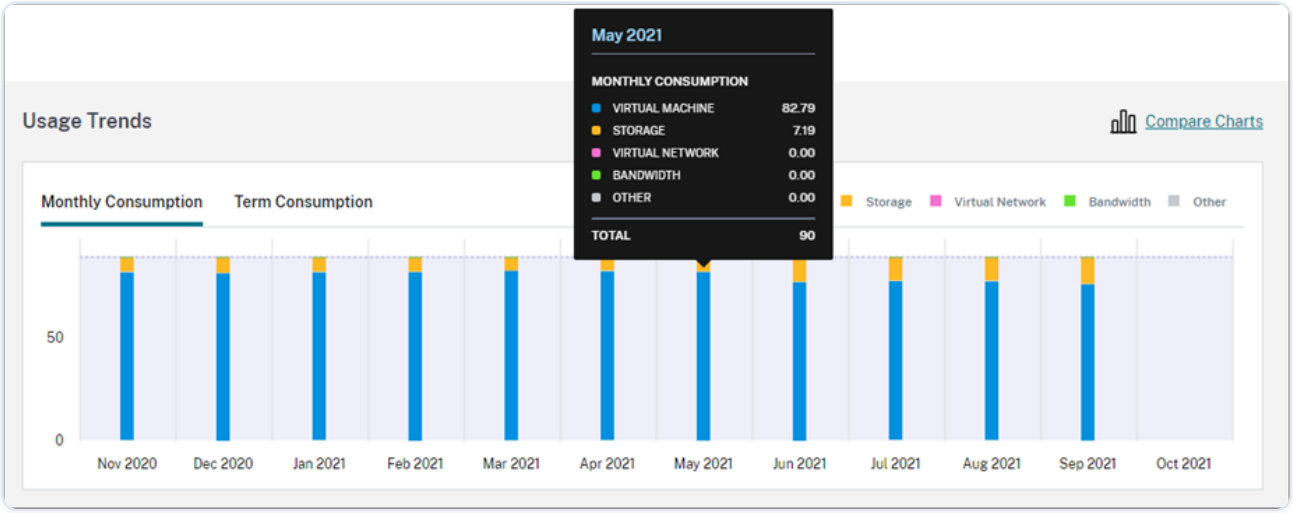
Date	Citrix Meter Name	Citrix Meter Description	Catalog Id	Catalog Name	Citrix Meter Region	Citrix Meter Category	Citrix Meter Sub Category	Citrix Meter Unit	Quantity	SRP	Total	Total Charged
11/1/2021	Bandwidth - Data Transfer Out - Zone 1		07f1d01f-9ffb-472e-93ab-ae2d7393202a	Win-11-MS-2	None	Bandwidth		10 GB	0.0000444	$1.13	$0.00	$0.00
11/1/2021	Bandwidth - Data Transfer Out - Zone 1		f061eeac-2507-459c-ab99-71fde94b318e	Finance desktops	None	Bandwidth		10 GB	0.0000018	$1.13	$0.00	$0.00
11/1/2021	Bandwidth - Data Transfer Out - Zone 1		N/A	N/A	None	Bandwidth		10 GB	0.0064263	$1.13	$0.01	$0.01
11/1/2021	Bandwidth - Data Transfer Out - Zone 1		cb7516c0-33e7-485a-9eb0-d84b7f2e9c5a	Windows-11-MultiSession	None	Bandwidth		10 GB	0.0000137	$1.13	$0.00	$0.00
11/1/2021	Bandwidth - Data Transfer Out - Zone 1		6dbcda61-cdf6-4135-86e0-76e2f5f45204	Windows-11-SingleSession	None	Bandwidth		10 GB	0.0000015	$1.13	$0.00	$0.00
11/1/2021	Bandwidth - Data Transfer Out - Zone 1		dfb04e0a-b08f-4f0a-af95-fff7cdd6cd83	AVD Desktops	None	Bandwidth		10 GB	0.0000073	$1.13	$0.00	$0.00
11/1/2021	Bandwidth - Data Transfer Out - Zone 1		e86cee4e-1930-4d87-b2e5-3b189bb3e6e3	Win-11-SS-22	None	Bandwidth		10 GB	0.0000334	$1.13	$0.00	$0.00
11/1/2021	Virtual Machines Dv3/DSv3 Series - D2 v3/D2s v3 - US East		f061eeac-2507-459c-ab99-71fde94b318e	Finance desktops	US East	VirtualMachine		10 Hours	2.4	$1.25	$3.00	$3.00
11/1/2021	Virtual Machines Dv3/DSv3 Series - D2 v3/D2s v3 - US East		e86cee4e-1930-4d87-b2e5-3b189bb3e6e3	Win-11-SS-22	US East	VirtualMachine		10 Hours	2.4	$1.25	$3.00	$3.00
11/1/2021	Virtual Machines Dv3/DSv3 Series - D2 v3/D2s v3 - US East		dfb04e0a-b08f-4f0a-af95-fff7cdd6cd83	AVD Desktops	US East	VirtualMachine		10 Hours	2.4	$1.25	$3.00	$3.00
11/1/2021	Virtual Machines Dv3/DSv3 Series - D2 v3/D2s v3 - US East		cb7516c0-33e7-485a-9eb0-d84b7f2e9c5a	Windows-11-MultiSession	US East	VirtualMachine		10 Hours	2.4	$1.25	$3.00	$3.00
11/1/2021	Virtual Machines Dv3/DSv3 Series - D2 v3/D2s v3 - US East		07f1d01f-9ffb-472e-93ab-ae2d7393202a	Win-11-MS-2	US East	VirtualMachine		10 Hours	2.4	$1.25	$3.00	$3.00
11/1/2021	Virtual Machines Dv3/DSv3 Series - D2 v3/D2s v3 - US East		6dbcda61-cdf6-4135-86e0-76e2f5f45204	Windows-11-SingleSession	US East	VirtualMachine		10 Hours	2.4	$1.25	$3.00	$3.00
11/1/2021	Virtual Network Peering - Ingress		N/A	N/A	None	VirtualNetwork		100 GB	0.00016714	$1.30	$0.00	$0.00
11/1/2021	Virtual Network Peering - Egress		f061eeac-2507-459c-ab99-71fde94b318e	Finance desktops	None	VirtualNetwork		100 GB	0.00000034	$1.30	$0.00	$0.00
11/1/2021	Virtual Network Peering - Ingress		cb7516c0-33e7-485a-9eb0-d84b7f2e9c5a	Windows-11-MultiSession	None	VirtualNetwork		100 GB	0.00000323	$1.30	$0.00	$0.00
11/1/2021	Virtual Network Peering - Ingress		07f1d01f-9ffb-472e-93ab-ae2d7393202a	Win-11-MS-2	None	VirtualNetwork		100 GB	0.00000422	$1.30	$0.00	$0.00
11/1/2021	Virtual Network Peering - Egress		07f1d01f-9ffb-472e-93ab-ae2d7393202a	Win-11-MS-2	None	VirtualNetwork		100 GB	0.00000165	$1.30	$0.00	$0.00
11/1/2021	Virtual Network Peering - Ingress		dfb04e0a-b08f-4f0a-af95-fff7cdd6cd83	AVD Desktops	None	VirtualNetwork		100 GB	0.00000307	$1.30	$0.00	$0.00
11/1/2021	Virtual Network Peering - Egress		e86cee4e-1930-4d87-b2e5-3b189bb3e6e3	Win-11-SS-22	None	VirtualNetwork		100 GB	0.00000129	$1.30	$0.00	$0.00
11/1/2021	Virtual Network Peering - Egress		cb7516c0-33e7-485a-9eb0-d84b7f2e9c5a	Windows-11-MultiSession	None	VirtualNetwork		100 GB	0.00000148	$1.30	$0.00	$0.00
11/1/2021	Virtual Network Peering - Egress		dfb04e0a-b08f-4f0a-af95-fff7cdd6cd83	AVD Desktops	None	VirtualNetwork		100 GB	0.00000115	$1.30	$0.00	$0.00
11/1/2021	Virtual Network Peering - Ingress		e86cee4e-1930-4d87-b2e5-3b189bb3e6e3	Win-11-SS-22	None	VirtualNetwork		100 GB	0.00000342	$1.30	$0.00	$0.00
11/1/2021	Virtual Network Peering - Egress		N/A	N/A	None	VirtualNetwork		100 GB	0.00012714	$1.30	$0.00	$0.00
11/1/2021	Virtual Network Peering - Egress		6dbcda61-cdf6-4135-86e0-76e2f5f45204	Windows-11-SingleSession	None	VirtualNetwork		100 GB	0.00000121	$1.30	$0.00	$0.00
11/1/2021	Virtual Network Peering - Ingress		6dbcda61-cdf6-4135-86e0-76e2f5f45204	Windows-11-SingleSession	None	VirtualNetwork		100 GB	0.00000323	$1.30	$0.00	$0.00
11/1/2021	Virtual Network Peering - Ingress		f061eeac-2507-459c-ab99-71fde94b318e	Finance desktops	None	VirtualNetwork		100 GB	0.00000094	$1.30	$0.00	$0.00
11/1/2021	General Block Blob - Read Operations		N/A	N/A	None	Storage		100000000	0.00000016	$4.68	$0.00	$0.00
11/1/2021	Standard HDD Managed Disks - S10 - Disks - US East		N/A	N/A	US East	Storage		1 /Month	0.400032	$7.64	$3.06	$3.06
11/1/2021	Standard HDD Managed Disks - S10 - Disks - US East		dfb04e0a-b08f-4f0a-af95-fff7cdd6cd83	AVD Desktops	US East	Storage		1 /Month	0.033336	$7.64	$0.25	$0.25
11/1/2021	Standard HDD Managed Disks - S10 - Disks - US East		6dbcda61-cdf6-4135-86e0-76e2f5f45204	Windows-11-SingleSession	US East	Storage		1 /Month	0.100008	$7.64	$0.76	$0.76
11/1/2021	Virtual Machines Av2 Series - A2 v2 - US East		N/A	N/A	US East	VirtualMachine		100 Hours	0.48	$11.83	$5.68	$5.68
11/1/2021	Premium SSD Managed Disks - P10 - Disks - US East		f061eeac-2507-459c-ab99-71fde94b318e	Finance desktops	US East	Storage		1 /Month	0.033336	$19.22	$0.64	$0.64
11/2/2021	Bandwidth - Data Transfer Out - Zone 1		07f1d01f-9ffb-472e-93ab-ae2d7393202a	Win-11-MS-2	None	Bandwidth		10 GB	0.0000235	$1.13	$0.00	$0.00

使用趋势和消耗活动

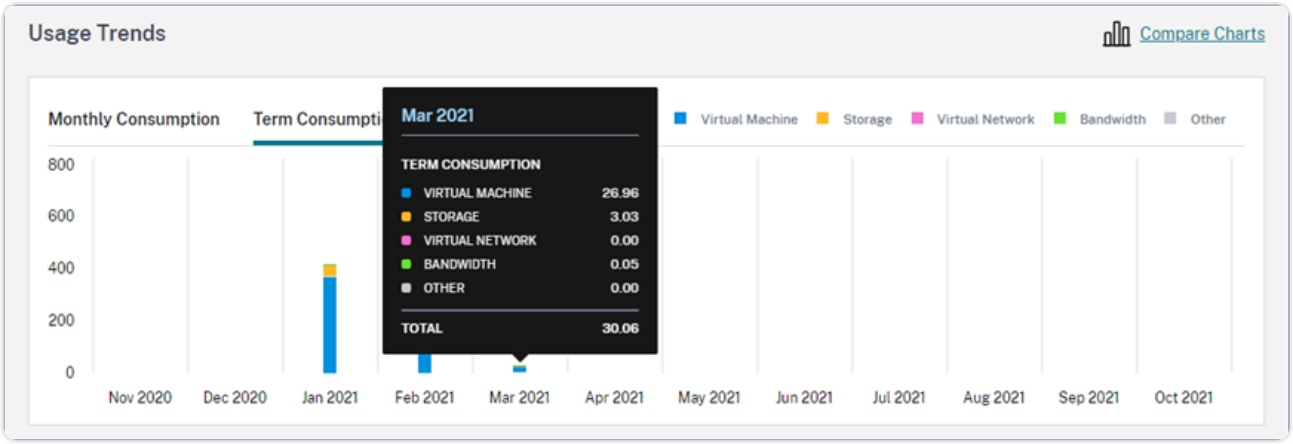
使用趋势部分显示您已使用的 Citrix Managed Azure 资源的图表。将鼠标指向图表上的条形图会显示您当月消耗的资源数量，包括虚拟机、存储、虚拟网络资源和带宽。

选择**每月消耗**以查看您过去 12 个月的每月消耗情况。

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

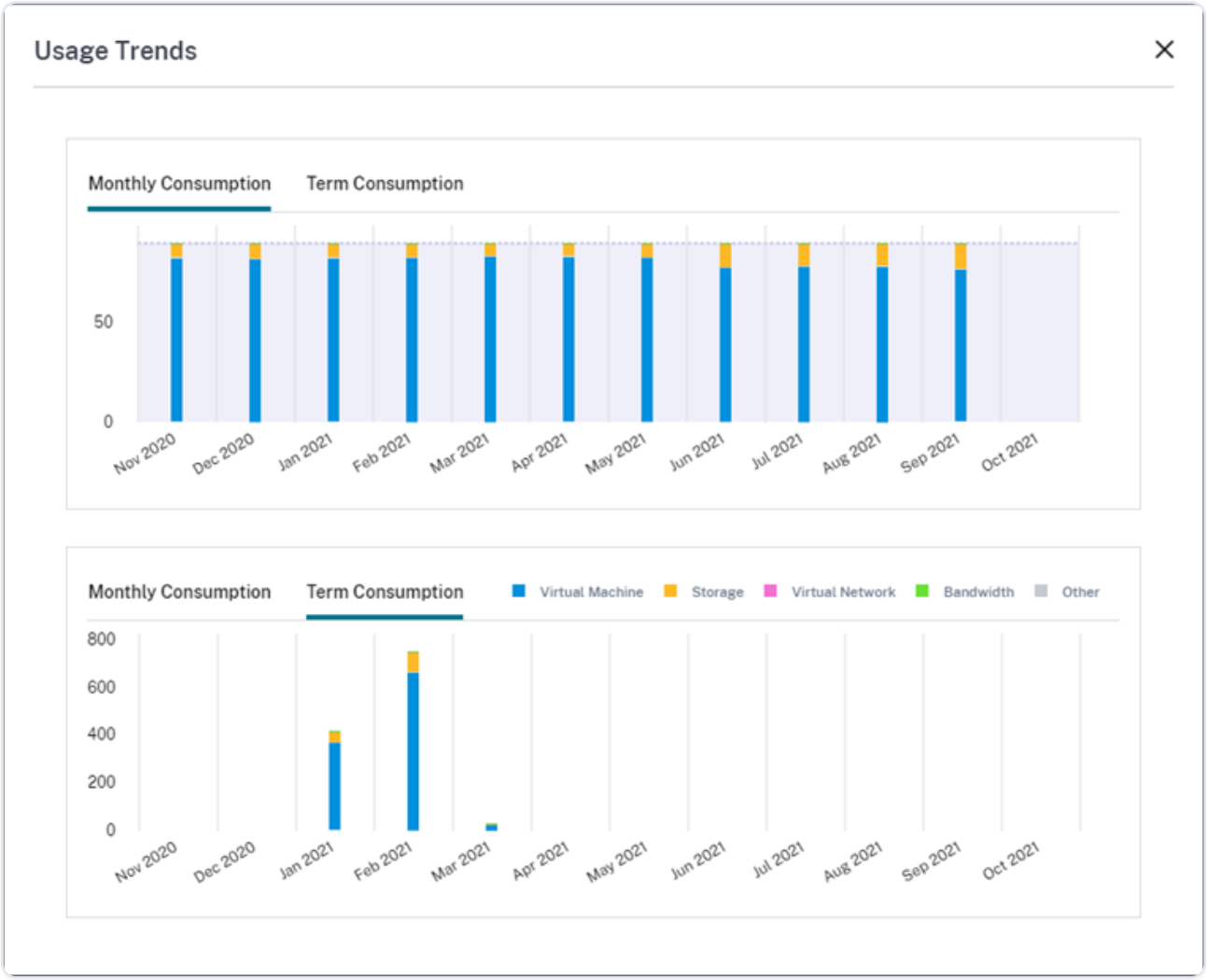


选择**定期消耗**以查看您过去一年中每个月的定期消耗情况。



如果您同时购买了每月和每年的消耗单位，请选择图表最右侧的**比较图表**，以在单个视图中查看每月和定期消耗趋势。

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



消耗活动部分还显示了您每个月的消耗单位列表。

Consumption Activity

1-12 of 23

Month	Used	Owned	Remaining	Overage
Oct 2021	0	1,200	0	0
Sep 2021	831	1,200	0	831
Aug 2021	1,375	1,200	0	1,375
Jul 2021	1,056	1,200	0	1,056

消耗活动包括以下信息：

- **已使用：** 每个月使用的单元数量。
- **已拥有：** 每个月购买的单元总数。
- **剩余：** 每个月未使用的已购买单元数量。
- **超额：** 每个月超出您购买单元数量的已消耗单元数量。

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

释放已分配的许可证

许可证分配何时符合释放条件取决于您购买的消费基金单元。

如果满足以下条件，您可以在 30 天后释放非活动许可证：

- 您未将 Citrix Managed Azure 订阅与您的服务部署配合使用。
- 您购买了年度消费单元以用于您的服务部署。

如果满足以下条件，您可以在当月释放非活动许可证，前提是没有用户或设备启动应用程序或桌面：

- 您购买了月度消费基金单元以用于您的服务部署。
- 您同时购买了月度和年度消费基金单元。

有关释放符合条件的许可证的说明，请参阅以下文章：

- 思杰 DaaS（用户/设备模型）：释放已分配的许可证
- 适用于 Azure 的 Citrix DaaS 标准版: 释放已分配的许可证

监控本地部署的许可证和使用情况

重要提示：

使用情况洞察仅适用于传统许可证文件，不适用于 许可证激活服务。

Citrix Cloud™ 中的许可部署体验包含以下功能：

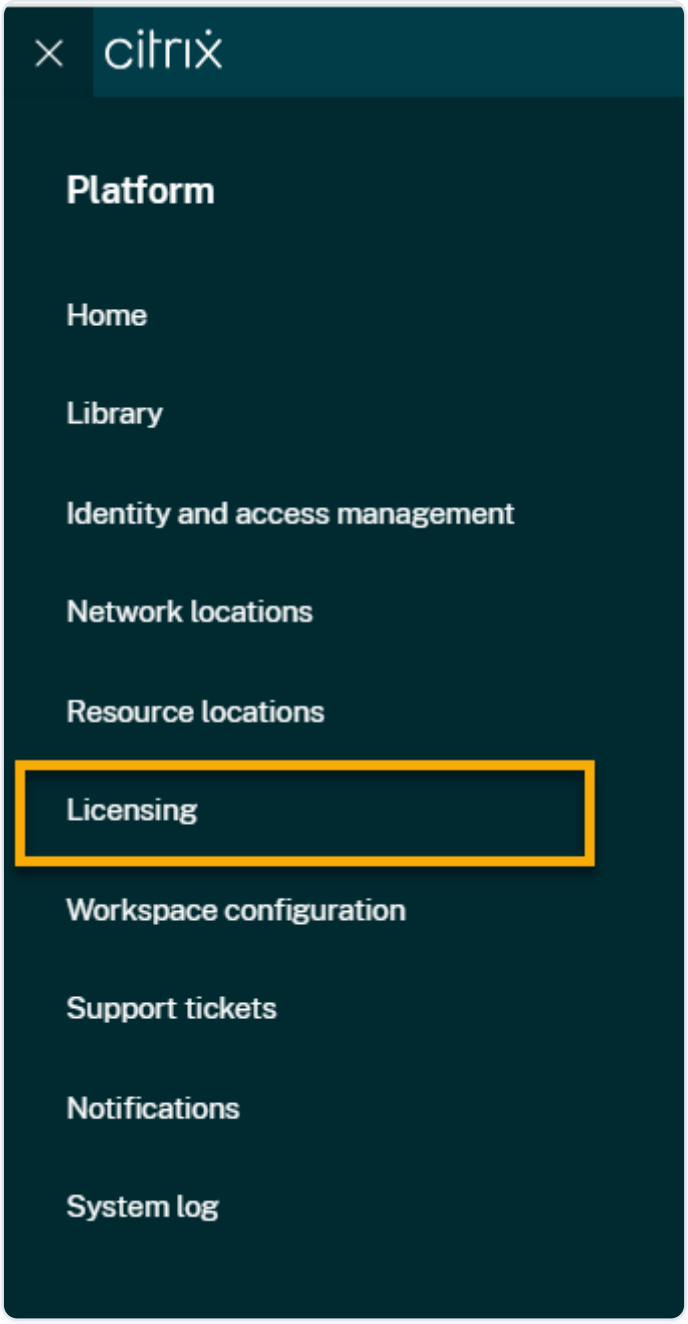
- 产品注册：将您现有的 Citrix 许可证服务器注册到 Citrix Cloud，以获取有关部署的更多使用情况洞察和报告。
- 许可证服务器状态：查看 Citrix 许可证服务器的状态，了解哪些服务器成功报告了使用情况以及它们上次向 Citrix Cloud 报告使用情况的时间。
- 使用情况洞察：查看您的 Citrix 许可证服务器上安装和使用了多少许可证，并深入了解历史许可证使用趋势。

支持的产品

Citrix 许可证服务器使用情况洞察适用于并发和用户/设备许可模型下的所有虚拟应用和桌面版本。

要查看 Citrix 许可证服务器使用情况洞察，请从控制台菜单中选择 **“许可”**，然后选择 **“许可部署”**。

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



先决条件

要使用 Citrix 许可证服务器使用情况洞察，请确保您具备以下各项：

- Citrix 许可证服务器版本 11.15.0.0 或更高版本
- Citrix Cloud 帐户
- 从 Citrix 许可证服务器到 Citrix Cloud 的网络访问

连接要求

要成功将许可证服务器注册到 Citrix Cloud，请确保以下地址可访问：

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

- `https://las.cloud.com:443`
- `https://customers.citrixworkspacesapi.net:443`
- `https://citrix.cloud.com/` （用于访问管理控制台以输入代码和查看许可证服务器状态）
- `https://trust.citrixnetworkapi.net` （用于检索代码）
- `https://trust.citrixworkspacesapi.net/` （用于确认许可证服务器已注册）
- `https://cis.citrix.com` （用于数据上传）
- `https://core-eastus-release-a.citrixworkspacesapi.net`
- `https://core.citrixworkspacesapi.net`
- `ocsp.digicert.com port 80`
- `crl3.digicert.com port 80`
- `crl4.digicert.com port 80`
- `ocsp.entrust.net port 80`
- `crl.entrust.net port 80`

连接到 Citrix Cloud

要启用 Citrix 许可证服务器使用情况洞察，请执行以下任务：

1. 使用许可管理器控制台为您的许可证服务器启用使用情况洞察。有关详细信息，请参阅许可产品文档中的共享使用情况统计信息。
2. 查看本文中连接要求所述的连接要求，并确保地址可访问。如果您将代理服务器与 Citrix 许可证服务器配合使用，请确保按照许可产品文档中步骤 5 配置代理服务器所述配置代理服务器。
3. 按照将本地产品注册到 Citrix Cloud中所述，将您的许可证服务器注册到 Citrix Cloud。

查看本地产品许可证使用情况

Citrix 许可证服务器使用情况洞察可让您全面了解整个 Citrix 环境中的许可证使用情况。您可以访问使用情况报告，这有助于您：

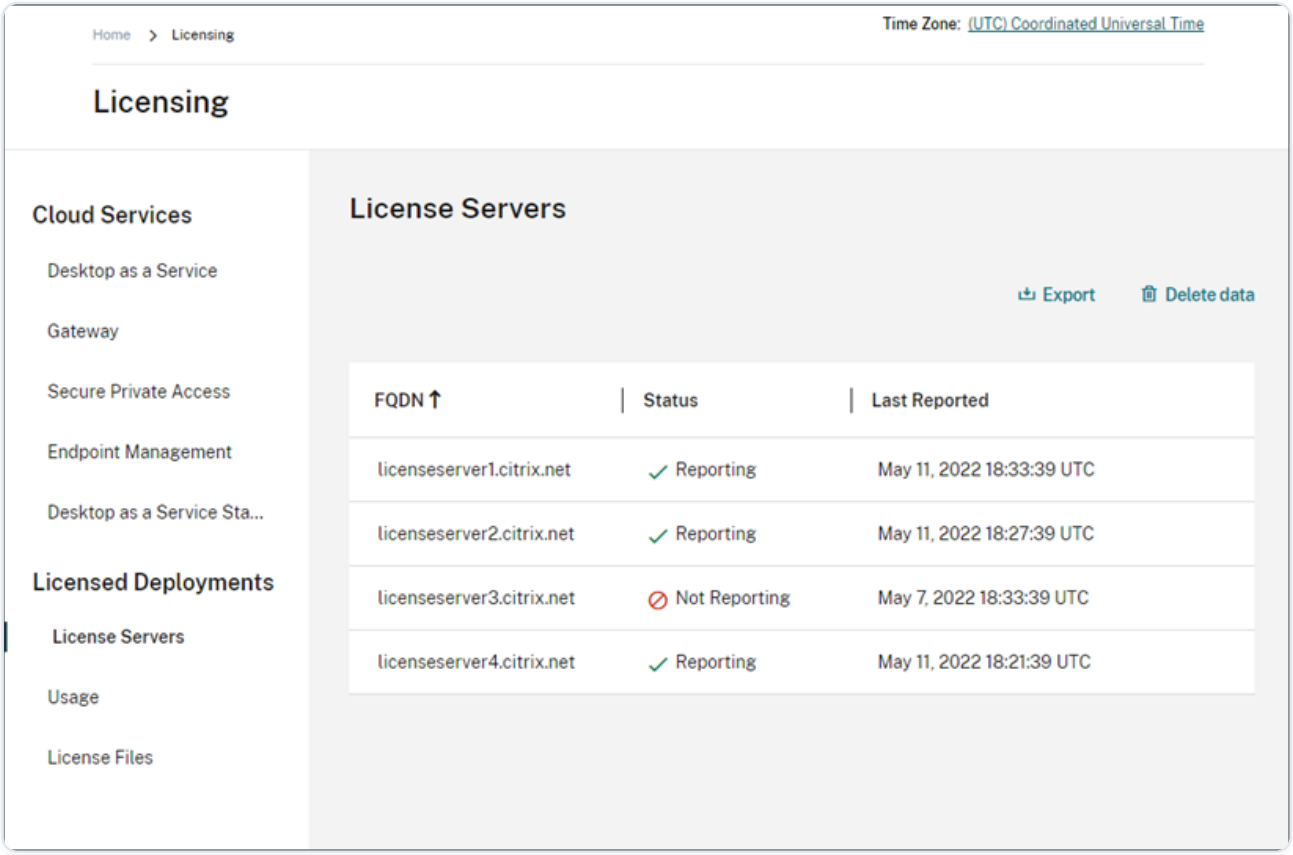
- 了解部署和注册的许可证服务器数量，以及它们是否向 Citrix Cloud 报告使用情况信息。
- 了解虚拟应用和桌面的并发和用户/设备许可证使用情况。
- 深入了解跨多个部署的并发和用户/设备许可证的聚合使用情况。
- 了解历史许可证使用情况和每月许可证使用趋势。
- 查看特定用户的上次登录时间。

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

- 比较 Citrix 许可证服务器中已安装许可证数量与正在使用的许可证数量。
- 监控许可证透支。
- 查看并发和用户/设备许可证使用情况的明细。

查看许可证服务器状态

许可证服务器状态视图显示了向 Citrix Cloud 报告使用情况的每个许可证服务器。



如果许可证服务器在过去三天内成功将使用情况上传到 Citrix Cloud，则会显示“正在报告”状态。如果许可证服务器在过去 30 天内报告过使用情况，但在过去三天内未报告，则会显示“未报告”状态。过去 30 天内未报告使用情况的许可证服务器将从列表中删除。

许可证服务器状态对许可证使用情况视图的影响

许可证服务器的报告状态和上次报告日期决定了特定许可证服务器的使用情况是否包含在使用情况洞察视图和报告中。

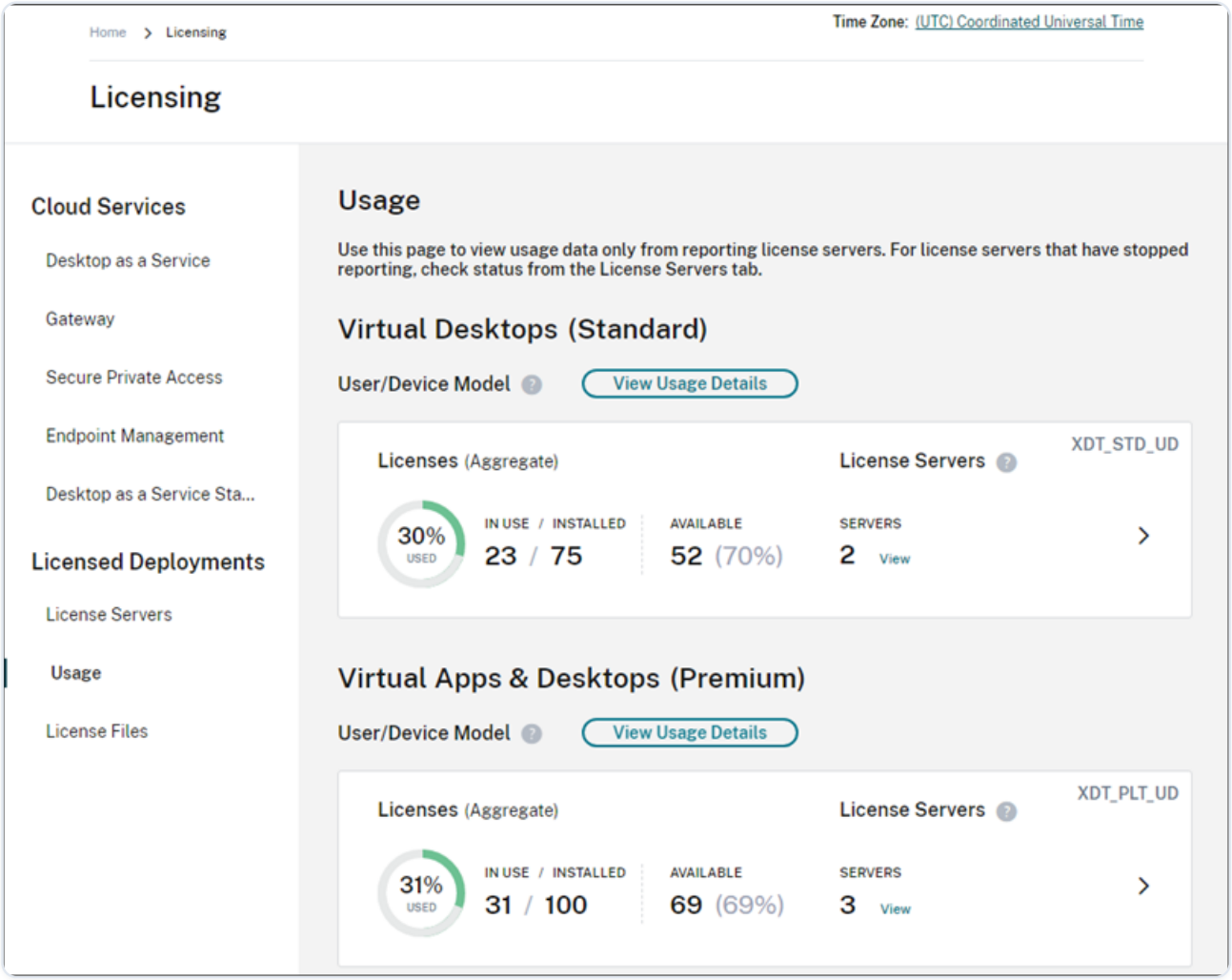
- 当前安装和正在使用的许可证完全基于来自报告许可证服务器的数据。如果许可证服务器被列为“未报告”，则该许可证服务器的已安装和正在使用的许可证不会反映在使用情况洞察体验中。
- 每个许可证服务器的上次报告日期决定了使用情况洞察体验中许可证使用情况信息的最新程度。显示的许可证使用情况报告仅与每个许可证服务器的上次报告时间一样最新。

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

- 配置为使用情况洞察并注册到 Citrix Cloud 的 Citrix 许可证服务器每天更新一次使用情况。如果需要，您可以从许可证服务器上的 Citrix License Manager 管理控制台强制更新。

许可证使用情况

“使用情况”选项卡提供了跨 Citrix 部署的许可证使用情况的综合视图。来自每个报告许可证服务器的许可信息被合并到一个视图中。此视图使您可以轻松查看跨许多不同部署和许可证服务器的完整许可情况。



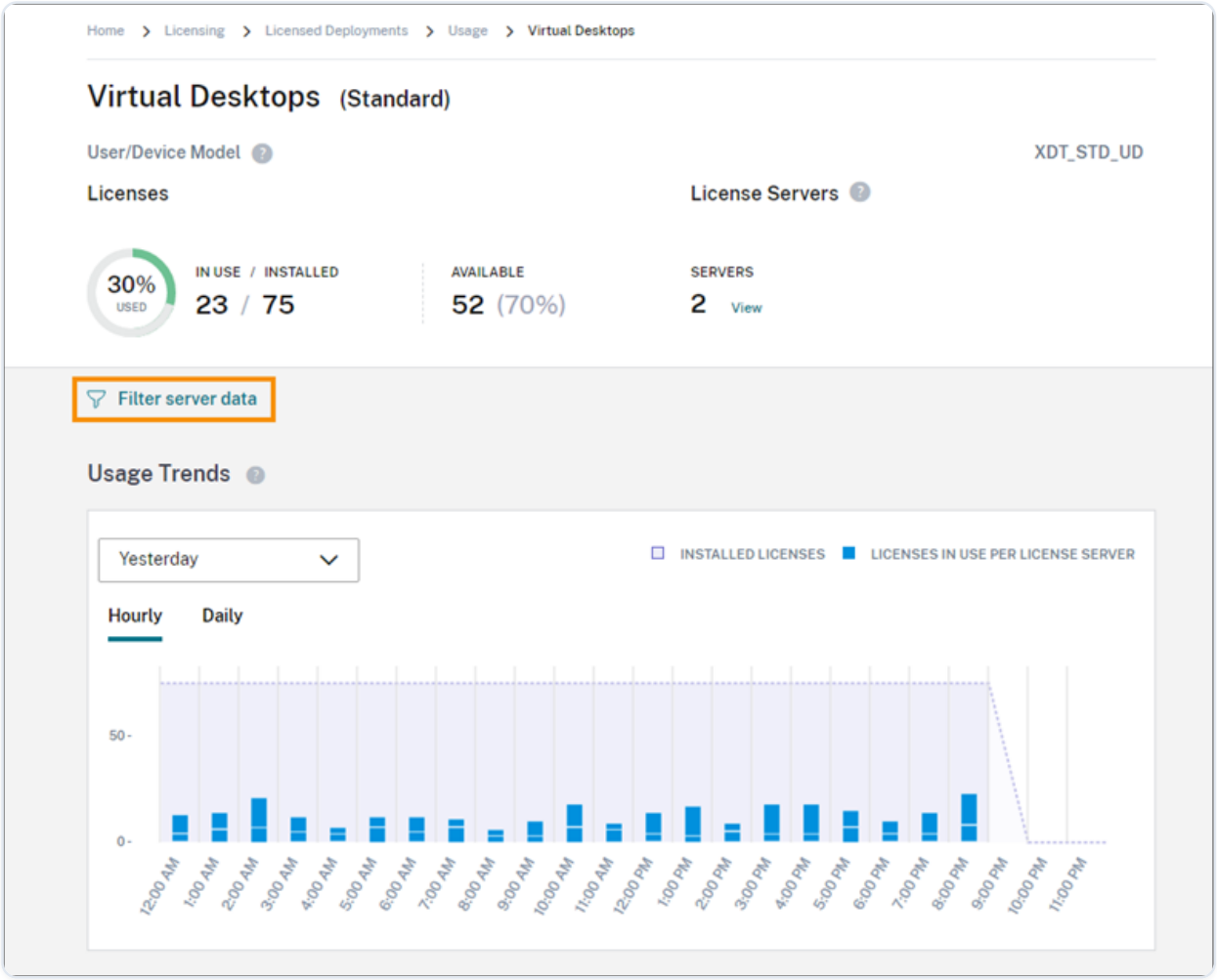
许可证使用情况根据产品版本和许可模型在多个许可证服务器之间进行组织和汇总。为在所有报告许可证服务器中找到的每个唯一许可证版本显示一个许可证使用情况摘要卡。为检测到的每个产品版本显示一个摘要卡。

每个许可证服务器的使用情况

要查看每个许可证服务器的产品许可证使用情况，您可以筛选服务器数据。

1. 在“**使用情况**”页面上，选择要管理的产品的“**查看使用情况详细信息**”。
2. 单击“**筛选服务器数据**”，然后选择要查看使用情况的许可证服务器。默认情况下，所有许可证服务器均处于选中状态。

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



3. 选择“**应用**”。

应用筛选器后，Citrix Cloud 仅显示您所选服务器的使用趋势、许可证服务器明细和许可证活动。

并发许可模型的峰值许可证使用情况

并发许可证的报告体验围绕以下数据点组织：

- 已安装的许可证：每个许可证服务器上安装的许可证数量。
- 峰值使用中许可证：在特定时间范围内使用的最大许可证数量。

在计算峰值使用中许可证时，Citrix Cloud 会检索以下时间段内使用的最大许可证数量：

- 最近 7 天：过去七天内一次性使用的最大许可证数量。
- 本月：当前日历月内一次性使用的最大许可证数量。
- 历史记录：自许可证服务器在 Citrix Cloud 中注册以来一次性使用的最大许可证数量。

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

重要提示：

这些时间段的数据可能与许可证服务器上正在使用的许可证数量不匹配。许可证服务器仅报告在任何给定时间正在使用的许可证数量。Citrix Cloud 接收这些单独的数据点并计算这些时间段的峰值。

解释许可证使用情况的注意事项

Citrix 许可支持多种使用场景，并包含详细信息。监控使用情况时，请牢记以下注意事项：

- 使用情况信息基于每个报告许可证服务器上安装的许可证。如果许可证服务器的可用许可证不足，您可以在许可证服务器上分配和放置额外的许可证以增加可用许可证的数量。
- Citrix 许可证服务器使用情况洞察视图中提供的信息仅包括由已注册且正在积极报告的 Citrix 许可证服务器收集和报告的信息。许可部署体验不代表也可能不匹配您实际拥有或购买的许可证总数。
- 可用许可证的百分比是根据正在使用的许可证数量相对于报告许可证服务器上安装的许可证数量计算的。

删除许可证服务器注册

从 Citrix Cloud 中完全删除许可证服务器注册包括以下任务：

1. 使用 Citrix Licensing Manager 控制台从 Citrix Cloud 中删除已注册的许可证服务器。有关完整说明，请参阅删除许可证服务器的注册。
2. 删除任何以前收集的使用数据。
3. 验证 Citrix Cloud 不再在“产品注册”页面上显示许可证服务器。如果许可证服务器仍显示在列表中，请按照删除产品注册中的说明删除该服务器。

删除使用数据

当您从 Citrix Cloud 中删除已注册的许可证服务器时，以前收集的使用数据仍会存储。如果您不再希望保留此数据，可以将其删除。

重要提示：

删除使用数据是永久性的，无法撤消。如果您删除使用数据但未删除许可证服务器的注册，Citrix Cloud 将继续收集使用数据。

1. 从 Citrix Cloud 菜单中，选择**许可**。

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

2. 在“**许可证服务器**”选项卡上，选择“**删除数据**”。
3. 出现提示时，选中复选框以确认您了解删除操作的影响。
4. 选择“**删除服务器数据**”。

Citrix 服务提供商的许可

Citrix Cloud™ 中的许可证使用情况洞察服务是一项免费云服务，可帮助 **Citrix 服务提供商 (CSP)** 了解并报告产品许可证和使用情况。只有 CSP 合作伙伴才能访问许可证使用情况洞察。

注意：

Citrix DaaS 以前称为 Citrix Virtual Apps and Desktops 服务。适用于 Azure 的 Citrix DaaS Standard 以前称为适用于 Azure 的 Citrix Virtual Apps and Desktops Standard。某些显示可能包含旧名称。

许可证使用情况洞察服务使您能够：

- 自动聚合来自遥测的产品使用信息
- 自动聚合单租户和多租户客户的云许可使用情况和消耗
- 轻松查看每月有哪些用户正在访问您的 Virtual Apps and Desktops 部署
- 创建客户许可使用情况明细
- 查看并了解您与 Citrix® 的历史业务
- 将 Virtual Apps and Desktops 和 Citrix DaaS 许可证使用情况、NetScaler VPX 分配数据以及适用于 Azure 的 Citrix DaaS Standard 许可和消耗数据导出到 CSV

其他信息

有关要求和设置说明，请参阅 许可证使用情况洞察入门。

要查看单租户和多租户客户的聚合使用情况，请参阅 Citrix 服务提供商的云服务许可证使用情况和报告。

要使用许可控制台查看客户对受支持服务的使用情况，请参阅以下文章：

- Citrix DaaS 的客户许可证和使用情况监控

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

开始使用许可证使用情况洞察

支持的 Citrix® 产品

许可证使用情况洞察服务提供以下 Citrix 产品的用法信息：

- Virtual Apps and Desktops（本地部署）产品使用情况
- Citrix DaaS™ Premium（以前称为虚拟应用高级版和虚拟应用和桌面高级版服务）
- 适用于 Azure 的 Citrix DaaS Standard（以前称为适用于 Azure 的 Citrix Virtual Apps and Desktops Standard）
- NetScaler® Console VPX 分配

要求

为了捕获 Citrix 本地部署产品的许可证和使用情况信息并符合要求，需要 Citrix License Server 11.17.2 build 51000 或更高版本。仅支持基于 Windows 和基于 VPX 的许可证服务器。

Citrix License Server 11.17.2 build 51000 及更高版本包含对 Citrix 服务提供商 (CSP) 合作伙伴很重要的关键功能：

- 优化的使用情况收集：License Server 包含新功能，可优化许可行为和跟踪，以更好地支持 CSP。
- 回拨：License Server 包含回拨功能，可自动为 CSP 合作伙伴收集产品使用情况。这些功能是 CSP 合作伙伴专有的，只有在许可证服务器上检测到 CSP 许可证时才会激活。
- 要过渡到许可证激活服务 (LAS)、支持新的基于事件的遥测并简化客户站点之间的 CSP 本地许可证分发，最低许可证服务器版本必须是 11.17.2 build 51000。

步骤 1：更新 Citrix License Server

如果您运行的许可证服务器版本低于 11.17.2 build 51000，则必须升级许可证服务器。就地升级简单快捷。完成以下任务：

1. 下载最新的许可证服务器。有关最新版 Citrix 许可证服务器的更多信息，请参阅 Citrix 许可文档。
2. 升级 您当前的许可证服务器。
3. 对每个许可证服务器重复升级过程。

步骤 2：使用 My Citrix 凭据登录 Citrix Cloud™

登录之前，如果您还没有 CSP 合作伙伴云帐户，则需要注册一个 Citrix Cloud 帐户。请按照 注册 Citrix Cloud 中所述的步骤操作。

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

创建帐户时，请使用您在 citrix.com 上分配和下载 Citrix 许可证时使用的相同 My Citrix 凭据。Citrix Cloud 会向与您的 My Citrix 凭据关联的电子邮件地址发送一封电子邮件以确认帐户。

当您的 Citrix Cloud 帐户准备就绪后，请使用您的电子邮件地址和密码登录 https://citrix.cloud.com 。

步骤 3（可选）：通过许可证服务器匿名化用户名

默认情况下，与 Virtual Apps and Desktops 或 Citrix DaaS 许可证签出关联的用户名会安全地回传给 Citrix。

回传用户名是为了让 CSP 合作伙伴能够充分利用 License Usage Insights 功能和 CSP 许可计划。

用户信息仅限于单个 user@domain 条目；不会回传其他个人身份数据。Citrix 不会共享此信息。

对上传用户名信息敏感的合作伙伴可以启用用户名匿名化。启用后，用户名匿名化会在上传之前使用安全且不可逆的算法将可读用户名转换为唯一的字符串。

License Usage Insights 使用这些唯一标识符来跟踪产品使用情况，而不是实际用户名。这种方法允许服务提供商利用逐月洞察，而无需在云服务用户界面中查看实际用户名。

配置用户名匿名化

1. 在许可证服务器上，使用文本编辑器打开配置文件。通常，配置文件位于 C:\Program Files\Citrix\Licensing\WebServicesForLicensing\SimpleLicenseServiceConfig.xml。
2. 在“**配置**”部分中，添加 **UsageBasedBillingScramble** 设置，如下所示：

```
<?xml version="1.0" encoding="utf-8"?>

<Configurations>

<EncoreConfiguration>

<SamplingPeriod>15</SamplingPeriod>

<RetentionTime>180</RetentionTime>

<Enabled>true</Enabled>

</EncoreConfiguration>

<SARenewalConfigOptions>Notify</SARenewalConfigOptions>

<UsageBasedBillingScramble>1</UsageBasedBillingScramble>
```

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

```
</Configurations>
```

3. 保存文件。

步骤 4：使用 License Usage Insights 服务

在 Citrix Cloud 控制台中，从九点菜单中找到并单击 License Usage Insights 服务磁贴。有关该服务主要功能的概述，请参阅管理产品使用情况、许可证服务器和通知。

更多详细信息

将 Citrix License Server 与 License Usage Insights 结合使用时，请考虑以下事项：

- 新更新的许可证服务器或站点可能需要长达 24 小时才能显示在 License Usage Insights 管理控制台中。
- 当使用数据从许可证服务器上传时，它会以安全的方式进行处理和存储，以便 License Usage Insights 可以在以后访问它。此过程可能需要长达 24 小时才能完成。
- 默认情况下，与 Virtual Apps and Desktops 或 Citrix DaaS 许可证签出关联的用户名会安全地回传给 Citrix。
- 用户名回传是为了让 CSP 合作伙伴能够充分利用 License Usage Insights 功能和 CSP 许可计划，该计划支持免费用户进行试用、测试和管理产品使用。
- 用户信息仅限于单个 user@domain 条目；不会回传其他个人身份数据。Citrix 绝不会共享此信息。

帮助和支持

如果您需要 License Usage Insights 方面的帮助，请在 My Support 门户上提交支持票证。要从 Citrix Cloud 访问 My Support：

1. 登录 Citrix Cloud。
2. 单击位于屏幕右上角附近的“**帮助**”图标。
3. 选择**开具工单**。
4. 选择**转到我的支持**并使用您的 My Citrix 凭据登录。
5. 填写并提交表单。

Citrix 技术支持团队成员将跟进并为您提供帮助。

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

常见问题

- **正在回传哪些信息？我能否查看我的许可证服务器正在发送给 Citrix 的信息？**可以，您可以查看回传给 Citrix 的信息副本。有关详细信息，请参阅上传中包含的许可证服务器信息。
- **License Usage Insights 是否适用于非 Citrix 服务提供商的 Citrix 客户或合作伙伴？**否。License Usage Insights 仅适用于签订了有效会员协议的 Citrix Service Provider™ 合作伙伴。
- **我能否在许可证服务器上禁用 Call Home？**否。根据 Citrix 服务提供商许可协议，所有许可证服务器都必须回传产品使用情况。对回传用例敏感的合作伙伴可以使用用户名匿名化功能。有关详细信息，请参阅通过许可证服务器匿名化用户名。
- **我是否会根据 License Usage Insights 中显示的产品使用情况进行计费？**否。License Usage Insights 可帮助合作伙伴了解其产品使用情况，以便他们准确地审计和向客户收费，并根据需要扩展订单。

管理产品使用情况、许可证服务器和通知

使用许可证使用情况洞察来监控产品使用情况、跟踪许可证服务器状态以及管理 Citrix Cloud 部署的客户通知。

注意：

要显示未混淆的用户信息（例如用户名和域）并正确解析站点和交付组名称，请将您的 Citrix Virtual Apps and Desktops™ Delivery Controllers 升级到以下最低支持版本之一：

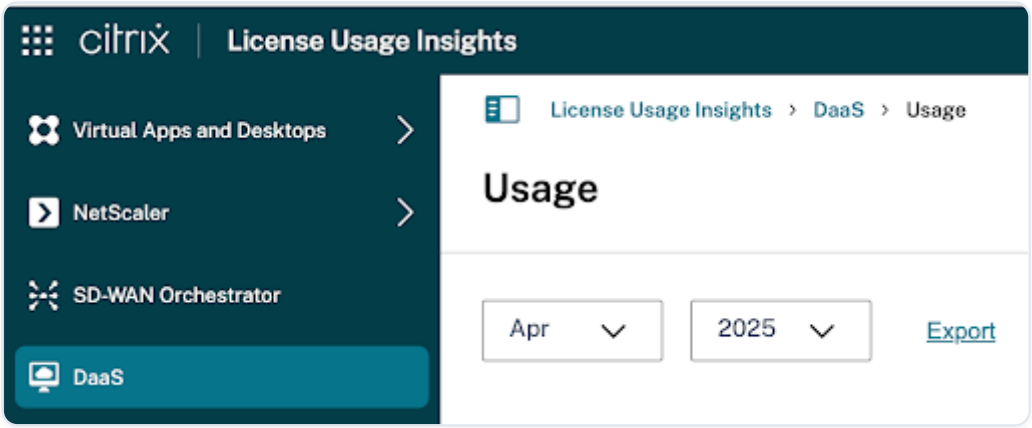
- **当前版本：** 2411 或更高版本
- **LTSR：** 2203 CU7、2402 CU3 或 2507

由于默认数据混淆，早期版本会显示 GUID 而非字段值。

产品选择

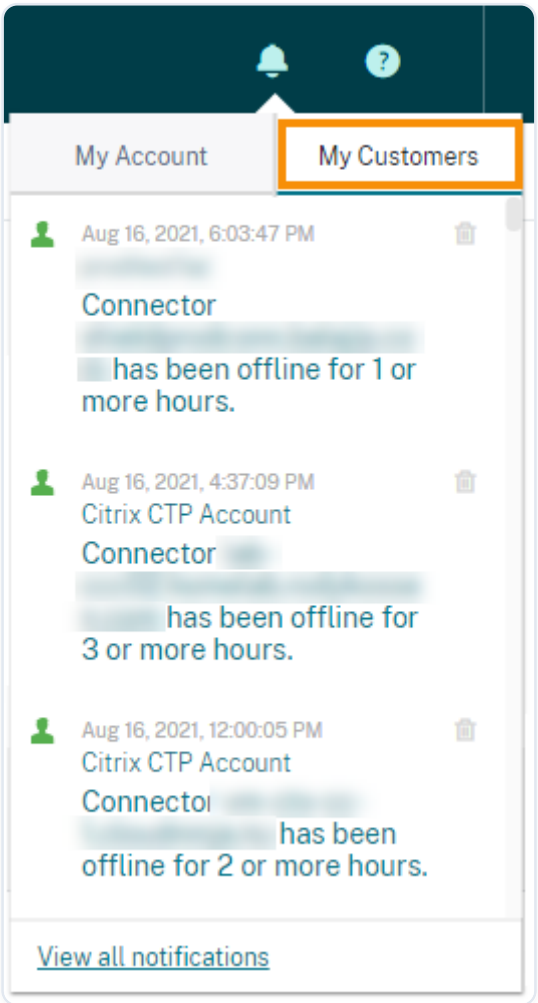
要查看其他产品的许可详细信息，请单击产品名称旁边的箭头，然后选择要查看的产品或服务。

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



客户通知

监控多个客户的解决方案运行状况，而无需单独访问每个部署。Citrix Cloud 中的“通知”区域会在您的控制面板上聚合来自所有客户的通知，以便您可以确保警报得到处理并且服务持续运行。



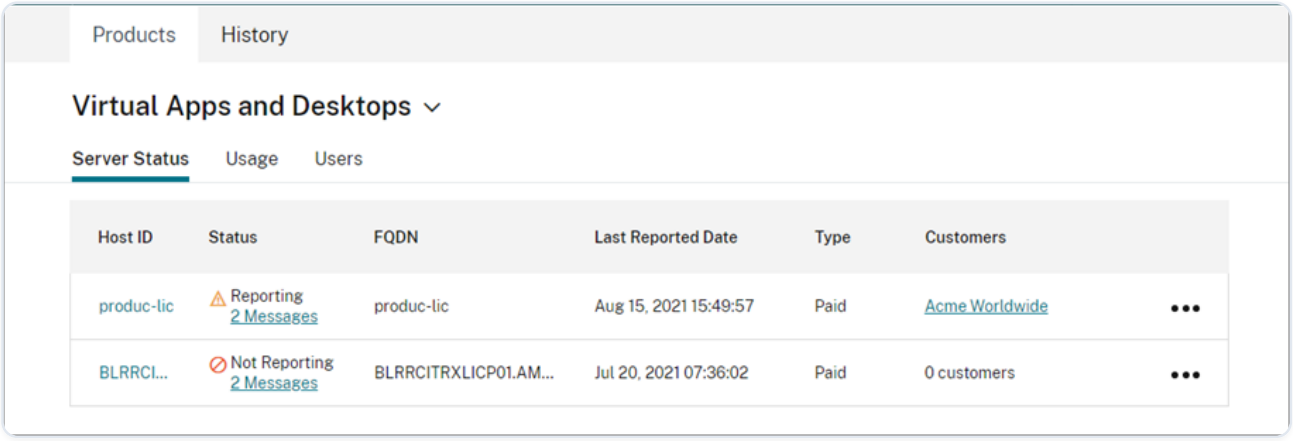
1. 在 Citrix Cloud 管理控制台中，单击**通知**图标，然后单击**我的客户**。将显示最新通知列表。
2. 要查看完整的客户通知列表，请单击**查看所有通知**。

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

许可证服务器状态

为符合 Citrix Service Provider™ 许可指南，所有活动的许可证服务器都必须更新并报告。许可证服务器状态显示您拥有的许可证服务器以及它们是否已更新以用于 License Usage Insights。

该服务使用存储在 Citrix® 后台的传统许可证分配数据来显示活动许可证服务器列表。如果许可证服务器已更新并成功报告，License Usage Insights 将显示“正在报告”状态，并包含最近一次上传的时间戳。



上传中包含的许可证服务器信息

当许可证服务器上激活 Call Home 时，每天上传以下信息：

- 许可证服务器版本
- 许可证文件信息：
  - 服务器上安装的许可证文件
  - 许可证文件到期日期
  - 产品功能和版本授权信息
  - 许可证数量
- 许可证使用情况：
  - 当前日历月使用的许可证
  - 与许可证签出关联的用户名
  - 产品功能和已激活的版本

查看许可证服务器上传

CSP 合作伙伴可以检查其许可证服务器上最后上传的有效负载，以全面了解许可证服务器发送给 Citrix 的所有详细信息。此有效负载的副本以 .zip 文件的形式存储在许可证服务器上。默认情况下，此位置为 C:\Program Files (x86)\Citrix\Licensing\LS\resource\usage\upload_1456166761.zip。

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

注意：

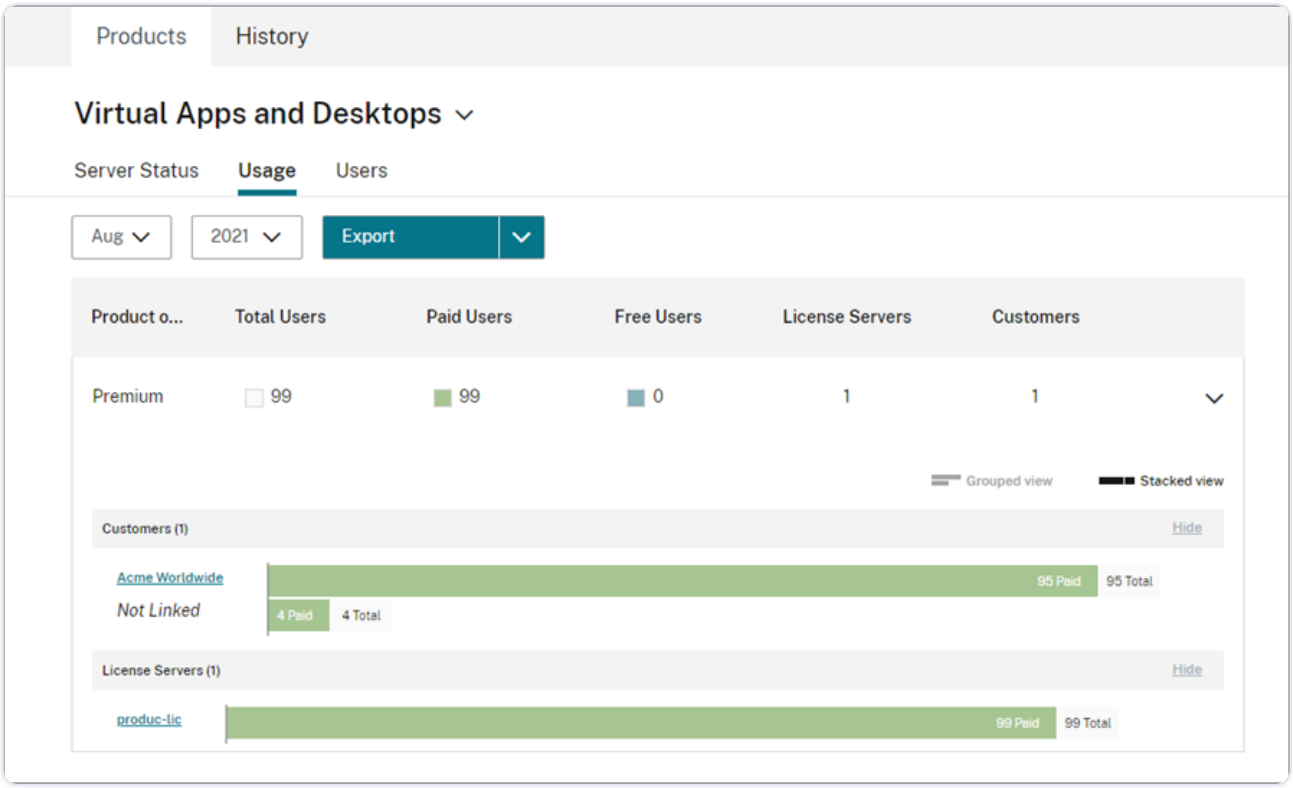
成功的上传会被删除，但最后一个除外。不成功的上传会保留在磁盘上，直到发生成功的上传。发生这种情况时，除最后一次上传之外的所有上传都将被删除。

使用情况收集

使用情况收集通过自动数据收集和聚合帮助您了解产品使用情况。无需部署其他工具。

许可证使用情况洞察会自动聚合所有 Citrix 许可证服务器（用于传统许可证服务器回拨）和站点（用于许可证激活服务）的产品使用情况，以提供所有部署的完整使用情况视图。您还可以通过将特定用户与其所属的客户或租户关联来创建许可证使用情况细分。

许可证服务器收集并跟踪产品许可证使用情况，并使用安全的电话回拨通道将其报告给 Citrix。这种自动化方法为您提供持续更新的使用情况数据流，从而节省时间并帮助合作伙伴更好地了解其部署中的使用趋势。



用于按客户细分 Virtual Apps and Desktops 产品使用情况的用户分配（标记）

此功能提供每个客户的许可证使用情况数据细分，包括支持管理和报告单租户和多租户站点（与 LAS 集成）或许可证服务器（传统回拨）架构。许可证使用情况洞察的对象包括：

- **许可证服务器**：列表中的“正在报告”或“未报告”许可证服务器。
- **站点**：专用于某个客户或由多个租户客户共享的 Virtual Apps and Desktops 站点。

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

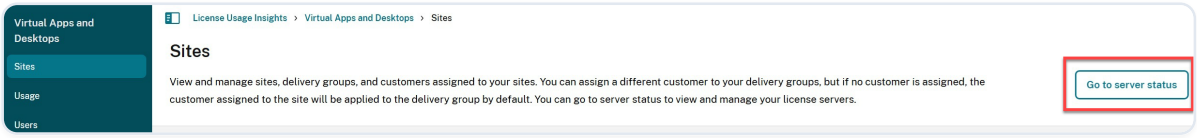
- **交付组**：通常专用于某个客户的 Virtual Apps and Desktops 交付组。
- **用户**：在回拨使用数据中找到的单个用户名。
- **NetScaler**：单个 NetScaler VPX™ 许可证分配（VPX 列表中的 VPX）。

注意：

CSP 可以更新上个月和当月的客户标记，直到下个月的 10 号。

要按客户细分许可使用情况，您必须首先将用户与其所属的客户或租户关联起来。如果您的“客户”控制板中没有定义任何客户，您可以添加新客户，或者您可以与现有 Citrix Cloud 客户建立连接。

1. 如果适用，将客户添加到“客户”控制板：从 Citrix Cloud 管理控制台的九宫格菜单中，单击“**我的客户**”，单击“**添加或邀请**”，然后按照屏幕上的说明进行操作。
2. 单击九宫格菜单，然后选择“**许可证使用情况洞察**”磁贴。
3. 选中“**Virtual Apps and Desktops**”产品后，默认情况下将加载通过许可证激活服务 (LAS) 激活的“**站点**”。
4. 要继续从 LAS 集成站点分配用户：
   a. 单击“**用户**”。
   b. 选择要关联的用户，然后单击“**批量操作 > 分配给客户**”。
5. 要从传统许可证服务器回拨分配用户：
   a. 单击“**转到服务器状态**”按钮。



   b. 加载许可证“**服务器状态**”页面后（您也可以通过单击此页面上的“**转到站点**”导航回 LAS 集成站点），从菜单选项中选择“**所有用户**”。
   c. 筛选并搜索用户，选择未关联的用户，然后点击“**批量操作 > 管理客户链接**”。
6. 从客户列表中，选择您要将用户与之关联的客户。
7. 点击“**分配**”或“**保存**”。
8. 要查看按客户细分的数据，请点击“**使用情况**”视图。

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

用户客户标记

此功能提供每个客户的许可证使用情况数据的细分，包括支持管理和报告单租户和多租户许可证服务器架构。许可证使用情况洞察的对象包括：

- 许可证服务器 - 列表中“正在报告”或“未报告”的许可证服务器。
- 用户 - 在回拨使用情况数据中找到的单个用户名。
- NetScaler® - 单个 NetScaler VPX 许可证分配（VPX 列表中的 VPX）。

注意：

用户客户标记功能具有与免费用户标记相同的行为，即 CSP 可以在当前计费周期内更新客户标记，直到下个月的 10 号。

服务器客户标记

此功能允许将用于传统回拨的许可证服务器标记或分配给特定客户。通过利用服务器客户标记，来自该服务器的任何用户将自动与标记的客户关联，管理员可以轻松识别和跟踪与不同客户关联的资源，从而促进客户计费、报告和更高效的资源分配。

站点和交付组客户标记

站点客户标记功能适用于专用于特定客户的 Virtual Apps and Desktops 站点（也称为单租户站点），它允许将与 LAS 集成的站点标记并分配给客户。分配后，来自该站点的任何用户将自动在使用情况报告客户细分中与标记的客户关联。

交付组客户标记功能适用于多个客户共享的 Virtual Apps and Desktops 站点（又称多租户站点），它允许将 LAS 集成站点的交付组标记到其相关客户。分配后，该交付组中的任何用户都将在使用情况报告客户明细中自动与标记的客户关联。

站点和交付组客户标记(/en-us/citrix-cloud/media/site-delivery-group-customer-tagging.png)

站点可以专门分配给单个客户（站点标记），也可以通过交付组标记分配给多个客户，但不能同时进行。

要访问站点或交付组标记，请从 waffle 菜单导航并选择 License Usage Insights，在“**站点**”页面中，在“站点”表中选择站点，然后单击“**分配客户**”。通过在“交付组”表中选择一个交付组，同一页面也可用于交付组标记。如果站点已专门分配给某个客户，则该站点的交付组将是只读的，并且在您清除站点客户分配之前，无法单独分配给客户。

基于站点和交付组的客户标记现已进入技术预览阶段，您可以使用此表单申请参与预览。

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

历史趋势

您可以根据传统的许可证服务器回拨功能，查看与 Citrix 开展的所有过往业务的完整历史记录。查看您上个月、去年或在可配置时间段内报告的使用情况。

历史视图提供有价值的业务洞察。作为 Citrix 服务提供商，您可以快速了解您与 Citrix 的业务趋势，以及哪些产品在您的客户和最终用户中增长最快。 在“服务器状态”页面上，单击“查看产品历史记录”图标和链接。

月度服务使用历史记录图(/en-us/citrix-cloud/media/lui-history-console-2.png)

导出使用情况和分配数据

您可以从 License Usage Insights 导出以下类型的数据作为 CSV 文件：

- 指定月份的 Virtual Apps and Desktops 产品使用情况和用户列表
- 当前 NetScaler VPX 分配详细信息

1. 从产品列表中选择“**Virtual Apps and Desktops**”或“**Networking**”。
2. 如果适用，选择要导出的视图。例如，要导出 Virtual Apps and Desktops 使用情况详细信息，请单击“**使用情况**”视图。
3. 如果适用，请选择要导出的月份和年份。
4. 在屏幕右侧，单击**导出**。

使用 API 访问许可数据

Citrix 提供了多个 API，您可以使用这些 API 在 Citrix Cloud 外部访问您的许可数据。要了解有关这些 API 的更多信息，请参阅 Citrix 开发者文档中的用于管理 Citrix Cloud 许可的 API。

要使用这些 API，您必须首先创建服务主体并生成持有者令牌。要创建服务主体，请参阅Citrix Cloud API 入门。

分销商对 API 的访问权限

您可以允许您的 Citrix 分销商或授权的第三方通过 Citrix Cloud API 访问您的许可数据，而无需授予他们对您的 Citrix Cloud 帐户的完整管理员访问权限。您这样做是为了让您的分销商能够验证您的使用情况报告并确保准确计费。

要向分销商提供对您的许可数据的访问权限，您可以创建具有所需自定义访问权限的服务主体。要创建服务主体，请参阅Citrix Cloud API 入门。

对于此用例，请选择**自定义**访问权限，然后选择 **License Usage Insights** > **License Usage Insights: Distributor Access**。

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

分销商可用的许可数据

本节介绍您的 Citrix 分销商可以使用您提供的服务主体详细信息访问的许可数据和 API。使用以下链接了解每个 API 的更多详细信息。

CSP 报告每月和历史 Virtual Apps and Desktops 许可证使用情况 (License Usage Insights)：

- Virtual Apps and Desktops 当前使用情况
- Virtual Apps and Desktops 历史使用情况

CSP 报告单租户和多租户云许可证使用情况 (License Usage Insights)：

- DaaS 当前使用情况
- DaaS 历史使用情况

CSP 的云许可证使用情况（许可）：

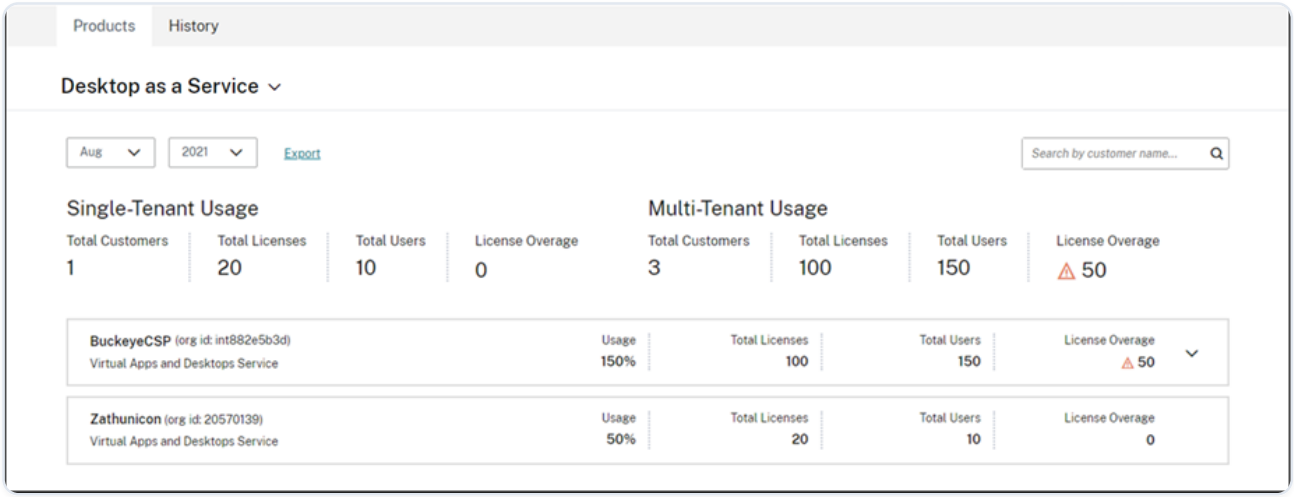
- DaaS 当前使用情况
- DaaS 历史使用情况

租户的云许可证使用情况（客户控制板 -> 查看许可）

- DaaS CCU 当前使用情况
- DaaS CCU 历史使用情况
- DaaS UD 当前使用情况
- DaaS UD 历史使用情况

Citrix 服务提供商的云服务许可证使用情况和报告

许可证使用情况洞察会自动聚合云服务使用情况，以提供所有单租户和多租户客户的完整视图。您还可以将给定月份的这些详细信息导出到 CSV 文件以进行进一步分析。



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

支持的服务

CSP DaaS 许可证使用情况适用于 Citrix DaaS™ Premium（以前称为 Virtual Apps and Desktops Premium 服务）多租户和单租户权利。

注意：

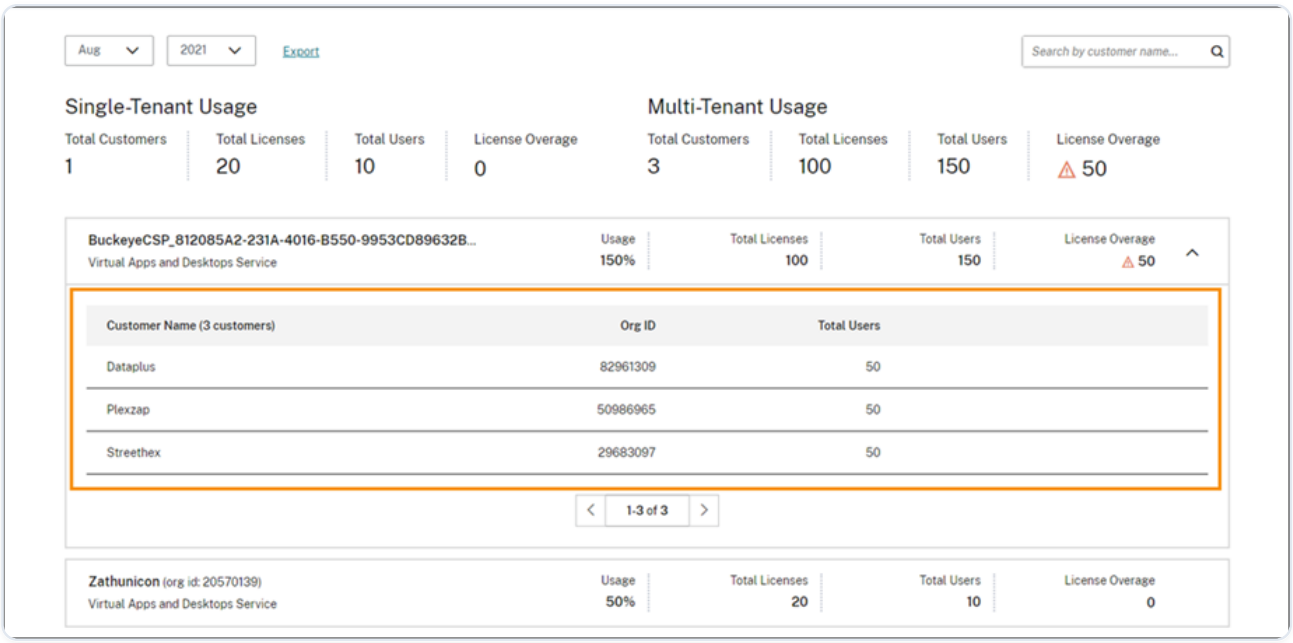
不支持在同一云帐户中混合使用 CSP DaaS 权利与其他非 CSP DaaS 权利。 单租户 CSP DaaS 权利只能交付给链接到同一 Citrix Cloud™ 控制平面上 CSP 帐户的租户客户帐户。

许可证摘要

许可证使用情况洞察为 Citrix 服务提供商 (CSP) 的单租户和多租户使用情况提供以下细分：

- 按租户类型分组的合作伙伴级别概览摘要，包括所有客户的总客户数以及购买的许可证、用户和超额（过度使用）许可证的总数。
- 每个单租户客户的使用情况摘要，包括正在使用的许可证总数百分比、购买的许可证总数、用户数和过度使用的许可证数。

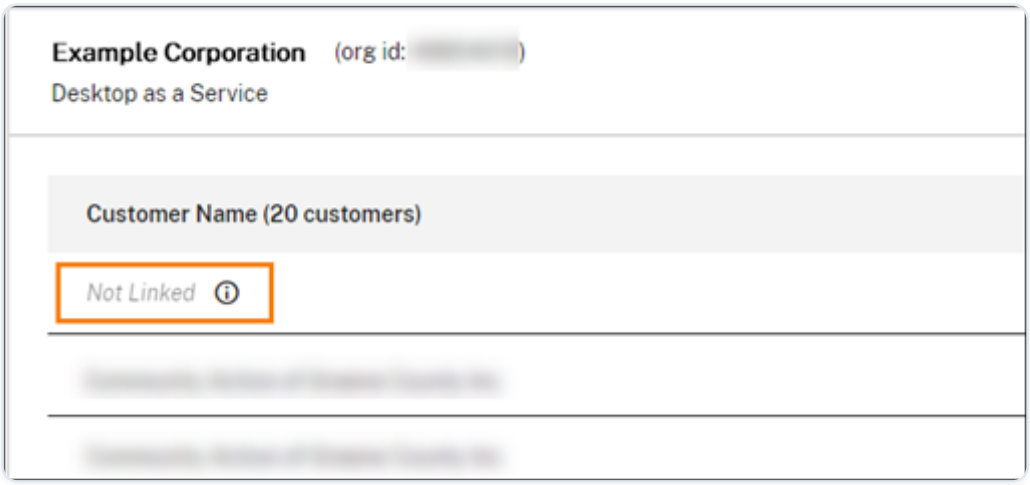
对于多租户服务，您可以展开使用情况摘要以查看客户细分、帐户 ID 以及与每个租户客户关联的总用户数。



未链接的租户客户

如果租户客户的某些用户通过合作伙伴的共享商店 URL 而不是租户自己的商店 URL 启动会话，则这些用户可能会被列为“未链接”。

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

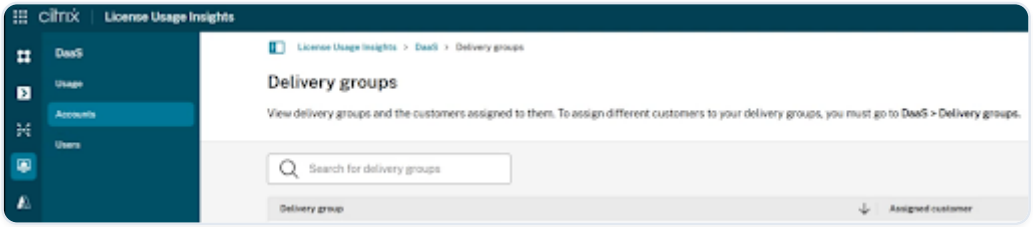


为确保这些未链接的用户与其相关的租户客户正确关联，以便进行准确的计费和报告，同时继续允许用户访问合作伙伴商店 URL，服务提供商（合作伙伴）管理员可以利用以下两种方法来链接用户。

基于交付组的自动用户分配（标记）

当用户从这些交付组启动会话时，License Usage Insights (LUI) 服务现在可以通过范围交付组自动将多租户 DaaS 用户链接到租户客户，但每个交付组都必须已分配一个特定的租户范围。从无范围或共享交付组启动会话的用户无法链接。您可以通过 **License Usage Insights > DaaS > Accounts** 查看多租户 DaaS 交付组的整体租户范围分配（或未分配）情况。

要为交付组分配或更新范围，您需要转到多租户 DaaS 的 Studio 控制台。

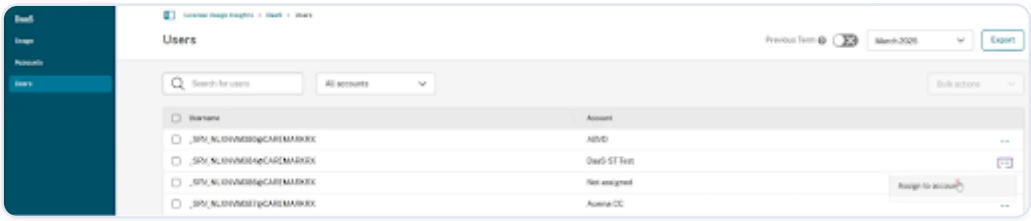


将用户分配（标记）给租户客户

在多租户环境中，租户应拥有专用的交付组；但在某些特殊用例中，如果交付组是共享的，或者某些 CSP 管理员属于具有不同范围的多个交付组，则需要手动标记用户以将用户分配或取消分配给租户客户。

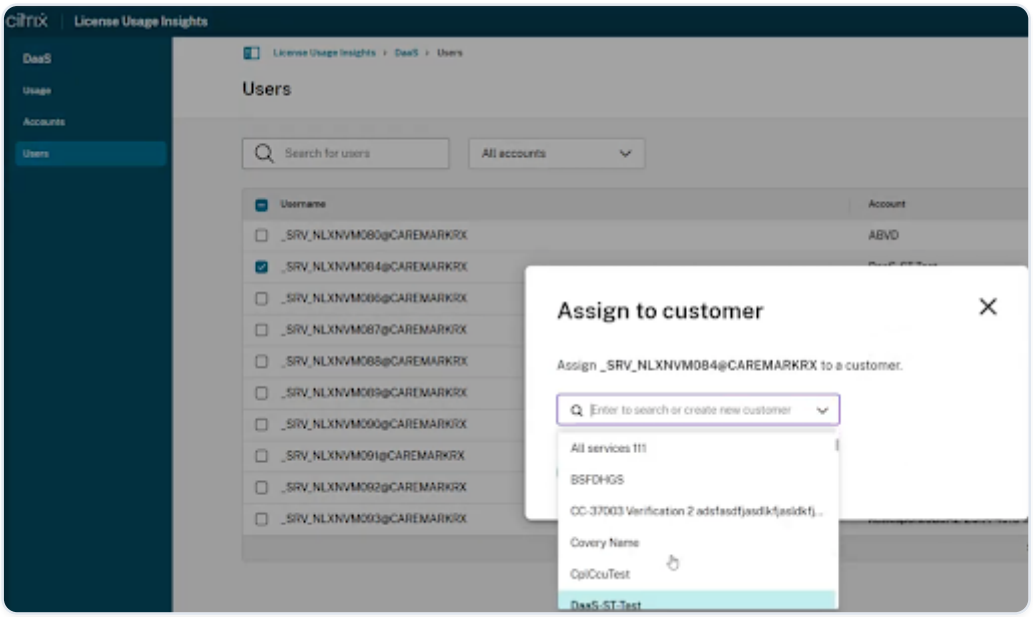
从九宫格菜单导航到 > **License Usage Insights > DaaS > Users**：

- 要分配单个用户，请单击用户行末尾的“...”，选择 **Assign to customer**，然后选择租户客户。



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

- 要批量分配用户，请搜索具有相关条件的用户，选中用户行中的复选框，在 **Bulk actions** 下，单击 **Assign to customer**，选择租户客户，然后单击 **Assign**。



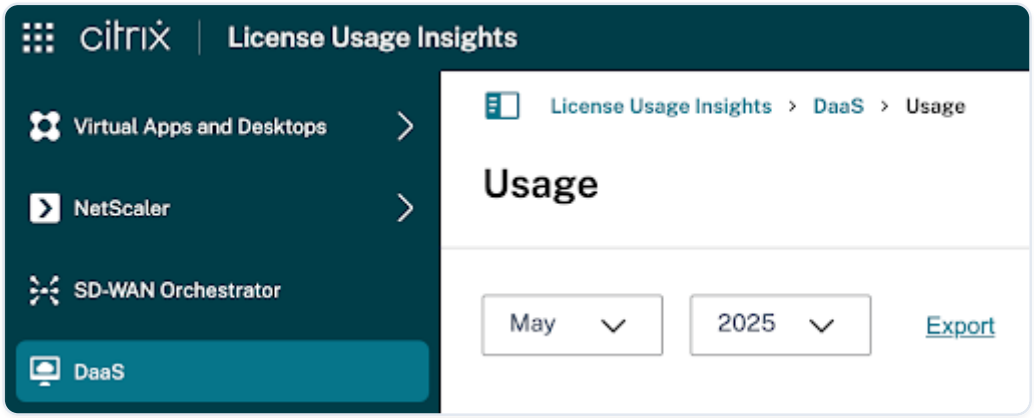
- 您也可以使用类似的过程取消分配客户。

查看和导出每月使用情况

随时可以查看所有客户前几个月的许可证使用情况。您还可以将此数据导出为 CSV 文件以进行进一步分析。

1. 从产品菜单中，选择要查看的产品。

对于 Citrix DaaS，选择要查看的月份和年份，然后选择 **导出**。

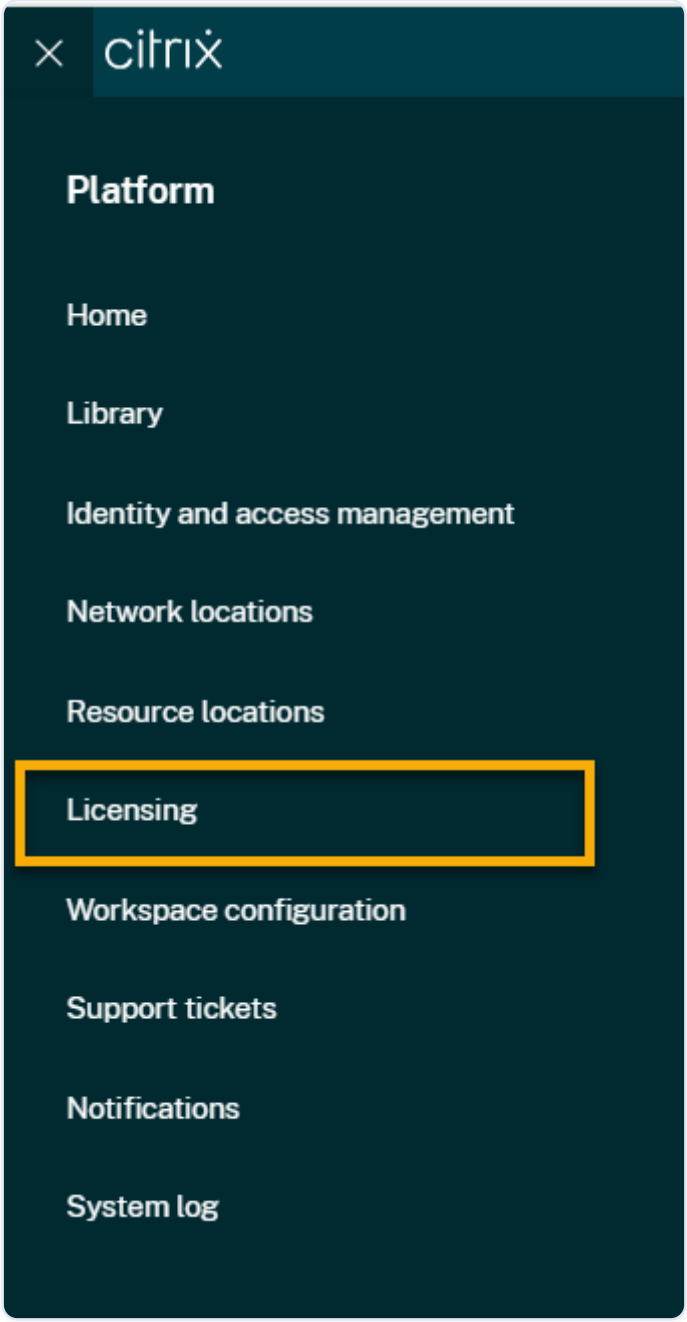


客户许可证和使用情况监控（适用于 Citrix DaaS™）

Citrix 服务提供商 (CSP) 的客户可以在 Citrix Cloud 中轻松监控其用户的 Citrix DaaS 许可证。作为 CSP，您可以通过登录客户在 Citrix Cloud 中的帐户来访问这些详细信息。要查看跨单租户和多租户客户的聚合许可证使用情况信息，请参阅适用于 Citrix 服务提供商的云服务许可证使用情况和报告。

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

客户可以通过从 Citrix Cloud™ 菜单中选择**许可**来查看其许可数据。



许可证分配

用户/设备许可模式： Citrix Cloud 在唯一客户用户当月首次启动应用程序或桌面时分配许可证。

并发用户许可模式：

有关并发许可模式的信息，请参阅许可产品文档中的并发许可证。

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

许可摘要

Citrix Cloud 显示用户/设备和并发用户许可模式下正在使用的许可证的摘要视图。对于由 CSP 管理的单租户客户，不支持在同一客户帐户中混合使用 CSP 许可证和非 CSP 许可证（无论**并发**还是**用户/设备**）。

用户和设备摘要

对于用户/设备模式，许可摘要提供了一个一目了然的视图，显示正在使用的许可证相对于您拥有的许可证总数的情况。

当百分比接近 100% 时，百分比从绿色变为黄色。如果百分比超过 100%，则百分比变为红色。

Citrix Cloud 还显示已分配许可证与已购买许可证的比率以及剩余可用许可证的数量。

计算正在使用的峰值许可证

为准确反映并发许可模型，Citrix Cloud 每五分钟统计一次同时访问服务的唯一设备数量。如果该数量大于当前显示的峰值使用量，Citrix Cloud 将显示新的峰值使用量以及达到该峰值的日期和时间。如果该数量小于当前峰值使用量，则当前峰值使用量保持不变。

重要提示：

如果您在 Director 中使用 Monitor 来获取有关并发会话的信息，请注意 Monitor 报告对并发会话的解释不同，并且不能准确反映正在使用的并发用户许可证数量。有关 Monitor 报告和许可报告之间差异的更多信息，请参阅常见问题解答。

计算每月活跃使用量

在每个月初，Citrix Cloud 会拍摄上一个日历月的快照。Citrix Cloud 会显示在该日历月期间发生的唯一连接总数。

计算每日活跃使用量

每天在同一时间，Citrix Cloud 会拍摄过去 24 小时的快照。Citrix Cloud 会显示在该 24 小时期间发生的唯一连接总数。

使用趋势

Citrix Cloud 会显示用户/设备许可证或并发用户许可证的使用趋势细分。要查看此细分，请从许可摘要页面中选择 **查看使用详情**。

用户和设备的趋势

对于用户/设备许可证，**使用趋势**部分会以图表形式显示已分配许可证的细分。

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

将鼠标指向图表上的某个时间间隔会显示以下信息：

- **许可证总数：** 您为云服务购买的跨所有授权的许可证总数。
- **以前分配：** 上个月分配的许可证数量。例如，用户在 7 月首次访问云服务并被分配一个许可证。此许可证在 7 月份计为“新分配”。在 8 月份，此许可证计为“以前分配”。
- **新分配：** 每个月分配的新许可证数量。例如，用户在 7 月首次访问云服务并被分配一个许可证。此许可证在 7 月份计为“新分配”。

已授权用户

“**许可证活动**”部分显示了当前月份分配了许可证的单个客户用户列表。此列表还显示了每个用户所属的域、分配许可证的日期以及上次使用服务的时间。

每月许可证发布

每个月的第一天，上个月分配的 CSP 许可证会自动发布。发生这种情况时，分配的许可证数量将重置为零，并且已授权客户用户列表将被清除。当用户在新月份首次启动应用程序或桌面时，许可证将重新分配。

查看每月许可证历史记录

每个月的第一天，当分配的许可证数量重置为零时，“**许可证活动**”下上个月的 CSP 已授权客户用户列表将被清除。但是，您可以随时访问前几个月的用户详细信息，并在需要时将其下载为 CSV 文件。

1. 在“**许可证活动**”部分，选择该部分最右侧的“**查看许可证历史记录**”。
2. 选择要查看的月份。此时将显示所选月份的用户详细信息列表。
3. 要导出列表，请选择该部分最右侧的“**导出到 CSV**”，然后保存文件。

导出许可证详细信息

客户可以随时将已授权用户详细信息导出到 CSV 文件以进行进一步分析。然后，客户可以根据需要使用 CSV 文件来分析许可证详细信息。

要导出当月的详细信息，请在“**许可证活动**”部分中，选择该部分最右侧的“**导出到 CSV**”，然后保存文件。

要导出前几个月的详细信息，请按照查看每月许可证历史记录 中所述为选定月份生成列表。选择“**导出到 CSV**”并保存文件。

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

Citrix Platform Flex 的授权许可

Citrix Platform Flex 是一个托管的云交付平台，旨在跨云提供安全、弹性且灵活的数字工作区和平台服务交付。

Citrix Platform Flex 使客户摆脱僵化、以基础设施为中心的部署模型，转向基于角色的运营模型。客户无需手动调整和管理基础设施，而是使用可根据工作执行方式进行扩展的 Citrix 服务。

Citrix Platform Flex 的核心旨在支持：

- 员工队伍的可变性（员工、承包商、合作伙伴和临时用户）
- 通过 Citrix 管理的基础设施实现运营简便性
- 与实际使用情况保持一致的可预测且灵活的消费
- 跨区域的企业级弹性和安全性

Citrix Platform Flex 被设计为一个构建于 Citrix Cloud 之上的多服务平台。通过该平台提供的服务共享一个共同的运营、安全和经济基础，使客户能够随着时间的推移采用更多功能，而无需重新架构其环境。了解有关 Citrix Cloud 的更多信息。

功能

Citrix Platform Flex 提供以下平台级功能：

- **基于角色的计算**：服务根据员工角色进行消费，而非基于静态基础设施或使用 Citrix Flex Credits 的按虚拟机许可。积分每月根据所提供的服务消耗。这使得能够针对不同类型的用例，合理调整性能、安全性和成本。
- **Citrix 管理的基础设施**：Citrix 拥有并运营底层云基础设施，包括生命周期管理、修补和弹性。客户专注于应用程序、策略和用户体验，而非基础设施运营。
- **弹性**：平台服务旨在实现高可用性和业务连续性，支持多区域部署模式和集成的弹性功能。
- **统一控制平面**：管理、监控、访问和策略通过 Citrix Cloud 提供，在各项服务中提供一致的管理体验。

可用服务

Citrix Platform Flex 提供与平台角色和能力模型相匹配的服务。

当前服务包括：

- **Citrix DaaS Flex**：使用 Microsoft Azure 上由 Citrix 管理的基础设施，提供基于角色的虚拟应用和桌面交付。请参阅 Citrix DaaS Flex。

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

- **Citrix SecurSpaces™ Flex**：使用 Microsoft Azure 上由 Citrix 管理的基础设施，为开发人员、数据分析师和 AI 代理提供基于角色的工作区。请参阅 Citrix SecurSpaces Flex。
- **Citrix Experience Insights Flex**：Citrix Experience Insights Flex 帮助组织更快地将工作区遥测数据转化为可操作的洞察，涵盖体验、性能、运营弹性以及安全用例。通过 Citrix 管理的分析模型交付，并由 Splunk 提供支持。

随着时间的推移，可能会通过 Citrix Platform Flex 交付其他平台服务，利用相同的平台基础来实现安全性、运营和使用。

概念和术语

Flex 点数

购买 Citrix Platform Flex 的客户获得了一定数量的许可点数，也称为 **Flex 点数**。Flex 点数具有灵活性，可用于消费上述可用服务。请参阅下表，了解与每个角色相关的点数。

角色

Citrix Platform Flex 采用基于角色的计算方法，以便轻松定义员工配置文件。角色由虚拟应用或桌面交付模型定义，并根据 Citrix 的最佳实践进行预配置。可以配置自定义角色，以使 Citrix DaaS Flex 适应不同的用户要求。

Citrix Platform Flex 的服务和角色定义如下：

类别	服务	角色	版本	描述	CITRIX 交付模型
Flex 服务	Citrix DaaS 灵活	任务工作者（轻量级）	v1	适用于日常基本生产力、网页浏览和轻量级基于云的 SaaS 应用程序。	每个 VDA 16 个用户的多会话虚拟应用程序。8 个 vCPU，32 GB RAM，128 GB 存储。Windows Server 操作系统，RDS
		任务工作者（中等）	v1	与大多数现代企业员工的使用情况相符。现代	多会话虚拟应用程序，每个 VDA 8 个用户。8

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

类别	服务	角色	版本	描述	CITRIX 交付模型
				员工的应用程序需求通常是 SaaS 和企业应用程序的组合。	个 vCPU，32 GB RAM，128 GB 存储。Windows Server 操作系统，RDS
		任务工作者（重度）*	v2	适用于需要频繁访问企业应用程序以完成任务的用户。	多会话虚拟应用程序和桌面，每个 VDA 4 个用户。8 个 vCPU，32 GB RAM，128 GB 存储（非持久性）。Windows Server 操作系统，RDS
		知识工作者（轻度）	v1	专为标准管理任务、轻度多任务处理和核心基于 Web 的通信工具而设计。	单会话虚拟桌面。2 个 vCPU，8 GB RAM，128 GB 存储。BYOL Windows 11
		知识工作者（中等）	v1	适用于仅在虚拟桌面环境 (VDI) 中工作的用户。适用于高度安全的用例、呼叫中心或寻求采用瘦客户	单会话虚拟桌面。4 个 vCPU，16 GB RAM，128 GB 存储。自带许可证 Windows 11

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

类别	服务	角色	版本	描述	CITRIX 交付模型
				端或零客户端的组织。	
		知识工作者（重度）	v1	专为运行多个并发业务应用程序、大型电子表格和数据分析的高级用户而设计。	单会话虚拟桌面。8 个 vCPU，32 GB RAM，128 GB 存储。自带许可证 Windows 11
		知识工作者（超重度）	v1	针对需要大量内存、大型数据集和繁重本地处理的复杂多任务工作流进行了优化。	单会话虚拟桌面。8 个 vCPU，64 GB RAM，128 GB 存储。BYOL Windows 11
		强力工作者 (GPU)	v1	适用于对图形要求较高的用户，例如从事人工智能 (AI)、机器学习或数据可视化工作的用户。	启用 GPU 的单会话虚拟桌面。6 个 vCPU，55 GB RAM，4 GB GPU (A10)，128 GB 存储。BYOL Windows 11
		强力工作者 (非 GPU)	v1	专为 CPU 密集型计算、代码编译和无需专用图形渲染的数据处理而设计。	单会话虚拟桌面。16 个 vCPU，64 GB RAM，128 GB 存储。BYOL Windows 11

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

类别	服务	角色	版本	描述	CITRIX 交付模型
	思杰安全空间弹性版	开发人员（轻量级）	v1	适用于轻量级开发、脚本编写、代码审查和短期工作区，用户需要安全访问源代码、工具和依赖项，但计算要求不高。非常适合从事小型服务、文档、自动化任务或偶尔开发活动的开发人员、承包商和技术用户。	具有 2 个 vCPU、8 GB RAM 和 32 GB 存储的 Linux 容器
		开发人员（中等）	v1	适用于日常应用程序开发、测试和调试，用户需要具有额外 CPU、内存和存储容量的平衡工作区。非常适合使用标准 IDE、构建工具、应用程序运行时和中等规模存储库的全职开发人员。	具有 4 个 vCPU、16 GB RAM 和 64 GB 存储的 Linux 容器

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

类别	服务	角色	版本	描述	CITRIX 交付模型
		开发人员（重型）	v1	适用于计算密集型开发、大型存储库、复杂构建、本地测试环境和高级工作负载，这些工作负载需要更高的性能和更大的工作区容量。非常适合高级开发人员、平台工程师、数据工程师以及运行要求苛刻的开发工具链或频繁构建和测试周期的团队。	Linux 容器，8vCPU，32 GB RAM，128 GB 存储
同上	Citrix 体验洞察 Flex	所有	v1	为企业所有平台上的最终用户体验和安全性提供可操作的洞察。	数字员工体验 (DEX)。可选择添加安全功能以获取额外积分。
SaaS	Citrix 安全访问与 Chrome 企业版	所有	v1	适用于日常使用 Chrome Enterprise Premium 访问 Web 或 SaaS 应用	CSA 与 CE 功能作为 DaaS Flex 的附加组件或独立使用

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

类别	服务	角色	版本	描述	CITRIX 交付模型
				程序的用户。	
仅限软件	Citrix DaaS (本地部署或云端)	全部	v1	客户自托管选项。	客户定义。存储不适用

注意：

- *Citrix 将在即将发布的版本中弃用任务工作者（重型）角色。请为即将推出的计算机目录使用其他可用的 Flex 角色。
- 所示的积分适用于非持久性池化工作负载。持久性专用工作负载会产生额外的附加费用，具体请参见附加选项部分。

附加选项

Citrix Flex 提供了灵活性，可根据最终用户的需求自定义工作负载。附加选项定义为与 Flex 角色结合使用的可选功能或服务。

思杰 DAAS FLEX

每个角色的可选磁盘大小和类型由映像中使用的磁盘决定。其相应的 Flex 积分成本定义如下：

描述	大小
单会话持久性角色的磁盘成本	128 GB 标准 SSD 磁盘
	256 GB 标准 SSD 磁盘
	512 GB 标准 SSD 磁盘
	1024 GB 标准 SSD 磁盘
	128 GB 高级 SSD 磁盘
	256 GB 高级 SSD 磁盘
	512 GB 高级 SSD 磁盘

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

描述	大小
	1024 GB 高级 SSD 磁盘
多会话非持久性用户配置文件的磁盘成本	128 GB 高级 SSD 磁盘

服务

请参阅以下 Citrix Platform Flex 服务文档：

- 思杰 DaaS Flex
- 思杰 SecurSpaces Flex
- 思杰体验洞察灵活版

平台 Flex 积分消耗和报告

Flex 积分根据您在“角色”部分定义的 Flex 服务每月消耗。其他服务不消耗 Flex 积分。每月 Flex 积分消耗报告可帮助您了解整体使用模式。

按服务计算消耗量

- **Citrix DaaS Flex（托管容量角色）**：这适用于 Citrix 托管容量角色（例如，任务工作者（重度、中度）、知识工作者、高级工作者、自定义角色）以及相关的附加组件，例如用于持久性桌面的磁盘。消耗量基于每个角色配置的唯一用户数量。即使从未主动使用，配置的角色也会消耗 Flex 积分。目录创建和容量增加按月按比例计算，而容量减少和删除则不按比例计算。如果目录创建失败，则不消耗 Flex 积分。

  示例：100 个任务工作者用户 × 任务工作者 Flex 积分值 = 每月扣除的 Flex 积分总数。

  > **注意：**
  >
  > 为保持效率，这些实例在不活动期间可能会休眠。Azure 中的典型恢复时间少于五分钟。

- **Citrix SecurSpaces™ Flex（托管容量角色）**：这适用于 Citrix 托管容量角色（例如，开发人员（轻度、中度、重度））。消耗量基于每个角色配置的唯一工作区数量。即使从未主动使用，配置的角色也会消耗 Flex 积分。Citrix SecurSpaces 工作区创建和容量增加按月按比例计算。如果 SecurSpaces 工作区创建失败，则不消耗 Flex 积分。

  示例：100 个开发人员（中度）用户 × 开发人员（中度）Flex 积分值 = 每月扣除的 Flex 积分总数。

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

- **Citrix Experience Insights Flex**：消耗量基于唯一用户数量。即使用户未主动加入，每个指定的用户数量也会消耗 Flex 积分。用户增加按月按比例计算。

  示例：

  - 10,000 个用户体验用户 × 用户体验积分 = 每月扣除的 Flex 积分总数。
  - 10,000 个用户体验 + 安全用户 × 用户体验 + 安全积分 = 每月扣除的 Flex 积分总数。

- **Citrix DaaS Cloud/Local（自带基础设施）**：这适用于使用 Citrix Virtual Apps and Desktops 或 Citrix DaaS 并采用自带基础设施部署模型的客户。消耗量按每个唯一用户计算，无论他们访问多少服务。即使单个用户同时使用 Citrix Virtual Apps and Desktops 和 Citrix DaaS，也只算作一个用户。当月部分使用不按比例计算。

  示例：1,000 个用户 × 每用户 Flex 积分值 = 每月扣除的 Flex 积分总数。

- **Citrix Secure Access with Chrome Enterprise (CSA with CE)**：消费严格按照唯一用户计算。当月部分使用不按比例计算。

> **注意：**
>
> Flex Credit 将每月从您的许可总单位中扣除，这在《业务部门条款和条件》中称为 **Flex Credit 配额**。

附加条款

- **调整**：如果您认为需要调整 Flex Credit，则必须提交支持工单。Citrix 将进行调查并确定适当的后续步骤。
- **暂停**：如果您已用完所有许可金额，或者剩余的 Flex Credit 余额不足以支付您所需的使用量，则无法使用基于 Flex Credit 的服务。
- **到期**：在订阅期内未使用的任何 Flex Credit 将在您的订单中指定的期限结束日期到期。

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

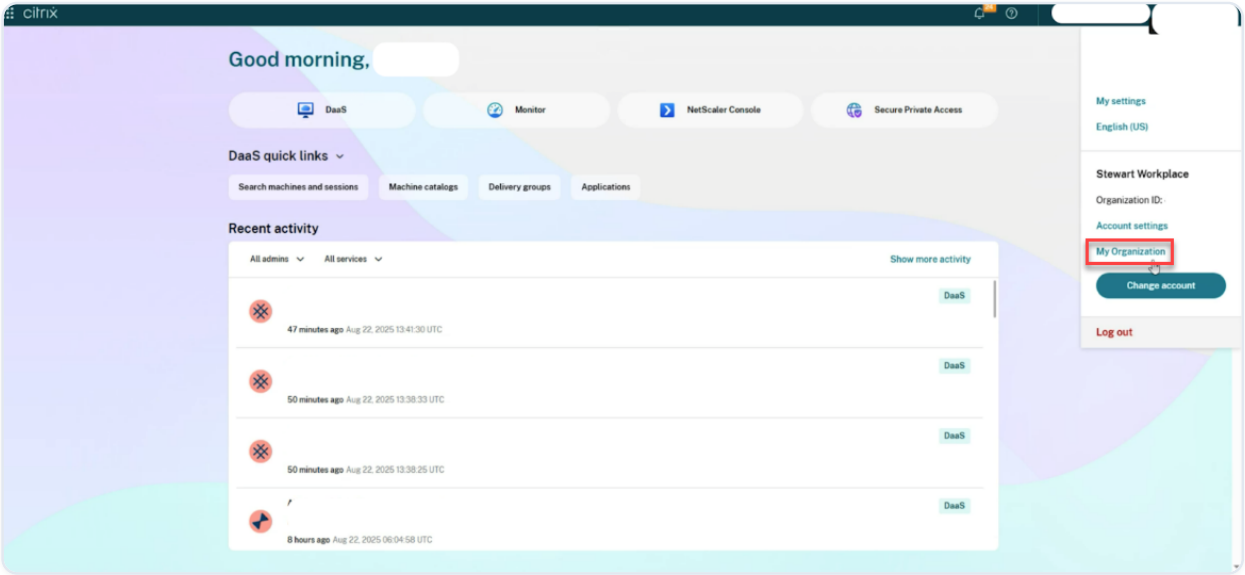
管理 Citrix Cloud

Citrix Cloud™ 账户管理

本文将引导您完成 Citrix Cloud 账户的入驻流程以及账户的许可证管理。

创建 Citrix Cloud 账户

1. 在 Citrix **Cloud** 控制台中，在**配置文件菜单**中，单击 我的组织 以开始。



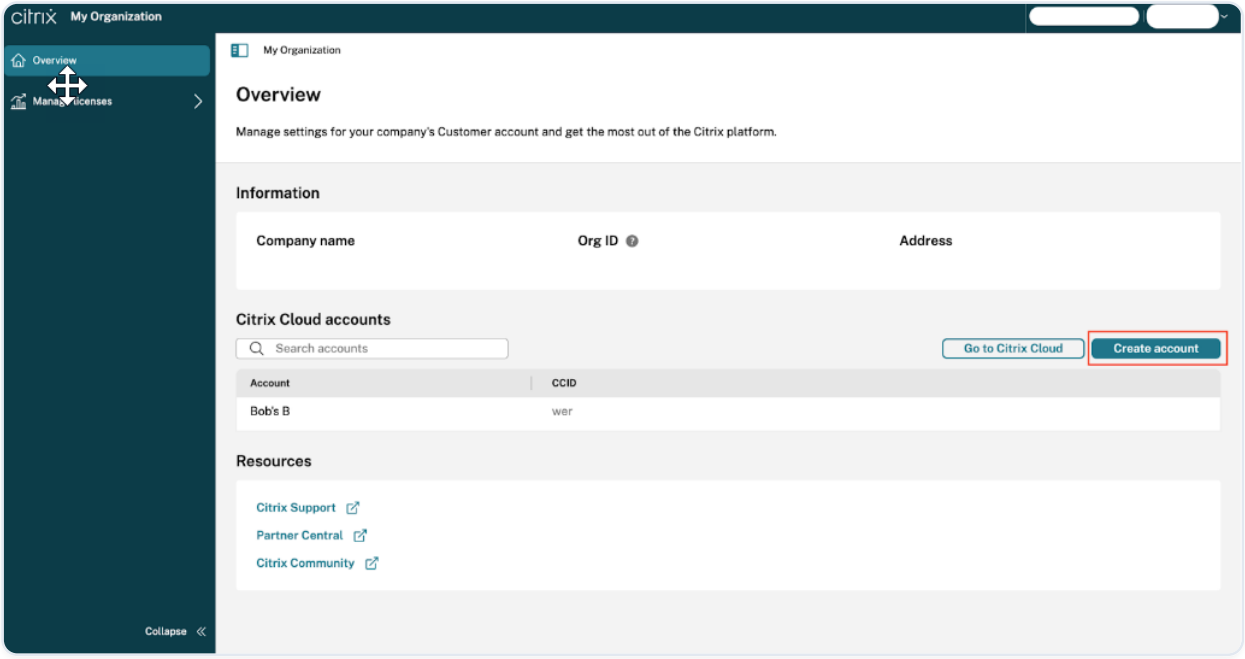
> **注意：**
>
> 如果您没有看到 我的组织 选项，则表示您没有访问它的正确权限。请请求您的 MyCitrix 账户 管理员将您添加为管理许可证的正确管理员。有关详细信息，请参阅 支持链接。

如果您是现有的 Citrix 客户但没有 Citrix Cloud 账户，请访问 我的组织 并按照 Citrix Cloud 账户管理 中的步骤入驻云租户。

如果您是 Citrix® 新用户，请联系客户代表注册以创建您的 OrgID。

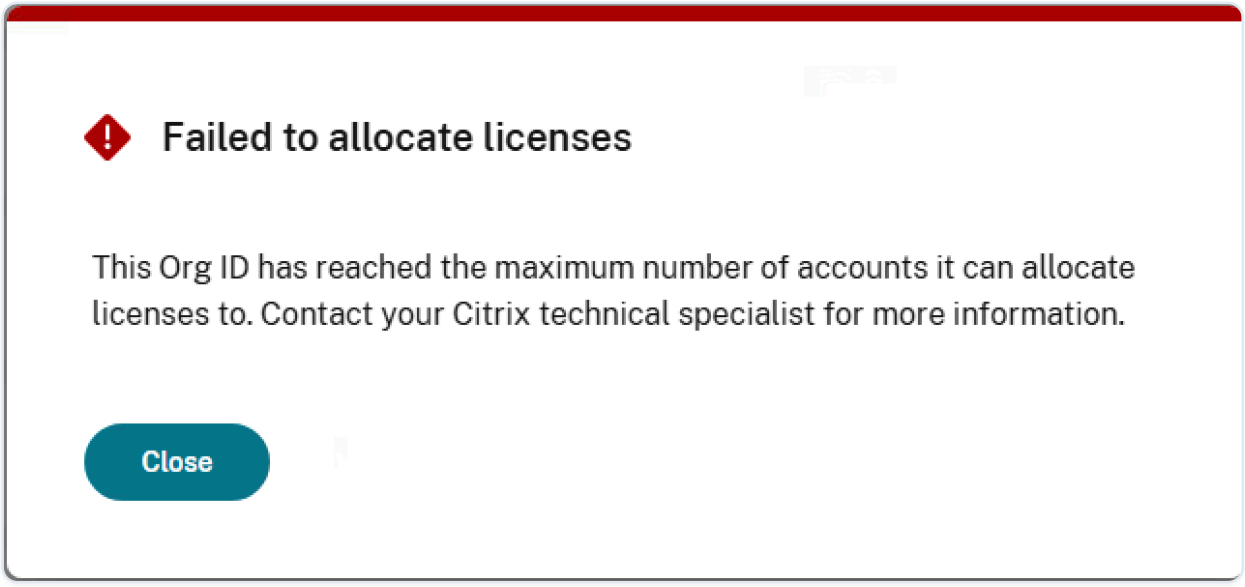
2. 在 我的组织 主页上，单击**创建账户**。

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



注意：

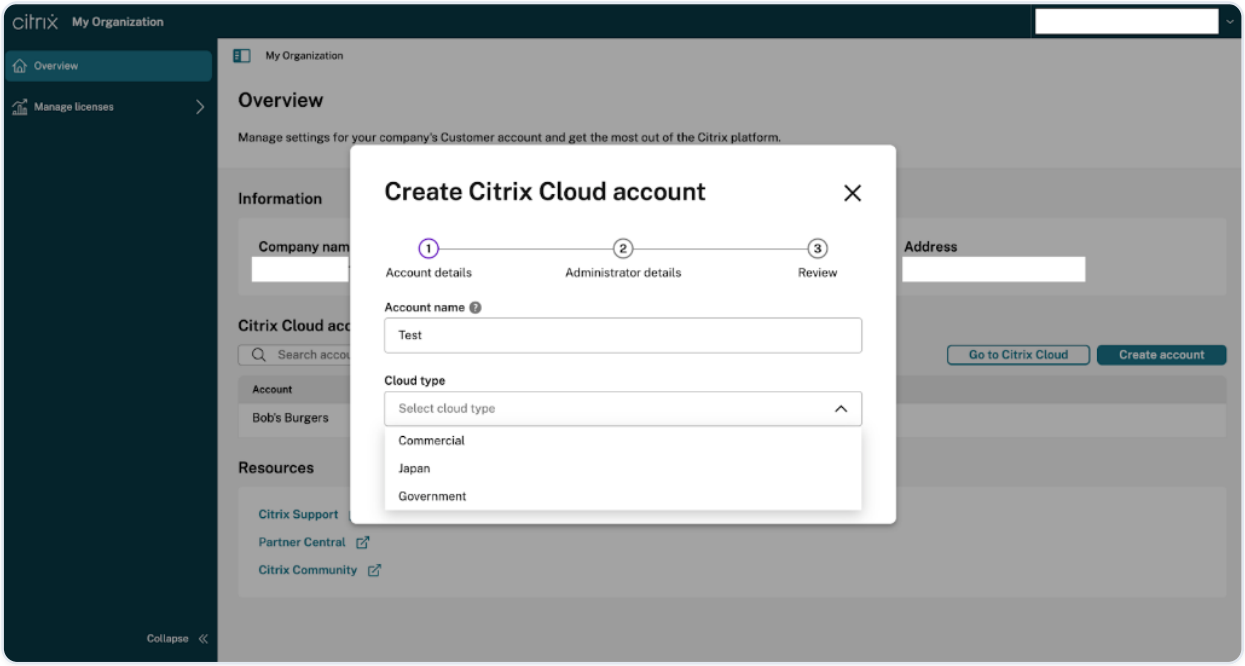
Citrix 客户可以在 我的组织 中独立创建新的云租户并管理许可证。如果您在将许可证分配给已入驻的云租户时看到以下消息，则表示您已达到根据您的总许可证数量可以分配许可证的最大账户数。有关详细信息，请联系您的 Citrix 联系人。



Citrix 合作伙伴 只能从 我的组织 入驻其第一个合作伙伴 Citrix Cloud 账户。要入驻任何新客户，请参阅 我的客户控制板。

3. 输入**帐户名称**，从下拉列表选项中选择**云类型**，然后单击**下一步**。

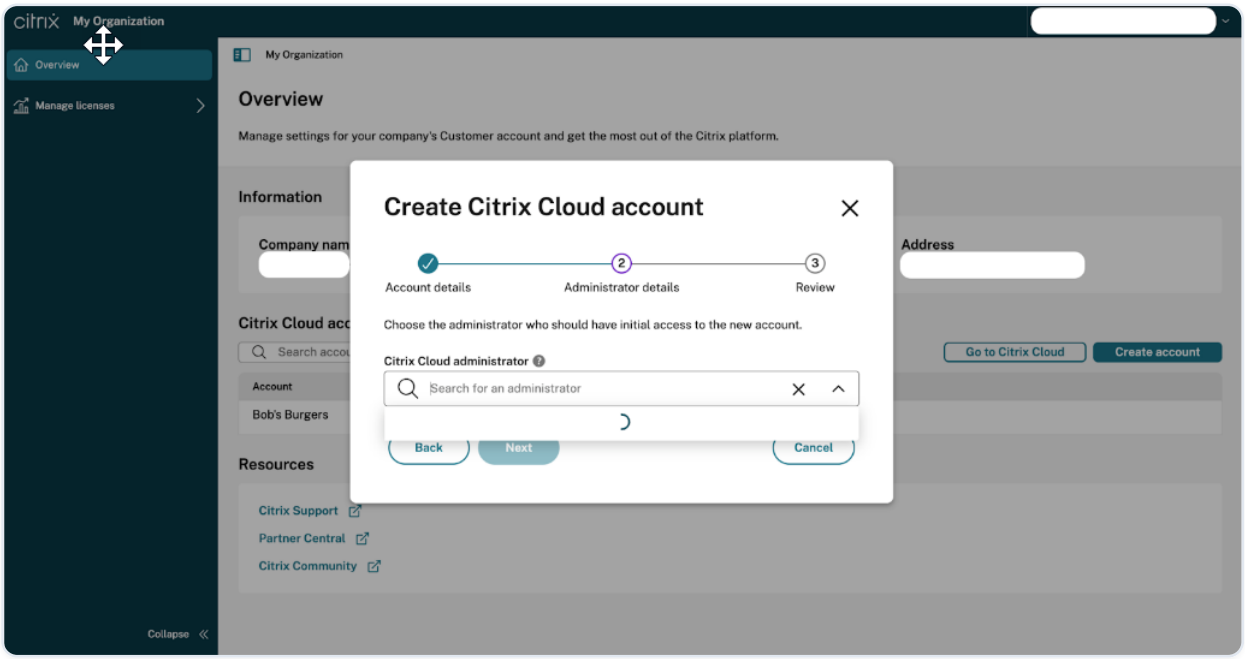
© 1997–2026 Citrix Systems, Inc. All rights reserved.



注意：

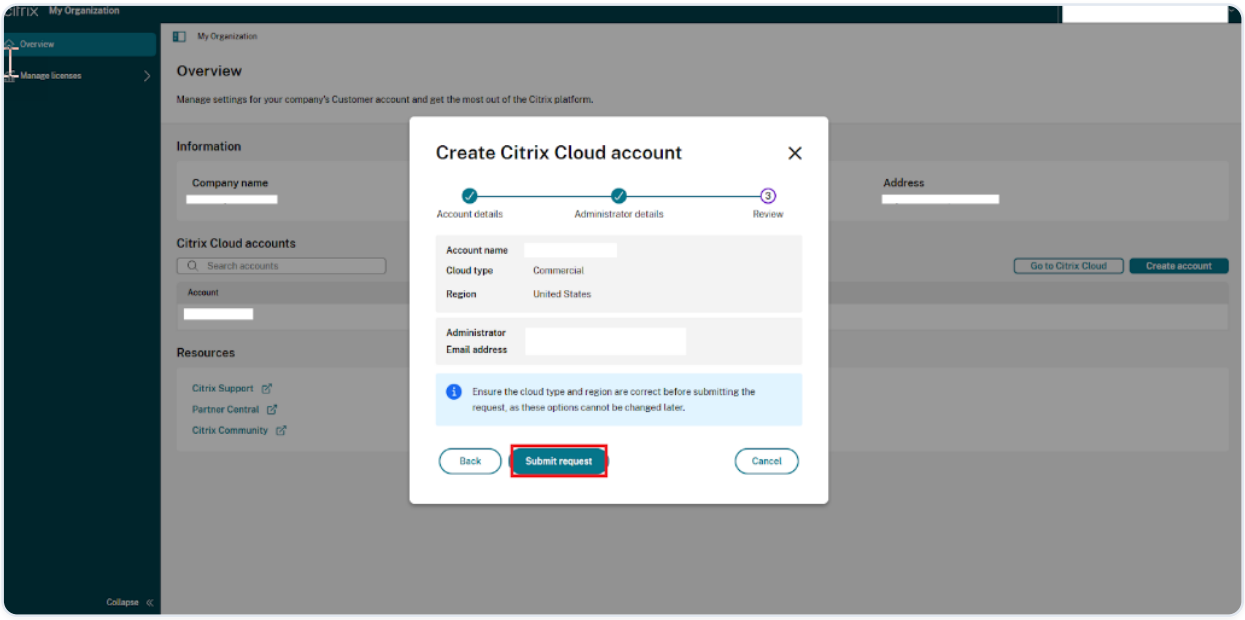
可用的云类型选项包括政府、日本和商业。

4. 选择应具有帐户初始访问权限的 **Citrix Cloud 管理员**。此管理员将收到初始登录信息。然后单击**下一步**。

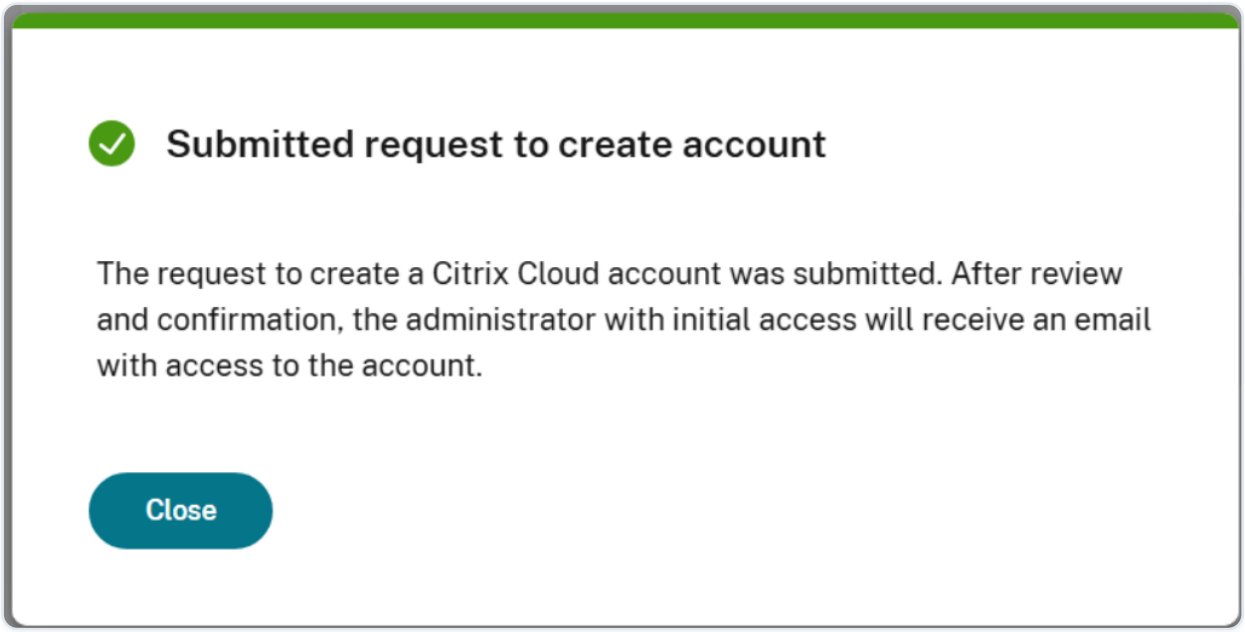


5. 确认**帐户名称**、**云类型**和**管理员**详细信息，然后单击**提交请求**。

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



6. 您会看到一个弹出消息，指出帐户已成功创建。



注意：

如果创建 Citrix Cloud 帐户的提交失败，请联系客户支持团队寻求帮助。

许可证管理

A. 云许可证管理

许可证分配

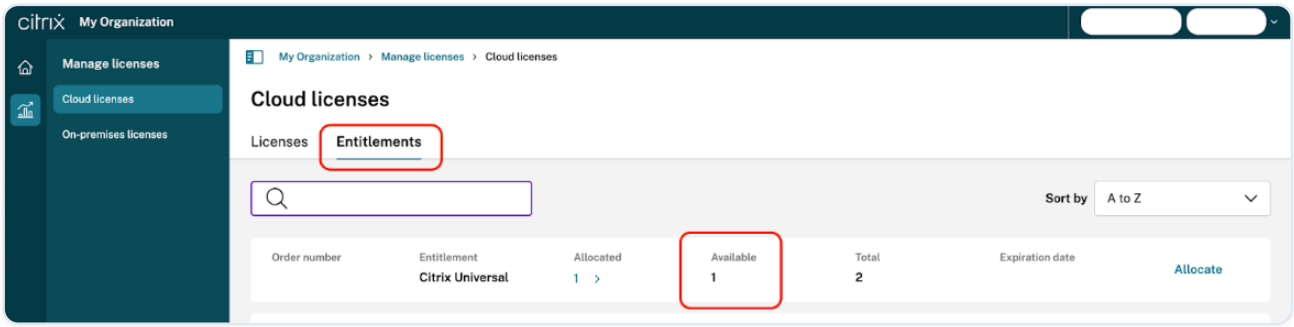
用户现在可以将其许可证分配给其 Citrix Cloud 客户帐户。

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

注意：

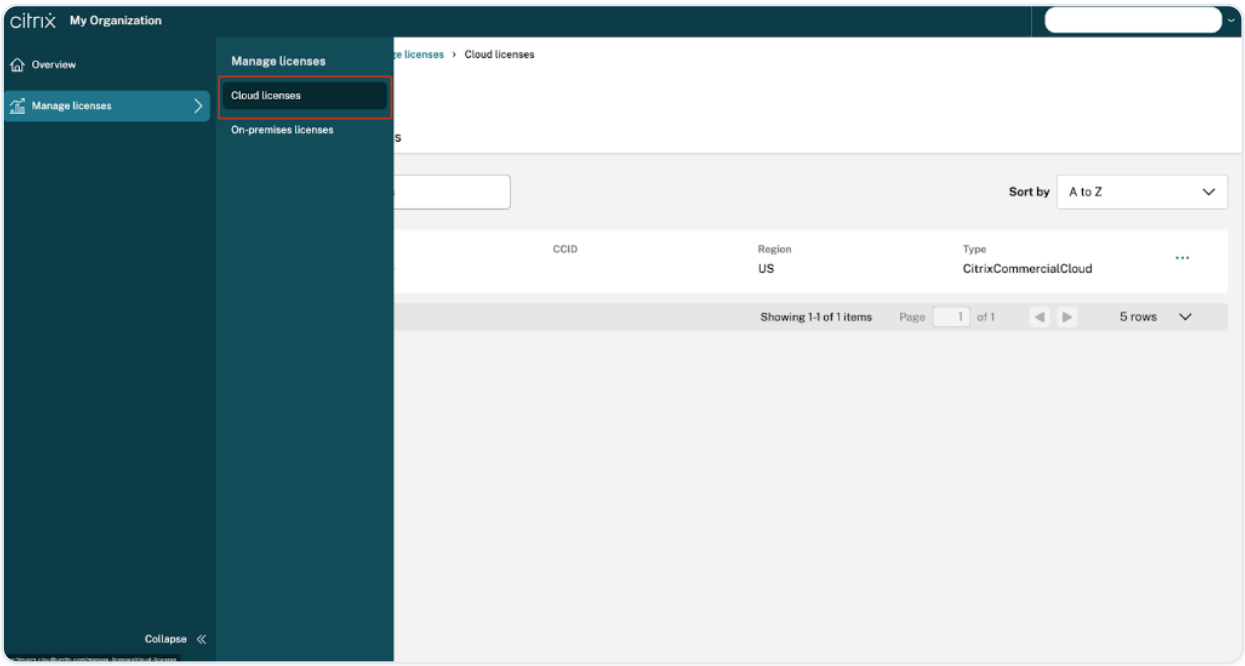
不支持从旧版许可证模型（不包括 UHMC 和 CPL）跨不同控制平面（例如政府、日本和商业）分配许可证。

确保您拥有可分配给 Citrix Cloud 帐户的所需许可证。请从 **我的组织 > 管理许可证 > 云许可证 > 权利** 中检查。否则，通过从合适的权利中执行解除分配来使许可证可用。有关解除分配步骤的更多信息，请参阅 许可证解除分配 部分。



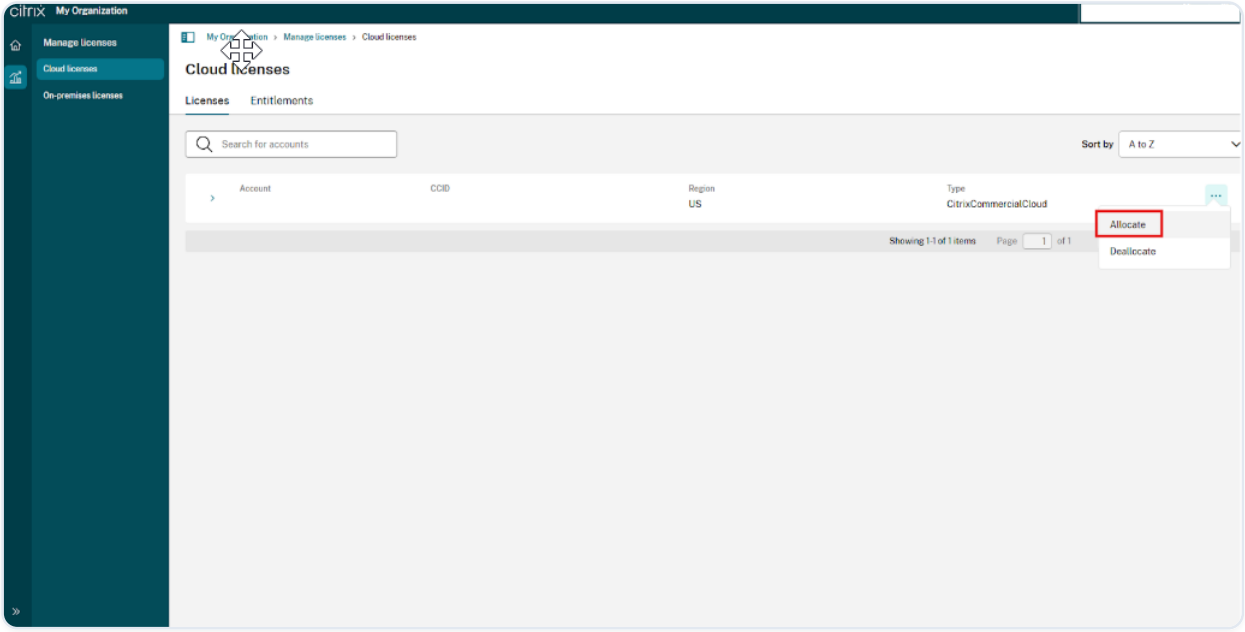
要将许可证分配给帐户，请执行以下步骤：

1. 导航到 **管理许可证** 部分，然后单击 **云许可证**。

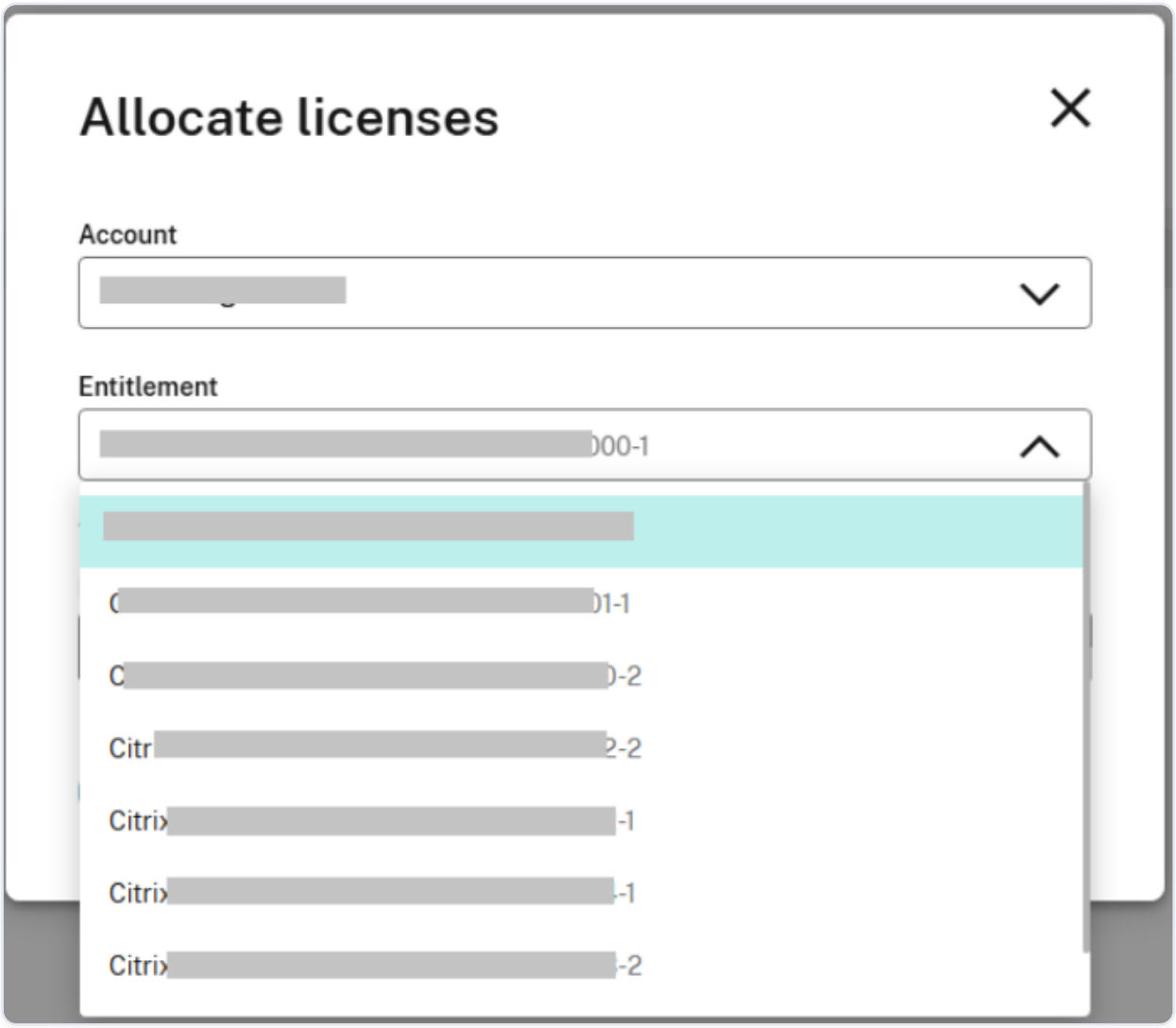


2. 单击新帐户的省略号，然后选择 **分配**。

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

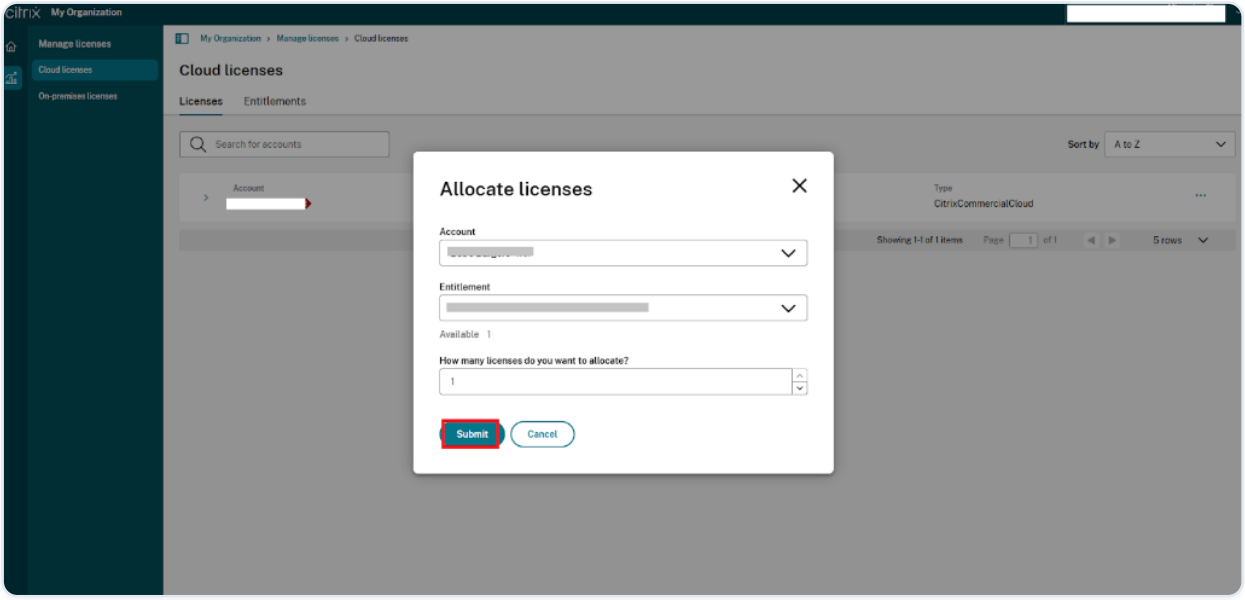


3. 从下拉列表选项中的可用列表中选择 **权利**。

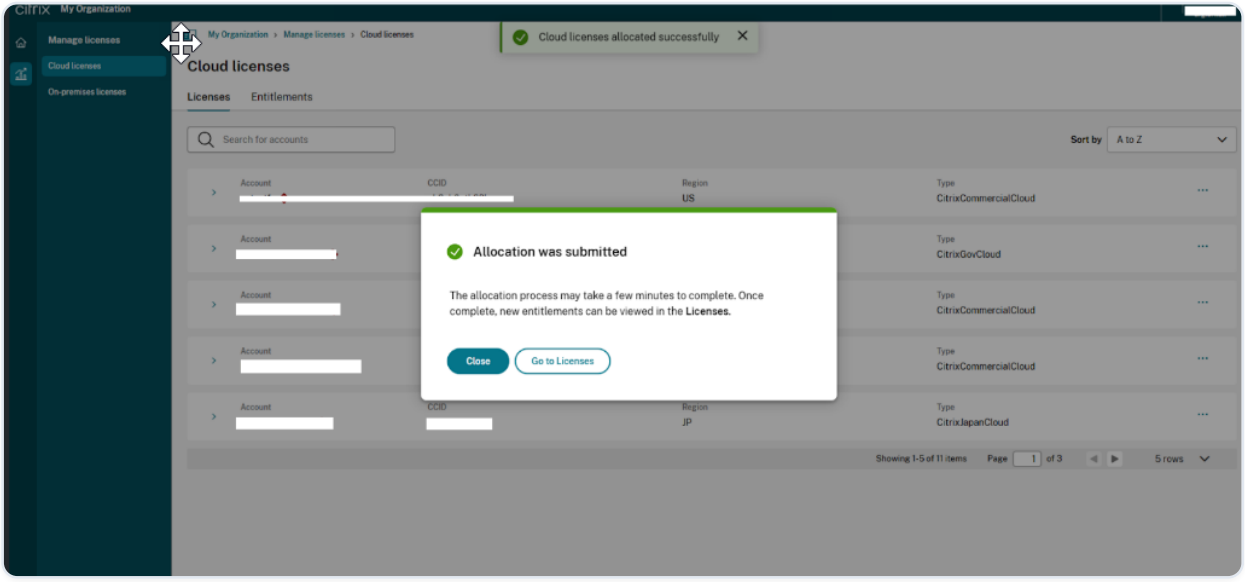


4. 指定要在帐户级别分配的每个产品的数量，然后单击 **提交**。

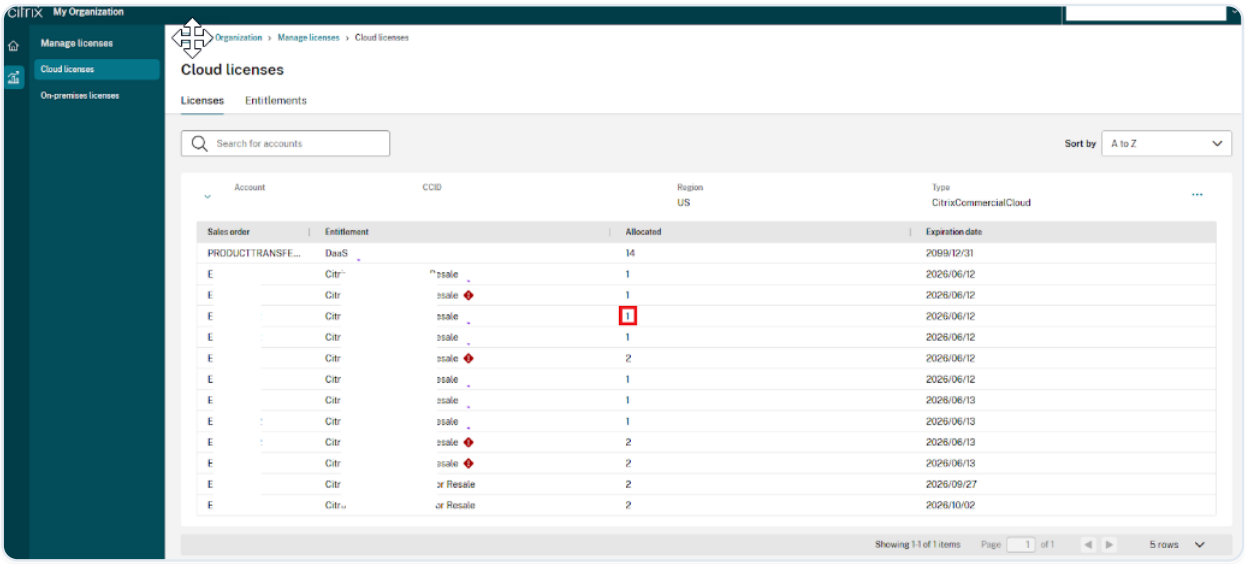
© 1997–2026 Citrix Systems, Inc. All rights reserved.



5. 成功提交分配请求后，单击 **关闭**。



6. 要验证分配，请从 **管理许可证** > **云许可证**，展开帐户以查看分配后的数量。



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

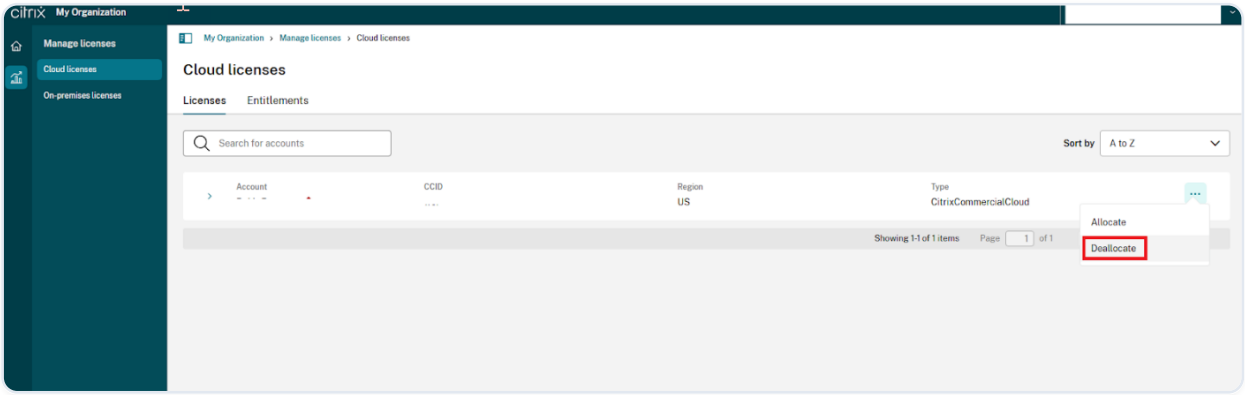
注意：

完成此过程后，分配将在数小时内进行，以启用所有服务并将许可证分配给帐户。在此期间，客户会看到一个指示处理状态的图标。分配完成后，该图标将消失，客户可以继续进入云管理员控制台并开始使用服务。如果分配失败，请联系 Citrix 客户支持寻求帮助。

许可证解除分配

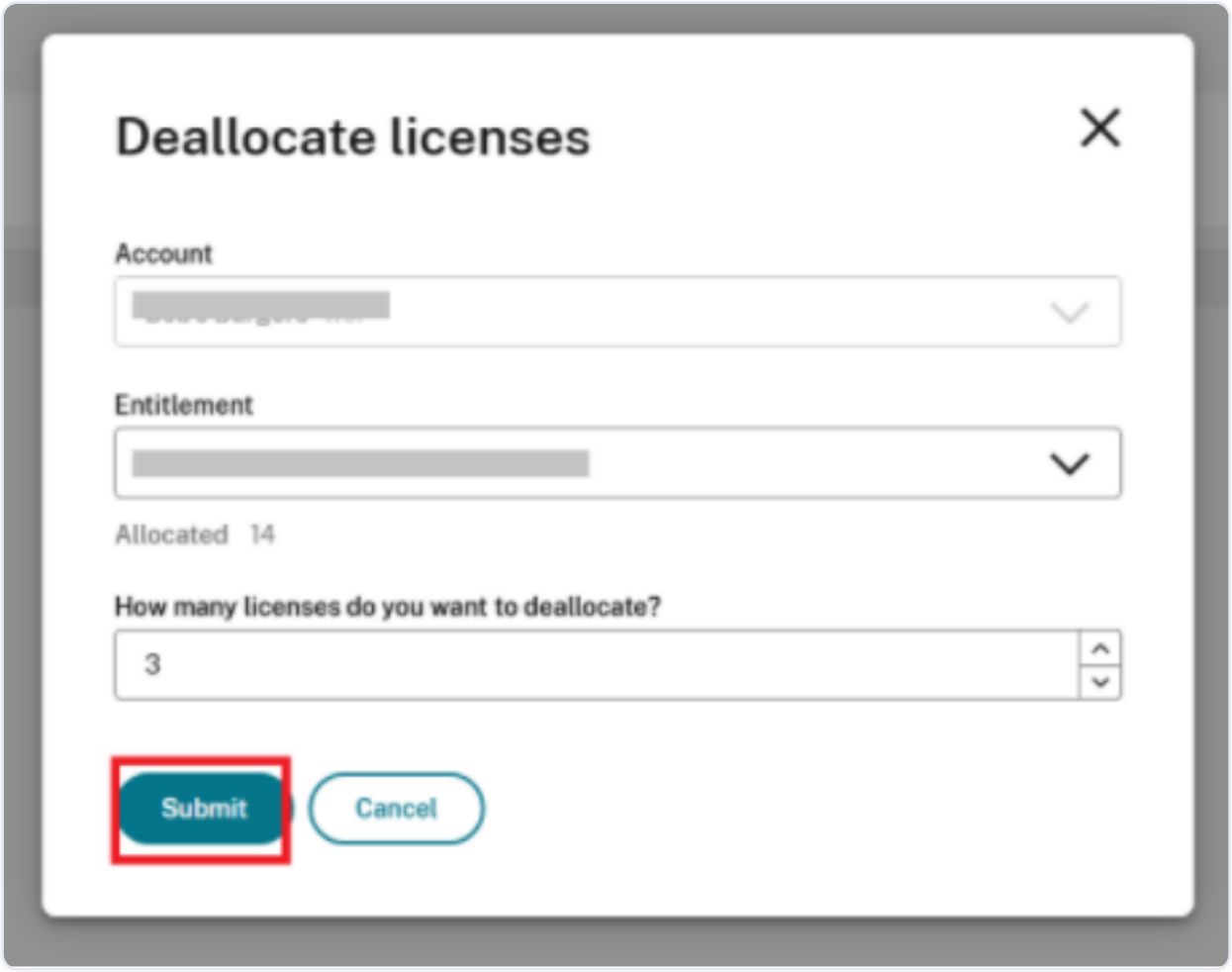
要从帐户解除分配许可证，请使用以下步骤：

1. 导航到 **管理许可证** 页面并单击 **云许可证**。
2. 单击新帐户的省略号并选择 **解除分配**。

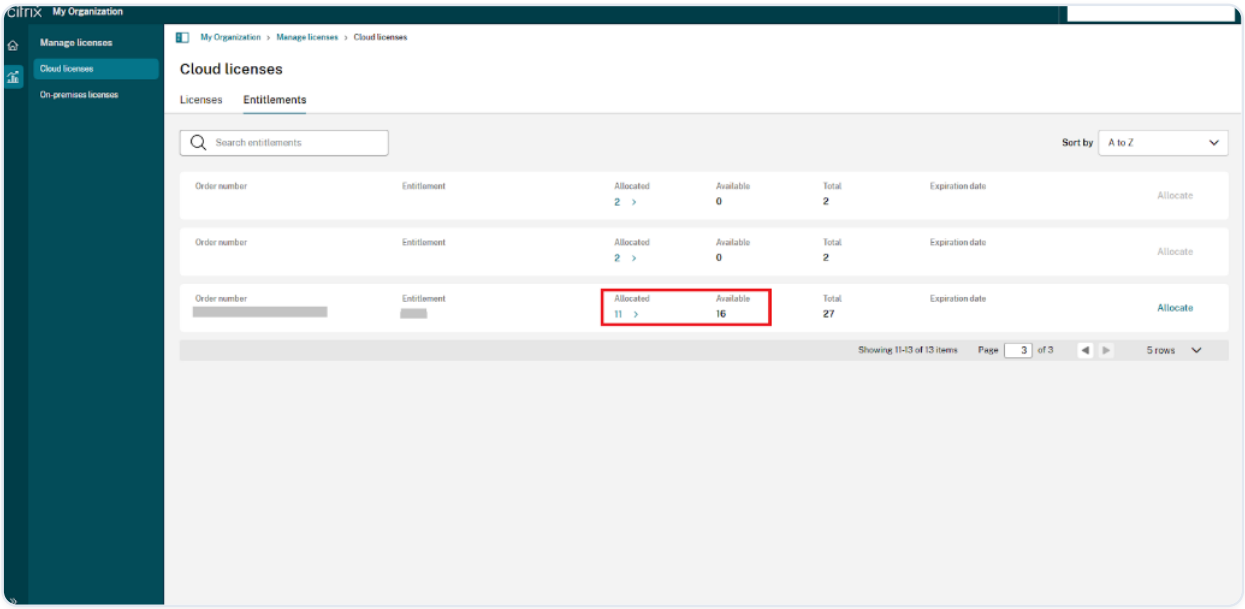


3. 从下拉列表中选择 **帐户**。确保选择正确的帐户。
4. 从下拉列表中选择 **权利**，在 **数量** 选项卡中输入要解除分配的许可证数量，然后单击 **提交**。

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



5. 验证解除分配。从 **管理许可证** > **云许可证>权利**，展开帐户以查看解除分配后的数量。



已知问题

产品重复 (管理许可证 > 云许可证) 客户可能会遇到与单个销售订单关联的具有相同许可证数量的重复产品记录。这些重复项可能会显示在“权益”下 **(管理许可证 > 云许可证 > 权益)**，或者直接分配到其

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

Citrix Cloud 帐户。因此，客户可能会被错误地授权使用“创建帐户”按钮创建额外的 Citrix Cloud 帐户，或者将重复产品中的额外许可证分配给新的 Citrix Cloud 帐户。

建议 这是一个已知问题，Citrix 正在积极通过删除不符合条件的重复订单来解决此问题。如果客户创建云租户并对这些租户执行许可证分配或取消分配，Citrix 即将推出的修复程序可能会影响其服务。因此，如果客户遇到这种情况，他们应联系 Citrix 客户服务团队，以验证其创建新 Citrix Cloud 租户的资格，并确保他们拥有云租户创建和/或任何许可证分配或取消分配的正确权限。

更名订单 客户可能会在 **管理许可证** 中注意到更名产品的多个分配。原始产品分配与两到三个附加产品一起出现，所有这些产品都共享许可证数量、到期日期和销售订单。

如果客户看到同一资产有多个分配，且这些分配具有相同的许可证数量和到期日期，则可以识别更名订单。所有重复分配都将“DaaS”显示为产品名称。客户可以通过以下方式检查他们是否有更名订单：

- 在 **管理许可证 > 云许可证 > 权益** 中查看其购买的资产，并将其与列出的可分配软件包进行比较。
- 通过检查浏览器中的网络跟踪，您可以在分配列表中看到遵循 `<Random_GUID>-<OrderId>` 模式的多个 ID，其中 `OrderId` 重复，但 `Random_GUID` 不重复。

建议 这是一个已知问题，Citrix 正在积极通过删除任何无效订单来解决此问题。在创建帐户之前，客户应遵循 创建 Citrix Cloud 帐户 中概述的步骤，以确保他们创建的是符合资格的帐户，并避免创建不符合资格的帐户。如果客户发现其帐户上有任何无效或重复订单，可以联系客户服务团队。此外，因无效订单资格而创建的任何 Citrix Cloud 客户实例都将被删除，这可能会影响客户运营。

自定义登录页面

许多管理员访问云控制台以执行特定任务，例如在 Web Studio 控制台中管理应用程序或在 DaaS 监控中查看数据。 然而，这些任务每次管理员登录时都需要多次点击并浏览多个页面，这可能非常耗时。这项新功能允许管理员设置或修改自定义登录页面，从而节省时间并提供增强的控制台体验。

目前，以下页面可配置为自定义登录页面，未来预计会添加更多页面：

- DaaS
- DaaS 监控
- NetScaler® 控制台
- CAS
- CAS 安全
- CAS 性能

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

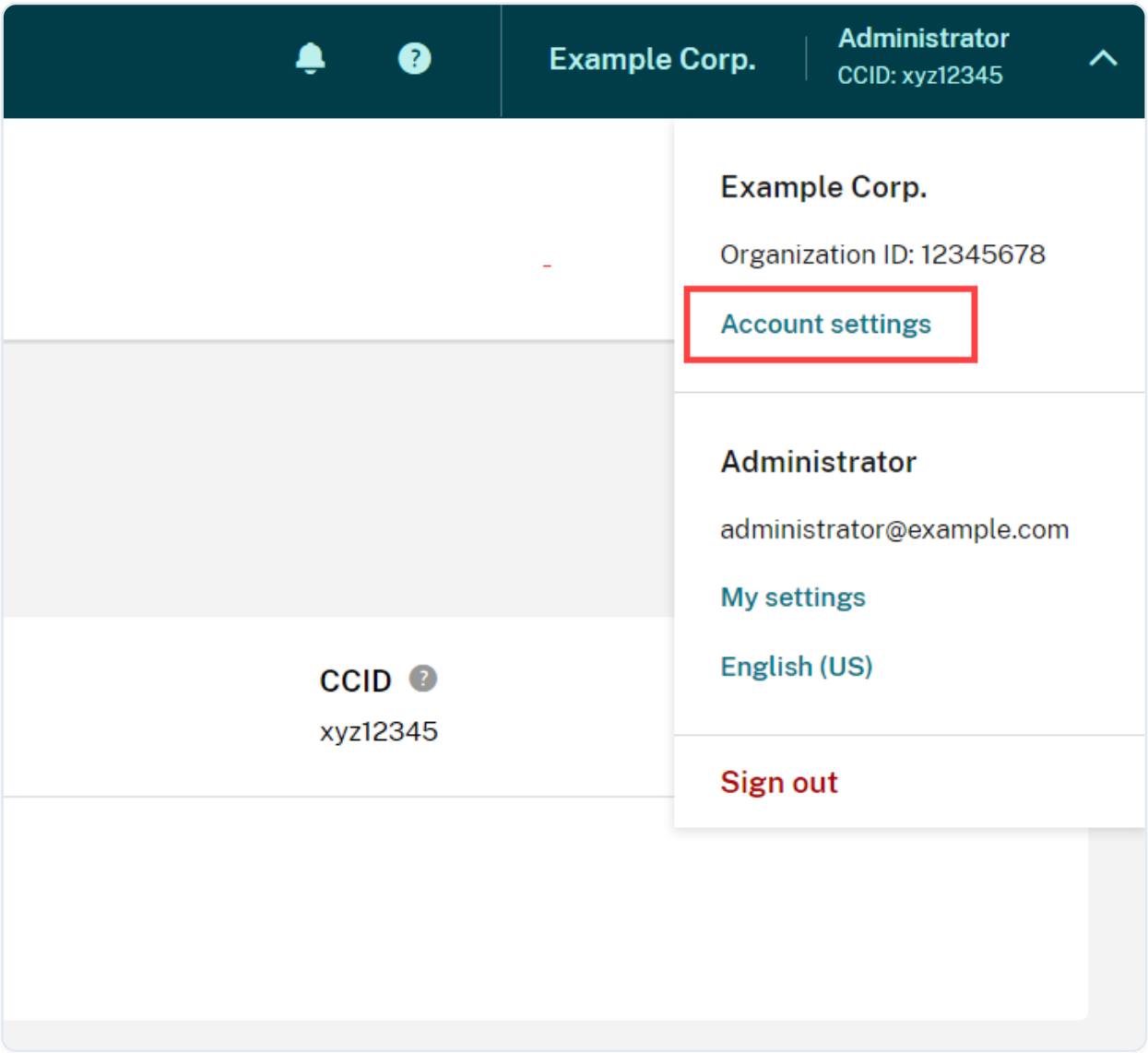
- WEM
- 常规

注意：

自定义登录页面设置是可选的，并且是按帐户设置的。因此，每个管理员都可以在 Citrix Cloud 中自定义自己的体验。所有管理员（无论是自定义管理员还是完全管理员）都可以访问此功能。

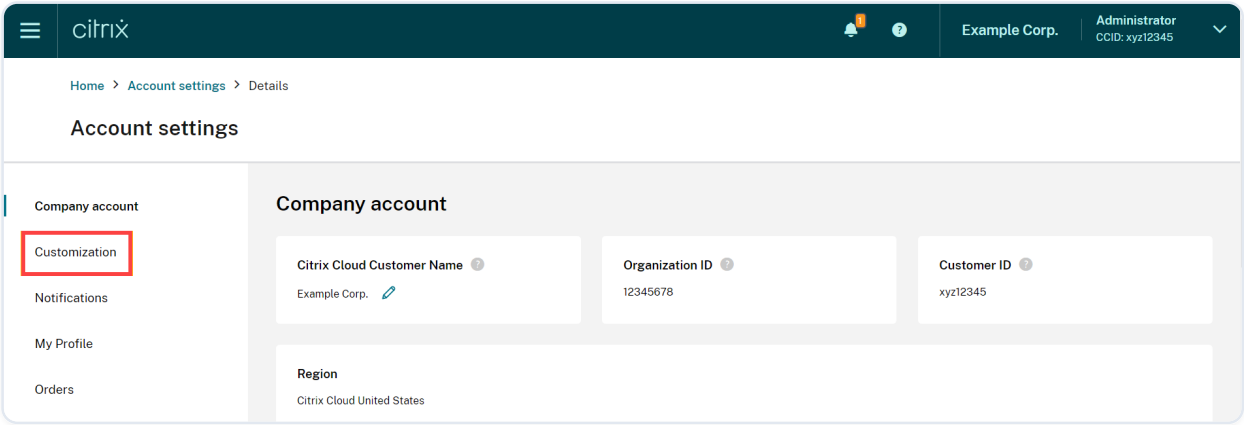
配置自定义登录页面

1. 单击配置文件名称并选择**帐户设置**。

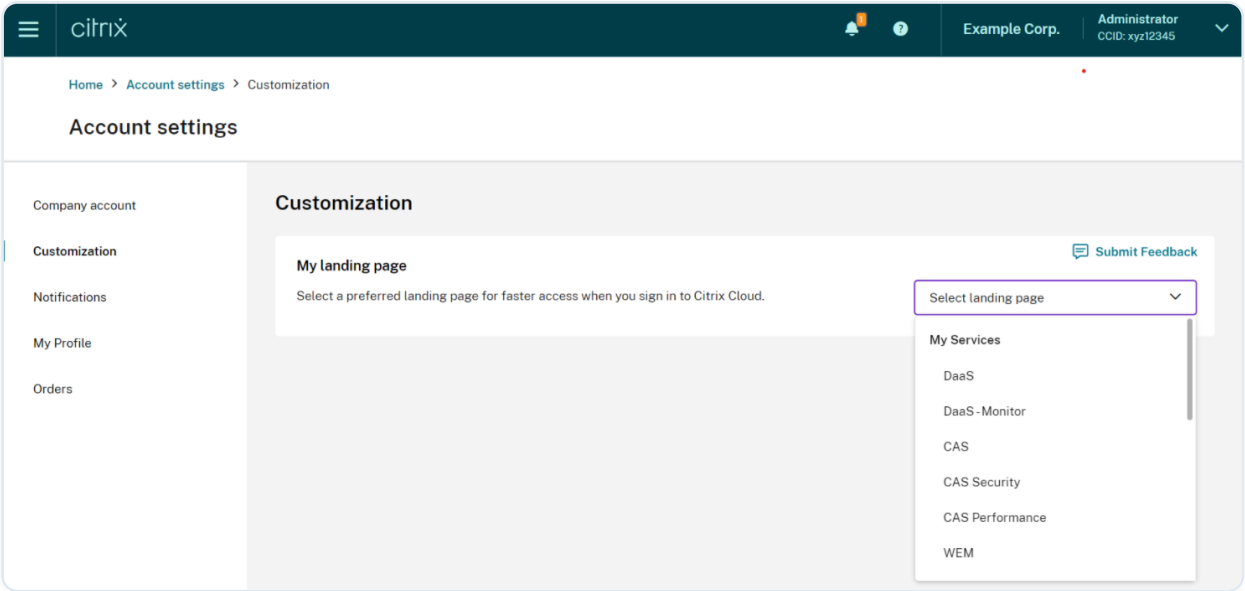


2. 单击 **自定义**。

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



3. 选择您要配置为自定义登录页面的服务。



4. 单击 **应用**。

   您的自定义登录页面现已设置完成。

注意：

- 您可以随时通过单击 **重置为默认值** 将自定义登录页面重置为默认的云主页。
- 如果您在刚刚注销的同一页面上再次登录，系统会将您带到上次查看的页面，而不是新的登录页面。

如何删除 Citrix Cloud™ 帐户并重新加入

Citrix Cloud 提供了让客户安全删除其 Citrix Cloud 帐户并在需要时无缝重新加入的功能。

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

先决条件

- 如果您的帐户具有活动的 DaaS 权利并且您的 DaaS 环境已预配，请在继续之前联系 Citrix 技术支持以执行 快速停用。有关如何检查您的 DaaS 环境是否已预配的详细信息，请参阅 Studio 控制台显示“启用 DaaS”以供首次使用 文章。
- 删除与此帐户关联的所有 Cloud Connector 和 Connector Appliance。
- 客户必须拥有其 Citrix Cloud 帐户的管理员访问权限才能执行删除请求。
  - 对于没有其 Citrix Cloud 帐户管理员访问权限的客户，必须在继续删除请求之前通过 SSAO 获取访问权限。
  - 如果只有一个管理员拥有访问权限，则该管理员必须删除其他管理员。
- 取消注册您的许可证服务器。如果您想将许可证服务器注册到不同的或新的 Citrix Cloud 帐户，请参阅 取消注册 以了解所需步骤。

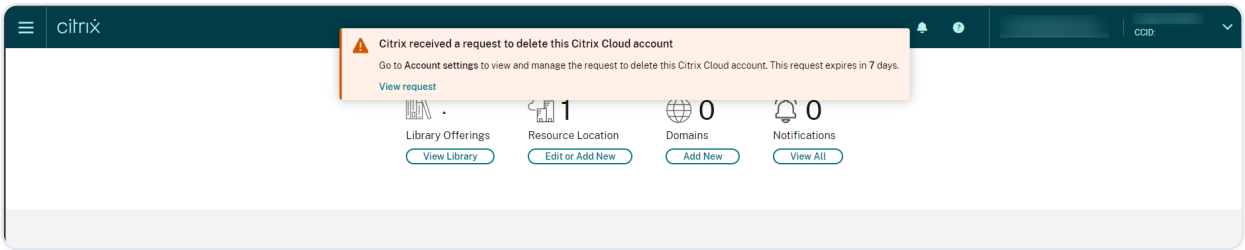
重要提示

在删除 Citrix Cloud 帐户之前，请考虑以下几点：

- 所有客户相关数据将从 Citrix® 数据库中删除。
- 所有与 Citrix Cloud 服务相关的资源，包括 Citrix 在您的云环境中预配的 Citrix 管理的虚拟机，都将被删除。有关特定 Citrix Cloud 服务中包含的 Citrix 管理组件的说明，请参阅 Citrix Cloud 服务。
- 管理员和用户对 Citrix Cloud 和服务的访问权限将被禁用。
- 正在积极使用服务的管理员或用户将遇到服务中断。
- 此操作不可逆。数据一旦删除，将无法恢复。

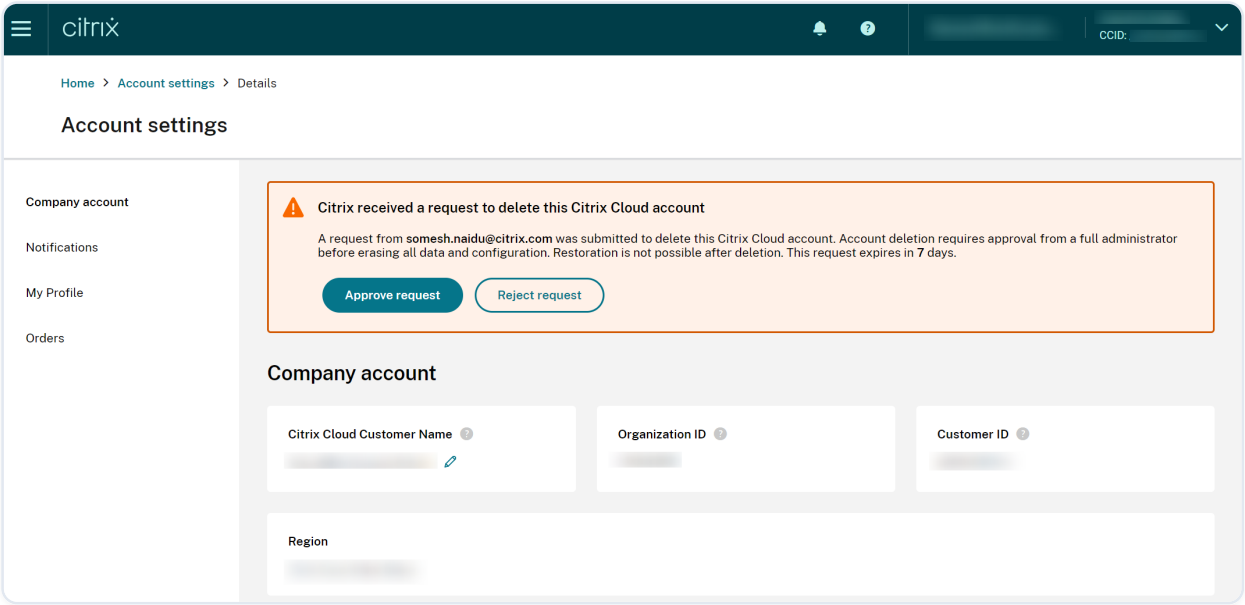
步骤

1. 联系 Citrix 客户服务 提交删除请求。Citrix Cloud 帐户上的 *完整管理员* 才能提交此请求。
2. 请求发起后，登录您的 Citrix Cloud 帐户。您将看到 Citrix Cloud 帐户删除工作流程。

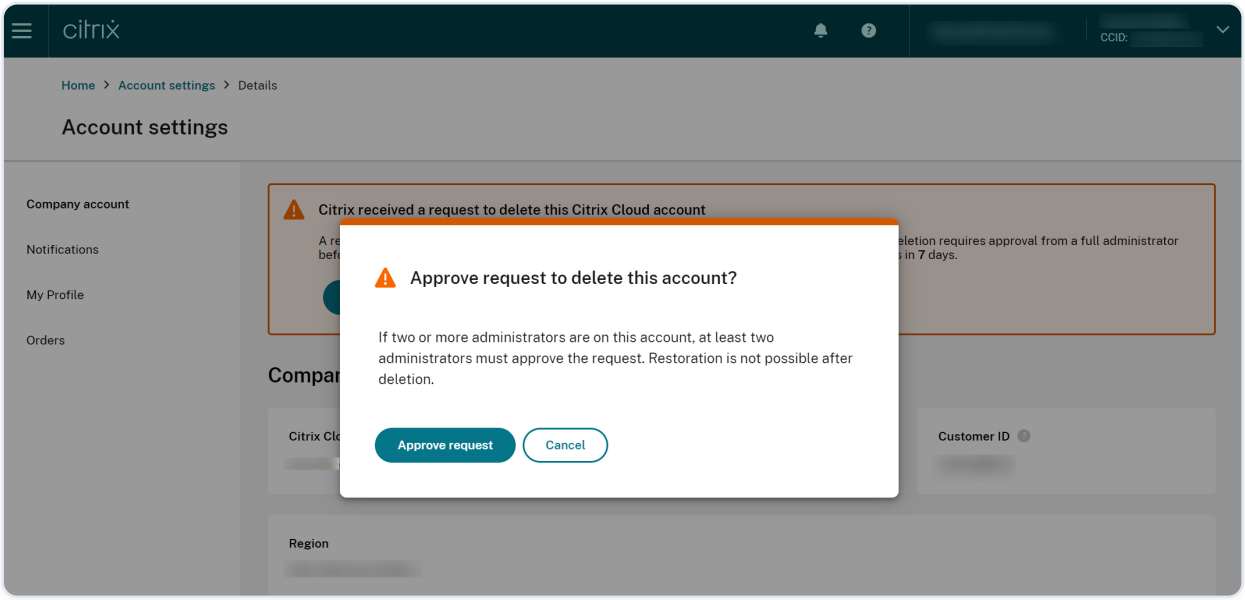


3. 按照屏幕上的指导批准或拒绝此请求。

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



4. 要批准此删除请求，请登录帐户，导航到 **帐户设置**，然后单击批准工作流程横幅上的 **批准请求**。



要取消删除请求，请登录帐户，导航到 **帐户设置**，然后单击删除批准工作流程横幅上的 **拒绝并移除请求**。

注意：

- 如果此帐户关联了两个或更多管理员，则至少需要两名管理员批准该请求。
- 如果未在 7 天内收到所需的批准，此请求将过期。

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

网络位置

在 Citrix Cloud™ 中，您可以根据公共 IP 地址配置网络位置。这些网络位置可用于以下目的：

- Citrix® StoreFront Cloud 使用网络位置来确定是指示客户端直接连接到 VDA 还是通过 Citrix Gateway 连接。有关详细信息，请参阅 连接到 DaaS 资源。
- 当用户从网络位置连接时，StoreFront Cloud 可以添加智能访问标签，您可以将其用作 Studio 中访问策略的输入。有关详细信息，请参阅 基于用户网络位置的自适应访问。此功能仅在启用 自适应访问 时可用。
- 您可以根据用户的网络位置选择用户身份验证方式。有关详细信息，请参阅 条件身份验证。
- 您可以根据网络位置连接类型配置不同的超时。有关详细信息，请参阅 根据网络连接类型配置会话。

通常，您会为每个办公地点创建一个网络位置。

注意：

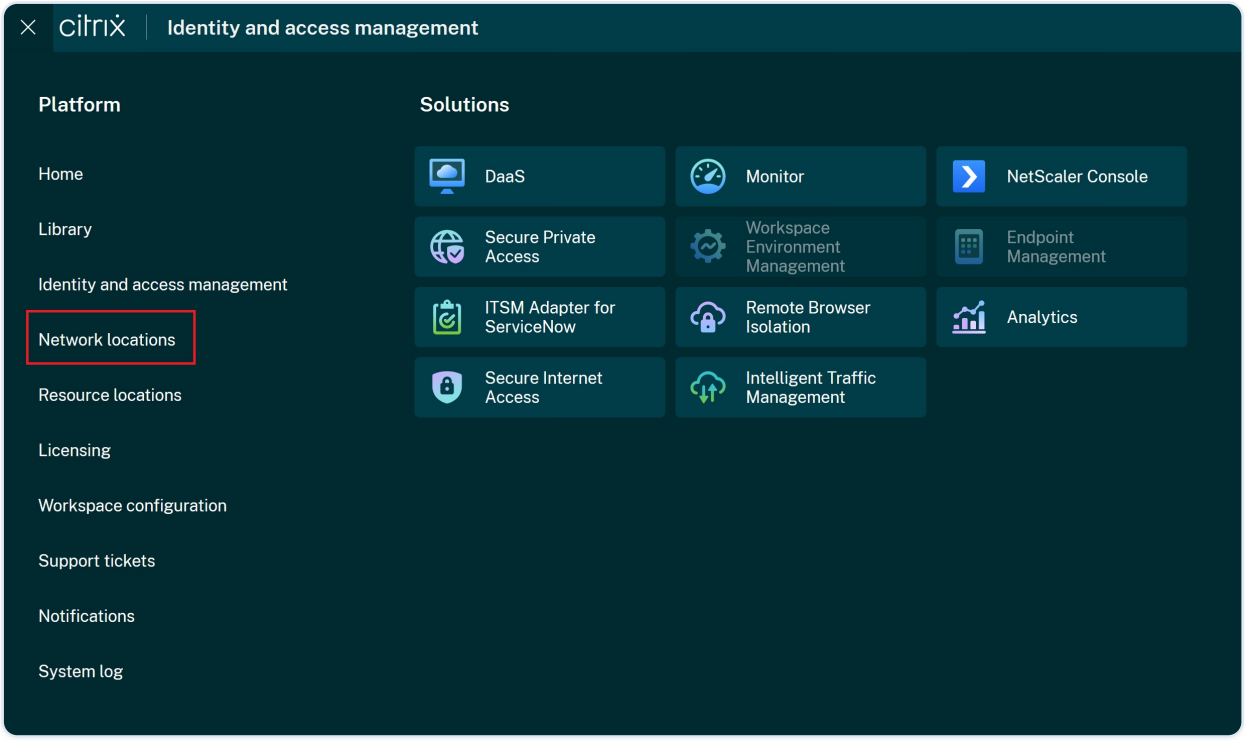
无法区分具有相同公共 IP 地址的不同网络。例如，如果您的公司网络和访客 Wi-Fi 网络共享一个公共 IP 地址，则它们被视为相同的网络位置。

查看网络位置

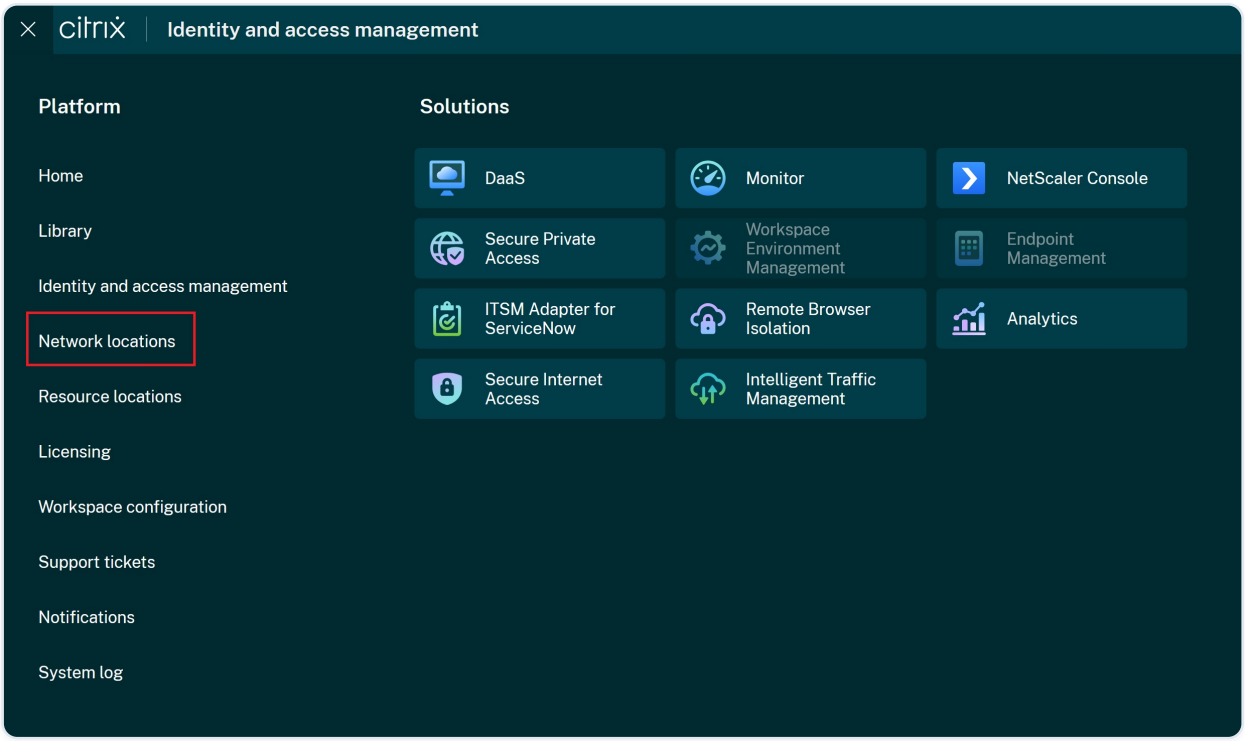
要查看已配置的网络位置：

1. 登录 Citrix Cloud。
2. 打开主菜单。
3. 从主菜单中选择 **网络位置**。

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



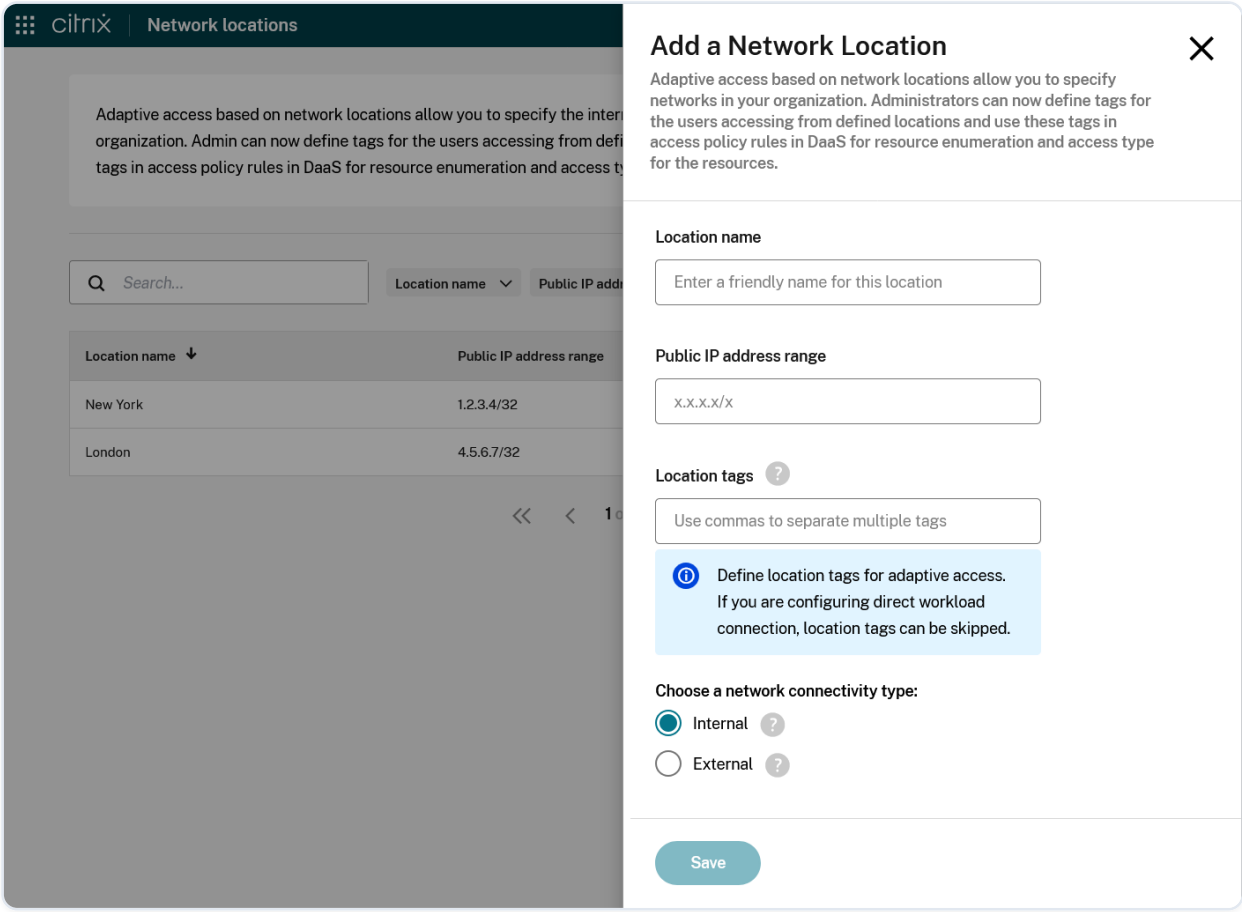
4. 网络位置屏幕加载。



添加网络位置

1. 在“网络位置”屏幕上，按 **添加网络位置**

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



仅当启用 Adaptive Access 时，**位置标签** 和 **连接类型** 选项才可用。

2. 输入 **位置名称**。
3. 以 CIDR 格式输入 **公共 IP 地址范围**。
4. 如果启用了 Adaptive Access，您可以选择输入一个或多个 **位置标签** 的名称。使用逗号分隔多个标签。智能访问标签是通过添加后缀 `LOCATION_TAG_` 生成的。例如，如果您输入位置标签 `BranchOffice`，则会生成一个名为 `LOCATION_TAG_BranchOffice` 的智能访问标签，您可以在 Studio 中使用它。
5. 如果启用了 Adaptive Access，您可以选择位置是 **内部** 还是 **外部**。对于所有内部位置，会生成一个名为 `LOCATION_internal` 的智能访问标签。对于所有外部位置，会生成一个名为 `LOCATION_external` 的智能访问标签。如果客户端的 IP 地址与网络位置不匹配，则该网络位置被视为 **未定义**。

   如果 Adaptive Access 被禁用，则此选项将被隐藏。所有配置的网络位置都被视为内部位置，并且不会创建任何智能访问标签。
6. 按 **保存**。

编辑网络位置

1. 导航到并打开“网络位置”屏幕

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

2. 在您希望编辑的行上，按 **...** 打开菜单，然后选择 **编辑**。
3. 进行必要的更改。
4. 按下**保存**。

删除网络位置

1. 导航到“网络位置”屏幕
2. 在您希望编辑的行上，按下**...**以打开菜单，然后选择**删除**。
3. 在确认屏幕上，按下**是，删除**。

使用 PowerShell 管理网络位置

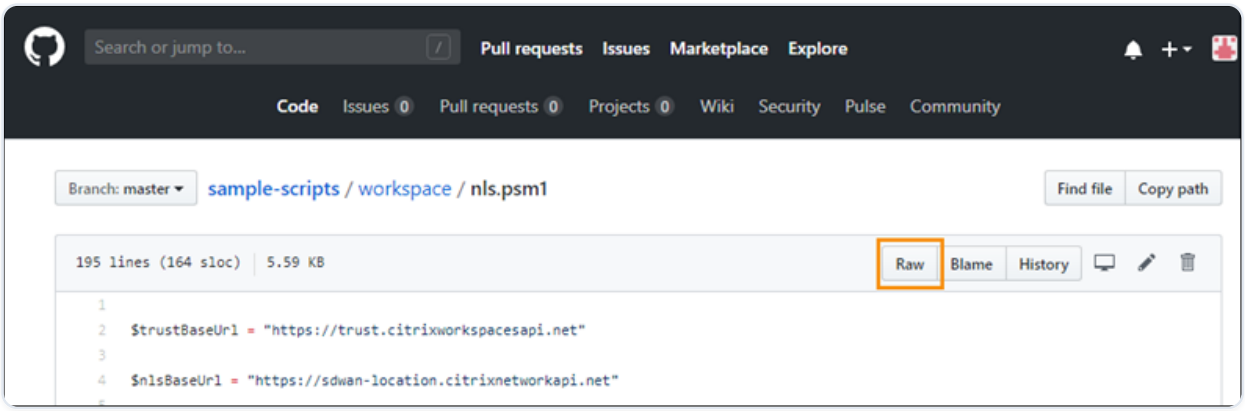
您可以使用 PowerShell 脚本配置直接工作负载连接，而不是使用 Citrix Cloud 管理控制台界面。使用 PowerShell 配置直接工作负载连接涉及以下内容：

1. 下载 PowerShell 模块。
2. 在 Citrix Cloud 中创建服务主体，并记下客户端 ID 和密钥。
3. 导入 PowerShell 模块 并使用您的 API 客户端详细信息连接到网络位置服务 (NLS)。
4. 使用 PowerShell cmdlet 为您的每个位置创建网络位置。

下载 PowerShell 模块

在设置网络位置之前，请从 Citrix GitHub 存储库下载 Citrix 提供的 PowerShell 模块 (nls.psm1)。使用此模块，您可以根据 VDA 的需要设置任意数量的网络位置。

1. 在 Web 浏览器中，转到 `<https://github.com/citrix/sample-scripts/blob/master/workspace/NLS2.psm1>`。
2. 按下 **Raw**。



3. 按 Ctrl+S 并选择一个位置来保存文件。

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

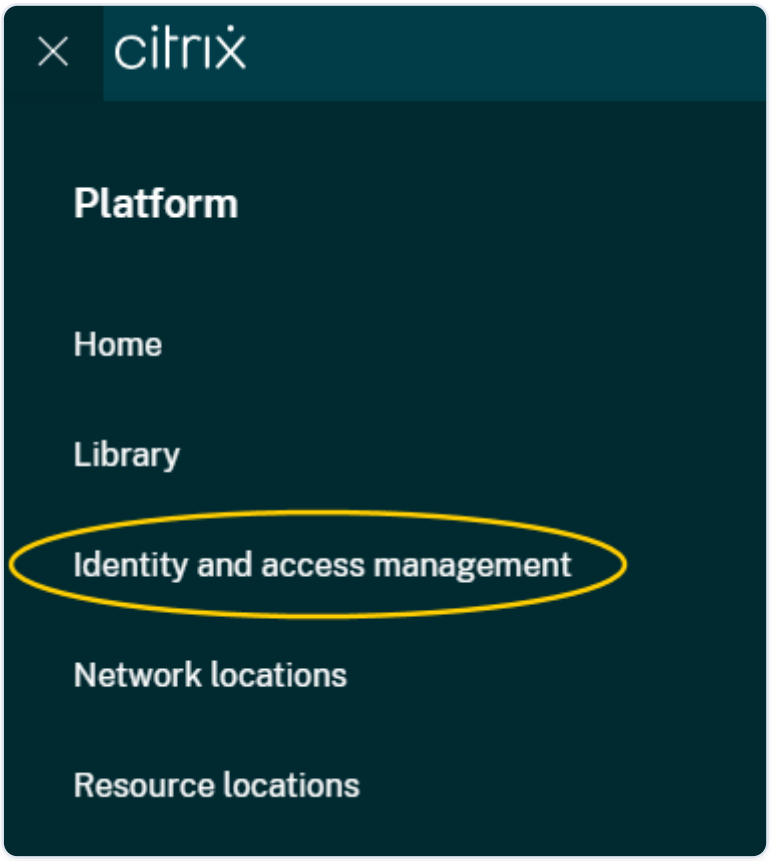
创建服务主体

1. 在 Citrix Cloud 控制台中，单击左上角的菜单。

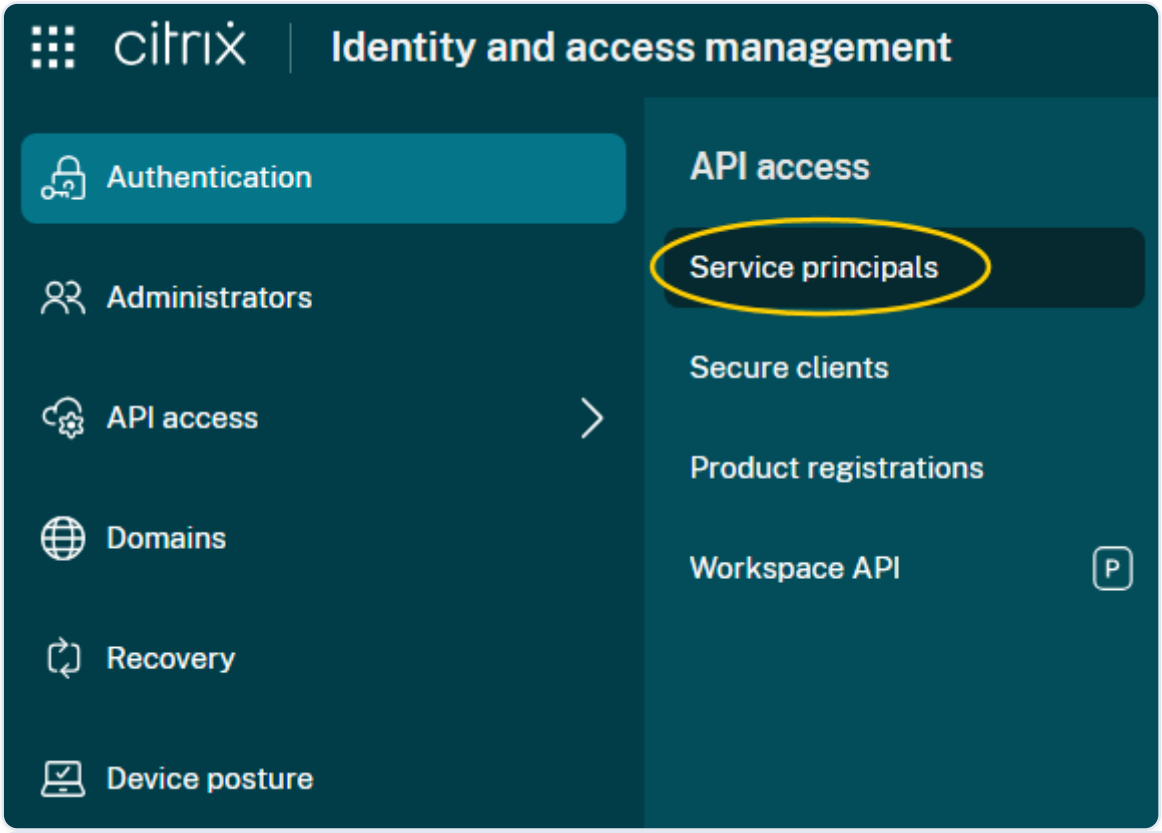
2. 选择 **身份和访问管理** > **API 访问** > **服务主体** > **创建服务主体**，然后按照步骤完成操作。

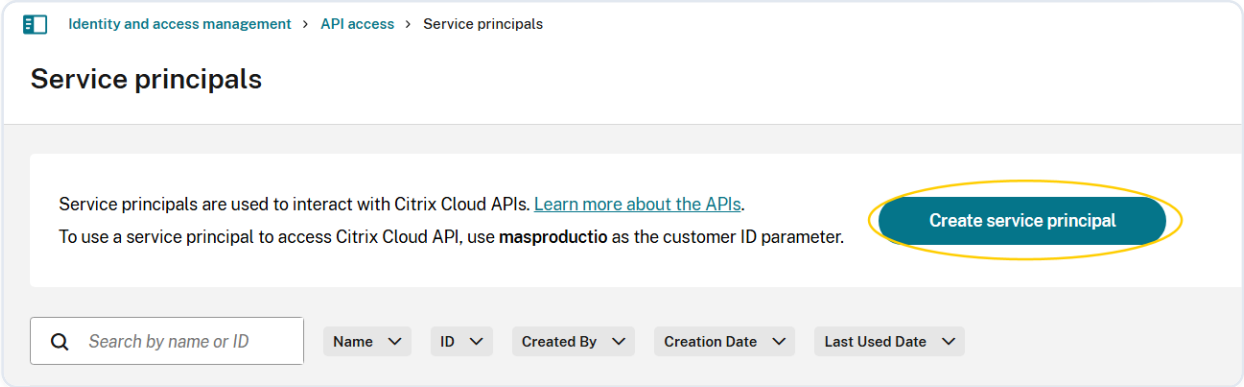
   如果这些选项未显示，您可能没有足够的权限来管理服务主体。请联系您的管理员以获取所需的完全访问权限。

3. 在“**服务主体**”选项卡上，记下您的客户 ID。

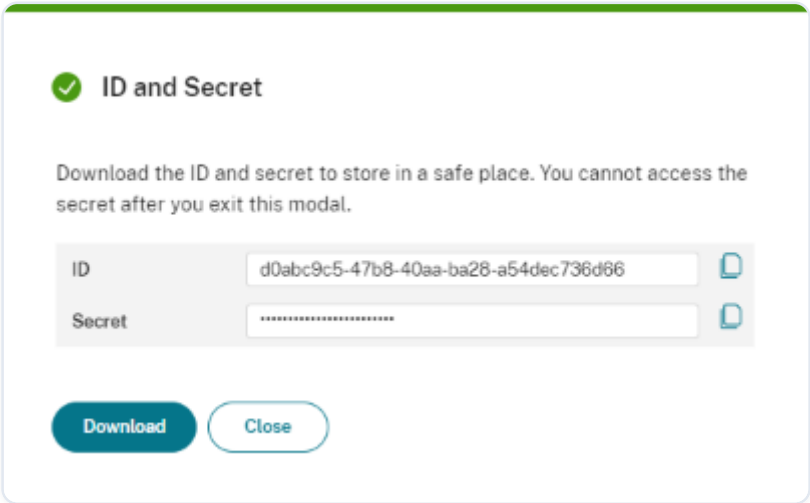


© 1997–2026 Citrix Systems, Inc. All rights reserved.





4. 将凭据添加到您的密钥管理工具中，因为该密钥只会显示一次。



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

配置网络位置

1. 打开 PowerShell 命令窗口，然后导航到保存 PowerShell 模块的目录。
2. 导入模块：`Import-Module .\nls.psm1 -Force`
3. 使用 中的服务主体信息设置所需的变量：(#create-a-secure-client):
   - `$clientId = "YourServicePrincipalClientId"`
   - `$customer = "YourCustomerID"`
   - `$clientSecret = "YourServicePrincipalSecret"`
4. 使用您的服务主体凭据连接到网络位置服务：

```
Connect-NLS -clientId $clientId -clientSecret $clientSecret -customer
$customer
```

5. 创建一个网络位置，将参数值替换为与内部用户直接连接的内部网络相对应的值：

```
New-NLSSite -name "YourSiteName" -tags @("YourTags") -ipv4Ranges
@("PublicIpsOfYourNetworkSites") -longitude 12.3456 -latitude 12.3456
-internal $True
```

要指定单个 IP 地址而不是范围，请在 IP 地址末尾添加 **/32**。例如：

```
New-NLSSite -name "YourSiteName" -tags @("YourTags") -ipv4Ranges
@("PublicIpOfYourNetworkSite/32") -longitude 12.3456 -latitude 12.3456
-internal $True
```

重要提示：

使用 `New-NLSSite` 命令时，请为每个参数至少包含一个值。如果您在不带任何命令行参数的情况下运行此命令，PowerShell 将提示您逐个输入每个参数的相应值。`internal` 属性是一个强制性布尔属性，可能的值为：`$True` 或 `$False`，它通过 PowerShell 映射到 UI。例如，`(UI) Network Internal -> (PowerShell) –internal=$True`。

成功创建网络位置后，命令窗口将显示网络位置的详细信息。

6. 对所有用户连接的网络位置重复步骤 5。

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

7. 运行命令 `Get-NLSSite` 以返回您使用 NLS 配置的所有站点的列表，并验证其详细信息是否正确。

修改网络位置

要更改现有网络位置：

1. 在 PowerShell 命令窗口中，列出所有现有网络位置：`Get-NLSSite`
2. 要修改特定网络位置的 IP 范围，请键入

   ```
   (Get-NLSSite)[N] | Set-NLSSite -ipv4Ranges @("1.2.3.4/32","4.3.2.1/32")
   ```

   其中 `[N]` 是列表中位置对应的数字（从零开始），且 `"1.2.3.4/32","4.3.2.1/32"` 是您要使用的逗号分隔的 IP 范围。例如，要修改列表中的第一个位置，请键入以下命令：

   ```
   (Get-NLSSite)[0] | Set-NLSSite -ipv4Ranges
   @("98.0.0.1/32","141.43.0.0/24")
   ```

删除网络位置

要删除不再使用的网络位置：

1. 在 PowerShell 命令窗口中，列出所有现有网络位置：`Get-NLSSite`
2. 要删除所有网络位置，请键入 `Get-NLSSite | Remove-NLSSite`
3. 要删除特定的网络位置，请键入 `(Get-NLSSite)[N] | Remove-NLSSite`，其中 `[N]` 是列表中位置对应的数字。例如，要删除列表中的第一个位置，请键入 `(Get-NLSSite)[0] | Remove-NLSSite`。

示例脚本

示例脚本包含您可能需要添加、修改和删除分支位置的公共 IP 地址范围的所有命令。但是，您无需运行所有命令来执行任何单个功能。要运行脚本，请始终包含前 10 行，从 **Import-Module** 到 **Connect-NLS**。之后，您只需包含要执行功能的命令即可。

```
Import-Module .\nls.psm1 -Force



$clientId = "XXXX" #Replace with your clientId
```

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

```
$clientSecret = "YYY"    #Replace with your clientSecret

$customer = "CCCCCC"  #Replace with your customerid



# Connect to Network Location Service

Connect-NLS -clientId $clientId -clientSecret $clientSecret -customer
$customer



# Create a new Network Location Service Site (Replace with details
corresponding to your branch locations)

New-NLSSite -name "New York" -tags @("EastCoast") -ipv4Ranges
@("1.2.3.0/24") -longitude 40.7128 -latitude -74.0060 -internal $True



# Get the existing Network Location Service Sites (optional)

Get-NLSSite



# Update the IP Address ranges of your first Network Location Service Site
(optional)

$s = (Get-NLSSite)[0]

$s.ipv4Ranges = @("1.2.3.4/32","4.3.2.1/32")

$s | Set-NLSSite



# Remove all Network Location Service Sites (optional)

Get-NLSSite | Remove-NLSSite
```

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

```
# Remove your third site (optional)

(Get-NLSSite)[2] | Remove-NLSSite
```

通知

通知提供管理员可能感兴趣的问题或事件信息，例如新的 Citrix Cloud™ 功能或资源位置中计算机的问题。通知可以来自 Citrix Cloud 中的任何服务。

查看通知

通知数量显示在 Citrix Cloud 控制台页面的顶部附近。有关更多详细信息，请在控制台的“**通知**”下单击“**查看全部**”，或从控制台菜单中选择“**通知**”。

选择了“通知”菜单的 Citrix Cloud 控制台(/en-us/citrix-cloud/media/notifications-menu.png)

“通知”页面显示您收到的通知。最新通知显示在列表顶部。

包含新通知的“通知”页面(/en-us/citrix-cloud/media/notifications-page.png)

关闭通知

通知是按管理员进行管理的。当您关闭通知时，关闭操作将以您在 Citrix Cloud 中的管理员身份进行。即使您关闭了所有通知，其他管理员仍然可以查看和关闭他们自己的通知。

要关闭您收到的所有通知，请选择页面顶部的“**全部关闭**”。

要关闭单个通知，请选择每个通知，然后选择“**关闭**”。

突出显示了单个通知和“关闭”按钮的“通知”页面(/en-us/citrix-cloud/media/notifications-page-selections.png)

接收电子邮件通知

您可以选择通过电子邮件接收通知，而不是登录查看。默认情况下，电子邮件通知处于关闭状态。

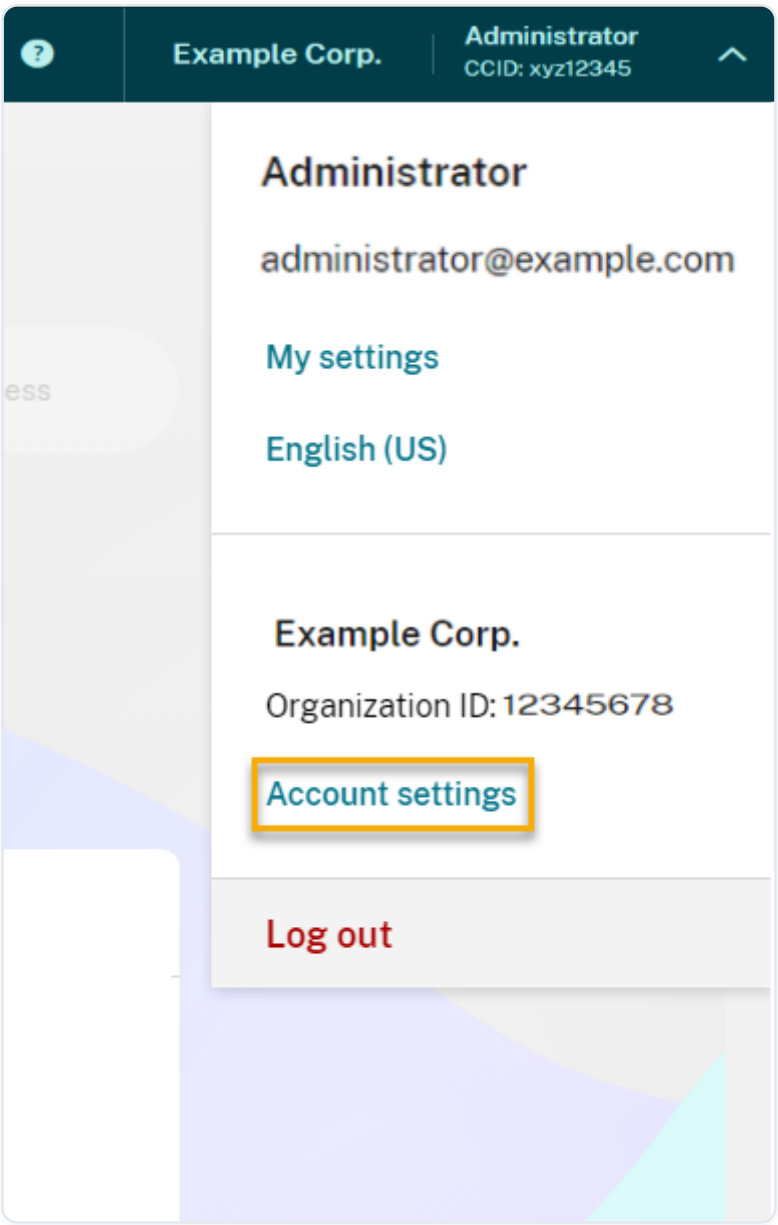
您还可以为没有您的 Citrix Cloud 帐户管理员访问权限的其他利益相关者（例如您组织的安全和审计团队成员）启用电子邮件通知。

当您启用电子邮件通知时，Citrix Cloud 会为每条通知发送一封电子邮件。通知会尽快发送。它们不会被分组到一封电子邮件中，也不会批量发送。

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

为自己启用电子邮件通知

1. 在 Citrix Cloud 管理控制台中，选择“**帐户设置**”。



2. 选择“**通知**”。
3. 开启“**我的电子邮件通知**”设置。
4. 在“**管理我的通知设置**”下，选择您要接收的通知类型。默认情况下，仅选择“关键”类型。
5. 单击“**应用**”以保存您的设置。

为非管理员启用电子邮件通知

使用本节中的步骤将非管理员添加为电子邮件通知的联系人。如果您尝试将现有管理员添加为联系人，Citrix Cloud 将显示错误。

1. 在 Citrix Cloud 管理控制台中，单击“**帐户设置**”。

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

2. 选择“**通知**”。
3. 在“**联系人管理**”下，选择“**添加联系人**”。
4. 输入联系人的姓名、电子邮件地址及其首选语言。
5. 在“**管理通知设置**”下，选择要发送的通知类型。
6. 选择**添加联系人**以保存联系人信息。

修改通知设置

作为管理员，您可以通过选中或清除**管理我的通知设置**下的复选框来更改您接收的通知类型。更改您的通知不会影响其他管理员接收的通知。

您还可以修改非管理员接收的通知。

修改非管理员的通知

1. 在 Citrix Cloud 管理控制台中，单击**帐户设置**。
2. 选择**通知**。
3. 在**联系人管理**下，找到您要管理的联系人。
4. 指向联系人，然后选择铅笔图标。
5. 在**管理通知设置**下，选中或清除每种通知类型的复选框。

要修改联系人的电子邮件地址，您必须先删除该联系人，然后将其添加为使用新电子邮件地址的新联系人。

禁用电子邮件通知

作为管理员，您可以通过关闭**我的电子邮件通知**设置随时禁用自己的电子邮件通知。

非管理员可以通过单击每封通知电子邮件中显示的取消订阅链接来停止接收通知。已取消订阅的联系人在**联系人管理**部分的表格中具有**已取消订阅**的通知状态。

要禁用非管理员的通知，您可以执行以下操作之一：

- 清除针对该联系人的“**管理通知设置**”中的所有复选框。
- 从“**联系人管理**”下的表中删除联系人。

删除非管理员联系人

1. 在 Citrix Cloud 管理控制台中，单击“**帐户设置**”。
2. 选择“**通知**”。

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

3. 在“**联系人管理**”下，找到您要管理的联系人。
4. 指向联系人，然后选择垃圾桶图标。

Citrix Cloud 会从表中删除该联系人。

系统日志

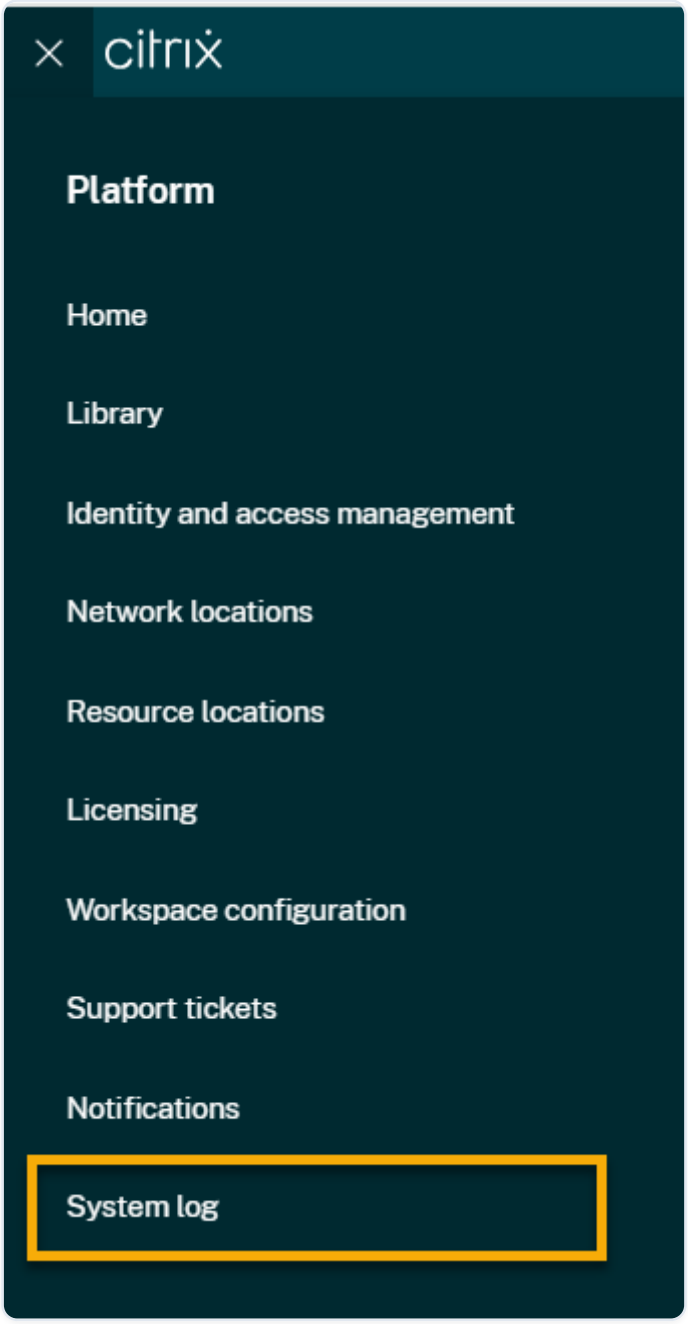
系统日志显示了在 Citrix Cloud 中发生的带时间戳的事件列表。这包括配置更改以及连接器升级等其他事件。您可以将这些更改导出为 CSV 文件，以满足组织的法规遵从性要求或支持安全分析。

注意：

> DaaS Studio 将日志写入单独的日志。有关详细信息，请参阅配置日志记录。

要查看系统日志，请从 Citrix Cloud 菜单中选择**系统日志**。

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



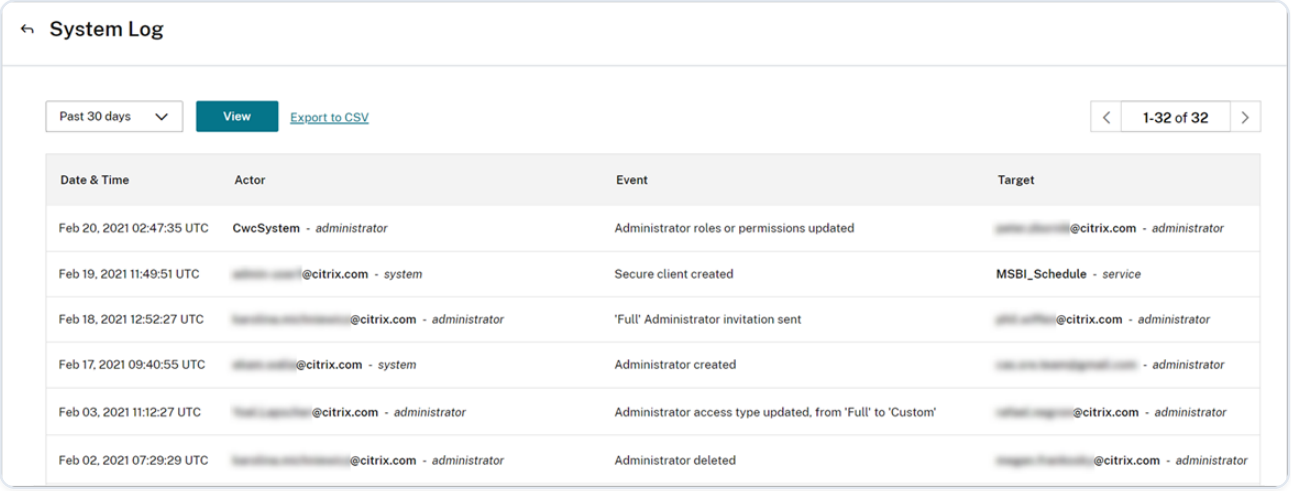
有关系统日志中数据保留的更多信息，请参阅本文中的数据保留。

记录的事件

系统日志捕获某些 Citrix Cloud 平台和云服务操作的事件。有关这些事件的完整列表和捕获数据的说明，请参阅系统日志事件参考。

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。

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



显示的列表包括以下信息：

- 事件发生的日期和时间 (UTC)。
- 发起事件的操作者，例如管理员或服务主体。操作者为 **CwcSystem** 的条目表示 Citrix Cloud 执行了该操作。
- 事件的简要说明，例如编辑管理员或创建新的服务主体。
- 事件的目标。目标是受事件影响或因事件而更改的系统对象。例如，被添加为管理员的用户。

要查看 30 天以前的事件，请通过选择要查看的时间段并选择 **查看** 来筛选列表。您可以查看过去 90 天内发生的事件。

突出显示筛选菜单的系统日志列表(/en-us/citrix-cloud/media/system-log-date-range.png)

要检索在您指定的时间段内发生的较早事件，可以使用 SystemLog API。有关详细信息，请参阅本文中的检索特定时间段的事件。

导出事件

您可以导出过去 90 天内发生的系统日志事件的 CSV 文件。下载文件的名称遵循 `SystemLog-CustomerName-OrgID-DateTimeStamp.csv` 的格式。

1. 在 Citrix Cloud 菜单中，选择 **系统日志**。
2. 如果需要，筛选列表以显示要导出事件的时间段。
3. 选择 **导出到 CSV** 并保存文件。 突出显示“导出到 CSV”链接的系统日志(/en-us/citrix-cloud/media/system-log-export.png)

CSV 文件包含以下信息：

- 每个事件的 UTC 时间戳
- 启动事件的参与者详细信息，包括名称和参与者 ID。

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

- 事件详细信息，例如事件类型和事件文本
- 事件目标的详细信息，例如目标 ID、管理员或服务主体的名称。

检索特定时间段的事件

如果您需要检索特定时间段的事件，请使用 SystemLog API。

SystemLog API

您可以使用 SystemLog API 读取日志条目并将其导出到另一个系统。在使用此 API 之前，您需要按照 Citrix Developer Docs 网站上的 入门 中所述创建服务主体。

有关使用 SystemLog API 的更多信息，请参阅 Citrix Developer Docs 网站上的 Citrix Cloud - SystemLog。

有关 Citrix DaaS 日志，请参阅 如何在 Citrix DaaS 中获取配置操作。

数据保留

Citrix 与您（客户）共同负责保留 Citrix Cloud 捕获的系统日志数据。

Citrix® 在事件记录后保留系统日志记录 90 天。

您负责下载您希望保留的系统日志记录，以满足您组织的合规性要求，并将其存储在长期存储解决方案中。

系统日志事件参考

要查看您的 Citrix Cloud™ 帐户的所有系统日志事件数据，您可以：

- 下载包含过去 30、60 或 90 天内发生的所有事件的 (/zh-cn/citrix-cloud/citrix-cloud-management/system-log.html#export-events) CSV 文件。
- 使用 SystemLog API 检索特定时间段的事件。

请参阅本文中的 事件数据说明，了解检索系统日志事件时捕获的数据的说明。请参阅 生成事件的云组件和服务，了解事件特定值，例如事件消息文本、事件类型以及事件发生前后是否记录对象字段数据。

生成事件的云组件和服务

系统日志记录以下 Citrix Cloud 实体、组件和服务的事件：

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

- Citrix Cloud 平台：与 Citrix Cloud 平台功能相关的事件，例如管理管理员、Workspace 订阅者的设备重置、Microsoft Entra ID 租户以及管理域和网络位置。
- 连接器：与注册和更新 Citrix Cloud 连接器和连接器设备相关的事件。
- 许可：与注册本地许可证服务器、管理云服务的分配许可证以及导出许可数据相关的事件。
- 安全私有访问服务：与安全私有访问服务配置相关的事件。
- Citrix Workspace：与 Workspace 配置设置相关的事件。

事件数据说明

当您下载系统日志事件或使用 SystemLog API 检索它们时，将包含以下数据：

- **RecordID：** 事件的唯一标识符。
- **UtcTimestamp：** 事件发生的日期和 UTC 时间。
- **CustomerID：** Citrix Cloud 帐户的唯一组织标识符。
- **EventType：** 所记录事件类型的标识符。事件类型使用 `OriginatingService/Actor/Action` 格式记录。例如，创建管理员的事件类型为 `platform/administrator/create`。
- **TargetID：** 受影响或更改的系统对象的 ID。
- **TargetDisplayName：** 受影响或更改的系统对象的显示名称。例如，所创建管理员的名称。
- **TargetEmail：** 系统对象的电子邮件地址。例如，所创建管理员的电子邮件地址。
- **TargetUserID：** 受影响或更改的系统对象的用户 ID。例如，创建管理员时，目标用户 ID 是所创建管理员的用户 ID。
- **TargetType：** 事件的目标类别。
- **BeforeChanges** 和 **AfterChanges：** 事件发生前后对象字段的内容。对于某些事件，这些对象字段包括：
  - CustomerID
  - 用户主体
  - UserID
  - 管理员访问类型，例如“自定义”或“完全”
  - CreatedDate
  - UpdatedDate
  - 显示名称
- **AgentID:** 事件类别。

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

- **ActorID:** 启动事件的系统对象的 ID。例如，对于创建管理员，这是邀请其他用户加入 Citrix Cloud 帐户的管理员的对象 ID。
- **ActorDisplayName:** 启动事件的人员或实体的显示名称。例如，邀请其他用户加入 Citrix Cloud 帐户的管理员的名称。
- **ActorType:** 生成事件的服务。
- **EventMessage:** 发生的事件的简要描述。

适用于 Citrix Cloud™ 平台的系统日志事件

本文介绍了系统日志捕获的适用于 Citrix Cloud 平台的事件数据。有关系统日志事件数据的更多信息，请参阅系统日志事件参考。

要了解有关系统日志的更多信息，请参阅系统日志。

微软 Entra ID 租户

事件消息	事件类型	目标类型	参与者类型	参与者 ID	事件发生前记录的当前对象字段	事件发生后记录的更新后的对象字段
Microsoft Entra ID 租户已连接	platform/identityprovider/azuread/connect	服务	管理员	是	否	
Microsoft Entra ID 租户已断开连接	platform/identityprovider/azuread/disconnect	服务	管理员	是	否	
Microsoft Entra ID 身份验证域名已更改	platform/identityprovider/azuread/authdomain/updatename	工作区	Customer ID	否	否	

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

事件消息	事件类型	目标类型	参与者类型	参与者 ID	事件发生前记录的当前对象字段	事件发生后记录的更新后的对象字段
Microsoft Entra ID 身份验证域名更改失败	platform/identityprovider/azuread/authdomain/updatenamefailed	思杰工作区	Customer ID	否	否	

Citrix Cloud 管理员和服务主体

事件消息	事件类型	目标类型	参与者类型	事件发生前记录的当前对象字段	事件发生后记录的更新对象字段
管理员已创建	platform/administrator/create	管理员	系统	否	是
管理员邀请已发送	平台/管理员/邀请	管理员	管理员	否	是
管理员角色或权限已更新	平台/管理员/更新	管理员	管理员	是	是
管理员已删除	platform/administrator/delete	管理员	管理员	否	是
管理员组已创建	platform/administratorgroup/create	管理员组	否	是	
管理员组角色或权限已更新	platform/administrato	管理员组	是	是	

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

事件消息	事件类型	目标类型	参与者类型	事件发生前记录的当前对象字段	事件发生后记录的更新对象字段
	rgroup/update				
管理员组已删除	platform/administratorgroup/delete	管理员组	管理员	是	否

Citrix Cloud 服务主体

事件消息	事件类型	目标类型	参与者类型	事件发生前记录的当前对象字段	事件发生后记录的更新对象字段
服务主体已创建	platform/serviceprincipal/create	服务主体	管理员	不适用	是
创建服务主体失败	platform/serviceprincipal/createfailed	服务主体	管理员	不适用	不适用
服务主体角色或权限已更新	platform/serviceprincipal/updatepolicyset	服务主体	管理员	是	是
未能更新服务主体	platform/serviceprincipal/updatefailed	服务主体	管理员	不适用	不适用
服务主体已删除	platform/serviceprincipal/delete	服务主体	管理员	是	不适用

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

事件消息	事件类型	目标类型	参与者类型	事件发生前记录的当前对象字段	事件发生后记录的更新对象字段
未能删除服务主体	平台/服务主体/删除失败	服务主体	管理员	不适用	不适用
服务主体密钥已轮换	平台/服务主体/密钥轮换	服务主体	管理员	是	是
轮换服务主体密钥失败	平台/服务主体/密钥轮换失败	服务主体	管理员	不适用	不适用
服务主体辅助密钥已删除	platform/serviceprincipal/secondarysecretdeletion	服务主体	管理员	是	是
删除服务主体辅助密钥失败	platform/serviceprincipal/secondarysecretdeletionfailed	服务主体	管理员	不适用	不适用

Active Directory Plus 令牌的设备重置

事件消息	事件类型	目标类型	参与者类型	事件发生前记录的当前对象字段	事件发生后记录的更新对象字段
订阅者设备令牌重置完成	platform/authenticationdevice/delete	订阅者	管理员	否	是

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

域管理

事件消息	事件类型	目标类型	执行者类型	事件发生前记录的当前对象字段	事件发生后记录的更新对象字段
域已移除	platform/domain/remove	服务	管理员	否	否

网络位置

事件消息	事件类型	目标 ID	执行者 ID	事件发生前记录的当前对象字段	事件发生后记录的更新对象字段
网络位置已创建	sdwan/networklocation/create	已创建的网络位置的 ID	添加网络位置的管理员的名称	否	是
网络位置已更新	sdwan/networklocation/edit	已修改的网络位置的 ID	修改网络位置的管理员的名称	是	是
网络位置已删除	sdwan/networklocation/delete	已删除的网络位置的ID	删除网络位置的管理员的姓名	是	否

资源位置

事件消息	事件类型	目标ID	执行者ID	事件发生前记录的当前对象字段	事件发生后记录的更新对象字段
资源位置已创建	platform/resourcelocation/create	已创建的资源位置的名称	创建资源位置的管理员的名称	是	是
资源位置已更新	platform/resourcelocation/update	已修改的资源位置的名称	修改资源位置的管理员的名称	是	是

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

事件消息	事件类型	目标ID	执行者ID	事件发生前记录的当前对象字段	事件发生后记录的更新对象字段
资源位置已删除	platform/resourcelocation/delete	已删除的资源位置的名称	删除资源位置的管理员的名称	是	是

账户名称和徽标更改

事件消息	事件类型	目标 ID	执行者 ID	事件发生前记录的当前对象字段	事件发生后记录的更新对象字段
管理员账户名称已更新	platform/account/name/update	客户	管理员	是	是
管理员账户徽标已更新	platform/account/logo/update	客户	管理员	否	否

连接器的系统日志事件

本文介绍了系统日志为 Citrix Cloud Connector 和 Connector Appliance for Cloud Services 捕获的事件数据。有关系统日志事件数据的更多信息，请参阅 系统日志事件参考。

要了解有关系统日志的更多信息，请参阅 系统日志。

连接器注册

事件消息	事件类型	目标类型	执行者 ID	事件发生前记录的当前对象字段	事件发生后记录的更新后的对象字段
连接器已注册	platform/edgeserver/create	**云连接器** 或 **连接器设备**	注册连接器的管理员	是	是
连接器已删除	platform/edgeserver/delete	**云连接器**或 **连接器设备**	删除连接器的管理员	是	是

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

连接器更新

事件消息	事件类型	目标 ID	参与者 ID	事件发生前记录的当前对象字段	事件发生后记录的更新对象字段
资源位置维护窗口已更新	platform/resourcelocation/maintenancewindow	已修改的资源位置的名称	更改配置的管理员	是	是
管理员触发的连接器升级	platform/edgeserver/manualupgrade	**云连接器** 或 **连接器设备**	启动更新的管理员	否	否
连接器升级已启动	platform/edgeserver/upgradestarted	**云连接器** 或 **连接器设备**	**自动** 或启动更新的管理员	是	否
连接器升级完成	platform/edgeserver/upgradecompleted	**云连接器** 或 **连接器设备**	**自动** 或发起更新的管理员	否	是

连接器公钥

事件消息	事件类型	目标 ID	参与者 ID	事件发生前记录的当前对象字段	事件发生后记录的更新对象字段
公钥已添加到信任	platform/authentication/createedgeserverkey	执行此操作的管理员	否	否	
公钥已从信任中移除	platform/authentication/	执行此操作的管理员	否	否	

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

事件消息	事件类型	目标 ID	参与者 ID	事件发生前记录的当前对象字段	事件发生后记录的更新对象字段
	deleteedgeserverkey				

Citrix Cloud™ 中许可的系统日志事件

本文介绍了系统日志为本地 Citrix 许可与 Citrix Cloud 注册捕获的事件数据。有关系统日志事件数据的更多信息，请参阅 系统日志事件参考。

要了解有关系统日志的更多信息，请参阅 系统日志。

本地许可证服务器

事件消息	事件类型	目标类型	参与者 ID	事件发生前记录的当前对象字段	事件发生后记录的更新对象字段
本地许可证服务器已删除	lui/onpremlicenseservers/delete	许可	删除许可证服务器的管理员	否	否
删除本地许可证服务器失败	lui/onpremlicenseservers/deletefailed	许可	尝试删除许可证服务器的管理员	否	否

云服务许可

事件消息	事件类型	目标类型	参与者 ID	事件发生前记录的当前对象字段	事件发生后记录的更新对象字段
Citrix Cloud 服务许可证已发布	lui/cloudlicense/release	CloudLicense	为云服务发布许可证的管理员	否	否
未能发布 Citrix Cloud 服务许可证	lui/cloudlicense/	CloudLicense	尝试为云服务发布许可证的管理员	否	否

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

事件消息	事件类型	目标类型	参与者 ID	事件发生前记录的当前对象字段	事件发生后记录的更新对象字段
	releasefailed				

适用于 Citrix 服务提供商的许可证使用情况洞察

事件消息	事件类型	目标类型	参与者 ID	事件发生前记录的当前对象字段	事件发生后记录的更新对象字段
合作伙伴本地用户列表数据已导出	lui/csp/userlistdataexport	许可	导出合作伙伴用户列表数据的管理员	否	否
导出合作伙伴本地用户列表数据失败	lui/csp/userlistdataexportfailed	许可	尝试导出合作伙伴用户列表数据的管理员	否	否

云服务和本地产品的许可证使用情况

事件消息	事件类型	目标类型	参与者 ID	事件发生前记录的当前对象字段	事件发生后记录的更新对象字段
许可证使用数据已导出	lui/cloudlicense/usagedataexport	云许可或许可	导出许可证使用数据的管理员	否	否
导出许可证使用数据失败	lui/cloudlicense/usagedataexportfailed	CloudLicense 或 许可	尝试导出许可证使用数据的管理员	否	否

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

Secure Private Access 的系统日志事件

本文介绍了系统日志为 Secure Private Access 服务捕获的事件数据。有关系统日志事件数据的更多信息，请参阅 系统日志事件参考。

要了解有关系统日志的更多信息，请参阅 系统日志。

Web 和 SaaS 应用程序

事件消息	事件类型	目标类型	事件发生前记录的当前对象字段	事件发生后记录的更新对象字段
Web/SaaS 应用程序已创建	swa/websaasapplication/create	Web SaaS 应用程序	否	是
Web/SaaS 应用程序已更新	swa/websaasapplication/update	Web 和 SaaS 应用程序	是	是
Web/SaaS 应用程序已删除	swa/websaasapplication/delete	Web 和 SaaS 应用程序	是	否
Web/SaaS 应用程序创建失败	swa/websaasapplication/createfailed	Web 和 SaaS 应用程序	否	否
Web/SaaS 应用程序更新失败	swa/websaasapplication/updatefailed	Web SaaS 应用程序	是	是
Web/SaaS 应用程序删除失败	swa/websaasapplication/deletefailed	Web SaaS 应用程序	是	是

用户和组订阅

事件消息	事件类型	目标类型	事件发生前记录的当前对象字段	事件发生后记录的更新对象字段
用户/组订阅已添加	swa/websaasapplicati	Web SaaS 应用程序订阅者	否	是

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

事件消息	事件类型	目标类型	事件发生前记录的当前对象字段	事件发生后记录的更新对象字段
	onsubscribers/subscribe			
用户/组订阅已移除	swa/websaaspplicationsubscribers/unsubscribe	Web SaaS 应用程序订阅者	否	是
用户/组订阅失败	swa/websaaspplicationsubscribers/subscribefailed	Web SaaS 应用程序订阅者	否	否
用户/组取消订阅失败	swa/websaaspplicationsubscribers/unsubscribefailed	Web SaaS 应用程序订阅者	否	否

上下文策略

事件消息	事件类型	目标类型	事件发生前记录的当前对象字段	事件发生后记录的更新对象字段
上下文策略已创建	swa/contextualpolicy/create	情境策略	否	是
上下文策略已更新	swa/contextualpolicy/update	上下文策略	是	是
上下文策略已删除	swa/contextualpolicy/delete	上下文策略	是	否
上下文策略创建失败	swa/contextualpolicy/createfailed	上下文策略	否	否

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

事件消息	事件类型	目标类型	事件发生前记录的当前对象字段	事件发生后记录的更新对象字段
上下文策略更新失败	swa/contextualpolicy/updatefailed	情境策略	否	否
上下文策略删除失败	swa/contextualpolicy/deletefailed	情境策略	是	否

应用程序域

事件消息	事件类型	目标类型	事件发生前记录的当前对象字段	事件发生后记录的更新对象字段
应用程序域已创建	swa/applicationdomain/create	应用程序域	否	是
应用程序域已更新	swa/applicationdomain/update	应用程序域	是	是
应用程序域已删除	swa/applicationdomain/delete	应用程序域	是	否
应用程序域创建失败	swa/applicationdomain/createfailed	应用程序域	否	否
应用程序域更新失败	swa/applicationdomain/updatefailed	应用程序域	是	否
应用程序域删除失败	swa/applicationdomain/deletefailed	应用程序域	是	否

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

浏览器扩展设置

事件消息	事件类型	目标类型	事件发生前记录的当前对象字段	事件发生后记录的更新对象字段
浏览器扩展设置已更新	swa/browserextensionsettings/update	浏览器扩展设置	是	是
浏览器扩展设置更新失败	swa/browserextensionsettings/updatefailed	浏览器扩展设置	是	否

网站 URL 列表和筛选类别

事件消息	事件类型	目标类型	事件发生前记录的当前对象字段	事件发生后记录的更新对象字段
已启用的网站筛选列表和类别	swa/website/filterlistsenabledfiltercategoriesenabled/update	网站 URL 列表分类功能	是	是
已启用的网站筛选列表和已禁用的筛选类别	swa/website/filterlistsenabledfiltercategoriesdisabled/update	网站URL列表类别功能	是	是
禁用了网站筛选列表并启用了筛选类别	swa/website/filterlistsdisabledfiltercategoriesenabled/update	网站URL列表类别功能	是	是
禁用了网站筛选列表和类别	swa/website/filterlistsdisabledfiltercategoriesdisabled/update	网站URL列表类别功能	是	是
未能启用网站筛选列表和类别	swa/website/filterlistsenabledfiltercategories	网站 URL 列表类别功能	是	是

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

事件消息	事件类型	目标类型	事件发生前记录的当前对象字段	事件发生后记录的更新对象字段
	enabled/updatefailed			
未能启用网站筛选列表并禁用筛选类别	swa/website/filterlistsenabledfiltercategoriesdisabled/updatefailed	网站 URL 列表类别功能	是	是
未能禁用网站筛选列表并启用筛选类别	swa/website/filterlistsdisabledfiltercategoriesenabled/updatefailed	网站 URL 列表类别功能	是	是
未能禁用网站筛选列表和类别	swa/website/filterlistsdisabledfiltercategoriesdisabled/updatefailed	网站URL列表类别功能	是	是
网站 URL 列表已创建	swa/websiteurlfilteringlist/create	网站URL过滤列表	否	是
网站 URL 列表已更新	swa/websiteurlfilteringlist/update	网站URL过滤列表	是	是
网站 URL 列表已删除	swa/websiteurlfilteringlist/delete	网站 URL 过滤列表	是	否
网站 URL 列表创建失败	swa/websiteurlfilteringlist/createfailed	网站 URL 过滤列表	否	否
网站 URL 列表更新失败	swa/websiteurlfilteri	网站 URL 过滤列表	是	否

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

事件消息	事件类型	目标类型	事件发生前记录的当前对象字段	事件发生后记录的更新对象字段
	nglist/updatefailed			
网站 URL 列表删除失败	swa/websiteurlfilteringlist/deletefailed	网站URL过滤列表	是	否
网站 URL 筛选类别已创建	swa/websiteurlfiltercategory/create	网站URL过滤类别	否	是
网站 URL 筛选类别已更新	swa/websiteurlfiltercategory/update	网站URL过滤类别	是	是
网站 URL 筛选类别已删除	swa/websiteurlfiltercategory/delete	网站URL过滤类别	否	否
网站 URL 筛选类别创建失败	swa/websiteurlfiltercategory/createfailed	网站URL过滤类别	否	否
网站 URL 筛选类别更新失败	swa/websiteurlfiltercategory/updatefailed	网站URL过滤类别	是	否
网站 URL 筛选类别删除失败	swa/websiteurlfiltercategory/deletefailed	网站URL过滤类别	是	否

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

网站筛选类别预设

事件消息	事件类型	目标类型	事件发生前记录的当前对象字段	事件发生后记录的更新对象字段
已更新的网站筛选类别预设	swa/websiteurlfiltercategorypreset/update	网站URL过滤类别预设	是	是
未能更新网站筛选类别预设	swa/websiteurlfiltercategorypreset/updatefailed	网站URL筛选类别预设	是	是

已阻止的网站 URL 列表和筛选类别

事件消息	事件类型	目标类型	事件发生前记录的当前对象字段	事件发生后记录的已更新对象字段
已创建已阻止的网站 URL 列表	swa/websiteurlfilteringlist/blocked/create	网站URL筛选列表	否	是
已更新阻止的网站 URL 列表	swa/websiteurlfilteringlist/blocked/update	网站URL过滤列表	否	是
已删除阻止的网站 URL 列表	swa/websiteurlfilteringlist/blocked/delete	网站URL过滤列表	否	是
阻止的网站 URL 列表创建失败	swa/websiteurlfilteringlist/blocked/createfailed	网站URL过滤列表	否	是

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

事件消息	事件类型	目标类型	事件发生前记录的当前对象字段	事件发生后记录的已更新对象字段
阻止的网站 URL 列表更新失败	swa/websiteurlfilteringlist/blocked/updatefailed	网站URL过滤列表	否	是
阻止的网站 URL 列表删除失败	swa/websiteurlfilteringlist/blocked/deletefailed	网站URL过滤列表	否	是
阻止的网站 URL 筛选类别已创建	swa/websiteurlfiltercategory/blocked/create	网站URL过滤列表	否	是
已更新阻止的网站 URL 筛选类别	swa/websiteurlfiltercategory/blocked/update	网站 URL 过滤列表	否	是
已删除阻止的网站 URL 筛选类别	swa/websiteurlfiltercategory/blocked/delete	网站 URL 过滤列表	否	是
阻止的网站 URL 筛选类别创建失败	swa/websiteurlfiltercategory/blocked/createfailed	网站 URL 过滤列表	否	是
阻止的网站 URL 筛选类别更新失败	swa/websiteurlfiltercategory/blocked/updatefailed	网站 URL 过滤列表	否	是

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

事件消息	事件类型	目标类型	事件发生前记录的当前对象字段	事件发生后记录的已更新对象字段
阻止的网站 URL 筛选类别删除失败	swa/websiteurlfiltercategory/blocked/deletefailed	网站 URL 过滤列表	否	是

允许的网站 URL 列表和筛选类别

事件消息	事件类型	目标类型	事件发生前记录的当前对象字段	事件发生后记录的更新对象字段
已创建允许的网站 URL 列表	swa/websiteurlfilteringlist/allowed/create	网站URL过滤列表	否	是
已更新允许的网站 URL 列表	swa/websiteurlfilteringlist/allowed/update	网站URL过滤列表	否	是
已删除允许的网站 URL 列表	swa/websiteurlfilteringlist/allowed/delete	网站URL过滤列表	否	是
允许的网站 URL 列表创建失败	swa/websiteurlfilteringlist/allowed/createfailed	网站URL过滤列表	否	是
允许的网站 URL 列表更新失败	swa/websiteurlfilteringlist/allowed/updatefailed	网站URL过滤列表	否	是
允许的网站 URL 列表删除失败	swa/websiteurlfilteri	网站URL过滤列表	否	是

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

事件消息	事件类型	目标类型	事件发生前记录的当前对象字段	事件发生后记录的更新对象字段
	nglist/allowed/deletefailed			
已创建允许的网站 URL 筛选类别	swa/websiteurlfiltercategory/allowed/create	网站URL过滤列表	否	是
已更新允许的网站 URL 筛选类别	swa/websiteurlfiltercategory/allowed/update	网站URL过滤列表	否	是
已删除允许的网站 URL 筛选类别	swa/websiteurlfiltercategory/allowed/delete	网站URL过滤列表	否	是
允许的网站 URL 筛选类别创建失败	swa/websiteurlfiltercategory/allowed/createfailed	网站 URL 过滤列表	否	是
允许的网站 URL 筛选类别更新失败	swa/websiteurlfiltercategory/allowed/updatefailed	网站 URL 过滤列表	否	是
允许的网站 URL 筛选类别删除失败	swa/websiteurlfiltercategory/allowed/deletefailed	网站 URL 过滤列表	否	是

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

重定向到远程浏览器隔离（以前称为 Secure Browser）网站 URL 列表和筛选类别

事件消息	事件类型	目标类型	事件发生前记录的当前对象字段	事件发生后记录的更新对象字段	
重定向到 Secure Browser 网站 URL 列表已创建	swa/websiteurlfilteringlist/redirected/create	网站URL过滤列表	否	是	
重定向到 Secure Browser 网站 URL 列表已更新	swa/websiteurlfilteringlist/redirected/update	网站 URL 过滤列表	否	是	
重定向到安全浏览器网站 URL 列表已删除	swa/websiteurlfilteringlist/redirected/delete	网站 URL 过滤列表	否	是	
重定向到安全浏览器网站 URL 列表创建失败	swa/websiteurlfilteringlist/redirected/createfailed	网站 URL 过滤列表	否	是	
重定向到安全浏览器网站 URL 列表更新失败	swa/websiteurlfilteringlist/redirected/updatedfailed	网站URL过滤列表	否	是	
重定向到安全浏览器网站 URL 列表删除失败	swa/websiteurlfilteringlist/redirected/deletefailed	网站URL过滤列表	否	是	

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

事件消息	事件类型	目标类型	事件发生前记录的当前对象字段	事件发生后记录的更新对象字段	
重定向到安全浏览器网站 URL 筛选类别已创建	swa/websiteurlfiltercategory/redirected/create	网站URL过滤列表	否	是	
重定向到安全浏览器网站 URL 筛选类别已更新	swa/websiteurlfiltercategory/redirected/update	网站 URL 过滤列表	否	是	
重定向到安全浏览器网站 URL 筛选类别已删除	swa/websiteurlfiltercategory/redirected/delete	网站 URL 过滤列表	否	是	
重定向到安全浏览器网站 URL 筛选类别创建失败	swa/websiteurlfiltercategory/redirected/createfailed	网站 URL 过滤列表	否	是	
重定向到安全浏览器网站 URL 筛选类别更新失败	swa/websiteurlfiltercategory/redirected/updatefailed	网站URL过滤列表	否	是	
重定向到安全浏览器网站URL过滤类别删除失败	swa/websiteurlfiltercategory/redirected/deletefailed	网站URL过滤列表	否	是	

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

Citrix® StoreFront Cloud 的系统日志事件

本文介绍了系统日志为 StoreFront Cloud 捕获的事件数据。有关系统日志事件数据的更多信息，请参阅系统日志事件参考。

要了解有关系统日志的更多信息，请参阅系统日志。

商店 URL

事件消息	事件类型	目标类型	参与者 ID	事件发生前记录的当前对象字段	事件发生后记录的更新对象字段
工作区 URL 已更新	wxp/url/update	订阅者	更新了 URL 的管理员	是	是
更新 Workspace URL 失败	wxp/url/updatefailed	订阅者	尝试更新 URL 的管理员	是	是
Workspace URL 已启用	wxp/url/enable	订阅者	启用 Workspace URL 自定义的管理员	否	是
启用 Workspace URL 失败	wxp/url/enablefailed	订阅者	尝试启用工作区 URL 自定义功能的管理员	否	是
工作区 URL 已禁用	wxp/url/disable	订阅者	禁用工作区 URL 自定义功能的管理员	否	是
禁用工作区 URL 失败	wxp/url/disablefailed	订阅者	尝试禁用工作区 URL 自定义功能的管理员	否	是

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

StoreFront 身份验证

事件消息	事件类型	目标类型	参与者 ID	事件发生前记录的当前对象字段	事件发生后记录的更新对象字段
工作区身份提供程序已更新	wxp/identityprovider/update	订阅者	更新工作区身份验证方法的管理员	是	是
未能更新工作区身份提供程序	wxp/identityprovider/updatefailed	订阅者	尝试更新工作区身份验证方法的管理员	是	是

Citrix 联合身份验证服务

事件消息	事件类型	目标类型	参与者 ID	事件发生前记录的当前对象字段	事件发生后记录的已更新对象字段
工作区联合身份验证服务 (FAS) 已启用	wxp/fas/enable	订阅者	启用 FAS 的管理员	否	是
启用 Workspace 联合身份验证服务 (FAS) 失败	wxp/fas/enablefailed	订阅者	尝试启用 FAS 的管理员	否	是
Workspace 联合身份验证服务 (FAS) 已禁用	wxp/fas/disable	订阅者	禁用 FAS 的管理员	否	是
未能禁用 Workspace 联合身份验证服务 (FAS)	wxp/fas/disablefailed	订阅者	尝试禁用 FAS 的管理员	否	是

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

收藏夹

事件消息	事件类型	目标类型	参与者 ID	事件发生前记录的当前对象字段	事件发生后记录的更新对象字段
Workspace 收藏夹已启用	wxp/favorites/enable	订阅者	启用收藏夹的管理员	否	是
启用 Workspace 收藏夹失败	wxp/favorites/enablefailed	订阅者	尝试启用收藏夹的管理员	否	是
Workspace 收藏夹已禁用	wxp/favorites/disable	订阅者	禁用收藏夹的管理员	否	是
禁用 Workspace 收藏夹失败	wxp/favorites/disablefailed	订阅者	尝试禁用收藏夹的管理员	否	是

更改密码

事件消息	事件类型	目标类型	参与者 ID	事件发生前记录的当前对象字段	事件发生后记录的更新对象字段
Workspace 更改密码选项策略已更新	wxp/changepasswordoptions/updatepolicy	订阅者	更新了 Citrix Workspace 中更改密码策略的管理员	是	是
未能更新 Workspace 更改密码选项策略	wxp/changepasswordoptions/updatepolicyfailed	订阅者	尝试更新 Citrix Workspace 中更改密码策略的管理员	是	是

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

事件消息	事件类型	目标类型	参与者 ID	事件发生前记录的当前对象字段	事件发生后记录的更新对象字段
Workspace 更改密码选项已启用	wxp/changepasswordoptions/enable	订阅者	启用了 Citrix Workspace 中更改密码设置的管理员	否	是
未能启用 Workspace 更改密码选项	wxp/changepasswordoptions/enablefailed	订阅者	尝试在 Citrix Workspace 中启用更改密码设置的管理员	否	是
Workspace 更改密码选项已禁用	wxp/changepasswordoptions/disable	订阅者	在 Citrix Workspace 中禁用更改密码设置的管理员	否	是
未能禁用 Workspace 更改密码选项	wxp/changepasswordoptions/disablefailed	订阅者	尝试禁用 Citrix Workspace 中更改密码设置的管理员	否	是

长期令牌

事件消息	事件类型	目标类型	参与者 ID	事件发生前记录的当前对象字段	事件发生后记录的更新对象字段
Workspace 长期令牌配置已更新	wxp/longlivedtoken/update	订阅者	更新了令牌配置的管理员	是	是
未能更新 Workspace 长期令牌配置	wxp/longlivedtoken/updatefailed	订阅者	尝试更新令牌配置的管理员	是	是

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

Web 不活动超时

事件消息	事件类型	目标类型	参与者 ID	事件发生前记录的当前对象字段	事件后记录的已更新对象字段
Workspace 会话配置已更新	wxp/sessions/update	订阅者	更新了“Web 不活动超时”设置的空闲时间的管理员	是	是
更新 Workspace 会话配置失败	wxp/sessions/updatefailed	订阅者	尝试更新“Web 不活动超时”设置的空闲时间的管理员	是	是

功能发布

事件消息	事件类型	目标类型	参与者 ID	事件发生前记录的当前对象字段	事件发生后记录的更新对象字段
为智能 Workspace 体验更新了分配的用户和组	wxp/iws/features/updateusersgroups	订阅者	更新了分配的用户和组以访问 Citrix Workspace 中活动源通知的管理员	否	否
未能为智能 Workspace 体验分配更新的用户和组	wxp/iws/features/updateusersgroupsfailed	订阅者	尝试更新分配的用户和组以访问 Citrix Workspace 中活动源通知的管理员	否	否
智能工作区体验已启用	wxp/iws/features/enable	订阅者	在 Citrix Workspace 中启用活动	否	否

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

事件消息	事件类型	目标类型	参与者 ID	事件发生前记录的当前对象字段	事件发生后记录的更新对象字段
			源通知的管理员		
未能启用智能工作区体验	wxp/iws/features/enablefailed	订阅者	尝试在 Citrix Workspace 中启用活动源通知的管理员	否	否
智能工作区体验已禁用	wxp/iws/features/disable	订阅者	在 Citrix Workspace 中禁用活动源通知的管理员	否	否
未能禁用智能 Workspace 体验	wxp/iws/features/disablefailed	订阅者	尝试在 Citrix Workspace 中禁用活动源通知的管理员	否	否

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

SDK 和 API

Citrix Cloud™ 提供多个 API，可用于检索信息并自动执行复杂和重复性任务，包括：

- 静默安装 Citrix Cloud Connector™
- 创建和使用报告以管理云许可证
- 确定客户的授权状态
- 向 Citrix Cloud 管理员发送通知
- 检索系统日志事件
- 检索有关您的资源位置的详细信息，以与其他 API 配合使用

多个 Citrix Cloud 服务也提供 SDK 和 API，可让您检索信息、查询数据并执行管理任务。

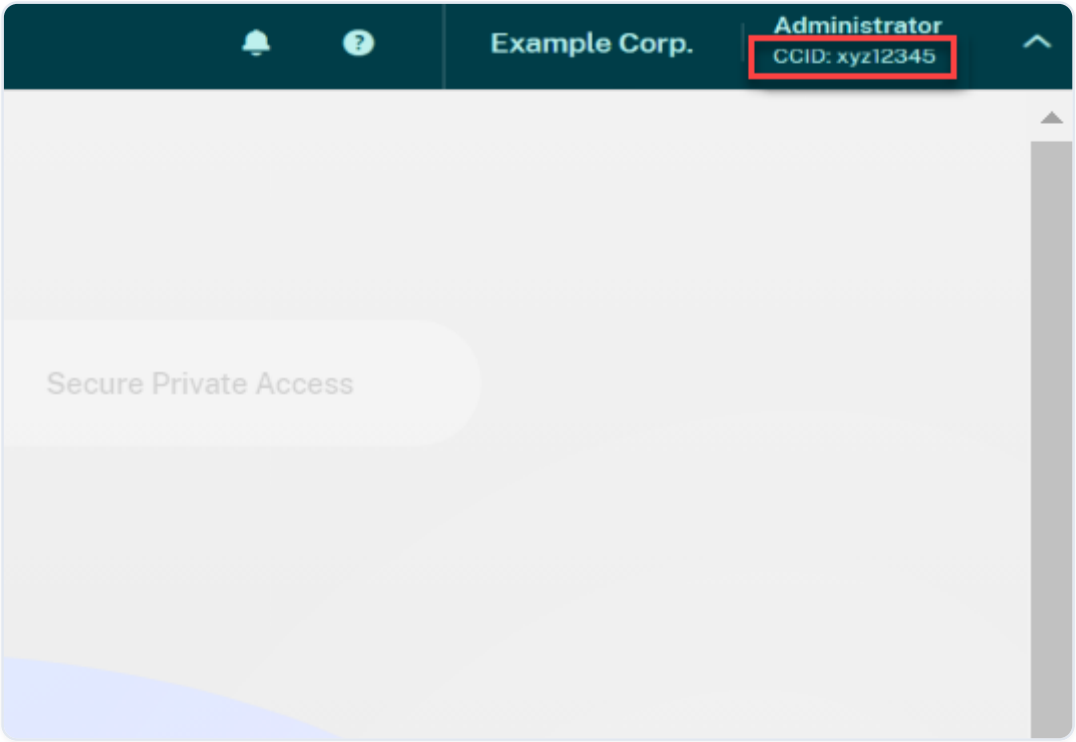
您可以通过安全客户端或服务主体访问 API。

服务主体

要使用 Citrix Cloud API，您需要创建一个服务主体，代表您访问 Citrix Cloud。要创建服务主体，您需要提供 Citrix Cloud 帐户的客户 ID。您的客户 ID 位于管理控制台中的以下位置：

- 控制台的右上角，在您的用户名下方。

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



- 您的**帐户设置**页面。

  突出显示“帐户设置”的客户菜单(/en-us/citrix-cloud/media/customer-id-acct-settings-page.png)

- **API 访问**页面。

  API 访问示例(/en-us/citrix-cloud/media/api-access-example.png)

云许可 API

企业客户可以使用云许可 API 执行管理任务，例如导出使用情况数据和释放已分配的许可证。Citrix 合作伙伴可以使用这些 API 检索本地 Citrix Virtual Apps and Desktops™ 和 Citrix DaaS 的摘要和历史数据。

有关详细信息，请参阅 Citrix Developer 文档中的管理 Citrix 云许可的 API。

SystemLog API

SystemLog API 允许您检索在指定时间段内 Citrix Cloud 帐户中发生的事件。有关使用此 API 的更多信息，请参阅 Citrix Developer 文档中的 Citrix Cloud - SystemLog。

资源位置 API

资源位置 API 允许您检索有关资源位置的信息，以便与其他应用程序和脚本一起使用。例如，假设您想在 Citrix Cloud 帐户中的多个资源位置之一中静默安装 Citrix Cloud Connector。您可以使用此 API 检索资源位置 ID 并将其传递给安装脚本。

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

有关使用此 API 的更多信息，请参阅 Citrix Developer 文档中的 Citrix Cloud - 资源位置。

服务授权 API

服务授权 API 检索客户有权使用的服务、每个授权的剩余天数以及客户购买的授权数量。有关使用此 API 的更多信息，请参阅 Citrix Developer 文档中的 Citrix Cloud - 服务授权。

通知 API

通知 API 允许您向其他 Citrix Cloud 管理员发送消息。收件人通过管理控制台中的 通知 页面接收您的消息。有关使用此 API 的更多信息，请参阅 创建和查看通知。

其他服务的 SDK 和 API

有关适用于其他 Citrix Cloud 服务的 SDK 和 API 的更多信息，请参阅以下文章：

- Citrix® StoreFront Cloud：包括适用于 StoreFront Cloud 的 SDK 和 API。
- 应用程序交付和安全性：包括适用于网络和应用程序交付服务（如 Console 和 SD-WAN Orchestrator）的 SDK 和 API。

更多信息

要了解有关 Citrix Cloud API 如何帮助您执行复杂操作（例如迁移到云以及使用推送令牌配置身份验证）的更多信息，请参阅以下 Tech Zone 文章：

- 部署指南：将 思杰虚拟应用和桌面 从 威睿 vSphere 迁移到 微软 Azure 上的 思杰虚拟应用和桌面 服务
- PoC 指南：自动化配置工具

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

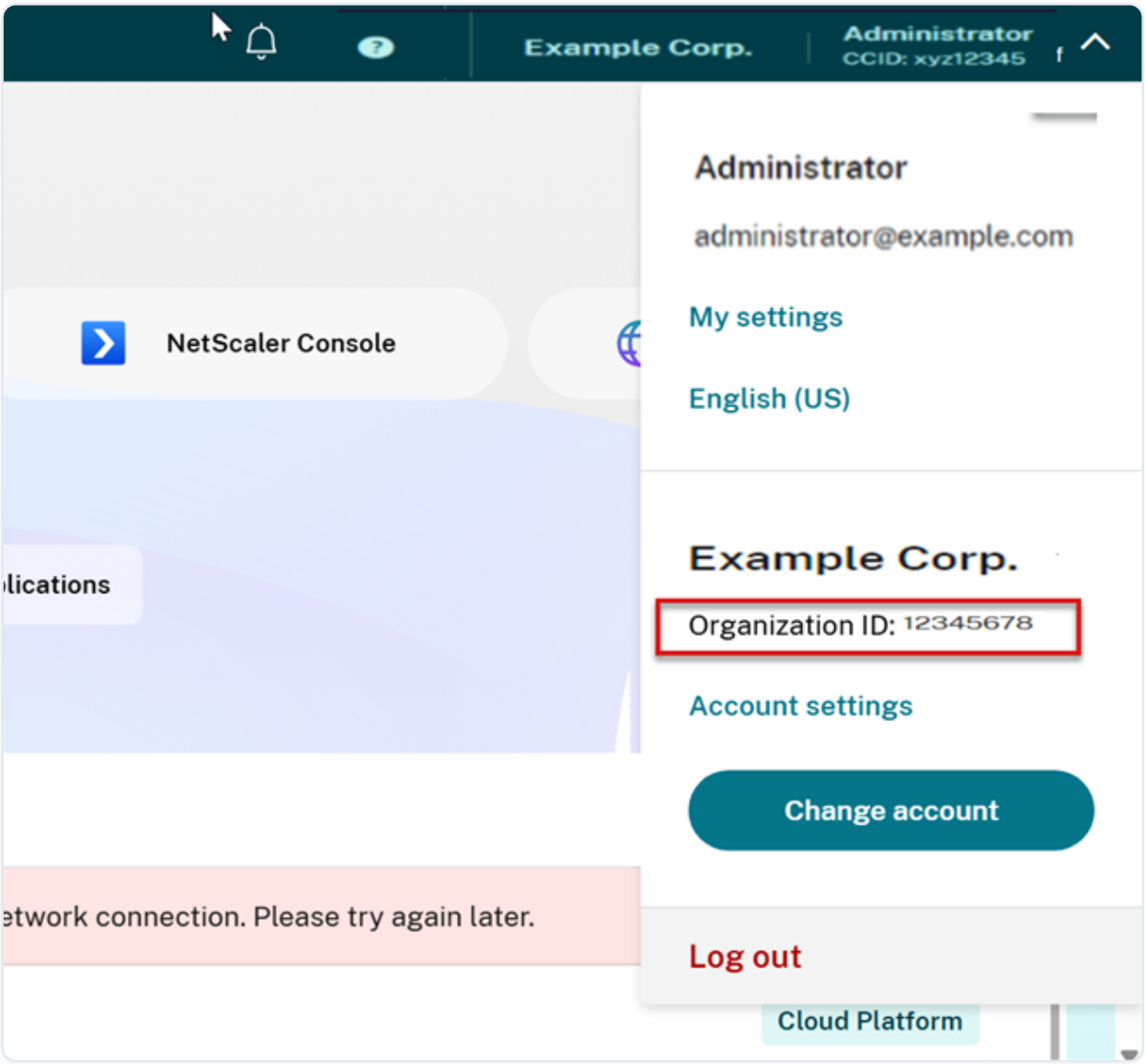
Citrix Cloud™ 面向合作伙伴

Citrix Cloud 包含专为客户和合作伙伴设计的服务、功能和体验。本节概述了 Citrix 合作伙伴可用的功能，这些功能可帮助他们与客户协作处理 Citrix Cloud 服务和解决方案。

合作伙伴身份识别

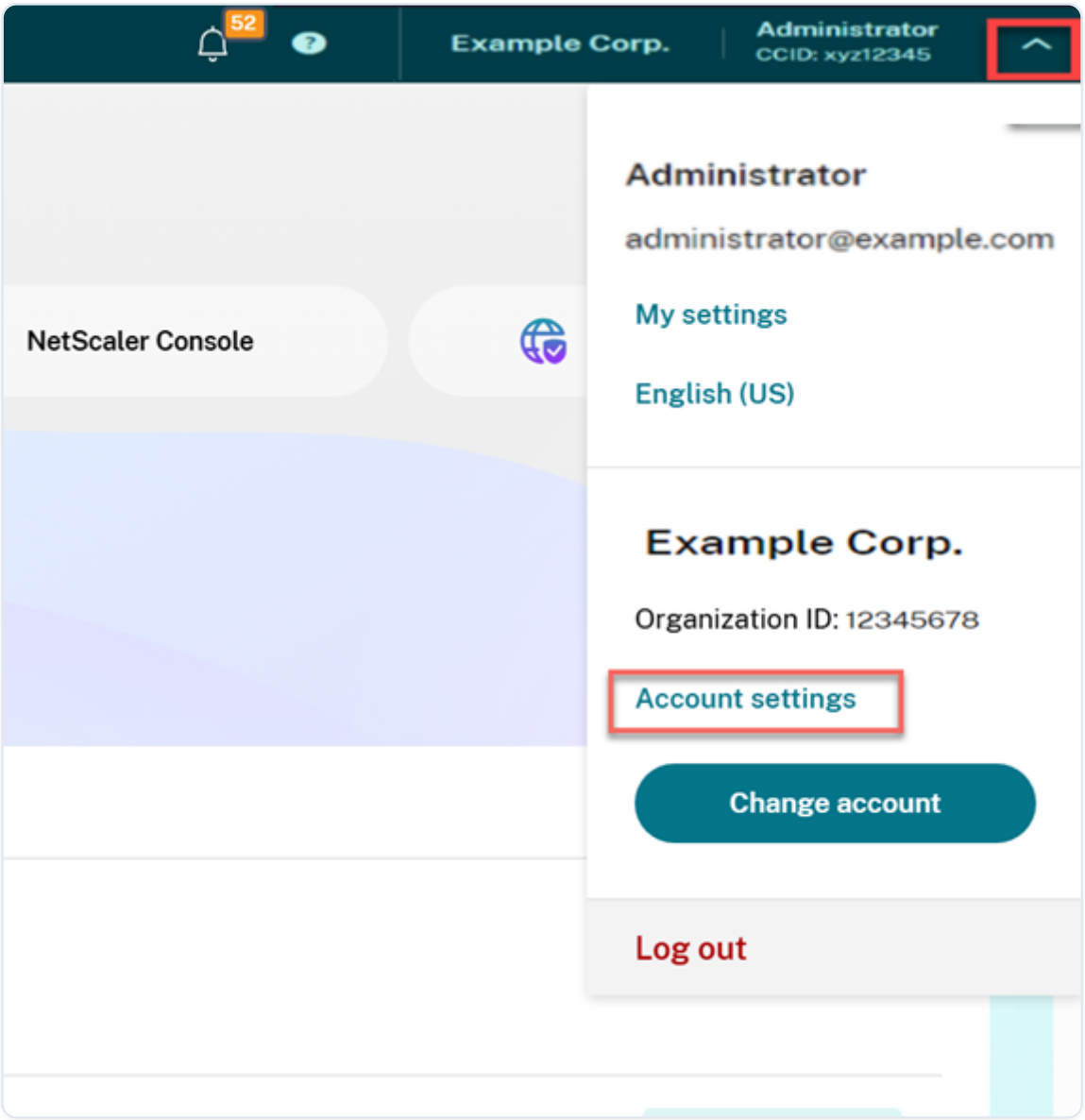
Citrix Cloud 根据 Citrix 组织 ID (ORGID) 识别合作伙伴。合作伙伴可以在 Citrix Cloud 管理控制台的以下位置查看与其 Citrix Cloud 帐户关联的 ORGID：

- 从客户菜单中。单击控制台右上角的客户名称。您的 ORGID 将显示在菜单中的公司名称下方。



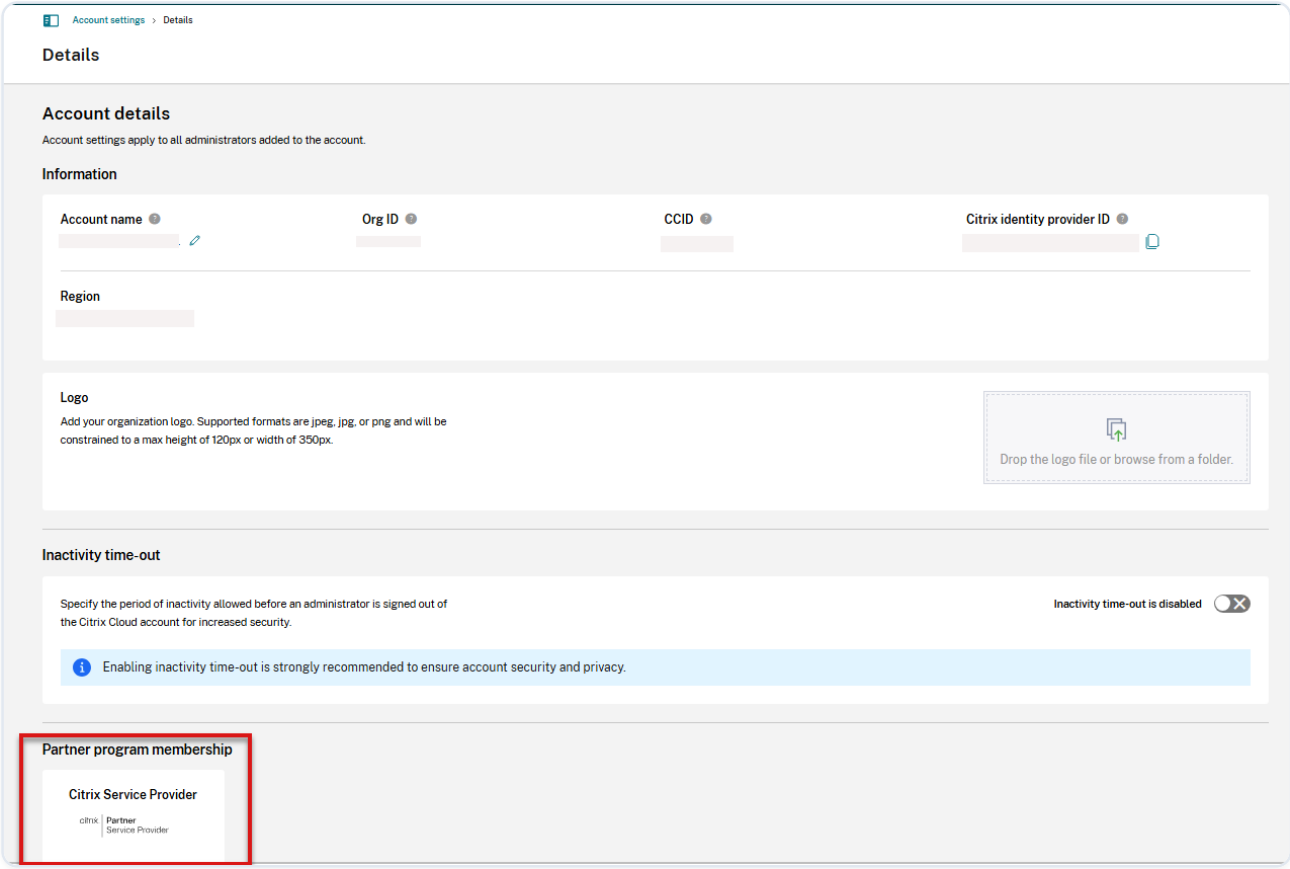
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 从右上角的客户菜单中，选择**帐户设置**。



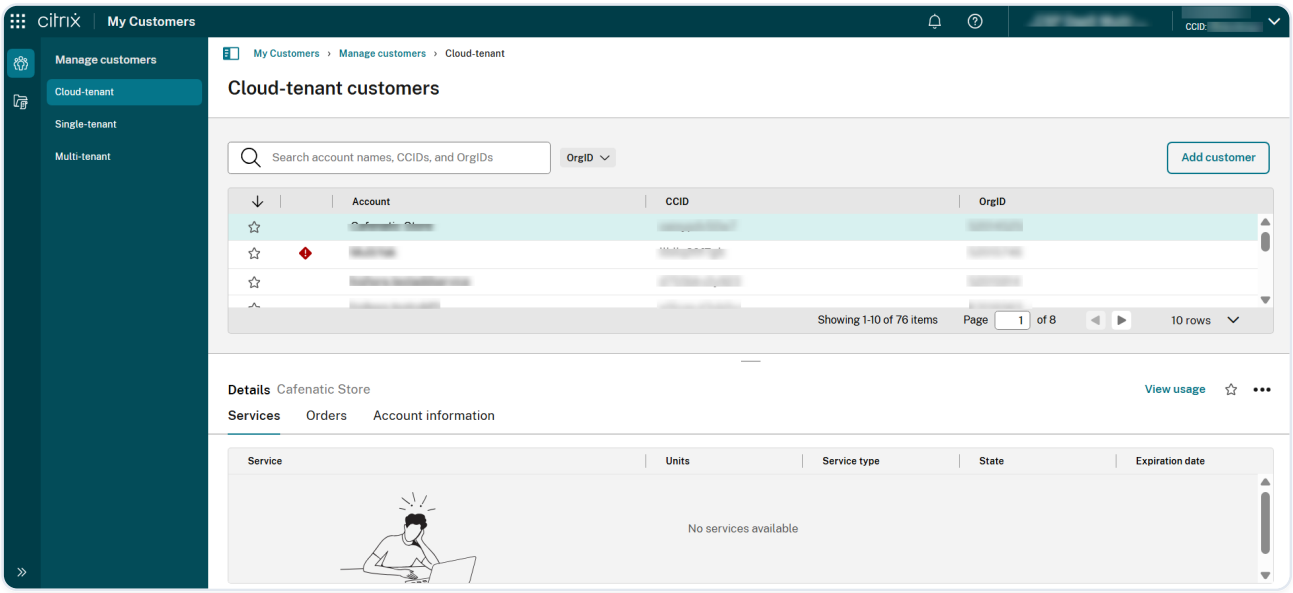
如果帐户上的 ORGID 是 Citrix 合作伙伴计划（例如 Citrix Solution Advisor 或 Citrix Service Provider™）的活跃成员，则计划徽章表示此帐户归 Citrix 合作伙伴所有。然后，合作伙伴身份识别用于管理对其他云服务或功能的访问。

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



客户控制板

我的客户控制板旨在供合作伙伴以整合视图查看多个 Citrix Cloud 客户的状态。要使客户显示在控制板上，必须在合作伙伴和客户之间建立连接。我的客户控制板在具有合作伙伴徽章的 Citrix Cloud 帐户上可用。



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

谁可以查看客户控制板?

默认情况下，完全访问权限管理员可以查看客户控制板。如果选择了**客户控制板**权限，自定义访问权限管理员可以查看控制板。有关 Citrix Cloud 中管理员权限的更多信息，请参阅修改管理员权限。

自定义访问管理员权限，突出显示类别和客户仪表板(/en-us/citrix-cloud/media/csp-customer-dashboard-permission-new.png)

合作伙伴与客户的连接

与客户协作开发 Citrix Cloud 解决方案的合作伙伴可以在其帐户之间建立信任链接。这种帐户级别的关系允许客户轻松地与合作伙伴共享特定信息。通过与合作伙伴建立连接，客户授予合作伙伴查看其 Citrix Cloud 帐户信息以及其与 Citrix 关系信息的权限。

建立合作伙伴连接可实现以下功能：

- 客户显示在合作伙伴的仪表板上
- 合作伙伴显示为客户帐户设置中的活动连接
- 合作伙伴可以查看 Citrix Cloud 服务权利
- 合作伙伴可以查看 Citrix Cloud 权利的许可证使用情况和活动使用情况

在合作伙伴和客户建立连接后，合作伙伴管理员可以查看客户的基本帐户信息、客户下的订单以及权利信息，例如服务、许可证数量和到期日期。

合作伙伴与客户的连接不会过期。

与多个合作伙伴或客户的连接

合作伙伴可以与多个客户建立连接。或者，合作伙伴可以考虑删除他们不再需要管理的客户帐户。

客户可以与多个合作伙伴建立连接。客户到合作伙伴的连接数量没有限制。

连接通知

Citrix Cloud 在以下情况下向合作伙伴发送通知：

- 合作伙伴与客户建立连接
- 客户终止与合作伙伴的连接

当合作伙伴终止与客户的连接时，Citrix Cloud 会向客户发送通知。

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

合作伙伴对服务授权的可见性

连接到客户后，合作伙伴可以查看该客户的服务授权状态。此信息包括试用和非试用授权的状态。合作伙伴还可以查看以下信息：

- 活动服务授权（为客户购买或以其他方式授权或启用的服务）
- 授权的许可证数量和到期日期
- 活动服务试用
- 已过期服务试用

带有“服务”选项卡的合作伙伴控制面板(/en-us/citrix-cloud/media/partner-customer-services.png)

许可可见性仅限于查看许可证分配和历史使用趋势的摘要。

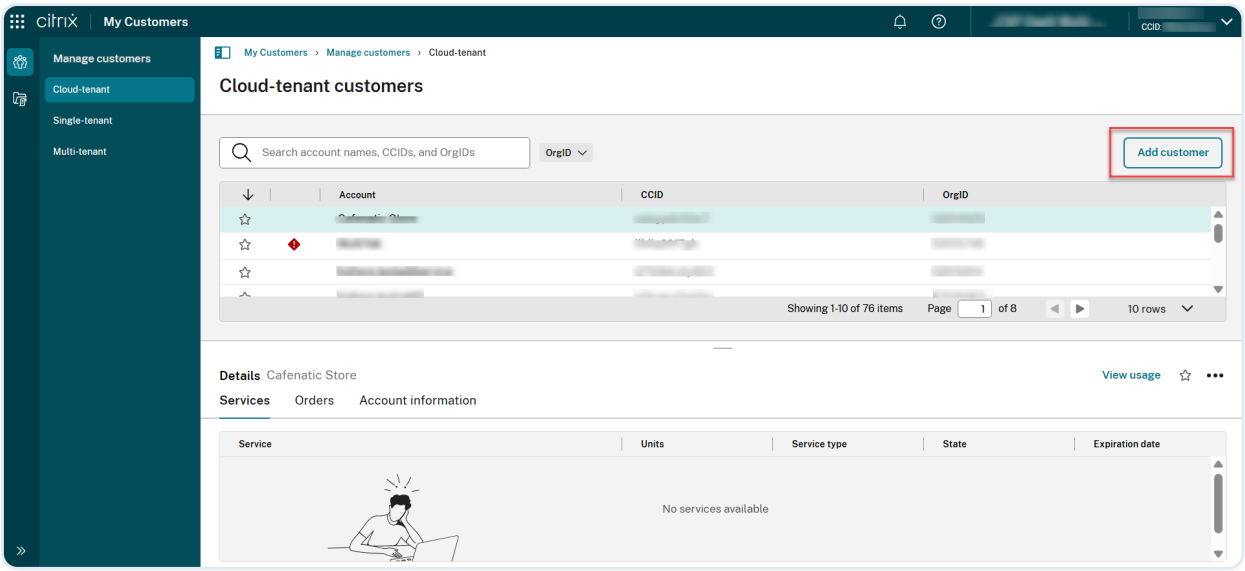
添加新客户

请按照以下步骤添加新客户：

1. 在 Citrix Cloud 菜单中，单击 **“我的客户”**。

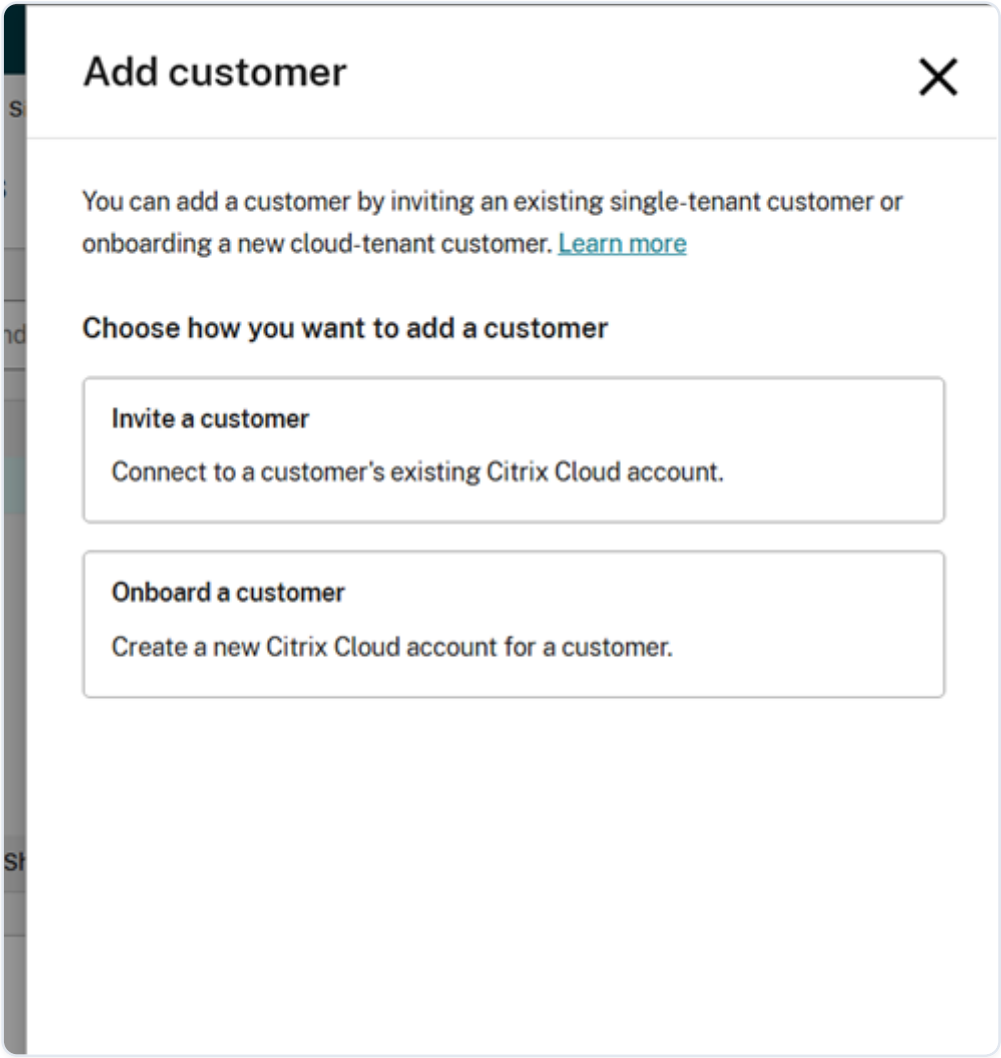
   我的客户(/en-us/citrix-cloud/media/my-customers.png)

2. 转到 **管理客户 > 云租户**，单击 **添加客户**。



3. 系统将提示您在以下选项之间进行选择，如下图所示。

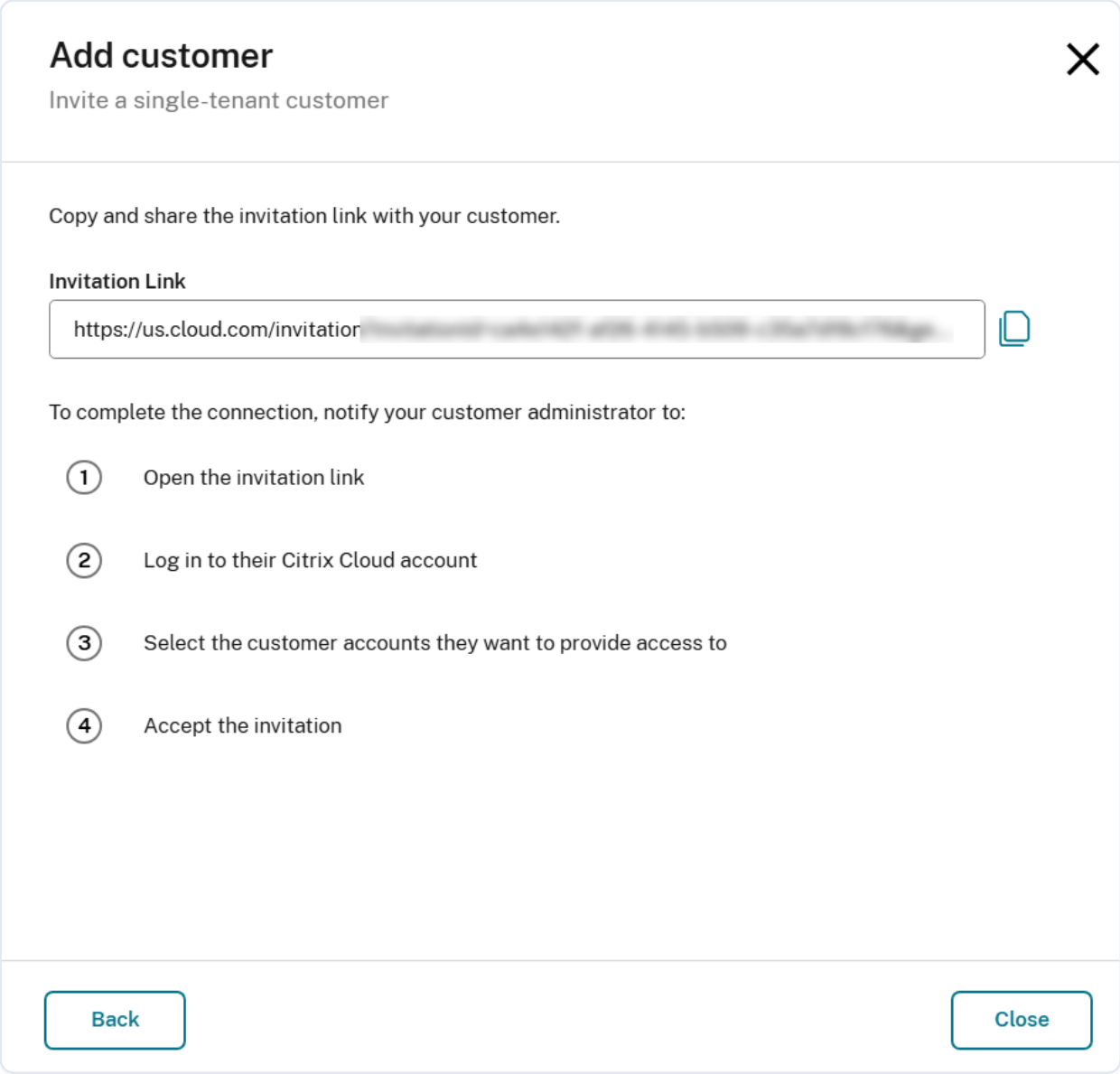
© 1997–2026 Citrix Systems, Inc. All rights reserved.



注意：

- **邀请客户**：使用此选项邀请现有的单租户客户。此受邀客户保留其自己唯一的 OrgID。

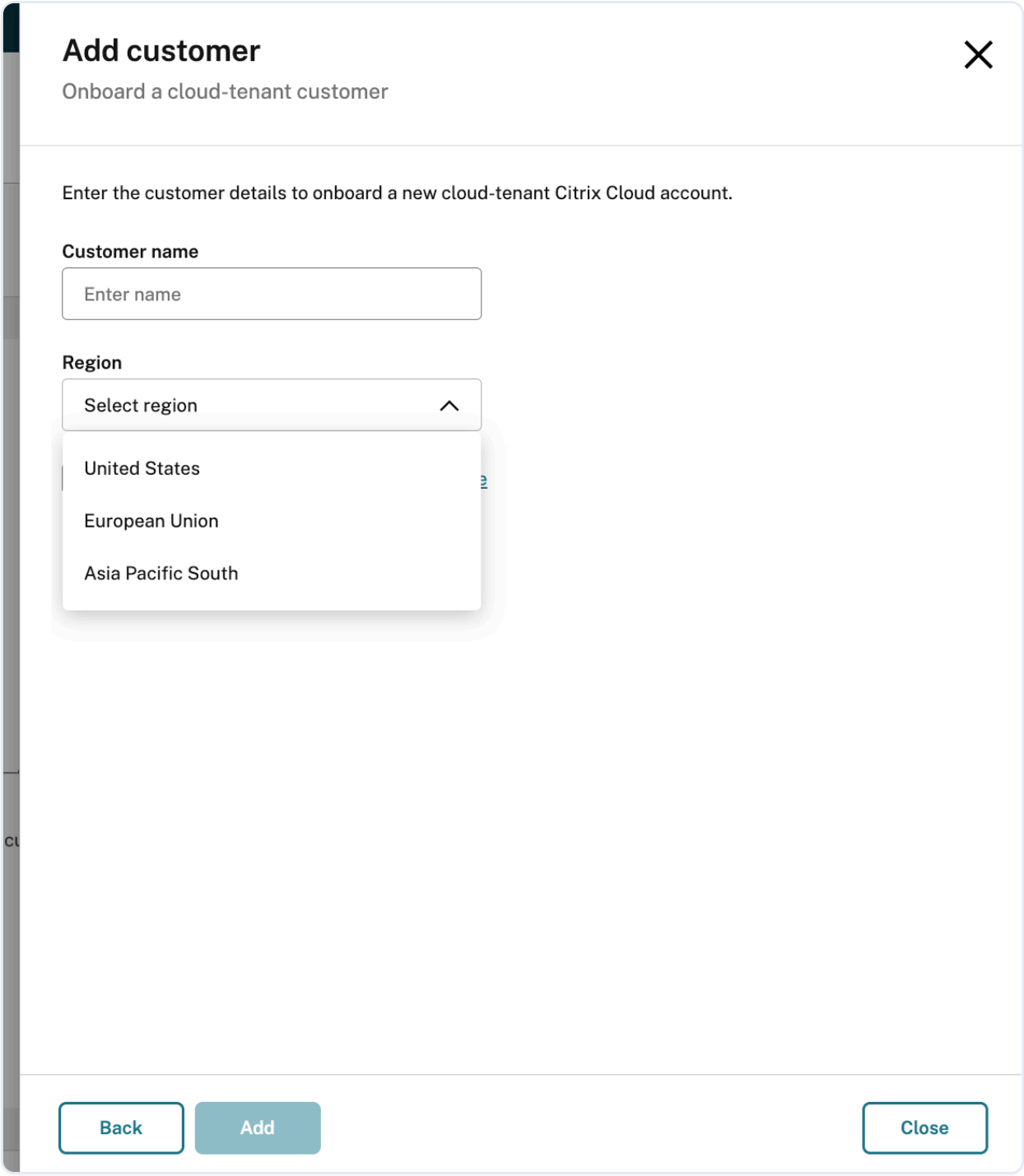
© 1997–2026 Citrix Systems, Inc. All rights reserved.



注意：

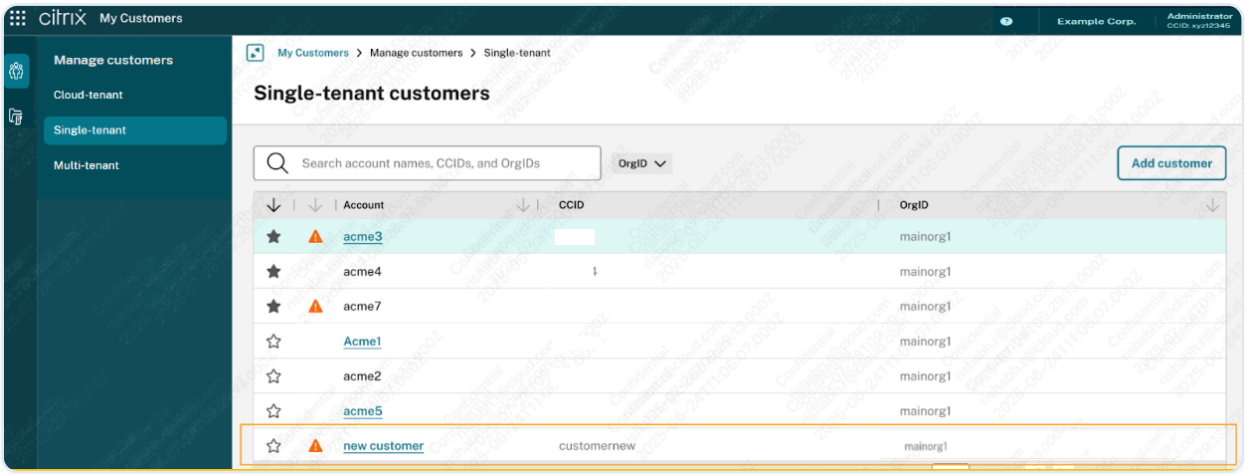
- **加入客户** 选项适用于加入单租户和多租户客户。此已加入客户与合作伙伴共享相同的 OrgID。

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

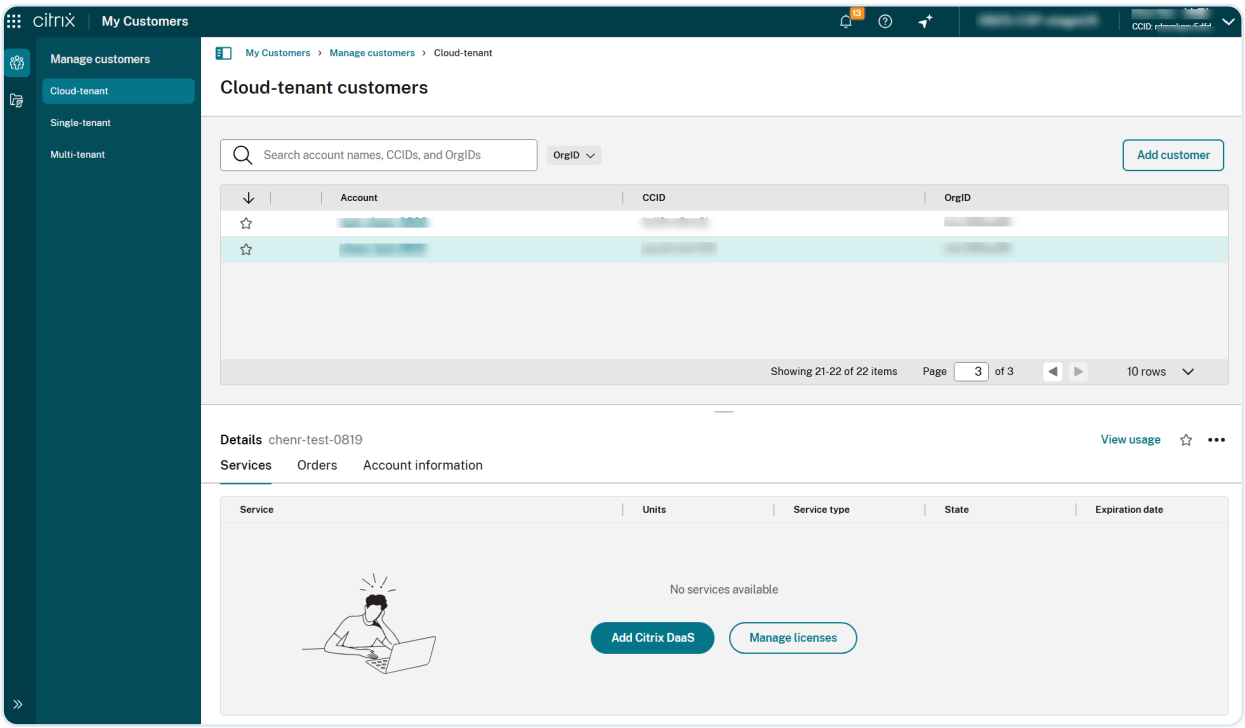


4. 通过 **邀请客户** 流程添加的客户显示在单租户客户列表中。此受邀客户拥有自己唯一的 OrgID。

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



5. 通过 **加入客户** 流程添加的客户显示在云租户客户列表中。此已加入客户与合作伙伴拥有相同的 OrgID。

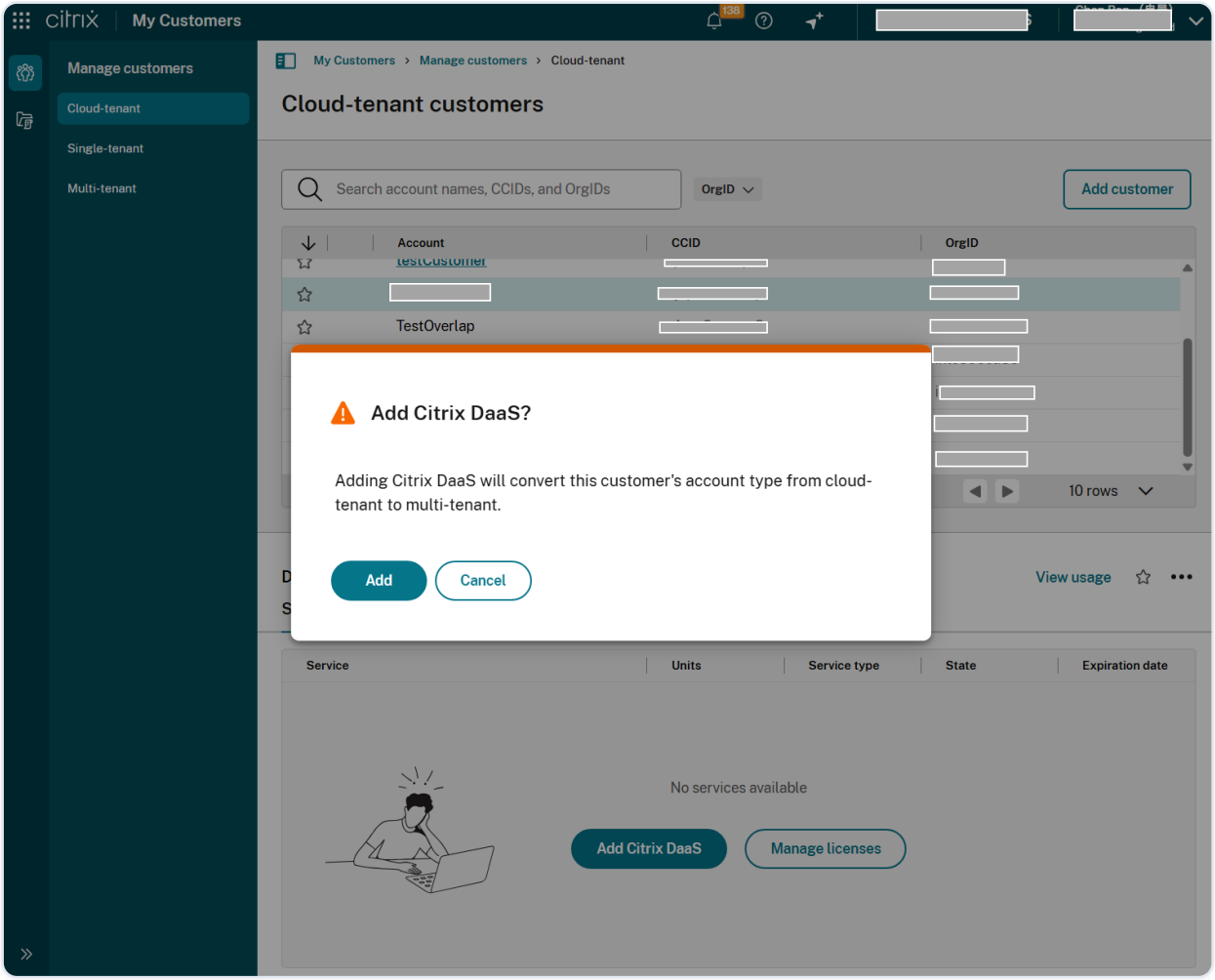


激活已添加的客户

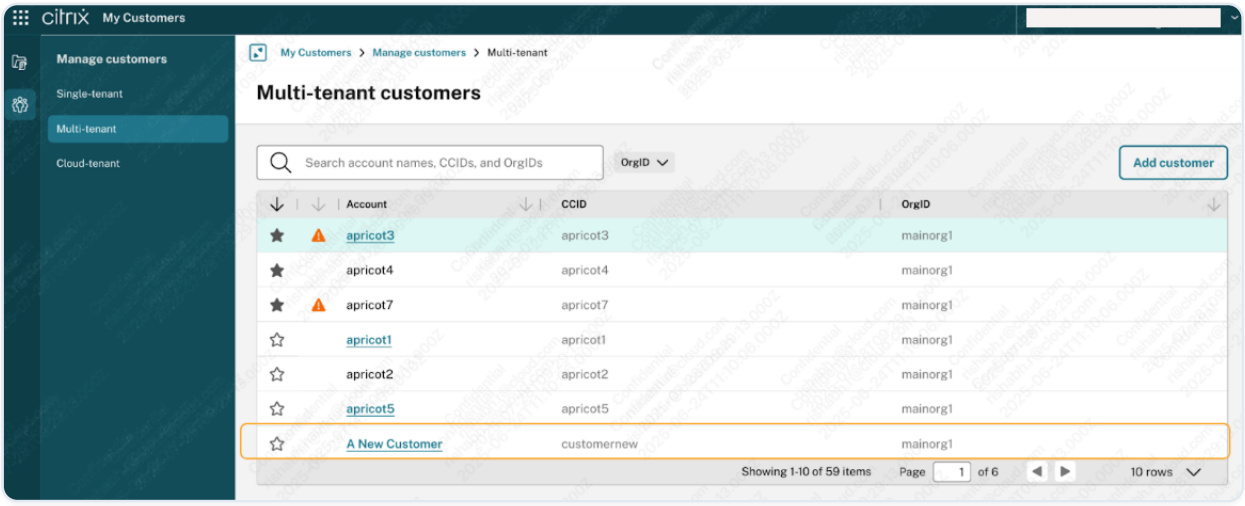
将云租户设为多租户 DaaS 客户

1. 转到**管理客户 > 云租户**，单击**添加 Citrix DaaS™**以分配**DaaS 服务**。

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



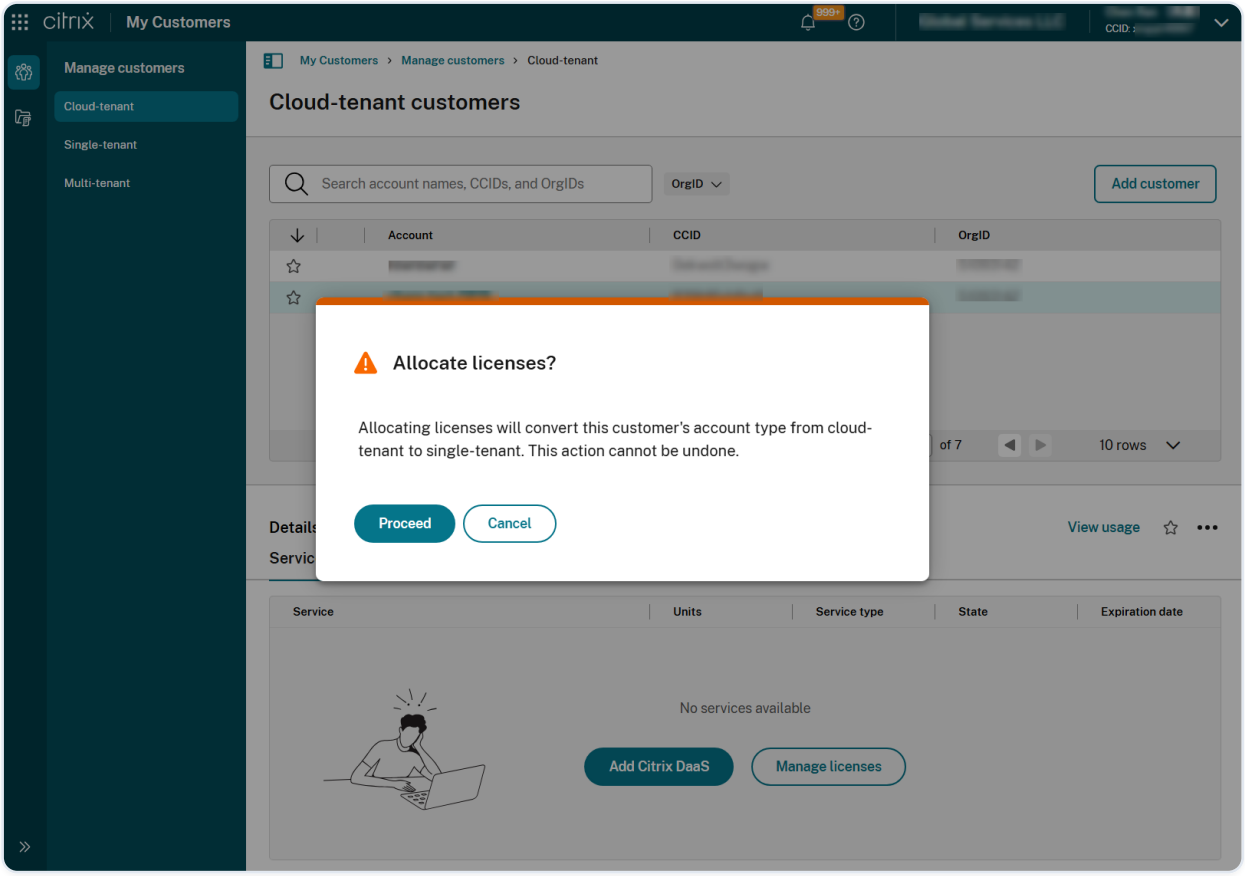
2. 客户将进入多租户客户列表。



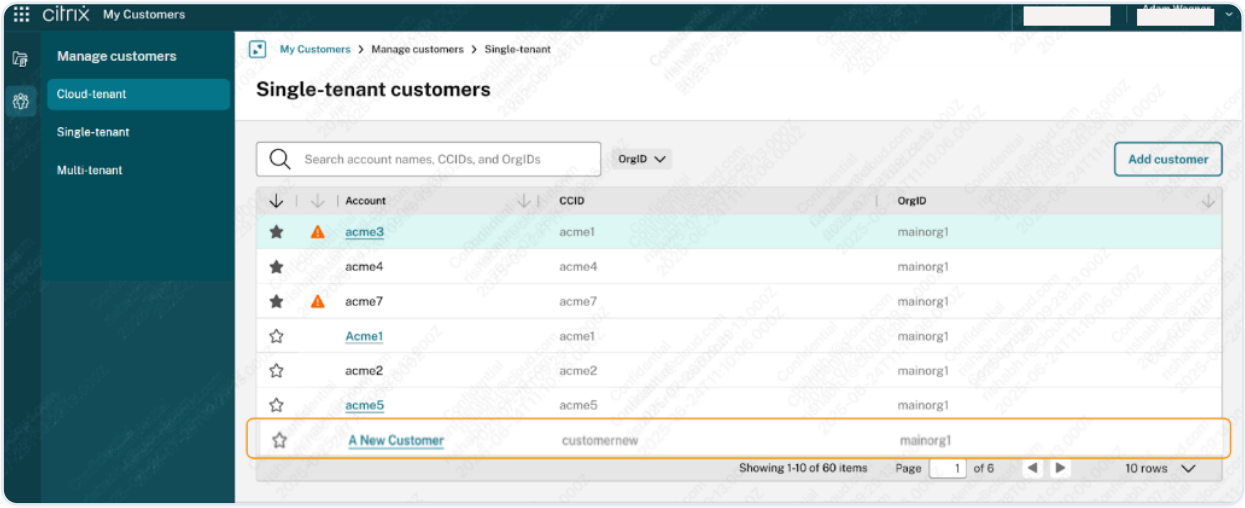
将云租户设为单租户客户

1. 转到**管理客户 > 云租户**，单击**管理许可证**以选择**分配许可证**。

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

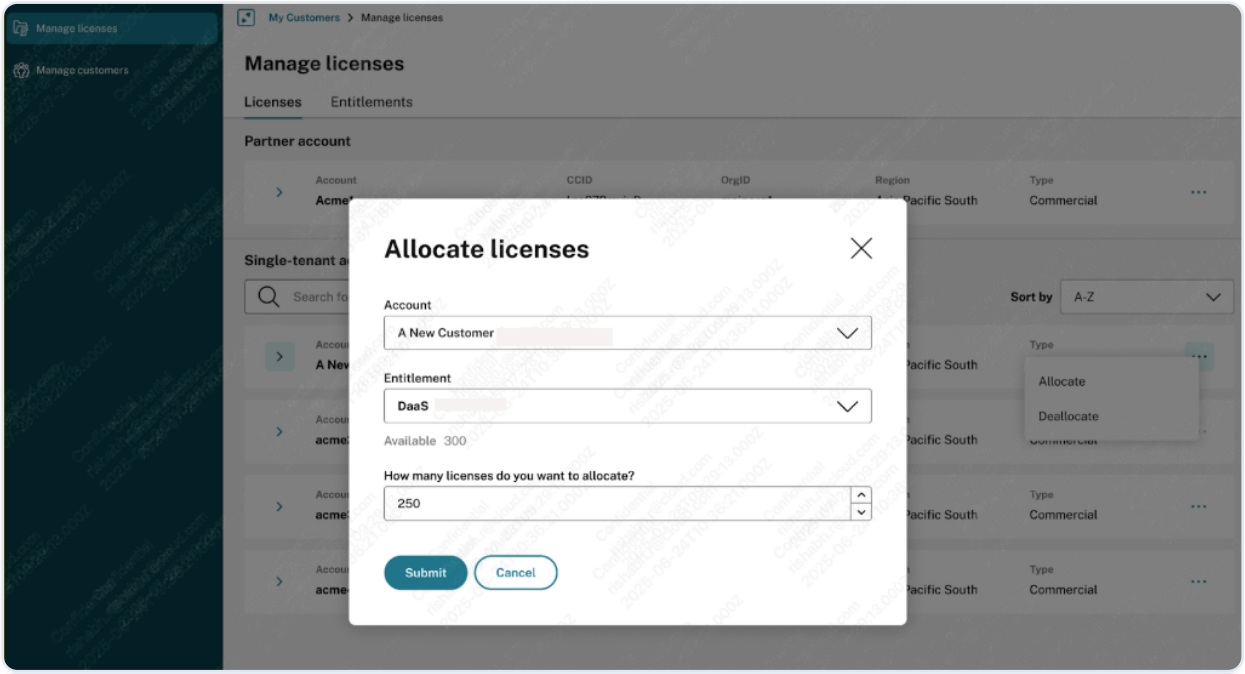


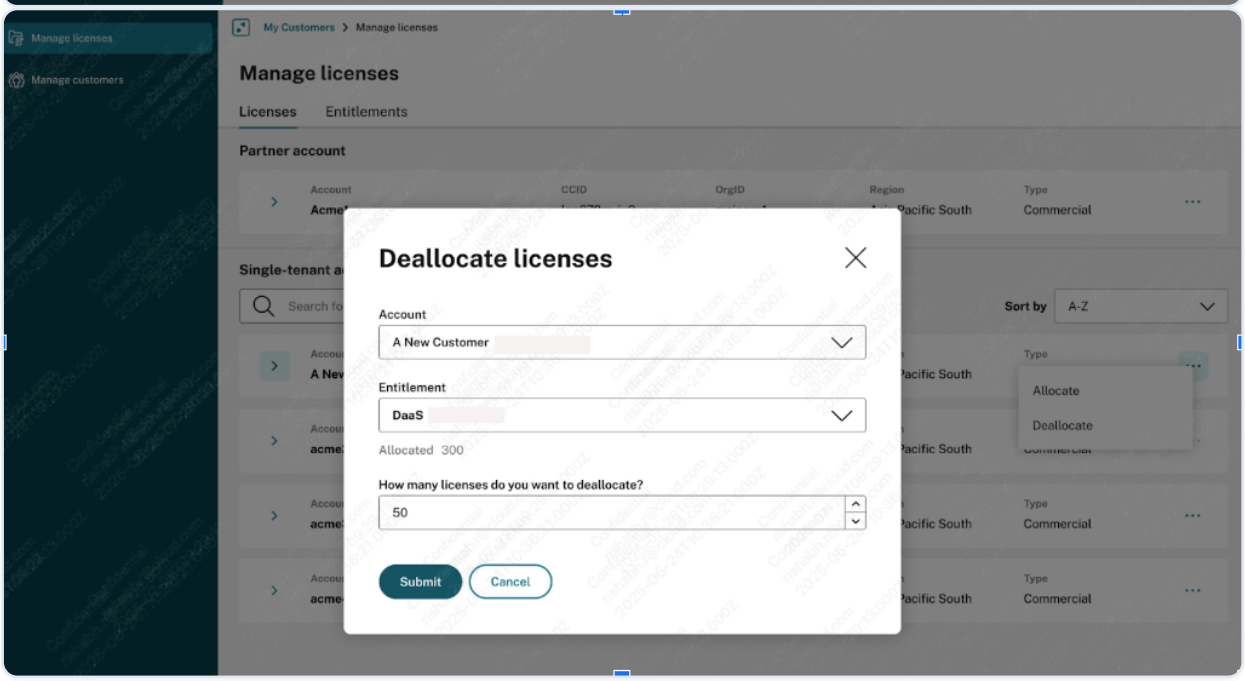
2. 客户将进入单租户客户列表。



3. 您可以通过选择**分配**或**取消分配**选项，从**管理许可证 > 许可证**选项卡更新许可证。

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

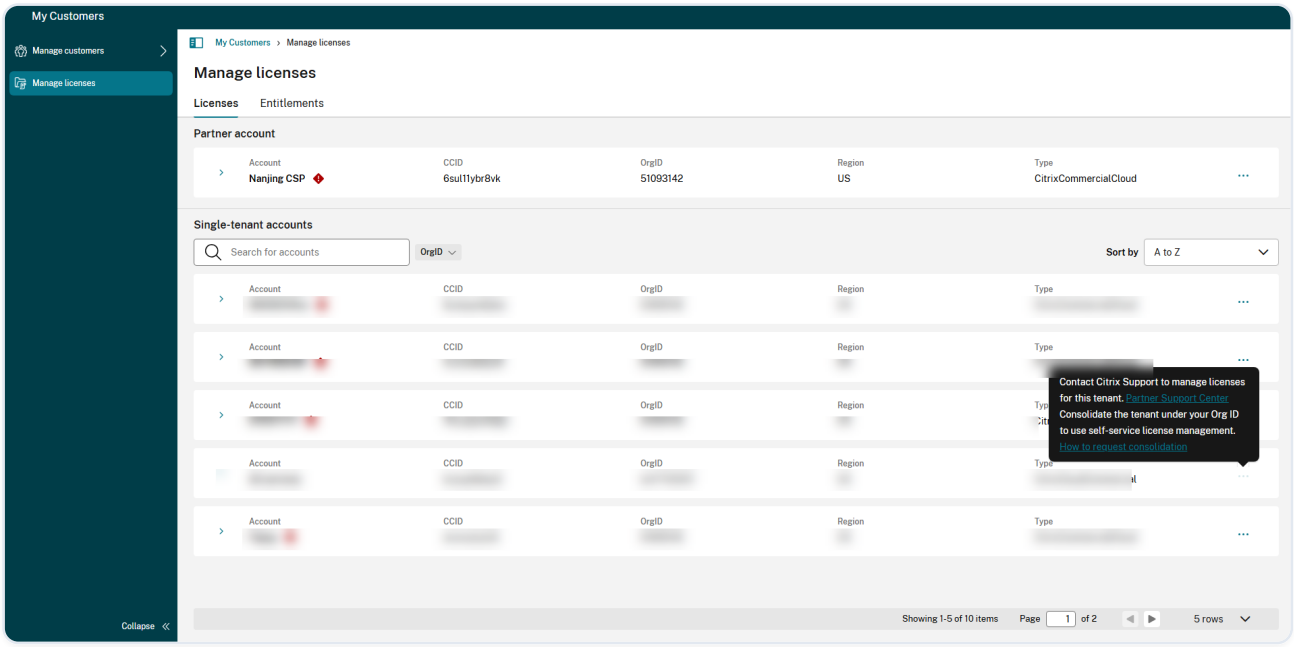




注意：

通过**邀请客户**选项添加的单租户客户拥有自己唯一的 OrgID。要为这些客户分配或取消分配许可证，合作伙伴必须联系 Citrix 客户服务。如果 CSP 希望以自助服务方式管理其单租户客户的许可证（分配或取消分配），则 CSP 必须按照 CTX695209 向 Citrix 提交案例，以将其单租户客户整合到 CSP 拥有的 OrgID 下。UI 中的消息将指导合作伙伴完成此过程。

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



与客户建立连接

合作伙伴使用唯一的邀请链接与客户建立连接。此链接是固定的，无法更改或自定义。

合作伙伴可以无限次使用其邀请链接来创建或重新创建连接。邀请链接不会过期。

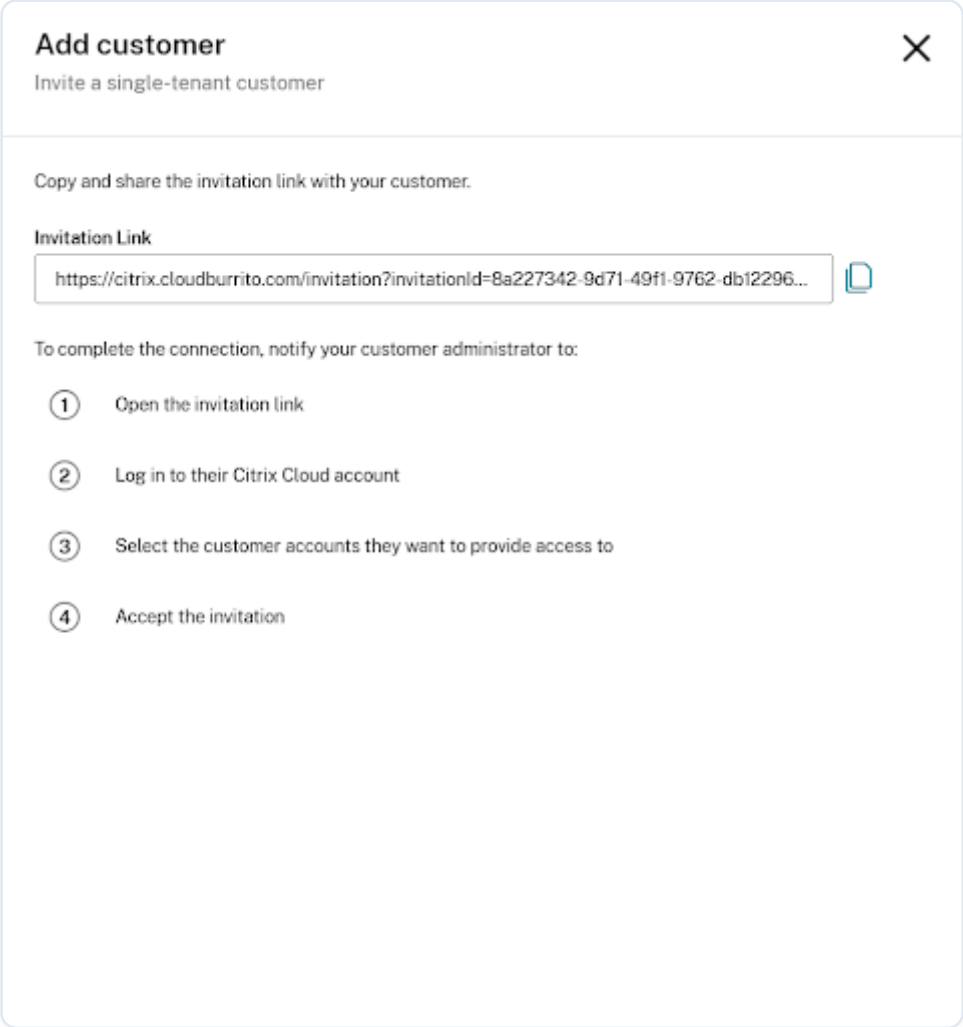
注意：

本节中描述的客户手动链接仅用于载入已拥有现有组织 ID 及其关联云帐户的单个租户客户。在 Citrix Cloud Commercial 中，合作伙伴可以与来自美国、欧盟和亚太地区的客户建立连接。

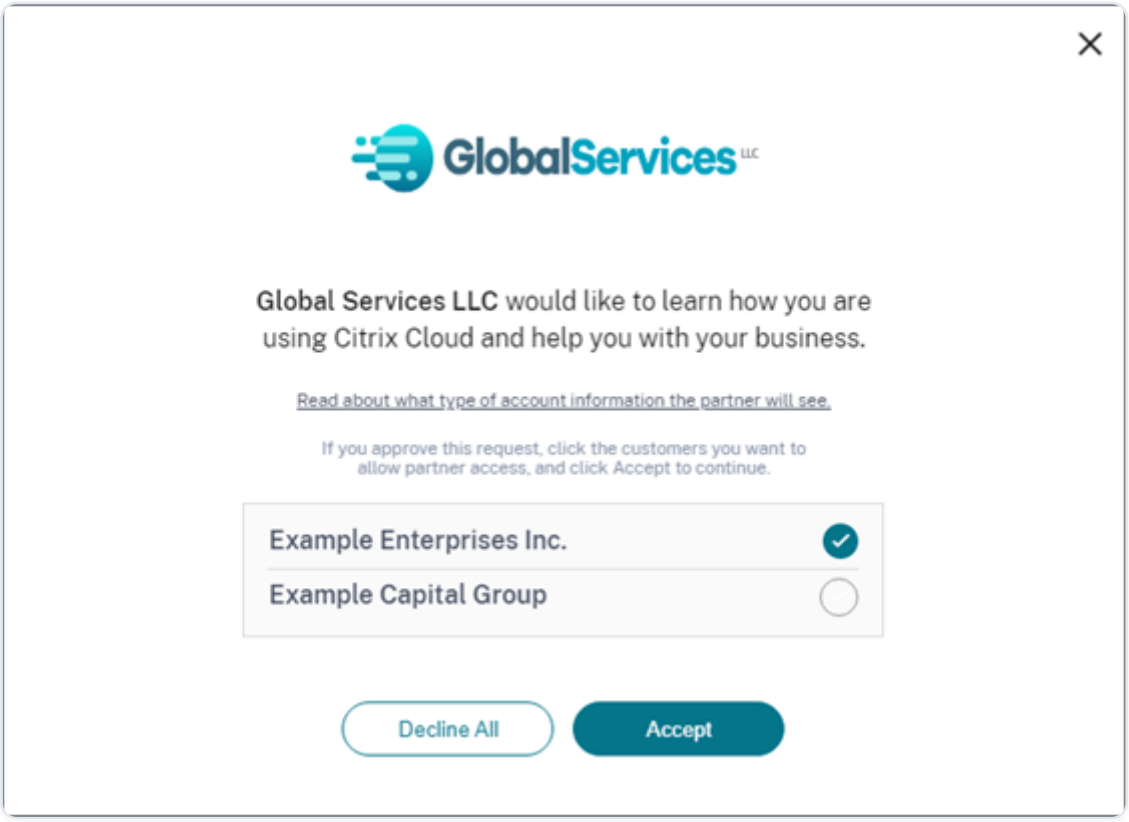
要创建连接：

1. 在 Citrix Cloud 菜单中，选择**我的客户**。
2. 在客户控制板侧边栏中，选择**管理客户**。
3. 要连接现有 Citrix Cloud 客户：
   a. 选择**添加客户**，然后选择**邀请单个租户客户**。
   b. 复制邀请链接并将其发送给客户。

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



要完成连接，客户需要单击邀请链接，登录 Citrix Cloud，然后接受邀请。



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

4. 要连接尚未拥有 Citrix Cloud 帐户的新客户：

   a. 选择 **添加客户**，然后选择 **载入客户**。

   b. 输入客户的业务联系方式，然后选择 **添加**。Citrix Cloud 会为客户创建一个新帐户。

   之后，客户会收到通知，确认合作伙伴已作为管理员添加到新帐户。客户可以使用 Citrix Cloud 登录页面上的“忘记密码？”链接为帐户设置密码。设置密码后，客户可以使用其业务电子邮件地址登录其帐户，并按照 (/zh-cn/citrix-cloud/overview/signing-up-for-citrix-cloud/signing-up-for-citrix-cloud) 中所述完成载入过程。

删除合作伙伴或客户连接

合作伙伴或客户都可以随时终止连接。

删除与客户的连接

要终止与客户的连接，合作伙伴请执行以下步骤：

1. 在控制台右上角的 Citrix Cloud 菜单中，选择 **我的客户**。
2. 在“客户控制板”中，找到要管理的客户。
3. 单击客户的省略号菜单，然后选择 **删除客户**。
4. 当系统提示确认删除时，选择 **删除**。

删除与合作伙伴的连接

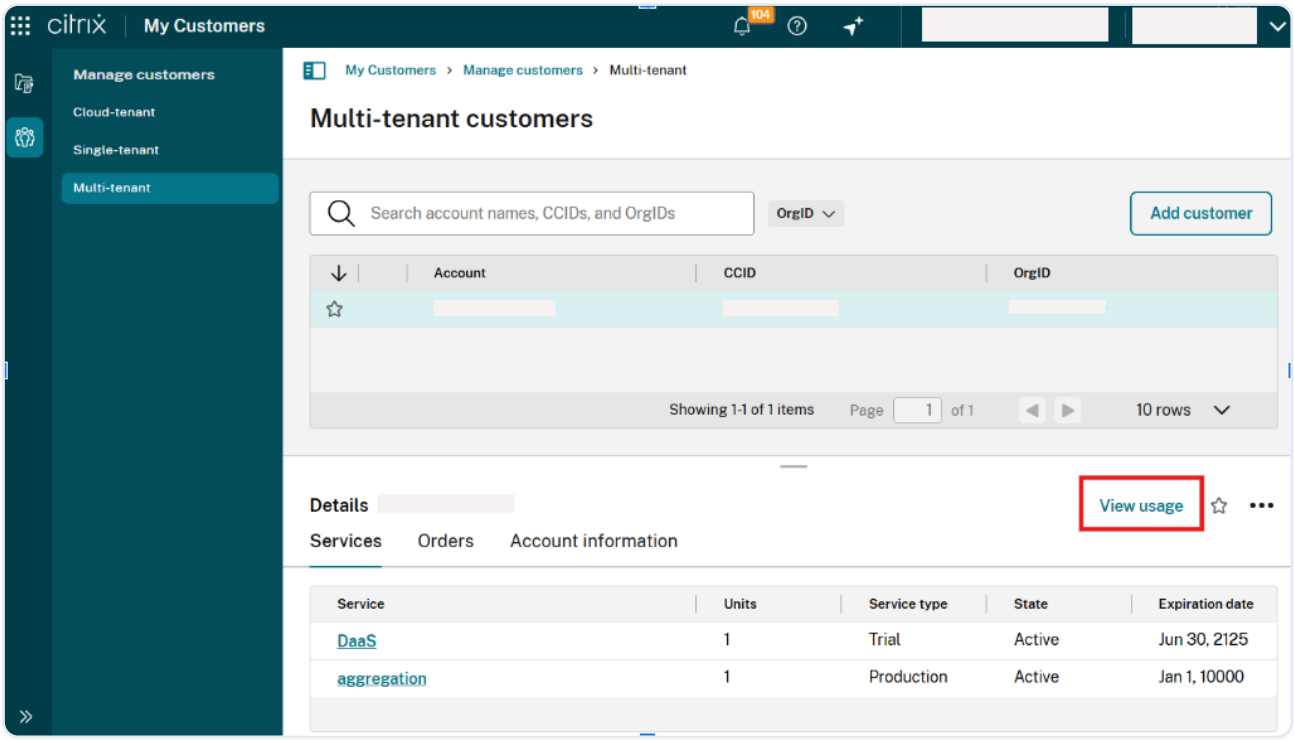
要终止与合作伙伴的连接，客户请执行以下步骤：

1. 在左上角的用户菜单中，选择 **帐户设置**。
2. 从**公司帐户**页面，找到**合作伙伴连接**部分。
3. 找到您要管理的合作伙伴，然后选择**删除**。
4. 当系统提示您确认删除时，选择**确认**。

许可趋势

合作伙伴可以通过单击客户仪表板中详细信息面板中的**查看使用情况**来查看客户的许可信息。

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

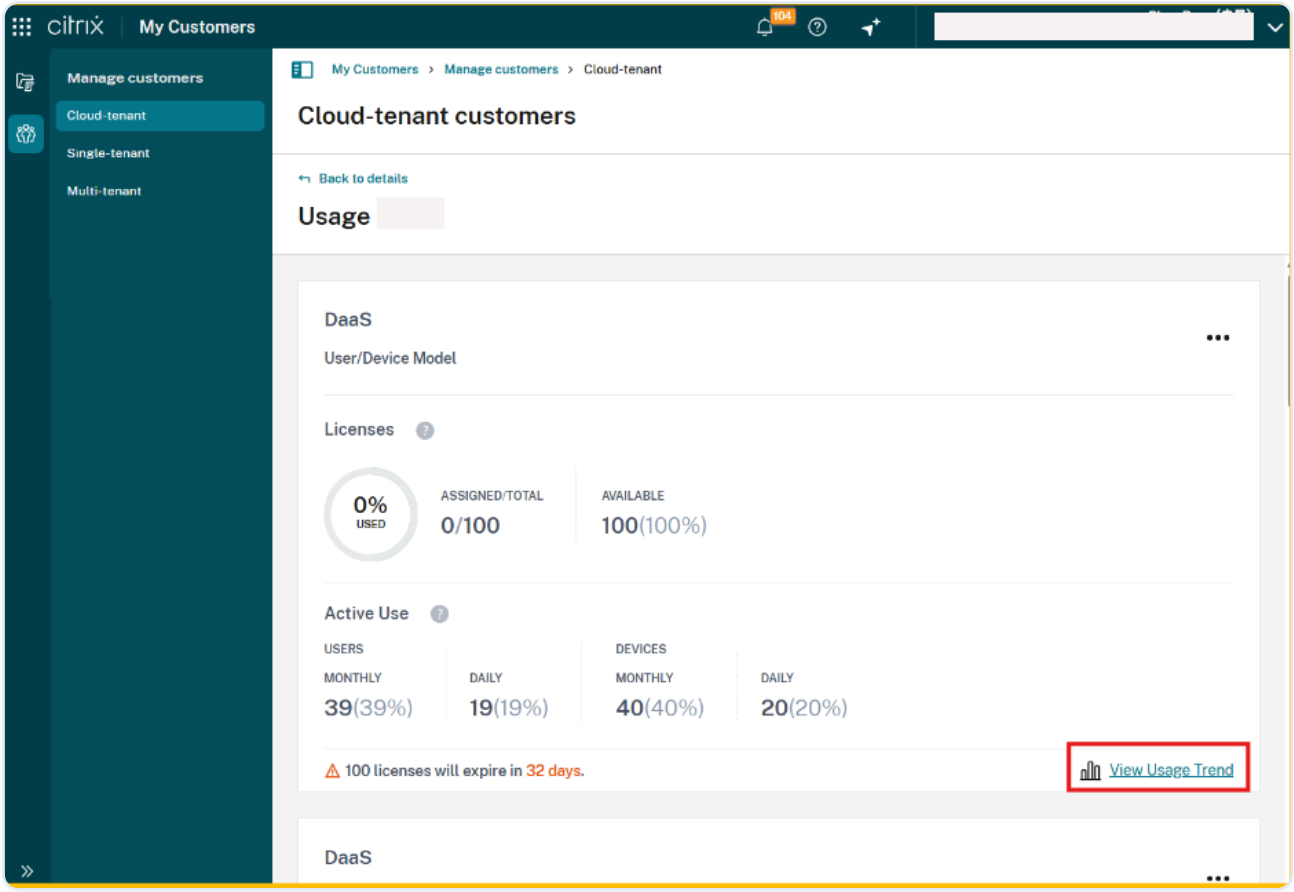


注意：

Citrix 合作伙伴只能查看许可摘要视图和历史活动使用情况趋势。他们无法查看使用特定服务许可证的单个用户。

要查看客户的每个服务的许可摘要，请单击**查看使用情况**选项卡。有关更多使用情况信息，请选择您要查看的服务授权的**查看使用情况趋势**。

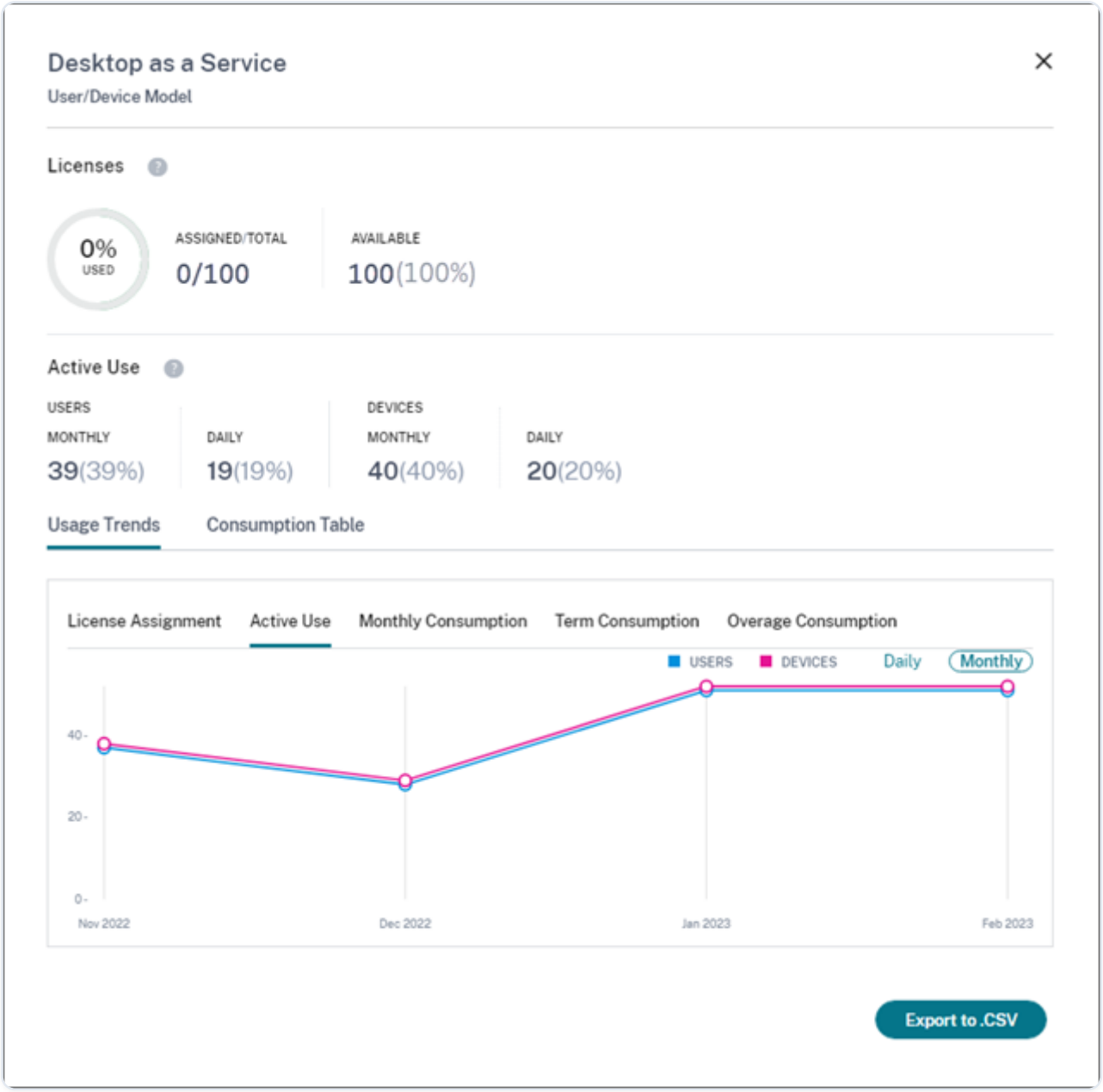
© 1997–2026 Citrix Systems, Inc. All rights reserved.



根据服务，使用情况趋势包括以下信息：

- 已分配许可证与购买总数的比率
- 每月和每日活跃用户
- 许可证分配、活动使用、每个授权的消耗以及超额使用的可视化细分。

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



如果需要，合作伙伴可以将此信息导出为 .csv 文件。

带宽使用情况

对于 Citrix Gateway 服务，许可摘要包含以下信息：

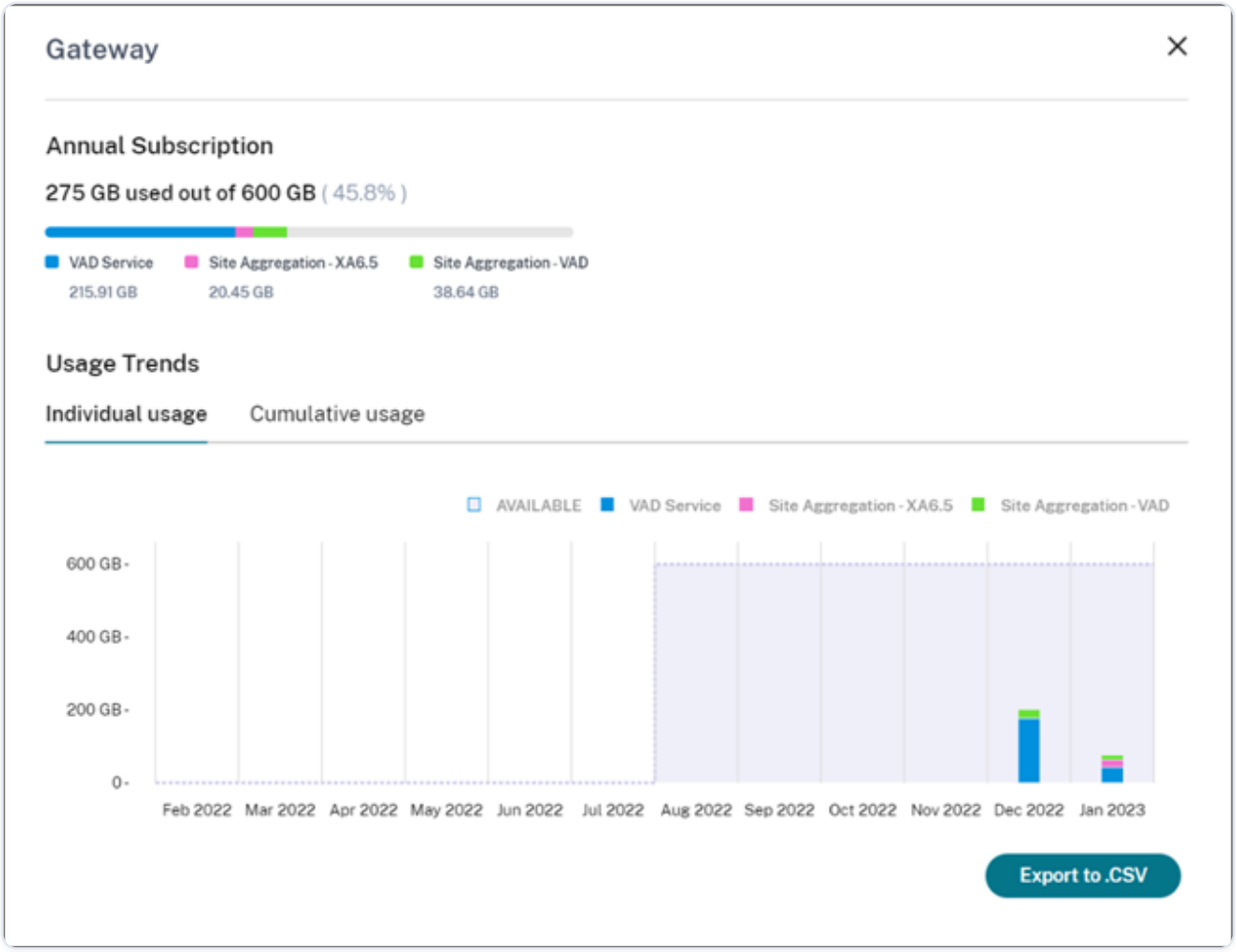
- 客户所有授权的总带宽使用量。
- 按客户的月度、年度和定期授权细分的总带宽使用量。
- 当月总超额使用量。有关超额使用量如何计算的更多信息，请参阅超额使用量。

在页面最右侧选择 **查看使用趋势** 以查看授权的使用摘要。选择 **查看超额使用量图表** 以查看过去 12 个月的超额使用量。

根据授权，使用趋势包括以下信息：

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

- Citrix DaaS (**VAD 服务**) 和具有站点聚合的本地 Virtual Apps and Desktops 部署所消耗的带宽量。
- 在每个使用带宽的月份中，带宽使用量的可视化细分。（月度授权）
- 在计费周期的每个月中发生的带宽**个人使用量**的可视化细分。（年度和定期授权）
- 在计费周期的每个月中累积的带宽**累计使用量**的可视化细分。（年度和定期授权）



如果需要，合作伙伴可以将此信息导出为 .csv 文件。

Citrix 服务提供商的客户许可和使用情况

Citrix Cloud 中的许可功能使 Citrix 服务提供商 (CSP) 的客户能够监控其支持的 Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops™）产品的许可证和使用情况。CSP 也可以在其客户的 Citrix Cloud 帐户下登录，以查看和导出此信息。有关详细信息，请参阅以下文章：

- Citrix DaaS 的客户许可证和使用情况监控

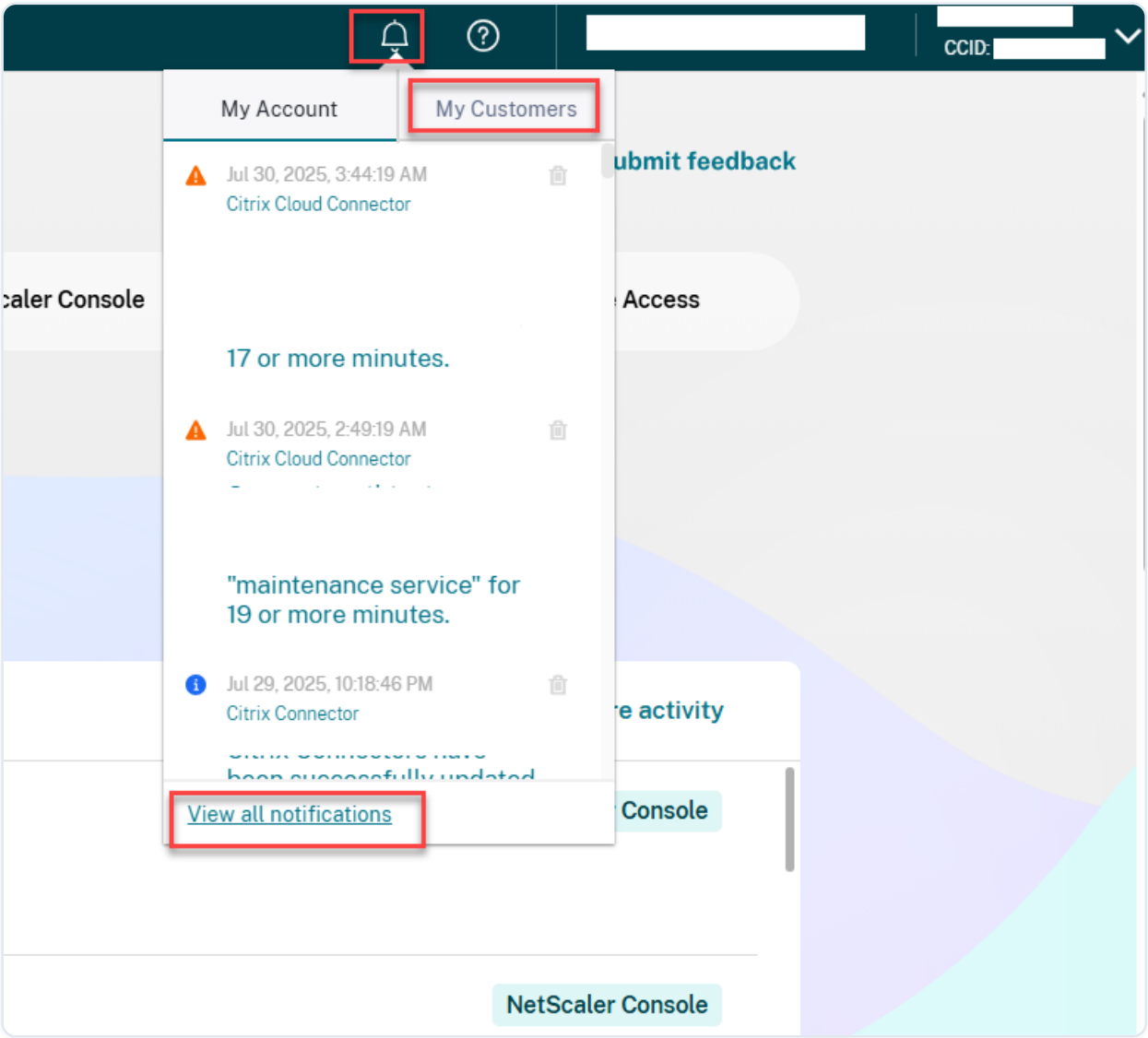
© 1997–2026 Citrix Systems, Inc. All rights reserved.

合作伙伴对客户通知的可见性

合作伙伴可以查看其关联客户的通知。合作伙伴还可以筛选特定于客户的通知并采取操作，例如关闭通知。已关闭的通知不会向合作伙伴显示。但是，客户登录 Citrix Cloud 后，仍可以在其帐户中看到该通知。

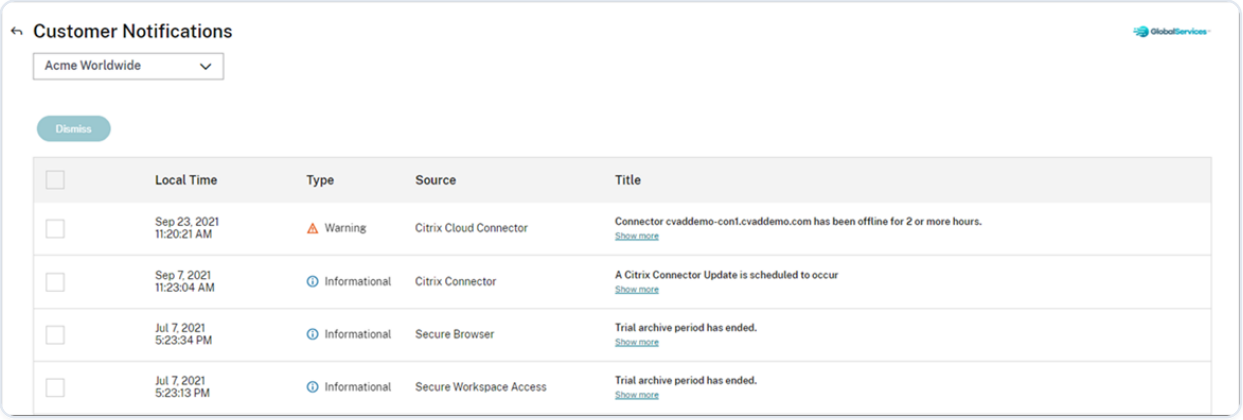
要查看客户通知，请执行以下操作：

1. 单击管理控制台顶部附近的铃铛图标，选择 **My Customers**（我的客户），然后选择 **View all notifications**（查看所有通知）。



2. 从下拉菜单中选择一个客户以查看该客户的通知。

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



Citrix 服务提供商的联合域

联合域 使客户用户能够使用附加到您的 CSP 资源位置的域中的凭据登录到应用商店。这使您能够通过自定义应用商店 URL（例如 *customer.cloud.com*）为客户用户提供专用应用商店。资源位置仍在您的合作伙伴 Citrix Cloud 帐户中。您可以提供专用应用商店以及客户可以使用您的 CSP 应用商店 URL（例如 csppartner.cloud.com）访问的共享应用商店。要使客户能够访问其专用应用商店，您需要将他们添加到您管理的相应域中。配置应用商店后，客户用户可以登录其应用商店并访问您通过 Citrix DaaS 提供的应用程序和桌面。

当您从联合域中删除客户时，客户的用户将无法再使用合作伙伴域中的凭据访问其应用商店。

有关使用联合域交付应用程序和桌面的详细信息，请参阅 Citrix DaaS for Citrix Service Providers。

Citrix 服务提供商的应用商店外观选项

您可以使用自定义主题配置应用商店颜色和徽标。要了解如何创建自定义主题，请参阅 Customize the appearance of stores。

注意

自定义主题是单租户功能。目前不支持服务提供商租户共享资源位置、云连接器和 Active Directory 域（多租户）的 Citrix 服务提供商。拥有自己的专用资源位置、云连接器和专用 Active Directory 域（单租户）的 Citrix 服务提供商租户受到完全支持。

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

云服务

本文列出了通过 Citrix Cloud 提供的云服务，并链接到每项服务的产品文档。有关这些服务及其所包含产品的说明，请参阅Citrix 服务说明。

Citrix® 服务

分析

- 安全分析
- 性能分析
- 分析 - 用量

思杰桌面即服务

适用于 Azure 的 Citrix DaaS Standard

端点管理

网关

全局应用程序配置服务

适用于 ServiceNow 的 ITSM 适配器

远程浏览器隔离

安全专用访问

会话录制服务

虚拟应用基础版

虚拟桌面基础版

工作区环境管理

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

NetScaler® 服务

控制台

应用交付和安全

SD-WAN 编排器

安全互联网访问

Web 应用防火墙

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

Virtual Apps and Desktops Essentials

Citrix 虚拟应用精简版™

注意：

Citrix Virtual Apps Essentials 和 Citrix Virtual Desktops Essentials 已停止销售并终止生命周期。有关更多信息，请参阅 CTX583004。

Citrix Virtual Apps™ Essentials 允许您将 Windows 应用程序和共享托管桌面从 Microsoft Azure 交付给任何设备上的任何用户。该服务将业界领先的 Citrix Virtual Apps 服务与 Microsoft Azure 的强大功能和灵活性相结合。您还可以使用 Virtual Apps Essentials 发布 Windows Server 桌面。

服务器操作系统计算机从一台计算机运行多个会话，以向多个同时连接的用户交付多个应用程序和桌面。每个用户都需要一个会话，他们可以从中运行所有托管应用程序。

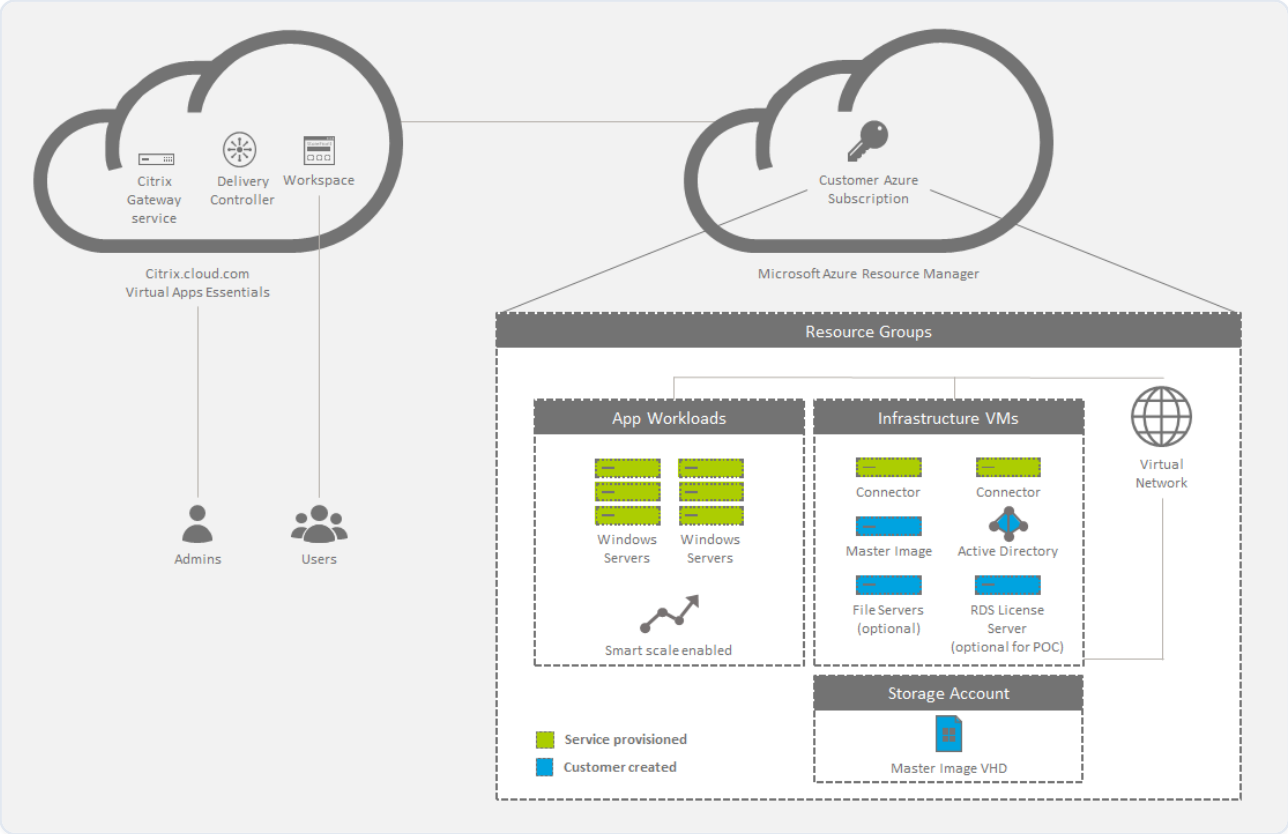
该服务通过 Citrix Cloud™ 交付，并帮助您轻松地在 Azure 订阅中部署应用程序工作负载。当用户从 store experience 打开应用程序时，应用程序似乎在用户计算机上本地运行。用户可以从任何设备、任何地点安全地访问其应用程序。

Virtual Apps Essentials 除了其核心管理服务外，还包括 store experience 和 Citrix Gateway service 。您的应用程序工作负载在您的 Azure 订阅中运行。

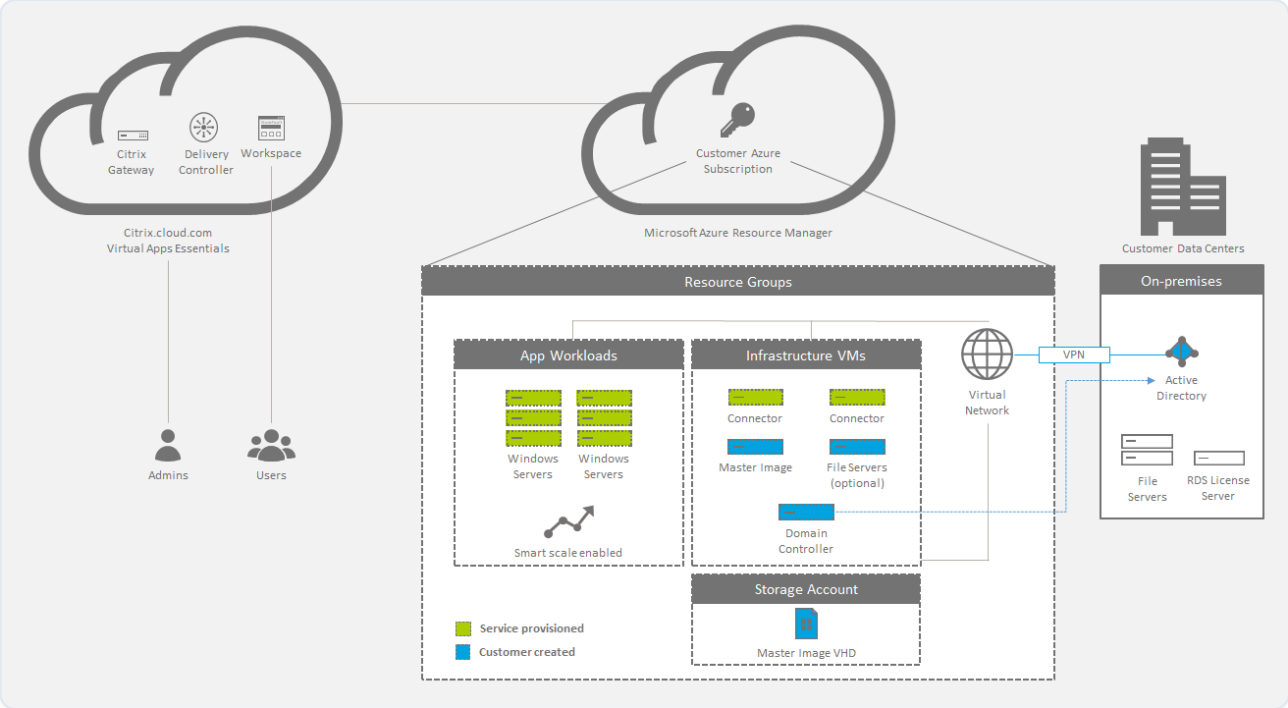
部署架构

下图显示了基本 Virtual Apps Essentials 云部署的架构概述：

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



您还可以允许用户连接到您的本地数据中心。Azure 云与您的本地数据中心之间的连接通过 VPN 连接进行。用户通过 Virtual Apps Essentials 经由 VPN 连接到您的许可证服务器、文件服务器或 Active Directory。



部署摘要

请按照以下步骤部署 Citrix Virtual Apps Essentials：

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

- 从 Azure Marketplace 购买 Citrix 虚拟应用精简版。
- 准备并链接您的 Azure 订阅。
- 创建并上传您的主映像。
- 部署目录、发布应用程序和桌面，并分配最终用户

新增功能

- 2018 年 12 月：**云托管 StoreFront™ 已移除**

  云托管 StoreFront 不再适用于 Virtual Desktops Essentials。在 2017 年 12 月之前购买 Virtual Desktops Essentials（以前称为 XenDesktop® Essentials）的客户可以使用本文所述的 Citrix Workspace 为订阅者提供桌面访问权限。

- 2018 年 8 月：**新产品名称**

  如果您是 Citrix® 的长期客户或合作伙伴，您会注意到我们的产品和产品文档中出现了新名称。如果您是 Citrix 产品的新用户，您可能会看到产品或组件的不同名称。

  新的产品和组件名称源于不断扩展的 Citrix 产品组合和云战略。本文使用以下名称。

  - **Citrix Virtual Apps Essentials：** XenApp® 是我们商店战略的一部分，在该战略中，多种类型的应用程序汇集在访问工作工具的首选位置。作为统一、上下文相关、安全商店的一部分，XenApp Essentials 现已更名为 Citrix Virtual Apps Essentials。
  - **Citrix Workspace 应用程序：** Citrix Workspace 应用程序整合了现有的 Citrix Receiver™ 技术以及其他 Citrix Workspace 客户端技术。它已得到增强，可提供更多功能，为最终用户提供统一的、上下文相关的体验，让他们能够与所有工作应用程序、文件和设备进行交互，从而发挥最佳工作表现。
  - **Citrix Gateway：** NetScaler® Unified Gateway 允许安全、上下文相关地访问您完成最佳工作所需的应用程序和数据，现已更名为 Citrix Gateway。

  产品内内容可能仍包含旧名称。例如，您可能会在控制台文本、消息和目录/文件名中看到旧名称的实例。某些项目（例如命令和 MSI）可能会继续保留其旧名称，以防止破坏现有客户脚本。

  相关产品文档、其他资源（例如视频和博客文章）以及其他站点（例如 Azure Marketplace）可能仍包含旧名称。感谢您在此过渡期间的耐心等待。有关我们新名称的更多详细信息，请参阅 `<https://www.citrix.com/about/citrix-product-guide.html>`。

- 2018 年 5 月：**从 Virtual Apps Essentials 界面构建其他映像**

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

从 Azure Resource Manager 界面创建生产映像后，您可以根据需要通过 Azure 创建其他映像。现在，作为通过 Azure 界面创建其他映像的可选替代方案，您可以从 Virtual Apps Essentials 界面构建新的主映像。有关详细信息，请参阅 准备和上传主映像。

- 2018 年 5 月：**显示器显示增强功能**

  Monitor 显示屏现在包含有关应用程序和热门用户的使用信息。有关详细信息，请参阅 监视服务。

系统要求

微软 Azure

Citrix Virtual Apps Essentials 仅支持通过 Azure Resource Manager 配置计算机。

使用 Azure Resource Manager 执行以下操作：

- 部署资源，例如虚拟机 (VM)、存储帐户和虚拟网络。
- 创建和管理资源组（用于将要作为组管理的资源的容器）。

要在 Microsoft Azure 中预配和部署资源，您需要：

- 一个 Azure 帐户。
- 一个 Azure Resource Manager 订阅。
- 一个与您的订阅关联的目录中的 Microsoft Entra ID 全局管理员帐户。该用户帐户必须具有 Azure 订阅的所有者权限才能用于预配资源。有关如何设置 Microsoft Entra ID 租户的更多信息，请参阅 如何获取 Microsoft Entra ID 租户。

思杰云

Virtual Apps Essentials 通过 Citrix Cloud 交付，需要一个 Citrix Cloud 帐户才能完成入门流程。您可以在前往 Azure Marketplace 完成交易之前，在 Citrix Cloud 注册页面 上创建 Citrix Cloud 帐户。

您使用的 Citrix Cloud 帐户不能与现有 Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops 服务）或 Citrix Virtual Desktops Essentials™ 服务帐户关联。

虚拟应用基本版控制台

您可以在 Google Chrome Web 浏览器中打开 Virtual Apps Essentials 管理控制台。

已知问题

Virtual Apps Essentials 存在以下已知问题：

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

- 在 Windows Server 2019 VDA 上，某些应用程序图标在配置期间和用户应用商店中可能无法正确显示。解决方法是，在发布应用程序后，使用**更改图标**功能分配一个可以正确显示的不同图标。
- 如果您使用 Microsoft Entra ID Domain Services：存储登录 UPN 必须包含在启用 Microsoft Entra ID Domain Services 时指定的域名。登录不能使用您创建的自定义域的 UPN，即使该自定义域被指定为主域。
- 为目录配置用户并选择域时，您可以查看并选择 Builtin\users 组中的用户。
- 如果所选区域的虚拟机大小不可用，则创建目录会失败。要查看您所在区域可用的虚拟机，请参阅 Microsoft 网站上“按区域提供的产品”图表。
- 您无法同时从“开始”菜单创建和发布同一应用程序的多个实例。例如，您从“开始”菜单发布 Internet Explorer。然后，您想发布 Internet Explorer 的第二个实例，该实例在启动时打开特定网站。为此，请使用应用程序的路径而不是“开始”菜单来发布第二个应用程序。
- Virtual Apps Essentials 支持使用 Microsoft Entra ID 用户帐户链接订阅。Virtual Apps Essentials 不支持 Live.com 身份验证帐户。
- 如果 VDA 上存在现有远程桌面协议 (RDP) 会话，则用户无法启动应用程序。此行为仅在没有其他用户登录 VDA 时启动 RDP 会话时发生。
- 您无法输入比 server.domain.subdomain 更长的许可证服务器地址。
- 如果您对容量管理执行多次连续更新，则更新的设置可能无法正确传播到 VDA。
- 如果您使用非英语 Web 浏览器，则文本将以英语和浏览器语言的组合形式显示。

如何购买服务

注意：

本节信息也可作为 PDF 提供。该内容包含早期产品名称。

使用您的 Microsoft Azure 帐户，直接从 Azure Marketplace 购买 Citrix Virtual Apps Essentials。Citrix Virtual Apps Essentials 至少需要 25 个用户。

该服务通过 Citrix Cloud 交付，需要一个 Citrix Cloud 帐户才能完成入门过程。有关详细信息，请参阅 系统要求 > Citrix Cloud。

购买 Citrix Virtual Apps Essentials 时，请确保输入所有详细信息的正确信息，包括地址字段，以确保您的订单快速处理。在配置 Virtual Apps Essentials 之前，请确保在 Azure Marketplace 中完成以下操作：

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

- 提供联系信息和您的公司详细信息。
- 提供您的账单信息。
- 创建您的订阅。

要配置客户和定价：

1. 在 **选择客户** 中，选择客户名称。
2. 在 **定价** 下的 **用户数** 中，键入有权访问 Virtual Apps Essentials 的用户数。
3. 在 **每月价格** 下，选中协议复选框，然后单击 **创建**。

摘要页面出现并显示资源的详细信息。

帐户预配完成后，单击 **通过 Citrix Cloud 管理**。

重要提示：

等待 Microsoft Azure 预配您的服务。在预配完成之前，请勿单击 **通过 Citrix Cloud 管理** 链接。此过程可能需要长达四个小时。

单击链接后，Citrix Cloud 将在 Web 浏览器中打开，您可以开始下面介绍的配置过程。

准备 Azure 订阅

选择您的 Azure 订阅作为您的 VDA 和相关资源的主机连接。这些资源可能会根据您的使用量产生费用。

注意：

此服务要求您使用 Microsoft Entra ID 帐户登录。Virtual Apps Essentials 不支持其他帐户类型，例如 live.com。

要准备 Azure 订阅，请在 Azure Resource Manager 中配置以下内容：

1. 创建资源组并提供：
    - 资源组名称
    - 订阅名称
    - 位置

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

2. 在 Azure Resource Manager 中，在资源组中创建虚拟网络并为该网络提供名称。您可以保留所有其他默认设置。创建主映像时，您将创建一个存储帐户。
3. 使用现有域控制器或创建一个。如果您创建域控制器：
   a. 在资源组和虚拟网络中使用 A3 Standard 或任何其他大小的 Windows Server 2012 R2 虚拟机。此虚拟机将成为域控制器。如果您计划创建多个域控制器，请创建一个可用性集并将所有域控制器放入此集中。
   b. 为虚拟机的网络适配器分配专用静态 IP 地址。您可以在 Azure 门户中分配该地址。有关详细信息，请参阅 Microsoft 文档网站上的 使用 Azure 门户为虚拟机配置专用 IP 地址。
   c. 将新的数据磁盘附加到虚拟机，以存储 Active Directory 用户和组以及任何 Active Directory 日志。有关详细信息，请参阅 使用 Azure 门户将托管数据磁盘附加到 Windows VM。附加磁盘时，选择所有默认选项以完成设置。
   d. 将域控制器虚拟机的私有 IP 地址添加到虚拟网络 DNS 服务器。有关详细信息，请参阅使用 Azure 门户（经典）管理虚拟网络（经典）使用的 DNS 服务器。
   e. 除了 Microsoft DNS 服务器之外，再添加一个公共 DNS 服务器。第二个 DNS 服务器使用 IP 地址 168.63.129.16。
   f. 将 Active Directory 域服务角色添加到域控制器虚拟机。完成此步骤后，将域控制器虚拟机提升为域控制器和 DNS。
   g. 创建林并添加一些 Active Directory 用户。有关详细信息，请参阅在 Azure 虚拟网络上安装新的 Active Directory 林。

如果您更喜欢使用 Microsoft Entra ID 域服务而不是域控制器，Citrix 建议查阅 Microsoft 网站上的文档Microsoft Entra ID Domain Services for Beginners。

链接您的 Azure 订阅

在 Citrix Cloud 中，将您的 Citrix Virtual Apps Essentials 链接到您的 Azure 订阅。

1. 登录到Citrix Cloud。在左上角菜单中，选择 **My Services > Virtual Apps and Desktops**。
2. 在“**管理**”选项卡上，单击“**Azure 订阅**”。
3. 单击“**添加订阅**”。Azure 门户随即打开。
4. 使用您的全局管理员 Azure 凭据登录到您的 Azure 订阅。
5. 单击“**接受**”以允许 Virtual Apps Essentials 访问您的 Azure 帐户。您的帐户中可用的订阅将列出。
6. 选择您要使用的订阅，然后单击“**链接**”。
7. 返回 Virtual Apps Essentials 控制台，查看处于链接状态的订阅。

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

将 Azure 订阅链接到 Virtual Apps Essentials 后，上传您的主映像。

准备和上传主映像

目录创建使用主映像来部署包含应用程序和桌面的 VM。这可以是您准备的主映像（安装了应用程序和 VDA），也可以是 Citrix 准备的映像。对于生产部署，Citrix 建议准备和使用您自己的主映像。Citrix 准备的映像仅用于试点或测试部署。

第一个生产映像必须通过 Azure Resource Manager 界面准备。之后，您可以根据需要通过 Azure 创建其他映像。

除了通过 Azure 界面创建其他映像之外，您还可以从 Virtual Apps Essentials 界面构建新的主映像。

- 此方法使用先前创建的主映像。您可以从现有目录获取网络设置，或手动指定它们。
- 使用现有主映像创建新映像后，您将连接到新映像并对其进行自定义，添加或删除从模板复制的应用程序。VDA 已安装，因此您无需再次执行此操作。
- 此方法让您可以使用 Essentials 服务。您无需导航到 Azure 创建新映像，然后再返回 Essentials 服务导入映像。

例如，假设您有一个名为 HR 的目录，它使用包含多个 HR 应用程序的主映像。最近发布了一个新应用程序，您希望将其提供给 HR 目录用户。使用 Virtual Apps Essentials 中的构建映像功能，您选择当前主映像作为模板来创建新的主映像。您还选择 HR 目录，以便新的主映像使用相同的网络连接设置。在初始映像设置后，在新映像上安装新应用程序。测试后，使用新的主映像更新 HR 目录，使其可供该目录的用户使用。原始 HR 主映像保留在“我的映像”列表中，以防将来再次需要。

以下部分介绍如何通过 Azure 界面准备和上传主映像。有关在 Virtual Apps Essentials 中构建映像的详细信息，请参阅 在 Virtual Apps Essentials 中准备主映像。

过程摘要

1. 在 Azure 或 Virtual Apps Essentials 中准备主映像 VM。
2. 在主映像上安装应用程序。
3. 在主映像上安装 Citrix VDA。
4. 将主映像从 Azure Resource Manager 上传到 Virtual Apps Essentials（如果需要）。

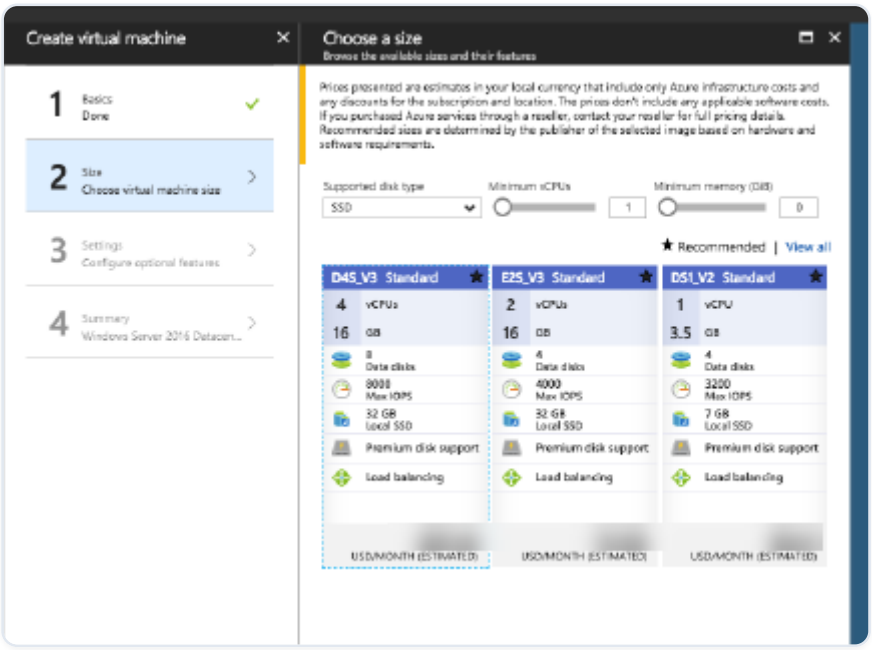
Citrix 建议在 Windows Server 2016 或 Windows Server 2012 R2 计算机上安装服务器 VDA 的最新当前版本 (CR) 或服务器 VDA 7.15 长期服务版本 (LTSR) 的最新累积更新 (CU)。如果您有 Windows Server 2008 R2 计算机，则必须安装服务器 VDA 7.15 LTSR（建议使用最新 CU），该版本也可在下载页面上获取。请参阅 Citrix Virtual Apps and Desktops Service 的生命周期策略，了解 CR 和 LTSR VDA 的生命周期策略。

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

在 Azure 中创建主映像 VM

1. 登录到 Azure 门户。
2. 在导航窗格中单击“**创建资源**”。选择或搜索 Windows Server 2008 R2、Windows Server 2012 R2 或 Windows Server 2016 条目。单击“**创建**”。 (/en-us/citrix-cloud/media/arm-create-resource.png)
3. 在“**创建虚拟机**”页面的“1 基础”面板中：
   a. 输入 VM 的名称。
   b. 选择 VM 磁盘类型（可选）。创建标准磁盘。
   c. 输入本地用户名和密码，并确认密码。
   d. 选择您的订阅。
   e. 创建新的资源组或选择现有资源组。
   f. 选择位置。
   g. 选择资源组和位置。
   h. 选择是否使用您已拥有的 Windows 许可证。
   i. 单击“**确定**”。

   (/en-us/citrix-cloud/media/arm-create-vm.png)
4. 在“**创建虚拟机**”页面的“2 大小”面板中，选择虚拟机大小：
   a. 选择虚拟机类型，然后指明最小 vCPU 数量和最小内存。将显示推荐选项。您也可以显示所有选项。
   b. 选择大小，然后单击**选择**。



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

5. 在**创建虚拟机**页面上，在面板 3 设置中：

   a. 指明是否要使用高可用性。

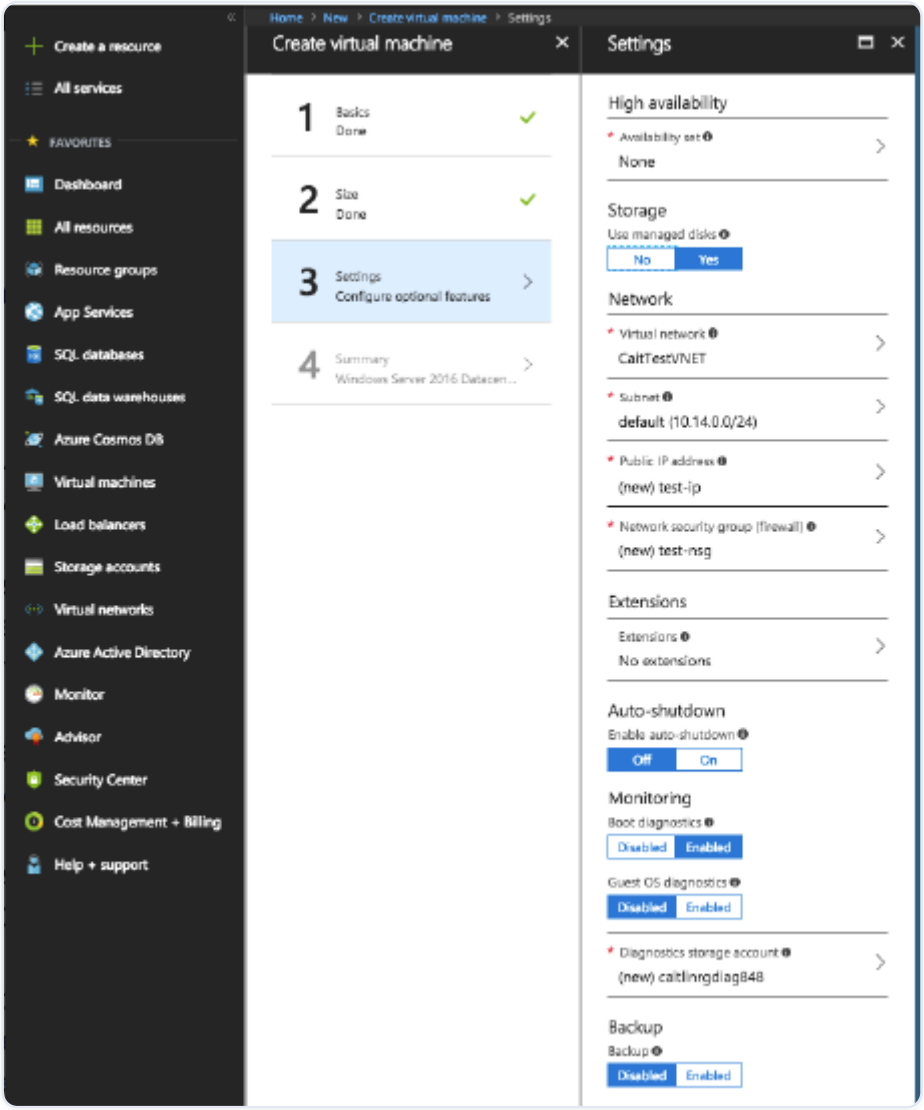
   b. 提供虚拟网络名称、子网、公共 IP 地址和网络安全。

   c. （可选）选择扩展。

   d. 启用或禁用自动关机、监视（启动诊断、来宾操作系统诊断、诊断存储帐户）。

   e. 启用或禁用备份。

   f. 单击**确定**。



6. 在面板 4 摘要中，单击**确定**以开始创建 VM。

不要对映像执行 Sysprep。

在主映像上安装应用程序

在您刚刚创建的主映像 VM 上，添加用户使用商店 URL 登录时可用的应用程序。（稍后，在您创建使用此主映像的目录后，您将精确指定哪些应用程序可供您指定的用户使用。）

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

1. 在创建主映像 VM 之后以及它运行时，连接到该 VM。
2. 安装应用程序。

在主映像上安装 VDA

1. 连接到主映像 VM（如果尚未连接）。
2. 您可以通过 Citrix Cloud 导航栏上的“**下载**”链接下载适用于服务器操作系统的 VDA。或者，使用浏览器导航到 Citrix DaaS 下载页面。将适用于服务器操作系统的 VDA 下载到 VM 上。（有关 VDA 版本信息，请参阅上面的指南。）
3. 双击下载的文件以启动 VDA 安装程序。安装向导将启动。
4. 在“**环境**”页面上，选择“**使用 MCS 创建主映像**”，然后单击“**下一步**”。
5. 在“**核心组件**”页面上，单击“**下一步**”。
6. 在“**交付控制器**”页面上，选择“**让 Machine Creation Services™ 自动执行**”，然后单击“**下一步**”。
7. 除非 Citrix 另有指示，否则请在“**附加组件**”、“**功能**”和“**防火墙**”页面上保留默认设置。在每个页面上单击“**下一步**”。
8. 在“**摘要**”页面上，单击“**安装**”。先决条件开始安装。当提示重新启动时，请同意。
9. VDA 安装自动恢复。先决条件安装完成后，将安装组件和功能。在“**回拨**”页面上，保留默认设置（除非 Citrix 另有指示），然后单击“**下一步**”。
10. 单击“**完成**”。计算机自动重新启动。
11. 为确保配置正确，请启动您安装的一个或多个应用程序。
12. 关闭 VM。不要对映像进行 Sysprep。

上传主映像

在此过程中，您将主映像从 Azure Resource Manager 上传到 Virtual Apps Essentials。

1. 如果您尚未登录 Citrix Cloud，请登录。在左上角菜单中，选择 **我的服务 > Virtual Apps and Desktops**。
2. 在 **管理** 选项卡上，单击 **主映像**。
3. 单击 **添加主映像**。
4. 在 **添加映像** 页面上，通过选择订阅、资源组、存储帐户、VHD 和区域来指定映像的位置。
5. 输入主映像的名称。
6. 单击 **保存**。

服务将验证主映像。验证后，上传的映像将显示在 **主映像 > 我的映像** 下。

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

提示： 作为在创建目录之前上传主映像的替代方法，您可以在创建目录时从 Azure Resource Manager 导入主映像。

在 Virtual Apps Essentials 中准备主映像

此方法使用现有主映像作为模板（以及可选地，来自现有目录的连接详细信息）来构建另一个主映像。然后，您可以自定义新的主映像。此过程完全通过 Virtual Apps Essentials 界面完成。

1. 如果您尚未登录 Citrix Cloud，请登录。在左上角菜单中，选择 **我的服务 > Virtual Apps and Desktops**。
2. 单击 **管理**，然后选择 **主映像** 选项卡。
3. 单击 **构建映像**。
4. 在 **构建映像** 页面上，在 **选择映像** 面板中，选择一个主映像。为您的新映像指定一个名称。单击 **下一步**。
5. 在 **指定网络连接设置** 面板中，您可以使用现有目录中的设置，也可以指定设置。这些设置包括：订阅、虚拟网络、区域、子网、域和 VM 实例类型。（如果您没有目录，则必须输入这些设置。）

   如果您选择**从目录复制设置**，请选择该目录。网络连接设置将显示，以便您可以直观地验证是否要将它们与新的主映像一起使用。输入您的服务帐户用户名和密码以加入域。单击**保存**。

   如果您选择**输入新设置**，请在相应的设置字段中选择值。输入您的服务帐户用户名和密码以加入域。单击**保存**。
6. 单击**开始预配**。
7. 新映像创建完成后，它将显示在**管理 > 主映像**列表中，状态为**需要输入**。单击**连接到 VM**。RDP 客户端将下载。使用 RDP 连接到新创建的 VM。通过添加或删除应用程序和其他软件来自定义新映像。与所有主映像一样，请勿对映像执行 Sysprep 操作。
8. 完成新映像的自定义后，返回**管理 > 主映像**页面，然后为您的新主映像单击**完成**。新映像随后将发送到验证过程。
9. 验证过程完成后，新映像将显示在**我的映像**列表中，状态为**就绪**。

稍后，当您创建目录并在**选择主映像**页面上选择**链接现有映像**时，新映像将显示在**映像名称**选项中。

部署目录、发布应用程序和桌面以及分配最终用户

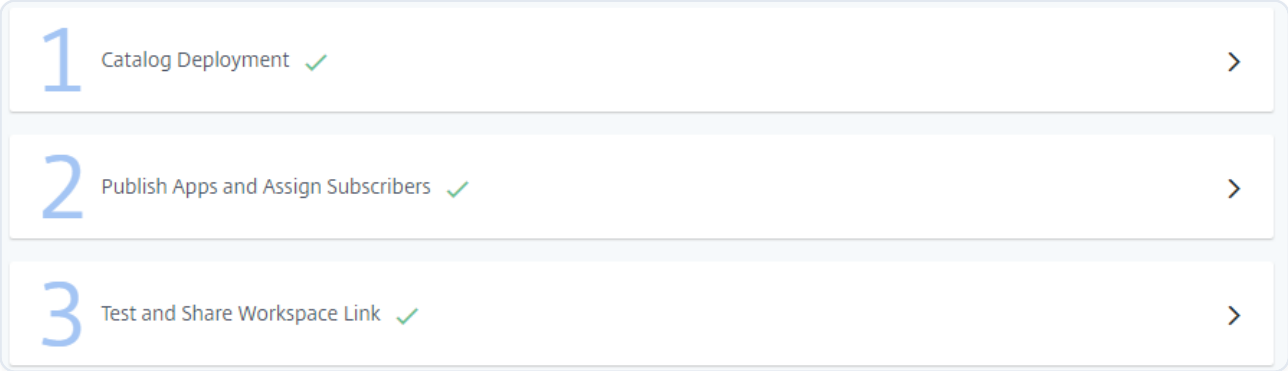
目录列出了您选择与选定用户共享的应用程序和桌面。

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

如果您熟悉其他 Citrix 应用程序和桌面交付产品，则此服务中的目录类似于结合了计算机目录和交付组。但是，其他服务中的计算机目录和交付组创建工作流在此服务中不可用。

部署目录并与最终用户共享应用程序是一个多步骤过程。

- 创建目录
- 发布应用程序并为该目录分配最终用户
- 测试并共享最终用户将使用的应用商店链接

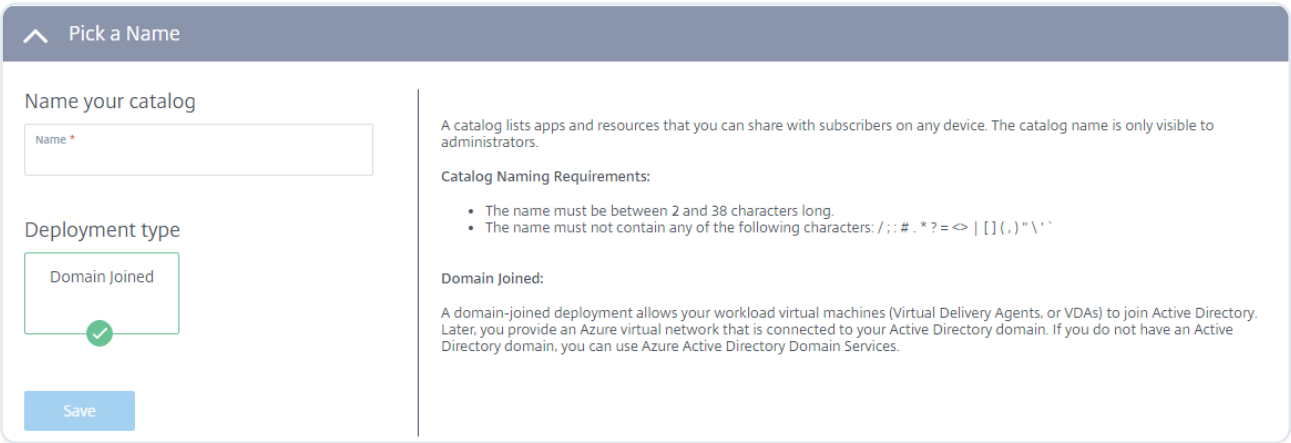


创建目录

创建目录时，请准备好 Microsoft Entra ID 帐户凭据和订阅名称。

1. 如果您尚未登录 Citrix Cloud，请登录。在左上角菜单中，选择 **My Services > Virtual Apps and Desktops**。
2. 在“**管理**”选项卡上，单击“**目录**”，然后单击“**添加目录**”。
3. 在以下面板中提供信息。完成每个面板后，单击“**保存**”。如果缺少或信息无效，面板标题中会显示警告标志。复选标记表示信息完整。

选择名称

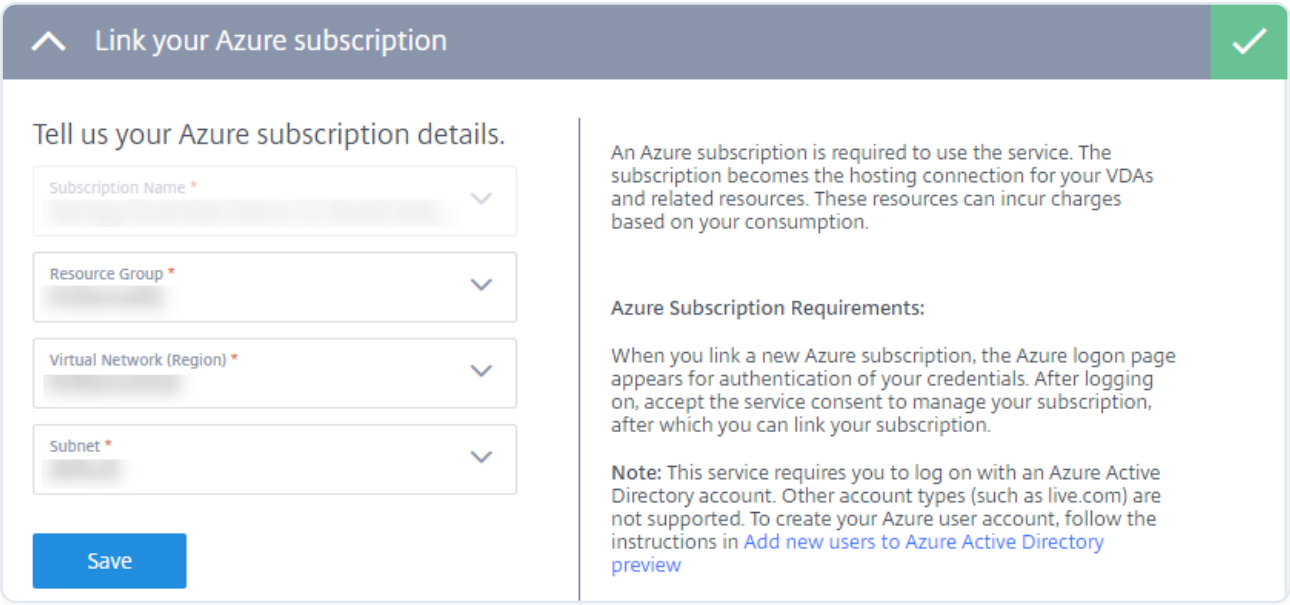


1. 为目录键入一个 2-38 个字符的名称。（仅限字母和数字，无特殊字符。）此名称仅对管理员可见。

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

2. 如果尚未选择“**已加入域**”，请选择它。已加入域的部署允许 VDA 加入 Active Directory。稍后，您将提供连接到域的 Azure 虚拟网络。如果您没有域，可以使用 Microsoft Entra ID 域服务。
3. 单击“**保存**”。

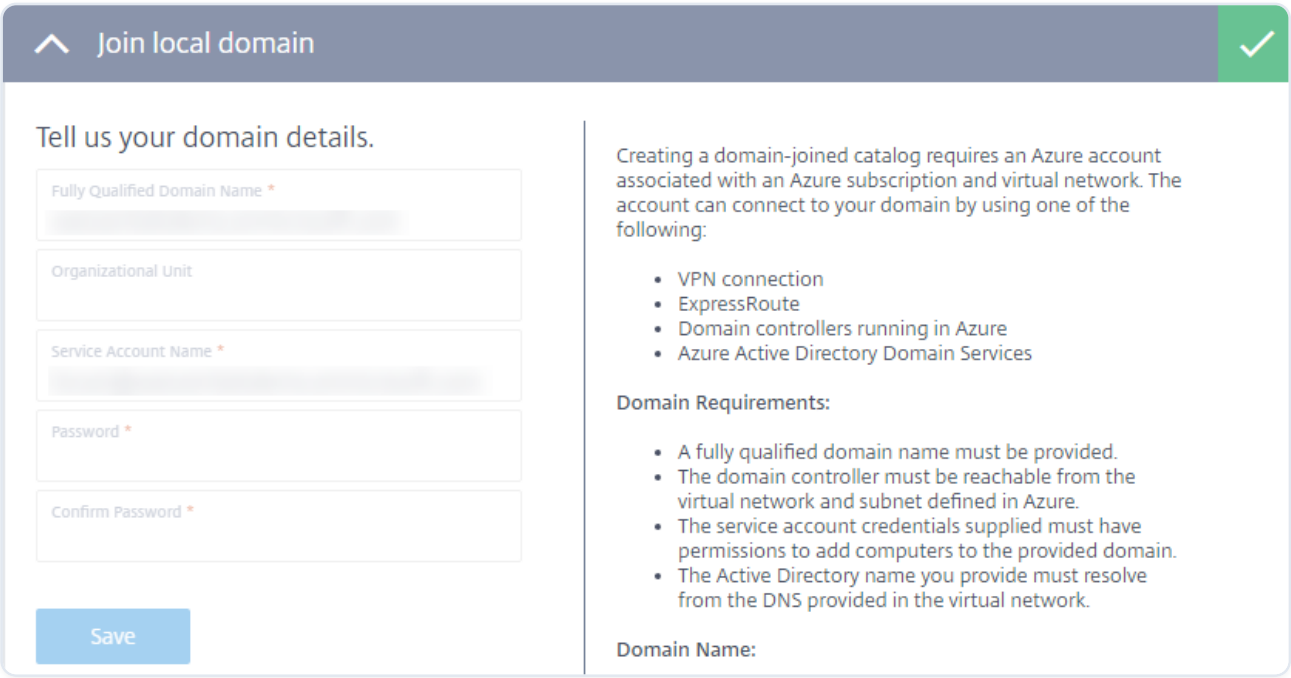
链接您的 Azure 订阅



1. 选择您的 Azure 订阅。当您链接新的 Azure 订阅时，将显示 Azure 登录页面以验证您的 Azure 凭据。登录后，接受服务同意以管理您的订阅。然后，您可以链接订阅。Virtual Apps Essentials 要求您使用 Microsoft Entra ID 帐户登录。不支持其他帐户类型（例如 live.com）。
2. 选择您的资源组、虚拟网络 (VNET) 和子网。VNET 决定了部署资源的 Azure 区域。子网必须能够访问您的域控制器。
3. 单击“**保存**”。

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

加入本地域



1. 输入域信息：
   - **完全限定域名：** 输入域名。该名称必须通过虚拟网络中提供的 DNS 解析。
   - **组织单位：**（可选）确保 Active Directory 包含指定的 OU。如果将此字段留空，则计算机将放置在默认的“计算机”容器中。
   - **服务帐户名称**、**密码**和**确认密码**：输入具有将计算机添加到域权限的帐户的用户主体名称 (UPN)。然后输入并确认该帐户的密码。
2. 单击**保存**。

您可以通过在 Azure 订阅中创建 VM 来测试通过虚拟网络的连接。该 VM 必须与您用于部署目录的资源组、虚拟网络和子网相同。确保 VM 可以连接到 Internet。此外，通过将 VM 加入域来确保您可以访问该域。您可以使用用于部署此目录的相同凭据进行测试。

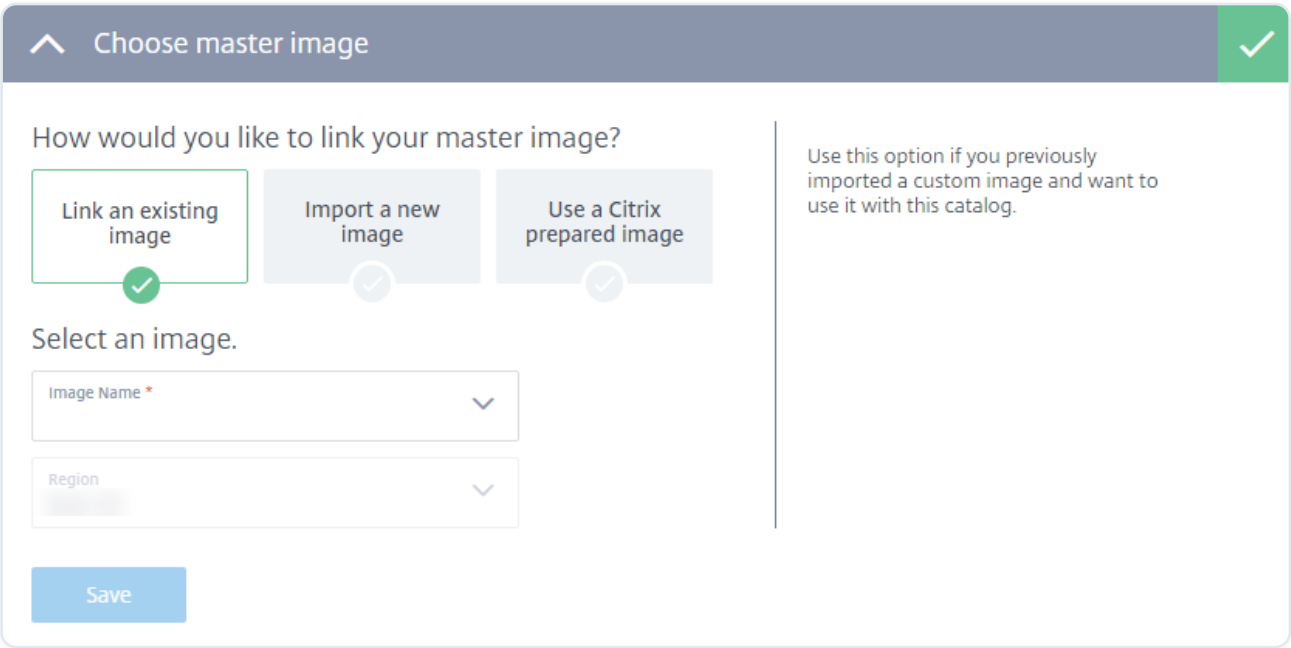
连接到资源位置

每个资源位置必须有两个或更多 Cloud Connector，它们与 Citrix Cloud 通信。当目录部署时，服务会自动处理 Cloud Connector 部署。两个 Windows Server VM 在 Azure Resource Manager 中创建，然后每个服务器上会自动安装一个 Cloud Connector。 如果选定的资源位置可用，则会自动建立连接。只需单击**保存**。 要创建资源位置，请输入其名称。

- 要在特定的 Azure 资源组中创建 Cloud Connector，请单击**Azure 资源组**旁边的**编辑**以更改资源位置。否则，服务将使用您在链接 Azure 订阅时指定的资源组。
- 要将 Cloud Connector 放入单独的 OU 中，请单击**组织单位**旁边的**编辑**以更改 OU。否则，Virtual Apps Essentials 将使用您在链接 Azure 订阅时指定的资源组。

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

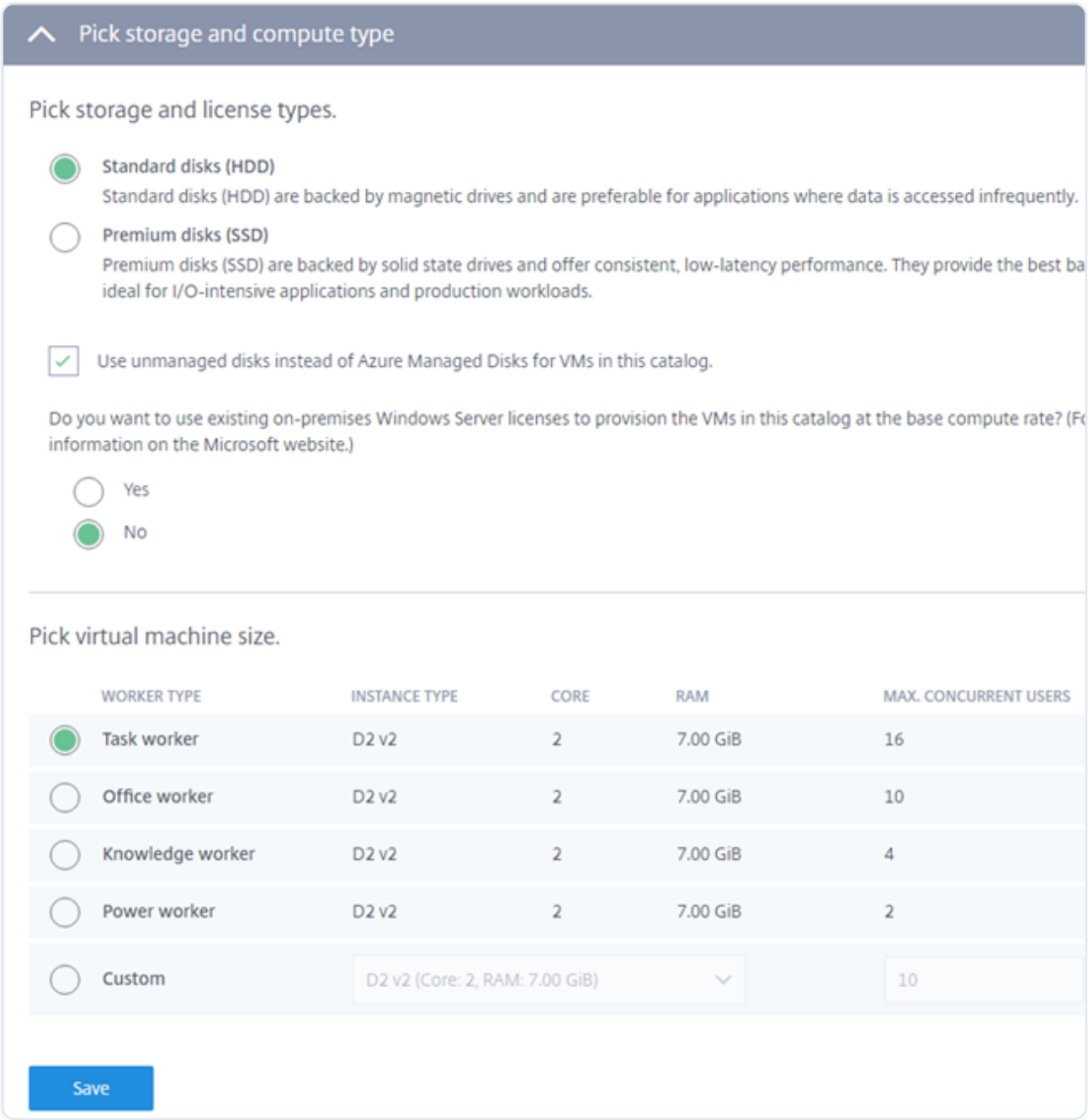
选择主映像



1. 选择以下其中一项：
   - **链接现有映像：** 如果您之前导入了自定义映像并希望将其用于此目录，请使用此选项。选择映像，并可选择一个区域。
   - **导入新映像：** 如果您希望将自定义映像用于此目录但尚未导入，请使用此选项。选择订阅、资源组、存储帐户和 VHD。为映像输入一个友好名称。
   - **使用 Citrix 准备的映像：** 如果您想在不使用自己的自定义映像的情况下测试服务，请使用此选项。这些映像仅适用于演示环境，不建议用于生产。选择一个准备好的映像。
2. 单击 **保存**。

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

选择存储和计算类型



1. 配置以下各项：

   - **标准磁盘或高级磁盘：** 标准磁盘 (HDD) 由磁性驱动器支持。它们更适用于数据访问不频繁的应用程序。高级磁盘 (SDD) 由固态驱动器支持。它们是 I/O 密集型应用程序的理想选择。
   - **使用 Azure 托管磁盘或非托管磁盘：** 在 https://docs.microsoft.com/zh-cn/azure/virtual-machines/windows/managed-disks-overview 了解有关 Azure 托管磁盘的更多信息。
   - **Azure 混合使用权益：** 选择是否使用现有的本地 Windows Server 许可证。启用此功能并使用现有的本地 Windows Server 映像将使用 Azure 混合使用权益 (HUB)。有关详细信息，请参阅 https://azure.microsoft.com/pricing/hybrid-use-benefit/。

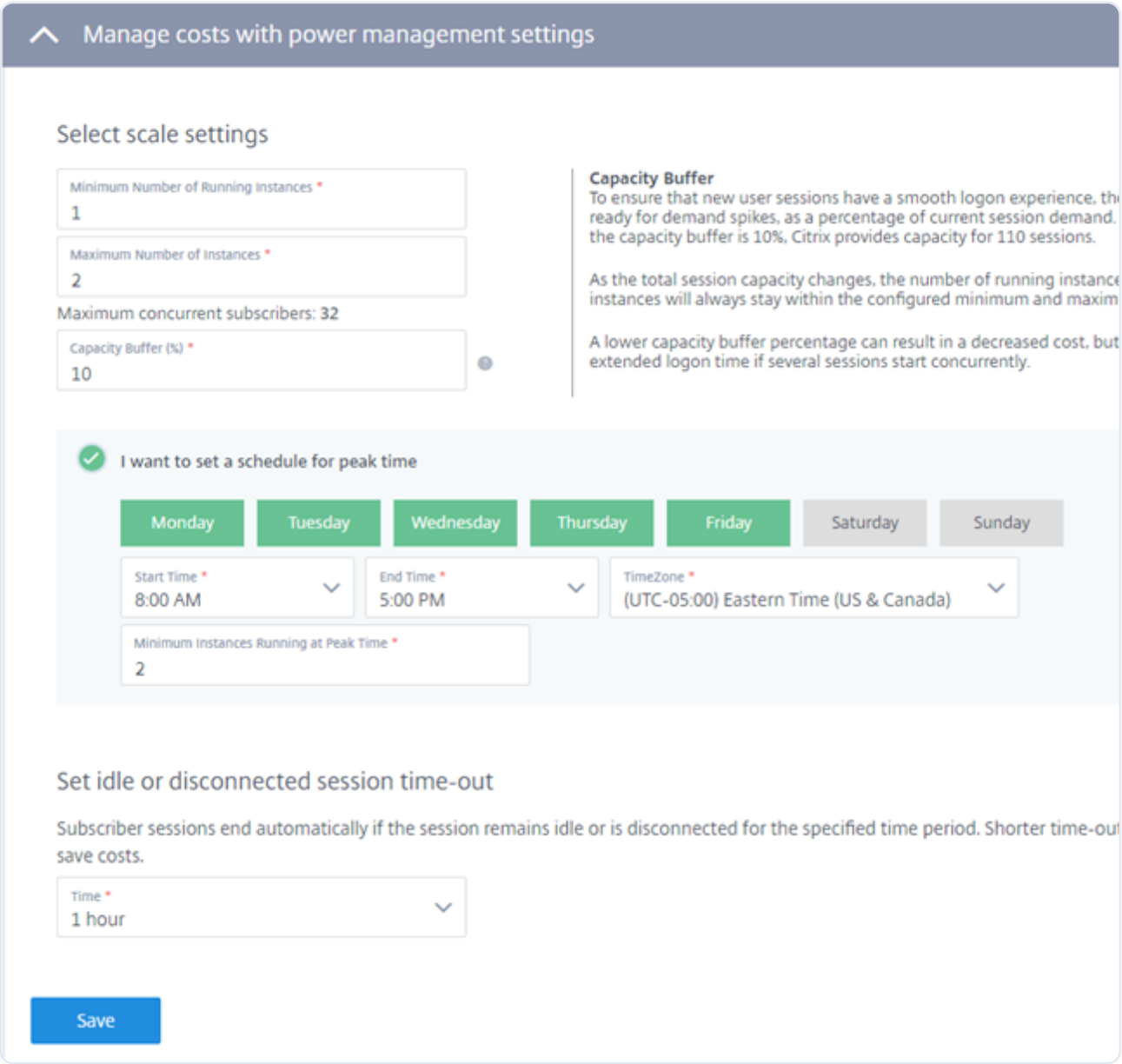
© 1997–2026 Citrix Systems, Inc. All rights reserved.

HUB 将 Azure 中运行 VM 的成本降低到基本计算费率，因为它免除了 Azure 库中额外 Windows Server 许可证的价格。您需要将本地 Windows Server 映像带到 Azure 才能使用 HUB。不支持 Azure 库映像。目前不支持本地 Windows 客户端许可证。请参阅 Microsoft 网站上的 适用于 Windows Server 的 Azure 混合权益。

- **选择虚拟机大小：** 选择一个工作角色（例如，任务、办公、知识、电源）。工作角色定义了所使用的资源。当您指定工作角色时，服务会确定每个实例的正确负载。您可以选择一个选项或创建自己的自定义选项。

2. 单击 **保存**。

使用电源管理设置管理成本



1. 输入以下信息：

   - **缩放设置：**

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

  - **最少运行实例数：** 服务确保始终有这么多虚拟机处于开机状态。
  - **最多运行实例数：** 服务不会超过此虚拟机数量。
  - **最大并发用户数：** 服务不允许并发用户超过此限制。
  - **容量缓冲区：** 允许额外的会话为需求高峰做好准备，作为当前会话需求的百分比。例如，如果有 100 个活动会话且容量缓冲区为 10%，则服务将提供 110 个会话的容量。

    随着总会话容量的变化，此目录的运行实例数会相应地向上或向下缩放。运行实例数始终保持在配置的最小值和最大值范围内。较低的容量缓冲区百分比可以降低成本。但是，如果多个会话同时启动，也可能导致某些会话的登录时间延长。

- **高峰时段计划：** 如果您希望在高峰时段运行的虚拟机数量与非高峰时段不同，请选择此选项。选择高峰时段的星期几、开始和结束时间以及时区。指定高峰时段最少运行实例数。
- **空闲或断开连接会话超时：** 设置会话结束的时间。如果会话在指定时间段内保持空闲或断开连接，则用户会话会自动结束。较短的超时值允许未使用的 VDA 关机并节省成本。

2. 单击“**保存**”。

部署目录

完成配置面板后，单击“**开始部署**”以开始目录创建。创建目录可能需要 1 到 2 小时（如果指定了大量虚拟机，则可能更长）。

创建目录时：

- 将在 Azure 中自动为工作负载计算机创建资源组（以及该资源组中的存储帐户）。
- 虚拟机命名为 Xenappxx-xx-yyy，其中 xx 源自环境因素，yy 是一个序数。

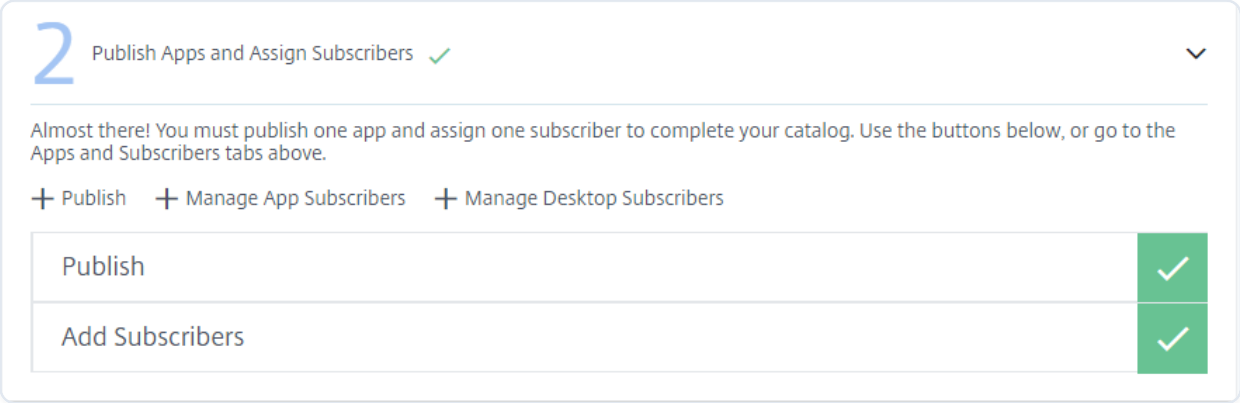
发布应用程序并为目录分配最终用户

部署目录后，您必须发布一个应用程序或桌面，并分配至少一个最终用户才能完成目录。

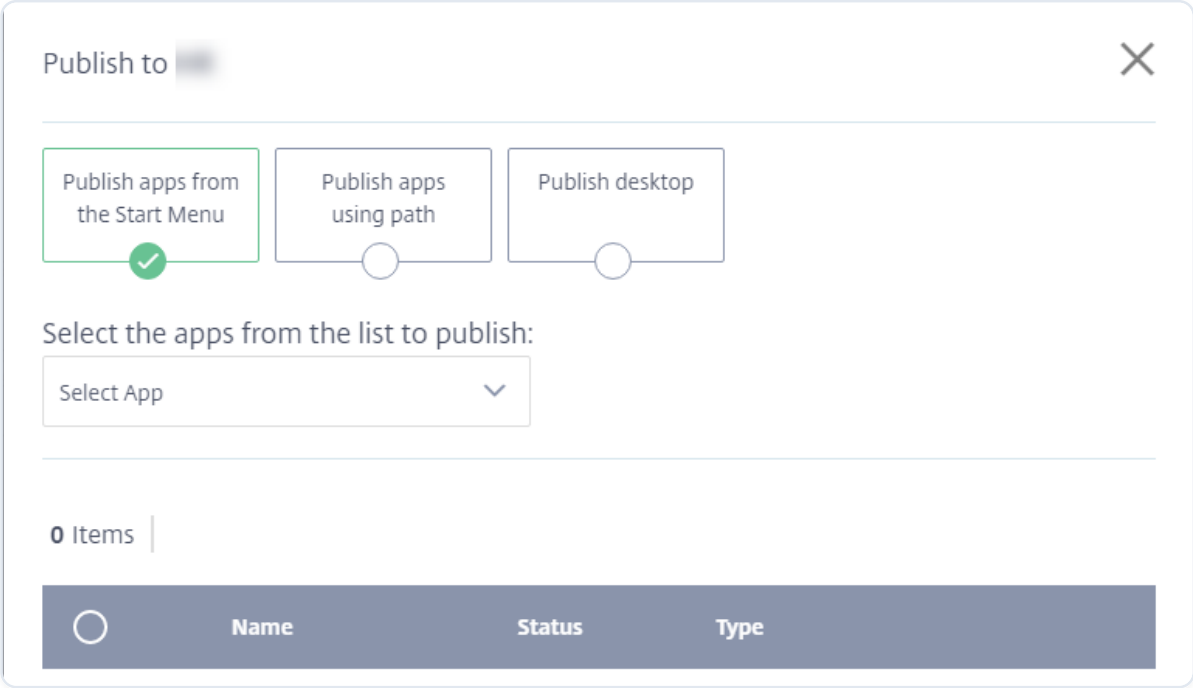
用于创建目录的映像包含您可以发布的应用程序（或桌面）。您可以从“开始”菜单中选择应用程序，或指定计算机上的目录路径。

1. 如果您尚未登录 Citrix Cloud，请登录。在左上角菜单中，选择 **My Services > Virtual Apps and Desktops**。
2. 在 **Manage** 选项卡上，单击 **Catalogs**。
3. 在已创建目录的省略号菜单 (…) 中，选择 **Manage Catalog**。
4. 选择 **Publish Apps and Assign end users**。将显示以下页面。

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

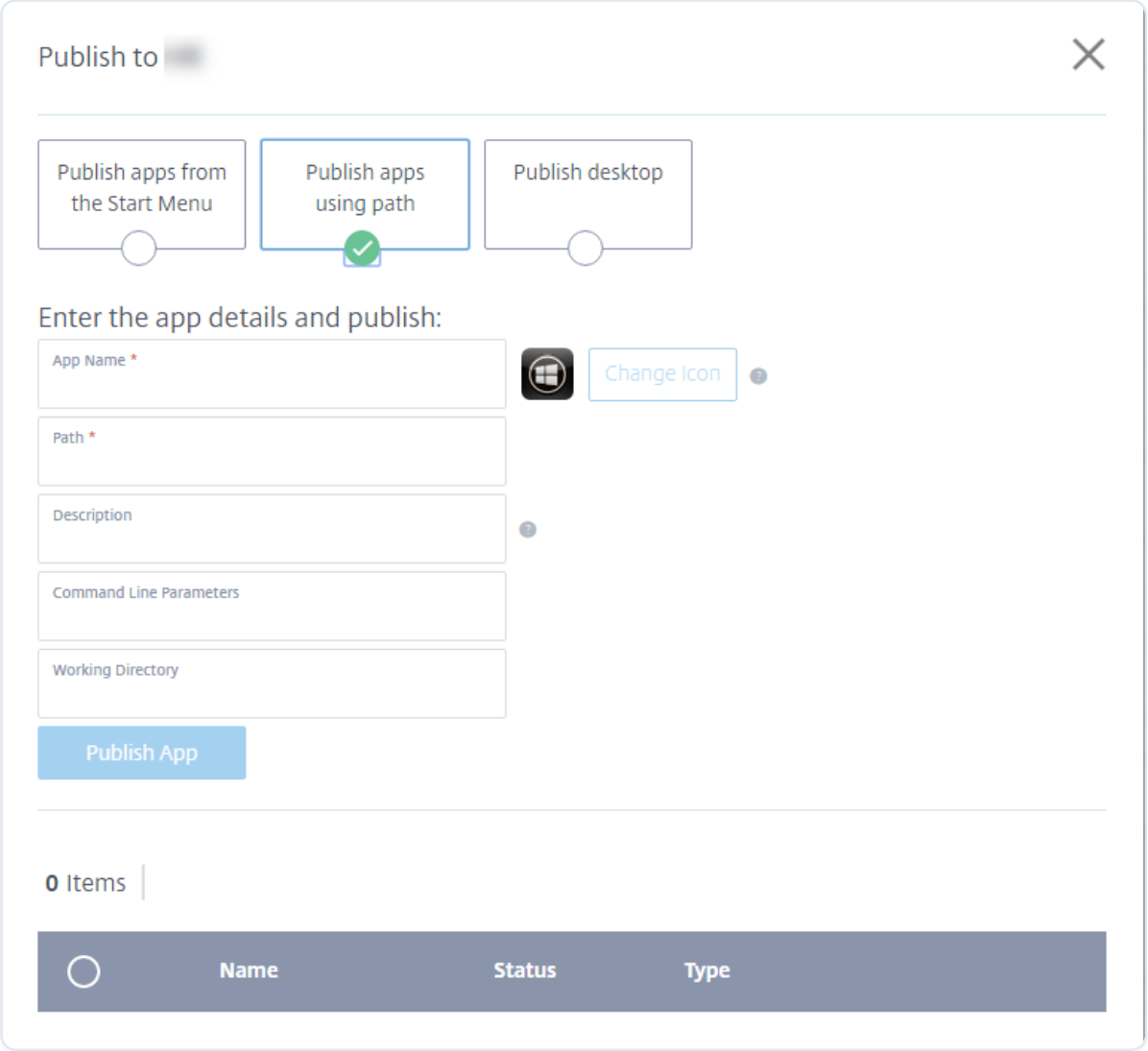


5. 在 **Publish Apps and Assign end users** 对话框中，单击 **Publish**。“发布到目录名称”页面包含三个选项。至少完成一个。或者，您可以选择另一个（例如，使用此目录同时发布应用程序和桌面）。
6. 要发布位于“开始”菜单中的应用程序：
   a. 选择 **从“开始”菜单发布**。
   b. 从列表中选择应用程序。



7. 要通过指定应用程序的位置和其他信息来发布应用程序：
   a. 选择 **使用路径发布**。
   b. 输入每个应用程序的名称和路径（例如，c:\Windows\system1\app.exe）。
   c. 可选地，输入将在用户商店、命令行参数和工作目录中显示的描述。
   d. 要更改代表已发布应用程序的图标，请单击 **更改图标**，然后导航到图标的位置。如果无法提取所选图标，将显示一条消息。在这种情况下，您可以重试或继续使用现有图标。
   e. 单击 **发布应用程序**。

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



8. 要发布桌面：

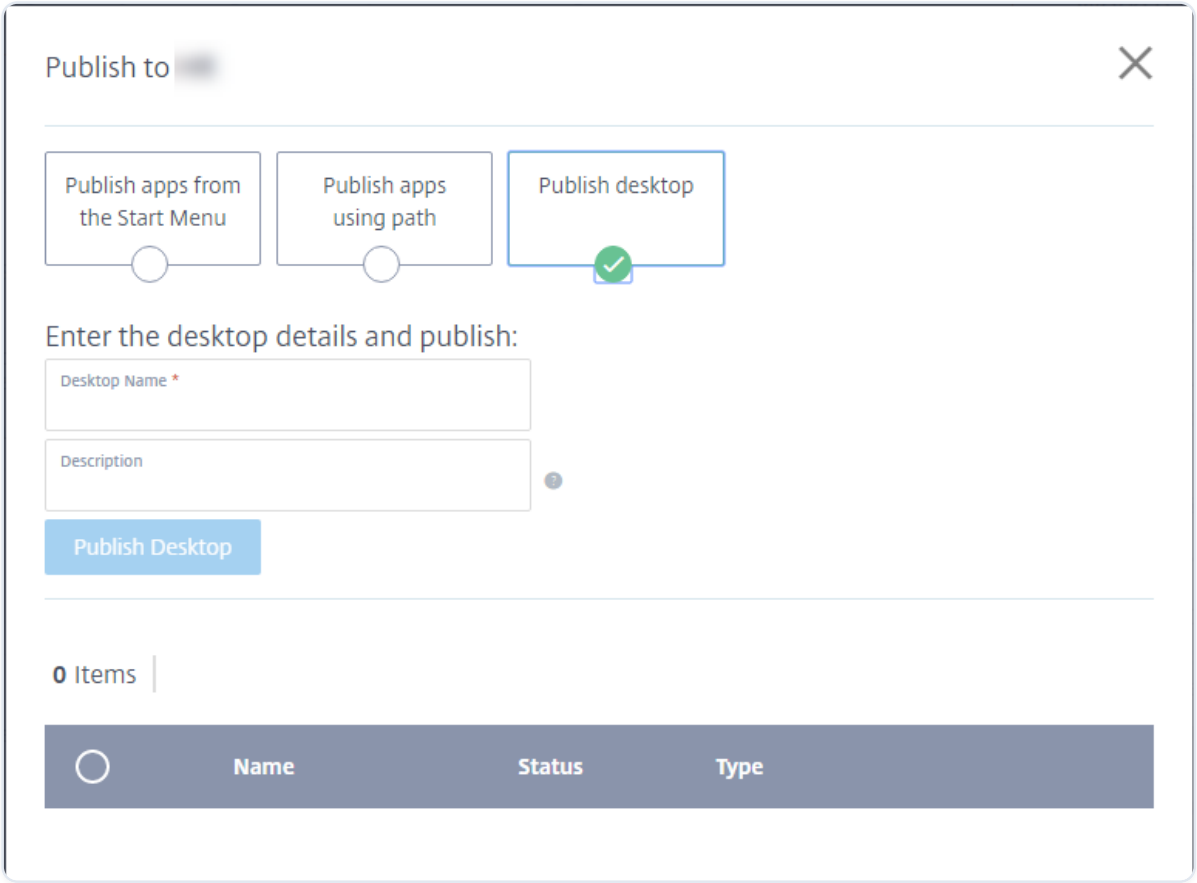
   a. 选择 **发布桌面**。

   b. 输入桌面的名称。

   c. 可选地，输入将在用户商店中显示的描述。

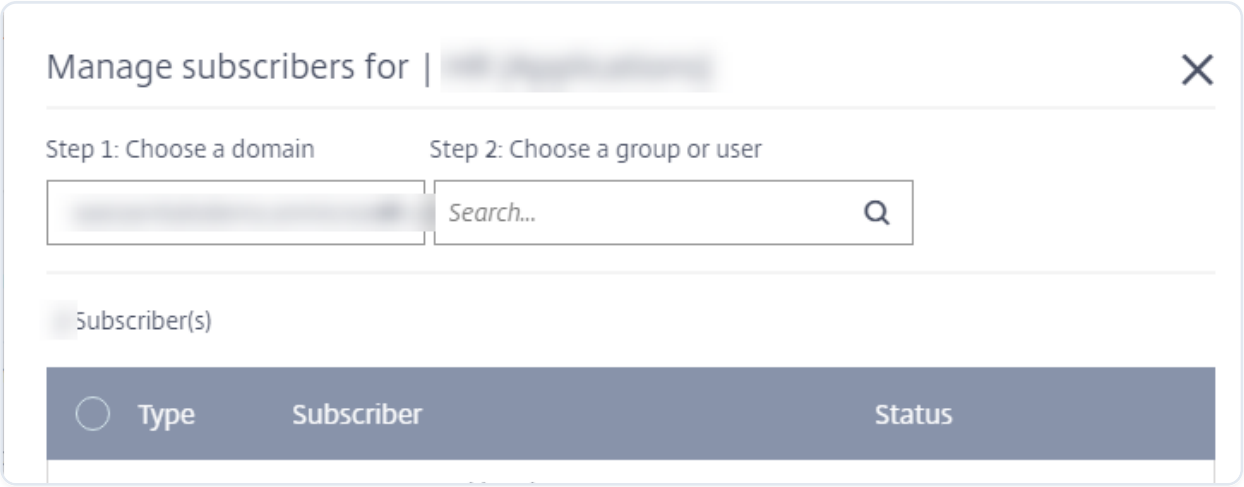
   d. 单击 **发布桌面**。

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



添加应用程序或桌面后，它们将显示在选择器下方的列表中。要删除您添加的应用程序或桌面，请选择条目左侧的按钮（或单击条目旁边的垃圾桶图标），然后单击 **删除**。稍后，如果您想取消发布应用程序或桌面，请选择条目左侧的按钮，然后单击 **取消发布**。

9. 在 **发布应用程序和分配最终用户** 对话框中，单击 **管理应用程序最终用户** 或 **管理桌面最终用户**。



10. 选择一个域，然后搜索用户或用户组。
11. 应用程序和桌面的用户分配是独立的。要为用户分配对应用程序和桌面的访问权限，请使用 **管理应用程序最终用户** 和 **管理桌面最终用户** 为该用户进行分配。

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

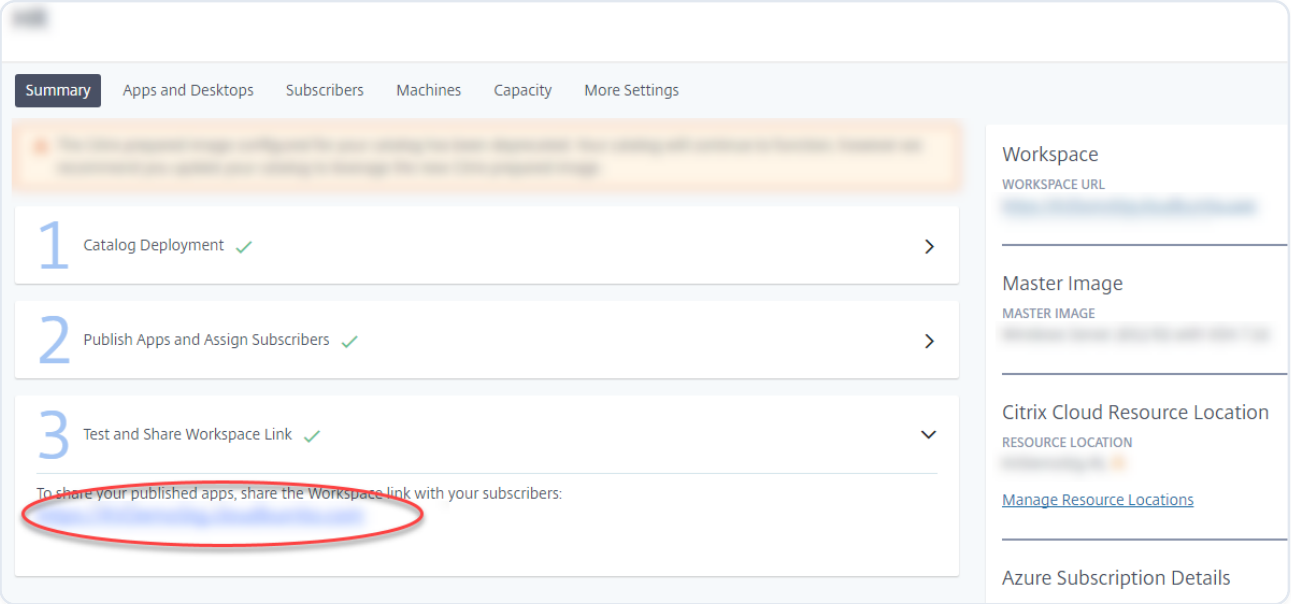
添加用户或组后，它会出现在选择器下方的列表中。要删除您选择的用户或组，请单击条目旁边的垃圾桶图标，然后单击“**删除**”。稍后，如果您想删除用户，请选择条目左侧的按钮，然后单击“**删除所选**”。

测试并共享应用商店链接

部署目录、发布应用程序并分配最终用户后，您将获得最终用户用于访问您为其发布的应用程序和桌面的链接。

1. 如果您尚未登录 Citrix Cloud，请登录。在左上角菜单中，选择“**我的服务 > Virtual Apps and Desktops**”。
2. 在“**管理**”选项卡上，单击“**目录**”。
3. 在目录的省略号菜单 (...) 中，选择“**管理目录**”。
4. 选择“**测试并共享应用商店链接**”。

在下图中，应用商店链接显示在圈出的区域中。与您的最终用户共享此链接。页面的右侧列出了应用商店 URL，以及有关目录的主映像、资源位置、Azure 订阅和域的信息。



有关详细信息，请参阅 应用商店体验。

更新主映像和目录

要更新或添加应用程序，请更新用于创建目录主映像的虚拟机。

更新主映像

1. 启动主映像 VM。启动计算机不会影响安装在 Azure Resource Manager 中的主映像。
2. 在 VM 上安装任何更新或应用程序。

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

3. 关闭虚拟机。
4. 在 Virtual Apps Essentials 控制台中，添加新映像，其中包含虚拟机 VHD 映像的路径。

使用新映像更新目录

1. 如果您尚未登录 Citrix Cloud，请登录。在左上角菜单中，选择 **我的服务 > Virtual Apps and Desktops**。
2. 在**管理**选项卡上，单击**目录**。
3. 单击目录的省略号菜单，然后单击**更新目录映像**。
4. 选择**链接现有映像**或**导入新映像**。输入与您的选择相符的信息。
5. 在**自动注销前的时间**中，选择会话结束前的时间量。
6. 单击**更新**。

启动目录更新时，用户可以继续工作，直到初始处理完成。然后，用户会收到一条警告消息，要求他们保存工作并关闭应用程序。关闭 VDA 上的所有活动会话后，该 VDA 上的更新完成。如果用户未在给定时间内注销，会话将自动关闭。

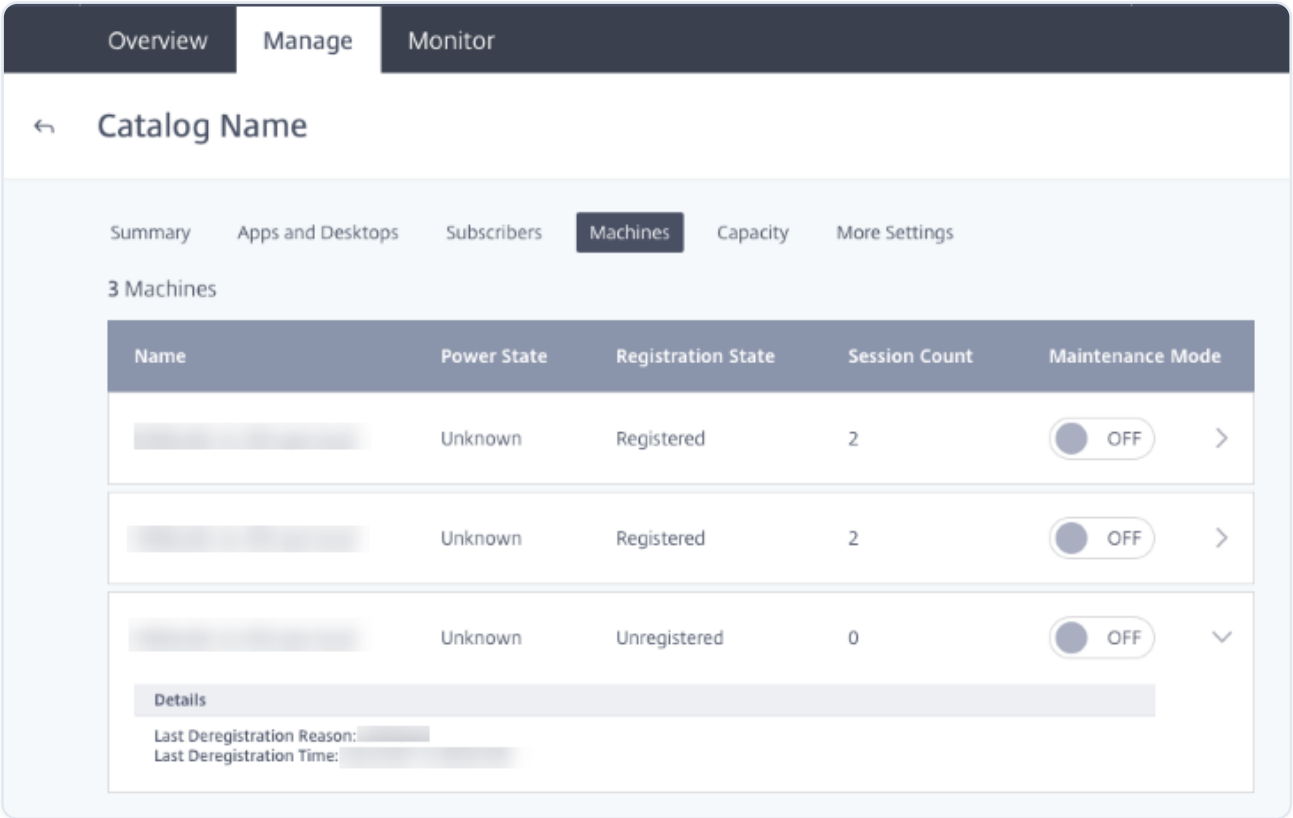
更新目录中的 VDA 数量

1. 如果您尚未登录 Citrix Cloud，请登录。在左上角菜单中，选择 **我的服务 > Virtual Apps and Desktops**。
2. 单击**管理**选项卡。
3. 在**目录**选项卡上，选择一个目录。
4. 在**容量**选项卡上，在**选择缩放设置**下，单击**编辑**。
5. 将“**最大运行实例数**”值更改为目录所需的 VDA 计数。
6. 单击“**保存**”。

监视计算机状态

选择目录时，目录摘要页面上的“计算机”选项卡会列出该目录中的所有计算机。显示内容包括每台计算机的电源和注册状态以及当前会话计数。

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

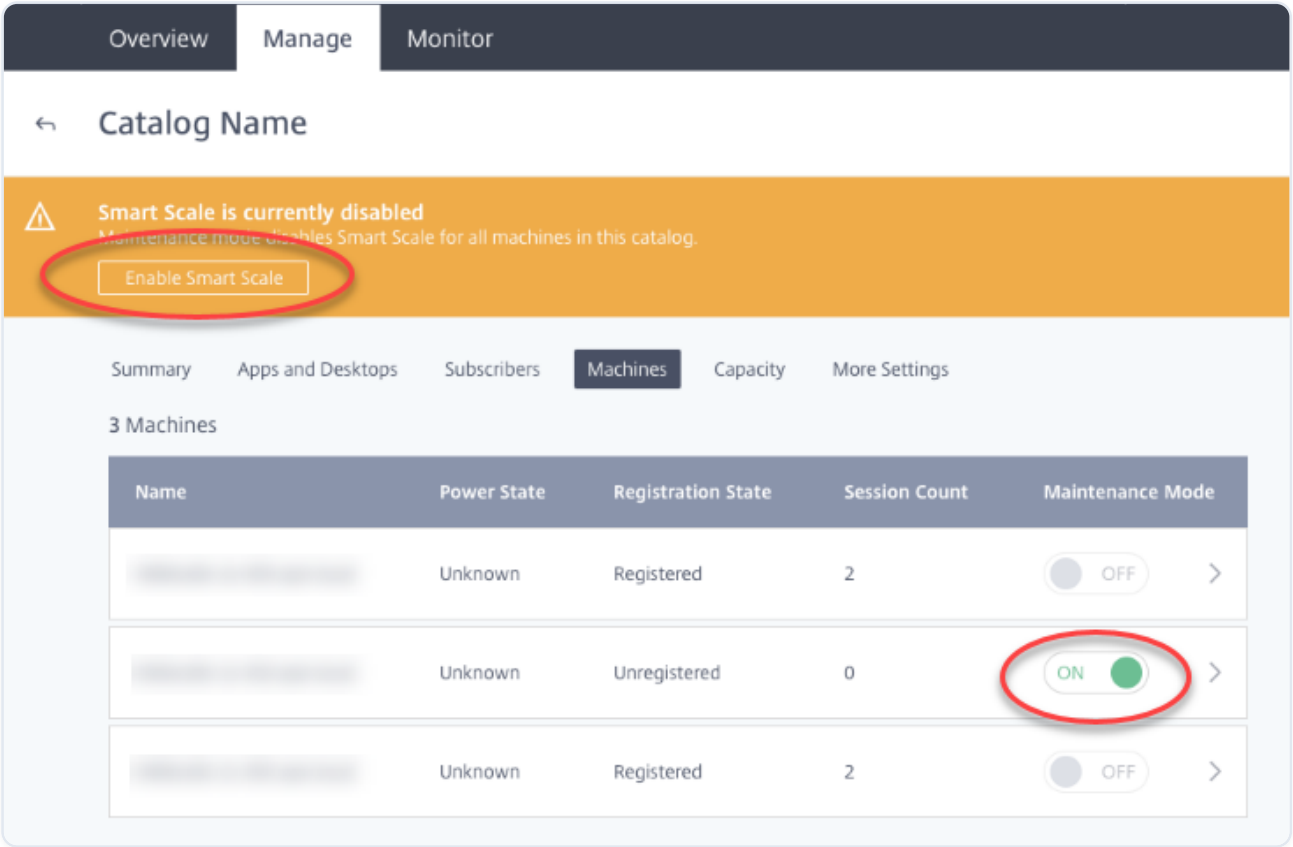


您可以为计算机启用或禁用维护模式。启用维护模式可防止新连接连接到计算机。用户可以连接到现有会话，但无法启动新会话。您可能需要在应用修补程序之前将计算机置于维护模式。

如果您为一台或多台计算机启用维护模式，则该目录中的所有计算机的 Smart Scale 将暂时禁用。以下任一操作都将再次启用 Smart Scale：

- 单击屏幕顶部警告中的“**启用 Smart Scale**”。此操作会自动关闭目录中所有已启用维护模式的计算机的维护模式。
- 明确关闭当前已启用维护模式的每台计算机的维护模式。

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



监视服务

1. 如果您尚未登录 Citrix Cloud，请登录。在左上角菜单中，选择“**我的服务 > Virtual Apps and Desktops**”。
2. 单击“**监视**”选项卡。

会话信息

要监视 Citrix Virtual Apps Essentials 的整体性能：

1. 选择要监视的目录。您可以查看有关会话、登录持续时间和其他信息。
2. 选择一个会话，然后：
   - 断开会话
   - 从会话注销
   - 发送消息
3. 单击每个会话可查看有关该会话的更多详细信息，例如进程、正在运行的应用程序等。

使用情况信息

使用情况信息显示所有目录的聚合数据（而非指定目录的数据）。

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

- **使用情况概述**显示过去六周内应用程序启动总次数以及启动应用程序的唯一用户数。
- **热门应用程序**列出了当前月份和上个月最常用的应用程序。将鼠标悬停在某个条目上会显示该应用程序的启动次数。
- **热门用户**列出了当前月份和上个月的前十名用户，以及他们启动应用程序的次数。

每周数据间隔为星期一（UTC 00:00）到查询时间。每月数据间隔为该月的第一天（UTC 00:00）到查询时间。

配置文件管理

配置文件管理可确保个人设置应用于用户的虚拟应用程序，无论用户设备位于何处。

配置配置文件管理是可选的。

您可以通过配置文件优化服务启用配置文件管理。此服务提供了一种可靠的方式来管理 Windows 中的这些设置。通过维护一个随用户移动的单一配置文件，管理配置文件可确保一致的体验。它会自动整合和优化用户配置文件，以最大程度地减少管理和存储要求。配置文件优化服务所需的管理、支持和基础架构最少。此外，配置文件优化还为用户提供了改进的登录和注销体验。

配置文件优化服务需要一个文件共享，所有个人设置都将持久保存在其中。您必须将文件共享指定为 UNC 路径。该路径可以包含系统环境变量、Active Directory 用户属性或 Profile Management 变量。要了解有关 UNC 文本字符串格式的更多信息，请参阅 指定用户存储的路径。

您可以在 Citrix Cloud 中配置 Profile Management。

配置用户配置文件管理

1. 如果您尚未登录 Citrix Cloud，请登录。在左上角菜单中，选择 **我的服务 > Virtual Apps and Desktops**。
2. 在“**管理**”选项卡上，单击“**目录**”。
3. 单击目录名称。
4. 单击“**更多设置**”。
5. 在“**在 Azure 订阅中设置 Profile Management**”中，输入配置文件共享的路径。例如，\\fileserver\share#sAMAccountName#
6. 单击“**保存**”。

启用 Profile Management 时，请考虑通过配置文件夹重定向来进一步优化用户配置文件，以最大程度地减少用户配置文件大小的影响。应用文件夹重定向可补充 Profile Management 解决方案。有关详细信息，请参阅 Microsoft 文件夹重定向。

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

配置 Microsoft RDS 许可证服务器

Citrix Virtual Apps Essentials 访问 Windows Server 远程会话功能，这些功能通常需要远程桌面服务客户端访问许可证 (RDS CAL)。VDA 必须能够联系 RDS 许可证服务器以请求 RDS CAL。安装并激活许可证服务器。有关详细信息，请参阅 激活远程桌面服务许可证服务器。对于概念验证环境，您可以使用 Microsoft 提供的宽限期。

使用此方法，您可以让 Virtual Apps Essentials 应用许可证服务器设置。您可以在主映像上的 RDS 控制台中配置许可证服务器和每用户模式。您还可以使用 Microsoft 组策略设置配置许可证服务器。有关详细信息，请参阅 使用客户端访问许可证 (CAL) 许可您的 RDS 部署。

使用组策略设置配置 RDS 许可证服务器

1. 在其中一个可用 VM 上安装远程桌面服务许可证服务器。该 VM 必须始终可用。Citrix 服务工作负载必须能够访问此许可证服务器。
2. 使用 Microsoft 组策略指定许可证服务器地址和每用户许可证模式。有关详细信息，请参阅 指定 RD 会话主机服务器的远程桌面授权模式。
3. 如果您从 Microsoft 远程访问购买了 CAL 许可证，则无需安装这些许可证。您可以从 Azure Marketplace 中的 Microsoft 远程访问购买许可证，以及 Virtual Apps Essentials。

配置 RDS 许可证服务器

1. 如果您尚未登录 Citrix Cloud，请登录。在左上角菜单中，选择 **My Services > Virtual Apps and Desktops**。
2. 在 **Manage** 选项卡上，单击 **Catalogs**。
3. 选择目录，然后选择 **More Settings**。
4. 在“输入许可证服务器的 FQDN”中，键入许可证服务器的完全限定域名。
5. 单击 **Save**。

连接用户

店面体验

Citrix Cloud 中的 Virtual Apps Essentials 为每个客户提供店面体验。创建第一个目录后，Virtual Apps Essentials 会自动配置店面 URL。用户可以通过此 URL 访问其应用程序和桌面。店面 URL 显示在“摘要”选项卡上的目录详细信息面板中。Virtual Apps Essentials 不支持本地 StoreFront 部署。

创建目录后，您可以使用 Citrix® StoreFront Cloud 自定义店面 URL 和店面外观。您还可以使用 Microsoft Entra ID 启用联合身份验证的预览版本。

使用 Microsoft Entra ID 启用联合身份验证包括以下任务：

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

- 将 Microsoft Entra ID 设置为您的身份提供程序。有关详细信息，请参阅 将 Microsoft Entra ID 连接到 Citrix Cloud。
- 为云店面启用 Microsoft Entra ID 身份验证。

有关详细信息，请参阅 StoreFront Cloud。

思杰网关服务

为允许用户安全访问其发布的应用程序，Virtual Apps Essentials 使用 Citrix Gateway 服务。此服务无需您进行任何配置。每位用户每月出站数据传输限制为 1 GB。您可以从 Azure Marketplace 购买 25 GB 附加组件。附加组件按月收费。

取消虚拟应用精简版

您可能会因 Virtual Apps Essentials 而产生 Azure 费用，原因如下：

- 虚拟应用 Essentials 订阅
- 由 Virtual Apps Essentials 创建的 Azure 资源

Virtual Apps Essentials 服务的 Microsoft Azure 费用按月收取。购买 Virtual Apps Essentials 时，您将支付当月的费用。如果您取消订单，您的服务将在下个月停止续订。您可以通过 Citrix Cloud 继续访问 Virtual Apps Essentials，直到当月月底。

您的 Azure 账单可能包含 Virtual Apps Essentials 的多个明细项，包括：

- Virtual Apps Essentials 服务订阅
- Citrix Gateway 服务附加组件（如果已购买）
- Microsoft 远程访问费用
- 使用 Virtual Apps Essentials 时创建的 Azure 资源

在 Azure 中取消 虚拟应用 Essentials

要取消您的 Virtual Apps Essentials 订阅，请在 Azure 门户中删除订单资源。

1. 登录到 Azure portal。
2. 单击 **所有资源**。
3. 在 **类型** 列中，双击打开 Citrix Virtual Apps Essentials。
4. 单击垃圾桶图标。删除过程开始。

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

删除由 Virtual Apps Essentials 创建的 Azure 资源

在 Citrix Cloud 中，删除与您的帐户关联的目录和映像。此外，删除订阅链接并确保从 Citrix Cloud 中删除 Cloud Connector VM。

如果您尚未登录 Citrix Cloud，请登录。在左上角菜单中，选择 **我的服务 > Virtual Apps and Desktops**。

删除目录

1. 在 **管理** 选项卡上，单击 **目录**。
2. 在要删除的目录旁边的省略号菜单 (...) 中，选择 **删除目录**。
3. 对每个要删除的目录重复上一步。

删除主映像

1. 在 **管理** 选项卡上，单击 **主映像**。
2. 选择一个映像并单击 **删除**。
3. 对每个要删除的主映像重复上一步。

移除 Azure 订阅链接

1. 在“**管理**”选项卡上，单击“**订阅**”。
2. 单击订阅旁边的垃圾桶图标。Azure 门户将打开。
3. 使用您的全局管理员 Azure 凭据登录到您的 Azure 订阅。
4. 单击“**接受**”以允许 Virtual Apps Essentials 访问您的 Azure 帐户。
5. 单击“**删除**”以取消订阅链接。
6. 对其他已链接的 Azure 订阅重复上述步骤。

确保移除 Citrix Cloud Connector™ VM

1. 在左上角菜单中，选择“**资源位置**”。
2. 识别 Cloud Connector 虚拟机。
3. 登录到 Azure 门户。
4. 从 Azure 的“**资源**”页面删除 VM。

合作伙伴资源

此服务现已通过 Microsoft 云解决方案提供商渠道提供。有关详细信息，请参阅 Microsoft CSP 启用 Citrix Essentials。

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

获取帮助

如果您在使用 Virtual Apps Essentials 时遇到问题，请按照如何获取帮助和支持中的说明开具工单。

更多信息

- 有关在 Virtual Apps Essentials 环境中使用 Citrix 策略的信息，请参阅 CTX220345。
- 要排查目录创建失败问题，请参阅 CTX224151。

升级到适用于 Azure 的 Citrix DaaS 标准版

了解如何从 Citrix Virtual Apps 基本版 升级到适用于 Azure 的 Citrix DaaS 标准版。

Citrix 虚拟桌面基础版™

注意：

Citrix Virtual Apps Essentials 和 Citrix Virtual Desktops Essentials 已停止销售并终止生命周期。有关详细信息，请参阅 CTX583004。

Citrix Virtual Desktops™ Essentials 允许通过 Microsoft Azure 管理和交付 Windows 10 虚拟桌面。

Virtual Desktops Essentials 专为 Azure Marketplace 设计。Citrix® 和 Microsoft 合作，为 Virtual Desktops Essentials 和 Azure IaaS 提供集成体验。这种合作关系为您提供了一个单一界面，可通过 Azure 交付完整的 Windows 10 数字商店。

使用 Virtual Desktops Essentials，您可以：

- 在 Azure 上部署和保护 Windows 10 虚拟桌面
- 通过使用 Citrix HDX™ 功能提供一流的用户体验
- 通过使用 Citrix Workspace™ 应用程序在任何设备上提供安全访问
- 从 Microsoft Azure 和 Citrix Cloud™ 管理和维护部署

Citrix Virtual Desktops Essentials 简化了 Windows 10 部署。您可以快速部署桌面，进行大规模管理，并通过单一管理平面提供丰富的用户访问体验。

您可以使用 Studio 管理 Windows 10 桌面，并使用 Director 监控会话。用户通过 Citrix Workspace 应用程序登录来连接到他们的 Windows 10 虚拟桌面。

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

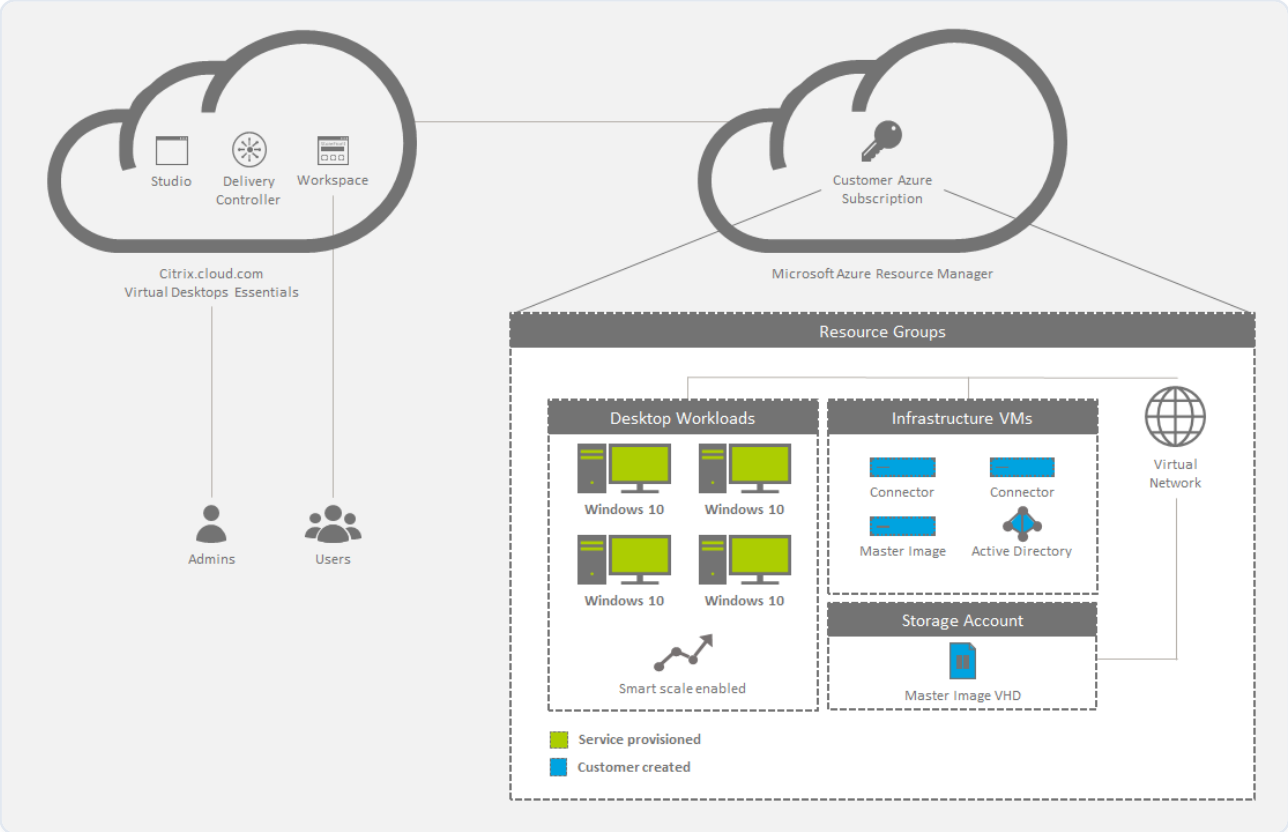
配置 Citrix Virtual Desktops Essentials 后，您将向用户提供 Citrix® StoreFront Cloud 的 URL。用户通过其设备上的 Citrix Workspace 应用程序连接到其桌面，使用您提供的 URL。当用户登录 Citrix Workspace 应用程序时，Windows 10 桌面图标将显示在商店窗口中。

重要提示：

Virtual Desktops Essentials 包含一个 StoreFront Cloud URL，通常采用 `https://<yourcompanyname>.cloud.com` 格式。设置 Virtual Desktops Essentials 后，测试并将商店 URL 链接分享给您的最终用户，以授予他们对其桌面的访问权限。Virtual Desktops Essentials 不支持本地 StoreFront。

有关商店的详细信息，请参阅 StoreFront Cloud。

此图显示了 Virtual Desktops Essentials 部署的架构概述。



新增功能

2018 年 12 月：**云托管 StoreFront™ 已移除**

云托管 StoreFront 不再适用于 Virtual Desktops Essentials。在 2017 年 12 月之前购买 Virtual Desktops Essentials（以前称为 XenDesktop® Essentials）的客户可以使用本文所述的 StoreFront Cloud 来为最终用户提供桌面访问权限。

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

2018 年 8 月：**新产品名称**

如果您是 Citrix 的长期客户或合作伙伴，您会注意到我们的产品和产品文档中出现了新名称。如果您是 Citrix 产品的新用户，您可能会看到产品或组件的不同名称。

新的产品和组件名称源于不断扩展的 Citrix 产品组合和云战略。本文使用以下名称。

- **Citrix Virtual Desktops Essentials：** 使 XenDesktop 成为行业领导者的技术现在是 Citrix Virtual Desktops，它将 VDI 引入一个现代、上下文相关、安全的应用程序，从而提供安全访问所有工作应用程序的首选方式。XenDesktop Essentials 现在是 Citrix Virtual Desktops Essentials。
- **Citrix Workspace 应用程序：** Citrix Workspace 应用程序整合了现有的 Citrix Receiver™ 技术以及其他 Citrix Workspace 客户端技术。它已得到增强，可提供更多功能，为最终用户提供统一的、上下文相关的体验，让他们能够与所有工作应用程序、文件和设备进行交互，从而发挥最佳工作效率。
- **Citrix Gateway：** NetScaler® Gateway 允许安全、上下文相关地访问您完成最佳工作所需的应用程序和数据，现在更名为 Citrix Gateway。

产品内内容可能仍包含旧名称。例如，控制台文本、消息以及目录/文件名中可能存在旧名称实例。某些项目（例如命令和 MSI）可能会继续保留其旧名称，以防止破坏现有客户脚本。

与此产品文档链接的相关产品文档和其他资源（例如视频和博客文章）可能仍包含旧名称。感谢您在此过渡期间的耐心等待。有关我们新名称的更多详细信息，请参阅 `<https://www.citrix.com/about/citrix-product-guide.html>`。

如何购买虚拟桌面基础版

有关购买或取消 Virtual Desktops Essentials 的详细信息，请下载 如何购买或取消 Virtual Desktops Essentials 服务。

系统要求、先决条件和兼容性

Virtual Desktops Essentials 需要某些补充产品和组件以及特定的帐户权限才能进行安装、配置和操作。

微软 Azure

Virtual Desktops Essentials 专门用于支持 Microsoft Azure。您的 Azure 环境必须满足某些最低要求才能支持 Virtual Desktops Essentials：

- 具有企业协议的 Azure 订阅，或 Microsoft CSP Azure 订阅。
- Windows Server 活动目录 或 Microsoft Entra ID 域服务。

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

- 一个 Microsoft Entra ID 租户。

> **重要提示：**
>
> Microsoft 要求 Azure 订阅中的 Microsoft Entra ID 租户才能部署 Windows 10 桌面。您可以使用 Microsoft Entra ID 租户或其他 Active Directory 来识别授权用户。

- 一个 Active Directory 域控制器。
- 在您首选区域中的 Azure Resource Manager (ARM) 虚拟网络和子网。使用指向域控制器的自定义域名服务器 (DNS) 条目配置虚拟网络。虚拟网络必须具有一个足够大的子网来容纳桌面。

  对 DNS 条目和桌面子网使用相同的虚拟网络。
- 一个在订阅中具有参与者（或更高）权限的 Microsoft Entra ID 用户。
- 一台已安装 Microsoft Windows 10 的虚拟机，包括您所需的自定义项和应用程序。

思杰云连接器™

Citrix Cloud Connector 验证并加密 Citrix Cloud 与您的资源位置之间的通信。对于 Virtual Desktops Essentials，您的资源位于 Microsoft Azure 中。Citrix Cloud 要求您在两台 Windows 服务器 VM 上安装 Citrix Cloud Connector，以确保您的资源位置的持续可用性。

有关 Cloud Connector 的更多信息，请参阅 Citrix Cloud Connector

思杰云

- 一个 Citrix Cloud 帐户。
- 在 Citrix Cloud 中访问 Citrix DaaS™，此访问作为您购买 Virtual Desktops Essentials 的一部分而启用。
- （可选）一个配置为 ICA® 代理模式的 NetScaler Console VPX，用于从公司网络外部进行访问。
  - ICA 代理可实现对提供给用户的应用程序和桌面的安全访问。
  - 有关设置 NetScaler Console VPX 的信息，请参阅 在 Microsoft Azure 上部署 Citrix NetScaler VPX。

已知问题

- Citrix 帮助台管理员自定义访问角色无法正常工作。作为一种解决方法，请使用 Cloud Administrator 角色，或启用完全访问权限。

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

- 如果您使用 Microsoft Entra ID Domain Services：存储登录 UPN 必须包含在启用 Microsoft Entra ID Domain Services 时指定的域名。登录不能使用您创建的自定义域的 UPN，即使该自定义域被指定为主域。

步骤 1：将您的 Azure 订阅连接到 Virtual Desktops Essentials

1. 登录到 Azure 门户。
2. 在 Azure 中，打开一台已加入域的 Windows Server 虚拟机，然后打开 Web 浏览器。
3. 在 VM 上的 Web 浏览器中，登录到 Citrix Cloud。Citrix DaaS 将打开。
4. 从左上角菜单中，选择 **资源位置**。
5. 在 **资源位置** 页面上，单击 **下载**。文件 `cwcconnector.exe` 将下载。
6. 双击下载的程序以启动安装程序。
7. 出现提示时，输入您的 Citrix Cloud 凭据。按照屏幕上的说明安装和配置 Citrix Cloud Connector。
8. 在至少一个其他服务器 VM 上重复步骤 4 到 7，以安装另一个 Cloud Connector。

在安装过程中，Cloud Connector 访问 Citrix Cloud 以进行身份验证、验证安装程序权限，然后下载和配置 Cloud Connector 提供的服务。安装使用启动安装的用户的权限。

安装后，Citrix Cloud 会在 **身份和访问管理** 中注册您的域。有关详细信息，请参阅 身份和访问管理。

步骤 2：创建主机连接

在开始之前，请确保您拥有 Microsoft Entra ID 凭据和订阅 ID。创建主机连接的 Microsoft Entra ID 用户必须是 Microsoft Entra ID 中的本机云用户或为企业域同步的用户。用户帐户不能是受邀或委派的 Microsoft 帐户。

1. 登录到 Citrix Cloud。
2. 在左上角菜单中，选择 **我的服务 > Virtual Apps and Desktops**。
3. 单击 **管理**。Studio 管理控制台将打开。
4. 在 Studio 导航窗格中选择 **配置 > 托管**。
5. 在“操作”窗格中单击 **添加连接和资源**。
6. 在“**添加连接和资源**”页面上：
   a. 在“**连接类型**”中，选择“**Microsoft Azure**”。
   b. 在 Azure 环境中，选择“**Azure Global**”，然后单击“**下一步**”。

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

7. 在“**连接详细信息**”中：
   a. 在“**订阅 ID**”中，键入 Azure 订阅 ID。
   b. 在“**连接名称**”中，键入连接名称，然后执行以下操作之一：
      i. 单击“**新建**”，然后按照过程 选项 1：创建连接。
      ii. 单击“**使用现有**”并继续配置设置。按照过程 选项 2：使用现有主机连接。

选项 1：创建连接

1. 使用订阅参与者（或更高级别）帐户登录 Azure。
2. Azure 会自动创建主机连接。在 Studio 中，“**添加连接和资源**”页面上会显示一个带有“**已连接**”字样的绿色复选标记。
3. 单击“**下一步**”。
4. 在“**区域**”页面上，选择您的虚拟网络所在的区域，然后单击“**下一步**”。
5. 在“**网络**”页面上：
   a. 键入资源的名称。
   b. 选择用于资源组的虚拟网络。
   c. 选择适用于资源组的子网，然后单击“**下一步**”。
6. 在“**摘要**”页面上，单击“**完成**”。与 Microsoft Azure Resource Manager 的主机连接已完成。

选项 2：使用现有主机连接

单击“**使用现有**”后，将显示“**现有服务主体详细信息**”页面：

1. 在“**订阅 ID**”中，键入 Microsoft Azure 订阅 ID。
2. 在“**订阅名称**”中，键入 Azure 订阅的名称。
3. 单击“**确定**”。
4. 在“**连接**”页面上：
   a. 单击“**创建新连接**”，键入您的 Microsoft Azure 订阅 ID 和连接名称（可选），然后单击“**新建**”。将显示 Microsoft 身份验证对话框。

      如果要使用您在其他时间创建的连接，请选择“**使用现有连接**”。然后，选择该连接。
   b. 键入 Microsoft Microsoft Entra ID 用户的用户名和密码。Citrix Cloud 会创建一个服务主体，该主体具有为此订阅创建和管理计算机的权限。
5. 在“**区域**”页面上，选择 Microsoft Azure 资源组所在的 Azure 区域。

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

6. 在“**网络**”页面上：
   a. 键入资源的名称。如果您键入了连接名称，请将其用作资源名称。
   b. 选择您的 Microsoft Azure 资源组的虚拟网络。
   c. 选择用于此连接的子网。如果只有一个子网，则默认选择该子网。

步骤 3：创建 Windows 10 桌面池

为托管桌面做准备，请在 Windows 10 虚拟机上安装 Citrix Virtual Delivery Agent (VDA) 软件。VDA 的作用是：

- 使计算机能够向 Virtual Desktops Essentials 注册。
- 建立并管理计算机与用户设备之间的连接。
- 验证用户或会话是否具有可用的 Citrix 许可证。
- 应用为会话配置的任何策略。
- 将会话信息传达给 Virtual Desktops Essentials。

在基础映像上安装 VDA

1. 启动 Windows 10 映像。
2. 转到 https://www.citrix.com/downloads/citrix-cloud/product-software/xenapp-and-xendesktop-service.html 并下载适用于桌面操作系统的 VDA。
3. 开始 VDA 安装。
4. 在“**环境**”页面上，单击“**使用 MCS 创建主映像**”。
5. 在“**附加组件**”页面上，选择除“**启用 Citrix App-V**”之外的所有组件。
6. 在 **Delivery Controller™** 页面上，输入您的 Cloud Connector 虚拟机的位置。单击 **Next** 并确认所有警告消息。
7. 在 **Features** 页面上，保留默认设置，然后单击 **Next**。
8. 单击 **Next** 以接受其余页面上的默认设置。
9. 在 **Summary** 页面上，单击 **Install**。
10. 重新启动虚拟机并重新登录。
11. 确认设置已生效。
12. 关闭虚拟机。VDA 注册需要关闭虚拟机。

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

创建存储帐户

在 Microsoft Azure 中，您需要一个存储帐户来托管基础映像虚拟硬盘。您可以将驱动器托管在现有存储帐户中，或创建存储帐户。

重要提示：

在创建计算机目录之前，将 Windows 10 主映像上传到 Azure 中的目标存储帐户。

创建映像存储帐户

1. 在 Microsoft Azure 导航窗格中，单击 **Storage accounts**。
2. 在 **Storage accounts** 页面上，单击 **Add**。
3. 在 **Name** 中，提供一个名称。
4. 在 **部署模型** 中，选择 **资源管理器**。
5. 在 **性能** 中，选择 **标准**。
6. 对于 **复制**、**存储服务加密** 和 **订阅**，保留默认设置。
7. 在 **资源组** 中，单击以下选项之一：
   a. 单击 **新建** 以创建资源组。键入组的名称。
   b. 单击 **使用现有** 以使用现有资源组。选择一个组。
8. 要使存储帐户显示在仪表板上，请单击 **固定到仪表板**。
9. 单击 **创建**。

创建存储帐户后，创建一个 blob 容器，然后将其命名以反映虚拟硬盘，例如“VHDs”。

创建映像 VHD 的 blob 容器

1. 在 Microsoft Azure 导航窗格中，单击 **存储帐户** 并导航到您之前创建的存储帐户。
2. 在中心导航窗格的 **BLOB 服务** 下，单击 **容器**。
3. 在详细信息窗格中，单击 **容器**。
4. 在 **新建容器** 窗格中，为容器命名。
5. 在 **访问类型** 中，选择 **Blob**，然后单击 **创建**。新 blob 容器将显示在窗格中。
6. 复制 blob URL 并将其保存到文本文件中。此 URL 稍后用于上传转换后的 VHD。

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

为 Citrix Virtual Desktops Essentials 创建计算机目录

计算机目录是作为单个实体管理的虚拟桌面集合。这些虚拟桌面是您提供给用户的资源。目录中的所有计算机都安装了相同的操作系统和相同的 VDA。

通常，您会创建一个主映像，并使用它在目录中创建相同的虚拟机。

1. 登录 Citrix Cloud。在左上角菜单中，选择 **My Services > Virtual Apps and Desktops**。
2. 选择 **Manage** 选项卡。
3. 在 Studio 导航窗格中，单击 **Machine Catalogs**。
4. 在“操作”窗格中，单击 **Create Machine catalog**。
5. 在 **Operating System** 页面上，Desktop OS 是唯一可用的选项。选择它，然后单击 **Next**。
6. 在 **Desktop Experience** 页面上：
   a. 选择 **我希望用户每次登录时都连接到相同的（静态）桌面**。
   b. 选择 **是，创建专用虚拟机并将更改保存到本地磁盘**。
7. 在 **Master Image** 页面上：
   a. 导航到并选择您之前在 blob 存储中创建的 VHD。导航树的结构与 Azure 层次结构一致：
      - 资源组
      - 存储帐户
      - 容器
      - 虚拟硬盘 (VHD)
      - 映像名称
   b. 在 **选择此目录的最低功能级别** 中保留默认选择。
8. 在 **存储和许可证类型** 页面上，选择目标存储类型和您的许可证首选项。
9. 在 **虚拟机** 页面上，选择虚拟机数量和 Azure 虚拟机大小。
10. 在 **网络接口卡** 页面上，选择一个网络适配器以与 Citrix 计算机的 Azure 子网名称关联。您还可以单击 **添加网卡** 以添加另一个网络适配器。
11. 在 **计算机帐户** 页面上：
    a. 单击 **创建新的 Active Directory 帐户**。
    b. 选择计算机帐户的域。
    c. 导航到新计算机的组织单位 (OU)。

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

   d. 为新计算机键入帐户命名方案。包含两个井号 (##) 以自动递增数字。选择数字或字母。井号将转换为命名方案。例如，mymachcatalog## 变为 mymachcatalog01 或 mymachcatalogAB。

12. 在 **域凭据** 页面上，单击 **输入凭据**，然后在 **Windows 安全中心** 对话框中，键入您的用户名和密码。此帐户用于创建计算机帐户。
13. 在 **摘要** 页面上，为目录键入名称并为管理员键入描述。
14. 点击 **完成**。

虚拟机已创建，并且 Microsoft Azure 仪表板中会出现一个新的存储帐户。当 Machine Catalog Services 部署虚拟机时，Azure 中会临时创建一个带 VHD 的准备虚拟机。

在 Microsoft Azure 中识别映像名称

1. 登录到 Azure 门户。
2. 在仪表板导航窗格中，点击 **所有资源**。将显示订阅列表。
3. 选择订阅。
4. 点击 **所有设置**。
5. 点击 **资源组**。
6. 选择资源组。
7. 选择包含 Citrix VDA 的 Windows 10 虚拟机。
8. 点击 **所有设置**。
9. 点击 **磁盘**。
10. 选择操作系统磁盘。操作系统磁盘窗口中的第一个文本框包含映像的 URL，其结构如以下示例所示。您可以从 URL 获取存储帐户名称和映像名称。例如：`https://<storage account name>.blob.core.window.net/vhds/<image name>`。
11. 在 **计算机** 页面上，列出的模板直接从您的 Azure 订阅中检索。

步骤 4：将 Windows 10 桌面分配给您的用户

交付组是选自一个或多个计算机目录的计算机集合。交付组指定哪些用户可以使用这些计算机。

1. 在 Studio 导航窗格中选择**交付组**，然后在“操作”窗格中选择**创建交付组**。
2. 指定要提供给交付组的计算机数量。您指定的数量不能超过计算机目录中可用计算机的数量。
3. 在**交付类型**页面上，选择**桌面**。

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

4. 在**用户**页面上，选择将用户管理留给 Citrix Cloud 的选项。选择此选项后，您可以使用 Citrix Cloud 管理谁可以访问交付组中的计算机。（您也可以通过 Studio 添加用户。）
5. 在**摘要**页面上，为交付组提供名称和（可选）描述。

完成这些步骤后，编辑交付组以配置用户访问权限。您可以添加或删除用户以及更改用户设置。

通过 Studio 在交付组中添加或删除用户

1. 在 Studio 导航窗格中选择**交付组**。
2. 选择一个组，然后在“操作”窗格中单击**编辑交付组**。
3. 在**用户**页面上，要添加用户，请单击**添加**，然后指定要添加的用户。要删除用户，请选择一个或多个用户，然后单击**删除**。您还可以选中或清除用于启用或禁用未经身份验证的用户访问权限的复选框。
4. 单击**确定**。

通过 Studio 更改交付组中的用户设置

此页面的名称可以显示为**用户设置**或**基本设置**。

1. 在 Studio 导航窗格中选择**交付组**。
2. 选择一个组，然后在“操作”窗格中单击**编辑交付组**。
3. 在**用户设置**（或**基本设置**）页面上：
   a. 在**描述**中，键入商店向用户显示的文本。
   b. 设置时区以匹配 Azure 时区。
   c. 选择**启用交付组**。
   d. 设置每个用户的最大桌面数。
4. 单击**确定**保存设置。

通过 Citrix Cloud 添加用户访问权限

1. 登录 Citrix Cloud，然后单击**查看库**。
2. 在桌面磁贴上，单击右下角的省略号 (…) 。
3. 搜索允许访问交付组的用户组，并将其添加到列表中。
4. 完成后，单击 **X** 关闭窗口。

您的 Windows 10 虚拟桌面已分配给添加到最终用户列表的组。

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

步骤 5：在 Azure 中配置 NetScaler Console VPX（可选）

NetScaler Console VPX 虚拟设备在 Microsoft Azure Marketplace 中以映像形式提供。在 Microsoft Azure Resource Manager 上部署 NetScaler Console VPX 时，可以使用 Azure 云计算功能。您可以根据业务需求使用 Citrix Gateway 负载平衡和流量管理功能。

您可以通过以下两种方式之一在 Azure Resource Manager 中部署 NetScaler Console VPX 实例：

- 独立实例。
- 主动-主动或主动-备用模式下的高可用性对。

如果您的用户从远程位置连接，请在 Azure 中配置 NetScaler Console VPX，以在 Citrix Workspace 应用程序和 Windows 10 桌面之间创建安全连接。

部署完成后，使用远程桌面协议 (RDP) 连接到其中一台云连接器计算机。连接后，您可以从 Citrix Gateway 管理控制台继续进行 NetScaler Console VPX 配置。

有关完整的配置信息，请参阅 在 Microsoft Azure 上部署 NetScaler Console VPX 实例。

在 Azure 中配置 NetScaler Console VPX 后，在 Citrix Cloud 中启用 Citrix Gateway。

配置 Citrix Gateway 设置以实现安全访问

1. 使用 Citrix Gateway 管理员凭据登录管理控制台。您无需配置更多 IP 地址。单击 **Skip**（跳过）。
2. 在 **Host Name**（主机名）、**DNS IP Address**（DNS IP 地址）和 **Time Zone**（时区）中，使用虚拟网络的 IP 地址和 DNS 设置。这些设置位于您的 Active Directory 域控制器上。
3. 单击 **Done**（完成）。您现在无需重新启动 NetScaler Console VPX。
4. 在“Configuration”（配置）选项卡上，单击 **Licenses**（许可证）并上传必要的许可证以配置 Citrix Gateway。
5. 许可证上传后，重新启动设备。
6. 虚拟机重新启动后，使用 Citrix Gateway 凭据再次登录。

在 Citrix 网关中配置 Citrix 虚拟桌面精简版设置

配置完上述设置后，在 Citrix Gateway 中运行快速配置向导。有关详细信息，请参阅使用快速配置向导配置设置。

配置 Citrix Gateway 以实现高可用性和负载平衡

在 Microsoft Azure 部署中，通过使用 Azure 负载均衡器实现两个 Citrix Gateway 虚拟机的高可用性配置。负载均衡器将客户端流量分配到两个 Citrix Gateway 实例上配置的虚拟服务器。

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

如果客户端流量源自 Internet，请在 Internet 和 Citrix Gateway 实例之间部署外部负载均衡器以分配客户端流量。有关此配置的详细信息，请参阅使用单个 IP 地址和单个 NIC 配置高可用性设置。

您还可以将入站端口 80 添加到 Citrix Gateway 网络安全组，以使用其公共 IP 地址配置 Citrix Gateway。配置完成后，您可以删除入站端口 80 规则以保护对管理控制台的访问。

步骤 6：连接用户

StoreFront Cloud 将服务交付给用户设备。在 Citrix Cloud 控制台中，从左上角菜单中选择 **StoreFront Cloud**。

创建第一个目录后，Virtual Desktops Essentials 会自动配置应用商店 URL。此 URL 显示在目录详细信息下。您可以自定义应用商店 URL 和应用商店的外观。您还可以启用使用 Microsoft Entra ID 的联合身份验证的预览版本。有关详细信息，请参阅StoreFront Cloud。

1. 在 Citrix Cloud 控制台中，从左上角菜单中选择 **StoreFront Cloud**。选择**服务集成**选项卡。将列出该服务。
2. 使用您的域凭据登录到应用商店 URL 并启动桌面，以测试您的连接。
3. 向您的用户提供 URL，他们可以复制该 URL。用户可以在其浏览器或 Citrix Workspace 应用程序的地址栏中键入或粘贴该 URL 以访问桌面。

使用 NetScaler Console VPX 进行远程访问

1. 在 Citrix Cloud 控制台中，单击**管理**，然后单击**服务交付**。
2. 启用 **Citrix 网关**。
3. 在资源位置中选择**使用您自己的 Citrix Gateway**。
4. 在文本字段中输入 Citrix Gateway 地址。不要包含协议。您可以包含端口号。
5. 如果您需要该功能，请启用会话可靠性。
6. 保存。
7. 使用您的域凭据登录商店 URL 并启动桌面，以测试您的连接。
8. 向您的用户提供 URL，他们可以复制该 URL。用户可以在其浏览器或 Citrix Workspace 应用程序的地址栏中键入或粘贴该 URL 以访问桌面。

合作伙伴资源

此服务也可通过 Microsoft 云解决方案提供商渠道获得。有关详细信息，请参阅 Microsoft CSP enablement for Citrix Essentials。

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

升级到适用于 Azure 的 Citrix DaaS Standard

了解如何 从 Citrix Virtual Desktops Essentials 升级到适用于 Azure 的 Citrix DaaS Standard。

微软 CSP 对 Citrix Essentials 的启用

Citrix Virtual Apps Essentials 和 Citrix Virtual Desktops Essentials™ 服务现已通过 Microsoft 云解决方案提供商渠道提供。作为 Microsoft 云解决方案提供商，您可以代表您的客户购买 Citrix Virtual Apps Essentials 或 Citrix Virtual Desktops Essentials。作为 Citrix 服务提供商，您可以访问 Citrix Cloud 合作伙伴帐户，该帐户允许您为客户创建新的 Citrix Cloud 帐户。（如果您不是 Citrix 服务提供商合作伙伴，客户必须授予您对其 Citrix Cloud 帐户的访问权限。）

在本文中，*Citrix Essentials* 指的是 Citrix Virtual Apps Essentials™ 或 Citrix Virtual Desktops Essentials。示例和屏幕截图显示的是 Citrix Virtual Apps Essentials。

新增功能

产品名称变更：

- XenApp Essentials 现已更名为 **Citrix Virtual Apps™ 基本版**。
- XenDesktop Essentials 现已更名为 **Citrix Virtual Desktops™ 基本版**。

其他站点和信息源可能包含旧名称。例如，本文中的一些屏幕截图显示的是旧名称。感谢您在此过渡期间的耐心等待。有关产品名称变更的更多信息，请参阅 `<https://www.citrix.com/about/citrix-product-guide.html>`。

要求

- Citrix Cloud 合作伙伴帐户：您必须是 Citrix 服务提供商。
- Microsoft Azure 帐户：您必须是 Microsoft 云解决方案提供商（一级或二级），并有权访问 Microsoft 合作伙伴中心。

过程摘要

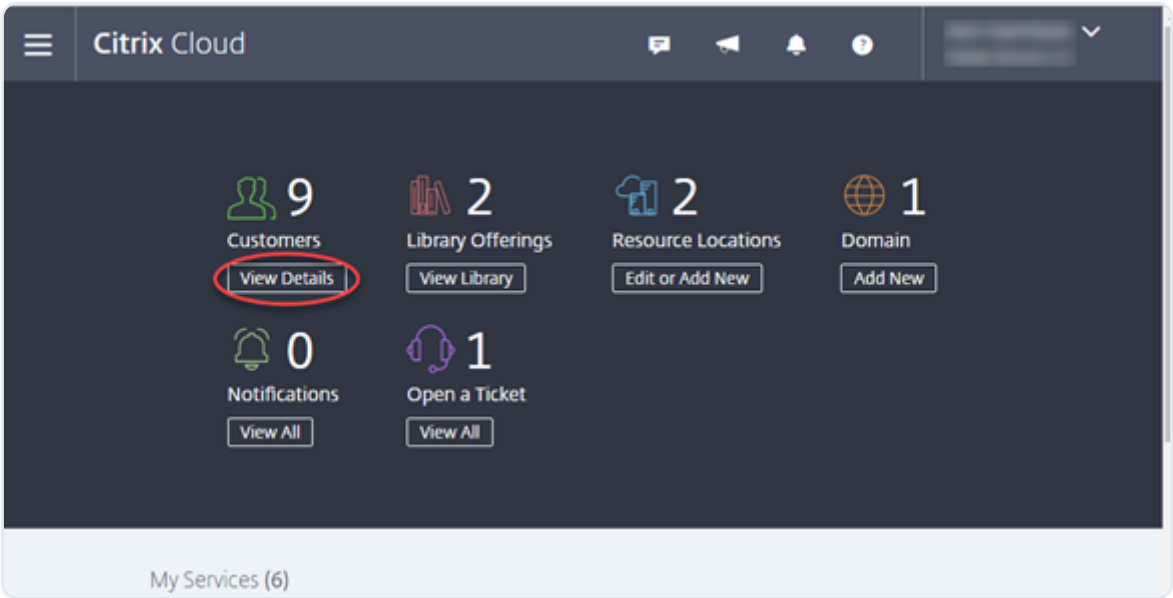
- 从 Citrix Cloud™，为客户创建 Citrix Cloud 帐户。如果客户已有 Citrix Cloud 帐户，请跳过此过程。但是，当您购买 Citrix Essentials 服务时，您将需要这些帐户详细信息。
- 从 Microsoft 合作伙伴中心门户，为客户创建 Azure 订阅。如果客户已有 Azure 订阅，请跳过此过程。
- 从 Azure Marketplace，为客户购买 Citrix Essentials 服务。

完成本文概述的任务后，从 Citrix Cloud 部署环境。有关详细信息，请参阅 Essentials 产品文档。

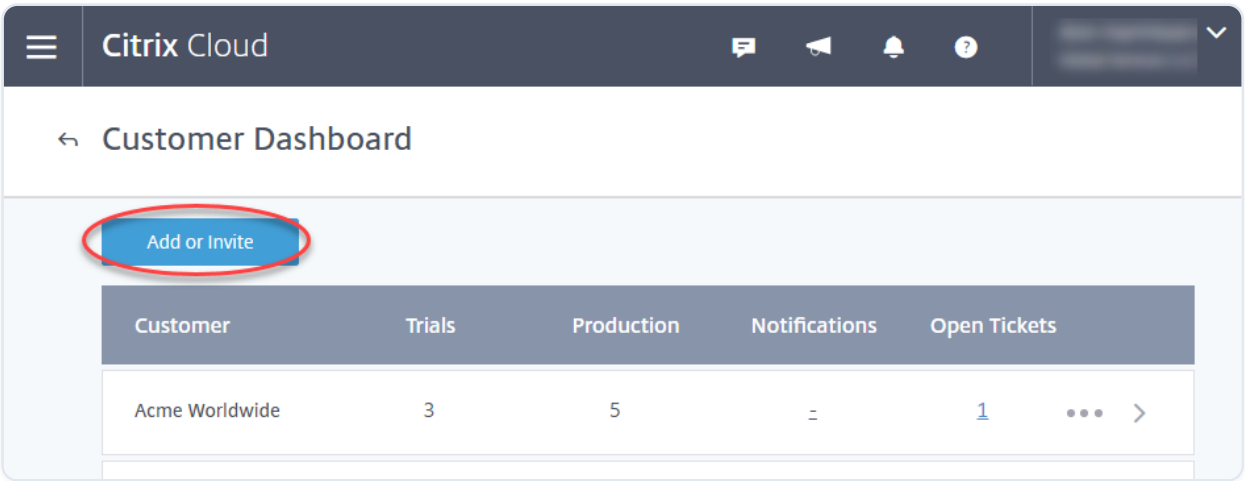
© 1997–2026 Citrix Systems, Inc. All rights reserved.

为客户创建 Citrix Cloud 帐户

1. 使用您的 Citrix Cloud 合作伙伴帐户凭据登录到 Citrix Cloud。
2. 在 **客户** 下，单击 **查看详细信息**。

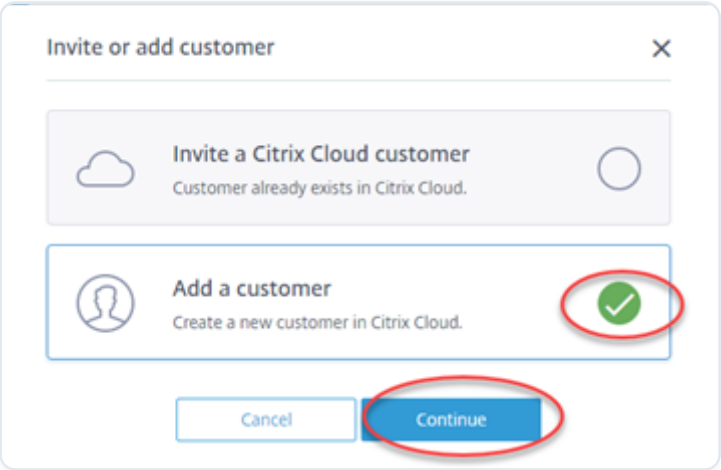


3. 在 **客户控制板** 页面上，单击 **添加或邀请**。

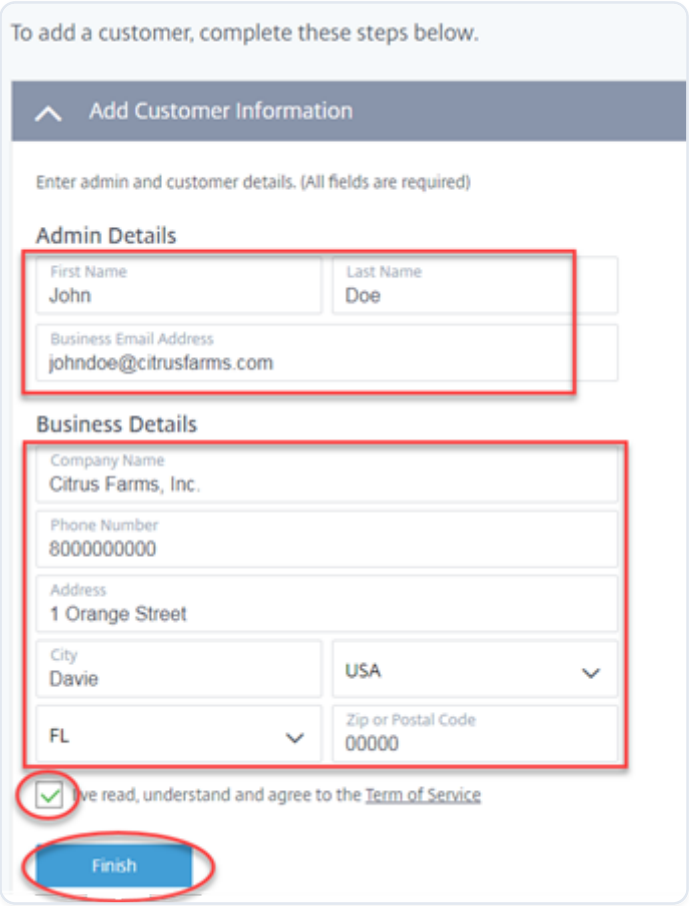


4. 在 **邀请或添加客户** 页面上，选择 **添加客户**，然后单击 **继续**。

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

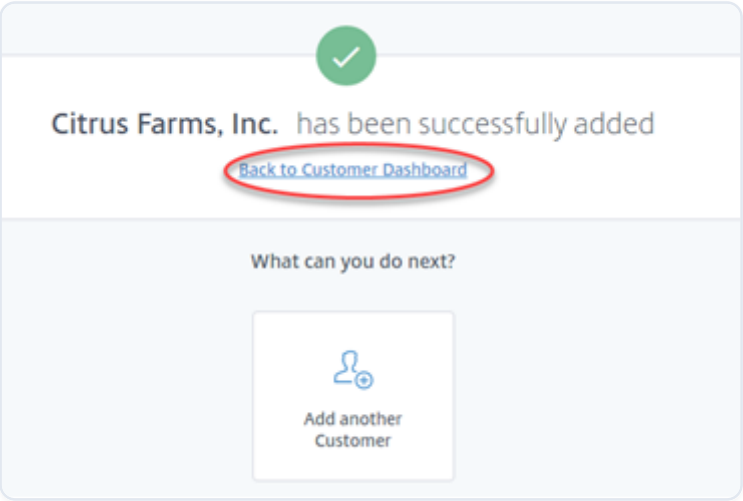


5. 输入管理员和业务详细信息。所有字段均为必填项。查看服务条款，然后选中确认复选框。然后，单击 **完成**。



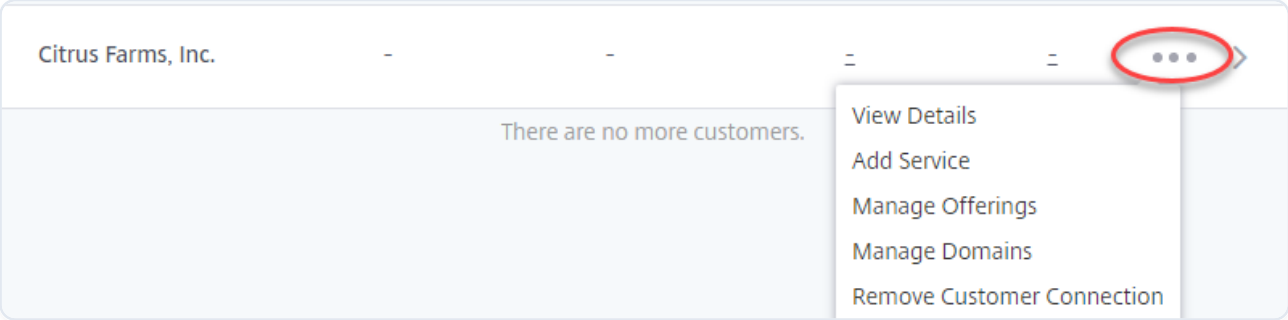
6. 成功添加客户后，选择 **返回客户控制板**。

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



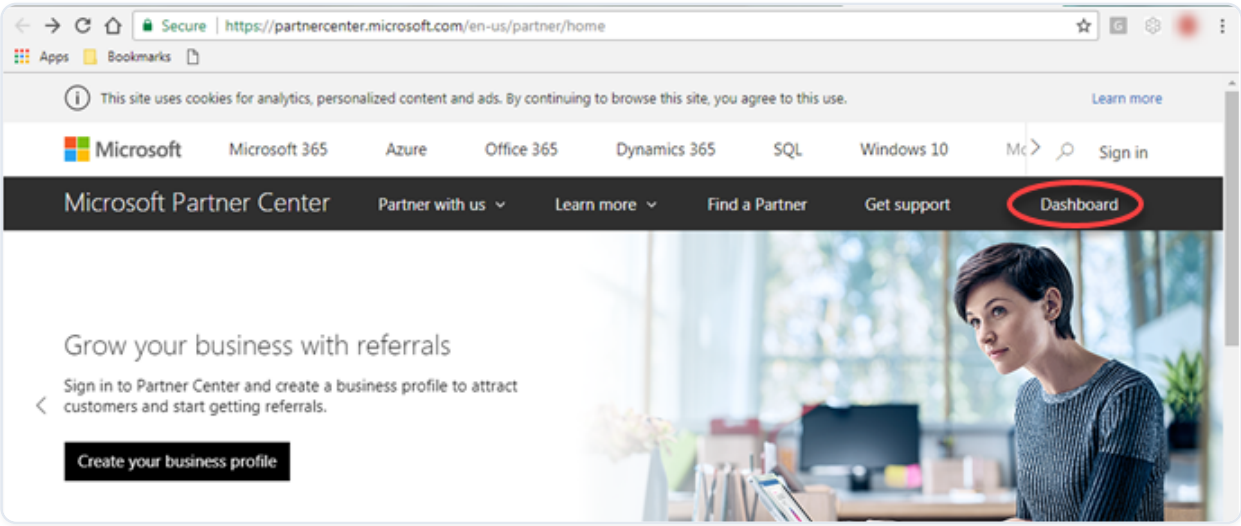
结果

客户控制板现在列出了您添加的客户。选择客户行上的省略号会显示一个操作菜单，您可以在以后使用该菜单。



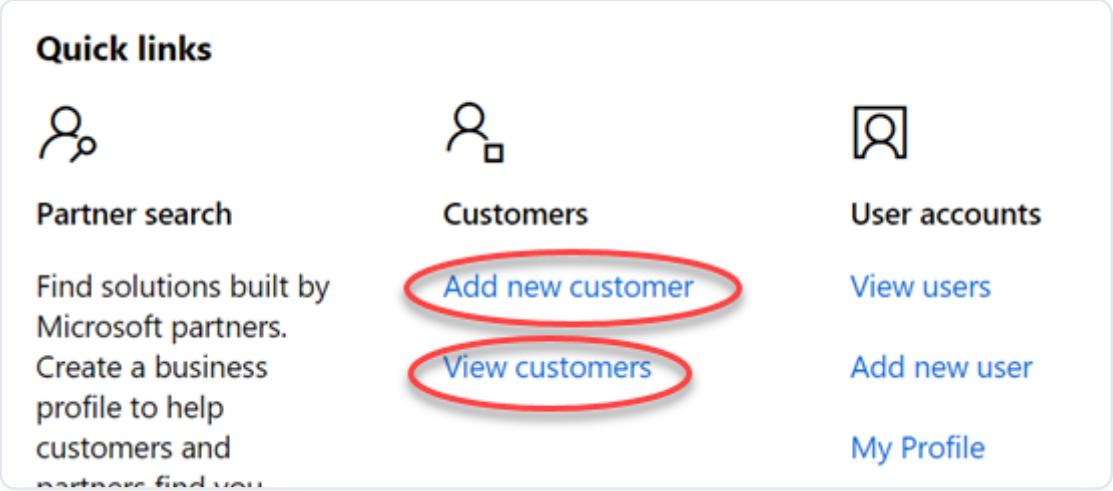
为客户创建 Azure 订阅

1. 使用您的 Microsoft 帐户凭据登录到 Microsoft 合作伙伴中心。如果您有多个 CSP 帐户，请选择您要使用的帐户。
2. 在合作伙伴中心主页上，单击 **仪表板**。



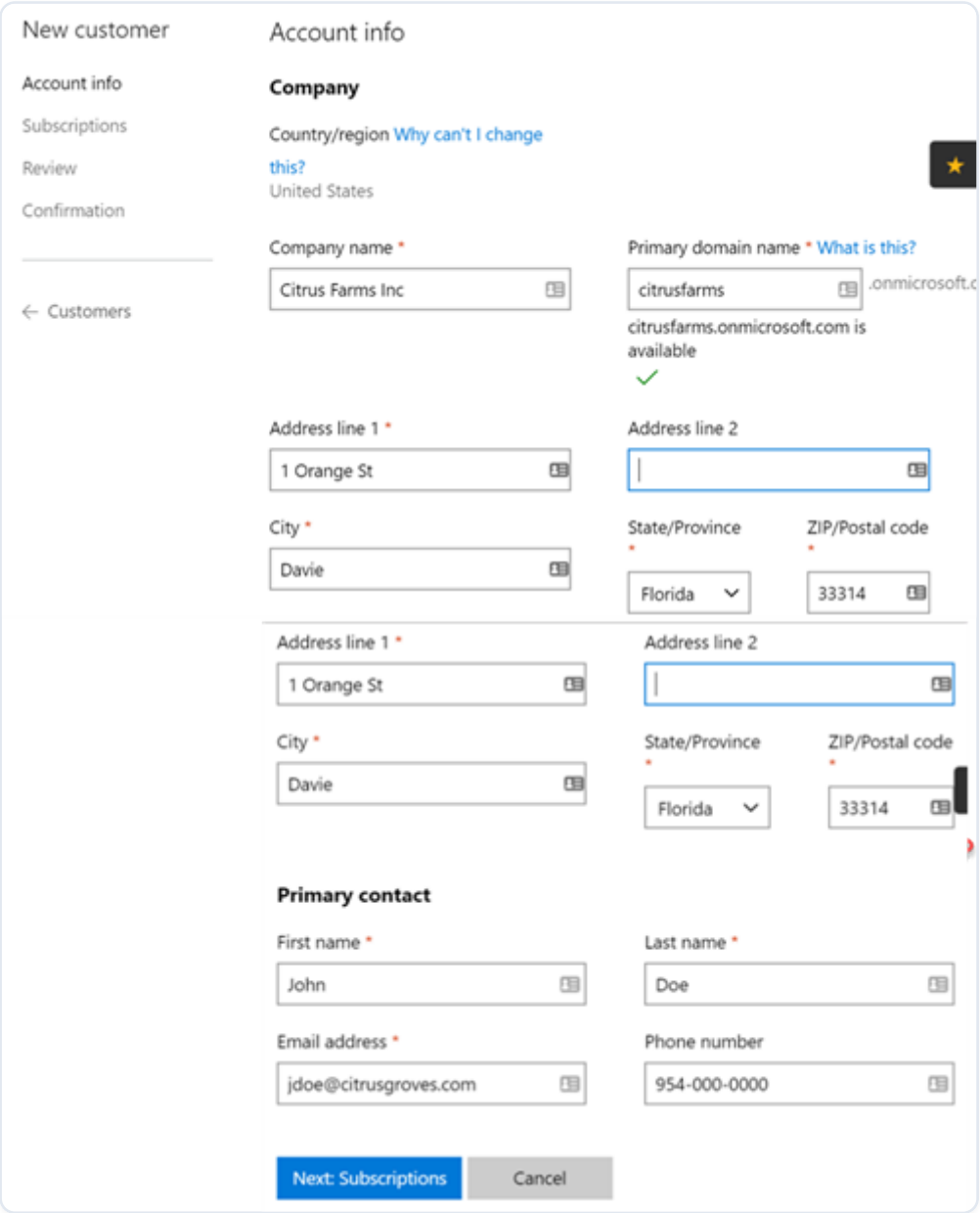
© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. 在仪表板概览页面的 **快速链接** 部分中，如果您要添加客户，请单击 **添加新客户**。如果您的客户已存在，请单击 **查看客户**。



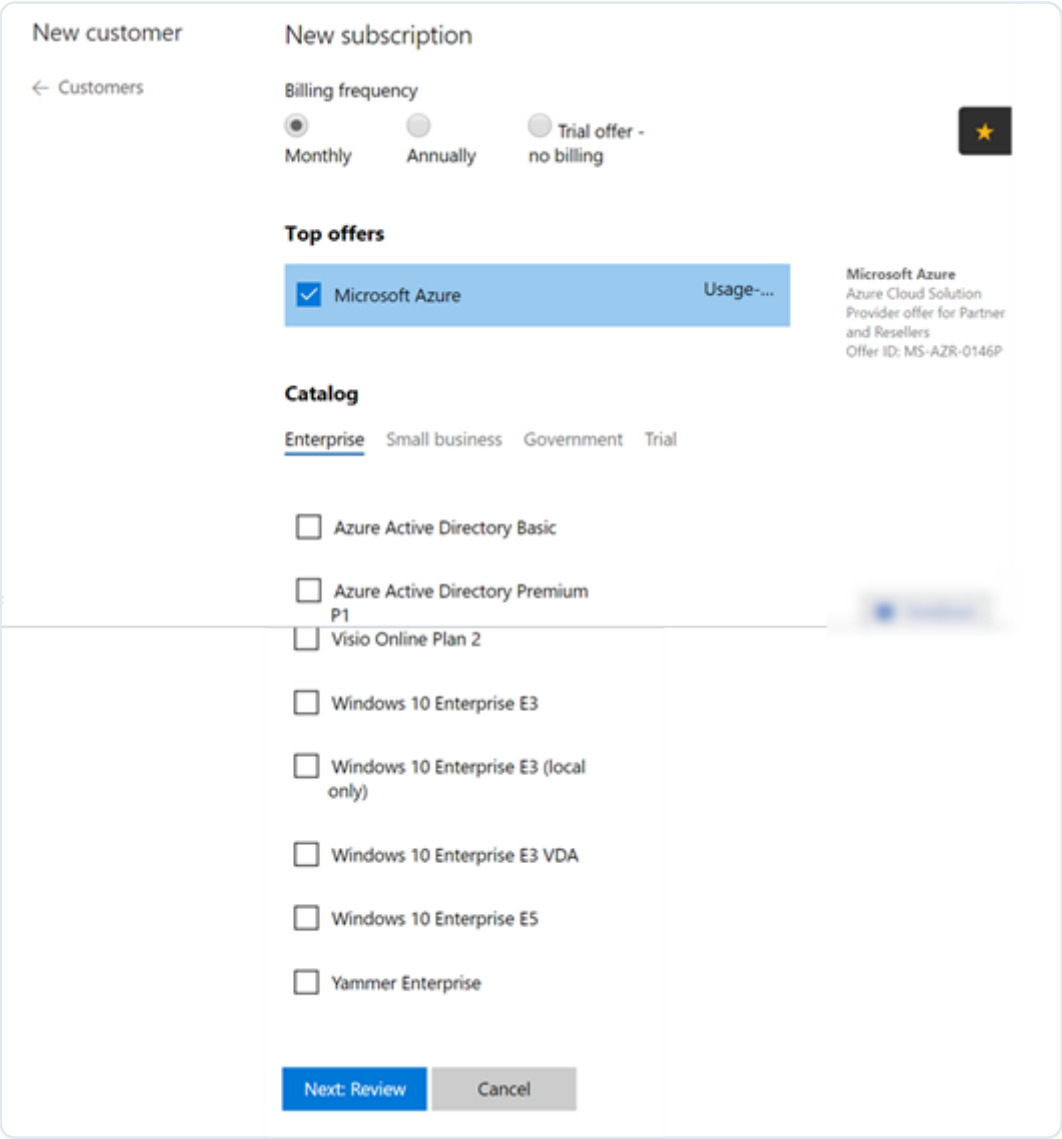
4. 如果您的客户已存在，请在客户名称右侧的快速链接菜单中，选择 **查看订阅**。如果客户没有 Microsoft Azure 订阅，请单击 **添加订阅**，然后继续执行步骤 6。如果客户已有 Microsoft Azure 订阅，请跳过本节的其余部分，然后继续执行 为客户购买 Citrix Essentials 服务。
5. 如果您要添加客户，请在 **帐户信息** 页面上，输入公司名称、域名、地址和联系方式。然后单击 **下一步: 订阅**。

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

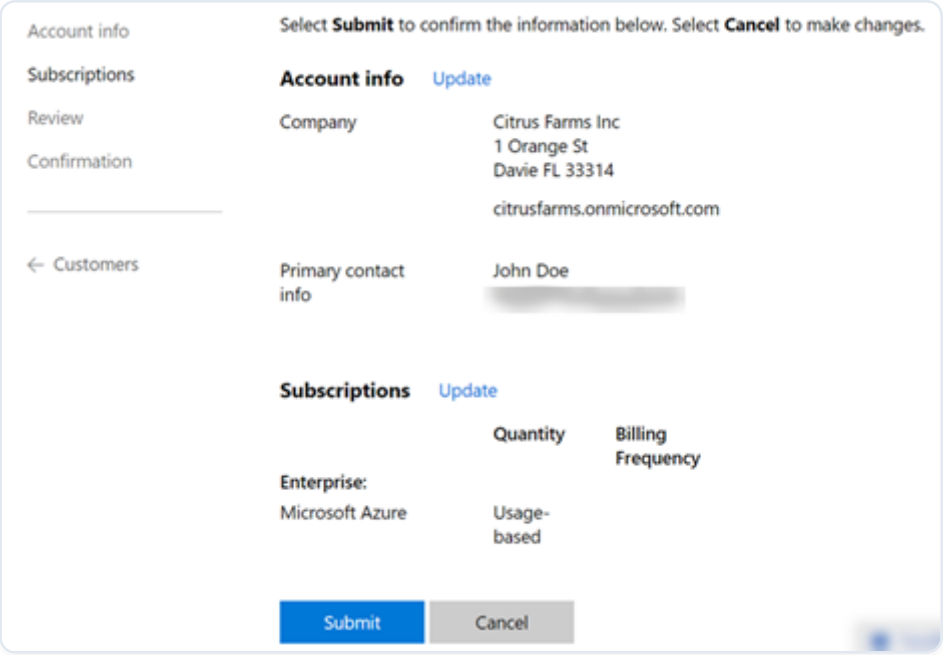


6. 在 **新建订阅** 页面上，选择计费频率、**Microsoft Azure** 顶级优惠和目录类型。然后单击 **下一步: 审阅**。

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



7. 在 **审阅** 页面上，确保信息正确无误。然后单击 **提交**。



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

8. **重要提示：** 从 **确认** 页面复制设置信息：Microsoft ID、管理员用户帐户和密码。离开此页面后，您将无法再次查看密码。

复制设置信息后，在左侧窗格中选择 **客户**。

返回客户列表(/en-us/citrix-cloud/media/ms-newcustomer-confirm-60.png)

结果

客户 页面现在列出了您添加的客户。

客户列表中的新条目(/en-us/citrix-cloud/media/ms-customers-60.png)

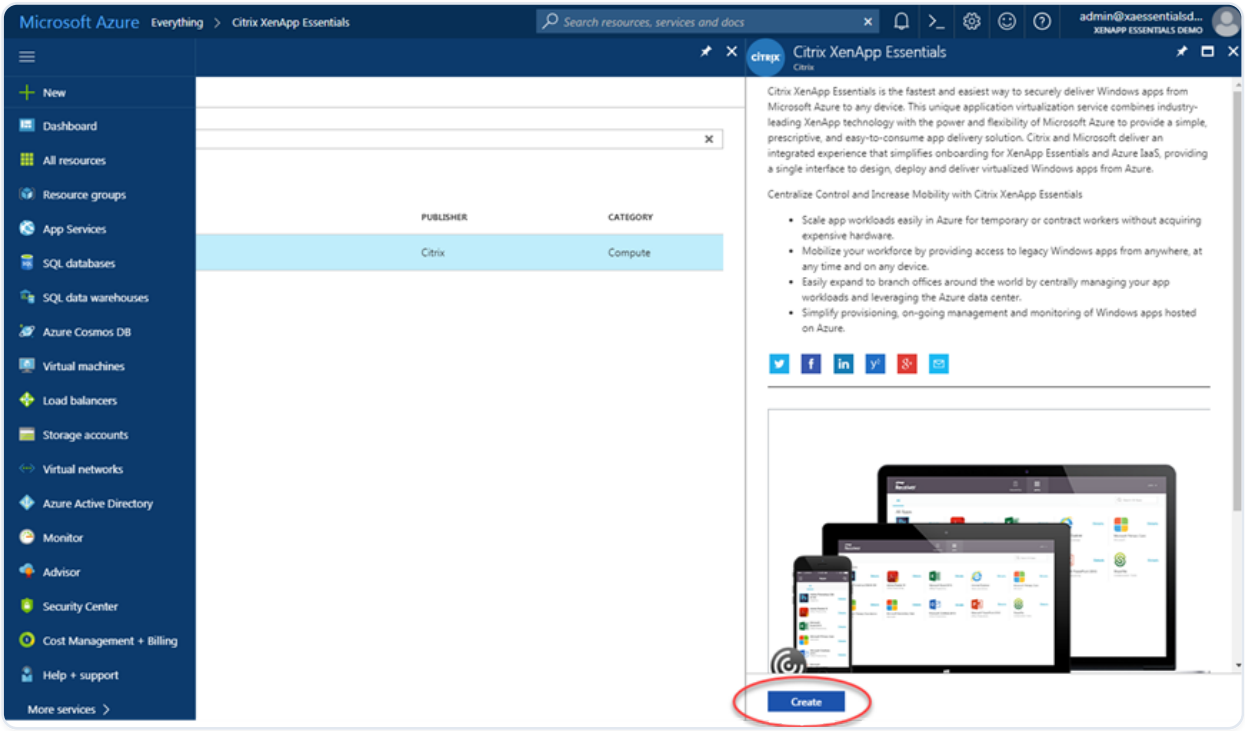
订阅 页面现在列出了您为所添加客户选择的订阅。

订阅列表中的新条目(/en-us/citrix-cloud/media/ms-subscriptions-60.png)

为客户购买 Citrix Essentials

1. 如果您尚未登录 Microsoft Partner Center，请立即登录。
2. 在 **订阅** 页面上，单击 **服务管理**。此页面列出了服务的管理门户。单击 **Azure 管理** 门户。
3. 在左侧窗格中单击 **新建**。在搜索字段中，开始键入 Citrix Essentials 服务名称。例如 **Citrix Virtual Apps Essentials**。在 **结果** 下，选择相应的条目。例如 **Citrix Virtual Apps**。

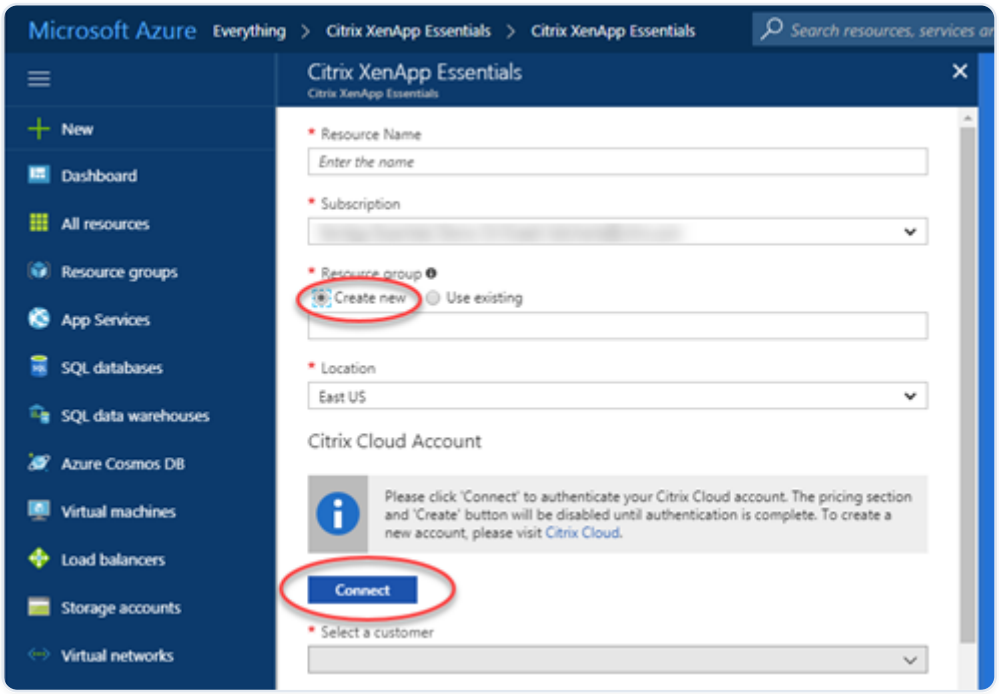
   查找并选择 Citrix Virtual Apps Essentials(/en-us/citrix-cloud/media/ms-xae.png)
4. 单击 **创建**。



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

5. 完成以下配置，然后单击 **连接**。

   - **资源名称：** 键入一个易于识别的名称。如果您将来决定取消 Citrix Essentials 服务，请使用此名称。此资源仅代表 Citrix Essentials 服务订单。如果您在 Azure 中删除此资源，则会取消您的 Citrix Essentials 服务订阅。）
   - **订阅：** 选择客户的 Microsoft Azure 订阅。
   - **资源组：** 创建资源组。（默认情况下，此页面已选择“使用现有”。如果您已有此订阅和客户的资源组，请选择它。否则，请创建一个新的。）
   - **位置：** 选择资源的位置。



   您将自动转到 Citrix Cloud 登录页面。

6. 输入您的 Citrix Cloud 凭据，然后单击“**登录**”。Microsoft Azure 将确认您的凭据并将您返回到 Azure 门户。

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

Citrix Cloud 文档历史记录

下表描述了 Citrix Cloud 产品文档的重要更改。要接收有关这些更新的通知，请订阅 RSS 源。

日期	更改	描述
29 Jan 2025	添加了服务主体信息	添加了新部分 服务主体
16 Dec 2024	添加了新功能条件身份验证	添加了新功能 条件身份验证
27 Sep 2024	添加了新部分引导新客户入驻	添加了新部分 引导新客户入驻
17 Sep 2024	更新了账户管理部分	更新了 账户管理 中的许可证管理
13 Sep 2024	添加了新部分用于高级故障排除的数据包捕获功能	添加了新部分 用于高级故障排除的数据包捕获功能
10 Jun 2024	添加了新文章	添加了新文章 使用 Azure AD 进行工作区身份验证的 SAML（适用于访客和 B2B 身份）
29 Apr 2024	添加了 2 个新部分	添加了 更新服务提供商 SAML 签名证书 和 更新身份提供商 SAML 签名证书
08 Apr 2024	添加了新部分允许客户删除 Citrix Cloud 账户并重新入驻	添加了新部分 允许客户删除 Citrix Cloud 账户并重新入驻
22 Mar 2024	添加了新部分	添加了新部分 将本地 PingFederate 服务器配置为工作区和 Citrix Cloud 的 SAML 提供商
19 Mar 2024	添加了新说明	在 使用库将用户和组分配给服务产品 中添加了新说明

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

日期	更改	描述
14 Mar 2024	添加了自定义登录页面部分	添加了新部分 自定义登录页面
28 Feb 2024	删除了 NetScaler App Delivery and Security Service - Citrix Managed	从 服务级别协议 中删除了对 NetScaler App Delivery and Security Service - Citrix Managed 的引用
27 Feb 2024	使用情况收集部分更新	在 使用情况收集 中添加了用户客户标记、免费服务器标记和服务器客户标记子部分
19 Feb 2024	添加了其他证书	在 证书验证要求 中添加了 Citrix DaaS 的其他证书
02 Feb 2024	新的 SAML 身份提供商文章	添加了新文章 使用 Azure AD 和 AD 身份进行工作区身份验证的 SAML
31 Jan 2024	更新了支持的服务	在 支持的服务 中将 Citrix Application Delivery Management service 更改为 NetScaler Console
31 Jan 2024	添加了 License Usage Insights 作为新服务	在 支持的服务 中添加了 License Usage Insights 作为新服务
23 Jan 2024	添加了 Citrix 身份提供商	在 身份和访问管理 中添加了 Citrix 身份提供商部分
20 Dec 2023	删除了 Citrix App Delivery and Security Service - Citrix Managed	在 地域注意事项 中删除了对 Citrix App Delivery and Security Service - Citrix Managed 的引用
20 Dec 2023	删除了 Citrix App Delivery and Security Service	从 在 Citrix Cloud 中配置具有范围实体 ID 的 SAML 应用程序 中删除了 Citrix App Delivery and Security Service

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

日期	更改	描述
30 Nov 2023	SAML 作为身份提供商的新功能	添加了一篇新文章，描述了对范围实体 ID 的支持：在 Citrix Cloud 中配置具有范围实体 ID 的 SAML 应用程序
16 Nov 2023	删除了 Directory.Read.All 引用	从 Azure AD 与 Citrix Cloud 之间的默认连接 Citrix Cloud 的 Azure Active Directory 权限 中删除了对 Directory.Read.All 的引用
20 Oct 2023	删除了 ShareFile 引用	由于将这些服务与 Citrix Cloud 解耦，已删除对 ShareFile 和 Citrix Files 的引用：常见问题解答：将您的 ShareFile 账户与 Citrix Workspace 解耦)
19 Oct 2023	SAML 作为身份提供商的新文章	添加了新文章，用于使用 Okta 作为 SAML 提供商配置 SAML 身份验证：将 Okta 配置为工作区身份验证的 SAML 提供商)
18 Sep 2023	DaaS Standard for Azure 许可的新功能	添加了对用户/设备许可模型的域名截断支持：监控 Citrix DaaS Standard for Azure 的许可证和使用情况)
18 Sep 2023	DaaS 许可的新功能	添加了对域名截断的支持：监控 Citrix DaaS（用户/设备）的许可证和活动使用情况
07 Sep 2023	新的 SAML 身份提供商文章	添加了新文章，用于为使用 Azure AD 身份的 Citrix Workspace 订阅者配置 SAML 身份验证：使用 Azure Active Directory 身份通过 SAML 登录工作区

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

日期	更改	描述
06 Sep 2023	SAML 身份验证更新	添加了支持的提供商并澄清了几个步骤：将 SAML 作为身份提供商连接到 Citrix Cloud
04 Aug 2023	新的 SAML 身份提供商文章	添加了新文章，用于配置 ADFS 中的信赖方信任，以便将 SAML 用作 Citrix Cloud 中的身份提供商：将 SAML 作为身份提供商连接到 Citrix Cloud
01 Aug 2023	SAML 身份验证更新	更新了 SAML 自定义属性和故障排除信息：使用 ADFS 在 Citrix Cloud 中配置 SAML 身份验证
21 Jul 2023	ITSM Adapter service 2307 的初始版本	有关新增功能的摘要，请参阅新增功能
17 Jul 2023	管理员更新	添加了访问支持票证菜单选项的管理员权限：修改管理员权限
30 Jun 2023	系统日志更新	添加了管理网络位置的事件：Citrix Cloud 平台的系统日志事件
27 Jun 2023	身份和访问管理更新	添加了对使用 Google Cloud Identity 进行管理员身份验证的支持：身份和访问管理
27 Jun 2023	身份和访问管理更新	添加了对使用 Google Cloud Identity 进行管理员组身份验证的支持：管理管理员组
21 Jun 2023	服务运行状况仪表板更新	更新了访问服务运行状况仪表板的方法：Citrix Cloud 服务运行状况

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

日期	更改	描述
25 May 2023	管理员更新	更新了管理 MFA 验证方法的步骤：管理您的 MFA 恢复方法
25 May 2023	管理员更新	更新了更改 MFA 设备、主要 MFA 登录方法的步骤：管理您的主要 MFA 方法
25 May 2023	管理员更新	为 Citrix Cloud 管理员添加了对电子邮件作为 MFA 方法的支持：设置多重身份验证
15 May 2023	Citrix 服务提供商更新	为分销商添加了对许可 API 访问的支持：分销商对 API 的访问
03 May 2023	系统日志更新	添加了用于创建、修改和删除资源位置的系统日志事件：Citrix Cloud 平台的系统日志事件
03 Apr 2023	管理员管理更新	可以将对某些 Citrix Cloud 平台功能的自定义访问权限分配给管理员组：管理管理员组
30 Mar 2023	Citrix 合作伙伴更新	合作伙伴可以通过客户仪表板查看 Citrix Gateway service 的带宽使用趋势：许可趋势
22 Mar 2023	已停用内容	AppBuilder 文章已删除，因为该服务在 Citrix Cloud 中不再可用。
09 Jan 2023	Citrix 服务提供商的 DaaS 许可更新	更新了文章以包含 Citrix DaaS 并发用户模型的活动使用情况：Citrix DaaS 的客户许可证和使用情况监控
06 Jan 2023	DaaS 许可更新	更新了文章以包含 Citrix DaaS 并发用户模型的活动使用情况：监控 Citrix DaaS

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

日期	更改	描述
		（并发用户）的许可证和峰值使用情况
06 Jan 2023	License Usage Insights 服务更新	更新了文章以包含管理免费用户的增强功能：管理产品使用情况、许可证服务器和通知
30 Nov 2022	已删除已弃用的 MDX Service 文章	MDX Service 已于 2021 年 9 月达到生命周期结束 (EOL)。有关详细信息，请参阅 CXM-100702。
02 Nov 2022	服务存在表更新	将欧盟添加到 Citrix DaaS for Google Cloud 的区域列表中：各区域的服务存在
10 Oct 2022	通知更新	为非管理员联系人添加了通知：通知
28 Sep 2022	Azure AD 身份更新	更新了添加管理员的部分：从 Azure AD 将管理员添加到 Citrix Cloud
28 Sep 2022	管理员管理更新	更新了添加单个 Citrix Cloud 管理员的屏幕截图和工作流程：管理对 Citrix Cloud 的管理员访问
22 Sep 2022	ITSM Adapter service 2209 的初始版本	有关新增功能的摘要，请参阅新增功能
11 Aug 2022	SAML 身份更新	更新了添加 AD 管理员组的屏幕截图和工作流程：从 AD 将管理员添加到 Citrix Cloud
11 Aug 2022	Azure AD 身份更新	更新了添加 Azure AD 管理员组的屏幕截图和工作流程：管理管理员组
11 Aug 2022	管理员管理更新	更新了添加单个 Citrix Cloud 管理员的屏幕截图和工作流程：管理 Citrix Cloud 管理员

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

日期	更改	描述
25 Jul 2022	SAML 身份更新	为 AD 组添加了对 SAML 身份验证的支持：将 SAML 作为身份提供商连接到 Citrix Cloud
18 Jul 2022	Citrix DaaS 许可更新	更新了文章以包含对 Citrix DaaS 和 Citrix DaaS Standard for Azure 的并发许可支持：监控 Citrix DaaS（并发用户）的许可证和峰值使用情况
18 Jul 2022	Citrix DaaS Standard 许可更新	更新了文章以包含对并发许可模型的支持引用：监控 Citrix DaaS Standard for Azure 的许可证和使用情况
29 Jun 2022	Google 作为身份提供商的新文章	Citrix Cloud 现在支持使用 Google 进行工作区身份验证：将 Google 作为身份提供商连接到 Citrix Cloud
23 Jun 2022	ITSM Adapter service 2206 的初始版本	有关新增功能的摘要，请参阅新增功能
05 May 2022	Cloud Connector 高级运行状况检查功能的新文章	添加了描述新 Cloud Connector 高级运行状况检查功能的文章：Cloud Connector 高级运行状况检查
02 May 2022	更新了许可文章	Citrix DaaS 和 Endpoint Management 分配许可证的发布体验已优化，以更好地支持批量发布许可证：监控 Citrix DaaS 的许可证和活动使用情况 和 监控 Endpoint Management 的许可证和活动使用情况
28 Apr 2022	合作伙伴的新管理员权限	添加了访问客户仪表板的新权限：Citrix Cloud for Partners

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

日期	更改	描述
28 Apr 2022	SDK 和 API 新文章	添加了一篇新文章，总结了适用于 Citrix Cloud 和云服务的 SDK 和 API：SDK 和 API
25 Apr 2022	Azure AD 权限更新	新的 Azure AD 连接现在包含 GroupMember.Read.All 权限，而不是 Group.Read.All：Citrix Cloud 的 Azure Active Directory 权限。
15 Apr 2022	Cloud Connector 上的 Windows 支持更新	Citrix Cloud Connector 支持在 Windows Server 2022 上部署。有关详细信息，请参阅 Cloud Connector 技术详细信息。
30 Mar 2022	系统日志正式发布	系统日志已正式发布，并包含生成事件的描述。有关功能详细信息，请参阅 系统日志。有关事件描述，请参阅 系统日志事件参考
21 Mar 2022	Gateway service 许可更新	许可现在显示 Gateway service 的每个用户的带宽使用情况：监控 Gateway service 的带宽使用情况
17 Mar 2022	更新了 ITSM Adapter 文章	有关 ITSM Adapter 新功能的摘要，请参阅 新增功能
14 Mar 2022	Citrix Cloud 管理员更新	管理员可以添加电子邮件地址以进行账户恢复：添加或更改您的恢复电子邮件
12 Jan 2022	许可更新	添加了对 Citrix Virtual Apps and Desktops 多类型许可的支持：监控云服务的许可证和活动使用情况
17 Dec 2021	本地产品注册更新	支持删除从注册的 Citrix License Servers 收集的使用

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

日期	更改	描述
		数据：在 Citrix Cloud 中注册本地产品
13 Dec 2021	更新了 ITSM Adapter 文章	有关新增功能的摘要，请参阅新增功能
08 Dec 2021	新的云许可文章	许可包括对 Citrix Managed Azure 消耗监控的支持：监控 Virtual Apps and Desktops service 的 Citrix Managed Azure 资源消耗
01 Dec 2021	新的云许可文章	许可包括对 Secure Private Access service 的支持：监控 Secure Private Access 的许可证和使用情况
08 Nov 2021	添加 Azure AD 组的新文章	支持使用 Azure AD 组添加管理员：管理管理员组
03 Nov 2021	更新了 Cloud Connector 网络要求	添加了有关如何为 Cloud Connectors 使用完全限定域名的详细信息，请参阅 互联网连接要求：Citrix Cloud Connector
25 Oct 2021	更新了 ITSM Adapter 文章	有关新增功能的摘要，请参阅新增功能
29 Sep 2021	更新了 Remote Browser Isolation（以前称为 Secure Browser）文章	请参阅 Remote Browser Isolation。
14 Sep 2021	身份文章更新	Citrix Cloud 的 SAML 身份验证已向客户正式发布：将 SAML 作为身份提供商连接到 Citrix Cloud
26 Aug 2021	License Usage Insights 更新	添加了用于监控 CSP 客户的 Virtual Apps and Desktops service 许可和使用情况的文章：Citrix Virtual Apps and

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

日期	更改	描述
		Desktops service 的客户许可证和使用情况监控
26 Aug 2021	License Usage Insights 更新	添加了用于许可证使用情况的单租户和多租户聚合的文章：Citrix 服务提供商的云服务许可证使用情况和报告
19 Aug 2021	更新了 ITSM Adapter 文章	有关新增功能的摘要，请参阅新增功能
20 Jul 2021	Cloud Connector 更新的更多故障排除	添加了有关故障排除 Cloud Connector 更新失败的信息：故障排除更新失败
14 Jul 2021	添加了 Azure Active Directory 的权限	添加了 Citrix Cloud 在连接和使用 Azure Active Directory 时请求的权限：Citrix Cloud 的 Azure Active Directory 权限
13 Jul 2021	许可更新	添加了由于迁移而导致许可证重复计算的常见问题解答项：监控云服务的许可证和活动使用情况
13 Jul 2021	许可更新	更新了技术预览通知，以包含带宽分配的强制执行：监控 Gateway service 的带宽使用情况
13 Jul 2021	新的身份和访问管理文章	添加了与 Citrix Cloud 一起使用的企业应用程序的 Azure AD 权限：Citrix Cloud 的 Azure Active Directory 权限
01 Jul 2021	服务级别协议更新	将 Citrix Wrike 添加到按服务可用性度量表：服务级别协议

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

日期	更改	描述
29 Jun 2021	系统日志功能新文章	添加了用于记录 Citrix Cloud 中某些事件的新技术预览文章：系统日志
24 Jun 2021	更新了 ITSM Adapter 文章	有关新增功能的摘要，请参阅新增功能
16 Jun 2021	Citrix Gateway service 的新许可文章	添加了一篇新文章，用于查看 Citrix Gateway service 的带宽使用情况：监控 Gateway service 的带宽使用情况
27 Apr 2021	Cloud Connector 新文章	添加了一篇新文章，用于收集 Cloud Connector 的 CDF 日志：日志收集
23 Apr 2021	更新了 ITSM Adapter 文章	有关新增功能的摘要，请参阅新增功能
16 Mar 2021	更新了 Remote Browser Isolation（以前称为 Secure Browser）文章	有关新增和更改功能的摘要，请参阅 Remote Browser Isolation
17 Feb 2021	SLA 正常运行时间更新	将 Citrix Application Delivery Management 的服务正常运行时间添加到服务级别协议：服务级别协议
08 Feb 2021	SLA 正常运行时间更新	将 Citrix Analytics 的服务正常运行时间添加到服务级别协议：服务级别协议
05 Feb 2021	服务区域更新	添加了 Secure Internet Access service 的服务位置：Secure Internet Access service 位置
03 Feb 2021	已删除 Citrix Cloud Labs 内容	已删除已弃用的 Citrix Cloud Labs 和 Session Manager 文章。Citrix Cloud Labs 和 Session Manager 服务已于

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

日期	更改	描述
		2020 年 9 月弃用并从 Citrix Cloud 中删除。
07 Dec 2020	Cloud Connector 调度增强	Cloud Connector 更新，可根据您偏好的时间和星期几进行：Cloud Connector 更新
30 Oct 2020	SLA 正常运行时间更新	更新了服务级别协议中的服务正常运行时间：服务级别协议
17 Sep 2020	已删除已弃用文章	Access Control Sync for StoreFront 实用程序的内容已弃用并从 Citrix Cloud 文档中删除。该实用程序不再可供下载，Citrix 也不再支持此实用程序。有关当前支持的功能，请参阅 Secure Private Access service 文档。
04 Sep 2020	Virtual Apps and Desktops service 的新许可文章	添加了对 Virtual Apps and Desktops service 并发许可的支持：监控 Citrix Virtual Apps and Desktops service（并发）的许可证和峰值使用情况
19 Jun 2020	多重身份验证注册更新	所有 Citrix Cloud 管理员都必须注册多重身份验证：多重身份验证要求
18 Jun 2020	Connector Appliance 已正式发布	Connector Appliance for Cloud Services 已正式发布，可在生产环境中使用。有关详细信息，请参阅 Connector Appliance for Cloud Services 。
18 May 2020	Citrix Cloud 管理员的多重身份验证注册	添加了新部分，用于注册 Citrix Cloud 管理员的多重身份验证、更改设备和更新恢复方法：设置多重身份验证

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

日期	更改	描述
27 Mar 2020	Cloud Connector 证书要求更新	添加了在 Cloud Connector 安装期间验证证书的端口要求：Cloud Connector 技术详细信息
26 Mar 2020	许可常见问题解答更新	在常见问题解答部分添加了关于在许可控制台中将多类型许可与 Virtual Apps and Desktops service 结合使用的影响的项：监控云服务的许可证和活动使用情况
26 Mar 2020	添加了新连接器	添加了新文章：Connector Appliance for Cloud Services。
28 Feb 2020	Managed Desktops service 的许可证和使用情况信息新文章	添加了新文章：监控 Citrix Managed Desktops service 的许可证和活动使用情况。
07 Feb 2020	本地许可证使用情况文章中添加了新部分	添加了“并发许可模型的峰值许可证使用情况”部分：监控本地部署的许可证和使用情况
11 Dec 2019	Workspace 的 Citrix Federated Authentication Service 新文章	添加了新文章：使用 Citrix Federated Authentication Service 为工作区启用单点登录。
03 Dec 2019	URL 过滤新策略	更新了文章以包含新功能 URL 过滤。有关详细信息，请参阅 Remote Browser Isolation。
03 Dec 2019	跟踪用户会话期间主机名的新功能	更新了文章以包含新功能 URL 过滤。有关详细信息，请参阅 Remote Browser Isolation。
15 Nov 2019	改进内部 Workspace 订阅者与 VDA 连接的新文章	添加了新文章：使用网络位置服务优化与工作区的连接

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

日期	更改	描述
06 Nov 2019	新型 Remote Browser Isolation（以前称为 Secure Browser）	添加了一种新的浏览器类型，支持共享密码身份验证。有关详细信息，请参阅 Remote Browser Isolation。
23 Oct 2019	Remote Browser Isolation（以前称为 Secure Browser）的新策略	添加了一项策略，允许管理员在用户启动应用程序时更改新会话的起始 URL。有关详细信息，请参阅 Remote Browser Isolation。
11 Sep 2019	Citrix Cloud 中客户数据和日志处理的新文章	添加了新文章：Citrix Cloud Services 客户内容和日志处理
09 Sep 2019	Virtual Apps and Desktops service 的许可证和使用情况内容更新	添加了用户/设备许可证模型支持；特定于服务的许可证和使用情况功能已移至专用文章：监控 Citrix Virtual Apps and Desktops service 的许可证和活动使用情况
06 Sep 2019	Citrix Cloud 中添加了新的身份提供商	将 Okta 添加到 Citrix Cloud 中支持的身份提供商：将 Okta 作为身份提供商连接到 Citrix Cloud
06 Sep 2019	Workspace 中添加了新的身份提供商	将 Okta 添加到 Workspace 支持的身份提供商：Okta
29 Aug 2019	本地产品的新许可证和使用情况文章	添加了一篇新文章，描述了“**许可证和使用情况**”的“**已许可部署**”选项卡中可用的见解：监控本地部署的许可证和使用情况
27 Aug 2019	更新了 Citrix Cloud Connector 技术详细信息文章	添加了 Cloud Connector 安装的数字证书验证要求：证书验证要求

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

日期	更改	描述
18 Jun 2019	更新了 Citrix Cloud 服务级别协议文章	添加了 CSP 资格和单位订阅最低要求：Citrix Cloud 服务级别协议
17 Jun 2019	Citrix Cloud 中添加了新的身份提供商	将 Citrix Gateway 添加到 Citrix Cloud 中支持的身份提供商：将本地 Citrix Gateway 作为身份提供商连接到 Citrix Cloud
17 Jun 2019	Workspace 中添加了新的身份提供商	将 Citrix Gateway 添加到 Workspace 支持的身份提供商：Citrix Gateway
05 Jun 2019	Remote Browser Isolation 新策略	添加了新策略，可自动将您发布的浏览器传输到不同区域。有关详细信息，请参阅 Remote Browser Isolation。
22 May 2019	新的高级概念文章	添加了新文章，讨论了如何通过本地 StoreFront 向 SaaS 和 Web 应用程序提供安全访问。请注意：本文已于 2020 年 9 月 17 日弃用。
17 May 2019	“管理 Citrix Cloud”部分中的新文章	添加了在 Citrix Cloud 中注册本地产品的新文章：管理本地产品注册
14 May 2019	从 Azure 订阅中删除过期服务的新部分	添加了“客户管理的 Azure 订阅”部分，描述了从客户的自管理 Azure 订阅中删除过期和被阻止服务的方法：延长 Citrix Cloud 服务订阅
09 May 2019	新的高级概念文章	添加了一篇新文章，讨论了使用 Citrix Virtual Apps and Desktops service 部署本地 StoreFront 的场景：Citrix Virtual Apps and Desktops

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

日期	更改	描述
		service 的本地 StoreFront 身份验证参考架构
07 May 2019	更新了服务订阅扩展	添加了月度服务订阅的到期条款：延长 Citrix Cloud 服务订阅
09 Apr 2019	更新	添加了在 Cloud Connector 代理和防火墙配置 中指定通配符域的理由
05 Apr 2019	更新	更新了 MDX Service 中的 MDX Service 版本
04 Apr 2019	更新	更新了 配置工作区访问 中对 Mac 和 iOS Workspace 应用程序的 AAD 支持
22 Mar 2019	发布	添加了 Citrix Cloud 中 Active Directory + 令牌身份验证的配置步骤：将 Active Directory 连接到 Citrix Cloud
22 Mar 2019	发布	添加了 Active Directory + 令牌身份验证的工作区要求：Active Directory 加令牌
22 Mar 2019	发布	添加了 Active Directory + 令牌身份验证的设备重置：Active Directory 加令牌
22 Mar 2019	发布	添加了注册 Active Directory + 令牌身份验证设备的步骤：双因素身份验证（可选）

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

index

- 远程浏览器隔离

远程浏览器隔离

Citrix Remote Browser Isolation™ 服务（前身为 Secure Browser 服务）隔离 Web 浏览，以保护公司网络免受基于浏览器的攻击。Remote Browser Isolation 服务提供对互联网托管 Web 应用程序的一致、安全的远程访问，无需用户设备配置。管理员可以快速部署远程隔离浏览器，从而实现即时价值。通过隔离互联网浏览，IT 管理员可以为最终用户提供安全的互联网访问，而不会损害企业安全性。

用户登录到其应用商店，并在配置的 Web 浏览器中打开 Web 应用程序。网站不会直接将任何浏览数据传输到用户设备或从用户设备传输，因此体验是安全的。

Remote Browser Isolation 服务可以发布远程隔离浏览器，以用于：

- **共享密码外部 Web 应用程序：** 如果您发布了使用共享密码身份验证的浏览器，用户必须输入密码才能启动应用程序。
- **经过身份验证的外部 Web 应用程序：** 当您发布经过身份验证的外部 Web 应用程序并从其应用商店启动这些应用程序时，Remote Browser Isolation 服务需要一个资源位置，其中包含至少一个 Cloud Connector（建议使用两个或更多）。您必须为经过身份验证的应用程序添加用户。有关详细信息，请参阅 Citrix Cloud Connector。
- **未经身份验证的外部 Web 应用程序：** 当您发布未经身份验证的外部 Web 应用程序并从其应用商店启动这些应用程序时，Remote Browser Isolation 服务需要一个资源位置，其中包含至少一个 Cloud Connector（建议使用两个或更多）。有关详细信息，请参阅 Citrix Cloud Connector。

  尽管通常不建议这样做，但未经身份验证的外部 Web 应用程序可用于简单的概念验证。

有关详细信息，请参阅 发布远程隔离浏览器。

该服务还提供：

- 将已发布的应用程序与 Citrix® StoreFront Cloud 集成
- 将已发布的应用程序与本地 StoreFront 集成
- 用于安全性的简单 URL 允许列表功能

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

- 使用情况监控
- 剪贴板使用、打印、自助服务终端模式、区域故障转移和客户端驱动器映射的控件

与 Citrix Secure Private Access™ 结合的远程浏览器隔离服务

您可以使用 Citrix Secure Private Access 控制台启动远程浏览器隔离服务的已发布浏览器，以访问企业 Web、TCP 和 SaaS 应用程序。您还可以通过 Citrix Secure Private Access 将未经批准的网站重定向到远程浏览器隔离服务的已发布浏览器中打开。

有关通过 Citrix Secure Private Access 访问隔离的远程浏览器的更多信息，请参阅 Citrix Secure Private Access 文档中的配置具有多个规则的访问策略和未经批准的网站。

参考文章

- Secure Private Access 服务解决方案概述
- 思杰云
- 远程浏览器隔离（安全浏览器）的自助服务搜索
- Citrix 企业浏览器(/zh-cn/citrix-enterprise-browser)
- 安全和合规性信息
- 开发人员文档

相关产品中的新增功能

- 安全私有访问(/zh-cn/citrix-secure-private-access/service/whats-new)
- Citrix 企业浏览器(/zh-cn/citrix-enterprise-browser/whats-new)
- Citrix 安全分析(/zh-cn/security-analytics/whats-new)

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