

联合身份验证服务

Contents

联合身份验证服务 2411	10
早期版本	10
参考	11
联合身份验证服务 2411	12
续订 FAS 授权证书，不中断用户服务	12
改进了 FAS 中密钥存储的管理流程	12
支持椭圆曲线密钥	12
联合身份验证服务 KSP 远程处理（正式发布）	12
已修复的问题	12
已知问题	12
第三方通知	13
系统要求	14
安装和配置	16
安装和设置顺序	16
安装联合身份验证服务	16
升级 FAS	17
在 StoreFront 存储上启用 FAS 插件	17
配置交付控制器™	17
配置组策略	18
会话内行为	21
提示范围	21
同意超时	21
锁定后断开连接	21
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
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 服务器以用于 FAS	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	47
FAS 服务器	48
续订 FAS 授权证书	49
使用 FAS 管理控制台	49
使用 PowerShell	51
取消 FAS 授权并删除 FAS 证书	51
使用 FAS 管理控制台	51
使用 PowerShell	52
脱机授权	53
相关信息	58

私钥保护	59
简介	59
关于 FAS 证书和模板的信息	59
FAS 授权证书	60
FAS 用户证书	61
私钥存储选项	61
密钥配置 PowerShell 命令	62
配置方案示例	66
示例 1 - 将所有密钥存储在 Microsoft 软件密钥存储提供程序中	66
示例 2 - 将授权证书密钥存储在 TPM 中	66
示例 3 - 将所有密钥存储在 HSM 中	67
示例 4 - 使用椭圆曲线密钥	67
测试私钥配置	68
检查 FAS 证书	68
检查授权证书	68
检查用户证书	69
从 Citrix Virtual Apps and Desktops 2411 之前的 FAS 版本升级	70
加密远程处理	73
禁用 KSP 远程处理	73
维护模式	73
使用管理控制台	74
使用 PowerShell	74
相关信息	74
安全和网络配置	74
网络体系结构	75
防火墙和网络安全	75
Citrix 联邦身份验证服务与 Citrix Cloud™ 之间的连接	76
安全注意事项	77

委派的注册代理	77
访问控制列表配置	78
防火墙设置	78
事件日志监控	78
硬件安全模块	78
管理职责	78
组策略设置	79
证书模板	79
重命名证书模板	79
修改常规属性	79
修改请求处理属性	79
修改加密属性	79
修改密钥证明属性	80
修改已取代的模板属性	80
修改扩展属性	80
修改安全属性	80
修改使用者名称属性	81
修改服务器属性	81
修改颁发要求属性	81
修改兼容性属性	82
证书颁发机构管理	82
发布模板	82
防火墙设置	82
受限注册	83
策略模块和审计	83
FAS 管理	83
通过 ACL 限制 StoreFront、用户和 VDA	83
配置规则	84

配置证书颁发机构和模板	84
会话内和身份验证证书	84
私钥保护和密钥长度	84
事件日志	85
管理访问和管理工具	85
Citrix 虚拟应用、Citrix 虚拟桌面和 VDA 管理员	85
通用 Windows 服务器安全性	85
相关信息	85
性能计数器	85
排查 Windows 登录问题	87
证书和公钥基础设施	87
UPN 名称和证书映射	88
Active Directory 中的 UPN 名称	88
证书映射服务	88
控制登录域控制器选择	89
控制域控制器选择	89
识别正在使用的域控制器	89
启用帐户审核事件	89
证书验证日志	89
检查证书有效性	89
启用 CAPI 日志记录	89
CAPI 日志	90
错误消息	90
Kerberos 日志	91
域控制器和工作站日志	91
域控制器 CAPI2 日志	92
域控制器安全日志	92
VDA 安全日志	93

VDA CAPI 日志	94
VDA 系统日志	95
使用 Windows 事件日志监视 FAS	95
FAS 服务是否正在运行？	96
FAS 运行状况事件	96
云连接的 FAS 事件	97
安全事件	98
FAS 事件日志	98
管理事件	98
创建身份断言	101
作为信赖方	102
会话内证书服务器	102
FAS 断言插件	103
启用 Workspace 的 FAS	103
登录	105
会话内证书	105
证书请求和密钥对生成	106
最终用户错误消息	106
相关信息	107
PowerShell cmdlet 命令	107
部署架构	108
简介	108
架构概述	108
内部部署	109
思杰网关部署	111
ADFS SAML 部署	113
B2B 帐户映射	115
Windows 10 Azure 活动目录加入	116

ADFS 部署	117
简介	117
SAML 概述	118
重定向 URL	119
标识符	119
返回地址	119
签名证书	119
单点注销 URL	119
配置	119
填写 SAML 策略	120
相关信息	121
Azure AD 集成	121
简介	121
体系结构	122
创建 DNS 区域	123
创建云服务	125
创建 Windows 虚拟机	125
域控制器	126
ADFS 控制器和 Web 应用程序代理服务器	126
Citrix Virtual Desktops™ 投递控制器和 VDA	127
配置内部 DNS	127
配置外部 DNS 地址	128
配置安全组	128
创建 ADFS 证书	129
设置 Azure AD	130
创建新目录	130
创建全局管理员用户 (AzureAdmin)	132
将您的域注册到 Azure AD	133

安装 Azure AD 连接	134
启用 Azure AD Join	143
安装 Citrix 虚拟应用 或 Citrix 虚拟桌面	146
安装联合身份验证服务	147
配置 StoreFront	147
配置 StoreFront 以使用 Citrix Gateway	148
为 StoreFront 的单点登录配置新的 Azure AD 应用程序	149
配置图标	149
配置 SAML 身份验证	150
将应用程序分配给用户	152
MyApps 页面	153
单点登录 URL	153
安装和配置 Citrix Gateway	154
运行 Citrix Virtual Apps and Desktops 安装向导	154
配置用于 AD 帐户管理的域控制器	155
配置 StoreFront 地址	156
验证 Citrix Gateway 部署	157
启用 Citrix Gateway SAML 身份验证支持	158
验证端到端系统	158
附录	158
提供公共 IP 地址和 DNS 地址	158
设置防火墙规则（安全组）	159
相关信息	160
联合身份验证服务 2411 文档历史记录	161

联合身份验证服务 2411

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 2411 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 2407](#)
- [联合身份验证服务 2402 LTSR](#)
- [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 and 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。

参考

- [Active Directory 证书服务概述](#)
- [配置 Windows 以进行证书登录](#)

联合身份验证服务 2411

续订 FAS 授权证书，不中断用户服务

以前，续订 FAS 授权证书会导致用户服务中断。通过此更改，该过程已得到简化和改进，不再导致用户服务中断。有关详细信息，请参阅 [续订 FAS 授权证书](#)。

改进了 FAS 中密钥存储的管理流程

以前，FAS 私钥的存储位置配置是通过

`Citrix.Authentication.FederatedAuthenticationService.exe.config` XML 文件处理的。这在管理上一直是一个痛点，并且配置在 FAS 升级后不会保留。通过此更改，PowerShell cmdlet 用于私钥配置。用户和 RA 证书私钥的配置是单独存储的，进一步简化，并在升级后保留。有关详细信息，请参阅 [私钥保护](#)

支持椭圆曲线密钥

到目前为止，FAS 仅支持在其证书中使用 RSA 密钥。通过此更改，FAS 引入了对 ECC 证书的支持。有关详细信息，请参阅 [示例 4 - 使用椭圆曲线密钥](#)。

联合身份验证服务 KSP 远程处理（正式发布）

通过此更改，通过使用一对在 VDA 上运行的密钥存储提供程序 (KSP)，实现了将加密操作从 Windows VDA 远程传输到 FAS 服务器。这取代了 FAS 早期版本中使用的加密服务提供程序 (CSP)。KSP 是向 Windows 应用程序公开加密操作的最新方式，它支持更多功能。有关详细信息，请参阅 [KSP 远程处理](#)。

有关错误修复的信息，请参阅 [已修复的问题](#)。

已修复的问题

联合身份验证服务 2411 中没有已修复的问题。

已知问题

当 FAS 配置为使用 EC（椭圆曲线）密钥生成用户证书时，以下 PowerShell 命令无法按预期工作：

Test-FasCrypto

Test-FasUserCertificateCrypto

即使加密和用户证书正常，这些命令也始终返回失败响应。

第三方通知

此版本的 Federated Authentication Service 可能包含根据以下文档中定义的条款获得许可的第三方软件：

- [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 \(PDF 下载\)](#)

系统要求

- 联合身份验证服务 (FAS) 支持以下 Windows Server 版本：
 - Windows Server 2025 标准版和数据中心版
 - Windows Server 2022 标准版和数据中心版
 - Windows Server 2019 Standard 和 Datacenter 版本，以及带 Server Core 选项的版本
 - Windows Server 2016 Standard 和 Datacenter 版本，以及带 Server Core 选项的版本
- 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](#) 要求在 FAS 服务器上安装 Windows PowerShell 64 位版本。
- 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 配合使用。有关这些验证的支持，请联系供应商：
 - Keyfactor 命令
 - Sectigo 证书管理器
 - Venafi 零接触 PKI
 - HDI PKIaaS (维纳菲)
 - Entrust WNES 系统
 - AppViewX
 - 艾弗信浩睿 CLM
 - 开放信任 PKI
 - 身份识别 PKI-3
 - 迪吉证书自动注册服务器
- 如需在非 Microsoft CA 环境中使用 FAS 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。

- CA 证书位于域控制器上的 NTAAuth 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 NTAAuth 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 思杰虚拟应用 或 思杰虚拟桌面™ 站点中：

- Delivery Controller、Virtual Delivery Agent (VDA) 和 StoreFront™ 服务器都必须是受支持的版本。

规划此服务的部署时，请查看 [安全注意事项](#) 部分。

安装和配置

安装和设置顺序

1. 安装联合身份验证服务(/zh-cn/federated-authentication-service/2411/install-configure.html#install-the-federated-authentication-service) (FAS)
2. 在 StoreFront 商店中启用 FAS 插件(/zh-cn/federated-authentication-service/2411/install-configure.html#enable-the-fas-plug-in-on-storefront-stores)
3. 配置交付控制器(/zh-cn/federated-authentication-service/2411/install-configure.html#configure-the-delivery-controller)
4. 配置组策略(/zh-cn/federated-authentication-service/2411/install-configure.html#configure-group-policy)
5. 使用 FAS 管理控制台执行以下操作：
 - a. 部署证书模板(/zh-cn/federated-authentication-service/2411/install-configure.html#deploy-certificate-templates)
 - b. 设置证书颁发机构(/zh-cn/federated-authentication-service/2411/install-configure.html#set-up-active-directory-certificate-services)
 - c. 授权 FAS 使用您的证书颁发机构(/zh-cn/federated-authentication-service/2411/install-configure.html#authorize-federated-authentication-service)
 - d. 配置规则(/zh-cn/federated-authentication-service/2411/install-configure.html#configure-rules)
 - e. 将 FAS 连接到 Citrix Cloud(/zh-cn/federated-authentication-service/2411/install-configure.html#connect-to-citrix-cloud) (可选)

安装联合身份验证服务

为安全起见，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（从插入 ISO 时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](#) 上以 MSI 文件的形式获取）。

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
- 性能计数器 和 事件日志

升级 FAS

您可以使用就地升级将 FAS 升级到较新版本。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 安装程序或从独立的 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。

有关如何在 StoreFront 商店中启用 FAS 插件的更多详细信息，请参阅 <https://docs.citrix.com/zh-cn/storefront/current-release/configure-authentication-and-delegation/fas>。

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。每个站点只需运行此命令一次，无论站点上有多少个 Delivery Controller。

配置组策略

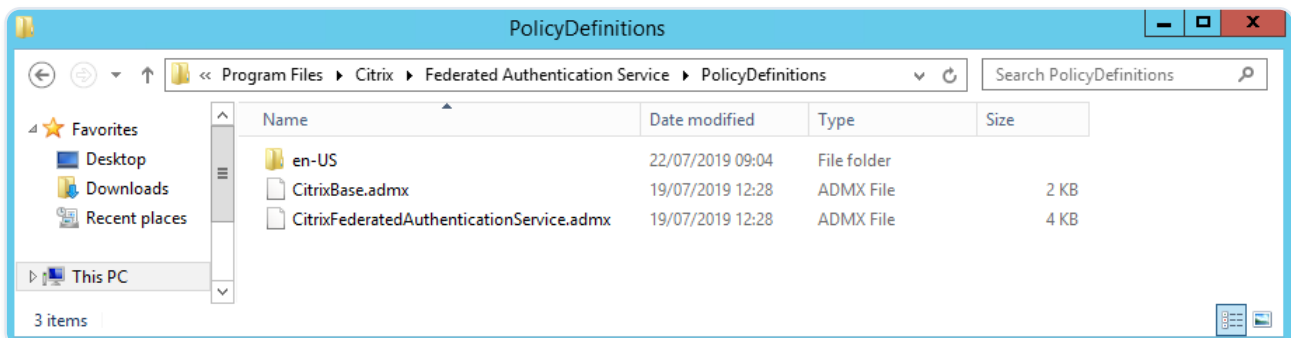
安装 FAS 后，使用安装中提供的组策略模板在组策略中指定服务器的完全限定域名 (FQDN)。

重要：

确保请求票证的 StoreFront 服务器和兑换票证的 Virtual Delivery Agents (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。

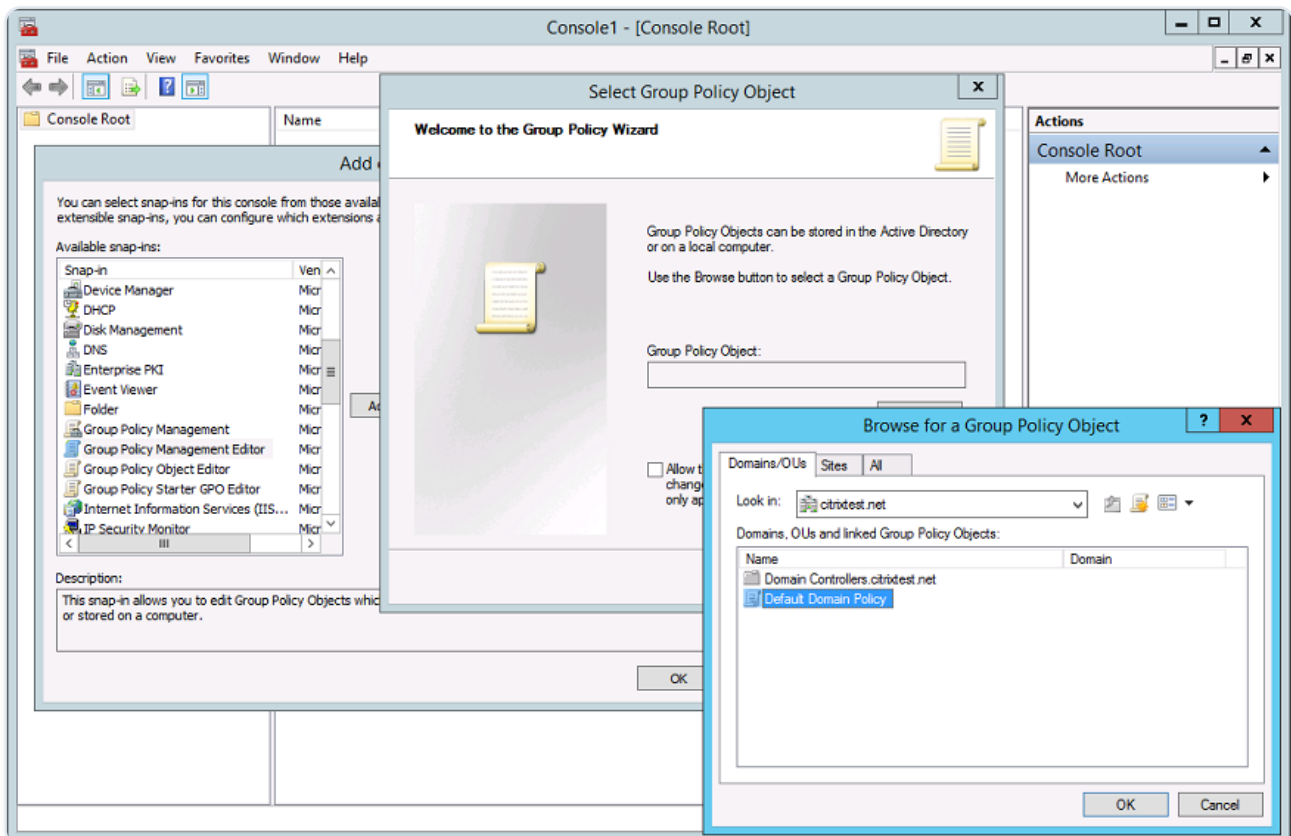
步骤 1. 在安装 FAS 的服务器上，找到 C:\Program Files\Citrix\Federated Authentication Service\PolicyDefinitions\CitrixFederatedAuthenticationService.admx 和 CitrixBase.admx 文件以及 en-US 文件夹。



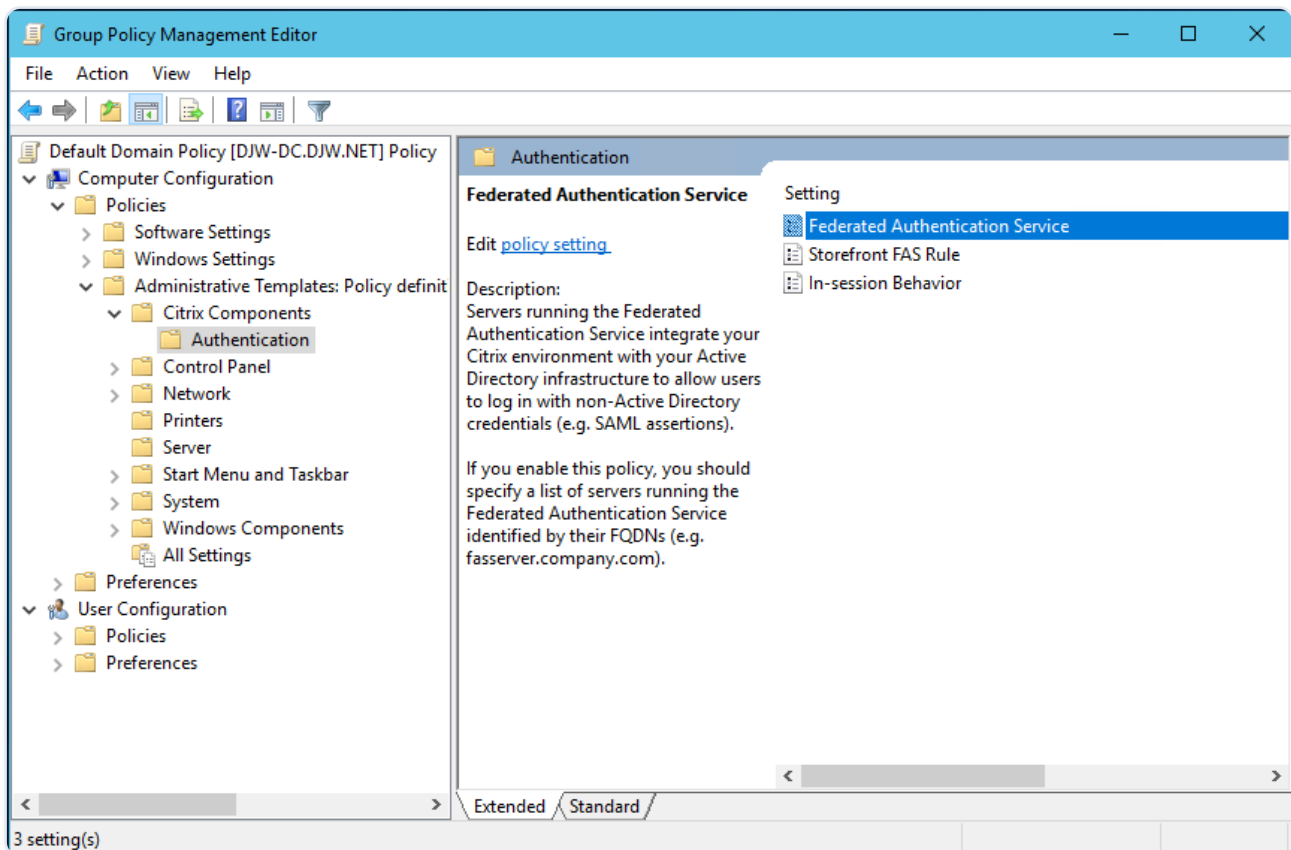
步骤 2. 将这些文件复制到您的域控制器，并将其放置在 C:\Windows\PolicyDefinitions 和 en-US 子文件夹中。

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。



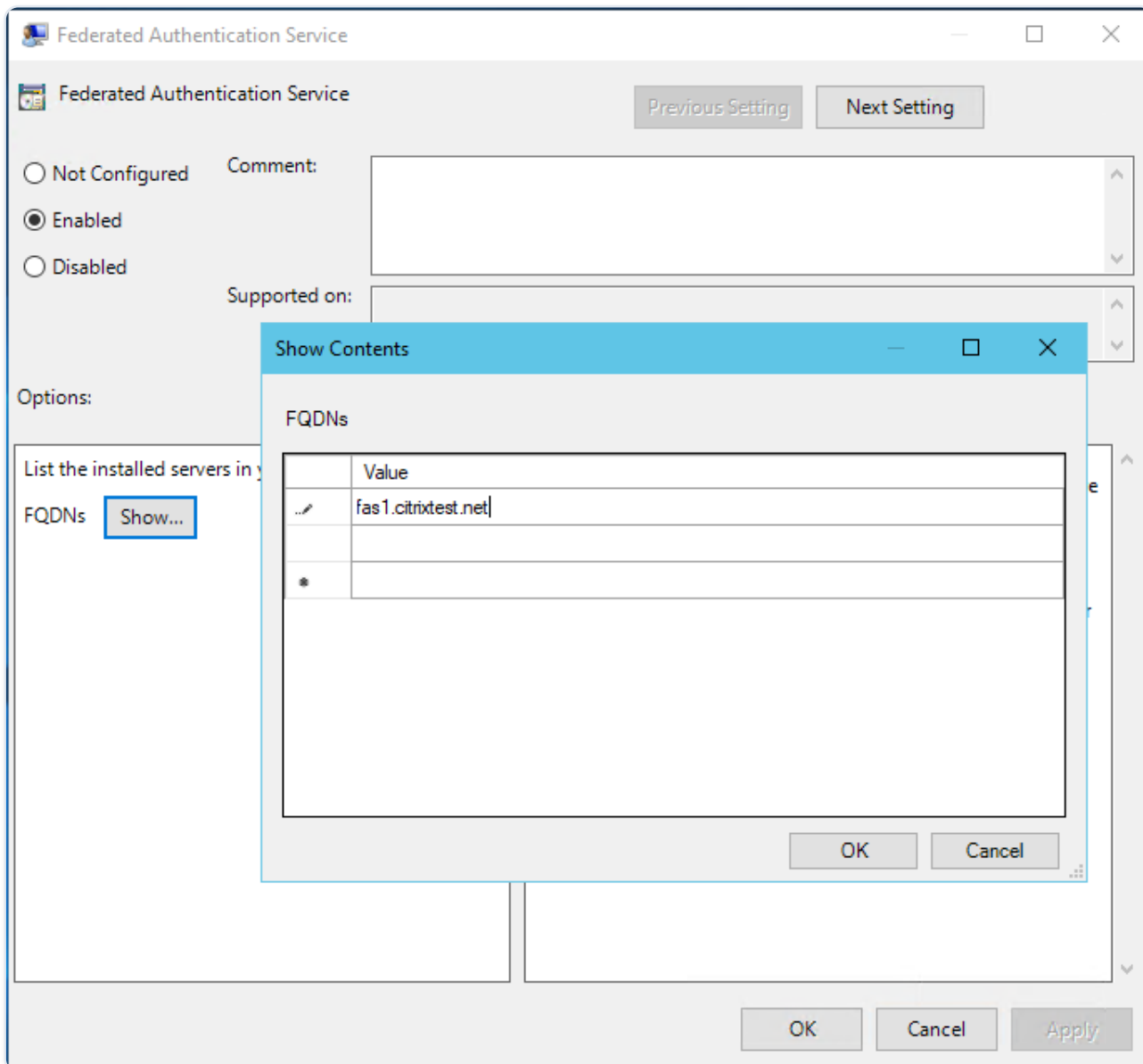
步骤 4. 导航到计算机配置/策略/管理模板/Citrix 组件/身份验证中的 **联合身份验证服务策略**。



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**。这将允许您选择**显示**按钮，您可以在其中配置 FAS 服务器的 FQDN。



步骤 6. 输入 FAS 服务器的 FQDN。

重要提示：

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**以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**）以使更改生效。

会话内行为

此策略在用户的 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。仅当此策略已启用并且用于创建证书的 FAS 规则允许会话内使用时，会话内证书才可用，请参阅[配置规则](#)。

会话中行为。(/en-us/federated-authentication-service/2411/media/in-session-behavior.png)

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，并阻止 FAS 代理进程运行。

提示范围

如果启用此策略，**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中证书。有三个选项：

- **无需同意**—此选项禁用安全提示，并以静默方式使用私钥。
- **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。

同意超时

如果启用此策略，**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。

锁定后断开连接

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

注意：

锁定后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](#)。

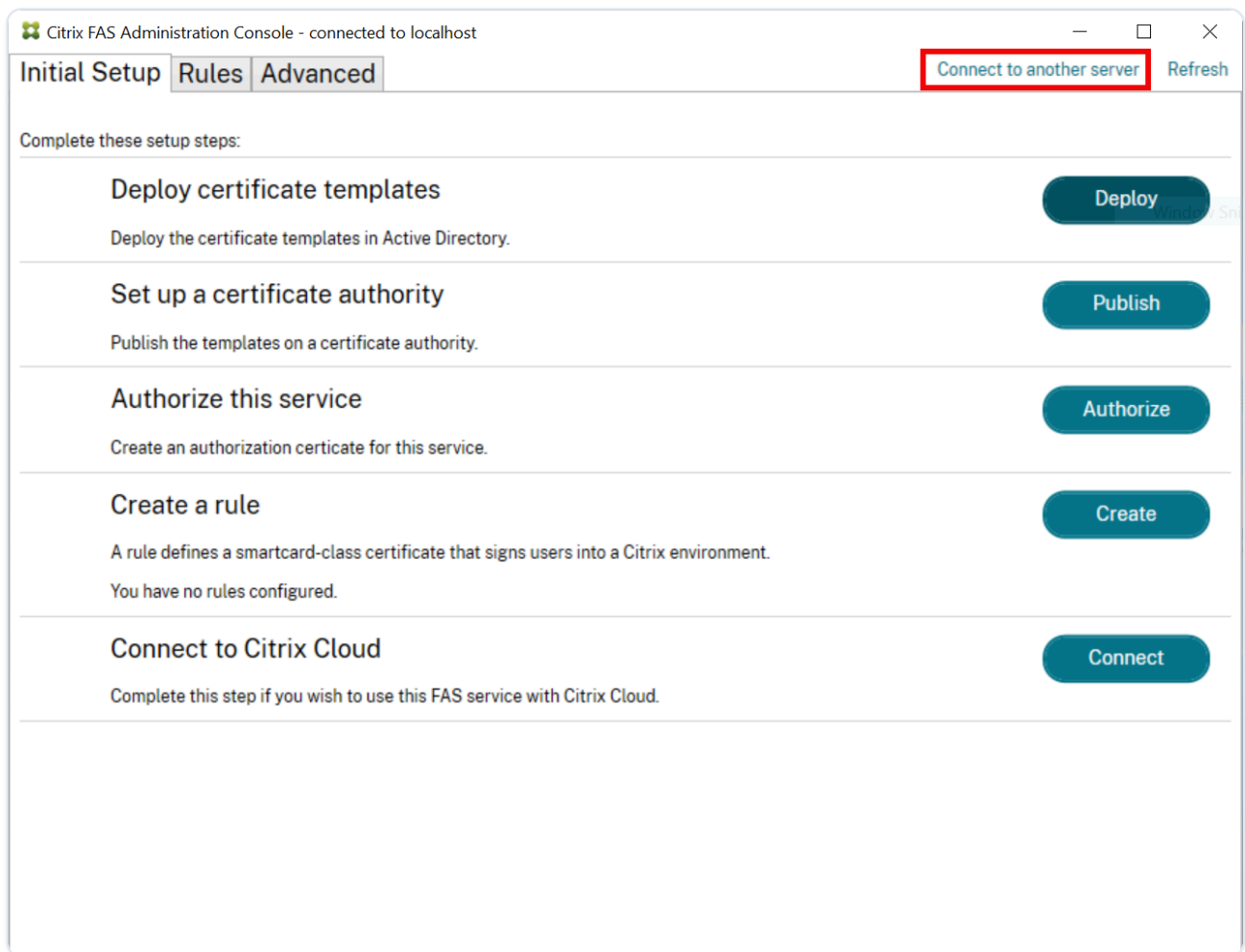
FAS 管理控制台作为 FAS 的一部分安装。启动菜单中会放置一个图标（Citrix Federated Authentication Service）。

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。

您还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。如有需要，您可以使用控制台右上角的“**连接到另一台服务器**”连接到远程服务。

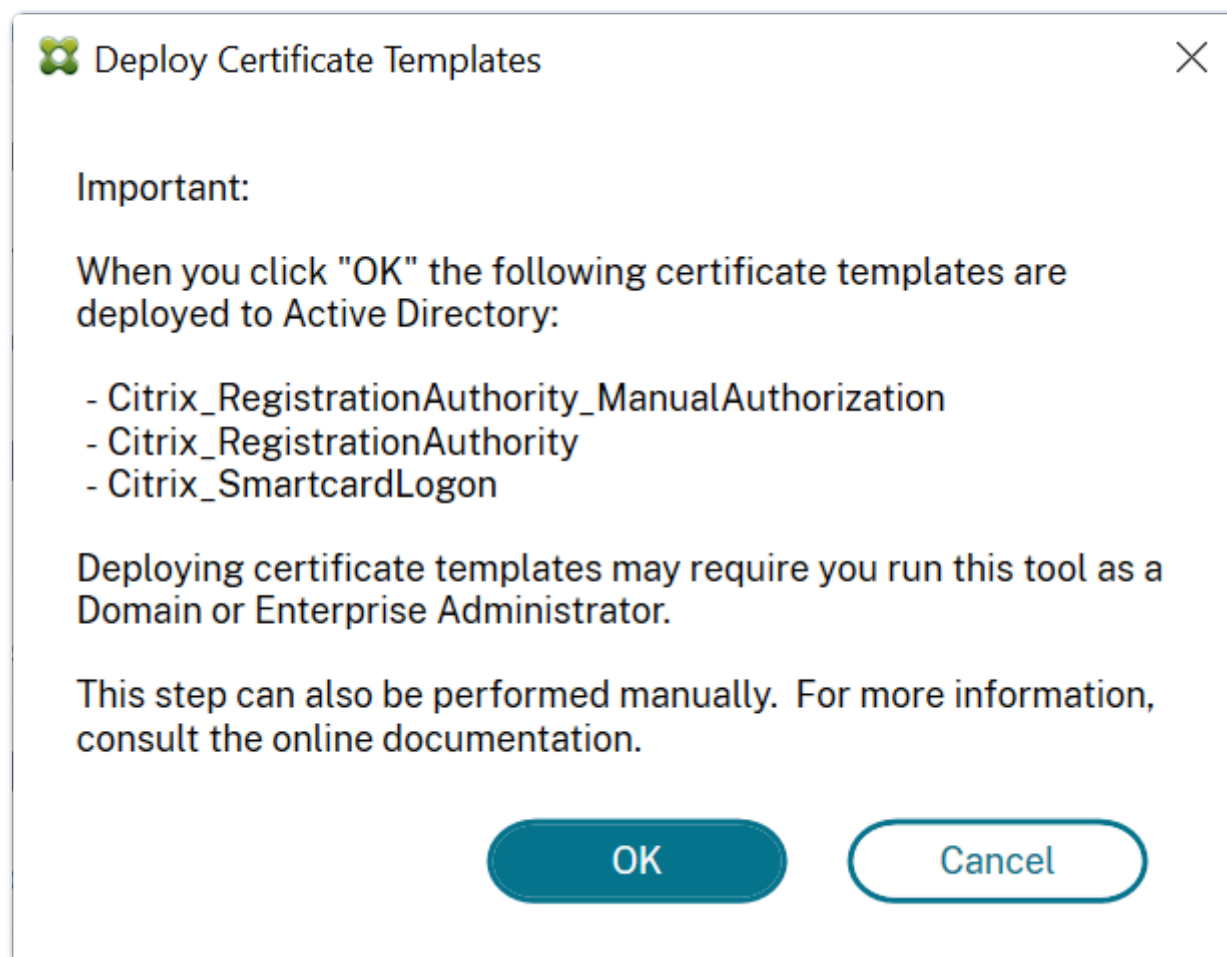


部署证书模板

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。

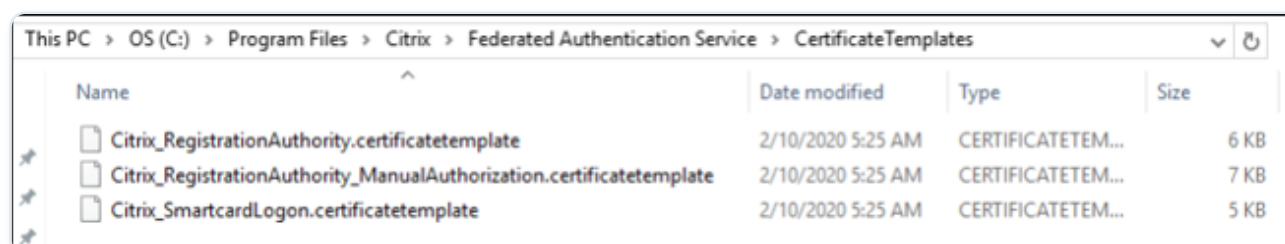
- Citrix_RegistrationAuthority_ManualAuthorization
- Citrix_RegistrationAuthority
- Citrix_SmartcardLogon

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



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\Federated Authentication Service\CertificateTemplates



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，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)
```

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

$writabletemplate = New-Object -ComObject
X509Enrollment.CX509CertificateTemplateADWritable

$writabletemplate.Initialize($comtemplate)

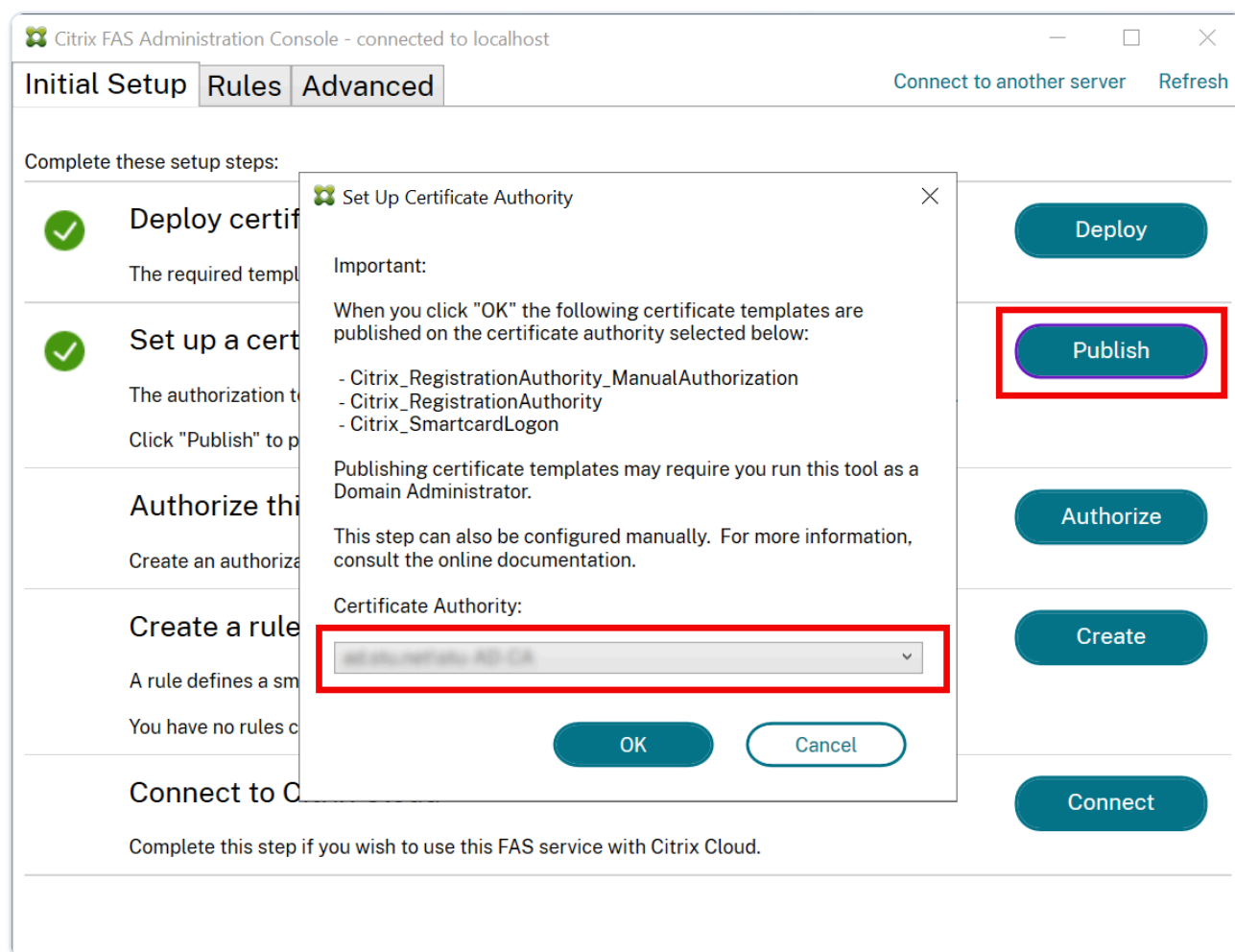
$writabletemplate.Commit(1, $NULL)
```

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 证书服务的详细信息，请参阅 Microsoft 文档。

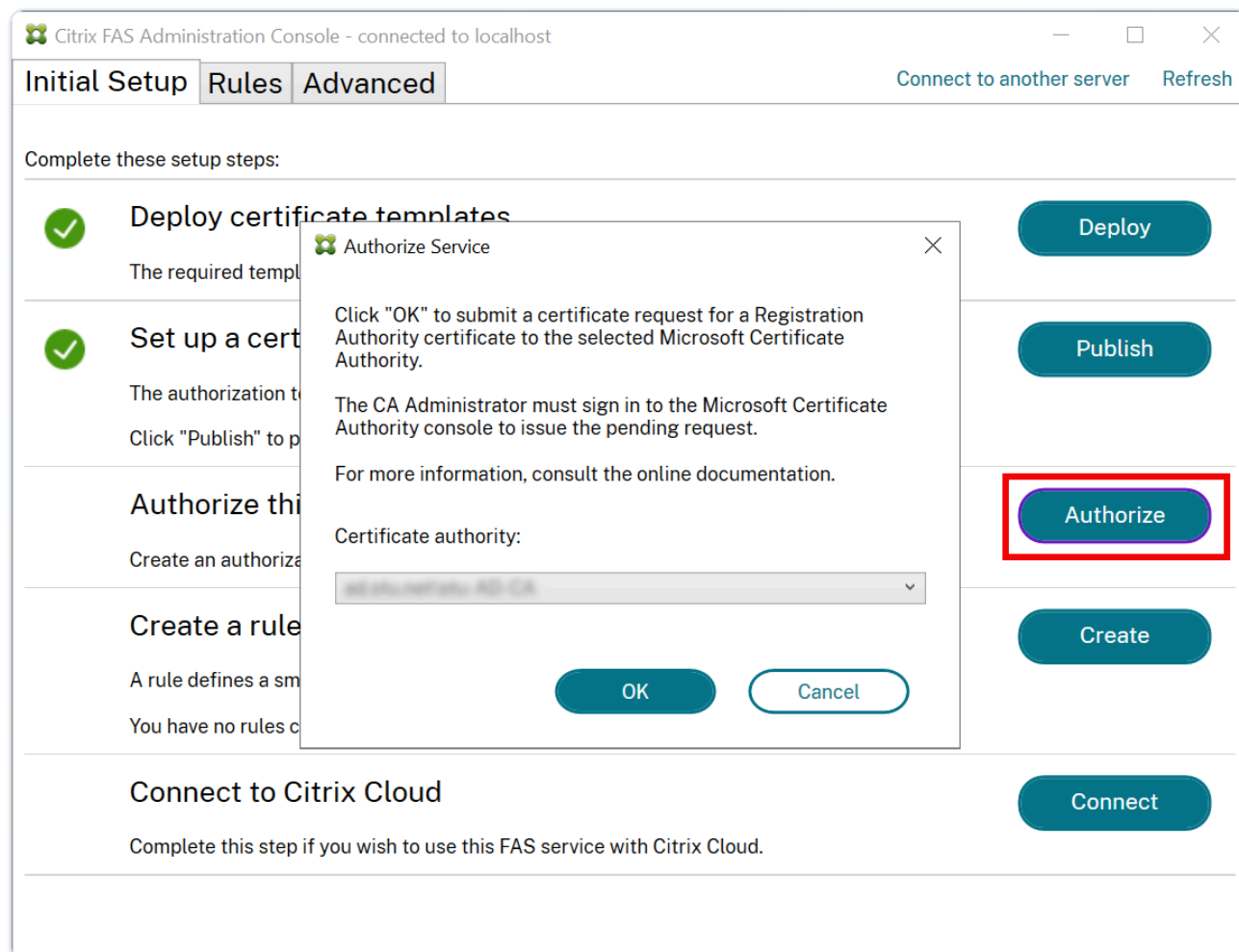
具有管理证书颁发机构权限的用户必须在至少一台服务器上发布模板。使用“设置证书颁发机构”来发布它们。

(也可以使用 Microsoft 证书颁发机构控制台发布证书模板。)



授权联合身份验证服务

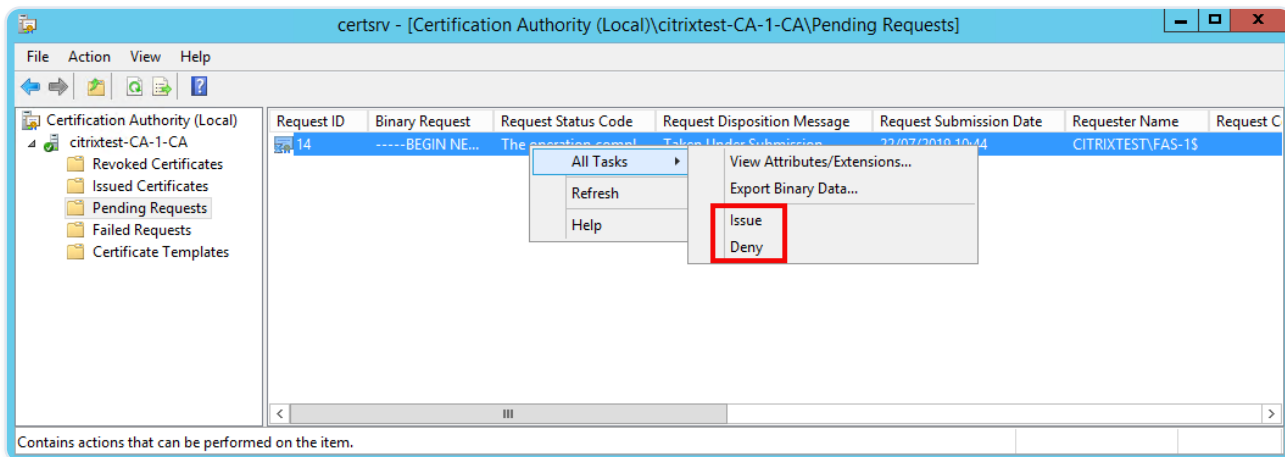
此步骤启动 FAS 的授权。管理控制台使用 Citrix_RegistrationAuthority_ManualAuthorization 模板生成证书请求，然后将其发送到发布该模板的某个证书颁发机构。



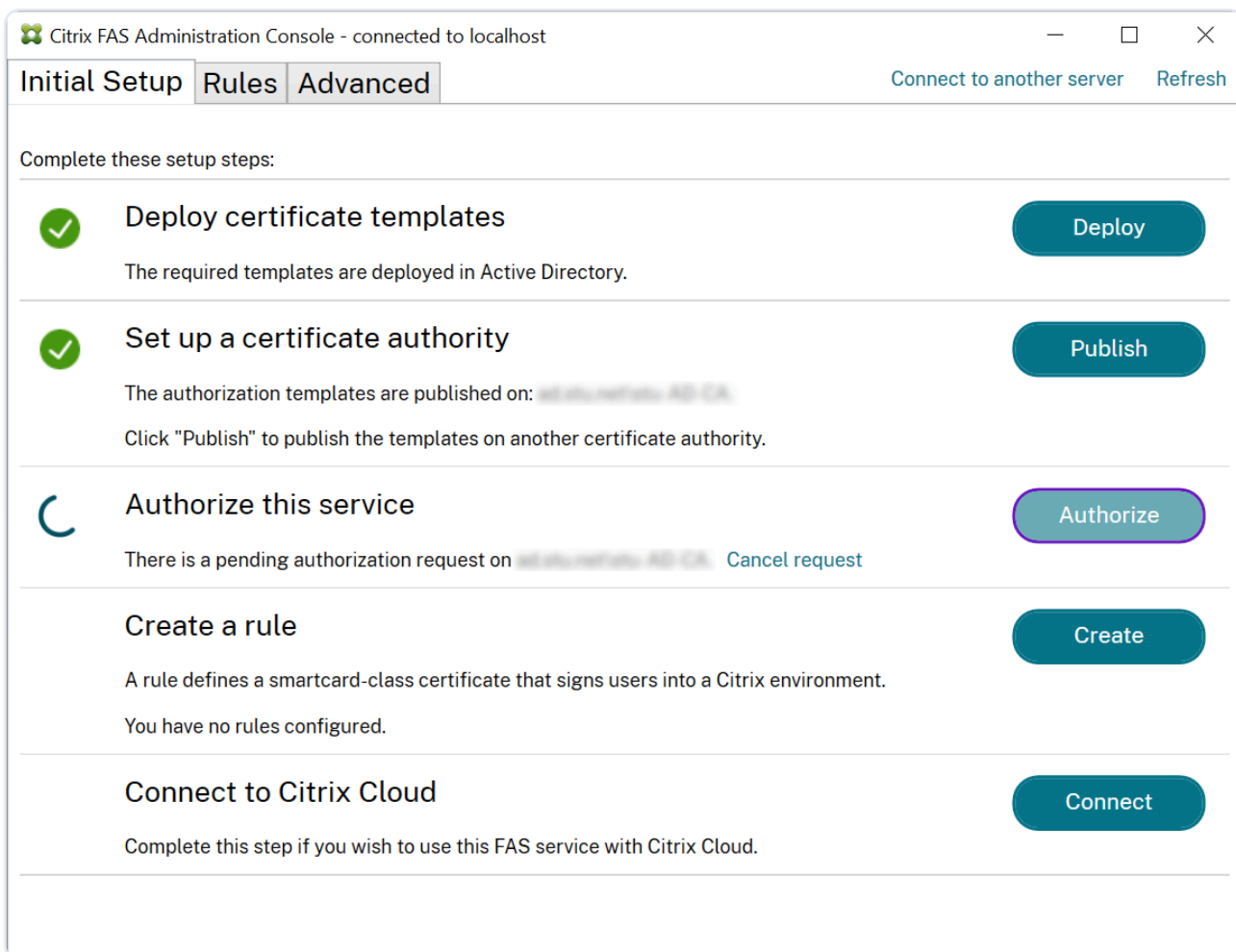
请求发送后，它会出现 Microsoft 证书颁发机构控制台的 **Pending Requests** 列表中，作为来自 FAS 计算机帐户的待处理请求。在 FAS 配置继续之前，证书颁发机构管理员必须颁发或拒绝该请求。

FAS 管理控制台会显示一个忙碌的“加载中”图标，直到管理员选择 **Issue** 或 **Deny**。

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



FAS 管理控制台会自动检测此过程何时完成。这可能需要几分钟时间。



配置规则

FAS 使用这些规则，根据 StoreFront 的指示，授权颁发用于 VDA 登录和会话内使用的证书。

每条规则指定以下内容：

- 受信任可请求证书的 StoreFront 服务器。

- 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来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配置 StoreFront 服务器，以按名称请求自定义规则。

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

Citrix FAS Administration Console - connected to localhost

Initial Setup Rules Advanced Connect to another server Refresh

A rule defines a smartcard-class certificate that signs users into a Citrix environment.

[+ Create rule](#)

Default	Summary
	Rule name: Default
	Status: OK
	Template: Citrix_SmartcardLogon
	Certificate authorities:
	Certificate available in-session: No
	Access control: Configured
	Restrictions: Not configured
	Cloud rule: No

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。请确保您选择的证书颁发机构的状态显示“模板可用”。请参阅[证书颁发机构管理](#)。

会话内使用：允许会话内使用选项控制证书是否可在登录到 VDA 后使用。

- **允许会话内使用**未选中（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证书。
- **允许会话内使用**已选中—用户在身份验证后有权访问证书。大多数客户不得选择此选项。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。然后，证书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：受信任的 StoreFront 服务器计算机列表，这些计算机有权请求用于用户登录或重新连接的证书。对于所有这些权限，您可以添加单个 AD 对象或组。

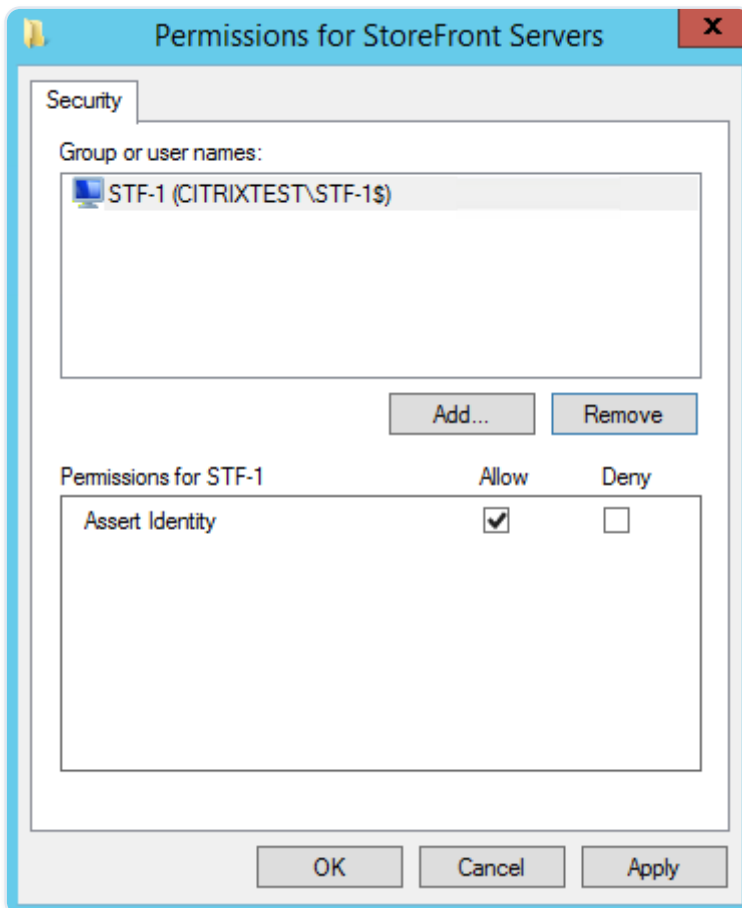
重要提示：

访问控制设置对安全性至关重要，必须谨慎管理。

注意：

如果仅将 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。您可以将相同的规则与 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。

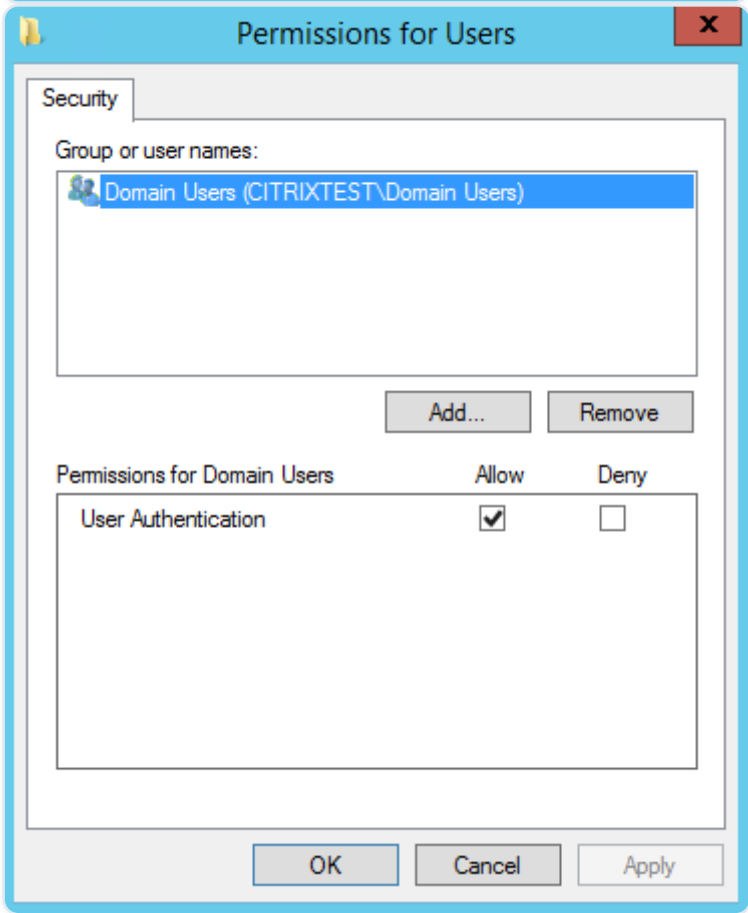
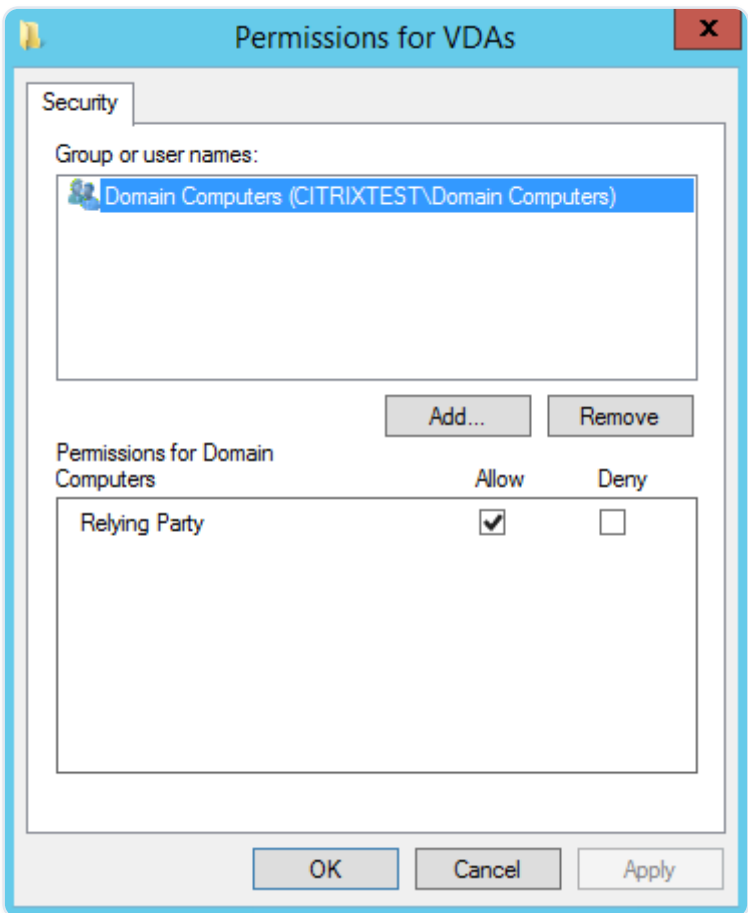


限制：可以使用 FAS 登录用户的 VDA 计算机列表以及可以通过 FAS 颁发证书的用户列表。

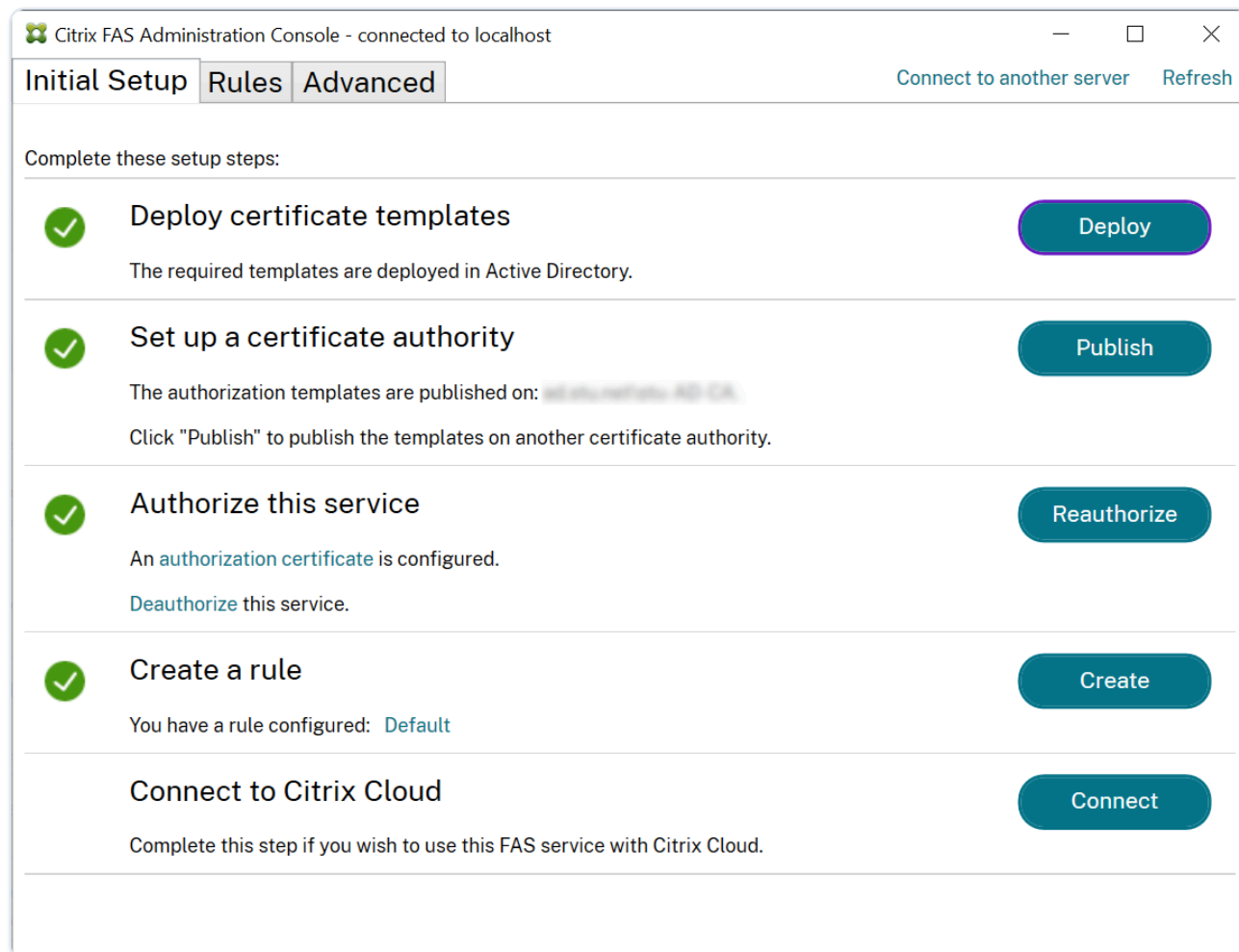
- **管理 VDA 权限**允许您指定哪些 VDA 可以使用 FAS 登录用户。VDA 列表默认为域计算机。
- **管理用户权限**允许您指定哪些用户可以使用 FAS 登录 VDA。用户列表默认为域用户。

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。



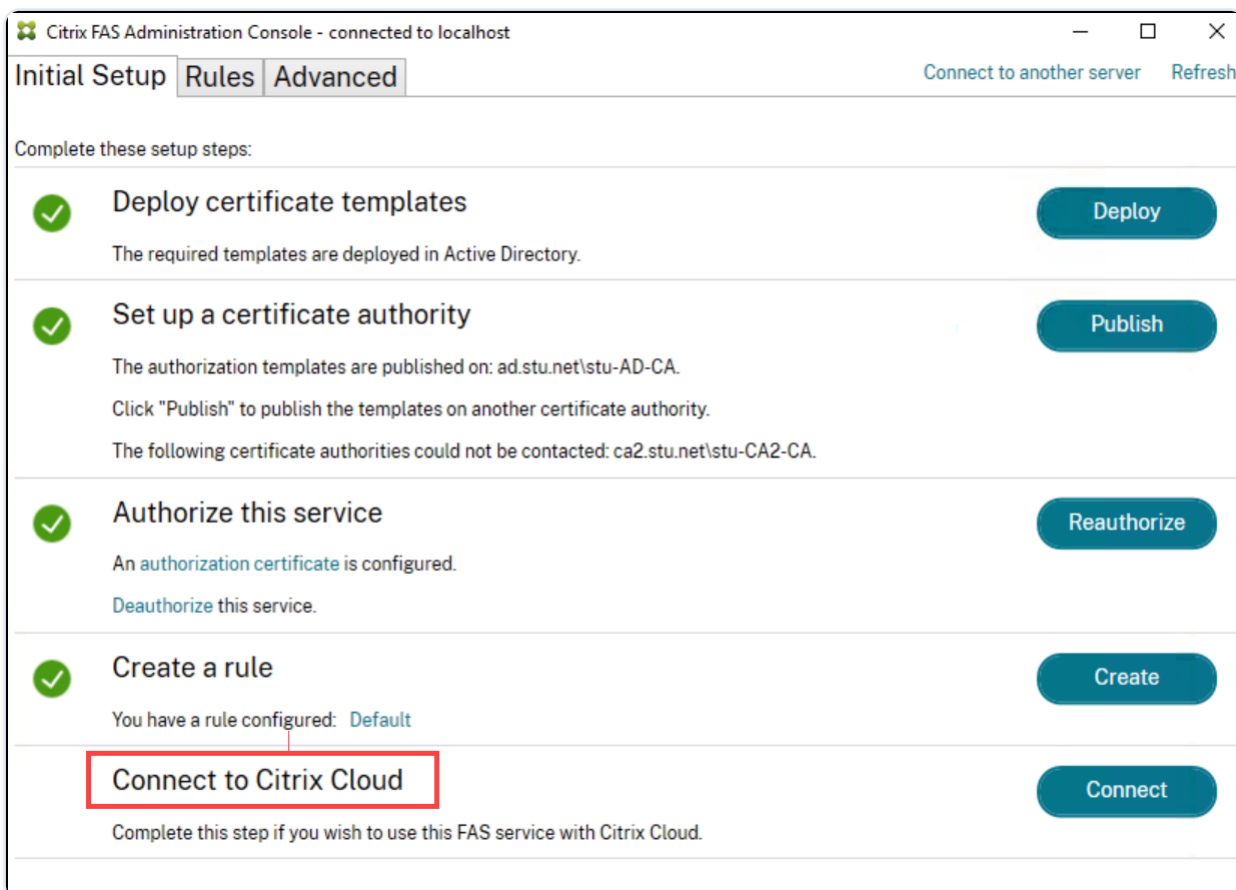
云规则：指示从 Citrix Workspace 收到身份断言时是否应用该规则。连接到 Citrix Cloud 时，您可以选择要用于 Citrix Cloud 的规则。连接到 Citrix Cloud 后，您还可以通过“**连接到 Citrix Cloud**”部分中的链接更改规则。



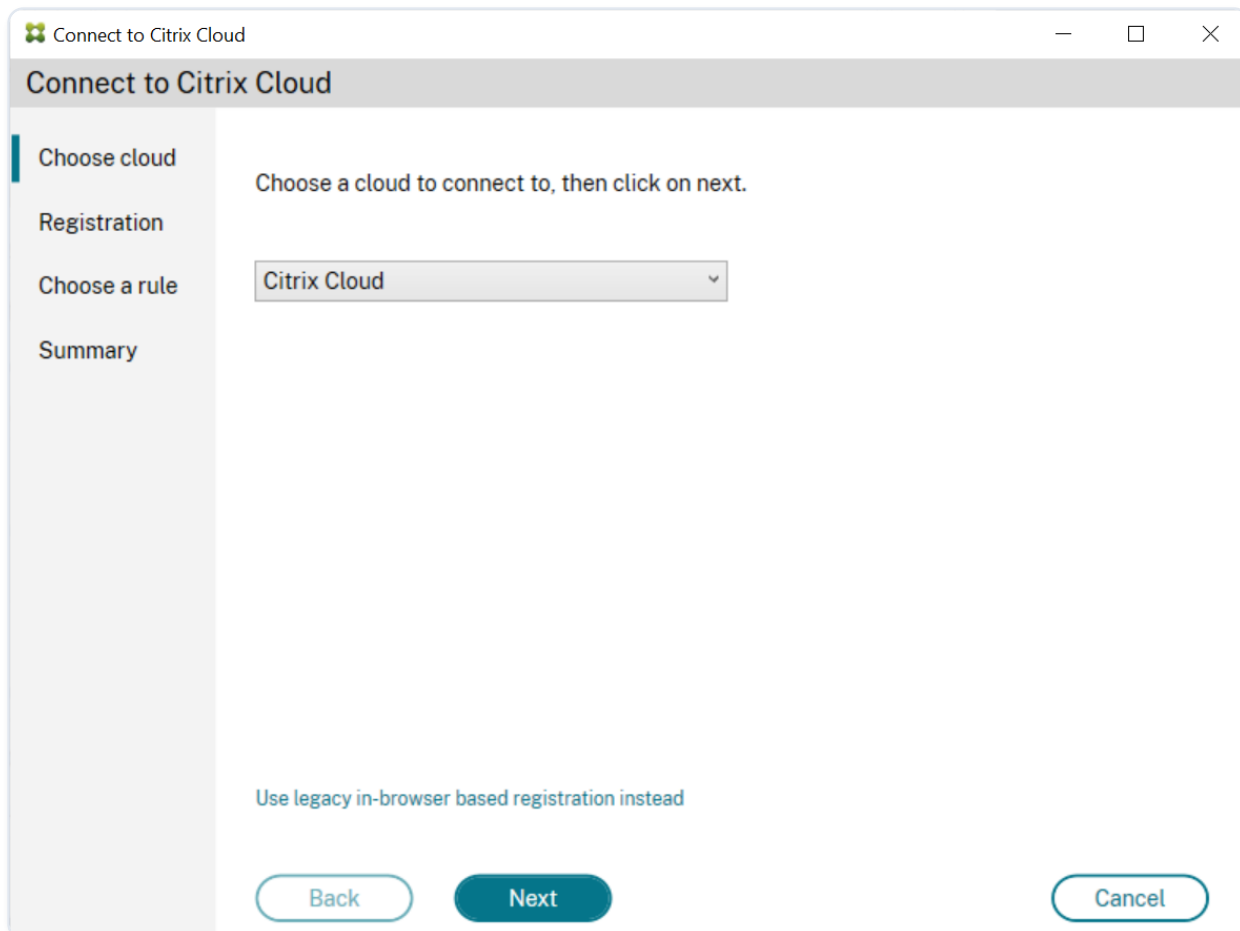
连接到 Citrix Cloud

您可以使用 Citrix Workspace 将 FAS 服务器连接到 Citrix Cloud。请参阅这篇 [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**”。



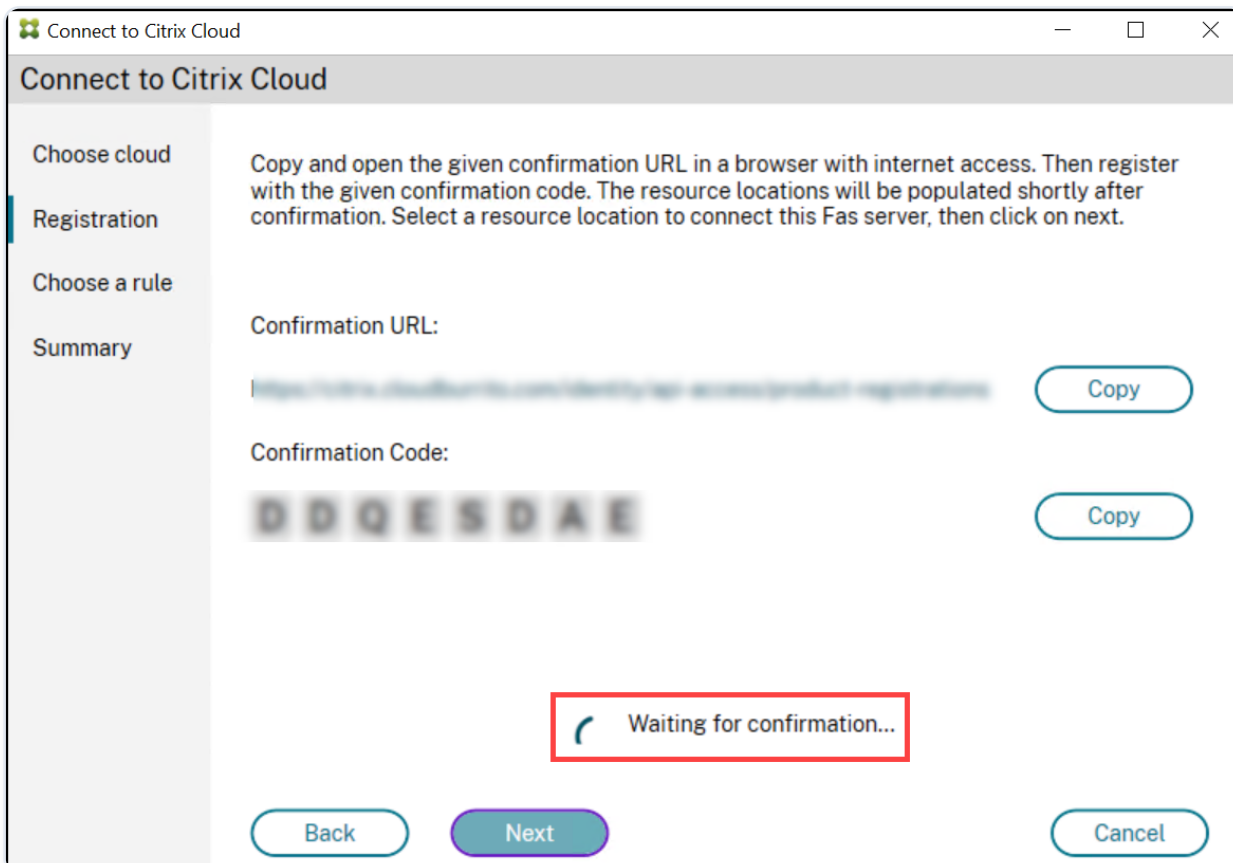
2. 选择要连接的云，然后单击“下一步”。



注意

只有 **Citrix Cloud** 在预览版中可用。

- 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 [将本地产品注册到 Citrix Cloud](#)。



- 注册码验证通过后，从下拉列表中选择所需的资源位置。

Connect to Citrix Cloud

Choose cloud

Registration

Choose a rule

Summary

Copy and open the given confirmation URL in a browser with internet access. Then register with the given confirmation code. The resource locations will be populated shortly after confirmation. Select a resource location to connect this Fas server, then click on next.

Confirmation URL:

[Redacted URL]

Copy

Confirmation Code:

[Redacted Code]

Copy

Resource location:

My Resource Location

Back Next Cancel

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**。

The screenshot shows the 'Connect to Citrix Cloud' wizard window. The title bar says 'Connect to Citrix Cloud'. The left sidebar has four steps: 'Choose cloud', 'Registration', 'Choose a rule' (which is selected with a blue dot), and 'Summary'. The main area is titled 'Choose a FAS rule to use with Citrix Cloud.' and contains three radio button options: 'I will configure a rule later', 'Create a rule when this wizard finishes', and 'Use an existing rule:'. Under 'Use an existing rule:', there is a sub-option 'Default' which is selected. At the bottom, there is a note: 'The rule you use for Citrix Cloud can also be used with on-premises StoreFront.' and three buttons: 'Back', 'Next' (highlighted in blue), and 'Cancel'.

7. 在摘要部分，单击完成以完成 Citrix Cloud 连接。

The screenshot shows the 'Connect to Citrix Cloud' wizard window at the 'Summary' step. The left sidebar now has 'Summary' selected with a blue dot. The main area is titled 'Summary' and displays four configuration items: 'Customer:' with a blurred value, 'Resource location:' with a blurred value, 'Rule:' with the value 'Default', and 'Cloud:' with the value 'Citrix Cloud'. At the bottom, there are three buttons: 'Back', 'Finish' (highlighted in blue), and 'Cancel'.

Citrix Cloud 注册 FAS 服务器，并将其显示在您的 Citrix Cloud 帐户的资源位置页面上。

注意：

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

断开与 Citrix Cloud 的连接

从 Citrix Cloud 资源位置中移除 FAS 服务器后，如这篇 [Citrix Workspace 文章](#) 中所述，在“**连接到 Citrix Cloud**”中选择“**禁用**”。

高级配置

本节中的文章提供了有关联邦身份验证服务 (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](#)文章提供了主要 FAS 体系结构的摘要，以及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

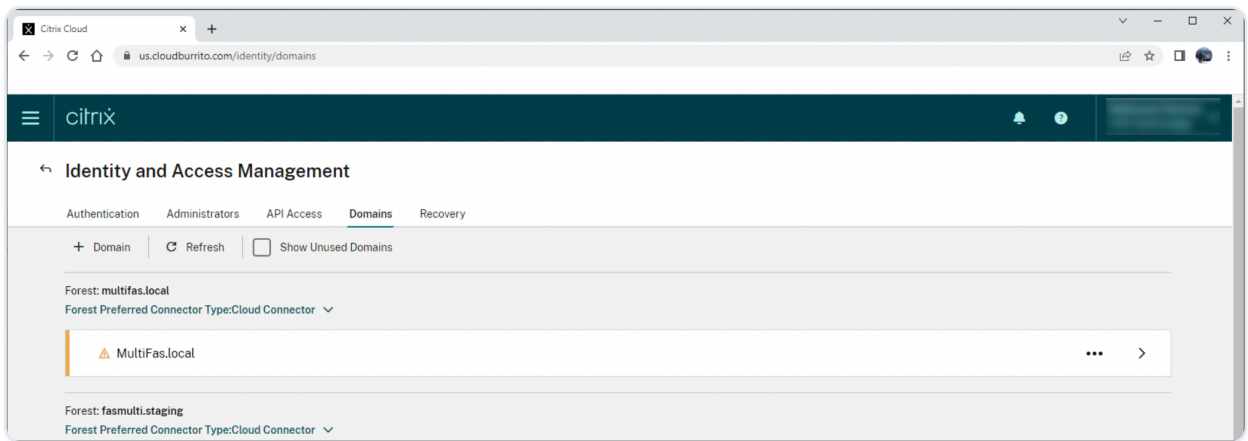
- 您拥有对 Citrix Cloud 上的域和资源位置的管理员访问权限。有关详细信息，请参阅 [修改管理员权限](#)。
- 您已设置租户-MSP 关系。有关详细信息，请参阅 [适用于 Citrix 服务提供商的 Citrix DaaS](#)。

配置 MSP 客户

1. 使用云连接器使活动目录域可用于 Citrix Cloud。

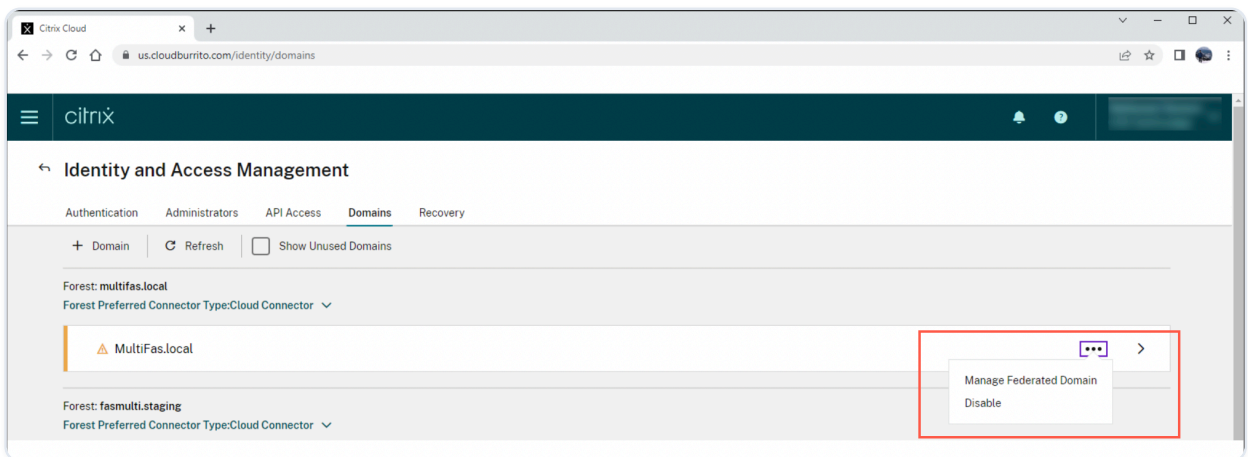
通过 [安装 Cloud Connector](#) 将本地基础架构连接到 Citrix Cloud。

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。

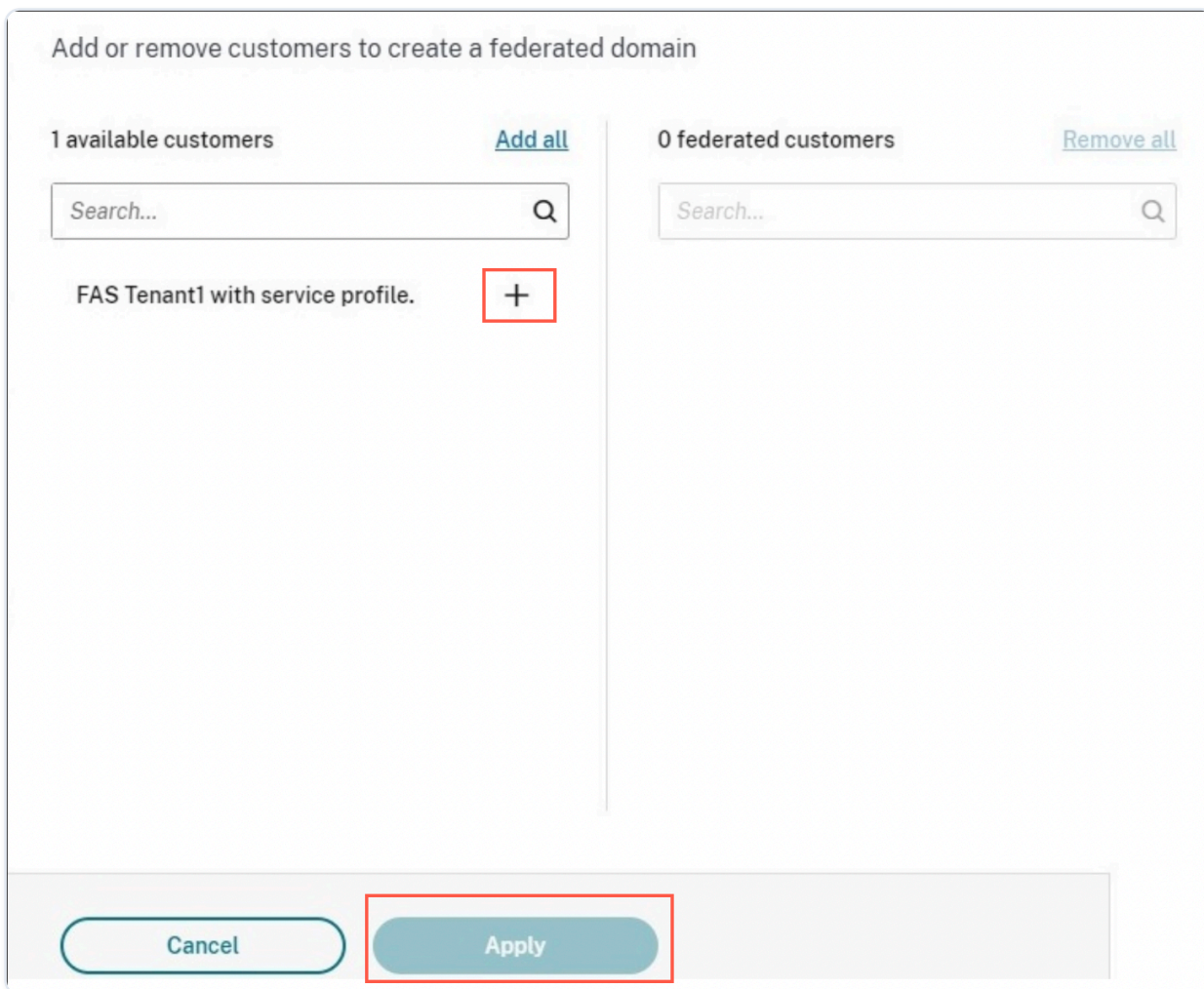


2. 将域联合到租户。

选择域，然后单击下拉菜单 (...)，并单击 **管理联合域**。

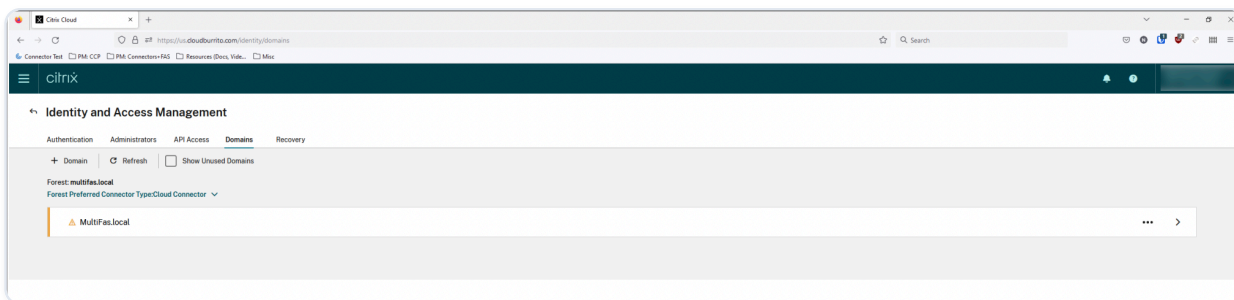


找到租户，然后单击 +。然后单击 **应用**。



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。



返回 MSP 客户。

4. 安装 FAS 服务器并将其注册到 Citrix Cloud。

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

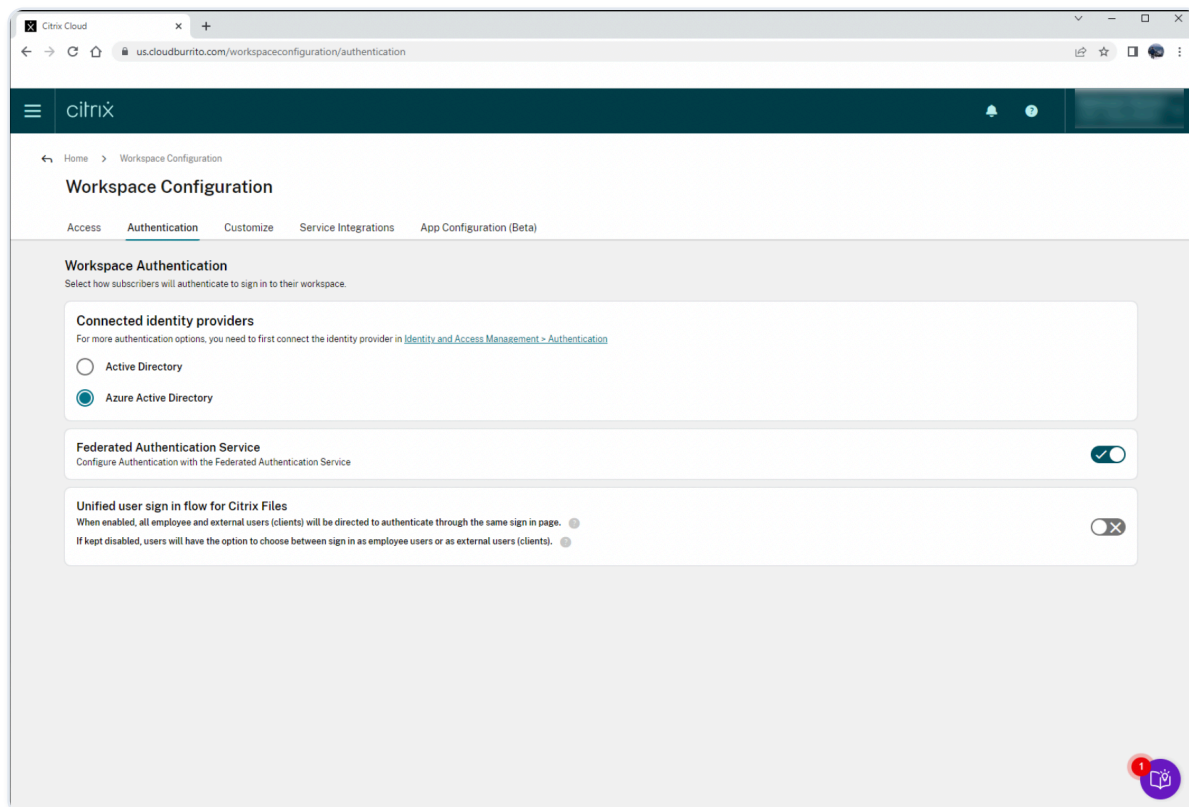
为租户客户启用 FAS

- 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。

- 为租户启用 FAS

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



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

注意：

自 2023 年 7 月起，Microsoft 已将 Azure Active Directory (Azure AD) 重命名为 Microsoft Entra ID。在本文档中，任何提及 Azure Active Directory、Azure AD 或 AAD 的地方均指 Microsoft Entra ID。

Citrix Federated Authentication Service (FAS) 为已加入域的 Virtual Delivery Agent (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，Microsoft Entra ID (ME-ID) 的实施会与您的 AD 和 Microsoft Entra ID 之间进行同步，从而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 Microsoft Entra ID SSO 所需的额外配置，这允许用户无需重新验证即可访问受 Microsoft Entra ID 保护的应用程序。

注意：

- 您无需为 FAS 使用 Microsoft Entra ID 的 SSO 进行任何特殊配置。
- 您不需要 FAS 会话内证书。
- 您可以使用任何版本的 FAS。
- 您可以使用支持 FAS 的任何版本 VDA。

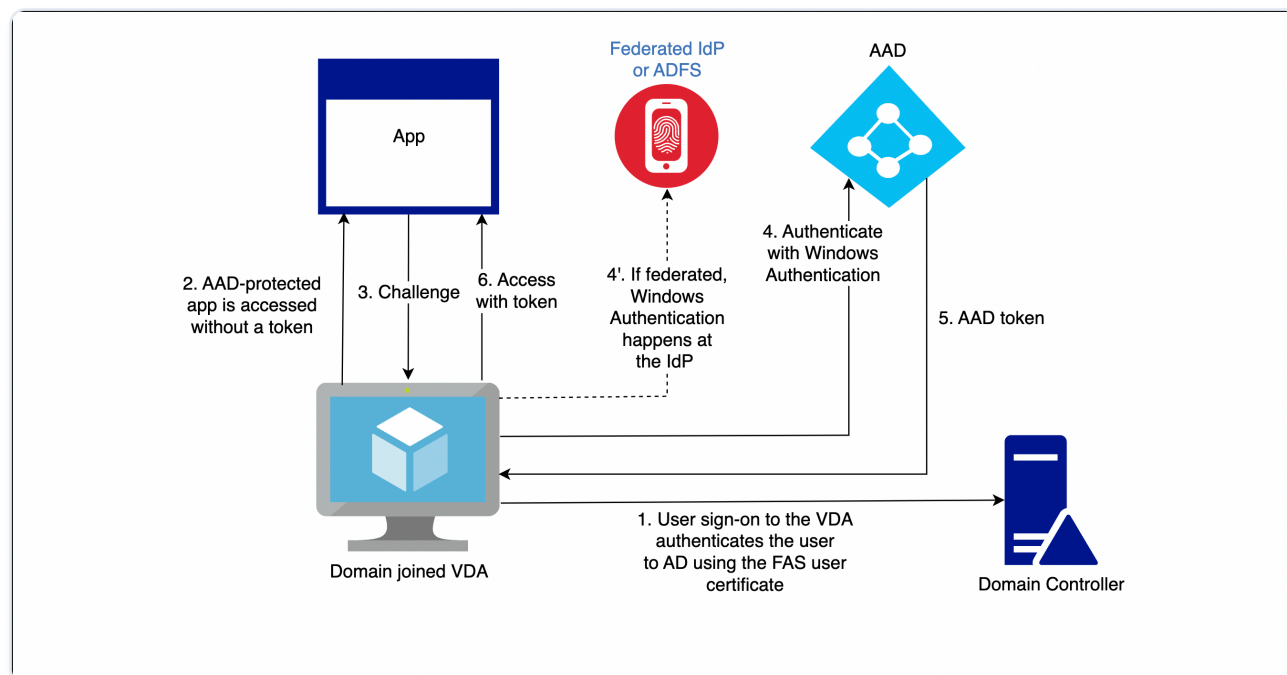
Microsoft Entra ID SSO 的技术总结在下表中：

ME-ID 身份验证类型	VDA 已加入域	VDA 已混合加入
托管	使用 ME-ID 无缝 SSO	使用 ME-ID 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 启用 Windows 身份验证	确保 WS-Trust <i>certificatemixed</i> 端点已启用
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

- 托管的 Microsoft Entra ID 域是指用户身份验证在 Microsoft Entra ID 中进行的域，有时也称为本机 Microsoft Entra ID 身份验证。
- 联合的 Microsoft Entra ID 域是指 Microsoft Entra ID 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 已加入 AD 和 Microsoft Entra ID。

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 Microsoft Entra ID 的 SSO。当用户从 VDA 会话中访问受 Microsoft Entra ID 保护的应用程序时，将进行对 Microsoft Entra ID 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 Microsoft Entra ID 域是托管的还是联合的而异。

有关托管 Microsoft Entra ID 域设置的信息，请参阅 [无缝单点登录](#)。

对于联合到 ADFS 的 Microsoft Entra ID 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程序的 Microsoft Entra ID 域，存在类似的解决方案。请联系您的身份提供程序寻求帮助。

注意：

您也可以将为已加入域的 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 Microsoft Entra ID 主刷新令牌 (PRT)。

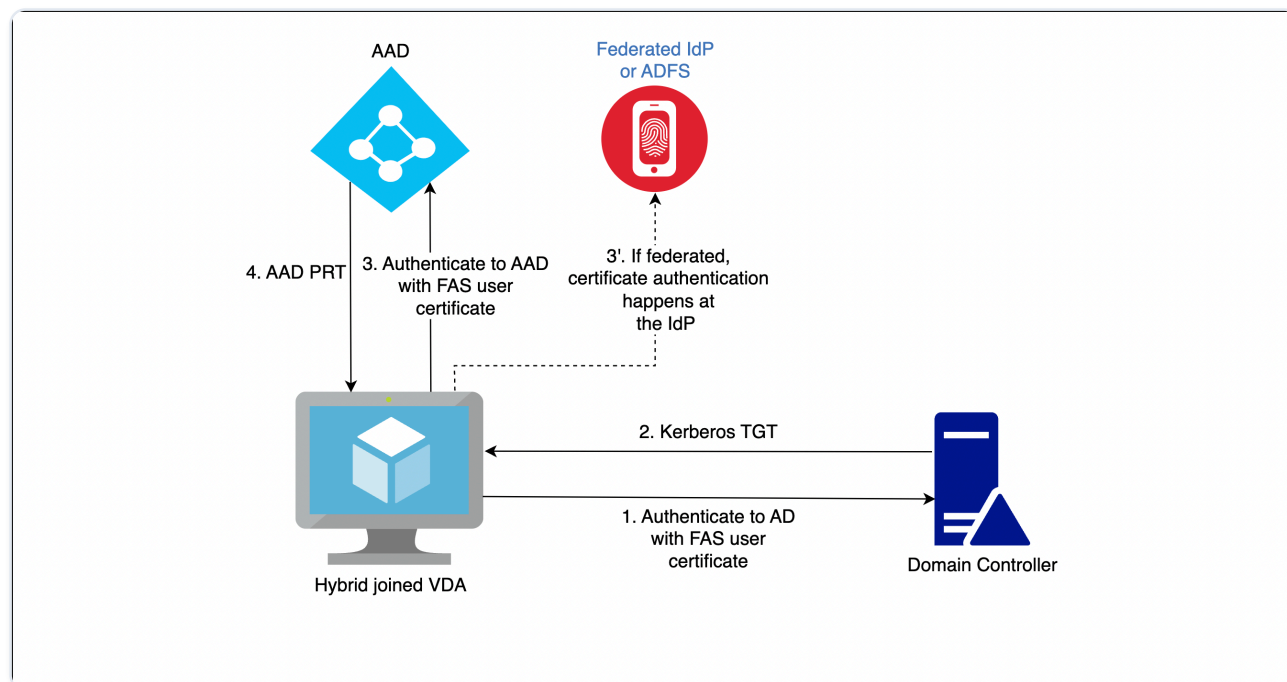
混合加入的 VDA

混合加入的 VDA 同时加入 AD 和 Microsoft Entra ID。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 Microsoft Entra ID 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 Microsoft Entra ID 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 Microsoft Entra ID 的基于证书的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 Microsoft Entra ID 域是托管的还是联合的而异。

对于托管的 Microsoft Entra ID 域，请配置 Microsoft Entra ID 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 Microsoft Entra ID CBA 通过用户的 FAS 证书向 Microsoft Entra ID 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 用户证书登录的情况。

对于联合到 ADFS 的 Microsoft Entra ID 域，VDA 使用 ADFS 服务器的 WS-Trust *certificatemixed* 端点，通过用户的 FAS 证书向 Microsoft Entra ID 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程序的 Microsoft Entra ID 域，可能存在类似的解决方案。身份提供程序必须实现 WS-Trust *certificatemixed* 端点。请联系您的身份提供程序寻求帮助。

证书颁发机构配置

本文介绍了联合身份验证服务 (FAS) 的高级配置，以便与证书颁发机构 (CA) 服务器集成。FAS 管理控制台不支持其中大多数配置。这些说明使用 FAS 提供的 PowerShell API。在执行本文中的任何说明之前，您必须具备 PowerShell 的基本知识。

设置多个 CA 服务器以用于 FAS

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

Name	Status
☒ ad-itu-net-itu-AD-CA	Template available
☒ ad-itu-net-itu-CA2-CA	Template available

☒ Only show CAs publishing Citrix_SmartcardLogon (recommended).

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）。

如果您要使用的某个 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。

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。

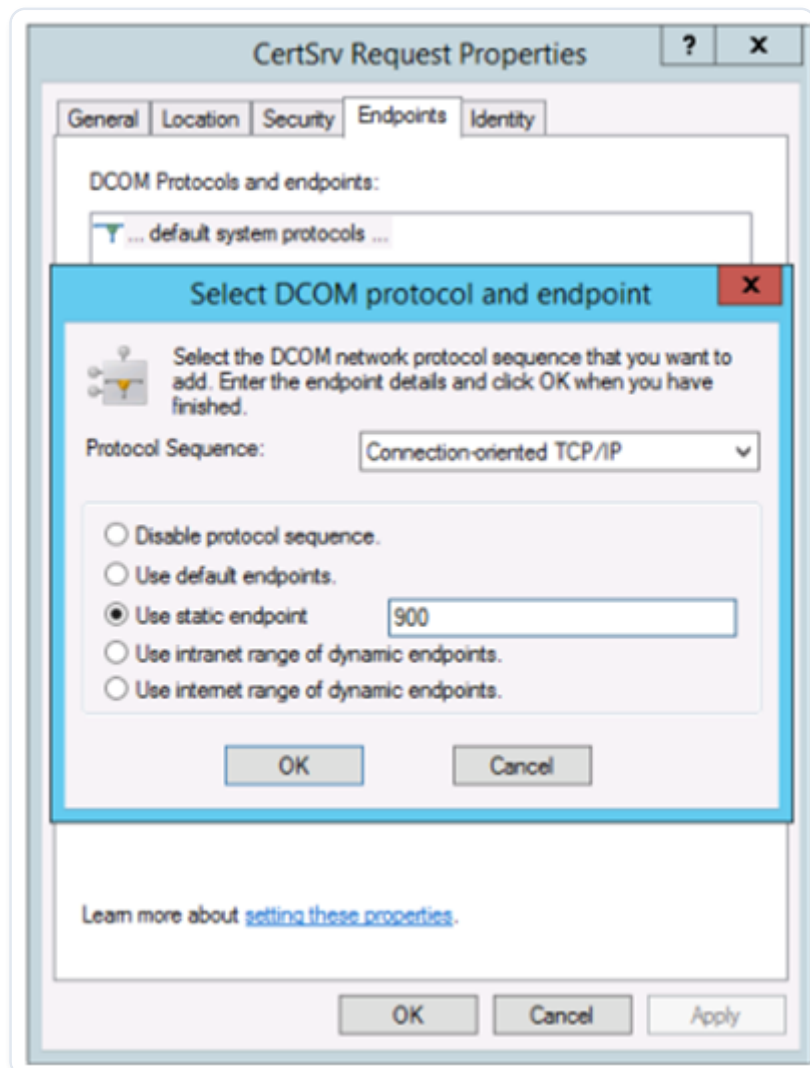
预期行为更改

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：



更改“**终结点**”以选择静态终结点并指定 TCP 端口号（在上一图中为 900）。

在此示例中，防火墙需要允许端口 135 和端口 900。

重新启动 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。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改善。以下部分描述了如何为单个或多个 FAS 服务器完成此操作。

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。

```
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 -NoTypeInfoInformation -Encoding utf8
-delimiter "," $filename

} else {

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

}
```

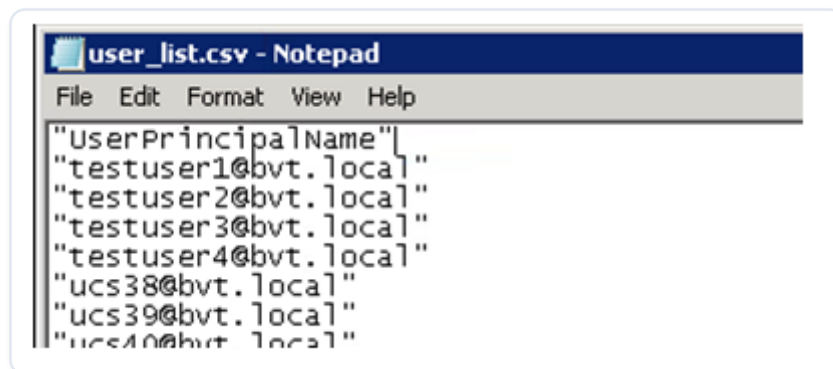
`Get-ADUser` 是一个用于查询用户列表的标准 cmdlet。前面的示例包含一个筛选器参数，用于仅列出具有 UserPrincipalName 且帐户状态为“enabled”的用户。

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，可以保留此项。

注意：

此查询可能会返回大量用户。

CSV 文件看起来像这样：



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 -UserPrincipalName
    $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

    }
}
```

```
}
```

如果您的 FAS 服务器不止一个，则特定用户的证书会生成两次：一次在主服务器中，另一次在故障转移服务器中。

此前的脚本适用于名为“default”的规则。如果您有不同的规则名称（例如，“hello”），请更改脚本中的 `$rule` 变量。

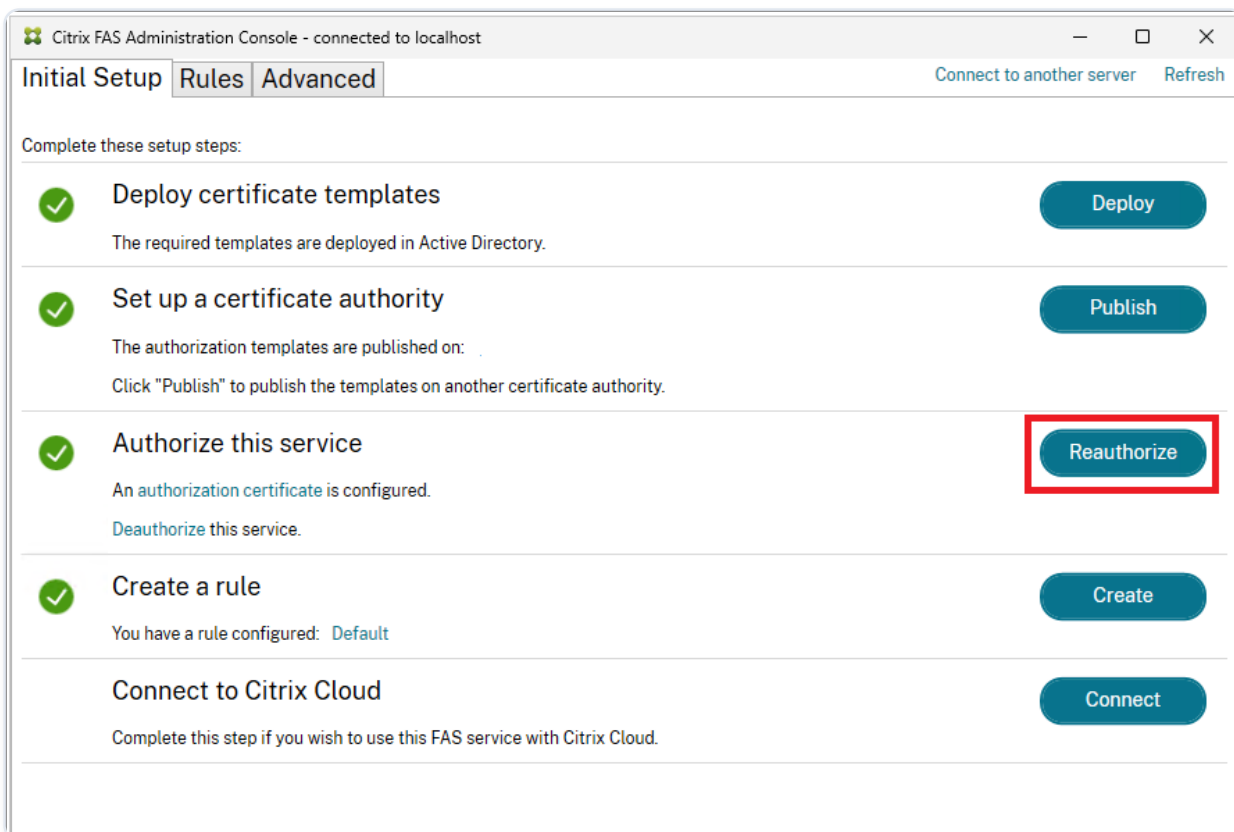


续订 FAS 授权证书

您可以在不中断 FAS 用户的情况下续订 FAS 授权证书。

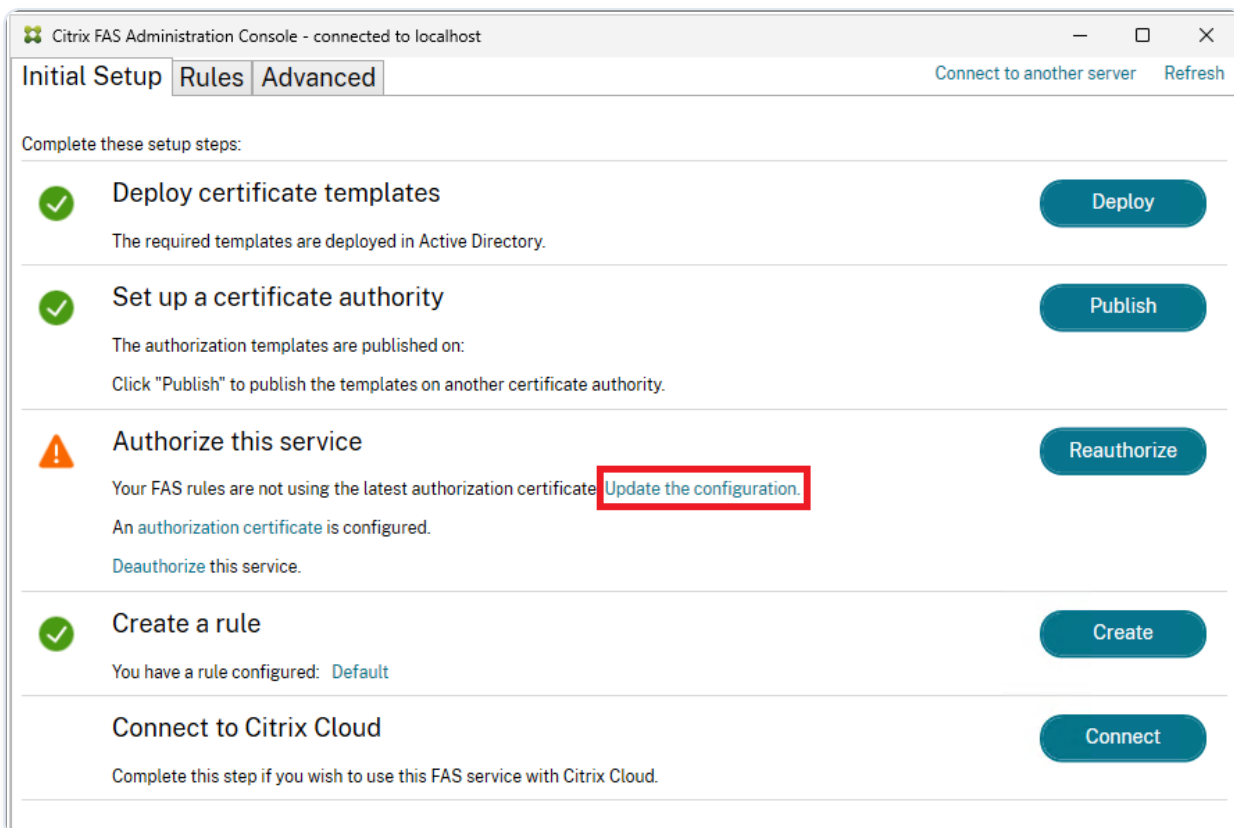
使用 FAS 管理控制台

- 单击 **重新授权** 以生成新的 FAS 授权证书请求：



您需要在 CA 手动批准该请求。有关详细信息，请参阅 [授权联合身份验证服务](#)。

- 生成新的授权证书后，FAS 会指示其尚未与您的规则关联。单击 **更新配置** 以将新的授权证书与您的规则关联。



使用 PowerShell

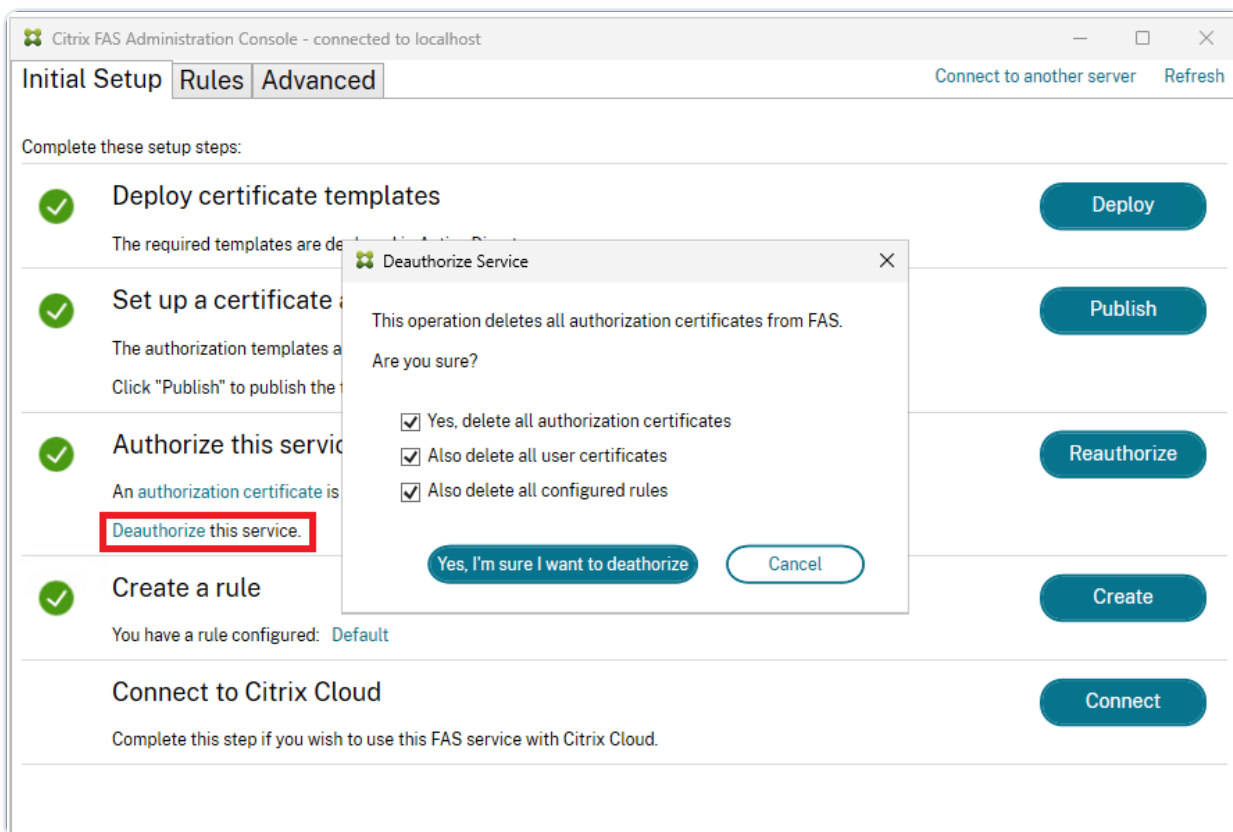
完成以下序列：

1. 创建授权证书：`New-FasAuthorizationCertificate`
2. 记下新授权证书的 GUID，如以下命令返回：`Get-FasAuthorizationCertificate`
3. 交换新的授权证书：`Set-FasCertificateDefinition -AuthorizationCertificate <GUID>`
4. 删除旧的授权证书：`Remove-FasAuthorizationCertificate`。请务必使用 `DeleteUserCerts $false` option，以免中断用户活动。

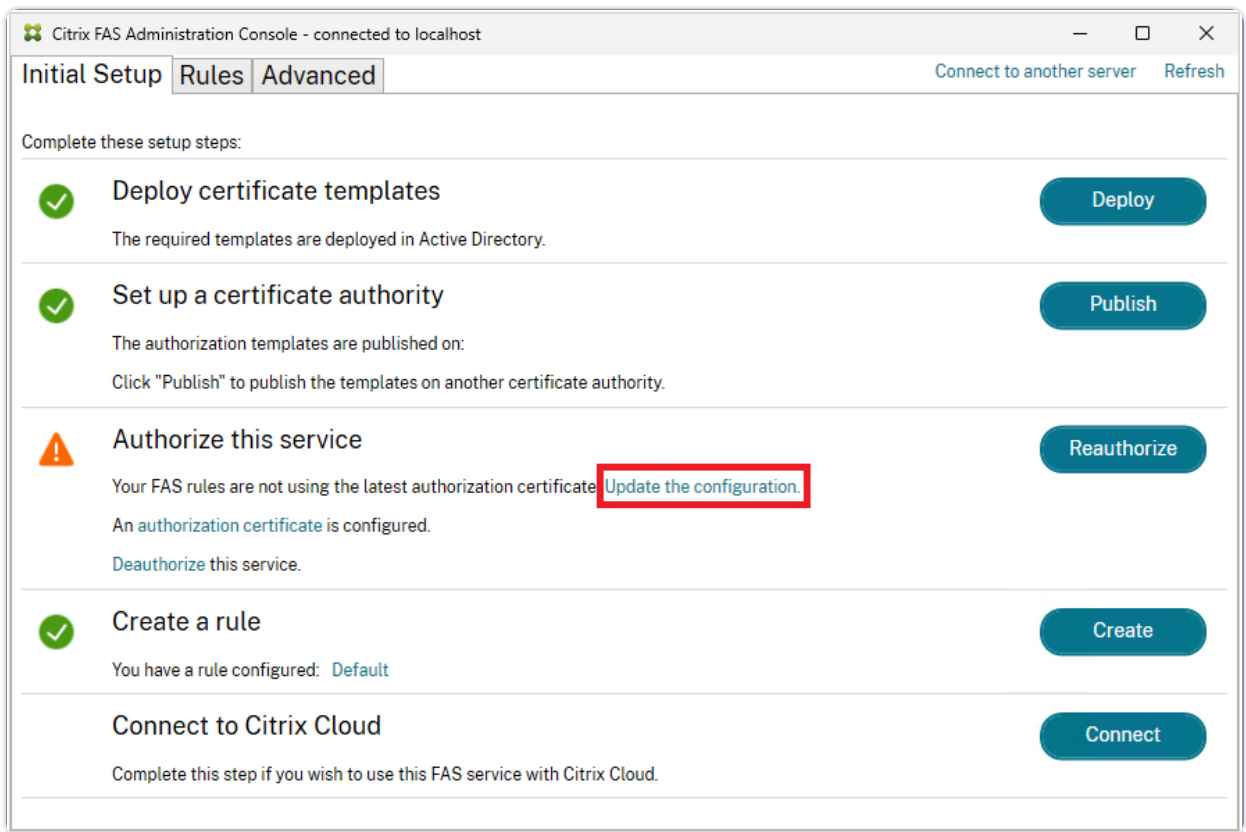
取消 FAS 授权并删除 FAS 证书

使用 FAS 管理控制台

- 单击**取消授权**链接并删除授权证书。您可以删除所有用户证书和所有规则（尽管清除证书并非必需）。



- 如果您不删除规则，当您以后授权 FAS 时，您会收到警告：



该警告表明授权证书尚未与您的规则关联。单击**更新配置**以将新的授权证书与您的规则关联。

使用 PowerShell

使用以下 PowerShell 命令删除授权证书和用户证书：

```
$AuthCert = Get-FasAuthorizationCertificate -Address localhost  
  
Remove-FasAuthorizationCertificate -Address localhost -Id $AuthCert.Id
```

注意：

`Get-FasAuthorizationCertificate` 返回授权证书和待处理授权证书请求的列表，供您检查 `$AuthCert` 的值，然后继续执行 `Remove-FasAuthorizationCertificate`。

您可以删除授权证书，但保留用户证书，方法是将 `DeleteUserCerts` 参数设置为 `false`：

```
Remove-FasAuthorizationCertificate -Address localhost -Id $AuthCert.Id  
-DeleteUserCerts $false
```

剩余的用户证书仍可由 FAS 用于 VDA 登录和会话内证书，这在续订 FAS 授权时很有用。有关更多详细信息，请参阅[续订 FAS 授权证书](#)。

- 您可以按如下方式删除用户证书：

```
Remove-FasUserCertificate -Address localhost
```

此命令从 FAS 服务器中删除所有用户证书。该命令具有用于筛选要删除的证书集的选项。

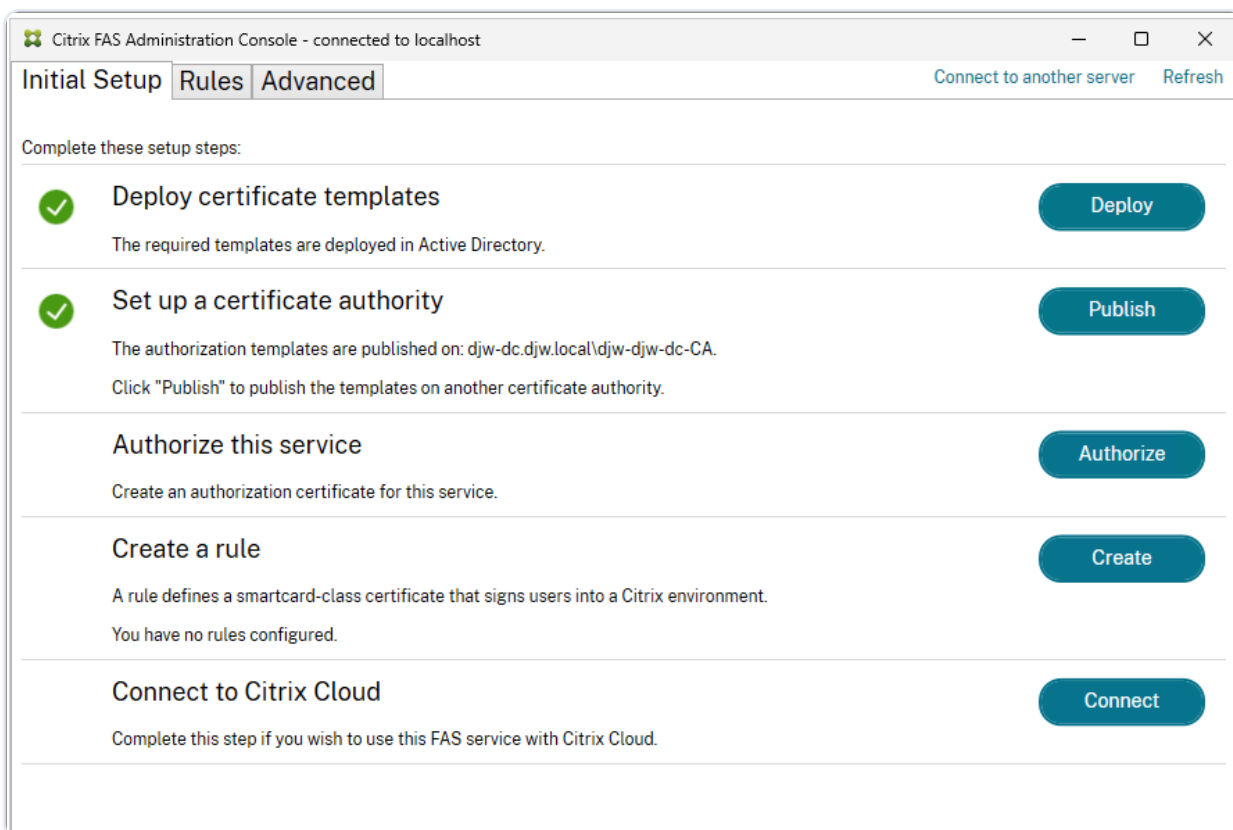
注意：

当 FAS 从其内部存储中移除授权或用户证书时，它还会删除关联的密钥对。

脱机授权

可以使用 PowerShell 脱机请求 FAS 授权证书。这适用于不希望其证书颁发机构通过联机证书签名请求颁发授权证书的组织。

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**。



2. 在 FAS 服务器上加载以下 PowerShell cmdlet：

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

3. 通过在 FAS 服务器上输入以下 PowerShell cmdlet 来生成密钥对并创建证书签名请求：

```
$AuthCertRequest = New-FasAuthorizationCertificateRequest -Address  
localhost $AuthCertRequest
```

结果如下：

```
PS C:\> $AuthCertRequest = New-FasAuthorizationCertificateRequest -Address localhost  
PS C:\> $AuthCertRequest  
  
Id           : a0da658f-a7e4-49b7-a0c3-6381c26a83a5  
Address      : [Offline CSR]  
TrustArea    :  
CertificateRequest : -----BEGIN CERTIFICATE REQUEST-----  
               [REDACTED]  
               -----END CERTIFICATE REQUEST-----  
Status       : WaitingForApproval
```

注意：

生成的密钥对的属性由 FAS 授权密钥配置决定。有关详细信息，请参阅[私钥保护](#)。

4. 将证书请求复制到磁盘：

```
`$AuthCertRequest.CertificateRequest > c:\temp\authcert.csr
```

5. 将证书请求文件（在此示例中为 authcert.csr）提交给您的证书颁发机构，批准请求，并获取证书响应。

以下五个步骤专门针对使用 Microsoft 企业证书颁发机构；对于其他 CA，请联系您的 CA 供应商寻求帮助。

- 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*，有效期为两年：

Properties of New Template

Subject Name	Server	Issuance Requirements
Superseded Templates		Extensions
Security		
Compatibility	General	Request Handling
	Cryptography	Key Attestation

Template display name:
Offline_RA

Template name:
Offline_RA

Validity period: 2 years
Renewal period: 0 days

☐ Publish certificate in Active Directory
☐ Do not automatically reenroll if a duplicate certificate exists in Active Directory

OK Cancel Apply Help

- 在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**。选择您创建的模板。
- 通过在 FAS 服务器上的 PowerShell 命令提示符中键入以下内容，将证书签名请求提交到您的证书颁发机构：

```
certreq -submit -attrib "certificatetemplate:<certificate template  
from step 5a>" <certificate request file from step 4>
```

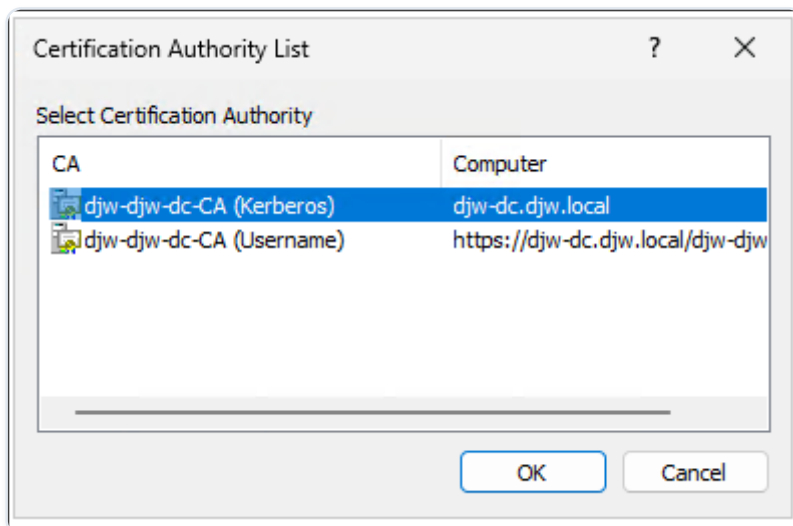
例如：

```
certreq -submit -attrib "certificatetemplate:Offline_RA" C:  
\temp\authcert.csr
```

运行上述命令结果如下：

```
PS C:\> certreq -submit -attrib "certificatetemplate:Offline_RA" C:\temp\authcert.csr
Active Directory Enrollment Policy
{3C06E1D3-4E2D-4B8B-94FA-C254192D09C6}
ldap:
```

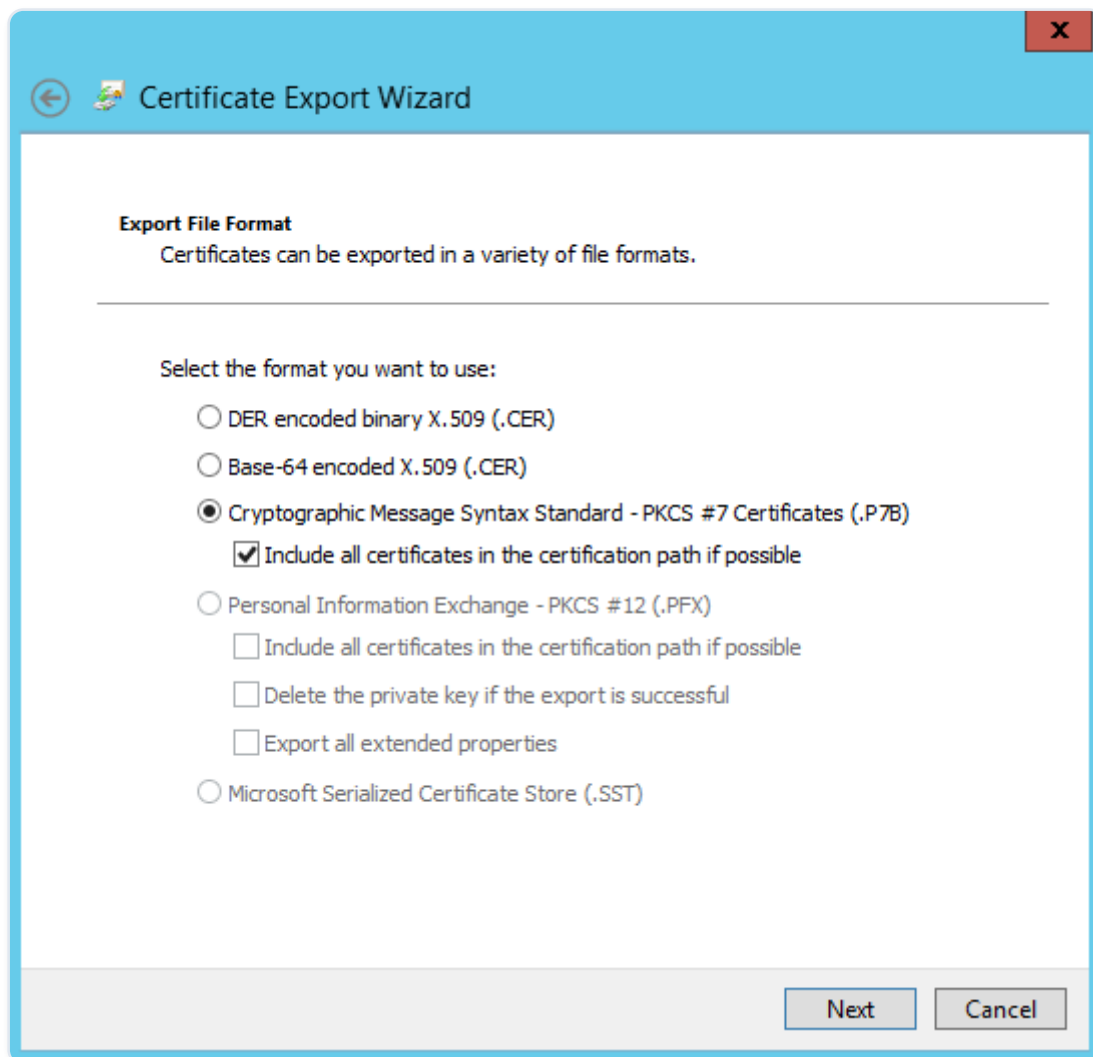
此时可能会出现一个**证书颁发机构列表**窗口。此示例中的证书颁发机构已启用 DCOM（顶部）和 HTTP（底部）注册。如果可用，请选择 **DCOM**，然后单击**确定**：



指定证书颁发机构后，命令完成并显示 RequestID：

```
PS C:\> certreq -submit -attrib "certificatetemplate:Offline_RA" C:\temp\authcert.csr
Active Directory Enrollment Policy
{3C06E1D3-4E2D-4B8B-94FA-C254192D09C6}
ldap:
RequestId: 358
RequestId: "358"
Certificate request is pending: Taken Under Submission (0)
PS C:\> |
```

- 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**。查找请求 ID。然后右键单击该请求并选择**颁发**。
- 选择**已颁发的证书**节点。查找已颁发的证书（请求 ID 必须匹配）。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：



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

6. 将导出的证书文件复制到 FAS 服务器。
7. 通过在 FAS 服务器上输入以下 PowerShell cmdlet，将注册机构证书导入 FAS 服务器：

```
Import-FasAuthorizationCertificateResponse -Address localhost -Id  
$AuthCertRequest.Id -Pkcs7CertificateFile <Certificate file from step  
6>
```

例如：

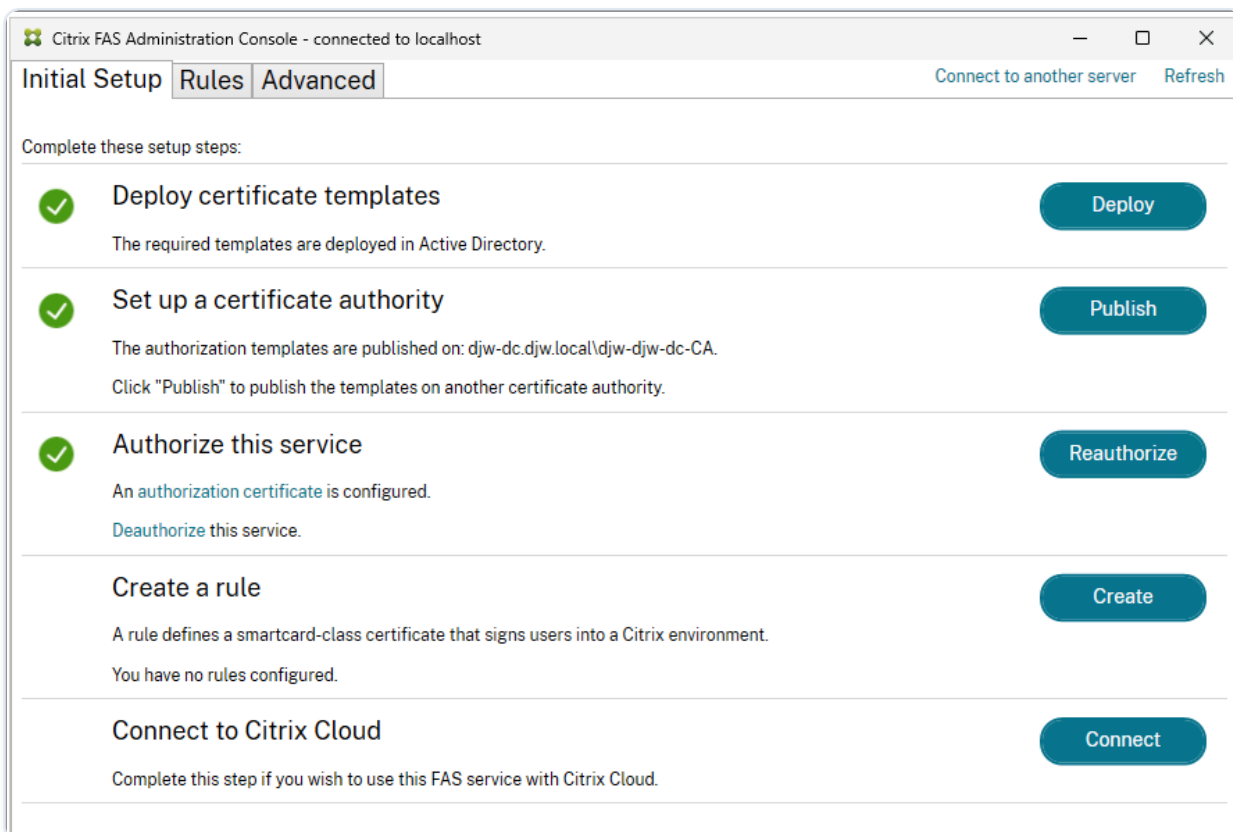
```
Import-FasAuthorizationCertificateResponse -Address localhost -Id  
$AuthCertRequest.Id -Pkcs7CertificateFile C:\temp\response.p7b
```

运行此命令将得到：

```
PS C:\> Import-FasAuthorizationCertificateResponse -Address localhost -Id $AuthCertRequest.Id -Pkcs7CertificateFile C:\temp\response.p7b

Id           : a0da658f-a7e4-49b7-a0c3-6381c26a83a5
Address      : [Offline CSR]
TrustArea    : 7abab16b-e5ac-424f-90d5-ec1aebc13d07
CertificateRequest : 
Status       : Ok
```

8. 检查 FAS 管理控制台。它必须显示 FAS 现已获得授权。



注意：

“授权此服务”步骤旁边有一个绿色复选标记。

9. 通过创建规则继续配置。有关详细信息，请参阅[配置规则](#)。

相关信息

- [安装和配置](#)文章是 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在[部署体系结构](#)文章中进行了总结。
- 其他[操作方法](#)文章在[高级配置](#)文章中介绍。

私钥保护

简介

FAS 证书存储在 FAS 服务器上的嵌入式数据库中。与 FAS 证书关联的私钥存储在 FAS 服务器的网络服务帐户下。默认情况下，这些密钥是不可导出的 2048 位 RSA 密钥，在 Microsoft 软件密钥存储提供程序中创建和存储。

使用 FAS PowerShell 命令 `PowerShell cmdlet`，可以更改私钥的属性和存储位置。

注意：

FAS 配置和证书本地存储在 FAS 服务器上。数据不在 FAS 服务器之间共享。

在 Citrix Virtual Apps and Desktops 2411 之前的 FAS 版本中，私钥属性通过编辑

```
%programfiles%\Citrix\Federated Authentication
```

`Service\Citrix.Authentication.FederatedAuthenticationService.exe.config` 处的

XML 文件进行配置。这已被 PowerShell 命令取代，PowerShell 命令提供了更大的灵活性，并且无需重新启动 FAS 服务器即可应用。此外，与 XML 文件设置不同，使用 PowerShell 进行的配置在 FAS 服务器升级时会保留。因此，不再支持使用 XML 文件进行以下设置的配置：

- `Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.KeyProtection`
- `Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderLegacyCsp`
- `Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderName`
- `Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderType`
- `Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.KeyLength`

请参阅以下部分：[从 Citrix Virtual Apps and Desktops™ 2411 之前的 FAS 版本升级](#)。

关于 FAS 证书和模板的信息

FAS 持有两种类型的证书：授权证书（通常只有一个实例）和用户证书。

注意：

FAS 授权证书有时也称为**注册机构或请求代理 (RA)** 证书。

FAS 在请求证书时使用证书模板，如下一节所述。虽然 FAS 在证书请求中指定了模板名称，但它不读取模板内容。因此，更改模板设置不会影响 FAS 发出的证书请求。更改模板的某些属性会影响 CA 生成的证书。例如，您可以使用模板更改有效期。

FAS 授权证书

此证书在您配置 FAS 时创建。您可以使用 FAS 管理控制台的**授权**或**重新授权**按钮来请求新的授权证书。

也可以使用 PowerShell 命令，这提供了更大的灵活性：

- `New-FasAuthorizationCertificate`：此命令的行为类似于 FAS 管理控制台，不同之处在于可以指定在授权过程中使用的证书模板。
- `New-FasAuthorizationCertificateRequest`：此命令为授权证书创建**脱机**请求；**脱机授权**。

授权证书有时也称为 RA 证书，因为 FAS 充当注册机构，代表用户请求证书。该证书具有增强的密钥用法**证书请求代理**，允许其在请求 FAS 用户证书时用作授权凭据。

默认情况下，授权过程使用以下模板：

- `Citrix_RegistrationAuthority_ManualAuthorization`：使用此模板创建的证书是临时且短期有效的，用于**引导**授权过程；
- `Citrix_RegistrationAuthority`：使用此模板创建的证书具有较长的有效期，并由 FAS 服务器存储。

授权 FAS 会产生以下步骤：

1. FAS 创建密钥对，并向 CA 发送**证书签名请求 (CSR)**，指定密钥对的公钥和模板 `Citrix_RegistrationAuthority_ManualAuthorization`。
2. 模板的颁发要求规定 CSR 必须由 CA 管理员手动批准。
3. 一旦 CA 管理员批准了 CSR，CA 就会创建一个证书，FAS 会检索该证书。此证书有效期为一天，仅用于以下步骤。使用后，FAS 会销毁该证书及其密钥对。
4. FAS 创建另一个密钥对，并向 CA 发送第二个 CSR，指定此密钥对的公钥和模板 `Citrix_RegistrationAuthority`。该请求由上一步中的证书授权并签名。
5. CA 自动颁发证书，FAS 检索证书，FAS 现在已**获得授权**。默认情况下，此授权证书的有效期为两年。

可以使用此 PowerShell 命令查看用于创建前面提到的密钥对的设置：

```
Get-FasKeyConfig -Address localhost -CertificateType ra
```

FAS 用户证书

FAS 创建用户证书以将用户登录到 VDA。

当 FAS 创建用户证书时，会发生以下步骤：

- FAS 创建一个密钥对，并向 CA 发送一个 CSR，指定密钥对的公钥、用户身份，以及默认情况下，模板 `Citrix_SmartcardLogon`（使用的模板是可配置的）。
- CSR 使用 FAS 授权证书签名。
- `Citrix_SmartcardLogon` 模板具有颁发要求 `Application Policy: Certificate Request Agent`。由于此属性存在于 FAS 授权证书中，CA 会自动颁发用户证书。
- FAS 检索证书，并将其存储在 FAS 服务器上的嵌入式数据库中。
- 默认情况下，证书的有效期为一周。

稍后，用户证书将提供给 VDA 以登录用户。

可以使用以下 PowerShell 命令查看用于创建前面提到的密钥对的设置：

```
Get-FasKeyConfig -Address localhost -CertificateType user
```

私钥存储选项

FAS 可以配置为在以下三类存储中创建和存储密钥对：

- **软件**：通常使用 **Microsoft 软件密钥存储提供程序**，该提供程序仅通过软件保护；数据存储在磁盘上。
- **受信任的平台模块 (TPM)**：TPM 可以是计算机上的物理硬件，也可以是虚拟机管理程序提供的虚拟 TPM。
- **硬件安全模块 (HSM)**：这是一种硬件外设或网络设备，旨在安全存储加密密钥。

注意：

需要权衡利弊。硬件存储可能更安全，但性能通常较低，尤其是在创建和存储大量用户证书密钥对时。

与 FAS 授权证书关联的私钥特别敏感，因为该证书的策略允许拥有私钥的任何人授权任何用户的证书请求。因此，控制此密钥的任何人都可以作为任何用户连接到环境。

注意：

Microsoft CA 可以配置为限制 FAS 授权证书的权限，包括可以为其颁发证书的用户集。请参阅 [委派注册代理](#)。

因此，FAS 允许您独立配置授权证书和用户证书的私钥属性。

一些典型配置如下：

授权证书密钥	用户证书密钥	注释
软件	软件	默认配置
TPM	软件	授权证书具有硬件保护
HSM	HSM	所有证书都具有硬件保护

注意：

不建议将硬件 TPM 用于用户密钥。仅将 TPM 用于授权证书密钥。如果您计划在虚拟化环境中运行 FAS 服务器，请咨询您的虚拟机管理程序供应商是否支持 TPM 虚拟化。

密钥配置 PowerShell 命令

与私钥配置相关的命令如下：

- `Get-FasKeyConfig`
- `Set-FasKeyConfig`
- `Reset-FasKeyConfig`
- `Test-FasKeyConfig`

有关详细信息，请参阅 [PowerShell cmdlet](#)。

授权和用户证书的密钥配置是独立的，由 `CertificateType` 参数指定。例如，要获取请求授权证书（RA 证书）时使用的私钥配置：

```
Get-FasKeyConfig -Address localhost -CertificateType ra
```

要获取请求用户证书时使用的私钥配置：

```
Get-FasKeyConfig -Address localhost -CertificateType user
```

您可以使用 **Set-FasKeyConfig** 和 **Get-FasKeyConfig** 来设置和检查以下私钥属性：

属性	默认值	注释
长度	2048	以位为单位的密钥长度。请注意，在 Microsoft 模板 GUI 中，Cryptograhy 选项卡指定了*最小*密钥大小。如果 FAS 中配置的密钥长度小于模板中指定的最小密钥大小，则 CA 将拒绝 CSR。 对于 RSA 密钥，长度可以是 1024 位、2048 位或 4096 位。 对于 ECC 密钥，长度可以是 256 位、384 位或 521 位。
可导出	否	私钥是否可以从其提供程序导出。
前缀	无	指定要添加到 FAS 生成的私钥标识符的前缀。生成的标识符由前缀和 GUID 组成。 例如， <code>MyPrefix70277985-6908-4C6F-BE59-B08691456804</code>。
椭圆曲线	否	如果为 true，则生成 ECC 密钥对；否则，生成 RSA 密钥对。
密钥存储提供程序 (KSP)	真	如果为 true，FAS 使用现代 Windows CNG API，并且必须

属性	默认值	注释
		在 Provider 属性中指定 KSP。 如果为 false，FAS 使用旧版 CAPI API，并且必须在 Provider 属性中指定加密服务提供程序 (CSP)。Citrix 建议使用 KSP。
提供程序	Microsoft 软件密钥存储提供程序	创建和存储密钥对的提供程序名称。您可以更改此属性以指定 TPM 或 HSM。HSM 的 KSP（或 CSP）由 HSM 供应商提供。他们提供有关如何安装其软件以及提供程序名称的说明。
CSP类型	24	仅当 KSP 属性设置为 false 时才相关。 指的是 <code>Microsoft KeyContainerPermissionAccessEntry.ProviderType Property</code> <code>PROV_RSA_AES 24</code> 。必须始终为 24，除非您使用的是带 CSP 的 HSM，并且 HSM 供应商另有规定。

此外，**Set-FasKeyConfig** 可与以下开关一起使用，以方便操作：

标志	说明
-UseDefaultSoftwareProvider	将 Provider 属性设置为 Microsoft Software Key Storage Provider ，并将 KSP 字段设置为 true 。
-UseDefaultTpmProvider	将 Provider 属性设置为 Microsoft Platform Crypto Provider ，并将 KSP 字段设置为 true 。

Microsoft Software Key Storage Provider 是通常用于在磁盘上创建和存储密钥的提供程序。

Microsoft Platform Crypto Provider 是通常用于在 TPM 中创建和存储密钥的提供程序。

Get-FasKeyConfig 还提供字段，有助于确认正在使用哪个提供程序和算法：

字段	含义
IsDefaultSoftwareProvider	如果为 true ，则表示提供程序设置为 Microsoft Software Key Storage Provider ，并且 KSP 字段设置为 true 。
IsDefaultTpmProvider	如果为 true ，表示提供程序设置为 Microsoft Platform Crypto Provider 且 KSP 字段设置为 true 。
算法	RSA 表示将创建 RSA 密钥（ EllipticCurve 属性为 false ）。 ECC 表示将创建 ECC 密钥（ EllipticCurve 属性为 true ）。

您可以使用 `Reset-FasKeyConfig` 将设置恢复为默认值。

```
Reset-FasKeyConfig -Address localhost -CertificateType ra  
  
Reset-FasKeyConfig -Address localhost -CertificateType user
```

注意：

对私钥配置所做的更改（使用 `Set-FasKeyConfig` 或 `Reset-FasKeyConfig`）会立即应用于新创建的证书。但是，具有不同配置的现有授权和用户证书不受影响。

您可以通过从管理控制台取消授权 FAS 服务，或通过使用 [取消授权 FAS 并删除 FAS 证书](#) 中的 PowerShell 命令来删除现有证书。

密钥池中任何不符合当前用户密钥配置的预生成密钥都将被丢弃。

配置方案示例

在每个示例中，请在授权 FAS 服务之前使用提供的 PowerShell 设置密钥配置，因为现有证书不受任何配置更改的影响。

如果您已有密钥配置错误的授权或用户证书，可以通过 [检查 FAS 证书](#) 和 [取消授权 FAS 并删除 FAS 证书](#) 将其删除。

如果您的 FAS 服务器处于实时部署中，请考虑在进行配置更改时将其置于维护模式 [维护模式](#)。

示例 1 - 将所有密钥存储在 Microsoft 软件密钥存储提供程序中

由于这是默认设置，因此无需额外配置。

如果您之前更改了密钥配置，可以使用以下命令恢复为使用 **Microsoft Software Key Storage Provider**：

```
Set-FasKeyConfig -Address localhost -CertificateType ra  
-UseDefaultSoftwareProvider  
  
Set-FasKeyConfig -Address localhost -CertificateType user  
-UseDefaultSoftwareProvider
```

您可以使用 `Reset-FasKeyConfig` 恢复为 **Microsoft Software Key Storage Provider**，并额外将所有其他密钥配置设置恢复为默认值。

示例 2 - 将授权证书密钥存储在 TPM 中

此示例说明了将 FAS 授权证书密钥存储在 TPM（物理或虚拟）中，而用户证书密钥存储在 **Microsoft Software Key Storage Provider** 中。

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 硬件可能过慢或受限于大小。

使用以下 PowerShell 命令：

```
Set-FasKeyConfig -Address localhost -CertificateType ra  
-UseDefaultTpmProvider  
  
Set-FasKeyConfig -Address localhost -CertificateType user  
-UseDefaultSoftwareProvider
```

示例 3 - 将所有密钥存储在 HSM 中

此示例说明了使用 HSM 存储授权证书和用户证书私钥。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 Key Storage Provider**。

使用以下 PowerShell 命令（将示例文本替换为您的 HSM 提供程序的名称）：

```
Set-FasKeyConfig -Address localhost -CertificateType ra -Provider "HSM  
Vendor Key Storage Provider"  
  
Set-FasKeyConfig -Address localhost -CertificateType user -Provider "HSM  
Vendor Key Storage Provider"
```

示例 4 - 使用椭圆曲线密钥

默认情况下，FAS 生成 RSA 密钥。在此示例中，为授权证书和用户证书配置了椭圆曲线 (ECC) 密钥。

此示例使用不同的密钥长度。授权证书配置为 384 位密钥，用户证书配置为 256 位密钥。

```
Set-FasKeyConfig -Address localhost -CertificateType ra -EllipticCurve  
$true -Length 384  
  
Set-FasKeyConfig -Address localhost -CertificateType user -EllipticCurve  
$true -Length 256
```

此时，授权和用户证书请求可能会被 CA 拒绝，因为 FAS 证书模板中的最小密钥大小默认设置为 1024 位。

因此，对于此示例，需要按如下方式更改模板中的最小密钥大小：

- **Citrix_RegistrationAuthority_ManualAuthorization and Citrix_RegistrationAuthority**：将最小密钥大小更改为 384（或更小）

- `Citrix_SmartcardLogon`：将最小密钥大小更改为 256（或更小）

要编辑模板，请运行 `mmc.exe`，然后添加“证书模板”管理单元。找到模板，然后打开其属性。最小密钥大小设置位于模板属性的“加密”选项卡中。

注意：

带有 ECC 密钥的用户证书仅在运行 Citrix Virtual Apps and Desktops 2411 或更高版本的 Windows VDA 上受支持。Linux VDA 不支持 ECC 密钥。

测试私钥配置

尽管 `Set-FasKeyConfig` 命令会执行一些验证，但仍可能设置无效的密钥配置。例如，您可能在 HSM 的提供程序名称中犯了错误，或者您指定的密钥长度可能不受硬件支持。

命令 `Test-FasKeyConfig` 可以提供帮助。它尝试使用当前密钥配置创建密钥对，并报告成功或失败。如果发生故障，将提供故障原因的指示。如果成功，密钥对将立即销毁。

以下 PowerShell 命令分别测试授权和用户密钥配置：

```
Test-FasKeyConfig -Address localhost -CertificateType ra  
  
Test-FasKeyConfig -Address localhost -CertificateType user
```

授权 FAS 服务器并创建规则后，您还可以按如下方式为用户证书创建测试 CSR：

```
Test-FasCertificateSigningRequest -Address localhost -UserPrincipalName  
user@example.com -Rule default
```

将 `<mailto:user@example.com/>` 替换为 Active Directory 部署中的真实 UPN。FAS 规则通常命名为 **default**。但是，如果您希望测试已配置的其他规则，请指定该名称。

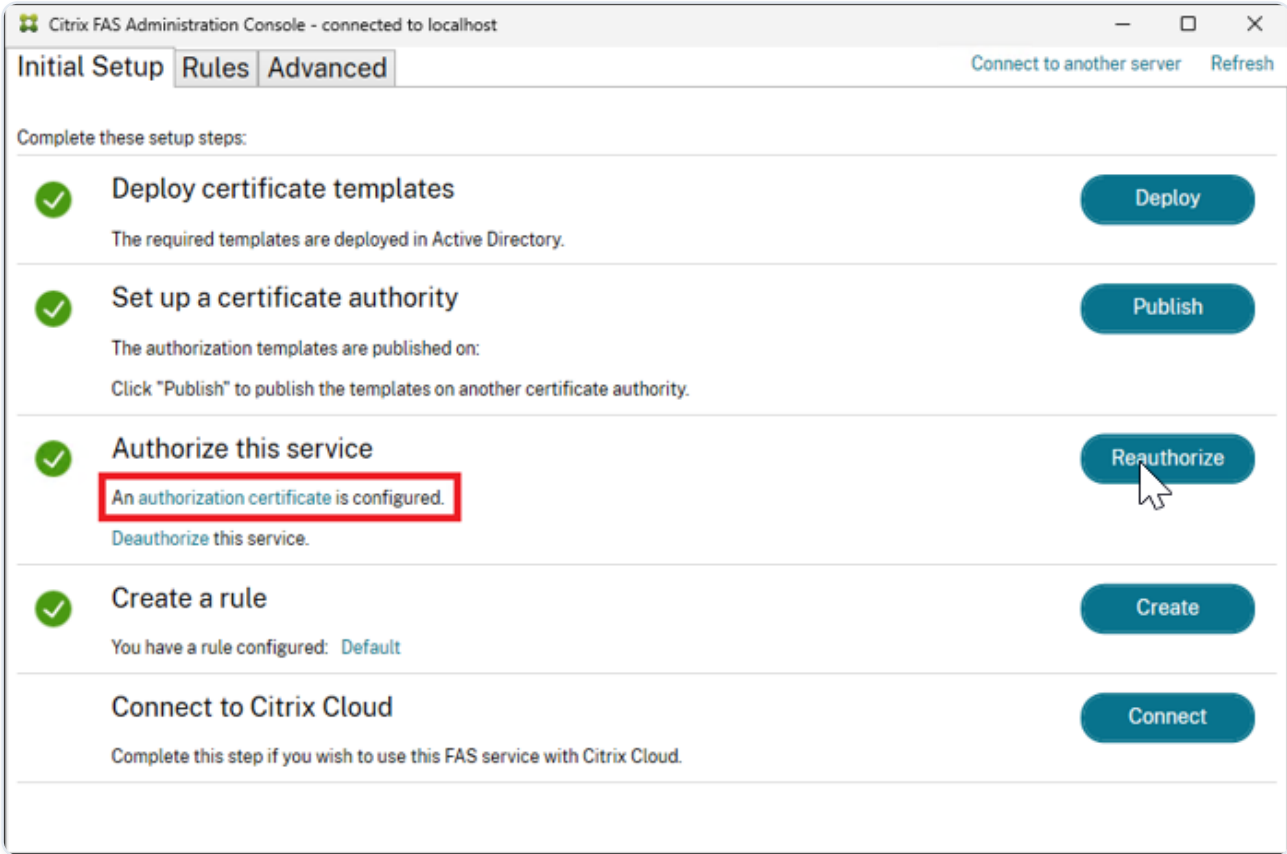
如果 CSR 成功，FAS 将丢弃生成的证书。

检查 FAS 证书

您可以使用 PowerShell 检查证书的属性并确定关联的私钥存储位置。

检查授权证书

您可以通过单击 FAS 管理控制台中的**授权证书**链接来查看授权证书：



但是，要获取更详细的信息，请使用 PowerShell：

```
Get-FasAuthorizationCertificate -Address localhost -FullCertInfo
```

将返回多个字段，其中包括 **PrivateKeyProvider**，它指示了创建和存储证书的提供程序。

PRIVATEKEYPROVIDER	密钥存储位置
微软软件密钥存储提供程序	密钥存储在磁盘上，受 Microsoft 软件提供程序保护。
微软平台加密提供程序	密钥存储在 TPM 中（物理或虚拟）。
HSM 供应商密钥存储提供程序（仅限示例）	密钥存储在 HSM 中（在此示例中，供应商的提供程序名为 HSM Vendor Key Storage Provider ）

检查用户证书

您可以按如下方式获取 FAS 服务器上缓存的所有用户证书列表：

```
Get-FasUserCertificate -Address localhost -KeyInfo $true
```

KeyInfo 参数使输出包含有关与证书关联的私钥的更多信息。特别是，**PrivateKeyProvider** 字段指示与证书关联的密钥对的存储位置（有关此值的解释，请参阅上一节）。

您可以使用各种可选参数（例如 `-UserPrincipalName`）筛选返回的证书集。

命令输出的证书字段是 PEM 编码的用户证书。将文本复制到 `.cert` 文件中，然后按如下方式使用 Windows 证书 GUI 显示证书：

命令	说明
<code>\$CertInfos = Get-FasUserCertificate -Address localhost</code>	此列表中可能包含多个用户证书
<code>\$CertInfo = \$CertInfos[0]</code>	在此示例中，我们选择第一个用户证书
<code>\$CertInfo.Certificate > c: \temp\user.cert</code>	将 PEM 数据通过管道传输到 <code>.cert</code> 文件
<code>c:\temp\user.cert</code>	在 Windows GUI 中打开 <code>.cert</code> 文件

从 Citrix Virtual Apps and Desktops 2411 之前的 FAS 版本升级

在 Citrix Virtual Apps and Desktops 2411 之前的 FAS 版本中，私钥属性通过编辑以下位置的 XML 文件进行配置

```
%programfiles%\Citrix\Federated Authentication  
Service\Citrix.Authentication.FederatedAuthenticationService.exe.config
```

这已被本文档中描述的 PowerShell 命令取代，这些命令提供了更大的灵活性，并且无需重新启动 FAS 服务器即可应用。

此外，与 XML 文件设置不同，使用 PowerShell 完成的配置在 FAS 服务器升级时会保留。

与私钥配置相关的 XML 文件设置如下所示，及其对应的 PowerShell 参数（如 `Get-FasKeyConfig` 和 `Set-FasKeyConfig` 中所用）：

XML 文件设置	XML 文件中的默认值	POWERSHELL 等效项	注释
<code>Citrix.Trust Fabric.Client SDK.TrustArea JoinParameters. KeyLength</code>	2048	-长度	-

XML 文件设置	XML 文件中的默认值	POWERSHELL 等效项	注释
<code>Citrix.Trust</code> <code>Fabric.Client</code> <code>SDK.TrustArea</code> <code>JoinParameter</code> <code>s.KeyProtection</code>	GenerateNonExportableKey	<code>-Exportable</code> <code>-UseDefault</code> <code>TpmProvider</code>	• NoProtection 通过将 <code>-Exportable</code> 设置为 <code>\$true</code> 来实现 <code>-GenerateNonExportableKey</code> 通过将 <code>-Exportable</code> 设置为 <code>\$false</code> 来实现 <code>-GenerateTPMProtectedKey</code> 通过指定 <code>-UseDefaultTpmProvider</code> 开关来实现
<code>Citrix.Trust</code> <code>Fabric.Client</code> <code>SDK.TrustArea</code> <code>JoinParameters.ProviderLegacyCsp</code>	假	<code>-Ksp</code>	<code>-ProviderLegacyCsp false</code> 通过将 <code>-Ksp</code> 设置为 <code>\$true</code> 来实现 <code>-ProviderLegacyCsp</code> 通过将 <code>-Ksp</code> 设置

XML 文件设置	XML 文件中的默认值	POWERSHELL 等效项	注释
			为 <code>\$false</code> 来实现 <code>true</code>
<code>Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderName</code>	-	-提供程序	-
<code>Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderType</code>	-	-CspType	-

XML 配置默认值和 PowerShell 默认值在功能上是等效的。也就是说，默认情况下，此版本以及 Citrix Virtual Apps and Desktops 2411 之前版本中 FAS 生成的密钥对的属性是相同的。

因此，如果您未更改 XML 配置文件中的任何上述设置，则在升级 FAS 时无需执行任何操作。

但是，如果您更改了任何上述设置，请按以下步骤升级 FAS：

- 将 FAS 置于维护模式；[维护模式](#)。
- 只需运行 FAS 安装程序即可[就地](#)升级 FAS；升级后，所有以前的设置将不会出现在 XML 文件中，并且无法在 XML 文件中配置。
- 使用 PowerShell 命令 `Set-FasKeyConfig`（如 [密钥配置 PowerShell 命令](#) 中所述）根据需要设置 FAS 私钥配置；考虑授权和用户证书所需的设置。
- 测试您的配置，如 [测试私钥配置](#) 中所述
- 使 FAS 服务器退出维护模式

下次升级时，FAS 私钥配置设置将保留，无需采取任何特殊操作。

加密远程处理

与 FAS 用户证书关联的私钥绝不会传输到 VDA。相反，当 VDA 需要使用用户的 FAS 证书时（无论是用于登录 VDA 还是用于会话内使用），加密请求都会远程回传到 FAS 服务器。这提高了安全性，因为私钥永远不会离开 FAS 密钥存储（无论是软件存储、TPM 还是 HSM）。

在 Windows VDA 上，这是通过在 VDA 上使用一对提供程序来实现的。发出加密请求的应用程序或操作系统代码并不知道该操作正在远程回传到 FAS 服务器。

在 Citrix Virtual Apps and Desktops 2411 之前，提供程序是 **加密服务提供程序 (CSP)**，应用程序和操作系统代码通过较旧的 Windows CAPI API 进行访问。这些提供程序是：

- `CitrixLogonCsp.dll`：用于 VDA 的单点登录
- `CitrixVirtualSmartcardCsp.dll`：用于会话内证书

从 Citrix Virtual Apps and Desktops 2411 开始，VDA 上提供了额外的密钥存储提供程序 (KSP)。应用程序和操作系统代码通过较新的 Windows CNG API 访问这些提供程序。新的提供程序是：

- `CitrixLogonKsp.dll`：用于 VDA 的单点登录
- `CitrixVirtualSmartcardKsp.dll`：用于会话内证书

KSP 是一种向 Windows 应用程序公开加密操作的更新方式，提供了更多功能。例如：

- 支持带 ECC 密钥的证书
- 支持概率签名方案 (PSS) 填充

如果 FAS 和 VDA 都运行 Citrix Virtual Apps and Desktops 2411 或更高版本，则使用 KSP 远程处理（即通过新 KSP 进行远程处理）。否则，系统将回退到使用旧版 CSP 进行远程处理。

禁用 KSP 远程处理

如果出现任何兼容性问题，可以禁用 KSP 远程处理，以便始终使用旧版 CSP 远程处理。

使用以下 PowerShell：

```
Set-FasServer -Address localhost -KspRemoting $false
```

维护模式

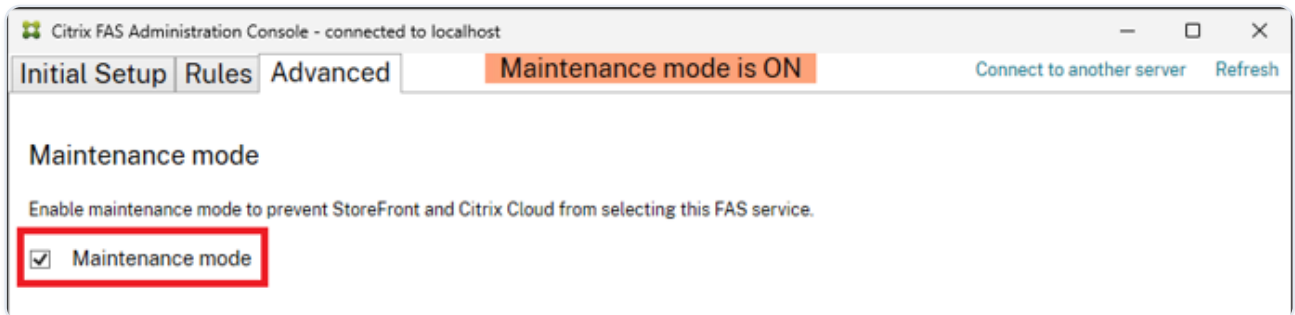
对 *活动* FAS 服务器的配置进行更改时，请考虑将其置于维护模式。

当 FAS 处于维护模式时，以下情况适用：

- 当 **Workspace** 或 **StoreFront™** 作为已发布应用程序或桌面启动序列的一部分调用 FAS 时，FAS 会指示其处于维护模式；调用方必须通过选择不同的 FAS 服务器来对此作出反应。
- 作为一项额外的预防措施，FAS 在维护模式下不允许自动创建用户证书。因此，可以避免因意外设置而无意中创建用户证书。
- 但是，涉及现有用户证书的活动（例如 VDA 登录或会话内使用）仍然允许。

尽管不允许自动创建用户证书，但管理员仍然可以使用 PowerShell 命令（例如 `New-FasUserCertificate` 或 `Test-FasCertificateSigningRequest`）创建用户证书。

使用管理控制台



使用 PowerShell

将 FAS 服务器置于维护模式，如下所示：

```
Set-FasServer -Address localhost -MaintenanceMode $true
```

将 FAS 服务器从维护模式中取出（并恢复正常运行），如下所示：

```
Set-FasServer -Address localhost -MaintenanceMode $false
```

相关信息

- [安装和配置](#) 是 FAS 安装和配置的主要参考资料。
- 常见的 FAS 部署在 [联合身份验证服务体系结构概述](#) 文章中进行了总结。
- 其他 [操作方法](#) 文章在 [高级配置](#) 文章中介绍。

安全和网络配置

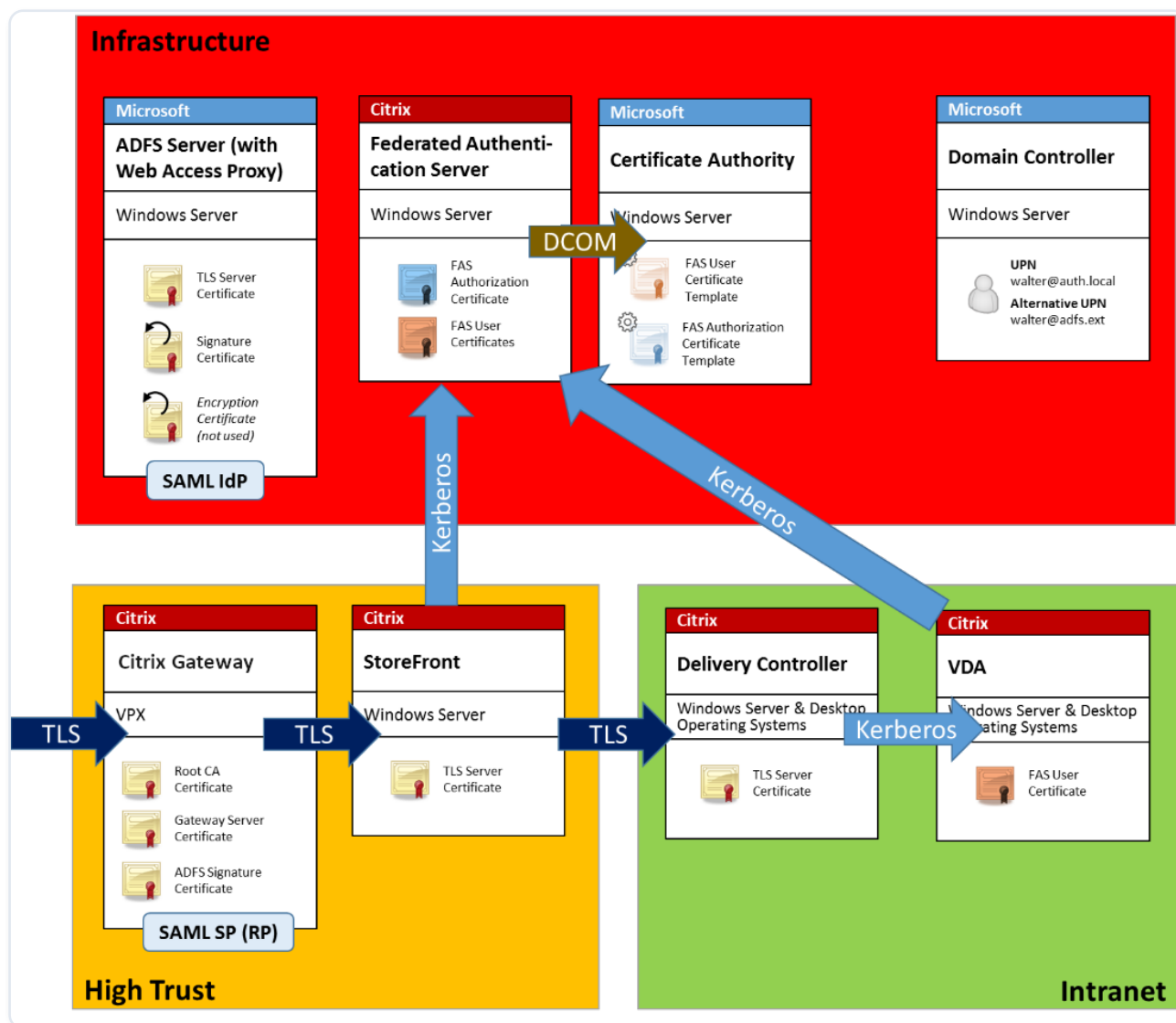
联合身份验证服务 (FAS) 与 Microsoft Active Directory 和 Microsoft 证书颁发机构紧密集成。确保系统得到适当的管理和保护，制定安全策略，就像您为域控制器或其他关键基础设施所做的那样。

本文档概述了部署 FAS 时需要考虑的安全问题。它还概述了可能有助于保护您的基础设施的可用功能。

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 服务器是安全关键基础设施的一部分，以及证书颁发机构和域控制器。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。



防火墙和网络安全

端口 443 上的 TLS 保护了 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 仅接受通过 Internet 使用 HTTPS 端口 443 的连接。

StoreFront 服务器通过端口 80 使用相互验证的 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 通信，该通信可配置为使用固定 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。

服务器	防火墙端口
联合身份验证服务	[in] 来自 StoreFront™ 和 VDA 的通过 HTTP 的 Kerberos, [out] DCOM 到 Microsoft 证书颁发机构
Citrix 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] HDX 到 VDA
StoreFront	[in] 来自 Citrix 网关的 HTTPS, [out] 到 Delivery Controller 的 HTTPS, [out] Kerberos HTTP 到 FAS
交付控制器	[in] 来自 StoreFront 服务器的 HTTPS, [in/out] 来自 VDA 的通过 HTTP 的 Kerberos
VDA	[in/out] 来自 Delivery Controller 的通过 HTTP 的 Kerberos, [in] 来自 Citrix Gateway 的 HDX, [out] Kerberos HTTP 到 FAS
Microsoft 证书颁发机构	[in] 来自 FAS 的 DCOM 和签名

Citrix 联邦身份验证服务与 Citrix Cloud™ 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

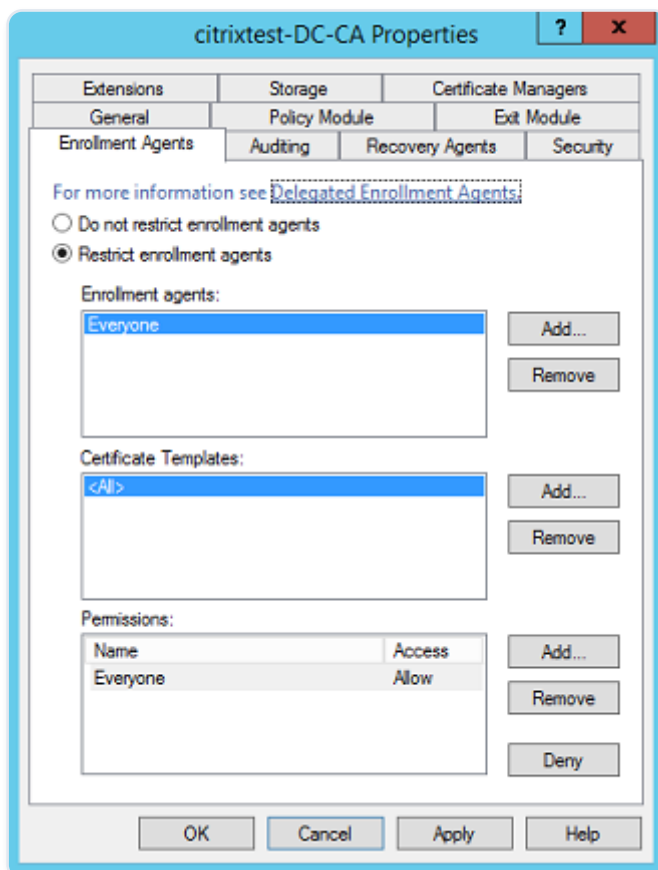
如果您的环境包含代理服务器，请使用 FAS 管理控制台的地址配置用户代理。此外，请确保使用 netsh 或类似工具配置网络服务帐户的地址。

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来确保：

- “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。

防火墙设置

与 FAS 服务器的所有通信都使用通过端口 80 进行的相互身份验证的 Windows Communication Foundation (WCF) Kerberos 网络连接。

事件日志监控

FAS 和 VDA 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](#) 部分列出了可以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。

可以使用 PowerShell 命令进行低级别加密配置。FAS 授权证书私钥和用户证书密钥可以使用不同的设置。有关更多详细信息，请参阅 [私钥保护](#)

管理职责

环境管理可分为以下几组：

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，从而允许采用纵深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。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）。停用 FAS 服务器后，请注意避免立即重用计算机 FQDN 名称。

证书模板

如果您不想使用 FAS 提供的 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，您必须：

- 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。

修改常规属性

默认情况下，用户证书的生命周期为七天。您可以在证书模板中修改有效期。

请勿修改续订期。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。

修改已取代的模板属性

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。

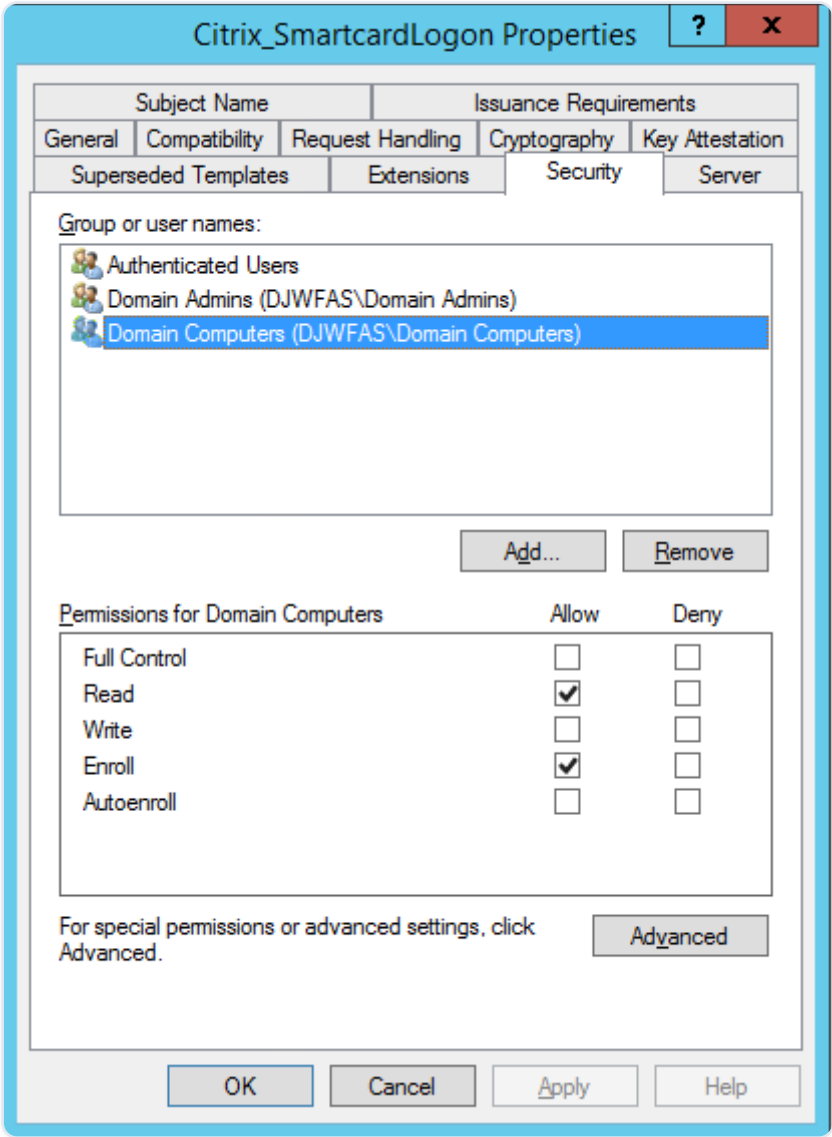
注意：

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，以仅允许 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



修改使用者名称属性

Citrix 建议您不要修改这些属性。

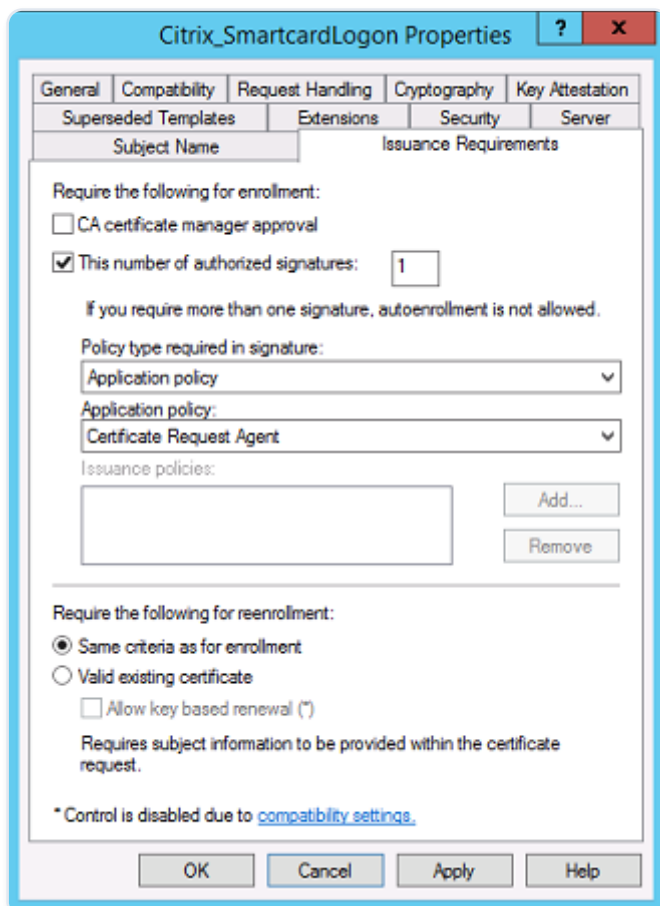
该模板已选择“从此 Active Directory 信息构建”，这会导致证书颁发机构在证书扩展中包含用户的 SID，从而提供与用户 Active Directory 帐户的强映射。

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：



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）可用的其他设置。

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。

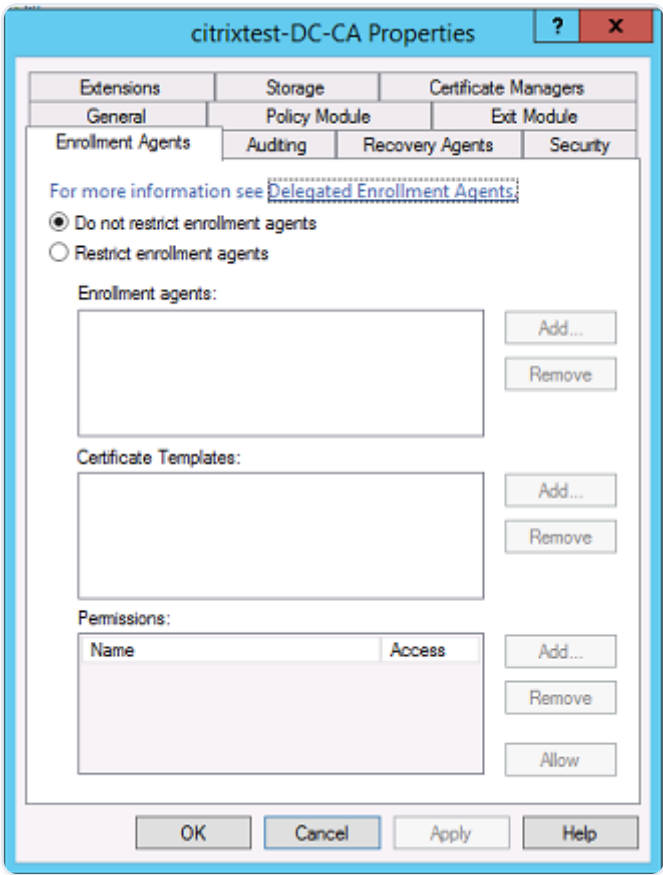
一种简单的安全做法是，在安装 FAS 服务器时仅发布注册机构证书模板，或者坚持完全脱机颁发过程。无论哪种情况，证书颁发机构管理员都必须完全控制授权注册机构证书请求，并制定授权 FAS 服务器的策略。

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。

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任何允许访问的证书模板向任何用户颁发证书。证书的颁发必须通过“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。

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 检索到的凭据句柄，因此此组中受损的 VDA 帐户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，则规则会很有用。每个规则都有一组单独的配置选项；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

可以为不同的访问权限配置不同的证书模板和 CA。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是否可在用户会话中使用。例如，用户可能只有“签名”证书可在会话中使用，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 建议至少将 FAS 授权证书私钥存储在 TPM 中以进行保护。

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

注意：

尽管 FAS 可以在 TPM 或 HSM 中生成和存储用户证书密钥，但对于大型部署，硬件可能太慢或受大小限制。

有关更多详细信息，请参阅 [私钥保护](#)。

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。

管理访问和管理工具

FAS 包含远程管理功能（相互认证的 Kerberos）和工具。“本地管理员组”的成员对 FAS 配置拥有完全控制权。FAS 配置必须妥善维护。

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 的“凭据句柄”只是替换了“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。

通用 Windows 服务器安全性

所有服务器都必须完全打补丁，并配备标准防火墙和防病毒软件。安全关键型基础设施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。

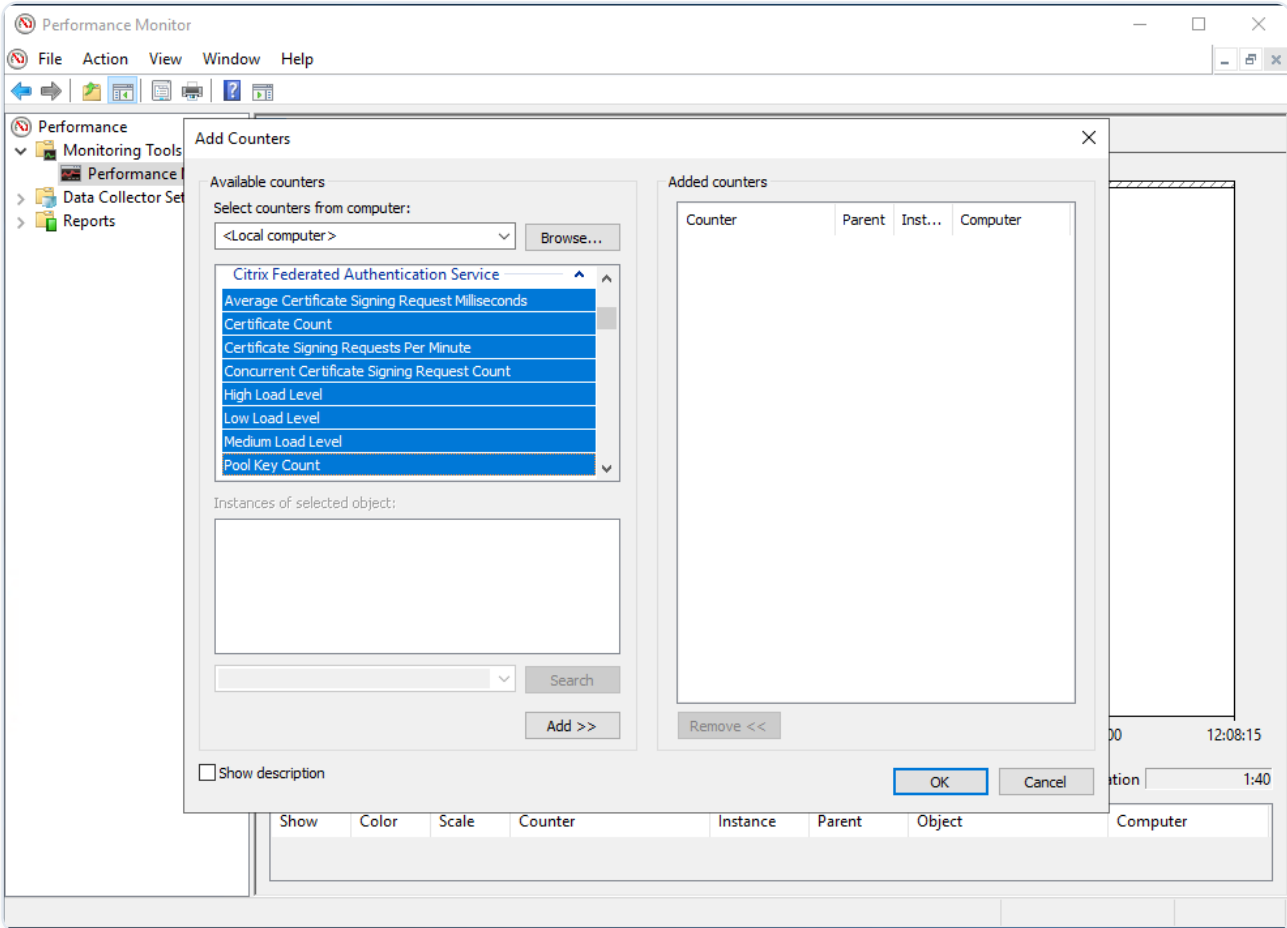
RDP 访问必须仅限于授权管理员。Citrix 建议对用户帐户，特别是对证书颁发机构和域管理员帐户使用智能卡登录。

相关信息

- [安装和配置](#) 是 FAS 安装和配置的主要参考资料。
- FAS 架构在[部署架构](#) 一文中介绍。
- 其他“操作方法”文章在[高级配置](#) 一文中介绍。

性能计数器

FAS 包含一组用于负载跟踪的性能计数器。



下表列出了可用的计数器。除非另有说明，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量，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量。
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。

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。

排查 Windows 登录问题

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

证书和公钥基础设施

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

- **NTAuth 证书存储区：**要向 Windows 进行身份验证，立即颁发用户证书的证书颁发机构（即不支持链式结构）必须放置在 NTAuth 存储区中。要查看这些证书，请在 certutil 程序中输入：
`certutil -viewstore -enterprise NTAuth`
- ****根证书和中间证书存储区：**通常，证书登录系统只能提供单个证书，因此，如果使用链式结构，则所有计算机上的中间证书存储区都必须包含这些证书。根证书必须位于受信任的根存储区中，倒数第二个证书必须位于 NTAuth 存储区中。
- ****登录证书扩展和组策略：**可以将 Windows 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\(v=ws.10\)>](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 会筛选出不允许 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 会筛选出已过期的证书。此选项会覆盖该筛选器。
EnumerateECCerts	启用椭圆曲线认证。

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)，或者它不明确，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 的进程的身份）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，这可能会解析到林中的不同域。

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，允许用户指定一个用户帐户，以加快此搜索速度，并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高效地查找任何域中的用户帐户。

控制登录域控制器选择

当环境中包含多个域控制器时，查看并限制用于身份验证的域控制器非常有用，这样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（\Windows\System32\drivers\etc\lmhosts）来明确设置 Windows 计算机使用的域控制器列表。

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 域控制器不会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。要在域控制器上打开组策略编辑器，请运行 **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/2411/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，打开事件查看器并启用 Microsoft/Windows/CAPI2/Operational Logs 的日志记录。

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。如果要恢复默认 CAPI2 日志记录设置，请删除这些值。

值	描述
DiagLevel (DWORD)	详细级别（0 到 5）
DiagMatchAnyMask (QUADWORD)	事件筛选器（全部使用 0xffffffff）
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 (/zh-cn/federated-authentication-service/2411/config-manage/troubleshoot-logon.html#certificates-and-

错误代码	描述
	public-key-infrastructure) 部分中的[证书和公钥基础结构]。
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。

Kerberos 日志

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

配置单元	值名称	值 [DWORD]
CurrentControlSet\Control\LocalSecurity\Kerberos\Parameters	LogLevel	0x1
CurrentControlSet\Control\LocalSecurity\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** 之类的消息必须易于诊断。
- 两个错误代码是信息性的，可以安全忽略：
 - 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。

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，并验证了其有效性（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

域控制器显示了一系列登录事件，其中关键事件是 4768，在该事件中，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。

Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	21/06/2016 15:14:56	Security-Auditing	4624	Logon
Audit Success	21/06/2016 15:14:56	Security-Auditing	4624	Logon
Audit Success	21/06/2016 15:14:54	Security-Auditing	4769	Kerberos Service Ticket Operations
Audit Success	21/06/2016 15:14:54	Security-Auditing	4768	Kerberos Authentication Service
Audit Success	21/06/2016 15:14:54	Security-Auditing	4769	Kerberos Service Ticket Operations
Audit Success	21/06/2016 15:14:54	Security-Auditing	4634	Logoff
Audit Success	21/06/2016 15:14:54	Security-Auditing	4624	Logon
Audit Success	21/06/2016 15:14:54	Security-Auditing	4624	Logon

Event 4768, Security-Auditing

General | Details

☒ Friendly View ☐ XML View

+ System

- EventData

TargetUserName fred

TargetDomainName CITRIXTEST.NET

TargetSid S-1-5-21-390731715-1143989709-1377117006-1106

ServiceName krbtgt

ServiceSid S-1-5-21-390731715-1143989709-1377117006-502

TicketOptions 0x40810010

Status 0x0

TicketEncryptionType 0x12

PreAuthType 16

IpAddress ::ffff:192.168.0.10

IpPort 49348

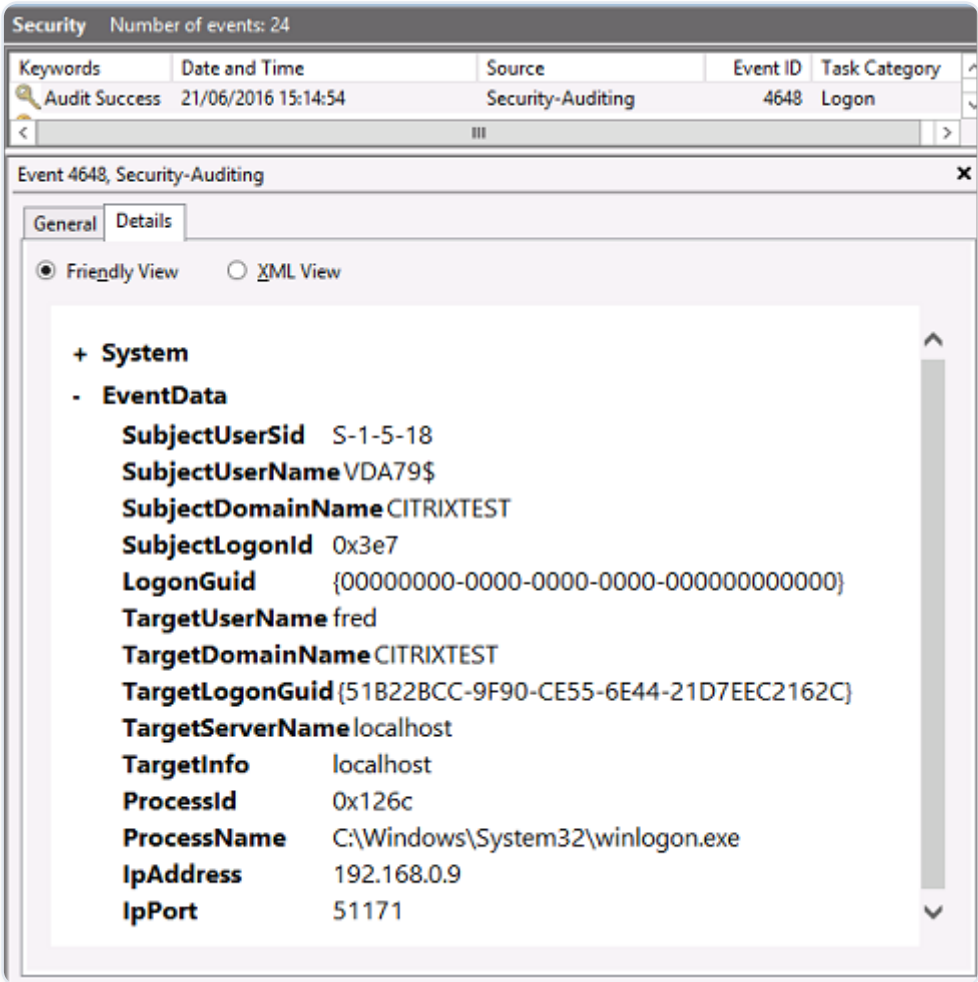
CertIssuerName citrixtest-DC-CA

CertSerialNumber 5F0001D1FCA2AC30F36879CEEC00000001D1FC

CertThumbprint 23BC65AFB7F18787ADAAAD5CEF09CC7505C4176F

VDA 安全日志

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



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)。

Information	21/06/2016 15:14:54	CAPI2	30	Verify Chain P...
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 Revocat...
Information	21/06/2016 15:14:54	CAPI2	40	Verify Revocat...
Information	21/06/2016 15:14:54	CAPI2	10	Build Chain

- UserData

- CertVerifyCertificateChainPolicy

- Policy

[type]

CERT_CHAIN_POLICY_NT_AUTH

[constant]

6

- Certificate

[fileRef]

813C6D12E1E1800E61B8DB071E186EB912B7

[subjectName]

dc.citrixtest.net

- CertificateChain

[chainRef]

{84E0B3D1-A4D4-4AC7-BA99-5291415B343

- Flags

[value]

0

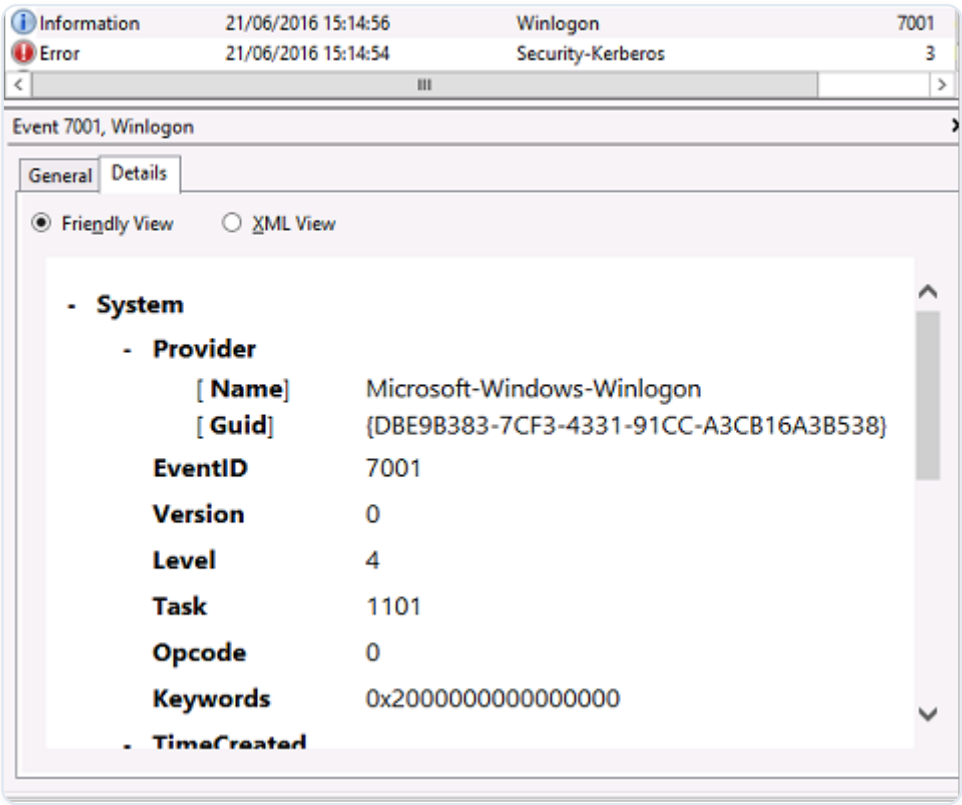
- Status

[chainIndex]

-1

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（可以忽略），以及 Windows 登录中显示 Kerberos 登录成功的条目。



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。

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。	此功能适用于 FAS 10.7 / Citrix Virtual Apps and Desktops 2109 及更高版本。
[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。	此功能适用于 FAS 10.7 / Citrix Virtual Apps and Desktops 2109 及更高版本。
[S123]	未能为 [upn: {0} role: {1}] [exception: {2}] 在任何证书颁发机构颁发证书	此事件在 [S124] 之后发生，如果 FAS 配置的任何证书颁发机构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证书颁发机构均无法正常工作。如果 FAS 配置为使用 HSM，这也可能表明 HSM 无法正常工作。
[S124]	未能为 [upn: {0} role: {1}] 在 [certificate authority: {2}] [exception: {3}] 颁发证书	当 FAS 尝试从给定证书颁发机构请求用户证书时发生故障。如果 FAS 配置了多个证书颁发机构，FAS 会	此事件可能表明证书颁发机构无法正常工作或无法联系。如果 FAS 配置为使用 HSM，这也可能表明 HSM 无法正常工作。

事件	事件文本	说明	备注
		尝试向另一个证书颁发机构发出请求。	作。可以使用异常来帮助识别问题的原因。
[S413]	授权证书即将过期（剩余 {0} 天）。证书详细信息：{1}	当 FAS 授权证书即将过期时，此事件会定期生成。默认情况下，如果授权证书在 30 天内过期，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 cmdlets 。
[S414]	授权证书已过期。证书详细信息：{0}	当 FAS 授权证书过期时，此事件会定期生成。默认情况下，此事件每天生成。	一旦过期，FAS 将无法生成新的用户证书，并且单点登录开始失败。

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）进行的单点登录应该正常工作。	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 服务无法用于 Citrix Cloud 的单点登录。[{0}] 更多详细信息可在管理控制台找到。	此事件表示 FAS 无法从 Workspace（即 Citrix Cloud）提供单点登录。该消息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存期策略）而偶尔终止。发生这种情况时，事件文本包含“Service is not connected to the cloud”。 这是正常行

事件	事件文本	说明	备注
			为，FAS 会立即尝试重新建立与 Citrix Cloud 的连接。

安全事件

以下事件表示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	尝试查看或更改 FAS 配置，但调用方不是 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，但调用者不是 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，但调用者无权执行此操作。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
[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}] 将维护模式设置为“关”
[S023] 管理员 [{0}] 将维护模式设置为“开”
[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

日志代码
[S028] 管理员 [{0}] 正在为 [{1}] 证书设置密钥配置为 [{2}]
[S029] 管理员 [{0}] 正在将 [{1}] 证书的密钥配置重置为默认值 [{2}]
[S030] 管理员 [{0}] 正在将服务属性设置为 [{1}]
[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}]
[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] 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 Federated Authentication Service 必须以 Network Service 身份运行 [currently running as: {0}]
[S404] 正在强制擦除 Citrix Federated Authentication Service 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}]

日志代码
[S409] 线程池配置成功 - MinThreads 已从 [workers: {0} completion: {1}] 调整为：[workers: {2} completion: {3}]
[S410] 线程池配置失败 - 未能将 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}
[S414] 授权证书已过期。证书详细信息：{0}
[S415] 授权证书检查完成。已记录 {0} 个问题。下次检查将在 {1} 进行

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 不被角色 [{2}] 允许)
[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} role: {1}][每分钟请求数 {2}]。
[S123] 未能为 [upn: {0} role: {1}] 在任何 CA 颁发证书 [exception: {2}]
[S124] 未能为 [upn: {0} role: {1}] 在 [certificate authority: {2}] 颁发证书 [exception: {3}]

日志代码
[S125] 等待挂起的证书请求完成的调用在 {0} 秒后超时 [upn: {1} role: {2} Security Context: [{3}]]
[S126] 服务器 [{0}] 尝试使用未定义的规则断言身份 [{1}]
[S127] FAS 无法为 [upn: {0} role: {1} definition: {2}] 请求证书，因为服务器处于维护模式；请使用 powershell cmdlet Set-FasServer 在维护模式下更改行为

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}] 无权访问登录提供程序
[S204] 信赖方 [{0}] 正在访问 [upn: {1}] 的登录提供程序，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] 调用账户 [{0}] 不是信赖方
[S208] 私钥操作失败 [操作: {0} UPN: {1} 角色: {2} 证书定义 {3} 错误 {4} {5}]。

会话内证书服务器

当用户使用会话内证书时，这些事件会记录在 FAS 服务器上。

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}] 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}]

日志代码

[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}] 不支持它）

[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}]）

[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，但未配置 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] Citrix Cloud 授权密钥已轮换 [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}

日志代码
[S003] FAS 已向云注册 [fas id: {0}] [transaction id: {1}]
[S004] FAS 未能向云注册 [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 [fas id: {0}] [transaction id: {1}] [exception: {2}]
[S007] FAS 已从云注销 [fas id: {0}] [transaction id: {1}]
[S009] FAS 未能从云注销 [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
[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
[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，因为调用者未获授权 [message ID {0}] [transaction ID {1}] [caller {2}]
[S016] 对云服务的调用 <service name> 成功 [fas id: {0}] [transaction id: {1}]
[S019] FAS 从云端下载了其配置 [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 授权密钥的轮换 [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}]

日志代码
[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}]
[S028] FAS 已将其当前遥测数据发送到云端 [fas id: {0}] [transaction id: {1}]
[S029] FAS 未能将其当前遥测数据发送到云端 [fas id: {0}] [transaction id: {1}] [exception: {2}]

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。未识别的联合身份验证服务 [id: {0}]
[S102] 身份断言登录失败。{0} 的 SID 查找失败 [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。对 {0} 的调用返回 [Error: {1} {2}]
[S105] 身份断言登录。正在登录 [Username: {0} Domain: {1}]
[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，用于 [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 服务器执行低级别加密操作时，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}] [Reason: {1}]
[S016] 私钥::创建 [Identifier: {0}] [MachineWide: {1}] [Provider: {2}] [ProviderType: {3}] [EllipticCurve: {4}] [KeyLength: {5}] [IsExportable: {6}] [CreateReason: {7}]
[S017] 私钥::删除 [Provider: {0}] [Identifier {1}]
[S018] PrivateKey::Create 失败 [Identifier: {0}] [MachineWide: {1}] [Provider: {2}] [ProviderType: {3}] [EllipticCurve: {4}] [KeyLength: {5}] [IsExportable: {6}] [CreateReason: {7}] [Exception: {8}]

日志代码
[S104] MicrosoftCertificateAuthority::GetCredentials: 已授权使用 {0}
[S105] MicrosoftCertificateAuthority::SubmitCertificateRequest 提交响应错误 [{0}]
[S106] MicrosoftCertificateAuthority::SubmitCertificateRequest 已颁发证书 [{0}]
[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 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	说明和参考
用户名或密码无效	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。
系统无法将您登录。您的凭据无法验证。/ 请求不受支持	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 身份验证”、“域控制器身份验证”。

显示的错误消息	说明和参考
	证”或“域控制器”证书。即使现有证书看起来有效，也值得尝试此操作。
系统可能无法将您登录。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）。

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指南](#)

PowerShell cmdlet 命令

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>` 显示 cmdlet 帮助。

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/>。

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 会将用户身份验证决策委派给受信任的 StoreFront 服务器。StoreFront 拥有一套基于现代 Web 技术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](#)

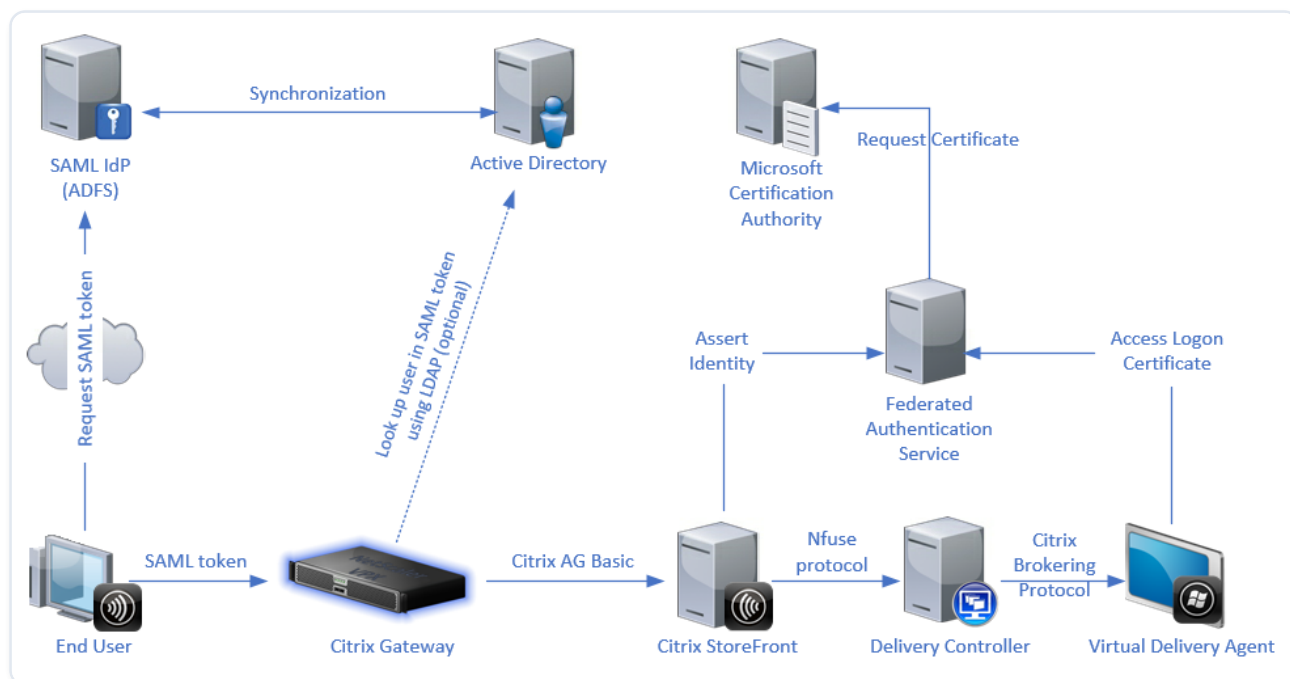
提供了相关 FAS 文章的链接。对于所有架构，[安装和配置](#) 文章是设置 FAS 的主要参考资料。

架构概述

FAS 获授权代表由 StoreFront 验证的 Active Directory 用户自动颁发智能卡类证书。这使用的 API 与允许管理员预配物理智能卡的工具类似。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 会授予一个票证，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。



内部部署

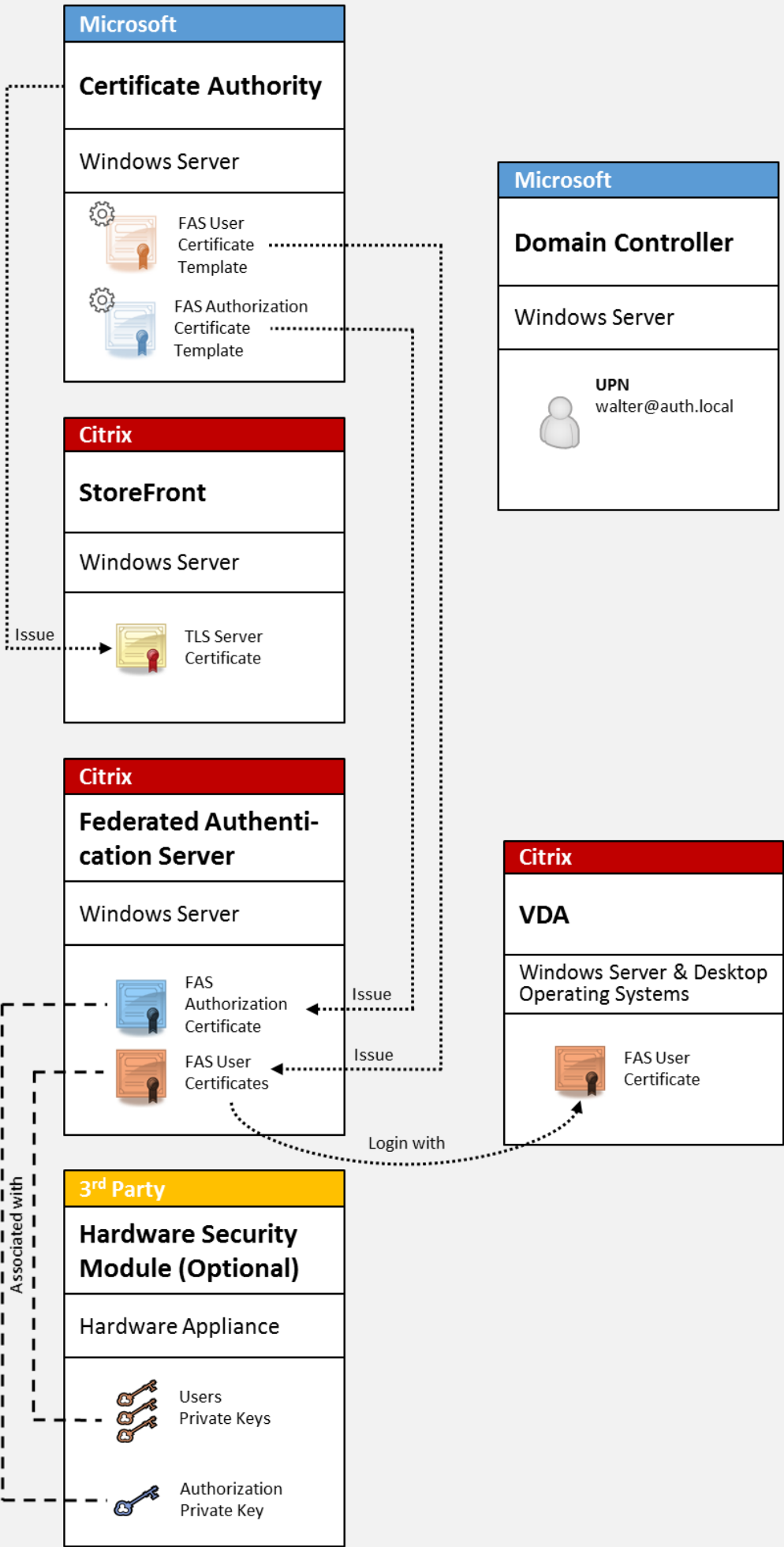
FAS 允许用户使用各种身份验证选项（包括 Kerberos 单点登录）安全地向 StoreFront 进行身份验证，并连接到完全经过身份验证的 Citrix HDX™ 会话。

这允许 Windows 身份验证，而无需提示输入用户凭据或智能卡 PIN，也无需使用“保存的密码管理”功能（例如单点登录服务）。这可用于取代早期版本 Citrix Virtual Apps 中提供的 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结构 (PKI) 证书，无论他们是否使用智能卡登录到端点设备。这使得可以顺利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。

此部署添加了一个运行 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，就像使用了智能卡登录一样。

AUTH.LOCAL domain



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。）

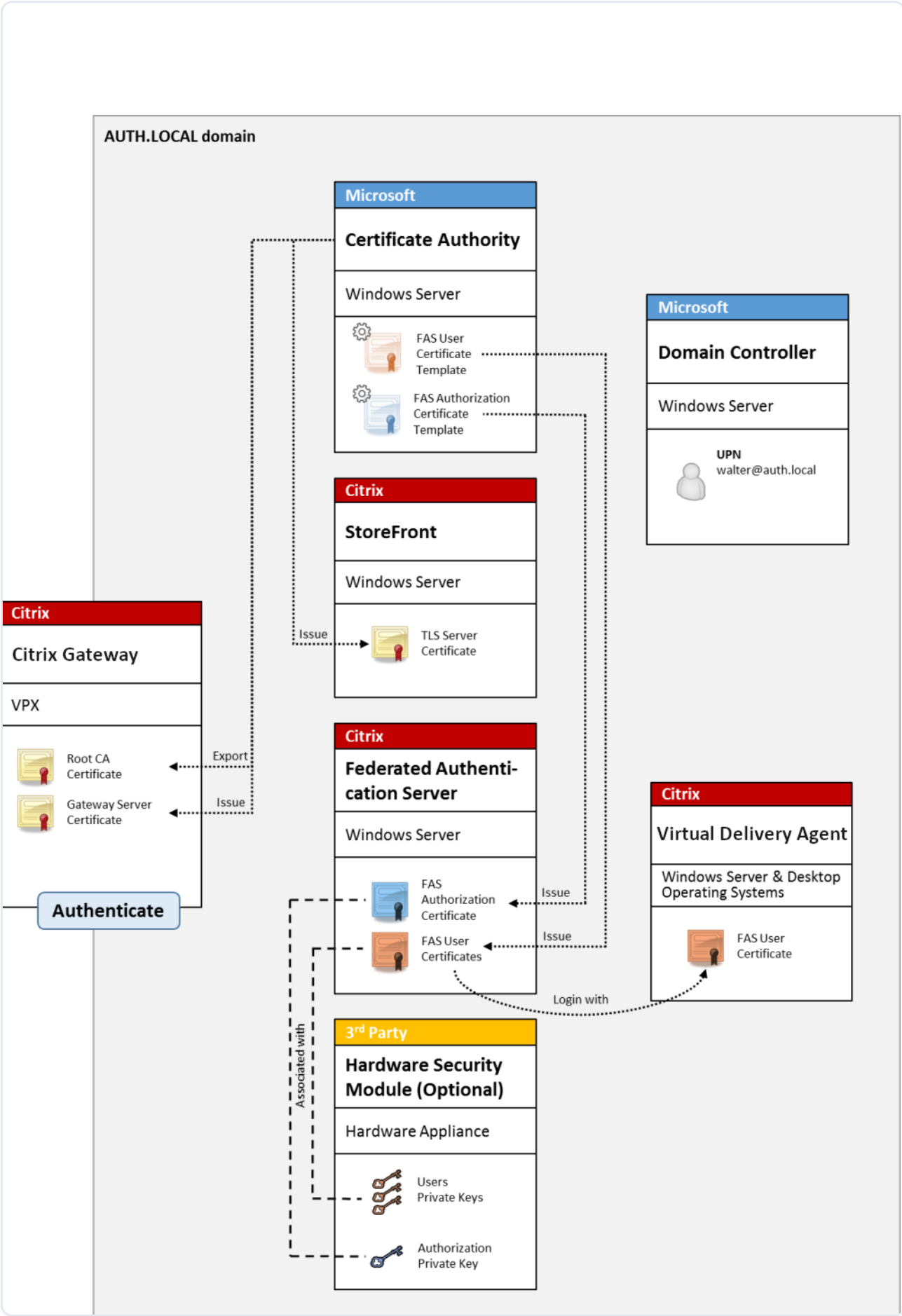
相关信息：

- 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个 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。



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）。

将 Citrix Gateway 配置为主要身份验证系统时，请确保 Citrix Gateway 和 StoreFront 之间的所有连接都使用 TLS 进行保护。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。

Add NetScaler Gateway Appliance

StoreFront

- ✓ General Settings
- ✓ Secure Ticket Authority
- Authentication Settings**
- Summary

Authentication Settings

These settings specify how the remote user provides authentication credentials

Version: 10.0 (Build 69.4) or later

VServer IP address: (optional) v10.0: SNIP or MIP, v10.1+: VIP

Logon type: Domain

Smart card fallback: None

Callback URL: (optional) https://NetScalerGatewayFQDN /CitrixAuthService/AuthService.asmx

⚠ When no Callback URL is specified, Smart Access is not available.

Back Create Cancel

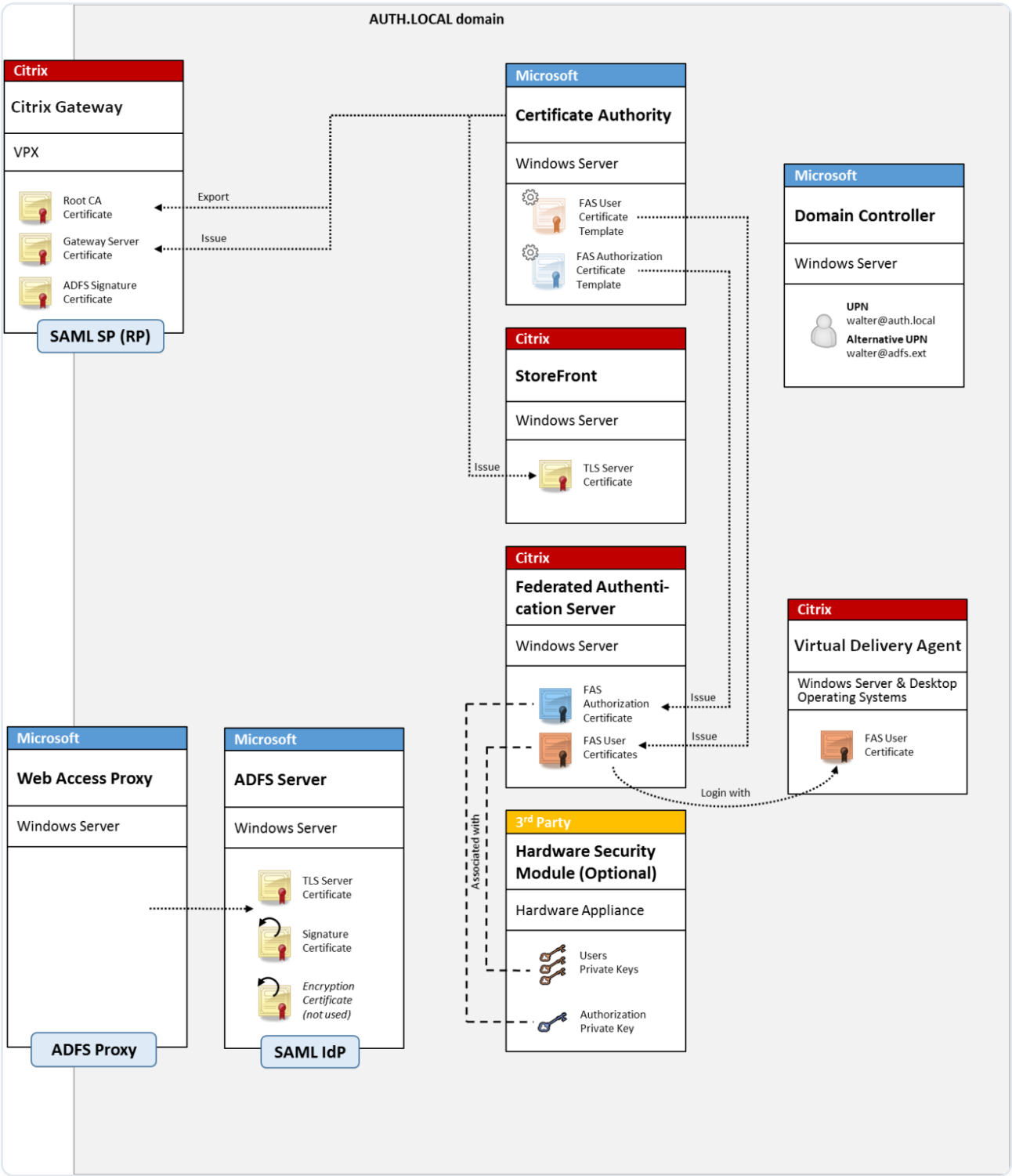
相关信息：

- 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。

ADFS SAML 部署

一项关键的 Citrix Gateway 身份验证技术允许与 Microsoft ADFS 集成，Microsoft ADFS 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 服务器允许将用户的身份验证委托给 Microsoft ADFS 服务器（或其他支持 SAML 的 IdP）。



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。

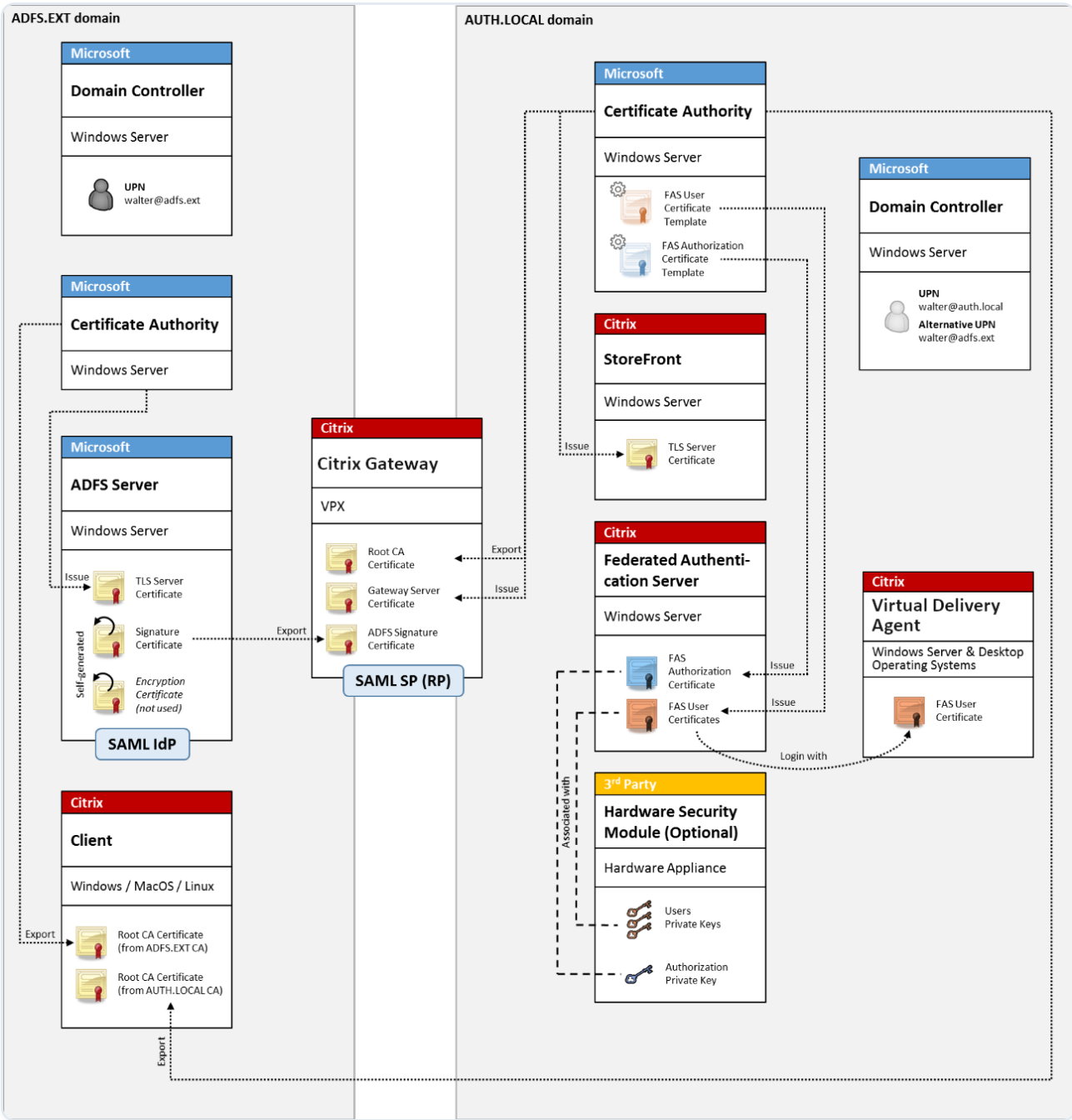
相关信息：

- 有关 [ADFS 部署](#) 文章中包含详细信息。

- 有关 [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 Active Directory 联合身份验证服务 (ADFS) 服务器。这允许一家公司的用户无缝地向另一家公司的 Active Directory (AD) 环境进行身份验证。登录时，每个用户都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”。

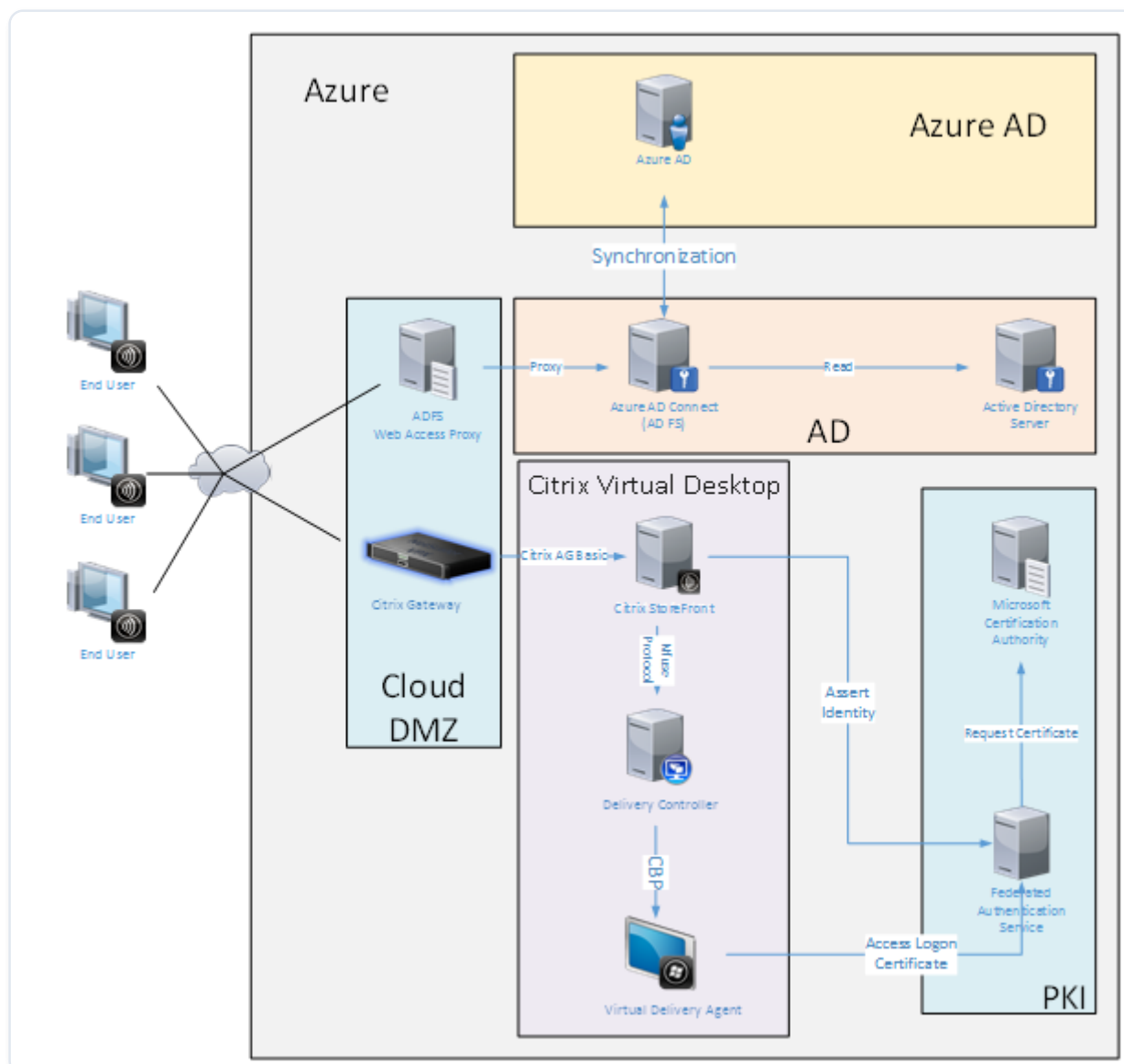


相关信息：

- [安装和配置](#) 一文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 Internet”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一登录模型的功能。这些都“支持 Internet”，因此可以在任何连接 Internet 的位置工作，而不仅仅是办公室局域网。



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 Internet 进行注册和身份验证。

请注意，此部署中的基础结构可以在任何可用的 IP 地址处运行：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。为简单起见，示例图形使用 Azure VM。

相关信息：

- [安装和配置](#) 一文介绍了如何安装和配置 FAS。
- [Azure AD 集成](#) 一文包含详细信息。

ADFS 部署

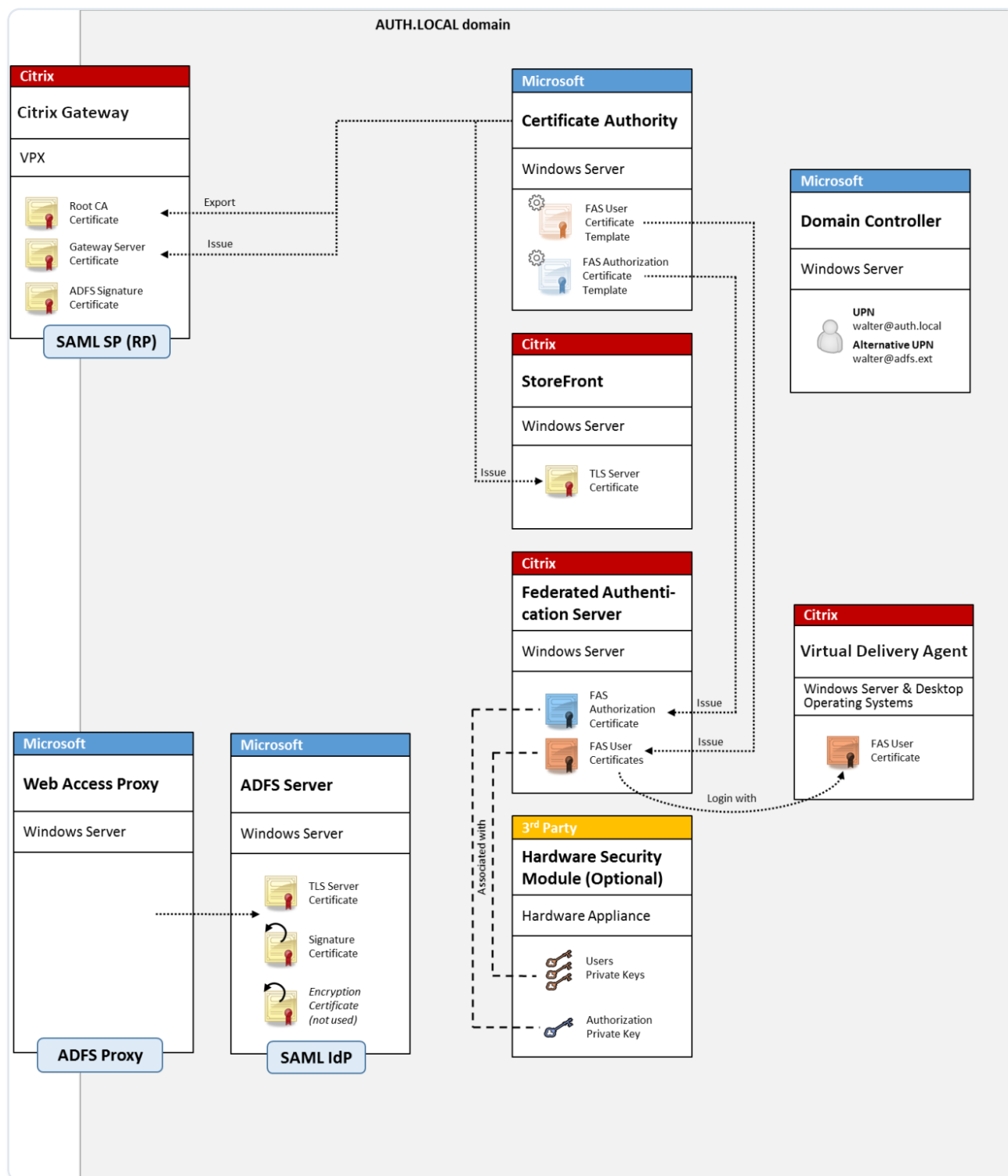
简介

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

许多组织使用 ADFS 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 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 作为信赖方集成到 Microsoft ADFS。



注意：

如果后端资源是 Windows VDA 或 Linux VDA，则没有区别。

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：

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 数据中包含的唯一标识符，用于发送给 ADFS。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。如果已颁发，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，但只要 Citrix Gateway 和 ADFS 达成一致，它通常可以是任何内容：`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，形式为：`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。

单点注销 URL

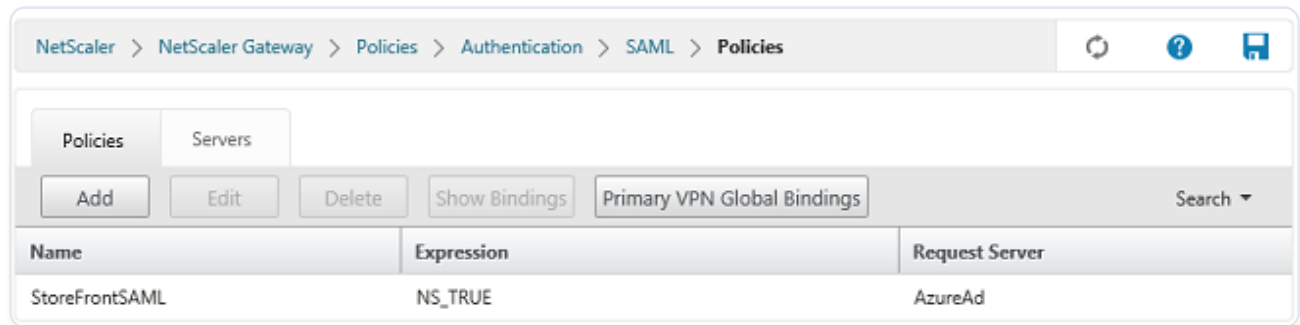
ADFS 和 Citrix Gateway 支持“集中注销”系统。这是一个 Citrix Gateway 偶尔轮询的 URL，用于检查 SAML 身份验证 XML blob 是否仍然代表当前已登录的会话。

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

配置

部分 (</zh-cn/federated-authentication-service/2411/deployment-architectures.html#citrix-gateway-deployment>) 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。

Create Authentication SAML Server

Create Authentication SAML Server

Name*

AzureAd

Authentication Type

SAML

IDP Certificate Name*

AzureADSAML

+

Redirect URL*

29f-4c20-9826-14d5e484c62e/saml2

Single Logout URL

29f-4c20-9826-14d5e484c62e/saml2

User Field

userprincipalname

Signing Certificate Name

Issuer Name

https://ns.citrixsaml demo.net/Citrix/

Reject Unsigned Assertion*

ON

SAML Binding*

POST

Default Authentication Group

Skew Time(mins)

5

Two Factor

☐ ON ☒ OFF

Assertion Consumer Service Index

255

Attribute Consuming Service Index

255

Requested Authentication Context*

Exact

Authentication Class Types

InternetProtocol
InternetProtocolPassword
..

Signature Algorithm*

☐ RSA-SHA1 ☒ RSA-SHA256

Digest Method*

☐ SHA1 ☒ SHA256

☐ Send Thumbprint

☒ Enforce Username

Attribute 1

Attri

Attribute 3

Attri

Attribute 5

Attri

Attribute 7

Attri

相关信息

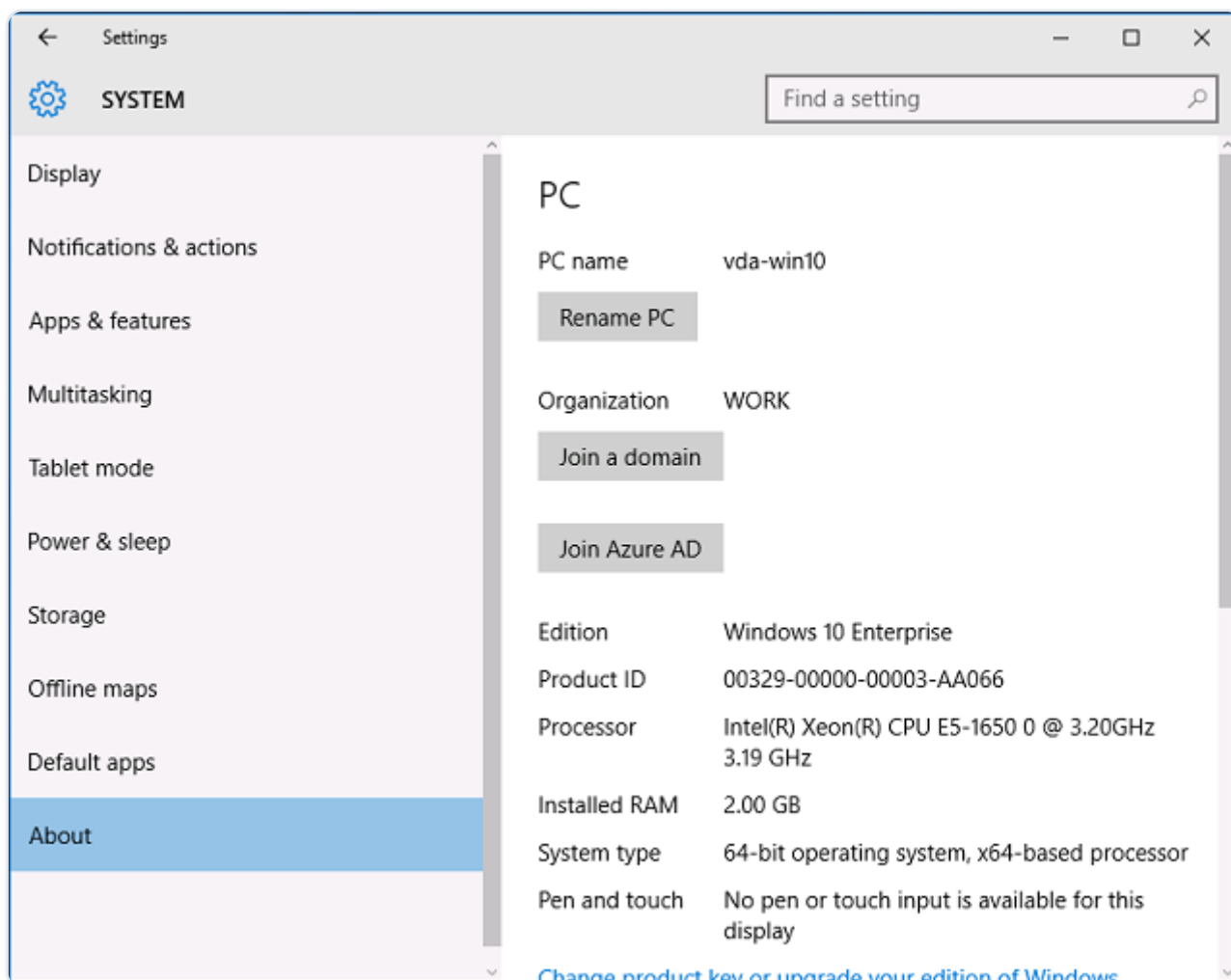
- [安装和配置](#) 是 FAS 安装和配置的主要参考资料。
- 常见的 FAS 部署在 [部署架构](#) 文章中进行了总结。
- “操作方法”文章在 [高级配置](#) 文章中介绍。

Azure AD 集成

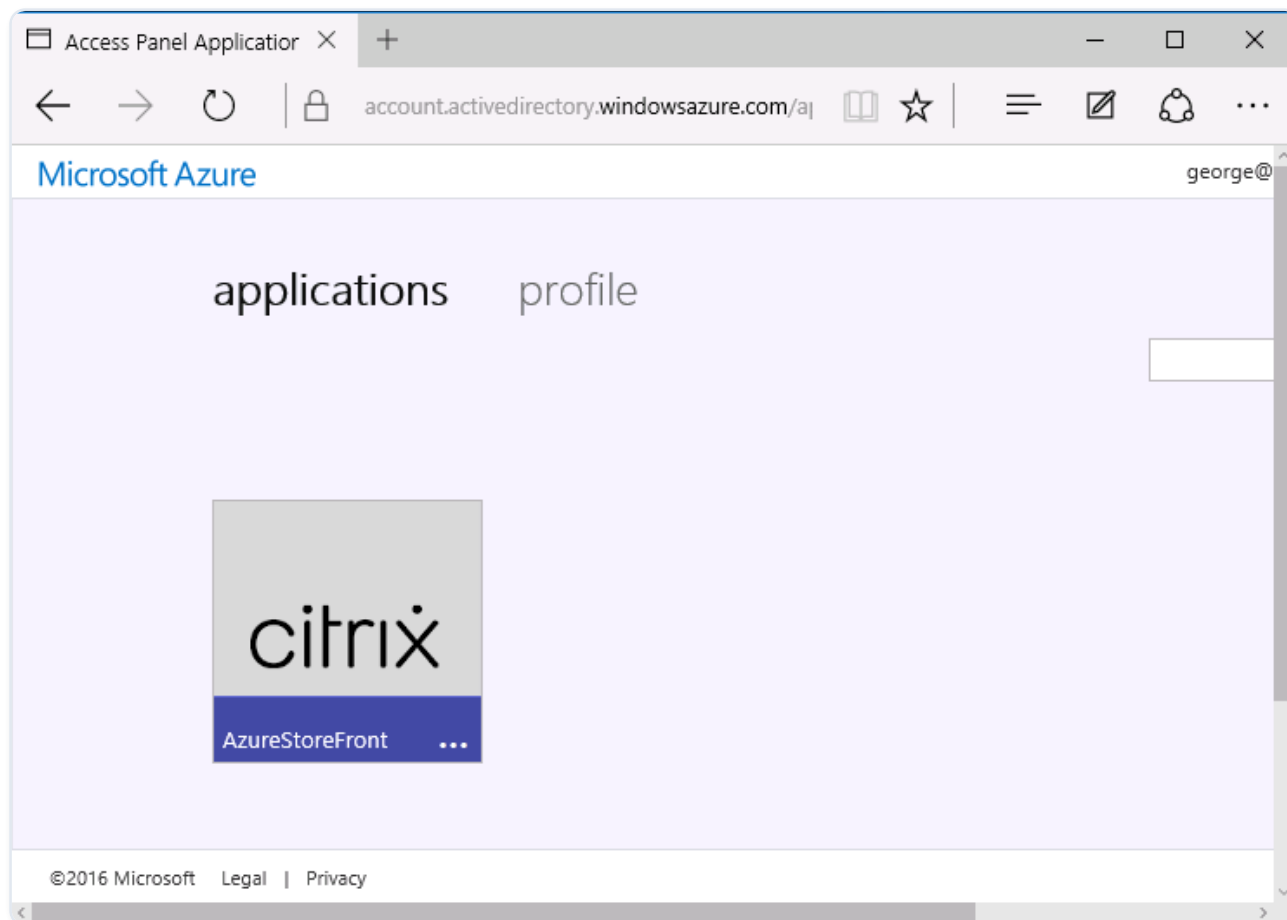
简介

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，其中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 为新用户提供公司电子邮件地址和其个人 Windows 10 笔记本电脑的注册码。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。



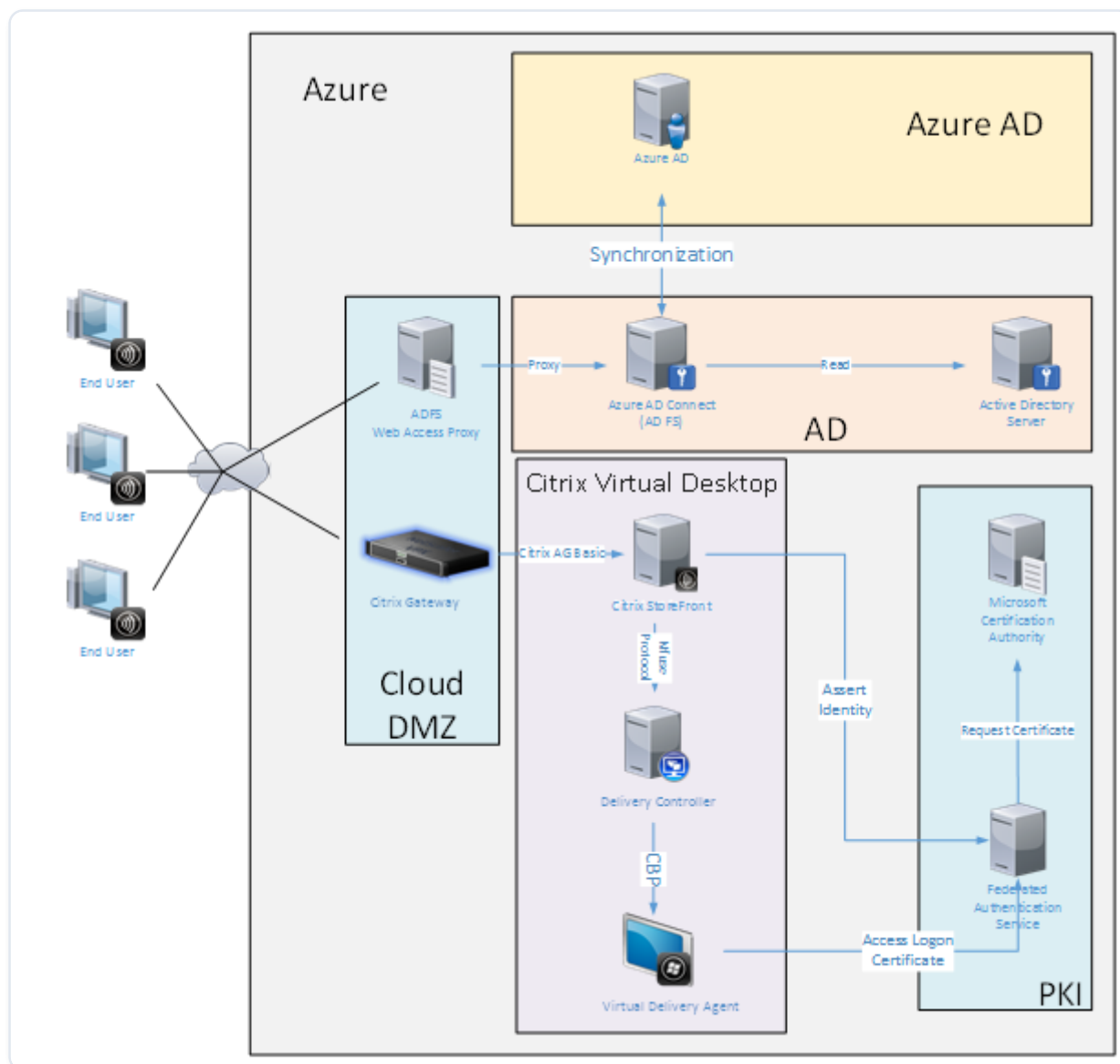
笔记本电脑注册后，Microsoft Edge Web 浏览器会自动通过 Azure SaaS 应用程序网页登录公司网站和 Citrix 发布应用程序，以及其他 Azure 应用程序（例如 Office 365）。



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 同步可以通过 Internet 连接到 Azure。



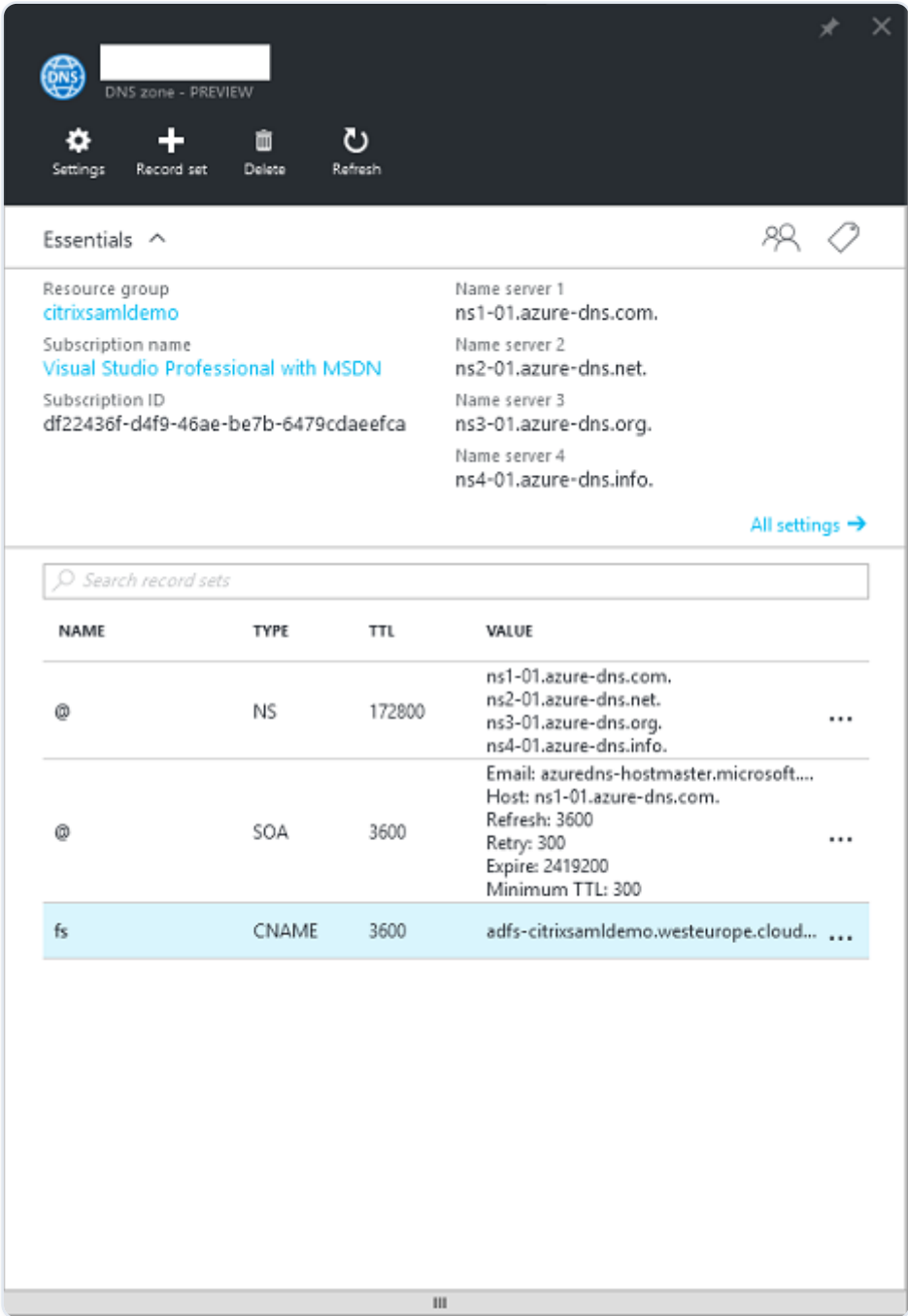
在此体系结构中，传统上通过防火墙 LAN 和 Kerberos/NTLM 身份验证实现的安全连接和单点登录被替换为到 Azure 的 TLS 连接和 SAML。新服务作为加入 Azure AD 的 Azure 应用程序构建。需要 Active Directory 的现有应用程序（例如 SQL Server 数据库）可以使用 Azure 云服务的 IAAS 部分中的标准 Active Directory 服务器 VM 运行。

当用户启动传统应用程序时，他们会使用 Citrix Virtual Apps and Desktops™ 发布应用程序进行访问。不同类型的程序通过用户的**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*。



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`）

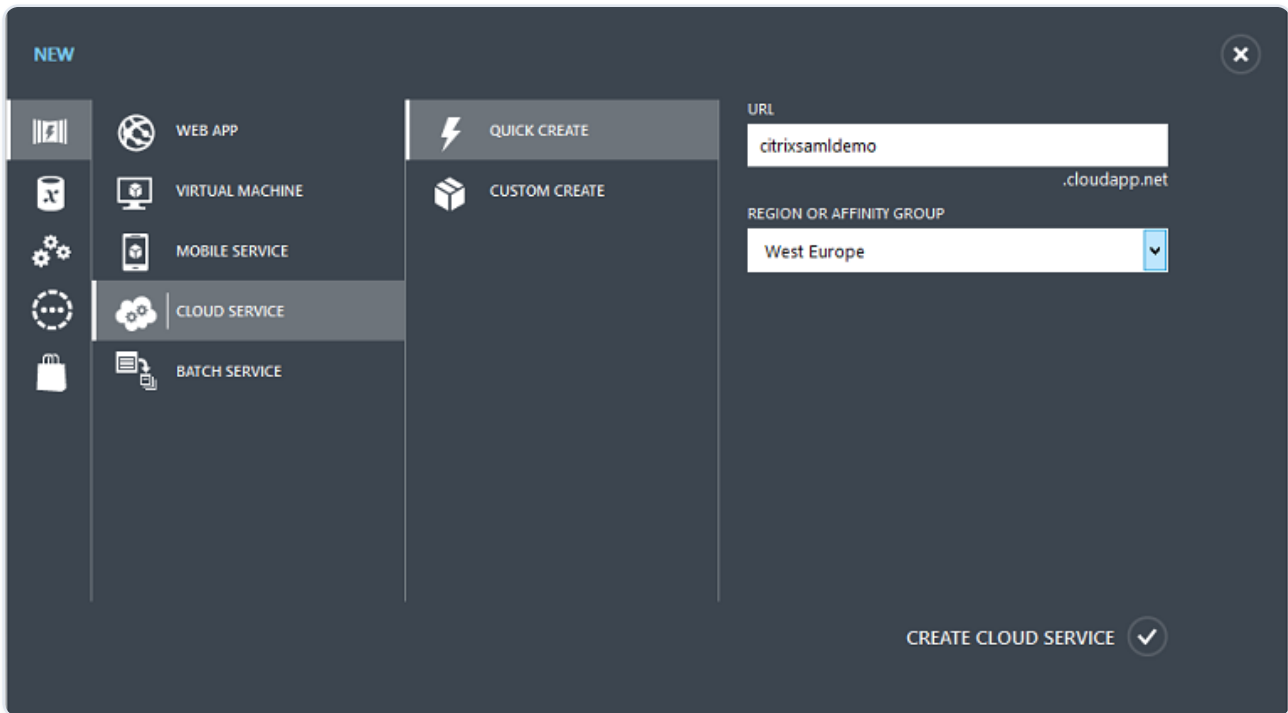
在添加对 Azure 中运行的 VM 的引用时，最简单的方法是使用 CNAME 指针指向 VM 的 Azure 管理的 DNS 记录。如果 VM 的 IP 地址发生更改，则无需手动更新 DNS 区域文件。

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。

创建云服务

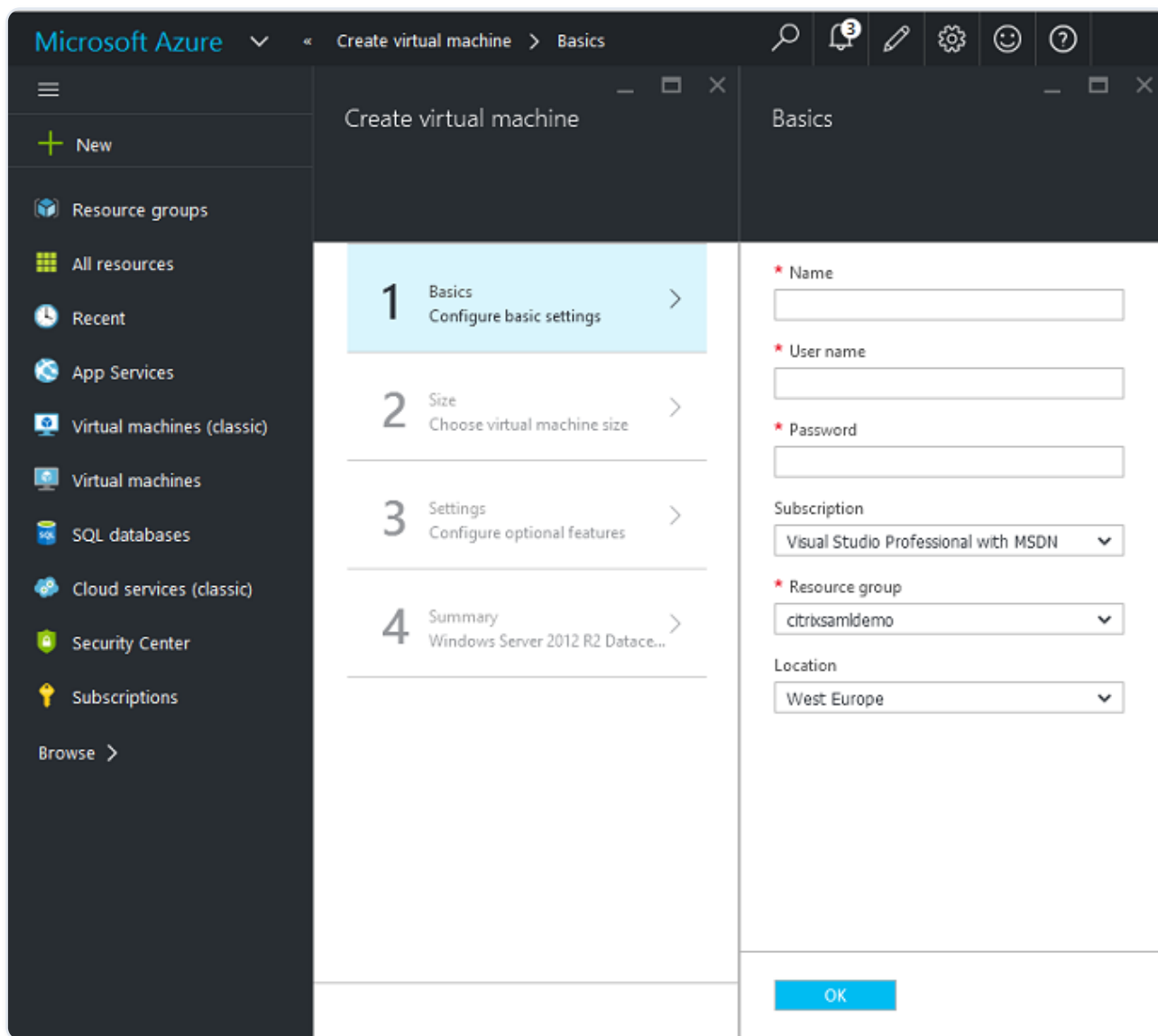
此示例配置了一个 Citrix 环境，其中包括一个在 Azure 中运行 ADFS 服务器的 AD 环境。创建了一个名为“citrixsamldemo.”的云服务。



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)



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。
- 创建一个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，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

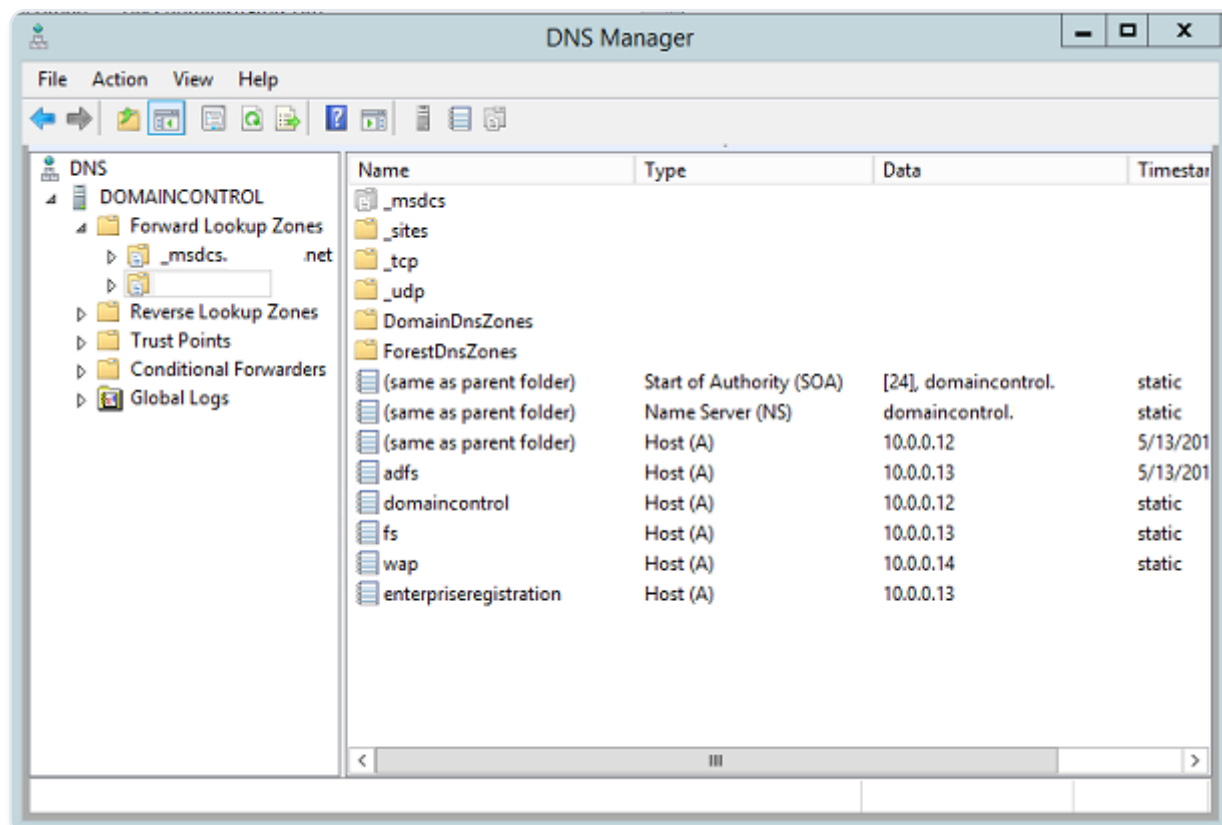
- 将 ADFS 服务器加入 citrixsamldemo 域。Web 应用程序代理服务器应保留在隔离的工作组中，因此请手动向 AD DNS 注册 DNS 地址。
- 在这些服务器上运行 **Enable-PSRemoting -Force** cmdlet，以允许 AzureAD Connect 工具通过防火墙进行 PS 远程处理。

Citrix Virtual Desktops™ 投递控制器和 VDA

- 在加入 citrixsaml demo 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

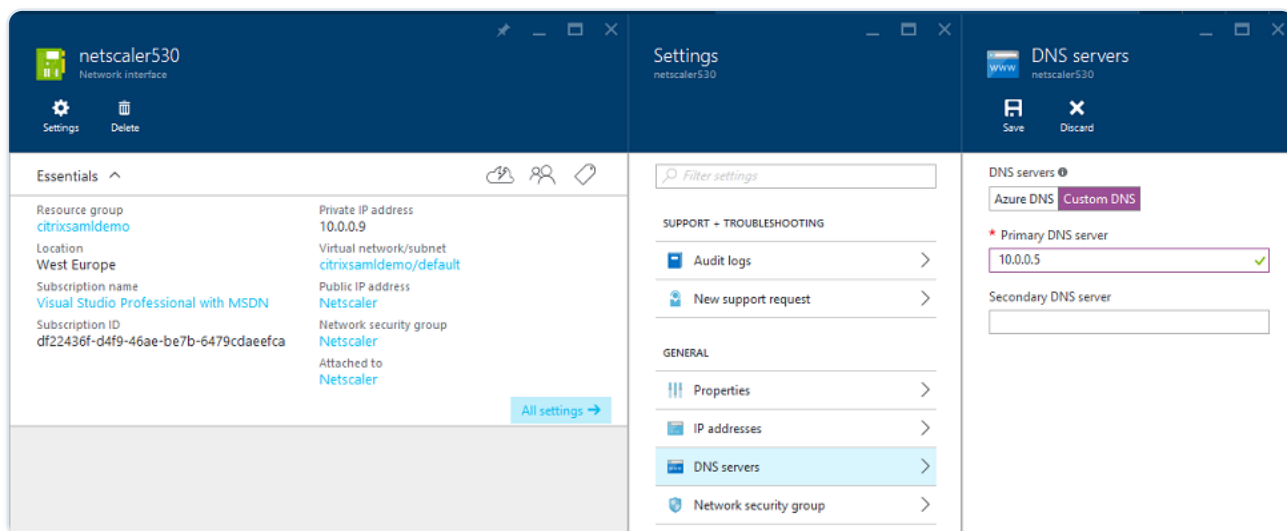
安装域控制器后，配置 DNS 服务器以处理 citrixsaml demo.net 的内部视图，并充当外部 DNS 服务器（例如：8.8.8.8）的转发器。



添加静态记录，用于：

- wap.citrixsaml demo.net
- fs.citrixsaml demo.net
- enterpriseregistration.citrixsaml.net

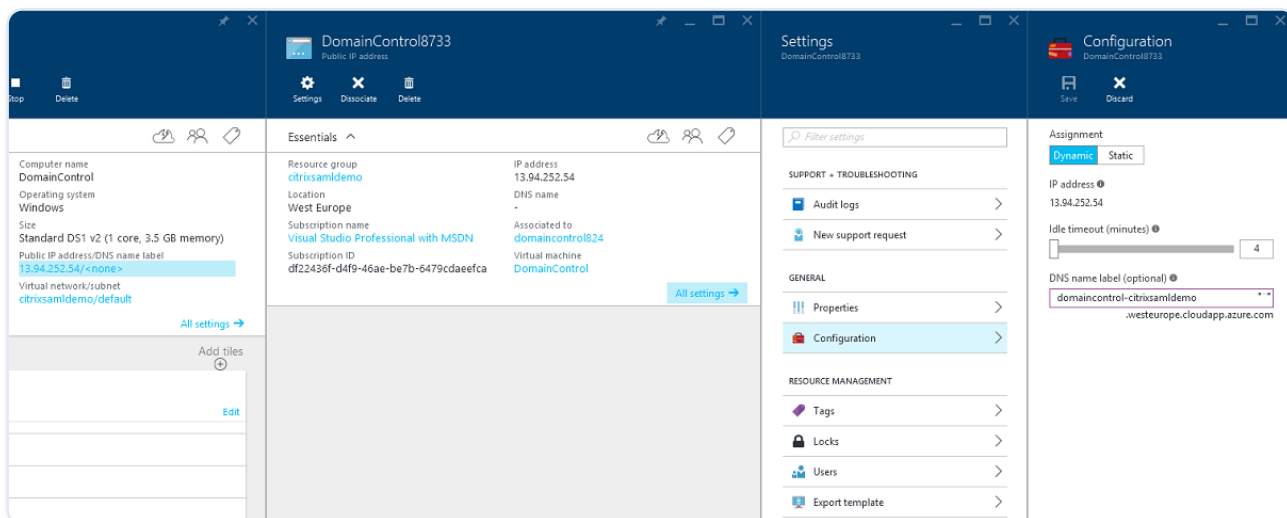
所有在 Azure 中运行的 VM 都应配置为仅使用此 DNS 服务器。您可以通过网络接口 GUI 完成此操作。



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。

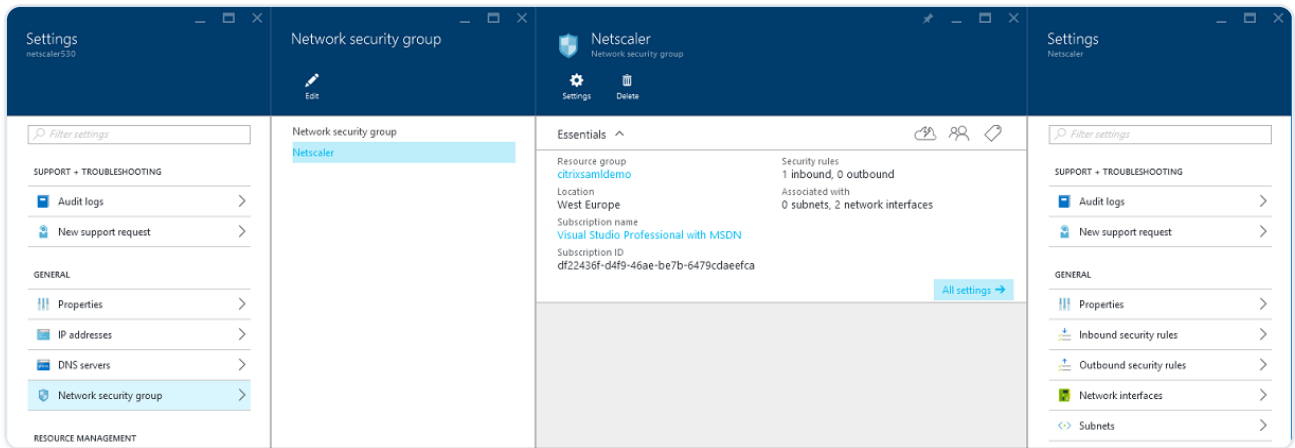


此示例将 DNS 地址 domaincontrol-citrixsaml-demo.westeurope.cloudapp.azure.com 分配给域控制器。

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 地址用于对环境进行 RDP 访问）。

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。

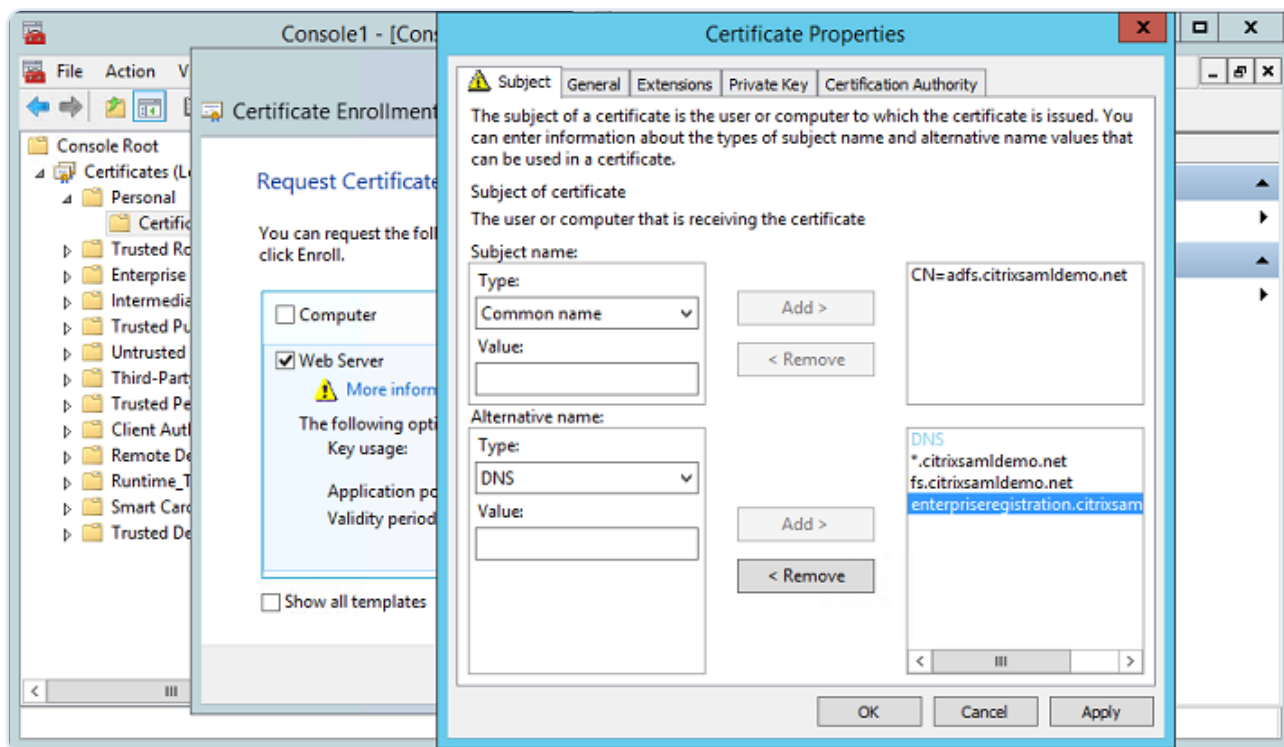


创建 ADFS 证书

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：

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



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。

DIRECTORY ACCESS CONTROL NAMESPACES MULTI-FACTOR AUTH PROVIDERS RIGHTS MANAGEN

×

Add directory

DIRECTORY ?

Create new directory

▼

NAME ?

CitrixSAMLDemo

DOMAIN NAME ?

citrixsaml demo

✓

.onmicrosoft.com

COUNTRY OR REGION ?

United Kingdom

▼

☐ This is a B2C directory. ? **PREVIEW**

✓

完成后，将显示摘要页面。

The screenshot shows the Citrix SAML Demo web application. At the top, the title 'citrixsamldemo' is displayed. Below it is a navigation bar with links: USERS, GROUPS, APPLICATIONS, DOMAINS, DIRECTORY INTEGRATION, CONFIGURE, REPORTS, and LICENSES. The main content area features a large blue hexagonal icon with a white network diagram. To the right of the icon, the text reads: 'Your directory is ready to use. Here are a few options to get started.' Below this text is a checkbox labeled 'Skip Quick Start the next time I visit'. Underneath the main content area is a section titled 'I WANT TO' with three buttons: 'Set Up Directory' (highlighted in blue), 'Manage Access', and 'Develop Applications'. Below this is a section titled 'GET STARTED' with three numbered steps: 1. 'Improve user sign-in experience' with a description and an 'Add domain' button; 2. 'Integrate with your local directory' with a description and a 'Download Azure AD Connect' link; 3. 'Get Azure AD Premium' with a description and a 'Try it now' button.

citrixsamldemo

USERS GROUPS APPLICATIONS DOMAINS DIRECTORY INTEGRATION CONFIGURE REPORTS
LICENSES

 Your directory is ready to use.
Here are a few options to get started.

☐ Skip Quick Start the next time I visit

I WANT TO **Set Up Directory** Manage Access Develop Applications

GET STARTED

- 1 Improve user sign-in experience
Add a custom domain so that your users can sign in with familiar user names. For example, if your organization owns 'contoso.com', users can sign in in Azure AD with user names such as 'joe@contoso.com'.
Add domain
- 2 Integrate with your local directory
Use the same user accounts and groups in the cloud that you already use on premises.
[Download Azure AD Connect](#)
- 3 Get Azure AD Premium
Improve access management experiences for end users and administrators, including self service password reset, group management, sign in customization, and reporting.
Try it now

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。

ADD USER

user profile

FIRST NAME: Azure

LAST NAME: Admin

DISPLAY NAME: Azure Admin

ROLE: Global Admin

ALTERNATE EMAIL ADDRESS:

MULTI-FACTOR AUTHENTICATION: ☐ Enable Multi-Factor Authentication

将您的域注册到 Azure AD

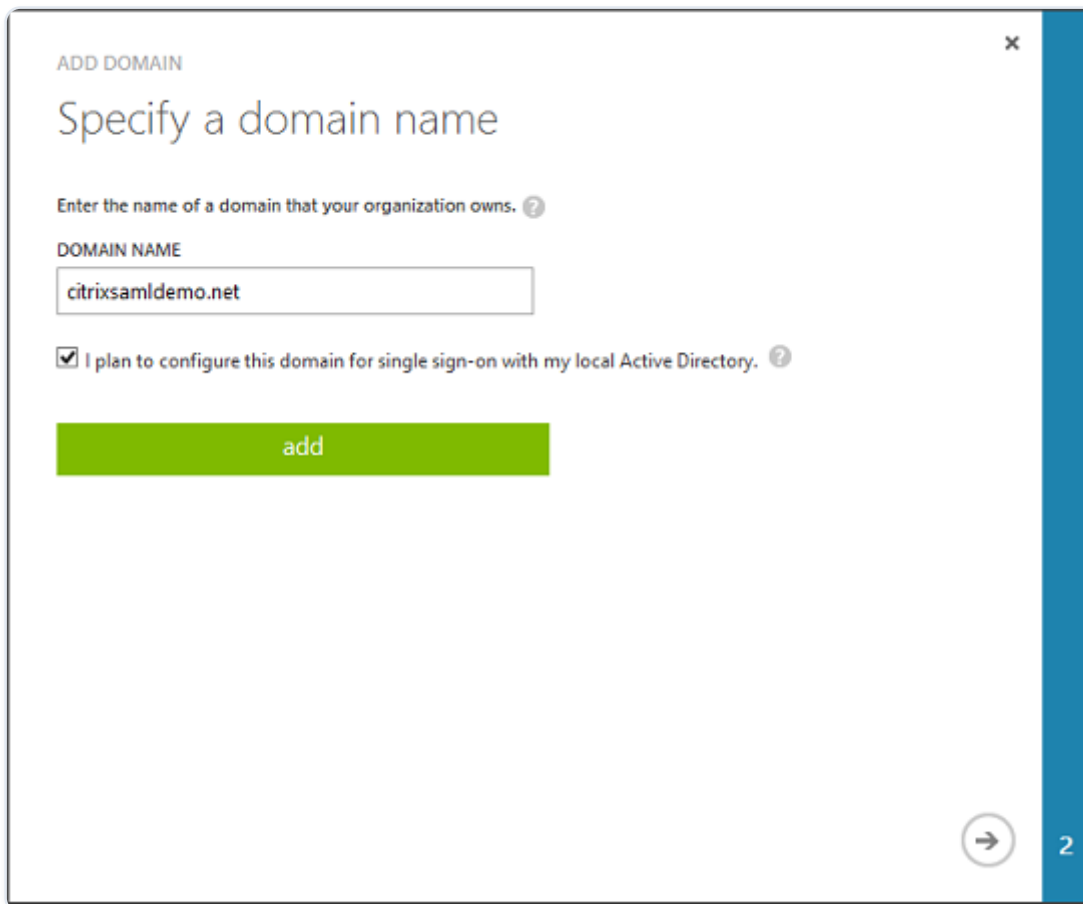
默认情况下，用户通过以下形式的电子邮件地址进行识别：

`<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地址：`<user.name>@<company>.com`。

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

如果您正在为单一登录设置 ADFS，请启用该复选框。



ADD DOMAIN

Specify a domain name

Enter the name of a domain that your organization owns. ?

DOMAIN NAME

citrixsaml-demo.net

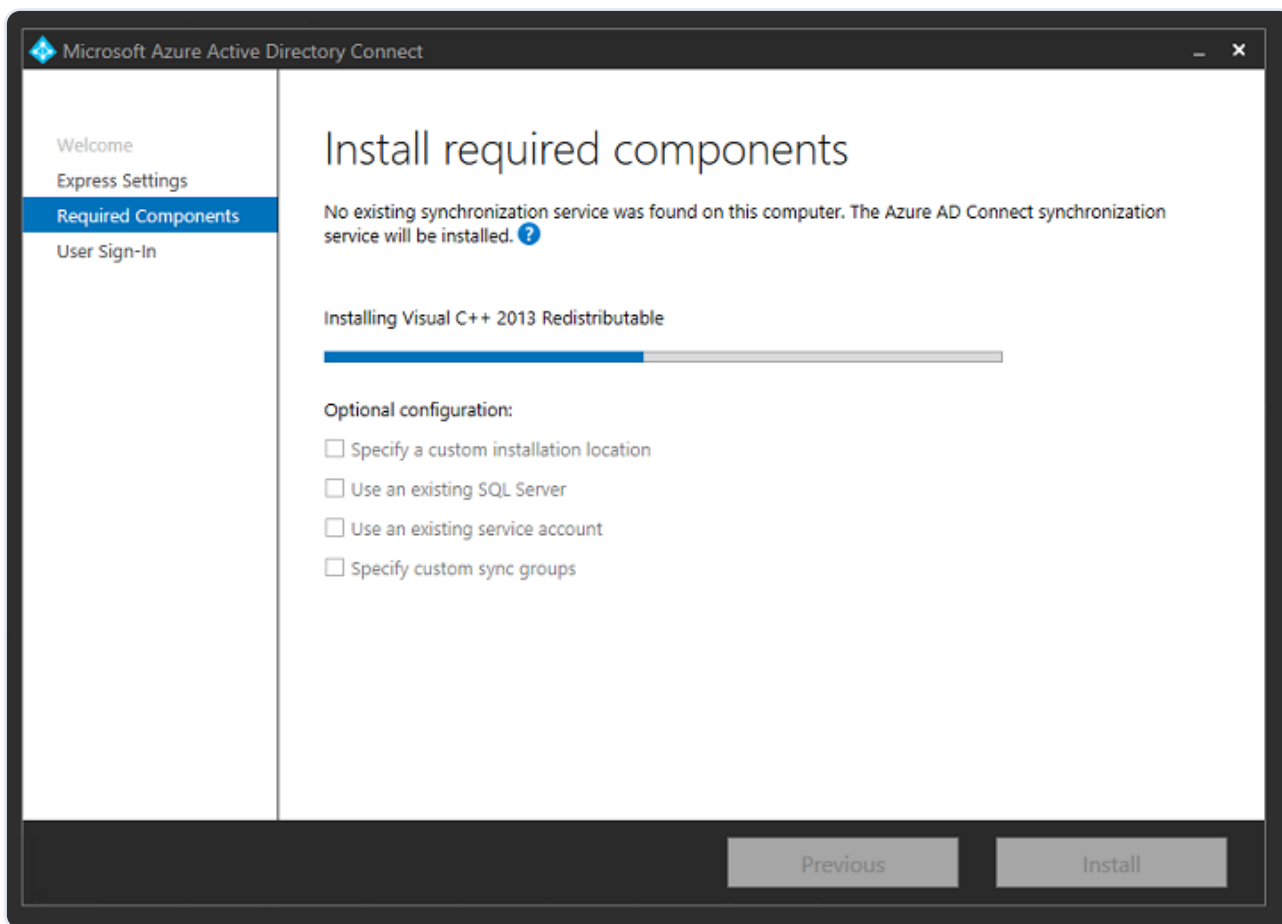
☒ I plan to configure this domain for single sign-on with my local Active Directory. ?

add

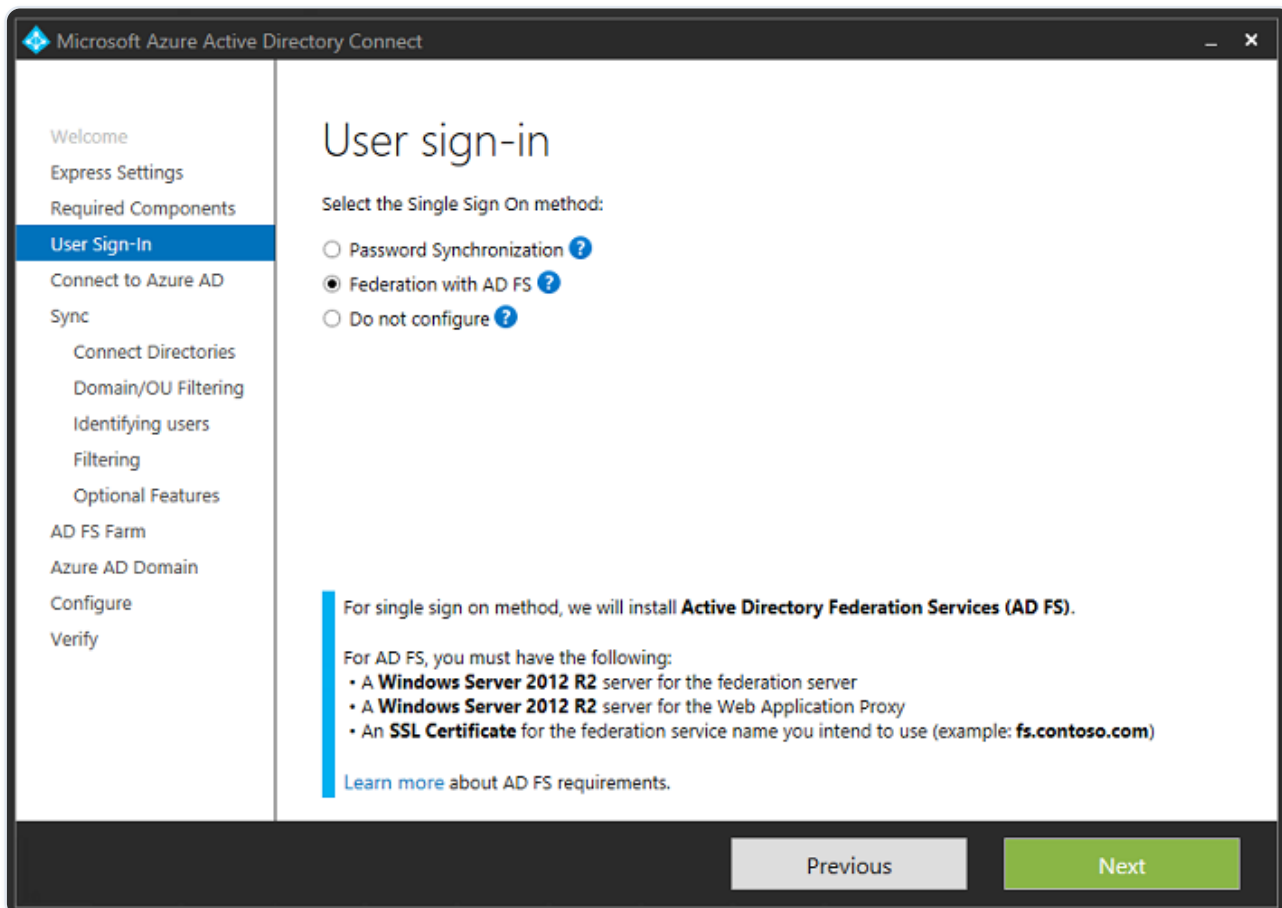
2

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。将其安装在 ADFS VM 上。使用“自定义安装”而不是“快速设置”，以便 ADFS 选项可用。



选择“与 AD FS 联合”单一登录选项。



使用您之前创建的管理员帐户连接到 Azure。

Microsoft Azure Active Directory Connect

Welcome

Express Settings

Required Components

User Sign-In

Connect to Azure AD

Sync

- Connect Directories
- Azure AD sign-in
- Domain/OU Filtering
- Identifying users
- Filtering
- Optional Features

AD FS Farm

Azure AD Domain

Configure

Verify

Connect to Azure AD

Enter your Azure AD credentials: ?

USERNAME

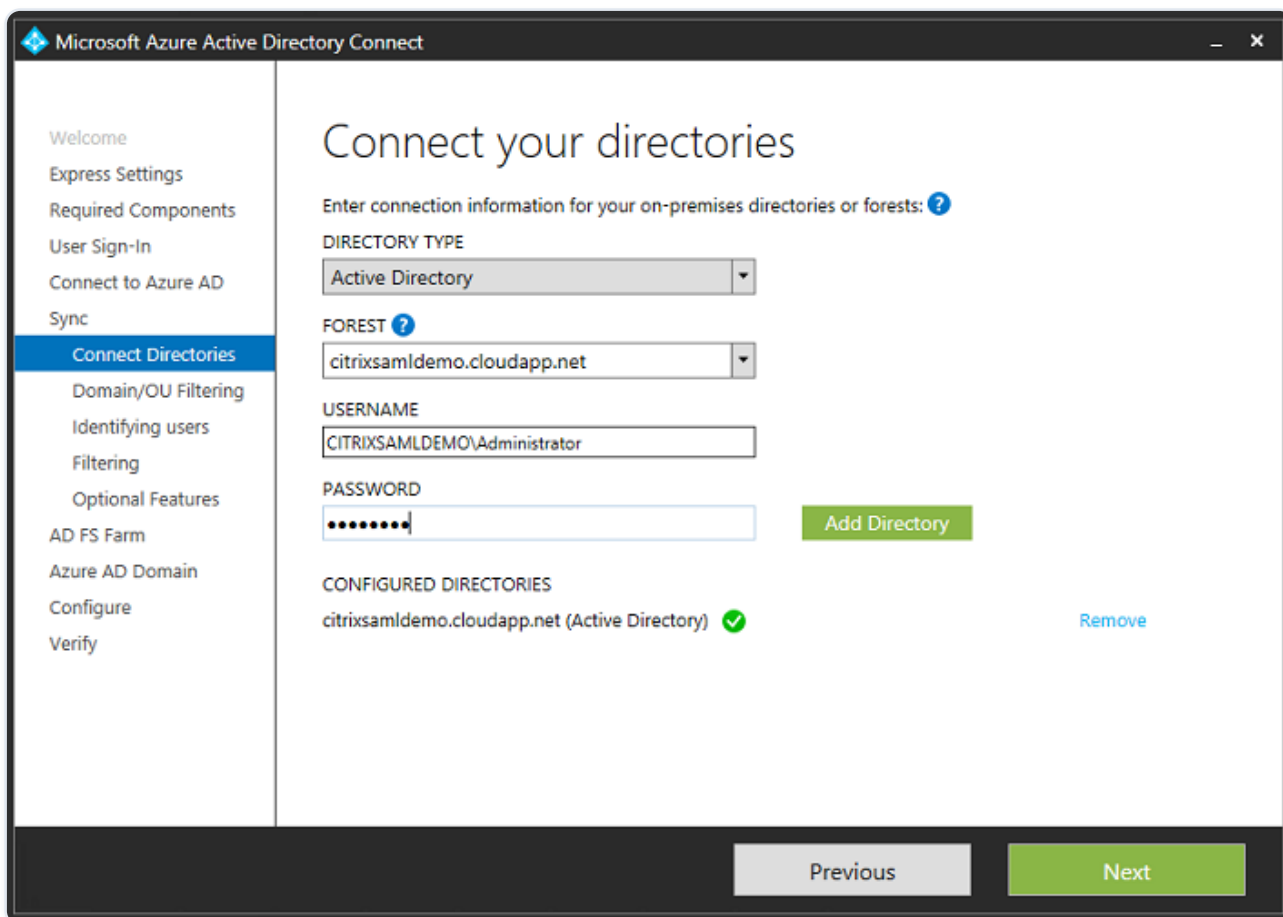
AzureAdmin@citrixsaml-demo.onmicrosoft.com

PASSWORD

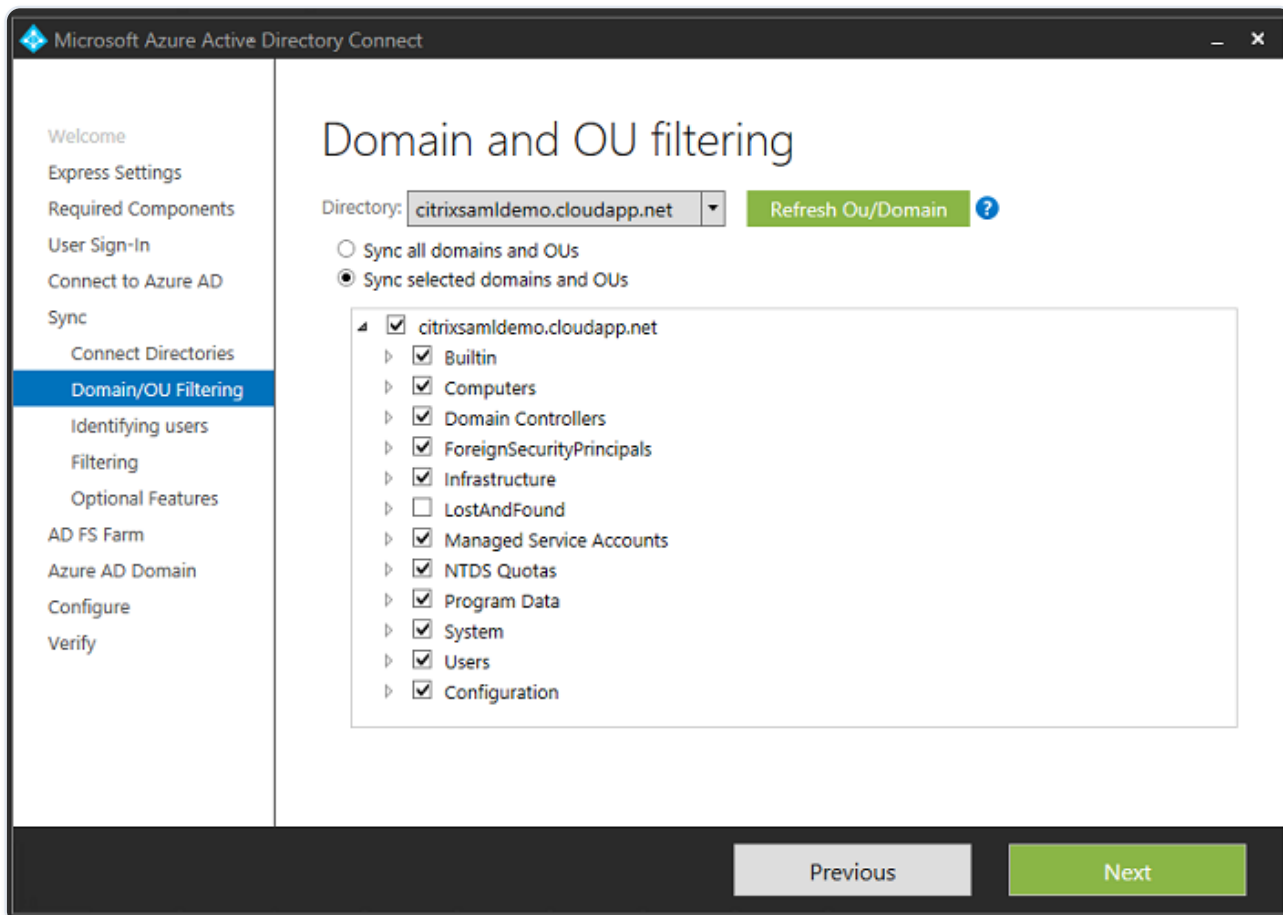
.....

Previous Next

选择内部 AD 林。



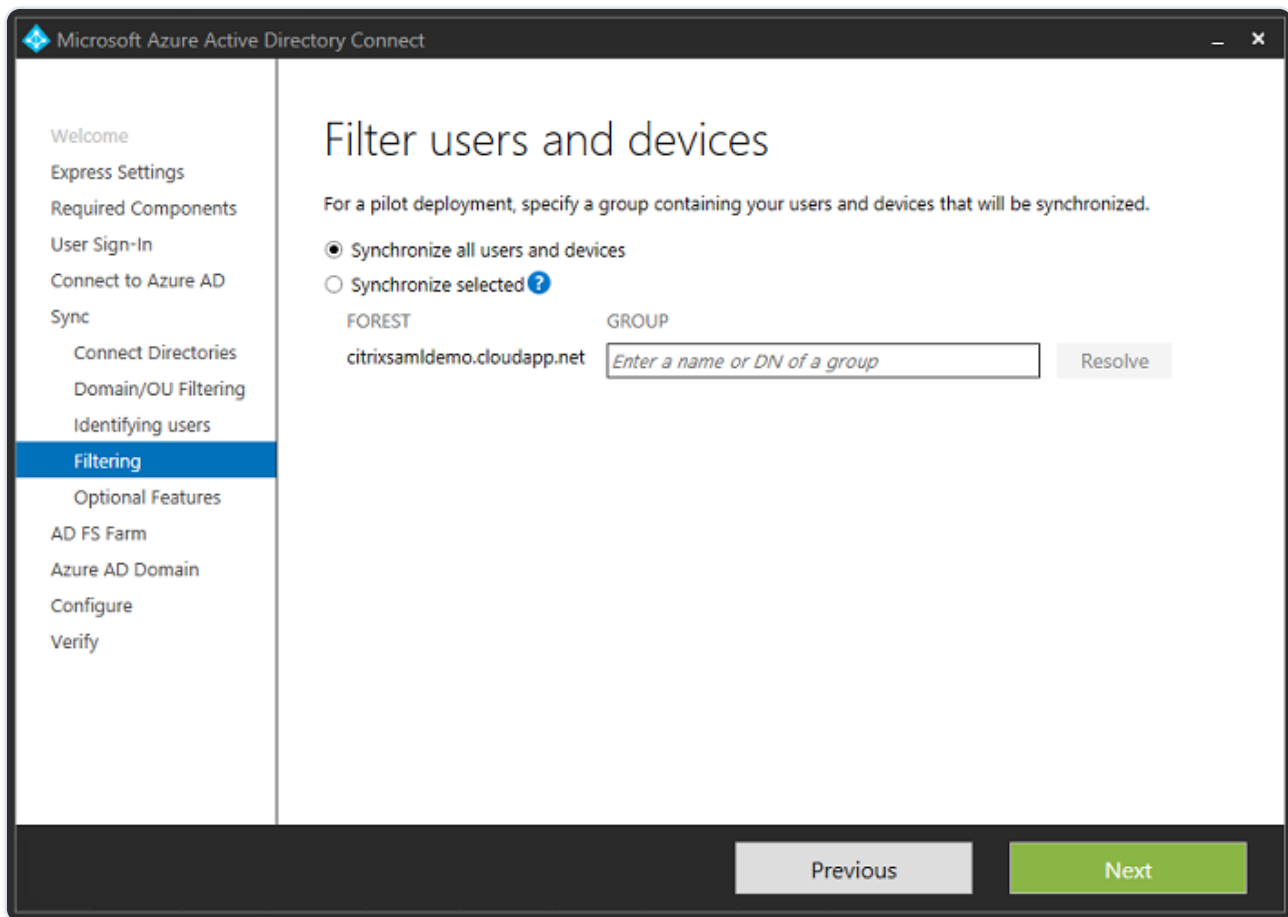
将所有旧版 Active Directory 对象与 Azure AD 同步。



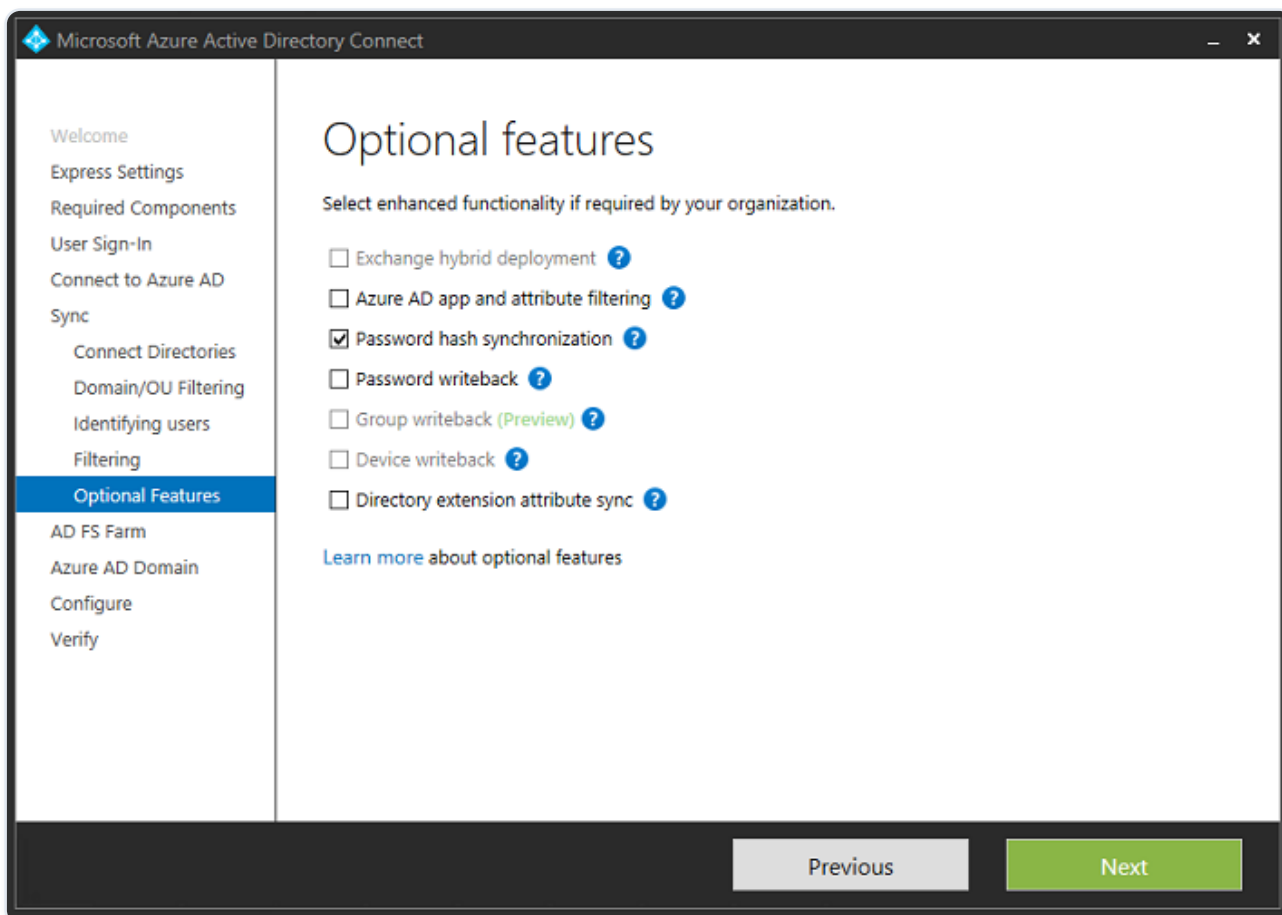
如果目录结构简单，您可以依靠足够唯一的用户名为登录用户进行身份识别。

The screenshot shows the 'Uniquely identifying your users' step in the Microsoft Azure Active Directory Connect wizard. The left sidebar contains a navigation menu with the following items: Welcome, Express Settings, Required Components, User Sign-In, Connect to Azure AD, Sync, Connect Directories, Domain/OU Filtering, **Identifying users** (highlighted), Filtering, Optional Features, AD FS Farm, Azure AD Domain, Configure, and Verify. The main content area is titled 'Uniquely identifying your users' and includes the instruction 'Select how users should be identified in your on-premises directories.' with a help icon. There are two radio button options: 'Users are represented only once across all directories.' (selected) and 'User identities exist across multiple directories. Match using:'. Under the second option, there are three radio buttons: 'Mail attribute', 'ObjectSID and msExchMasterAccountSID/msRTCSIP-OriginatorSID attributes', 'SAMAccountName and MailNickName attributes', and 'A specific attribute'. Below these is a 'CUSTOM ATTRIBUTE' label and a text input field. Further down, the instruction 'Select how users should be identified with Azure AD.' is followed by two dropdown menus: 'SOURCE ANCHOR' (set to 'objectGUID') and 'USER PRINCIPAL NAME' (set to 'userPrincipalName'). At the bottom right, there are 'Previous' and 'Next' buttons.

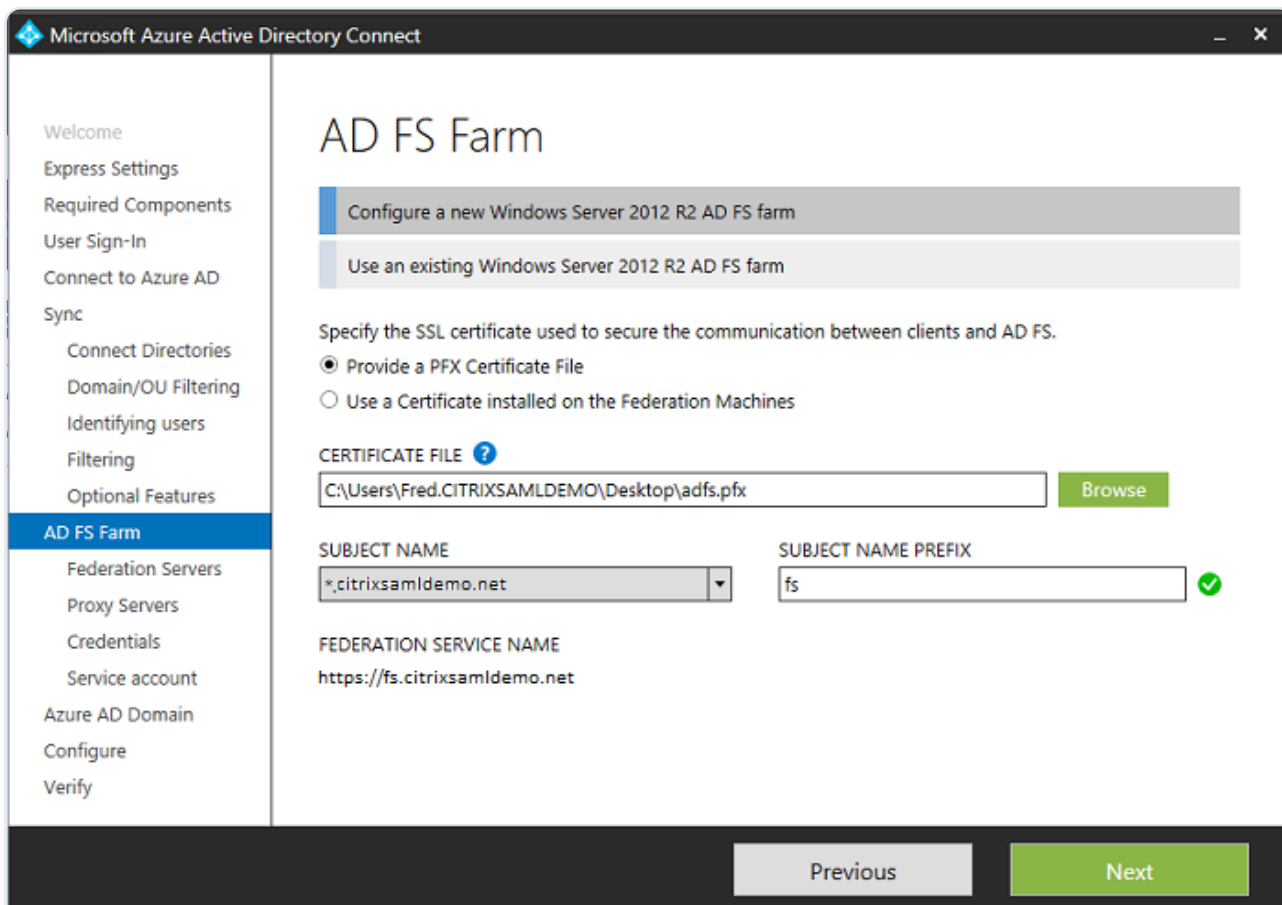
接受默认筛选选项，或将用户和设备限制到特定的组。



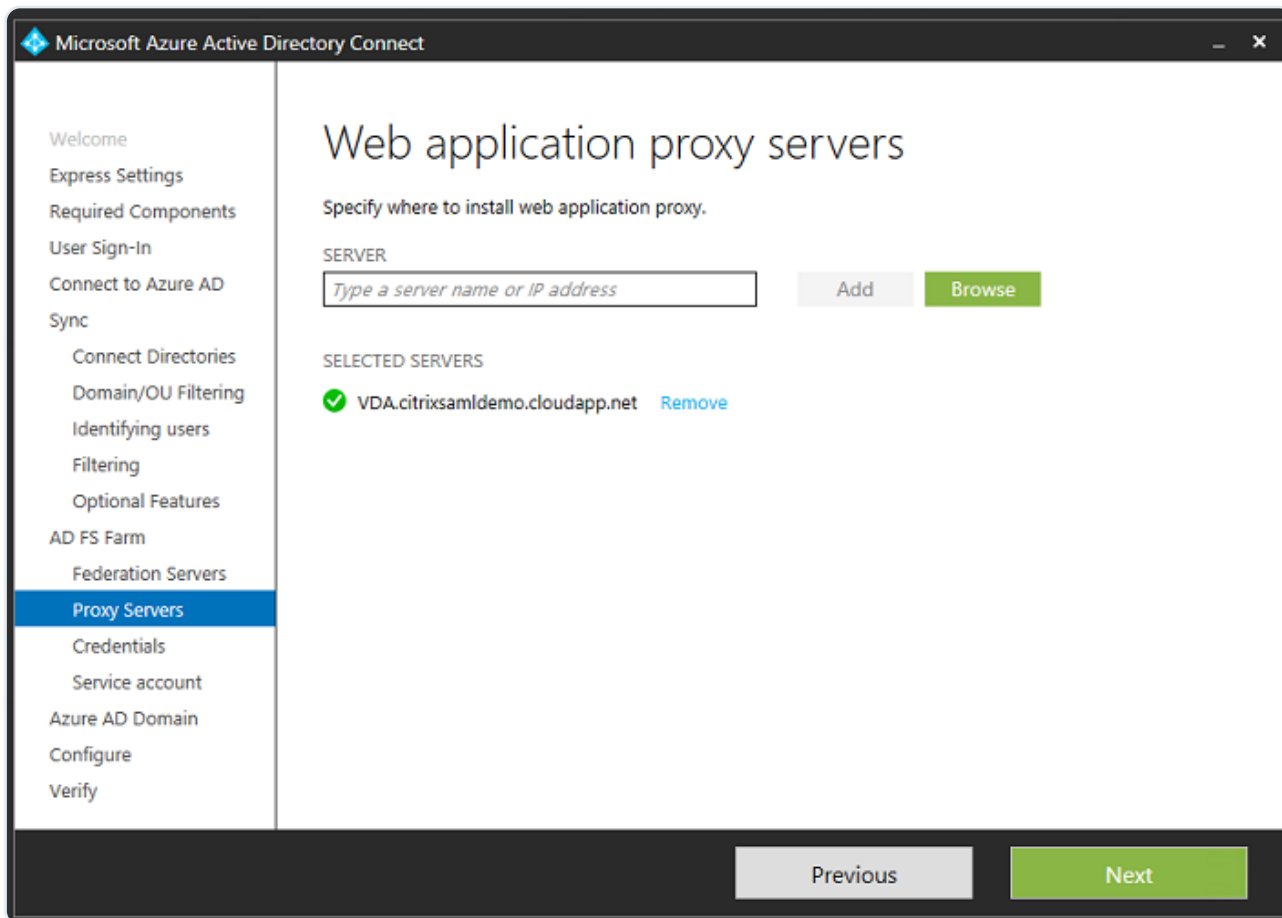
如果需要，您可以将 Azure AD 密码与 Active Directory 同步。对于基于 ADFS 的身份验证，通常不需要这样做。



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。



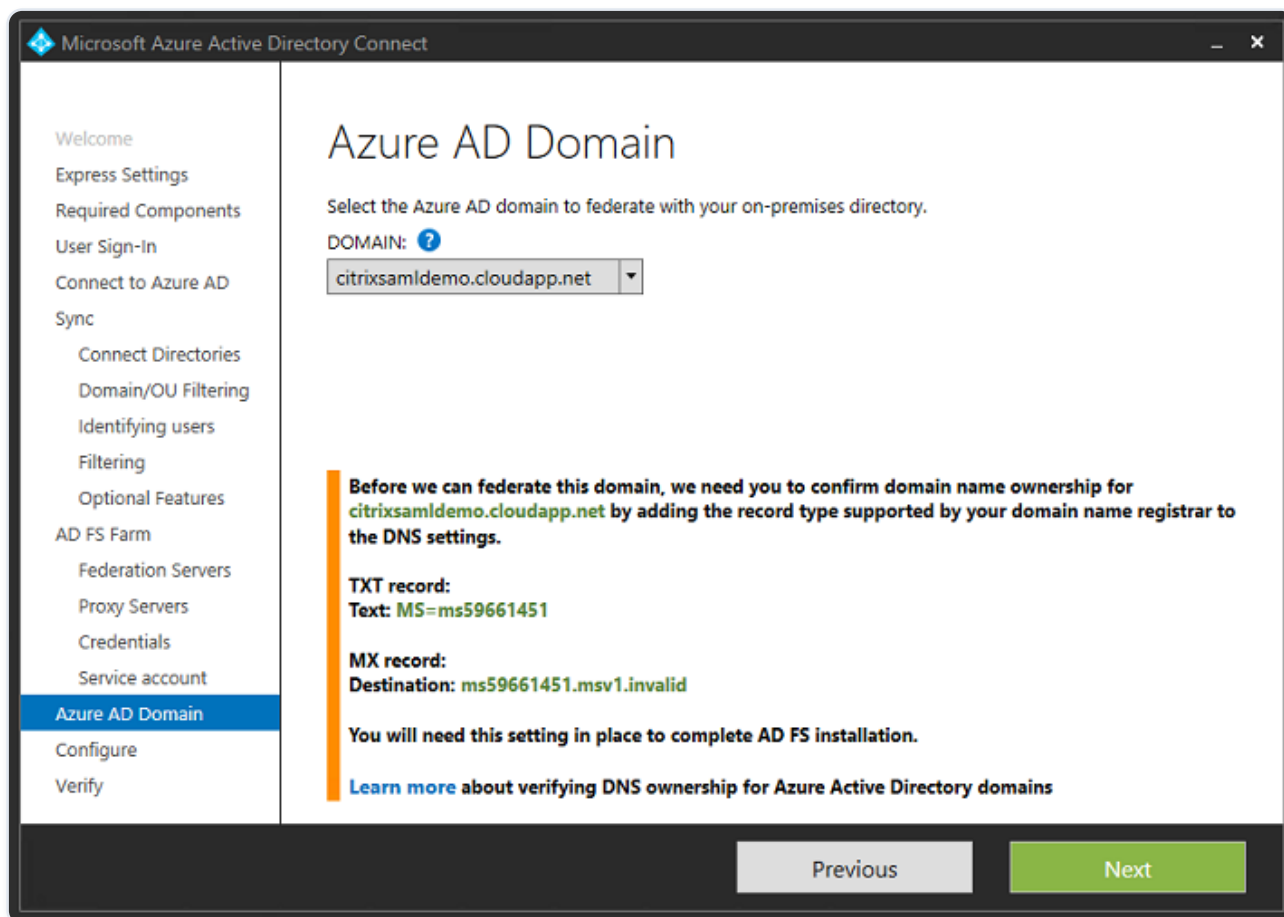
当系统提示选择代理服务器时，输入 wap.citrixsamldemo.net 服务器的地址。您可能需要在 Web Application Proxy 服务器上以管理员身份运行 **Enable-PSRemoting -Force** cmdlet，以便 Azure AD Connect 可以对其进行配置。



注意：

如果此步骤因 Remote PowerShell 信任问题而失败，请尝试将 Web Application Proxy 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。



将 TXT 和 MX 记录添加到 Azure 中的 DNS 地址记录。

Search record sets			
NAME	TYPE	TTL	VALUE
@	NS	172800	ns1-01.azure-dns.com, ns2-01.azure-dns.net, ns3-01.azure-dns.org, ns4-01.azure-dns.info. ...
@	SOA	3600	Email: azuredns-hostmaster.microsoft..., Host: ns1-01.azure-dns.com, Refresh: 3600 Retry: 300 Expire: 2419200 Minimum TTL: 300 ...
@	TXT	3600	ms70102213 ...
fs	CNAME	3600	adfs-citrixsamldemo.westeurope.cloud... ...

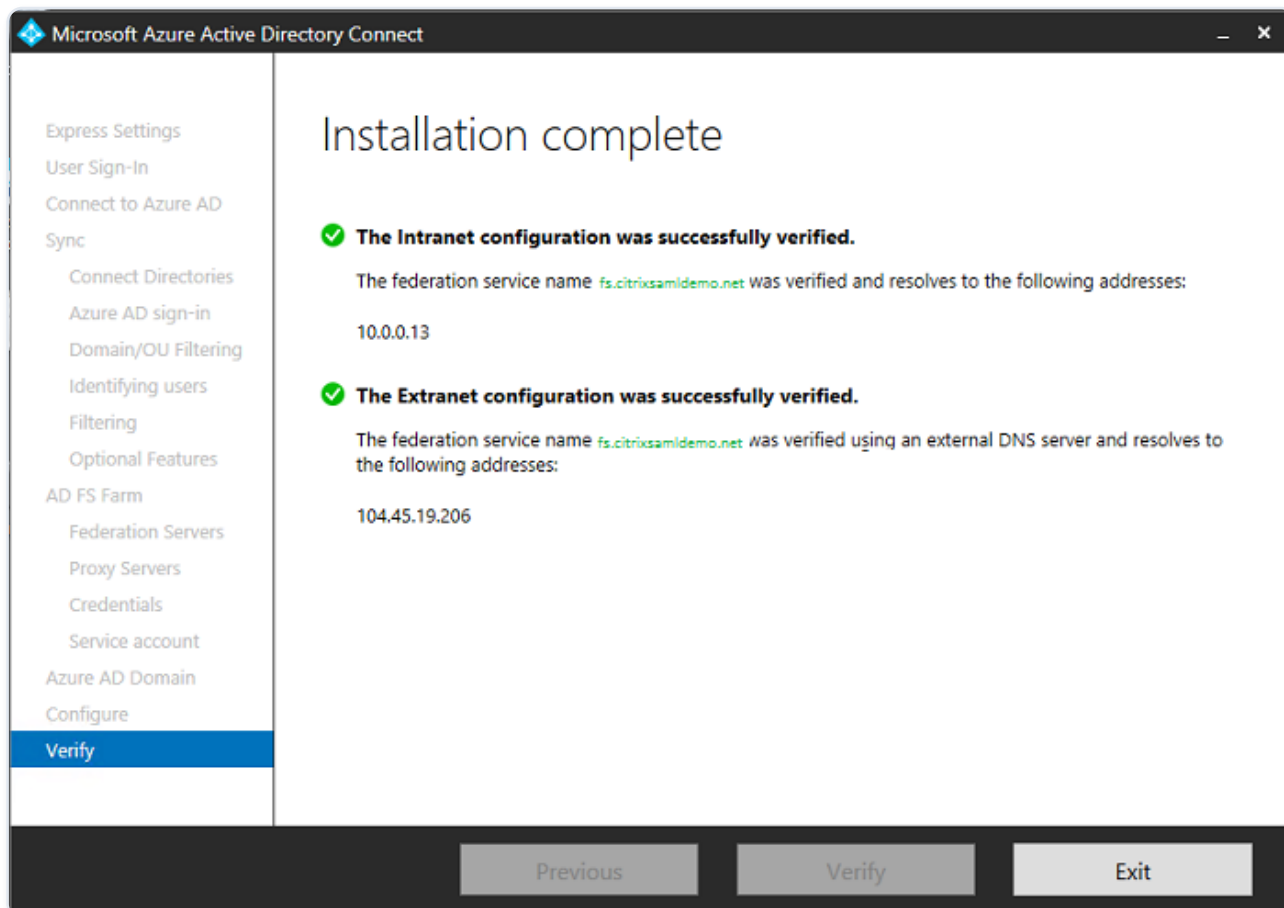
在 Azure 管理控制台中点击 验证。

CitrixSamIDemo					
	USERS	GROUPS	APPLICATIONS	DOMAINS	DIRECTORY INTEGRATION
	CONFIGURE	REPORTS	LICENSES		
DOMAIN NAME	TYPE	STATUS	SINGLE SIGN-ON	PRIMARY DOMAIN	
citrixsamldemo.onmicrosoft.com	Basic	✓ Active	Not Available	Yes	
citrixsamldemo.net	Custom	⚠ Unverified	Not Configured	No	

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 port 443 联系外部地址 fs.citrixsaml demo.net。

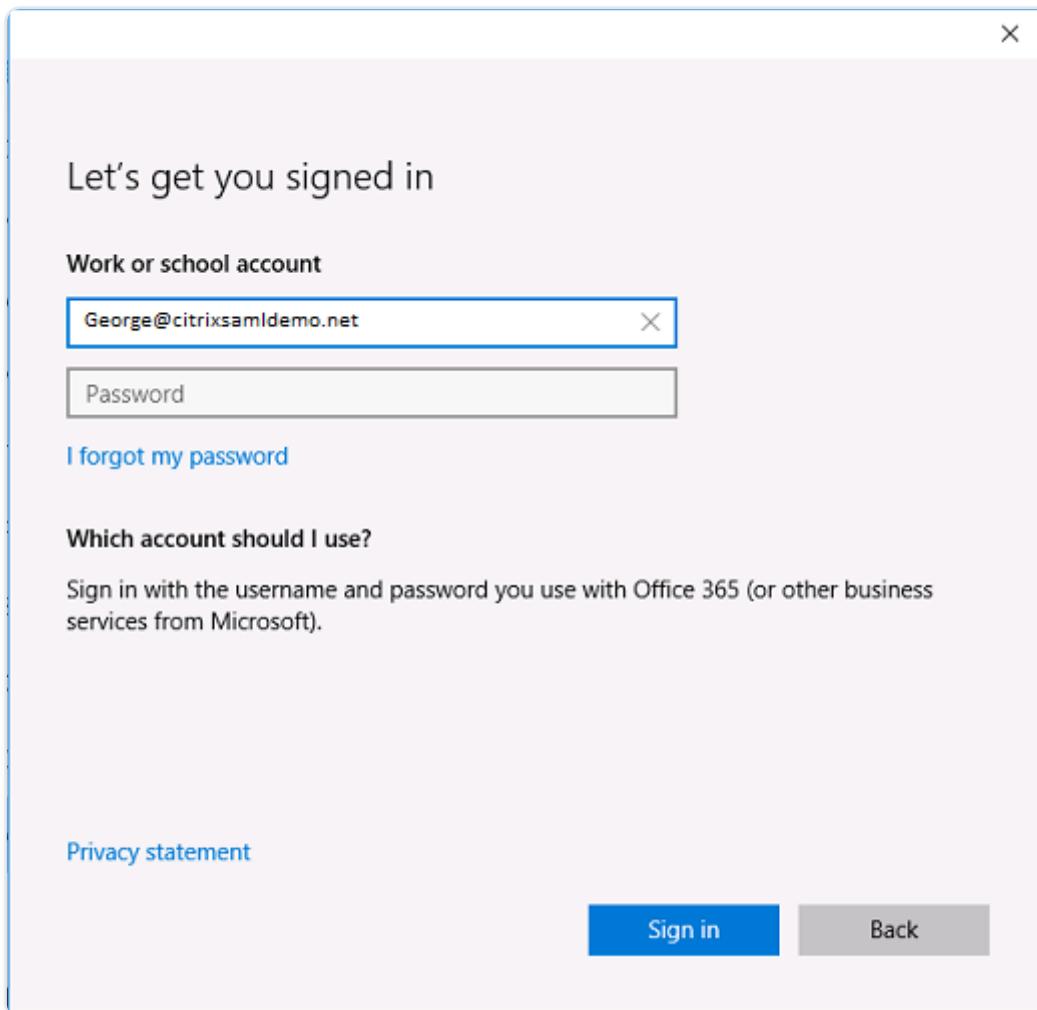


启用 Azure AD Join

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 后缀用于构建一个 CNAME DNS 记录，该记录应指向 ADFS: enterpriseregistration.\<upnsuffix>。

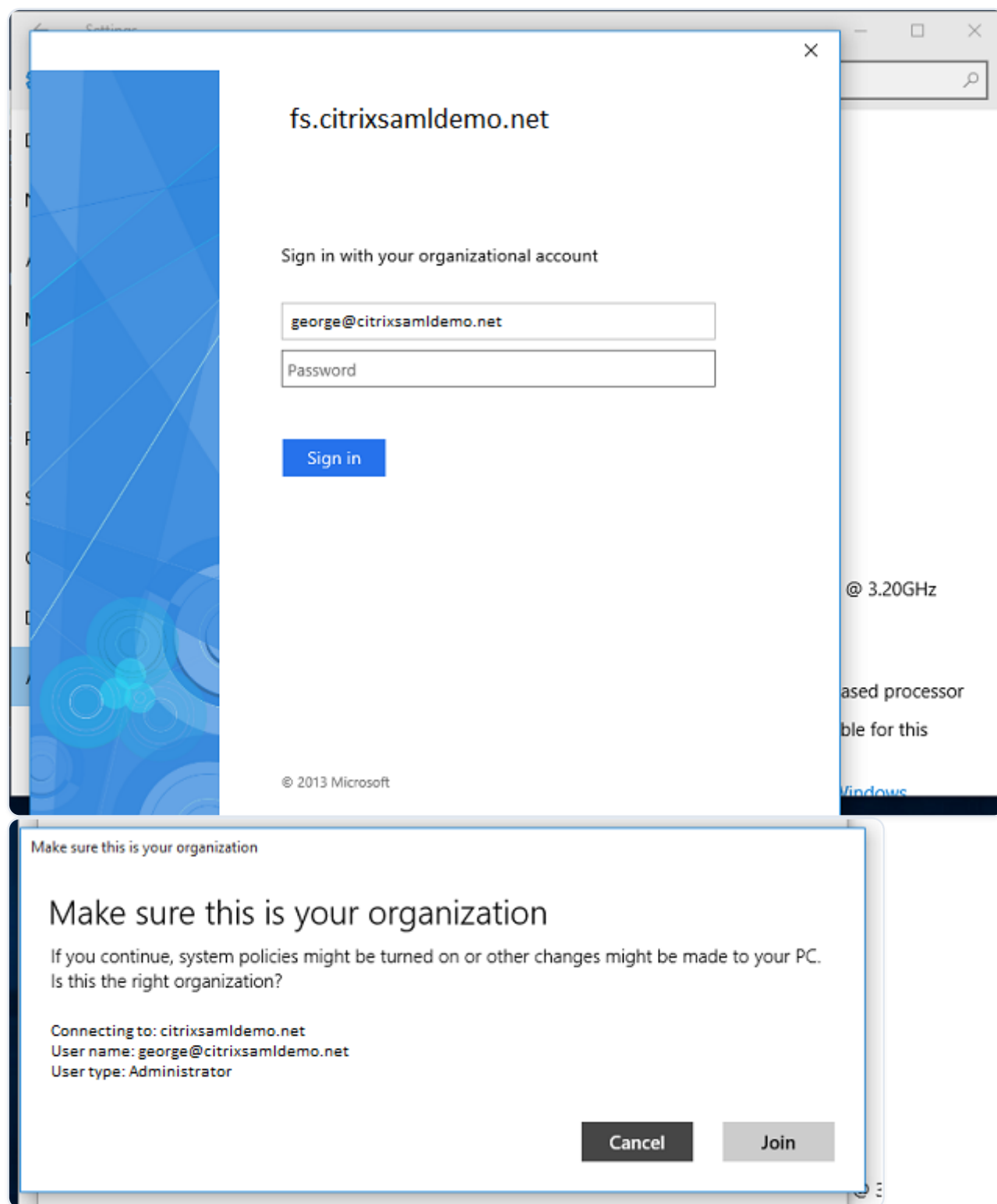
在此示例中，这是 fs.citrixsaml demo.net 。

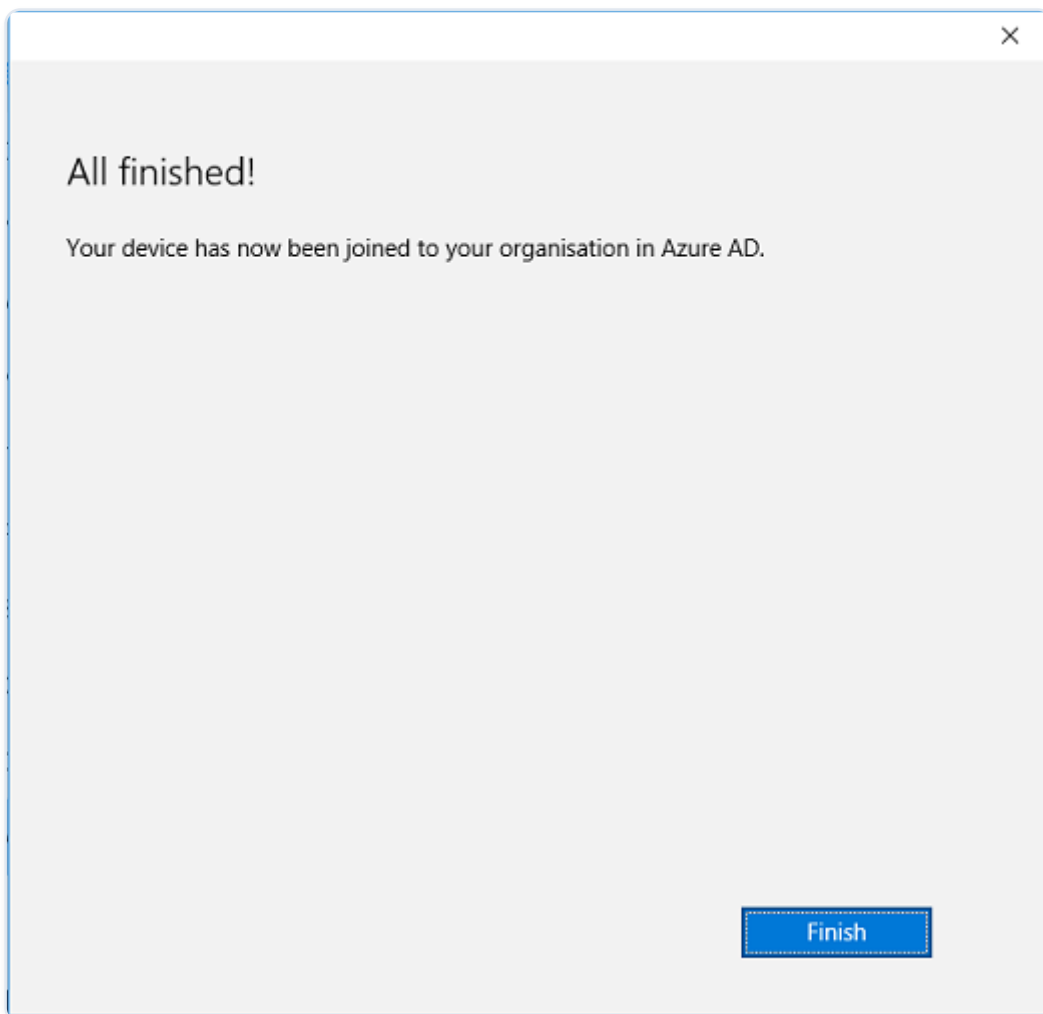
如果您未使用公共证书颁发机构，请确保 ADFS 根证书已安装在 Windows 10 计算机上，以便 Windows 信任 ADFS 服务器。使用之前生成的标准用户帐户执行 Azure AD 域加入。



The screenshot shows a Windows login window titled "Let's get you signed in". It is for a "Work or school account". The username field contains "George@citrixsamldemo.net" and the password field is labeled "Password". There is a link "I forgot my password". Below the password field, it asks "Which account should I use?" and provides instructions: "Sign in with the username and password you use with Office 365 (or other business services from Microsoft)." At the bottom, there is a link "Privacy statement" and two buttons: "Sign in" and "Back".

请注意，UPN 必须与 ADFS 域控制器识别的 UPN 匹配。



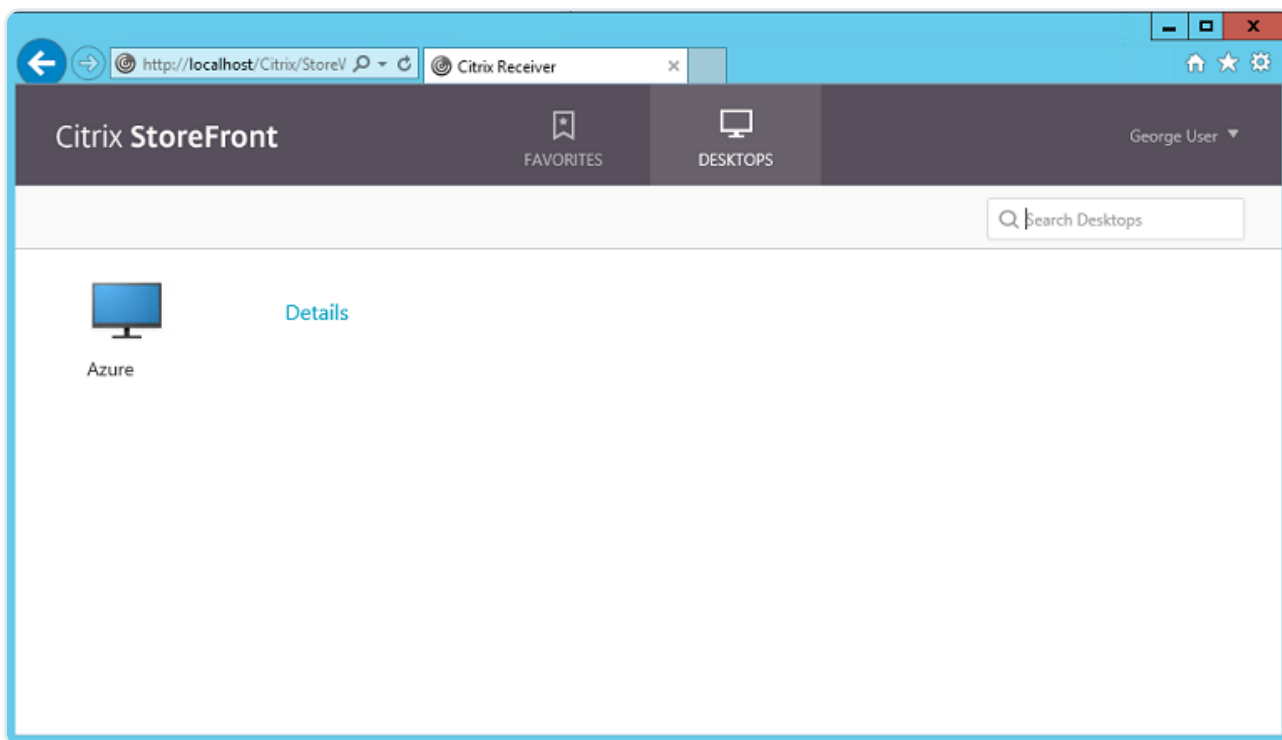


通过重启计算机并使用用户的电子邮件地址登录来验证 Azure AD 加入是否成功。登录后，启动 Microsoft Edge 并连接到 [<http://myapps.microsoft.com>](http://myapps.microsoft.com)。该网站应自动使用单点登录。

安装 Citrix 虚拟应用 或 Citrix 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。



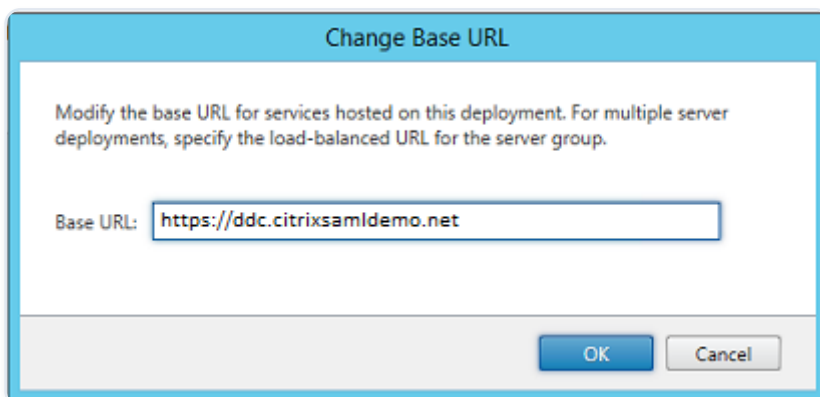
在 Controller 上运行 **Set-BrokerSite -TrustRequestsSentToTheXmlServicePort \$true** PowerShell cmdlet，以允许 StoreFront™ 在没有用户凭据的情况下进行身份验证。

安装联合身份验证服务

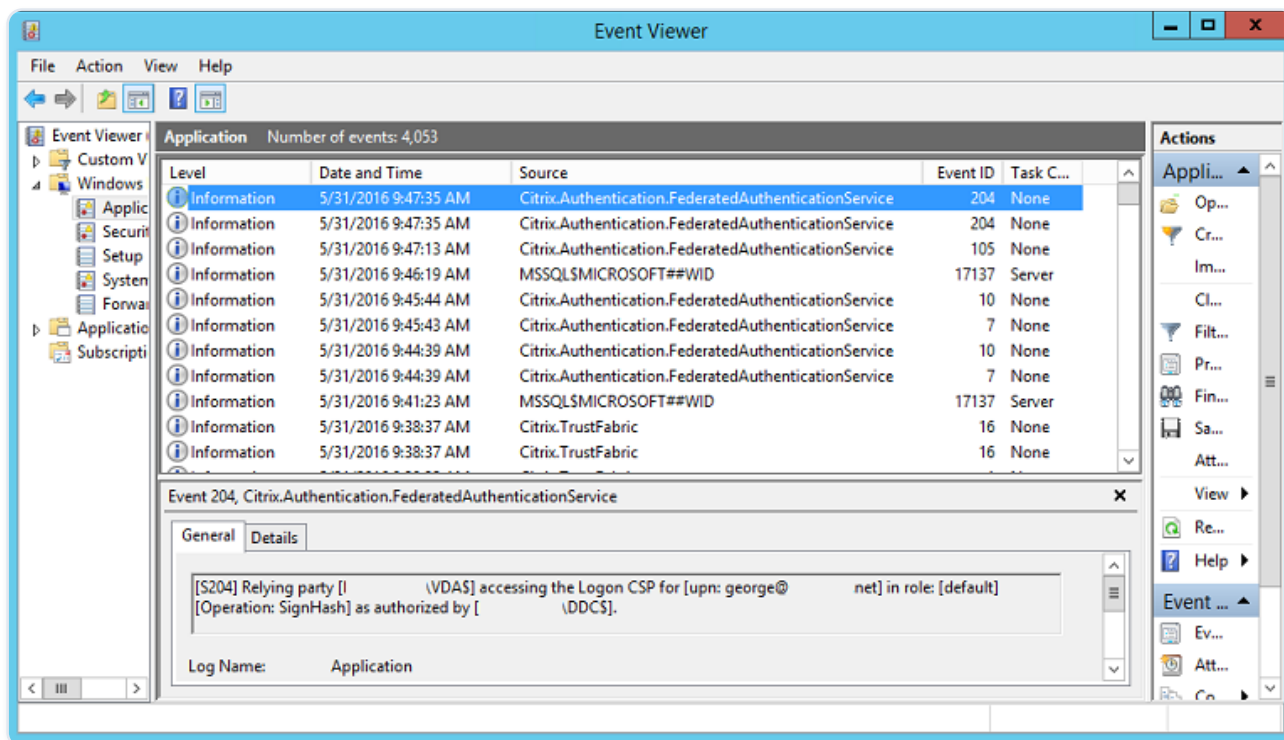
在 ADFS 服务器上安装 FAS，并为 Delivery Controller 配置一个规则，使其充当受信任的 StoreFront（因为在此示例中，StoreFront 与 Delivery Controller 安装在同一 VM 上）。请参阅[安装和配置](#)。

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。

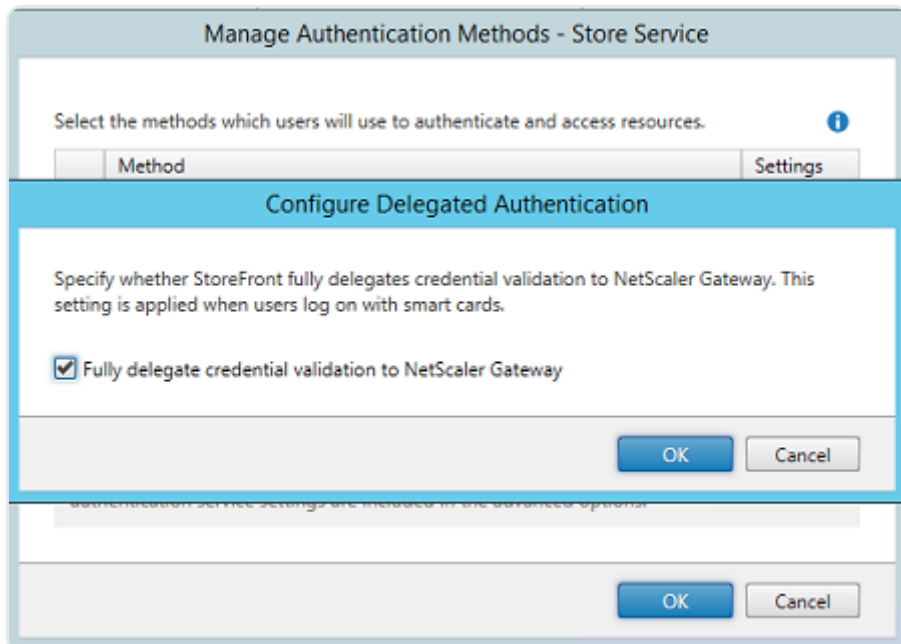


配置 StoreFront 以使用 FAS 服务器（使用[安装和配置](#)中的 PowerShell 脚本），并在 Azure 内部进行测试，通过检查 FAS 服务器上的事件查看器来确保登录使用 FAS。

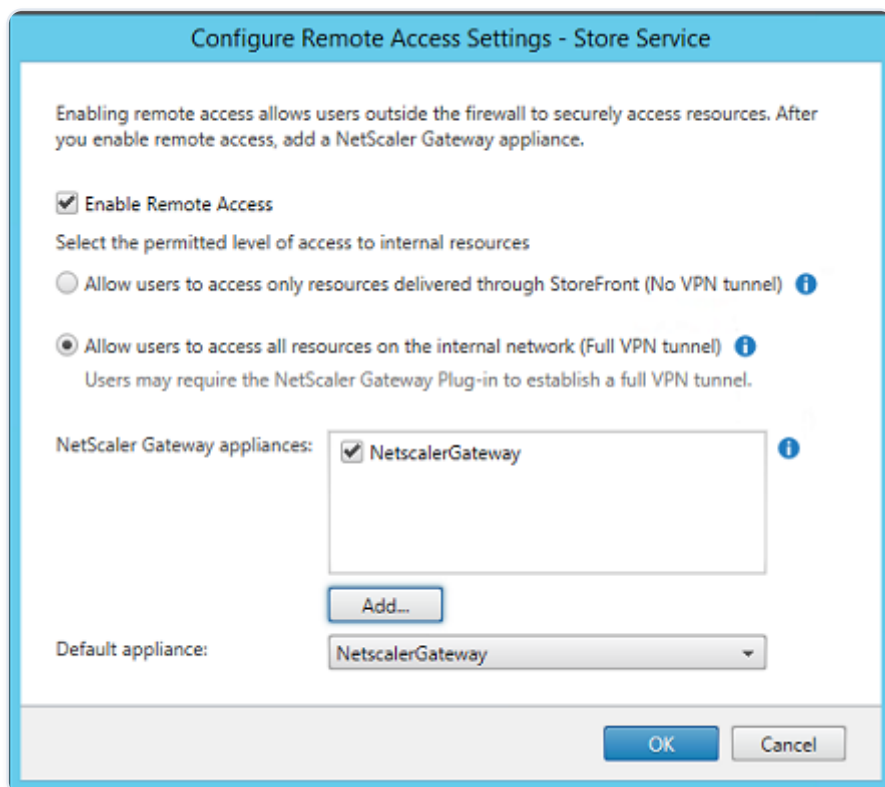


配置 StoreFront 以使用 Citrix Gateway

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。

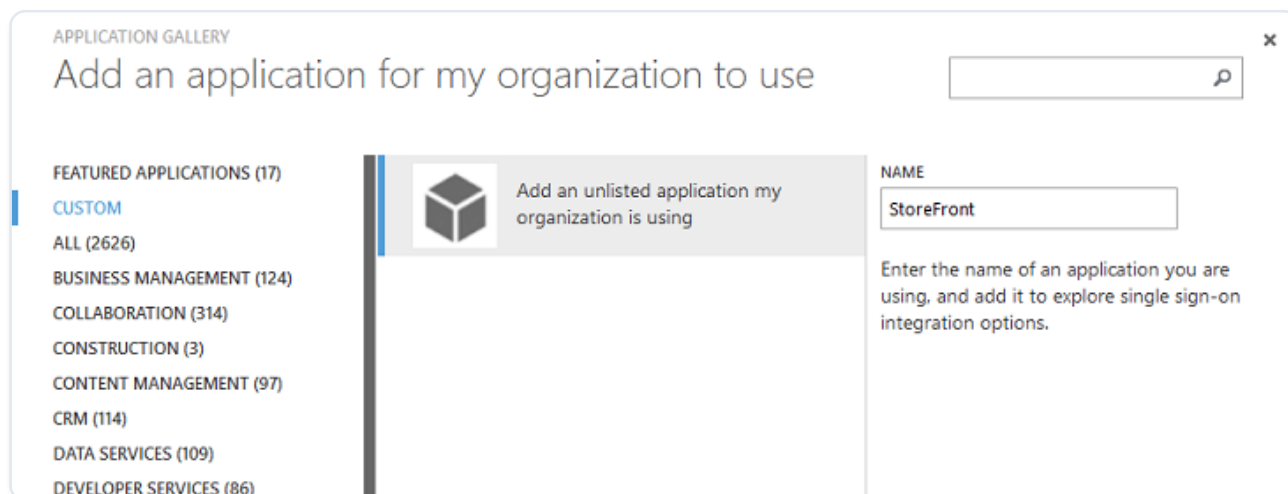


要集成 Citrix Gateway 身份验证选项，请配置安全票证颁发机构 (STA) 并配置 Citrix Gateway 地址。



为 StoreFront 的单点登录配置新的 Azure AD 应用程序

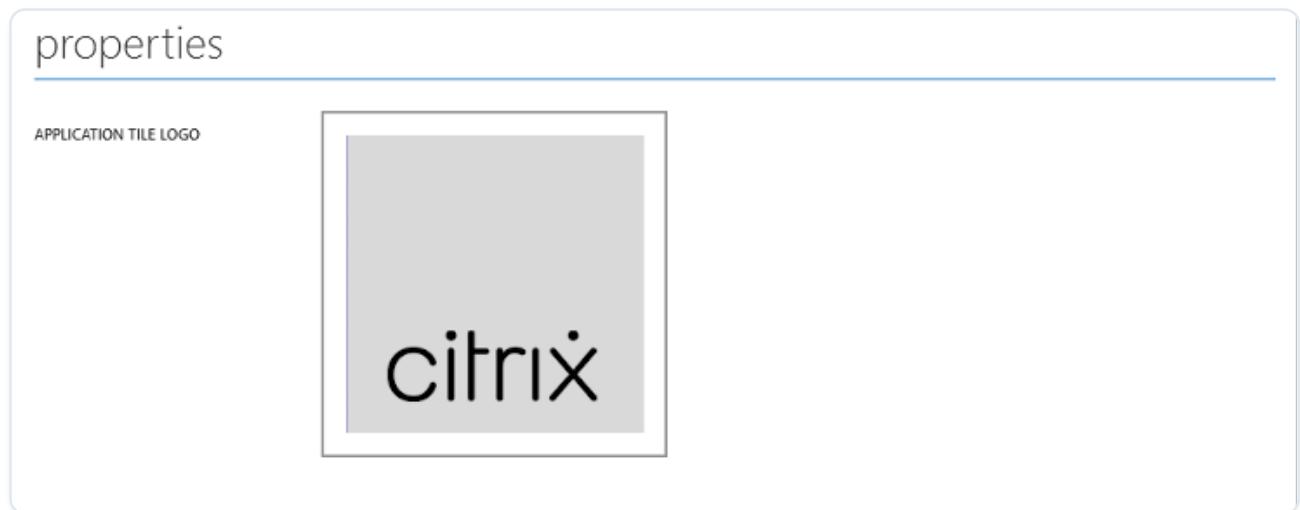
本节使用 Azure AD SAML 2.0 单点登录功能，该功能目前需要 Azure Active Directory Premium 订阅。在 Azure AD 管理工具中，选择**新建应用程序**，然后选择**从库中添加应用程序**。



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。

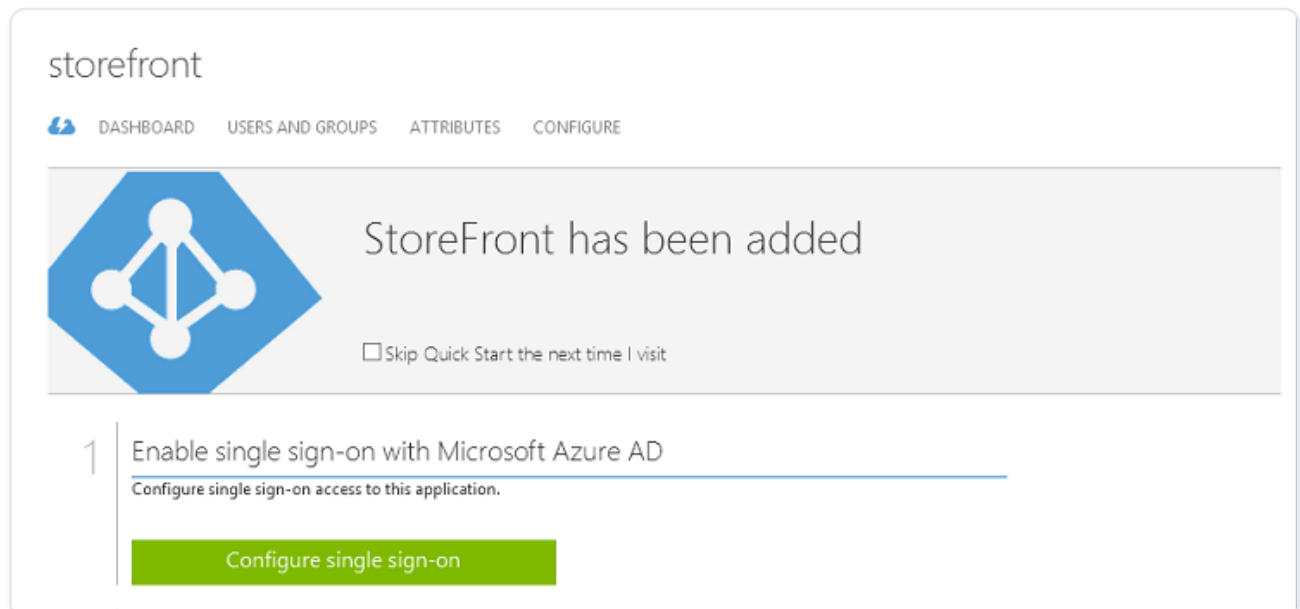
配置图标

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。



配置 SAML 身份验证

返回“应用程序仪表板概述”页面，然后选择 **配置单一登录**。



此部署将使用 SAML 2.0 身份验证，这对应于 **Microsoft Azure AD 单一登录**。

CONFIGURE SINGLE SIGN-ON

How would you like users to sign on to StoreFront?

- ☒ **Microsoft Azure AD Single Sign-On**
Establish federation between Microsoft Azure AD and StoreFront
[Learn more](#)
- ☐ **Password Single Sign-On**
Microsoft Azure AD stores account credentials for users to sign on to StoreFront
[Learn more](#)
- ☐ **Existing Single Sign-On**
Configures Microsoft Azure AD to support single sign-on to StoreFront using Active Directory Federation Services or another third-party single sign-on provider.
[Learn more](#)

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`。

CONFIGURE SINGLE SIGN-ON

Configure App Settings

Enter the settings of AzureStoreFront application below. [Learn more](#)

IDENTIFIER ?
 ✓

REPLY URL ?
 ✓

☐ Show advanced settings (optional).

☐ Configure the certificate used for federated single sign-on (optional).

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

CONFIGURE SINGLE SIGN-ON

Configure single sign-on at AzureStoreFront

To accept the SAML token issued by Azure Active Directory, your application will need the information below. Refer to your application's SAML documentation or source code for details.

- The following certificate will be used for federated single sign-on:
Thumbprint: 8D1E02EBF7C111EDDBBD325F526053BA9626A73B
Expiry: 05/31/2018 11:06:20 UTC

[Download Certificate \(Base 64 - most common\)](#)
[Download Certificate \(Raw\)](#)
[Download Metadata \(XML\)](#)
- Configure the certificate and values in AzureStoreFront
ISSUER URL

SINGLE SIGN-ON SERVICE URL

SINGLE SIGN-OUT SERVICE URL

☐ Confirm that you have configured single sign-on as described above. Checking this will enable the current certificate to start working for this application.

←
→

下载 base 64 受信任签名证书，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

最终步骤是启用应用程序，使其显示在用户的“myapps.microsoft.com”控制页面上。这在“用户和组”页面上完成。为通过 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。

storefront

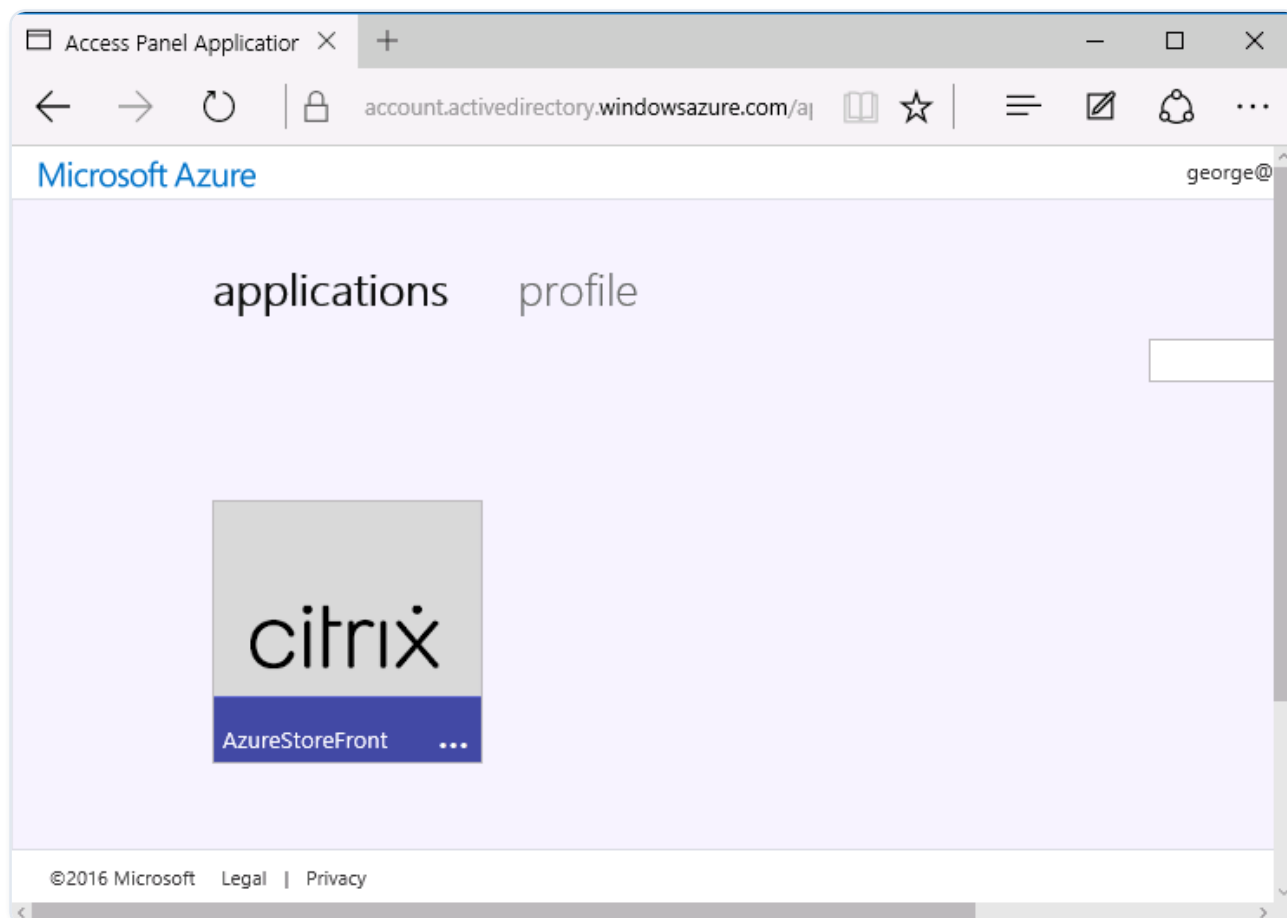
DASHBOARD
USERS AND GROUPS
ATTRIBUTES
CONFIGURE

SHOW
All Users

DISPLAY NAME	USER NAME	JOB TITLE	DEPARTMENT	ACCESS	METHOD	
Azure Admin	AzureAdmin@citrixsamld..			No	Unassigned	
George User	george@citrixsamldemo.net			No	Unassigned	
On-Premises Directory Sy...	Sync_ADFS_21a7e8060dcf...			No	Unassigned	

MyApps 页面

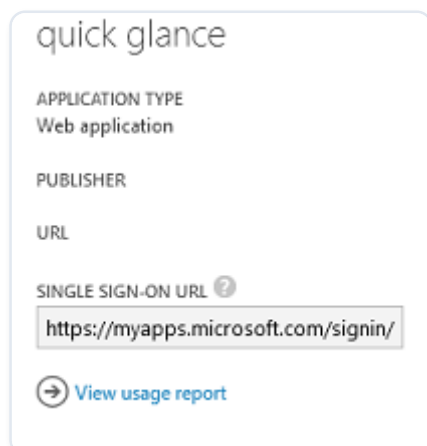
配置应用程序后，当用户访问 `<https://myapps.microsoft.com>` 时，它会显示在用户的 Azure 应用程序列表中。



当加入 Azure AD 后，Windows 10 支持登录用户对 Azure 应用程序进行单点登录。单击图标会将浏览器带到之前配置的 SAML cgi/samlauth 网页。

单点登录 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点登录 URL。此 URL 用于提供网页浏览器链接或创建可将用户直接带到 StoreFront 的“开始”菜单快捷方式。



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 Windows 10 Azure AD 加入的登录会话提供单点登录。（其他用户将需要提供 Azure AD 凭据。）

安装和配置 Citrix Gateway

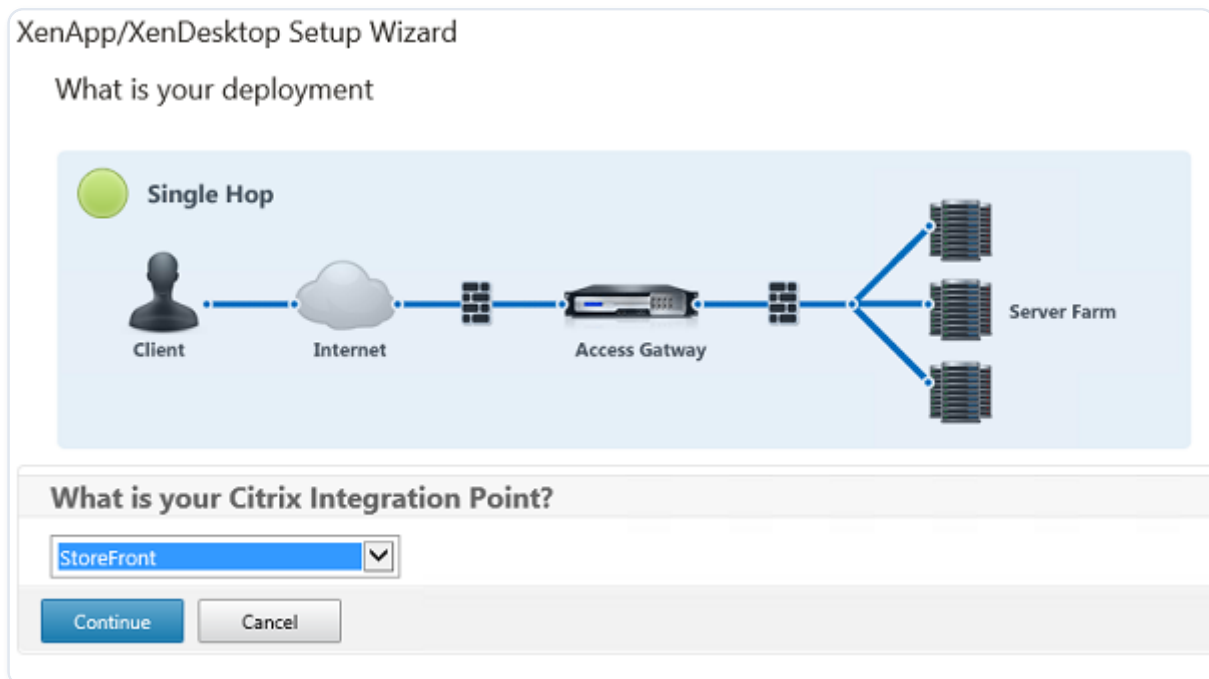
为了远程访问部署，此示例使用运行 NetScaler（现为 Citrix Gateway）的独立虚拟机。这可以从 Azure Store 购买。此示例使用 NetScaler 11.0 的“自带许可证”版本。

登录到 NetScaler® 虚拟机，将 Web 浏览器指向内部 IP 地址，并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 Citrix Gateway StoreFront 设置。为了在 Microsoft Azure 中使用，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。



NetScaler Gateway Settings

NetScaler Gateway IP Address*

10 . 0 . 0 . 18

Port*

4433

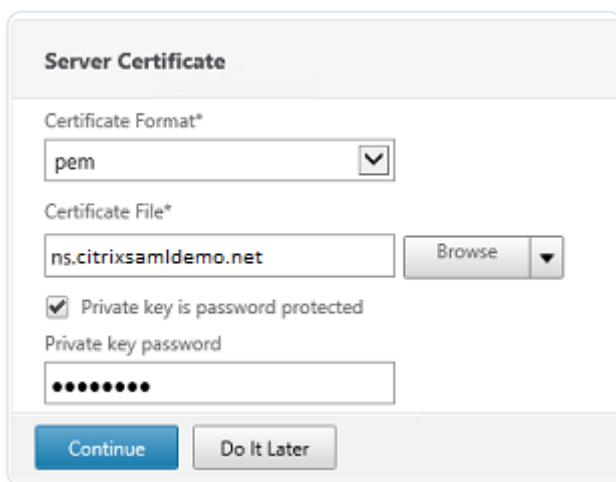
Virtual Server Name*

ns.citrixsamldemo.net

☐ Redirect requests from port 80 to secure port

Continue **Cancel**

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。



Server Certificate

Certificate Format*

pem

Certificate File*

ns.citrixsamldemo.net

Browse

☒ Private key is password protected

Private key password

.....

Continue **Do It Later**

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。

Primary authentication method*

Active Directory/LDAP

IP Address*

10 . 0 . 0 . 12 ☐ IPv6

☐ Load Balancing

Port*

389

Time out (seconds)*

3

Base DN*

CN=Users,DC=citrixsaml demo ,DC

Service account*

CN=internaladmin,CN=Users,DC=

☐ Group Extraction

Server Logon Name Attribute*

userPrincipalName

Password*

.....

Confirm Password*

.....

Secondary authentication method*

None

Continue Cancel

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。

StoreFront

StoreFront FQDN*

ddc.citrixsaml demo.net

Site Path*

/Citrix/StoreWeb

Single Sign-on Domain*

citrixsaml demo

Store Name*

/Citrix/StoreWeb

Secure Ticket Authority Server*

http://ddc.citrixsaml demo.net/sta

StoreFront Server*

10 . 0 . 0 . 15

Protocol*

SSL

Port*

443

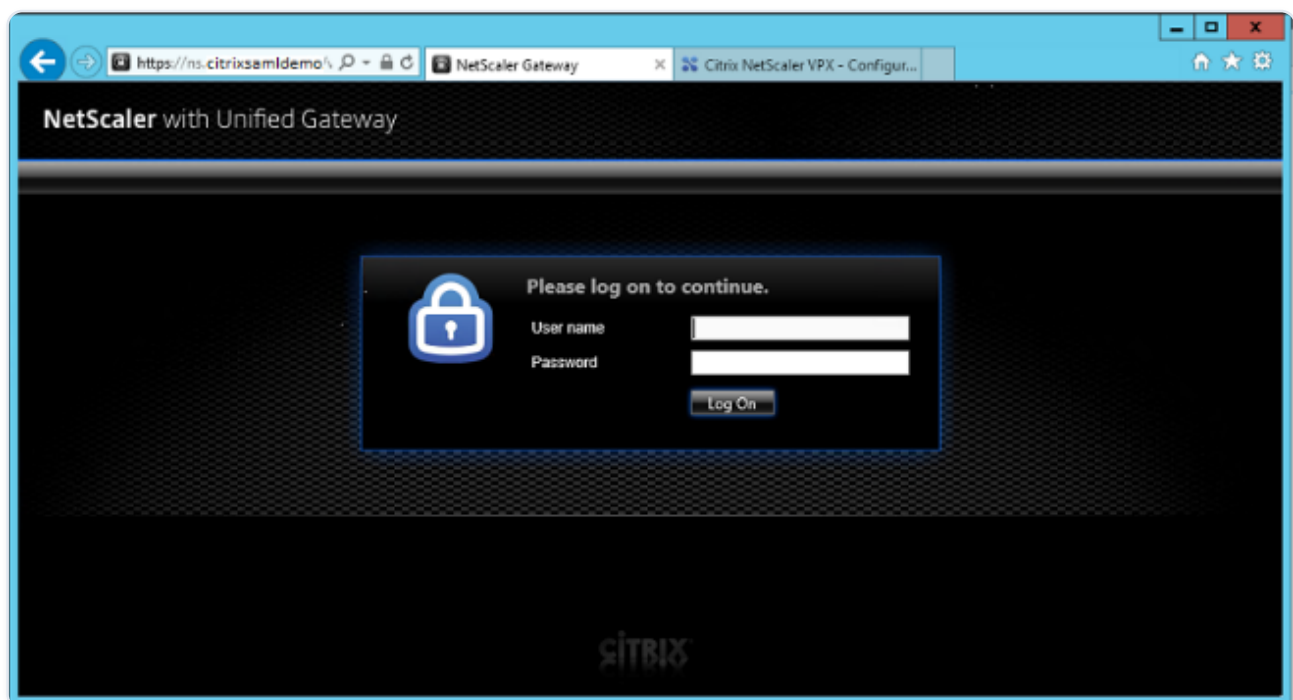
☐ Load Balancing

Continue

Cancel

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。



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**。

本地化图像(/en-us/federated-authentication-service/2411/media/fas-azure-enable-ns-saml-policy.png)

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

本地化图像(/en-us/federated-authentication-service/2411/media/fas-azure-enable-ns-saml-idp-server.png)

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。

本地化图像(/en-us/federated-authentication-service/2411/media/fas-azure-verify-end-to-end.png)

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。

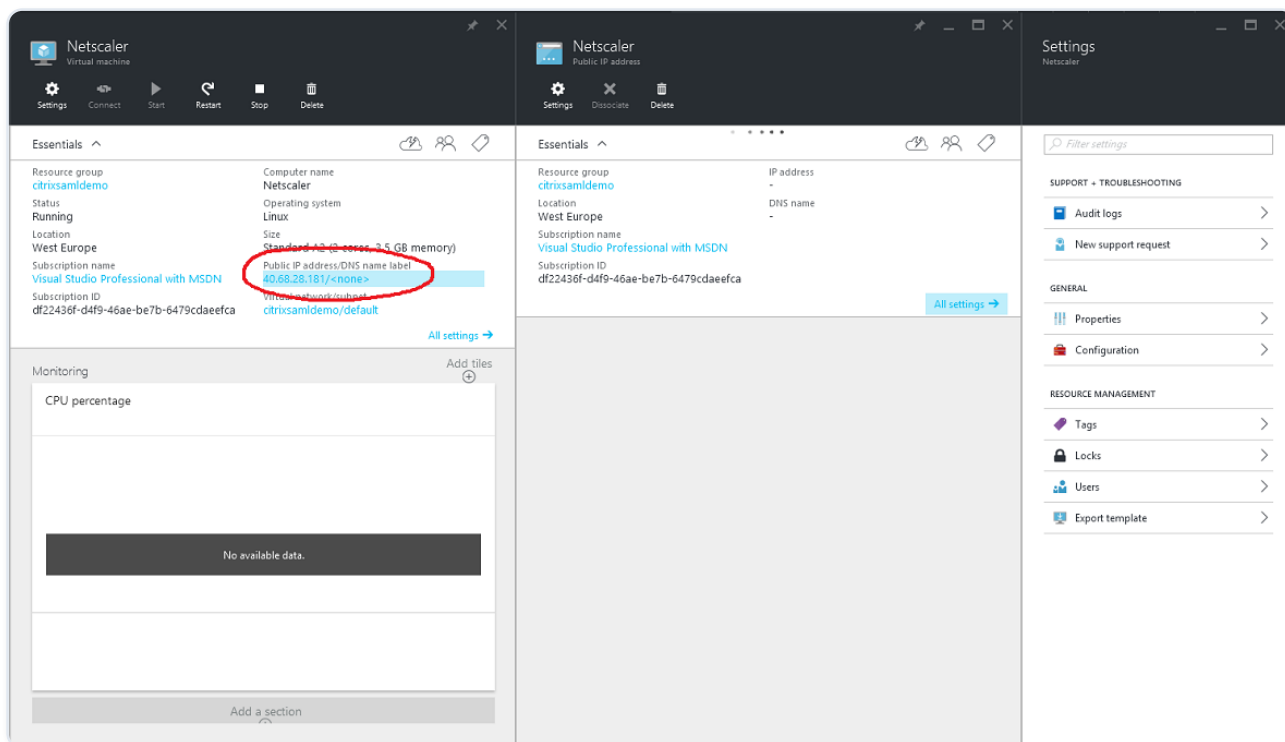
最后，验证未加入 Azure AD 的计算机是否也能使用相同的 URL 正常运行（尽管首次连接时需要 Azure AD 进行一次显式登录）。

附录

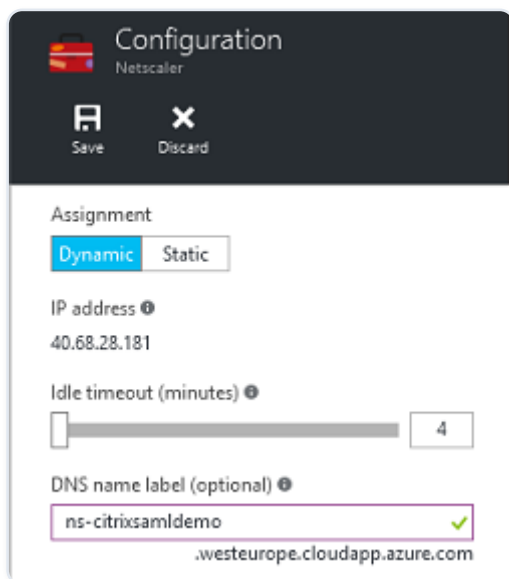
在 Azure 中设置 VM 时，应配置以下标准选项。

提供公共 IP 地址和 DNS 地址

Azure 为所有 VM 提供内部子网上的 IP 地址（在此示例中为 10.*.*）。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 标签引用。



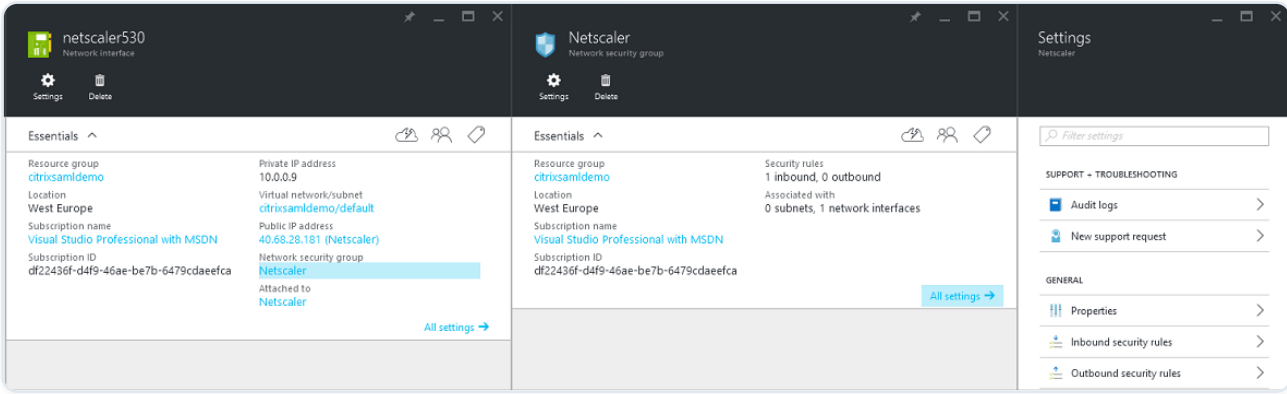
选择公共 IP 地址/DNS 名称标签的配置。为 VM 选择一个公共 DNS 地址。这可用于其他 DNS 区域文件中的 CNAME 引用，确保所有 DNS 记录即使在 IP 地址重新分配后也能正确指向 VM。



设置防火墙规则（安全组）

云中的每个 VM 都有一组自动应用的防火墙规则，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。



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[部署体系结构](#) 文章中进行了总结。
- “操作方法”文章在[高级配置](#) 文章中介绍。

联合身份验证服务 2411 文档历史记录

下表介绍了对联合身份验证服务 2411 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
18 Dec 2024	更新了解决 Windows 登录问题一文	有关详细信息，请参阅 解决 Windows 登录问题 。
11 Dec 2024	更新了在 StoreFront 应用商店中启用 FAS 插件一文	有关详细信息，请参阅在 StoreFront 应用商店中启用 FAS 插件 。
03 Dec 2024	首次发布联合身份验证服务 2411	有关详细信息，请参阅 新增功能 。