联合身份验证服务

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

Contents

联合身份验证服务 2402 LTSR 10

早期版本 10

参考资料 11

联邦身份验证服务 2402 LTSR 12

已修复的问题 12

已知问题 12

第三方通知 12

系统要求 13

安装和配置 15

安装和设置顺序 15

安装联合身份验证服务 15

升级 FAS 16

在 StoreFront 存储上启用 FAS 插件 16

配置交付控制器™ 17

配置组策略 17

会话中行为 20

提示范围 21

同意超时 22

锁定断开连接 22

使用联合身份验证服务管理控制台 22

部署证书模板 23

设置 Active Directory 证书服务 25

授权联合身份验证服务 26

配置规则 27

连接到 Citrix Cloud 32

断开与 Citrix Cloud 的连接 37

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

高级配置 38
相关信息 38
为租户客户启用联合身份验证服务 38
先决条件 38
配置 MSP 客户 38
已知问题 41
Azure Active Directory 单点登录 41
已加入域的 VDA 42
混合加入的 VDA 43
证书颁发机构配置 44
设置多个 CA 服务器以在 FAS 中使用 44
预期行为更改 45
配置 Microsoft 证书颁发机构以进行 TCP 访问 45
预生成用户证书 46
获取 Active Directory 用户列表 46
FAS 服务器 48
续订注册机构证书 49
相关信息 49
私钥保护 49
简介 49
私钥配置设置 50
配置方案示例 53
示例 1 53
示例 2 53
示例 3 63
FAS 证书存储 65
相关信息 67
安全和网络配置 67

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

网络体系结构 67
防火墙和网络安全 68
思杰联合身份验证服务与思杰云™ 之间的连接 69
安全注意事项 70
委派的注册代理 70
访问控制列表配置 70
防火墙设置 71
事件日志监控 71
硬件安全模块 71
管理职责 71
组策略设置 72
证书模板 72
重命名证书模板 72
修改常规属性 73
修改请求处理属性 73
修改加密属性 73
修改密钥证明属性 73
修改已取代模板属性 73
修改扩展属性 73
修改安全属性 73
修改主题名称属性 74
修改服务器属性 74
修改颁发要求属性 74
修改兼容性属性 75
证书颁发机构管理 75
发布模板 75
防火墙设置 75
受限注册 76

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

策略模块和审计 76
FAS 管理 76
通过 ACL 限制 StoreFront、用户和 VDA 76
配置规则 77
配置证书颁发机构和模板 77
会话内和身份验证证书 77
私钥保护和密钥长度 77
事件日志 77
管理访问和管理工具 78
Citrix 虚拟应用、Citrix 虚拟桌面和 VDA 管理员 78
常规 Windows 服务器安全性 78
相关信息 78
性能计数器 78
故障排除 Windows 登录问题 80
证书和公钥基础结构 80
UPN 名称和证书映射 81
Active Directory 中的 UPN 名称 81
证书映射服务 81
控制登录域控制器选择 82
控制域控制器选择 82
识别正在使用的域控制器 82
启用帐户审核事件 82
证书验证日志 82
检查证书有效性 82
启用 CAPI 日志记录 82
CAPI 日志 83
错误消息 83
Kerberos 日志 84

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

域控制器和工作站日志 84
域控制器 CAPI2 日志 84
域控制器安全日志 85
VDA 安全日志 86
VDA CAPI 日志 87
VDA 系统日志 88
使用 Windows 事件日志监视 FAS 88
FAS 服务是否正在运行? 89
FAS 运行状况事件 89
云连接的 FAS 事件 90
安全事件 91
FAS 事件日志 91
管理事件 91
创建身份断言 94
作为信赖方 94
会话内证书服务器 95
FAS 断言插件 95
启用 Workspace 的 FAS 96
登录 97
会话内证书 98
证书请求和密钥对生成 98
最终用户错误消息 99
FAS 始终开启的跟踪 99
收集始终开启的跟踪 100
禁用始终开启的跟踪 100
将始终开启的跟踪发送到中央日志服务器 100
相关信息 100
PowerShell 命令小程序 100

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

部署架构 102
简介 102
架构概述 102
内部部署 103
思杰网关部署 105
ADFS SAML 部署 106
B2B 帐户映射 106
Windows 10 Azure 活动目录 加入 107
ADFS 部署 109
简介 109
SAML 概述 110
重定向 URL 111
标识符 111
返回地址 111
签名证书 111
单一注销 URL 111
配置 112
填写 SAML 策略 112
相关信息 112
Azure AD 集成 112
简介 112
体系结构 114
创建 DNS 区域 115
创建云服务 117
创建 Windows 虚拟机 117
域控制器 118
ADFS 控制器和 Web 应用程序代理服务器 118
Citrix Virtual Desktops™ 投递控制器和 VDA 119

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

配置内部 DNS 119
配置外部 DNS 地址 120
配置安全组 120
创建 ADFS 证书 121
设置 Azure AD 122
创建新目录 122
创建全局管理员用户 (AzureAdmin) 124
向 Azure AD 注册您的域 125
安装 Azure AD 连接 126
启用 Azure AD 加入 135
安装 思杰虚拟应用 或 思杰虚拟桌面 138
安装联合身份验证服务 139
配置 StoreFront 139
配置 StoreFront 以使用 Citrix Gateway 140
配置新的 Azure AD 应用程序以实现 StoreFront 的单点登录 141
配置图标 141
配置 SAML 身份验证 142
将应用程序分配给用户 144
我的应用页面 145
单一登录 URL 145
安装和配置 Citrix Gateway 146
运行 Citrix Virtual Apps and Desktops 安装向导 146
配置用于 AD 帐户管理的域控制器 147
配置 StoreFront 地址 148
验证 Citrix Gateway 部署 149
启用 Citrix Gateway SAML 身份验证支持 150
验证端到端系统 151
附录 152

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

提供公共 IP 地址和 DNS 地址 152

设置防火墙规则（安全组） 153

相关信息 154

联合身份验证服务 2402 LTSR 文档历史记录 155

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

联合身份验证服务 2402 LTSR

联合身份验证服务 (FAS) 是一个特权组件，旨在与 Active Directory 证书服务集成。它动态地为用户颁发证书，允许他们像使用智能卡一样登录 Active Directory 环境。这使得 StoreFront™ 能够使用更广泛的身份验证选项，例如 SAML（安全断言标记语言）断言。SAML 通常用作 Internet 上传统 Windows 用户帐户的替代方案。

联合身份验证服务 2402 LTSR 是 FAS 的最新当前版本。本文反映了此最新版本中的功能和配置。

早期版本

有关早期 FAS 版本的文档，请参阅：

- 联合身份验证服务 2311
- 联合身份验证服务 2308
- 联合身份验证服务 2305
- 联合身份验证服务 2303
- 联合身份验证服务 2212
- 联合身份验证服务 2209
- 联合身份验证服务 2206
- 联合身份验证服务 2203 LTSR
- 联合身份验证服务 2112
- 联合身份验证服务 2109
- 联合身份验证服务 2106
- 联合身份验证服务 2103
- 联合身份验证服务 1912 LTSR
- XenApp 和 XenDesktop 7.15 长期服务版本

当前版本 (CR) 和长期服务版本 (LTSR) 的产品生命周期策略在 生命周期里程碑 中进行了描述。

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

参考资料

- Active Directory 证书服务概述
- 配置 Windows 以进行证书登录

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

联邦身份验证服务 2402 LTSR

此版本的联合身份验证服务 (FAS) 包含以下新功能：

- **联合身份验证服务证书请求增强以包含 SID。** FAS 发出的证书请求已增强以包含 SID 参数。对于在 `Citrix_SmartcardLogon` 模板中启用“**使用者名称**”属性的“**在请求中提供**”选项的用户，此新增功能允许 FAS 与 KB5014754 中详细说明的证书身份验证更改配合使用。对于使用默认设置“**从此 Active Directory 信息构建**”的用户，这些身份验证更改已受支持。

有关错误修复的信息，请参阅已修复的问题。

已修复的问题

Federated Authentication Service 2402 LTSR 中没有已修复的问题。

已知问题

联合身份验证服务 2402 LTSR 中没有已知问题。

以下警告适用于任何建议更改注册表项的变通方法：

警告：

不正确地编辑注册表可能导致严重问题，甚至可能需要重新安装操作系统。Citrix 无法保证能够解决因不正确使用注册表编辑器而导致的问题。请自行承担使用注册表编辑器的风险。编辑注册表之前，请务必备份注册表。

第三方通知

此版本的联合身份验证服务可能包含第三方软件，这些软件根据以下文档中定义的条款获得许可：

- Citrix Virtual Apps and Desktops 第三方通知 (PDF 下载)
- FlexNet Publisher 2017 (11.15.0.0) 的非商业软件披露 (PDF 下载)
- FlexNet Publisher 11.15.0 中使用的 FlexNet Publisher 文档补充第三方和开源软件 (PDF 下载)

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

系统要求

- 联合身份验证服务 (FAS) 支持以下 Windows Server 版本：
  - Windows Server 2022 标准版和数据中心版
  - Windows Server 2019 标准版和数据中心版，并支持 Server Core 选项
  - Windows Server 2016 标准版和数据中心版，并支持 Server Core 选项
- Citrix 建议将 FAS 安装在未安装任何其他 Citrix 组件的服务器上。
- Windows Server 必须是安全的，因为它有权访问注册机构证书和私钥。证书和私钥允许服务器为域用户颁发证书。服务器还有权访问已颁发的域用户证书和私钥。
- FAS PowerShell cmdlet 需要在 FAS 服务器上安装 64 位 Windows PowerShell。
- 需要 Microsoft 企业证书颁发机构或其他经过验证的证书颁发机构 (CA) 来颁发用户证书。以下非 Microsoft PKI 提供商已验证其解决方案可与 FAS 结合使用。有关这些验证的支持，请联系供应商：
  - 凯因子命令
  - 赛迪高证书管理器
  - 维纳菲零接触 PKI
  - HDI PKIaaS (维纳菲)
  - 恩特斯 WNES
  - AppViewX
  - 永信地平线客户生命周期管理
  - 开放信任公钥基础设施
  - 艾迪诺米克公钥基础设施-3
  - 迪吉证书自动注册服务器
- 如需将 FAS 与非 Microsoft CA 结合使用的支持和指导，您可以联系相关的 PKI 提供商。
- 对于非 Microsoft 证书颁发机构，请确保以下事项：
  - 证书颁发机构 (CA) 已在 Active Directory 中注册为注册服务。

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

  - CA 证书位于域控制器上的 NTAuth 存储中。有关详细信息，请参阅如何将第三方证书颁发机构 (CA) 证书导入企业 NTAuth 存储。

- 有关详细信息，请参阅部署指南：Citrix 联合身份验证服务和 Sectigo MS 代理。

在 Citrix 虚拟应用 或 Citrix 虚拟桌面™ 站点中：

- Delivery Controller、Virtual Delivery Agent (VDA) 和 StoreFront™ 服务器都必须是受支持的版本。
- 在创建计算机目录之前，将联合身份验证服务组策略配置应用于 VDA。有关详细信息，请参阅配置组策略部分。

在规划此服务的部署时，请查看安全注意事项部分。

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

安装和配置

安装和设置顺序

1. 安装联合身份验证服务 (FAS)
2. 在 StoreFront 存储上启用 FAS 插件
3. 配置交付控制器
4. 配置组策略
5. 使用 FAS 管理控制台执行以下操作：
    a. 部署证书模板
    b. 设置证书颁发机构
    c. 授权 FAS 使用您的证书颁发机构
    d. 配置规则
    e. 将 FAS 连接到 Citrix Cloud（可选）

安装联合身份验证服务

出于安全考虑，Citrix 建议在专用服务器上安装联合身份验证服务 (FAS)。此服务器必须以类似于域控制器或证书颁发机构的方式进行保护。FAS 可以通过以下方式安装：

- Citrix Virtual Apps and Desktops™ 安装程序（插入 ISO 后，从自动运行启动屏幕上的“**联合身份验证服务**”按钮），或者
- 独立的FAS安装程序文件（可在Citrix 下载上作为MSI文件获取）。

这些将安装以下组件：

- 联合身份验证服务
- 用于高级FAS配置的PowerShell 管理单元 cmdlet
- FAS 管理控制台
- FAS 组策略模板 (CitrixFederatedAuthenticationService.admx/adml)
- 证书模板文件

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

- 性能计数器和事件日志

升级 FAS

您可以使用就地升级将 FAS 升级到新版本。升级前，请考虑以下事项：

- 执行就地升级时，所有 FAS 服务器设置都将保留。
- 在升级 FAS 之前，请务必关闭 FAS 管理控制台。
- 确保始终至少有一个 FAS 服务器可用。如果启用了联合身份验证服务的 StoreFront™ 服务器无法访问任何服务器，则用户将无法登录或启动应用程序。

要开始升级，请从 Citrix Virtual Apps and Desktops 安装程序或独立的 FAS 安装程序文件安装 FAS。

在 StoreFront 存储上启用 FAS 插件

注意：

如果您仅将 FAS 与 Citrix Cloud 结合使用，则无需执行此步骤。

要在 StoreFront 商店上启用 FAS 集成，请以管理员帐户运行以下 PowerShell cmdlet。如果商店名称不同，请修改 `$StoreVirtualPath`。

```
Get-Module "Citrix.StoreFront.*" -ListAvailable | Import-Module

$StoreVirtualPath = "/Citrix/Store"

$store = Get-STFStoreService -VirtualPath $StoreVirtualPath

$auth = Get-STFAuthenticationService -StoreService $store

Set-STFClaimsFactoryNames -AuthenticationService $auth -ClaimsFactoryName
"FASClaimsFactory"

Set-STFStoreLaunchOptions -StoreService $store -VdaLogonDataProvider
"FASLogonDataProvider"
```

要停止使用 FAS，请使用以下 PowerShell 脚本：

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

```
Get-Module "Citrix.StoreFront.*" -ListAvailable | Import-Module

$StoreVirtualPath = "/Citrix/Store"

$store = Get-STFStoreService -VirtualPath $StoreVirtualPath

$auth = Get-STFAuthenticationService -StoreService $store

Set-STFClaimsFactoryNames -AuthenticationService $auth -ClaimsFactoryName
"standardClaimsFactory"

Set-STFStoreLaunchOptions -StoreService $store -VdaLogonDataProvider ""
```

配置交付控制器™

注意：

如果您仅将 FAS 与 Citrix Cloud 结合使用，则无需执行此步骤。

要使用 FAS，请将 Citrix Virtual Apps 或 Citrix Virtual Desktops™ Delivery Controller 配置为信任连接到它的 StoreFront 服务器：运行 **Set-BrokerSite -TrustRequestsSentToTheXmlServicePort $true** PowerShell cmdlet。无论站点上有多少个 Delivery Controller，每个站点只需运行一次此命令。

配置组策略

安装 FAS 后，使用安装中提供的组策略模板来指定组策略中服务器的完全限定域名 (FQDN)。

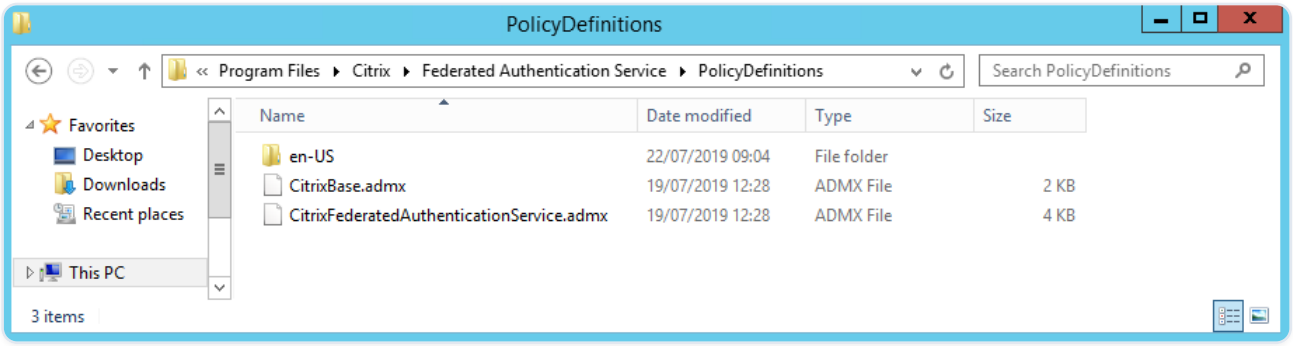
重要：

确保请求票证的 StoreFront 服务器和兑换票证的虚拟投递代理 (VDA) 具有相同的 FQDN 配置，包括组策略对象应用的自动服务器编号。

为简单起见，以下示例在域级别配置了一个适用于所有计算机的策略。但是，这不是必需的。只要 StoreFront 服务器、VDA 和运行 FAS 管理控制台的计算机看到相同的 FQDN 列表，FAS 即可正常运行。请参阅步骤 6。

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

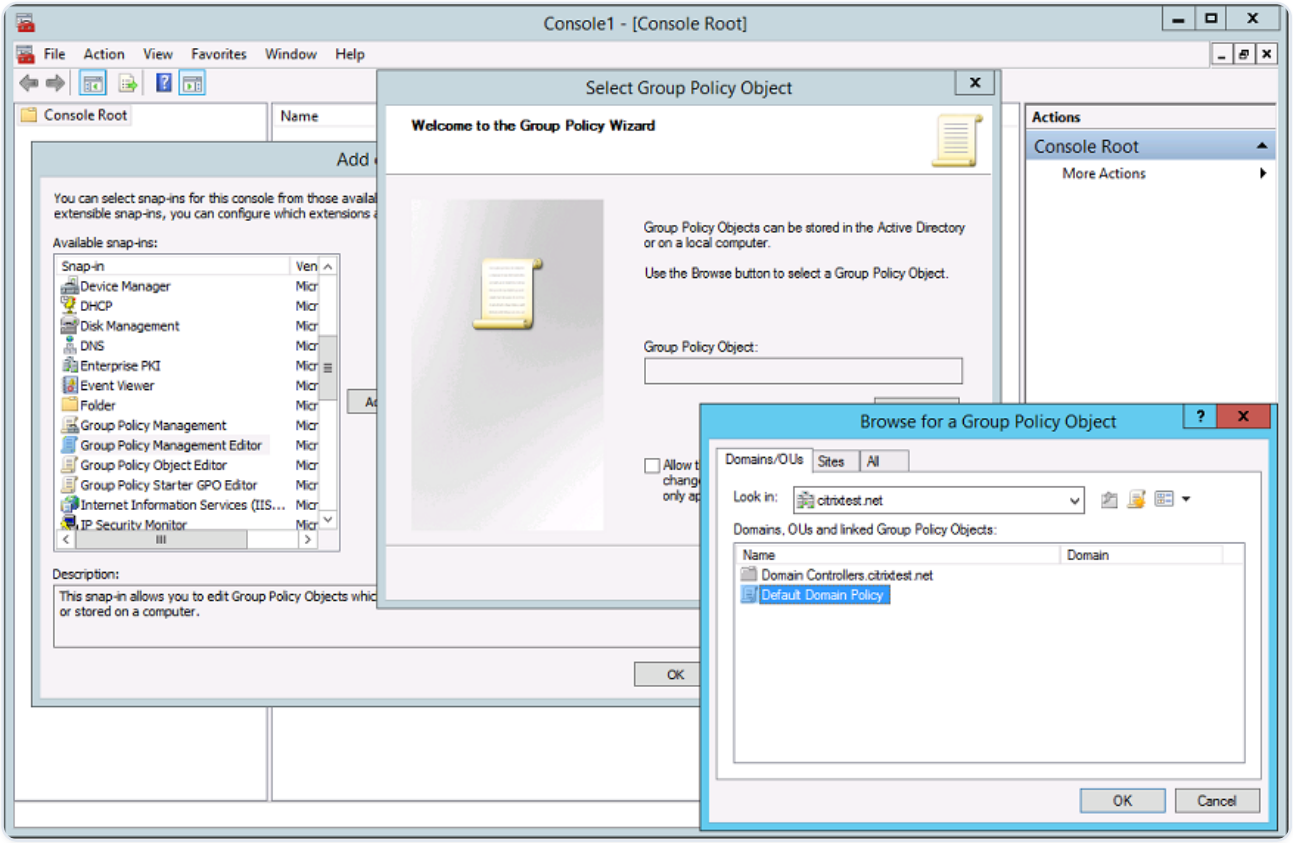
步骤 1. 在安装 FAS 的服务器上，找到 C:\Program Files\Citrix\Federated Authentication Service\PolicyDefinitions\CitrixFederatedAuthenticationService.admx 和 CitrixBase.admx 文件以及 en-US 文件夹。



步骤 2. 将这些文件复制到域控制器，并将其放置在 C:\Windows\PolicyDefinitions 和 en-US 子文件夹中。

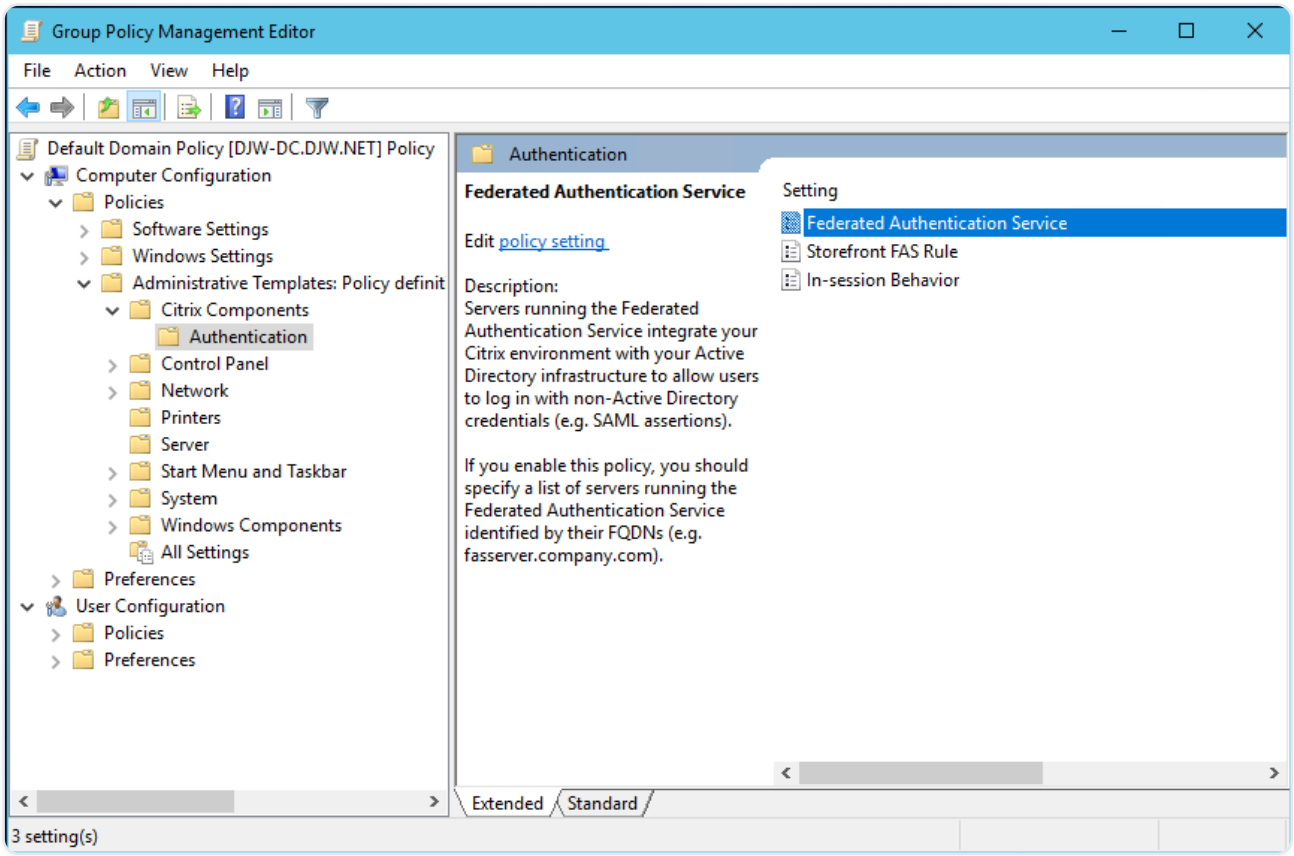
步骤 3. 运行 Microsoft 管理控制台（从命令行运行 mmc.exe）。从菜单栏中，选择**文件 > 添加/删除管理单元**。添加**组策略管理编辑器**。

当系统提示您选择组策略对象时，选择**浏览**，然后选择**默认域策略**。或者，您可以使用所选工具为您的环境创建并选择一个适当的策略对象。该策略必须应用于运行受影响的 Citrix 软件（VDA、StoreFront 服务器、管理工具）的所有计算机。



步骤 4. 导航到“计算机配置/策略/管理模板/Citrix 组件/身份验证”中的 *联合身份验证服务* 策略。

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

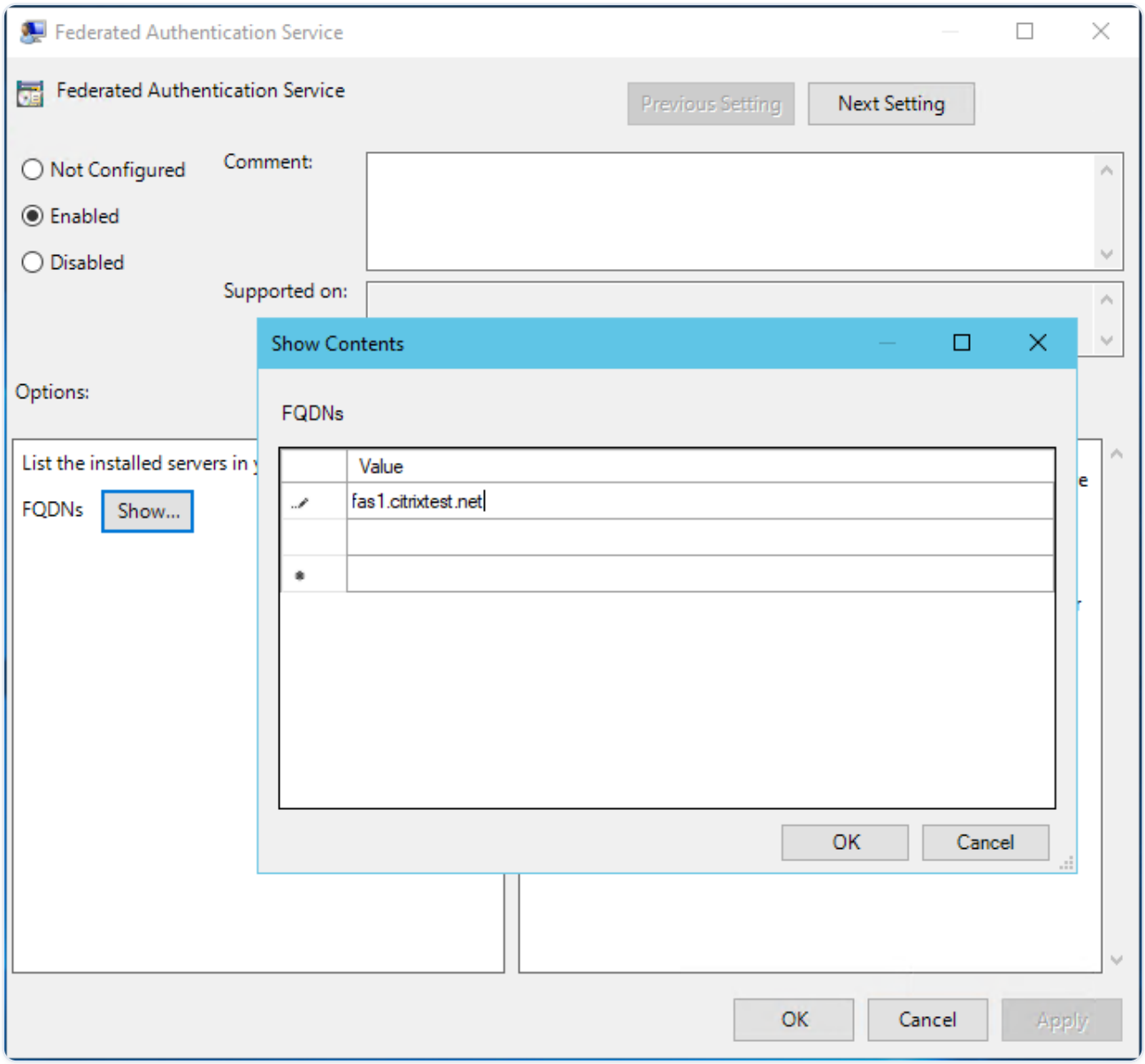


注意：

仅当您将 CitrixBase.admx/CitrixBase.adml 模板文件添加到 PolicyDefinitions 文件夹时，Federated Authentication Service 策略设置才在域 GPO 上可用。完成步骤 3 后，Federated Authentication Service 策略设置将列在**管理模板 > Citrix 组件 > 身份验证**文件夹中。

步骤 5. 打开 Federated Authentication Service 策略并选择**已启用**。这允许您选择**显示**按钮，在此处配置 FAS 服务器的 FQDN。

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



步骤 6. 输入 FAS 服务器的 FQDN。

重要：

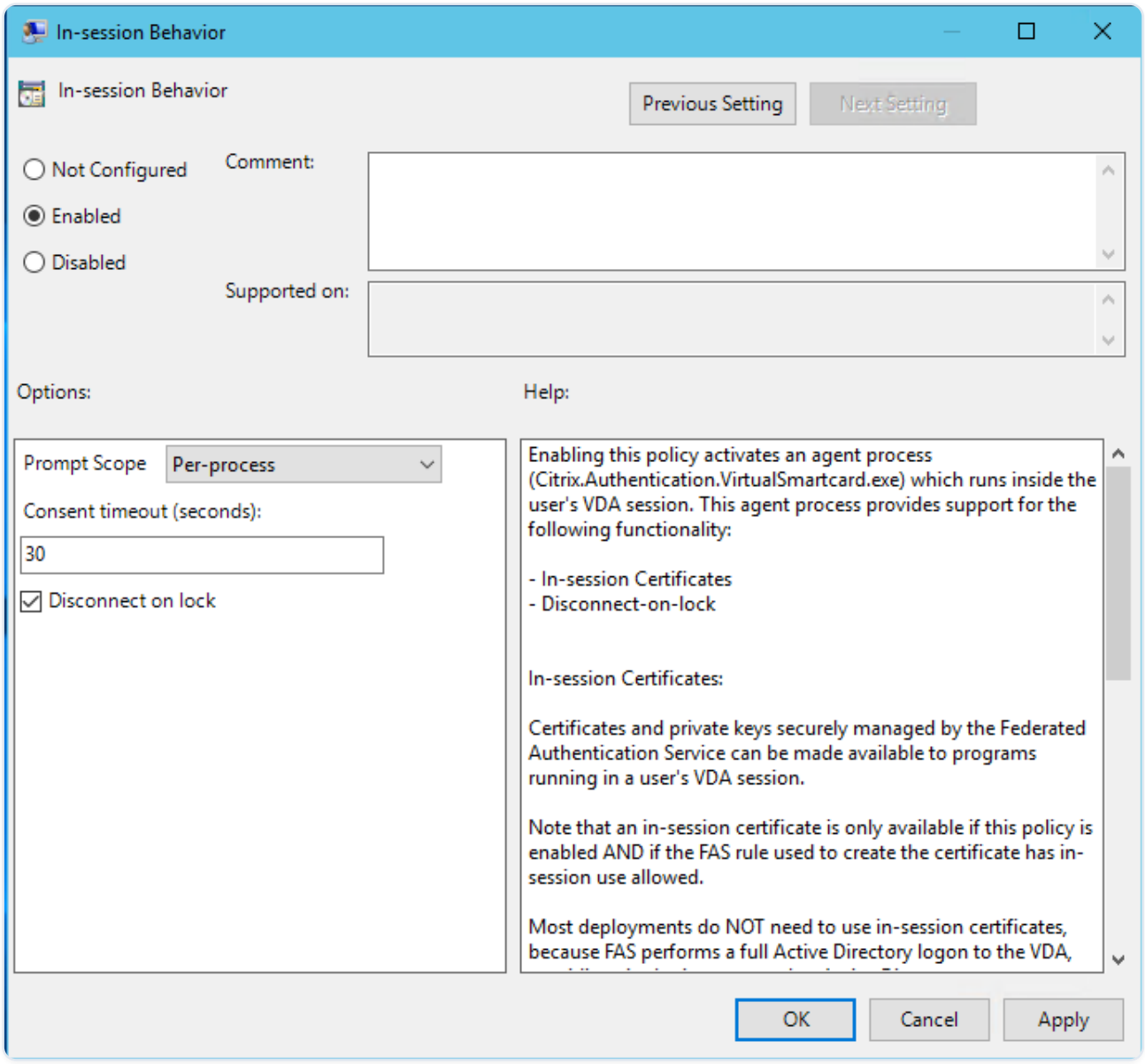
如果输入多个 FQDN，则列表的顺序必须与 VDA、StoreFront 服务器（如果存在）和 FAS 服务器所看到的顺序一致。请参阅组策略设置。

步骤 7. 单击**确定**退出组策略向导并应用组策略更改。您可能需要重新启动计算机（或从命令行运行 **gpupdate /force**）才能使更改生效。

会话中行为

此策略会在用户的 VDA 会话中激活一个代理进程，该进程支持会话内证书、同意和锁定断开连接。会话内证书仅在此策略启用 *并且* 用于创建证书的 FAS 规则允许会话内使用时可用，请参阅配置规则。

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



启用可启用此策略并允许 FAS 代理进程在用户的 VDA 会话中运行。

禁用可禁用此策略并停止 FAS 代理进程运行。

提示范围

如果此策略已启用，**提示范围**将控制如何提示用户同意允许应用程序使用会话内证书。有三个选项：

- **无需同意**—此选项禁用安全提示，私钥将静默使用。
- **按进程同意**—每个正在运行的程序都会单独提示同意。
- **按会话同意**—用户单击**确定**后，此选项将应用于会话中的所有程序。

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

同意超时

如果此策略已启用，**同意超时**将控制同意持续的时间（以秒为单位）。例如，如果设置为 300 秒，用户每五分钟会看到一次提示。值为零时，每次私钥操作都会提示用户。

锁定断开连接

如果此策略已启用，当用户锁定屏幕时，其会话将自动断开连接。此行为类似于“移除智能卡时断开连接”策略。当用户没有 Active Directory 登录凭据时，请使用此功能。

注意：

锁定断开连接策略适用于 VDA 上的所有会话。

使用联合身份验证服务管理控制台

注意：

尽管 FAS 管理控制台适用于大多数部署，但 PowerShell 界面提供了更高级的选项。有关 FAS PowerShell cmdlet 的信息，请参阅PowerShell cmdlet。

FAS 管理控制台作为 FAS 的一部分安装。一个图标（Citrix Federated Authentication Service）放置在“开始”菜单中。

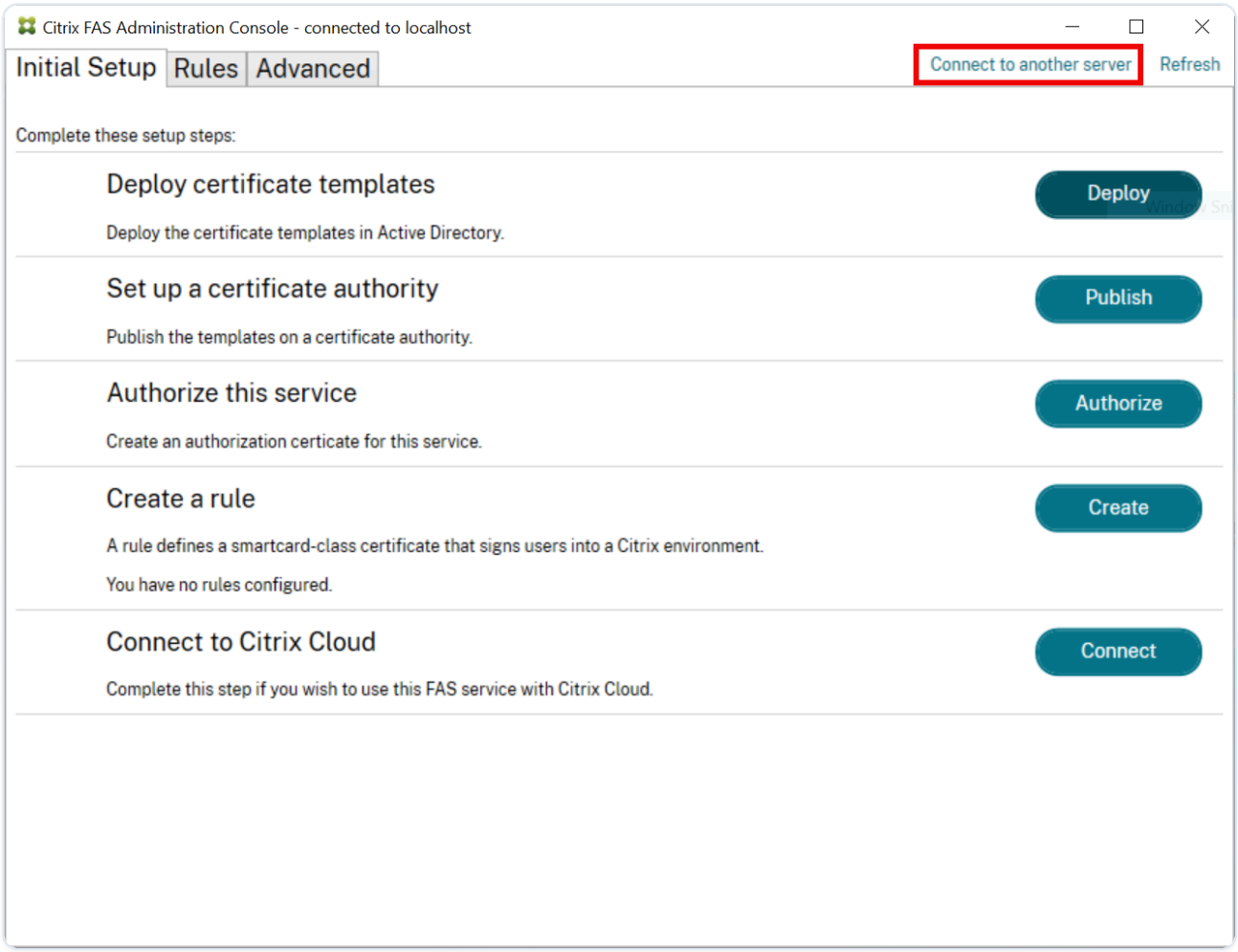
首次使用管理控制台时，它会引导您完成以下过程，以：

- 部署证书模板。
- 设置证书颁发机构。
- 授权 FAS 使用证书颁发机构。

您也可以使用操作系统配置工具手动完成其中一些步骤。

FAS 管理控制台默认连接到本地 FAS 服务。如果需要，您可以使用控制台右上角的“**连接到其他服务器**”连接到远程服务。

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



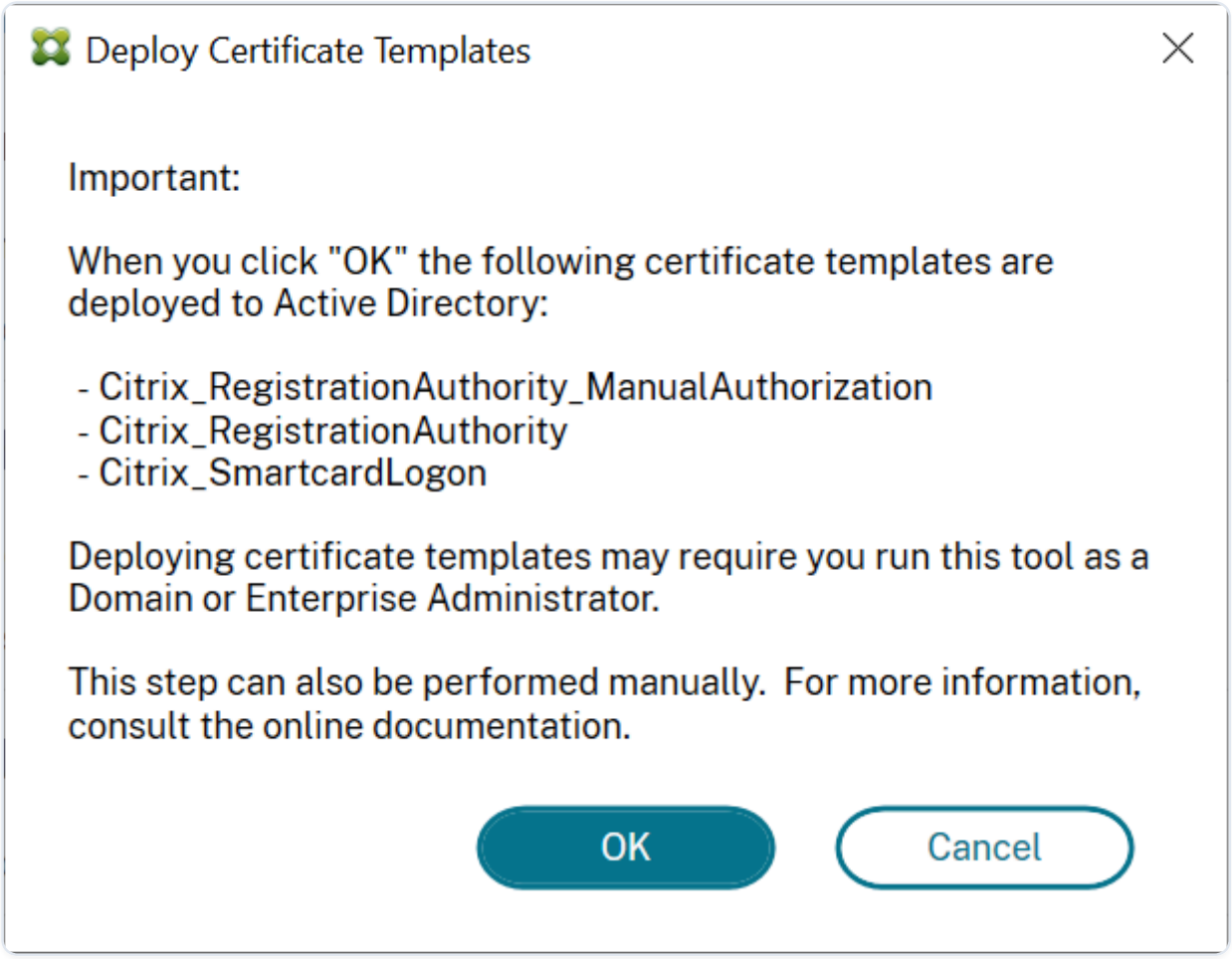
部署证书模板

为避免与其他软件出现互操作性问题，FAS 提供了三个 Citrix 证书模板供其自身使用。

- Citrix_RegistrationAuthority_ManualAuthorization
- Citrix_RegistrationAuthority
- Citrix_SmartcardLogon

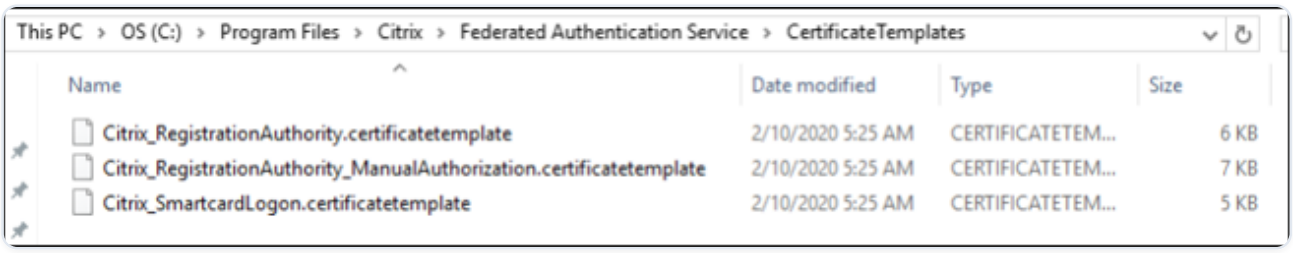
这些模板必须在 Active Directory 中注册。单击“**部署**”按钮，然后单击“**确定**”。

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



模板的配置可在随 FAS 安装的扩展名为 .certificatetemplate 的 XML 文件中找到，路径为：

C:\Program Files\Citrix\联合身份验证服务\证书模板



如果您没有安装这些模板文件的权限，请将其提供给您的 Active Directory 管理员。

要手动安装模板，您可以从包含模板的文件夹中运行以下 PowerShell 命令：

```
$template =
[System.IO.File]::ReadAllBytes("$Pwd\Citrix_SmartcardLogon.certificatetemp
late")

$CertEnrol = New-Object -ComObject
X509Enrollment.CX509EnrollmentPolicyWebService

$CertEnrol.InitializeImport($template)
```

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

```
$comtemplate = $CertEnrol.GetTemplates().ItemByIndex(0)

$writabletemplate = New-Object -ComObject
X509Enrollment.CX509CertificateTemplateADWritable

$writabletemplate.Initialize($comtemplate)

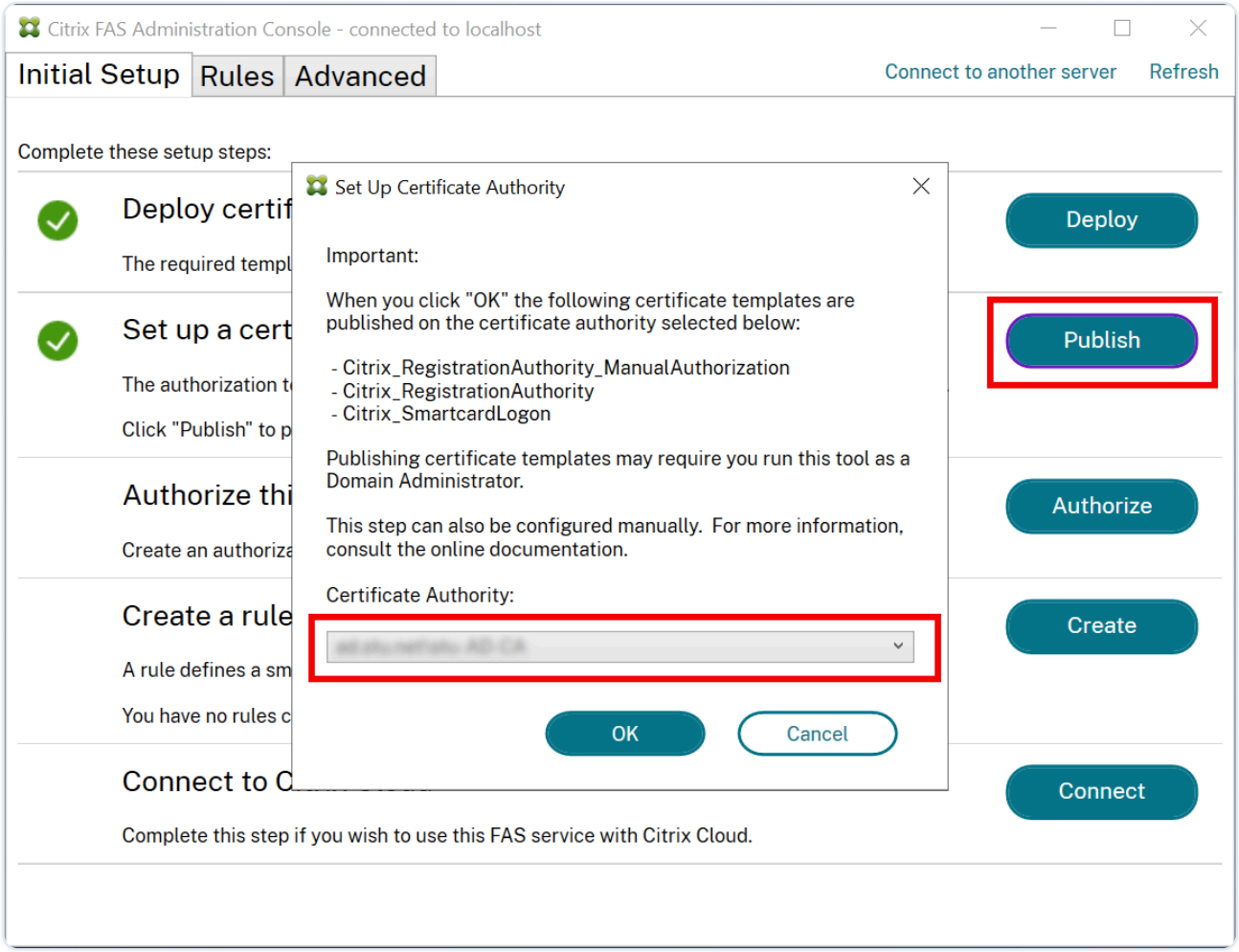
$writabletemplate.Commit(1, $NULL)
```

设置 Active Directory 证书服务

安装 Citrix 证书模板后，必须将其发布到一个或多个 Microsoft 企业证书颁发机构服务器上。有关如何部署 Active Directory 证书服务的信息，请参阅 Microsoft 文档。

具有管理证书颁发机构权限的用户必须在至少一台服务器上发布模板。使用“**设置证书颁发机构**”来发布它们。

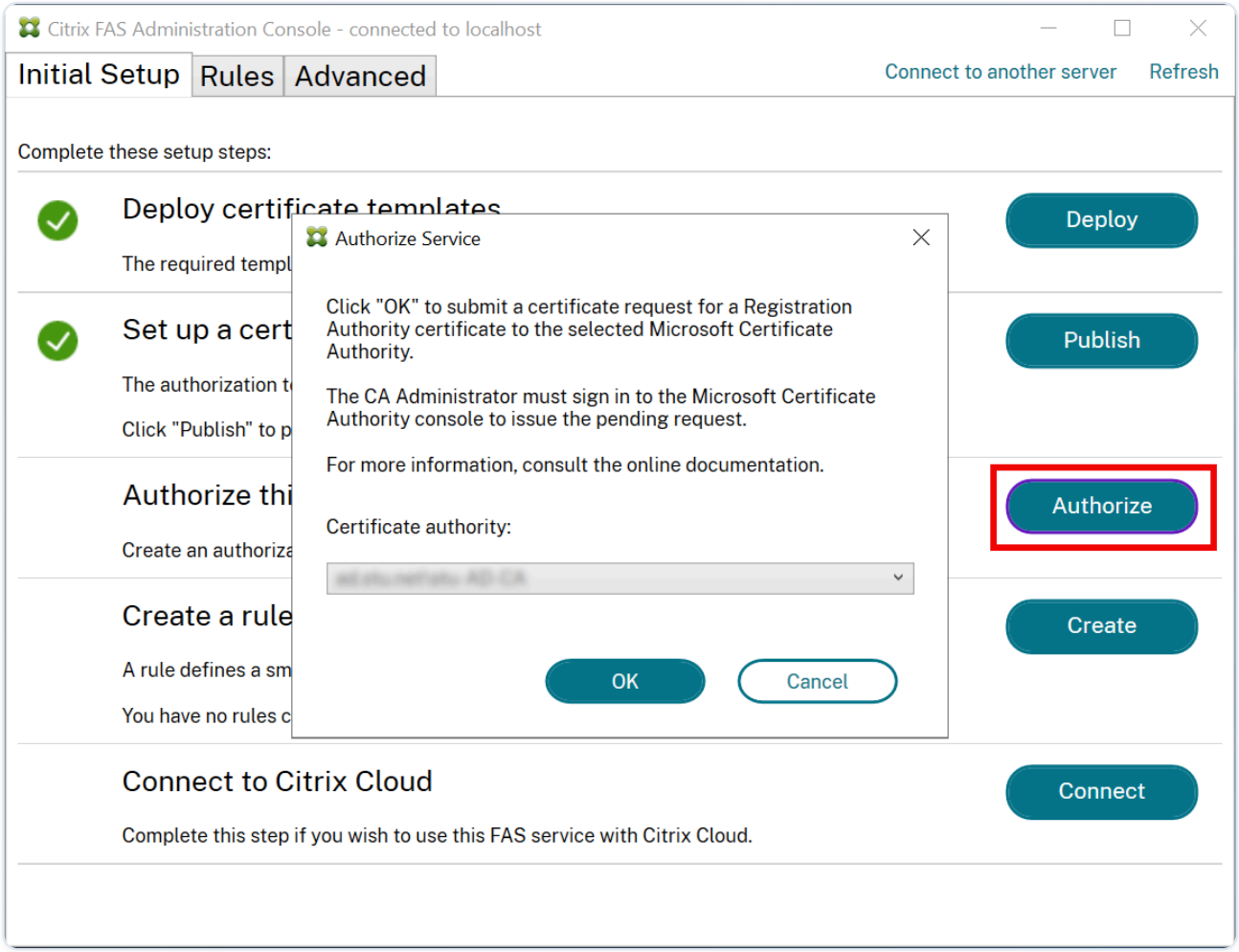
（也可以使用 Microsoft 证书颁发机构控制台发布证书模板。）



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

授权联合身份验证服务

此步骤启动 FAS 的授权。管理控制台使用 Citrix_RegistrationAuthority_ManualAuthorization 模板生成证书请求，然后将其发送到发布该模板的某个证书颁发机构。

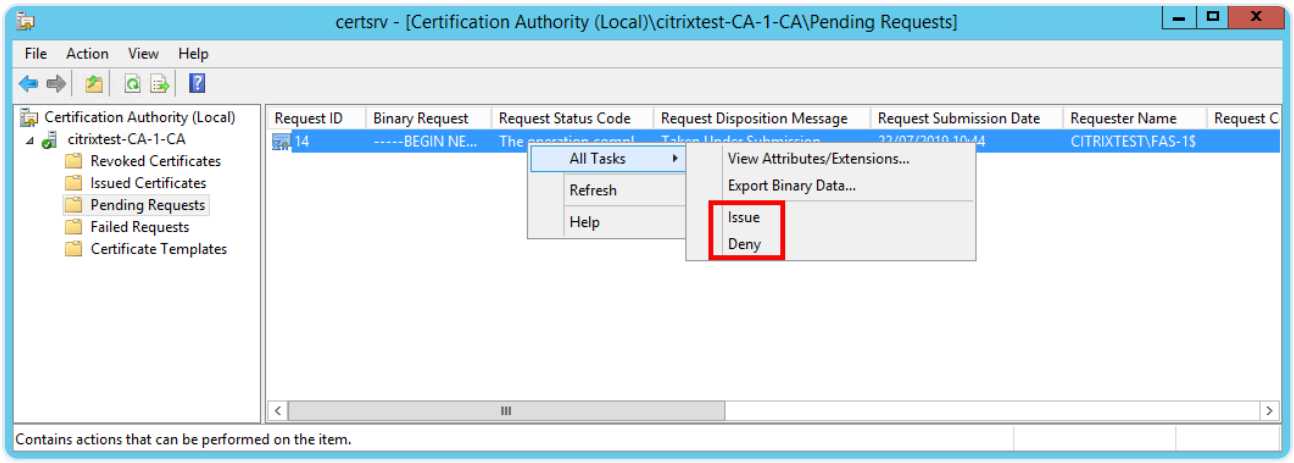


请求发送后，它会显示在 Microsoft 证书颁发机构控制台的“**待处理请求**”列表中，作为来自 FAS 计算机帐户的待处理请求。证书颁发机构管理员必须在 FAS 配置继续之前颁发或拒绝该请求。

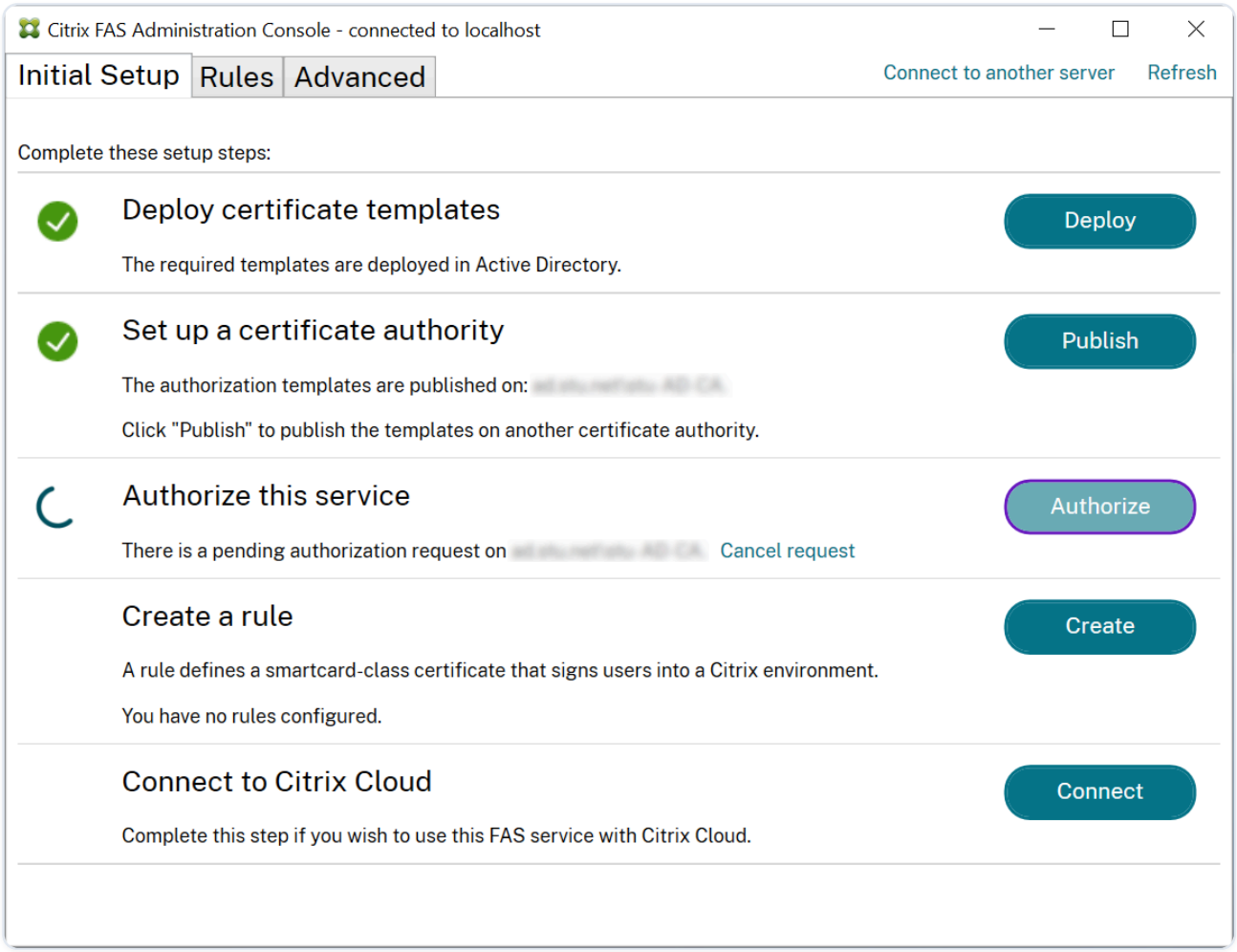
FAS 管理控制台会显示一个忙碌的“加载指示器”，直到管理员选择“**颁发**”或“**拒绝**”。

在 Microsoft 证书颁发机构控制台中，右键单击“**所有任务**”，然后为证书请求选择“**颁发**”或“**拒绝**”。如果选择“**颁发**”，FAS 管理控制台将显示授权证书。如果选择“**拒绝**”，控制台将显示错误消息。

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



FAS 管理控制台会自动检测此过程何时完成。这可能需要几分钟。



配置规则

FAS 使用规则来授权颁发用于 VDA 登录和会话内使用的证书，具体由 StoreFront 指示。

每条规则指定以下内容：

- 信任的 StoreFront 服务器，用于请求证书。

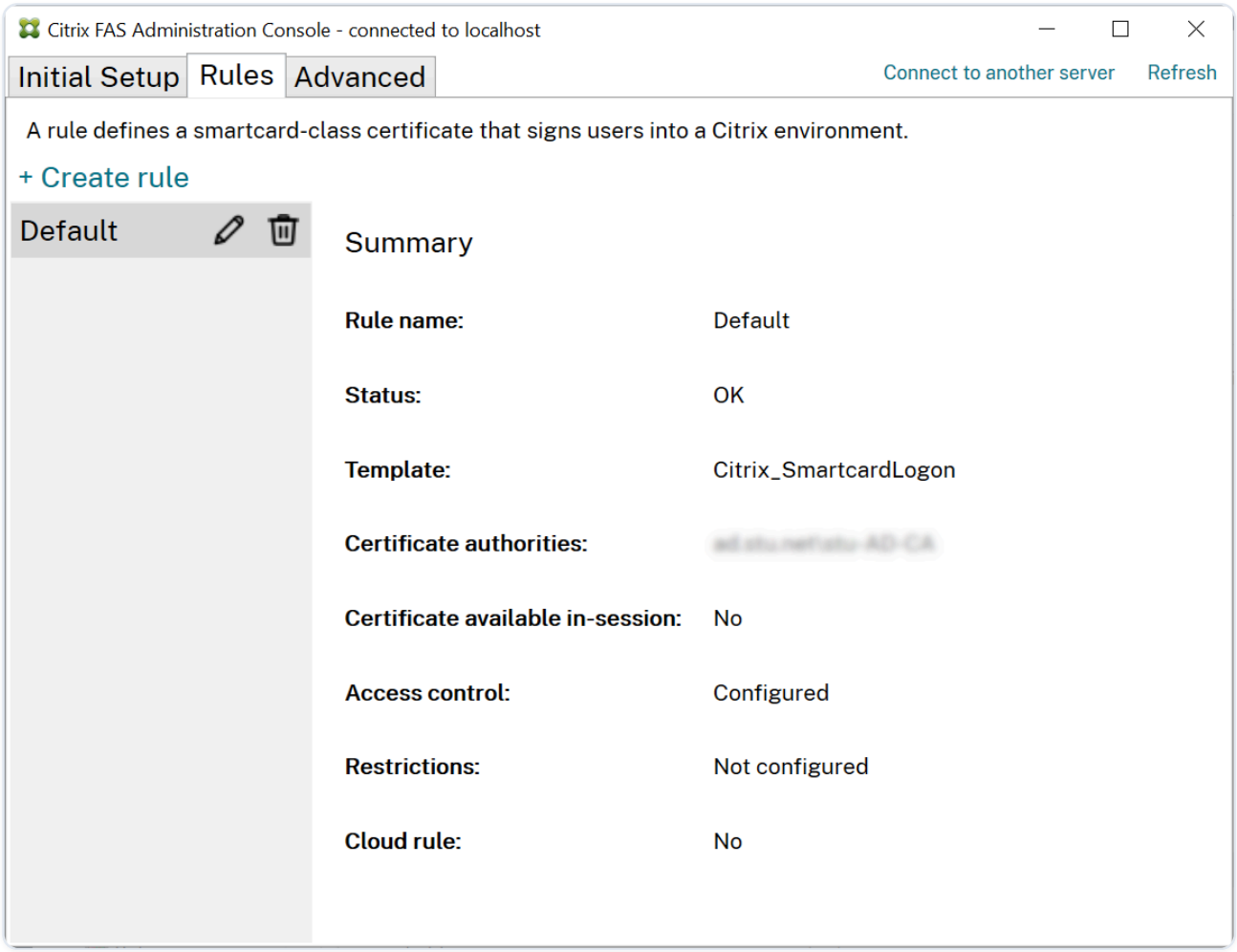
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 请求证书的用户集。
- 允许使用证书的 VDA 计算机集。

Citrix 建议创建名为“default”的规则，因为 StoreFront 在联系 FAS 时会请求同名规则。

您可以创建更多自定义规则，以引用不同的证书模板和证书颁发机构，并将其配置为具有不同的属性和权限。这些规则可以配置为供不同的 StoreFront 服务器或 Workspace 使用。使用组策略配置选项，将 StoreFront 服务器配置为按名称请求自定义规则。

点击“**创建**”（或在“规则”选项卡上点击“**创建规则**”）以启动规则创建向导，该向导将收集创建规则所需的信息。“规则”选项卡显示每条规则的摘要。



该向导收集以下信息：

模板：用于颁发用户证书的证书模板。这必须是 Citrix_SmartcardLogon 模板，或者是其修改后的副本（请参阅证书模板）。

证书颁发机构：颁发用户证书并发布模板的证书颁发机构。FAS 支持添加多个证书颁发机构以实现故障转移和负载平衡。确保您选择的证书颁发机构的状态显示为“模板可用”。请参阅证书颁发机构管理。

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

会话内使用：“**允许会话内使用**”选项控制在登录到 VDA 后是否可以使用证书。

- 未选择“**允许会话内使用**”（默认，*推荐*）—证书仅用于登录或重新连接，用户在身份验证后无权访问该证书。
- 已选择“**允许会话内使用**”—用户在身份验证后有权访问该证书。大多数客户不应选择此选项。从 VDA 会话中访问的资源（例如内部网网站或文件共享）可以使用 Kerberos 单点登录进行访问，因此不需要会话内证书。

  如果您选择“**允许会话内使用**”，则还必须启用 会话内行为 组策略并将其应用于 VDA。证书随后在登录后放置在用户的个人证书存储中以供应用程序使用。例如，如果您需要对 VDA 会话中的 Web 服务器进行 TLS 身份验证，则 Internet Explorer 可以使用该证书。

访问控制：经授权可为用户登录或重新连接请求证书的受信任 StoreFront 服务器计算机列表。对于所有这些权限，您可以添加单个 AD 对象或组。

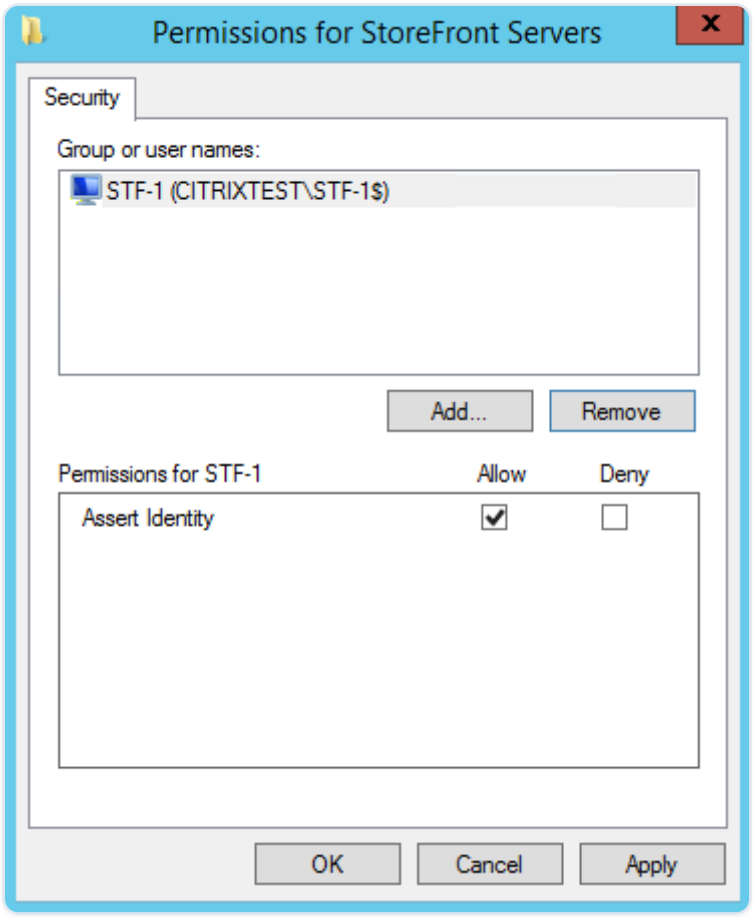
重要：

“**访问控制**”设置对安全性至关重要，必须谨慎管理。

注意：

如果您仅将 FAS 服务器与 Citrix Cloud 结合使用，则无需配置访问控制。当 Citrix Cloud 使用规则时，StoreFront 访问权限将被忽略。您可以将同一规则与 Citrix Cloud 和本地 StoreFront 部署结合使用。当本地 StoreFront 使用规则时，StoreFront 访问权限仍然适用。
默认权限（允许“断言身份”）拒绝所有内容。因此，您必须明确允许您的 StoreFront 服务器。

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



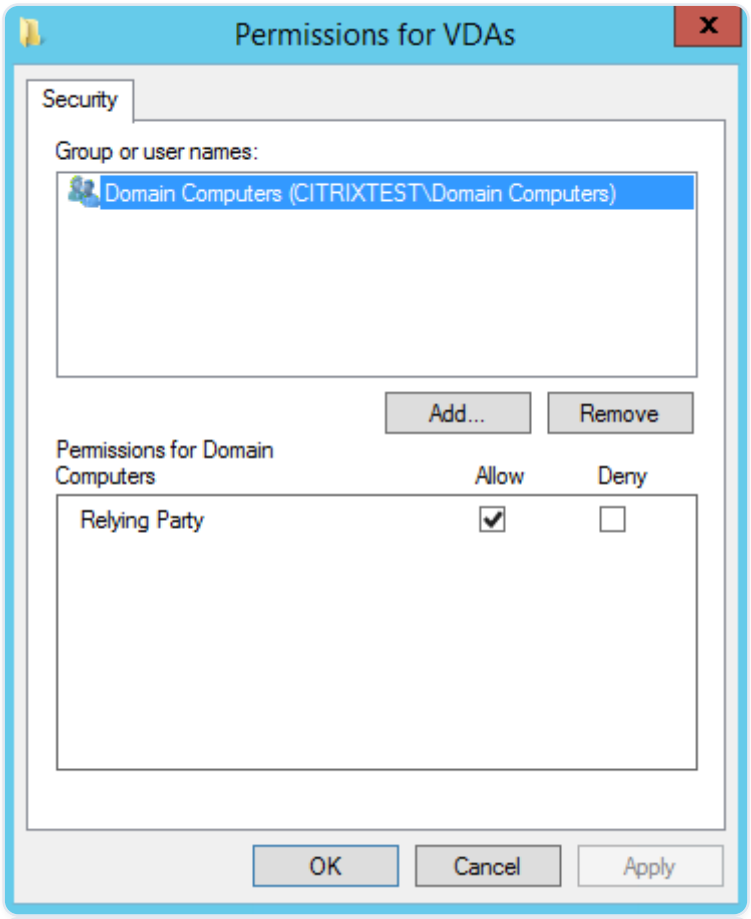
限制：可以使用 FAS 登录用户的 VDA 计算机列表，以及可以通过 FAS 颁发证书的用户列表。

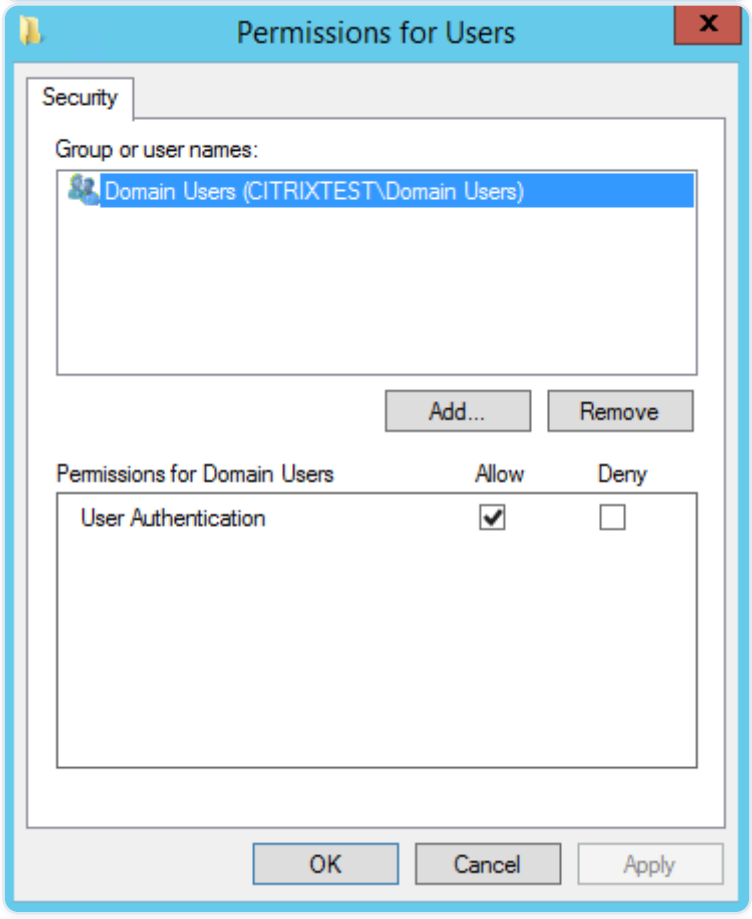
- **管理 VDA 权限**允许您指定哪些 VDA 可以使用 FAS 登录用户。VDA 列表默认为域计算机。
- **管理用户权限**允许您指定哪些用户可以使用 FAS 登录 VDA。用户列表默认为域用户。

注意：

如果 FAS 服务器的域与 VDA 和用户的域不同，则必须修改默认限制。

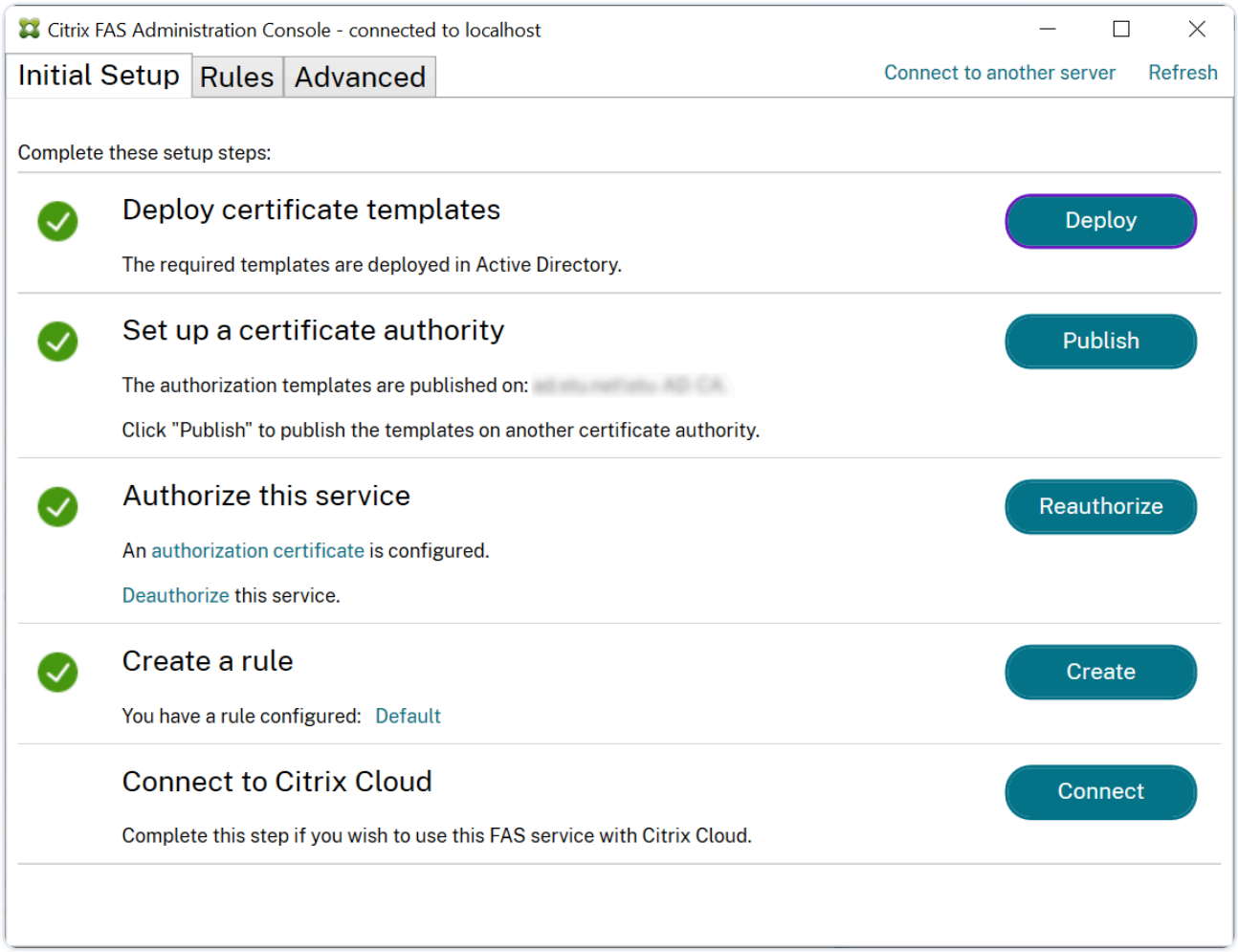
© 1997–2026 Citrix Systems, Inc. All rights reserved.





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

云规则：指示从 Citrix Workspace 收到身份断言时是否应用该规则。连接到 Citrix Cloud 时，您可以选择要用于 Citrix Cloud 的规则。连接到 Citrix Cloud 后，您还可以通过“**连接到 Citrix Cloud**”部分中的链接更改规则。

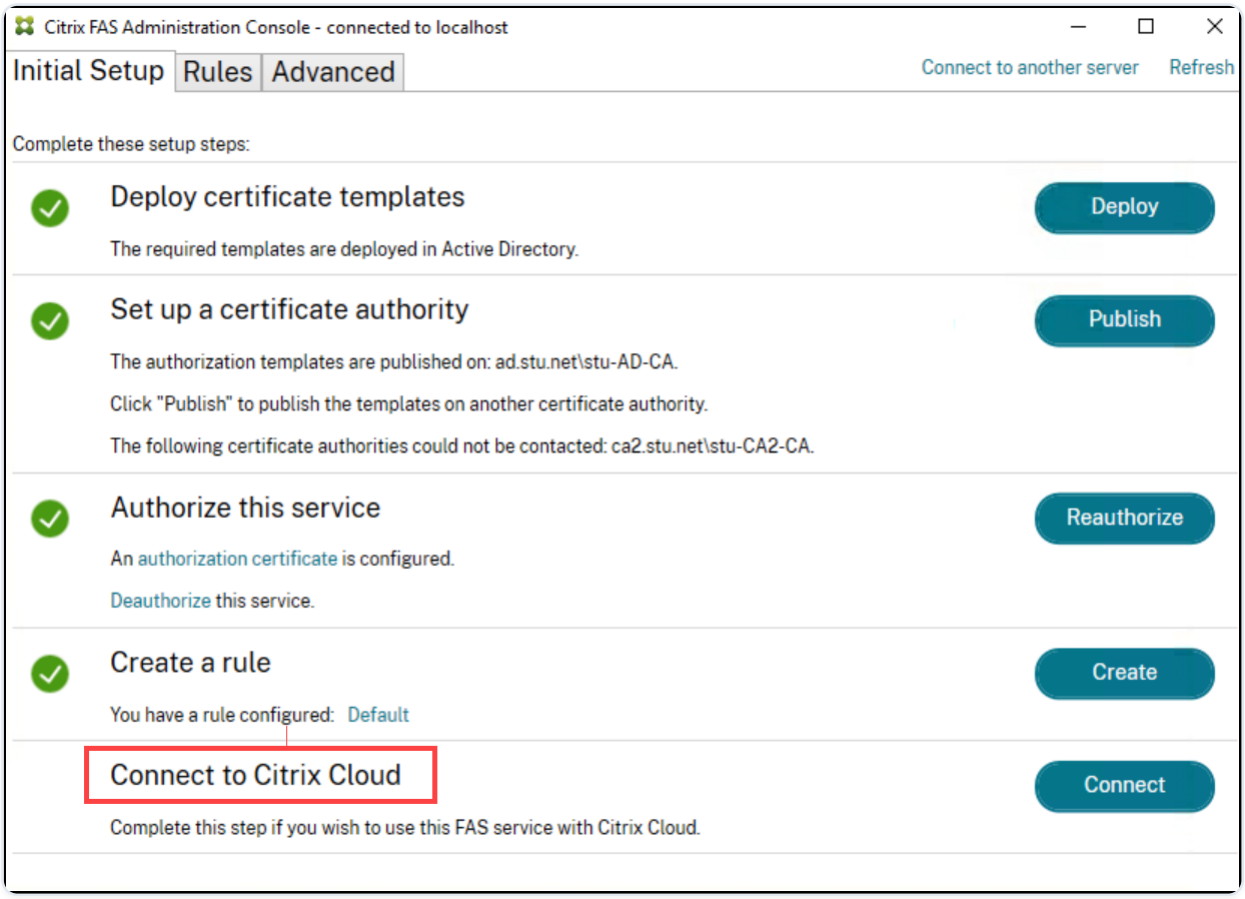


连接到 Citrix Cloud

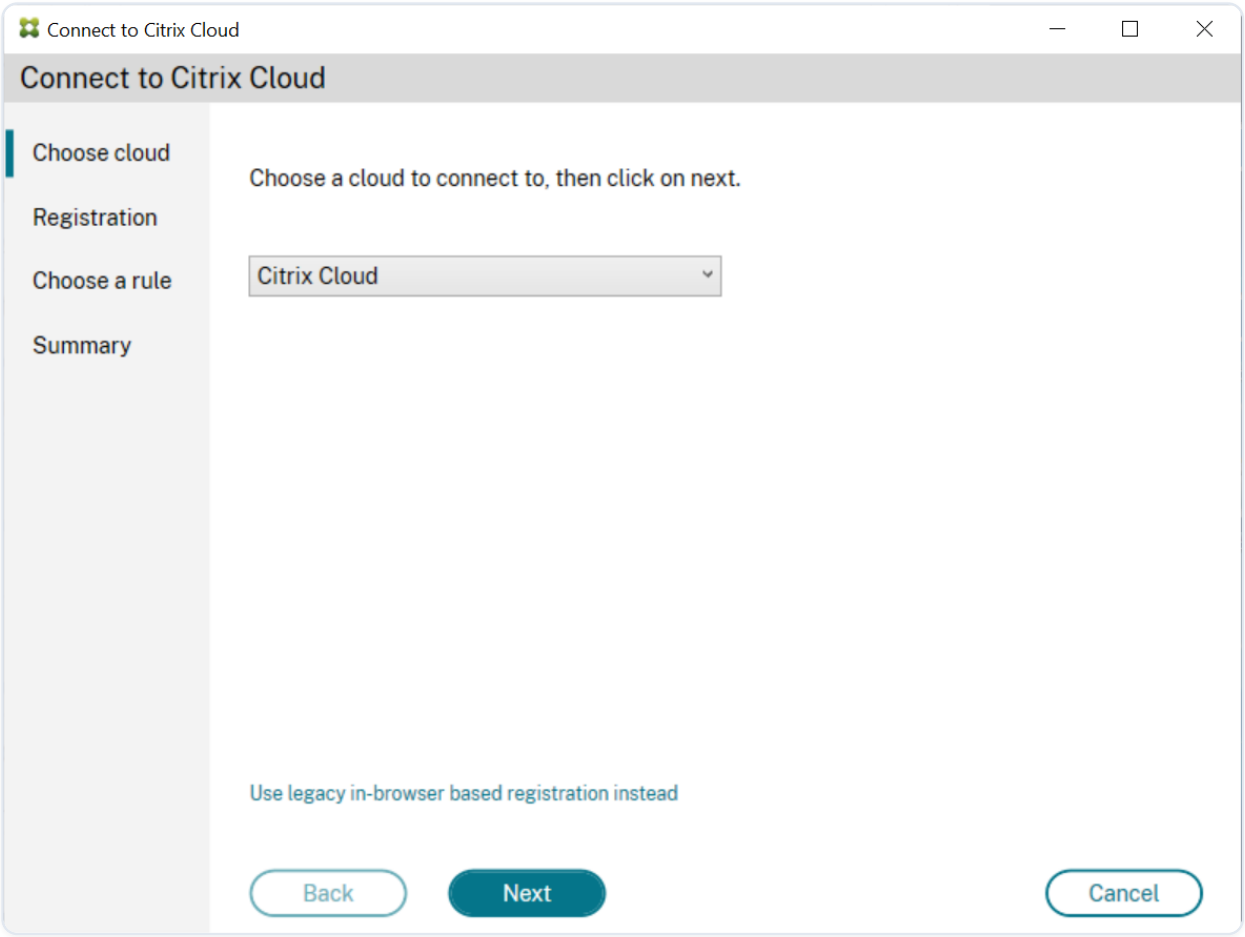
您可以将 FAS 服务器与 Citrix Workspace 连接到 Citrix Cloud。请参阅此Citrix Workspace 文章。

1. 在“初始设置”选项卡中，在“**连接到 Citrix Cloud**”下单击“**连接**”。

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



2. 选择要连接到的云，然后单击“**下一步**”。

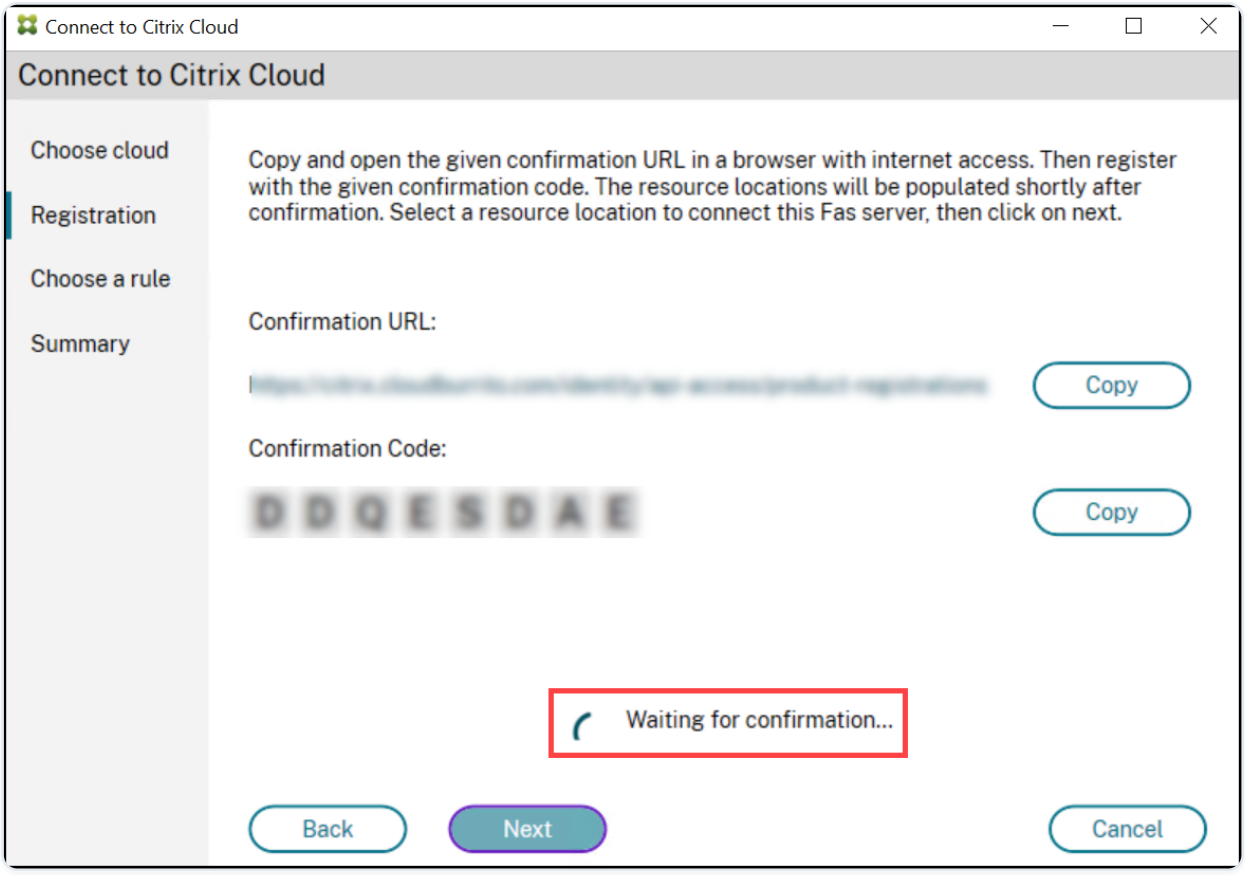


© 1997–2026 Citrix Systems, Inc. All rights reserved.

注意

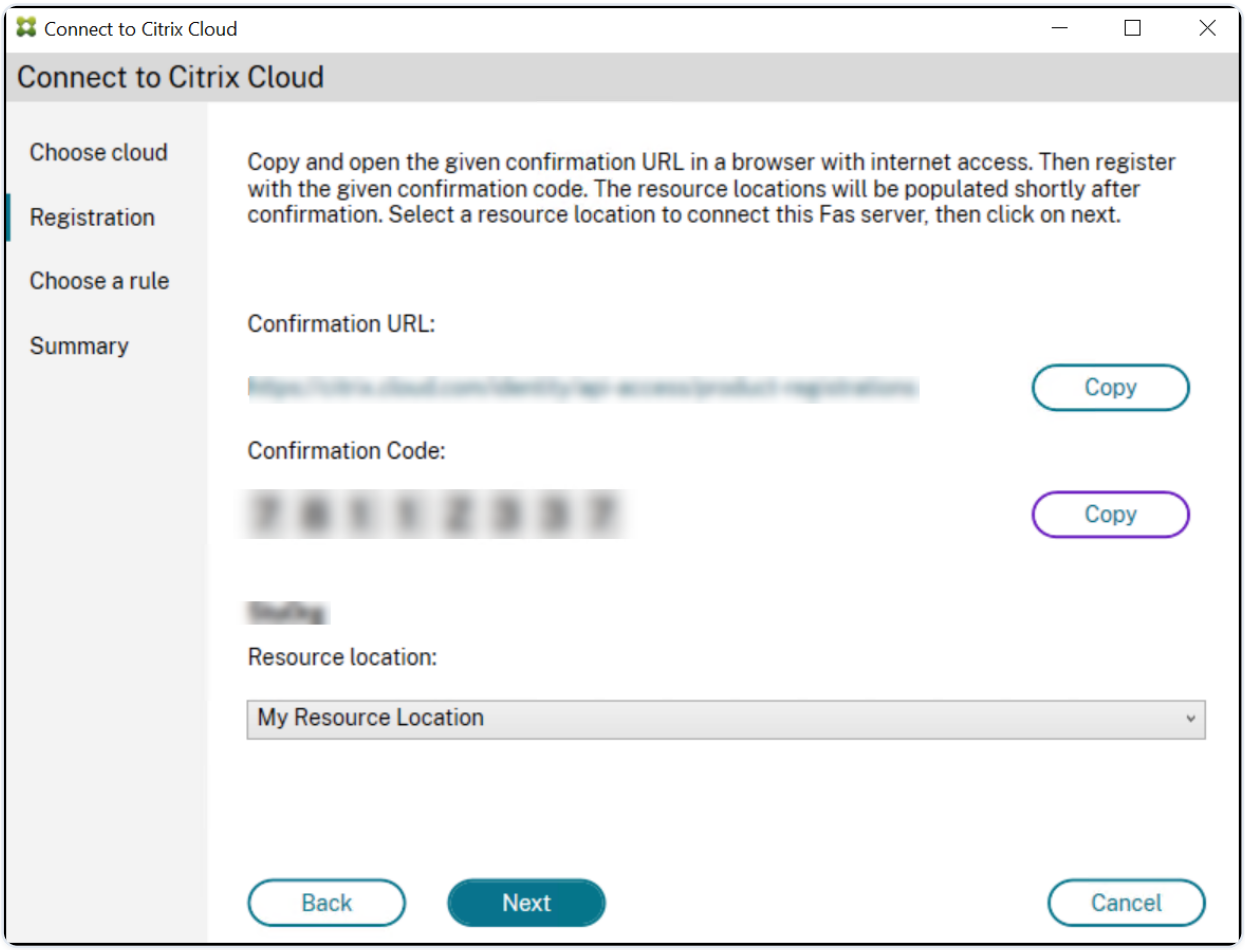
预览版中仅提供 **Citrix Cloud**。

3. 窗口显示一个唯一的注册码，该注册码必须在 Citrix Cloud 中获得批准。有关详细信息，请参阅在 Citrix Cloud 中注册本地产品。



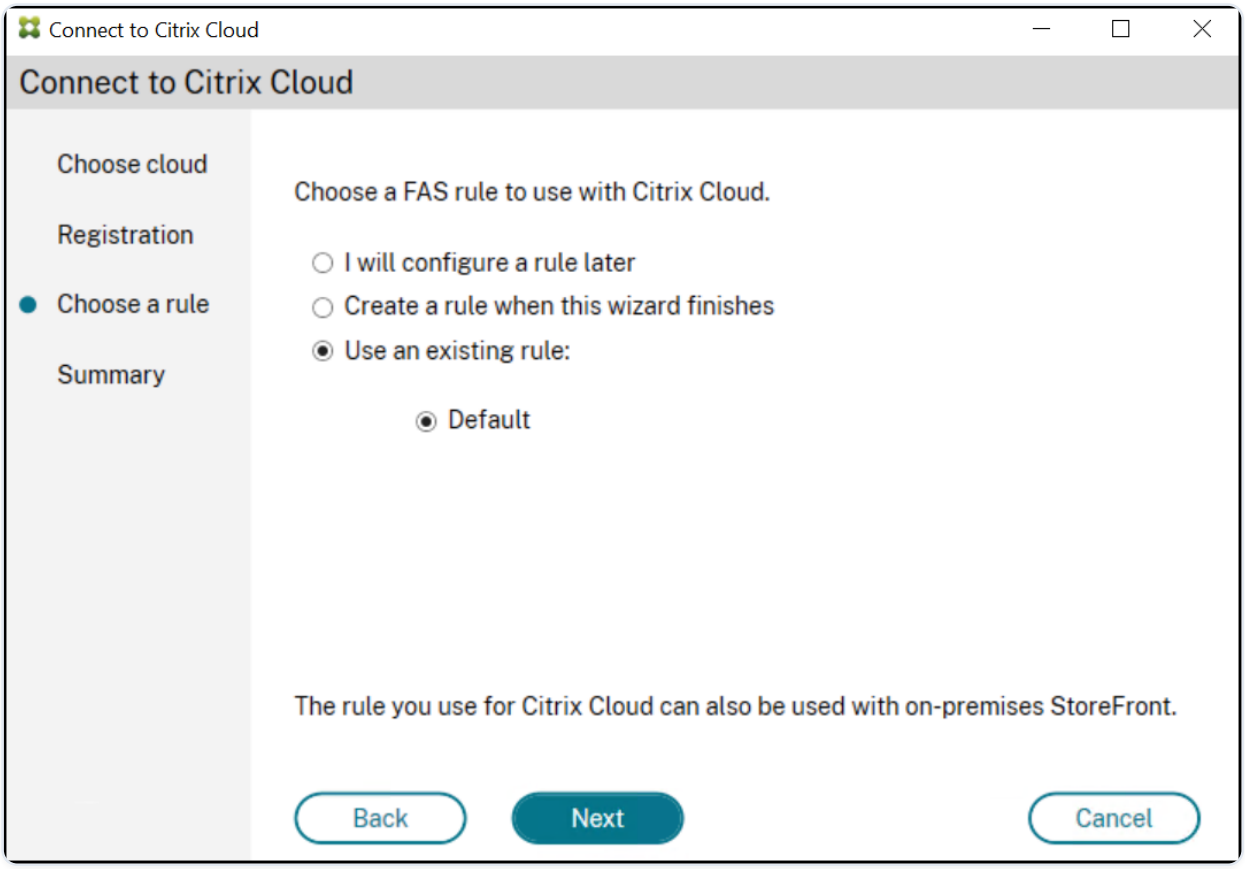
4. 注册码验证通过后，从下拉列表中选择所需的**资源位置**。

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

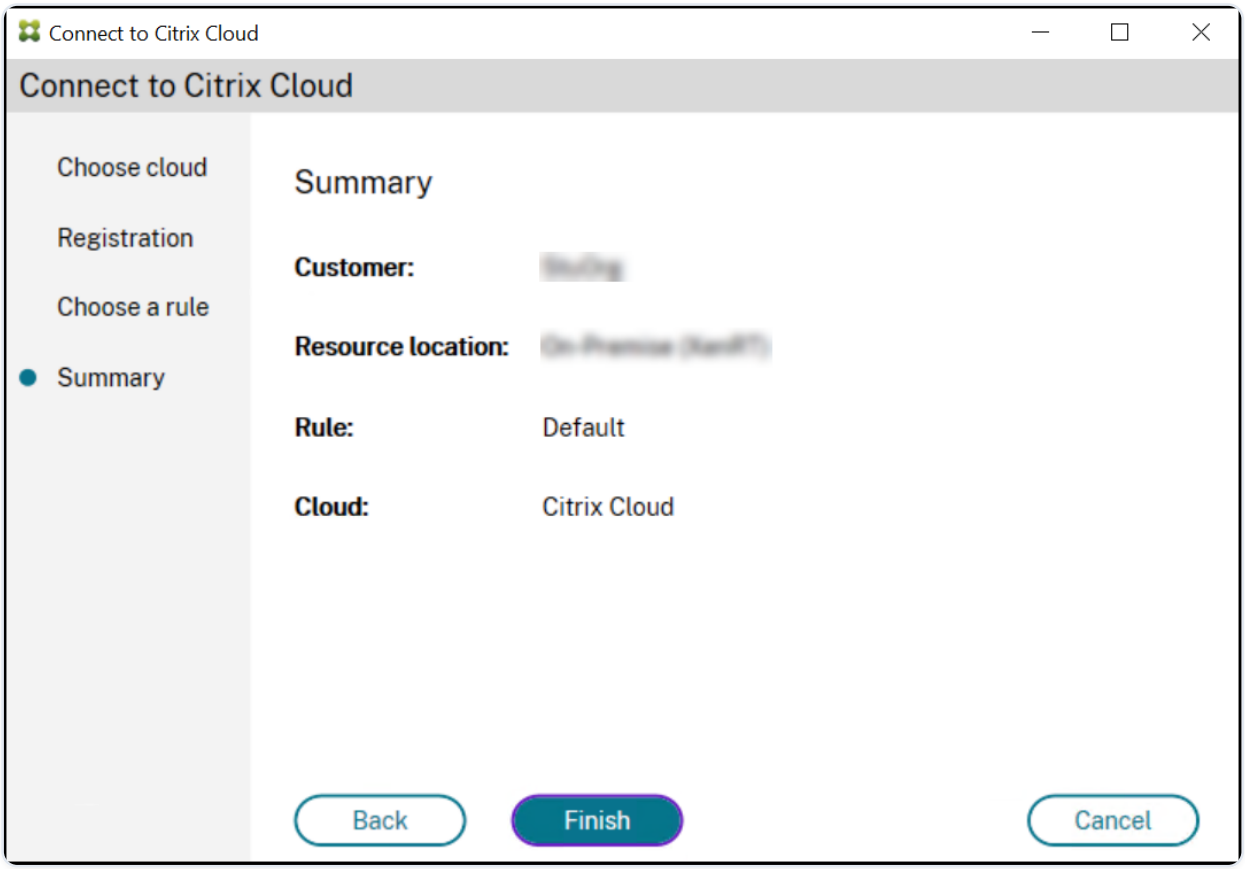


5. 如果适用，选择客户帐户，并选择要连接 FAS 服务器的资源位置。单击**继续**，然后关闭确认窗口。
6. 在**选择规则**部分，使用现有规则或创建规则。单击**下一步**。

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



7. 在**摘要**部分，单击**完成**以完成 Citrix Cloud 连接。



Citrix Cloud 注册 FAS 服务器，并在您的 Citrix Cloud 帐户的“资源位置”页面上显示它。

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

注意

本地 FAS 服务器可以颁发用户证书，以便同时访问 Citrix Cloud 和 Citrix Virtual Apps and Desktops。

断开与 Citrix Cloud 的连接

从 Citrix Cloud 资源位置移除 FAS 服务器后，如本Citrix Workspace 文章中所述，在**连接到 Citrix Cloud**中选择**禁用**。

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

高级配置

本节中的文章提供了有关联合身份验证服务 (FAS) 的高级配置和管理指南。

相关信息

- FAS 安装和初始设置的主要参考资料是安装和配置文章。
- 部署体系结构文章概述了主要的 FAS 体系结构，并提供了指向有关更复杂体系结构的其他文章的链接。

为租户客户启用联合身份验证服务

本文介绍了在多租户托管服务提供商 (MSP) 环境中启用联合身份验证服务 (FAS) 的步骤。有关详细信息，请参阅 参考架构：Citrix 服务提供商 DaaS。

先决条件

- 您拥有 Citrix Cloud 上域和资源位置的管理员访问权限。有关详细信息，请参阅 修改管理员权限。
- 您已建立租户-MSP 关系。有关详细信息，请参阅 适用于 Citrix 服务提供商的 Citrix DaaS。

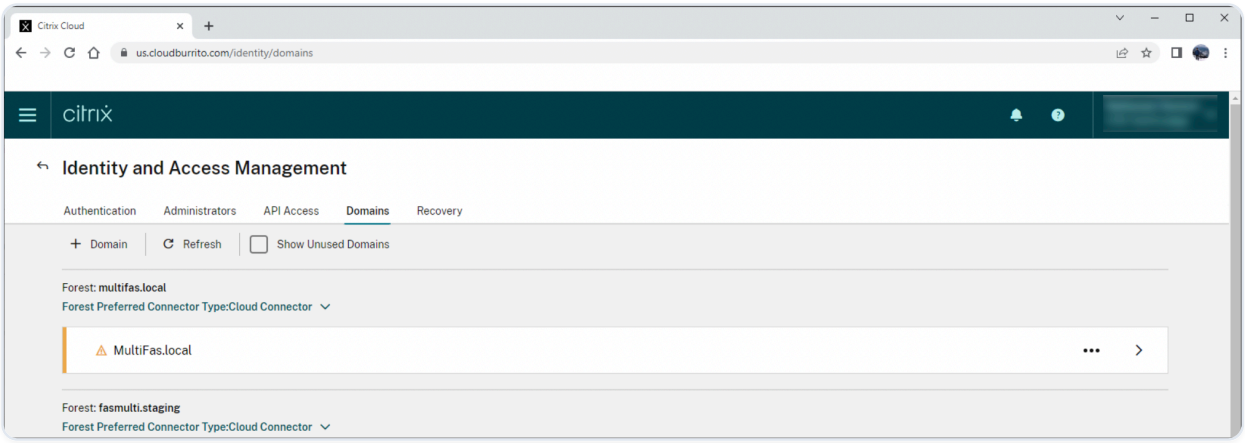
配置 MSP 客户

1. 使用云连接器使 Active Directory 域可用于 Citrix 云。

   通过 安装云连接器 将本地基础架构连接到 Citrix Cloud。

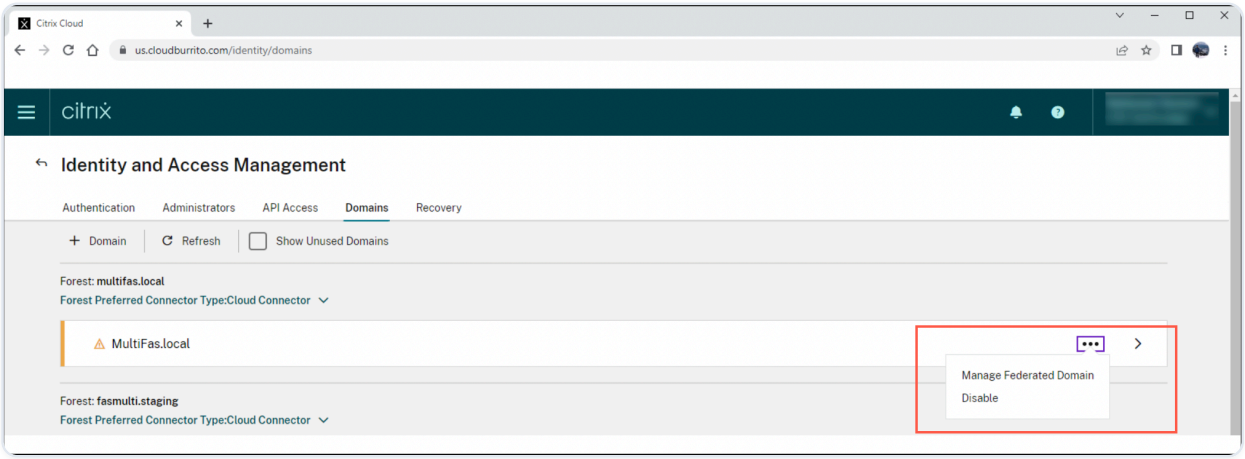
   验证与本地域控制器关联的域在 **身份和访问管理** > **域** 下可用。

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



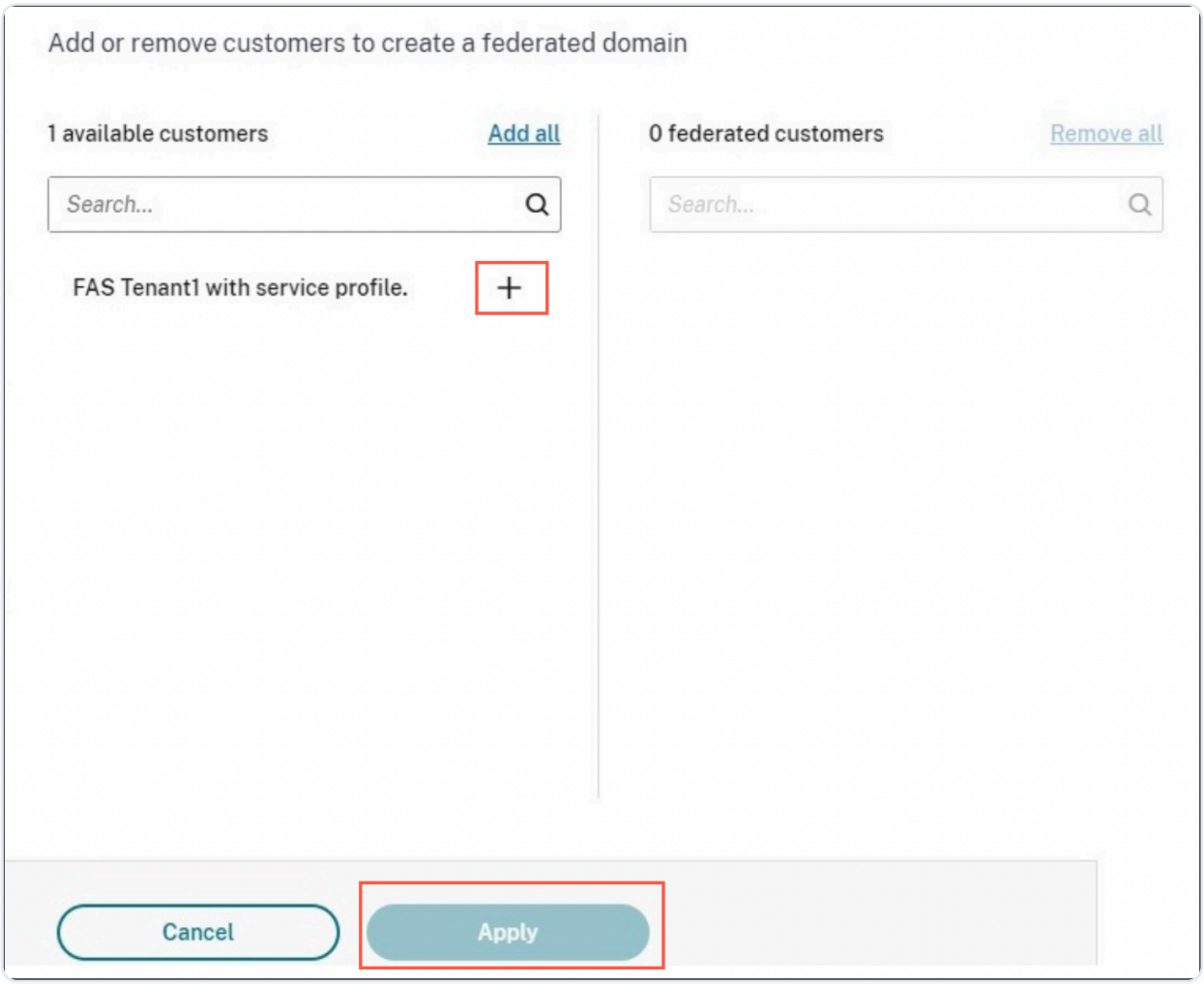
2. 将域联合到租户。

   选择域，然后单击下拉菜单 (...)，再单击 **管理联合域**。



   找到租户并单击 **+**。然后单击 **应用**。

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



3. 验证关联的域是否存在于租户中。

   此步骤是可选的。登录租户客户的控制台，验证域是否列在 **身份和访问管理** > **域** 下。

   验证关联的域是否存在于租户中(/en-us/federated-authentication-service/2402-ltsr/media/fas-verify-domains.png)

   返回 MSP 客户。

4. 在 Citrix Cloud 中安装并注册 FAS 服务器。

   在租户的 Citrix Virtual Apps and Desktops 资源所在的 Active Directory (AD) 林中安装 FAS。将 FAS 连接到与该 AD 林关联的云资源位置。要安装 FAS 服务器，请参阅安装和配置。

5. 配置租户客户

   为租户客户启用 FAS

   - 配置您的身份提供程序 (IdP)

     切换到租户客户。转到 **身份和访问管理** > **身份验证**。连接到您的 IdP 并确保 AD 与 IdP 同步。

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

- 为租户启用 FAS

  转到 **Workspace 配置** > **身份验证**。选择您已设置的身份验证并启用 FAS。

  启用 FAS 租户(/en-us/federated-authentication-service//current-release/media/fas-enable-tenant.png)

已知问题

在删除租户的联合域之前删除 MSP 域存在一个已知问题。您仍然可以为租户启用 FAS，但由于该域不再存在于 MSP 中，FAS 将失败。

Azure Active Directory 单点登录

Citrix 联邦身份验证服务 (FAS) 为已加入域的虚拟投递代理 (VDA) 提供单点登录 (SSO)。FAS 通过向 VDA 提供用户证书来实现 SSO，VDA 使用该证书向 Active Directory (AD) 验证用户身份。登录 VDA 会话后，无需重新验证即可访问 AD 资源。

通常会实施 Azure Active Directory (AAD)，并在 AD 和 AAD 之间进行同步，这会为用户和计算机创建混合身份。本文介绍了在使用 FAS 时，从 VDA 会话内部实现 AAD 单点登录所需的额外配置，这允许用户无需重新验证即可访问受 AAD 保护的应用程序。

注意：

- 您不需要任何特殊配置即可让 FAS 将 SSO 用于 AAD。
- 您不需要 FAS 会话内证书。
- 您可以使用任何版本的 FAS。
- 您可以使用任何支持 FAS 的 VDA 版本。

AAD SSO 的技术总结在下表中：

AAD 身份验证类型	VDA 已加入域	VDA 已混合加入
托管	使用 AAD 无缝 SSO	使用 AAD 基于证书的身份验证
联合到 Active Directory 联合身份验证服务 (ADFS)	在 ADFS 上启用 Windows 身份验证	确保 WS-Trust *certificatemixed* 端点已启用

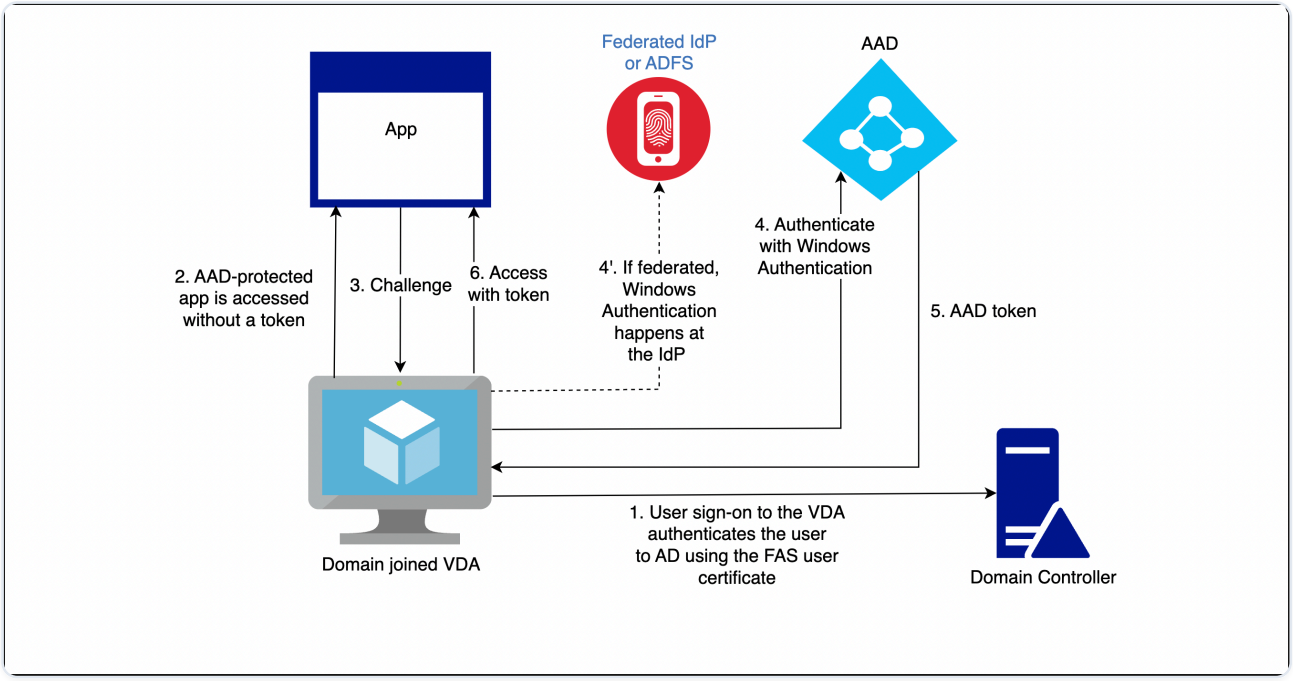
© 1997–2026 Citrix Systems, Inc. All rights reserved.

AAD 身份验证类型	VDA 已加入域	VDA 已混合加入
联合到第三方身份提供程序	使用第三方解决方案	使用第三方解决方案

- 托管 AAD 域是指用户身份验证在 AAD 中进行，有时也称为本机 AAD 身份验证。
- 联合 AAD 域是指 AAD 配置为将身份验证重定向到其他位置的域。例如，重定向到 ADFS 或第三方身份提供程序。
- 混合加入的 VDA 是已加入 AD 和 AAD 的 VDA。

已加入域的 VDA

对于已加入域的 VDA，使用 Windows 身份验证（传统上称为集成 Windows 身份验证或 Kerberos）实现对 AAD 的 SSO。当用户从 VDA 会话中访问受 AAD 保护的应用程序时，将进行对 AAD 的身份验证。下图显示了高级别的身份验证过程：



具体细节因 AAD 域是托管域还是联合域而异。

有关托管 AAD 域设置的信息，请参阅 无缝单点登录。

对于联合到 ADFS 的 AAD 域，请在 ADFS 服务器上启用 Windows 身份验证。

对于联合到第三方身份提供商的 AAD 域，存在类似的解决方案。请联系您的身份提供商寻求帮助。

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

注意：

您也可以将为域加入的 VDA 列出的解决方案用于混合加入的 VDA。但是，使用 FAS 时不会生成 AAD 主刷新令牌 (PRT)。

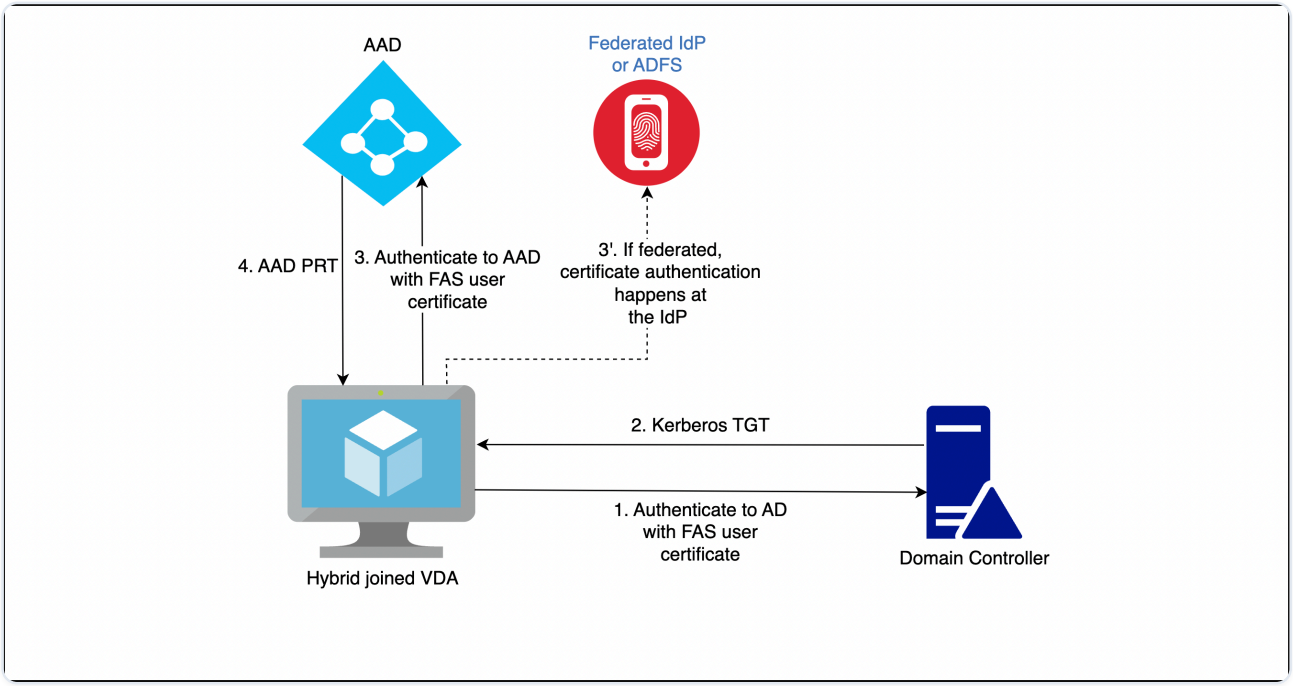
混合加入的 VDA

混合加入的 VDA 同时加入 AD 和 AAD。当用户登录到 VDA 时，会创建以下工件：

- Kerberos 票证授予票证 (TGT)，用于对 AD 资源进行身份验证
- 主刷新令牌 (PRT)，用于对 AAD 资源进行身份验证

PRT 包含有关用户和计算机的信息。如有必要，此信息将用于 AAD 条件访问策略。

由于 FAS 通过向 VDA 提供证书来验证用户身份，因此只有在实施了基于证书的 AAD 身份验证时才能创建 PRT。下图显示了高级别的身份验证过程：



具体细节因 AAD 域是托管的还是联合的而异。

对于托管的 AAD 域，请配置 AAD CBA。有关详细信息，请参阅 Azure AD 基于证书的身份验证概述。VDA 使用 AAD CBA 通过用户的 FAS 证书向 AAD 验证用户身份。

注意：

Microsoft 文档描述了使用智能卡证书登录，但底层技术适用于使用 FAS 用户证书登录。

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

对于联合到 ADFS 的 AAD 域，VDA 使用 ADFS 服务器的 WS-Trust *certificatemixed* 端点通过用户的 FAS 证书向 AAD 验证用户身份。此端点默认启用。

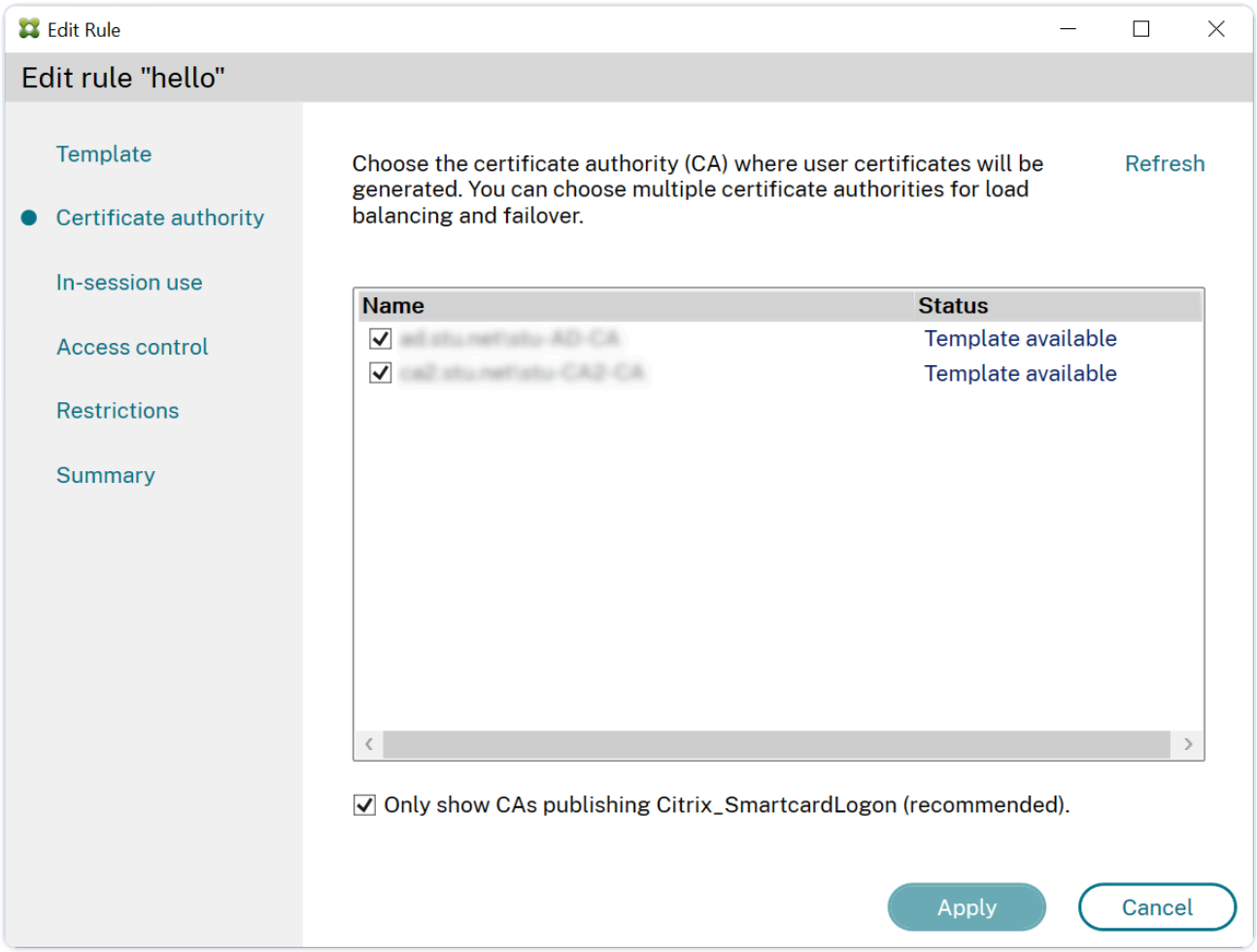
对于联合到第三方身份提供商的 AAD 域，可能存在类似的解决方案。身份提供商必须实现一个 WS-Trust *certificatemixed* 端点。请联系您的身份提供商以获取帮助。

证书颁发机构配置

This article describes the advanced configuration of Federated Authentication Service (FAS) to integrate with certificate authority (CA) servers. Most of these configurations are not supported by the FAS administration console. The instructions use PowerShell APIs provided by FAS. You should have a basic knowledge of PowerShell before executing any instructions in this article.

设置多个 CA 服务器以在 FAS 中使用

您可以在创建或编辑规则时，使用 FAS 管理控制台配置 FAS 以使用多个 CA：



您选择的所有 CA 都必须发布 Citrix_SmartcardLogon 证书模板（或您在规则中选择的任何模板）。

如果您希望使用的某个 CA 未发布所需的模板，请为该 CA 执行 设置证书颁发机构 步骤。

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

注意：

您无需为每个 CA 执行 授权此服务 步骤，因为在此步骤中配置的授权证书可用于您的任何 CA。

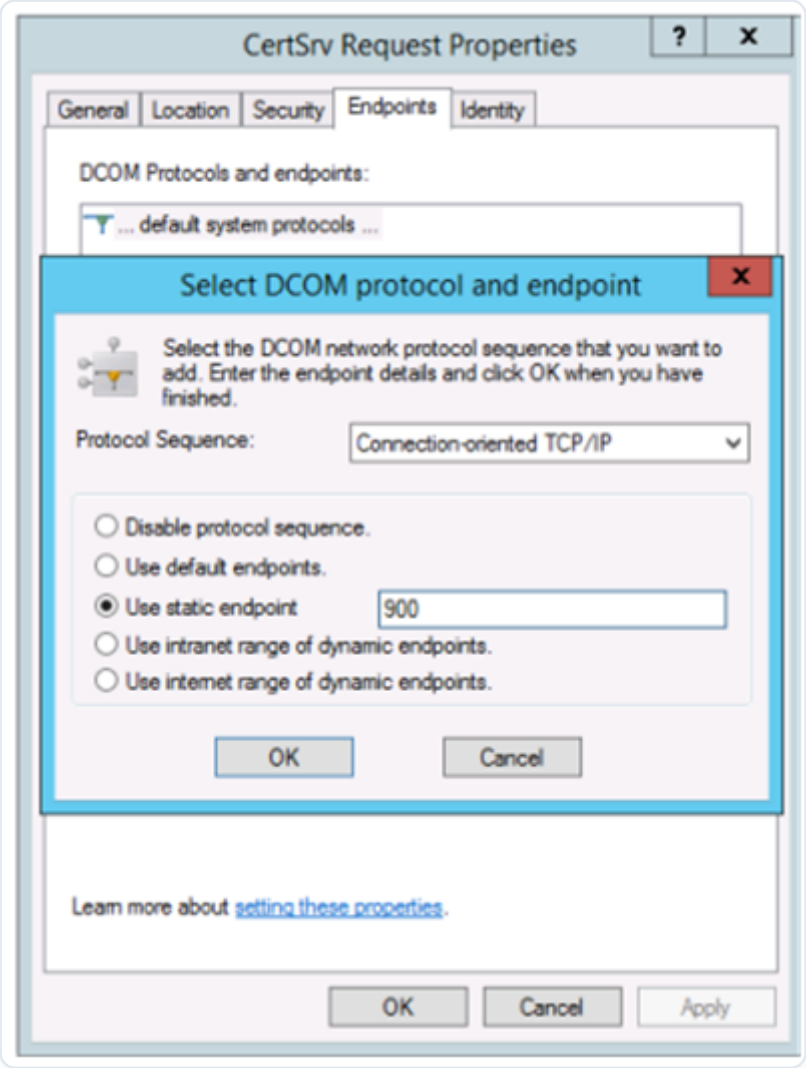
预期行为更改

在您使用多个 CA 服务器配置 FAS 服务器后，用户证书生成将在所有已配置的 CA 服务器之间分发。此外，如果其中一个已配置的 CA 服务器发生故障，FAS 服务器将切换到另一个可用的 CA 服务器。

配置 Microsoft 证书颁发机构以进行 TCP 访问

FAS 使用 DCOM 访问 Microsoft CA。DCOM 使用端口 135 来发现服务正在侦听的端口。默认情况下，侦听端口是动态分配的。 这在实施防火墙安全时可能会导致复杂性。因此，Microsoft 提供了一种配置静态端口的方法。 要在 Microsoft CA 上配置静态端口，请选择“**开始**”>“**运行**”> `dcomcnfg.exe` 以打开 DCOM 配置面板。展开“**计算机**”>“**我的电脑**”>“**DCOM 配置**”以显示 CertSrv 请求节点。然后，编辑 CertSrv 请求 DCOM 应用程序的属性：

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



更改“**终结点**”以选择静态终结点并指定 TCP 端口号（在上图中为 900）。

在此示例中，防火墙需要允许端口 135 和端口 900。

重启 Microsoft 证书颁发机构以应用更改。

无需配置 FAS 服务器（或任何其他使用证书颁发机构的计算机），因为 DCOM 使用 RPC 端口 135 进行协商阶段。当客户端需要使用 DCOM 时，它会连接到服务器上的 DCOM RPC 服务并请求访问特定的 DCOM 服务器。这会触发端口 900（在此示例中）打开，并且 DCOM 服务器会指示客户端连接到该端口。

预生成用户证书

在 FAS 服务器中预生成用户证书后，用户的登录时间将显著缩短。以下部分介绍了如何为单个或多个 FAS 服务器执行此操作。

获取 Active Directory 用户列表

您可以通过查询 AD 并将用户列表存储到文件中（例如，.csv 文件）来改进证书生成，如下例所示。

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

```
Import-Module ActiveDirectory



$searchbase = "cn=users,dc=bvt,dc=local" # AD User Base to Look for Users,
leave it blank to search all

$filename = "user_list.csv" # Filename to save



if ($searchbase -ne ""){

    Get-ADUser -Filter {(UserPrincipalName -ne "null") -and (Enabled -eq
"true")} -SearchBase $searchbase -Properties UserPrincipalName | Select
UserPrincipalName | Export-Csv -NoTypeInformation -Encoding utf8
-delimiter "," $filename

} else {

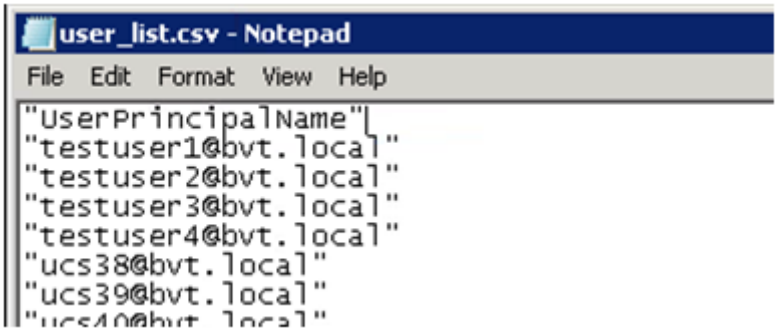
    Get-ADUser -Filter {(UserPrincipalName -ne "null") -and (Enabled -eq
"true")} -Properties UserPrincipalName | Select UserPrincipalName |
Export-Csv -NoTypeInformation -Encoding utf8 -delimiter "," $filename

}
```

Get-ADUser 是一个标准的 cmdlet，用于查询用户列表。上面的示例包含一个筛选器参数，用于仅列出具有 UserPrincipalName 且帐户状态为“enabled”的用户。

SearchBase 参数缩小了在 AD 中搜索用户的范围。如果您想包含 AD 中的所有用户，可以省略此参数。注意：此查询可能会返回大量用户。

CSV 文件内容如下所示：



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

FAS 服务器

以下 PowerShell 脚本获取之前生成的用户列表并创建用户证书列表。

```
Add-PSSnapin Citrix.A*

$csv = "user_list.csv"

$rule = "default" # rule/role in your admin console

$users = Import-Csv -encoding utf8 $csv

foreach ( $user in $users )

{

    $server = Get-FasServerForUser -UserPrincipalNames
$user.UserPrincipalName

    if( $server.Server -ne $NULL) {

        New-FasUserCertificate -Address $server.Server -UserPrincipalName
$user.UserPrincipalName -CertificateDefinition $rule"_Definition" -Rule
$rule

    }

    if( $server.Failover -ne $NULL) {

        New-FasUserCertificate -Address $server.Failover
-UserPrincipalName $user.UserPrincipalName -CertificateDefinition
$rule"_Definition" -Rule $rule

    }

}
```

如果您有多个 FAS 服务器，特定用户的证书将生成两次：一个在主服务器中，另一个在故障转移服务器中。

上述脚本适用于名为“default”的规则。如果您有不同的规则名称（例如，“hello”），只需更改脚本中的 $rule 变量即可。

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

本地化图像(/en-us/federated-authentication-service/2402-ltsr/media/fas-caconfig-rule-name.png)

续订注册机构证书

如果正在使用多个 FAS 服务器，您可以续订 FAS 授权证书，而不会影响已登录的用户。

注意：

您还可以使用 GUI 重新授权 FAS：

本地化图像(/en-us/federated-authentication-service/2402-ltsr/media/admin-console-reauthorize.png)
完成以下序列：

1. 创建新的授权证书：`New-FasAuthorizationCertificate`
2. 记下新授权证书的 GUID，该 GUID 由以下命令返回：`Get-FasAuthorizationCertificate`
3. 将 FAS 服务器置于维护模式：`Set-FasServer –Address <FAS server> -MaintenanceMode $true`
4. 交换新的授权证书：`Set-FasCertificateDefinition –AuthorizationCertificate <GUID>`
5. 使 FAS 服务器退出维护模式：`Set-FasServer –Address <FAS server> -MaintenanceMode $false`
6. 删除旧的授权证书：`Remove-FasAuthorizationCertificate`

相关信息

- 安装和配置 一文是 FAS 安装和配置的主要参考资料。
- 常见的联合身份验证服务部署总结在部署架构一文中。
- 其他“操作方法”文章介绍在高级配置一文中。

私钥保护

简介

证书存储在 FAS 服务器的嵌入式数据库中。关联的私钥通过 FAS 服务器的网络服务帐户存储，并且默认标记为不可导出。

私钥有两种类型：

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

- 与注册机构证书关联的私钥，来自 Citrix_RegistrationAuthority 证书模板。
- 与用户证书关联的私钥，来自 Citrix_SmartcardLogon 证书模板。

实际上有两种注册机构证书：Citrix_RegistrationAuthority_ManualAuthorization（默认有效期为 24 小时）和 Citrix_RegistrationAuthority（默认有效期为两年）。

在联合身份验证服务 (FAS) 管理控制台的“**初始设置**”选项卡第 3 步中，当您单击“**授权**”时，FAS 服务器会生成一个密钥对，并向证书颁发机构发送一个针对 Citrix_RegistrationAuthority_ManualAuthorization 证书的证书签名请求。这是一个临时证书，默认有效期为 24 小时。证书颁发机构不会自动颁发此证书；其颁发必须由管理员在证书颁发机构上手动授权。证书颁发给 FAS 服务器后，FAS 会使用 Citrix_RegistrationAuthority_ManualAuthorization 证书自动获取 Citrix_RegistrationAuthority 证书（默认有效期为两年）。FAS 服务器在获取 Citrix_RegistrationAuthority 证书后，会立即删除 Citrix_RegistrationAuthority_ManualAuthorization 的证书和密钥。

与注册机构证书关联的私钥特别敏感，因为注册机构证书策略允许拥有该私钥的任何人针对模板中配置的用户集发出证书请求。因此，控制此密钥的任何人都可以作为该集合中的任何用户连接到环境。

您可以配置 FAS 服务器，以符合您组织安全要求的方式保护私钥，使用以下方法之一：

- Microsoft 增强型 RSA 和 AES 加密服务提供程序或 Microsoft 软件密钥存储提供程序，用于注册机构证书和用户证书的私钥。
- 带有受信任平台模块 (TPM) 芯片的 Microsoft 平台密钥存储提供程序，用于注册机构证书的私钥，以及 Microsoft 增强型 RSA 和 AES 加密服务提供程序或 Microsoft 软件密钥存储提供程序，用于用户证书的私钥。
- 硬件安全模块 (HSM) 供应商的加密服务或密钥存储提供程序（带 HSM 设备），用于注册机构证书和用户证书的私钥。

私钥配置设置

配置 FAS 以使用这三个选项之一。使用文本编辑器编辑 Citrix.Authentication.FederatedAuthenticationService.exe.config 文件。该文件的默认位置是 FAS 服务器上的 Program Files\Citrix\Federated Authentication Service 文件夹。

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

```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <appSettings>
    <!-- This option switch between CAPI API  (true) and CNG API (false) Cryptographic Providers  -->
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderLegacyCsp" value="false"/>

    <!-- Specify the Cryptographic Service Provider (CSP) / Key Storage Provider (KSP) Name.  -->
    <!-- add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderName" value="Microsoft Software Key Storage Provider"/ -->

    <!-- Specify the Cryptographic Service Provider Type (only for CSP - not KSP).  For example: PROV_RSA_AES is 24  -->
    <!-- add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderType" value="24"/ -->

    <!-- Specify Private Key protection [NoProtection|GenerateNonExportableKey|GenerateTPMProtectedKey] -->
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.KeyProtection" value="GenerateNonExportableKey"/>

    <!-- Specify RSA Key length -->
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.KeyLength" value="2048"/>

    <!-- Logging: Event log Verbosity (0 Disabled, 1 Errors, 2 Warnings, 3 Informational) -->
    <!-- add key="Citrix.Authentication.UserCredentialService.SystemLog.LogLevel" value="3" / -->

    <!-- Logging: Event IDs to not log (comma separated) -->
    <!-- add key="Citrix.Authentication.UserCredentialService.SystemLog.Supress" value="" / -->

    <!-- Logging: Disable Key Management logs -->
    <!-- add key="Citrix.TrustFabric.Logging.SystemLog" value=""/ -->
  </appSettings>
<startup><supportedRuntime version="v4.0" sku=".NETFramework,Version=v4.5.1"/></startup></configuration>
```

FAS 仅在服务启动时读取配置文件。如果更改了任何值，则必须重新启动 FAS 才能使新设置生效。

在 Citrix.Authentication.FederatedAuthenticationService.exe.config 文件中按如下方式设置相关值：

Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.**ProviderLegacyCsp**（在 CAPI 和 CNG API 之间切换）

值	注释
是	使用 CAPI API
false（默认）	使用 CNG API

Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.**ProviderName**（要使用的提供程序名称）

值	注释
微软增强型 RSA 和 AES 加密服务提供程序	默认 CAPI 提供程序
Microsoft 软件密钥存储提供程序	默认 CNG 提供程序
Microsoft 平台密钥存储提供程序	默认 TPM 提供程序。请注意，不建议将 TPM 用于用户密钥。仅将 TPM 用于注册机构密钥。如果您计划在虚拟化环境中运行 FAS 服务器，请咨询您的 TPM 和虚拟机管理程序供应商，以确认是否支持虚拟化。

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

值	注释
HSM_Vendor CSP/密钥存储提供程序	由 HSM 供应商提供。该值因供应商而异。如果您计划在虚拟化环境中运行 FAS 服务器，请咨询您的 HSM 供应商，以确认是否支持虚拟化。

Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.**ProviderType**（仅在 CAPI API 的情况下需要）

值	注释
24	默认值。指的是 Microsoft KeyContainerPermissionAccessEntry.ProviderType 属性 PROV_RSA_AES 24。除非您将 HSM 与 CAPI 结合使用且 HSM 供应商另有规定，否则应始终为 24。

Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.**KeyProtection**（当 FAS 需要执行私钥操作时，它会使用此处指定的值）控制私钥的“可导出”标志。如果硬件支持，则允许使用 TPM 密钥存储。

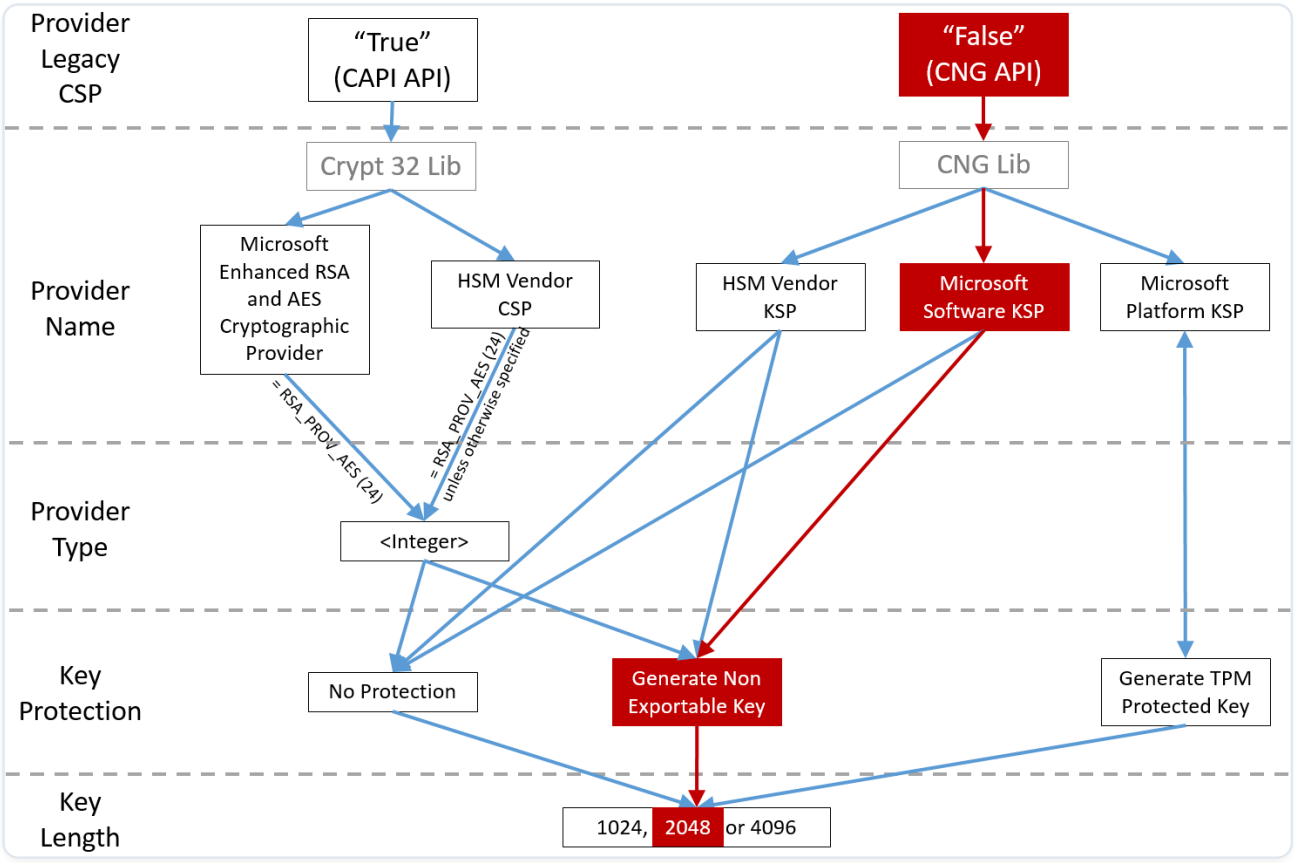
值	注释
无保护	私钥可以导出。
GenerateNonExportableKey	默认。私钥无法导出。
GenerateTPMProtectedKey	私钥将使用 TPM 进行管理。私钥通过您在 ProviderName 中指定的 ProviderName 存储（例如，Microsoft 平台密钥存储提供程序）

Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.**KeyLength**（指定私钥的位数）

值	注释
2048	默认。也可以使用 1024 或 4096。

配置文件设置以图形方式表示如下（安装默认值以红色显示）：

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



配置方案示例

示例 1

此示例涵盖使用 Microsoft 软件密钥存储提供程序存储的注册机构证书私钥和用户证书的私钥。

这是默认的安装后配置。无需额外的私钥配置。

示例 2

此示例展示了注册机构证书私钥通过 Microsoft 平台密钥存储提供程序存储在 FAS 服务器主板的硬件 TPM 中，以及用户证书私钥使用 Microsoft 软件密钥存储提供程序存储。

此方案假定您的 FAS 服务器主板上的 TPM 已根据 TPM 制造商的文档在 BIOS 中启用，然后在 Windows 中初始化；请参阅 `<https://docs.microsoft.com/zh-cn/previous-versions/windows/it-pro/windows-vista/cc749022(v=ws.10)>`。

使用 FAS 管理控制台

FAS 管理控制台无法执行离线证书签名请求，因此不建议使用它，除非您的组织允许对注册机构证书进行在线证书签名请求。

执行初始 FAS 设置时，在部署证书模板和设置证书颁发机构之后，但在授权服务之前（配置序列中的步骤 3）：

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

步骤 1： 通过如下更改以下行来编辑配置文件：

```
<add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.KeyProtection"
value="GenerateTPMProtectedKey"/>
```

文件现在应如下所示：

```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <appSettings>
    <!-- This option switch between CAPI API  (true) and CNG API (false) Cryptographic Providers  -->
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderLegacyCsp" value="false"/>

    <!-- Specify the Cryptographic Service Provider (CSP) / Key Storage Provider (KSP) Name.  -->
    <!-- add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderName" value="Microsoft Software Key Storage Provider"/ -->

    <!-- Specify the Cryptographic Service Provider Type (only for CSP - not KSP).  For example: PROV_RSA_AES is 24  -->
    <!-- add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderType" value="24"/ -->

    <!-- Specify Private Key protection [NoProtection|GenerateNonExportableKey|GenerateTPMProtectedKey] -->
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.KeyProtection" value="GenerateTPMProtectedKey"/>

    <!-- Specify RSA Key length -->
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.KeyLength" value="2048"/>

    <!-- Logging: Event log Verbosity (0 Disabled, 1 Errors, 2 Warnings, 3 Informational) -->
    <!-- add key="Citrix.Authentication.UserCredentialService.SystemLog.LogLevel" value="3" / -->

    <!-- Logging: Event IDs to not log (comma separated) -->
    <!-- add key="Citrix.Authentication.UserCredentialService.SystemLog.Supress" value="" / -->

    <!-- Logging: Disable Key Management logs -->
    <!-- add key="Citrix.TrustFabric.Logging.SystemLog" value=""/ -->
  </appSettings>
<startup><supportedRuntime version="v4.0" sku=".NETFramework,Version=v4.5.1"/></startup></configuration>
```

某些 TPM 限制密钥长度。默认密钥长度为 2048 位。请确保指定您的硬件支持的密钥长度。

步骤 2： 重新启动 Citrix Federated Authentication Service 以从配置文件中读取值。

步骤 3： 授权服务。

步骤 4： 从证书颁发机构服务器手动颁发待处理的证书请求。获取注册机构证书后，管理控制台设置序列中的步骤 3 将变为绿色。此时，注册机构证书的私钥将在 TPM 中生成。默认情况下，证书有效期为 2 年。

要确认注册机构证书的私钥是否正确存储在 TPM 中，请使用以下 PowerShell 命令。如果注册机构证书的私钥存储在 TPM 中，则 PrivateKeyProvider 字段将设置为 *Microsoft Platform Crypto Provider*：

```
Add-PSSnapin Citrix.Authentication.FederatedAuthenticationService.V1

Get-FasAuthorizationCertificate -FullCertInfo -Address localhost
```

步骤 5： 将配置文件改回以下内容：

```
<add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.KeyProtection"
value="GenerateNonExportableKey"/>
```

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

注意：

尽管 FAS 可以生成具有 TPM 保护密钥的用户证书，但对于大型部署而言，TPM 硬件可能太慢。

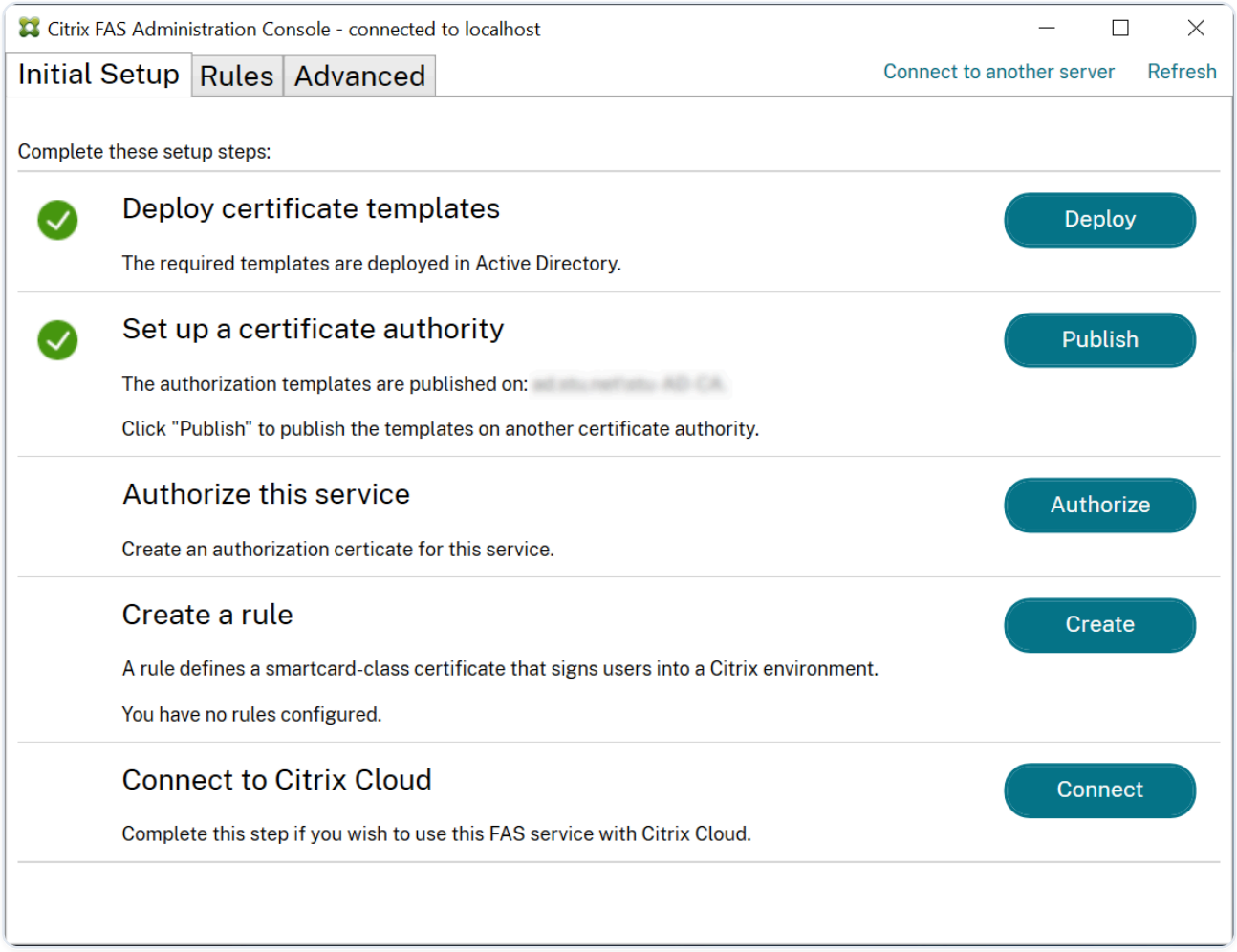
步骤 6： 重新启动 FAS。这将强制服务重新读取配置文件并反映更改的值。随后的自动私钥操作将影响用户证书密钥；这些操作不会将私钥存储在 TPM 中，而是使用 Microsoft Software Key Storage Provider。

步骤 7： 在 FAS 管理控制台中选择**规则**选项卡，并按照安装和配置中的说明编辑设置。

使用 PowerShell

可以使用 PowerShell 离线请求注册机构证书。这适用于不希望其证书颁发机构通过在线证书签名请求颁发注册机构证书的组织。您无法使用 FAS 管理控制台进行离线注册机构证书签名请求。

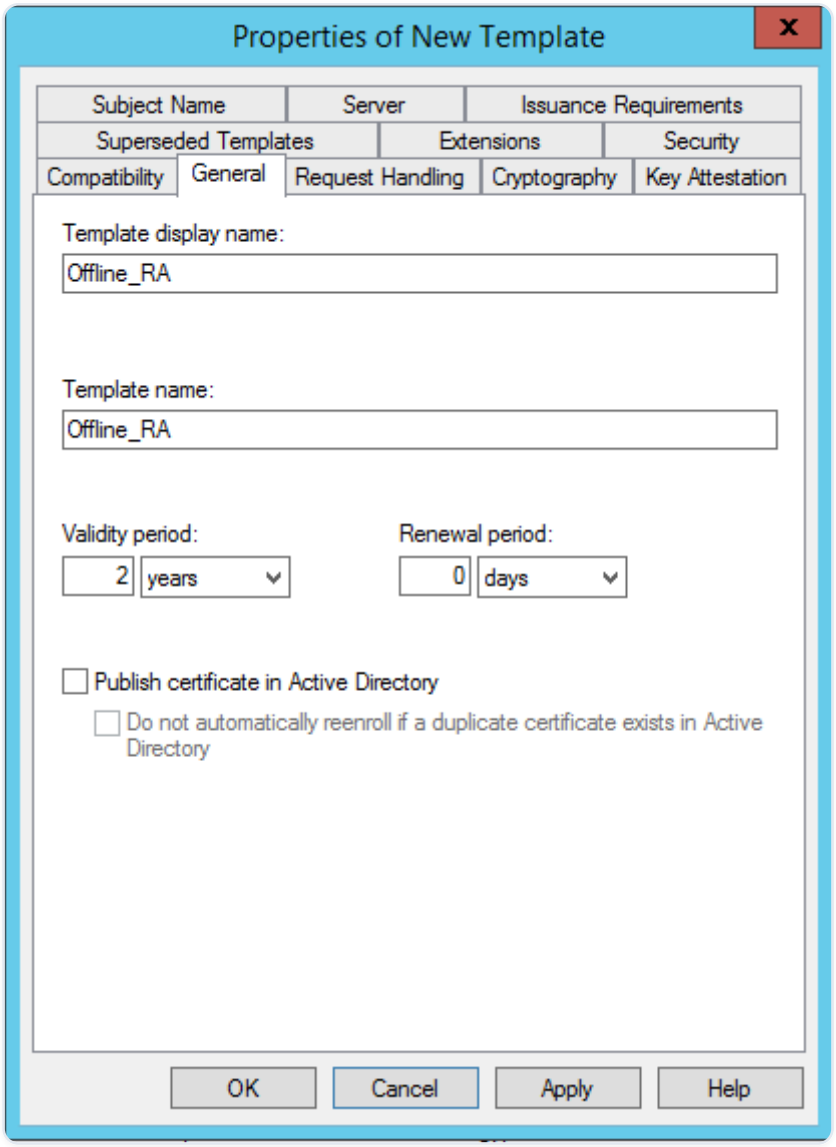
步骤 1： 在使用管理控制台进行初始 FAS 配置期间，仅完成前两个步骤："部署证书模板"和"设置证书颁发机构"。



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

步骤 2： 在您的证书颁发机构服务器上，添加证书模板 MMC 管理单元。右键单击 **Citrix_RegistrationAuthority_ManualAuthorization** 模板，然后选择**复制模板**。

选择**常规**选项卡。更改名称和有效期。在此示例中，名称为 *Offline_RA*，有效期为 2 年：



步骤 3： 在您的证书颁发机构服务器上，添加证书颁发机构 MMC 管理单元。右键单击**证书模板**。选择**新建**，然后单击**要颁发的证书模板**。选择您刚刚创建的模板。

步骤 4： 在 FAS 服务器上加载以下 PowerShell cmdlet：

```
Add-PSSnapin Citrix.Authentication.FederatedAuthenticationService.V1
```

步骤 5： 通过在 FAS 服务器上输入以下 PowerShell cmdlet，在 FAS 服务器的 TPM 中生成 RSA 密钥对并创建证书签名请求。**注意：** 某些 TPM 会限制密钥长度。默认密钥长度为 2048 位。请务必指定您的硬件支持的密钥长度。

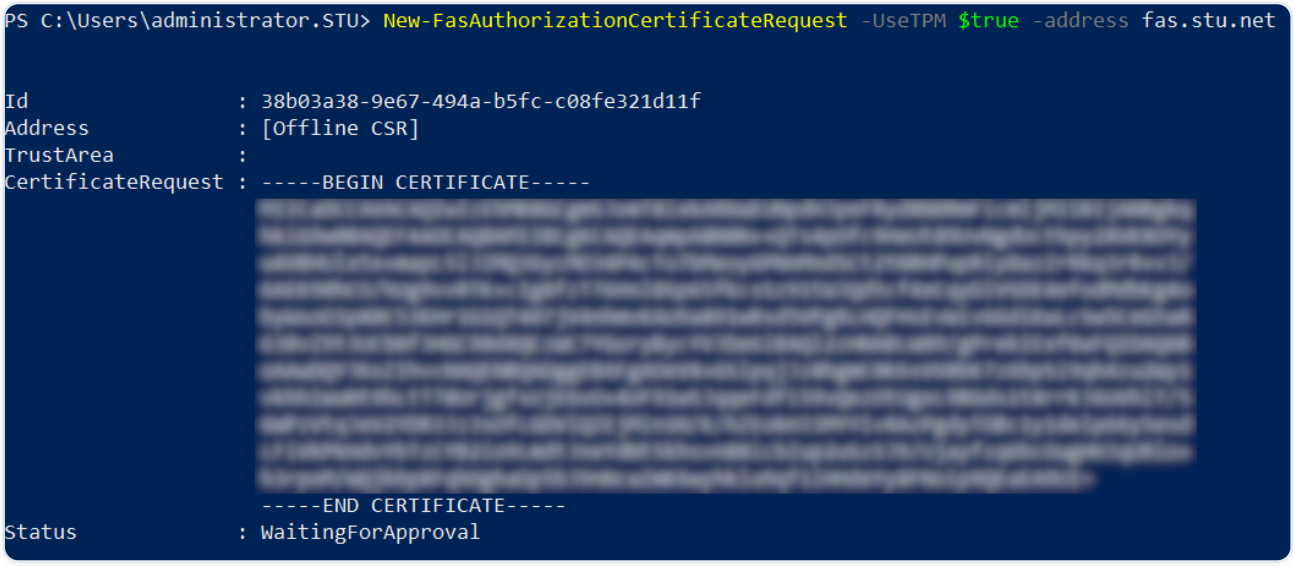
```
New-FasAuthorizationCertificateRequest -UseTPM $true -address \<FQDN of FAS Server>
```

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

例如：

```
New-FasAuthorizationCertificateRequest -UseTPM $true -address fashsm.auth.net
```

显示以下内容：

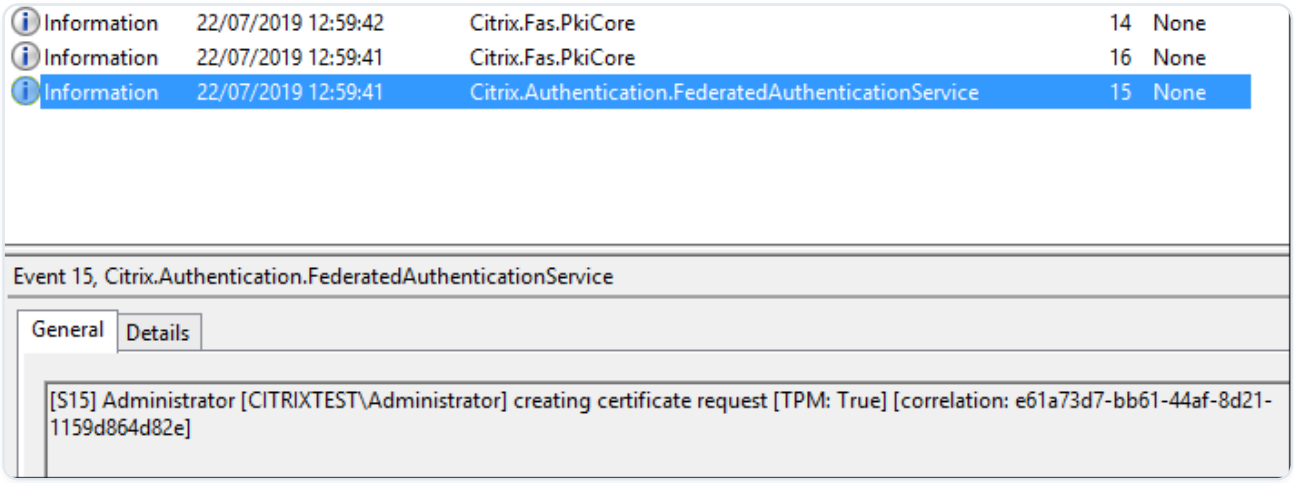


注意：

- ID GUID（在此示例中为“5ac3d8bd-b484-4ebe-abf8-4b2cfd62ca39”）在后续步骤中是必需的。
- 可将此 PowerShell cmdlet 视为一次性“覆盖”，用于生成注册机构证书的私钥。
- 运行此 cmdlet 时，将检查 FAS 启动时从配置文件中读取的值，以确定要使用的密钥长度（默认值为 2048）。
- 由于在此手动 PowerShell 启动的注册机构证书私钥操作中，-UseTPM 设置为 $true，因此系统将忽略文件中与使用 TPM 所需设置不匹配的值。
- 运行此 cmdlet 不会更改配置文件中的任何设置。
- 在后续自动 FAS 启动的用户证书私钥操作期间，将使用 FAS 启动时从文件中读取的值。
- 也可以在 FAS 服务器颁发用户证书以生成受 TPM 保护的用户证书私钥时，将配置文件中的 KeyProtection 值设置为 GenerateTPMProtectedKey。

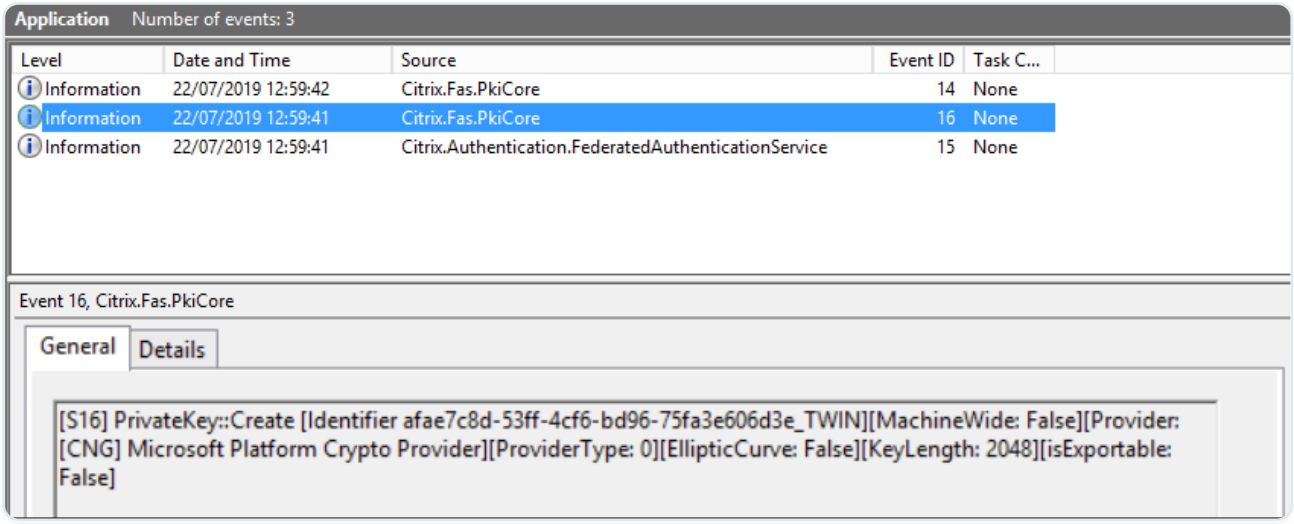
要验证是否使用 TPM 生成了密钥对，请在生成密钥对时，查看 FAS 服务器上 Windows 事件查看器中的应用程序日志。

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



注意： “”

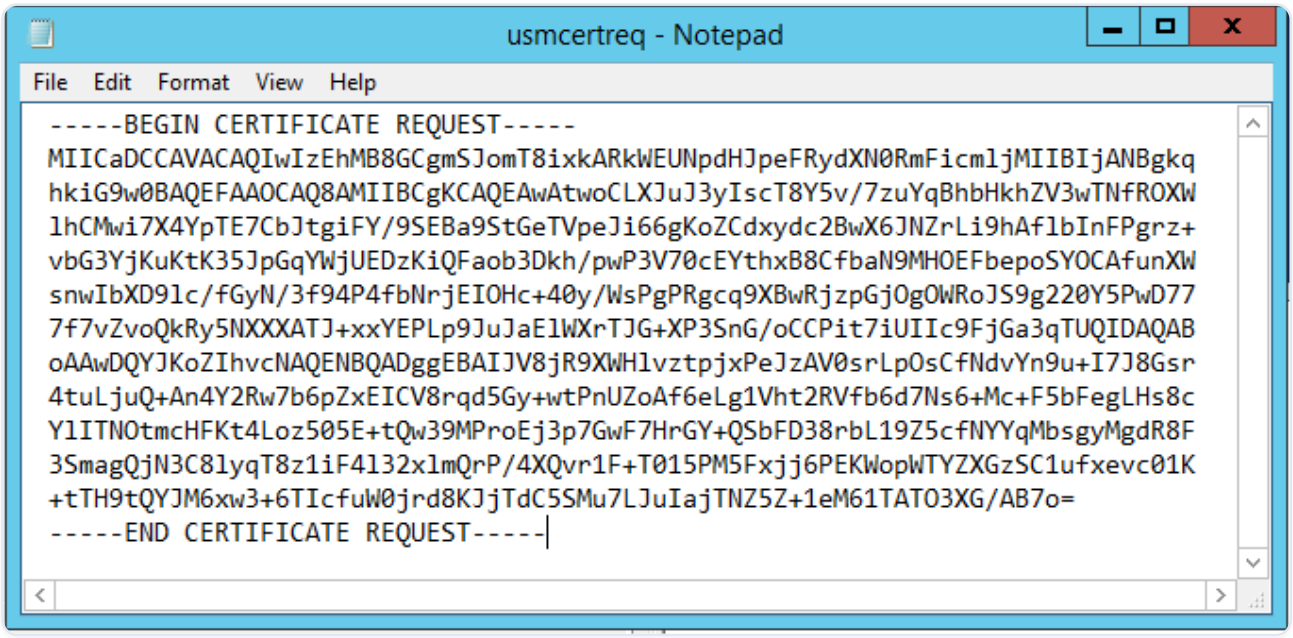
随后是：



注意： “提供程序： Microsoft Platform Crypto Provider”

步骤 6： 将证书请求部分复制到文本编辑器中，并将其保存到磁盘作为文本文件。

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



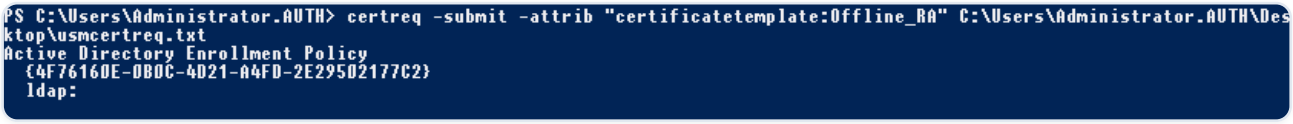
步骤 7： 通过在 FAS 服务器上的 PowerShell 中键入以下内容，将证书签名请求提交给您的证书颁发机构：

```
certreq -submit -attrib "certificatetemplate:\<certificate template from step 2>" \<certificate request file from step 6>
```

例如：

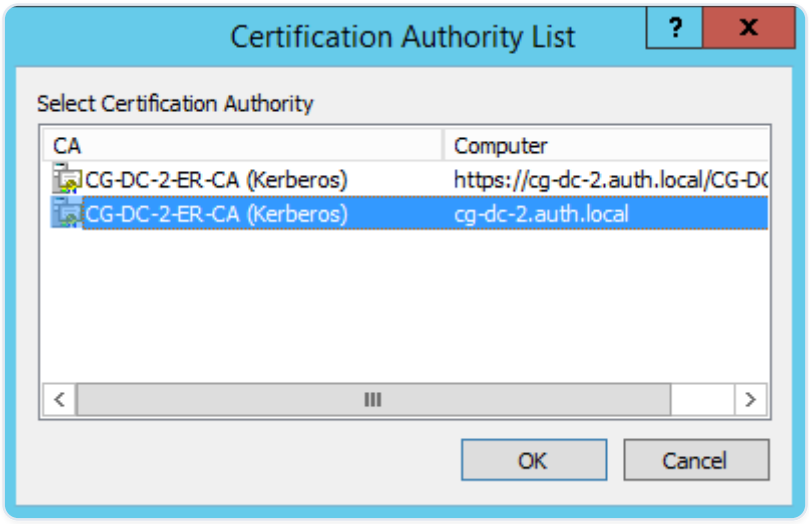
```
certreq -submit -attrib "certificatetemplate:Offline_RA" C:\Users\Administrator.AUTH\Desktop\usmcertreq.txt
```

显示以下内容：



此时可能会出现“证书颁发机构列表”窗口。此示例中的证书颁发机构同时启用了 HTTP（顶部）和 DCOM（底部）注册。如果可用，请选择 DCOM 选项：

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



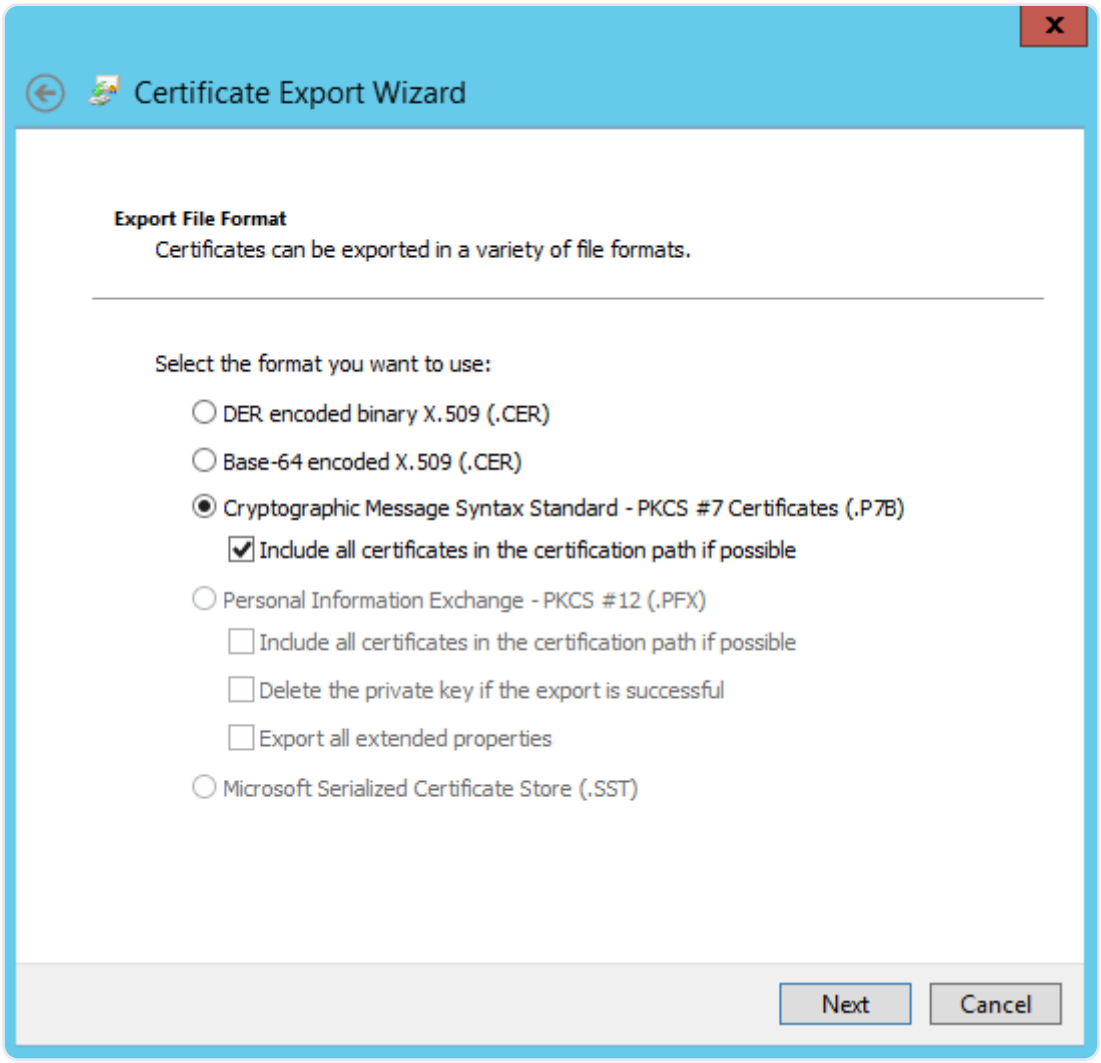
指定证书颁发机构后，PowerShell 将显示 RequestID：

```
PS C:\Users\Administrator.AUTH> certreq -submit -attrib "certificatetemplate:Offline_RA" C:\Users\Administrator.AUTH\Des
ktop\usmcertreq.txt
Active Directory Enrollment Policy
  {4F7616DE-0B0C-4D21-A4FD-2E29502177C2}
  ldap:
RequestId: 106
RequestId: "106"
Certificate request is pending: Taken Under Submission (0)
PS C:\Users\Administrator.AUTH>
```

步骤 8： 在证书颁发机构服务器上，在证书颁发机构 MMC 管理单元中，单击“**挂起的请求**”。记下请求 ID。然后右键单击该请求并选择“**颁发**”。

步骤 9： 选择“**已颁发的证书**”节点。找到刚刚颁发的证书（请求 ID 应匹配）。双击打开证书。选择“**详细信息**”选项卡。单击“**复制到文件**”。证书导出向导启动。单击“**下一步**”。为文件格式选择以下选项：

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



格式必须是“**加密消息语法标准 – PKCS #7 证书 (.P7B)**”，并且必须选中“**如果可能，包括证书路径中的所有证书**”。

步骤 10： 将导出的证书文件复制到 FAS 服务器上。

步骤 11： 通过在 FAS 服务器上输入以下 PowerShell cmdlet，将注册机构证书导入到 FAS 服务器中：

```
Import-FasAuthorizationCertificateResponse -address <FQDN of FAS server> -Id <ID
GUID from step 5> -Pkcs7CertificateFile <Certificate file from step 10>
```

例如：

```
Import-FasAuthorizationCertificateResponse -address fashsm.auth.net -Id 5ac3d8bd-
b484-4ebe-abf8-4b2cfd62ca39 -Pkcs7CertificateFile
C:\Users\Administrator.AUTH\Desktop\TPM_FAS_Cert.p7b
```

显示以下内容：

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

```
PS C:\Users\administrator.STU> Import-FasAuthorizationCertificateResponse -Address fas.stu.net -Id 74d427ff-c55b-4d6d-87
ae-1ff98b0c2705 -Pkcs7CertificateFile C:\Users\administrator.STU\Desktop\TPM_FAS_Cert.p7b

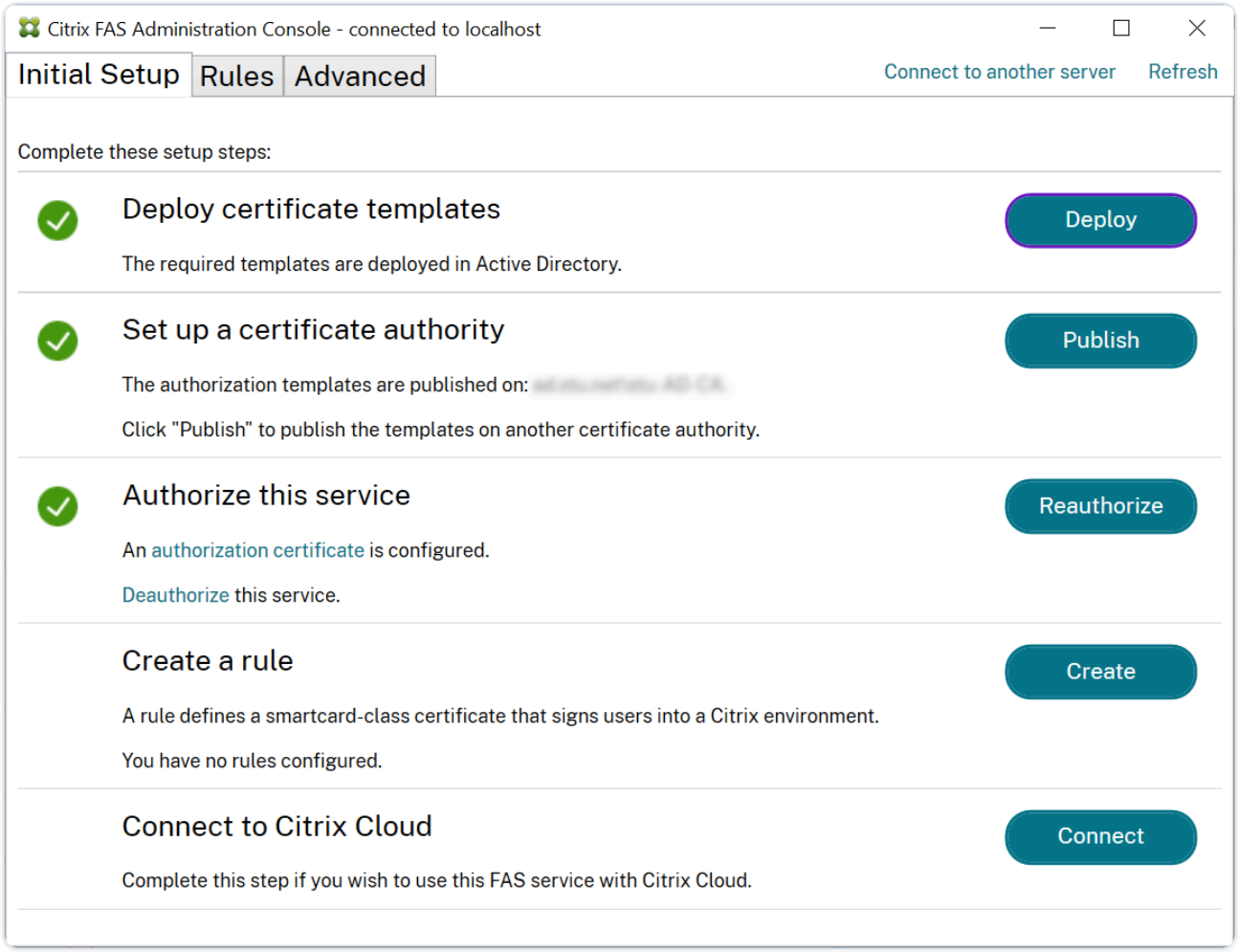

Id                : 74d427ff-c55b-4d6d-87ae-1ff98b0c2705
Address           : [Offline CSR]
TrustArea         : 978816cd-8b2f-4695-8c5d-08bb7df1816b
CertificateRequest :
Status            : Ok
```

要确认注册机构证书的私钥是否正确存储在 TPM 中，请使用以下 PowerShell 命令。如果注册机构证书的私钥存储在 TPM 中，则 PrivateKeyProvider 字段将设置为 *Microsoft Platform Crypto Provider*：

```
Add-PSSnapin Citrix.Authentication.FederatedAuthenticationService.V1

Get-FasAuthorizationCertificate -FullCertInfo -Address localhost
```

步骤 12： 关闭 FAS 管理控制台，然后重新启动它。



注意： “授权此服务”步骤有一个绿色勾号。

步骤 13： 在 FAS 管理控制台中选择“**规则**”选项卡，并编辑 (/zh-cn/federated-authentication-service/2402-ltsr/install-configure.html) 中所述的设置。

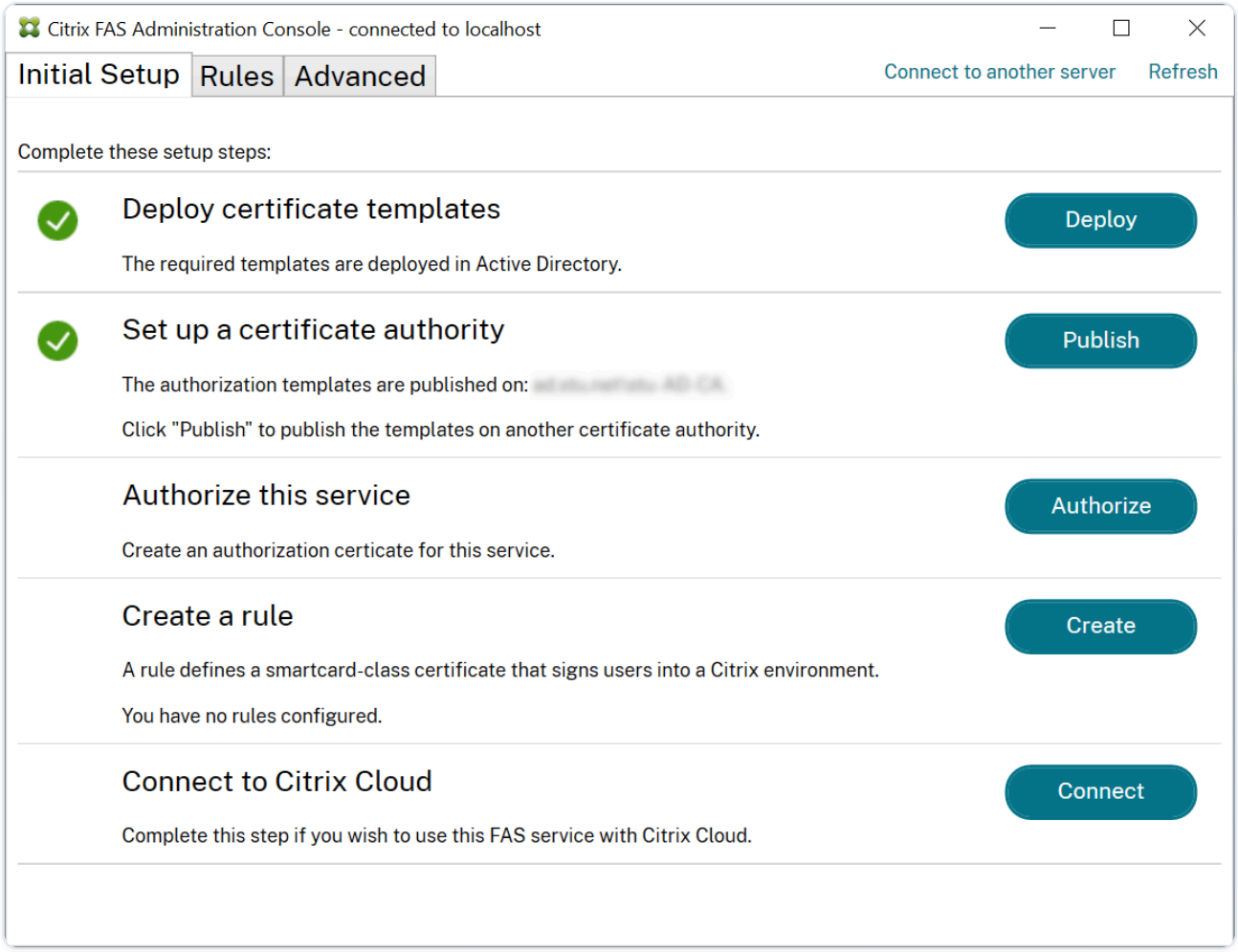
© 1997–2026 Citrix Systems, Inc. All rights reserved.

示例 3

此示例涵盖存储在 HSM 中的注册机构证书私钥和用户证书的私钥。此示例假定已配置 HSM。您的 HSM 将具有提供程序名称，例如“HSM_Vendor 的密钥存储提供程序”。

如果您计划在虚拟化环境中运行 FAS 服务器，请咨询您的 HSM 供应商以了解管理程序支持情况。

步骤 1. 在使用管理控制台进行 FAS 的初始设置期间，仅完成前两个步骤：“部署证书模板”和“设置证书颁发机构”。



步骤 2： 请查阅您的 HSM 供应商的文档，以确定您的 HSM 的 ProviderName 值应为何。如果您的 HSM 使用 CAPI，文档中可能会将提供程序称为加密服务提供程序 (CSP)。如果您的 HSM 使用 CNG，文档中可能会将提供程序称为密钥存储提供程序 (KSP)。

步骤 3： 如下编辑配置文件：

```
<add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderName"
value="HSM_Vendor's Key Storage Provider"/>
```

文件现在应如下所示：

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

```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <appSettings>
    <!-- This option switch between CAPI API  (true) and CNG API (false) Cryptographic Providers  -->
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderLegacyCsp" value="false"/>

    <!-- Specify the Cryptographic Service Provider (CSP) / Key Storage Provider (KSP) Name.  -->
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderName" value="HSM_Vendor's Key Storage Provider"/>

    <!-- Specify the Cryptographic Service Provider Type (only for CSP - not KSP).  For example: PROV_RSA_AES is 24  -->
    <!-- add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderType" value="24"/ -->

    <!-- Specify Private Key protection [NoProtection|GenerateNonExportableKey|GenerateTPMProtectedKey] -->
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.KeyProtection" value="GenerateNonExportableKey"/>

    <!-- Specify RSA Key length -->
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.KeyLength" value="2048"/>

    <!-- Logging: Event log Verbosity (0 Disabled, 1 Errors, 2 Warnings, 3 Informational) -->
    <!-- add key="Citrix.Authentication.UserCredentialService.SystemLog.LogLevel" value="3" / -->

    <!-- Logging: Event IDs to not log (comma separated) -->
    <!-- add key="Citrix.Authentication.UserCredentialService.SystemLog.Supress" value="" / -->

    <!-- Logging: Disable Key Management logs -->
    <!-- add key="Citrix.TrustFabric.Logging.SystemLog" value=""/ -->
  </appSettings>
<startup><supportedRuntime version="v4.0" sku=".NETFramework,Version=v4.5.1"/></startup></configuration>
```

此方案假定您的 HSM 使用 CNG，因此 ProviderLegacyCsp 值设置为 false。如果您的 HSM 使用 CAPI，则 ProviderLegacyCsp 值应设置为 true。请查阅您的 HSM 供应商文档，以确定您的 HSM 是使用 CAPI 还是 CNG。另请查阅您的 HSM 供应商文档，了解非对称 RSA 密钥生成支持的密钥长度。在此示例中，密钥长度设置为默认值 2048 位。请确保您指定的密钥长度受硬件支持。

步骤 4： 重新启动 Citrix Federated Authentication Service 以从配置文件中读取值。

步骤 5： 在 HSM 中生成 RSA 密钥对，并通过单击 FAS 管理控制台的**初始设置**选项卡中的**授权**来创建证书签名请求。

步骤 6： 要验证密钥对是否在 HSM 中生成，请检查 Windows 事件日志中的应用程序条目：

```
[S16] PrivateKey::Create [Identifier e1608812-6693-4c54-a937-91a2e27df75b_TWIN][MachineWide: False][Provider: [CNG] HSM_Vendor's Key Storage Provider][ProviderType: 0][EllipticCurve: False][KeyLength: 2048][isExportable: False]
```

注意：[提供程序： HSM 供应商的密钥存储提供程序]

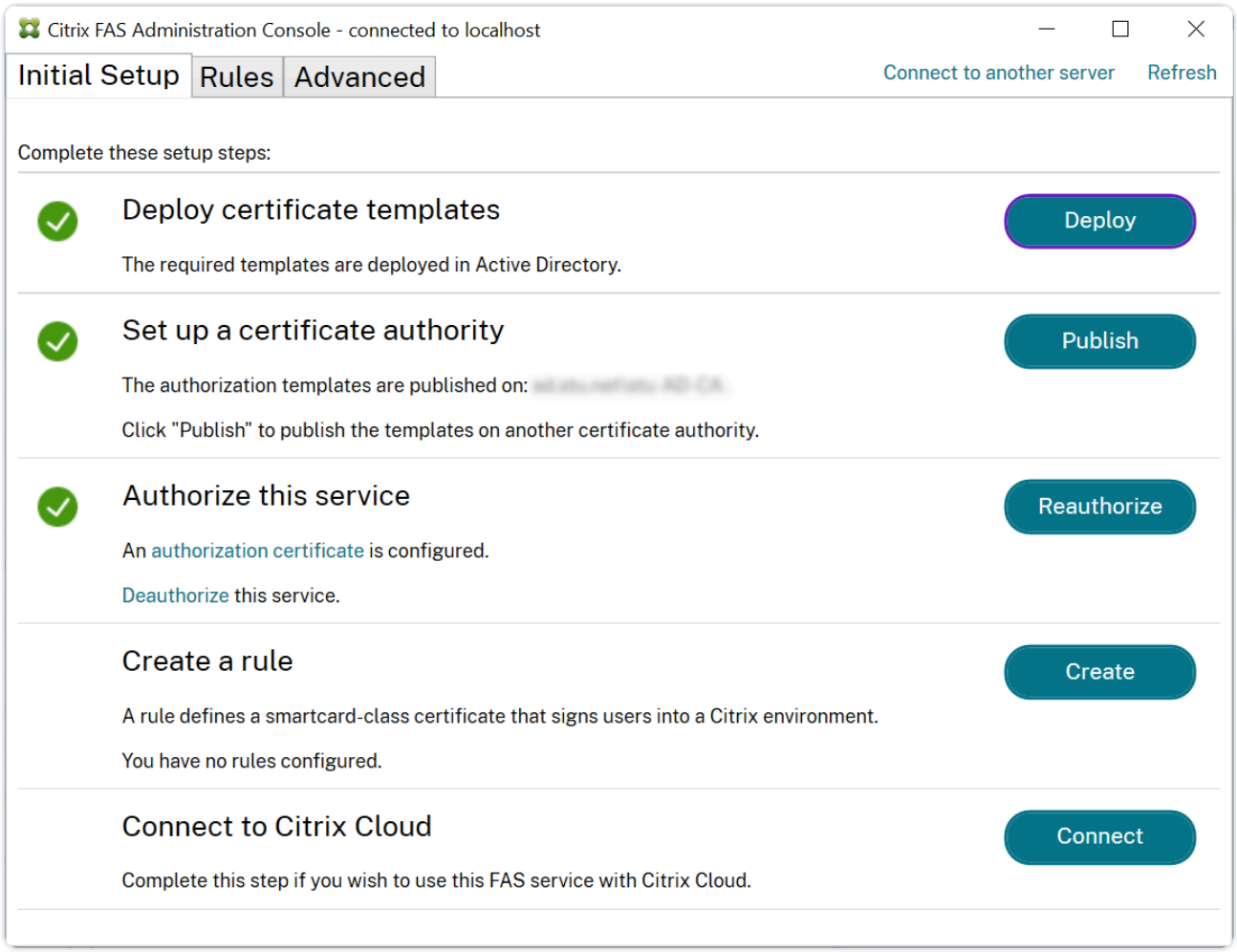
步骤 7： 在证书颁发机构服务器上，在证书颁发机构 MMC 中，选择**挂起请求**节点：

Request ID	Binary Request	Request Status Code	Request Disposition Message	Request Submission Date	Requester Name	Request Country/Region
107	-----BEGIN NE...	The operation compl...	Taken Under Submission	07/04/2016 14:04	AUTH\UCSHSM$	

右键单击该请求并选择**颁发**。

注意： “授权此服务”步骤带有绿色勾号。

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



步骤 8： 在 FAS 管理控制台中选择**规则**选项卡，并按照安装和配置中所述编辑设置。

FAS 证书存储

FAS 不使用 FAS 服务器上的 Microsoft 证书存储来存储其证书。它使用嵌入式数据库。

要确定注册机构证书的 GUID，请在 FAS 服务器上输入以下 PowerShell cmdlet：

```
Add-pssnapin Citrix.a&ast;
```

```
Get-FasAuthorizationCertificate –address \<FAS server FQDN>
```

例如，**Get-FasAuthorizationCertificate –address cg-fas-2.auth.net**：

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

```
PS C:\Users\administrator.STU> Get-FasAuthorizationCertificate -Address fas.stu.net


Id                : e3044634-6790-4de0-a8ee-d599bb047ad7
Address           : [Offline CSR]
TrustArea         :
CertificateRequest : -----BEGIN CERTIFICATE-----
                     [redacted]
                     -----END CERTIFICATE-----
Status            : WaitingForApproval


PS C:\Users\administrator.STU>
```

要获取用户证书列表，请输入：

```
Get-FasUserCertificate –address \<FAS server FQDN>
```

例如，**Get-FasUserCertificate –address cg-fas-2.auth.net**

```
PS C:\Users\administrator.STU> Get-FasUserCertificate -Address fas.stu.net


ThumbPrint            : 2A81185BBF8B696180F5FDE6FAC0FB8FBAEB99C5
UserPrincipalName     : stuart
Role                  : default
CertificateDefinition : default_Definition
SecurityContext       :
ExpiryDate            : 15/07/2021 16:34:50
```

注意：

使用 HSM 存储私钥时，HSM 容器通过 GUID 标识。可以使用以下方法获取 HSM 中私钥的 GUID：

```
Get-FasUserCertificate –address \<FAS server FQDN> -KeyInfo $true
```

例如：

```
Get-FasUserCertificate –address fas3.djwfas.net -KeyInfo $true
```

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

```
PS C:\Users\administrator> Get-FasUserCertificate -Address fas3.djwfas.net -KeyInfo $true


PrivateKeyIdentifier  : 38405c4d-63af-43e4-9135-2412246b1112
PrivateKeyProvider    : Microsoft Software Key Storage Provider
PrivateKeyIsCng       : True
ThumbPrint            : AD2441F050A02966AA4DB190BA084976528DB667
UserPrincipalName     : joe@djwfas.net
Role                  : default
CertificateDefinition : default_Definition
SecurityContext       :
ExpiryDate            : 19/01/2018 09:18:48
```

相关信息

- (/zh-cn/federated-authentication-service/2402-ltsr/install-configure.html) 是 FAS 安装和配置的主要参考资料。
- 常见的 FAS 部署在 (/zh-cn/federated-authentication-service/2402-ltsr/deployment-architectures.html) 文章中进行了总结。
- 其他“操作方法”文章在 (/zh-cn/federated-authentication-service/2402-ltsr/config-manage.html) 文章中介绍。

安全和网络配置

联合身份验证服务 (FAS) 与 Microsoft Active Directory 和 Microsoft 证书颁发机构紧密集成。请确保系统得到适当的管理和保护，并像为域控制器或其他关键基础结构开发安全策略一样，为 FAS 开发安全策略。

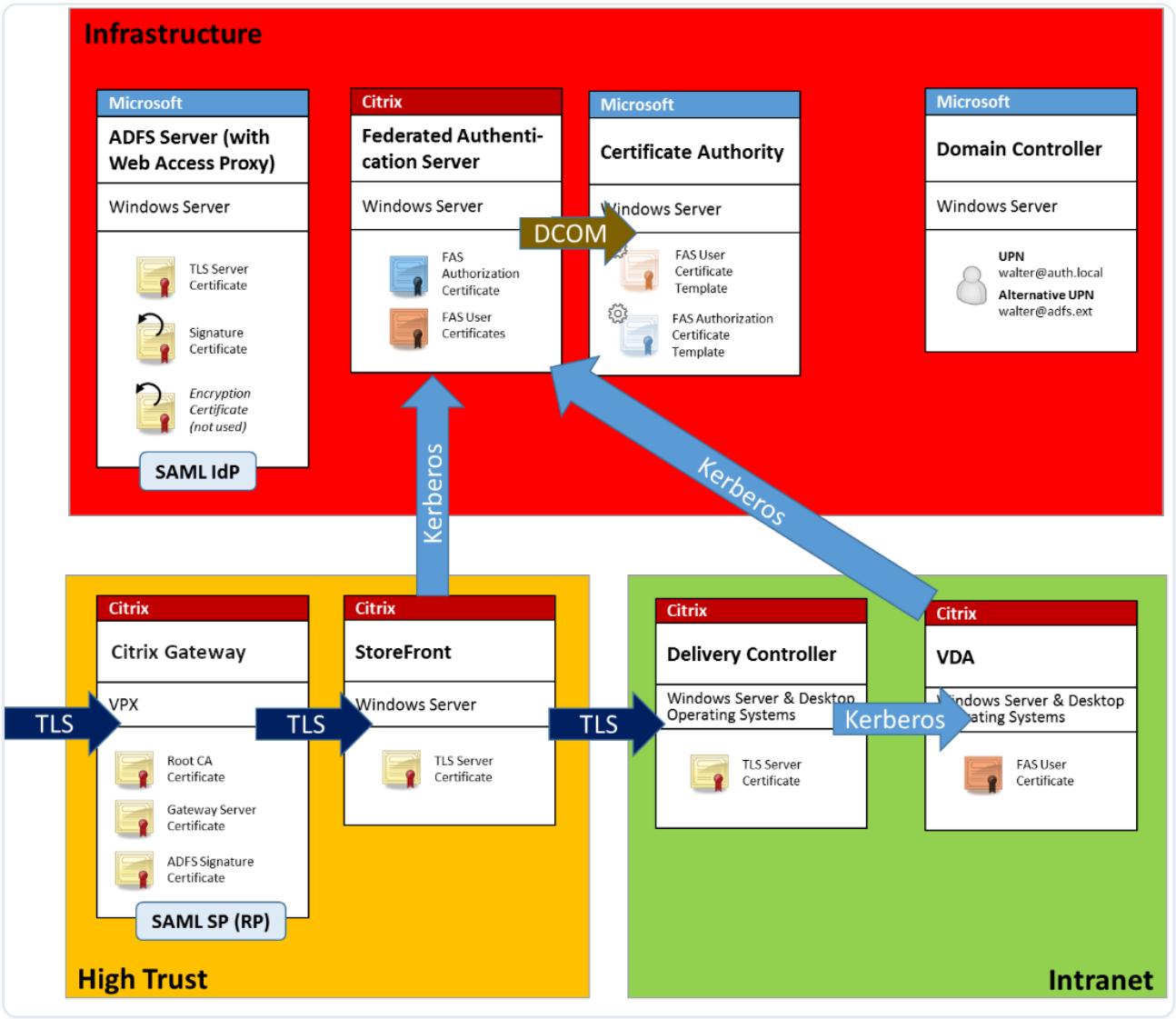
本文档概述了部署 FAS 时需要考虑的安全问题。它还概述了可用于帮助保护基础结构的功能。

网络体系结构

下图显示了 FAS 部署中使用的主要组件和安全边界。

FAS 服务器是安全关键型基础结构的一部分，与证书颁发机构和域控制器一起。在联合环境中，Citrix Gateway 和 Citrix StoreFront 是执行用户身份验证的组件。引入 FAS 不会影响其他 Citrix Virtual Apps and Desktops™ 组件。

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



防火墙和网络安全

端口 443 上的 TLS 保护 Citrix Gateway、StoreFront 和 Delivery Controller™ 组件之间的通信。StoreFront 服务器仅执行出站连接，Citrix Gateway 仅通过 Internet 使用 HTTPS 端口 443 接受连接。

StoreFront 服务器通过端口 80 使用相互身份验证的 Kerberos 联系 FAS 服务器。身份验证使用 FAS 服务器的 Kerberos HOST/fqdn 身份和 StoreFront 服务器的 Kerberos 计算机帐户身份。此身份验证方法生成 Citrix Virtual Delivery Agent (VDA) 登录用户所需的一次性“凭据句柄”。

当 HDX 会话连接到 VDA 时，VDA 也会通过端口 80 联系 FAS 服务器。身份验证使用 FAS 服务器的 Kerberos HOST/fqdn 身份和 VDA 的 Kerberos 计算机身份。此外，VDA 必须提供“凭据句柄”才能访问证书和私钥。

Microsoft 证书颁发机构接受使用 Kerberos 身份验证的 DCOM 进行通信，DCOM 可以配置为使用固定 TCP 端口。证书颁发机构要求 FAS 服务器提供由受信任的注册代理证书签名的 CMC 数据包。

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

服务器	防火墙端口
联合身份验证服务	[in] 来自 StoreFront™ 和 VDA 的 Kerberos over HTTP，[out] 到 Microsoft 证书颁发机构的 DCOM
思杰网关	[in] 来自客户端计算机的 HTTPS，[in/out] 到/来自 StoreFront 服务器的 HTTPS，[out] 到 VDA 的 HDX
StoreFront	[in] 来自 Citrix Gateway 的 HTTPS，[out] 到 Delivery Controller 的 HTTPS，[out] 到 FAS 的 Kerberos HTTP
交付控制器	[in] 来自 StoreFront 服务器的 HTTPS，[in/out] 来自 VDA 的 Kerberos over HTTP
VDA	[in/out] 来自交付控制器的 Kerberos over HTTP，[in] 来自思杰网关的 HDX，[out] 到 FAS 的 Kerberos HTTP
Microsoft 证书颁发机构	[in] 来自 FAS 的 DCOM 和签名

思杰联合身份验证服务与思杰云™ 之间的连接

控制台和 FAS 分别使用用户帐户和网络服务帐户访问以下地址。

- FAS 管理控制台，在用户帐户下
  - `*.cloud.com`
  - `*.citrixworkspacesapi.net`
  - 如果您的环境中使用第三方身份提供商，则需要其地址
- FAS 服务，在网络服务帐户下：
  - `*.citrixworkspacesapi.net`
  - `*.citrixnetworkapi.net`

如果您的环境包含代理服务器，请使用 FAS 管理控制台的地址配置用户代理。此外，请确保使用 netsh 或类似工具配置网络服务帐户的地址。

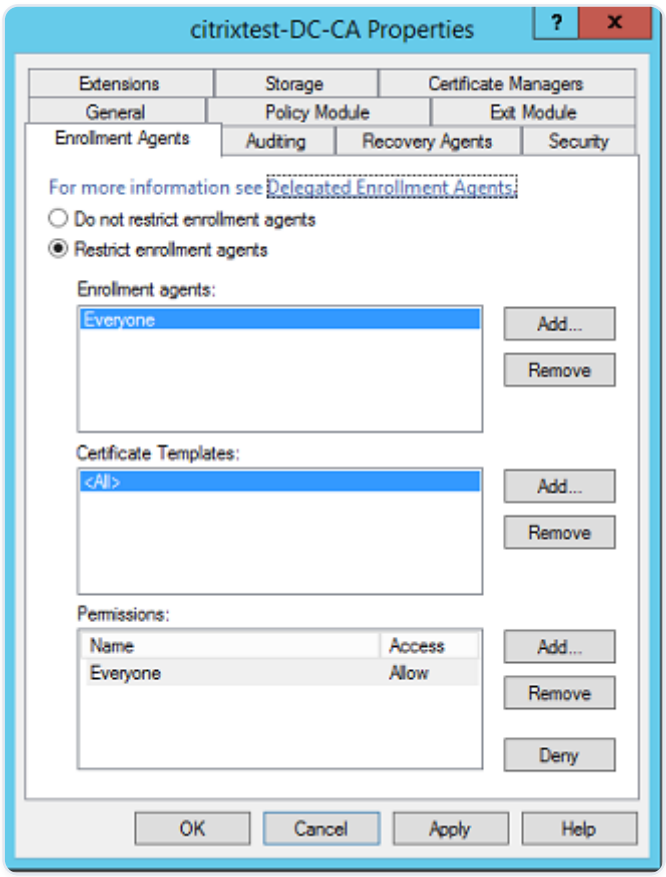
© 1997–2026 Citrix Systems, Inc. All rights reserved.

安全注意事项

FAS 具有注册机构证书，允许其为您的域用户自主颁发证书。这有助于制定和实施安全策略，以保护 FAS 服务器并限制其权限。

委派的注册代理

FAS 通过充当注册代理来颁发用户证书。Microsoft 证书颁发机构允许您限制注册代理、证书模板以及注册代理可以为其颁发证书的用户。



您可以使用给定对话框确保：

- *注册代理*列表仅包含 FAS 服务器。
- *证书模板*列表仅包含 FAS 模板。
- *权限*列表包含允许使用 FAS 的用户。例如，建议不要向管理员或受保护用户组颁发证书。

访问控制列表配置

如配置规则部分所述，您必须配置 StoreFront 服务器列表。颁发证书时，这些 StoreFront 服务器会向 FAS 断言用户身份。同样，您可以限制哪些用户将获得证书，以及他们可以向哪些 VDA 计算机进行身份验证。此功能是对您配置的任何标准 Active Directory 或证书颁发机构安全功能的补充。

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

防火墙设置

所有与 FAS 服务器的通信都使用通过端口 80 的相互认证的 Windows Communication Foundation (WCF) Kerberos 网络连接。

事件日志监控

FAS 和 VDA 会将信息写入 Windows 事件日志。此日志可用于监视和审计信息。事件日志部分列出了可能生成的事件日志条目。

硬件安全模块

所有私钥（包括 FAS 颁发的用户证书密钥）都由网络服务帐户存储为不可导出的私钥。如果您的安全策略要求，FAS 支持使用加密硬件安全模块。

低级别加密配置可在 FederatedAuthenticationService.exe.config 文件中找到。这些设置在首次创建私钥时应用。因此，注册机构私钥（例如，4096 位，TPM 保护）和运行时用户证书可以使用不同的设置。

参数	说明
ProviderLegacyCsp	设置为 true 时，FAS 使用 Microsoft CryptoAPI (CAPI)。否则，FAS 使用 Microsoft Cryptography Next Generation API (CNG)。
ProviderName	要使用的 CAPI 或 CNG 提供程序的名称。
提供程序类型	指 Microsoft KeyContainerPermissionAccessEntry.ProviderType 属性 PROV_RSA_AES 24。除非您使用带有 CAPI 的 HSM 且 HSM 供应商另有规定，否则此值必须始终为 24。
密钥保护	控制私钥的“可导出”标志。如果硬件支持，还允许使用可信平台模块 (TPM) 密钥存储。
密钥长度	RSA 私钥的密钥长度。支持的值为 1024、2048 和 4096（默认值：2048）。

管理职责

环境管理可分为以下几组：

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

名称	职责
企业管理员	在林中安装并保护证书模板
域管理员	配置组策略设置
证书颁发机构管理员	配置证书颁发机构
FAS 管理员	安装和配置 FAS 服务器
StoreFront/Citrix Gateway 管理员	配置用户身份验证
Citrix 虚拟桌面™ 管理员	配置 VDA 和控制器

每位管理员控制整体安全模型的不同方面，从而实现深度防御方法来保护系统。

组策略设置

信任的 FAS 计算机通过组策略配置的“索引号 -> FQDN”查找表进行标识。当联系 FAS 服务器时，客户端会验证 FAS 服务器的 `HOST\<fqdn>` Kerberos 身份。所有访问 FAS 服务器的服务器必须对同一索引具有相同的 FQDN 配置；否则，StoreFront 和 VDA 可能会联系不同的 FAS 服务器。

Citrix 建议对环境中的所有计算机应用单个策略，以避免配置错误。修改 FAS 服务器列表时请务必小心，尤其是在删除或重新排序条目时。

此 GPO 的控制权必须仅限于安装和停用 FAS 服务器的 FAS 管理员（和/或域管理员）。请注意避免在停用 FAS 服务器后不久重复使用计算机 FQDN 名称。

证书模板

如果您不想使用 FAS 随附的 Citrix_SmartcardLogon 证书模板，可以修改其副本。支持以下修改。

重命名证书模板

如果您想将 Citrix_SmartcardLogon 重命名以符合您的组织模板命名标准，则必须：

- 创建证书模板的副本，并将其重命名以符合您的组织模板命名标准。
- 使用 FAS PowerShell 命令管理 FAS，而不是使用管理用户界面。（管理用户界面仅适用于 Citrix 默认模板名称。）
    - 使用 Microsoft MMC 证书模板管理单元或 Publish-FasMsTemplate 命令发布您的模板，并且
    - 使用 New-FasCertificateDefinition 命令配置 FAS，并指定您的模板名称。

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

修改常规属性

默认情况下，用户证书的有效期为七天。您可以在证书模板中修改有效期。

请勿修改续订期限。FAS 会忽略证书模板中的此设置。FAS 会在其有效期过半时自动续订证书。

修改请求处理属性

请勿修改这些属性。FAS 会忽略证书模板中的这些设置。FAS 始终取消选择 **允许导出私钥** 并取消选择 **使用相同密钥续订**。

修改加密属性

请勿修改这些属性。FAS 会忽略证书模板中的这些设置。

有关 FAS 提供的等效设置，请参阅 私钥保护。

修改密钥证明属性

请勿修改这些属性。FAS 不支持密钥证明。

修改已取代模板属性

请勿修改这些属性。FAS 不支持取代模板。

修改扩展属性

您可以修改这些设置以符合您的组织策略。

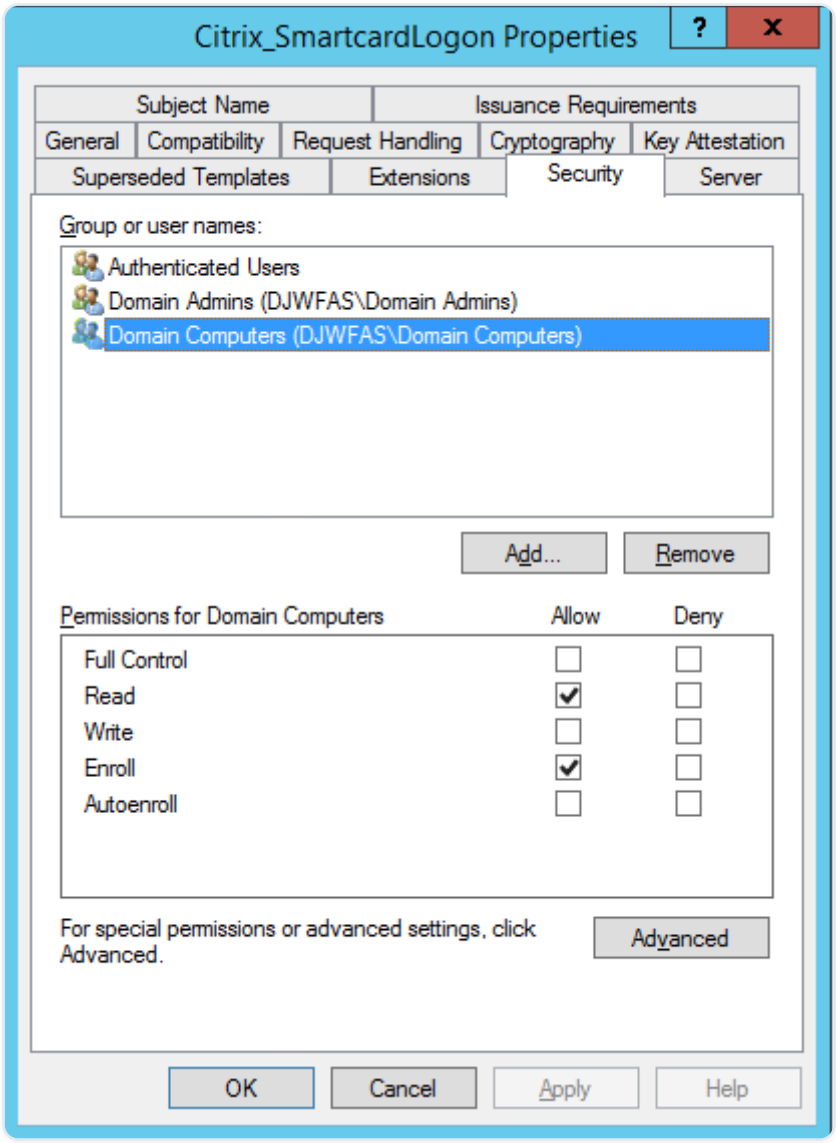
注意：不当的扩展设置可能会导致安全问题，或导致证书无法使用。

修改安全属性

Citrix 建议您修改这些设置，仅允许 FAS 服务器的计算机帐户拥有 **读取** 和 **注册** 权限。FAS 服务不需要任何其他权限。但是，与其他证书模板一样，您可以：

- 允许管理员读取或写入模板
- 允许经过身份验证的用户读取模板

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



修改主题名称属性

Citrix 建议您不要修改这些属性。

该模板已选择 *从此 Active Directory 信息构建*，这会导致证书颁发机构在证书扩展中包含用户的 SID，从而提供与用户 Active Directory 帐户的强映射。

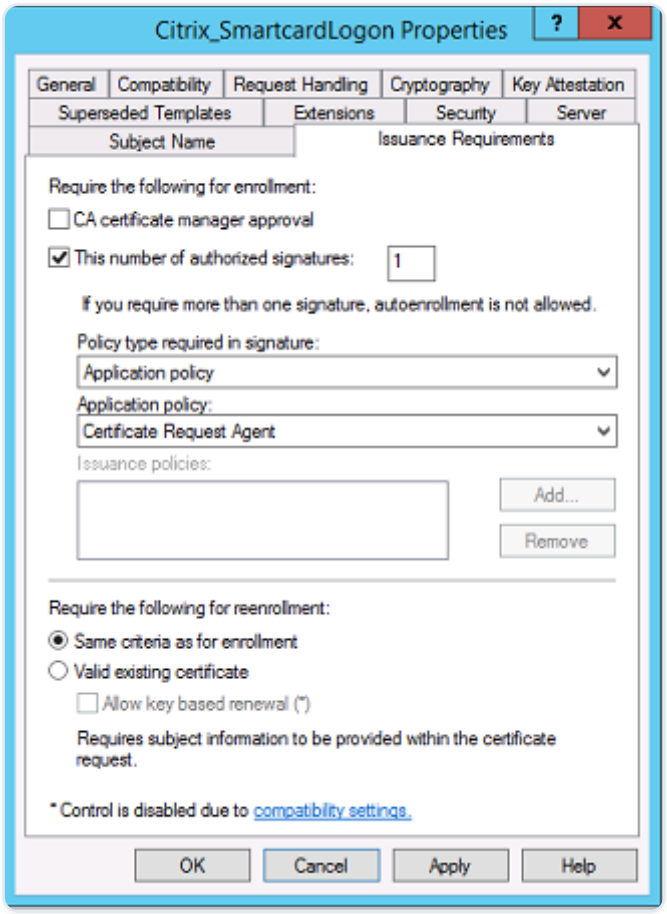
修改服务器属性

尽管 Citrix 不建议这样做，但如果需要，您可以修改这些设置以符合您的组织策略。

修改颁发要求属性

请勿修改这些设置。这些设置必须如下所示：

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



修改兼容性属性

您可以修改这些设置。该设置必须至少为 **Windows Server 2003 CA**（架构版本 2）。但是，FAS 仅支持 Windows Server 2008 及更高版本的 CA。此外，如上所述，FAS 会忽略通过选择 **Windows Server 2008 CA**（架构版本 3）或 **Windows Server 2012 CA**（架构版本 4）而提供的其他设置。

证书颁发机构管理

证书颁发机构管理员负责配置证书颁发机构服务器及其使用的颁发证书私钥。

发布模板

证书颁发机构若要根据企业管理员提供的模板颁发证书，证书颁发机构管理员必须选择发布该模板。

一种简单的安全做法是，在安装 FAS 服务器时仅发布注册机构证书模板，或者坚持完全脱机颁发过程。无论哪种情况，证书颁发机构管理员都必须完全控制注册机构证书请求的授权，并制定授权 FAS 服务器的策略。

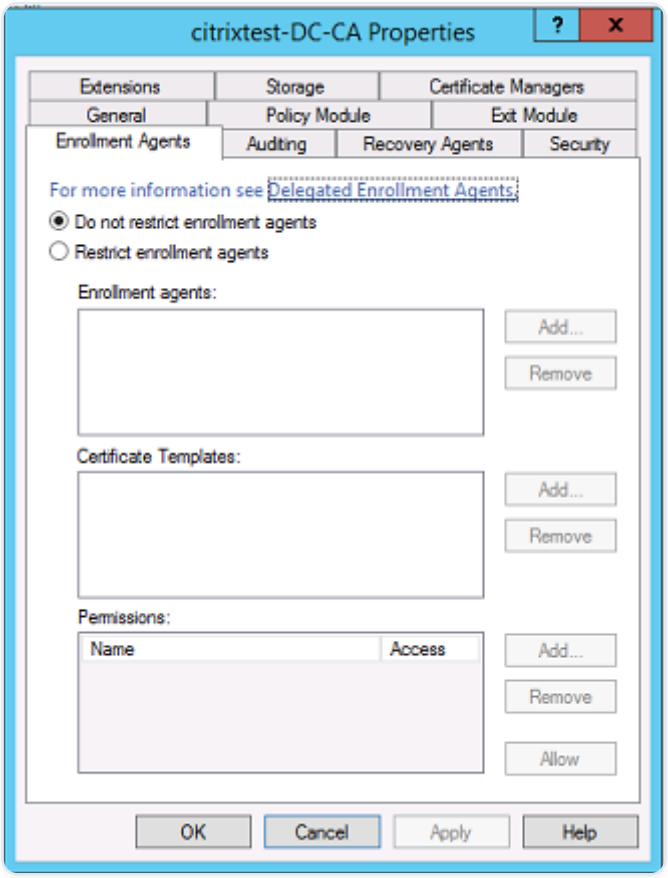
防火墙设置

证书颁发机构管理员控制证书颁发机构的网络防火墙设置，从而控制传入连接。证书颁发机构管理员可以配置 DCOM TCP 和防火墙规则，以便只有 FAS 服务器才能请求证书。

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

受限注册

默认情况下，任何注册机构证书的持有者都可以使用允许访问的任何证书模板向任何用户颁发证书。此证书颁发必须使用“限制注册代理”证书颁发机构属性限制为一组非特权用户。



策略模块和审计

对于高级部署，可以使用自定义安全模块来跟踪和否决证书颁发。

FAS 管理

FAS 具有多项安全功能。

通过 ACL 限制 StoreFront、用户和 VDA

FAS 安全模型的核心是控制哪些 Kerberos 帐户可以访问功能：

访问向量	描述
StoreFront [IdP]	这些 Kerberos 帐户受信任，可声明用户已正确通过身份验证。如果其中一个帐户遭到入侵，则可以为 FAS 配置允许的用户创建和使用证书。

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

访问向量	描述
VDA [Relying party]	这些是允许访问证书和私钥的计算机。还需要 IdP 检索的凭据句柄，因此此组中受损的 VDA 帐户对攻击系统的范围有限。
用户	此选项控制 IdP 可以断言哪些用户。请注意，这与证书颁发机构的“受限注册代理”配置选项存在重叠。通常，建议在此列表中仅包含非特权帐户。这可以防止受损的 StoreFront 帐户将权限提升到更高的管理级别。特别是，此 ACL 不得允许域管理员帐户。

配置规则

如果多个独立的 Citrix Virtual Apps™ 或 Citrix Virtual Desktops 部署使用相同的 FAS 服务器基础结构，则规则很有用。每条规则都有一组独立的配置选项；特别是，Kerberos 访问控制列表 (ACL) 可以独立配置。

配置证书颁发机构和模板

不同的证书模板和 CA 可以针对不同的访问权限进行配置。高级配置可以选择使用功能较弱或较强的证书，具体取决于环境。例如，被识别为“外部”的用户可以拥有比“内部”用户权限更少的证书。

会话内和身份验证证书

FAS 管理员可以控制用于身份验证的证书在用户会话中是否可用。 例如，用户在会话中只能使用“签名”证书，而功能更强大的“登录”证书仅在登录时使用。

私钥保护和密钥长度

FAS 管理员可以将 FAS 配置为将私钥存储在硬件安全模块 (HSM) 或可信平台模块 (TPM) 中。Citrix 建议至少通过将注册机构证书私钥存储在 TPM 中来保护它。FAS 提供了将私钥作为“脱机”证书请求过程的一部分保存到 TPM 中的选项。

同样，用户证书私钥可以存储在 TPM 或 HSM 中。所有密钥都必须生成为“不可导出”并且长度至少为 2048 位。

事件日志

FAS 服务器提供详细的配置和运行时事件日志，可用于审计和入侵检测。

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

管理访问和管理工具

FAS 包括远程管理功能（相互身份验证的 Kerberos）和工具。“本地管理员组”的成员对 FAS 配置拥有完全控制权。必须妥善维护 FAS 配置。

Citrix 虚拟应用、Citrix 虚拟桌面和 VDA 管理员

FAS 的使用不会改变 Delivery Controller 和 VDA 管理员的安全模型，因为 FAS“凭据句柄”只是取代了“Active Directory 密码”。Controller 和 VDA 管理组必须只包含受信任的用户。必须维护审计和事件日志。

常规 Windows 服务器安全性

所有服务器都必须完全打上补丁，并配备标准防火墙和防病毒软件。安全关键型基础结构服务器必须保存在物理安全的位置，并注意磁盘加密和虚拟机维护选项。

审计和事件日志必须安全地存储在远程计算机上。

RDP 访问必须仅限于授权管理员。Citrix 建议为用户帐户使用智能卡登录，尤其是对于证书颁发机构和域管理员帐户。

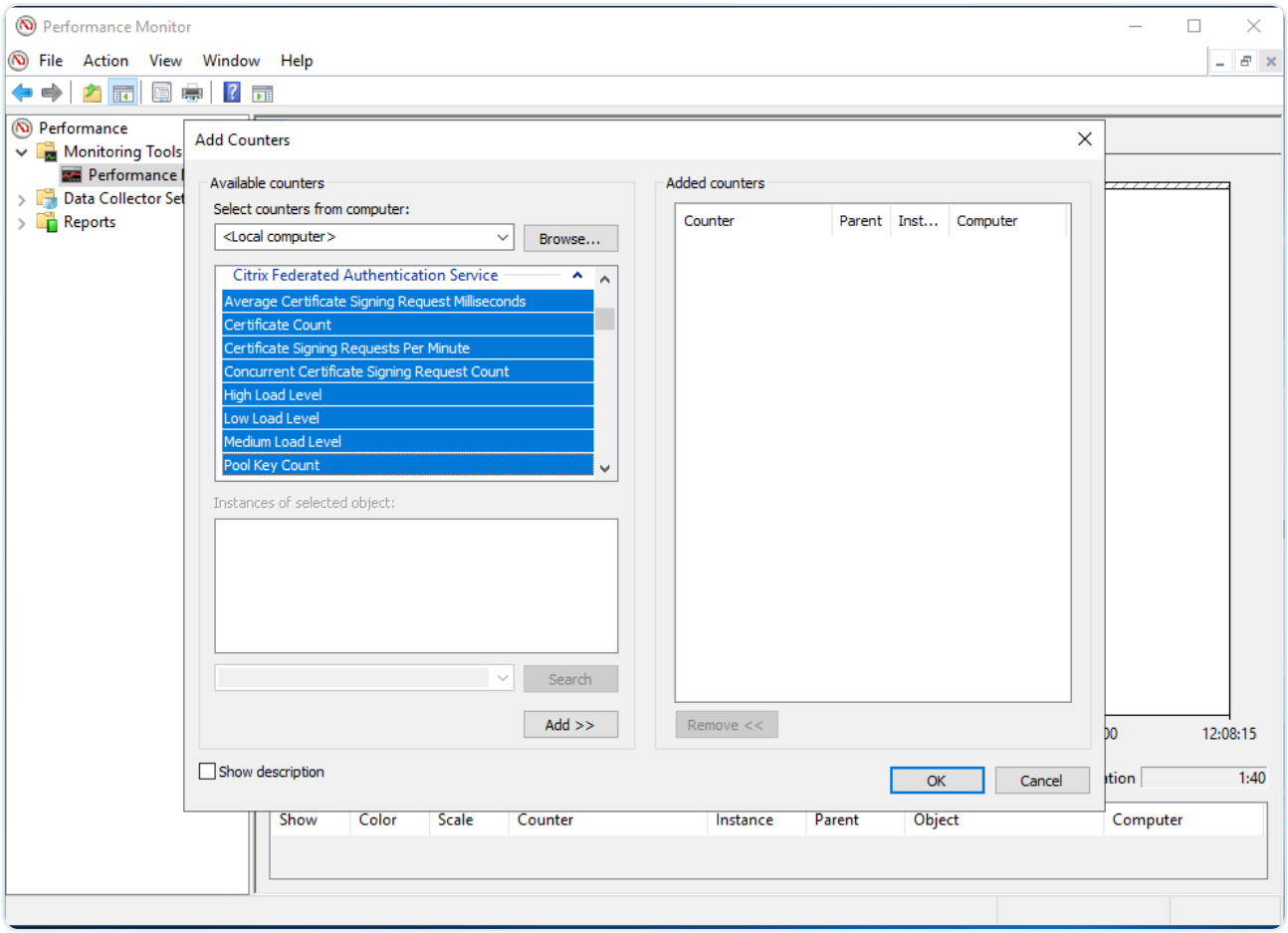
相关信息

- 安装和配置 是 FAS 安装和配置的主要参考。
- FAS 体系结构在 部署体系结构 文章中介绍。
- 其他“操作方法”文章在 高级配置 文章中介绍。

性能计数器

FAS 包含一组用于负载跟踪的性能计数器。

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



下表列出了可用的计数器。除非另有说明，否则每个计数器每 10 秒更新一次。

名称	描述
平均证书签名请求毫秒数	证书签名请求的平均持续时间（以毫秒为单位），使用前一分钟的数据计算。
证书计数	由联合身份验证服务管理的证书数量。
每分钟证书签名请求数	联合身份验证服务每分钟发出的证书签名请求数，使用前一分钟的数据计算。
并发证书签名请求计数	联合身份验证服务正在处理的并发证书签名请求数。
池密钥计数	密钥池中可用于证书签名请求的预生成密钥对的数量。
每分钟私钥操作数	联合身份验证服务每分钟执行的证书私钥操作数，使用前一分钟的数据计算。
会话计数	联合身份验证服务正在跟踪的 VDA 会话数。

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

名称	描述
低/中/高负载级别	联合身份验证服务每分钟可接受的证书签名请求负载的估计值。这些估计值每分钟更新一次，使用前一分钟的数据。超过“高负载”阈值可能会导致已发布的应用程序或桌面启动失败。

故障排除 Windows 登录问题

本文介绍了当用户使用证书或智能卡（或两者）登录时 Windows 提供的日志和错误消息。这些日志提供的信息可用于排查身份验证失败问题。

证书和公钥基础结构

Windows Active Directory 维护多个证书存储，用于管理登录用户的证书。

- **NTAuth 证书存储**：要向 Windows 进行身份验证，立即颁发用户证书的证书颁发机构（即不支持链式）必须放置在 NTAuth 存储中。要查看这些证书，请从 certutil 程序中输入：`certutil –viewstore –enterprise NTAuth`
- **根证书和中间证书存储：**通常，证书登录系统只能提供单个证书，因此如果正在使用链，则所有计算机上的中间证书存储必须包含这些证书。根证书必须在受信任的根存储中，倒数第二个证书必须在 NTAuth 存储中。
- **登录证书扩展和组策略：**Windows 可以配置为强制验证 EKU 和其他证书策略。请参阅 Microsoft 文档：`<https://docs.microsoft.com/zh-cn/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/ff404287(v=ws.10)>`。

注册表策略	描述
AllowCertificatesWithNoEKU	禁用时，证书必须包含智能卡登录扩展密钥用法 (EKU)。
AllowSignatureOnlyKeys	默认情况下，Windows 会筛选掉不允许 RSA 解密的证书私钥。此选项会覆盖该筛选器。
AllowTimeInvalidCertificates	默认情况下，Windows 会筛选掉过期的证书。此选项会覆盖该筛选器。
EnumerateECCCerts	启用椭圆曲线身份验证。

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

注册表策略	描述
需要X509提示	如果证书不包含唯一的“用户主体名称 (UPN)”，或者该名称不明确，此选项允许用户手动指定其 Windows 登录帐户。
UseCachedCRLOnlyAnd, IgnoreRevocationUnknownErrors	禁用吊销检查（在域控制器上设置）。

- **域控制器证书**：为了验证 Kerberos 连接，所有服务器都必须具有相应的“域控制器”证书。可以使用“本地计算机证书个人存储”MMC 管理单元菜单请求这些证书。

UPN 名称和证书映射

建议用户证书在主题备用名称扩展中包含唯一的“用户主体名称 (UPN)”。

Active Directory 中的 UPN 名称

默认情况下，Active Directory 中的每个用户都具有基于模式 \<samUsername>@\<domainNetBios> 和 \<samUsername>@\<domainFQDN> 的隐式 UPN。可用的域和 FQDN 包含在林的 RootDSE 条目中。单个域可以在 RootDSE 中注册多个 FQDN 地址。

此外，Active Directory 中的每个用户都具有显式 UPN 和 altUserPrincipalNames。这些是指定用户 UPN 的 LDAP 条目。

通过 UPN 搜索用户时，Windows 首先在当前域（基于查找 UPN 的进程的标识）中查找显式 UPN，然后查找备用 UPN。如果没有匹配项，它会查找隐式 UPN，这可能会解析为林中的不同域。

证书映射服务

如果证书不包含显式 UPN，Active Directory 可以选择在“x509certificate”属性中为每个用途存储一个精确的公共证书。要将此类证书解析为用户，计算机可以直接查询此属性（默认情况下，在单个域中）。

提供了一个选项，用户可以指定一个用户帐户，以加快此搜索速度，并且还允许在跨域环境中使用此功能。

如果林中存在多个域，并且用户未明确指定域，则 Active Directory rootDSE 会指定证书映射服务的位置。该服务位于全局编录计算机上，并具有林中所有 x509 证书属性的缓存视图。此计算机可用于仅根据证书在任何域中高效查找用户帐户。

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

控制登录域控制器选择

当环境包含多个域控制器时，了解并限制用于身份验证的域控制器很有用，以便可以启用和检索日志。

控制域控制器选择

要强制 Windows 使用特定的 Windows 域控制器进行登录，您可以通过配置 lmhosts 文件来明确设置 Windows 计算机使用的域控制器列表：\Windows\System32\drivers\etc\lmhosts。

该位置通常有一个名为“lmhosts.sam”的示例文件。只需包含一行：

1.2.3.4 dcnetbiosname #PRE #DOM:mydomai

其中“1.2.3.4”是“mydomain”域中名为“dcnetbiosname”的域控制器的 IP 地址。

重启后，Windows 计算机将使用该信息登录到 mydomain。调试完成后必须恢复此配置。

识别正在使用的域控制器

登录时，Windows 会设置一个 MSDOS 环境变量，其中包含登录用户的域控制器。要查看此信息，请使用命令 **echo %LOGONSERVER%** 启动命令提示符。

与身份验证相关的日志存储在此命令返回的计算机上。

启用帐户审核事件

默认情况下，Windows 域控制器不启用完整的帐户审核日志。这可以通过组策略编辑器中安全设置中的审核策略进行控制。要打开组策略编辑器，请在域控制器上运行 `gpedit.msc`。启用审核策略后，域控制器会在安全日志中生成额外的事件日志信息。

启用账户审核事件(/en-us/federated-authentication-service/2402-ltsr/media/fas-troubleshoot-logon-auditpolicy.png)

证书验证日志

检查证书有效性

如果智能卡证书导出为 DER 证书（无需私钥），您可以使用以下命令对其进行验证：certutil –verify user.cer

启用 CAPI 日志记录

在域控制器和用户计算机上，打开事件查看器并为 Microsoft/Windows/CAPI2/Operational Logs 启用日志记录。

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

在域控制器和 VDA 计算机上，打开事件查看器并导航到 **应用程序和服务日志** > **Microsoft** > **Windows** > **CAPI2** > **操作**。右键单击 **操作** 并选择 **启用日志**。

此外，可以使用以下注册表值微调 CAPI 日志记录：*HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\crypt32*。以下值默认不存在，您必须创建它们。如果您希望恢复到默认的 CAPI2 日志记录设置，请删除这些值。

值	描述
DiagLevel (DWORD)	详细程度级别（0 到 5）
DiagMatchAnyMask (QUADWORD)	事件筛选器（全部使用 0xffffff）
DiagProcessName (MULTI_SZ)	按进程名称筛选（例如，LSASS.exe）

CAPI 日志

消息	描述
构建链	LSA 调用 CertGetCertificateChain（包含结果）
验证吊销	LSA 调用 CertVerifyRevocation（包含结果）
X509 对象	在详细模式下，证书和证书吊销列表 (CRL) 将转储到 AppData\LocalLow\Microsoft\X509Objects
验证链策略	LSA 调用 CertVerifyChainPolicy（包含参数）

错误消息

错误代码	描述
证书不受信任	无法使用计算机的中间和受信任的根证书存储中的证书构建智能卡证书。
证书吊销检查错误	无法从证书 CRL 分发点指定的地址下载智能卡的 CRL。如果强制执行吊销检查，这将阻止登录成功。请参阅 证书和公钥基础结构 部分。
证书使用错误	该证书不适用于登录。例如，它可能是服务器证书或签名证书。

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

Kerberos 日志

要启用 Kerberos 日志记录，请在域控制器和最终用户计算机上创建以下注册表值：

配置单元	值名称	值 [DWORD]
CurrentControlSet\Control\Lsa\Kerberos\Parameters	LogLevel	0x1
CurrentControlSet\Control\Lsa\Kerberos\Parameters	KerbDebuglevel	0xffffffff
CurrentControlSet\Services\Kdc	KdcDebugLevel	0x1
CurrentControlSet\Services\Kdc	KdcExtraLogLevel	0x1f

Kerberos 日志输出到系统事件日志。

- 诸如“不受信任的证书”之类的消息应该很容易诊断。
- 两个错误代码是信息性的，可以安全地忽略：
  - KDC_ERR_PREAUTH_REQUIRED（用于与旧域控制器向后兼容）
  - 未知错误 0x4b

域控制器和工作站日志

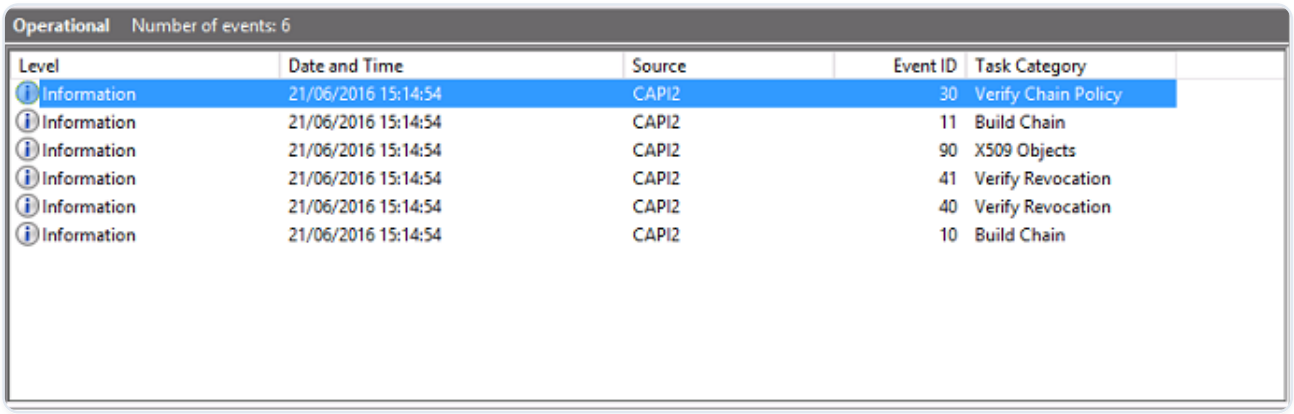
本节介绍用户使用证书登录时，域控制器和工作站上预期的日志条目。

- 域控制器 CAPI2 日志
- 域控制器安全日志
- 虚拟投递代理 (VDA) 安全日志
- VDA CAPI 日志
- VDA 系统日志

域控制器 CAPI2 日志

在登录期间，域控制器会验证调用者的证书，并生成以下形式的日志条目序列。

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



Operational Number of events: 6

Level	Date and Time	Source	Event ID	Task Category
Information	21/06/2016 15:14:54	CAPI2	30	Verify Chain Policy
Information	21/06/2016 15:14:54	CAPI2	11	Build Chain
Information	21/06/2016 15:14:54	CAPI2	90	X509 Objects
Information	21/06/2016 15:14:54	CAPI2	41	Verify Revocation
Information	21/06/2016 15:14:54	CAPI2	40	Verify Revocation
Information	21/06/2016 15:14:54	CAPI2	10	Build Chain

最终的事件日志消息显示，域控制器上的 lsass.exe 根据 VDA 提供的证书构建了一个链，并验证其有效性（包括吊销）。结果返回为“ERROR_SUCCESS”。

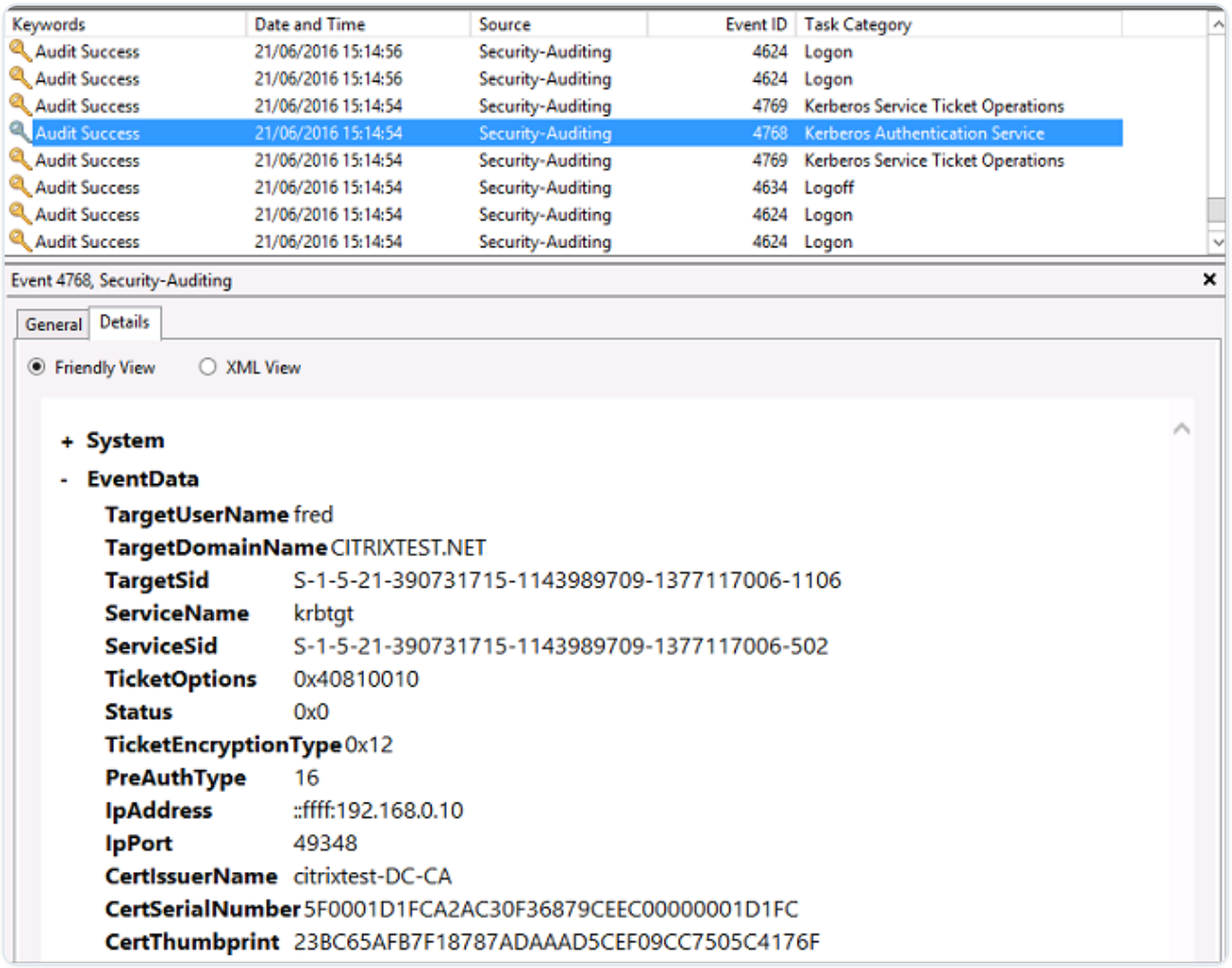
- **CertVerifyCertificateChainPolicy**
  - **Policy**
    - [**type**] CERT_CHAIN_POLICY_NT_AUTH
    - [**constant**] 6
  - **Certificate**
    - [**fileRef**] 23BC65AFB7F18787ADAAAD5CEF09CC7505C4176F.cer
    - [**subjectName**] fred
  - **CertificateChain**
    - [**chainRef**] {FF03F79B-52F8-4C93-877A-5DFFE40B9574}
  - **Flags**
    - [**value**] 0
  - **Status**
    - [**chainIndex**] -1
    - [**elementIndex**] -1
  - **EventAuxInfo**
    - [**ProcessName**] lsass.exe
  - **CorrelationAuxInfo**
    - [**TaskId**] {F5E7FD3F-628F-4C76-9B1C-49FED786318F}
    - [**SeqNumber**] 1
  - **Result**
    - [**value**] 0

域控制器安全日志

域控制器显示一系列登录事件，关键事件是 4768，其中证书用于颁发 Kerberos 票证授予票证 (krbtgt)。

此前的消息显示服务器的计算机帐户正在向域控制器进行身份验证。此后的消息显示属于新 krbtgt 的用户帐户正在用于向域控制器进行身份验证。

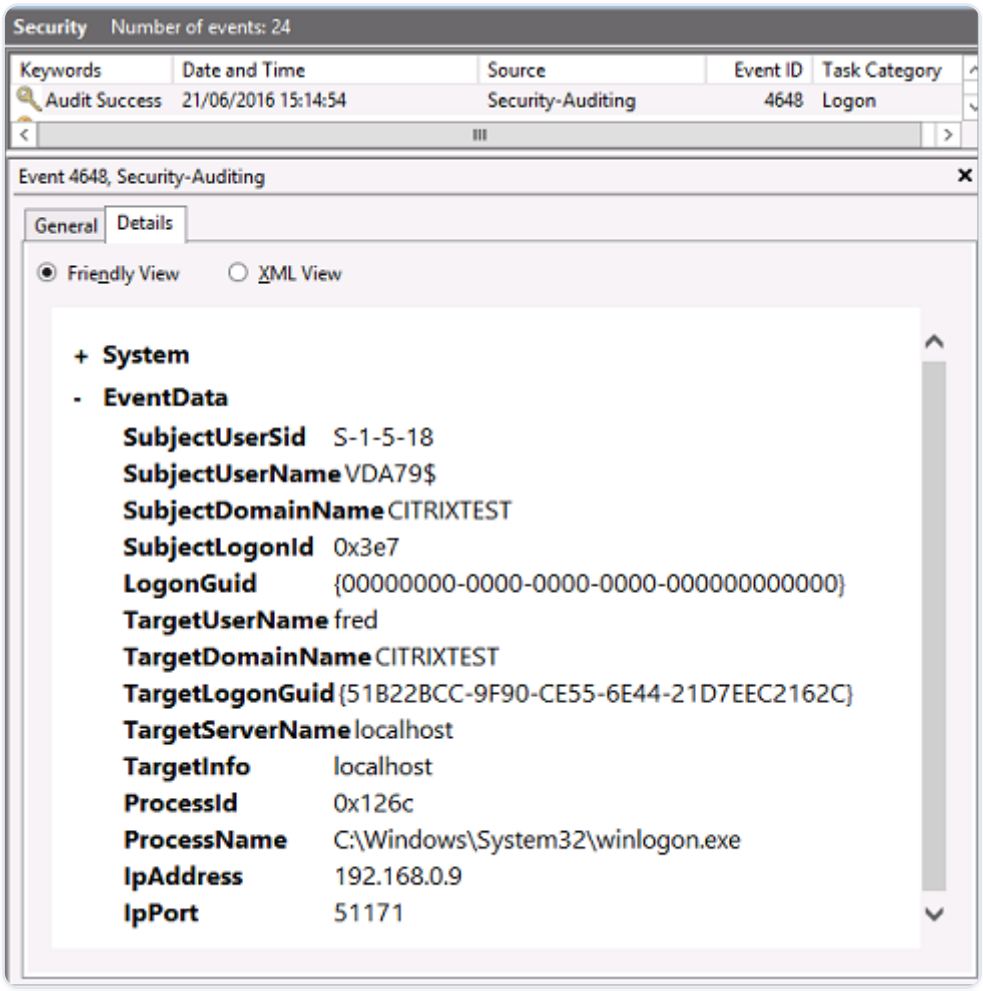
© 1997–2026 Citrix Systems, Inc. All rights reserved.



VDA 安全日志

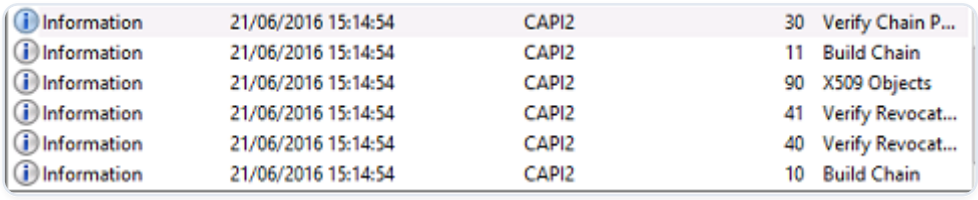
VDA 安全审核日志中与登录事件对应的条目是事件 ID 为 4648 的条目，它源自 winlogon.exe。

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

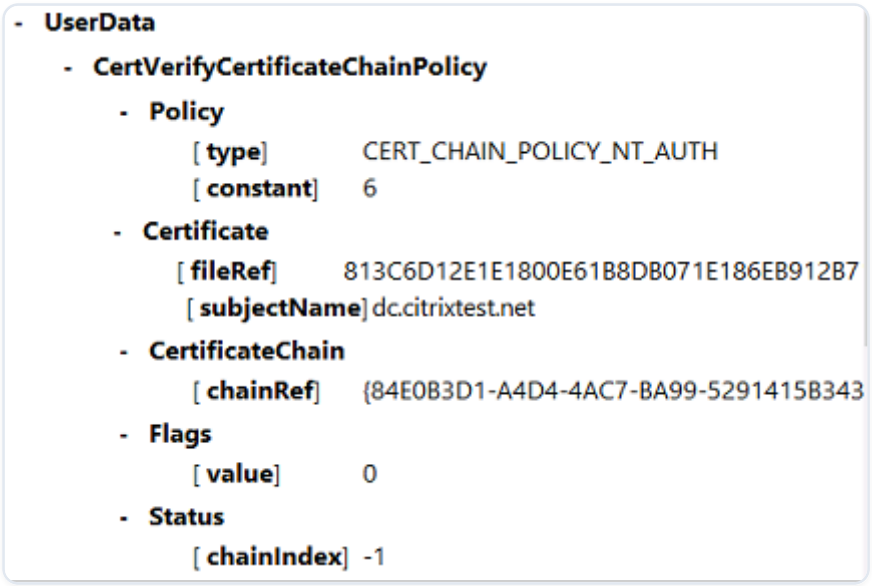


VDA CAPI 日志

此示例 VDA CAPI 日志显示了来自 lsass.exe 的单个链构建和验证序列，用于验证域控制器证书 (dc.citrixtest.net)。

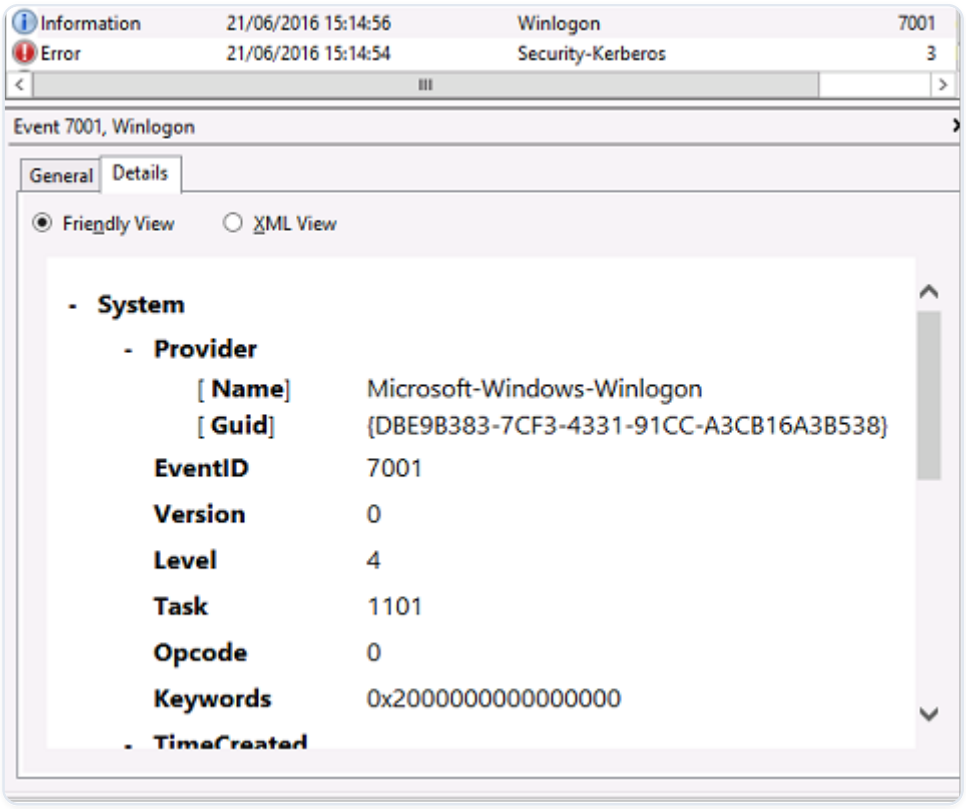


© 1997–2026 Citrix Systems, Inc. All rights reserved.



VDA 系统日志

启用 Kerberos 日志记录后，系统日志会显示错误 KDC_ERR_PREAUTH_REQUIRED（可忽略），以及来自 Winlogon 的条目，指示 Kerberos 登录成功。



使用 Windows 事件日志监视 FAS

所有 FAS 事件都写入 Windows 应用程序事件日志。您可以使用 System Center Operations Manager (SCOM) 等产品，通过此处描述的进程和事件来监视 FAS 服务的运行状况。

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

FAS 服务是否正在运行?

要确定 FAS 服务是否正在运行，请监视进程 Citrix.Authentication.FederatedAuthenticationService.exe。

本节仅介绍用于监视 FAS 服务的最重要事件。有关 FAS 事件代码的完整列表，请参阅 FAS 事件日志。

FAS 运行状况事件

以下事件显示您的 FAS 服务是否正常运行。

事件源为 **Citrix.Authentication.FederatedAuthenticationService**。

事件	事件文本	说明	备注
[S003]	管理员 [{0}] 将维护模式设置为 [{1}]	FAS 服务已进入或退出维护模式。	在维护模式下，FAS 服务器无法用于单点登录。
[S022]	管理员 [{0}] 将维护模式设置为“关”	FAS 服务已退出维护模式。	适用于 FAS 10.7 或 Citrix 虚拟应用和桌面 2109。
[S023]	管理员 [{0}] 将维护模式设置为开启	FAS 服务已进入维护模式。	适用于 FAS 10.7 或 Citrix 虚拟应用和桌面 2109。
[S123]	未能为 [upn: {0} role: {1}] 颁发证书 [exception: {2}]	此事件在 [S124] 之后发生，如果 FAS 配置的任何 CA 都未能成功颁发用户证书。该用户的单点登录将失败。	此事件表明所有配置的 CA 均无法正常工作。如果 FAS 配置为使用 HSM，这还可能表明 HSM 无法正常工作。
[S124]	未能为 [upn: {0} role: {1}] 在 [certificate authority: {2}] 颁发证书 [exception: {3}]	当 FAS 尝试从给定 CA 请求用户证书时发生故障。如果 FAS 配置了多个 CA，FAS 会尝试向另一个 CA 发出请求。	此事件可能表明 CA 无法正常工作或无法联系。如果 FAS 配置为使用 HSM，这还可能表明 HSM 无法正常工作。可以使用异常来帮助识别问题的原因。

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

事件	事件文本	说明	备注
[S413]	授权证书即将到期（剩余 {0} 天）。证书详细信息：{1}	当 FAS 授权证书即将到期时，会定期生成此事件。默认情况下，如果授权证书在 30 天内到期，则每天生成此事件。	可以使用 cmdlet **Set-FasRaCertificateMonitor** 调整默认设置；请参阅 PowerShell cmdlet。
[S414]	授权证书已过期。证书详细信息：{0}	当 FAS 授权证书过期时，会定期生成此事件。默认情况下，此事件每天生成一次。	一旦过期，FAS 将无法生成新的用户证书，并且单点登录将开始失败。

云连接的 FAS 事件

如果您将 FAS 与 Citrix Cloud™ 结合使用，以下事件将显示您的 FAS 服务是否正常运行。

事件源为 **Citrix.Fas.Cloud**。

事件	事件文本	说明	备注
[S012]	FAS 服务可用于从 Citrix Cloud 进行单点登录	此事件表明从 Workspace（即 Citrix Cloud）进行的单点登录应正常工作。	在发出此事件之前，FAS 会检查 (1) 是否已配置，(2) 是否未处于维护模式，以及 (3) 是否已连接到 Citrix Cloud。
[S013]	FAS 服务无法从 Citrix Cloud 进行单点登录。[{0}] 更多详细信息可在管理控制台中找到。	此事件表明 FAS 无法从 Workspace（即 Citrix Cloud）提供单点登录。消息中包含单点登录无法工作的原因。	FAS 维护与 Citrix Cloud 的持久连接。此连接可能因各种原因（例如网络故障或代理服务器上的连接生命周期策略）而偶尔终止。发生这种情况时，事件文本会包含“Service is not connected to the cloud”。**这是正常行为，FAS 会立即尝试重新建立与 Citrix Cloud 的连接。**

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

安全事件

以下事件表明未经授权的实体尝试使用 FAS。

事件源为 **Citrix.Authentication.FederatedAuthenticationService**。

事件	事件文本	说明
[S001]	访问被拒绝：用户 [{0}] 不是 Administrators 组的成员	有人尝试查看或更改 FAS 配置，但调用者不是 FAS 管理员。
[S002]	访问被拒绝：用户 [{0}] 不是角色 [{1}] 的管理员	尝试查看或更改 FAS 规则的配置，但调用方不是 FAS 管理员。
[S101]	服务器 [{0}] 无权在角色 [{1}] 中声明身份	尝试声明用户身份，但调用方无权执行此操作。只有在 FAS 规则配置中获得许可的 StoreFront™ 服务器（以及适用的 Workspace）才允许声明用户身份。
[S104]	服务器 [{0}] 未能声明 UPN [{1}]（角色 [{2}] 不允许此 UPN）	尝试声明用户身份，但根据 FAS 规则配置，不允许此用户帐户。
[S205]	依赖方访问被拒绝 - 调用帐户 [{0}] 不是规则 [{1}] 的允许依赖方	VDA 尝试使用 FAS 执行单点登录，但根据 FAS 规则配置，不允许此 VDA。

FAS 事件日志

下表列出了 FAS 生成的事件日志条目。

管理事件

这些事件是为响应 FAS 服务器中的配置更改而记录的。

日志代码
[S001] 访问被拒绝: 用户 [{0}] 不是 Administrators 组的成员
[S002] 访问被拒绝: 用户 [{0}] 不是角色 [{1}] 的管理员

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

日志代码
[S003] 管理员 [{0}] 将维护模式设置为 [{1}]
[S004] 管理员 [{0}] 正在使用模板 [{2} and {3}] 从 CA [{1}] 请求授权证书
[S005] 管理员 [{0}] 正在取消授权 CA [{1}]
[S006] 管理员 [{0}] 正在创建证书定义 [{1}]
[S007] 管理员 [{0}] 正在更新证书定义 [{1}]
[S008] 管理员 [{0}] 正在删除证书定义 [{1}]
[S009] 管理员 [{0}] 正在创建规则 [{1}]
[S010] 管理员 [{0}] 正在更新规则 [{1}]
[S011] 管理员 [{0}] 正在删除规则 [{1}]
[S012] 管理员 [{0}] 正在创建证书 [upn: {1} sid: {2} rule: {3}]证书定义: {4} 安全上下文: {5}]
[S013] 管理员 [{0}] 正在删除证书 [upn: {1} role: {2} Certificate Definition: {3} Security Context: {4}]
[S015] 管理员 [{0}] 正在创建证书请求 [TPM: {1}]
[S016] 管理员 [{0}] 正在导入授权证书 [Reference: {1}]
[S022] 管理员 [{0}] 正在将维护模式设置为关闭
[S023] 管理员 [{0}] 正在将维护模式设置为开启
[S024] 管理员 [{0}] 正在设置系统运行状况监视器
[S025] 管理员 [{0}] 正在设置系统运行状况监视器
[S026] 管理员 [{0}] 正在设置 RA 证书监视器
[S027] 管理员 [{0}] 正在重置 RA 证书监视器
[S050] 管理员 [{0}] 正在创建云配置: [{1}]
[S051] 管理员 [{0}] 正在更新云配置: [{1}]

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

日志代码
[S052] 管理员 [{0}] 正在删除云配置
[S060] 管理员 [{0}] 正在请求云注册。实例: {1}
[S060] 管理员 [{0}] 正在请求直接信任云注册。实例: {1} 云服务 URL 格式: {2}
[S061] 管理员 [{0}] 正在完成云注册。资源位置: {1}, 规则名称: {2}
[S062] 管理员 [{0}] 已完成云注册。资源位置: {1} ({2}), 规则名称: {3}, 客户: {4} ({5})
[S063] 在云注册期间发生 KRS 错误。异常为 {0}
[S064] 云注册期间发生未知错误。异常为 {0}

日志代码
[S401] 正在执行配置升级 - [From version {0} to version {1}]
[S402] 错误：Citrix 联合身份验证服务必须以网络服务身份运行 [currently running as: {0}]
[S404] 正在强制擦除 Citrix 联合身份验证服务数据库
[S405] 将数据从注册表迁移到数据库时发生错误: [{0}]
[S406] 数据从注册表到数据库的迁移已完成（注意：用户证书未迁移）
[S407] 基于注册表的数据未迁移到数据库，因为数据库已存在
[S408] 无法降级配置 -- [From version {0} to version {1}]
[S409] 线程池配置成功 - MinThreads 从 [workers: {0} completion: {1}] 调整为: [workers: {2} completion: {3}]
[S410] 线程池配置失败 - 无法将 MinThreads 从 [workers: {0} completion: {1}] 调整为: [workers: {2} completion: {3}]; 这可能会影响 FAS 服务器的可伸缩性
[S411] 启动 FAS 服务时出错: [{0}]
[S412] 配置升级完成 -- [From version {0} to version {1}]
[S413] 授权证书即将过期（剩余 {0} 天）。证书详细信息: {1}

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

日志代码
[S414] 授权证书已过期。证书详细信息: {0}
[S415] 授权证书检查已完成。已记录 {0} 个问题。下次检查时间为 {1}

创建身份断言

当受信任的服务器断言用户登录时，这些事件会在 FAS 服务器上运行时记录。

日志代码
[S101] 服务器 [{0}] 无权在角色 [{1}] 中断言身份
[S102] 服务器 [{0}] 未能断言 UPN [{1}] (异常: {2}{3})
[S103] 服务器 [{0}] 请求了 UPN [{1}] SID {2}，但查找返回了 SID {3}
[S104] 服务器 [{0}] 未能断言 UPN [{1}] (UPN 不允许通过角色 [{2}])
[S105] 服务器 [{0}] 发布了身份断言 [upn: {1}, 角色 {2}, 安全上下文: [{3}]]
[S120] 正在向 [upn: {0} 角色: {1} 安全上下文: [{2}]] 颁发证书
[S121] 证书已由 [certificate authority: {2}] 颁发给 [upn: {0} role: {1}]
[S122] 警告: 服务器过载 [upn: {0} 角色: {1}][每分钟请求数 {2}]。
[S123] 未能为 [upn: {0} role: {1}] [exception: {2}] 颁发证书
[S124] 未能为 [upn: {0} role: {1}] 在 [certificate authority: {2}] 颁发证书 [exception: {3}]

作为信赖方

当 VDA 登录用户时，这些事件会在 FAS 服务器上运行时记录。

日志代码
[S201] 信赖方 [{0}] 无权访问密码。
[S202] 信赖方 [{0}] 无权访问证书。
[S203] 信赖方 [{0}] 无权访问登录 CSP

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

日志代码
[S204] 信赖方 [{0}] 正在访问 [upn: {1}] 的登录 CSP，角色为：[{2}] [Operation: {3}]，由 [{4}] 授权
[S205] 信赖方访问被拒绝 - 调用帐户 [{0}] 不是规则 [{1}] 允许的信赖方
[S206] 调用帐户 [{0}] 不是信赖方
[S208] 私钥操作失败 [Operation: {0} upn: {1} role: {2} certificateDefinition {3} Error {4} {5}]。

会话内证书服务器

当用户使用会话内证书时，这些事件会在 FAS 服务器上记录。

日志代码
[S301] 访问被拒绝：用户 [{0}] 无权访问虚拟智能卡
[S302] 用户 [{0}] 请求了未知的虚拟智能卡 [thumbprint: {1}]
[S303] 访问被拒绝：用户 [{0}] 与虚拟智能卡 [upn: {1}] 不匹配
[S304] 用户 [{0}] 正在计算机 [{2}] 上运行程序 [{1}]，使用虚拟智能卡 [upn: {3} role: {4} thumbprint: {5}] 进行私钥操作 [{6}]
[S305] 私钥操作失败 [Operation: {0}] [upn: {1} role: {2} containerName {3} Error {4} {5}]。

FAS 断言插件

这些事件由 FAS 断言插件记录。

日志代码
[S500] 未配置 FAS 断言插件
[S501] 无法加载已配置的 FAS 断言插件 [exception:{0}]
[S502] FAS 断言插件已加载 [pluginId={0}] [assembly={1}] [location={2}]
[S503] 服务器 [{0}] 未能断言 UPN [{1}]（提供了登录凭据，但插件 [{2}] 不支持）
[S504] 服务器 [{0}] 未能断言 UPN [{1}]（提供了登录凭据，但未配置 FAS 插件）
[S505] 服务器 [{0}] 未能断言 UPN [{1}]（插件 [{2}] 拒绝了登录凭据，状态为 [{3}]，消息为 [{4}]）

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

日志代码
[S506] 插件 [{0}] 接受了来自服务器 [{1}] 的 UPN [{2}] 的登录凭据，消息为 [{3}]
[S507] 服务器 [{0}] 未能断言 UPN [{1}]（插件 [{2}] 在方法 [{4}] 期间抛出异常 [{3}]）
[S507] 服务器 [{0}] 未能断言 UPN [{1}]（插件 [{2}] 抛出异常 [{3}]）
[S508] 服务器 [{0}] 未能断言 UPN [{1}]（提供了访问处置，但插件 [{2}] 不支持它）
[S509] 服务器 [{0}] 未能断言 UPN [{1}]（提供了访问处置，但没有配置 FAS 插件）
[S510] 服务器 [{0}] 未能断言 UPN [{1}]（访问处置被插件 [{2}] 视为无效）

启用 Workspace 的 FAS

当 FAS 与 Workspace 结合使用时，会记录这些事件。

日志代码
[S001] 轮换了 Citrix Cloud 授权密钥 [fas id: {0}] [old key id:{1}] [new key id:{2}]
[S002] 云支持模块正在启动。FasHub 云服务 URL: {0}
[S003] FAS 已在云中注册 [fas id: {0}] [transaction id: {1}]
[S004] FAS 未能注册到云 [fas id: {0}] [transaction id: {1}] [exception: {2}]
[S005] FAS 已将其当前配置发送到云 [fas id: {0}] [transaction id: {1}]
[S006] FAS 未能将其当前配置发送到云端 [fas id: {0}] [transaction id: {1}] [exception: {2}]
[S007] FAS 已从云端注销 [fas id: {0}] [transaction id: {1}]
[S009] FAS 未能从云端注销 [fas id: {0}] [transaction id: {1}] [exception: {2}]
[S010] FAS 服务已连接到云消息传递 URL: {0}
[S011] FAS 服务未连接到云端
[S012] FAS 服务可用于 Citrix Cloud 的单点登录
[S013] FAS 服务不可用于 Citrix Cloud 的单点登录。[{0}] 更多详细信息可在管理控制台中找到

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

日志代码
[S014] 对云服务 `<service name>` 的调用失败 [fas id: {0}] [transaction id: {1}] [exception: {2}]
[S015] 来自 Citrix Cloud 的消息被阻止，因为调用者未获得许可 [message ID {0}] [transaction ID {1}] [caller {2}]
[S016] 对云服务 `<service name>` 的调用成功 [fas id: {0}] [transaction id: {1}]
[S019] FAS 已从云端下载其配置 [fas id: {0}] [transaction id: {1}]
[S020] FAS 未能从云端下载其配置 [fas id: {0}] [transaction id: {1}] [exception: {2}]
[S021] 云支持模块启动失败。异常: {0}
[S022] 云支持模块正在停止
[S023] 未能轮换 Citrix Cloud 授权密钥 [fas id: {0}] [current key id:{1}] [new key id:{2}] [keys in cloud:{3}]
[S024] 正在启动 Citrix Cloud 授权密钥轮换 [fas id: {0}] [current key id:{1}] [new key id:{2}]
[S025] 此服务的授权密钥存在于 Citrix Cloud 中 [current key: {0}] [keys in cloud: {1}]
[S026] 此服务的授权密钥不存在于 Citrix Cloud 中 [current key: {0}] [keys in cloud: {1}]
[S027] 已升级 Citrix Cloud 授权密钥存储格式 [fas id: {0}]

登录

这些事件在登录阶段记录在 VDA 上。

日志代码
[S101] 身份断言登录失败。无法识别的 Federated Authentication Service [id: {0}]
[S102] 身份断言登录失败。无法查找 {0} 的 SID [Exception: {1}{2}]
[S103] 身份断言登录失败。用户 {0} 的 SID 为 {1}，预期 SID 为 {2}
[S104] 身份断言登录失败。无法连接到 Federated Authentication Service: {0} [Error: {1} {2}]
[S105] 身份断言登录。正在登录 [Username: {0} Domain: {1}]

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

日志代码
[S106] 身份断言登录。 联合身份验证服务：{0}。 正在登录 [Certificate: {1}]
[S107] 身份断言登录失败。 [Exception: {0}{1}]
[S108] 身份断言子系统。访问被拒绝 [Caller: {0}]

会话内证书

当用户尝试使用会话内证书时，这些事件会记录在 VDA 上。

日志代码
[S201] 虚拟智能卡访问由 [{0}] 授权给 [PID: {1} Program Name: {2}Certificate thumbprint: {3}]
[S203] 虚拟智能卡子系统。访问被拒绝 [caller: {0}, session {1}]
[S204] 虚拟智能卡子系统。智能卡支持已禁用

证书请求和密钥对生成

当 FAS 服务器执行低级加密操作时，会记录这些事件。

日志代码
[S001] TrustArea::TrustArea: 已安装证书 [TrustArea: {0} Certificate {1}TrustAreaJoinParameters {2}]
[S014] Pkcs10Request::Create: 已创建 PKCS10 请求 [Distinguished Name {0}]
[S016] 创建私钥 [Identifier {0}MachineWide: {1} Provider: {2} ProviderType: {3} EllipticCurve: {4} KeyLength: {5} isExportable: {6}]
[S017] 私钥::删除 [CspName: {0}, Identifier {1}]

日志代码
[S104] MicrosoftCertificateAuthority::GetCredentials: 授权使用 {0}
[S105] MicrosoftCertificateAuthority::SubmitCertificateRequest 提交响应错误 [{0}]
[S106] MicrosoftCertificateAuthority::SubmitCertificateRequest 已颁发证书 [{0}]

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

日志代码
[S112] MicrosoftCertificateAuthority::SubmitCertificateRequest - 等待批准 [CR_DISP_UNDER_SUBMISSION] [Reference: {0}]

最终用户错误消息

本节列出了在 Windows 登录页面上向用户显示的常见错误消息。

显示的错误消息	描述和参考
无效的用户名或密码	计算机认为您拥有有效的证书和私钥，但 Kerberos 域控制器拒绝了连接。请参阅本文的 ***Kerberos 日志*** 部分。
系统无法登录您。您的凭据无法验证。/ 不支持该请求	无法联系域控制器，或者域控制器未配置支持智能卡身份验证的证书。为域控制器注册“Kerberos Authentication”、“Domain Controller Authentication”或“Domain Controller”证书。即使现有证书看起来有效，也值得尝试此操作。
系统可能无法登录您。用于身份验证的智能卡证书不受信任。	中间证书和根证书未安装在本地计算机上。请参阅证书和公钥基础结构。
错误请求	这通常表示证书上的扩展未正确设置，或者 RSA 密钥太短（<2048 位）。

FAS 始终开启的跟踪

通过始终开启的跟踪，FAS 会将其活动记录到文件系统。这有助于故障排除，并可能消除重现已发生事件的需要。此配置仅适用于 LTSR 2402 CU4 及更高版本。

使用以下任一方法安装或升级 FAS 时，将启用始终开启的跟踪：

- Citrix Virtual Apps and Desktops™ 安装程序：插入 ISO 时，从自动运行启动屏幕上的“**Federated Authentication Service**”按钮进行安装
- `XenDesktopFasSetup.exe`：位于 Citrix Virtual Apps and Desktops ISO 镜像中，路径为 `x64\XenDesktop Setup\XenDesktopFasSetup.exe`
- `FasSetup_xxxx.exe`：独立的 FAS 安装程序文件，可从 Citrix Downloads 获取。

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

注意：

如果您使用 **FAS 安装程序 MSI** 文件 `FederatedAuthenticationService_x64.msi` 进行安装或升级，则始终开启的跟踪不可用。

收集始终开启的跟踪

使用 Citrix Scout 从 FAS 服务器收集始终开启的跟踪和其他诊断数据。使用上述任一方法安装 FAS 时，将安装 **Citrix Scout**。

禁用始终开启的跟踪

如果出于任何原因希望禁用始终开启的跟踪，请在 FAS 服务器上停止并禁用 **Citrix Telemetry Service**。

将始终开启的跟踪发送到中央日志服务器

有关详细信息和配置步骤，请参阅始终开启的跟踪 (AOT) 文章。

相关信息

- 为智能卡登录配置域
- 智能卡登录策略
- 启用 CAPI 日志记录
- 启用 Kerberos 日志记录
- 使用第三方证书颁发机构启用智能卡登录的准则

PowerShell 命令小程序

您可以将联合身份验证服务 (FAS) 管理控制台用于简单部署；但是，PowerShell 界面提供了更高级的选项。如果您计划使用控制台中不可用的选项，Citrix 建议仅使用 PowerShell 进行配置。

以下命令添加 FAS PowerShell cmdlet：

```
Add-PSSnapin Citrix.Authentication.FederatedAuthenticationService.V1
```

在 PowerShell 窗口中，您可以使用 Get-Help \<*cmdlet name*> 来显示 cmdlet 帮助。

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

有关 FAS PowerShell SDK cmdlet 的更多信息，请参阅 `<https://developer-docs.citrix.com/projects/federated-authentication-service-powershell-cmdlets/en/latest/>`。

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

部署架构

简介

联合身份验证服务 (FAS) 是一个 Citrix® 组件，它与您的 Active Directory 证书颁发机构集成，允许用户在 Citrix 环境中无缝进行身份验证。本文档介绍了可能适用于您的部署的各种身份验证架构。

启用后，FAS 将用户身份验证决策委托给受信任的 StoreFront 服务器。StoreFront 拥有一套围绕现代 Web 技术构建的全面内置身份验证选项，并且可以使用 StoreFront SDK 或第三方 IIS 插件轻松扩展。基本设计目标是，任何能够对用户进行网站身份验证的技术，现在都可以用于登录 Citrix Virtual Apps 或 Citrix Virtual Desktops™ 部署。

本文档介绍了按复杂性递增的示例顶级部署架构。

- 内部部署
- Citrix 网关部署
- ADFS SAML
- B2B 帐户映射
- Windows 10 Azure 活动目录加入

提供了相关 FAS 文章的链接。对于所有架构，安装和配置 文章是设置 FAS 的主要参考资料。

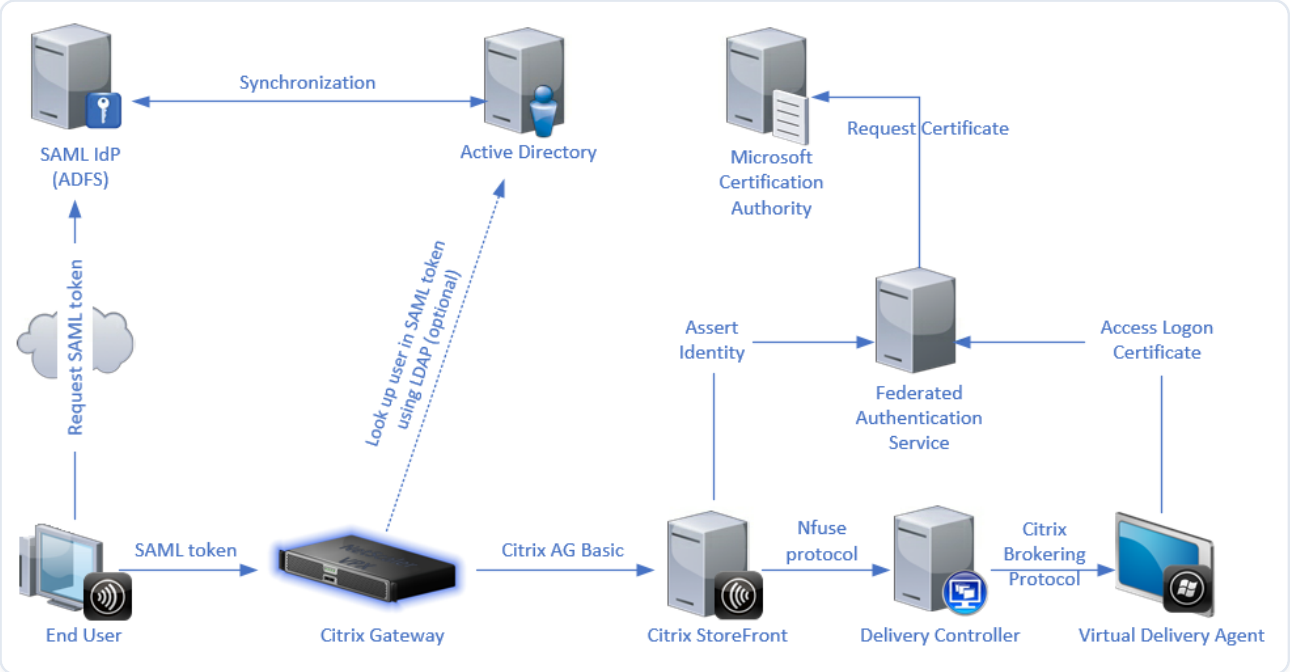
架构概述

FAS 被授权代表由 StoreFront 验证的 Active Directory 用户自动颁发智能卡类证书。这使用了与允许管理员配置物理智能卡的工具类似的 API。当用户被代理到 Citrix Virtual Apps™ 或 Citrix Virtual Desktops 虚拟投递代理 (VDA) 时，证书会附加到计算机，并且 Windows 域会将登录视为标准智能卡身份验证。

当用户请求访问 Citrix 环境时，受信任的 StoreFront™ 服务器会联系 FAS。FAS 授予一个票证，允许单个 Citrix Virtual Apps 或 Citrix Virtual Desktops 会话使用该会话的证书进行身份验证。当 VDA 需要对用户进行身份验证时，它会连接到 FAS 并兑换票证。只有 FAS 才能访问用户证书的私钥；VDA 必须将它需要使用证书执行的每个签名和解密操作发送给 FAS。

下图显示了 FAS 与 Microsoft 证书颁发机构集成，并为 StoreFront 和 Citrix Virtual Apps and Desktops™ 虚拟投递代理 (VDA) 提供支持服务。

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



内部部署

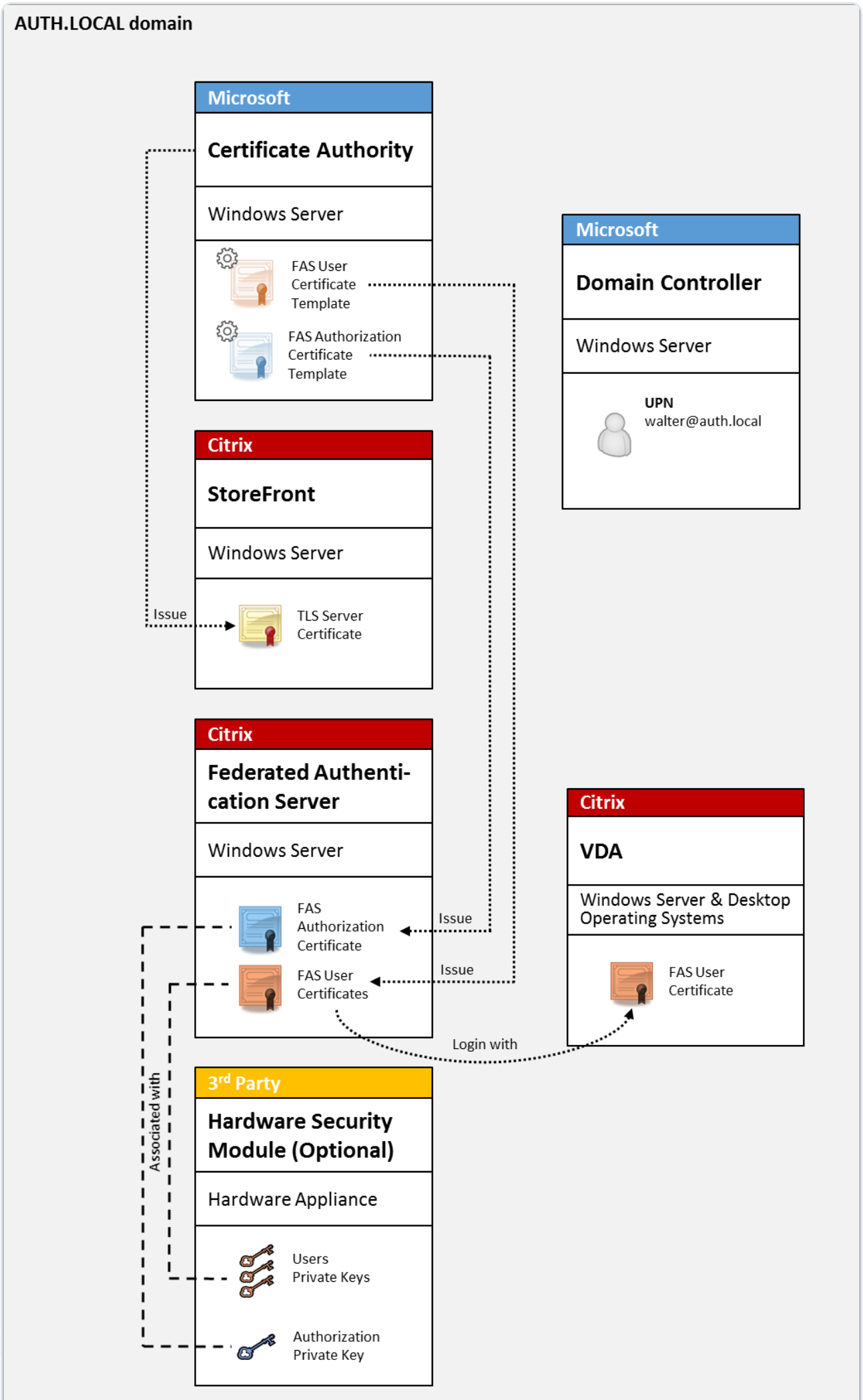
FAS 允许用户使用各种身份验证选项（包括 Kerberos 单点登录）安全地向 StoreFront 进行身份验证，并连接到完全经过身份验证的 Citrix HDX™ 会话。

这允许 Windows 身份验证，无需提示输入用户凭据或智能卡 PIN，并且无需使用“保存的密码管理”功能，例如单点登录服务。这可以用于替代早期版本 Citrix Virtual Apps 中可用的 Kerberos 约束委派登录功能。

所有用户都可以在其会话中访问公钥基础设施 (PKI) 证书，无论他们是否使用智能卡登录到端点设备。这允许平稳迁移到双因素身份验证模型，即使是从没有智能卡读卡器的智能手机和平板电脑等设备。

此部署添加了一台运行 FAS 的新服务器，该服务器被授权代表用户颁发智能卡类证书。然后，这些证书用于登录 Citrix HDX 环境中的用户会话，如同使用了智能卡登录一样。

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


AUTH.LOCAL domain
Microsoft
Certificate Authority
Windows Server
FAS User Certificate Template
FAS Authorization Certificate Template
Microsoft
Domain Controller
Windows Server
UPN
walter@auth.local
Citrix
StoreFront
Windows Server
Issue
TLS Server Certificate
Citrix
Federated Authenti-cation Server
Windows Server
FAS Authorization Certificate
FAS User Certificates
Issue
Issue
Citrix
VDA
Windows Server & Desktop Operating Systems
FAS User Certificate
Login with
3rd Party
Hardware Security Module (Optional)
Hardware Appliance
Users Private Keys
Authorization Private Key
Associated with

Citrix Virtual Apps 或 Citrix Virtual Desktops 环境必须以与智能卡登录类似的方式进行配置，这在 CTX206156 中有详细说明。

在现有部署中，这通常只涉及确保域加入的 Microsoft 证书颁发机构可用，并且域控制器已分配域控制器证书。（请参阅 CTX206156 中的“颁发域控制器证书”部分。）

相关信息：

- 密钥可以存储在硬件安全模块 (HSM) 或内置的可信平台模块 (TPM) 中。有关详细信息，请参阅私钥保护 文章。
- 安装和配置 文章介绍了如何安装和配置 FAS。

思杰网关部署

Citrix Gateway 部署与内部部署类似，但增加了与 StoreFront 配对的 Citrix Gateway，将主要的身份验证点移至 Citrix Gateway 本身。Citrix Gateway 包含复杂的身份验证和授权选项，可用于保护对公司网站的远程访问。

此部署可用于避免在首次向 Citrix Gateway 进行身份验证然后登录用户会话时出现的多次 PIN 提示。它还允许使用高级 Citrix Gateway 身份验证技术，而无需额外要求 AD 密码或智能卡。

本地化图像(/en-us/federated-authentication-service/2402-ltsr/media/fas-architectures-netscaler.png)

Citrix Virtual Apps 或 Citrix Virtual Desktops 环境必须以与智能卡登录类似的方式进行配置，这在 CTX206156 中有说明。

在现有部署中，这通常只涉及确保已加入域的 Microsoft 证书颁发机构可用，并且域控制器已分配域控制器证书。（请参阅 CTX206156 中的“颁发域控制器证书”部分）。

将 Citrix Gateway 配置为主要身份验证系统时，请确保 Citrix Gateway 和 StoreFront 之间的所有连接都通过 TLS 保护。特别是，请确保回调 URL 已正确配置为指向 Citrix Gateway 服务器，因为这可用于在此部署中对 Citrix Gateway 服务器进行身份验证。

本地化图像(/en-us/federated-authentication-service/2402-ltsr/media/fas-architectures-netscaler-auth-settings.png)

相关信息：

- 要配置 Citrix Gateway，请参阅“如何配置 NetScaler Gateway 10.5 以与 StoreFront 3.6 和 Citrix Virtual Desktops 7.6 配合使用。”
- 安装和配置 介绍了如何安装和配置 FAS。

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

ADFS SAML 部署

一项关键的 Citrix Gateway 身份验证技术允许与 Microsoft ADFS 集成，后者可充当 SAML 身份提供程序 (IdP)。SAML 断言是由受信任的 IdP 颁发的经过加密签名的 XML 块，它授权用户登录计算机系统。这意味着 FAS 服务器允许将用户身份验证委托给 Microsoft ADFS 服务器（或其他支持 SAML 的 IdP）。

本地化图像(/en-us/federated-authentication-service/2402-ltsr/media/fas-architectures-adfs-saml.png)

ADFS 通常用于通过 Internet 远程安全地对用户进行企业资源身份验证；例如，它通常用于 Office 365 集成。

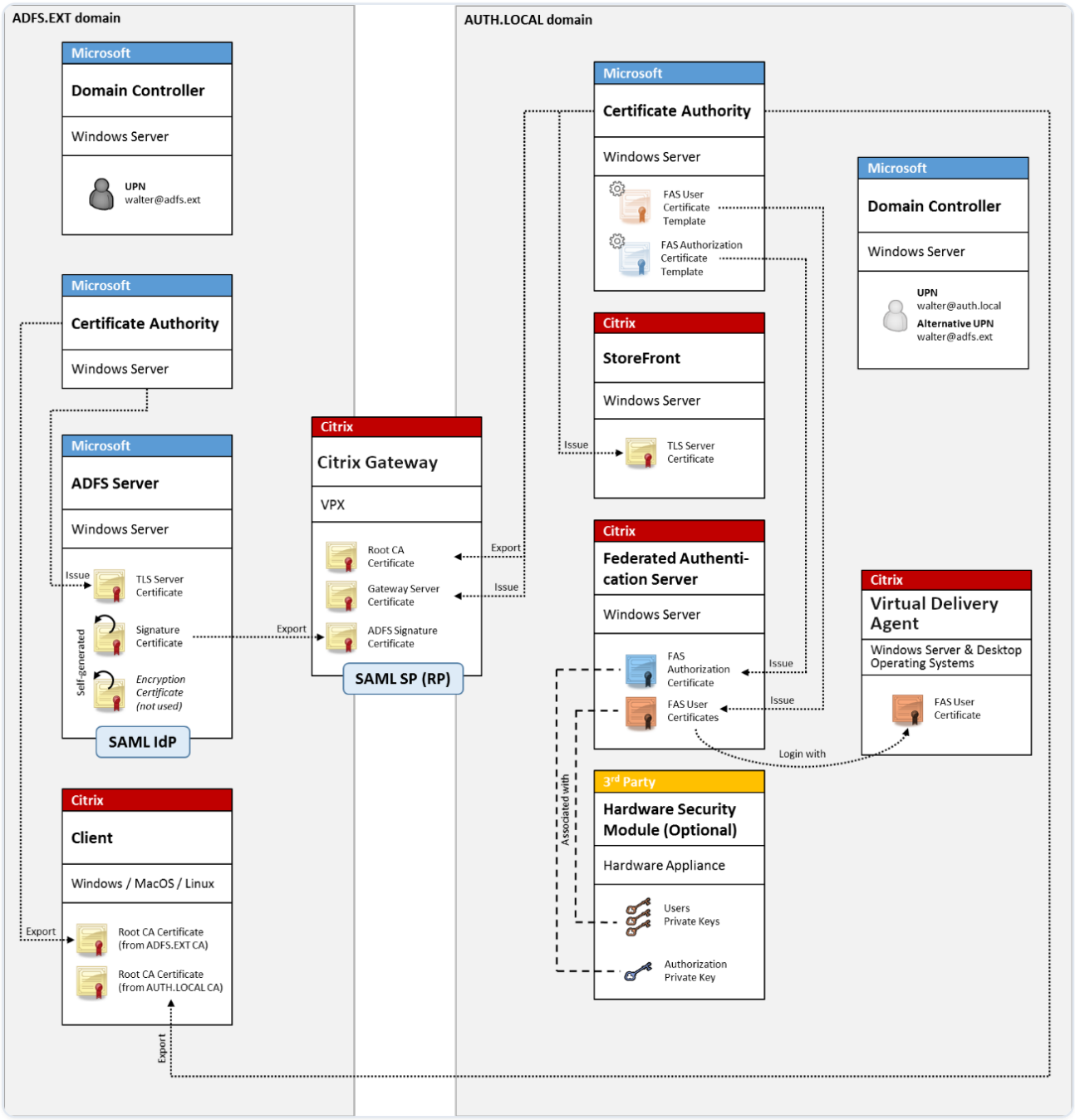
相关信息：

- ADFS 部署 文章包含详细信息。
- 安装和配置 文章介绍了如何安装和配置 FAS。
- 本文中的 Citrix Gateway 部署 部分包含配置注意事项。

B2B 帐户映射

如果两家公司希望使用彼此的计算机系统，一种常见的选择是设置一个具有信任关系的 Active Directory Federation Service (ADFS) 服务器。这允许一家公司的用户无缝地验证到另一家公司的 Active Directory (AD) 环境中。登录时，每个用户使用自己的公司登录凭据；ADFS 会自动将其映射到对等公司 AD 环境中的“影子帐户”。

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



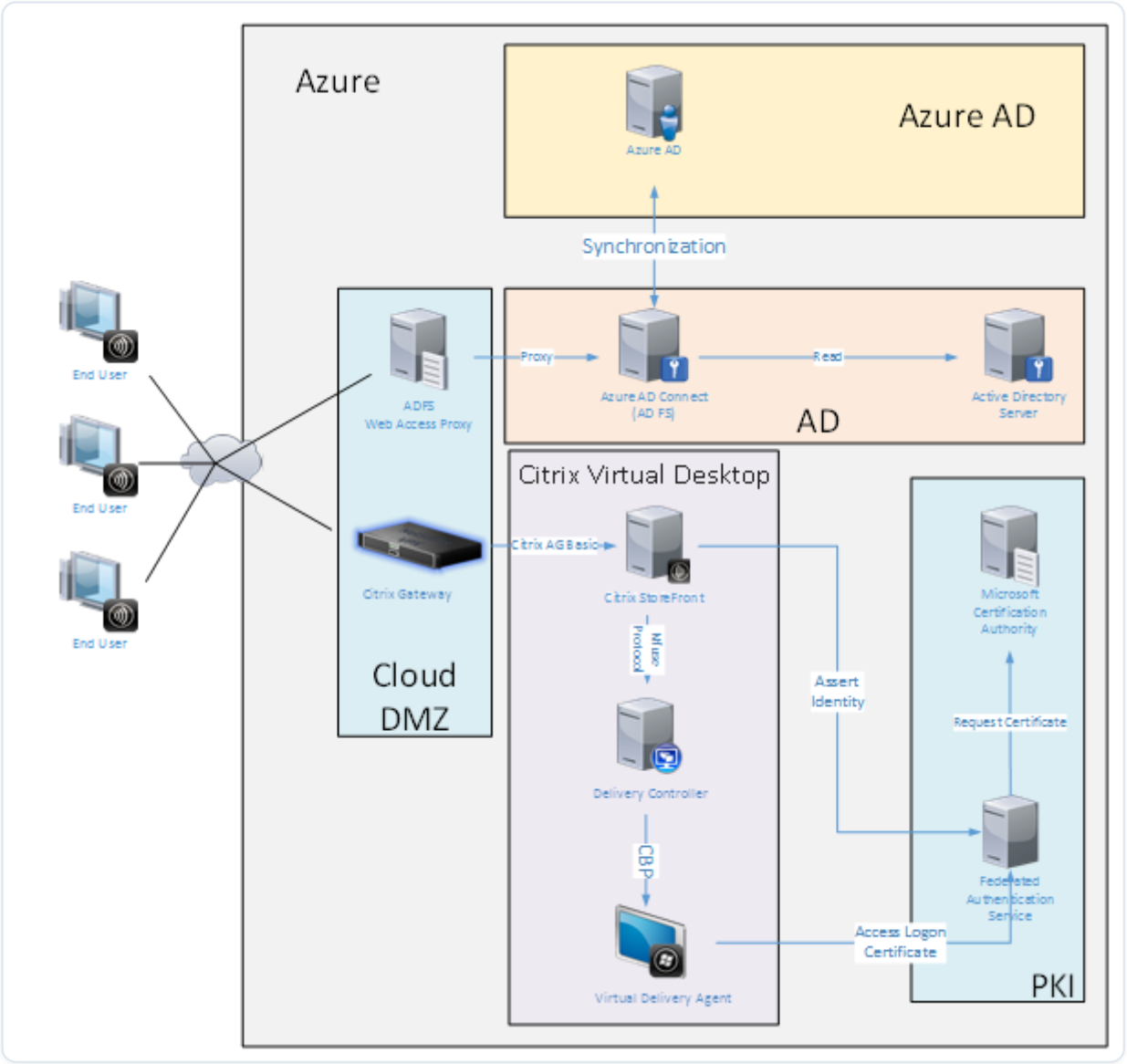
相关信息：

- 文章 安装和配置 介绍了如何安装和配置 FAS。

Windows 10 Azure 活动目录 加入

Windows 10 引入了“Azure AD 加入”的概念，它在概念上类似于传统的 Windows 域加入，但针对的是“通过互联网”的场景。这非常适用于笔记本电脑和平板电脑。与传统的 Windows 域加入一样，Azure AD 具有允许公司网站和资源使用单点登录模型的功能。这些都“支持互联网”，因此可以在任何连接互联网的位置工作，而不仅仅是办公室局域网。

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



此部署是一个示例，其中实际上没有“办公室中的最终用户”的概念。笔记本电脑使用现代 Azure AD 功能完全通过互联网进行注册和身份验证。

请注意，此部署中的基础架构可以在任何可用的 IP 地址上运行：本地、托管提供商、Azure 或其他云提供商。Azure AD Connect 同步器将自动连接到 Azure AD。示例图为了简化起见使用了 Azure VM。

相关信息：

- 文章 安装和配置 介绍了如何安装和配置 FAS。
- 文章 Azure AD 集成 包含详细信息。

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

ADFS 部署

简介

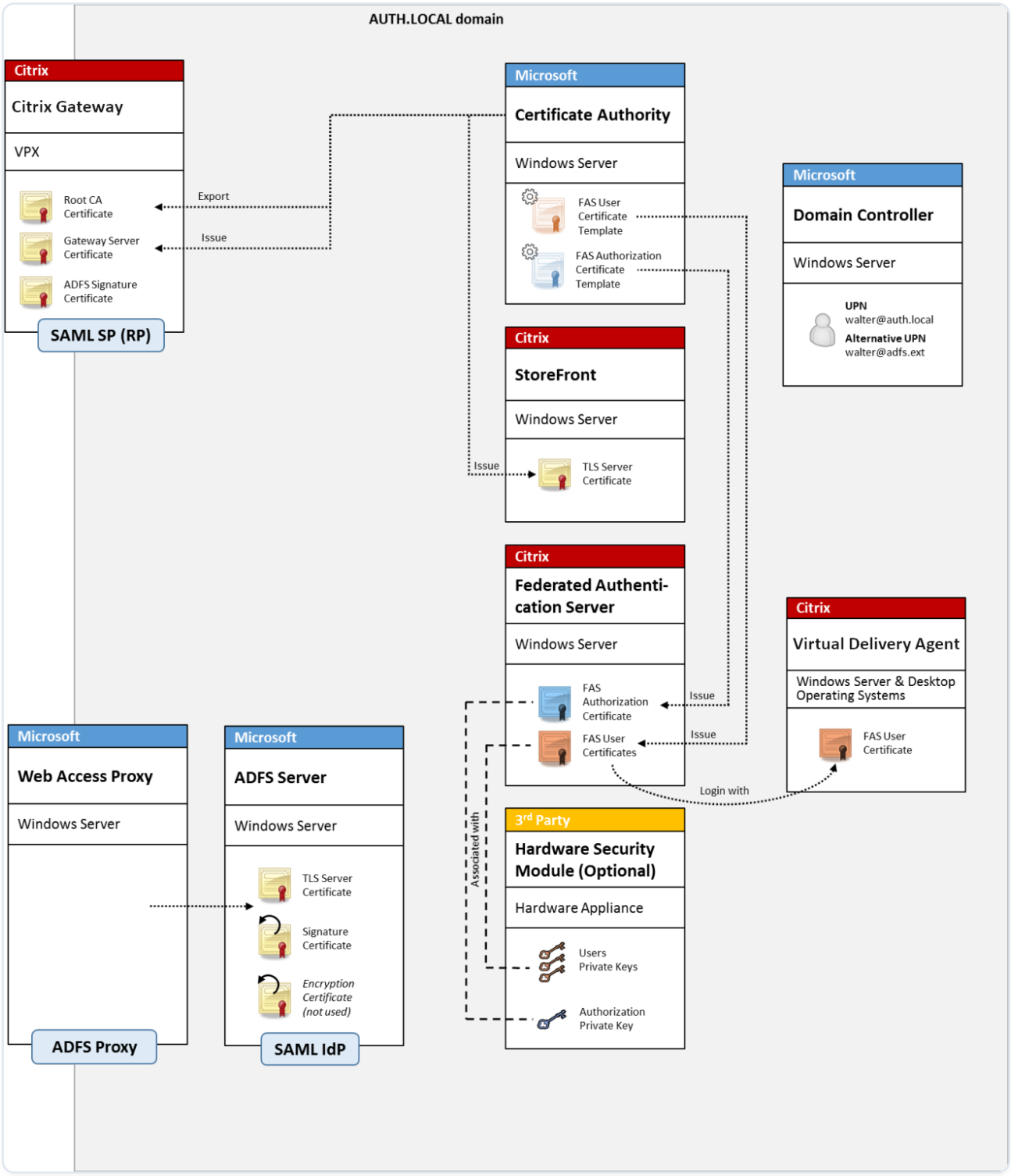
本文档介绍了如何将 Citrix 环境与 Microsoft ADFS 集成。

许多组织使用 ADFS 来管理对需要单一身份验证点的网站的安全用户访问。例如，公司可能拥有可供员工使用的额外内容和下载；这些位置需要使用标准 Windows 登录凭据进行保护。

联合身份验证服务 (FAS) 还允许将 Citrix Gateway 和 Citrix StoreFront™ 与 ADFS 登录系统集成，从而减少员工的潜在困惑。

此部署将 Citrix Gateway 作为信赖方与 Microsoft ADFS 集成。

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



注意：

无论后端资源是 Windows VDA 还是 Linux VDA，都没有区别。

SAML 概述

安全断言标记语言 (SAML) 是一种简单的“重定向到登录页面”的 Web 浏览器登录系统。配置包括以下各项：

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

重定向 URL

当 Citrix Gateway 发现用户需要进行身份验证时，它会指示用户的 Web 浏览器向 ADFS 服务器上的 SAML 登录网页执行 HTTP POST。这通常是 `https://` 形式的地址：`https://adfs.mycompany.com/adfs/ls`。

此网页 POST 包含其他信息，包括 ADFS 在登录完成后将用户返回到的“返回地址”。

标识符

EntityId 是 Citrix Gateway 在其 POST 数据中包含到 ADFS 的唯一标识符。这会告知 ADFS 用户正在尝试登录哪个服务，并根据需要应用不同的身份验证策略。如果颁发，SAML 身份验证 XML 将仅适用于登录由 EntityId 标识的服务。

通常，EntityID 是 Citrix Gateway 服务器登录页面的 URL，但它通常可以是任何内容，只要 Citrix Gateway 和 ADFS 对此达成一致即可：`https://ns.mycompany.com/application/logonpage`。

返回地址

如果身份验证成功，ADFS 会指示用户的 Web 浏览器将 SAML 身份验证 XML POST 回为 EntityId 配置的回复 URL 之一。这通常是原始 Citrix Gateway 服务器上的 `https://` 地址，格式为：`https://ns.mycompany.com/cgi/samlauth`。

如果配置了多个回复 URL 地址，Citrix Gateway 可以在其最初 POST 到 ADFS 的请求中选择一个。

签名证书

ADFS 使用其私钥对 SAML 身份验证 XML blob 进行加密签名。为了验证此签名，必须将 Citrix Gateway 配置为使用证书文件中包含的公钥检查这些签名。证书文件通常是从 ADFS 服务器获取的文本文件。

单一注销 URL

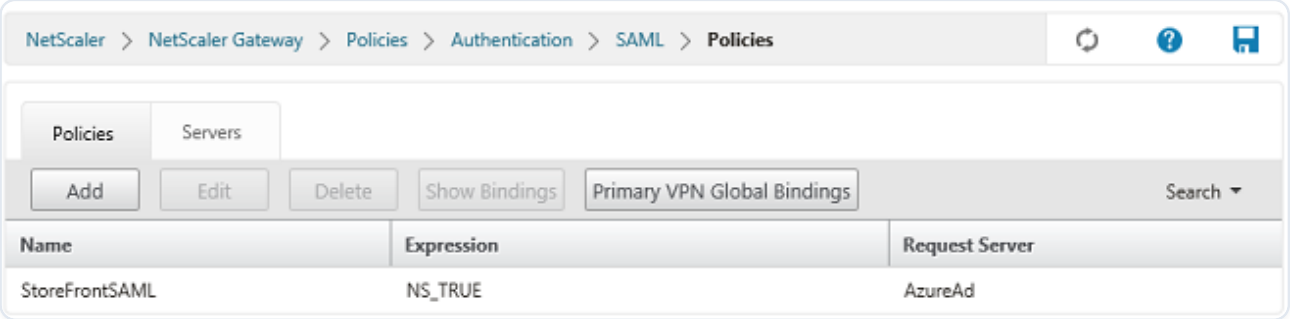
ADFS 和 Citrix Gateway 支持“集中注销”系统。这是一个 Citrix Gateway 会偶尔轮询的 URL，用于检查 SAML 身份验证 XML blob 是否仍然代表当前已登录的会话。

这是一个可选功能，无需配置。它通常是 `https://` 地址，格式为 `https://adfs.mycompany.com/adfs/logout`。（请注意，它可以与单一登录 URL 相同。）

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

配置

Citrix Gateway 部署 部分介绍了如何设置 Citrix Gateway 以处理标准 LDAP 身份验证选项。成功完成后，您可以在 Citrix Gateway 上创建新的身份验证策略，以允许 SAML 身份验证。然后，这可以替换 Citrix Gateway 向导使用的默认 LDAP 策略。



填写 SAML 策略

使用之前从 ADFS 管理控制台获取的信息配置新的 SAML IdP 服务器。应用此策略后，Citrix Gateway 会将用户重定向到 ADFS 进行登录，并接受 ADFS 签名的 SAML 身份验证令牌作为回报。

本地化图像(/en-us/federated-authentication-service/2402-ltsr/media/fas-adfs-create-auth-saml-server.png)

相关信息

- 安装和配置 是 FAS 安装和配置的主要参考。
- 常见的 FAS 部署在部署架构 文章中进行了总结。
- “操作方法”文章在高级配置 文章中介绍。

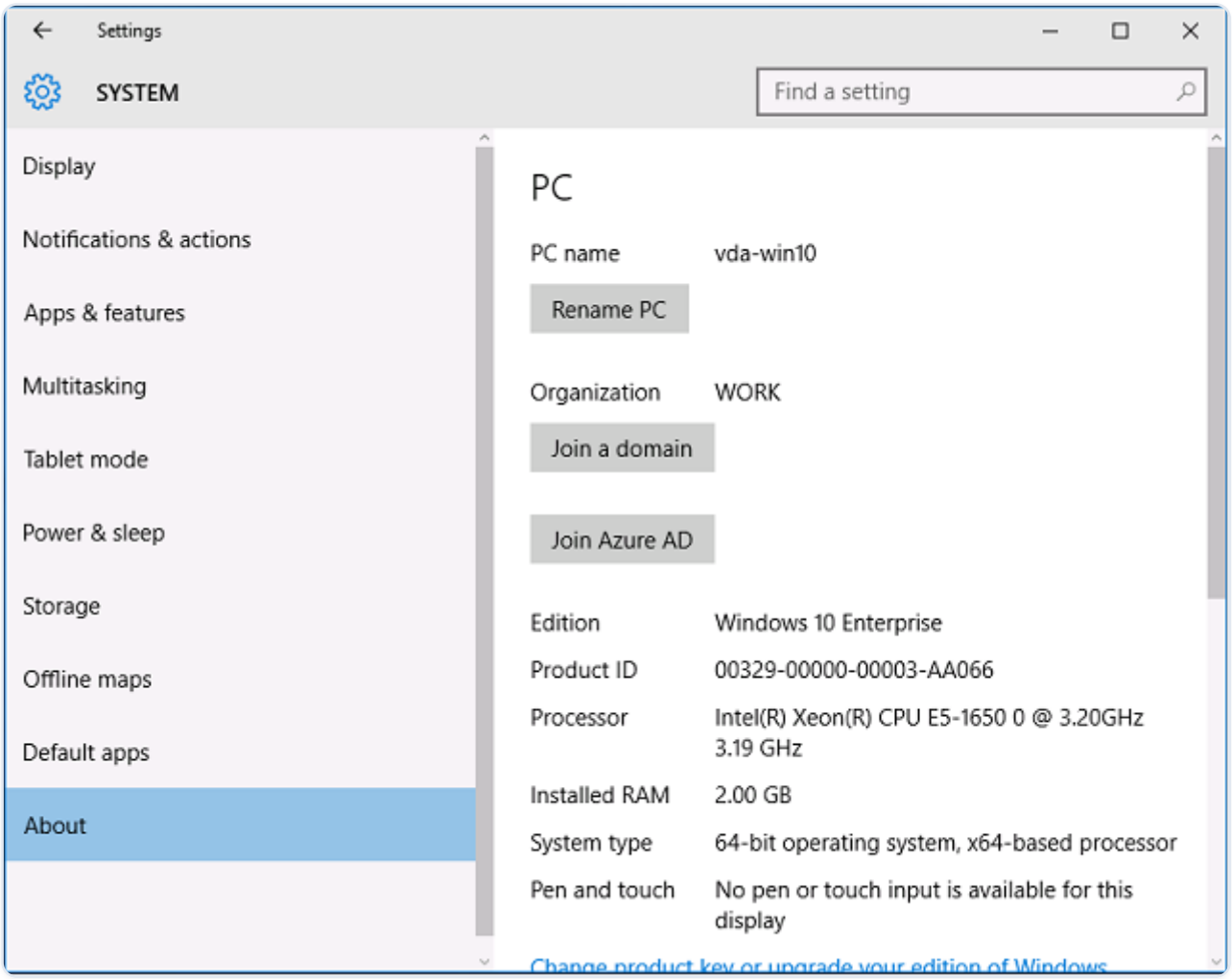
Azure AD 集成

简介

本文档介绍了如何将 Citrix 环境与 Windows 10 Azure AD 功能集成。Windows 10 引入了 Azure AD，这是一种新的域加入模型，漫游笔记本电脑可以通过 Internet 加入公司域，以实现管理和单点登录。

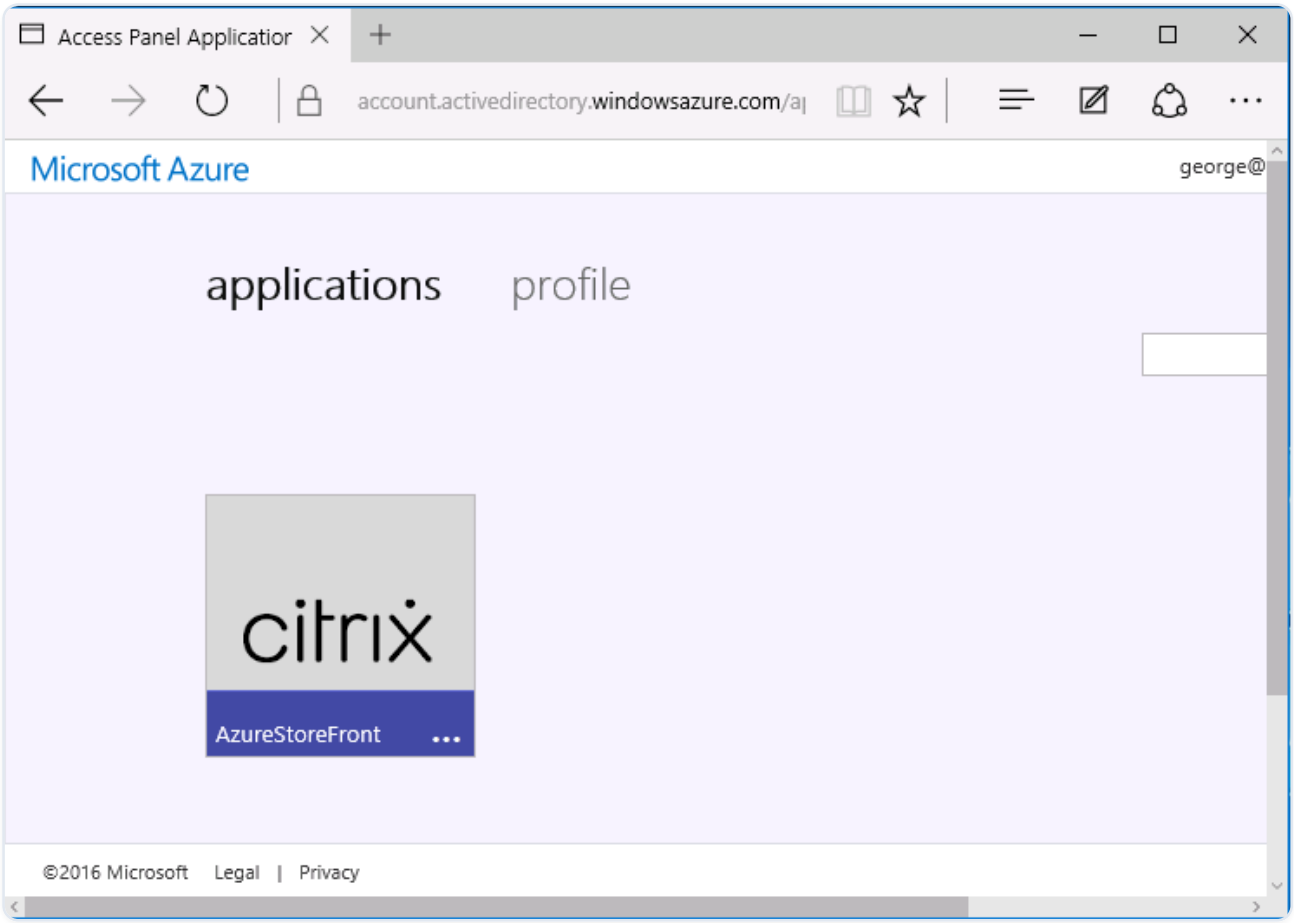
本文档中的示例部署描述了一个系统，其中 IT 部门为新用户提供公司电子邮件地址和注册码，供其个人 Windows 10 笔记本电脑使用。用户可以通过“**设置**”面板中的“**系统 > 关于 > 加入 Azure AD**”选项访问此代码。

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



笔记本电脑注册后，Microsoft Edge Web 浏览器将通过 Azure SaaS 应用程序网页自动登录公司网站和 Citrix 发布的应用程序，以及其他 Azure 应用程序（例如 Office 365）。

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

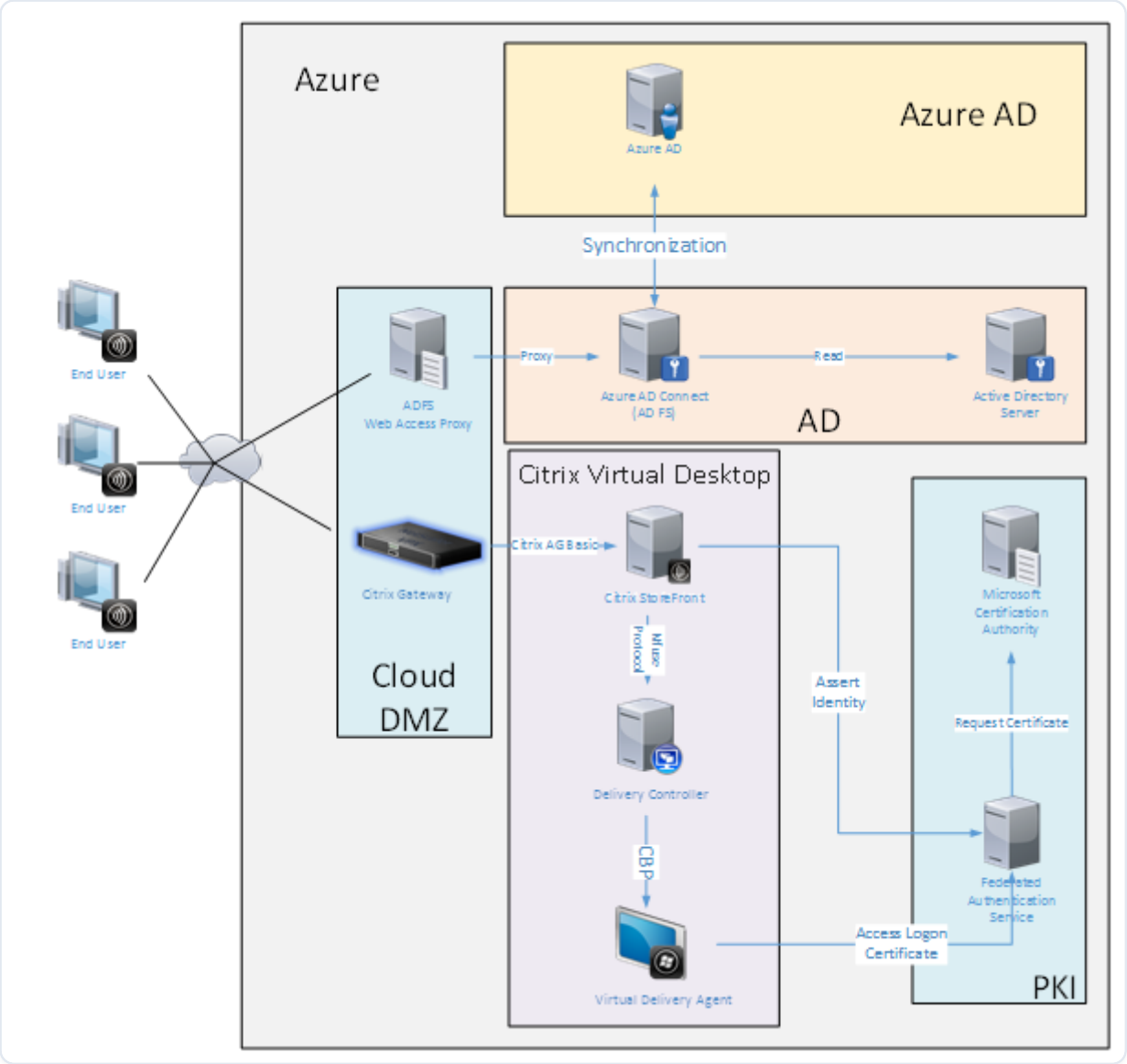


体系结构

此体系结构在 Azure 中完全复制了传统的公司网络，并与 Azure AD 和 Office 365 等现代云技术集成。最终用户都被视为远程工作人员，没有在办公室内部网络上的概念。

该模型可应用于拥有现有本地系统的公司，因为 Azure AD Connect Synchronization 可以通过 Internet 连接到 Azure。

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



在此体系结构中，传统上由防火墙 LAN 和 Kerberos/NTLM 身份验证实现的安全连接和单点登录，被替换为到 Azure 的 TLS 连接和 SAML。新服务作为加入 Azure AD 的 Azure 应用程序构建。需要 Active Directory 的现有应用程序（例如 SQL Server 数据库）可以使用 Azure 云服务的 IAAS 部分中的标准 Active Directory 服务器 VM 运行。

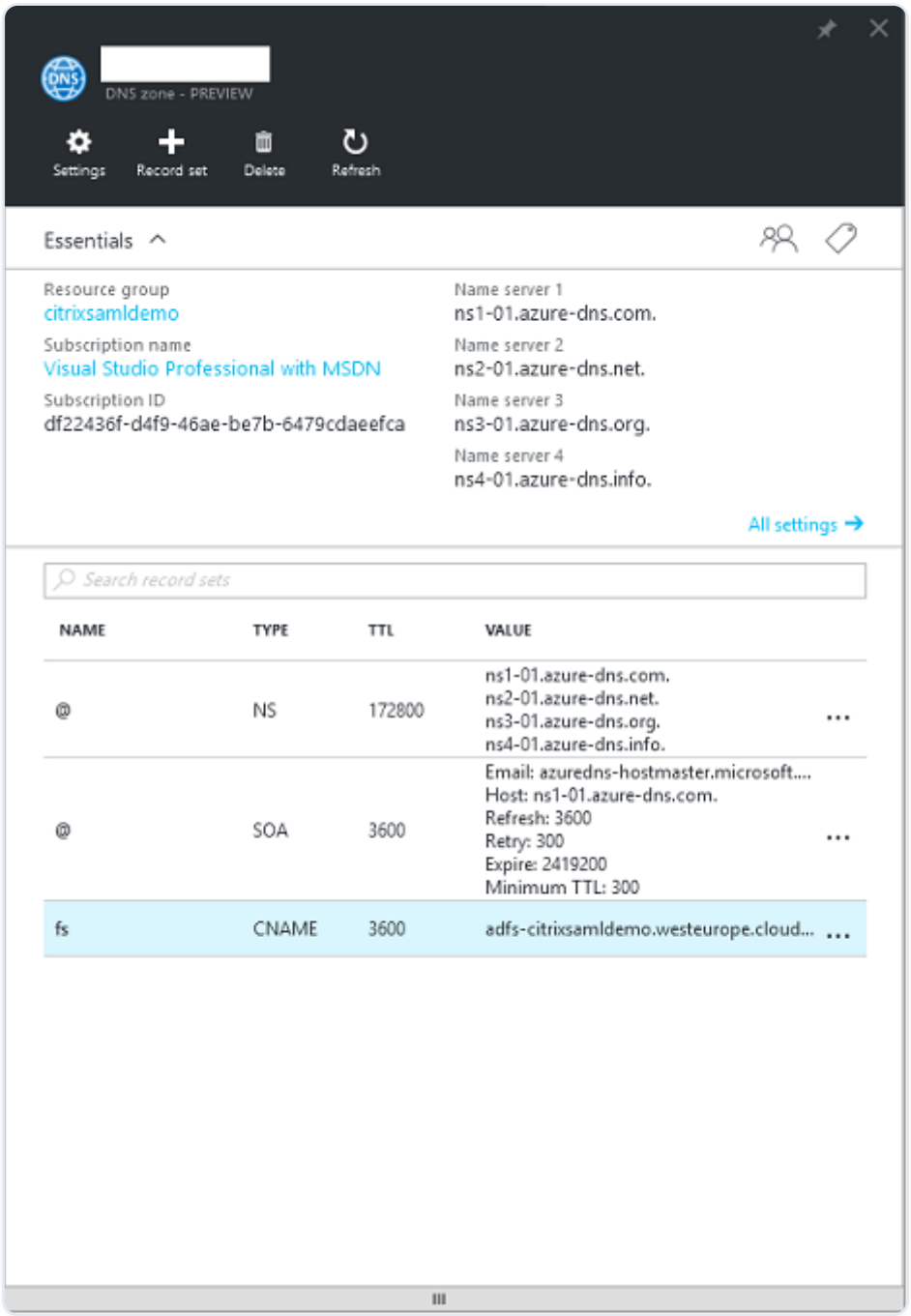
当用户启动传统应用程序时，他们通过 Citrix Virtual Apps and Desktops™ 发布的应用程序进行访问。不同类型的应用程序通过用户的“**Azure 应用程序**”页面，使用 Microsoft Edge 单点登录功能进行整理。Microsoft 还提供可以枚举和启动 Azure 应用程序的 Android 和 iOS 应用程序。

创建 DNS 区域

Azure AD 要求管理员已注册公共 DNS 地址并控制域名后缀的委派区域。为此，管理员可以使用 Azure DNS 区域功能。

此示例使用 DNS 区域名称 *citrixsamldemo.net*。

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



控制台显示 Azure DNS 名称服务器的名称。这些名称应在 DNS 注册商的区域 NS 条目中引用（例如，`citrixsamldemo.net. NS n1-01.azure-dns.com`）

在添加对 Azure 中运行的 VM 的引用时，最简单的方法是使用 CNAME 指针指向 VM 的 Azure 托管 DNS 记录。如果 VM 的 IP 地址发生更改，则无需手动更新 DNS 区域文件。

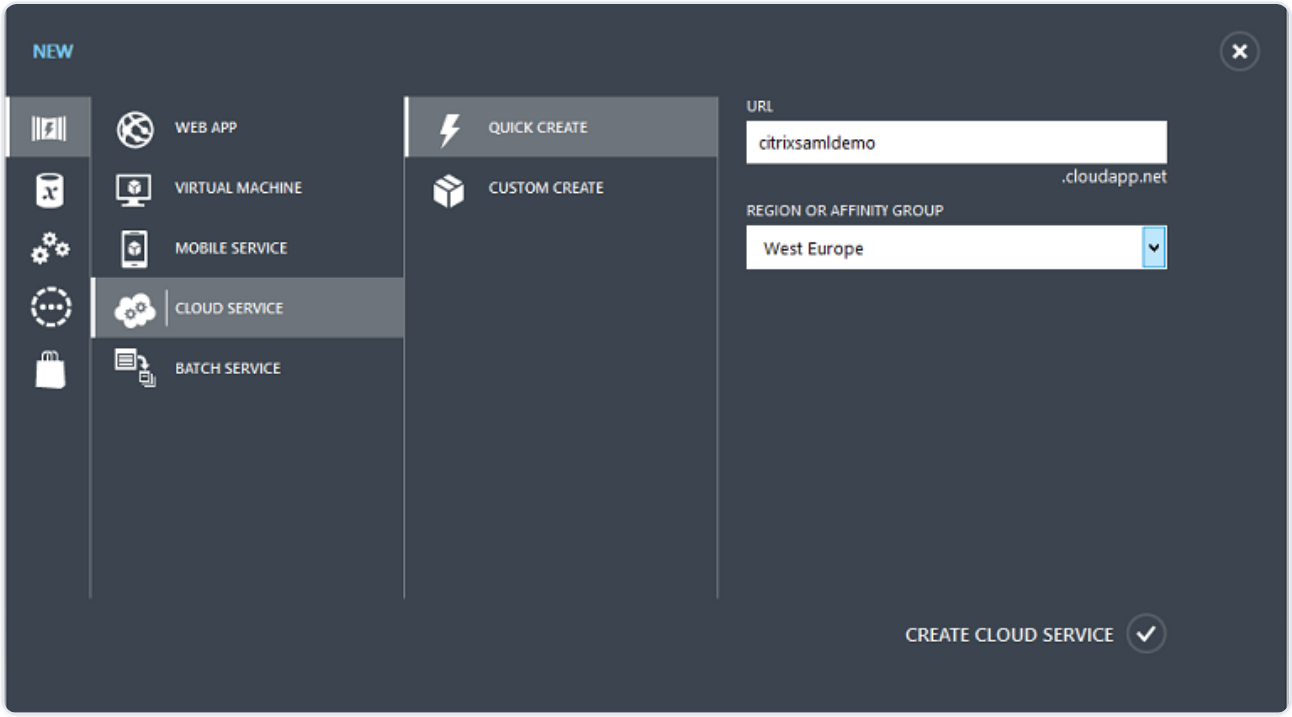
此部署的内部和外部 DNS 地址后缀将匹配。域为 citrixsamldemo.net，并使用拆分 DNS（内部为 10.0.0.*）。

添加一个引用 Web 应用程序代理服务器的“fs.citrixsamldemo.net”条目。这是此区域的联合服务。

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

创建云服务

此示例配置了一个 Citrix 环境，其中包括一个在 Azure 中运行 ADFS 服务器的 AD 环境。创建了一个名为“citrixsamldemo.”的云服务。

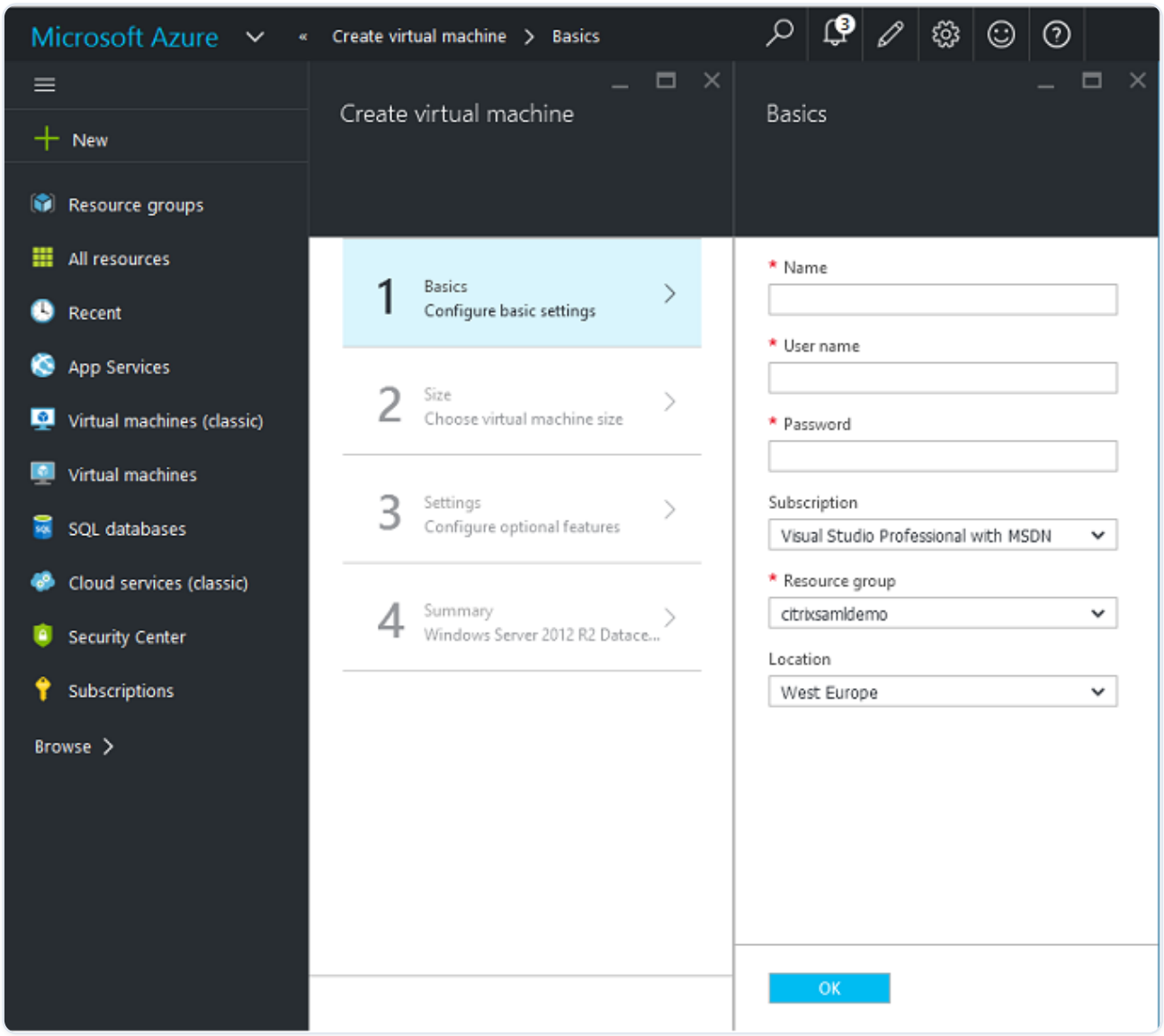


创建 Windows 虚拟机

在云服务中创建五个 Windows VM：

- 域控制器 (domaincontrol)
- Azure Connect ADFS 服务器 (adfs)
- ADFS Web 访问代理（Web 应用程序代理，未加入域）
- Citrix Virtual Apps and Desktops 交付控制器
- Citrix Virtual Apps and Desktops 虚拟投递代理 (VDA)

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



域控制器

- 添加 **DNS 服务器** 和 **Active Directory 域服务** 角色以创建标准 Active Directory 部署（在此示例中为 citrixsamldemo.net）。域升级完成后，添加 **Active Directory 证书服务** 角色。
- 创建用于测试的普通用户帐户（例如，George@citrixsamldemo.net）。
- 由于此服务器将运行内部 DNS，因此所有服务器都应引用此服务器进行 DNS 解析。这可以通过 **Azure DNS 设置** 页面完成。（有关详细信息，请参阅本文档中的附录。）

ADFS 控制器和 Web 应用程序代理服务器

- 将 ADFS 服务器加入 citrixsamldemo 域。Web 应用程序代理服务器应保留在隔离的工作组中，因此请手动向 AD DNS 注册 DNS 地址。
- 在这些服务器上运行 **Enable-PSRemoting –Force** cmdlet，以允许 AzureAD Connect 工具通过防火墙进行 PS 远程处理。

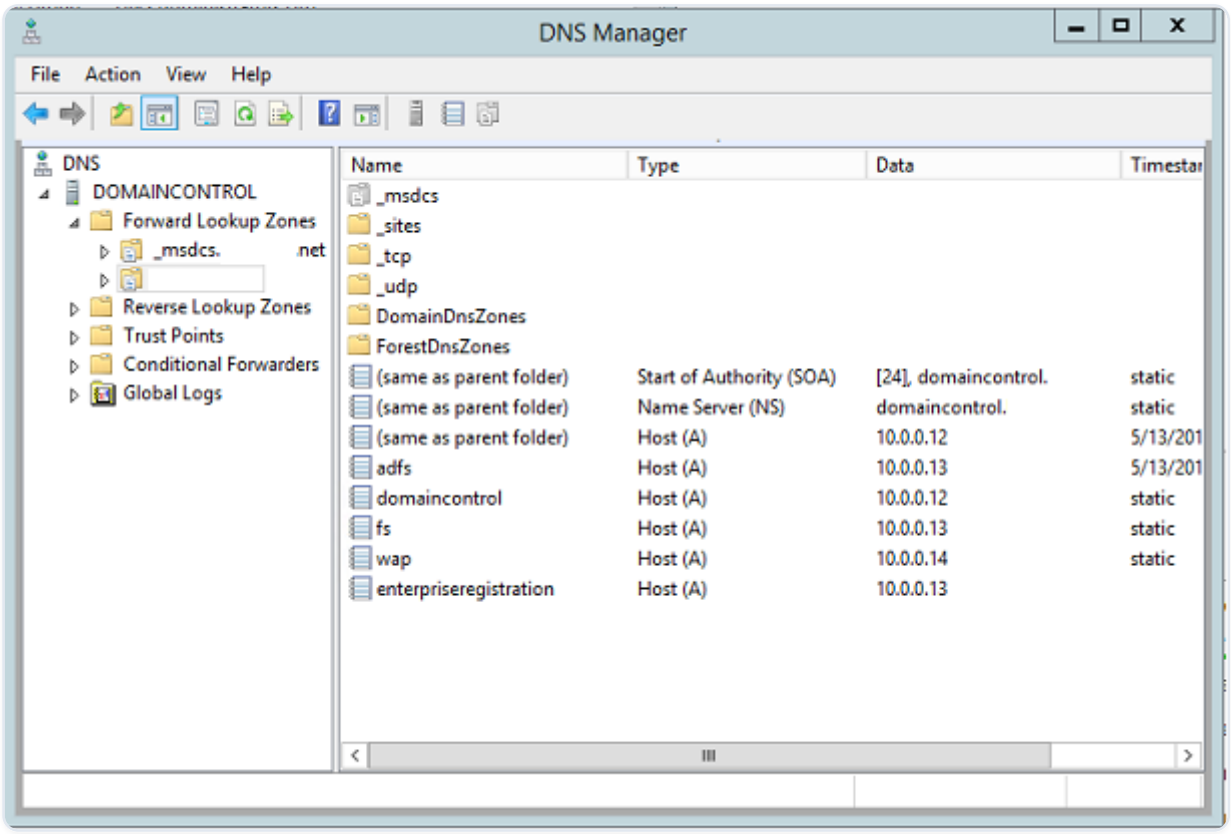
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix Virtual Desktops™ 投递控制器和 VDA

- 在已加入 citrixsamldemo 的其余两台 Windows 服务器上安装 Citrix Virtual Apps 或 Citrix Virtual Desktops Delivery Controller™ 和 VDA。

配置内部 DNS

安装域控制器后，配置 DNS 服务器以处理 citrixsamldemo.net 的内部视图，并充当外部 DNS 服务器（例如：8.8.8.8）的转发器。

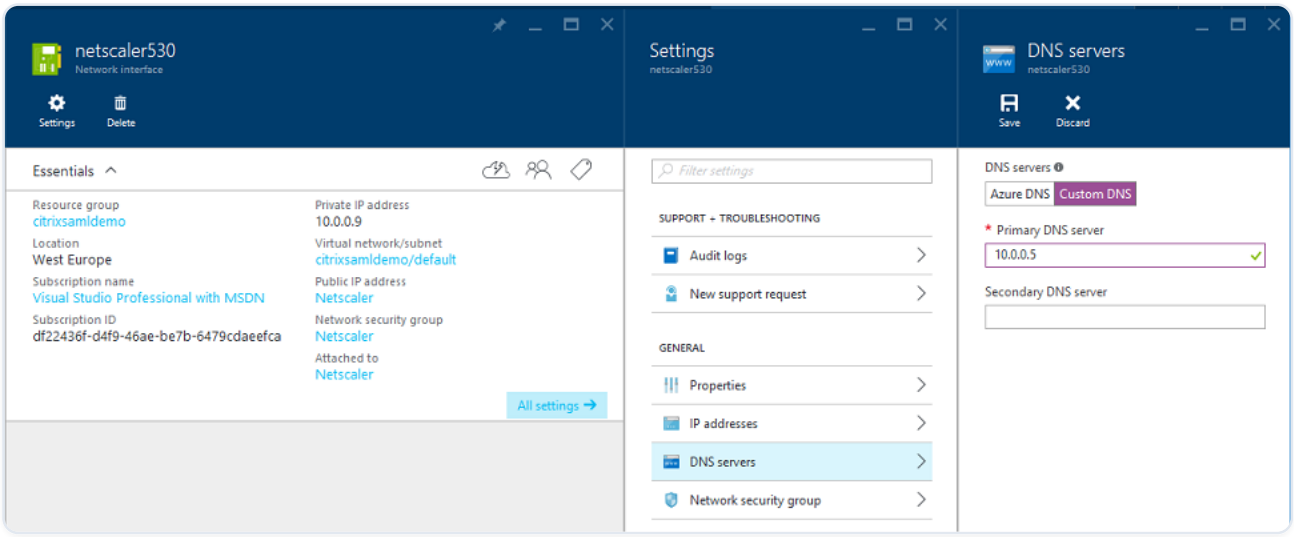


添加静态记录，用于：

- wap.citrixsamldemo.net
- fs.citrixsamldemo.net
- enterpriseregistration.citrixsaml.net

所有在 Azure 中运行的 VM 都应配置为仅使用此 DNS 服务器。您可以通过网络接口 GUI 执行此操作。

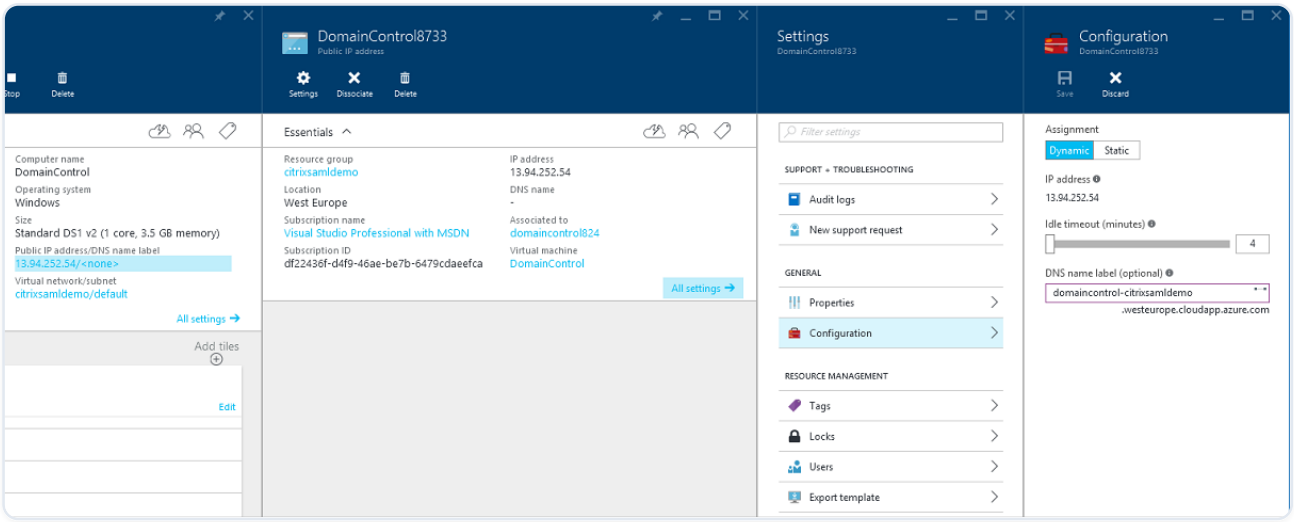
© 1997–2026 Citrix Systems, Inc. All rights reserved.



默认情况下，内部 IP (10.0.0.9) 地址是动态分配的。您可以使用 IP 地址设置永久分配 IP 地址。Web 应用程序代理服务器和域控制器都应执行此操作。

配置外部 DNS 地址

当 VM 运行时，Azure 会维护自己的 DNS 区域服务器，该服务器指向分配给 VM 的当前公共 IP 地址。这是一个有用的功能，因为 Azure 默认在每个 VM 启动时分配 IP 地址。



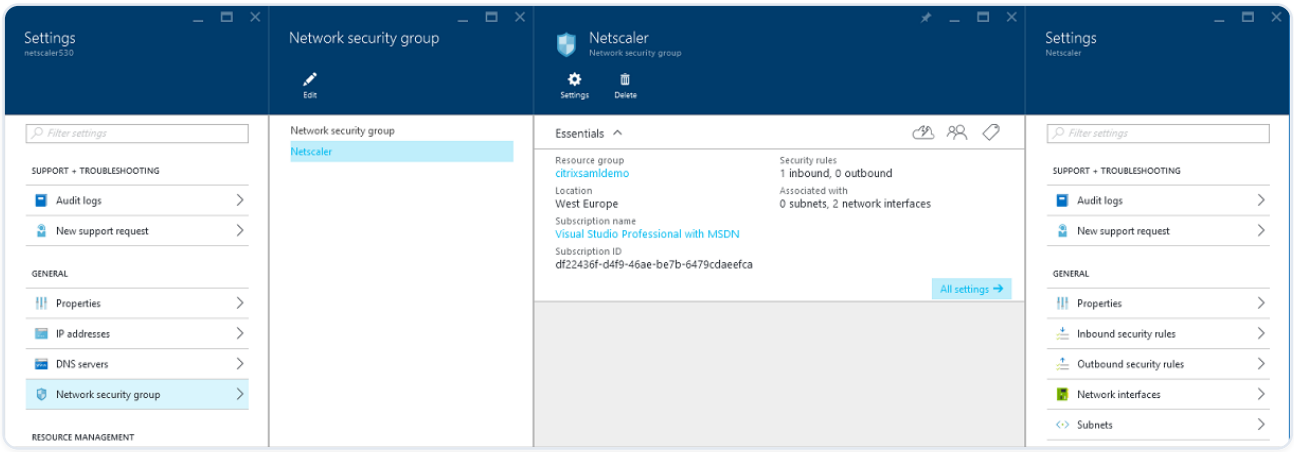
此示例将 DNS 地址 domaincontrol-citrixsamldemo.westeurope.cloudapp.azure.com 分配给域控制器。

请注意，远程配置完成后，只有 Web 应用程序代理和 Citrix Gateway VM 应启用公共 IP 地址。（在配置期间，公共 IP 地址用于 RDP 访问环境）。

配置安全组

Azure 云使用安全组管理从 Internet 到 VM 的 TCP/UDP 访问的防火墙规则。默认情况下，所有 VM 都允许 RDP 访问。Citrix Gateway 和 Web 应用程序代理服务器也应允许端口 443 上的 TLS。

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



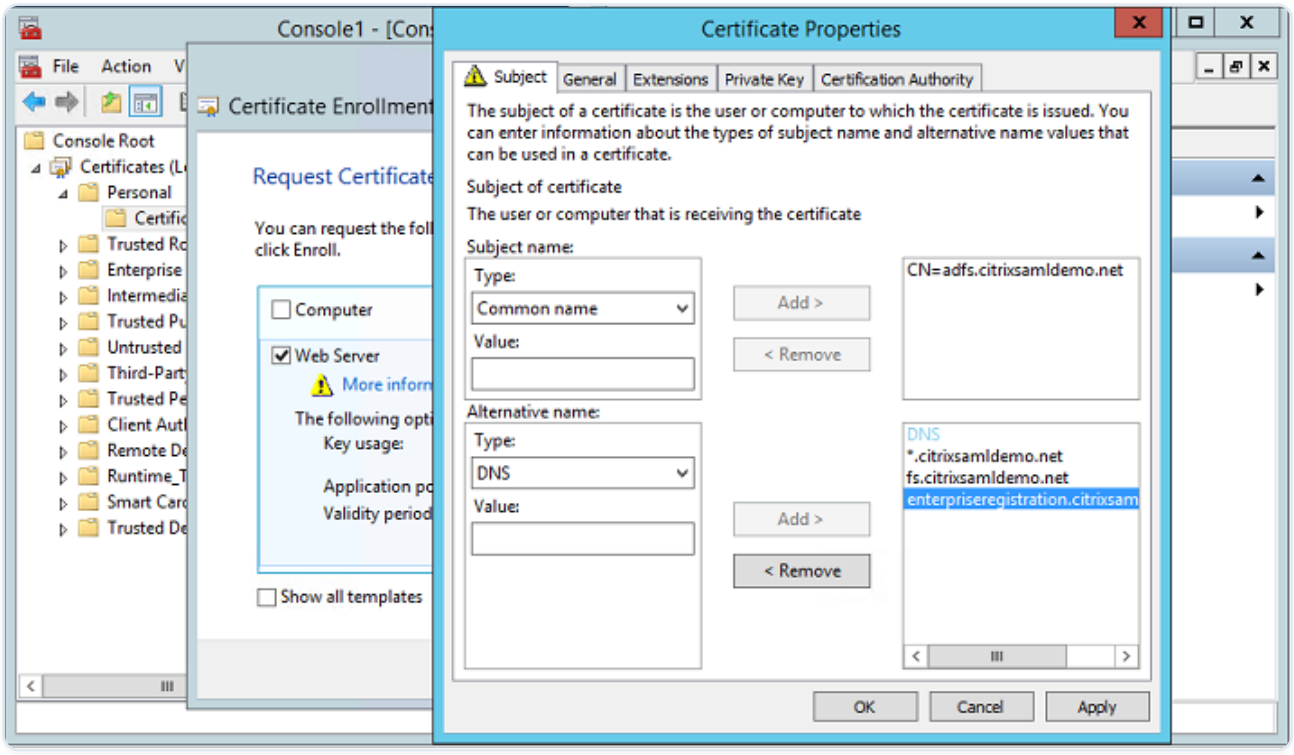
创建 ADFS 证书

在 Microsoft 证书颁发机构上启用 **Web 服务器**证书模板。这允许创建具有自定义 DNS 地址的证书，该证书可以导出（包括私钥）到 pfx 文件。您必须在 ADFS 和 Web 应用程序代理服务器上安装此证书，因此 PFX 文件是首选选项。

颁发具有以下主题名称的 Web 服务器证书：

- 通用名称：
  - adfs.citrixsamldemo.net
- 主题备用名称：
  - *.citrixsamldemo.net
  - fs.citrixsamldemo. 网络
  - enterpriseregistration.citrixsamldemo.net

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



将证书导出到 pfx 文件，包括受密码保护的私钥。

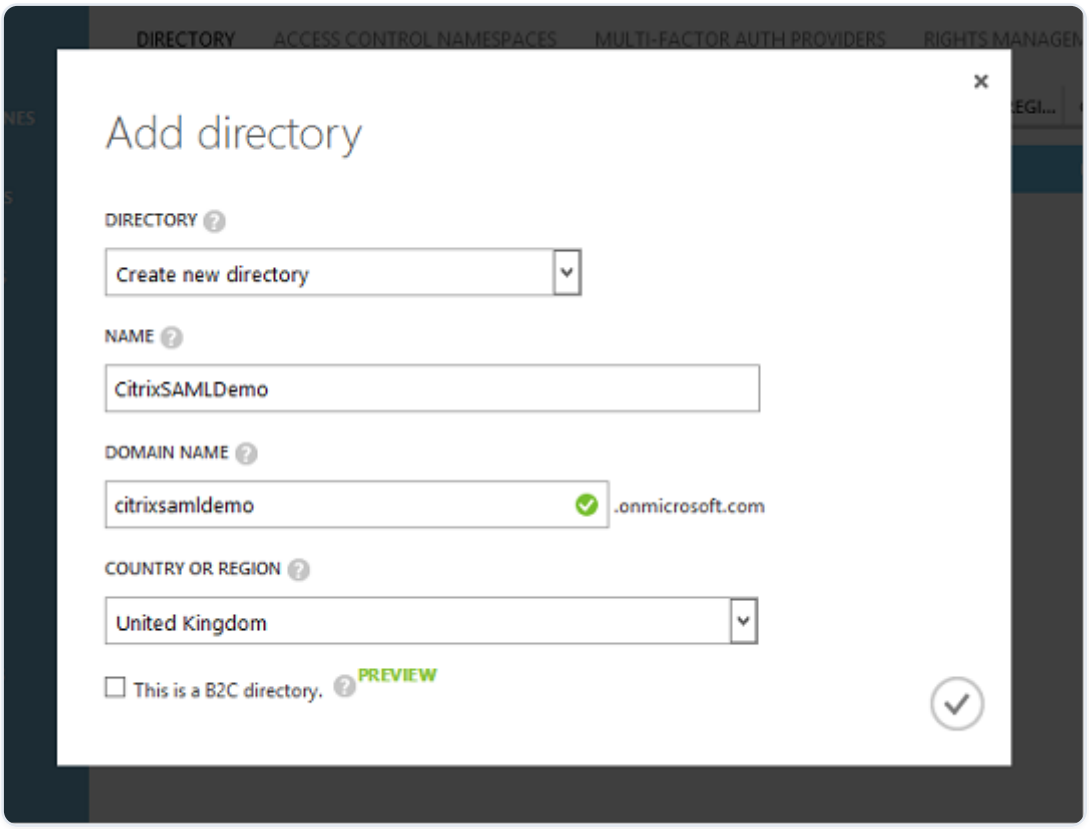
设置 Azure AD

本节详细介绍了设置新的 Azure AD 实例以及创建可用于将 Windows 10 加入 Azure AD 的用户身份的过程。

创建新目录

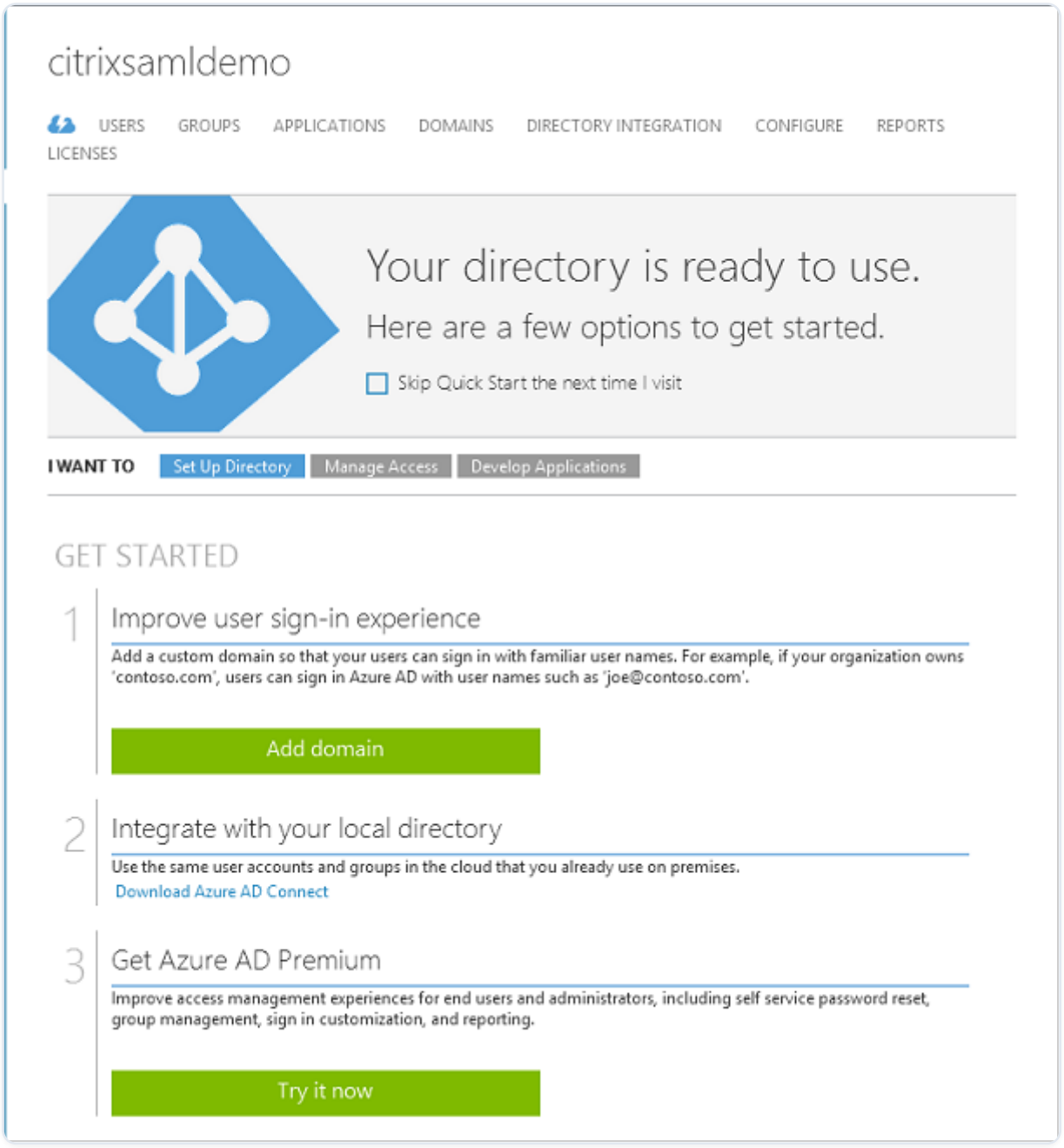
登录到经典 Azure 门户并创建新目录。

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



完成后，将显示摘要页面。

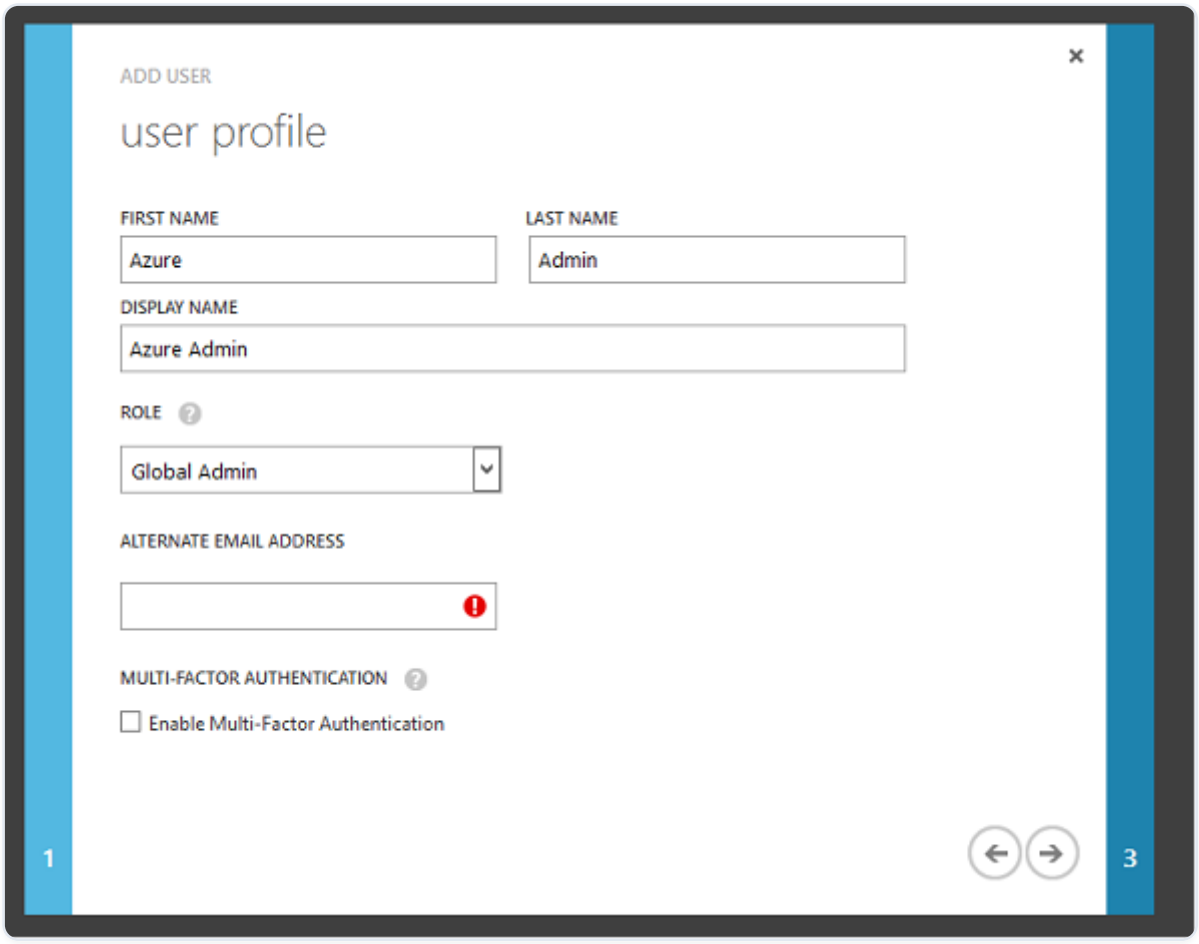
© 1997–2026 Citrix Systems, Inc. All rights reserved.



创建全局管理员用户 (AzureAdmin)

在 Azure 中创建全局管理员（在此示例中为 `AzureAdmin@citrixsamldemo.onmicrosoft.com`），并使用新帐户登录以设置密码。

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



向 Azure AD 注册您的域

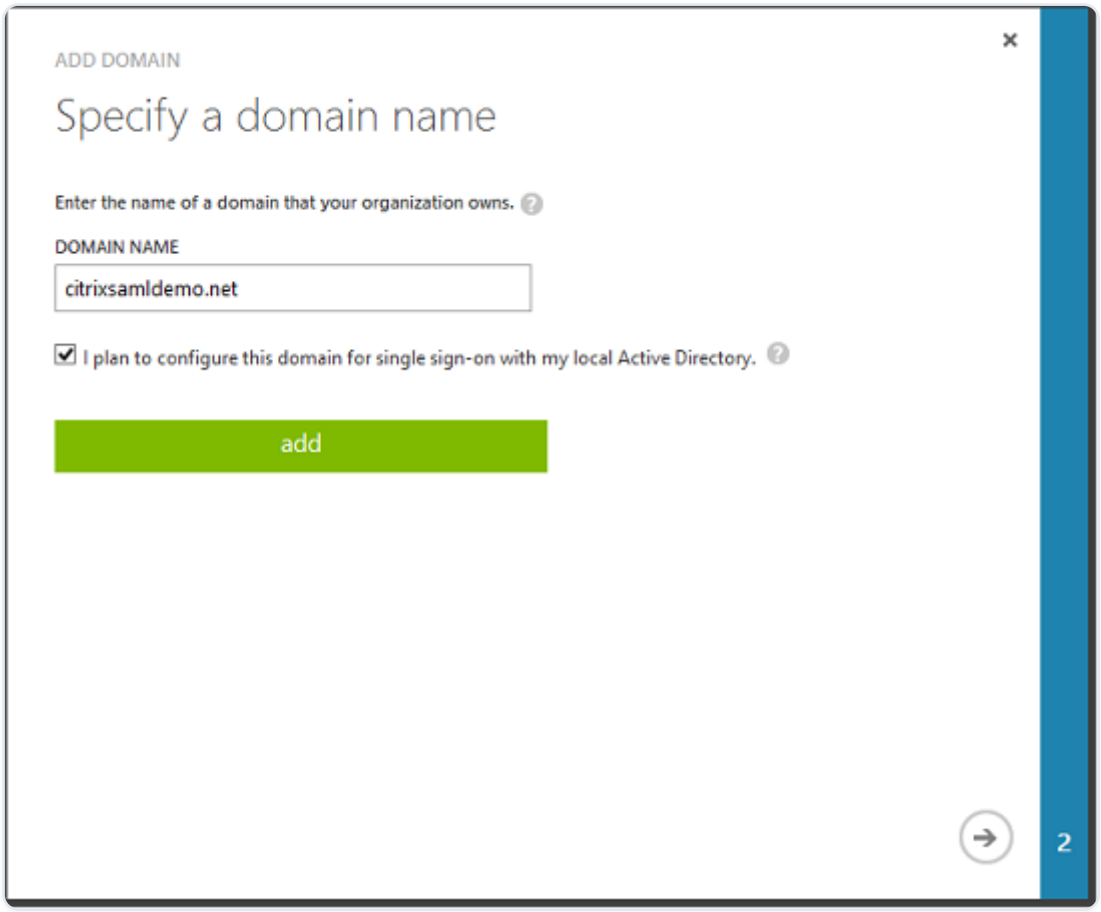
默认情况下，用户通过以下形式的电子邮件地址进行标识：`<user.name>@<company>.onmicrosoft.com`。

尽管这无需进一步配置即可工作，但标准格式的电子邮件地址更好，最好是与最终用户的电子邮件帐户匹配的电子邮件地址：`<user.name>@<company>.com`。

添加域操作可配置从您的真实公司域进行的重定向。此示例使用 `citrixsamldemo.net`。

如果要为单点登录设置 ADFS，请启用该复选框。

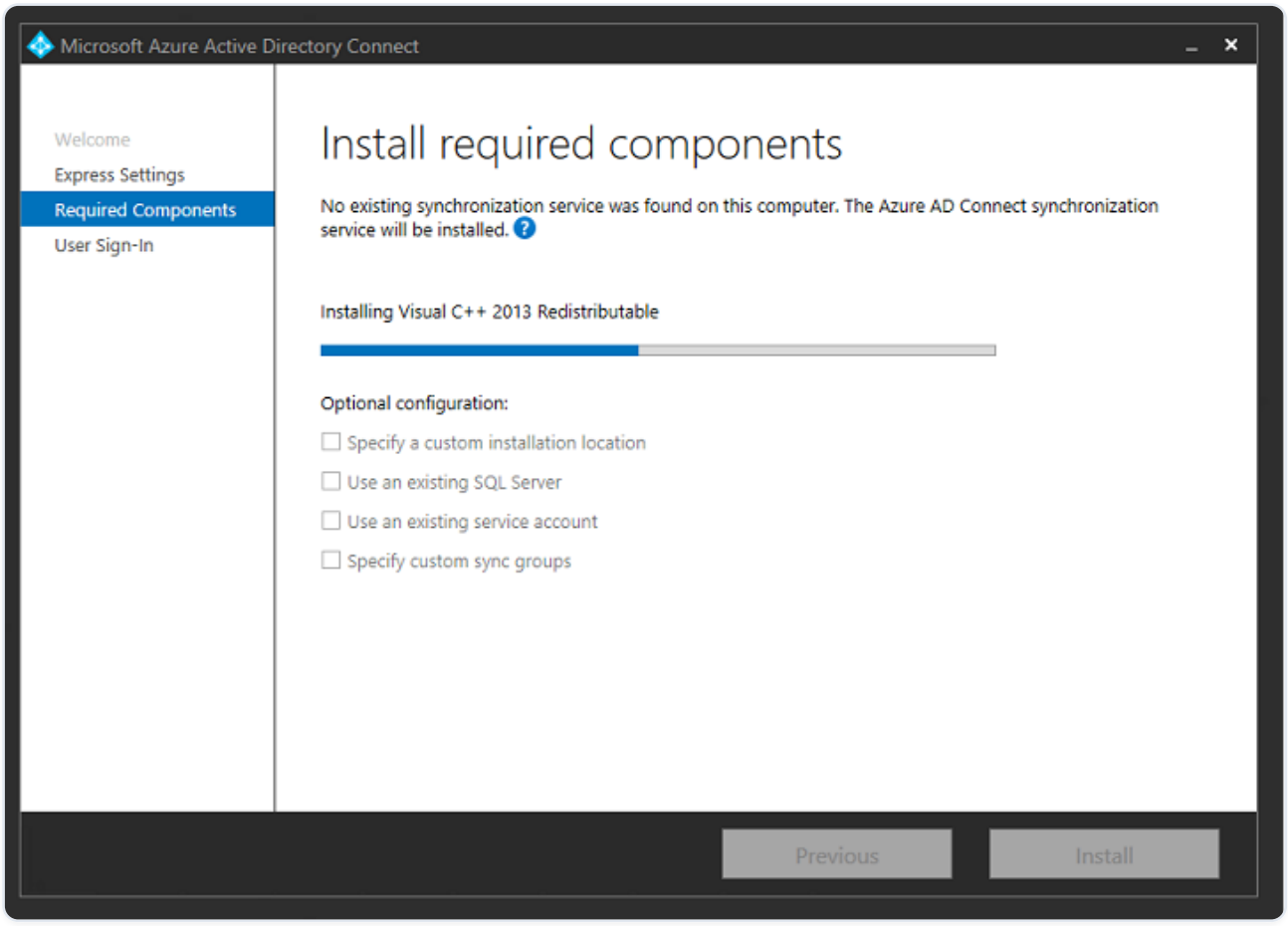
© 1997–2026 Citrix Systems, Inc. All rights reserved.



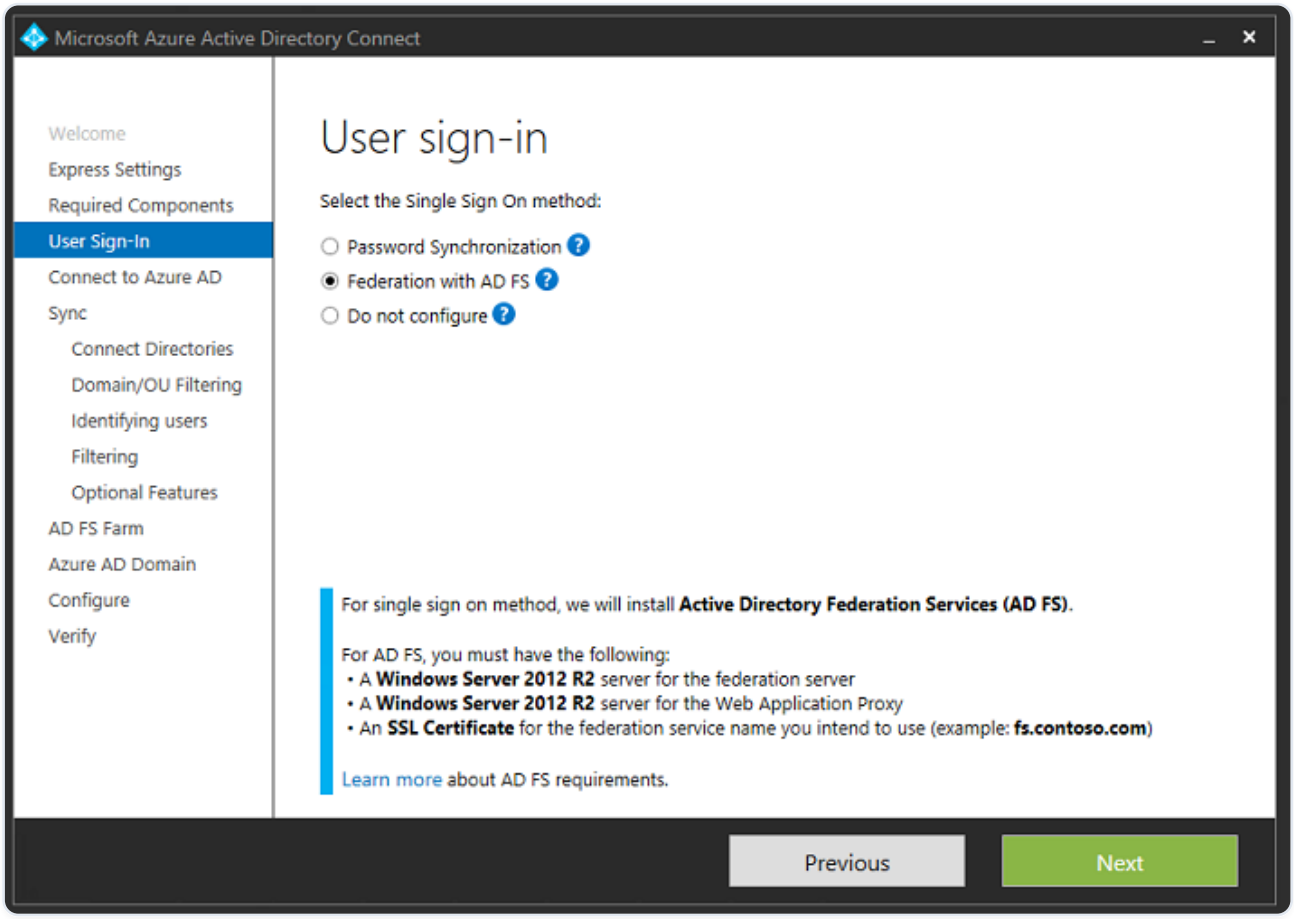
安装 Azure AD 连接

Azure AD 配置 GUI 的第 2 步将重定向到 Microsoft Azure AD Connect 下载页面。在 ADFS VM 上安装此项。使用**自定义安装**而不是**快速设置**，以便可以使用 ADFS 选项。

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

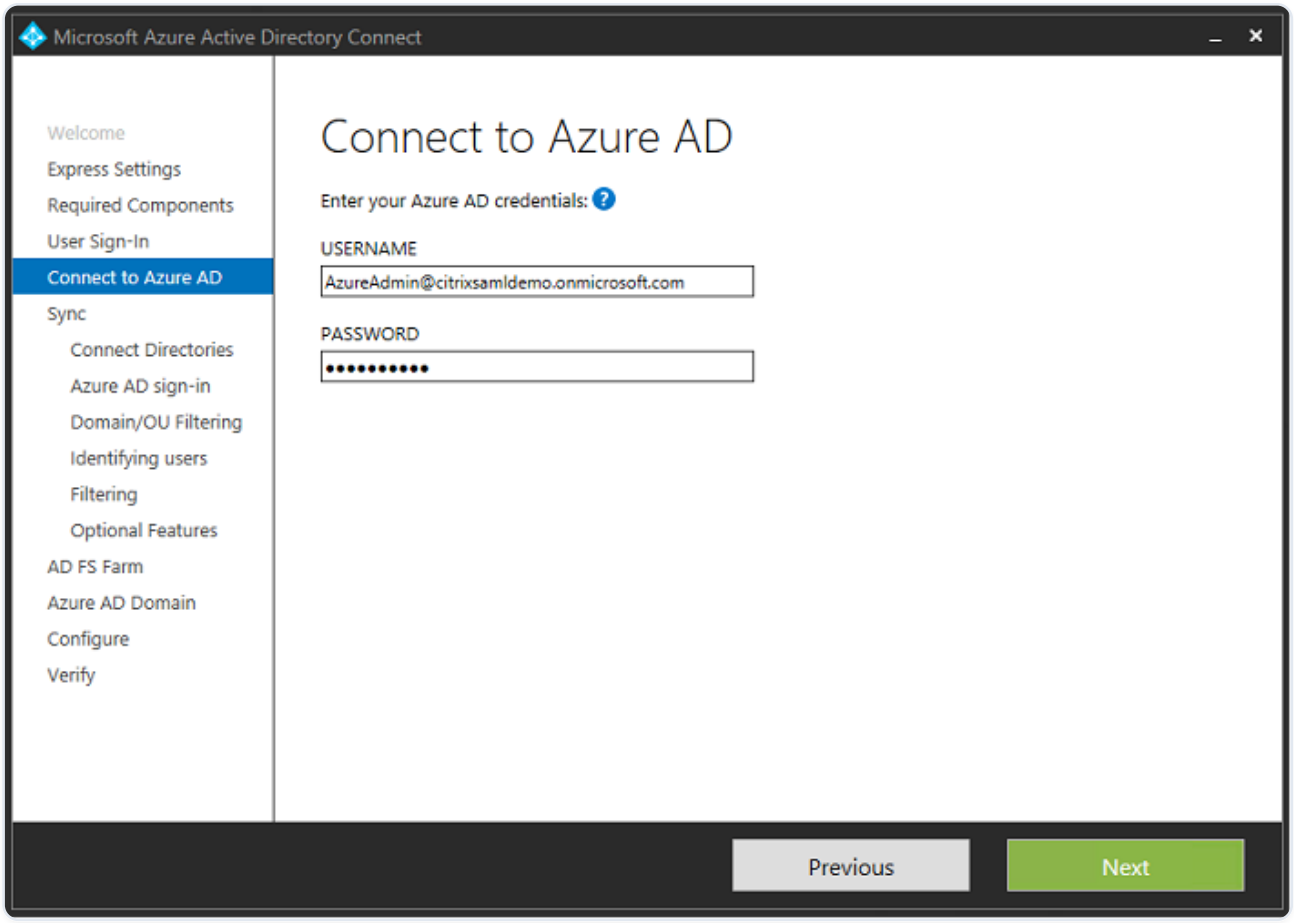


选择**与 AD FS 联合**单点登录选项。



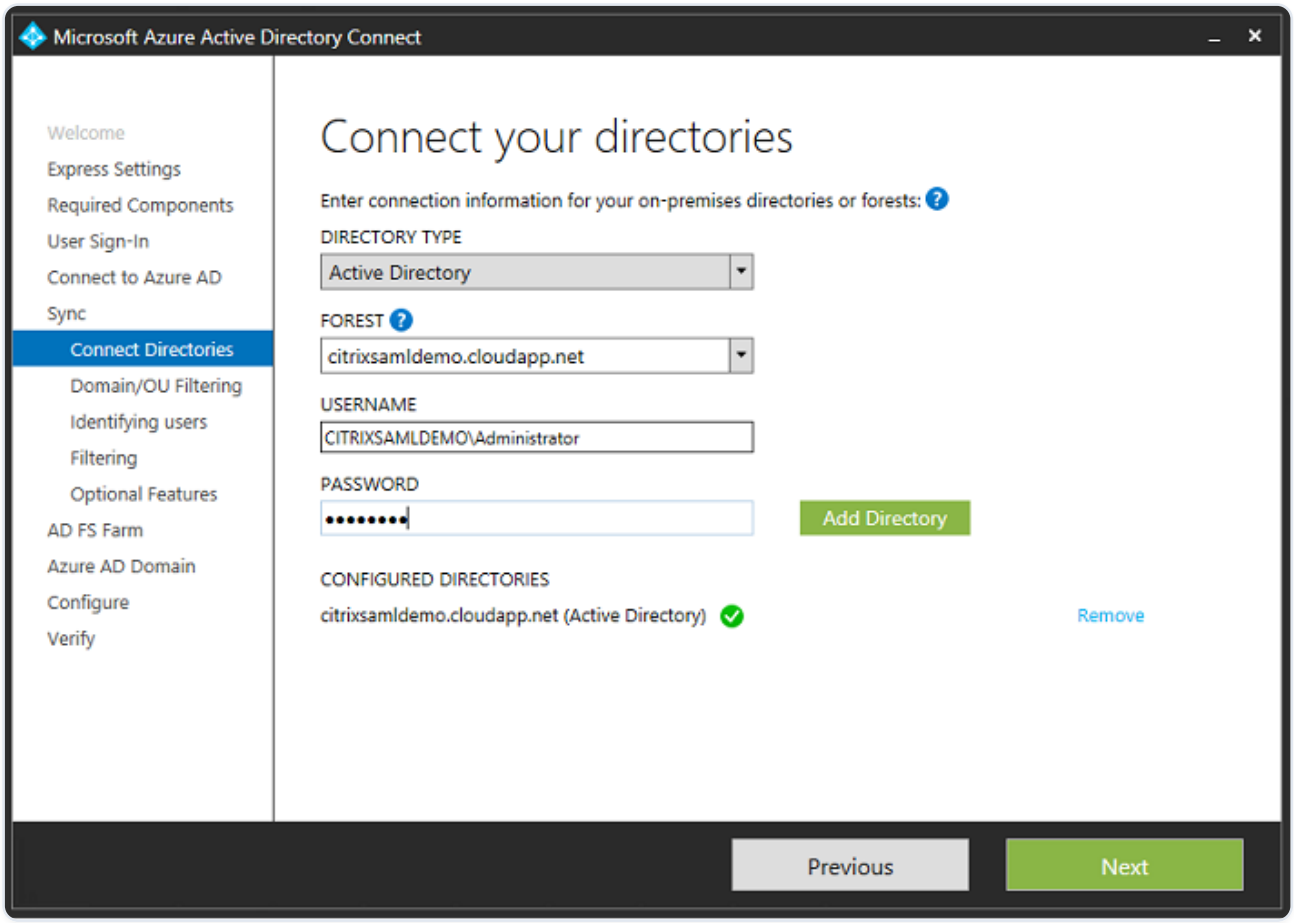
© 1997–2026 Citrix Systems, Inc. All rights reserved.

使用您之前创建的管理员帐户连接到 Azure。

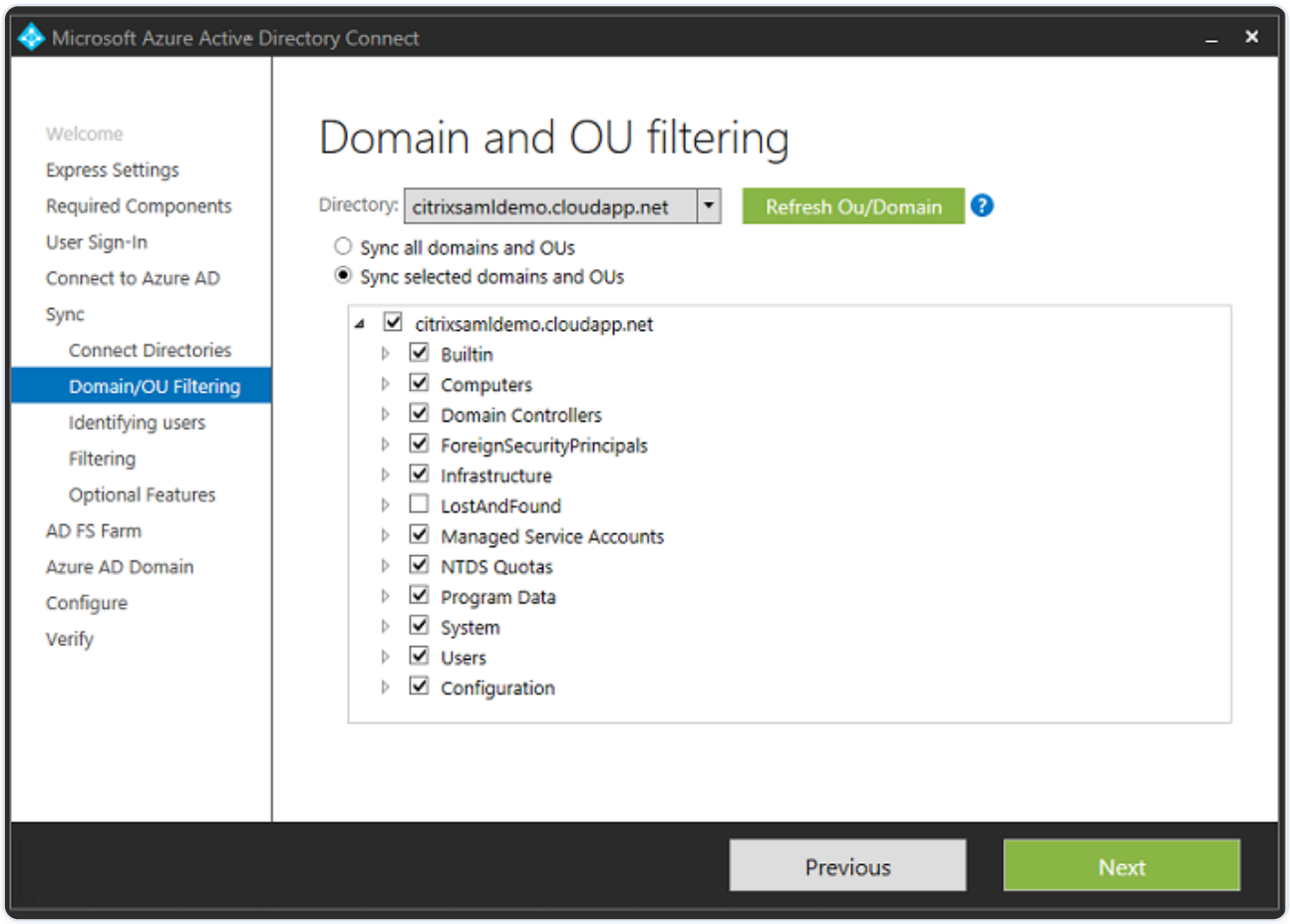


选择内部 AD 林。

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

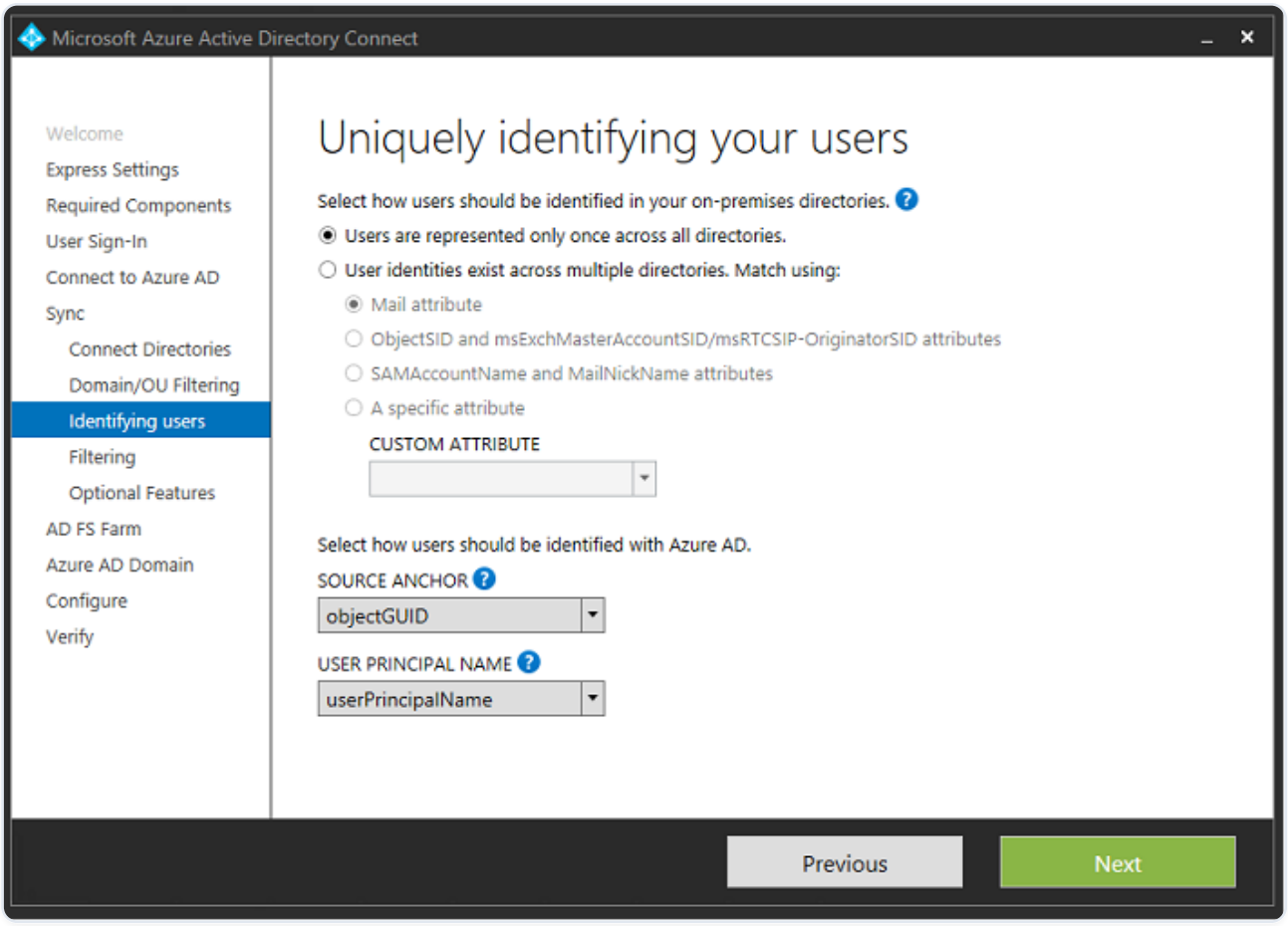


将所有旧版 Active Directory 对象与 Azure AD 同步。



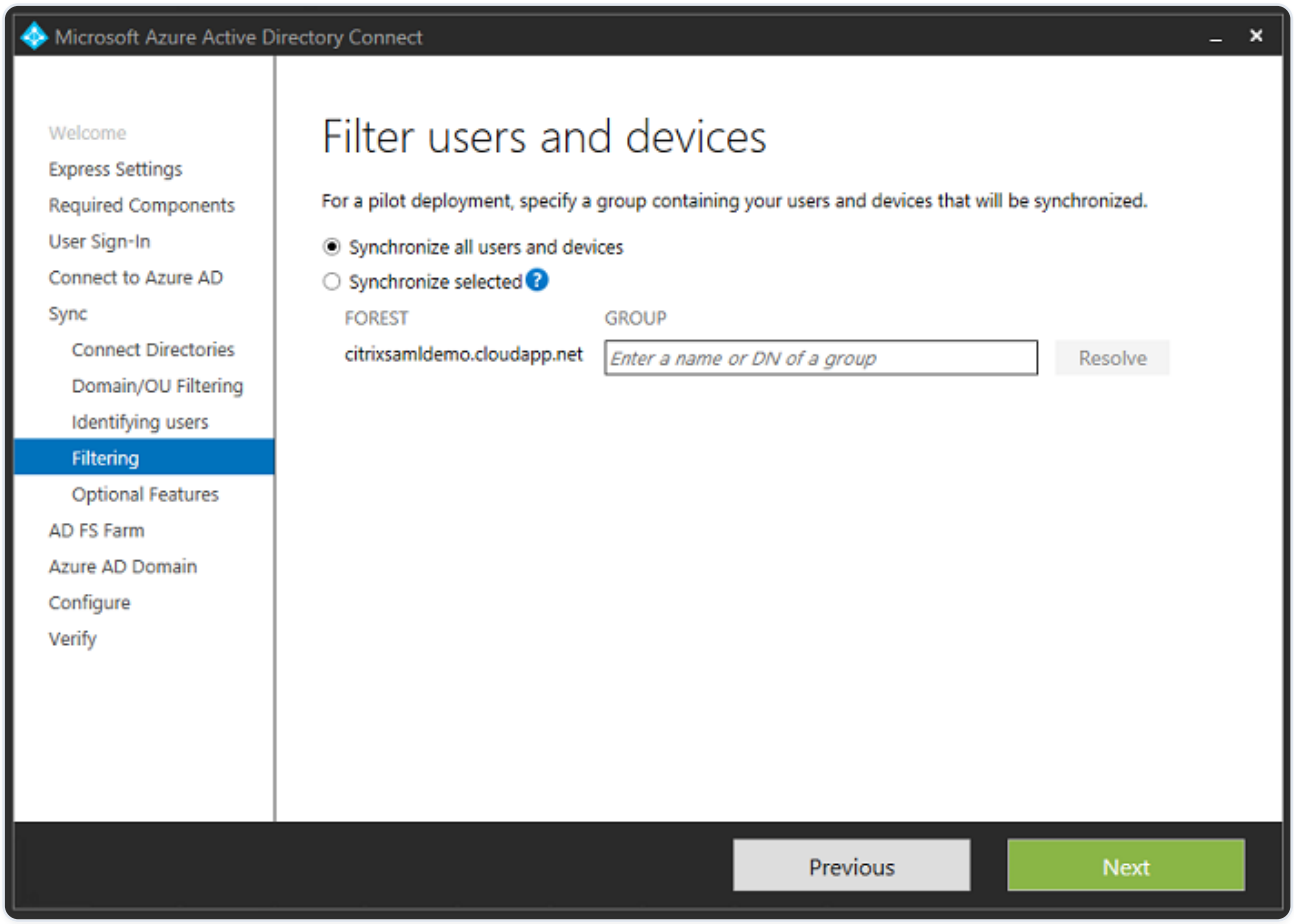
© 1997–2026 Citrix Systems, Inc. All rights reserved.

如果目录结构简单，您可以依赖用户名足够唯一来识别登录用户。



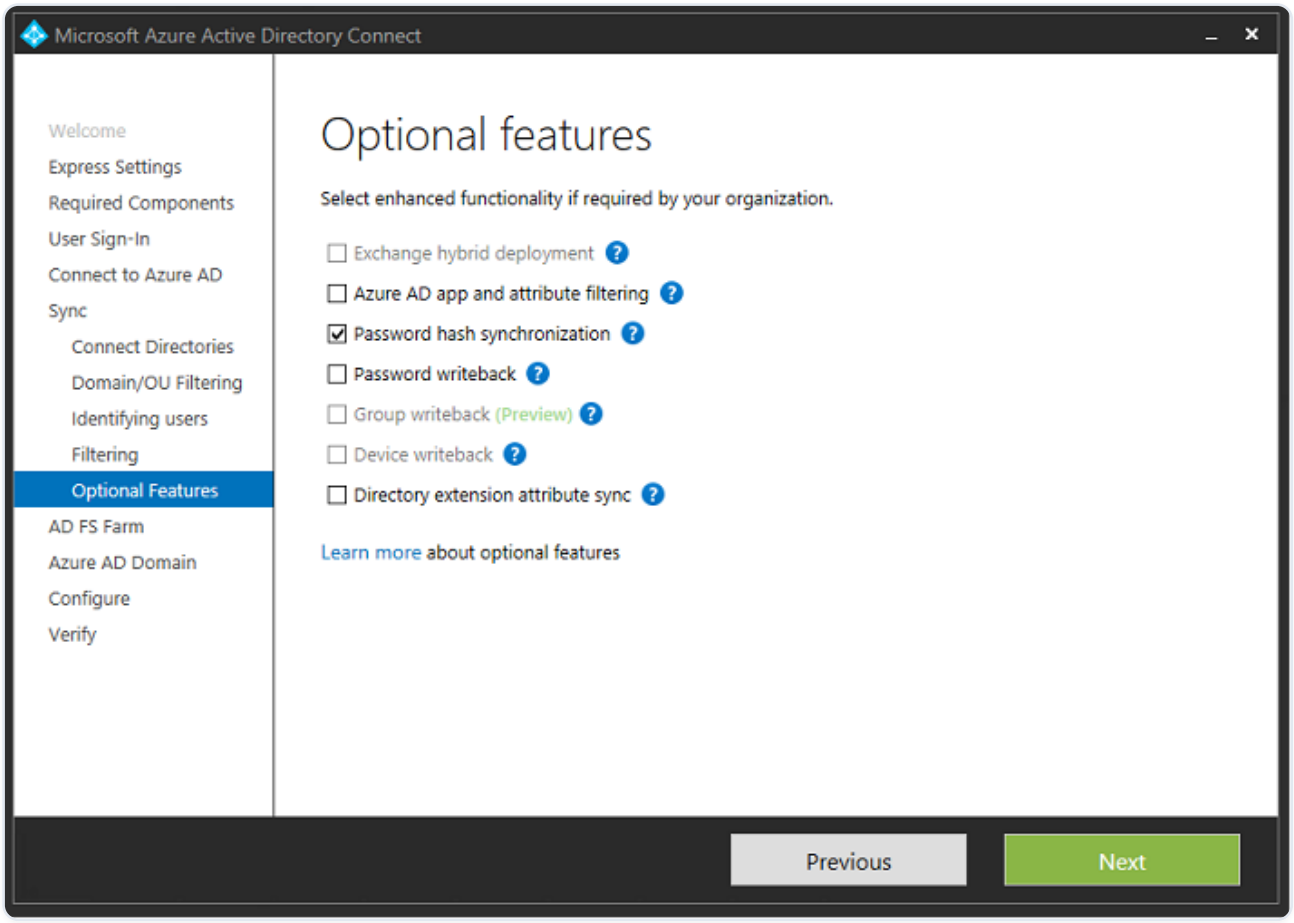
接受默认筛选选项，或将用户和设备限制到特定的组。

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

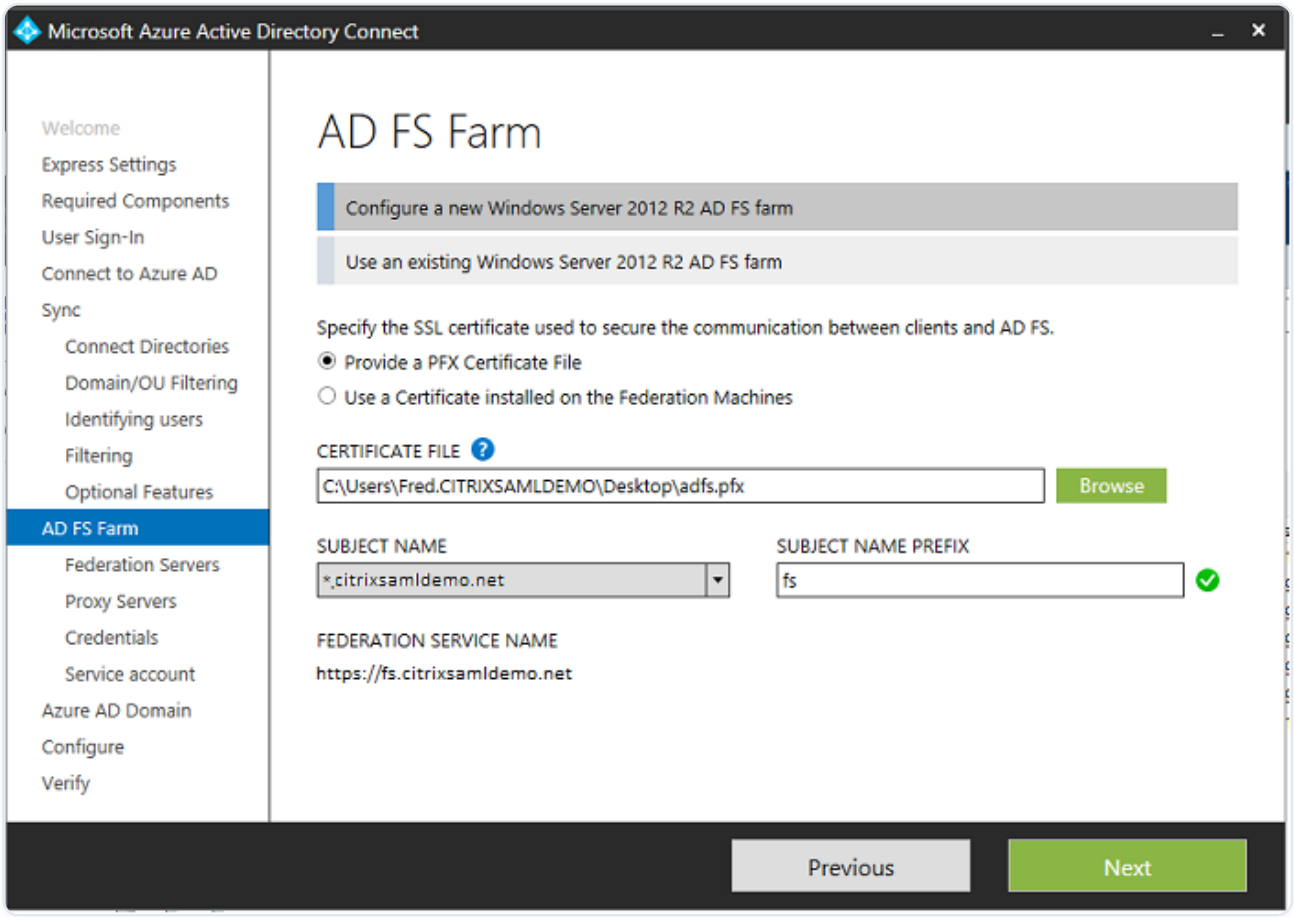


如果需要，您可以将 Azure AD 密码与 Active Directory 同步。对于基于 ADFS 的身份验证，通常不需要这样做。

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

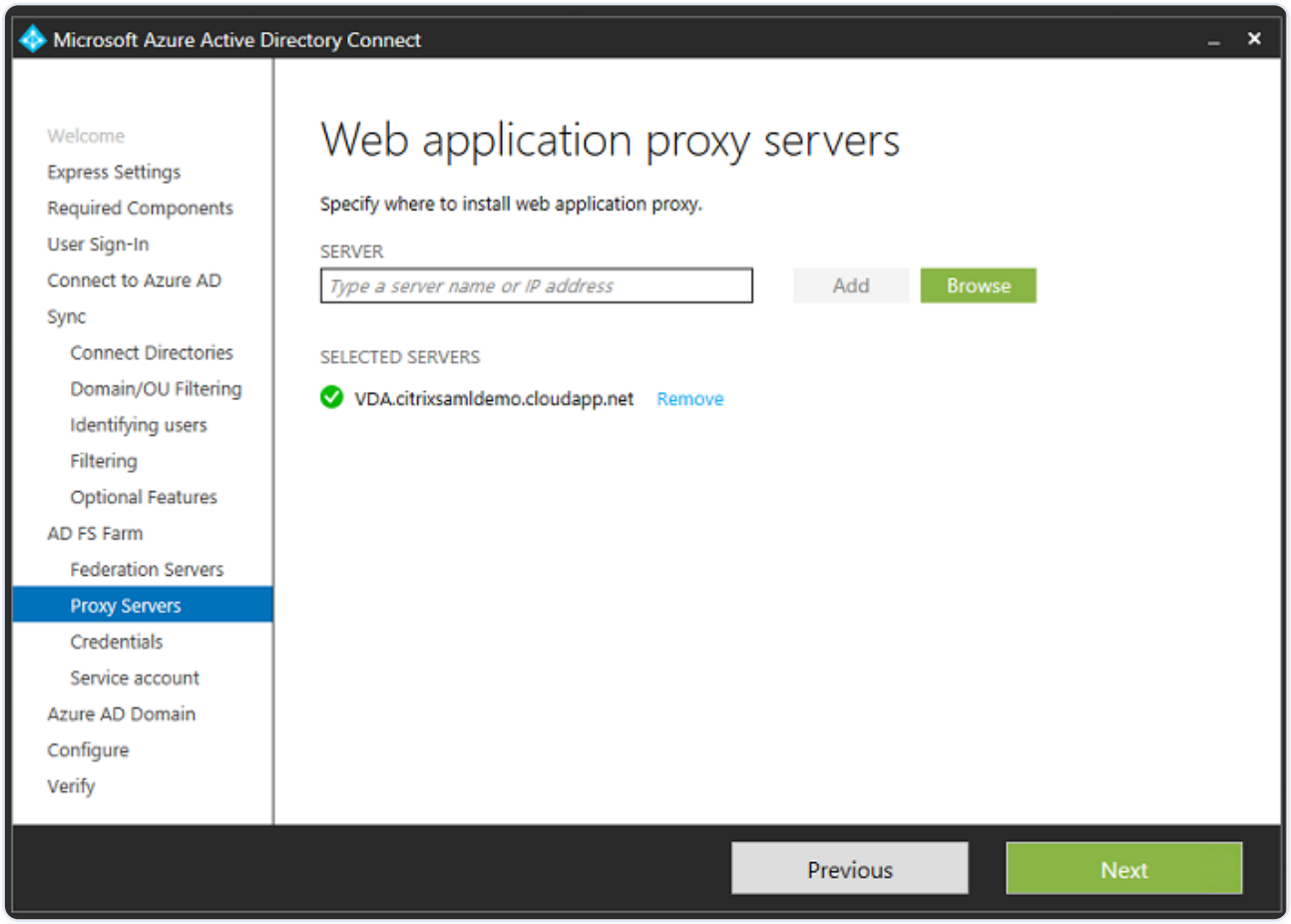


选择要在 AD FS 中使用的证书 PFX 文件，并将 fs.citrixsamldemo.net 指定为 DNS 名称。



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

当系统提示选择代理服务器时，输入 wap.citrixsamldemo.net 服务器的地址。您可能需要在 Web 应用程序代理服务器上以管理员身份运行 **Enable-PSRemoting –Force** cmdlet，以便 Azure AD Connect 可以对其进行配置。

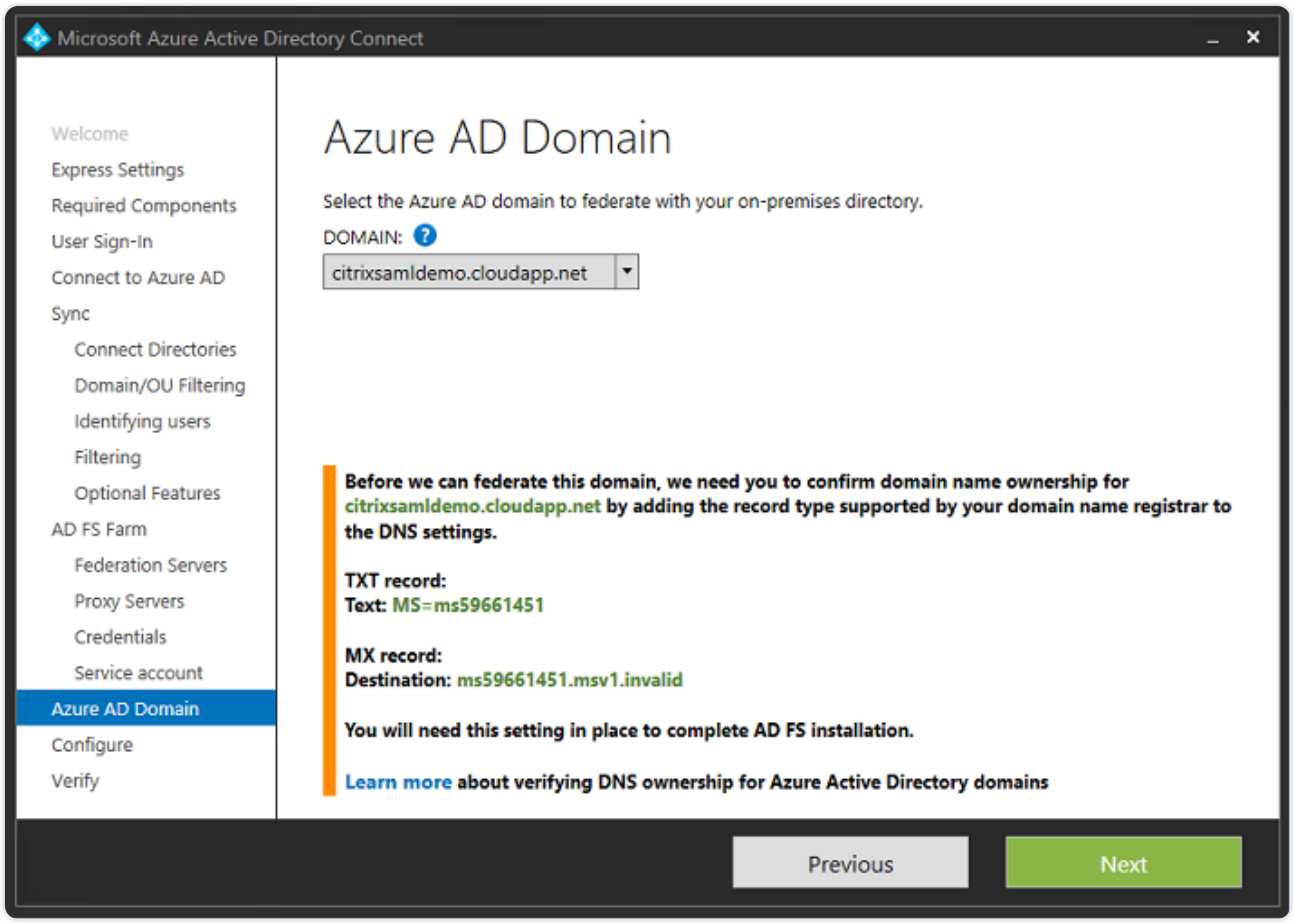


注意：

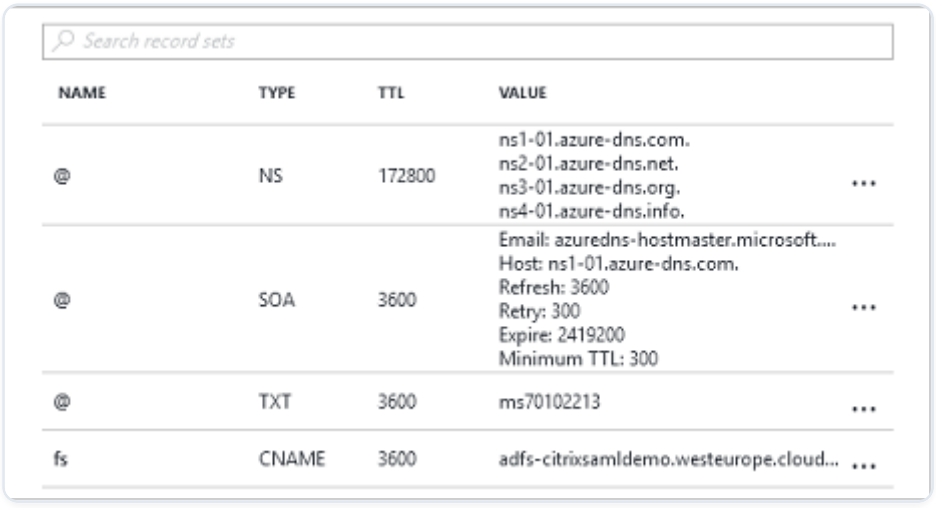
如果此步骤因远程 PowerShell 信任问题而失败，请尝试将 Web 应用程序代理服务器加入域。

对于向导的其余步骤，请使用标准管理员密码，并为 ADFS 创建一个服务帐户。然后，Azure AD Connect 将提示验证 DNS 区域的所有权。

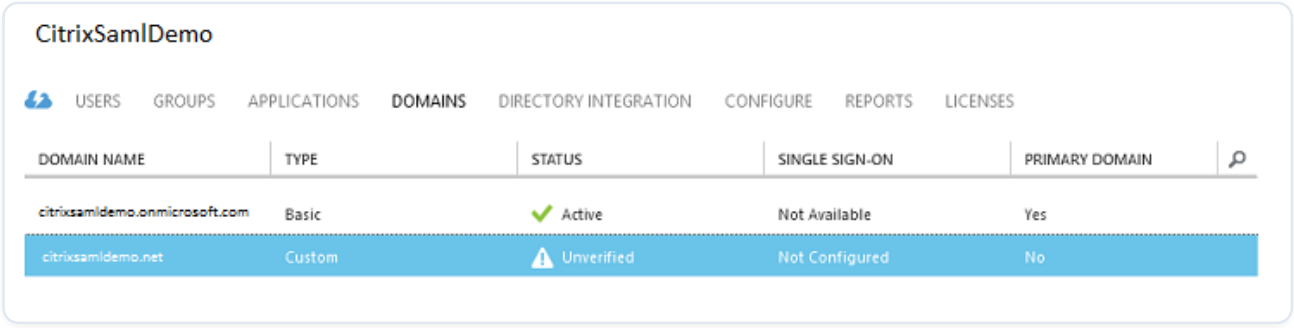
© 1997–2026 Citrix Systems, Inc. All rights reserved.



将 TXT 和 MX 记录添加到 Azure 中的 DNS 地址记录。



在 Azure 管理控制台中单击“**验证**”。

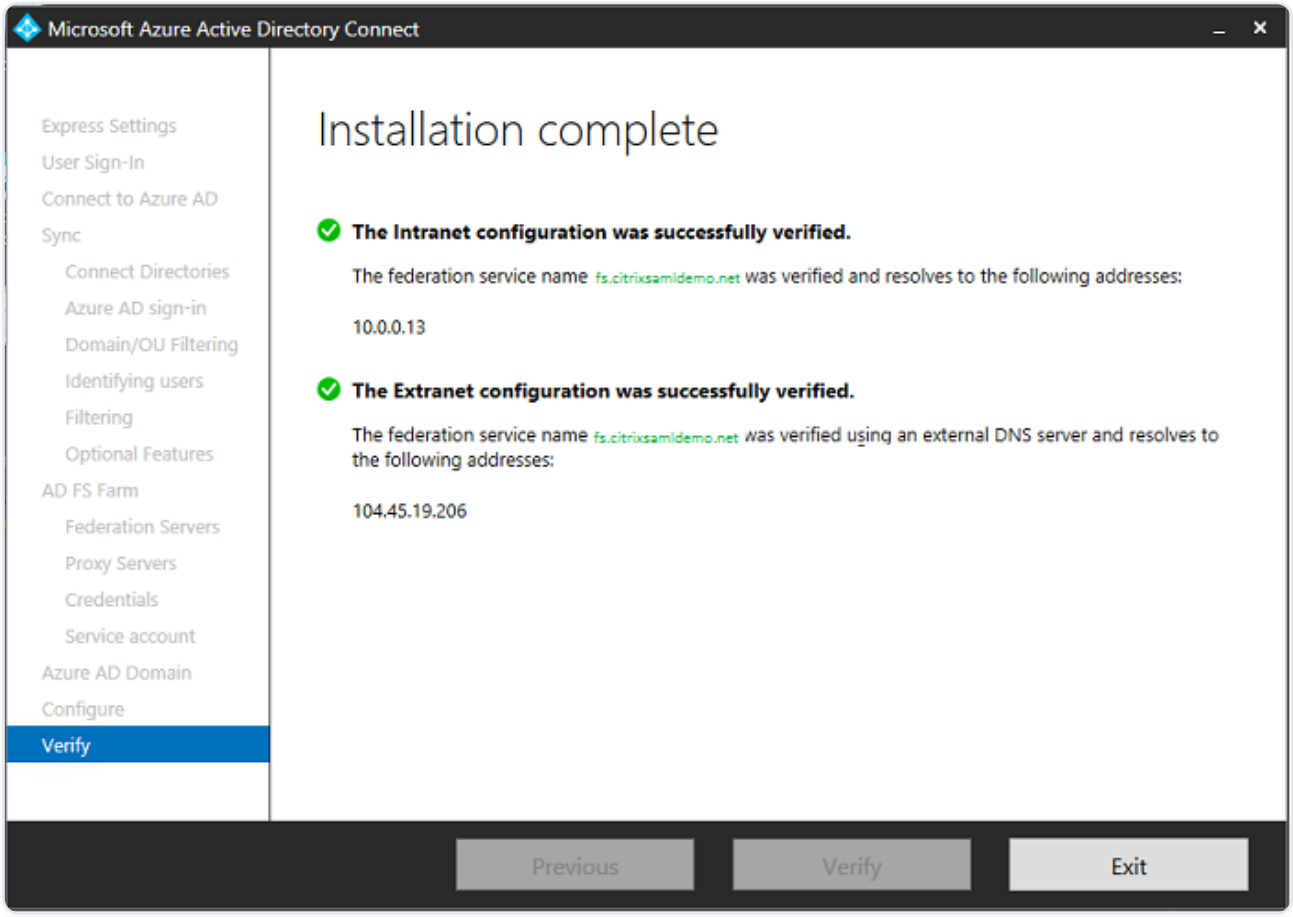


© 1997–2026 Citrix Systems, Inc. All rights reserved.

注意：

如果此步骤失败，您可以在运行 Azure AD Connect 之前验证域。

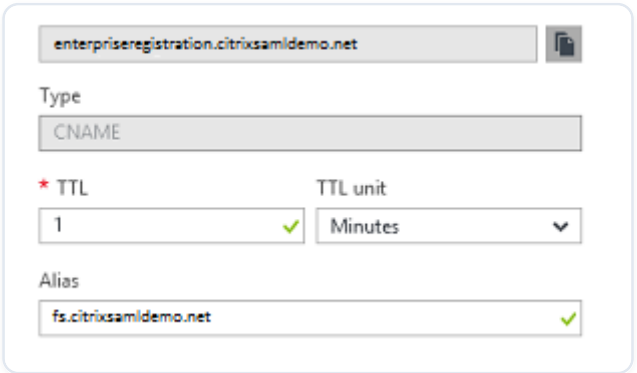
完成后，将通过端口 443 联系外部地址 fs.citrixsamldemo.net。



启用 Azure AD 加入

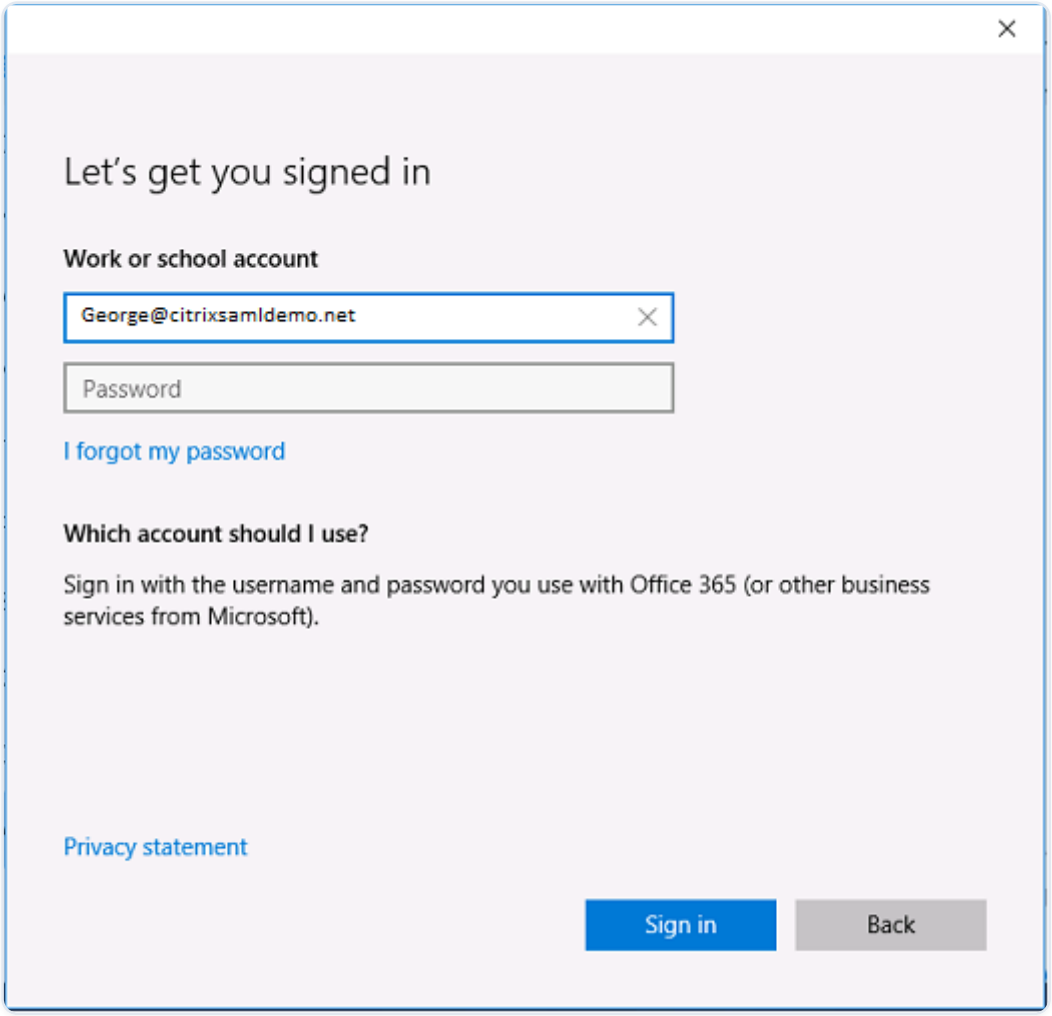
当用户输入电子邮件地址以便 Windows 10 可以执行 Azure AD 加入时，DNS 后缀用于构造一个 CNAME DNS 记录，该记录应指向 ADFS: enterpriseregistration.\<*upnsuffix*>。

在此示例中，这是 `fs.citrixsamldemo.net`。



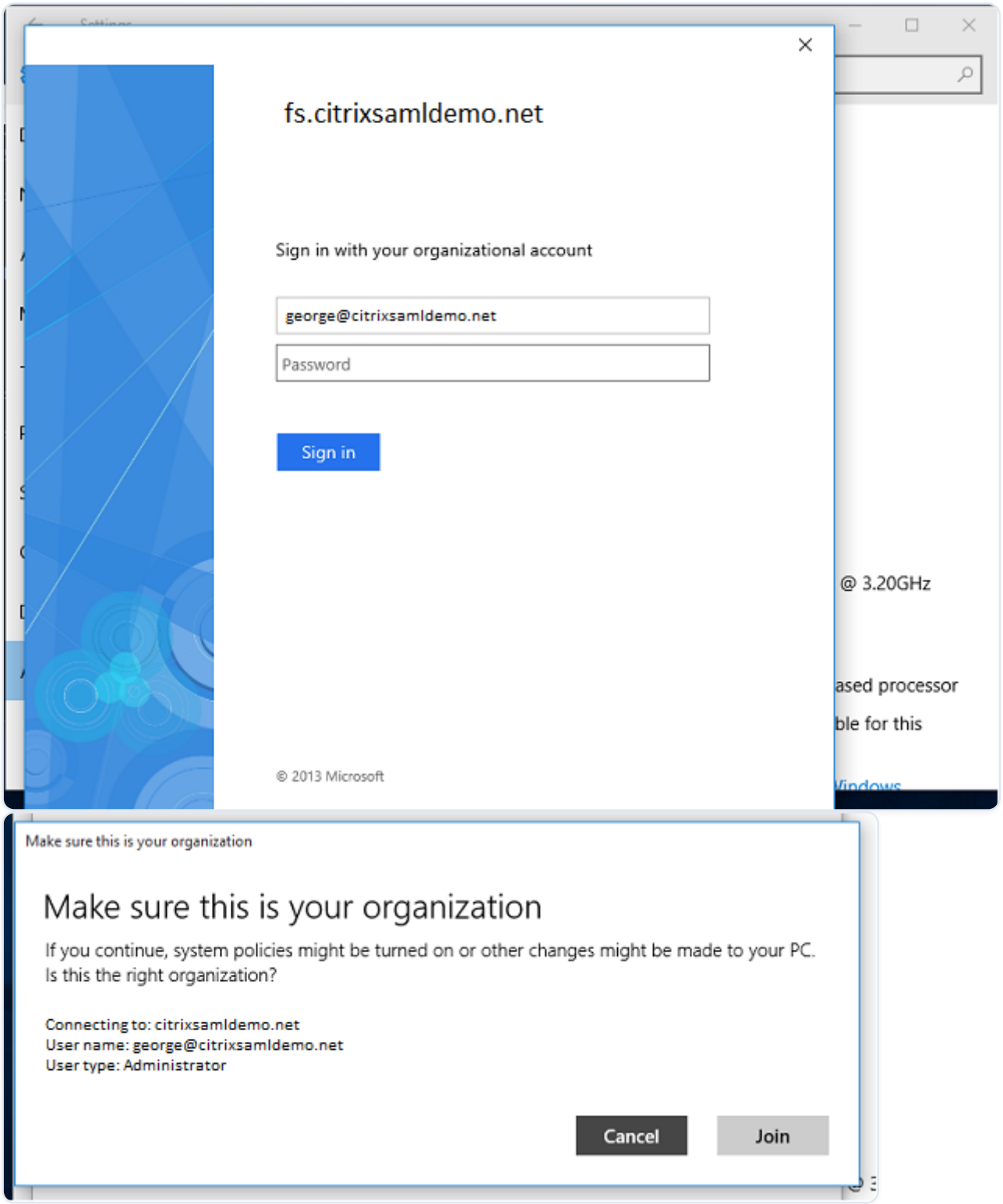
© 1997–2026 Citrix Systems, Inc. All rights reserved.

如果您未使用公共证书颁发机构，请确保 ADFS 根证书已安装在 Windows 10 计算机上，以便 Windows 信任 ADFS 服务器。使用之前生成的标准用户帐户执行 Azure AD 域加入。

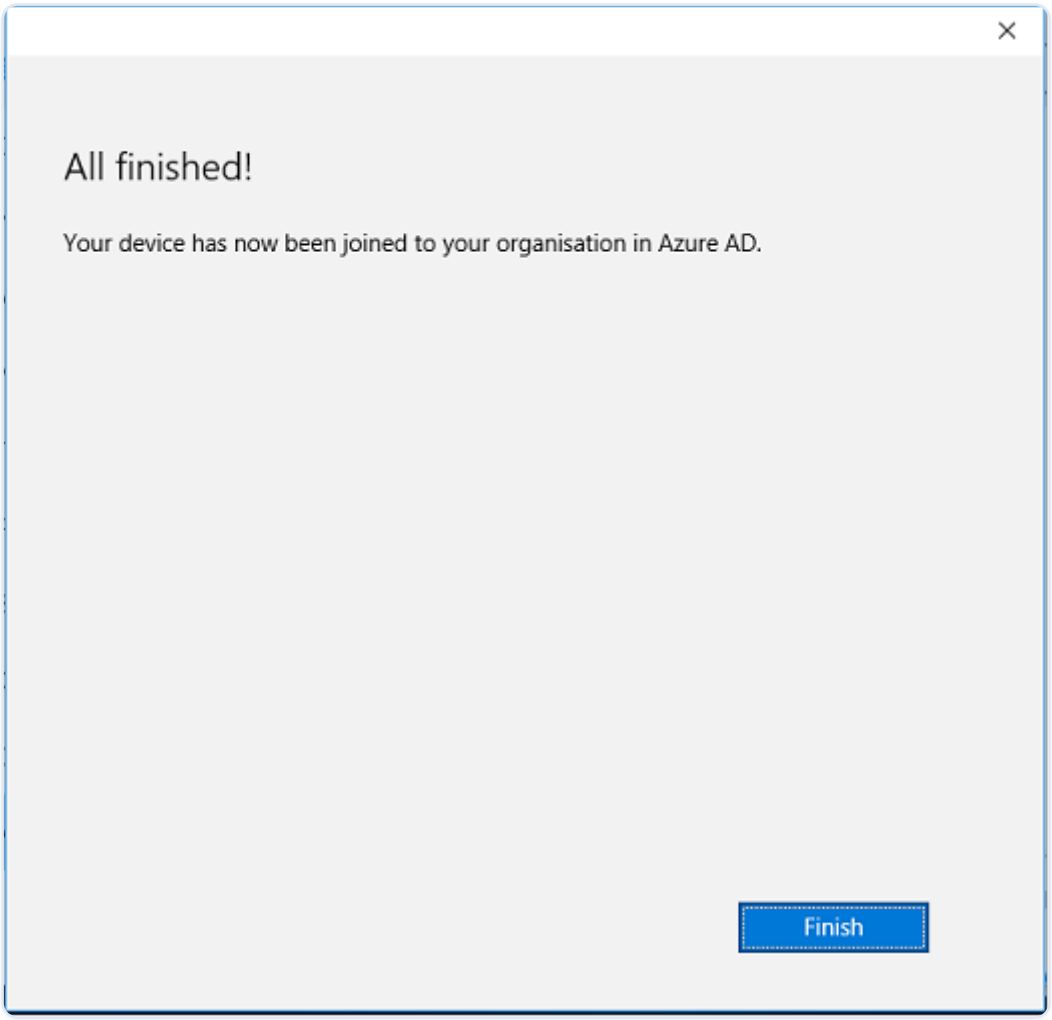


请注意，UPN 必须与 ADFS 域控制器识别的 UPN 匹配。

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



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



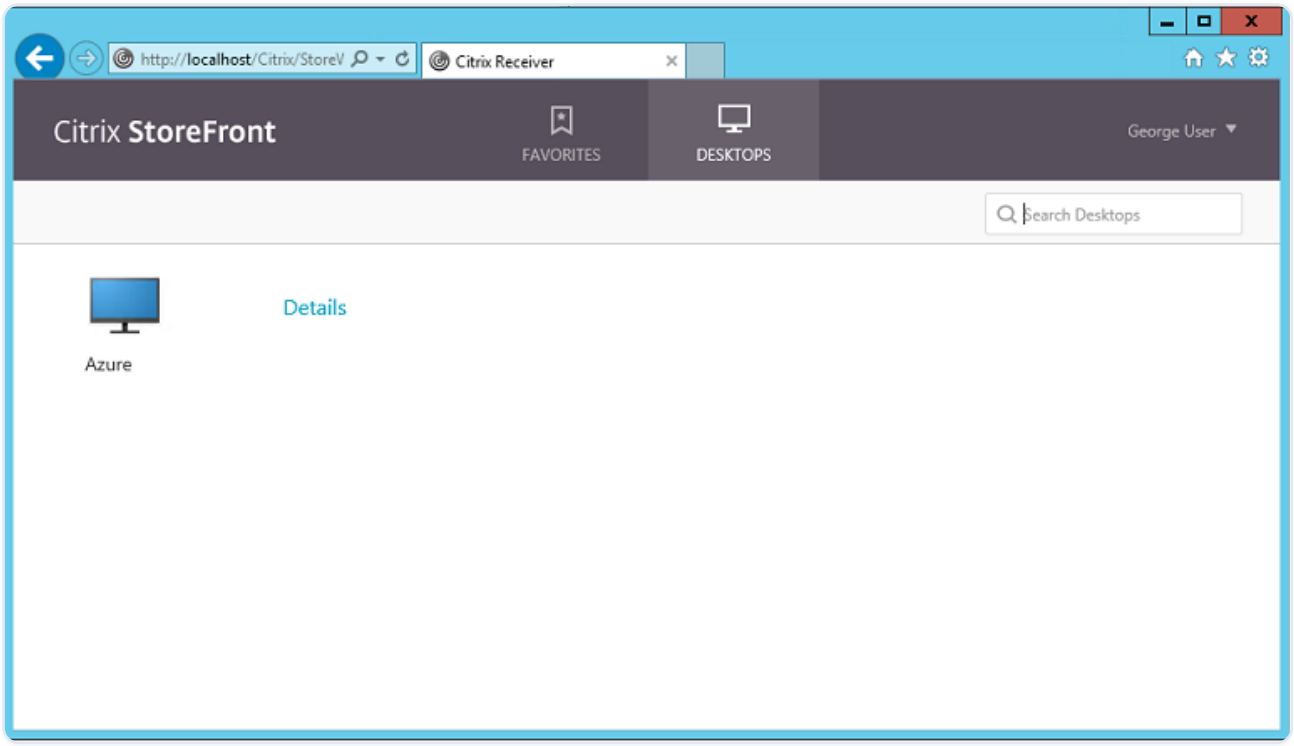
通过重启计算机并使用用户的电子邮件地址登录来验证 Azure AD 加入是否成功。登录后，启动 Microsoft Edge 并连接到 `<http://myapps.microsoft.com>`。该网站应自动使用单点登录。

安装 思杰虚拟应用 或 思杰虚拟桌面

您可以按照常规方式，直接从 Citrix Virtual Apps 或 Citrix Virtual Desktops ISO 在 Azure 中安装 Delivery Controller 和 VDA 虚拟机。

在此示例中，StoreFront 与 Delivery Controller 安装在同一服务器上。VDA 作为独立的 Windows 2012 R2 RDS 工作程序安装，未与 Machine Creation Services 集成（尽管可以可选地进行配置）。在继续之前，请检查用户 George@citrixsamldemo.net 是否可以使用密码进行身份验证。

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



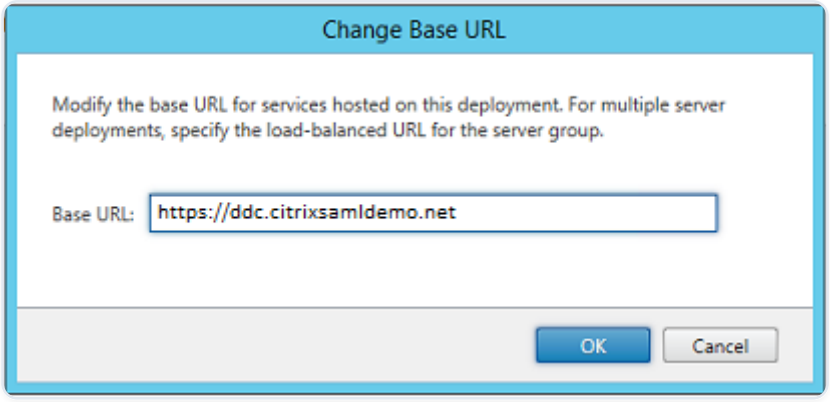
在 Controller 上运行 **Set-BrokerSite –TrustRequestsSentToTheXmlServicePort $true** PowerShell cmdlet，以允许 StoreFront™ 在没有用户凭据的情况下进行身份验证。

安装联合身份验证服务

在 ADFS 服务器上安装 FAS，并为 Delivery Controller 配置一个规则，使其充当受信任的 StoreFront（因为在此示例中，StoreFront 与 Delivery Controller 安装在同一 VM 上）。请参阅 安装和配置。

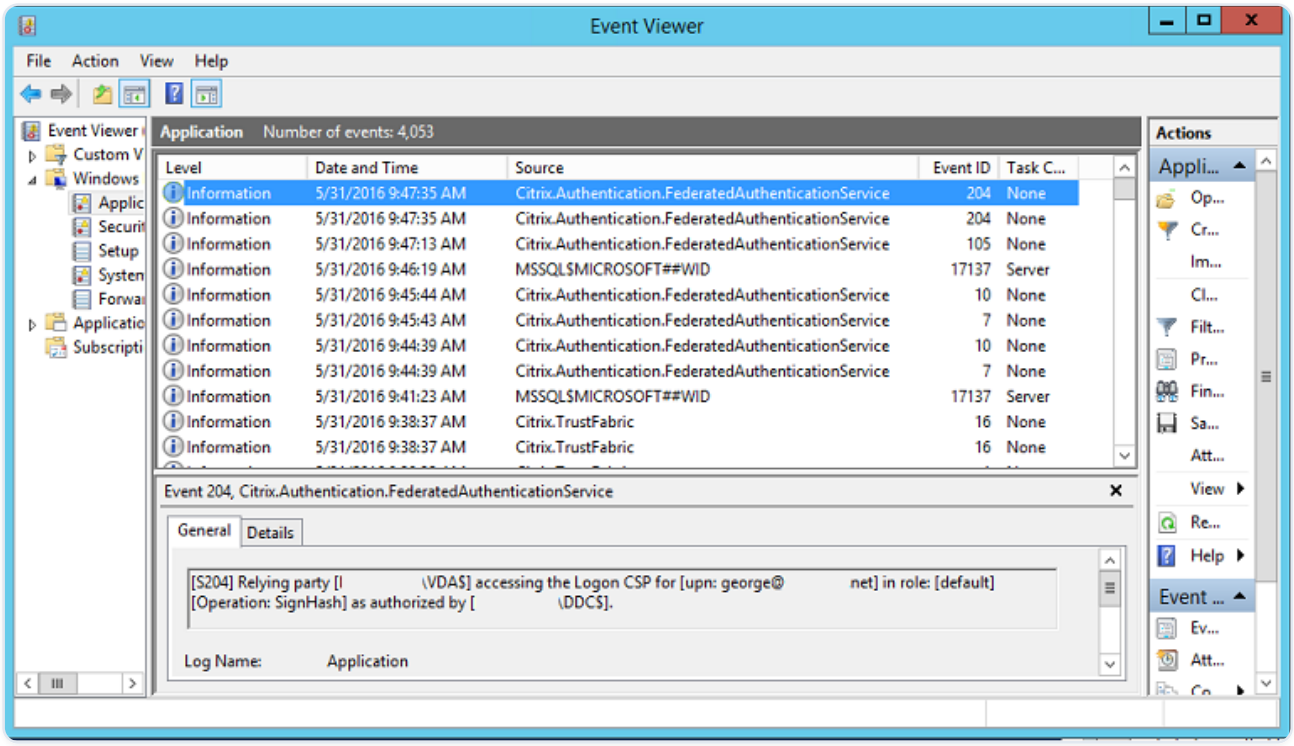
配置 StoreFront

为 Delivery Controller 请求计算机证书，并通过为端口 443 设置 IIS 绑定并将 StoreFront 基本地址更改为 https: 来配置 IIS 和 StoreFront 以使用 HTTPS。



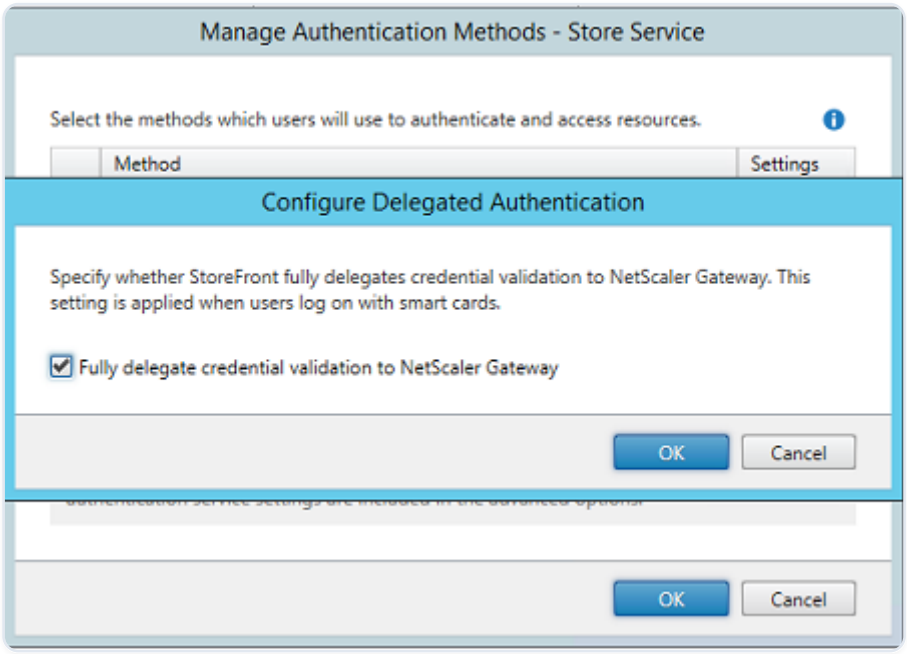
配置 StoreFront 以使用 FAS 服务器（使用 安装和配置 中的 PowerShell 脚本），并在 Azure 内部进行测试，通过检查 FAS 服务器上的事件查看器来确保登录使用 FAS。

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



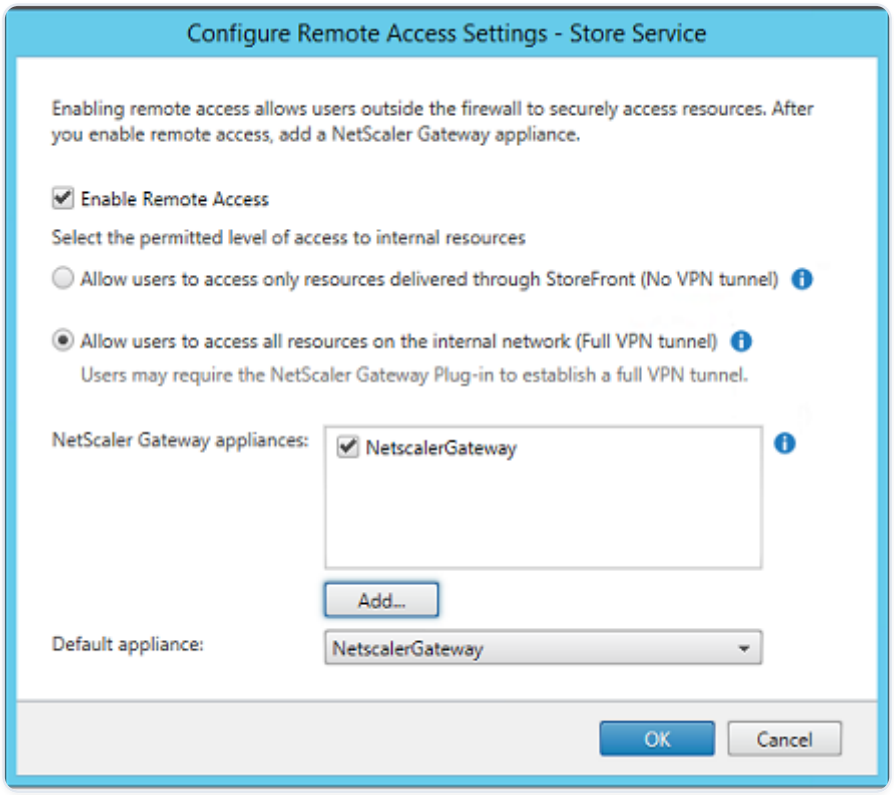
配置 StoreFront 以使用 Citrix Gateway

在 StoreFront 管理控制台中，使用“**管理身份验证方法**”GUI 配置 StoreFront 以使用 Citrix Gateway 执行身份验证。



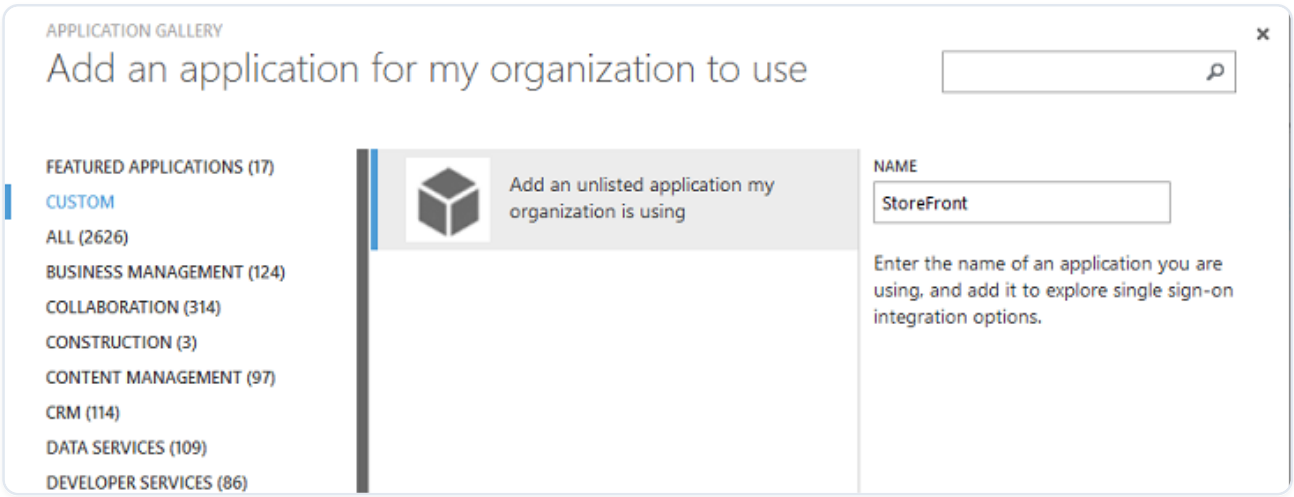
要集成 Citrix Gateway 身份验证选项，请配置安全票证颁发机构 (STA) 并配置 Citrix Gateway 地址。

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



配置新的 Azure AD 应用程序以实现 StoreFront 的单点登录

本节使用 Azure AD SAML 2.0 单点登录功能，该功能目前需要 Azure Active Directory Premium 订阅。在 Azure AD 管理工具中，选择“**新建应用程序**”，然后选择“**从库中添加应用程序**”。

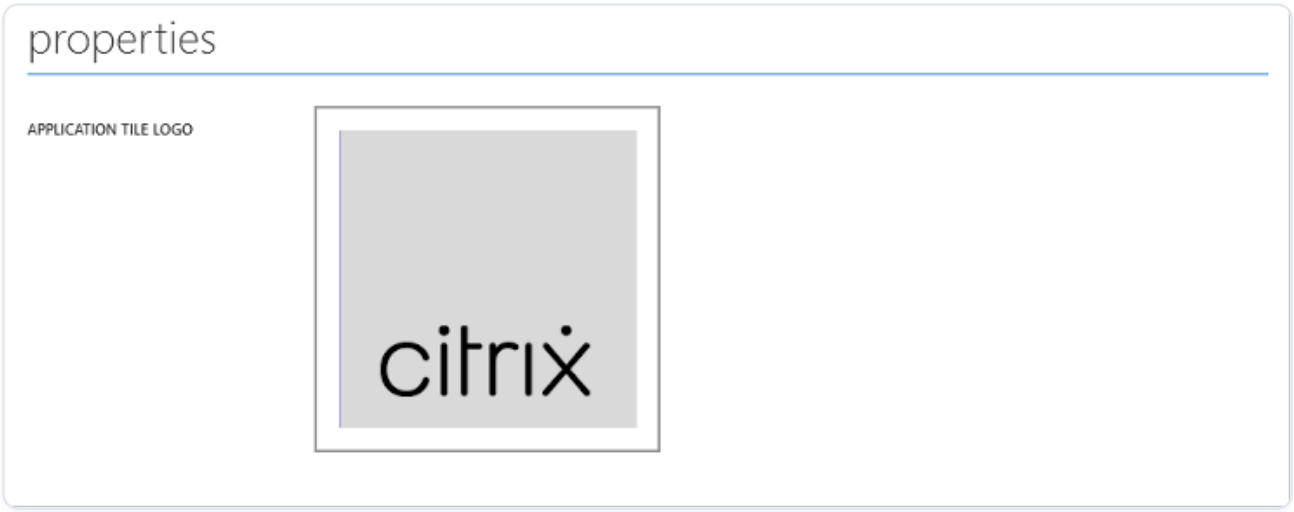


选择 **自定义 > 添加我的组织正在使用的未列出应用程序** 以创建供用户使用的新自定义应用程序。

配置图标

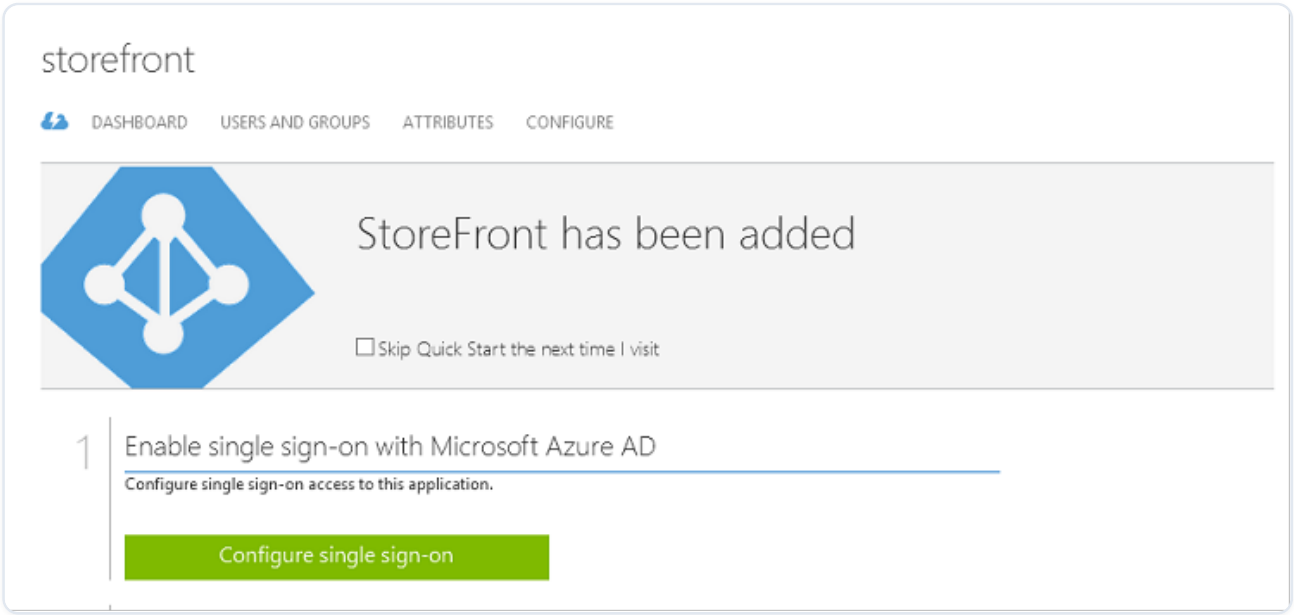
创建一张 215 x 215 像素的图像，并将其上传到“配置”页面，用作应用程序的图标。

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



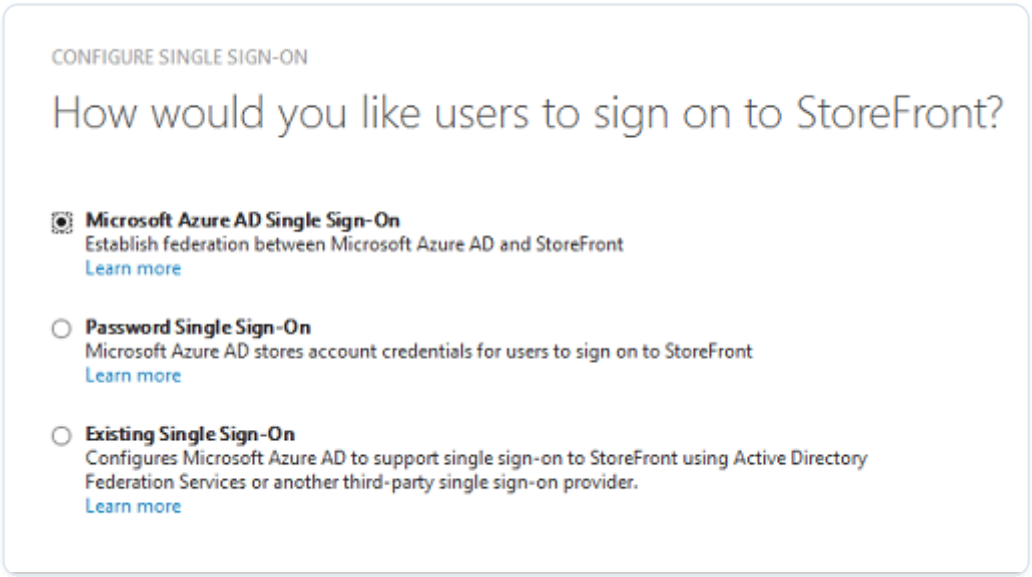
配置 SAML 身份验证

返回“应用程序仪表板概述”页面，然后选择 **配置单点登录**。

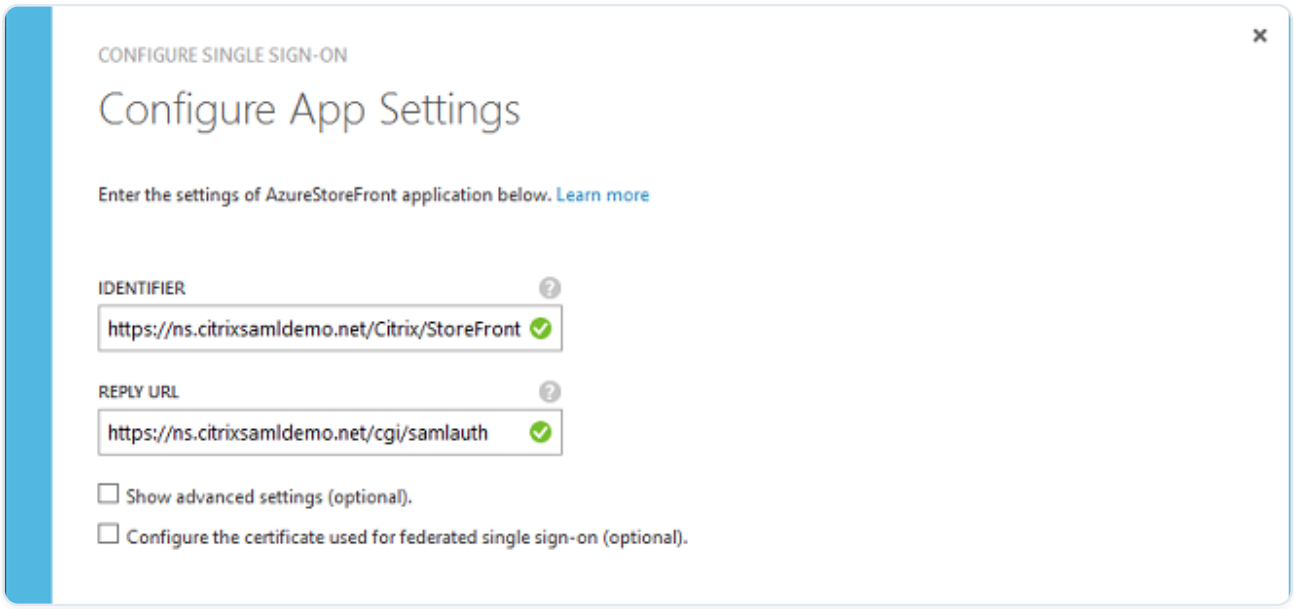


此部署将使用 SAML 2.0 身份验证，这对应于 **Microsoft Azure AD 单点登录**。

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

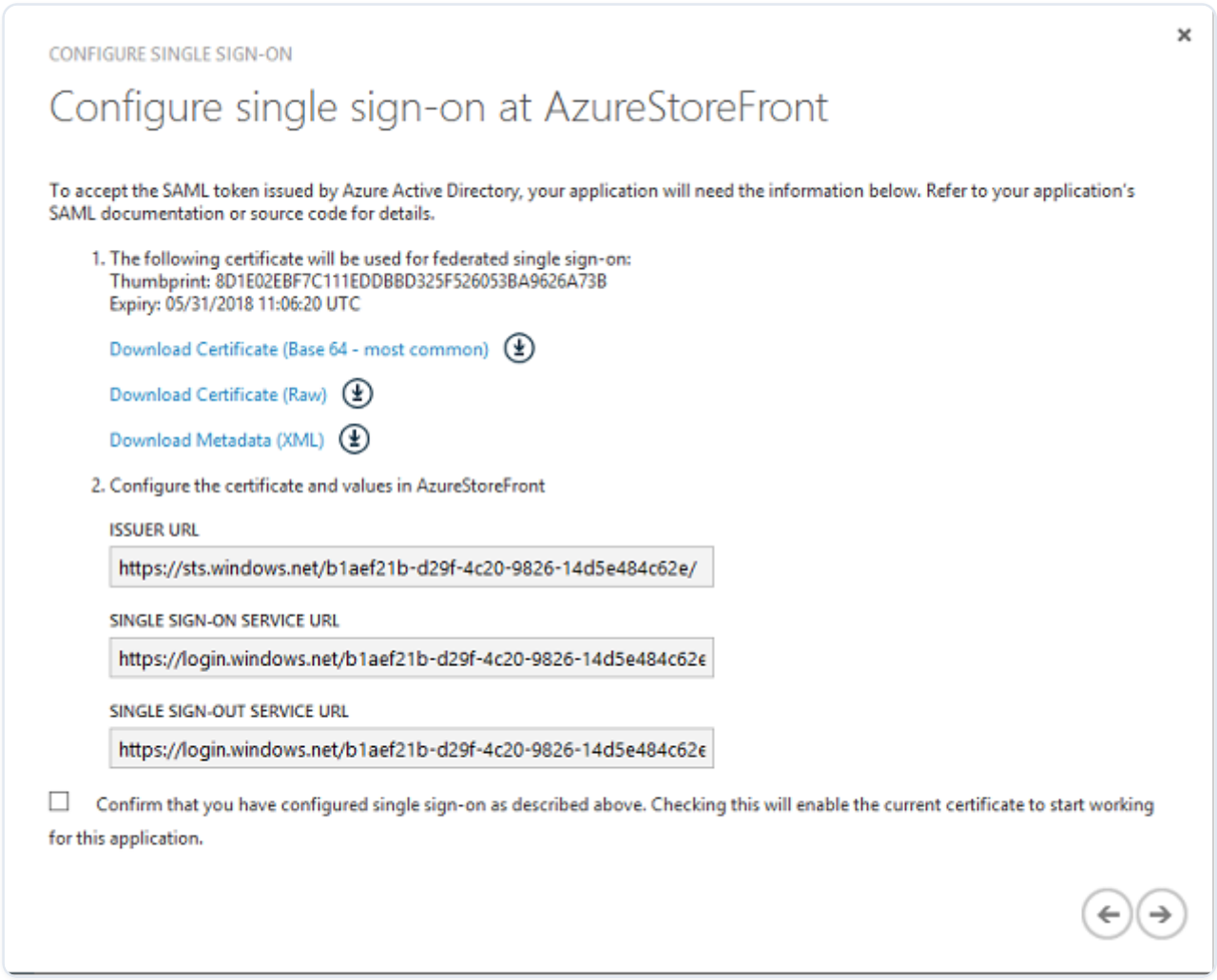


标识符 可以是任意字符串（它必须与提供给 Citrix Gateway 的配置匹配）；在此示例中，**回复 URL** 是 Citrix Gateway 服务器上的 */cgi/samlauth*。



下一页包含用于将 Citrix Gateway 配置为 Azure AD 的信赖方的信息。

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



下载 base 64 信任签名证书，并复制登录和注销 URL。稍后您将在 Citrix Gateway 配置屏幕中粘贴这些内容。

将应用程序分配给用户

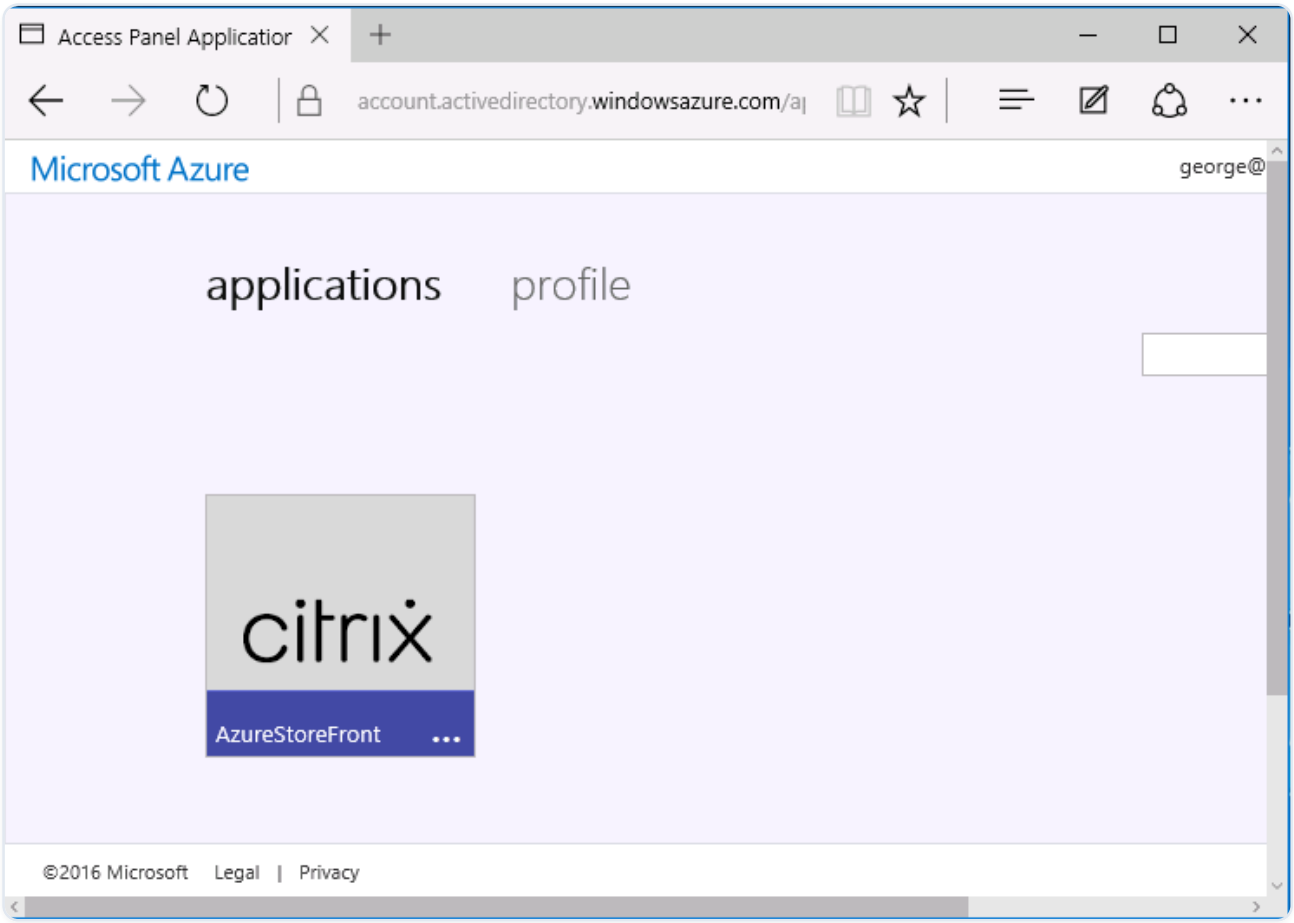
最后一步是启用应用程序，使其显示在用户的“myapps.microsoft.com”控制页面上。这在“USERS AND GROUPS”页面上完成。为由 Azure AD Connect 同步的域用户帐户分配访问权限。也可以使用其他帐户，但必须显式映射它们，因为它们不符合 \<user>@\<domain> 模式。



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

我的应用页面

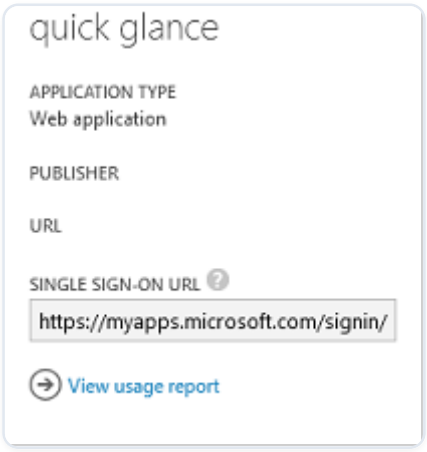
配置应用程序后，当用户访问 `<https://myapps.microsoft.com>` 时，它会显示在用户的 Azure 应用程序列表中。



当它加入 Azure AD 后，Windows 10 支持登录用户的 Azure 应用程序单一登录。单击图标会将浏览器带到之前配置的 SAML cgi/samlauth 网页。

单一登录 URL

返回 Azure AD 仪表板中的应用程序。现在应用程序有一个可用的单一登录 URL。此 URL 用于提供网页浏览器链接或创建“开始”菜单快捷方式，将用户直接带到 StoreFront。



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

将此 URL 粘贴到 Web 浏览器中，以确保您被 Azure AD 重定向到之前配置的 Citrix Gateway cgi/samlauth 网页。这仅适用于已分配的用户，并且仅为已加入 Azure AD 的 Windows 10 登录会话提供单一登录。（其他用户将需要输入 Azure AD 凭据。）

安装和配置 Citrix Gateway

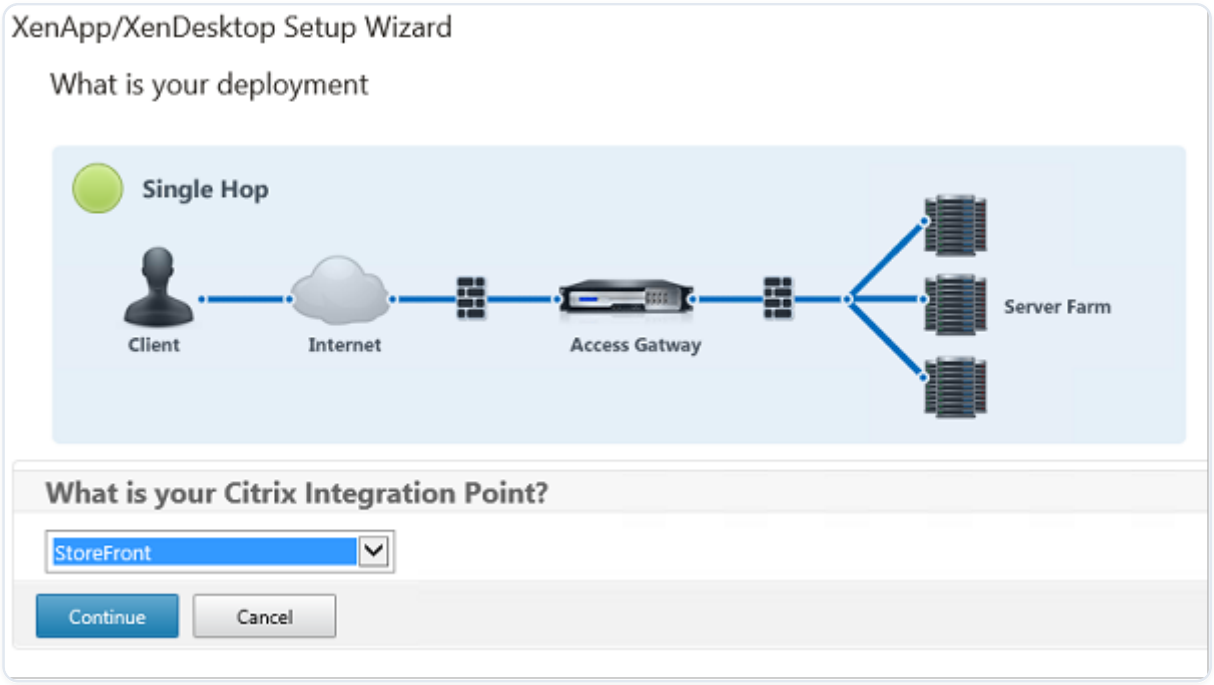
为了远程访问部署，此示例使用运行 NetScaler（现为 Citrix Gateway）的独立虚拟机。这可以从 Azure 应用商店购买。此示例使用 NetScaler 11.0 的“自带许可证”版本。

登录到 NetScaler® 虚拟机，将 Web 浏览器指向内部 IP 地址，使用用户进行身份验证时指定的凭据。请注意，您必须更改 Azure AD 虚拟机中 nsroot 用户的密码。

添加许可证，在添加每个许可证文件后选择**重新启动**，并将 DNS 解析器指向 Microsoft 域控制器。

运行 Citrix Virtual Apps and Desktops 安装向导

此示例首先配置一个不带 SAML 的简单 StoreFront 集成。在该部署正常工作后，它会添加一个 SAML 登录策略。

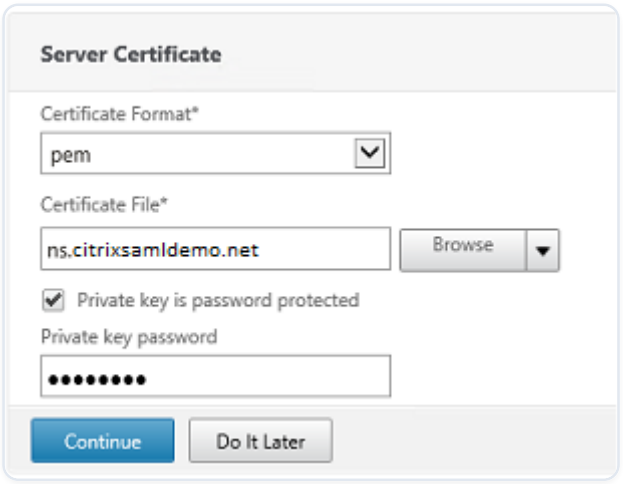


选择标准的 Citrix Gateway StoreFront 设置。在 Microsoft Azure 中使用时，此示例配置端口 4433，而不是端口 443。或者，您可以端口转发或重新映射 Citrix Gateway 管理网站。

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



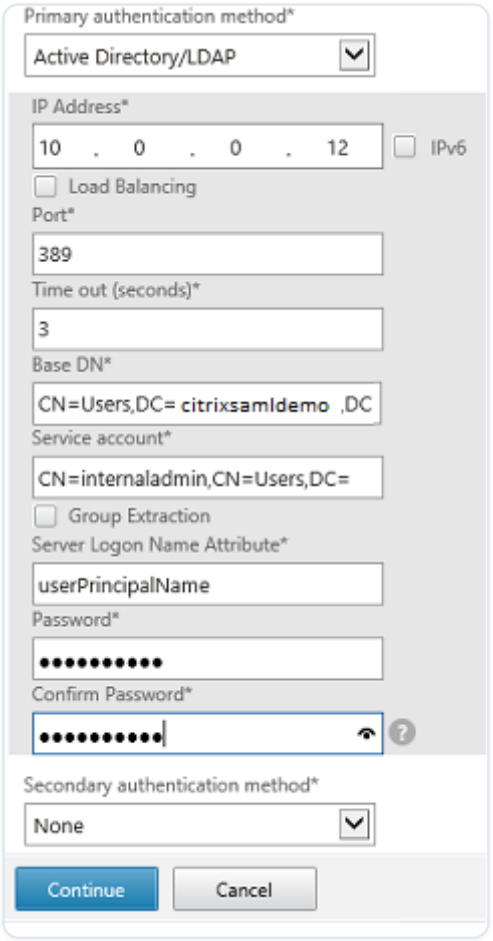
为简单起见，此示例上传存储在文件中的现有服务器证书和私钥。



配置用于 AD 帐户管理的域控制器

域控制器将用于帐户解析，因此请将其 IP 地址添加到主要身份验证方法中。请注意对话框中每个字段所需的格式。

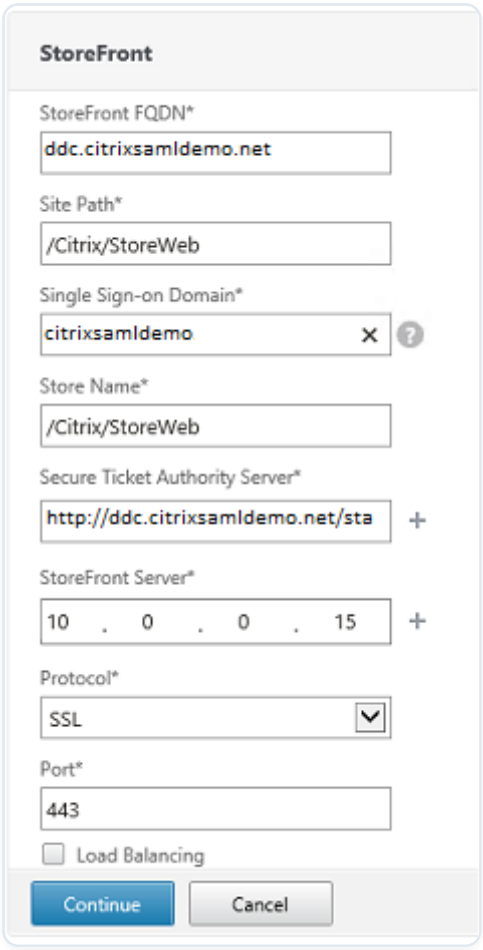
© 1997–2026 Citrix Systems, Inc. All rights reserved.



配置 StoreFront 地址

在此示例中，StoreFront 已使用 HTTPS 配置，因此请选择 SSL 协议选项。

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



验证 Citrix Gateway 部署

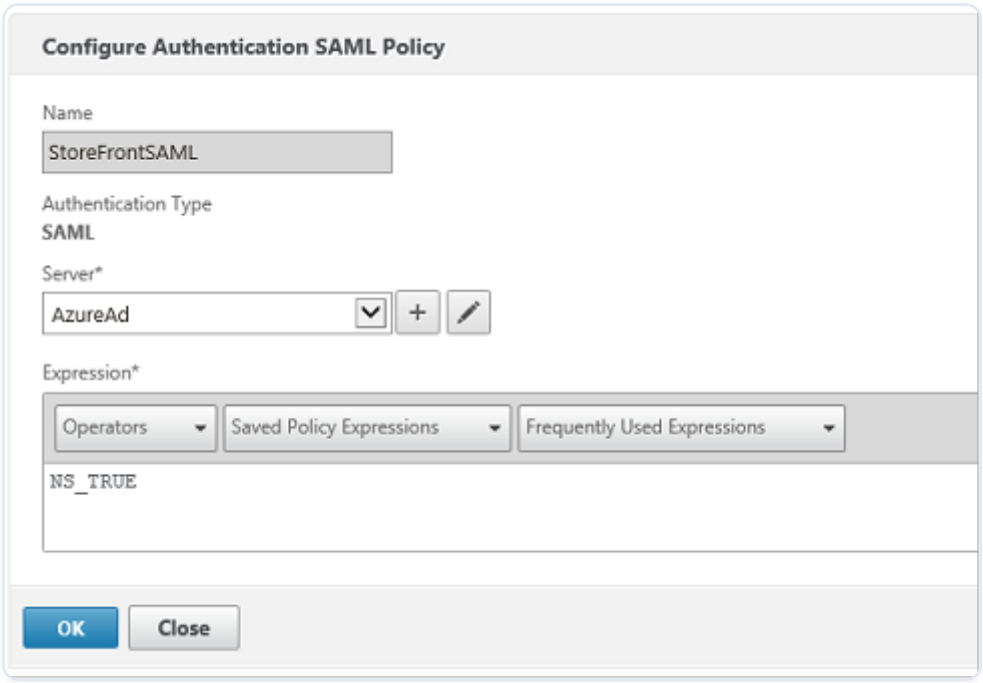
连接到 Citrix Gateway 并使用用户名和密码检查身份验证和启动是否成功。



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

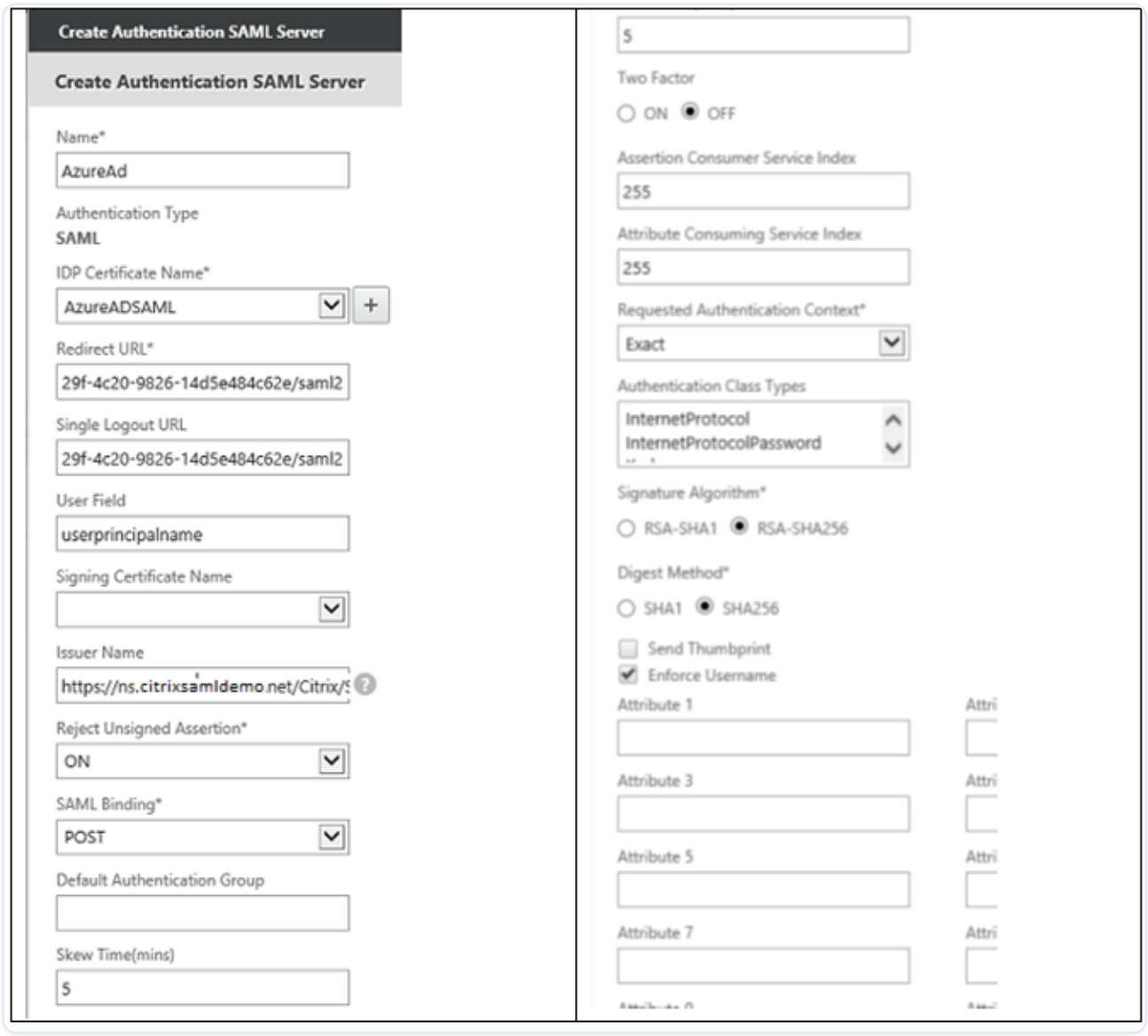
启用 Citrix Gateway SAML 身份验证支持

将 SAML 与 StoreFront 结合使用类似于将 SAML 与其他网站结合使用。添加新的 SAML 策略，其表达式为 **NS_TRUE**。



配置新的 SAML IdP 服务器，使用之前从 Azure AD 获取的信息。

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

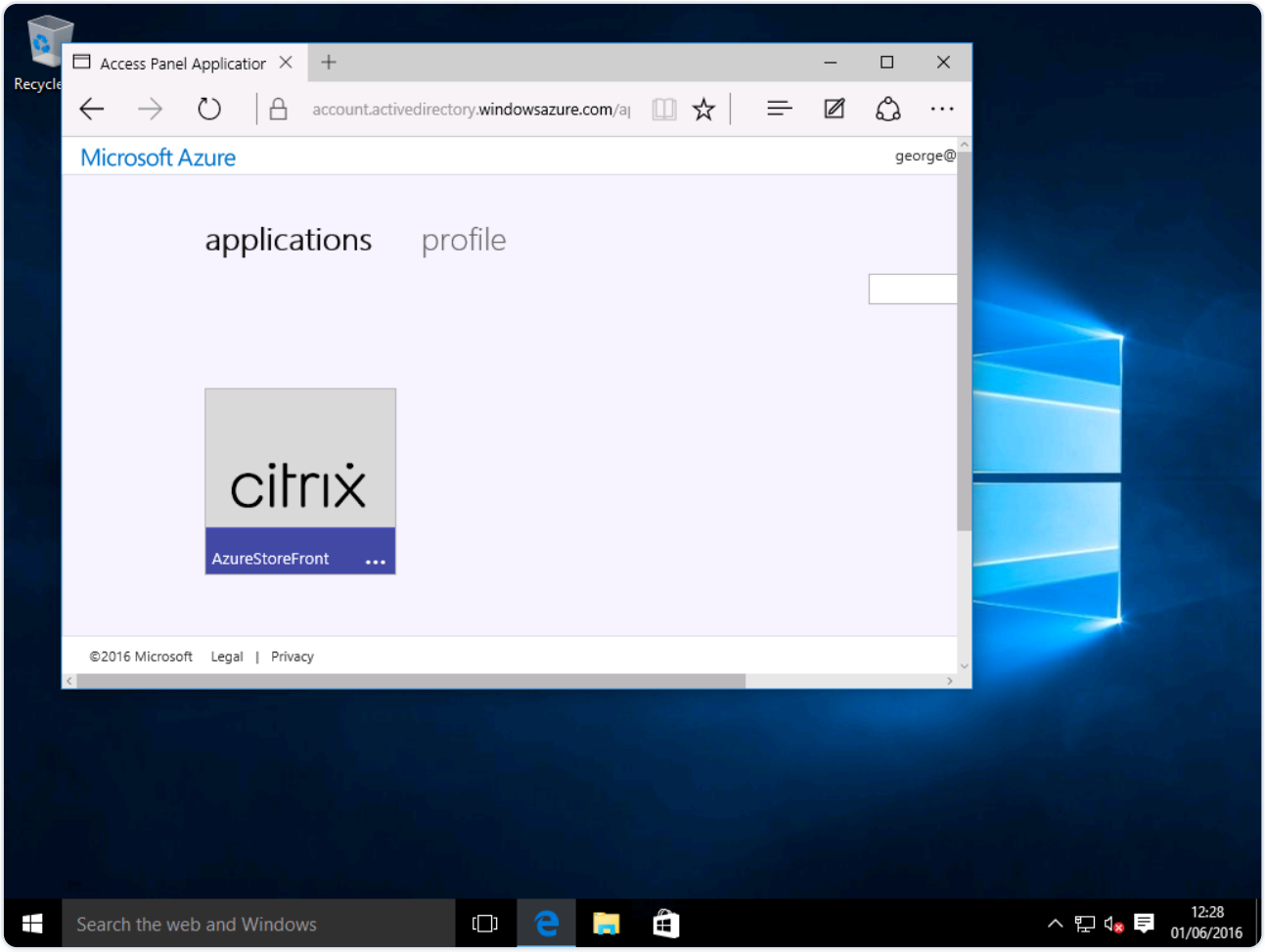


验证端到端系统

使用在 Azure AD 中注册的帐户登录到已加入 Azure AD 的 Windows 10 桌面。启动 Microsoft Edge 并连接到：`<https://myapps.microsoft.com>`。

Web 浏览器应显示用户的 Azure AD 应用程序。

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



验证单击图标是否会将您重定向到已通过身份验证的 StoreFront 服务器。

同样，验证使用单一登录 URL 的直接连接以及直接连接到 Citrix Gateway 站点是否会将您重定向到 Microsoft Azure 并返回。

最后，验证未加入 Azure AD 的计算机是否也能使用相同的 URL 正常运行（尽管首次连接时需要对 Azure AD 进行一次显式登录）。

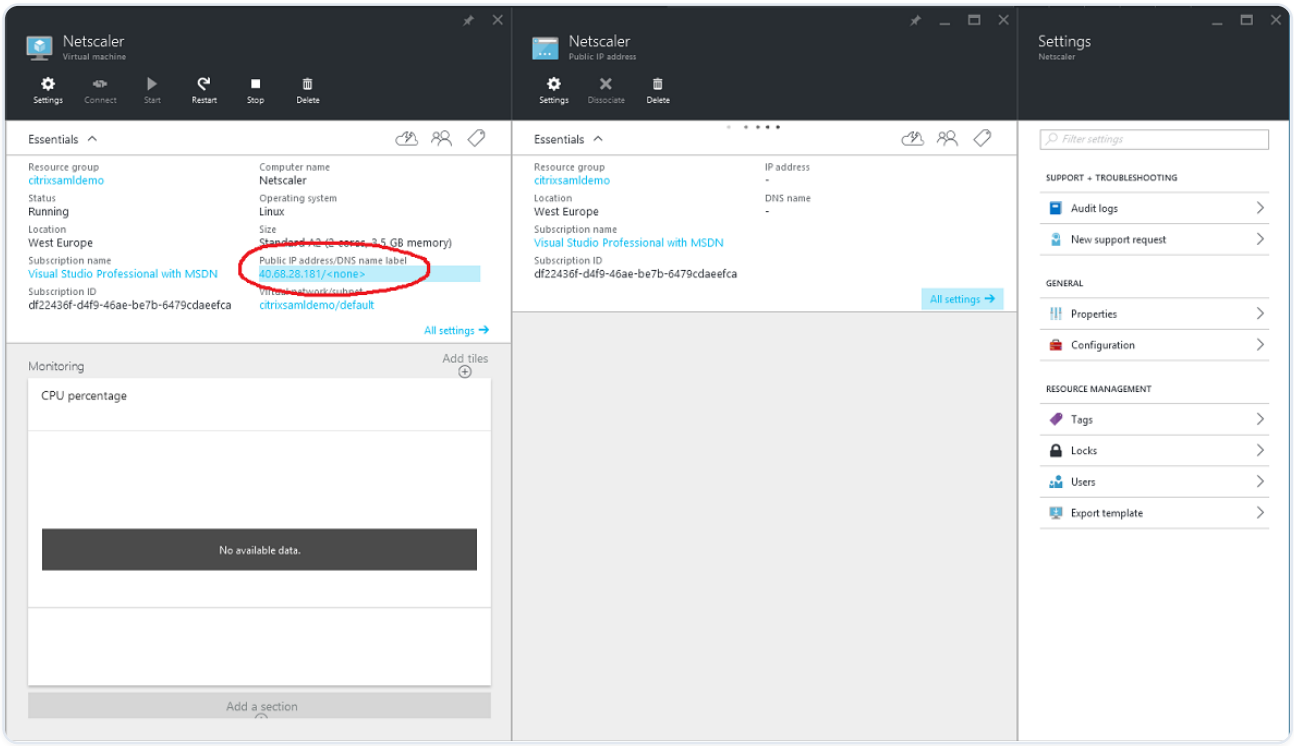
附录

在 Azure 中设置 VM 时，应配置以下标准选项。

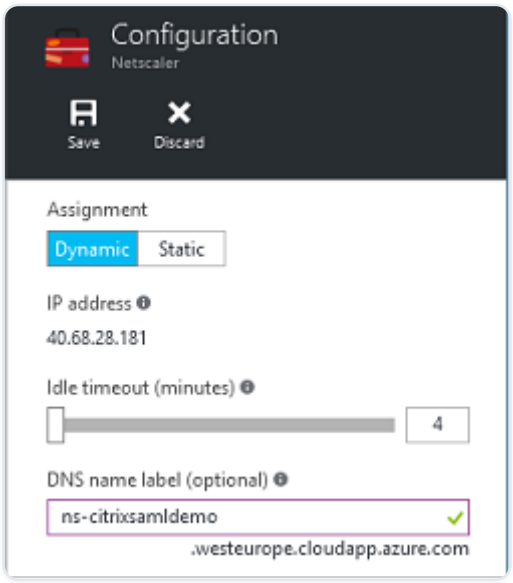
提供公共 IP 地址和 DNS 地址

Azure 为所有 VM 在内部子网（本例中为 10.*.*.*）上分配一个 IP 地址。默认情况下，还会提供一个公共 IP 地址，该地址可以通过动态更新的 DNS 标签进行引用。

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



选择 **公共 IP 地址/DNS 名称标签** 的 **配置**。为 VM 选择一个公共 DNS 地址。这可用于其他 DNS 区域文件中的 CNAME 引用，确保所有 DNS 记录即使在 IP 地址重新分配后也能正确指向 VM。

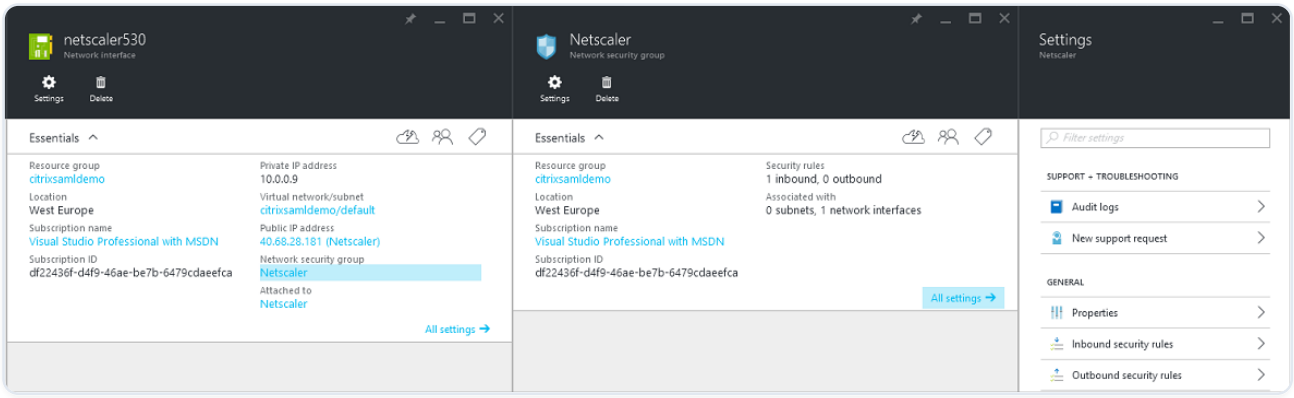


设置防火墙规则（安全组）

云中的每个 VM 都会自动应用一组防火墙规则，称为安全组。安全组控制从公共 IP 地址转发到私有 IP 地址的流量。默认情况下，Azure 允许将 RDP 转发到所有 VM。Citrix Gateway 和 ADFS 服务器也必须转发 TLS 流量 (443)。

打开 VM 的 **网络接口**，然后单击 **网络安全组** 标签。配置 **入站安全规则** 以允许适当的网络流量。

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



相关信息

- 安装和配置 是 FAS 安装和配置的主要参考。
- 常见的 FAS 部署在 部署架构 文章中进行了总结。
- “操作方法”文章在 高级配置 文章中介绍。

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

联合身份验证服务 2402 LTSR 文档历史记录

下表介绍了对联合身份验证服务 2311 文档所做的重要变更。要接收有关这些更新的通知，请订阅 RSS 源。

日期	更改	说明
15 Apr 2024	发布联合身份验证服务 2402	有关详细信息，请参阅新增功能。

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