



Verbundauthentifizierungsdienst 1912 LTSR

Contents

Federated Authentication Service 1912 LTSR	9
Referenzen	10
Federated Authentication Service 1912 LTSR	11
Behobene Probleme	11
Behobene Probleme in 1912	11
Bekannte Probleme	11
Hinweise von Drittanbietern	12
Systemanforderungen	13
Installieren und konfigurieren	15
Installations- und Einrichtungsreihenfolge	15
Installieren des Federated Authentication Service	15
FAS-Plug-In für StoreFront™-Stores aktivieren	15
Delivery Controller™ konfigurieren	16
Gruppenrichtlinie konfigurieren	17
Unterstützung für Zertifikate in der Sitzung und trennen bei Sperrung	21
Unterstützung für Zertifikate in der Sitzung	21
trennen bei Sperrung	22
Verwenden der Verwaltungskonsole des Federated Authentication Service	22
Bereitstellen von Zertifikatvorlagen	23
Active Directory-Zertifikatdienste einrichten	24
Federated Authentication Service autorisieren	25
Benutzerregeln konfigurieren	27
Erweiterte Nutzung	31
Überlegungen zum Upgrade	31
Sicherheitsüberlegungen	31
Delegierte Registrierungsagenten	31

Konfiguration der Zugriffssteuerungsliste	32
Firewall-Einstellungen	32
Ereignisprotokollüberwachung	33
Hardware sicherheitsmodule	33
PowerShell SDK	34
Leistungsindikatoren	35
Ereignisprotokolle	36
Verwaltungsereignisse	36
Erstellen von Identitätszusicherungen	38
Als vertrauende Partei agieren	38
Sitzungsinterner Zertifikatsserver	39
FAS-Assertions-Plug-in	39
Anmelden	40
Sitzungsinterne Zertifikate	41
Zertifikatanforderung und Schlüsselpaar-Generierung	41
Verwandte Informationen	42
Bereitstellungsarchitekturen	43
Einführung	43
Funktionsweise	43
Interne Bereitstellung	44
Citrix Gateway-Bereitstellung	46
ADFS SAML-Bereitstellung	49
B2B-Kontenzuordnung	50
Windows 10 Azure AD Join	51
ADFS-Bereitstellung	53
Einführung	53
SAML-Übersicht	55
Umleitungs-URL	55

Bezeichner	55
Rücksendeadresse	55
Signaturzertifikat	55
URL für einmaliges Abmelden	56
Konfiguration	56
SAML-Richtlinie ausfüllen	56
Verwandte Informationen	57
Azure AD-Integration	57
Einführung	57
Architektur	59
Eine DNS-Zone erstellen	61
Cloud-Dienst erstellen	62
Windows-VMs erstellen	62
Domänencontroller	63
ADFS-Controller und Webanwendungsproxy-Server	64
Citrix Virtual Desktops™ Delivery Controller und VDA	64
Internen DNS konfigurieren	64
Eine externe DNS-Adresse konfigurieren	65
Sicherheitsgruppen konfigurieren	66
Ein ADFS-Zertifikat erstellen	66
Azure AD einrichten	67
Neues Verzeichnis erstellen	67
Globalen Administratorbenutzer erstellen (AzureAdmin)	69
Ihre Domäne bei Azure AD registrieren	70
Azure AD Connect installieren	71
Azure AD Join aktivieren	81
Installieren Sie Citrix Virtual Apps oder Citrix Virtual Desktops	84
Federated Authentication Service installieren	85

StoreFront konfigurieren	85
StoreFront für die Verwendung von Citrix Gateway konfigurieren	86
Neue Azure AD-Anwendung für Single Sign-On bei StoreFront konfigurieren	87
Symbol konfigurieren	88
SAML-Authentifizierung konfigurieren	88
Anwendung Benutzern zuweisen	91
MyApps-Seite	91
Single Sign-On-URL	92
Citrix Gateway installieren und konfigurieren	93
Führen Sie den Einrichtungsassistenten für Citrix Virtual Apps and Desktops aus	94
Domänencontroller für die AD-Kontoverwaltung konfigurieren	95
StoreFront-Adresse konfigurieren	95
Citrix Gateway-Bereitstellung überprüfen	96
Citrix Gateway SAML-Authentifizierungsunterstützung aktivieren	97
End-to-End-System überprüfen	98
Anhang	99
Eine öffentliche IP-Adresse und DNS-Adresse bereitstellen	99
Firewallregeln einrichten (Sicherheitsgruppe)	100
Verwandte Informationen	101
Erweiterte Konfiguration	102
Zugehörige Informationen	102
Konfiguration der Zertifizierungsstelle	102
Konfigurieren der Microsoft-Zertifizierungsstelle für den TCP-Zugriff	102
Benutzerzertifikate vorab generieren	104
Liste der Active Directory-Benutzer abrufen	104
FAS-Server	105
Registrierungsstellenzertifikate erneuern	106
Zugehörige Informationen	107

Schutz privater Schlüssel	108
Einführung	108
Konfigurationseinstellungen für private Schlüssel	109
Beispiele für Konfigurationsszenarien	112
Beispiel 1	112
Beispiel 2	112
Beispiel 3	123
FAS-Zertifikatspeicher	125
Zugehörige Informationen	127
Sicherheit und Netzwerkkonfiguration	127
Netzwerkarchitektur	127
Firewall und Netzwerksicherheit	128
Verbindungen zwischen Citrix Federated Authentication Service und Citrix Cloud™	129
Verwaltungsaufgaben	130
Gruppenrichtlinieneinstellungen	130
Zertifikatvorlagen	131
Zertifikatvorlage umbenennen	131
Allgemeine Eigenschaften ändern	131
Eigenschaften der Anforderungsbehandlung ändern	131
Kryptografieeigenschaften ändern	131
Eigenschaften der Schlüsselbestätigung ändern	132
Eigenschaften für abgelöste Vorlagen ändern	132
Erweiterungseigenschaften ändern	132
Sicherheitseigenschaften ändern	132
Eigenschaften des Betreffnamens ändern	133
Servereigenschaften ändern	133
Eigenschaften der Ausstellungsanforderungen ändern	133
Kompatibilitätseigenschaften ändern	134

Verwaltung der Zertifizierungsstelle	134
Veröffentlichen von Vorlagen	134
Firewall-Einstellungen	135
Eingeschränkte Registrierung	135
Richtlinienmodule und Überwachung	136
FAS-Verwaltung	136
StoreFront, Benutzer und VDAs über eine ACL einschränken	136
Regeln konfigurieren	137
Zertifizierungsstelle und Vorlagen konfigurieren	137
Sitzungsinterne und Authentifizierungszertifikate	137
Schutz privater Schlüssel und Schlüssellänge	137
Ereignisprotokolle	137
Administrativer Zugriff und Verwaltungstools	138
Citrix Virtual Apps-, Citrix Virtual Desktops- und VDA-Administratoren	138
Allgemeine Windows-Serversicherheit	138
Verwandte Informationen	138
Problembehandlung bei Windows-Anmeldeproblemen	138
Zertifikate und Public-Key-Infrastruktur	139
UPN-Name und Zertifikatszuordnung	140
UPN-Namen in Active Directory	140
Zertifikatszuordnungsdienst	140
Auswahl des Anmelde-Domänencontrollers steuern	141
Auswahl des Domänencontrollers steuern	141
Verwendeten Domänencontroller identifizieren	141
Überwachungsereignisse für Konten aktivieren	142
Zertifikatsvalidierungsprotokolle	142
Zertifikatsgültigkeit prüfen	142
CAPI-Protokollierung aktivieren	142

CAPI-Protokolle	143
Fehlermeldungen	143
Kerberos-Protokolle	144
Ereignisprotokollmeldungen	144
CAPI2-Protokoll des Domänencontrollers	145
Sicherheitsprotokoll des Domänencontrollers	146
VDA-Sicherheitsprotokoll	147
VDA CAPI-Protokoll	148
VDA-Systemprotokoll	149
Fehlermeldungen für Endbenutzer	149
Verwandte Informationen	150
PowerShell-Cmdlets	151
Dokumentationshistorie des Federated Authentication Service 1912	152

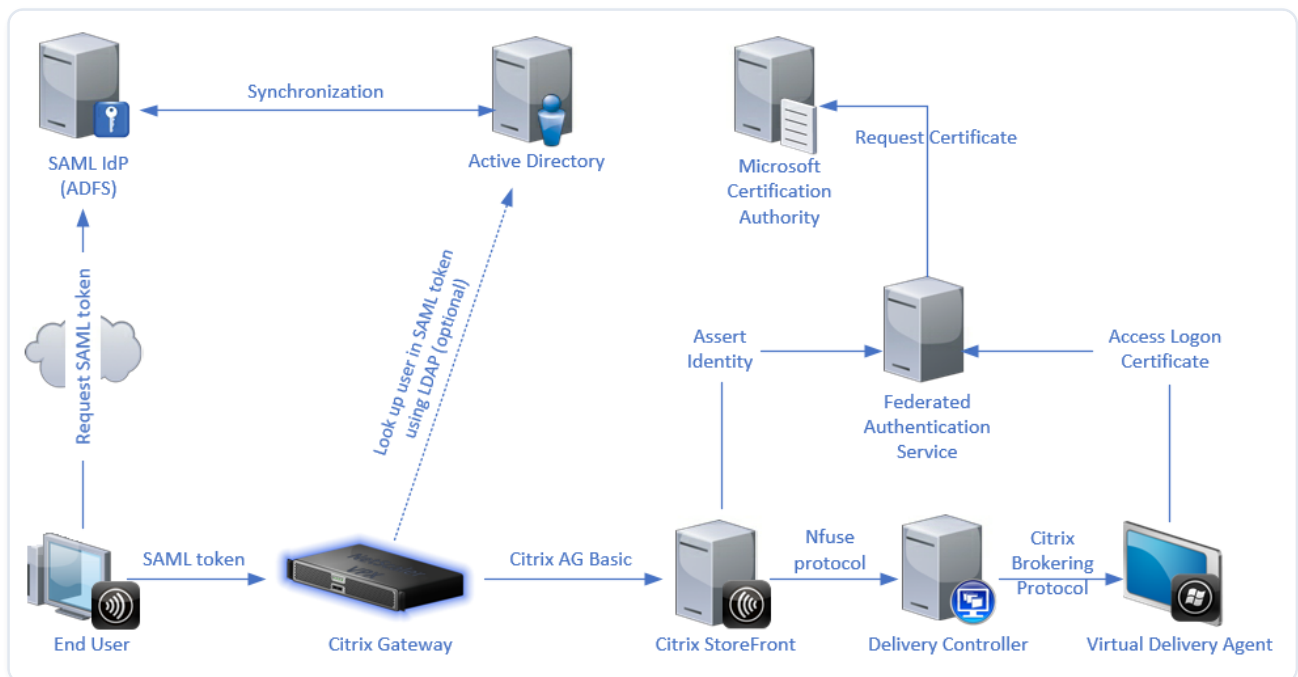
Federated Authentication Service 1912 LTSR

Hinweis:

Diese Dokumentation unterstützt **Federated Authentication Service 1912**, eine Basiskomponente für Citrix Virtual Apps and Desktops 7 1912 LTSR. Die aktuellsten Inhalte finden Sie in der Federated Authentication Service [Dokumentation zur aktuellen Version](#). Die Produktlebenszyklusstrategie für Current Releases (CR) und Long Term Service Releases (LTSR) wird beschrieben unter [Lifecycle Milestones](#).

Der Federated Authentication Service (FAS) ist eine privilegierte Komponente, die für die Integration mit Active Directory-Zertifikatdiensten entwickelt wurde. Sie stellt Benutzern dynamisch Zertifikate aus, sodass sie sich bei einer Active Directory-Umgebung anmelden können, als hätten sie eine Smartcard. Dadurch kann StoreFront™ eine breitere Palette von Authentifizierungsoptionen nutzen, wie z. B. SAML-Assertions (Security Assertion Markup Language). SAML wird häufig als Alternative zu herkömmlichen Windows-Benutzerkonten im Internet verwendet.

Das folgende Diagramm zeigt, wie FAS in eine Microsoft-Zertifizierungsstelle integriert wird und Supportdienste für StoreFront und Citrix Virtual Apps and Desktops™ Virtual Delivery Agents (VDAs) bereitstellt.



Vertrauenswürdige StoreFront-Server kontaktieren FAS, wenn Benutzer Zugriff auf die Citrix-Umgebung anfordern. FAS gewährt ein Ticket, das einer einzelnen Citrix Virtual Apps- oder Citrix Virtual Desktops™-Sitzung die Authentifizierung mit einem Zertifikat für diese Sitzung ermöglicht. Wenn ein VDA einen Benutzer authentifizieren muss, stellt er eine Verbindung zu FAS her und löst das Ticket ein. Nur FAS hat Zugriff auf den privaten Schlüssel des Benutzerzertifikats; der VDA muss jeden Signier- und Entschlüsselungsvorgang, den er mit dem Zertifikat durchführen muss, an FAS senden.

Referenzen

- Active Directory-Zertifikatdienste [https://docs.microsoft.com/de-de/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/hh831740\(v=ws.11\)>](https://docs.microsoft.com/de-de/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/hh831740(v=ws.11)>)
- Konfigurieren von Windows für die Zertifikatanmeldung <http://support.citrix.com/article/CTX206156>>

Federated Authentication Service 1912 LTSR

Diese Version von Federated Authentication Service behebt mehrere Probleme, die dazu beitragen, die Gesamtleistung und Stabilität zu verbessern. Es wurden keine neuen Funktionen hinzugefügt.

Informationen zu Fehlerbehebungen finden Sie unter [Behobene Probleme](#).

Behobene Probleme

Behobene Probleme in 1912

Verglichen mit: Federated Authentication Service 1909

Federated Authentication Service 1912 enthält die folgenden Korrekturen:

- In den Eigenschaften der Zertifikatvorlage Citrix_SmartcardLogon sollte die Beschreibung der Schlüsselnutzungserweiterung nur „Digitale Signatur“ und „Schlüsselverschlüsselung“ enthalten, listet aber zusätzliche Elemente auf. Die mit dieser Vorlage ausgestellten Zertifikate sind jedoch korrekt.
- Wenn die FAS-Verwaltungskonsole verwendet wird, um Zertifikatvorlagen in Active Directory bereitzustellen, enthalten die Sicherheitsberechtigungen der Vorlage nicht mehr die Berechtigung „auto-enroll“. Diese Berechtigung ist für den korrekten FAS-Betrieb nicht erforderlich und führte in einigen Kundenbereitstellungen zu unerwünschten Registrierungsversuchen von Domänencomputern.

Bekannte Probleme

Federated Authentication Service 1912 enthält keine bekannten Probleme.

Diese Warnung gilt für alle Problemumgehungen, die eine Änderung eines Registrierungseintrags vorschlagen:

WARNUNG:

Eine fehlerhafte Bearbeitung der Registrierung kann schwerwiegende Probleme verursachen, die eine Neuinstallation des Betriebssystems erforderlich machen können. Citrix® kann nicht garantieren, dass Probleme, die aus der falschen Verwendung des Registrierungs-Editors resultieren, behoben werden können. Die Verwendung des Registrierungs-Editors erfolgt auf eigene Gefahr. Sichern Sie die Registrierung unbedingt, bevor Sie sie bearbeiten.

Hinweise von Drittanbietern

Diese Version des Federated Authentication Service kann Software von Drittanbietern enthalten, die unter den in den folgenden Dokumenten definierten Bedingungen lizenziert ist:

- [Citrix Virtual Apps and Desktops Hinweise von Drittanbietern \(PDF-Download\)](#)
- [Offenlegungen zu nicht-kommerzieller Software für FlexNet Publisher 2017 \(11.15.0.0\) \(PDF-Download\)](#)
- [FlexNet Publisher Dokumentationsergänzung: In FlexNet Publisher 11.15.0 verwendete Software von Drittanbietern und Open-Source-Software \(PDF-Download\)](#)

Systemanforderungen

- Der Federated Authentication Service (FAS) wird auf den folgenden Windows Server-Versionen unterstützt:
 - Windows Server 2019, Standard- und Datacenter-Editionen sowie mit der Server Core-Option
 - Windows Server 2016, Standard- und Datacenter-Editionen sowie mit der Server Core-Option
 - Windows Server 2012 R2, Standard- und Datacenter-Editionen sowie Server Core für Windows Server 2012 R2
- Citrix® empfiehlt die Installation von FAS auf einem Server, der keine anderen Citrix-Komponenten enthält.
- Der Windows Server sollte gesichert sein. Er hat Zugriff auf ein Registrierungsstellenzertifikat und einen privaten Schlüssel, der es ihm ermöglicht, automatisch Zertifikate für Domänenbenutzer auszustellen, und er hat Zugriff auf diese Benutzerzertifikate und privaten Schlüssel.
- Die FAS [PowerShell-Cmdlets](#) erfordern die Installation von Windows PowerShell 64-Bit auf dem FAS-Server.
- Eine Microsoft Enterprise-Zertifizierungsstelle ist erforderlich, um Benutzerzertifikate auszustellen.

Auf der Citrix Virtual Apps- oder Citrix Virtual Desktops™-Site:

- Delivery Controller, Virtual Delivery Agents (VDAs) und StoreFront™-Server müssen alle unterstützte Versionen sein.

HINWEIS:

FAS wird auf XenApp und XenDesktop 7.6 Long Term Service Release (LTSR) nicht unterstützt.

- Vor dem Erstellen des Maschinenkatalogs muss die Gruppenrichtlinienkonfiguration des Federated Authentication Service korrekt auf die VDAs angewendet werden. Weitere Informationen finden Sie im Abschnitt [Gruppenrichtlinie konfigurieren](#).

Berücksichtigen Sie bei der Planung der Bereitstellung dieses Dienstes den Abschnitt [Sicherheitsüberlegungen](#).

Installieren und konfigurieren

Installations- und Einrichtungsreihenfolge

1. [Installieren des Federated Authentication Service \(FAS\)](#)
2. [FAS-Plug-In in StoreFront-Stores aktivieren](#)
3. [Gruppenrichtlinie konfigurieren](#)
4. Verwenden Sie die FAS-Verwaltungskonsole, um: (a) [Die bereitgestellten Vorlagen bereitzustellen](#), (b) [Zertifizierungsstellen einzurichten](#) und (c) [FAS zur Verwendung Ihrer Zertifizierungsstelle zu autorisieren](#)
5. [Benutzerregeln konfigurieren](#)

Installieren des Federated Authentication Service

Aus Sicherheitsgründen empfiehlt Citrix®, dass der Federated Authentication Service (FAS) auf einem dedizierten Server installiert wird, der ähnlich wie ein Domänencontroller oder eine Zertifizierungsstelle gesichert ist. FAS kann über die Schaltfläche **Federated Authentication Service** auf dem Autorun-Begrüßungsbildschirm installiert werden, wenn die ISO eingelegt wird.

Dabei werden folgende Komponenten installiert:

- Federated Authentication Service
- [PowerShell-Snap-In-Cmdlets](#) zur Remotekonfiguration von FAS
- [FAS-Verwaltungskonsole](#)
- FAS-Gruppenrichtlinienvorlagen (CitrixFederatedAuthenticationService.admx/adml)
- Zertifikatvorlagendateien für die einfache Zertifizierungsstellenkonfiguration
- [Leistungsindikatoren](#) und [Ereignisprotokolle](#)

FAS-Plug-In für StoreFront™-Stores aktivieren

Um die FAS-Integration in einem StoreFront-Store zu aktivieren, führen Sie die folgenden PowerShell-Cmdlets als Administratorkonto aus. Wenn Sie mehr als einen Store haben oder der Store einen anderen Namen hat, kann der unten angegebene Pfadtext abweichen.

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

$StoreVirtualPath = "/Citrix/Store"

$store = Get-STFStoreService -VirtualPath $StoreVirtualPath

$auth = Get-STFAuthenticationService -StoreService $store

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

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

Um die Verwendung von FAS zu beenden, verwenden Sie das folgende PowerShell-Skript:

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

$StoreVirtualPath = "/Citrix/Store"

$store = Get-STFStoreService -VirtualPath $StoreVirtualPath

$auth = Get-STFAuthenticationService -StoreService $store

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

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

Delivery Controller™ konfigurieren

Um FAS zu verwenden, konfigurieren Sie den Citrix Virtual Apps- oder Citrix Virtual Desktops™ Delivery Controller so, dass er den StoreFront-Servern vertraut, die sich mit ihm verbinden können: Führen Sie das PowerShell-Cmdlet **Set-BrokerSite -TrustRequestsSentToTheXmlServicePort \$true** aus.

Gruppenrichtlinie konfigurieren

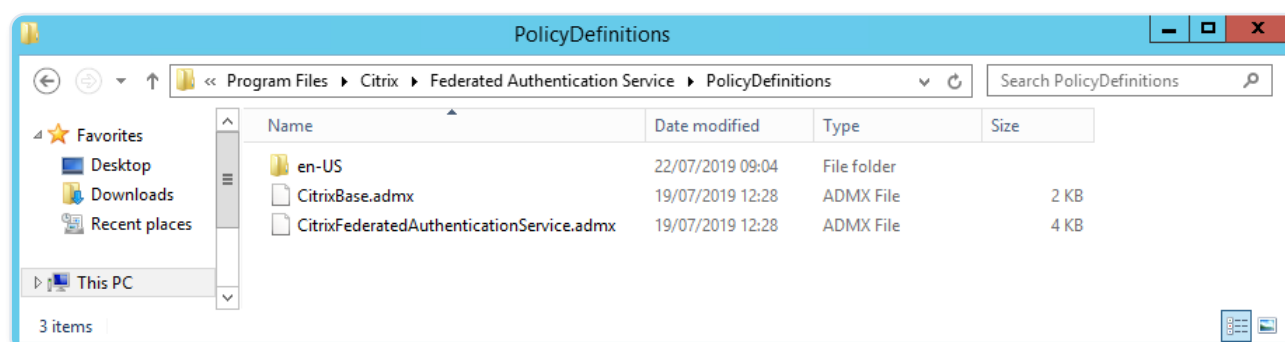
Nach der Installation von FAS müssen Sie die vollständigen DNS-Adressen der FAS-Server in der Gruppenrichtlinie unter Verwendung der in der Installation bereitgestellten Gruppenrichtlinienvorlagen angeben.

WICHTIG:

Stellen Sie sicher, dass die StoreFront-Server, die Tickets anfordern, und die Virtual Delivery Agents (VDAs), die Tickets einlösen, eine identische Konfiguration der DNS-Adressen aufweisen, einschließlich der automatischen Servernummerierung, die vom Gruppenrichtlinienobjekt angewendet wird.

Der Einfachheit halber konfigurieren die folgenden Beispiele eine einzelne Richtlinie auf Domänenebene, die für alle Maschinen gilt; dies ist jedoch nicht zwingend erforderlich. FAS funktioniert, solange die StoreFront-Server, VDAs und die Maschine, auf der die FAS-Verwaltungskonsole ausgeführt wird, dieselbe Liste von DNS-Adressen sehen. Beachten Sie, dass das Gruppenrichtlinienobjekt jeder Eintragung eine Indexnummer hinzufügt, die ebenfalls übereinstimmen muss, wenn mehrere Objekte verwendet werden.

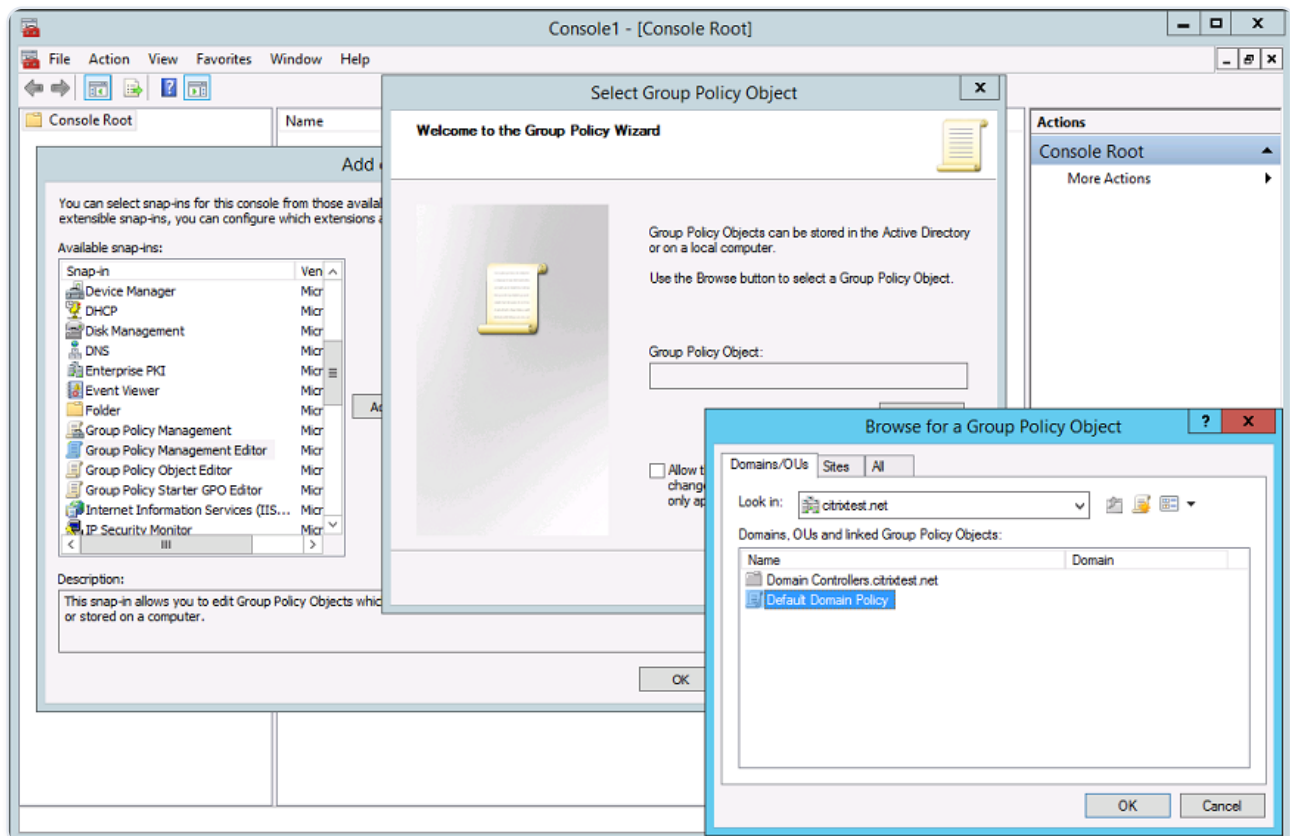
Schritt 1. Suchen Sie auf dem Server, auf dem Sie FAS installiert haben, die Dateien C:\Program Files\Citrix\Federated Authentication Service\PolicyDefinitions\CitrixFederatedAuthenticationService.admx und CitrixBase.admx sowie den Ordner en-US.



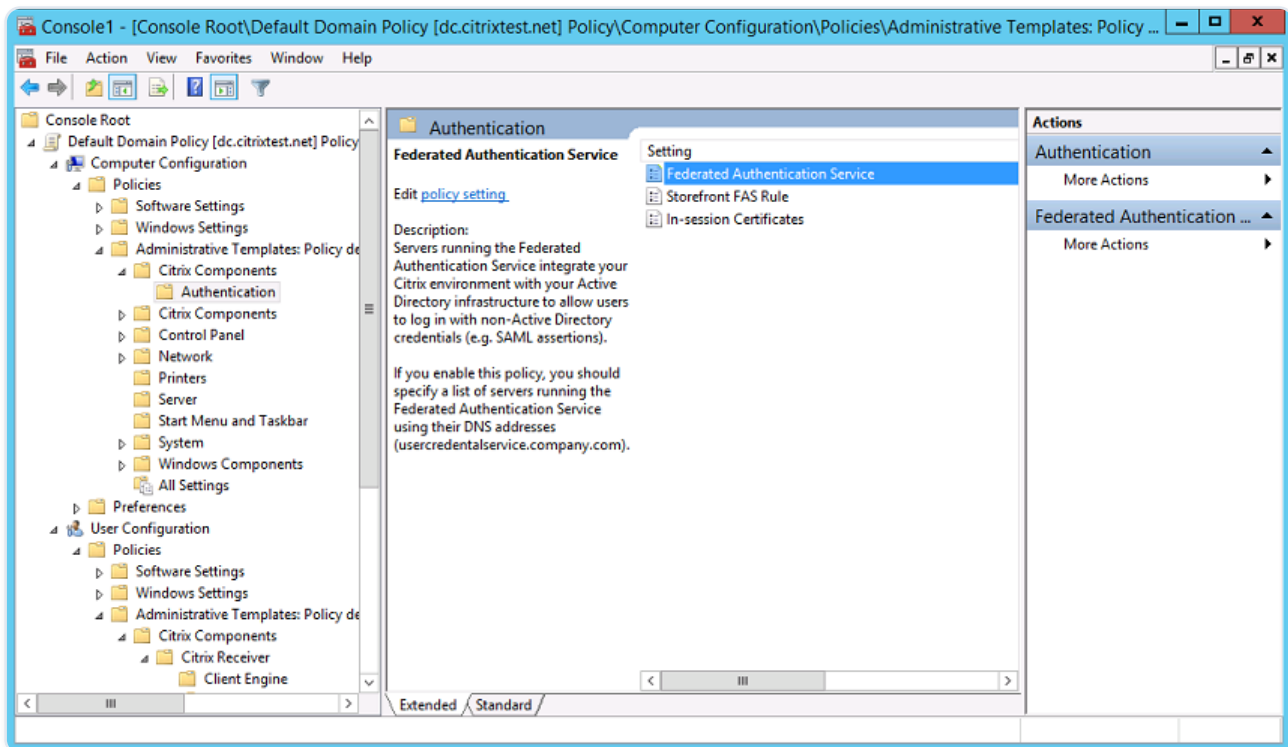
Schritt 2. Kopieren Sie diese auf Ihren Domänencontroller und legen Sie sie in den Unterordner C:\Windows\PolicyDefinitions und en-US.

Schritt 3. Führen Sie die Microsoft Management Console (mmc.exe über die Befehlszeile) aus. Wählen Sie in der Menüleiste **Datei > Snap-In hinzufügen/entfernen**. Fügen Sie den **Gruppenrichtlinienverwaltungs-Editor** hinzu.

Wenn Sie zur Eingabe eines Gruppenrichtlinienobjekts aufgefordert werden, wählen Sie **Durchsuchen** und dann **Standarddomänenrichtlinie**. Alternativ können Sie ein geeignetes Richtlinienobjekt für Ihre Umgebung mit den Tools Ihrer Wahl erstellen und auswählen. Die Richtlinie muss auf alle Computer angewendet werden, auf denen betroffene Citrix-Software (VDAs, StoreFront-Server, Verwaltungstools) ausgeführt wird.

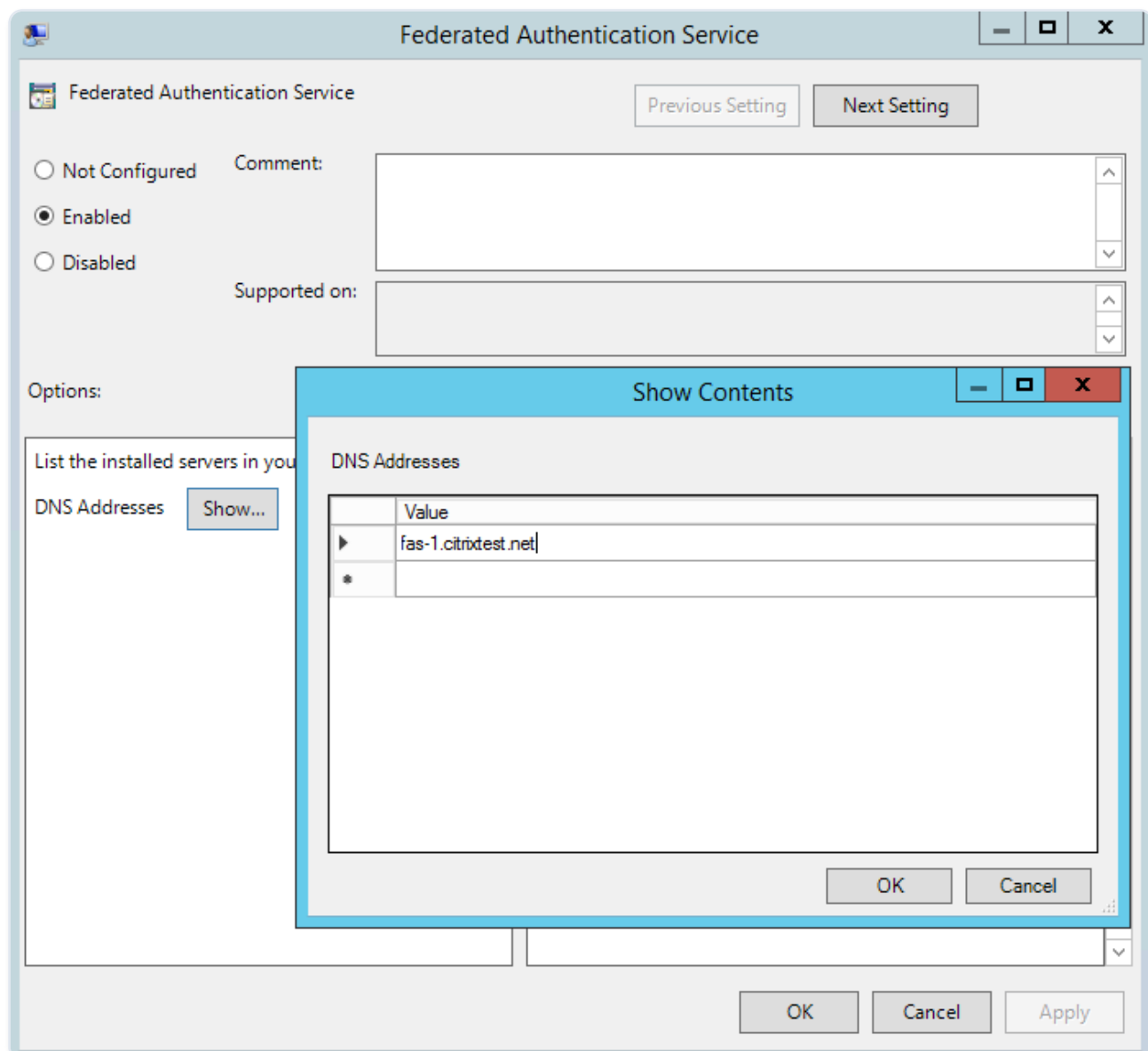


Schritt 4. Navigieren Sie zur Richtlinie *Federated Authentication Service* unter Computer Configuration/Policies/Administrative Templates/Citrix Components/Authentication.

**HINWEIS:**

Die Richtlinieneinstellung für den Federated Authentication Service ist nur in Domänen-GPOs verfügbar, wenn Sie die Vorlagendatei CitrixBase.admx/CitrixBase.adml zum Ordner PolicyDefinitions hinzufügen. Die Richtlinieneinstellung für den Federated Authentication Service wird dann im Ordner Administrative Templates > Citrix Components > Authentication aufgeführt.

Schritt 5. Öffnen Sie die Richtlinie für den Federated Authentication Service und wählen Sie **Aktiviert**. Dadurch können Sie die Schaltfläche **Anzeigen** auswählen, wo Sie die DNS-Adressen Ihrer FAS-Server konfigurieren.



Schritt 6. Geben Sie die vollqualifizierten Domännennamen (FQDNs) der Server ein, die FAS hosten.

Wichtig: Wenn Sie mehrere FQDNs eingeben, muss die Reihenfolge der Liste zwischen StoreFront-Servern und VDAs konsistent sein. Dies schließt leere oder ungenutzte Listeneinträge ein.

Schritt 7. Klicken Sie auf **OK**, um den Gruppenrichtlinien-Assistenten zu beenden und die Gruppenrichtlinienänderungen anzuwenden. Möglicherweise müssen Sie Ihre Computer neu starten (oder **gpupdate /force** über die Befehlszeile ausführen), damit die Änderung wirksam wird.

Unterstützung für Zertifikate in der Sitzung und trennen bei Sperrung

In-session Certificates

Previous Setting Next Setting

☐ Not Configured Comment:
☒ Enabled
☐ Disabled

Supported on:

Options:

Prompt Scope: Per-process

Consent timeout (seconds): 30

☒ Disconnect on lock

Help:

Certificates and private keys securely managed by the Federated Authentication Service can be made available to programs running in users' sessions. If this policy is disabled, this feature will be unavailable.

If this policy is enabled, the Prompt Scope setting will control how users are prompted for consent. There are three options:

- No consent required -- This option disables the security prompt and private keys are used silently.
- Per-process consent -- Each running program will individually prompt for consent.
- Per-session consent -- Once the user has clicked ok, this will apply to all programs in the session

If this policy is enabled, the Consent Timeout will control how long (in seconds) the consent lasts. So for example, if set to 300 seconds the user will see a prompt every five minutes. A value of zero will prompt the user for every private key operation.

If this policy is enabled, it is also possible to automatically disconnect a user's session rather than display the logon prompt. This functionality provides similar behaviour to the "disconnect on smart card removal" policy, and is useful for situations where users do not have Active Directory logon credentials.

OK Cancel Apply

Unterstützung für Zertifikate in der Sitzung

Standardmäßig erlauben VDAs nach der Anmeldung keinen Zugriff auf Zertifikate. Bei Bedarf können Sie die Gruppenrichtlinienvorlage verwenden, um das System für Zertifikate in der Sitzung zu konfigurieren. Dadurch werden Zertifikate nach der Anmeldung zur Anwendungsnutzung im persönlichen Zertifikatspeicher des Benutzers abgelegt. Wenn Sie beispielsweise eine TLS-Authentifizierung für Webserver innerhalb der VDA-Sitzung benötigen, kann das Zertifikat von Internet Explorer verwendet werden.

trennen bei Sperrung

Wenn diese Richtlinie aktiviert ist, wird die Sitzung des Benutzers automatisch getrennt, wenn der Bildschirm gesperrt wird. Diese Funktionalität bietet ein ähnliches Verhalten wie die Richtlinie „trennen bei Smartcard-Entfernung“ und ist nützlich für Situationen, in denen Benutzer keine Active Directory-Anmeldeinformationen besitzen.

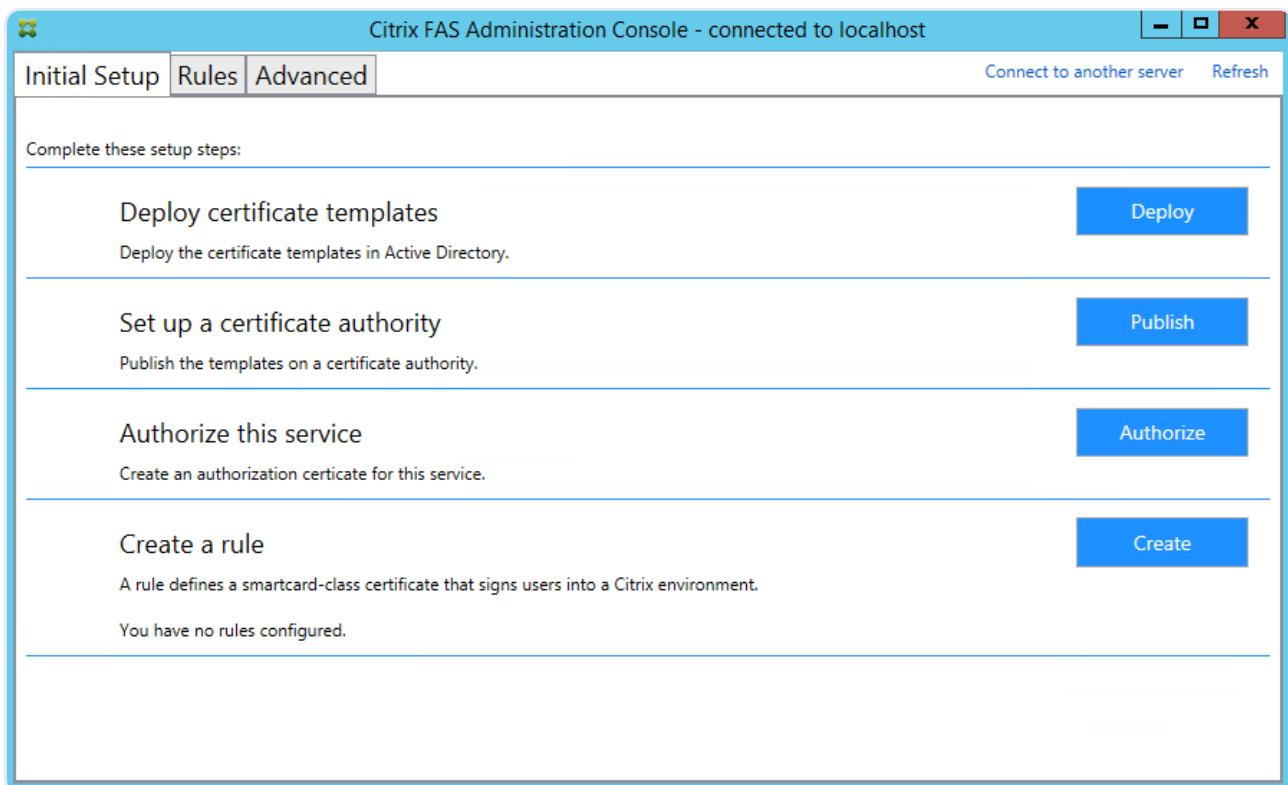
HINWEIS:

Die Richtlinie „trennen bei Sperrung“ gilt für alle Sitzungen auf dem VDA.

Verwenden der Verwaltungskonsole des Federated Authentication Service

Die FAS-Verwaltungskonsole wird als Teil von FAS installiert. Ein Symbol (Citrix Federated Authentication Service) wird im Startmenü platziert.

Wenn die Verwaltungskonsole zum ersten Mal verwendet wird, führt sie Sie durch einen Prozess, der Zertifikatvorlagen bereitstellt, die Zertifizierungsstelle einrichtet und FAS zur Verwendung der Zertifizierungsstelle autorisiert. Einige der Schritte können alternativ manuell mithilfe von Betriebssystem-Konfigurationstools abgeschlossen werden.

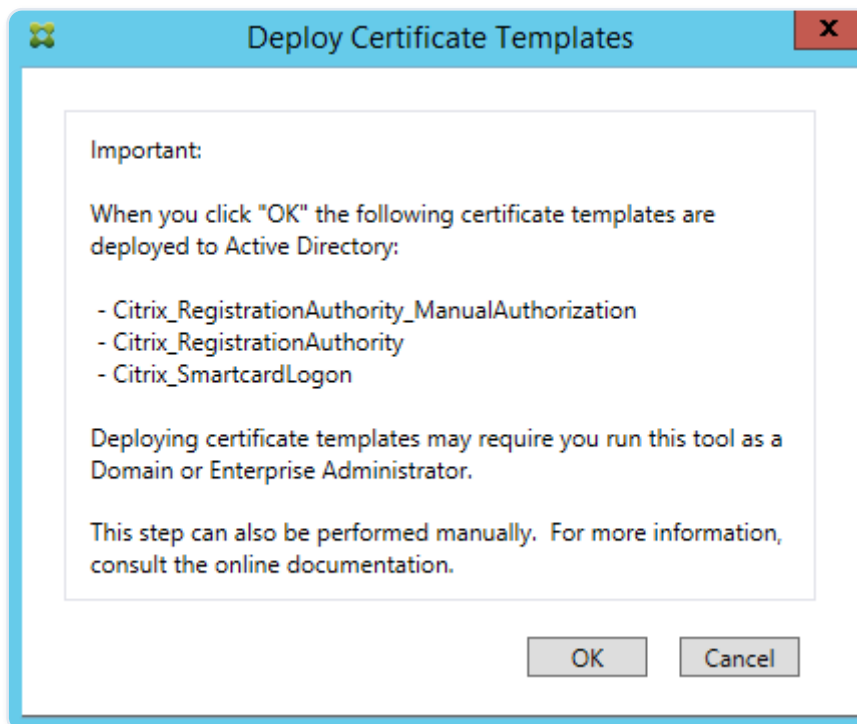


Bereitstellen von Zertifikatvorlagen

Um Interoperabilitätsprobleme mit anderer Software zu vermeiden, stellt FAS drei Citrix-Zertifikatvorlagen für den eigenen Gebrauch bereit.

- Citrix_RegistrationAuthority_ManualAuthorization
- Citrix_RegistrationAuthority
- Citrix_SmartcardLogon

Diese Vorlagen müssen bei Active Directory registriert werden. Wenn die Konsole sie nicht finden kann, kann das Tool **Zertifikatvorlagen bereitstellen** sie installieren. Dieses Tool muss als Konto ausgeführt werden, das über Berechtigungen zur Verwaltung Ihrer Unternehmensgesamtstruktur verfügt.



Die Konfiguration der Vorlagen ist in den XML-Dateien mit der Erweiterung .certificatetemplate zu finden, die mit FAS installiert werden unter:

C:\Program Files\Citrix\Federated Authentication Service\CertificateTemplates

Wenn Sie keine Berechtigung haben, diese Vorlagendateien zu installieren, geben Sie sie Ihrem Active Directory-Administrator.

Um die Vorlagen manuell zu installieren, können Sie die folgenden PowerShell-Befehle verwenden:

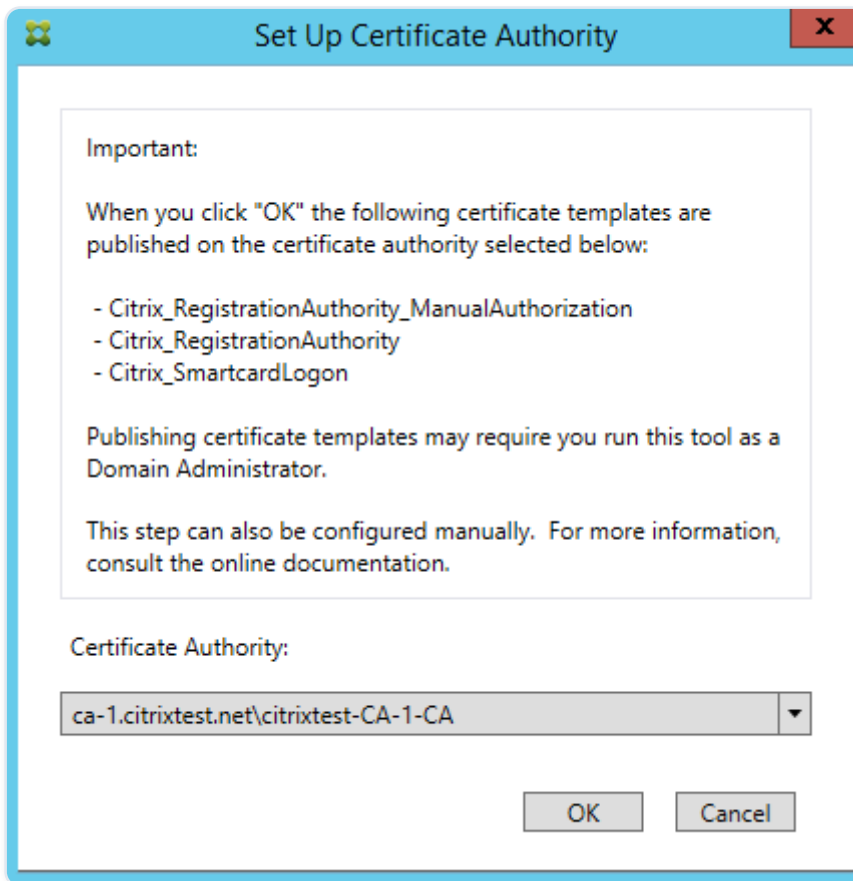
```
$template =  
[System.IO.File]::ReadAllBytes("$Pwd\Citrix_SmartcardLogon.certificatetemplate")  
  
$CertEnrol = New-Object -ComObject  
X509Enrollment.CX509EnrollmentPolicyWebService  
  
$CertEnrol.InitializeImport($template)  
  
$comtemplate = $CertEnrol.GetTemplates().ItemByIndex(0)  
  
$writabletemplate = New-Object -ComObject  
X509Enrollment.CX509CertificateTemplateADWritable  
  
$writabletemplate.Initialize($comtemplate)  
  
$writabletemplate.Commit(1, $NULL)
```

Active Directory-Zertifikatdienste einrichten

Nach der Installation der Citrix-Zertifikatvorlagen müssen diese auf einem oder mehreren Microsoft-Zertifizierungsstellenservern veröffentlicht werden. Informationen zur Bereitstellung von Active Directory-Zertifikatdiensten finden Sie in der Microsoft-Dokumentation.

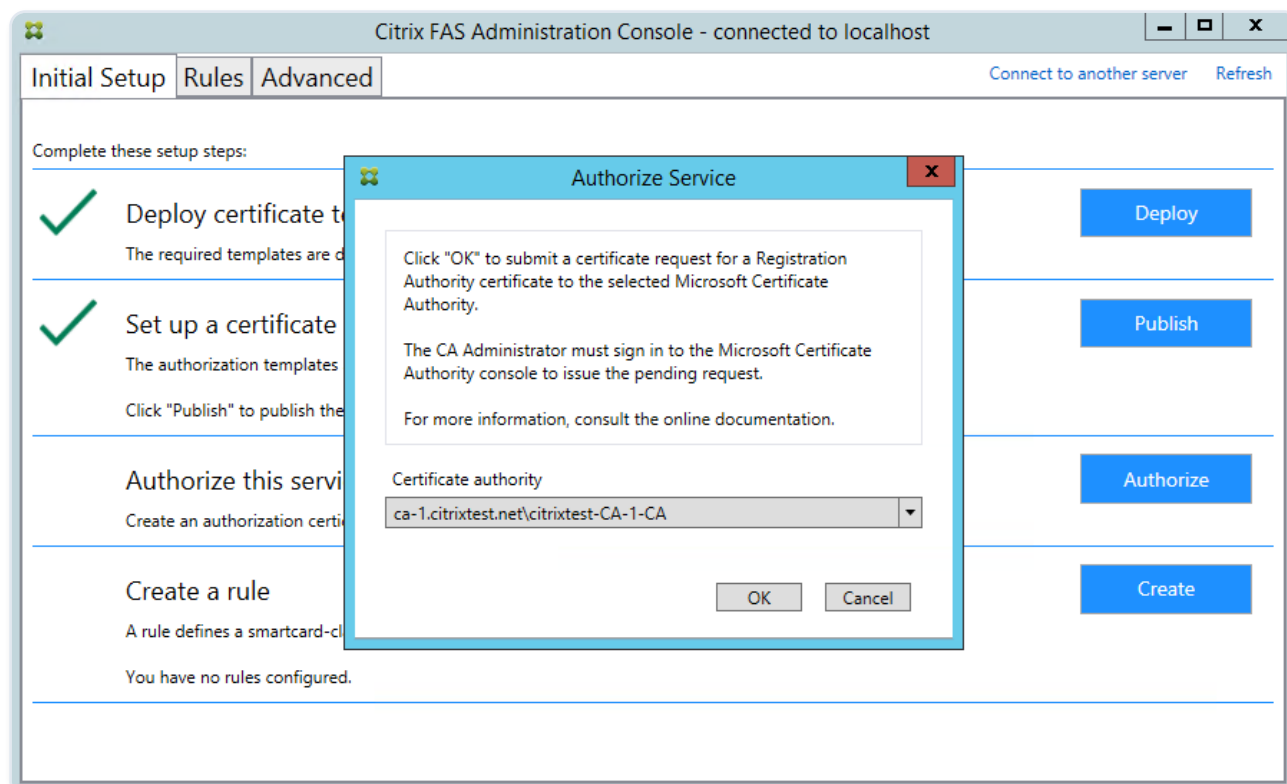
Wenn die Vorlagen nicht auf mindestens einem Server veröffentlicht sind, bietet das Tool **Zertifizierungsstelle einrichten** an, diese zu veröffentlichen. Sie müssen dieses Tool als Benutzer ausführen, der über Berechtigungen zur Verwaltung der Zertifizierungsstelle verfügt.

(Zertifikatvorlagen können auch mithilfe der Microsoft-Zertifizierungsstellenkonsole veröffentlicht werden.)

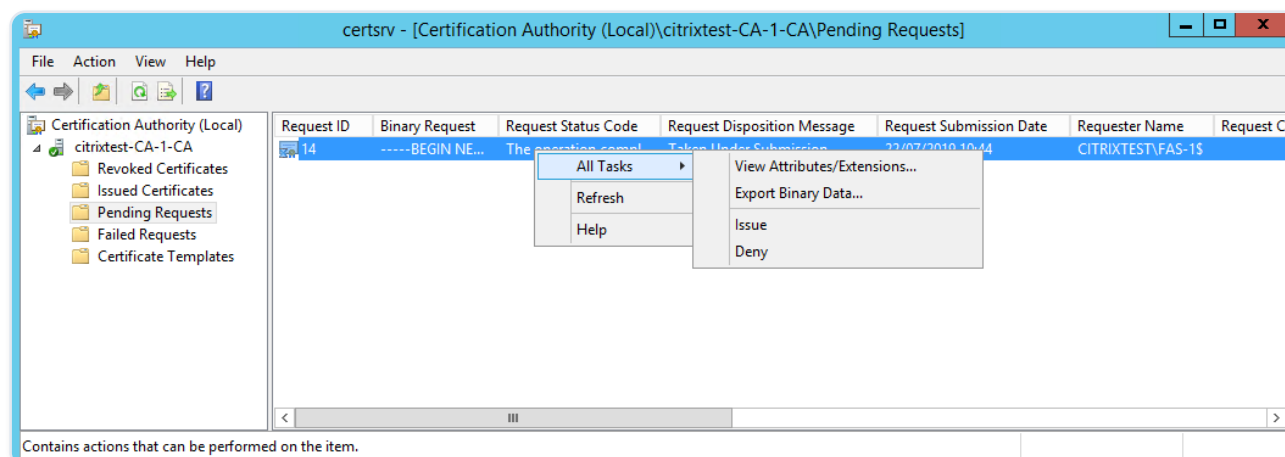


Federated Authentication Service autorisieren

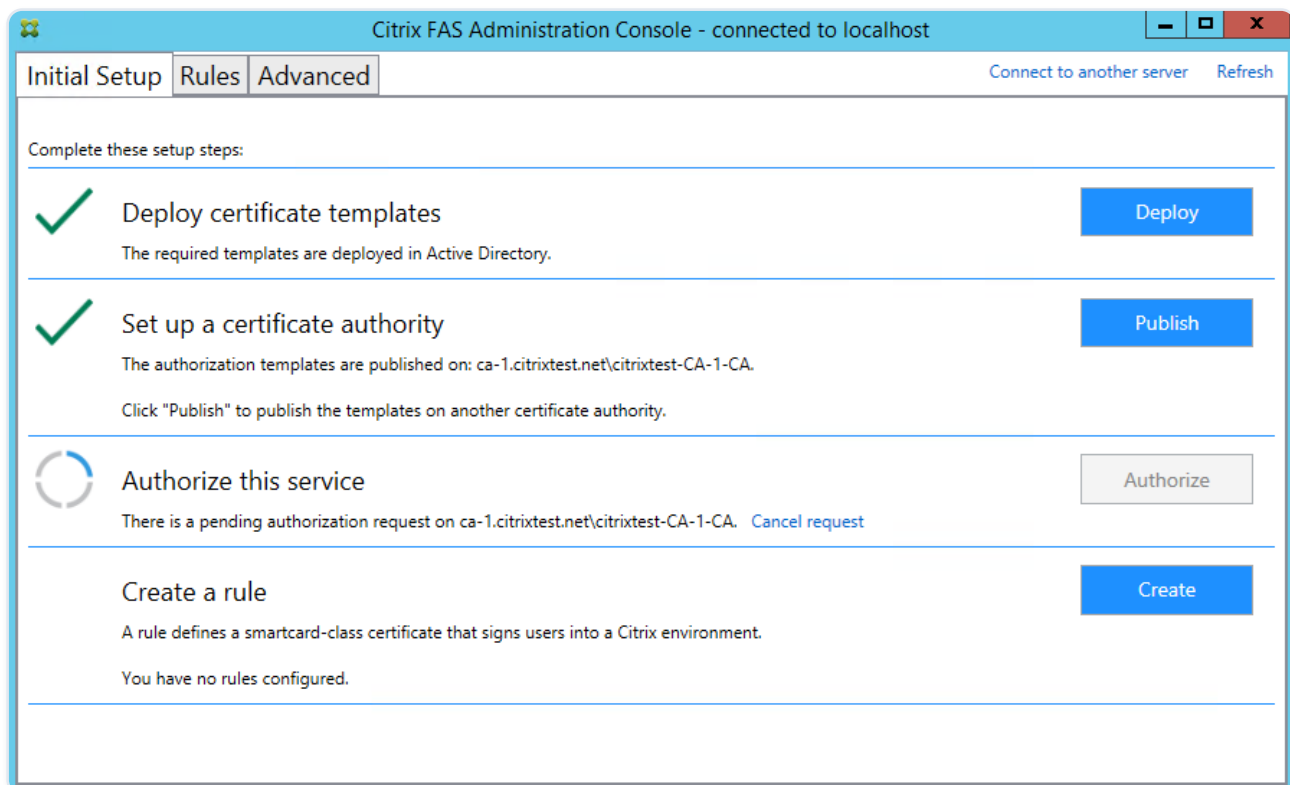
Dieser Schritt initiiert die Autorisierung von FAS. Die Verwaltungskonsole verwendet die Vorlage Citrix_RegistrationAuthority_ManualAuthorization, um eine Zertifikatanforderung zu generieren, und sendet diese dann an eine der Zertifizierungsstellen, die diese Vorlage veröffentlichen.



Nachdem die Anforderung gesendet wurde, erscheint sie in der Liste **Ausstehende Anforderungen** der Microsoft-Zertifizierungsstellenkonsole. Der Zertifizierungsstellenadministrator muss die Anforderung **Ausstellen** oder **Verweigern**, bevor die Konfiguration von FAS fortgesetzt werden kann. Beachten Sie, dass die Autorisierungsanforderung als **Ausstehende Anforderung** vom FAS-Computerkonto angezeigt wird.



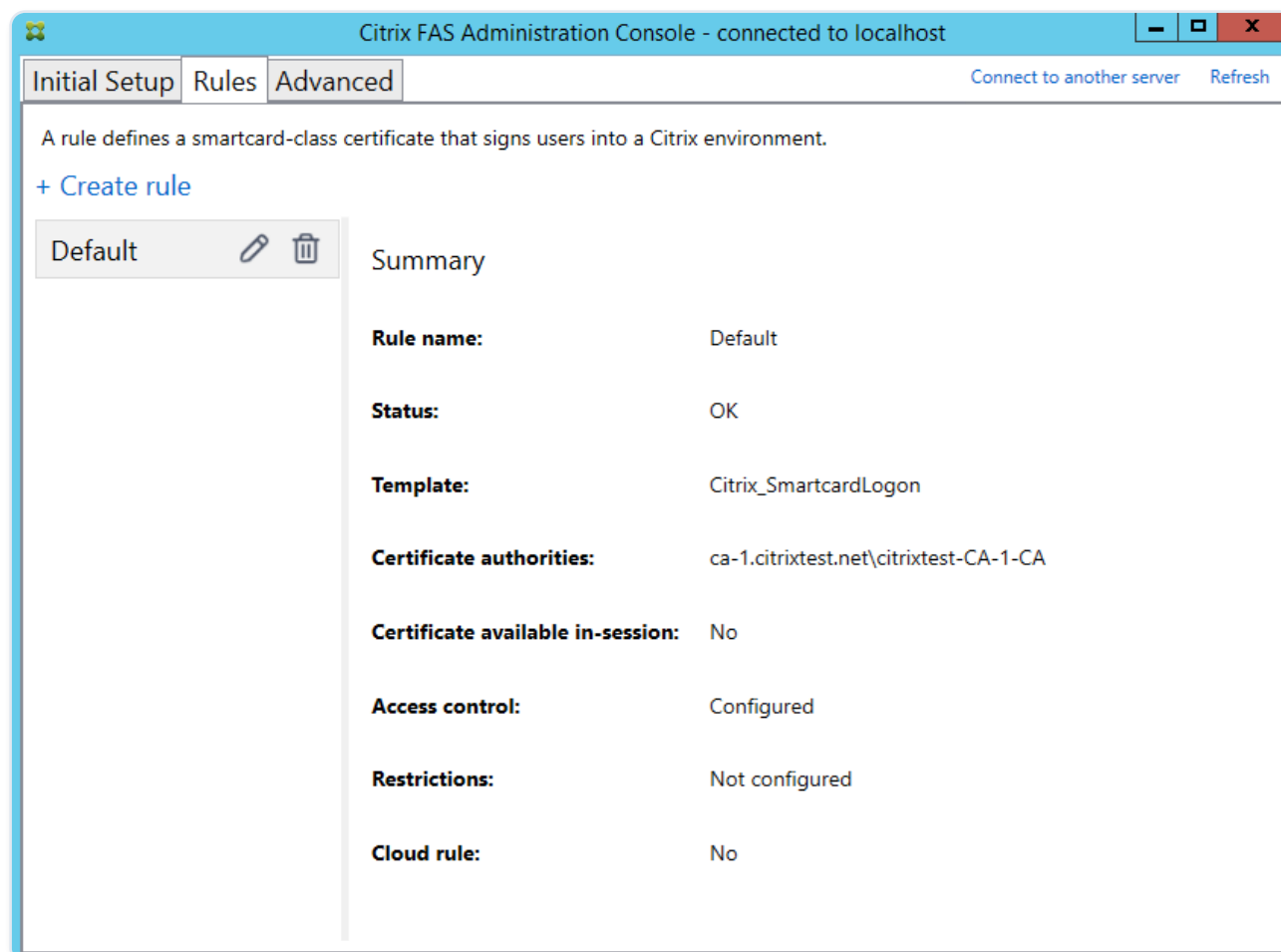
Klicken Sie mit der rechten Maustaste auf **Alle Aufgaben** und wählen Sie dann **Ausstellen** oder **Verweigern** für die Zertifikatanforderung. Die FAS-Verwaltungskonsolle erkennt automatisch, wann dieser Vorgang abgeschlossen ist. Dies kann einige Minuten dauern.



Benutzerregeln konfigurieren

Eine Benutzerregel autorisiert die Ausstellung von Zertifikaten für die VDA-Anmeldung und die Verwendung während der Sitzung, wie von StoreFront angewiesen. Jede Regel legt die StoreFront-Server fest, denen vertraut wird, Zertifikate anzufordern, die Gruppe von Benutzern, für die sie angefordert werden können, und die Gruppe von VDA-Maschinen, die sie verwenden dürfen.

Um die FAS-Einrichtung abzuschließen, müssen Sie die Standardregel definieren. Klicken Sie auf **Erstellen**, um eine Regel zu erstellen, oder wechseln Sie zur Registerkarte „Regeln“ und klicken Sie auf **Regel erstellen**. Der Assistent sammelt die Informationen, die zum Definieren einer Regel erforderlich sind.



Die folgenden Informationen werden vom Assistenten gesammelt:

Vorlage: Die Zertifikatvorlage, die zum Ausstellen von Benutzerzertifikaten verwendet wird. Dies sollte die Vorlage Citrix_SmartcardLogon oder eine geänderte Kopie davon sein.

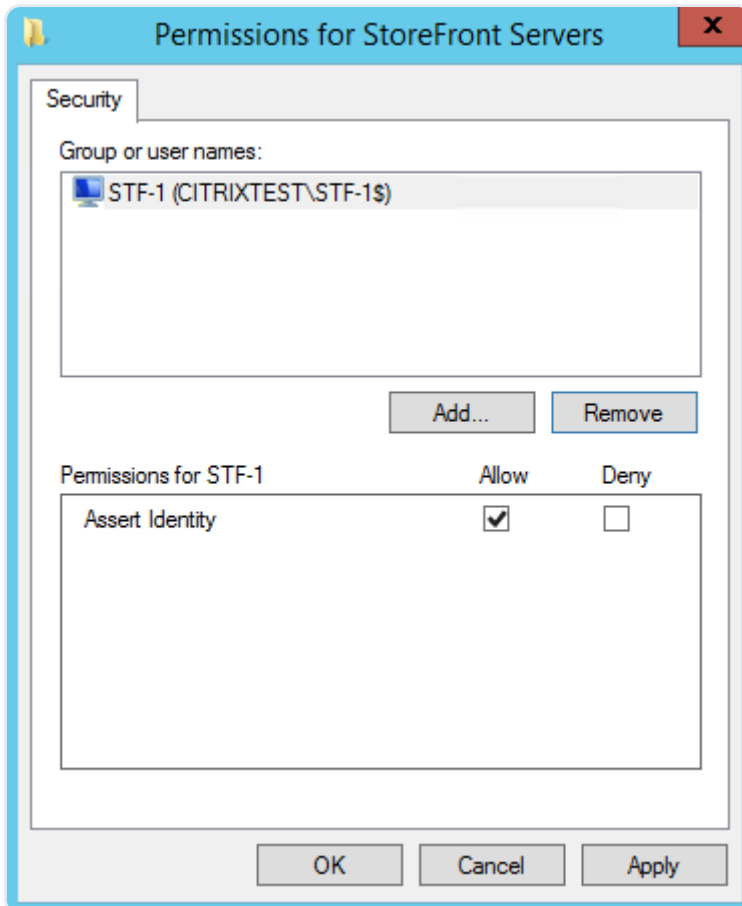
Zertifizierungsstelle: Die Zertifizierungsstelle, die Benutzerzertifikate ausstellt. Die Vorlage muss von der Zertifizierungsstelle veröffentlicht werden. FAS unterstützt das Hinzufügen mehrerer Zertifizierungsstellen für Failover und Lastenausgleich.

Verwendung während der Sitzung: Die Option **Verwendung während der Sitzung zulassen** steuert, ob ein Zertifikat nach der Anmeldung am VDA verwendet werden kann. Wählen Sie diese Option nur aus, wenn Benutzer nach der Authentifizierung Zugriff auf das Zertifikat haben sollen. Wenn diese Option nicht ausgewählt ist, wird das Zertifikat nur für die Anmeldung oder Wiederverbindung verwendet, und Benutzer haben nach der Authentifizierung keinen Zugriff auf das Zertifikat.

Zugriffssteuerung: Die Liste der vertrauenswürdigen StoreFront-Servermaschinen, die berechtigt sind, Zertifikate für die Anmeldung oder Wiederverbindung von Benutzern anzufordern.

WICHTIG:

Die Einstellung **Zugriffssteuerung** ist sicherheitskritisch und muss sorgfältig verwaltet werden.



Einschränkungen: Die Liste der VDA-Maschinen, die Benutzer über FAS anmelden können, und die Liste der Benutzer, denen Zertifikate über FAS ausgestellt werden können. Die Liste der VDAs ist standardmäßig auf Domain Computers eingestellt und die Liste der Benutzer ist standardmäßig auf Domain Users eingestellt; diese können geändert werden, wenn die Standardwerte ungeeignet sind.

Permissions for VDAs

Security

Group or user names:

Domain Computers (CITRIXTEST\Domain Computers)

Add...Remove

Permissions for Domain Computers

	Allow	Deny
Relying Party	☒	☐

OK

Cancel

Apply

Permissions for Users

Security

Group or user names:

Domain Users (CITRIXTEST\Domain Users)

Add...Remove

Permissions for Domain Users

	Allow	Deny
User Authentication	☒	☐

OK

Cancel

Apply

Cloud-Regel: Derzeit nicht unterstützt.

Erweiterte Nutzung

Sie können zusätzliche Regeln erstellen, um auf verschiedene Zertifikatvorlagen und Zertifizierungsstellen zu verweisen, die mit unterschiedlichen Eigenschaften und Berechtigungen konfiguriert werden können. Diese Regeln können für die Verwendung durch verschiedene StoreFront-Server konfiguriert werden, die so konfiguriert werden müssen, dass sie die neue Regel namentlich anfordern. Standardmäßig fordert StoreFront **default** an, wenn es FAS kontaktiert. Dies kann über die Gruppenrichtlinien-Konfigurationsoptionen geändert werden.

Um eine neue Zertifikatvorlage zu erstellen, duplizieren Sie die Vorlage Citrix_SmartcardLogon in der Microsoft-Zertifizierungsstellenkonsole, benennen Sie sie um (z. B. Citrix_SmartcardLogon2) und ändern Sie sie nach Bedarf. Erstellen Sie eine neue Benutzerregel, indem Sie auf **Hinzufügen** klicken, um auf die neue Zertifikatvorlage zu verweisen.

Überlegungen zum Upgrade

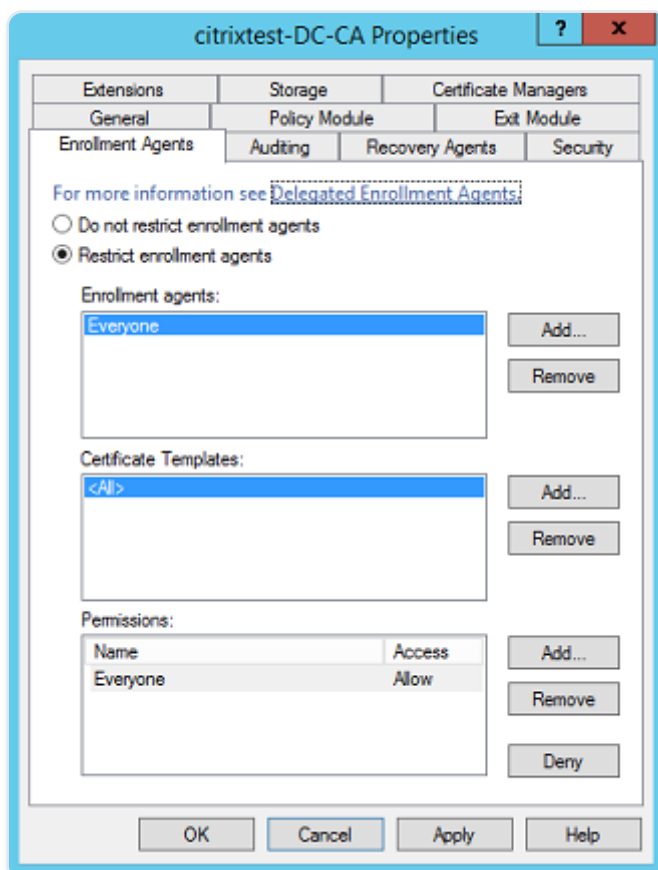
- Alle FAS-Servereinstellungen bleiben erhalten, wenn Sie ein direktes Upgrade durchführen.
- Führen Sie ein Upgrade von FAS durch, indem Sie das Installationsprogramm für das vollständige Produkt Virtual Apps and Desktops ausführen.
- Bevor Sie FAS aktualisieren, aktualisieren Sie den Controller und die VDAs (sowie andere Kernkomponenten) auf die erforderliche Version.
- Stellen Sie sicher, dass die FAS-Verwaltungskonsole geschlossen ist, bevor Sie FAS aktualisieren.
- Stellen Sie sicher, dass jederzeit mindestens ein FAS-Server verfügbar ist. Wenn kein Server von einem für den Federation Authentication Service aktivierten StoreFront-Server erreichbar ist, können sich Benutzer nicht anmelden oder Anwendungen starten.

Sicherheitsüberlegungen

FAS verfügt über ein Registrierungsstellenzertifikat, das es ihm ermöglicht, autonom Zertifikate im Namen Ihrer Domänenbenutzer auszustellen. Daher ist es wichtig, eine Sicherheitsrichtlinie zu entwickeln und zu implementieren, um FAS-Server zu schützen und ihre Berechtigungen einzuschränken.

Delegierte Registrierungsagenten

FAS stellt Benutzerzertifikate aus, indem es als Registrierungsagent fungiert. Die Microsoft-Zertifizierungsstelle ermöglicht die Kontrolle darüber, welche Vorlagen der FAS-Server verwenden kann, sowie die Einschränkung, für welche Benutzer der FAS-Server Zertifikate ausstellen kann.



Citrix empfiehlt dringend, diese Optionen so zu konfigurieren, dass FAS Zertifikate nur für die vorgesehenen Benutzer ausstellen kann. Es ist beispielsweise eine bewährte Praxis, zu verhindern, dass FAS Zertifikate für Benutzer in einer Administrations- oder geschützten Benutzergruppe ausstellt.

Konfiguration der Zugriffssteuerungsliste

Wie im Abschnitt [Benutzerregeln konfigurieren](#) beschrieben, müssen Sie eine Liste von StoreFront-Servern konfigurieren, denen vertraut wird, Benutzeridentitäten gegenüber FAS zu bestätigen, wenn Zertifikate ausgestellt werden. Ähnlich können Sie einschränken, welchen Benutzern Zertifikate ausgestellt werden und an welchen VDA-Maschinen sie sich authentifizieren können. Dies geschieht zusätzlich zu allen standardmäßigen Sicherheitsfunktionen von Active Directory oder Zertifizierungsstellen, die Sie konfigurieren.

Firewall-Einstellungen

Die gesamte Kommunikation mit FAS-Servern verwendet gegenseitig authentifizierte Windows Communication Foundation (WCF) Kerberos-Netzwerkverbindungen über Port 80.

Ereignisprotokollüberwachung

FAS und der VDA schreiben Informationen in das Windows-Ereignisprotokoll. Dies kann zur Überwachung und Prüfung von Informationen verwendet werden. Der Abschnitt [Ereignisprotokolle](#) listet Ereignisprotokolleinträge auf, die generiert werden können.

Hardwaresicherheitsmodule

Alle privaten Schlüssel, einschließlich der von FAS ausgestellten Benutzerzertifikate, werden vom Network Service-Konto als nicht exportierbare private Schlüssel gespeichert. FAS unterstützt die Verwendung eines kryptografischen Hardware Sicherheitsmoduls, falls Ihre Sicherheitsrichtlinie dies erfordert.

Die kryptografische Konfiguration auf niedriger Ebene ist in der Datei `FederatedAuthenticationService.exe.config` verfügbar. Diese Einstellungen werden angewendet, wenn private Schlüssel zum ersten Mal erstellt werden. Daher können unterschiedliche Einstellungen für private Schlüssel der Registrierungsstelle (z. B. 4096 Bit, TPM-geschützt) und Laufzeit-Benutzerzertifikate verwendet werden.

PARAMETER	BESCHREIBUNG
ProviderLegacyCsp	Wenn auf true gesetzt, verwendet FAS die Microsoft CryptoAPI (CAPI). Andernfalls verwendet FAS die Microsoft Cryptography Next Generation API (CNG).
ProviderName	Name des zu verwendenden CAPI- oder CNG-Anbieters.
ProviderType	Bezieht sich auf Microsoft KeyContainerPermissionAccessEntry.Provider Type Property PROV_RSA_AES 24. Sollte immer 24 sein, es sei denn, Sie verwenden ein HSM mit CAPI und der HSM-Anbieter gibt etwas anderes an.
KeyProtection	Steuert das Flag „Exportierbar“ für private Schlüssel. Ermöglicht auch die Verwendung des Trusted Platform Module (TPM) Schlüsselspeichers, sofern von der Hardware unterstützt.

PARAMETER	BESCHREIBUNG
KeyLength	Schlüssellänge für private RSA-Schlüssel. Unterstützte Werte sind 1024, 2048 und 4096 (Standard: 2048).

PowerShell SDK

Obwohl die FAS-Verwaltungskonsole für einfache Bereitstellungen geeignet ist, bietet die PowerShell-Schnittstelle erweiterte Optionen. Wenn Sie Optionen verwenden, die in der Konsole nicht verfügbar sind, empfiehlt Citrix, für die Konfiguration ausschließlich PowerShell zu verwenden.

Der folgende Befehl fügt die PowerShell-Cmdlets hinzu:

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

Verwenden Sie **Get-Help** \<cmdlet name> , um die Cmdlet-Hilfe anzuzeigen. Die folgende Tabelle listet mehrere Befehle auf, wobei * ein Standard-PowerShell-Verb (wie New, Get, Set, Remove) darstellt.

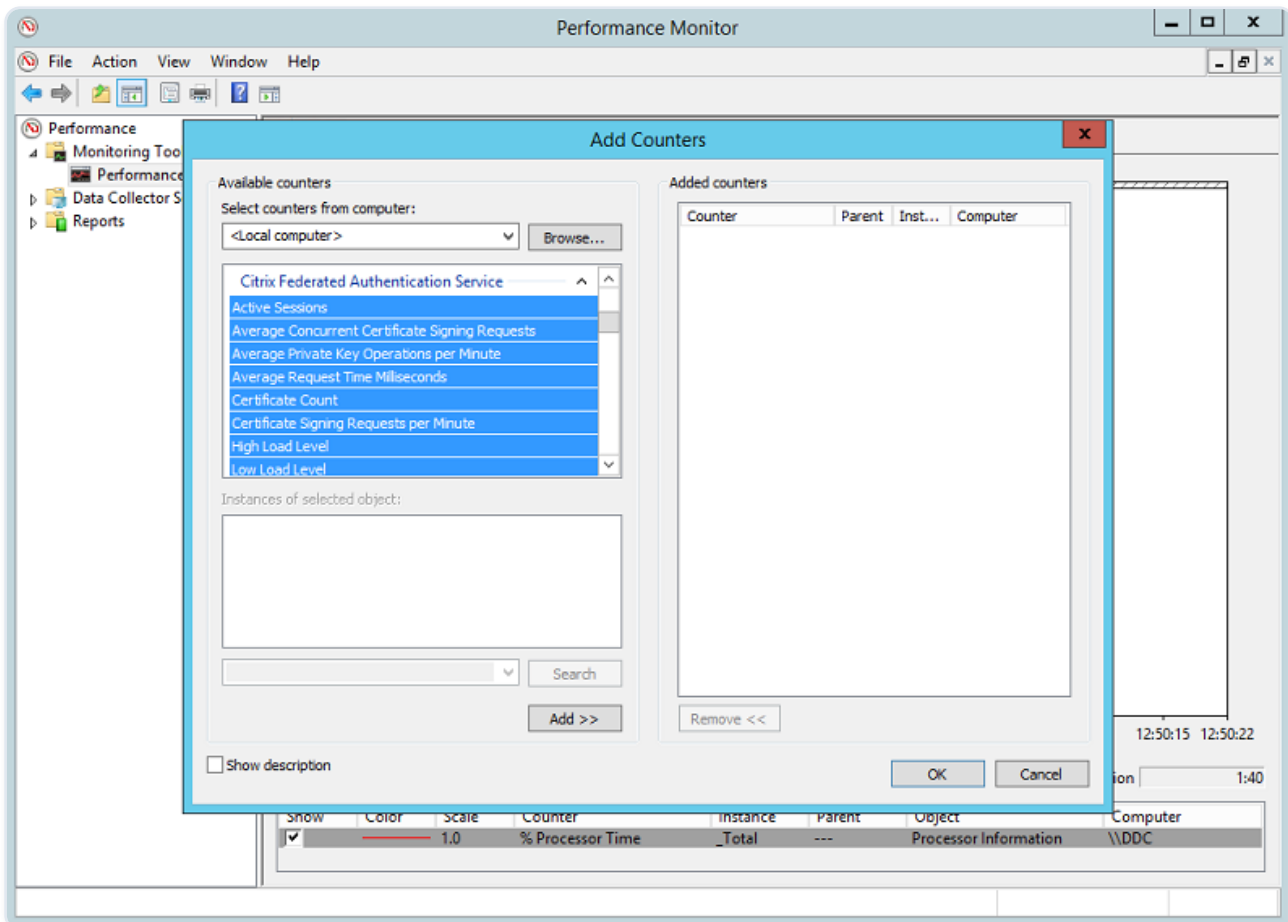
BEFEHLE	ÜBERSICHT
*-FasServer	Listet und rekonfiguriert die FAS-Server in der aktuellen Umgebung.
*-FasAuthorizationCertificate	Verwaltet das Zertifikat der Registrierungsstelle.
*-FasCertificateDefinition	Steuert die Parameter, die FAS zum Generieren von Zertifikaten verwendet.
*-FasRule	Verwaltet auf FAS konfigurierte Benutzerregeln.
*-FasUserCertificate	Listet und verwaltet von FAS zwischengespeicherte Zertifikate.

PowerShell-Cmdlets können remote verwendet werden, indem die Adresse eines FAS-Servers angegeben wird.

Informationen zu FAS PowerShell-Cmdlets finden Sie unter [PowerShell-Cmdlets](#).

Leistungsindikatoren

FAS enthält einen Satz Leistungsindikatoren zur Lastverfolgung.



Die folgende Tabelle listet die verfügbaren Leistungsindikatoren auf. Die meisten Leistungsindikatoren sind gleitende Durchschnitte über fünf Minuten.

NAME	BESCHREIBUNG
Aktive Sitzungen	Anzahl der von FAS verfolgten Verbindungen.
Gleichzeitige CSRs	Anzahl der gleichzeitig verarbeiteten Zertifikatanforderungen.
Private Schlüsseloperationen	Anzahl der pro Minute durchgeführten privaten Schlüsseloperationen.
Anforderungszeit	Zeitdauer zum Generieren und Signieren eines Zertifikats.

NAME	BESCHREIBUNG
Zertifikatsanzahl	Anzahl der in FAS zwischengespeicherten Zertifikate.
CSR pro Minute	Anzahl der pro Minute verarbeiteten Zertifikatsignieranforderungen.
Niedrig/Mittel/Hoch	Schätzungen der Last, die FAS in Bezug auf „CSRs pro Minute“ verarbeiten kann. Das Überschreiten des Schwellenwerts für „hohe Last“ kann dazu führen, dass Sitzungsstarts fehlschlagen.

Ereignisprotokolle

Die folgenden Tabellen listen die von FAS generierten Ereignisprotokolleinträge auf.

Verwaltungsereignisse

Diese Ereignisse werden als Reaktion auf eine Konfigurationsänderung im FAS-Server protokolliert.

PROTOKOLLCODES
[S001] ZUGRIFF VERWEIGERT: Benutzer [{0}] ist kein Mitglied der Administratorengruppe
[S002] ZUGRIFF VERWEIGERT: Benutzer [{0}] ist kein Administrator der Rolle [{1}]
[S003] Administrator [{0}] setzt den Wartungsmodus auf [{1}]
[S004] Administrator [{0}] registriert sich bei CA [{1}] mit Vorlagen [{2}] and {3}]
[S005] Administrator [{0}] deautorisiert CA [{1}]
[S006] Administrator [{0}] erstellt neue Zertifikatsdefinition [{1}]
[S007] Administrator [{0}] aktualisiert Zertifikatsdefinition [{1}]
[S008] Administrator [{0}] löscht Zertifikatsdefinition [{1}]
[S009] Administrator [{0}] erstellt neue Rolle [{1}]

PROTOKOLLCODES
[S010] Administrator [{0}] aktualisiert Rolle [{1}]
[S011] Administrator [{0}] löscht Rolle [{1}]
[S012] Administrator [{0}] erstellt Zertifikat [upn: {1} sid: {2} role: {3} Certificate Definition: {4} Security Context: {5}]
[S013] Administrator [{0}] löscht Zertifikate [upn: {1} role: {2} Certificate Definition: {3} Security Context: {4}]
[S015] Administrator [{0}] erstellt Zertifikatsanforderung [TPM: {1}]
[S016] Administrator [{0}] importiert Autorisierungszertifikat [Reference: {1}]

PROTOKOLLCODES
[S401] Führt Konfigurationsupgrade durch -- [From version {0} to version {1}]
[S402] FEHLER: Der Citrix Federated Authentication Service muss als Netzwerkdienst ausgeführt werden [currently running as: {0}]
[S404] Die Datenbank des Citrix Federated Authentication Service wird zwangsweise gelöscht
[S405] Beim Migrieren von Daten aus der Registrierung in die Datenbank ist ein Fehler aufgetreten: [{0}]
[S406] Die Migration der Daten aus der Registrierung in die Datenbank ist abgeschlossen (Hinweis: Benutzerzertifikate werden nicht migriert)
[S407] Registrierungsbasierte Daten wurden nicht in eine Datenbank migriert, da bereits eine Datenbank vorhanden war
[S408] Konfiguration kann nicht herabgestuft werden -- [From version {0} to version {1}]
[S409] ThreadPool MinThreads angepasst von [workers: {0} completion: {1}] auf: [workers: {2} completion: {3}]
[S410] Fehler beim Anpassen von ThreadPool MinThreads von [workers: {0} completion: {1}] auf: [workers: {2} completion: {3}]

Erstellen von Identitätszusicherungen

Diese Ereignisse werden zur Laufzeit auf dem FAS-Server protokolliert, wenn ein vertrauenswürdiger Server eine Benutzeranmeldung zusichert.

PROTOKOLLCODES
[S101] Server [{0}] ist nicht berechtigt, Identitäten in der Rolle [{1}] zuzusichern
[S102] Server [{0}] Fehler beim Zusichern des UPN [{1}] (Ausnahme: {2}{3})
[S103] Server [{0}] forderte UPN [{1}] SID {2} an, aber die Suche ergab SID {3}
[S104] Server [{0}] Fehler beim Zusichern des UPN [{1}] (UPN in Rolle [{2}] nicht zulässig)
[S105] Server [{0}] hat Identitätszusicherung ausgestellt [upn: {1}, role {2}, Security Context: [{3}]]
[S120] Zertifikat ausstellen für [upn: {0} role: {1} Security Context: [{2}]]
[S121] Zertifikat ausgestellt für [upn: {0} role: {1}] von [certificate authority: {2}]
[S122] Warnung: Server ist überlastet [upn: {0} role: {1}][Anfragen pro Minute {2}].
[S123] Fehler beim Ausstellen eines Zertifikats für [upn: {0} role: {1}] [exception: {2}]
[S124] Fehler beim Ausstellen eines Zertifikats für [upn: {0} role: {1}] bei [certificate authority: {2}] [exception: {3}]

Als vertrauende Partei agieren

Diese Ereignisse werden zur Laufzeit auf dem FAS-Server protokolliert, wenn ein VDA einen Benutzer anmeldet.

PROTOKOLLCODES
[S201] Vertrauende Partei [{0}] hat keinen Zugriff auf ein Kennwort.
[S202] Vertrauende Partei [{0}] hat keinen Zugriff auf ein Zertifikat.
[S203] Vertrauende Partei [{0}] hat keinen Zugriff auf den Anmelde-CSP
[S204] Vertrauende Partei [{0}] greift auf den Anmelde-CSP für [upn: {1}] in der Rolle: [{2}] [Operation: {3}] autorisiert durch [{4}]

PROTOKOLLCODES
[S205] Aufrufendes Konto [{0}] ist keine vertrauende Partei in der Rolle [{1}]
[S206] Aufrufendes Konto [{0}] ist keine vertrauende Partei
[S208] Vorgang mit privatem Schlüssel fehlgeschlagen [Operation: {0} upn: {1} role: {2} certificateDefinition {3} Error {4} {5}].

Sitzungsinterner Zertifikatsserver

Diese Ereignisse werden auf dem FAS-Server protokolliert, wenn ein Benutzer ein sitzungsinternes Zertifikat verwendet.

PROTOKOLLCODES
[S301] Zugriff verweigert: Benutzer [{0}] hat keinen Zugriff auf eine virtuelle Smartcard
[S302] Benutzer [{0}] hat eine unbekannte virtuelle Smartcard [thumbprint: {1}] angefordert
[S303] Zugriff verweigert: Benutzer [{0}] stimmt nicht mit der virtuellen Smartcard [upn: {1}] überein
[S304] Benutzer [{0}] führt Programm [{1}] auf Computer [{2}] aus und verwendet virtuelle Smartcard [upn: {3} role: {4} thumbprint: {5}] für privaten Schlüsselvorgang [{6}]
[S305] Privater Schlüsselvorgang fehlgeschlagen [Operation: {0} upn: {1} role: {2} containerName {3} Error {4} {5}].

FAS-Assertions-Plug-in

Diese Ereignisse werden vom FAS-Assertions-Plug-in protokolliert.

PROTOKOLLCODES
[S500] Kein FAS-Assertions-Plug-in konfiguriert
[S501] Das konfigurierte FAS-Assertions-Plug-in konnte nicht geladen werden [exception:{0}]
[S502] FAS-Assertions-Plug-in geladen [pluginId={0}] [assembly={1}] [location={2}]
[S503] Server [{0}] konnte UPN [{1}] nicht bestätigen (Anmeldeinformationen wurden bereitgestellt, aber das Plug-in [{2}] unterstützt dies nicht)

PROTOKOLLCODES
[S504] Server [{0}] konnte UPN [{1}] nicht bestätigen (Anmeldeinformationen wurden bereitgestellt, aber es ist kein FAS-Plug-in konfiguriert)
[S505] Server [{0}] konnte UPN [{1}] nicht beanspruchen (das Plugin [{2}] hat die Anmeldeinformationen mit Status [{3}] und Meldung [{4}] abgelehnt)
[S506] Das Plugin [{0}] hat die Anmeldeinformationen vom Server [{1}] für UPN [{2}] mit Meldung [{3}] akzeptiert
[S507] Server [{0}] konnte UPN [{1}] nicht beanspruchen (das Plugin [{2}] hat Ausnahme [{3}] ausgelöst)
[S507] Server [{0}] konnte UPN [{1}] nicht beanspruchen (das Plugin [{2}] hat Ausnahme [{3}] ausgelöst)
[S508] Server [{0}] konnte UPN [{1}] nicht beanspruchen (Zugriffsdisposition wurde bereitgestellt, aber das Plugin [{2}] unterstützt sie nicht)
[S509] Server [{0}] konnte UPN [{1}] nicht beanspruchen (Zugriffsdisposition wurde bereitgestellt, aber es ist kein FAS-Plugin konfiguriert)
[S510] Server [{0}] konnte UPN [{1}] nicht beanspruchen (die Zugriffsdisposition wurde vom Plugin [{2}] als ungültig erachtet)

Anmelden

Diese Ereignisse werden auf dem VDA während der Anmeldephase protokolliert.

PROTOKOLLCODES
[S101] Anmeldung mit Identitätsbestätigung fehlgeschlagen. Nicht erkannter Federated Authentication Service [id: {0}]
[S102] Anmeldung mit Identitätsbestätigung fehlgeschlagen. SID für {0} konnte nicht nachgeschlagen werden [Exception: {1}{2}]
[S103] Anmeldung mit Identitätsbestätigung fehlgeschlagen. Benutzer {0} hat SID {1}, erwartet wurde SID {2}
[S104] Anmeldung mit Identitätsbestätigung fehlgeschlagen. Verbindung zum Federated Authentication Service fehlgeschlagen: {0} [Error: {1} {2}]

PROTOKOLLCODES
[S105] Identitätsbestätigungs-Anmeldung. Anmeldung [Username: {0} Domain: {1}]
[S106] Identitätsbestätigungs-Anmeldung. Anmeldung [Certificate: {0}]
[S107] Identitätsbestätigungs-Anmeldung fehlgeschlagen. [Exception: {0}{1}]
[S108] Identitätsbestätigungs-Subsystem. ACCESS_DENIED [Caller: {0}]

Sitzungsinterne Zertifikate

Diese Ereignisse werden auf dem VDA protokolliert, wenn ein Benutzer versucht, ein sitzungsinternes Zertifikat zu verwenden.

PROTOKOLLCODES
[S201] Zugriff auf virtuelle Smartcard autorisiert durch [{0}] für [PID: {1} Program Name: {2} Certificate thumbprint: {3}]
[S203] Subsystem für virtuelle Smartcards. Zugriff verweigert [caller: {0}, session {1}]
[S204] Subsystem für virtuelle Smartcards. Smartcard-Unterstützung deaktiviert

Zertifikatanforderung und Schlüsselpaar-Generierung

Diese Ereignisse werden protokolliert, wenn der FAS-Server kryptografische Operationen auf niedriger Ebene durchführt.

PROTOKOLLCODES
[S001] TrustArea::TrustArea: Zertifikat installiert [TrustArea: {0}] [Certificate {1} TrustAreaJoinParameters{2}]
[S014] Pkcs10Request::Create: PKCS10-Anforderung erstellt [Distinguished Name {0}]
[S016] PrivateKey::Create [Identifier {0} MachineWide: {1} Provider: {2} ProviderType: {3} EllipticCurve: {4} KeyLength: {5} isExportable: {6}]
[S017] PrivateKey::Delete [CspName: {0}, Identifier {1}]

PROTOKOLLCODES
[S104] MicrosoftCertificateAuthority::GetCredentials: Autorisiert zur Verwendung von {0}
[S105] MicrosoftCertificateAuthority::SubmitCertificateRequest Fehler beim Senden der Antwort [{0}]
[S106] MicrosoftCertificateAuthority::SubmitCertificateRequest Zertifikat ausgestellt [{0}]
[S112] MicrosoftCertificateAuthority::SubmitCertificateRequest - Warten auf Genehmigung [CR_DISP_UNDER_SUBMISSION] [Reference: {0}]

Verwandte Informationen

- Die gängigen FAS-Bereitstellungen sind in [Bereitstellungsarchitekturen](#) zusammengefasst.
- „Anleitungen“ werden in [Erweiterte Konfiguration](#) vorgestellt.

Bereitstellungsarchitekturen

Einführung

Der Federated Authentication Service (FAS) ist eine Citrix®-Komponente, die sich in Ihre Active Directory-Zertifizierungsstelle integriert, wodurch Benutzer in einer Citrix-Umgebung nahtlos authentifiziert werden können. Dieses Dokument beschreibt verschiedene Authentifizierungsarchitekturen, die für Ihre Bereitstellung geeignet sein können.

Wenn aktiviert, delegiert FAS Benutzerauthentifizierungsentscheidungen an vertrauenswürdige StoreFront-Server. StoreFront verfügt über einen umfassenden Satz integrierter Authentifizierungsoptionen, die auf modernen Webtechnologien basieren, und ist mithilfe des StoreFront SDK oder von IIS-Plugins von Drittanbietern leicht erweiterbar. Das grundlegende Designziel ist, dass jede Authentifizierungstechnologie, die einen Benutzer an einer Website authentifizieren kann, nun zum Anmelden bei einer Citrix Virtual Apps- oder Citrix Virtual Desktops™-Bereitstellung verwendet werden kann.

Dieses Dokument beschreibt beispielhafte übergeordnete Bereitstellungsarchitekturen in aufsteigender Komplexität.

- [Interne Bereitstellung](#)
- [Citrix Gateway-Bereitstellung](#)
- [ADFS SAML](#)
- [B2B-Kontenzuordnung](#)
- [Windows 10 Azure AD-Beitritt](#)

Es werden Links zu verwandten FAS-Artikeln bereitgestellt. Für alle Architekturen ist der Artikel [Installieren und Konfigurieren](#) die primäre Referenz für die Einrichtung von FAS.

Funktionsweise

FAS ist berechtigt, automatisch Smartcard-Klassenzertifikate im Namen von Active Directory-Benutzern auszustellen, die von StoreFront authentifiziert werden. Dies verwendet ähnliche APIs wie Tools, die Administratoren das Bereitstellen physischer Smartcards ermöglichen.

Wenn ein Benutzer an einen Citrix Virtual Apps™- oder Citrix Virtual Desktops Virtual Delivery Agent (VDA) vermittelt wird, wird das Zertifikat an den Computer angehängt, und die Windows-Domäne betrachtet die Anmeldung als eine standardmäßige Smartcard-Authentifizierung.

Interne Bereitstellung

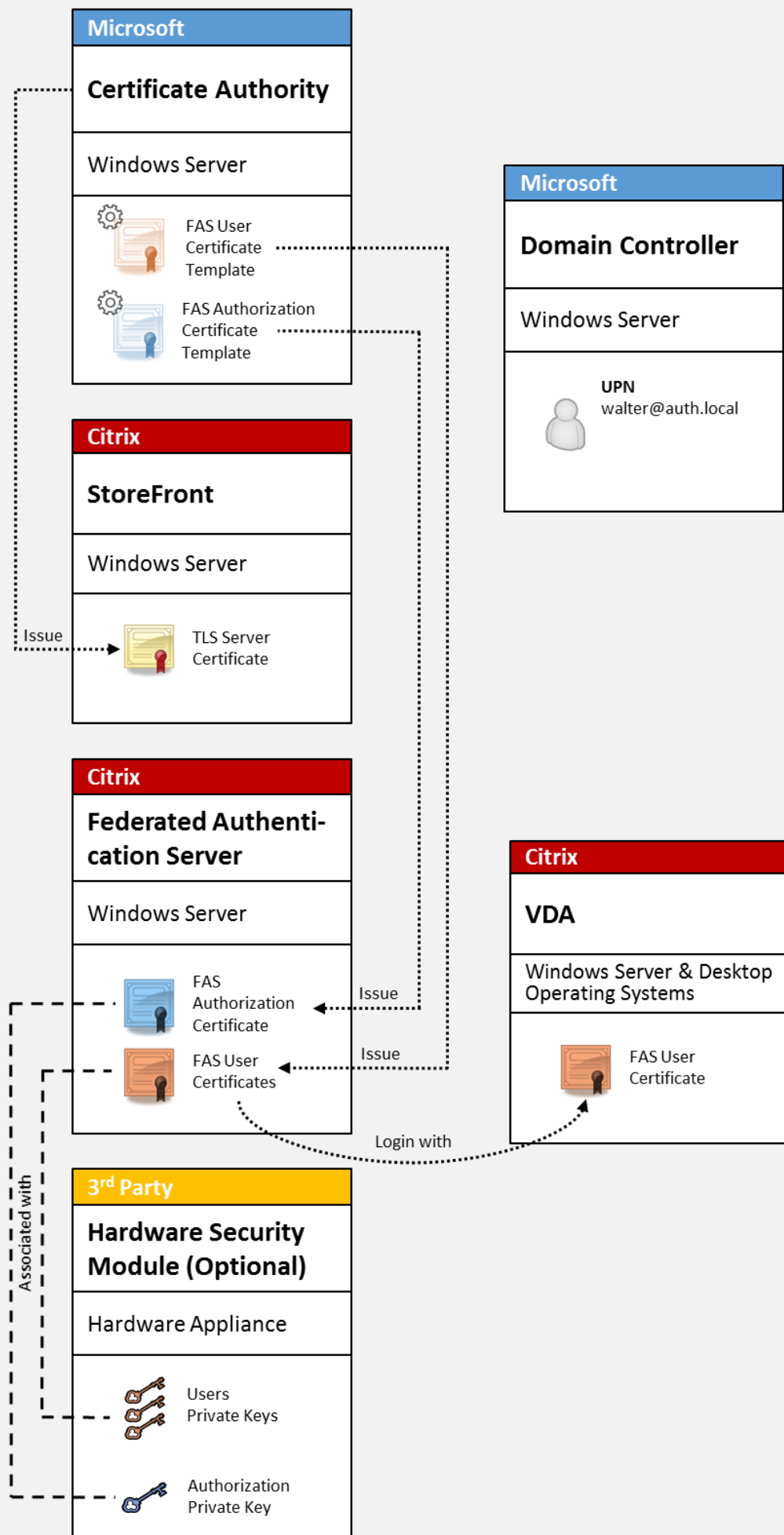
FAS ermöglicht Benutzern die sichere Authentifizierung bei StoreFront mit einer Vielzahl von Authentifizierungsoptionen (einschließlich Kerberos-Single-Sign-On) und die Verbindung zu einer vollständig authentifizierten Citrix HDX™-Sitzung.

Dies ermöglicht die Windows-Authentifizierung ohne Aufforderung zur Eingabe von Benutzeranmeldeinformationen oder Smartcard-PINs und ohne die Verwendung von Funktionen zur „gespeicherten Kennwortverwaltung“ wie dem Single Sign-on Service. Dies kann verwendet werden, um die in früheren Versionen von Citrix Virtual Apps verfügbaren Anmeldefunktionen für die eingeschränkte Kerberos-Delegierung zu ersetzen.

Alle Benutzer haben innerhalb ihrer Sitzung Zugriff auf PKI-Zertifikate (Public Key Infrastructure), unabhängig davon, ob sie sich mit einer Smartcard an den Endpunktgeräten anmelden oder nicht. Dies ermöglicht eine reibungslose Migration zu Zwei-Faktor-Authentifizierungsmodellen, selbst von Geräten wie Smartphones und Tablets, die keinen Smartcard-Leser besitzen.

Diese Bereitstellung fügt einen neuen Server hinzu, auf dem FAS ausgeführt wird, der berechtigt ist, Smartcard-Klassenzertifikate im Namen von Benutzern auszustellen. Diese Zertifikate werden dann verwendet, um sich bei Benutzersitzungen in einer Citrix HDX-Umgebung anzumelden, als ob eine Smartcard-Anmeldung verwendet worden wäre.

AUTH.LOCAL domain



Die Citrix Virtual Apps- oder Citrix Virtual Desktops-Umgebung muss ähnlich wie die Smartcard-Anmeldung konfiguriert werden, was in [CTX206156](#) dokumentiert ist.

In einer bestehenden Bereitstellung muss hierfür in der Regel nur sichergestellt werden, dass eine in die Domäne eingebundene Microsoft-Zertifizierungsstelle verfügbar ist und dass Domänencontrollern Domänencontroller-Zertifikate zugewiesen wurden. (Siehe den Abschnitt „Ausstellen von Domänencontroller-Zertifikaten“ in CTX206156.)

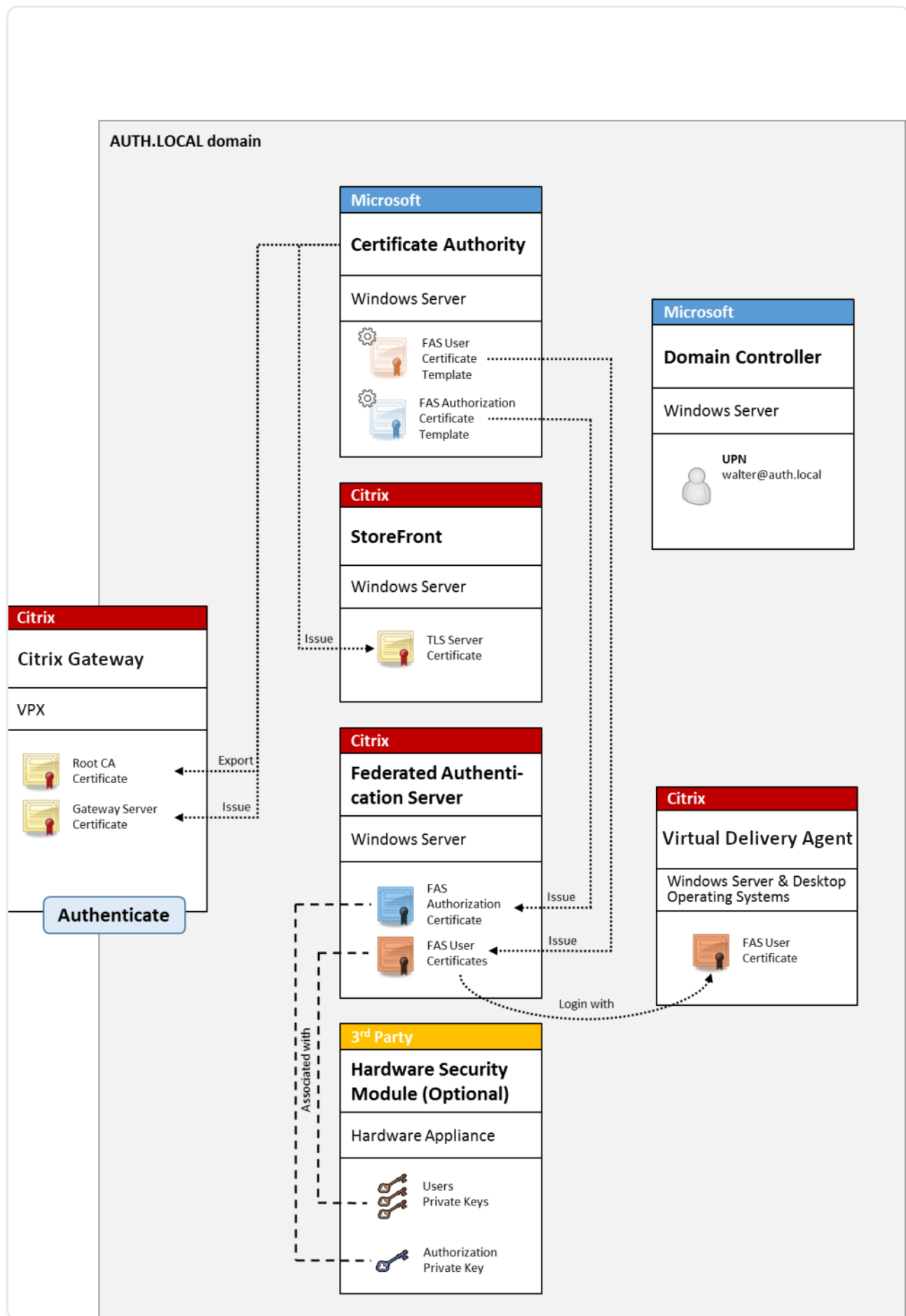
Zugehörige Informationen:

- Schlüssel können in einem Hardware Security Module (HSM) oder einem integrierten Trusted Platform Module (TPM) gespeichert werden. Weitere Informationen finden Sie im Artikel [Schutz privater Schlüssel](#).
- Der Artikel [Installieren und Konfigurieren](#) beschreibt, wie FAS installiert und konfiguriert wird.

Citrix Gateway-Bereitstellung

Die Citrix Gateway-Bereitstellung ähnelt der internen Bereitstellung, fügt jedoch Citrix Gateway in Verbindung mit StoreFront hinzu, wodurch der primäre Authentifizierungspunkt auf Citrix Gateway selbst verlagert wird. Citrix Gateway umfasst ausgeklügelte Authentifizierungs- und Autorisierungsoptionen, die zur Sicherung des Fernzugriffs auf die Websites eines Unternehmens verwendet werden können.

Diese Bereitstellung kann verwendet werden, um mehrere PIN-Eingabeaufforderungen zu vermeiden, die bei der Authentifizierung zuerst bei Citrix Gateway und dann bei der Anmeldung an einer Benutzersitzung auftreten. Sie ermöglicht auch die Verwendung fortschrittlicher Citrix Gateway-Authentifizierungstechnologien, ohne zusätzlich AD-Kennwörter oder Smartcards zu erfordern.



Die Citrix Virtual Apps- oder Citrix Virtual Desktops-Umgebung muss ähnlich wie die Smartcard-Anmeldung konfiguriert werden, was in [CTX206156](#) dokumentiert ist.

In einer bestehenden Bereitstellung muss in der Regel lediglich sichergestellt werden, dass eine in die Domäne eingebundene Microsoft-Zertifizierungsstelle verfügbar ist und dass Domänencontrollern Domänencontroller-Zertifikate zugewiesen wurden. (Siehe den Abschnitt „Ausstellen von Domänencontroller-Zertifikaten“ in CTX206156).

Wenn Sie Citrix Gateway als primäres Authentifizierungssystem konfigurieren, stellen Sie sicher, dass alle Verbindungen zwischen Citrix Gateway und StoreFront mit TLS gesichert sind. Stellen Sie insbesondere sicher, dass die Callback-URL korrekt konfiguriert ist und auf den Citrix Gateway-Server verweist, da dies zur Authentifizierung des Citrix Gateway-Servers in dieser Bereitstellung verwendet werden kann.

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: v10.0: SNIP or MIP, v10.1+: VIP

Logon type: Domain

Smart card fallback: None

Callback URL: https://NetScalerGatewayFQDN /CitrixAuthService/AuthService.asmx

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

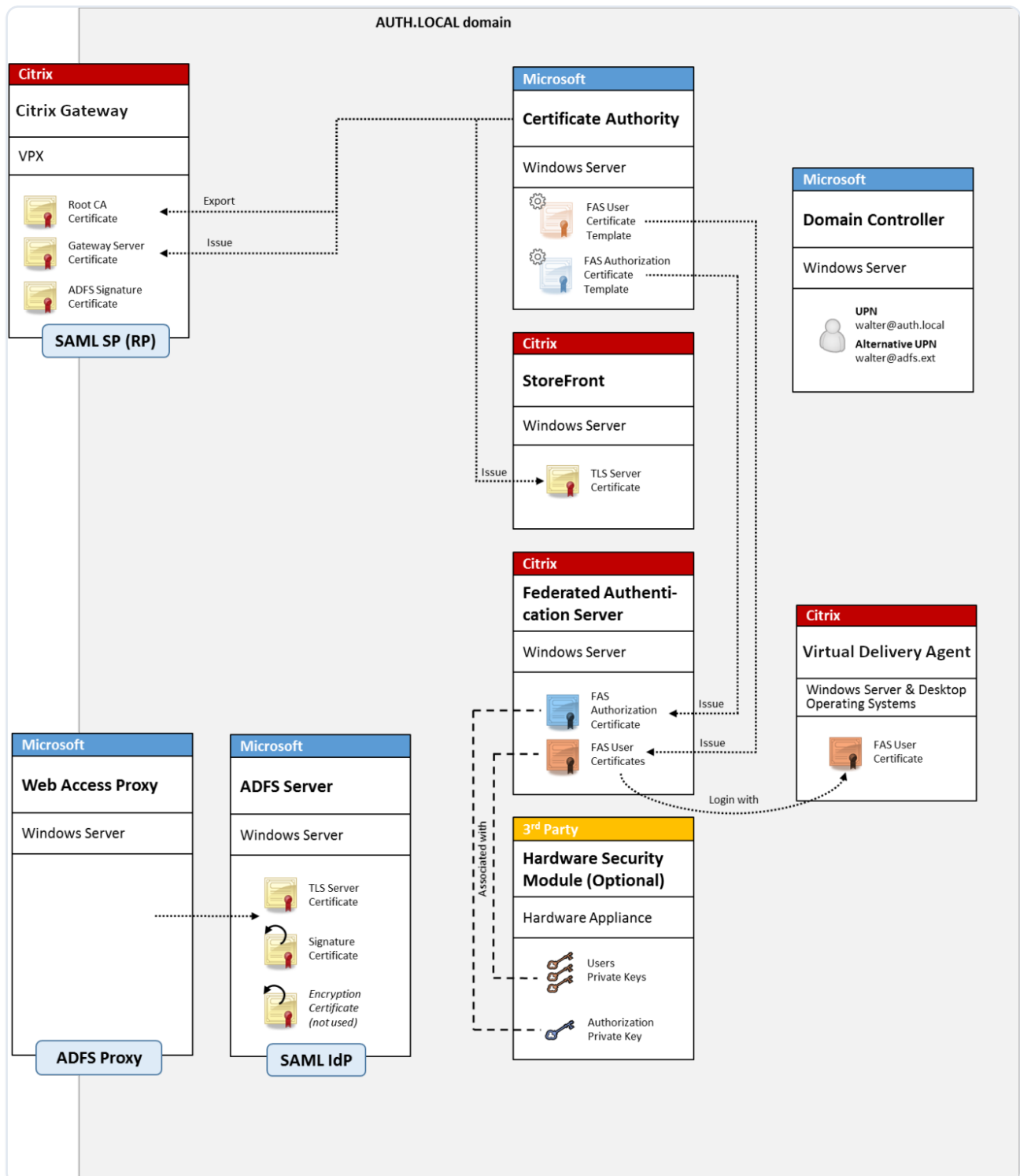
Back Create Cancel

Verwandte Informationen:

- Informationen zum Konfigurieren von Citrix Gateway finden Sie unter „[How to Configure NetScaler Gateway 10.5 to use with StoreFront 3.6 and Citrix Virtual Desktops 7.6](#)“.
- [Installieren und Konfigurieren](#) beschreibt, wie FAS installiert und konfiguriert wird.

ADFS SAML-Bereitstellung

Eine wichtige Authentifizierungstechnologie von Citrix Gateway ermöglicht die Integration mit Microsoft ADFS, das als SAML-Identitätsanbieter (IdP) fungieren kann. Eine SAML-Assertion ist ein kryptografisch signierter XML-Block, der von einem vertrauenswürdigen IdP ausgestellt wird und einen Benutzer zur Anmeldung an einem Computersystem autorisiert. Dies bedeutet, dass der FAS-Server die Authentifizierung eines Benutzers an den Microsoft ADFS-Server (oder einen anderen SAML-fähigen IdP) delegieren kann.



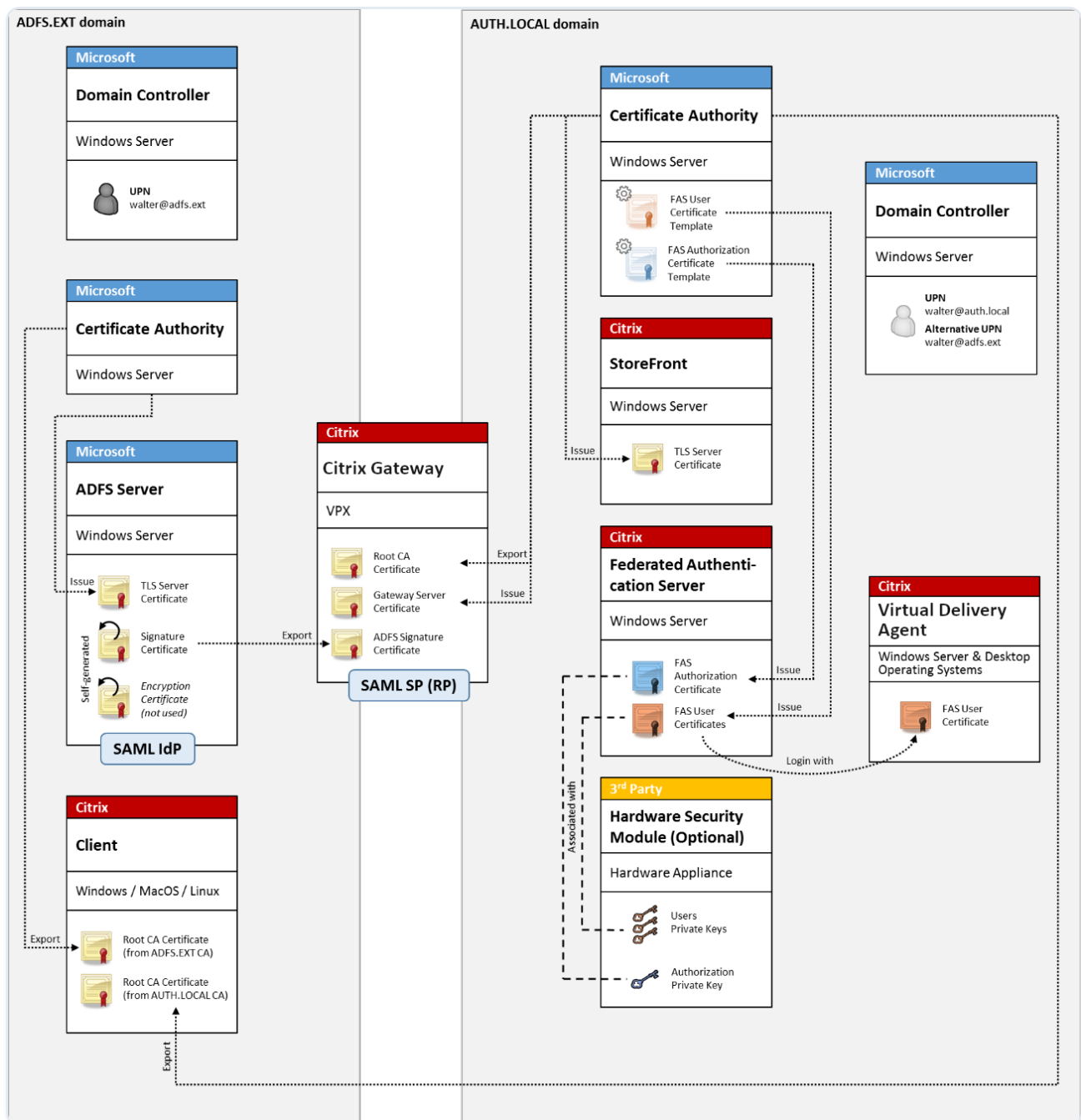
ADFS wird häufig verwendet, um Benutzer sicher und remote über das Internet bei Unternehmensressourcen zu authentifizieren; zum Beispiel wird es oft für die Office 365-Integration verwendet.

Verwandte Informationen:

- Der Artikel zur [ADFS-Bereitstellung](#) enthält Details.
- Der Artikel [Installieren und Konfigurieren](#) beschreibt, wie FAS installiert und konfiguriert wird.
- Der Abschnitt [Citrix Gateway-Bereitstellung](#) in diesem Artikel enthält Konfigurationsüberlegungen.

B2B-Kontenzuordnung

Wenn zwei Unternehmen die Computersysteme des jeweils anderen nutzen möchten, ist eine gängige Option, einen Active Directory Federation Service (ADFS)-Server mit einer Vertrauensstellung einzurichten. Dies ermöglicht Benutzern eines Unternehmens, sich nahtlos in die Active Directory (AD)-Umgebung eines anderen Unternehmens zu authentifizieren. Beim Anmelden verwendet jeder Benutzer seine eigenen Anmeldeinformationen des Unternehmens; ADFS ordnet dies automatisch einem „Schattenkonto“ in der AD-Umgebung des Partnerunternehmens zu.



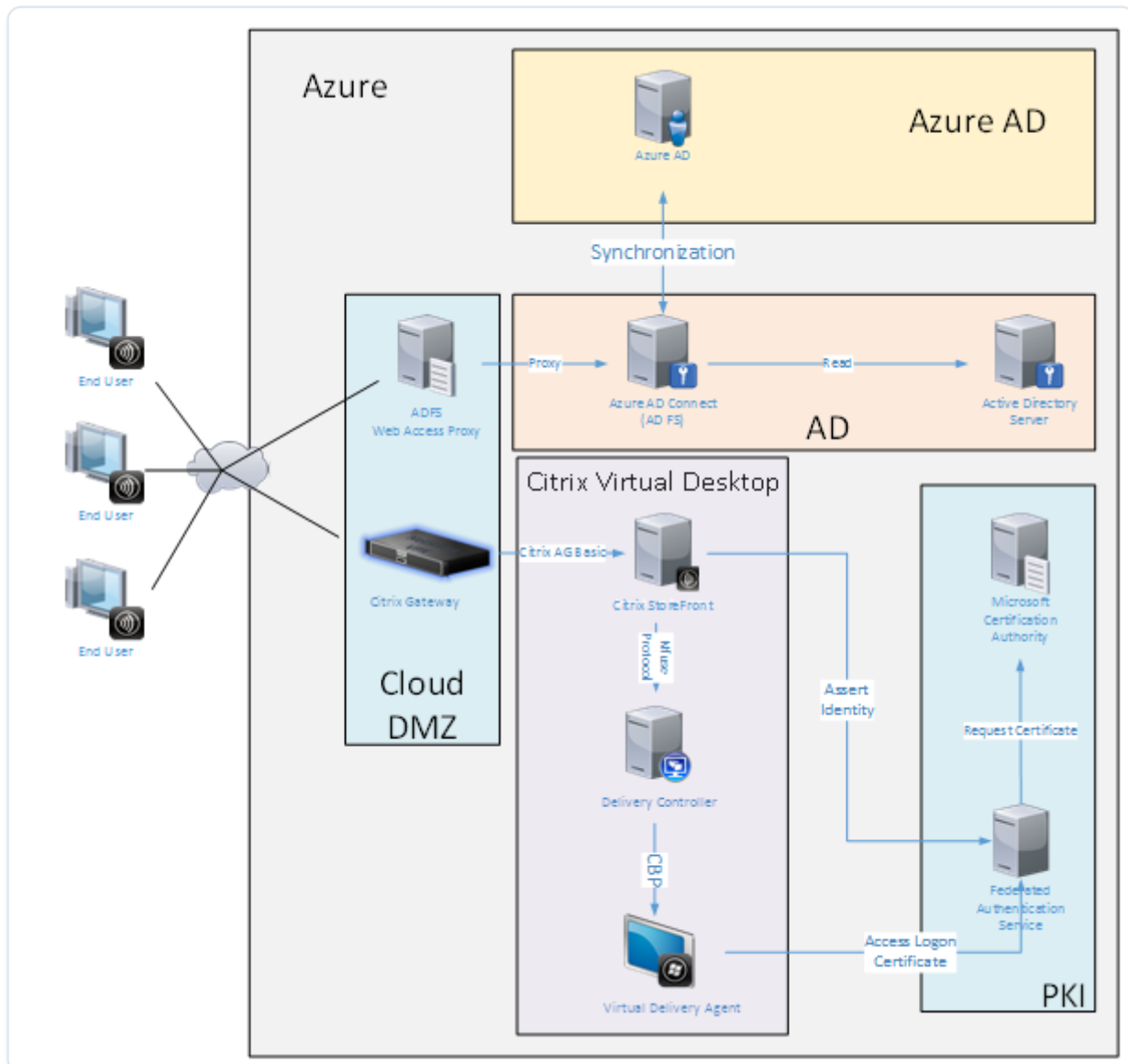
Verwandte Informationen:

- Der Artikel [Installieren und Konfigurieren](#) beschreibt, wie FAS installiert und konfiguriert wird.

Windows 10 Azure AD Join

Windows 10 führte das Konzept des „Azure AD Join“ ein, das konzeptionell dem traditionellen Windows-Domänenbeitritt ähnelt, aber auf „über das Internet“-Szenarien abzielt. Dies funktioniert gut mit Laptops und Tablets. Wie beim traditionellen Windows-Domänenbeitritt verfügt Azure AD über Funktionen, die Single-Sign-On-Modelle für Unternehmenswebsites und -ressourcen

ermöglichen. Diese sind alle „Internet-fähig“ und funktionieren daher von jedem mit dem Internet verbundenen Standort aus, nicht nur im Büronetzwerk (LAN).



Diese Bereitstellung ist ein Beispiel dafür, dass es effektiv kein Konzept von „Endbenutzern im Büro“ gibt. Laptops werden vollständig über das Internet registriert und authentifiziert, wobei moderne Azure AD-Funktionen verwendet werden.

Beachten Sie, dass die Infrastruktur in dieser Bereitstellung überall dort ausgeführt werden kann, wo eine IP-Adresse verfügbar ist: lokal, bei einem gehosteten Anbieter, in Azure oder bei einem anderen Cloud-Anbieter. Der Azure AD Connect-Synchronisator stellt automatisch eine Verbindung zu Azure AD her. Die Beispielgrafik verwendet Azure-VMs der Einfachheit halber.

Verwandte Informationen:

- Der Artikel [Installieren und Konfigurieren](#) beschreibt, wie FAS installiert und konfiguriert wird.
- Der Artikel [Azure AD-Integration](#) enthält Details.

ADFS-Bereitstellung

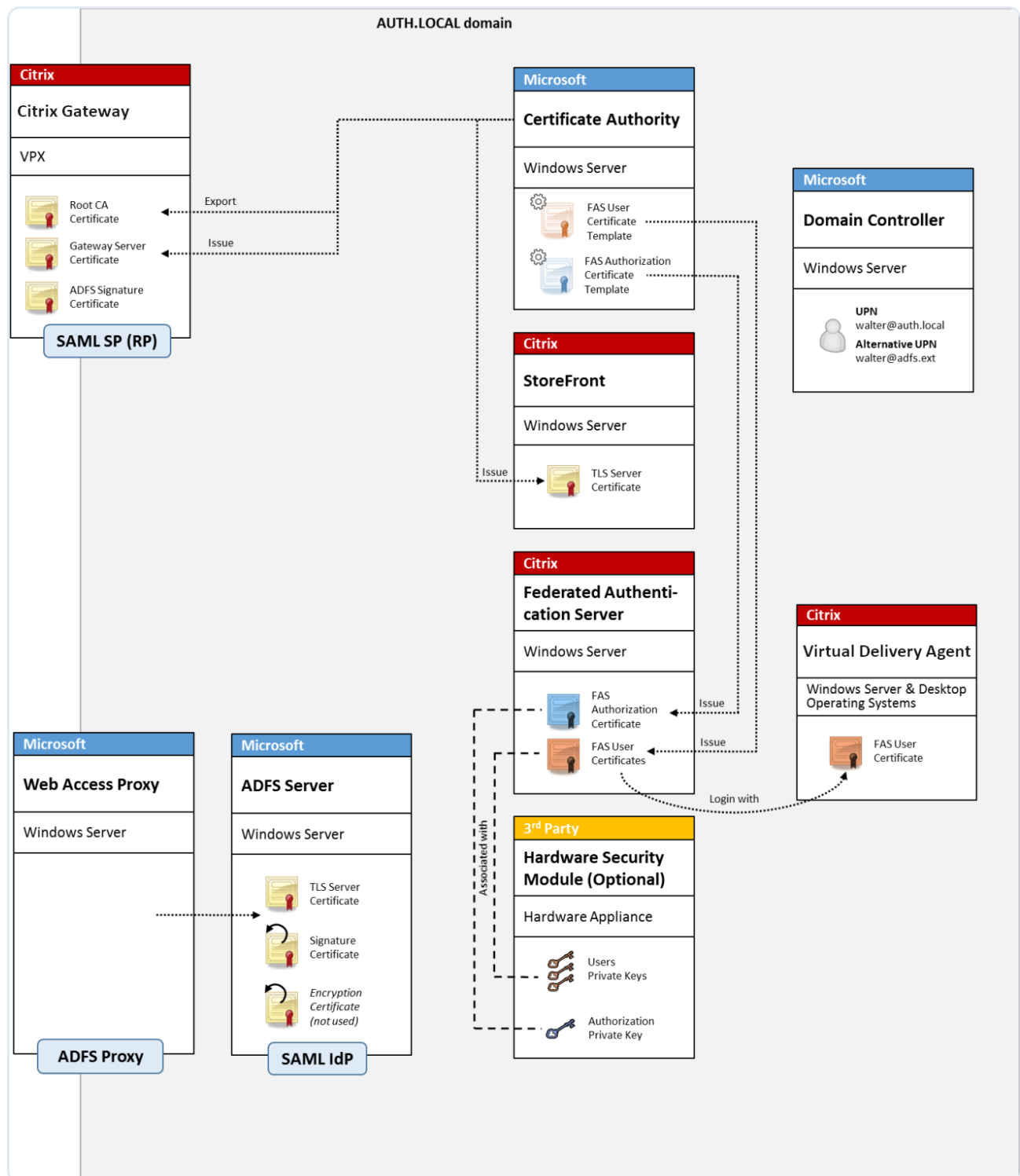
Einführung

Dieses Dokument beschreibt, wie eine Citrix®-Umgebung in Microsoft ADFS integriert wird.

Viele Organisationen verwenden ADFS, um den sicheren Benutzerzugriff auf Websites zu verwalten, die einen einzigen Authentifizierungspunkt erfordern. Beispielsweise kann ein Unternehmen zusätzliche Inhalte und Downloads für Mitarbeiter bereitstellen; diese Speicherorte müssen mit Standard-Windows-Anmeldeinformationen geschützt werden.

Der Federated Authentication Service (FAS) ermöglicht auch die Integration von Citrix Gateway und Citrix StoreFront™ in das ADFS-Anmeldesystem, wodurch potenzielle Verwirrung für die Mitarbeiter des Unternehmens reduziert wird.

Diese Bereitstellung integriert Citrix Gateway als vertrauende Seite in Microsoft ADFS.

**HINWEIS:**

Es gibt keine Unterschiede, ob die Backend-Ressource entweder Windows VDA oder Linux VDA ist.

SAML-Übersicht

Security Assertion Markup Language (SAML) ist ein einfaches Webbrowser-Anmeldesystem, das eine „Weiterleitung zu einer Anmeldeseite“ verwendet. Die Konfiguration umfasst die folgenden Elemente:

Umleitungs-URL

Wenn Citrix Gateway feststellt, dass ein Benutzer authentifiziert werden muss, weist es den Webbrowser des Benutzers an, einen HTTP-POST an eine SAML-Anmeldeseite auf dem ADFS-Server durchzuführen. Dies ist normalerweise eine `https://`-Adresse der Form: `https://adfs.mycompany.com/adfs/ls`.

Dieser Webseiten-POST enthält weitere Informationen, einschließlich der „Rücksendeadresse“, an die ADFS den Benutzer nach Abschluss der Anmeldung zurückleitet.

Bezeichner

Die EntityId ist ein eindeutiger Bezeichner, den Citrix Gateway in seine POST-Daten an ADFS aufnimmt. Dies informiert ADFS darüber, bei welchem Dienst sich der Benutzer anmelden möchte, und wendet gegebenenfalls unterschiedliche Authentifizierungsrichtlinien an. Wenn die SAML-Authentifizierungs-XML ausgestellt wird, ist sie nur für die Anmeldung bei dem Dienst geeignet, der durch die EntityId identifiziert wird.

Normalerweise ist die EntityID die URL der Anmeldeseite des Citrix Gateway-Servers, aber sie kann im Allgemeinen alles sein, solange Citrix Gateway und ADFS sich darauf einigen: `https://ns.mycompany.com/application/logonpage`.

Rücksendeadresse

Wenn die Authentifizierung erfolgreich ist, weist ADFS den Webbrowser des Benutzers an, eine SAML-Authentifizierungs-XML an eine der für die EntityId konfigurierten Antwort-URLs zu POSTen. Dies ist normalerweise eine `https://`-Adresse auf dem ursprünglichen Citrix Gateway-Server in der Form: `https://ns.mycompany.com/cgi/samlauth`.

Wenn mehr als eine Antwort-URL-Adresse konfiguriert ist, kann Citrix Gateway in seinem ursprünglichen POST an ADFS eine auswählen.

Signaturzertifikat

ADFS signiert SAML-Authentifizierungs-XML-Blobs kryptografisch mit seinem privaten Schlüssel. Um diese Signatur zu validieren, muss Citrix Gateway so konfiguriert werden, dass diese

Signaturen mit dem öffentlichen Schlüssel überprüft werden, der in einer Zertifikatsdatei enthalten ist. Die Zertifikatsdatei ist normalerweise eine Textdatei, die vom ADFS-Server bezogen wird.

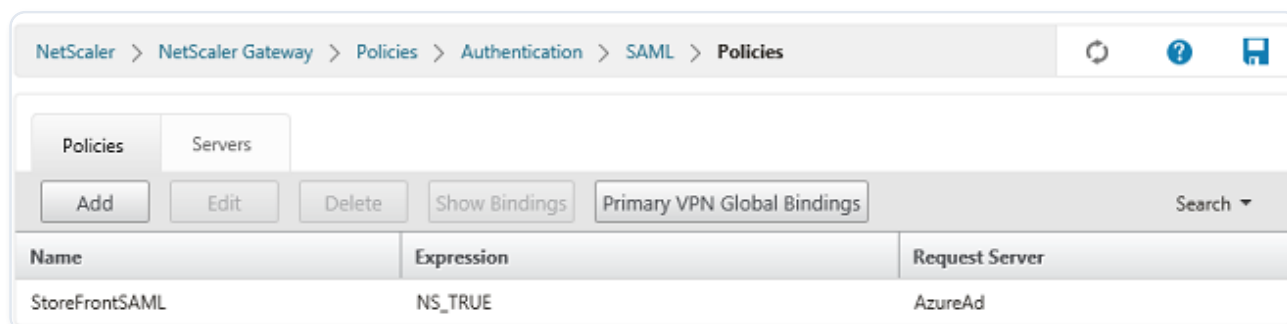
URL für einmaliges Abmelden

ADFS und Citrix Gateway unterstützen ein „zentrales Abmeldesystem“. Dies ist eine URL, die Citrix Gateway gelegentlich abfragt, um zu überprüfen, ob das SAML-Authentifizierungs-XML-Blob noch eine aktuell angemeldete Sitzung darstellt.

Dies ist eine optionale Funktion, die nicht konfiguriert werden muss. Es handelt sich normalerweise um eine `https://`-Adresse in der Form `https://adfs.mycompany.com/adfs/logout`. (Beachten Sie, dass sie dieselbe sein kann wie die URL für die einmalige Anmeldung.)

Konfiguration

Der Abschnitt [Citrix Gateway-Bereitstellung](#) beschreibt, wie Citrix Gateway für die Handhabung standardmäßiger LDAP-Authentifizierungsoptionen eingerichtet wird. Nach erfolgreichem Abschluss können Sie eine neue Authentifizierungsrichtlinie auf Citrix Gateway erstellen, die die SAML-Authentifizierung zulässt. Diese kann dann die vom Citrix Gateway-Assistenten verwendete Standard-LDAP-Richtlinie ersetzen.



SAML-Richtlinie ausfüllen

Konfigurieren Sie den neuen SAML IdP-Server mit den zuvor aus der ADFS-Verwaltungskonsole entnommenen Informationen. Wenn diese Richtlinie angewendet wird, leitet Citrix Gateway den Benutzer zur Anmeldung an ADFS weiter und akzeptiert im Gegenzug ein von ADFS signiertes SAML-Authentifizierungstoken.

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
Attribute 3
Attribute 5
Attribute 7

Attribute 1
Attribute 3
Attribute 5
Attribute 7

Verwandte Informationen

- [Installieren und Konfigurieren](#) ist die primäre Referenz für die FAS-Installation und -Konfiguration.
- Die gängigen FAS-Bereitstellungen sind im Artikel [Bereitstellungsarchitekturen](#) zusammengefasst.
- „How-to“-Artikel werden im Artikel [Erweiterte Konfiguration](#) vorgestellt.

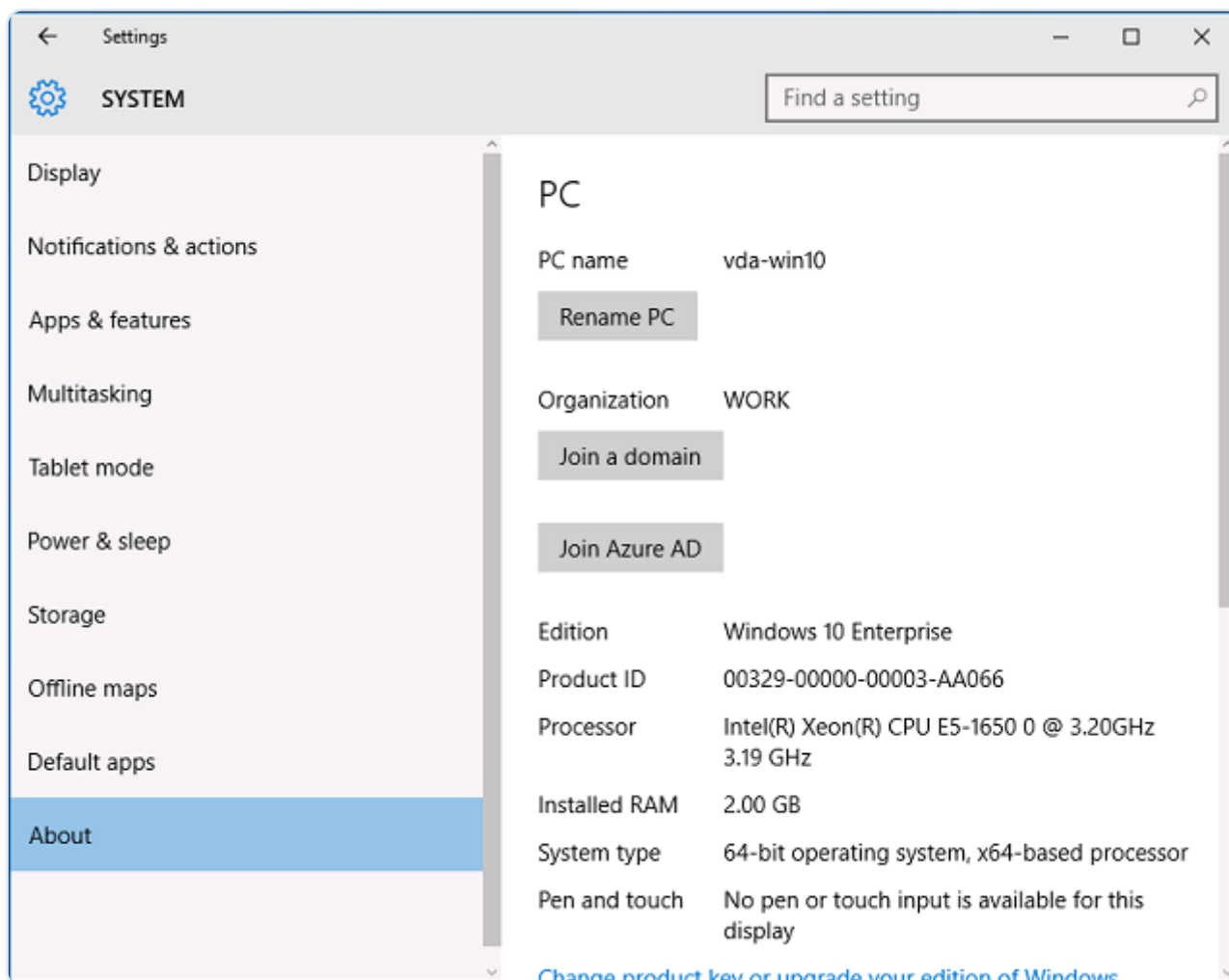
Azure AD-Integration

Einführung

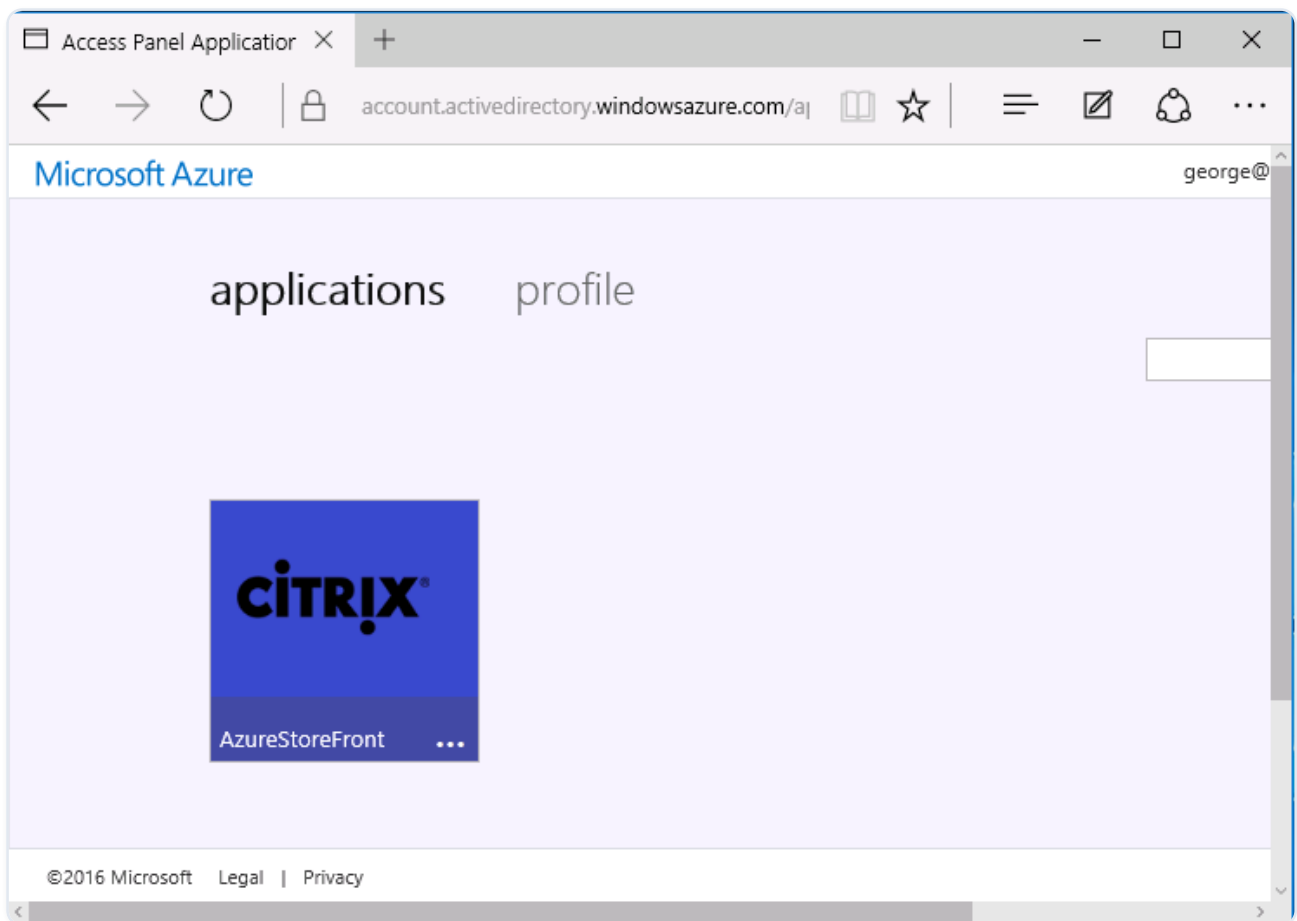
Dieses Dokument beschreibt, wie eine Citrix®-Umgebung mit der Windows 10 Azure AD-Funktion integriert wird. Windows 10 führte Azure AD ein, ein neues Domänenbeitrittsmodell, bei dem

Roaming-Laptops über das Internet einer Unternehmensdomäne beitreten können, zum Zweck der Verwaltung und des Single Sign-On.

Die Beispielbereitstellung in diesem Dokument beschreibt ein System, bei dem die IT neuen Benutzern eine Unternehmens-E-Mail-Adresse und einen Registrierungscode für ihre persönlichen Windows 10-Laptops zur Verfügung stellt. Benutzer greifen auf diesen Code über die Option **System > Info > Azure AD beitreten** im Bereich **Einstellungen** zu.



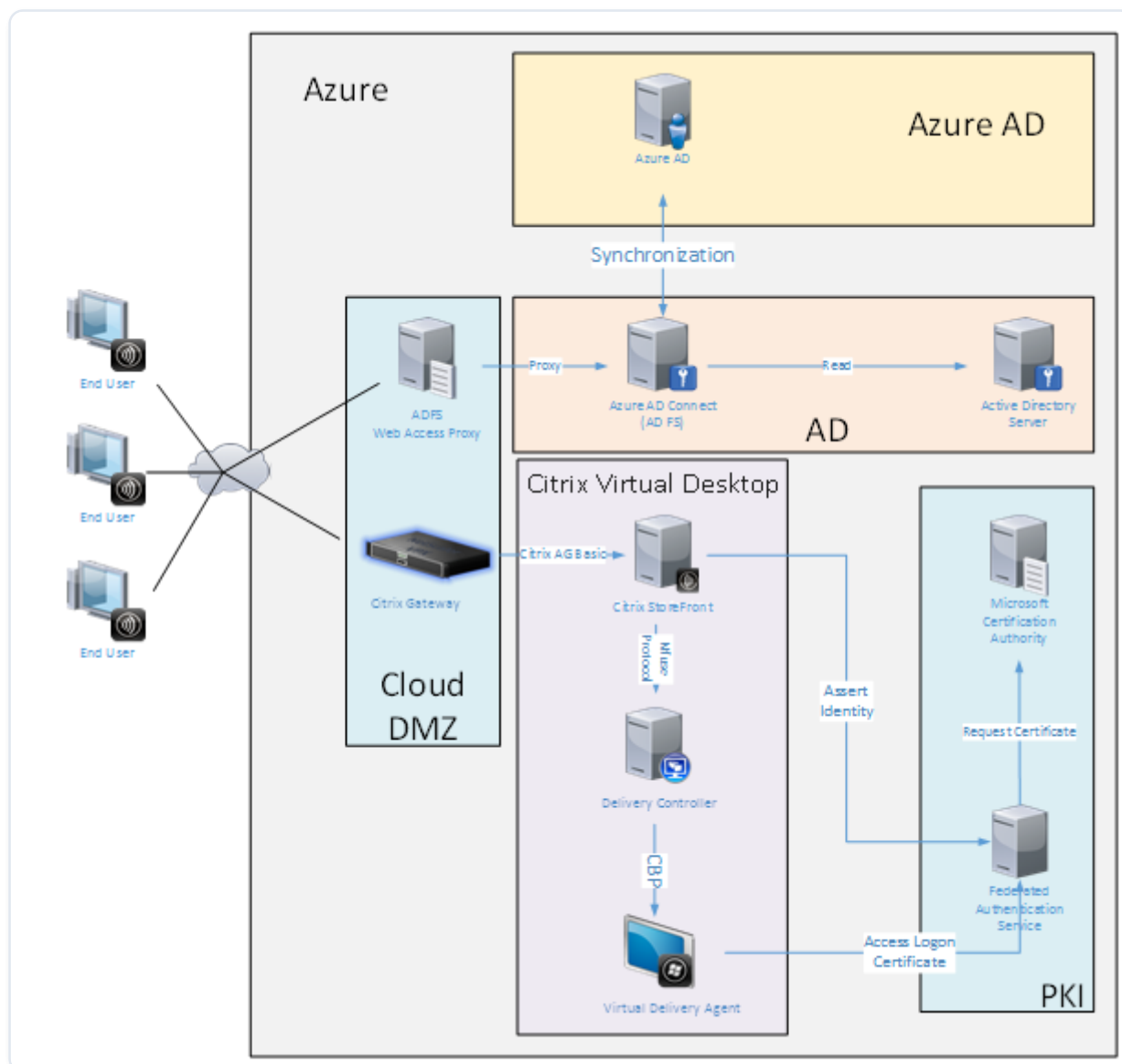
Nachdem der Laptop registriert wurde, meldet sich der Microsoft Edge-Webbrowser automatisch bei Unternehmenswebsites und veröffentlichten Citrix-Anwendungen über die Azure SaaS-Anwendungswebseite an, zusammen mit anderen Azure-Anwendungen wie Office 365.



Architektur

Diese Architektur repliziert ein traditionelles Unternehmensnetzwerk vollständig innerhalb von Azure und integriert sich in moderne Cloud-Technologien wie Azure AD und Office 365. Endbenutzer werden alle als Remote-Mitarbeiter betrachtet, ohne das Konzept, sich in einem Büro-Intranet zu befinden.

Das Modell kann auf Unternehmen mit bestehenden lokalen Systemen angewendet werden, da die Azure AD Connect-Synchronisierung über das Internet eine Brücke zu Azure schlagen kann.



Sichere Verbindungen und Single Sign-On, die traditionell Firewalled-LAN- und Kerberos/NTLM-Authentifizierung gewesen wären, werden in dieser Architektur durch TLS-Verbindungen zu Azure und SAML ersetzt. Neue Dienste werden als Azure-Anwendungen erstellt, die Azure AD beigetreten sind. Bestehende Anwendungen, die Active Directory erfordern (wie eine SQL Server-Datenbank), können mithilfe einer Standard-Active Directory Server-VM im IAAS-Teil des Azure Cloud Service ausgeführt werden.

Wenn ein Benutzer eine traditionelle Anwendung startet, werden diese über veröffentlichte Citrix Virtual Apps and Desktops™-Anwendungen aufgerufen. Die verschiedenen Anwendungstypen werden über die **Azure Applications**-Seite des Benutzers zusammengeführt, unter Verwendung der Microsoft Edge Single Sign-On-Funktionen. Microsoft bietet auch Android- und iOS-Apps an, die Azure-Anwendungen auflisten und starten können.

Eine DNS-Zone erstellen

Azure AD erfordert, dass der Administrator eine öffentliche DNS-Adresse registriert und die Delegationszone für das Domännennamensuffix kontrolliert. Dazu kann der Administrator die Azure DNS-Zonenfunktion verwenden.

Dieses Beispiel verwendet den DNS-Zonennamen *citrixsamldemo.net*.

The screenshot shows the Azure DNS console interface for a DNS zone named 'citrixsamldemo'. The top navigation bar includes 'Settings', 'Record set', 'Delete', and 'Refresh' icons. The 'Essentials' section displays the resource group 'citrixsamldemo', subscription name 'Visual Studio Professional with MSDN', and subscription ID 'df22436f-d4f9-46ae-be7b-6479cd4eefca'. It also lists four name servers: ns1-01.azure-dns.com, ns2-01.azure-dns.net, ns3-01.azure-dns.org, and ns4-01.azure-dns.info. Below this, a search bar for 'Search record sets' is present. The main table shows three record sets: an NS record for '@' with TTL 172800, an SOA record for '@' with TTL 3600, and a CNAME record for 'fs' with TTL 3600. The NS record value lists the four name servers. The SOA record value includes email, host, refresh, retry, expire, and minimum TTL. The CNAME record value points to 'adfs-citrixsamldemo.westeurope.cloud...'.

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
fs	CNAME	3600	adfs-citrixsamldemo.westeurope.cloud...

Die Konsole zeigt die Namen der Azure DNS-Nameserver an. Diese sollten in den NS-Einträgen des DNS-Registrars für die Zone referenziert werden (zum Beispiel, `citrixsamldemo.net . NS ns1-01.azure-dns.com`)

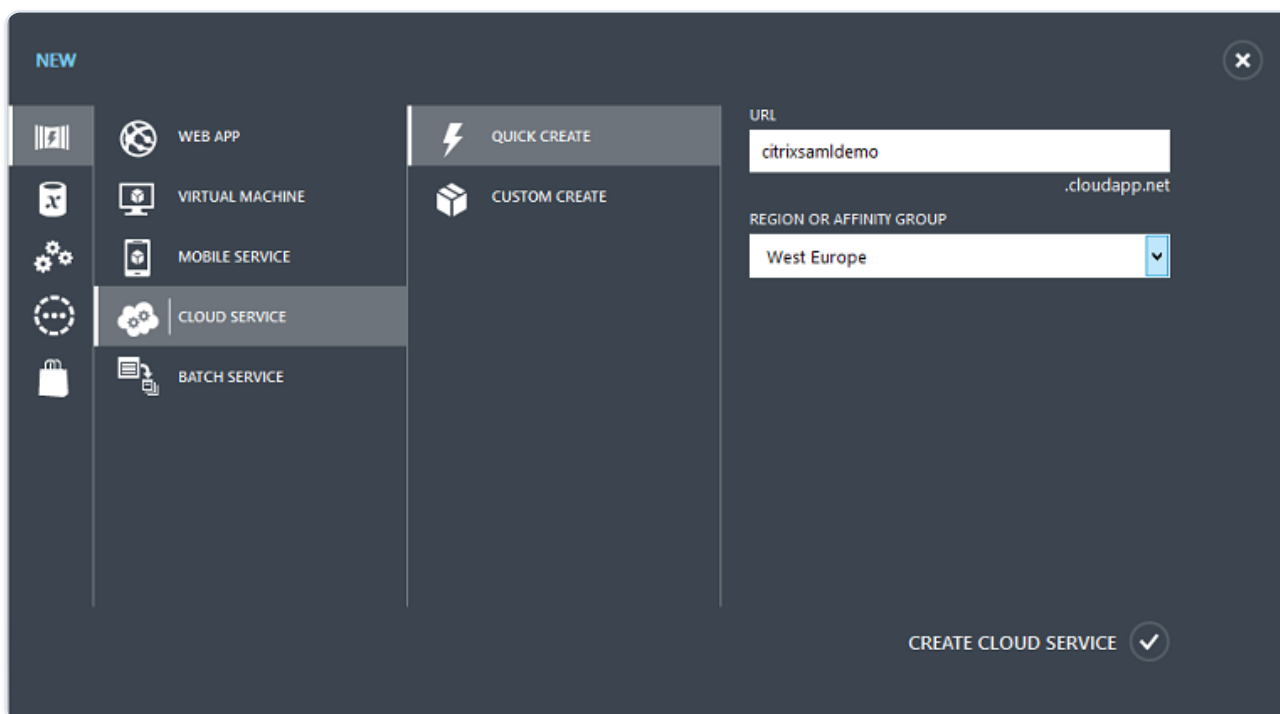
Beim Hinzufügen von Verweisen auf VMs, die in Azure ausgeführt werden, ist es am einfachsten, einen CNAME-Eintrag für den von Azure verwalteten DNS-Eintrag der VM zu verwenden. Wenn sich die IP-Adresse der VM ändert, müssen Sie die DNS-Zonendatei nicht manuell aktualisieren.

Sowohl interne als auch externe DNS-Adresssuffixe stimmen für diese Bereitstellung überein. Die Domäne ist citrixsamldemo.net und verwendet ein geteiltes DNS (10.0.0.* intern).

Fügen Sie einen Eintrag "fs.citrixsamldemo.net" hinzu, der auf den Web Application Proxy-Server verweist. Dies ist der Verbunddienst für diese Zone.

Cloud-Dienst erstellen

Dieses Beispiel konfiguriert eine Citrix-Umgebung, einschließlich einer AD-Umgebung mit einem ADFS-Server, der in Azure ausgeführt wird. Ein Cloud-Dienst mit dem Namen "citrixsamldemo." wird erstellt.



Windows-VMs erstellen

Erstellen Sie fünf Windows-VMs, die im Cloud-Dienst ausgeführt werden:

- Domänencontroller (domaincontrol)
- Azure Connect ADFS-Server (adfs)
- ADFS-Webzugriffsproxy (Web Application Proxy, nicht in Domäne eingebunden)
- Citrix Virtual Apps and Desktops Bereitstellungs-Controller
- Citrix Virtual Apps and Desktops Virtueller Bereitstellungsagent (VDA)

Microsoft Azure

Create virtual machine > Basics

Create virtual machine

Basics

- 1 Basics
Configure basic settings
- 2 Size
Choose virtual machine size
- 3 Settings
Configure optional features
- 4 Summary
Windows Server 2012 R2 Datacenter

Name

User name

Password

Subscription
Visual Studio Professional with MSDN

Resource group
citrixsamldemo

Location
West Europe

OK

Domänencontroller

- Fügen Sie die Rollen **DNS-Server** und **Active Directory-Domänendienste** hinzu, um eine Standard-Active Directory-Bereitstellung zu erstellen (in diesem Beispiel citrixsamldemo.net). Nachdem die Domänenheraufstufung abgeschlossen ist, fügen Sie die Rolle **Active Directory-Zertifikatdienste** hinzu.
- Erstellen Sie ein normales Benutzerkonto zum Testen (zum Beispiel George@citrixsamldemo.net).
- Da dieser Server einen internen DNS-Dienst ausführt, sollten sich alle Server für die DNS-Auflösung auf diesen Server beziehen. Dies kann über die Seite **Azure DNS-Einstellungen** erfolgen. (Weitere Informationen finden Sie im Anhang dieses Dokuments.)

ADFS-Controller und Webanwendungsproxy-Server

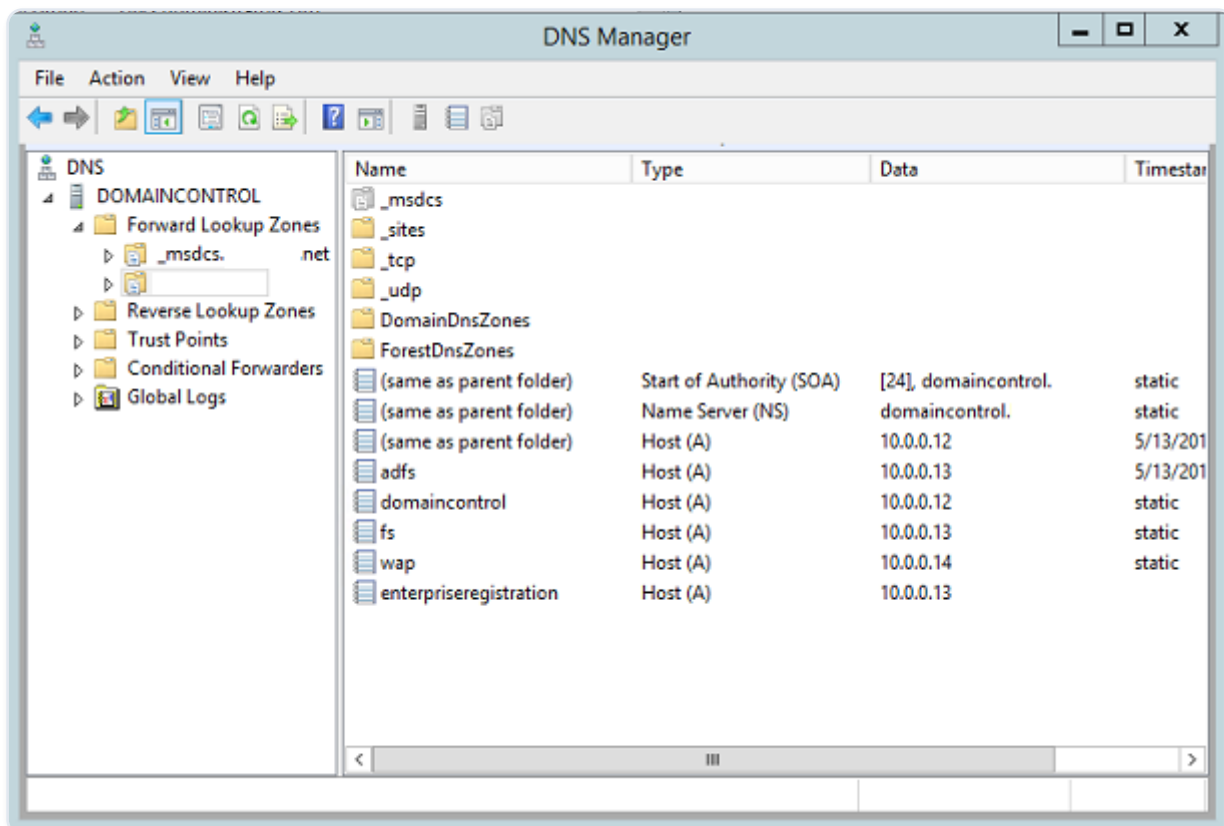
- Fügen Sie den ADFS-Server der Domäne citrixsamldemo hinzu. Der Webanwendungsproxy-Server sollte in einer isolierten Arbeitsgruppe verbleiben, registrieren Sie daher manuell eine DNS-Adresse beim AD-DNS.
- Führen Sie das Cmdlet **Enable-PSRemoting -Force** auf diesen Servern aus, um PS-Remoting durch Firewalls vom AzureAD Connect-Tool aus zu ermöglichen.

Citrix Virtual Desktops™ Delivery Controller und VDA

- Installieren Sie den Citrix Virtual Apps oder Citrix Virtual Desktops Delivery Controller™ und VDA auf den verbleibenden zwei Windows-Servern, die der Domäne citrixsamldemo beigetreten sind.

Internen DNS konfigurieren

Nach der Installation des Domänencontrollers konfigurieren Sie den DNS-Server so, dass er die interne Ansicht von citrixsamldemo.net verarbeitet und als Weiterleitung an einen externen DNS-Server fungiert (zum Beispiel: 8.8.8.8).

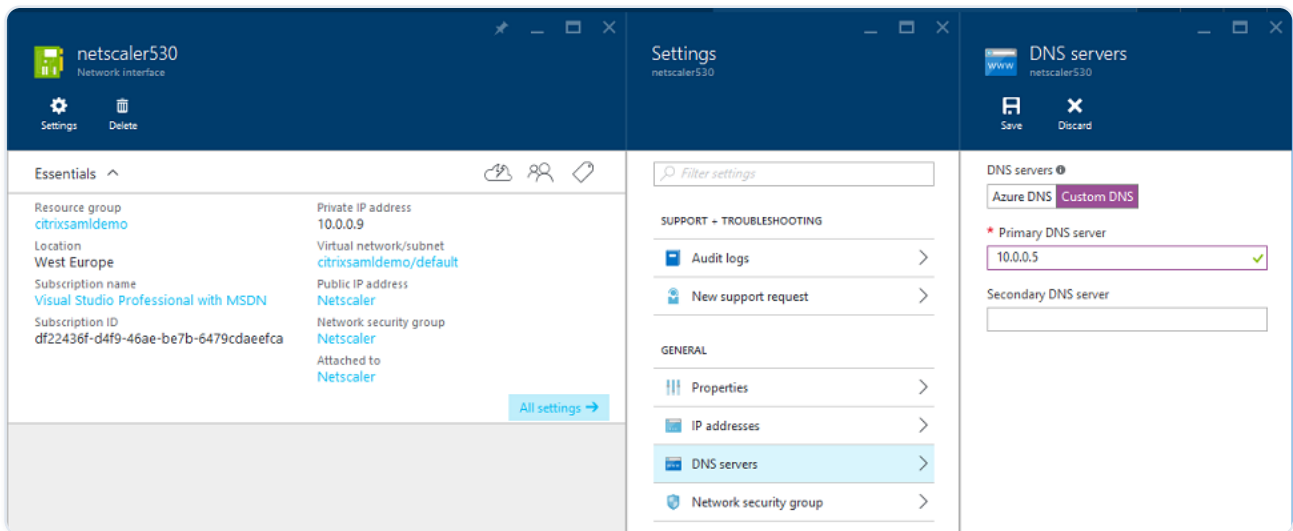


Fügen Sie einen statischen Eintrag hinzu für:

- wap.citrixsamldemo.net
- fs.citrixsamldemo.net

- enterpriseregistration.citrixsaml.net

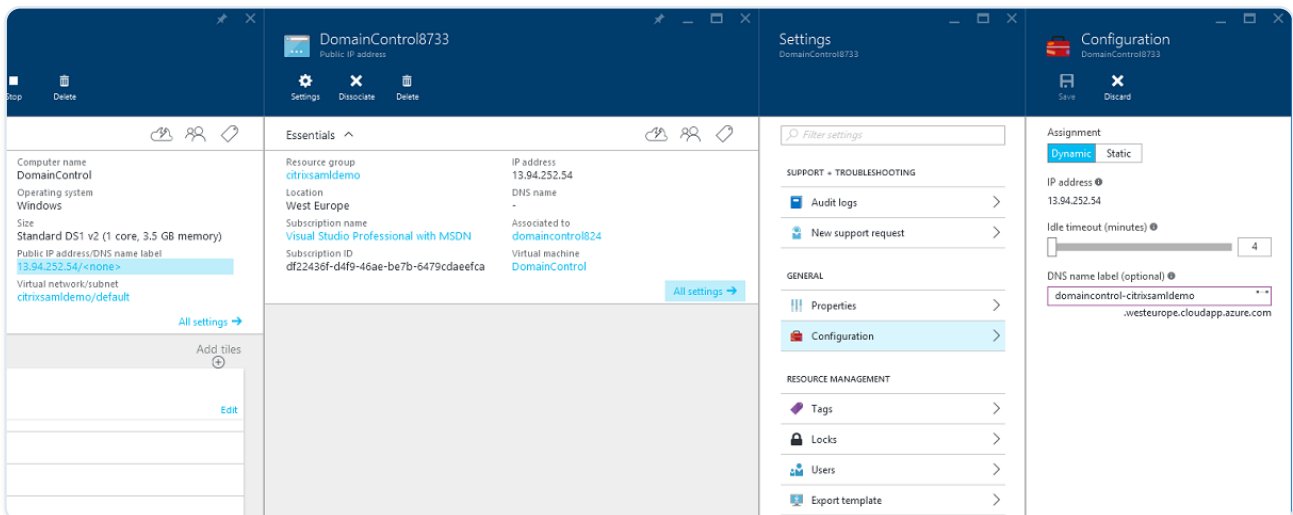
Alle in Azure ausgeführten VMs sollten so konfiguriert werden, dass sie nur diesen DNS-Server verwenden. Dies können Sie über die GUI der Netzwerkschnittstelle tun.



Standardmäßig wird die interne IP-Adresse (10.0.0.9) dynamisch zugewiesen. Sie können die Einstellung für IP-Adressen verwenden, um die IP-Adresse dauerhaft zuzuweisen. Dies sollte für den Web Application Proxy-Server und den Domänencontroller erfolgen.

Eine externe DNS-Adresse konfigurieren

Wenn eine VM ausgeführt wird, verwaltet Azure einen eigenen DNS-Zonenserver, der auf die aktuell der VM zugewiesene öffentliche IP-Adresse verweist. Dies ist eine nützliche Funktion, die aktiviert werden sollte, da Azure standardmäßig IP-Adressen zuweist, wenn jede VM startet.

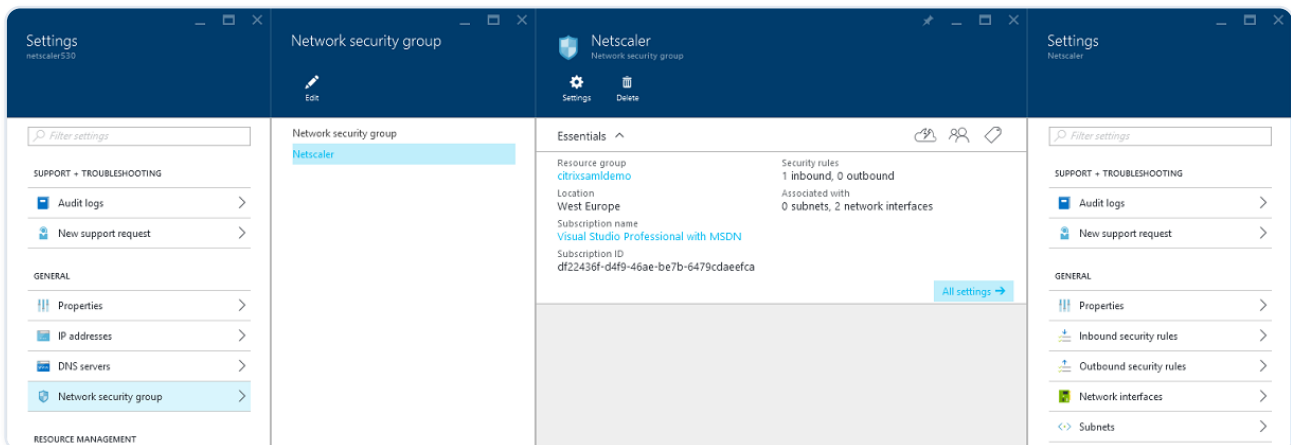


Dieses Beispiel weist die DNS-Adresse domaincontrol-citrixsaml demo.westeurope.cloudapp.azure.com dem Domänencontroller zu.

Beachten Sie, dass nach Abschluss der Remote-Konfiguration nur die VMs des Web Application Proxy und des Citrix Gateway öffentliche IP-Adressen aktiviert haben sollten. (Während der Konfiguration wird die öffentliche IP-Adresse für den RDP-Zugriff auf die Umgebung verwendet).

Sicherheitsgruppen konfigurieren

Die Azure-Cloud verwaltet Firewallregeln für den TCP/UDP-Zugriff auf VMs aus dem Internet mithilfe von Sicherheitsgruppen. Standardmäßig erlauben alle VMs den RDP-Zugriff. Die Citrix Gateway- und Web Application Proxy-Server sollten auch TLS auf Port 443 zulassen.

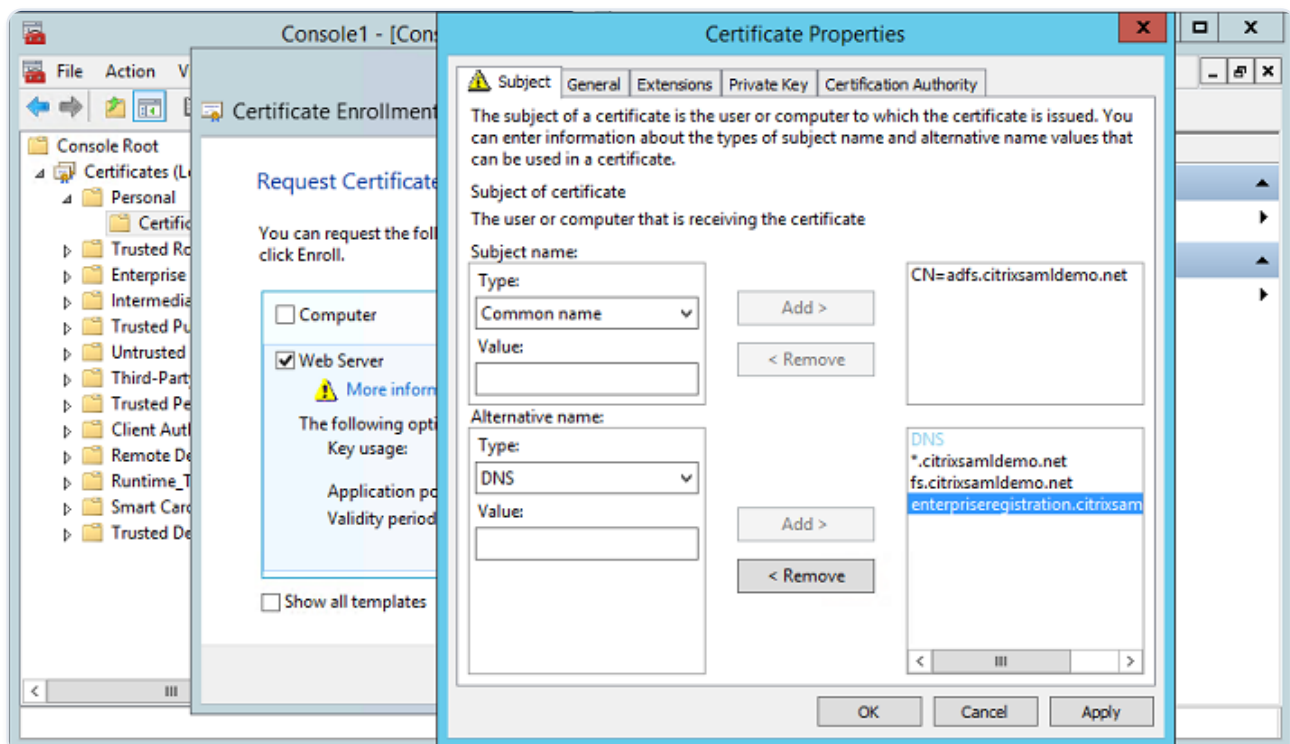


Ein ADFS-Zertifikat erstellen

Aktivieren Sie die Zertifikatvorlage **Webserver** auf der Microsoft-Zertifizierungsstelle. Dies ermöglicht die Erstellung eines Zertifikats mit benutzerdefinierten DNS-Adressen, das (einschließlich privatem Schlüssel) in eine PFX-Datei exportiert werden kann. Sie müssen dieses Zertifikat sowohl auf den ADFS- als auch auf den Web Application Proxy-Servern installieren, daher ist die PFX-Datei die bevorzugte Option.

Stellen Sie ein Webserver-Zertifikat mit den folgenden Antragstellernamen aus:

- Allgemeiner Name:
 - adfs.citrixsamldemo.net
- Alternativer Antragstellername:
 - *.citrixsamldemo.net
 - fs.citrixsamldemo. Netzwerk
 - enterpriseregistration.citrixsamldemo.net



Exportieren Sie das Zertifikat in eine PFX-Datei, einschließlich eines passwortgeschützten privaten Schlüssels.

Azure AD einrichten

Dieser Abschnitt beschreibt den Prozess der Einrichtung einer neuen Azure AD-Instanz und der Erstellung von Benutzeridentitäten, die zum Beitritt von Windows 10 zu Azure AD verwendet werden können.

Neues Verzeichnis erstellen

Melden Sie sich beim klassischen Azure-Portal an und erstellen Sie ein neues Verzeichnis.

ADD DIRECTORY

DIRECTORY ?

Create new directory

NAME ?

CitrixSAMLdemo

DOMAIN NAME ?

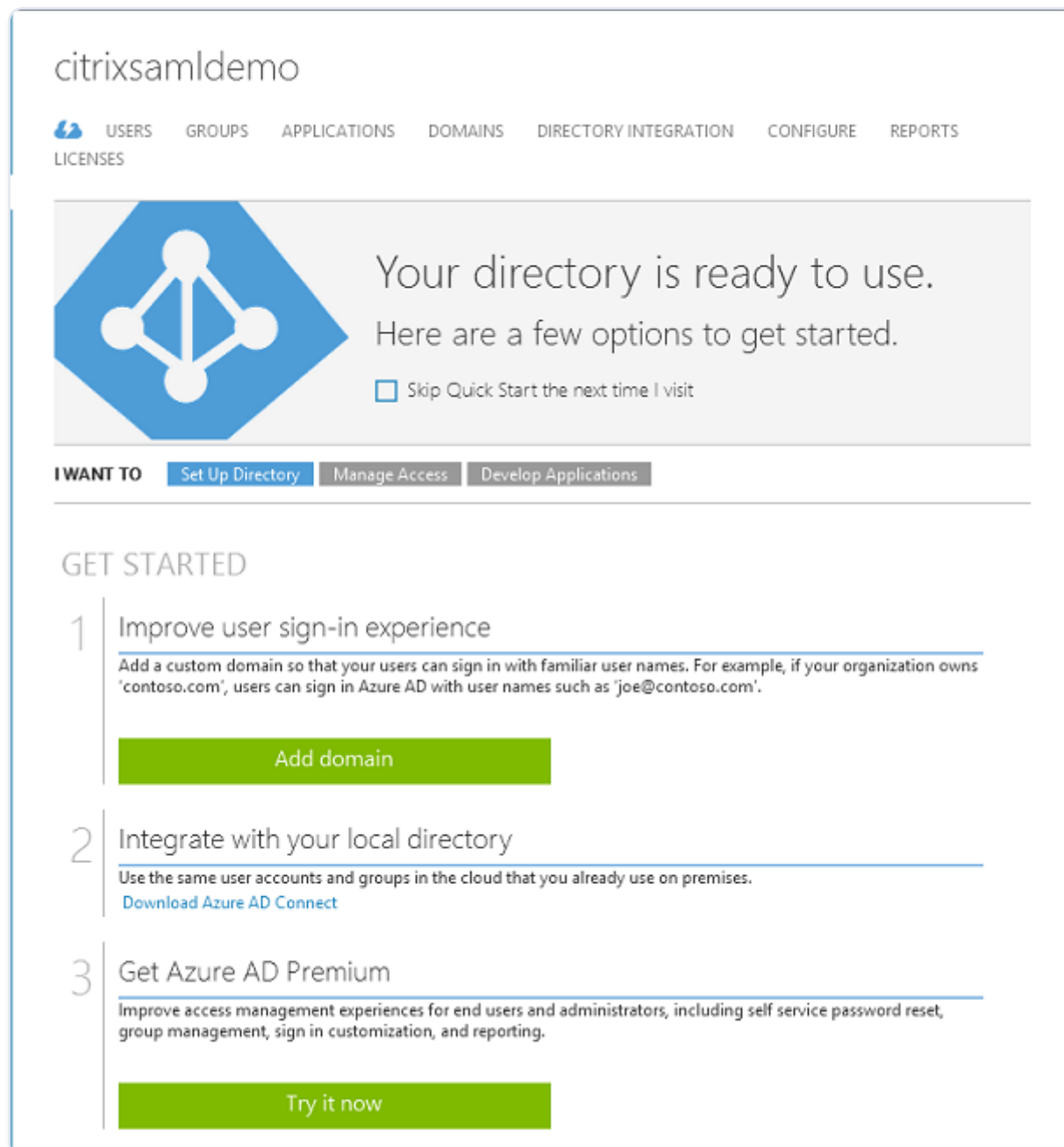
citrixsaml demo .onmicrosoft.com

COUNTRY OR REGION ?

United Kingdom

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

Wenn abgeschlossen, wird eine Übersichtsseite angezeigt.



citrixsamdemo

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 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](#)

Globalen Administratorbenutzer erstellen (AzureAdmin)

Erstellen Sie einen globalen Administrator in Azure (in diesem Beispiel

AzureAdmin@citrixsamdemo.onmicrosoft.com) und melden Sie sich mit dem neuen Konto an, um ein Kennwort einzurichten.

ADD USER

user profile

FIRST NAME: Azure

LAST NAME: Admin

DISPLAY NAME: Azure Admin

ROLE: Global Admin

ALTERNATE EMAIL ADDRESS: [Empty field with red error icon]

MULTI-FACTOR AUTHENTICATION: ☐ Enable Multi-Factor Authentication

1 3

Ihre Domäne bei Azure AD registrieren

Standardmäßig werden Benutzer mit einer E-Mail-Adresse in der Form

`<user.name>@<company>.onmicrosoft.com` identifiziert.

Obwohl dies ohne weitere Konfiguration funktioniert, ist eine E-Mail-Adresse im Standardformat besser, vorzugsweise eine, die dem E-Mail-Konto des Endbenutzers entspricht:

`<user.name>@<company>.com`.

Die Aktion **Domäne hinzufügen** konfiguriert eine Weiterleitung von Ihrer echten Unternehmensdomäne. Das Beispiel verwendet `citrixsamldemo.net`.

Wenn Sie ADFS für Single Sign-On einrichten, aktivieren Sie das Kontrollkästchen.

ADD DOMAIN

Specify a domain name

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

DOMAIN NAME

citrixsaml-demo.net

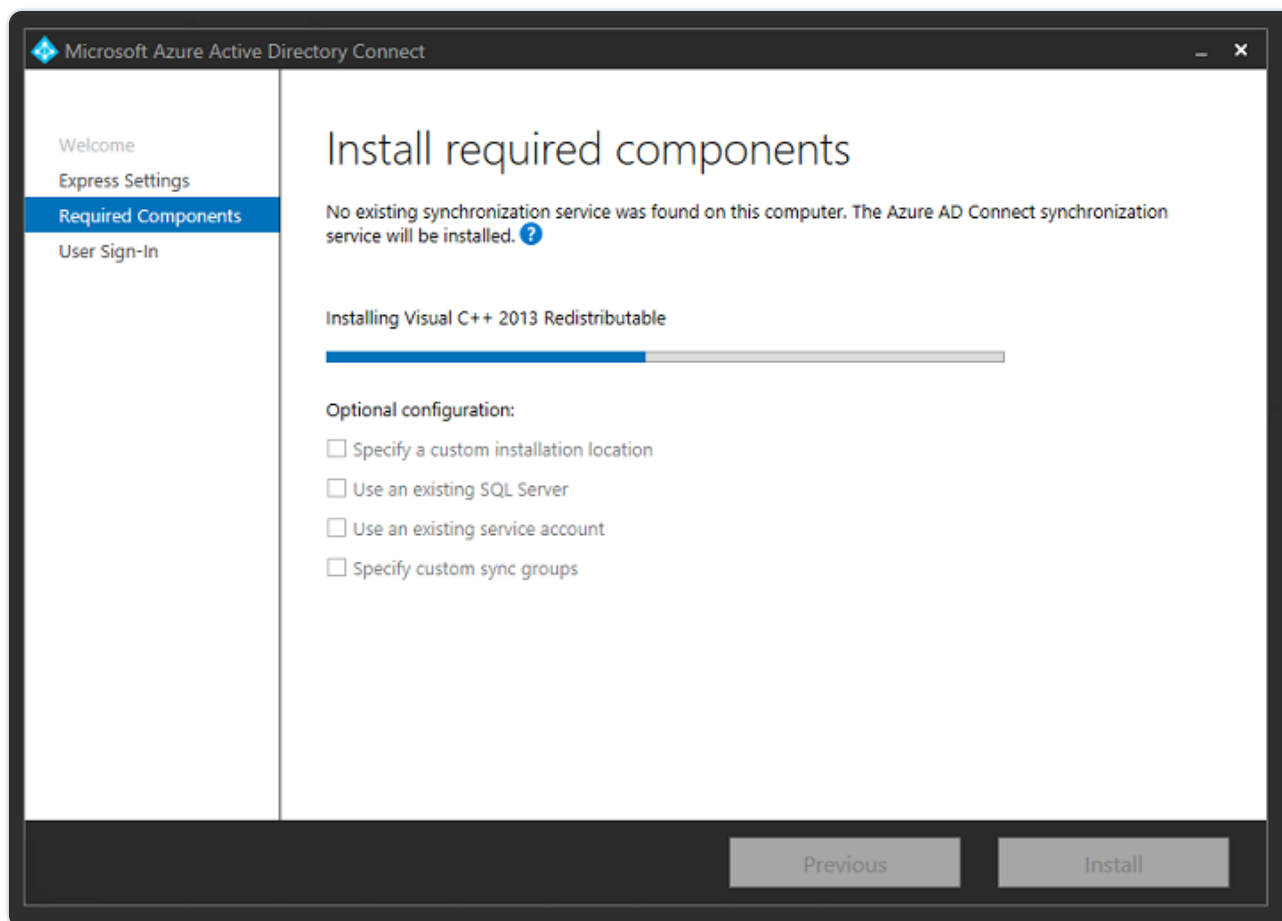
☒ I plan to configure this domain for single sign-on with my local Active Directory. ?

add

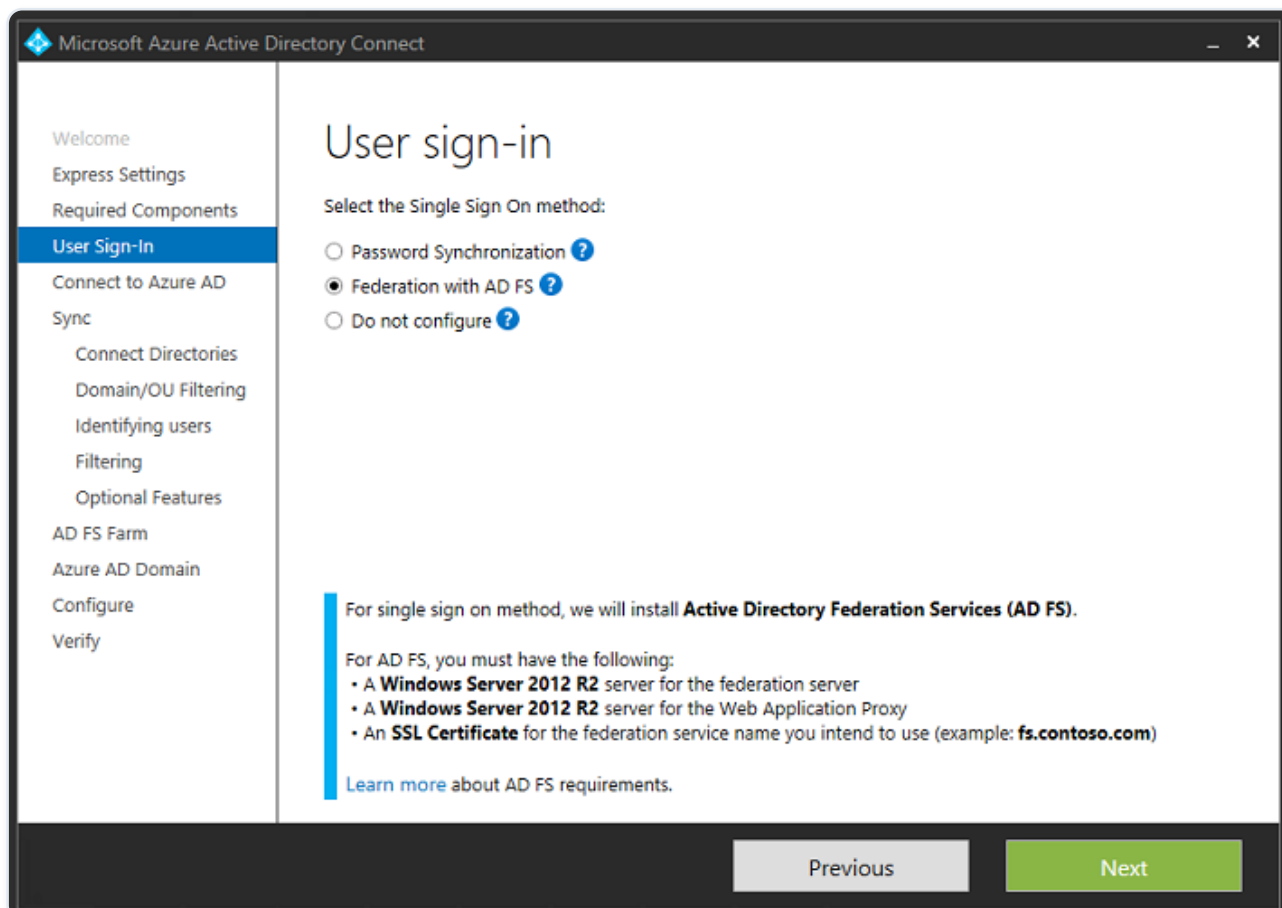
→ 2

Azure AD Connect installieren

Schritt 2 der Azure AD-Konfigurations-GUI leitet zur Microsoft-Downloadseite für Azure AD Connect weiter. Installieren Sie dies auf der ADFS-VM. Verwenden Sie die Option **Benutzerdefinierte Installation** anstelle von **Express-Einstellungen**, damit ADFS-Optionen verfügbar sind.



Wählen Sie die Option **Verbund mit AD FS** (Single Sign-On).



Verbinden Sie sich mit Azure mit dem zuvor erstellten Administratorkonto.

The screenshot shows the 'Microsoft Azure Active Directory Connect' application window. The title bar reads 'Microsoft Azure Active Directory Connect'. On the left is a navigation pane with the following items: 'Welcome', 'Express Settings', 'Required Components', 'User Sign-In', 'Connect to Azure AD' (highlighted in blue), 'Sync', 'Connect Directories', 'Azure AD sign-in', 'Domain/OU Filtering', 'Identifying users', 'Filtering', 'Optional Features', 'AD FS Farm', 'Azure AD Domain', 'Configure', and 'Verify'. The main area is titled 'Connect to Azure AD' and contains the text 'Enter your Azure AD credentials: ?'. Below this are two input fields: 'USERNAME' with the value 'AzureAdmin@citrixsaml-demo.onmicrosoft.com' and 'PASSWORD' with masked characters. At the bottom right are two buttons: 'Previous' (disabled) and 'Next' (active).

Wählen Sie die interne AD-Gesamtstruktur aus.

The screenshot shows the 'Connect your directories' window in the Microsoft Azure Active Directory Connect application. The left sidebar contains a navigation menu with options: Welcome, Express Settings, Required Components, User Sign-In, Connect to Azure AD, Sync, **Connect Directories**, Domain/OU Filtering, Identifying users, Filtering, Optional Features, AD FS Farm, Azure AD Domain, Configure, and Verify. The main content area is titled 'Connect your directories' and includes the instruction 'Enter connection information for your on-premises directories or forests: ?'. Below this, there are fields for 'DIRECTORY TYPE' (set to 'Active Directory'), 'FOREST ?' (set to 'citrixsaml demo.cloudapp.net'), 'USERNAME' (set to 'CITRIXSAMLdemo\Administrator'), and 'PASSWORD' (masked with dots). An 'Add Directory' button is to the right of the password field. Below these fields, the 'CONFIGURED DIRECTORIES' section shows 'citrixsaml demo.cloudapp.net (Active Directory)' with a green checkmark and a 'Remove' link. At the bottom, there are 'Previous' and 'Next' buttons.

Synchronisieren Sie alle älteren Active Directory-Objekte mit Azure AD.

The screenshot shows the 'Domain and OU filtering' window in the Microsoft Azure Active Directory Connect application. The left sidebar is the same as in the previous screenshot, but 'Domain/OU Filtering' is now selected. The main content area is titled 'Domain and OU filtering' and includes a 'Directory:' dropdown set to 'citrixsaml demo.cloudapp.net' and a 'Refresh Ou/Domain ?' button. Below this, there are two radio buttons: 'Sync all domains and OUs' and 'Sync selected domains and OUs' (which is selected). A list box shows the following items with checkboxes: 'citrixsaml demo.cloudapp.net' (checked), 'Builtin' (checked), 'Computers' (checked), 'Domain Controllers' (checked), 'ForeignSecurityPrincipals' (checked), 'Infrastructure' (checked), 'LostAndFound' (unchecked), 'Managed Service Accounts' (checked), 'NTDS Quotas' (checked), 'Program Data' (checked), 'System' (checked), 'Users' (checked), and 'Configuration' (checked). At the bottom, there are 'Previous' and 'Next' buttons.

Wenn die Verzeichnisstruktur einfach ist, können Sie sich darauf verlassen, dass die Benutzernamen ausreichend eindeutig sind, um einen sich anmeldenden Benutzer zu identifizieren.

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 a help icon. It contains two sections: 'Select how users should be identified in your on-premises directories.' and 'Select how users should be identified with Azure AD.' The first section has two radio button options: 'Users are represented only once across all directories.' (selected) and 'User identities exist across multiple directories. Match using:'. The second option has three sub-options: 'Mail attribute' (selected), 'ObjectSID and msExchMasterAccountSID/msRTCSIP-OriginatorSID attributes', and 'SAMAccountName and MailNickName attributes'. There is also an option for 'A specific attribute' with a 'CUSTOM ATTRIBUTE' dropdown menu. The second section has 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.

Microsoft Azure Active Directory Connect

Welcome
Express Settings
Required Components
User Sign-In
Connect to Azure AD
Sync
Connect Directories
Domain/OU Filtering
Identifying users
Filtering
Optional Features
AD FS Farm
Azure AD Domain
Configure
Verify

Uniquely identifying your users

Select how users should be identified in your on-premises directories. ?

☒ Users are represented only once across all directories.

☐ User identities exist across multiple directories. Match using:

- ☒ Mail attribute
- ☐ ObjectSID and msExchMasterAccountSID/msRTCSIP-OriginatorSID attributes
- ☐ SAMAccountName and MailNickName attributes
- ☐ A specific attribute

CUSTOM ATTRIBUTE

Select how users should be identified with Azure AD.

SOURCE ANCHOR ?

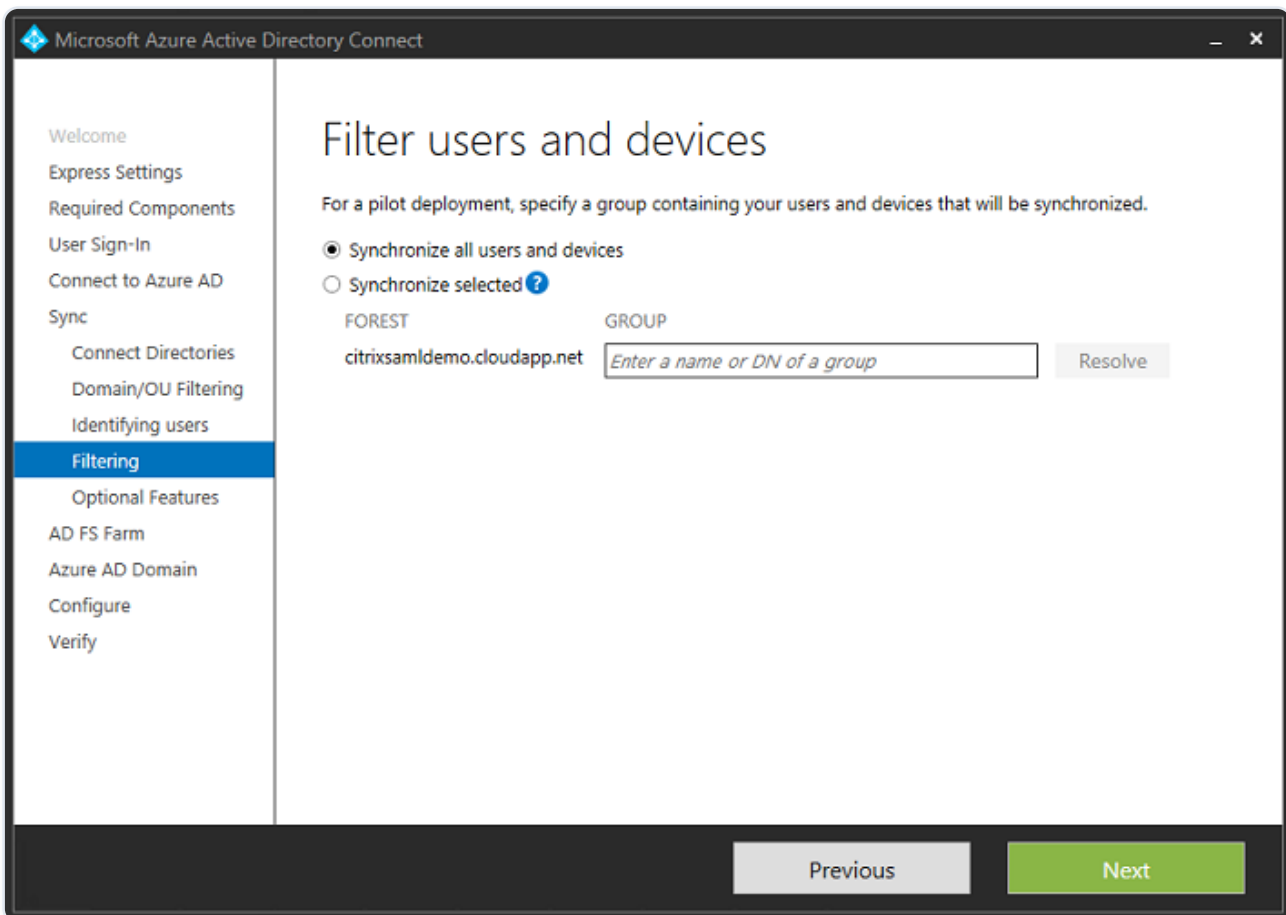
objectGUID

USER PRINCIPAL NAME ?

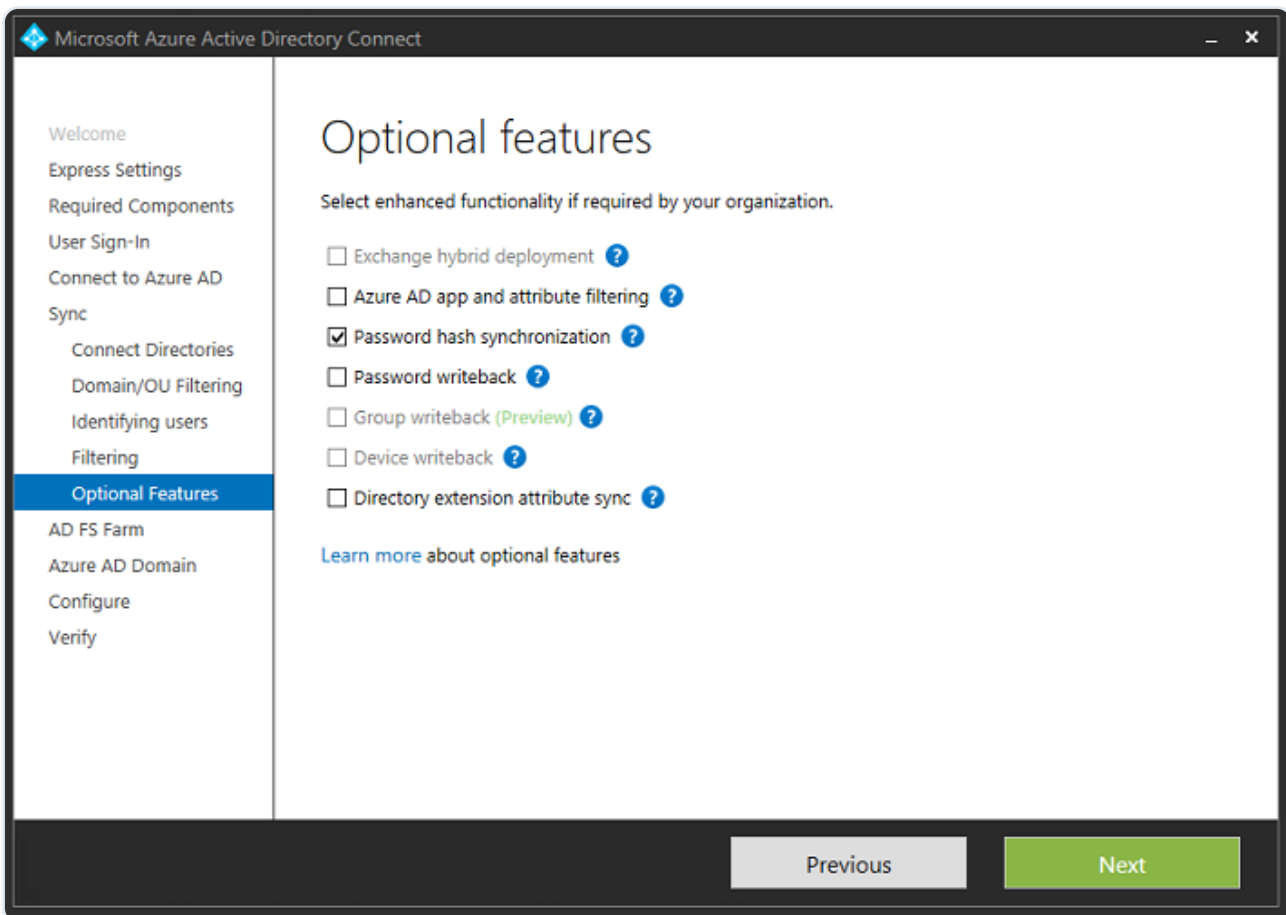
userPrincipalName

Previous Next

Akzeptieren Sie die Standardfilteroptionen, oder beschränken Sie Benutzer und Geräte auf eine bestimmte Gruppe von Gruppen.



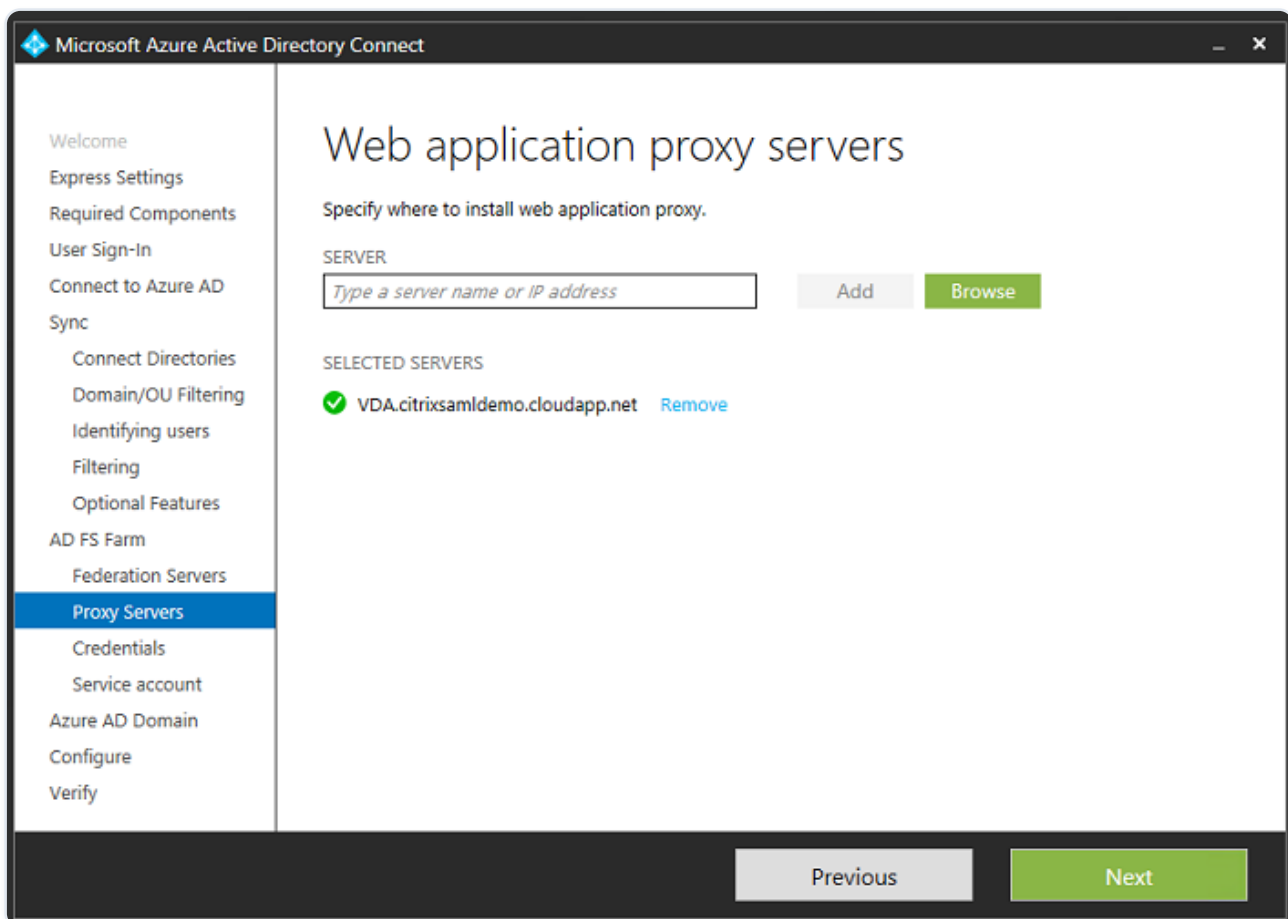
Falls gewünscht, können Sie die Azure AD-Passwörter mit Active Directory synchronisieren. Dies ist für die ADFS-basierte Authentifizierung normalerweise nicht erforderlich.



Wählen Sie die PFX-Zertifikatsdatei aus, die in AD FS verwendet werden soll, und geben Sie fs.citrixsamldemo.net als DNS-Namen an.

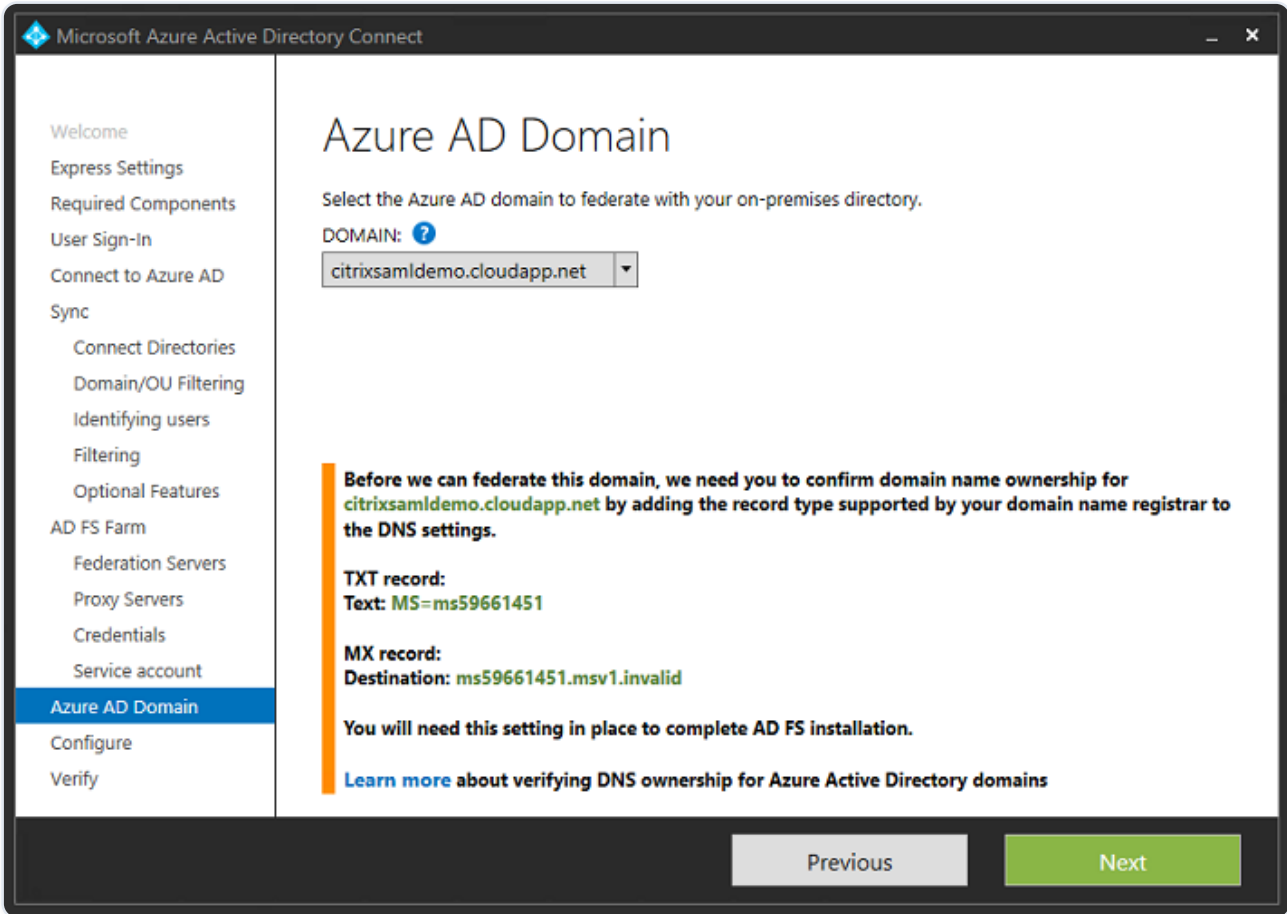
The screenshot shows the 'AD FS Farm' configuration window in Microsoft Azure Active Directory Connect. The left sidebar contains a navigation menu with the following items: Welcome, Express Settings, Required Components, User Sign-In, Connect to Azure AD, Sync, Connect Directories, Domain/OU Filtering, Identifying users, Filtering, Optional Features, **AD FS Farm** (highlighted), Federation Servers, Proxy Servers, Credentials, Service account, Azure AD Domain, Configure, and Verify. The main content area is titled 'AD FS Farm' and contains two options: 'Configure a new Windows Server 2012 R2 AD FS farm' (selected) and 'Use an existing Windows Server 2012 R2 AD FS farm'. Below these options, it says 'Specify the SSL certificate used to secure the communication between clients and AD FS.' with two radio buttons: 'Provide a PFX Certificate File' (selected) and 'Use a Certificate installed on the Federation Machines'. A 'CERTIFICATE FILE' section has a text box containing 'C:\Users\Fred.CITRIXSAMLDEMO\Desktop\adfs.pfx' and a 'Browse' button. The 'SUBJECT NAME' is a dropdown menu showing '*_citrixsaml demo.net'. The 'SUBJECT NAME PREFIX' is a text box containing 'fs' with a green checkmark icon to its right. The 'FEDERATION SERVICE NAME' is a text box containing 'https://fs.citrixsaml demo.net'. At the bottom, there are 'Previous' and 'Next' buttons.

Wenn Sie aufgefordert werden, einen Proxyserver auszuwählen, geben Sie die Adresse des Servers `wap.citrixsaml demo.net` ein. Möglicherweise müssen Sie das Cmdlet **Enable-PSRemoting -Force** als Administrator auf dem Web Application Proxy-Server ausführen, damit Azure AD Connect ihn konfigurieren kann.

**HINWEIS:**

Wenn dieser Schritt aufgrund von Remote PowerShell-Vertrauensproblemen fehlschlägt, versuchen Sie, den Web Application Proxy-Server der Domäne beizutreten.

Verwenden Sie für die restlichen Schritte des Assistenten die Standard-Administratorpasswörter und erstellen Sie ein Dienstkonto für ADFS. Azure AD Connect fordert Sie dann auf, den Besitz der DNS-Zone zu validieren.



Fügen Sie die TXT- und MX-Einträge zu den DNS-Adresstabellen in Azure hinzu.

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... ...

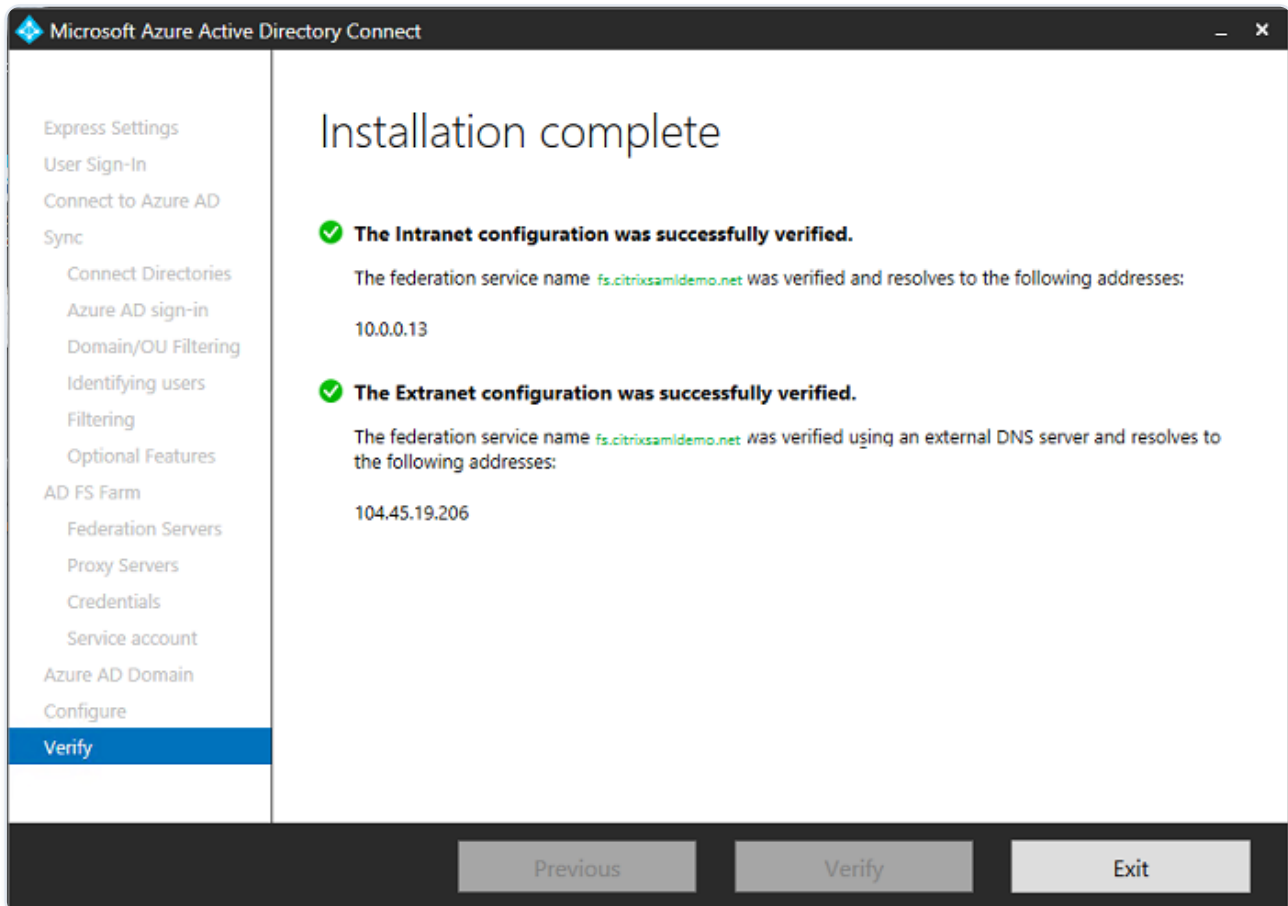
Klicken Sie in der Azure Management Console auf **Verify**.

CitrixSamI Demo					
	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

HINWEIS:

Wenn dieser Schritt fehlschlägt, können Sie die Domäne überprüfen, bevor Sie Azure AD Connect ausführen.

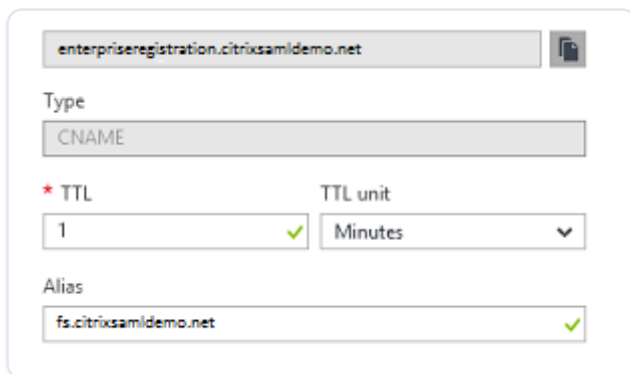
Nach Abschluss wird die externe Adresse `fs.citrixsamldemo.net` über Port 443 kontaktiert.



Azure AD Join aktivieren

Wenn ein Benutzer eine E-Mail-Adresse eingibt, damit Windows 10 dem Azure AD beitreten kann, wird das DNS-Suffix verwendet, um einen CNAME-DNS-Eintrag zu erstellen, der auf ADFS zeigen sollte: `enterpriseregistration.\<upnsuffix>`.

In diesem Beispiel ist dies `fs.citrixsamldemo.net`.



enterpriseregistration.citrixsaml-demo.net

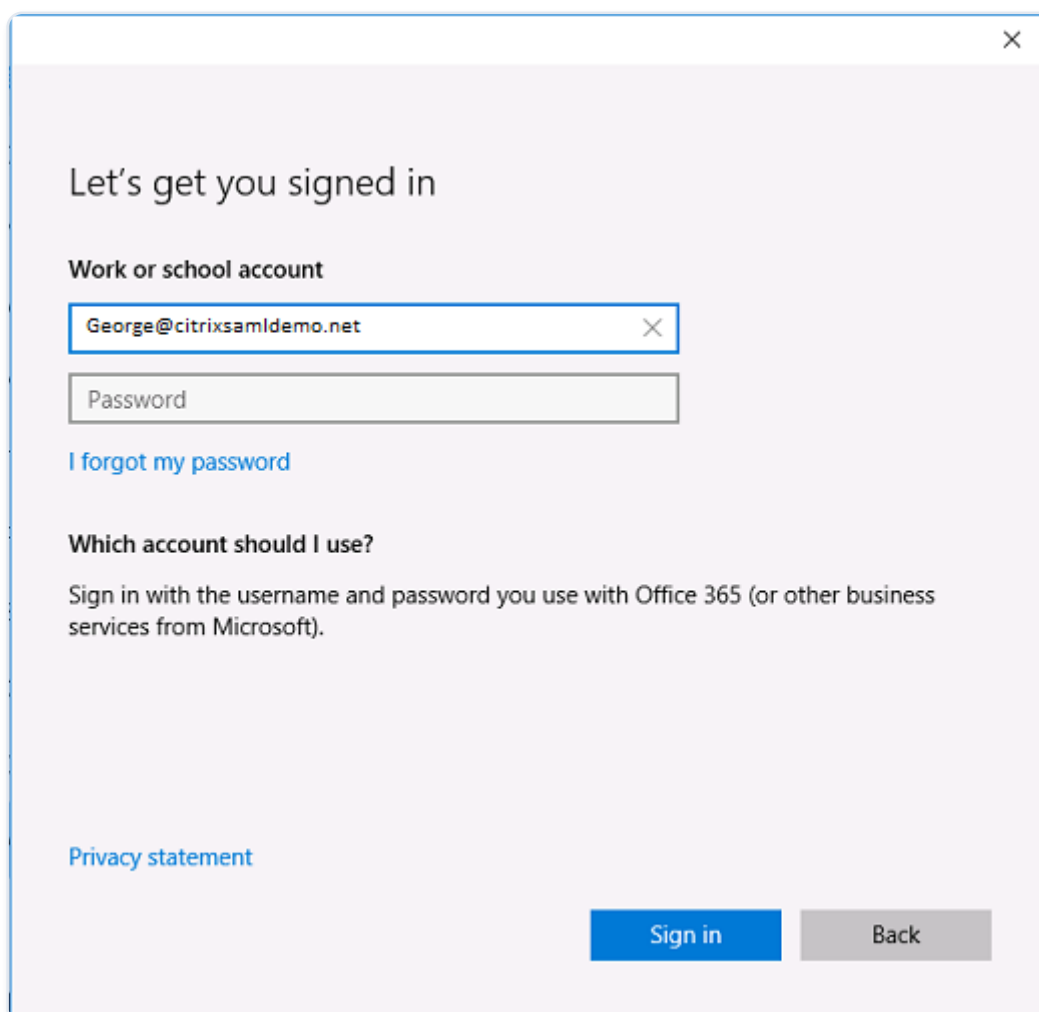
Type
CNAME

* TTL
1 ✓

TTL unit
Minutes

Alias
fs.citrixsaml-demo.net ✓

Wenn Sie keine öffentliche Zertifizierungsstelle verwenden, stellen Sie sicher, dass das ADFS-Stammzertifikat auf dem Windows 10-Computer installiert ist, damit Windows dem ADFS-Server vertraut. Führen Sie einen Azure AD-Domänenbeitritt mit dem zuvor generierten Standardbenutzerkonto durch.



Let's get you signed in

Work or school account

George@citrixsaml-demo.net

Password

[I forgot my password](#)

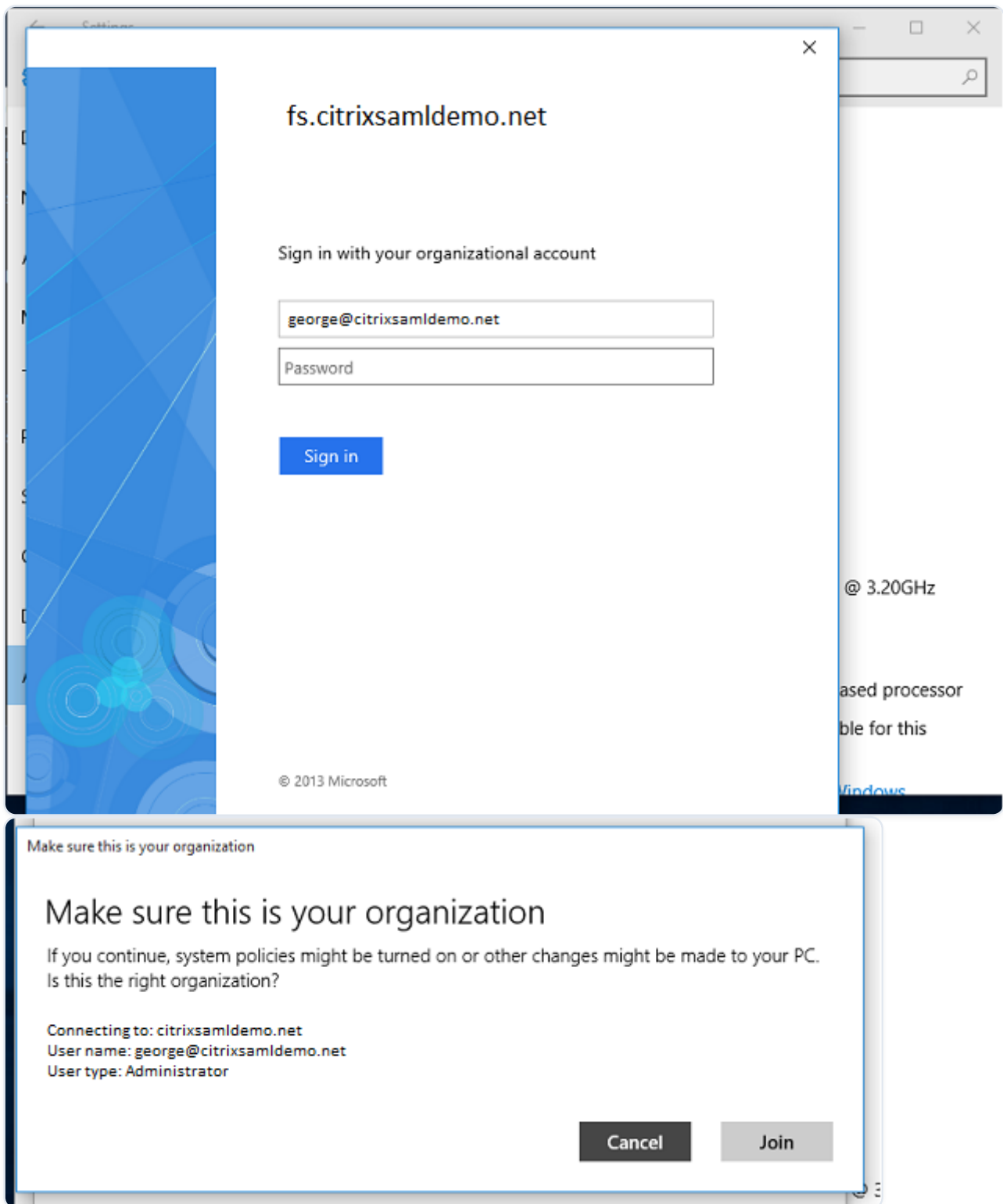
Which account should I use?

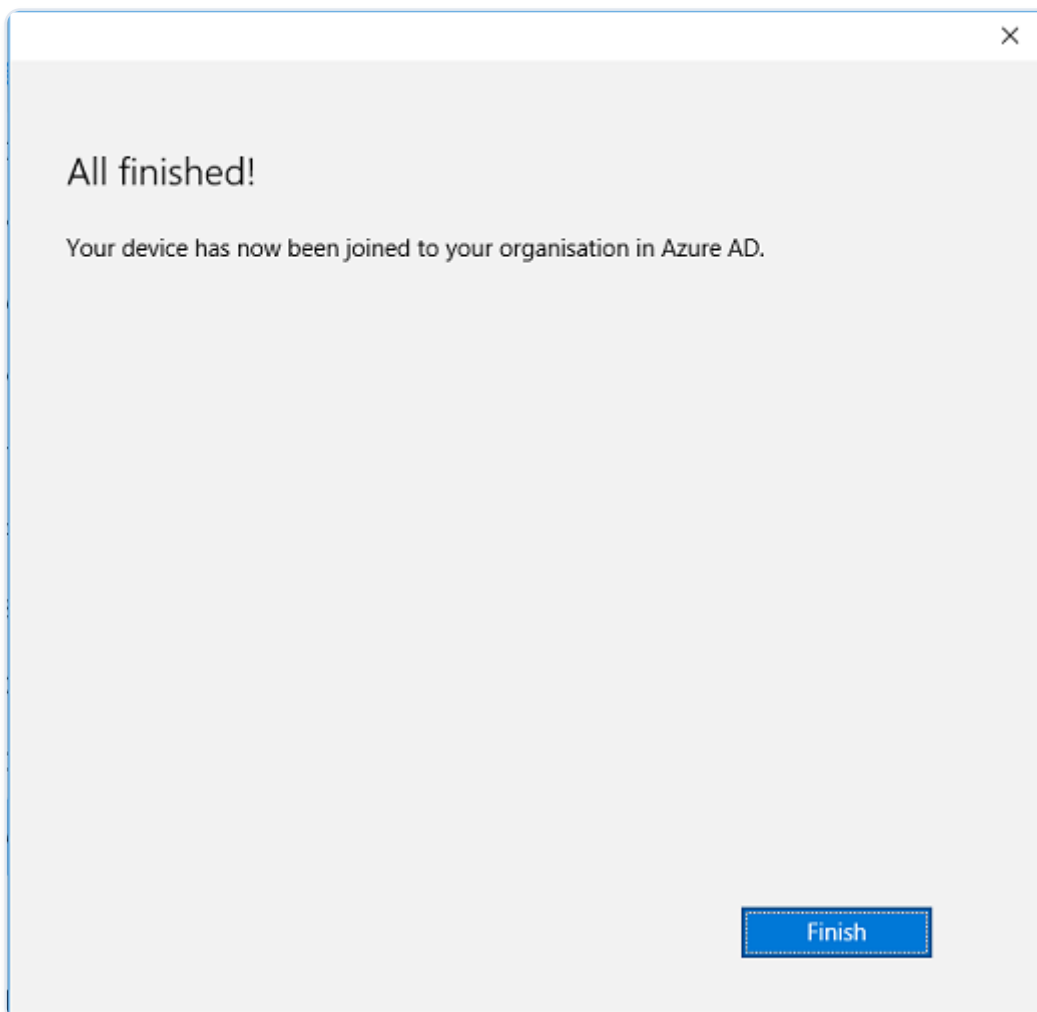
Sign in with the username and password you use with Office 365 (or other business services from Microsoft).

[Privacy statement](#)

Sign in Back

Beachten Sie, dass der UPN mit dem vom ADFS-Domänencontroller erkannten UPN übereinstimmen muss.



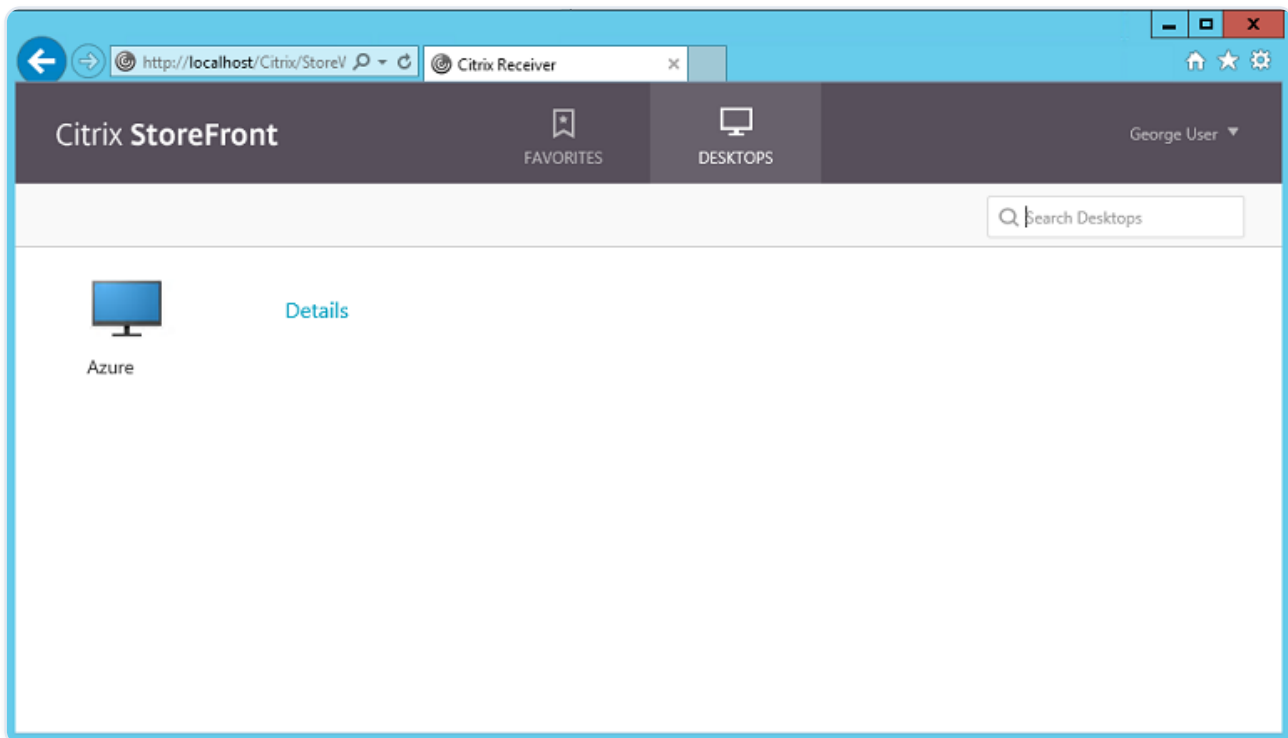


Überprüfen Sie, ob der Azure AD-Beitritt erfolgreich war, indem Sie den Computer neu starten und sich mit der E-Mail-Adresse des Benutzers anmelden. Starten Sie nach der Anmeldung Microsoft Edge und stellen Sie eine Verbindung zu `<http://myapps.microsoft.com>` her. Die Website sollte automatisch Single Sign-On verwenden.

Installieren Sie Citrix Virtual Apps oder Citrix Virtual Desktops

Sie können die virtuellen Maschinen des Delivery Controller und VDA in Azure direkt von der Citrix Virtual Apps- oder Citrix Virtual Desktops-ISO auf die übliche Weise installieren.

In diesem Beispiel ist StoreFront auf demselben Server wie der Delivery Controller installiert. Der VDA ist als eigenständiger Windows 2012 R2 RDS-Worker installiert, ohne Integration in Machine Creation Services (obwohl dies optional konfiguriert werden kann). Überprüfen Sie, ob der Benutzer George@citrixsamldemo.net sich mit einem Kennwort authentifizieren kann, bevor Sie fortfahren.



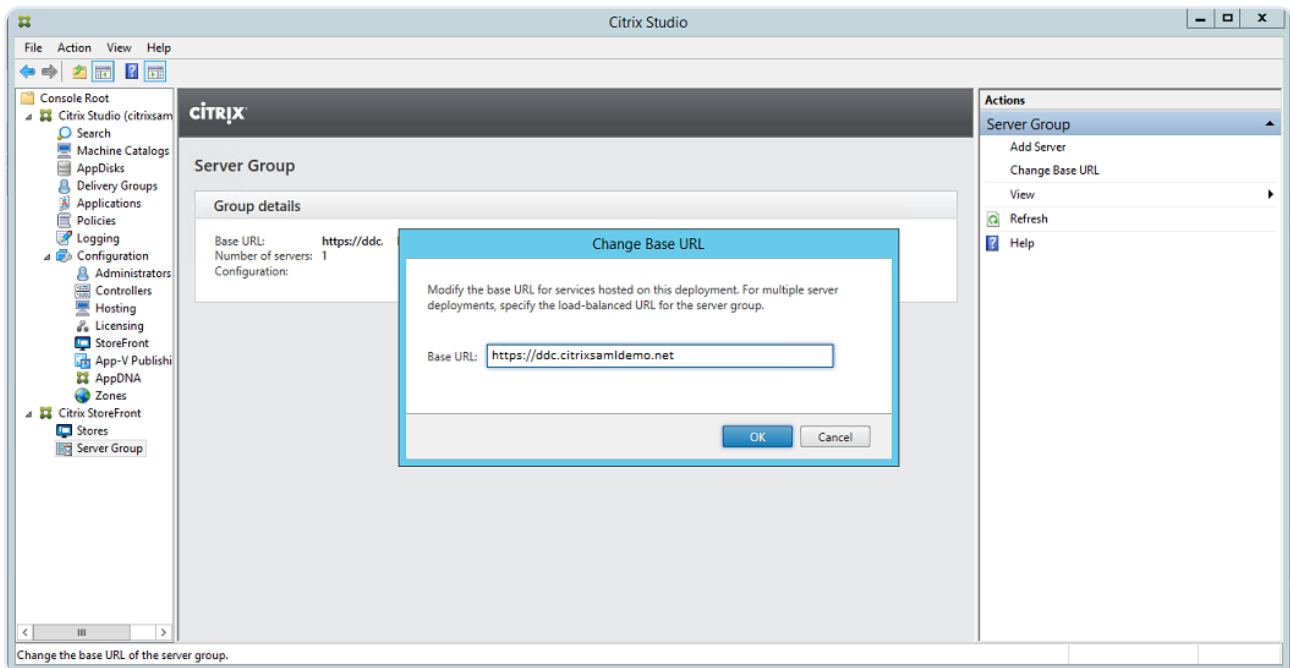
Führen Sie das PowerShell-Cmdlet **Set-BrokerSite -TrustRequestsSentToTheXmlServicePort \$true** auf dem Controller aus, um StoreFront™ die Authentifizierung ohne die Anmeldeinformationen der Benutzer zu ermöglichen.

Federated Authentication Service installieren

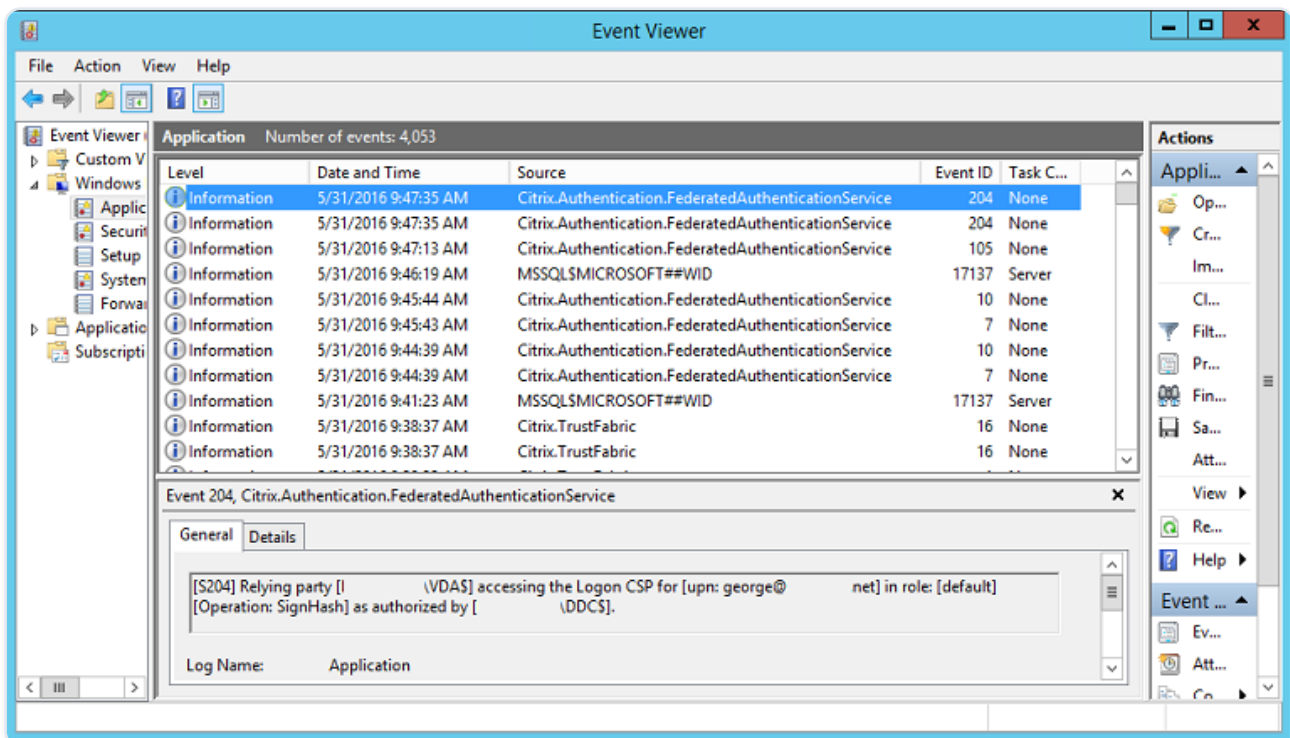
Installieren Sie FAS auf dem ADFS-Server und konfigurieren Sie eine Regel, damit der Delivery Controller als vertrauenswürdiger StoreFront fungiert (da StoreFront in diesem Beispiel auf derselben VM wie der Delivery Controller installiert ist). Siehe [Installieren und Konfigurieren](#).

StoreFront konfigurieren

Fordern Sie ein Computerzertifikat für den Delivery Controller an und konfigurieren Sie IIS und StoreFront für die Verwendung von HTTPS, indem Sie eine IIS-Bindung für Port 443 festlegen und die StoreFront-Basisadresse auf https: ändern.

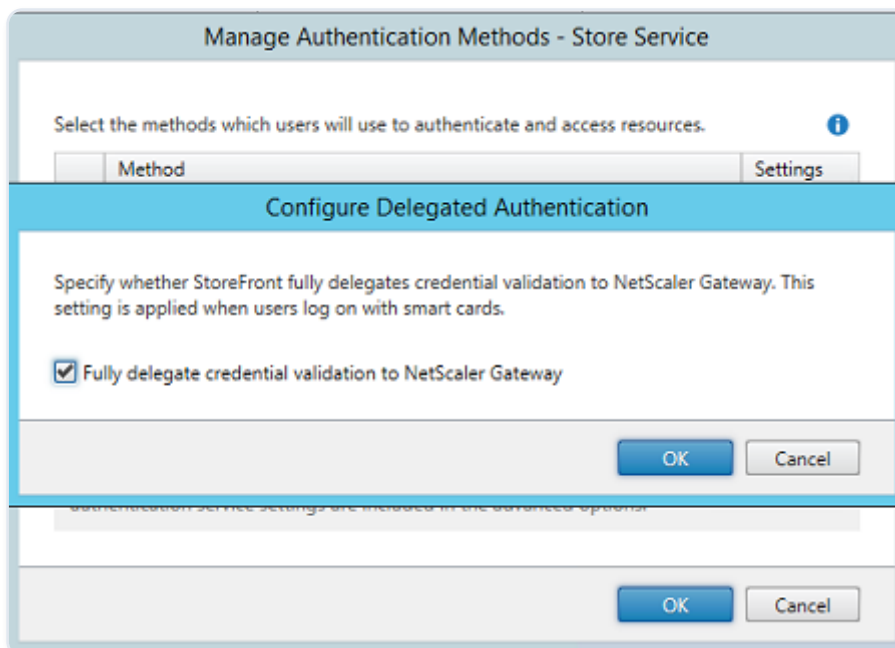


Konfigurieren Sie StoreFront für die Verwendung des FAS-Servers (verwenden Sie das PowerShell-Skript unter [Installieren und Konfigurieren](#)) und testen Sie intern in Azure, stellen Sie sicher, dass die Anmeldung FAS verwendet, indem Sie die Ereignisanzeige auf dem FAS-Server überprüfen.

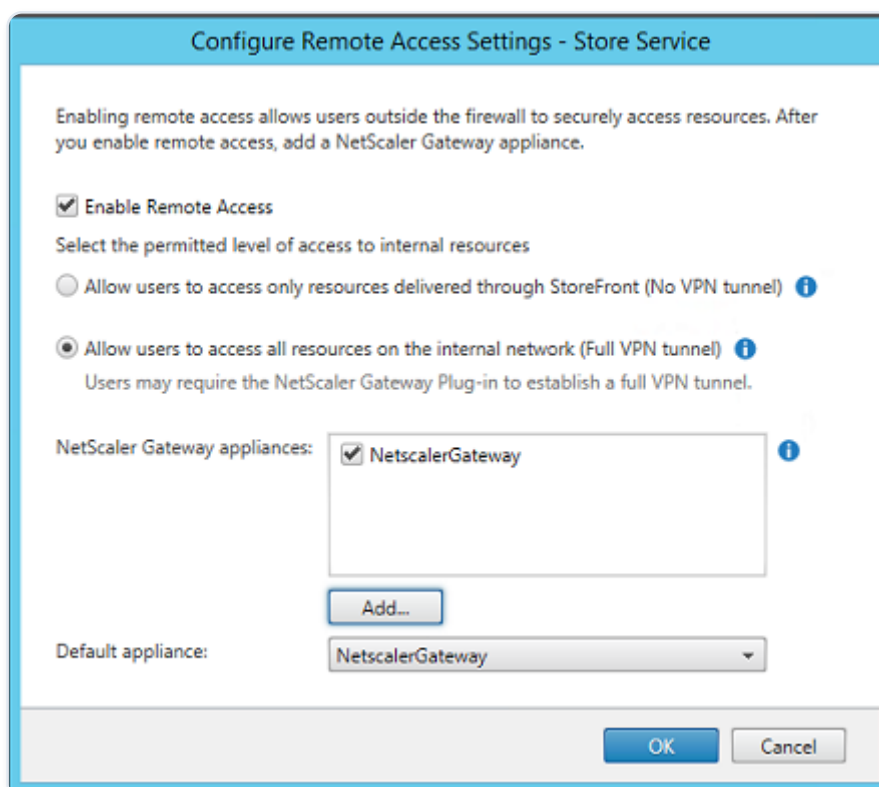


StoreFront für die Verwendung von Citrix Gateway konfigurieren

Verwenden Sie die GUI **Authentifizierungsmethoden verwalten** in der StoreFront-Verwaltungskonsolle, um StoreFront so zu konfigurieren, dass Citrix Gateway zur Authentifizierung verwendet wird.



Um die Authentifizierungsoptionen von Citrix Gateway zu integrieren, konfigurieren Sie eine Secure Ticket Authority (STA) und die Citrix Gateway-Adresse.



Neue Azure AD-Anwendung für Single Sign-On bei StoreFront konfigurieren

Dieser Abschnitt verwendet die Azure AD SAML 2.0 Single Sign-On-Funktionen, die derzeit ein Azure Active Directory Premium-Abonnement erfordern. Wählen Sie im Azure AD-Verwaltungstool **Neue Anwendung** und dann **Anwendung aus dem Katalog hinzufügen**.

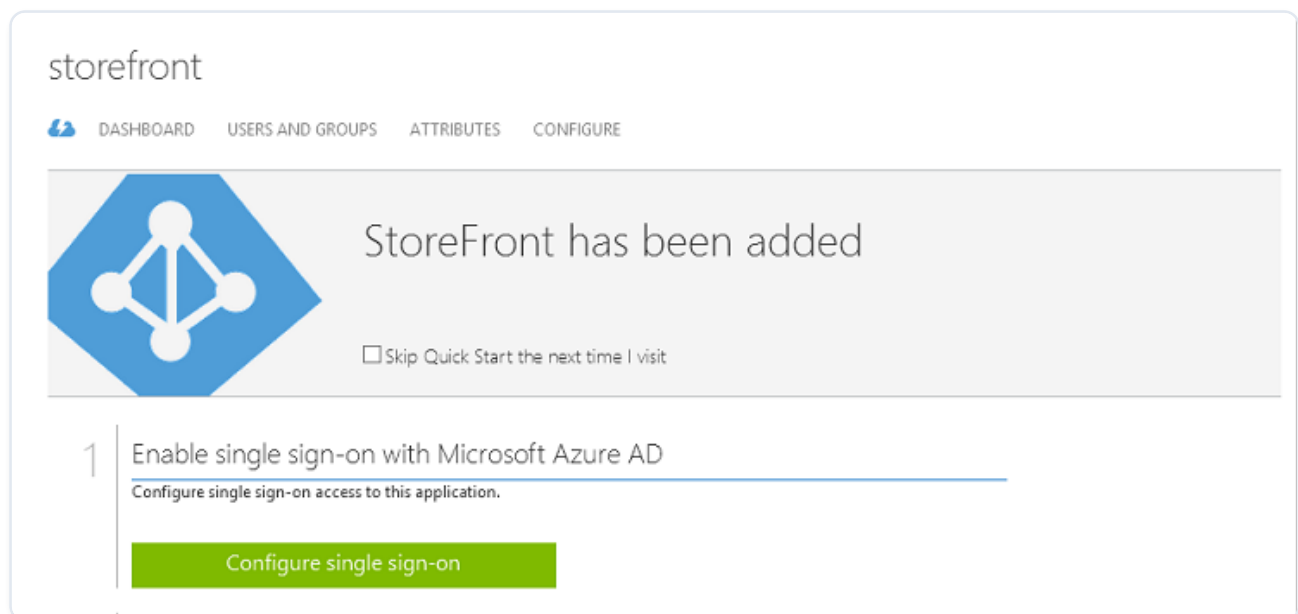
Wählen Sie **CUSTOM > Add an unlisted application my organization is using**, um eine neue benutzerdefinierte Anwendung für Ihre Benutzer zu erstellen.

Symbol konfigurieren

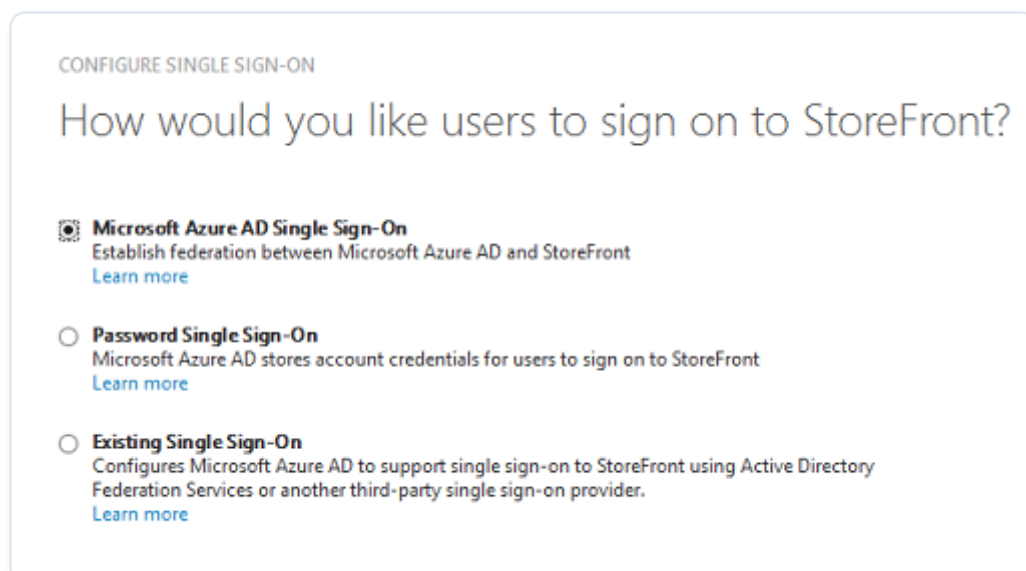
Erstellen Sie ein Bild mit einer Größe von 215 x 215 Pixeln und laden Sie es auf der Seite KONFIGURIEREN hoch, um es als Symbol für die Anwendung zu verwenden.

SAML-Authentifizierung konfigurieren

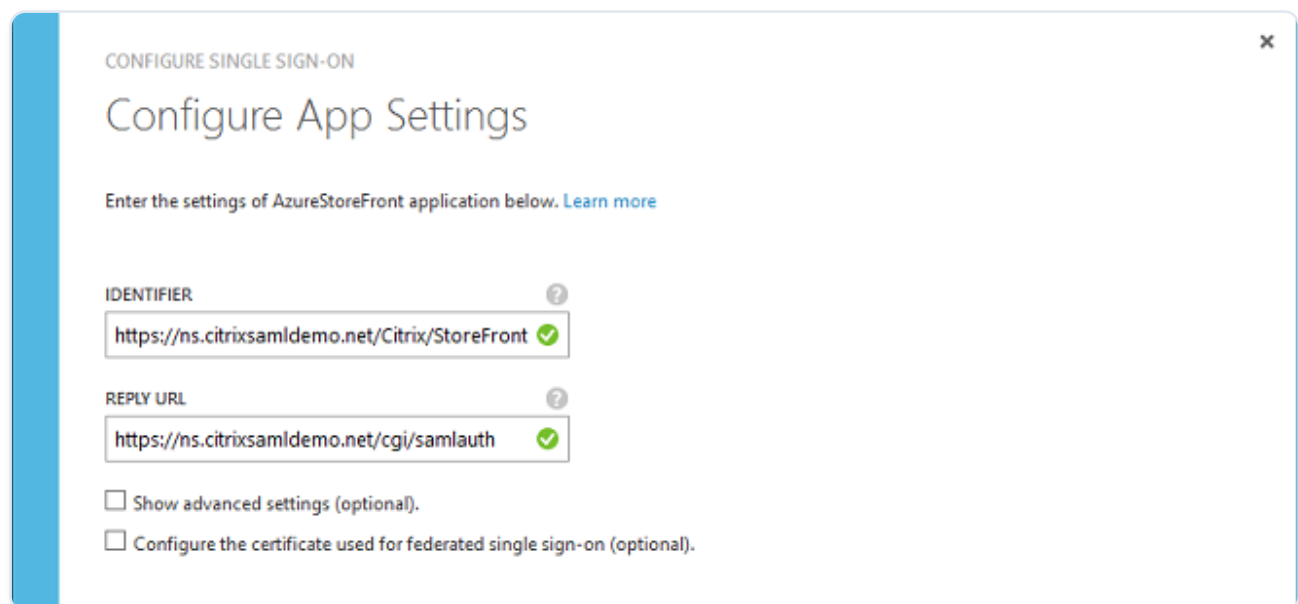
Kehren Sie zur Übersichtsseite des Anwendungs-Dashboards zurück und wählen Sie **Configure Single sign-on**.



Diese Bereitstellung verwendet SAML 2.0-Authentifizierung, was **Microsoft Azure AD Single Sign-On** entspricht.



Der **Identifier** kann eine beliebige Zeichenfolge sein (er muss mit der Konfiguration übereinstimmen, die Citrix Gateway bereitgestellt wird); in diesem Beispiel ist die **Reply URL** `/cgi/samlauth` auf dem Citrix Gateway-Server.



CONFIGURE SINGLE SIGN-ON

Configure App Settings

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

IDENTIFIER 

`https://ns.citrixsaml-demo.net/Citrix/StoreFront` 

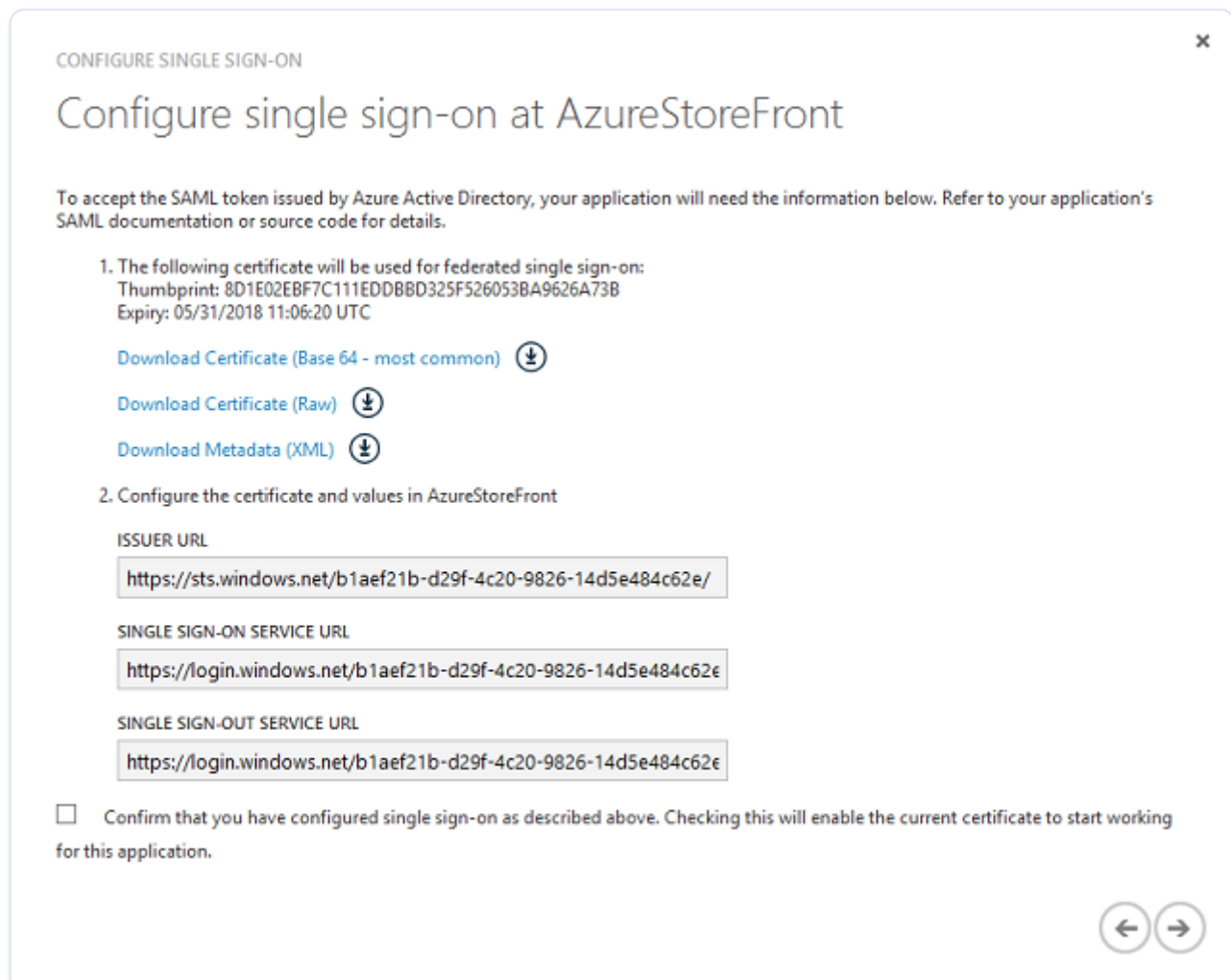
REPLY URL 

`https://ns.citrixsaml-demo.net/cgi/samlauth` 

☐ Show advanced settings (optional).

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

Die nächste Seite enthält Informationen, die zur Konfiguration von Citrix Gateway als vertrauende Partei für Azure AD verwendet werden.



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

`https://sts.windows.net/b1aef21b-d29f-4c20-9826-14d5e484c62e/`

SINGLE SIGN-ON SERVICE URL

`https://login.windows.net/b1aef21b-d29f-4c20-9826-14d5e484c62e`

SINGLE SIGN-OUT SERVICE URL

`https://login.windows.net/b1aef21b-d29f-4c20-9826-14d5e484c62e`

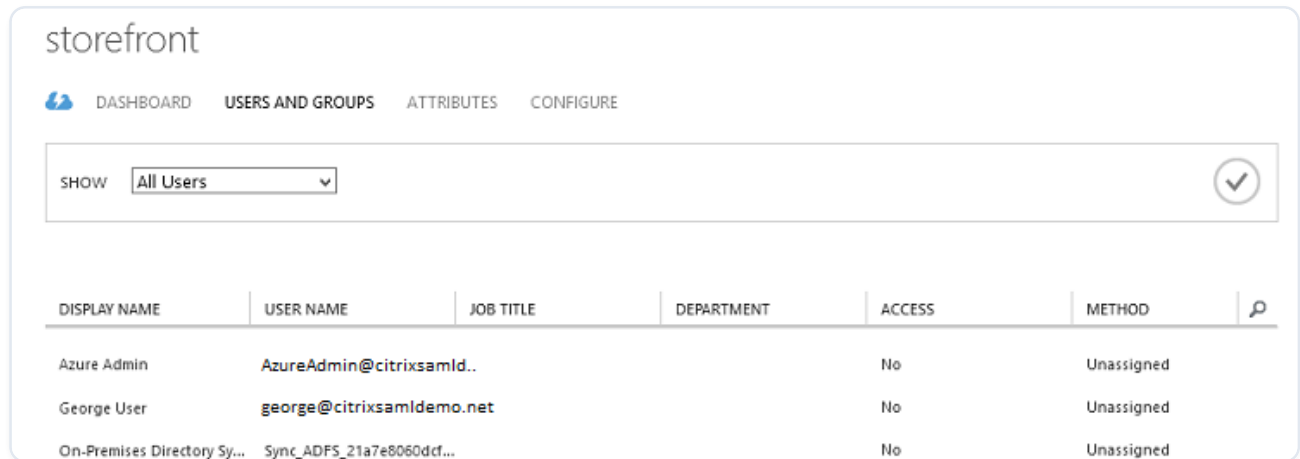
☐ Confirm that you have configured single sign-on as described above. Checking this will enable the current certificate to start working for this application.

Laden Sie das base 64 vertrauenswürdige Signaturzertifikat herunter und kopieren Sie die Anmelde- und Abmelde-URLs. Sie werden diese später in den Citrix Gateway-Konfigurationsbildschirmen einfügen.

Anwendung Benutzern zuweisen

Der letzte Schritt ist, die Anwendung zu aktivieren, damit sie auf der Steuerseite „myapps.microsoft.com“ der Benutzer angezeigt wird. Dies geschieht auf der Seite BENUTZER UND GRUPPEN. Weisen Sie den von Azure AD Connect synchronisierten Domänenbenutzerkonten Zugriff zu. Andere Konten können ebenfalls verwendet werden, müssen aber explizit zugeordnet werden, da sie nicht dem Muster \&user>@\&domain> entsprechen.



storefront

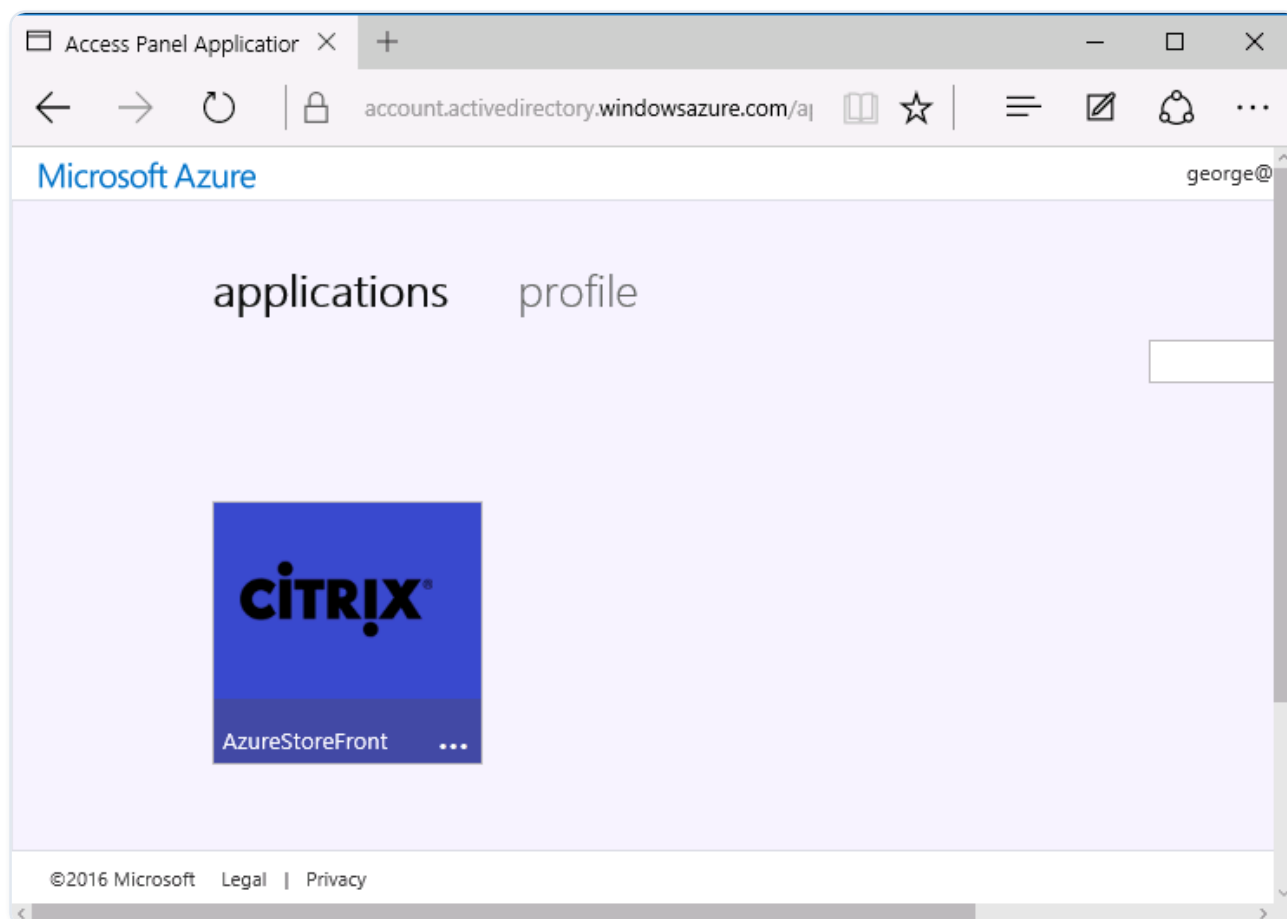
DASHBOARD USERS AND GROUPS ATTRIBUTES CONFIGURE

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-Seite

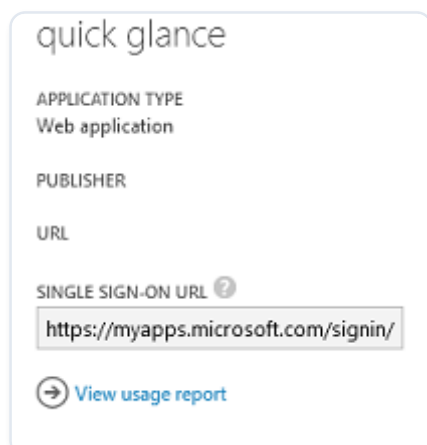
Wenn die Anwendung konfiguriert wurde, erscheint sie in den Listen der Azure-Anwendungen der Benutzer, wenn diese [<https://myapps.microsoft.com>](https://myapps.microsoft.com) besuchen.



Wenn es mit Azure AD verbunden ist, unterstützt Windows 10 Single Sign-On für Azure-Anwendungen für den angemeldeten Benutzer. Durch Klicken auf das Symbol gelangt der Browser zu der zuvor konfigurierten SAML cgi/samlauth Webseite.

Single Sign-On-URL

Kehren Sie zur Anwendung im Azure AD-Dashboard zurück. Es ist nun eine Single Sign-On-URL für die Anwendung verfügbar. Diese URL wird verwendet, um Webbrowser-Links bereitzustellen oder Startmenü-Verknüpfungen zu erstellen, die Benutzer direkt zu StoreFront führen.



Fügen Sie diese URL in einen Webbrowser ein, um sicherzustellen, dass Sie von Azure AD auf die zuvor konfigurierte Citrix Gateway cgi/samlauth Webseite umgeleitet werden. Dies funktioniert nur

für zugewiesene Benutzer und bietet Single Sign-On nur für Windows 10 Azure AD-verbundene Anmeldesitzungen. (Andere Benutzer werden zur Eingabe ihrer Azure AD-Anmeldeinformationen aufgefordert.)

Citrix Gateway installieren und konfigurieren

Um remote auf die Bereitstellung zuzugreifen, verwendet dieses Beispiel eine separate VM, auf der NetScaler (jetzt Citrix Gateway) ausgeführt wird. Diese kann im Azure Store erworben werden. Dieses Beispiel verwendet die „Bring your own License“-Version von NetScaler 11.0.



Melden Sie sich bei der NetScaler® VM an, indem Sie einen Webbrowser auf die interne IP-Adresse richten und die Anmeldeinformationen verwenden, die bei der Authentifizierung des Benutzers angegeben wurden. Beachten Sie, dass Sie das Kennwort des nsroot-Benutzers in einer Azure AD VM ändern müssen.

Fügen Sie Lizenzen hinzu, wählen Sie nach dem Hinzufügen jeder Lizenzdatei **Neustart** und richten Sie den DNS-Resolver auf den Microsoft-Domänencontroller.

Führen Sie den Einrichtungsassistenten für Citrix Virtual Apps and Desktops aus

Dieses Beispiel beginnt mit der Konfiguration einer einfachen StoreFront-Integration ohne SAML. Nachdem diese Bereitstellung funktioniert, wird eine SAML-Anmelderichtlinie hinzugefügt.

XenApp/XenDesktop Setup Wizard

What is your deployment

Single Hop



The diagram illustrates a 'Single Hop' deployment architecture. It shows a 'Client' (represented by a person icon) connected to the 'Internet' (cloud icon). The Internet connects to an 'Access Gateway' (server rack icon). The Access Gateway then connects to a 'Server Farm' (multiple server rack icons). The connection path is indicated by blue lines and dots.

What is your Citrix Integration Point?

StoreFront

Continue Cancel

Wählen Sie die Standardeinstellungen für Citrix Gateway StoreFront aus. Für die Verwendung in Microsoft Azure konfiguriert dieses Beispiel Port 4433 anstelle von Port 443. Alternativ können Sie die administrative Citrix Gateway-Website per Portweiterleitung konfigurieren oder neu zuordnen.

NetScaler Gateway Settings

NetScaler Gateway IP Address*

10 . 0 . 0 . 18

Port*

4433

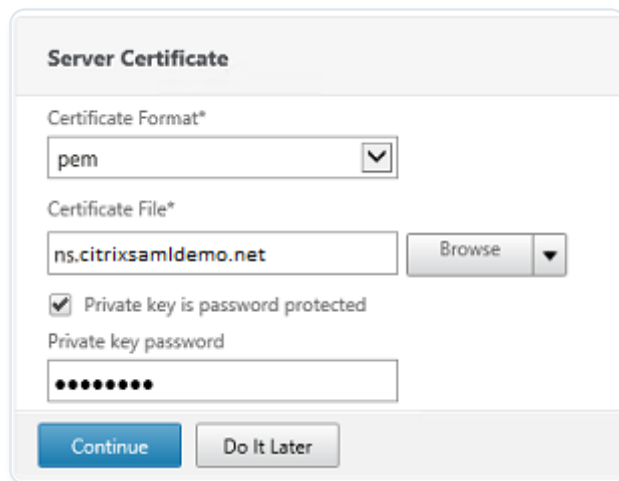
Virtual Server Name*

ns.citrixsaml-demo.net

☐ Redirect requests from port 80 to secure port

Continue Cancel

Der Einfachheit halber lädt das Beispiel ein vorhandenes Serverzertifikat und einen privaten Schlüssel hoch, die in einer Datei gespeichert sind.



Server Certificate

Certificate Format*
pem

Certificate File*
ns.citrixsamldemo.net Browse

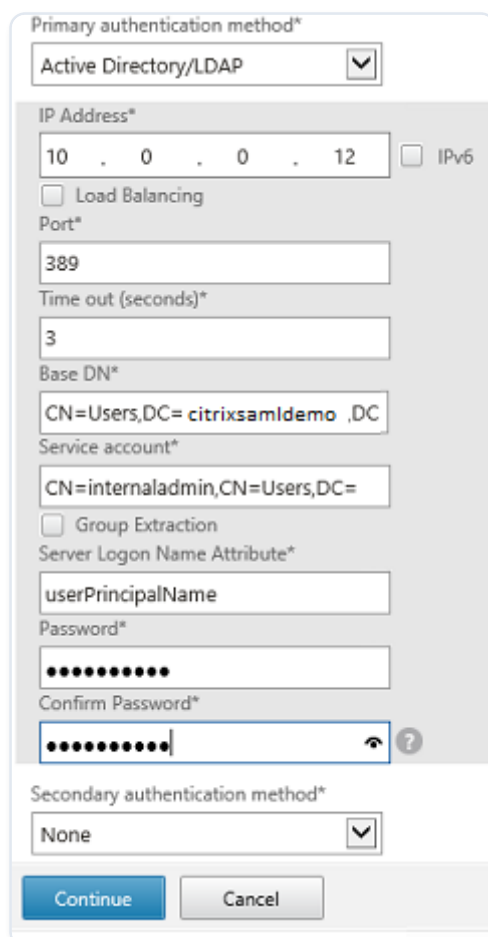
☒ Private key is password protected

Private key password
••••••••

Continue Do It Later

Domänencontroller für die AD-Kontoverwaltung konfigurieren

Der Domänencontroller wird für die Kontenauflösung verwendet. Fügen Sie daher seine IP-Adresse zur primären Authentifizierungsmethode hinzu. Beachten Sie die in jedem Feld des Dialogfelds erwarteten Formate.



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= citrixsamldemo .DC

Service account*
CN=internaladmin,CN=Users,DC=

☐ Group Extraction

Server Logon Name Attribute*
userPrincipalName

Password*
••••••••

Confirm Password*
••••••••

Secondary authentication method*
None

Continue Cancel

StoreFront-Adresse konfigurieren

In diesem Beispiel wurde StoreFront mit HTTPS konfiguriert, wählen Sie daher die SSL-Protokolloptionen aus.

StoreFront

StoreFront FQDN*

ddc.citrixsamldemo.net

Site Path*

/Citrix/StoreWeb

Single Sign-on Domain*

citrixsamldemo

Store Name*

/Citrix/StoreWeb

Secure Ticket Authority Server*

http://ddc.citrixsamldemo.net/sta

StoreFront Server*

10 . 0 . 0 . 15

Protocol*

SSL

Port*

443

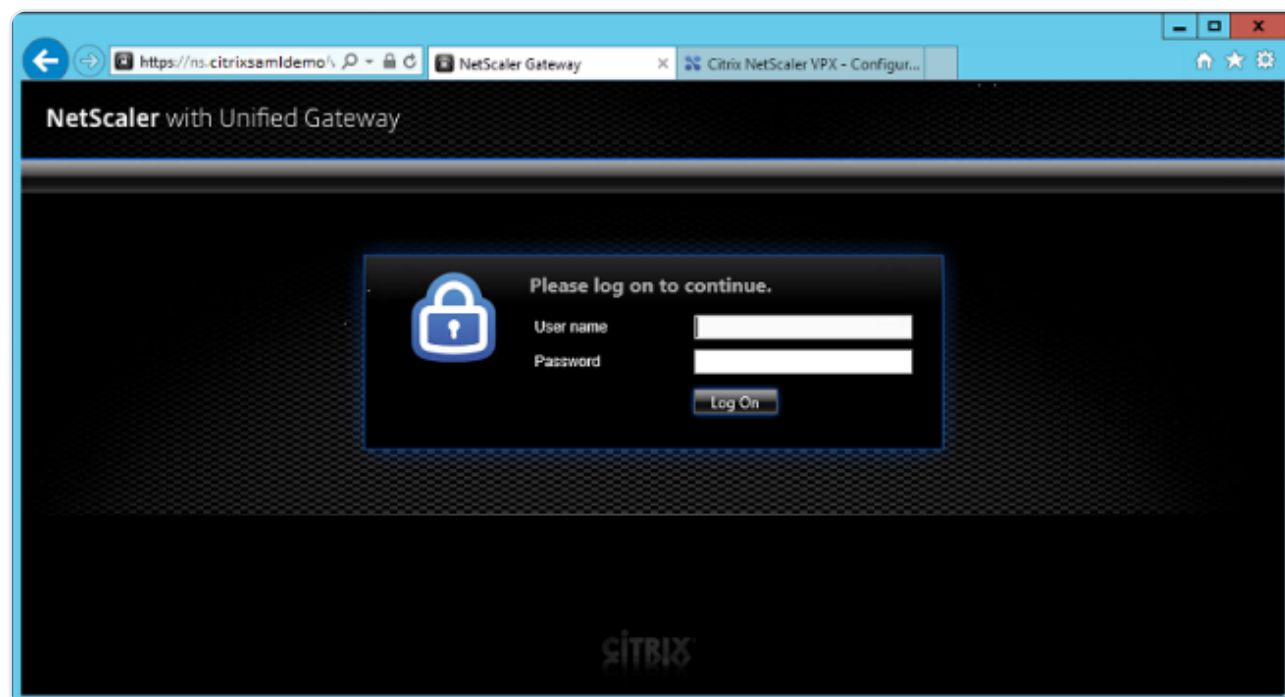
☐ Load Balancing

Continue

Cancel

Citrix Gateway-Bereitstellung überprüfen

Stellen Sie eine Verbindung mit Citrix Gateway her und überprüfen Sie, ob Authentifizierung und Start mit dem Benutzernamen und Kennwort erfolgreich sind.



Citrix Gateway SAML-Authentifizierungsunterstützung aktivieren

Die Verwendung von SAML mit StoreFront ähnelt der Verwendung von SAML mit anderen Websites. Fügen Sie eine neue SAML-Richtlinie mit dem Ausdruck **NS_TRUE** hinzu.

Configure Authentication SAML Policy

Name
StoreFrontSAML

Authentication Type
SAML

Server*
AzureAd

Expression*
Operators Saved Policy Expressions Frequently Used Expressions
NS_TRUE

OK Close

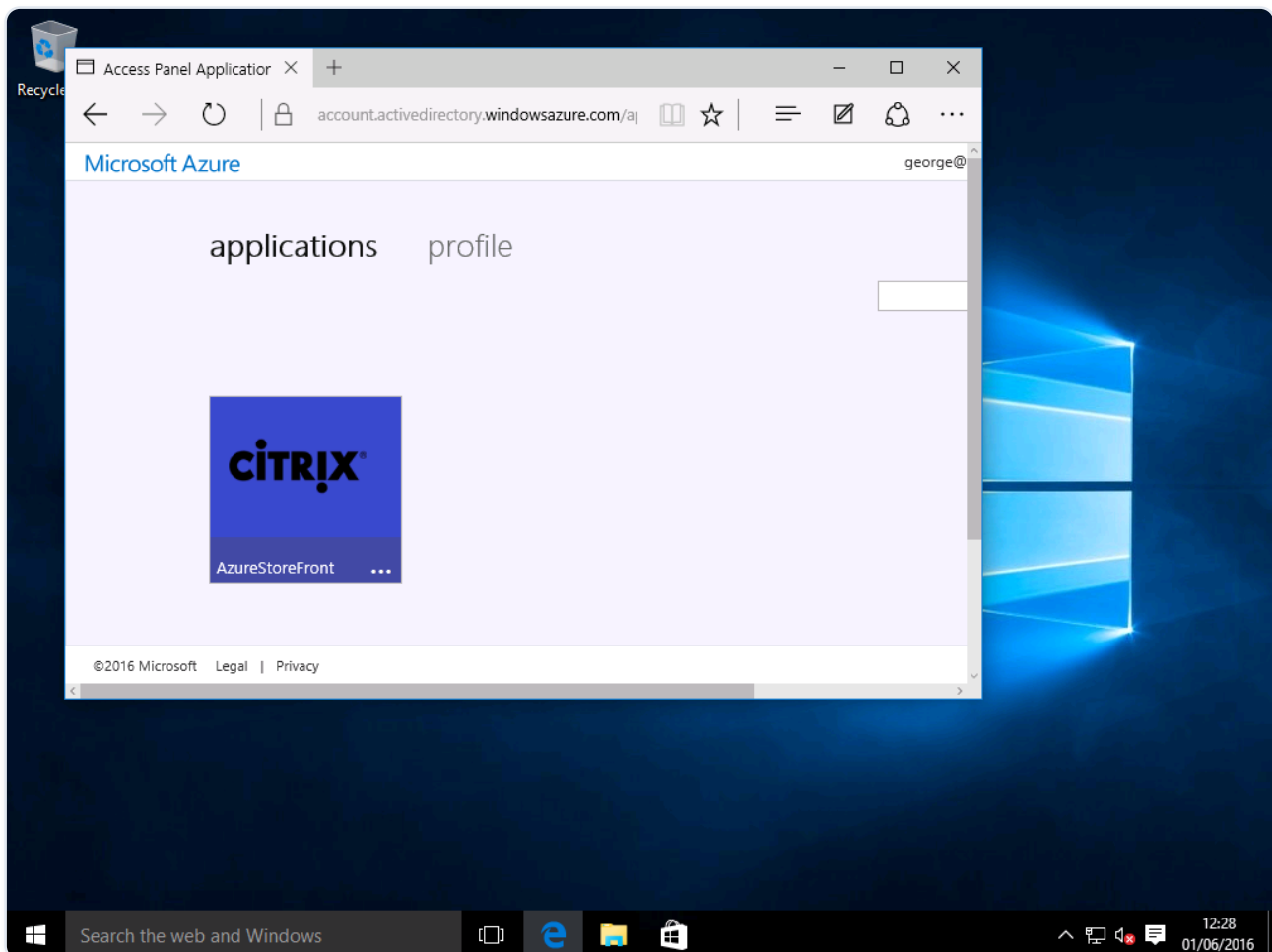
Konfigurieren Sie den neuen SAML IdP-Server mit den zuvor von Azure AD erhaltenen Informationen.

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	
	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

End-to-End-System überprüfen

Melden Sie sich mit einem in Azure AD registrierten Konto an einem Azure AD Joined Windows 10-Desktop an. Starten Sie Microsoft Edge und stellen Sie eine Verbindung her zu: `<https://myapps.microsoft.com>`.

Der Webbrowser sollte die Azure AD-Anwendungen für den Benutzer anzeigen.



Überprüfen Sie, ob das Klicken auf das Symbol Sie zu einem authentifizierten StoreFront-Server weiterleitet.

Überprüfen Sie ebenfalls, ob direkte Verbindungen über die Single Sign-on URL und eine direkte Verbindung zur Citrix Gateway-Site Sie zu Microsoft Azure und zurück umleiten.

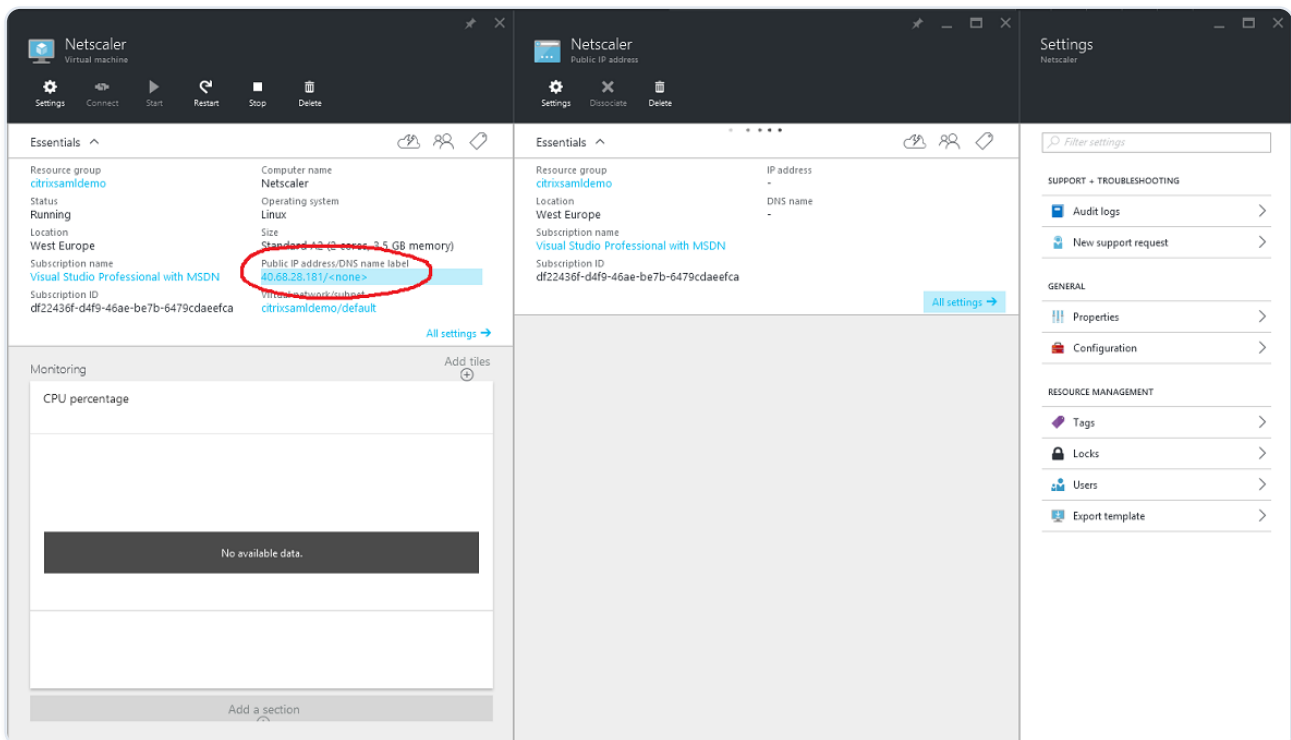
Überprüfen Sie schließlich, ob auch nicht-Azure AD-verbundene Maschinen mit denselben URLs funktionieren (obwohl für die erste Verbindung eine einmalige explizite Anmeldung bei Azure AD erforderlich ist).

Anhang

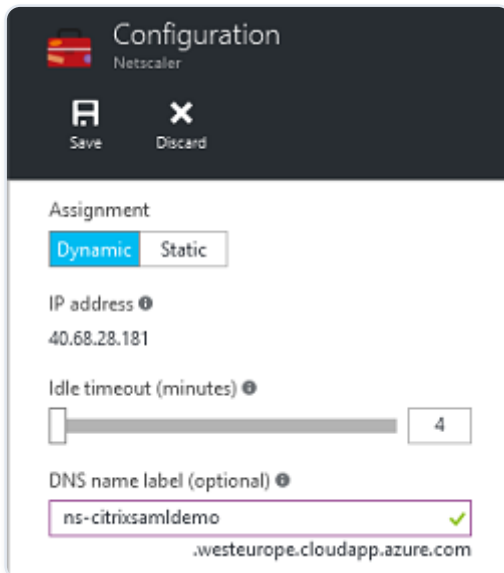
Sie sollten die folgenden Standardoptionen konfigurieren, wenn Sie eine VM in Azure einrichten.

Eine öffentliche IP-Adresse und DNS-Adresse bereitstellen

Azure weist allen VMs eine IP-Adresse im internen Subnetz zu (in diesem Beispiel 10.*.*.*). Standardmäßig wird auch eine öffentliche IP-Adresse bereitgestellt, auf die über ein dynamisch aktualisiertes DNS-Label verwiesen werden kann.



Wählen Sie **Konfiguration des Labels für öffentliche IP-Adresse/DNS-Name**. Wählen Sie eine öffentliche DNS-Adresse für die VM. Diese kann für CNAME-Verweise in anderen DNS-Zonendateien verwendet werden, um sicherzustellen, dass alle DNS-Einträge weiterhin korrekt auf die VM verweisen, selbst wenn die IP-Adresse neu zugewiesen wird.

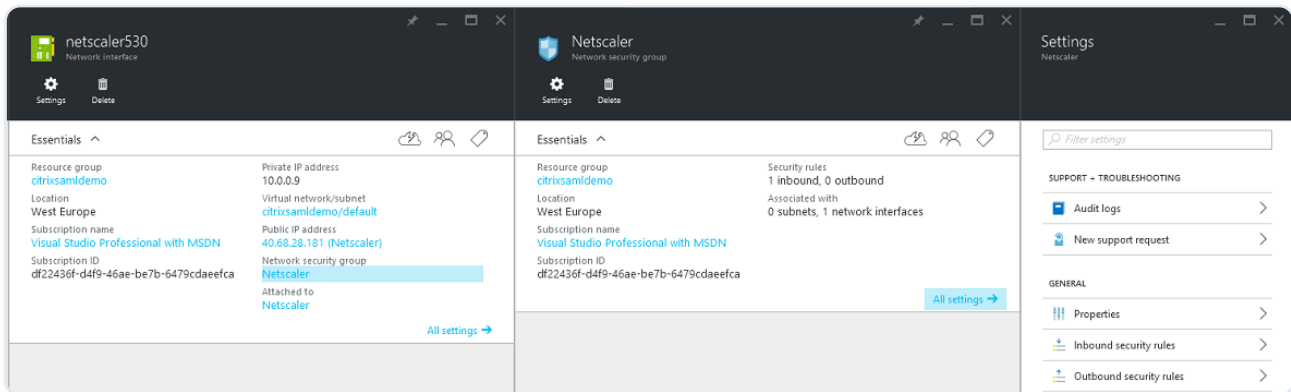


Firewallregeln einrichten (Sicherheitsgruppe)

Jede VM in einer Cloud verfügt über einen Satz automatisch angewendeter Firewallregeln, die als Sicherheitsgruppe bezeichnet werden. Die Sicherheitsgruppe steuert den Datenverkehr, der von der öffentlichen an die private IP-Adresse weitergeleitet wird. Standardmäßig erlaubt Azure die

Weiterleitung von RDP an alle VMs. Die Citrix Gateway- und ADFS-Server müssen auch TLS-Datenverkehr (443) weiterleiten.

Öffnen Sie **Netzwerkschnittstellen** für eine VM und klicken Sie dann auf das Label **Netzwerksicherheitsgruppe**. Konfigurieren Sie die **Regeln für eingehende Sicherheit**, um den entsprechenden Netzwerkverkehr zuzulassen.



Verwandte Informationen

- [Installieren und Konfigurieren](#) ist die primäre Referenz für die FAS-Installation und -Konfiguration.
- Die gängigen FAS-Bereitstellungen sind im Artikel [Bereitstellungsarchitekturen](#) zusammengefasst.
- „How-to“-Artikel werden im Artikel [Erweiterte Konfiguration](#) vorgestellt.

Erweiterte Konfiguration

Die Anleitungsaufgaben in diesem Abschnitt bieten erweiterte Konfigurations- und Verwaltungsaufgaben für den Federated Authentication Service (FAS).

Zugehörige Informationen

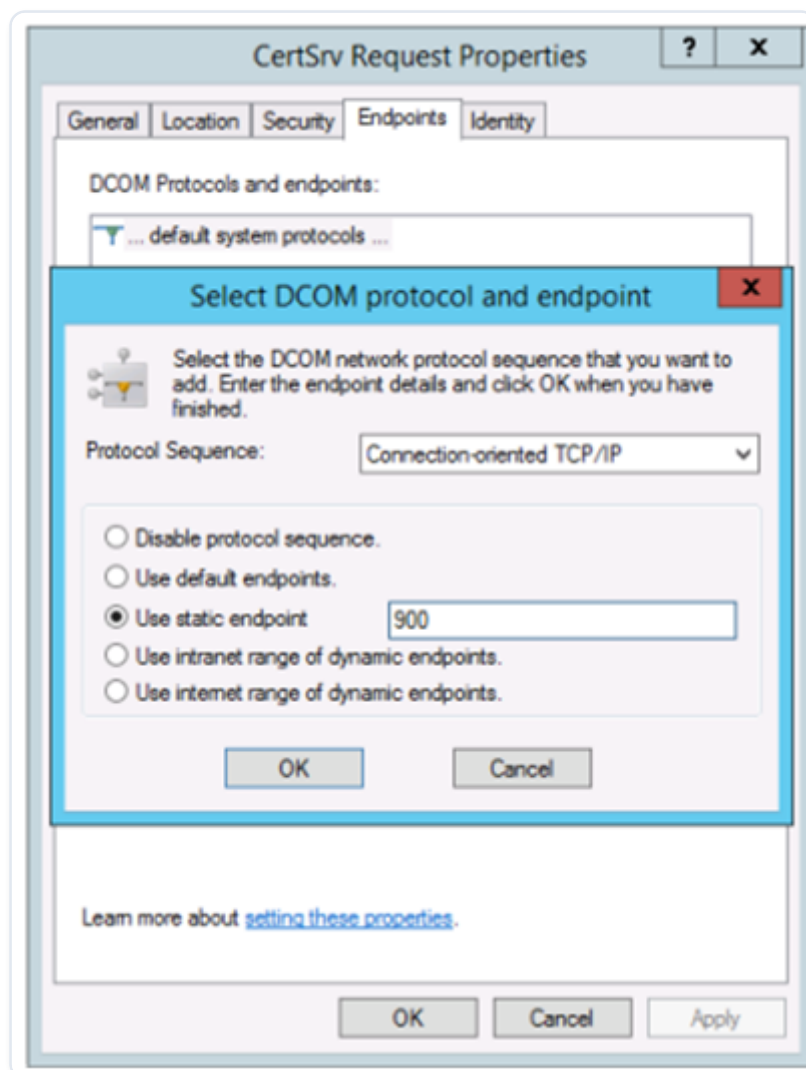
- Die primäre Referenz für die FAS-Installation und Ersteinrichtung ist der Artikel [Installieren und Konfigurieren](#).
- Der Artikel [Bereitstellungsarchitekturen](#) bietet Zusammenfassungen der wichtigsten FAS-Architekturen sowie Links zu weiteren Artikeln über die komplexeren Architekturen.

Konfiguration der Zertifizierungsstelle

Dieser Artikel beschreibt die erweiterte Konfiguration des Federated Authentication Service (FAS) zur Integration mit Zertifizierungsstellenservern, die von der FAS-Verwaltungskonsolle nicht unterstützt werden. Die Anweisungen verwenden PowerShell-APIs, die von FAS bereitgestellt werden. Sie sollten über grundlegende PowerShell-Kenntnisse verfügen, bevor Sie die Anweisungen in diesem Artikel ausführen.

Konfigurieren der Microsoft-Zertifizierungsstelle für den TCP-Zugriff

Standardmäßig verwendet die Microsoft-Zertifizierungsstelle DCOM für den Zugriff. Dies kann bei der Implementierung von Firewall-Sicherheit zu Komplexitäten führen, daher bietet Microsoft die Möglichkeit, auf einen statischen TCP-Port umzuschalten. Öffnen Sie auf der Microsoft-Zertifizierungsstelle das DCOM-Konfigurationsfenster und bearbeiten Sie die Eigenschaften der DCOM-Anwendung „CertSrv Request“:



Ändern Sie die „Endpunkte“, um einen statischen Endpunkt auszuwählen und eine TCP-Portnummer anzugeben (900 in der obigen Grafik).

Starten Sie die Microsoft-Zertifizierungsstelle neu und übermitteln Sie eine Zertifikatanforderung. Wenn Sie `netstat -a -n -b` ausführen, sollten Sie sehen, dass certsrv jetzt auf Port 900 lauscht:

TCP	0.0.0.0:636	dc:0	LISTENING
[lsass.exe]			
TCP	0.0.0.0:900	dc:0	LISTENING
[certsrv.exe]			
TCP	0.0.0.0:3268	dc:0	LISTENING
[lsass.exe]			
TCP	0.0.0.0:3269	dc:0	LISTENING

Es ist nicht erforderlich, den FAS-Server (oder andere Maschinen, die die Zertifizierungsstelle verwenden) zu konfigurieren, da DCOM eine Aushandlungsphase über den RPC-Port hat. Wenn ein Client DCOM verwenden muss, stellt er eine Verbindung zum DCOM-RPC-Dienst auf dem Zertifikatserver her und fordert Zugriff auf einen bestimmten DCOM-Server an. Dies führt dazu,

dass Port 900 geöffnet wird und der DCOM-Server den FAS-Server anweist, wie er sich verbinden soll.

Benutzerzertifikate vorab generieren

Die Anmeldezeit für Benutzer wird erheblich verbessert, wenn Benutzerzertifikate auf dem FAS-Server vorab generiert werden. Die folgenden Abschnitte beschreiben, wie dies für einzelne oder mehrere FAS-Server erfolgen kann.

Liste der Active Directory-Benutzer abrufen

Sie können die Zertifikatgenerierung verbessern, indem Sie das AD abfragen und die Benutzerliste in einer Datei (z. B. einer .csv-Datei) speichern, wie im folgenden Beispiel gezeigt.

```
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 {

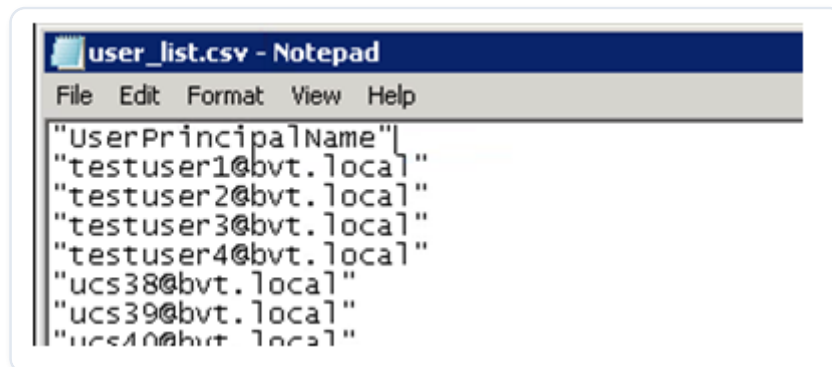
    Get-ADUser -Filter {(UserPrincipalName -ne "null") -and (Enabled -eq
"true")}} -Properties UserPrincipalName | Select UserPrincipalName |
Export-Csv -NoTypeInfoInformation -Encoding utf8 -delimiter "," $filename

}
```

Get-ADUser ist ein Standard-Cmdlet zum Abfragen einer Benutzerliste. Das obige Beispiel enthält ein Filterargument, um nur Benutzer mit einem UserPrincipalName und dem Kontostatus „enabled“ aufzulisten.

Das Argument SearchBase schränkt den Teil des AD ein, in dem nach Benutzern gesucht werden soll. Sie können dies weglassen, wenn Sie alle Benutzer im AD einschließen möchten. Hinweis: Diese Abfrage kann eine große Anzahl von Benutzern zurückgeben.

Die CSV-Datei sieht etwa so aus:



FAS-Server

Das folgende PowerShell-Skript übernimmt die zuvor generierte Benutzerliste und erstellt eine Liste von Benutzerzertifikaten.

```
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) {

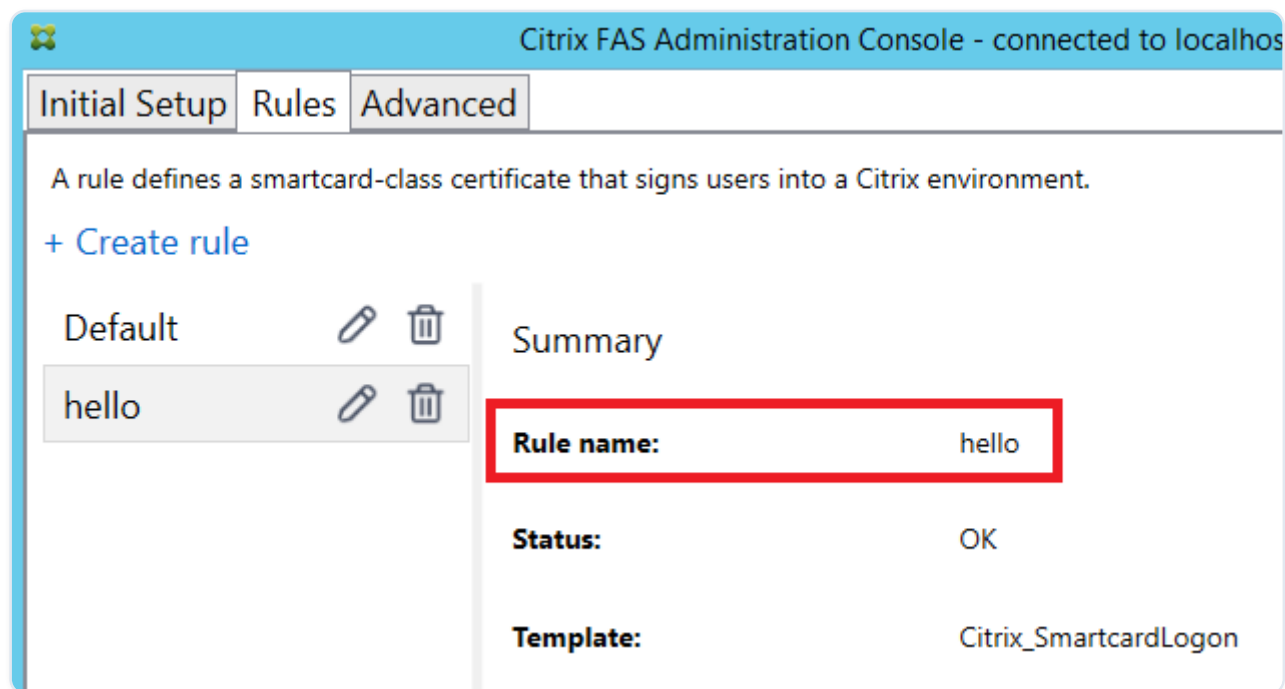
    New-FasUserCertificate -Address $server.Failover
    -UserPrincipalName $user.UserPrincipalName -CertificateDefinition
    $rule"_Definition" -Rule $rule

}

}
```

Wenn Sie mehr als einen FAS-Server haben, wird das Zertifikat eines bestimmten Benutzers zweimal generiert: einmal auf dem Hauptserver und einmal auf dem Failover-Server.

Das obige Skript ist für eine Regel namens 'default' ausgelegt. Wenn Sie einen anderen Regelnamen haben (zum Beispiel 'hello'), ändern Sie einfach die Variable \$rule im Skript.

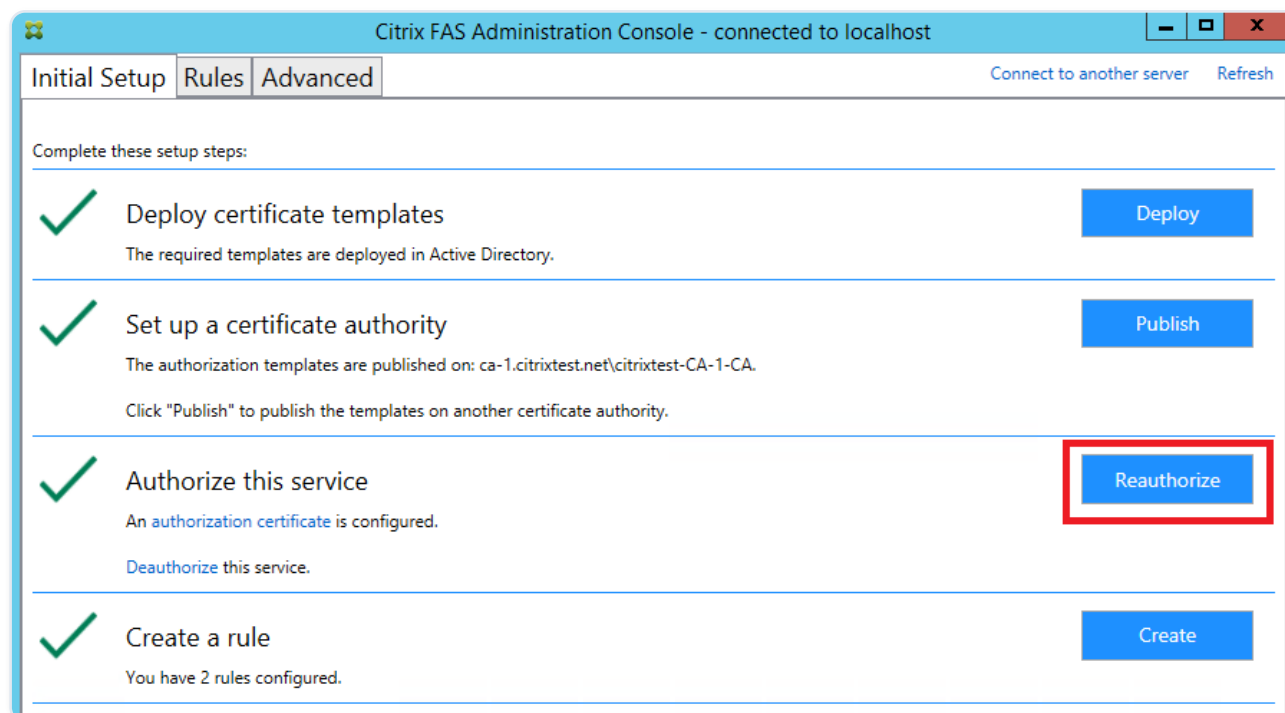


Registrierungsstellenzertifikate erneuern

Wenn mehr als ein FAS-Server verwendet wird, können Sie ein FAS-Autorisierungszertifikat erneuern, ohne angemeldete Benutzer zu beeinträchtigen.

HINWEIS:

Sie können FAS auch über die GUI erneut autorisieren:



Führen Sie die folgende Sequenz aus:

1. Erstellen Sie ein neues Autorisierungszertifikat: `New-FasAuthorizationCertificate`
2. Notieren Sie die GUID des neuen Autorisierungszertifikats, wie zurückgegeben von: `Get-FasAuthorizationCertificate`
3. Versetzen Sie den FAS-Server in den Wartungsmodus: `Set-FasServer -Address <FAS server> -MaintenanceMode $true`
4. Tauschen Sie das neue Autorisierungszertifikat aus: `Set-FasCertificateDefinition -AuthorizationCertificate <GUID>`
5. Nehmen Sie den FAS-Server aus dem Wartungsmodus: `Set-FasServer -Address <FAS server> -MaintenanceMode $false`
6. Löschen Sie das alte Autorisierungszertifikat: `Remove-FasAuthorizationCertificate`

Zugehörige Informationen

- Der Artikel [Install and configure](#) ist die primäre Referenz für die FAS-Installation und -Konfiguration.
- Die gängigen Bereitstellungen des Federated Authentication Service werden im Artikel [Deployment architectures](#) zusammengefasst.

- Weitere „How-to“-Artikel werden im Artikel [Advanced configuration](#) vorgestellt.

Schutz privater Schlüssel

Einführung

Private Schlüssel werden über das Netzwerkkonto gespeichert und sind standardmäßig als nicht exportierbar gekennzeichnet.

Es gibt zwei Arten von privaten Schlüsseln:

- Der private Schlüssel, der dem Zertifikat der Registrierungsstelle aus der Zertifikatvorlage Citrix_RegistrationAuthority zugeordnet ist.
- Die privaten Schlüssel, die den Benutzerzertifikaten aus der Zertifikatvorlage Citrix_SmartcardLogon zugeordnet sind.

Es gibt tatsächlich zwei Zertifikate der Registrierungsstelle:

Citrix_RegistrationAuthority_ManualAuthorization (standardmäßig 24 Stunden gültig) und Citrix_RegistrationAuthority (standardmäßig zwei Jahre gültig).

In Schritt 3 der Registerkarte **Erstmalige Einrichtung** in der Administrationskonsole des Federated Authentication Service (FAS) generiert der FAS-Server beim Klicken auf **Autorisieren** ein Schlüsselpaar und sendet eine Zertifikatsignieranforderung an die Zertifizierungsstelle für das Zertifikat Citrix_RegistrationAuthority_ManualAuthorization. Dies ist ein temporäres Zertifikat, das standardmäßig 24 Stunden gültig ist. Die Zertifizierungsstelle stellt dieses Zertifikat nicht automatisch aus; die Ausstellung muss von einem Administrator manuell bei der Zertifizierungsstelle autorisiert werden. Sobald das Zertifikat an den FAS-Server ausgestellt wurde, verwendet FAS das Zertifikat Citrix_RegistrationAuthority_ManualAuthorization, um automatisch das Zertifikat Citrix_RegistrationAuthority (standardmäßig zwei Jahre gültig) zu erhalten. Der FAS-Server löscht das Zertifikat und den Schlüssel für Citrix_RegistrationAuthority_ManualAuthorization, sobald er das Zertifikat Citrix_RegistrationAuthority erhalten hat.

Der private Schlüssel, der dem Zertifikat der Registrierungsstelle zugeordnet ist, ist besonders sensibel, da die Zertifikatsrichtlinie der Registrierungsstelle es jedem, der den privaten Schlüssel besitzt, erlaubt, Zertifikatsanforderungen für die in der Vorlage konfigurierte Benutzergruppe auszustellen. Folglich kann jeder, der diesen Schlüssel kontrolliert, sich als jeder der Benutzer in der Gruppe bei der Umgebung anmelden.

Sie können den FAS-Server so konfigurieren, dass private Schlüssel auf eine Weise geschützt werden, die den Sicherheitsanforderungen Ihres Unternehmens entspricht, indem Sie eine der folgenden Optionen verwenden:

- Microsoft Enhanced RSA and AES Cryptographic Provider oder Microsoft Software Key Storage Provider für die privaten Schlüssel des Registrierungsstellenzertifikats und der Benutzerzertifikate.
- Microsoft Platform Key Storage Provider mit einem Trusted Platform Module (TPM)-Chip für den privaten Schlüssel des Registrierungsstellenzertifikats und Microsoft Enhanced RSA and AES Cryptographic Provider oder Microsoft Software Key Storage Provider für die privaten Schlüssel der Benutzerzertifikate.
- Ein Cryptographic Service oder Key Storage Provider eines Hardware Security Module (HSM)-Anbieters mit dem HSM-Gerät für die privaten Schlüssel des Registrierungsstellenzertifikats und der Benutzerzertifikate.

Konfigurationseinstellungen für private Schlüssel

Konfigurieren Sie FAS für eine der drei Optionen. Bearbeiten Sie die Datei Citrix.Authentication.FederatedAuthenticationService.exe.config mit einem Texteditor. Der Standardspeicherort der Datei ist im Ordner Program Files\Citrix\Federated Authentication Service auf dem FAS-Server.

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

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

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

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

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

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

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

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

FAS liest die Konfigurationsdatei nur beim Start des Dienstes. Wenn Werte geändert werden, muss FAS neu gestartet werden, damit die neuen Einstellungen übernommen werden.

Legen Sie die relevanten Werte in der Datei

Citrix.Authentication.FederatedAuthenticationService.exe.config wie folgt fest:

Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.**ProviderLegacyCsp** (Wechsel zwischen CAPI- und CNG-APIs)

WERT	KOMMENTAR
wahr	CAPI-APIs verwenden
false (Standard)	CNG-APIs verwenden

Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.**ProviderName** (Name des zu verwendenden Anbieters)

WERT	KOMMENTAR
Microsoft Enhanced RSA- und AES-Kryptografieanbieter	Standard-CAPI-Anbieter
Microsoft Software-Schlüsselspeicheranbieter	Standard-CNG-Anbieter
Microsoft Plattform-Schlüsselspeicheranbieter	Standard-TPM-Anbieter. Beachten Sie, dass TPM nicht für Benutzerschlüssel empfohlen wird. Verwenden Sie TPM nur für den Registrierungsstellenschlüssel. Wenn Sie planen, Ihren FAS-Server in einer virtualisierten Umgebung zu betreiben, erkundigen Sie sich bei Ihrem TPM- und Hypervisor-Anbieter, ob die Virtualisierung unterstützt wird.
HSM_Vendor CSP/Schlüsselspeicheranbieter	Wird vom HSM-Anbieter bereitgestellt. Der Wert unterscheidet sich je nach Anbieter. Wenn Sie planen, Ihren FAS-Server in einer virtualisierten Umgebung zu betreiben, erkundigen Sie sich bei Ihrem HSM-Anbieter, ob die Virtualisierung unterstützt wird.

Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.**ProviderType** (Nur im Falle der CAPI-API erforderlich)

WERT	KOMMENTAR
24	Standard. Bezieht sich auf die Eigenschaft Microsoft KeyContainerPermissionAccessEntry.Provider Type PROV_RSA_AES 24. Sollte immer 24 sein, es sei denn, Sie verwenden ein HSM mit CAPI und der HSM-Anbieter gibt etwas anderes an.

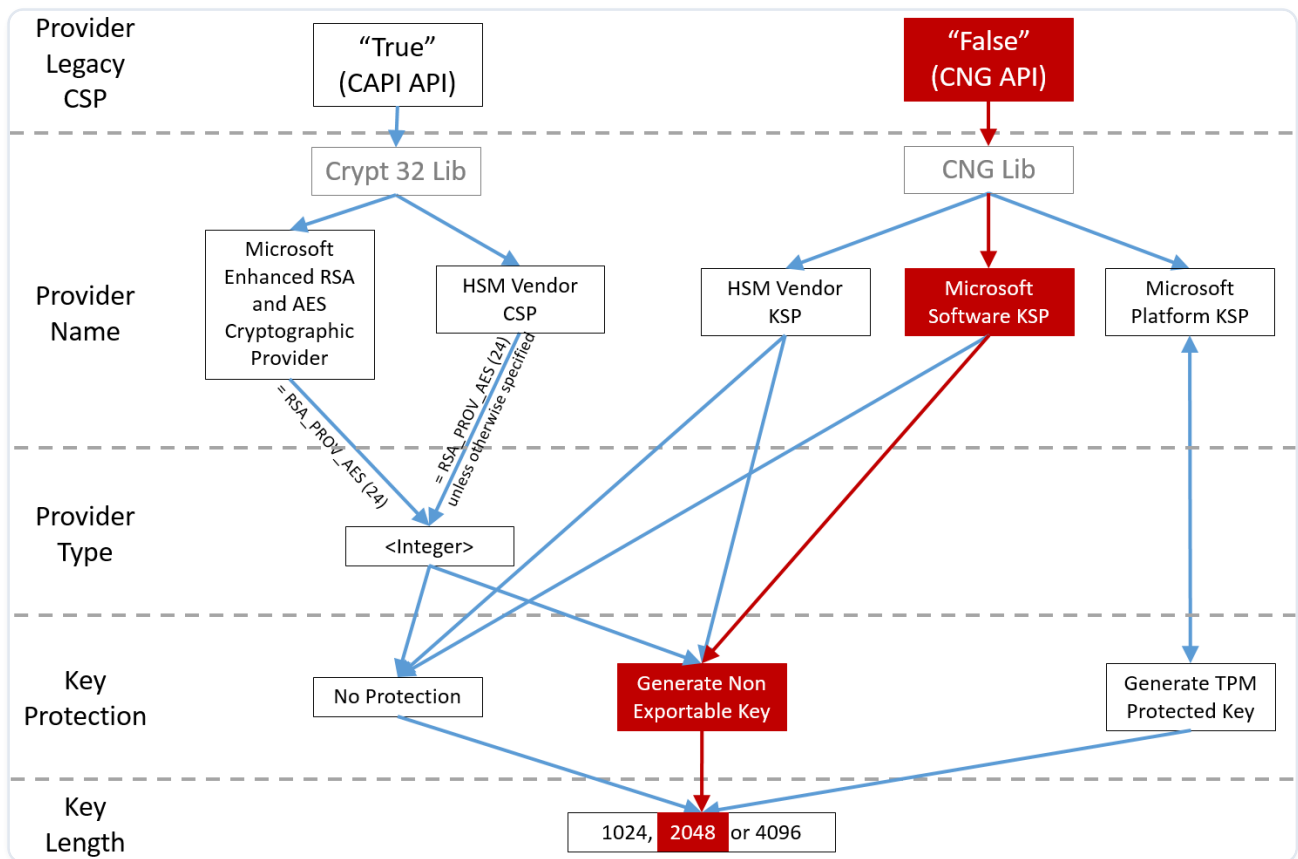
Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.**KeyProtection** (Wenn FAS eine private Schlüsseloperation durchführen muss, verwendet es den hier angegebenen Wert) Steuert das „exportierbare“ Flag privater Schlüssel. Ermöglicht die Verwendung von TPM-Schlüsselspeichern, sofern von der Hardware unterstützt.

WERT	KOMMENTAR
Kein Schutz	Privater Schlüssel kann exportiert werden.
GenerateNonExportableKey	Standard. Privater Schlüssel kann nicht exportiert werden.
GenerateTPMProtectedKey	Der private Schlüssel wird über das TPM verwaltet. Der private Schlüssel wird über den ProviderName gespeichert, den Sie in ProviderName angegeben haben (z. B. Microsoft Platform Key Storage Provider).

Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.**KeyLength** (Geben Sie die Größe des privaten Schlüssels in Bits an)

WERT	KOMMENTAR
2048	Standard. 1024 oder 4096 können ebenfalls verwendet werden.

Die Einstellungen der Konfigurationsdatei werden grafisch wie folgt dargestellt (Installationsstandards sind rot dargestellt):



Beispiele für Konfigurationsszenarien

Beispiel 1

Dieses Beispiel behandelt den privaten Schlüssel des Registrierungsstellenzertifikats und die privaten Schlüssel der Benutzerzertifikate, die mit dem Microsoft Software Key Storage Provider gespeichert werden.

Dies ist die Standardkonfiguration nach der Installation. Es ist keine zusätzliche Konfiguration des privaten Schlüssels erforderlich.

Beispiel 2

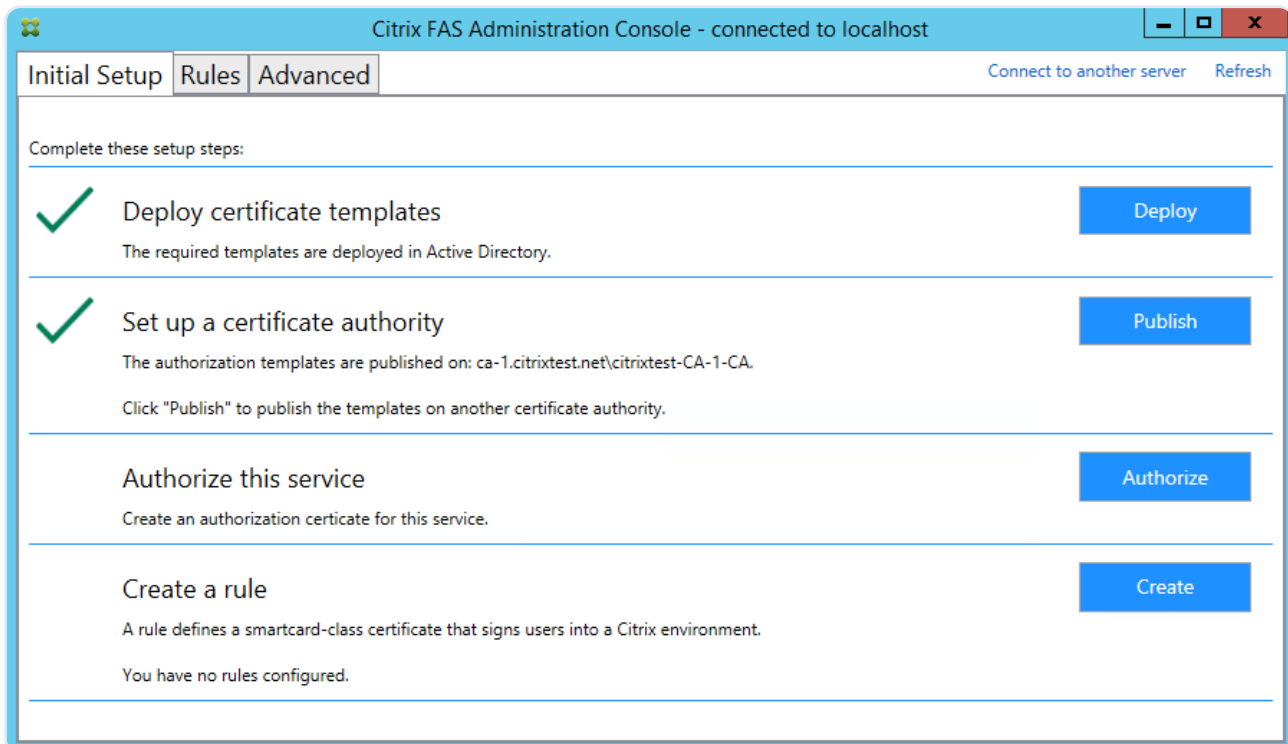
Dieses Beispiel zeigt den privaten Schlüssel des Registrierungsstellenzertifikats, der über den Microsoft Platform Key Storage Provider im Hardware-TPM des FAS-Server-Motherboards gespeichert ist, und die privaten Schlüssel der Benutzerzertifikate, die mit dem Microsoft Software Key Storage Provider gespeichert sind.

Dieses Szenario setzt voraus, dass das TPM auf dem Motherboard Ihres FAS-Servers gemäß der Dokumentation des TPM-Herstellers im BIOS aktiviert und anschließend in Windows initialisiert wurde; siehe [https://docs.microsoft.com/de-de/previous-versions/windows/it-pro/windows-vista/cc749022\(v=ws.10\)>](https://docs.microsoft.com/de-de/previous-versions/windows/it-pro/windows-vista/cc749022(v=ws.10)>).

Verwenden der FAS-Verwaltungskonsole

Die FAS-Verwaltungskonsole kann keine Offline-Zertifikatsignieranforderungen durchführen, daher wird ihre Verwendung nicht empfohlen, es sei denn, Ihre Organisation erlaubt Online-Zertifikatsignieranforderungen für Registrierungsstellenzertifikate.

Führen Sie während der anfänglichen FAS-Konfiguration über die Verwaltungskonsole nur die ersten beiden Schritte **Zertifikatvorlagen bereitstellen** und **Zertifizierungsstelle einrichten** aus und gehen Sie dann wie folgt vor:



Schritt 1: Bearbeiten Sie die Konfigurationsdatei, indem Sie die folgende Zeile wie folgt ändern:

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

Die Datei sollte nun wie folgt aussehen:

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

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

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

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

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

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

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

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

Einige TPMs beschränken die Schlüssellänge. Die Standardschlüssellänge beträgt 2048 Bit. Stellen Sie sicher, dass Sie eine von Ihrer Hardware unterstützte Schlüssellänge angeben.

Schritt 2: Starten Sie den Citrix Federated Authentication Service neu, um die Werte aus der Konfigurationsdatei zu lesen.

Schritt 3: Autorisieren Sie den Dienst.

Schritt 4: Stellen Sie die ausstehende Zertifikatsanforderung manuell vom Zertifizierungsstellenserver aus. Nachdem das Registrierungsstellenzertifikat abgerufen wurde, wird Schritt 3 in der Einrichtungssequenz in der Verwaltungskonsole grün angezeigt. Zu diesem Zeitpunkt wurde der private Schlüssel des Registrierungsstellenzertifikats im TPM generiert. Das Zertifikat ist standardmäßig 2 Jahre gültig.

Um zu bestätigen, dass der private Schlüssel des Registrierungsstellenzertifikats korrekt im TPM gespeichert wird, verwenden Sie die folgenden PowerShell-Befehle. Das Feld PrivateKeyProvider wird auf *Microsoft Platform Crypto Provider* gesetzt, wenn der private Schlüssel des Registrierungsstellenzertifikats im TPM gespeichert ist:

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

Get-FasAuthorizationCertificate -FullCertInfo -Address localhost
```

Schritt 5: Bearbeiten Sie die Konfigurationsdatei wieder wie folgt:

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

HINWEIS:

Obwohl FAS Benutzerzertifikate mit TPM-geschützten Schlüsseln generieren kann, kann die TPM-Hardware für große Bereitstellungen zu langsam sein.

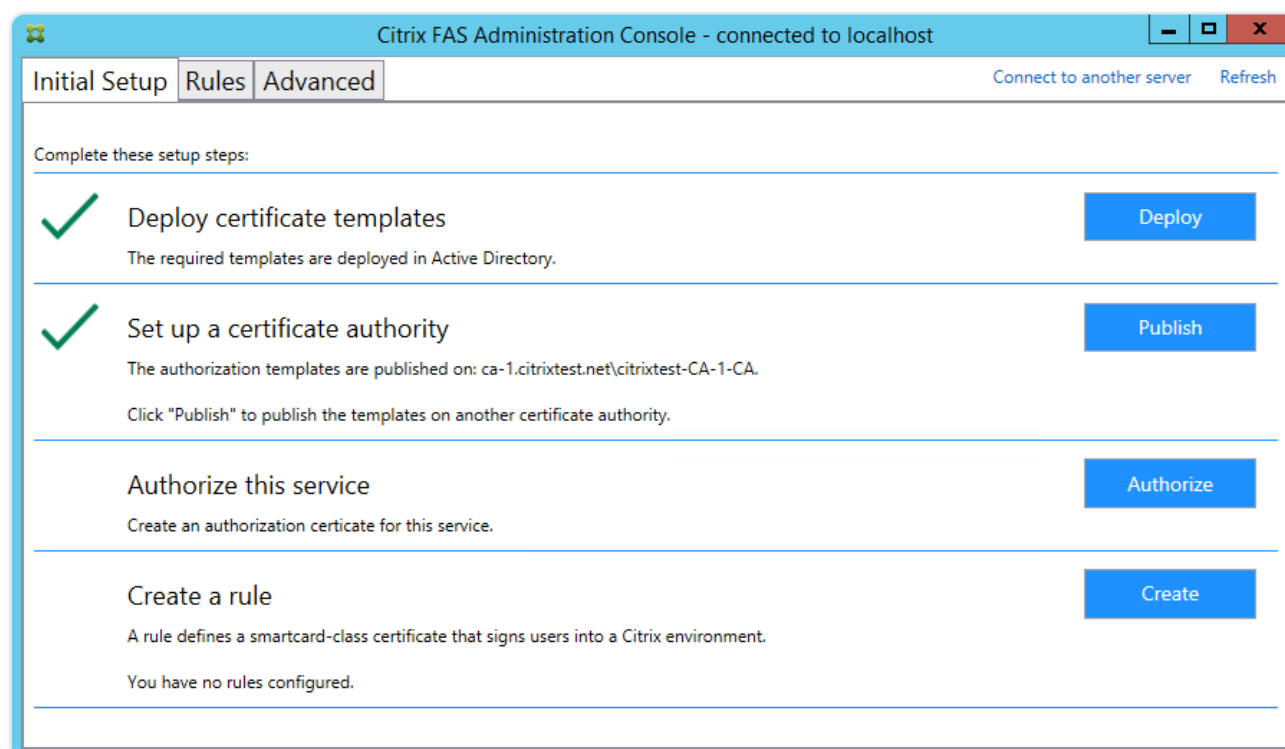
Schritt 6: Starten Sie FAS neu. Dadurch wird der Dienst gezwungen, die Konfigurationsdatei neu einzulesen und die geänderten Werte zu übernehmen. Die nachfolgenden automatischen Operationen mit privaten Schlüsseln wirken sich auf Benutzerzertifikatsschlüssel aus; diese Operationen speichern die privaten Schlüssel nicht im TPM, sondern verwenden den Microsoft Software Key Storage Provider.

Schritt 7: Wählen Sie die Registerkarte **Regeln** in der FAS-Verwaltungskonsolle aus und bearbeiten Sie die Einstellungen wie unter [Installieren und Konfigurieren](#) beschrieben.

Verwenden von PowerShell

Das Registrierungsstellenzertifikat kann offline mit PowerShell angefordert werden. Dies ist für Organisationen geeignet, die nicht möchten, dass ihre Zertifizierungsstelle ein Registrierungsstellenzertifikat über eine Online-Zertifikatsanforderung ausstellt. Sie können keine Offline-Registrierungsstellenzertifikatsanforderung über die FAS-Verwaltungskonsolle stellen.

Schritt 1: Führen Sie während der anfänglichen FAS-Konfiguration über die Verwaltungskonsolle nur die ersten beiden Schritte aus: „Zertifikatvorlagen bereitstellen“ und „Zertifizierungsstelle einrichten“.



Schritt 2: Fügen Sie auf Ihrem Zertifizierungsstellenserver das MMC-Snap-In „Zertifikatvorlagen“ hinzu. Klicken Sie mit der rechten Maustaste auf die Vorlage **Citrix_RegistrationAuthority_ManualAuthorization** und wählen Sie **Vorlage duplizieren**.

Wählen Sie die Registerkarte **Allgemein** aus. Ändern Sie den Namen und die Gültigkeitsdauer. In diesem Beispiel lautet der Name *Offline_RA* und die Gültigkeitsdauer beträgt 2 Jahre:

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

Schritt 3: Fügen Sie auf Ihrem Zertifizierungsstellenserver das MMC-Snap-In der Zertifizierungsstelle hinzu. Klicken Sie mit der rechten Maustaste auf **Zertifikatvorlagen**. Wählen Sie **Neu** und klicken Sie dann auf **Ausstellende Zertifikatvorlage**. Wählen Sie die soeben erstellte Vorlage aus.

Schritt 4: Laden Sie die folgenden PowerShell-Cmdlets auf dem FAS-Server:

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

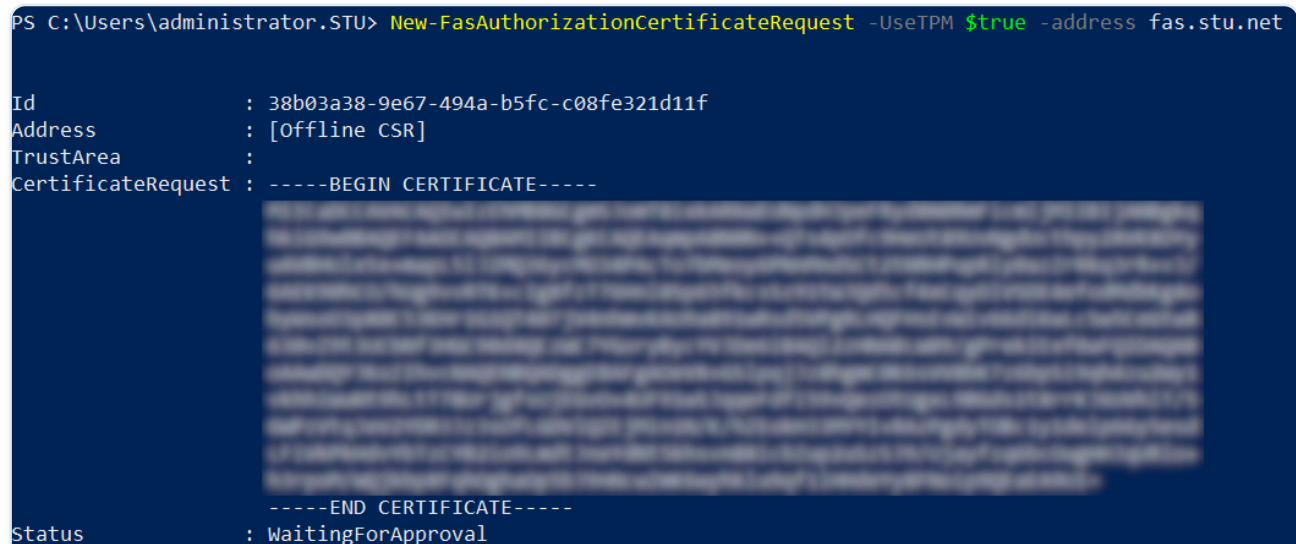
Schritt 5: Generieren Sie das RSA-Schlüsselpaar im TPM des FAS-Servers und erstellen Sie die Zertifikatsignieranforderung, indem Sie das folgende PowerShell-Cmdlet auf dem FAS-Server eingeben. **Hinweis:** Einige TPMs beschränken die Schlüssellänge. Die Standardschlüssellänge beträgt 2048 Bit. Stellen Sie sicher, dass Sie eine von Ihrer Hardware unterstützte Schlüssellänge angeben.

```
New-FasAuthorizationCertificateRequest -UseTPM $true -address \&lt;FQDN of FAS Server>
```

Zum Beispiel:

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

Folgendes wird angezeigt:



```
PS C:\Users\administrator.STU> New-FasAuthorizationCertificateRequest -UseTPM $true -address fas.stu.net

Id                : 38b03a38-9e67-494a-b5fc-c08fe321d11f
Address           : [Offline CSR]
TrustArea         :
CertificateRequest : -----BEGIN CERTIFICATE-----
                  [Blurred Certificate Content]
                  -----END CERTIFICATE-----
Status            : WaitingForApproval
```

HINWEISE:

- Die Id-GUID (in diesem Beispiel „5ac3d8bd-b484-4ebe-abf8-4b2cfd62ca39“) wird in einem späteren Schritt benötigt.
- Betrachten Sie dieses PowerShell-Cmdlet als eine einmalige „Überschreibung“, die zum Generieren des privaten Schlüssels für das Registrierungsstellenzertifikat verwendet wird.
- Beim Ausführen dieses Cmdlets werden die Werte, die beim Starten von FAS aus der Konfigurationsdatei gelesen wurden, überprüft, um die zu verwendende Schlüssellänge zu bestimmen (der Standardwert ist 2048).
- Da -UseTPM in diesem manuellen, PowerShell-initiierten Vorgang für den privaten Schlüssel des Registrierungsstellenzertifikats auf \$true gesetzt ist, ignoriert das System Werte aus der Datei, die nicht den für die Verwendung eines TPM erforderlichen Einstellungen entsprechen.
- Das Ausführen dieses Cmdlets ändert keine Einstellungen in der Konfigurationsdatei.
- Bei nachfolgenden automatischen, von FAS initiierten Vorgängen für den privaten Schlüssel des Benutzerzertifikats werden die Werte verwendet, die beim Starten von FAS aus der Datei gelesen wurden.
- Es ist auch möglich, den Wert KeyProtection in der Konfigurationsdatei auf GenerateTPMProtectedKey zu setzen, wenn der FAS-Server Benutzerzertifikate ausstellt, um private Schlüssel für Benutzerzertifikate zu generieren, die durch das TPM geschützt sind.

Um zu überprüfen, ob das TPM zum Generieren des Schlüsselpaars verwendet wurde, sehen Sie im Anwendungsereignisprotokoll in der Windows-Ereignisanzeige auf dem FAS-Server nach, zum Zeitpunkt der Generierung des Schlüsselpaars.

	Information	22/07/2019 12:59:42	Citrix.Fas.PkiCore	14	None
	Information	22/07/2019 12:59:41	Citrix.Fas.PkiCore	16	None
	Information	22/07/2019 12:59:41	Citrix.Authentication.FederatedAuthenticationService	15	None

Event 15, Citrix.Authentication.FederatedAuthenticationService

General	Details
[S15] Administrator [CITRIXTEST\Administrator] creating certificate request [TPM: True] [correlation: e61a73d7-bb61-44af-8d21-1159d864d82e]	

Hinweis: ""

Gefolgt von:

Application Number of events: 3					
Level	Date and Time	Source	Event ID	Task C...	
Information	22/07/2019 12:59:42	Citrix.Fas.PkiCore	14	None	
Information	22/07/2019 12:59:41	Citrix.Fas.PkiCore	16	None	
Information	22/07/2019 12:59:41	Citrix.Authentication.FederatedAuthenticationService	15	None	

Event 16, Citrix.Fas.PkiCore	
General	Details
[S16] PrivateKey::Create [Identifier afae7c8d-53ff-4cf6-bd96-75fa3e606d3e_TWIN][MachineWide: False][Provider: [CNG] Microsoft Platform Crypto Provider][ProviderType: 0][EllipticCurve: False][KeyLength: 2048][isExportable: False]	

Hinweis: "Anbieter: Microsoft Platform Crypto Provider"

Schritt 6: Kopieren Sie den Abschnitt der Zertifikatanforderung in einen Texteditor und speichern Sie ihn als Textdatei auf der Festplatte.

```

usmcertreq - Notepad
File Edit Format View Help
-----BEGIN CERTIFICATE REQUEST-----
MIICaDCCAVACAQIwIzEhMB8GCgmSjomT8ixkARKWEUNpdHJpeFRydXN0RmFicmljMIIBIjANBgkq
hkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAWAtwoCLXJuJ3yIscT8Y5v/7zuYqBhbHkhZV3wTNfROXW
1hCMwi7X4YpTE7CbJtgiFY/9SEBa9StGeTVpeJi66gKoZCdxyc2BwX6JNZrLi9hAf1bInFPgrz+
vbG3YjKuKtK35JpGqYWjUEDzKiQFaob3Dkh/pwP3V70cEYthxB8CfbaN9MHOEFbepoSYOCAfunXW
snwIbXD91c/fGyN/3f94P4fbNrjEI0Hc+40y/WsPgPRgcq9XBwRjzpGjOgOWRoJS9g220Y5PwD77
7f7vZvoQkRy5NXXXATJ+xxYEPLp9JuJaElWXrTJG+XP3SnG/oCCPit7iUIIc9FjGa3qTUQIDAQAB
oAAwDQYJKoZIhvcNAQENBQADggEBAIJV8jR9XWHlvtztpjxPeJzAV0srLp0sCfMdvYn9u+I7J8Gsr
4tuLjuQ+An4Y2Rw7b6pZxEICV8rqd5Gy+wtPnUzoAf6eLg1Vht2RVfb6d7Ns6+Mc+F5bFegLHs8c
Y1ITN0tmCHFKt4Loz505E+tQw39MPProEj3p7GwF7HrGY+QSbFD38rbL19Z5cfNYYqMbsgyMgdR8F
3SmagQjN3C8lyqT8z1iF4132xlmQrP/4XQvr1F+T015PM5Fxxj6PEKWopWTYZXGzSC1ufxevc01K
+tTH9tQYJM6xw3+6TicfuW0jrd8KJjTdC5SMu7LJuIajTNZ5Z+1eM61TAT03XG/AB7o=
-----END CERTIFICATE REQUEST-----

```

Schritt 7: Übermitteln Sie die Zertifikatsignieranforderung an Ihre Zertifizierungsstelle, indem Sie Folgendes in PowerShell auf dem FAS-Server eingeben:

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

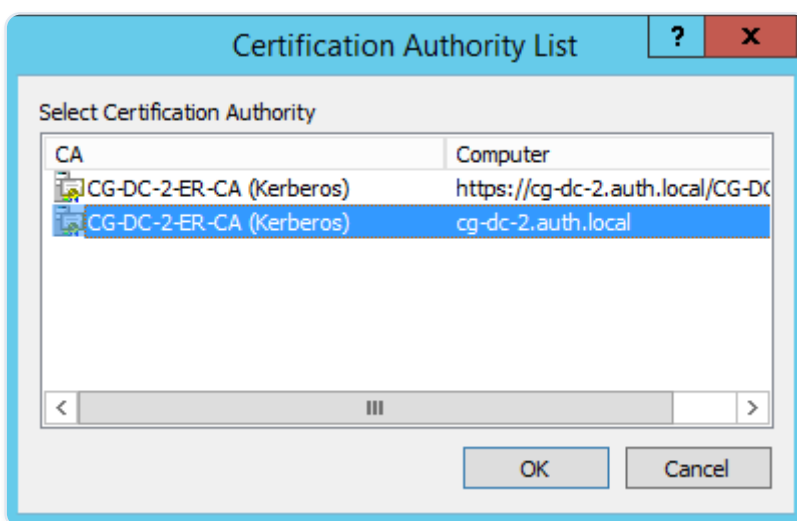
Zum Beispiel:

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

Folgendes wird angezeigt:

```
PS C:\Users\Administrator.AUTH> certreq -submit -attrib "certificatetemplate:Offline_RA" C:\Users\Administrator.AUTH\Desktop\usmcertreq.txt
Active Directory Enrollment Policy
{4F76160E-0B0C-4D21-A4FD-2E29502177C2}
ldap:
```

An dieser Stelle wird möglicherweise ein Fenster mit der Liste der Zertifizierungsstellen angezeigt. Die Zertifizierungsstelle in diesem Beispiel hat sowohl die HTTP- (oben) als auch die DCOM-Registrierung (unten) aktiviert. Wählen Sie die DCOM-Option aus, falls verfügbar:

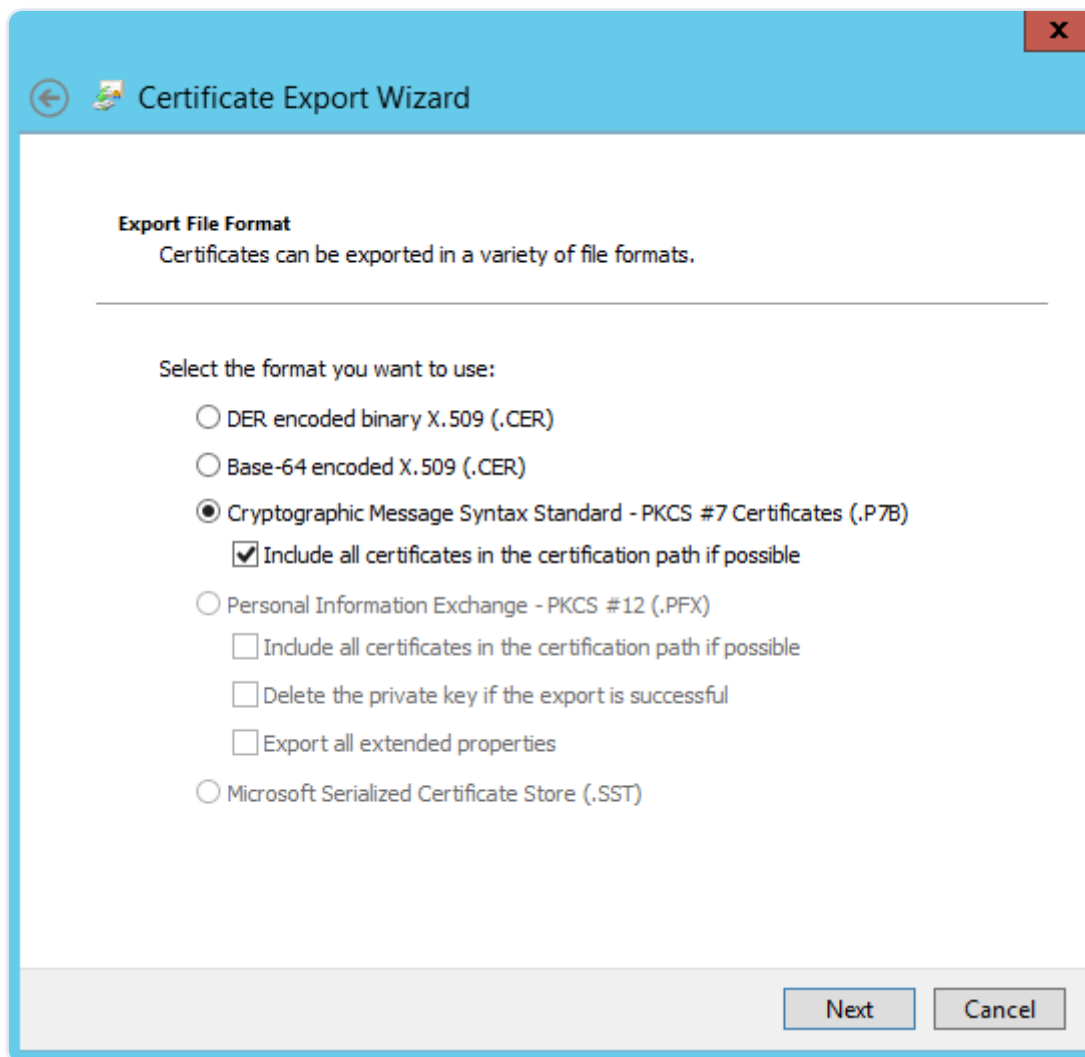


Nachdem die Zertifizierungsstelle angegeben wurde, zeigt PowerShell die RequestID an:

```
PS C:\Users\Administrator.AUTH> certreq -submit -attrib "certificatetemplate:Offline_RA" C:\Users\Administrator.AUTH\Desktop\usmcertreq.txt
Active Directory Enrollment Policy
{4F76160E-0B0C-4D21-A4FD-2E29502177C2}
ldap:
RequestID: 106
RequestID: "106"
Certificate request is pending: Taken Under Submission (0)
PS C:\Users\Administrator.AUTH>
```

Schritt 8: Klicken Sie auf dem Zertifizierungsstellenserver im MMC-Snap-In der Zertifizierungsstelle auf **Ausstehende Anforderungen**. Notieren Sie die Anforderungs-ID. Klicken Sie dann mit der rechten Maustaste auf die Anforderung und wählen Sie **Ausstellen**.

Schritt 9: Wählen Sie den Knoten **Ausgestellte Zertifikate** aus. Suchen Sie das soeben ausgestellte Zertifikat (die Anforderungs-ID sollte übereinstimmen). Doppelklicken Sie, um das Zertifikat zu öffnen. Wählen Sie die Registerkarte **Details** aus. Klicken Sie auf **In Datei kopieren**. Der Zertifikatexport-Assistent wird gestartet. Klicken Sie auf **Weiter**. Wählen Sie die folgenden Optionen für das Dateiformat aus:



Das Format muss „**Kryptografischer Nachrichtensyntaxstandard – PKCS #7-Zertifikate (.P7B)**“ sein, und „**Alle Zertifikate im Zertifizierungspfad einschließen, wenn möglich**“ muss ausgewählt sein.

Schritt 10: Kopieren Sie die exportierte Zertifikatsdatei auf den FAS-Server.

Schritt 11: Importieren Sie das Registrierungsstellenzertifikat in den FAS-Server, indem Sie das folgende PowerShell-Cmdlet auf dem FAS-Server eingeben:

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

Zum Beispiel:

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

Folgendes wird angezeigt:

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

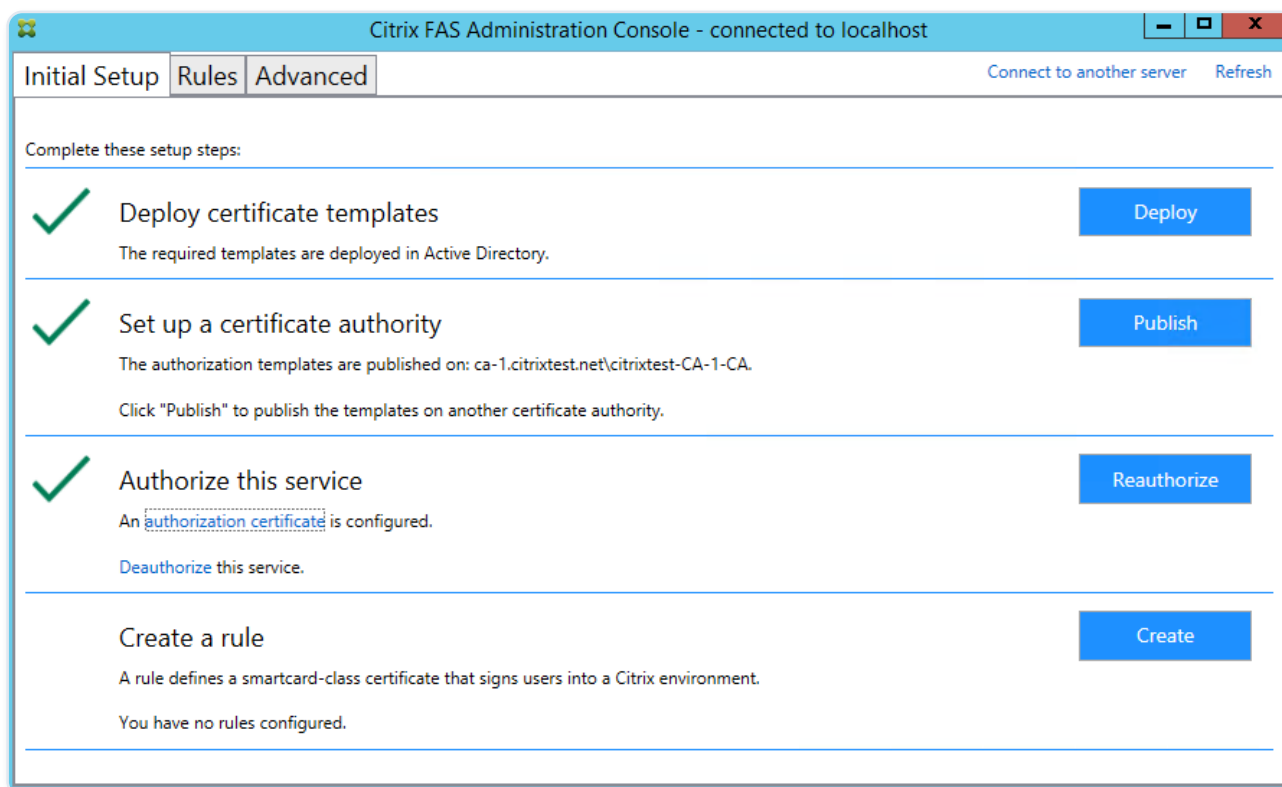
Id                : 74d427ff-c55b-4d6d-87ae-1ff98b0c2705
Address           : [Offline CSR]
TrustArea         : 978816cd-8b2f-4695-8c5d-08bb7df1816b
CertificateRequest :
Status            : Ok
```

Um zu bestätigen, dass der private Schlüssel des Registrierungsstellenzertifikats korrekt im TPM gespeichert wird, verwenden Sie die folgenden PowerShell-Befehle. Das Feld PrivateKeyProvider wird auf *Microsoft Platform Crypto Provider* gesetzt, wenn der private Schlüssel des Registrierungsstellenzertifikats im TPM gespeichert ist:

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

Get-FasAuthorizationCertificate -FullCertInfo -Address localhost
```

Schritt 12: Schließen Sie die FAS-Verwaltungskonsolle und starten Sie sie dann neu.



Hinweis: Der Schritt „Diesen Dienst autorisieren“ hat ein grünes Häkchen.

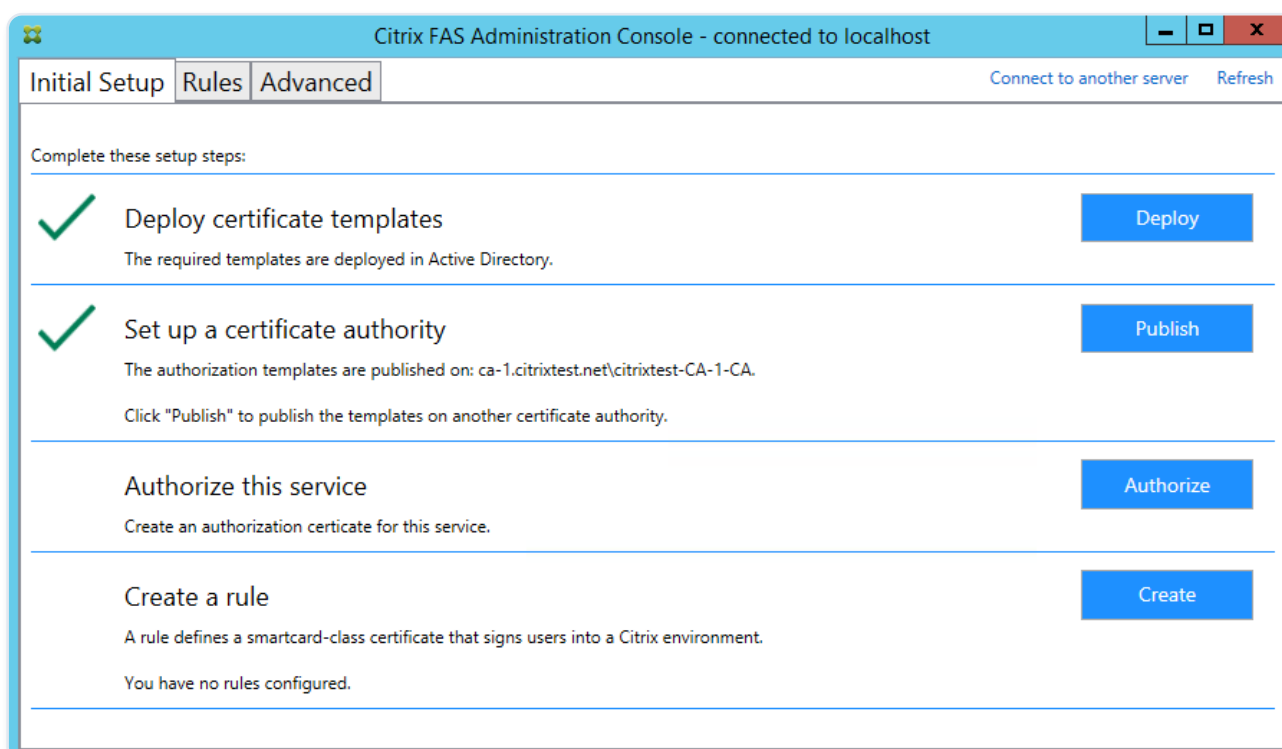
Schritt 13: Wählen Sie die Registerkarte **Regeln** in der FAS-Verwaltungskonsolle und bearbeiten Sie die Einstellungen, die unter **Installieren und Konfigurieren** beschrieben sind.

Beispiel 3

Dieses Beispiel behandelt einen privaten Schlüssel für ein Registrierungsstellen-Zertifikat und private Schlüssel für Benutzerzertifikate, die in einem HSM gespeichert sind. Dieses Beispiel setzt ein konfiguriertes HSM voraus. Ihr HSM hat einen Anbieternamen, zum Beispiel „HSM_Vendor's Key Storage Provider“.

Wenn Sie planen, Ihren FAS-Server in einer virtualisierten Umgebung zu betreiben, erkundigen Sie sich bei Ihrem HSM-Anbieter nach der Hypervisor-Unterstützung.

Schritt 1. Führen Sie während der Ersteinrichtung von FAS über die Verwaltungskonsole nur die ersten beiden Schritte aus: „Zertifikatvorlagen bereitstellen“ und „Zertifizierungsstelle einrichten“.



Schritt 2: Konsultieren Sie die Dokumentation Ihres HSM-Anbieters, um den Wert für ProviderName Ihres HSM zu ermitteln. Wenn Ihr HSM CAPI verwendet, wird der Anbieter in der Dokumentation möglicherweise als Cryptographic Service Provider (CSP) bezeichnet. Wenn Ihr HSM CNG verwendet, wird der Anbieter möglicherweise als Key Storage Provider (KSP) bezeichnet.

Schritt 3: Bearbeiten Sie die Konfigurationsdatei wie folgt:

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

Die Datei sollte nun wie folgt aussehen:

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

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

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

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

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

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

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

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

Dieses Szenario geht davon aus, dass Ihr HSM CNG verwendet, daher ist der Wert `ProviderLegacyCsp` auf „false“ gesetzt. Wenn Ihr HSM CAPI verwendet, sollte der Wert `ProviderLegacyCsp` auf „true“ gesetzt werden. Konsultieren Sie die Dokumentation Ihres HSM-Anbieters, um festzustellen, ob Ihr HSM CAPI oder CNG verwendet. Konsultieren Sie auch die Dokumentation Ihres HSM-Anbieters zu unterstützten Schlüssellängen für die asymmetrische RSA-Schlüsselgenerierung. In diesem Beispiel ist die Schlüssellänge auf den Standardwert von 2048 Bit eingestellt. Stellen Sie sicher, dass die von Ihnen angegebene Schlüssellänge von Ihrer Hardware unterstützt wird.

Schritt 4: Starten Sie den Citrix Federated Authentication Service neu, um die Werte aus der Konfigurationsdatei zu lesen.

Schritt 5: Generieren Sie das RSA-Schlüsselpaar im HSM und erstellen Sie die Zertifikatsignieranforderung, indem Sie in der Registerkarte **Ersteinrichtung** der FAS-Verwaltungskonsole auf **Autorisieren** klicken.

Schritt 6: Um zu überprüfen, ob das Schlüsselpaar im HSM generiert wurde, überprüfen Sie die Anwendungseinträge im Windows-Ereignisprotokoll:

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

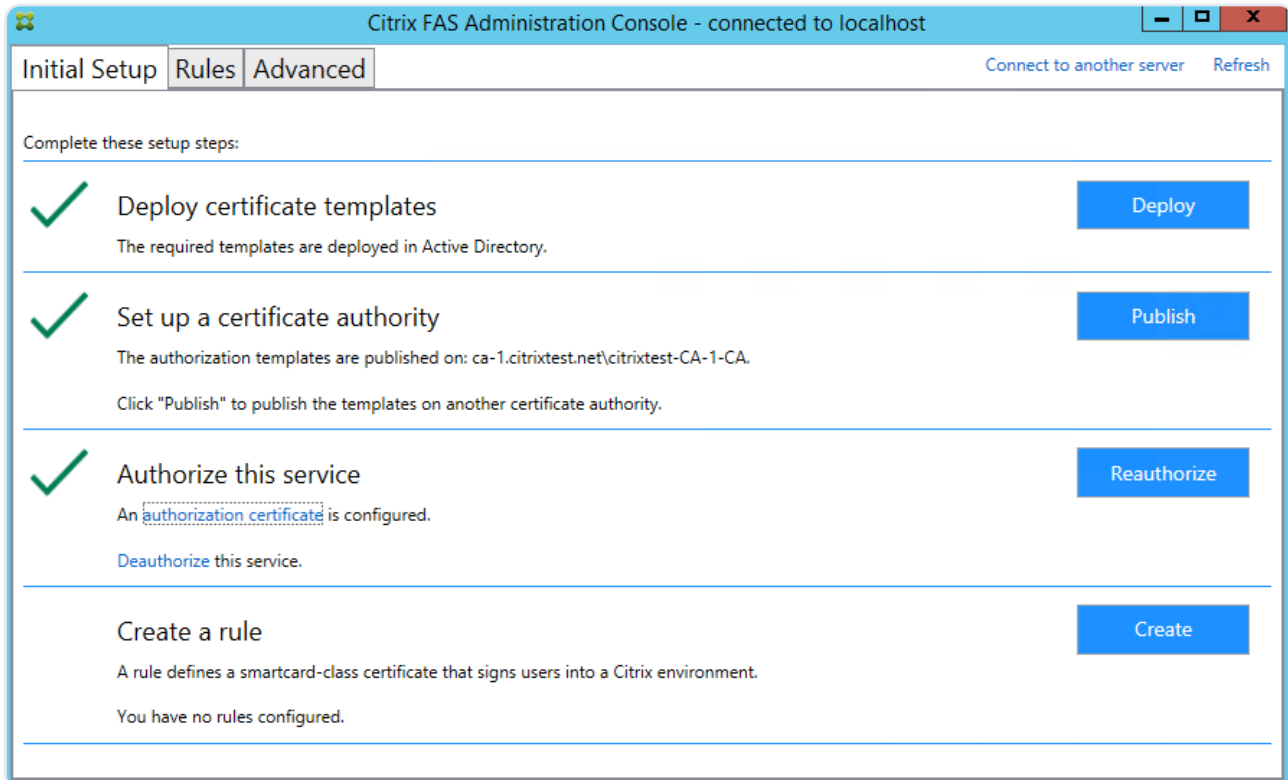
Hinweis: [Anbieter: Schlüsselspeicheranbieter des HSM-Anbieters]

Schritt 7: Wählen Sie auf dem Zertifizierungsstellenserver in der MMC der Zertifizierungsstelle den Knoten **Ausstehende Anforderungen** aus:

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

Klicken Sie mit der rechten Maustaste auf die Anforderung und wählen Sie **Ausstellen**.

Hinweis: Der Schritt „Diesen Dienst autorisieren“ ist mit einem grünen Häkchen versehen.



Schritt 8: Wählen Sie in der FAS-Verwaltungskonsolle die Registerkarte **Regeln** und bearbeiten Sie die Einstellungen wie beschrieben unter [Installieren und konfigurieren](#).

FAS-Zertifikatspeicher

FAS verwendet nicht den Microsoft-Zertifikatspeicher auf dem FAS-Server, um seine Zertifikate zu speichern. Es verwendet eine eingebettete Datenbank.

Um die GUID für das Registrierungsstellenzertifikat zu ermitteln, geben Sie die folgenden PowerShell-Cmdlets auf dem FAS-Server ein:

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

Get-FasAuthorizationCertificate -address \&lt;FAS server FQDN>
```

Beispiel: **Get-FasAuthorizationCertificate -address cg-fas-2.auth.net:**

[illegible]

Um eine Liste der Benutzerzertifikate zu erhalten, geben Sie ein:

```
Get-FasUserCertificate -address &lt;FAS server FQDN>
```

Beispiel: **Get-FasUserCertificate -address cg-fas-2.auth.net**

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

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

HINWEIS:

Bei Verwendung eines HSM zum Speichern privater Schlüssel werden HSM-Container mit einer GUID identifiziert. Die GUID für den privaten Schlüssel im HSM kann mit folgendem Befehl abgerufen werden:

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

Beispiel:

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

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

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

Zugehörige Informationen

- [Installieren und Konfigurieren](#) ist die primäre Referenz für die FAS-Installation und -Konfiguration.
- Die gängigen FAS-Bereitstellungen werden im Artikel [Übersicht über die Architekturen der Federated Authentication Services](#) zusammengefasst.
- Weitere Anleitungsartikel werden im Artikel [Erweiterte Konfiguration](#) vorgestellt.

Sicherheit und Netzwerkkonfiguration

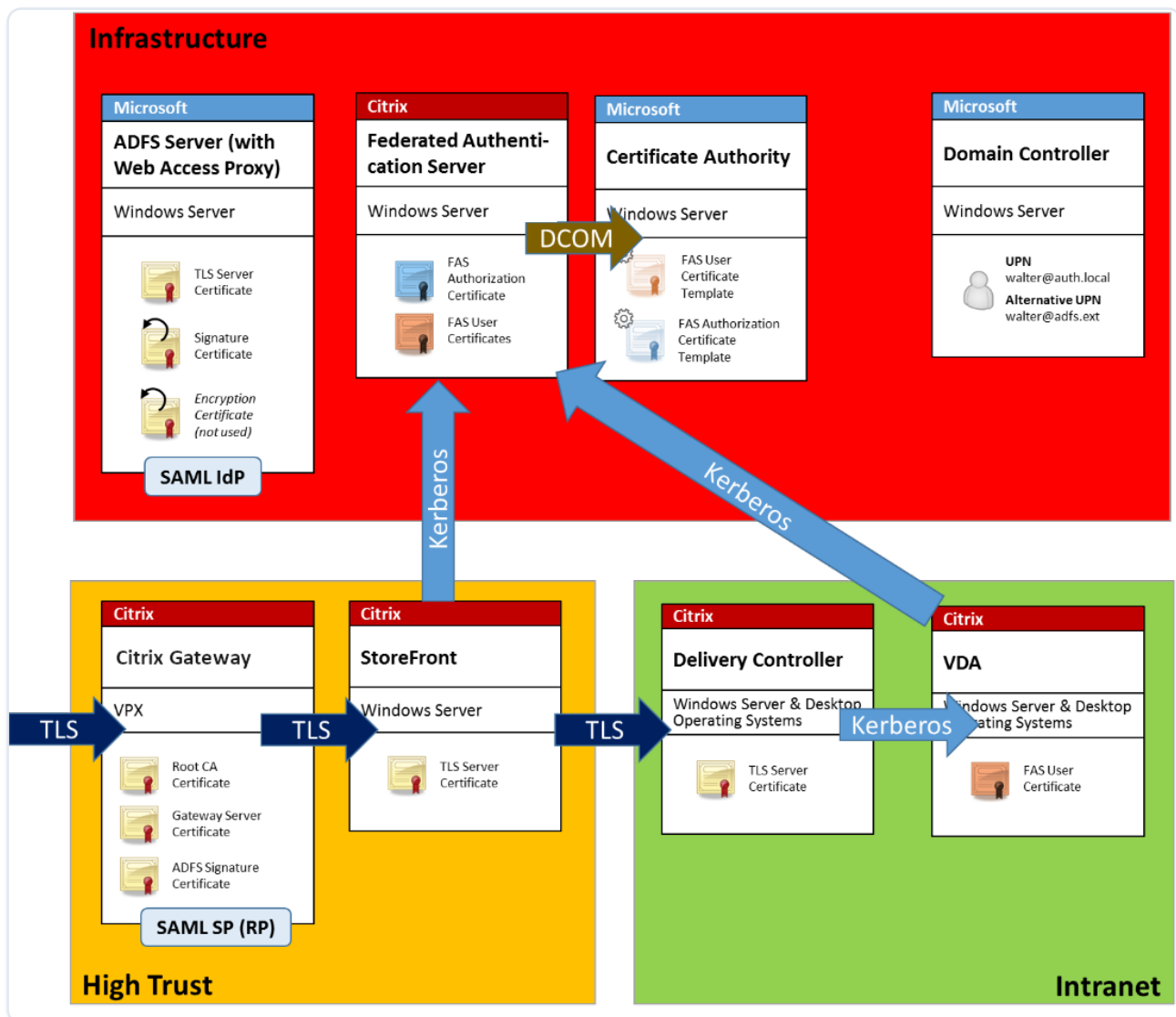
Der Federated Authentication Service (FAS) ist eng in Microsoft Active Directory und die Microsoft-Zertifizierungsstelle integriert. Es ist unerlässlich, dass das System angemessen verwaltet und gesichert wird, indem eine Sicherheitsrichtlinie entwickelt wird, wie Sie es für einen Domänencontroller oder eine andere kritische Infrastruktur tun würden.

Dieses Dokument bietet einen Überblick über Sicherheitsaspekte, die bei der Bereitstellung von FAS zu berücksichtigen sind. Es bietet auch einen Überblick über verfügbare Funktionen, die zur Sicherung Ihrer Infrastruktur beitragen können.

Netzwerkarchitektur

Das folgende Diagramm zeigt die Hauptkomponenten und Sicherheitsgrenzen, die in einer FAS-Bereitstellung verwendet werden.

Der FAS-Server sollte als Teil der sicherheitskritischen Infrastruktur behandelt werden, zusammen mit der Zertifizierungsstelle und dem Domänencontroller. In einer föderierten Umgebung sind Citrix Gateway und Citrix Storefront Komponenten, denen die Durchführung der Benutzerauthentifizierung anvertraut wird; andere Citrix Virtual Apps and Desktops™-Komponenten sind von der Einführung von FAS unberührt.



Firewall und Netzwerksicherheit

Die Kommunikation zwischen Citrix Gateway, StoreFront und den Delivery Controller™-Komponenten sollte durch TLS über Port 443 geschützt werden. Der StoreFront-Server stellt nur ausgehende Verbindungen her, und das Citrix Gateway sollte nur Verbindungen über das Internet über HTTPS-Port 443 akzeptieren.

Der StoreFront-Server kontaktiert den FAS-Server über Port 80 unter Verwendung von gegenseitig authentifiziertem Kerberos. Die Authentifizierung verwendet die Kerberos HOST/fqdn-Identität des FAS-Servers und die Kerberos-Maschinenkonto-Identität des StoreFront-Servers. Dies erzeugt ein einmalig verwendbares „Anmeldeinformations-Handle“, das vom Citrix Virtual Delivery Agent (VDA) benötigt wird, um den Benutzer anzumelden.

Wenn eine HDX-Sitzung mit dem VDA verbunden ist, kontaktiert der VDA den FAS-Server ebenfalls über Port 80. Die Authentifizierung verwendet die Kerberos HOST/fqdn-Identität des FAS-Servers und die Kerberos-Maschinenidentität des VDA. Zusätzlich muss der VDA das

„Anmeldeinformations-Handle“ bereitstellen, um auf das Zertifikat und den privaten Schlüssel zuzugreifen.

Die Microsoft-Zertifizierungsstelle akzeptiert die Kommunikation über Kerberos-authentifiziertes DCOM, das für die Verwendung eines festen TCP-Ports konfiguriert werden kann. Die Zertifizierungsstelle verlangt zusätzlich, dass der FAS-Server ein CMC-Paket bereitstellt, das von einem vertrauenswürdigen Registrierungsagenten-Zertifikat signiert ist.

SERVER	FIREWALL-PORTS
Federated Authentication Service	[in] Kerberos über HTTP von StoreFront™ und VDAs, [out] DCOM zur Microsoft-Zertifizierungsstelle
Citrix Gateway	[in] HTTPS von Clientcomputern, [in/out] HTTPS zum/vom StoreFront-Server, [out] HDX zum VDA
StoreFront	[in] HTTPS von Citrix Gateway, [out] HTTPS zum Delivery Controller, [out] Kerberos HTTP zu FAS
Delivery Controller	[in] HTTPS vom StoreFront-Server, [in/out] Kerberos über HTTP von VDAs
VDA	[in/out] Kerberos über HTTP vom Delivery Controller, [in] HDX von Citrix Gateway, [out] Kerberos HTTP zu FAS
Microsoft-Zertifizierungsstelle	[in] DCOM & signiert von FAS

Verbindungen zwischen Citrix Federated Authentication Service und Citrix Cloud™

Die Konsole und FAS greifen unter Verwendung des Benutzerkontos bzw. des Netzwerkkontos auf die folgenden Adressen zu.

- FAS-Verwaltungskonsole, unter dem Benutzerkonto
 - *.cloud.com
 - *.citrixworkspacesapi.net

- Adressen, die von einem Drittanbieter-Identitätsanbieter benötigt werden, falls dieser in Ihrer Umgebung verwendet wird
- FAS-Dienst, unter dem Netzwerkkontodienst: `*.citrixworkspacesapi.net`

Wenn Ihre Umgebung Proxyserver umfasst, konfigurieren Sie den Benutzerproxy mit den Adressen für die FAS-Verwaltungskonsole. Stellen Sie außerdem sicher, dass die Adresse für das Netzwerkkontodienst mithilfe von netsh oder einem ähnlichen Tool konfiguriert ist.

Verwaltungsaufgaben

Die Verwaltung der Umgebung kann in die folgenden Gruppen unterteilt werden:

NAME	VERANTWORTLICHKEIT
Unternehmensadministrator	Zertifikatvorlagen im Forest installieren und sichern
Domänenadministrator	Gruppenrichtlinieneinstellungen konfigurieren
Zertifizierungsstellenadministrator	Zertifizierungsstelle konfigurieren
FAS-Administrator	FAS-Server installieren und konfigurieren
StoreFront-/Citrix Gateway-Administrator	Benutzerauthentifizierung konfigurieren
Citrix Virtual Desktops™-Administrator	VDAs und Controller konfigurieren

Jeder Administrator steuert verschiedene Aspekte des gesamten Sicherheitsmodells, was einen mehrschichtigen Ansatz zur Systemsicherung ermöglicht.

Gruppenrichtlinieneinstellungen

Vertrauenswürdige FAS-Maschinen werden durch eine über Gruppenrichtlinien konfigurierte Nachschlagetabelle von „Indexnummer -> FQDN“ identifiziert. Beim Kontaktieren eines FAS-Servers überprüfen Clients die `HOST\<fqdn>` Kerberos-Identität des FAS-Servers. Alle Server, die auf den FAS-Server zugreifen, müssen identische FQDN-Konfigurationen für denselben Index aufweisen; andernfalls können StoreFront und VDAs unterschiedliche FAS-Server kontaktieren.

Um Fehlkonfigurationen zu vermeiden, empfiehlt Citrix, dass eine einzige Richtlinie auf alle Maschinen in der Umgebung angewendet wird. Seien Sie vorsichtig, wenn Sie die Liste der FAS-Server ändern, insbesondere beim Entfernen oder Neuordnen von Einträgen.

Die Kontrolle über dieses GPO sollte auf FAS-Administratoren (und/oder Domänenadministratoren) beschränkt sein, die FAS-Server installieren und außer Betrieb nehmen. Achten Sie darauf, einen Maschinen-FQDN-Namen nicht kurz nach der Außerbetriebnahme eines FAS-Servers wiederzuverwenden.

Zertifikatvorlagen

Wenn Sie die mit FAS gelieferte Zertifikatvorlage Citrix_SmartcardLogon nicht verwenden möchten, können Sie eine Kopie davon ändern. Die folgenden Änderungen werden unterstützt.

Zertifikatvorlage umbenennen

Wenn Sie die Citrix_SmartcardLogon umbenennen möchten, um sie an Ihren organisationsinternen Vorlagen-Benennungsstandard anzupassen, müssen Sie:

- Erstellen Sie eine Kopie der Zertifikatvorlage und benennen Sie sie um, um sie an Ihren organisationsinternen Vorlagen-Benennungsstandard anzupassen.
- Verwenden Sie FAS PowerShell-Befehle zur Verwaltung von FAS anstelle der administrativen Benutzeroberfläche. (Die administrative Benutzeroberfläche ist nur für die Verwendung mit den Citrix-Standardvorlagennamen vorgesehen.)
 - Verwenden Sie entweder das Microsoft MMC-Snap-In für Zertifikatvorlagen oder den Befehl Publish-FasMsTemplate, um Ihre Vorlage zu veröffentlichen, und
 - Verwenden Sie den Befehl New-FasCertificateDefinition, um FAS mit dem Namen Ihrer Vorlage zu konfigurieren.

Allgemeine Eigenschaften ändern

Sie können den Gültigkeitszeitraum in der Zertifikatvorlage ändern.

Ändern Sie nicht den Verlängerungszeitraum. FAS ignoriert diese Einstellung in der Zertifikatvorlage. FAS verlängert das Zertifikat automatisch nach der Hälfte seiner Gültigkeitsdauer.

Eigenschaften der Anforderungsbehandlung ändern

Ändern Sie diese Eigenschaften nicht. FAS ignoriert diese Einstellungen in der Zertifikatvorlage. FAS deaktiviert immer **Export des privaten Schlüssels zulassen** und deaktiviert **Mit demselben Schlüssel erneuern**.

Kryptografieeigenschaften ändern

Ändern Sie diese Eigenschaften nicht. FAS ignoriert diese Einstellungen in der Zertifikatvorlage.

Siehe [Schutz des privaten Schlüssels](#) für äquivalente Einstellungen, die FAS bereitstellt.

Eigenschaften der Schlüsselbestätigung ändern

Ändern Sie diese Eigenschaften nicht. FAS unterstützt keine Schlüsselbestätigung.

Eigenschaften für abgelöste Vorlagen ändern

Ändern Sie diese Eigenschaften nicht. FAS unterstützt keine abgelösten Vorlagen.

Erweiterungseigenschaften ändern

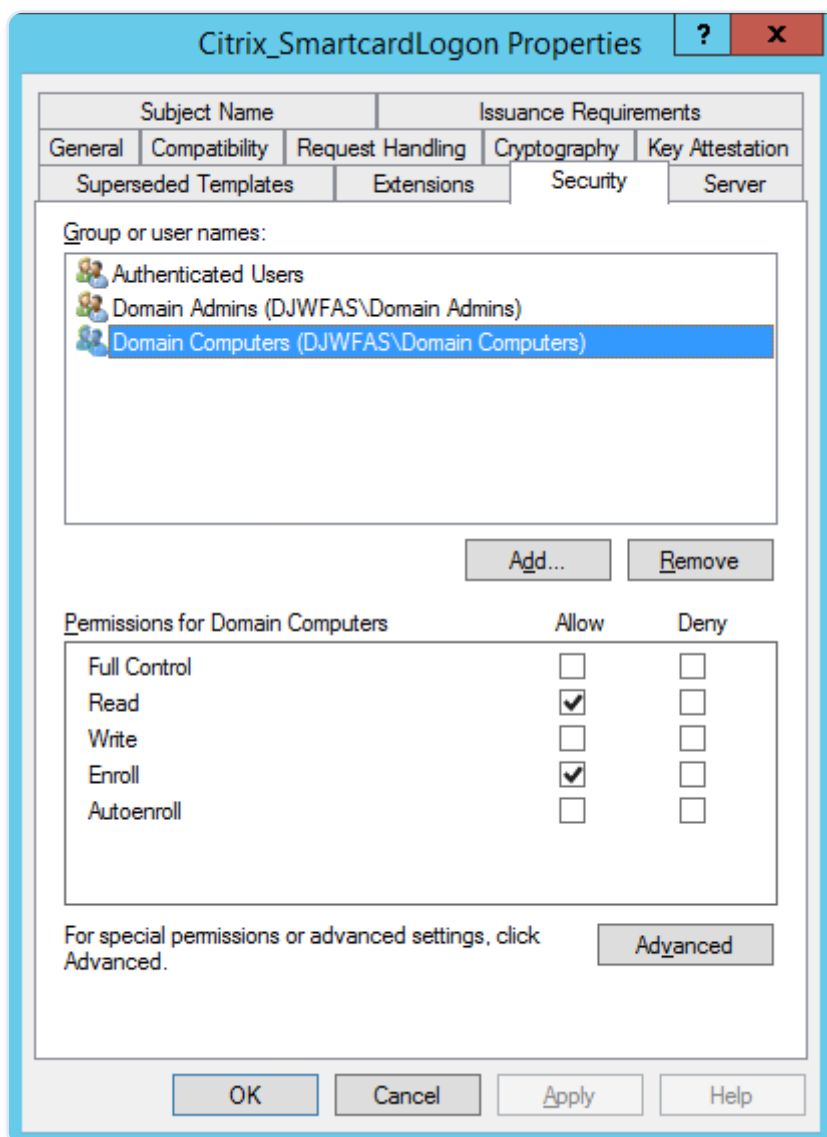
Sie können diese Einstellungen entsprechend Ihrer Unternehmensrichtlinie ändern.

Hinweis: Ungeeignete Erweiterungseinstellungen können Sicherheitsprobleme verursachen oder zu unbrauchbaren Zertifikaten führen.

Sicherheitseigenschaften ändern

Citrix empfiehlt, dass Sie diese Einstellungen ändern, um die Berechtigungen **Lesen** und **Registrieren** nur für die Computerkonten der FAS-Server zuzulassen. Der FAS-Dienst benötigt keine weiteren Berechtigungen. Wie bei anderen Zertifikatvorlagen möchten Sie jedoch möglicherweise:

- Administratoren das Lesen oder Schreiben der Vorlage erlauben
- authentifizierten Benutzern das Lesen der Vorlage erlauben



Eigenschaften des Betreffnamens ändern

Citrix empfiehlt, diese Eigenschaften nicht zu ändern.

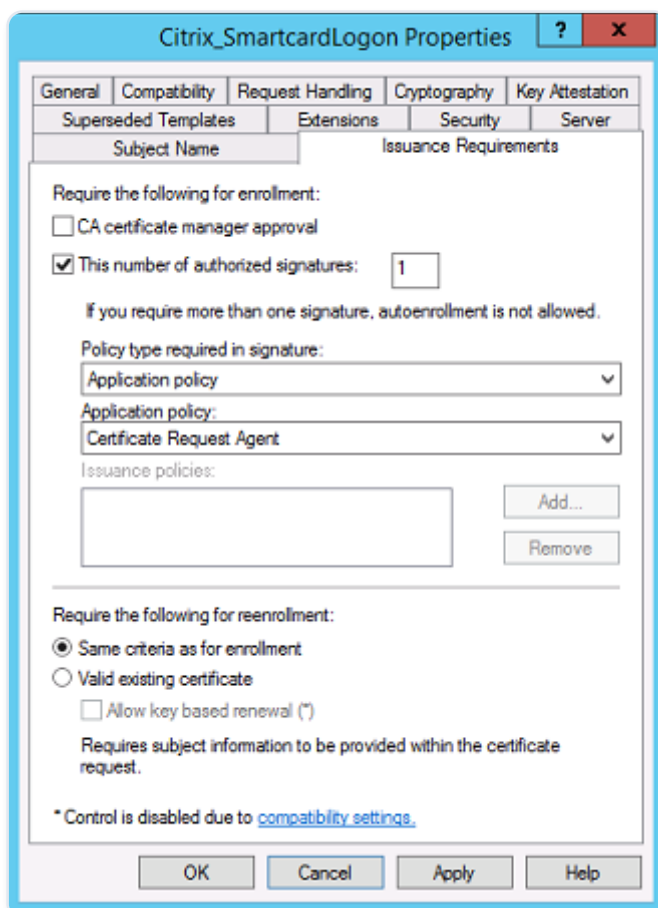
Die Vorlage hat *Aus diesen Active Directory-Informationen erstellen* ausgewählt, wodurch die Zertifizierungsstelle die SID des Benutzers in eine Zertifikatserweiterung einschließt. Dies bietet eine starke Zuordnung zum Active Directory-Konto des Benutzers.

Servereigenschaften ändern

Obwohl Citrix dies nicht empfiehlt, können Sie diese Einstellungen bei Bedarf entsprechend Ihrer Unternehmensrichtlinie ändern.

Eigenschaften der Ausstellungsanforderungen ändern

Ändern Sie diese Einstellungen nicht. Diese Einstellungen sollten wie folgt aussehen:



Kompatibilitätseigenschaften ändern

Sie können diese Einstellungen ändern. Die Einstellung muss mindestens **Windows Server 2003-Zertifizierungsstellen** (Schemaversion 2) sein. FAS unterstützt jedoch nur Windows Server 2008 und spätere Zertifizierungsstellen. Wie oben erläutert, ignoriert FAS auch die zusätzlichen Einstellungen, die durch Auswahl von **Windows Server 2008-Zertifizierungsstellen** (Schemaversion 3) oder **Windows Server 2012-Zertifizierungsstellen** (Schemaversion 4) verfügbar sind.

Verwaltung der Zertifizierungsstelle

Der Administrator der Zertifizierungsstelle ist verantwortlich für die Konfiguration des Zertifizierungsstellenservers und den privaten Schlüssel des ausstellenden Zertifikats, den dieser verwendet.

Veröffentlichen von Vorlagen

Damit eine Zertifizierungsstelle Zertifikate basierend auf einer vom Unternehmensadministrator bereitgestellten Vorlage ausstellen kann, muss der Administrator der Zertifizierungsstelle diese Vorlage veröffentlichen.

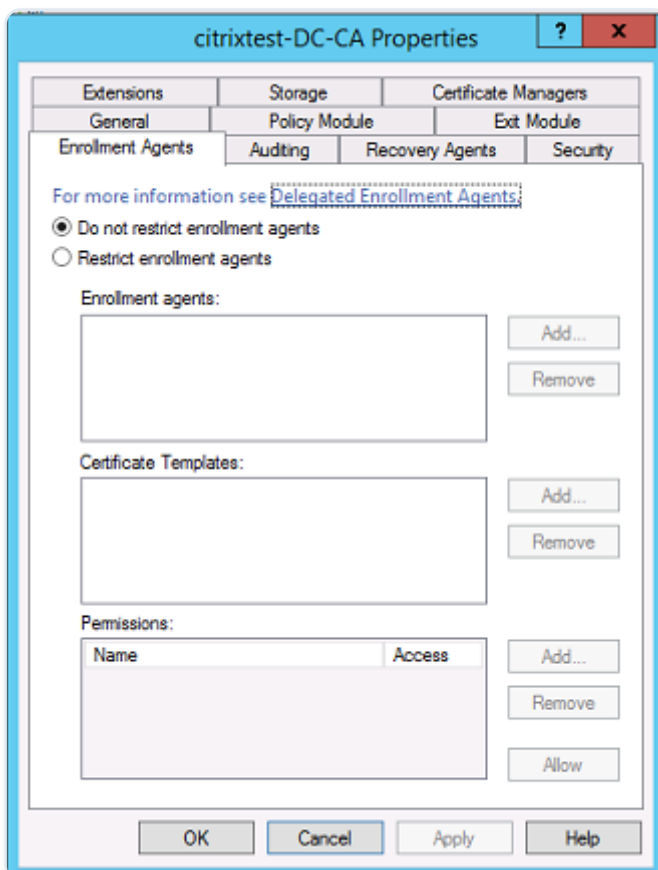
Eine einfache Sicherheitspraxis besteht darin, nur die Zertifikatvorlagen der Registrierungsstelle zu veröffentlichen, wenn FAS-Server installiert werden, oder auf einem vollständig Offline-Ausstellungsprozess zu bestehen. In beiden Fällen sollte der Administrator der Zertifizierungsstelle die vollständige Kontrolle über die Genehmigung von Zertifikatsanfragen der Registrierungsstelle behalten und eine Richtlinie zur Autorisierung von FAS-Servern haben.

Firewall-Einstellungen

Im Allgemeinen hat der Administrator der Zertifizierungsstelle auch die Kontrolle über die Netzwerk-Firewall-Einstellungen der Zertifizierungsstelle, was die Kontrolle über eingehende Verbindungen ermöglicht. Der Administrator der Zertifizierungsstelle kann DCOM-TCP- und Firewall-Regeln so konfigurieren, dass nur FAS-Server Zertifikate anfordern können.

Eingeschränkte Registrierung

Standardmäßig kann jeder Inhaber eines Registrierungsstellenzertifikats Zertifikate für jeden Benutzer ausstellen, unter Verwendung jeder Zertifikatvorlage, die den Zugriff erlaubt. Dies sollte auf eine Gruppe nicht privilegierter Benutzer beschränkt werden, indem die Eigenschaft der Zertifizierungsstelle „Registrierungsagenten einschränken“ verwendet wird.



Richtlinienmodule und Überwachung

Für erweiterte Bereitstellungen können benutzerdefinierte Sicherheitsmodule verwendet werden, um die Zertifikatsausstellung zu verfolgen und zu unterbinden.

FAS-Verwaltung

FAS verfügt über mehrere Sicherheitsfunktionen.

StoreFront, Benutzer und VDAs über eine ACL einschränken

Im Mittelpunkt des FAS-Sicherheitsmodells steht die Steuerung, welche Kerberos-Konten auf Funktionen zugreifen können:

ZUGRIFFSVEKTOR	BESCHREIBUNG
StoreFront [IdP]	Diesen Kerberos-Konten wird vertraut, dass sie deklarieren, dass ein Benutzer korrekt authentifiziert wurde. Wenn eines dieser Konten kompromittiert wird, können Zertifikate für Benutzer erstellt und verwendet werden, die durch die FAS-Konfiguration zugelassen sind.
VDAs [Relying party]	Dies sind die Maschinen, die auf die Zertifikate und privaten Schlüssel zugreifen dürfen. Ein vom IdP abgerufener Anmeldeinformations-Handle ist ebenfalls erforderlich, sodass ein kompromittiertes VDA-Konto in dieser Gruppe nur einen begrenzten Spielraum hat, um das System anzugreifen.
Benutzer	Dies steuert, welche Benutzer vom IdP bestätigt werden können. Beachten Sie, dass es Überschneidungen mit den Konfigurationsoptionen für den „Restricted Enrollment Agent“ bei der Zertifizierungsstelle gibt. Im Allgemeinen ist es ratsam, in dieser Liste nur nicht-privilegierte Konten aufzunehmen. Dies verhindert, dass ein kompromittiertes StoreFront-Konto Berechtigungen auf eine höhere administrative Ebene eskaliert. Insbesondere sollten

ZUGRIFFSVEKTOR	BESCHREIBUNG
	Domänenadministratorkonten von dieser ACL nicht zugelassen werden.

Regeln konfigurieren

Regeln sind nützlich, wenn mehrere unabhängige Citrix Virtual Apps™- oder Citrix Virtual Desktops-Bereitstellungen dieselbe FAS-Serverinfrastruktur verwenden. Jede Regel verfügt über einen separaten Satz von Konfigurationsoptionen; insbesondere können die ACLs unabhängig voneinander konfiguriert werden.

Zertifizierungsstelle und Vorlagen konfigurieren

Für verschiedene Zugriffsrechte können unterschiedliche Zertifikatvorlagen und CAs konfiguriert werden. Erweiterte Konfigurationen können je nach Umgebung weniger oder leistungsfähigere Zertifikate verwenden. Beispielsweise können als „extern“ identifizierte Benutzer ein Zertifikat mit weniger Berechtigungen als „interne“ Benutzer haben.

Sitzungsinterne und Authentifizierungszertifikate

Der FAS-Administrator kann steuern, ob das zur Authentifizierung verwendete Zertifikat in der Benutzersitzung verfügbar ist. Dies könnte beispielsweise dazu verwendet werden, dass nur „Signatur“-Zertifikate innerhalb der Sitzung verfügbar sind, während das leistungsfähigere „Anmelde“-Zertifikat nur bei der Anmeldung verwendet wird.

Schutz privater Schlüssel und Schlüssellänge

Der FAS-Administrator kann FAS so konfigurieren, dass private Schlüssel in einem Hardware-Sicherheitsmodul (HSM) oder Trusted Platform Module (TPM) gespeichert werden. Citrix empfiehlt, dass zumindest der private Schlüssel des Registrierungsstellenzertifikats durch Speicherung in einem TPM geschützt wird; diese Option wird als Teil des „Offline“-Zertifikatsanforderungsprozesses bereitgestellt.

Ähnlich können private Schlüssel von Benutzerzertifikaten in einem TPM oder HSM gespeichert werden. Alle Schlüssel sollten als „nicht exportierbar“ generiert werden und mindestens 2048 Bit lang sein.

Ereignisprotokolle

Der FAS-Server stellt detaillierte Konfigurations- und Laufzeitereignisprotokolle bereit, die für Audits und die Erkennung von Eindringversuchen verwendet werden können.

Administrativer Zugriff und Verwaltungstools

FAS umfasst Funktionen und Tools für die Remote-Verwaltung (gegenseitig authentifiziertes Kerberos). Mitglieder der „Gruppe der lokalen Administratoren“ haben die volle Kontrolle über die FAS-Konfiguration. Diese Liste sollte sorgfältig gepflegt werden.

Citrix Virtual Apps-, Citrix Virtual Desktops- und VDA-Administratoren

Im Allgemeinen ändert die Verwendung von FAS das Sicherheitsmodell der Delivery Controller- und VDA-Administratoren nicht, da das FAS-„Anmeldeinformations-Handle“ einfach das „Active Directory-Passwort“ ersetzt. Controller- und VDA-Administrationsgruppen sollten nur vertrauenswürdige Benutzer enthalten. Audits und Ereignisprotokolle sollten gepflegt werden.

Allgemeine Windows-Serversicherheit

Alle Server sollten vollständig gepatcht sein und über Standard-Firewall- und Antivirensoftware verfügen. Sicherheitskritische Infrastrukturserver sollten an einem physisch sicheren Ort aufbewahrt werden, wobei auf Festplattenverschlüsselung und Wartungsoptionen für virtuelle Maschinen geachtet werden sollte.

Audits und Ereignisprotokolle sollten sicher auf einem Remote-Computer gespeichert werden.

Der RDP-Zugriff sollte auf autorisierte Administratoren beschränkt sein. Wo möglich, sollten Benutzerkonten eine Smartcard-Anmeldung erfordern, insbesondere für Zertifizierungsstellen- und Domänenadministratorkonten.

Verwandte Informationen

- [Installieren und Konfigurieren](#) ist die primäre Referenz für die FAS-Installation und -Konfiguration.
- FAS-Architekturen werden im Artikel [Bereitstellungsarchitekturen](#) vorgestellt.
- Weitere „How-to“-Artikel werden im Artikel [Erweiterte Konfiguration](#) vorgestellt.

Problembehandlung bei Windows-Anmeldeproblemen

Dieser Artikel beschreibt die Protokolle und Fehlermeldungen, die Windows bereitstellt, wenn sich ein Benutzer mit Zertifikaten und/oder Smartcards anmeldet. Diese Protokolle enthalten Informationen, die Sie zur Behebung von Authentifizierungsfehlern verwenden können.

Zertifikate und Public-Key-Infrastruktur

Windows Active Directory verwaltet mehrere Zertifikatspeicher, die Zertifikate für sich anmeldende Benutzer verwalten.

- **NTAuth-Zertifikatspeicher:** Um sich bei Windows zu authentifizieren, muss die Zertifizierungsstelle, die Benutzerzertifikate direkt ausstellt (d. h. keine Verkettung wird unterstützt), im NTAuth-Speicher abgelegt werden. Um diese Zertifikate anzuzeigen, geben Sie im Programm certutil Folgendes ein: `certutil -viewstore -enterprise NTAuth`.
- **Stamm- und Zwischenzertifikatspeicher:** Normalerweise können Zertifikatsanmeldesysteme nur ein einziges Zertifikat bereitstellen. Wenn also eine Kette verwendet wird, muss der Zwischenzertifikatspeicher auf allen Computern diese Zertifikate enthalten. Das Stammzertifikat muss im Speicher für vertrauenswürdige Stammzertifikate und das vorletzte Zertifikat im NTAuth-Speicher liegen.
- **Anmeldezertifikaterweiterungen und Gruppenrichtlinien:** Windows kann so konfiguriert werden, dass die Überprüfung von EKUs und anderen Zertifikatsrichtlinien erzwungen wird. Siehe die Microsoft-Dokumentation: [https://docs.microsoft.com/de-de/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/ff404287\(v=ws.10\)>](https://docs.microsoft.com/de-de/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/ff404287(v=ws.10)>).

REGISTRIERUNGSRICHTLINIE	BESCHREIBUNG
AllowCertificatesWithNoEKU	Wenn deaktiviert, müssen Zertifikate die erweiterte Schlüsselverwendung (EKU) für die Smartcard-Anmeldung enthalten.
AllowSignatureOnlyKeys	Standardmäßig filtert Windows private Zertifikatsschlüssel heraus, die keine RSA-Entschlüsselung zulassen. Diese Option überschreibt diesen Filter.
AllowTimeInvalidCertificates	Standardmäßig filtert Windows abgelaufene Zertifikate heraus. Diese Option überschreibt diesen Filter.
EnumerateECCerts	Ermöglicht die Authentifizierung mit elliptischen Kurven.
X509HintsNeeded	Wenn ein Zertifikat keinen eindeutigen Benutzerprinzipalnamen (UPN) enthält oder dieser mehrdeutig sein könnte, können

REGISTRIERUNGSRICHTLINIE	BESCHREIBUNG
	Benutzer mit dieser Option ihr Windows-Anmeldekonto manuell angeben.
UseCachedCRLOnlyAnd, IgnoreRevocationUnknownErrors	Deaktiviert die Überprüfung des Widerrufs (wird normalerweise auf dem Domänencontroller festgelegt).

- **Domänencontroller-Zertifikate:** Um Kerberos-Verbindungen zu authentifizieren, müssen alle Server über entsprechende „Domänencontroller“-Zertifikate verfügen. Diese können über das MMC-Snap-In-Menü „Persönlicher Zertifikatspeicher des lokalen Computers“ angefordert werden.

UPN-Name und Zertifikatszuordnung

Es wird empfohlen, dass Benutzerzertifikate einen eindeutigen Benutzerprinzipalnamen (UPN) in der Erweiterung „Alternativer Antragstellername“ enthalten.

UPN-Namen in Active Directory

Standardmäßig hat jeder Benutzer in Active Directory einen impliziten UPN, der auf dem Muster `<samUsername>@\<domainNetBios>` und `<samUsername>@\<domainFQDN>` basiert. Die verfügbaren Domänen und FQDNs sind im RootDSE-Eintrag für die Gesamtstruktur enthalten. Beachten Sie, dass eine einzelne Domäne mehrere im RootDSE registrierte FQDN-Adressen haben kann.

Zusätzlich hat jeder Benutzer in Active Directory einen expliziten UPN und `altUserPrincipalNames`. Dies sind LDAP-Einträge, die den UPN für den Benutzer angeben.

Bei der Suche nach Benutzern anhand des UPN sucht Windows zuerst in der aktuellen Domäne (basierend auf der Identität des Prozesses, der den UPN nachschlägt) nach expliziten UPNs, dann nach alternativen UPNs. Wenn es keine Übereinstimmungen gibt, sucht es den impliziten UPN, der in verschiedenen Domänen der Gesamtstruktur aufgelöst werden kann.

Zertifikatszuordnungsdienst

Wenn ein Zertifikat keinen expliziten UPN enthält, bietet Active Directory die Möglichkeit, für jede Verwendung ein exaktes öffentliches Zertifikat in einem Attribut „x509certificate“ zu speichern. Um ein solches Zertifikat einem Benutzer zuzuordnen, kann ein Computer dieses Attribut direkt abfragen (standardmäßig in einer einzelnen Domäne).

Es wird eine Option bereitgestellt, mit der der Benutzer ein Benutzerkonto angeben kann, das diese Suche beschleunigt und es ermöglicht, diese Funktion in einer domänenübergreifenden Umgebung zu verwenden.

Wenn mehrere Domänen in der Gesamtstruktur vorhanden sind und der Benutzer keine Domäne explizit angibt, gibt das Active Directory rootDSE den Speicherort des Zertifikatsuordnungsdienstes an. Dieser befindet sich normalerweise auf einem globalen Katalogserver und verfügt über eine zwischengespeicherte Ansicht aller x509-Zertifikatattribute in der Gesamtstruktur. Dieser Computer kann verwendet werden, um ein Benutzerkonto in jeder Domäne effizient zu finden, basierend nur auf dem Zertifikat.

Auswahl des Anmelde-Domänencontrollers steuern

Wenn eine Umgebung mehrere Domänencontroller enthält, ist es nützlich zu sehen und einzuschränken, welcher Domänencontroller für die Authentifizierung verwendet wird, damit Protokolle aktiviert und abgerufen werden können.

Auswahl des Domänencontrollers steuern

Um Windows zu zwingen, einen bestimmten Windows-Domänencontroller für die Anmeldung zu verwenden, können Sie die Liste der Domänencontroller, die ein Windows-Computer verwendet, explizit festlegen, indem Sie die lmhosts-Datei konfigurieren:

\\Windows\\System32\\drivers\\etc\\lmhosts.

An diesem Speicherort befindet sich normalerweise eine Beispieldatei namens „lmhosts.sam“. Fügen Sie einfach eine Zeile ein:

1.2.3.4 dcnetbiosname #BEVORZUGT #DOMÄNE:mydomai

Wobei „1.2.3.4“ die IP-Adresse des Domänencontrollers mit dem Namen „dcnetbiosname“ in der Domäne „mydomain“ ist.

Nach einem Neustart verwendet der Windows-Computer diese Informationen, um sich bei mydomain anzumelden. Beachten Sie, dass diese Konfiguration rückgängig gemacht werden muss, wenn das Debugging abgeschlossen ist.

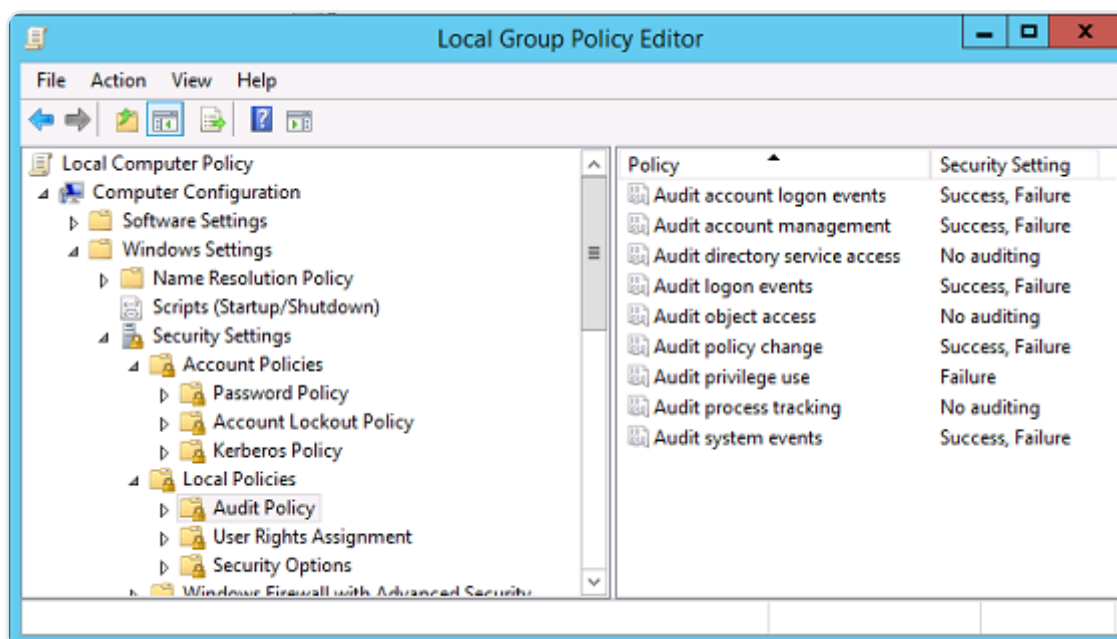
Verwendeten Domänencontroller identifizieren

Bei der Anmeldung setzt Windows eine MSDOS-Umgebungsvariable mit dem Domänencontroller, der den Benutzer angemeldet hat. Um dies zu sehen, starten Sie die Eingabeaufforderung mit dem Befehl: **echo %LOGONSERVER%**.

Protokolle, die sich auf die Authentifizierung beziehen, werden auf dem Computer gespeichert, der von diesem Befehl zurückgegeben wird.

Überwachungsereignisse für Konten aktivieren

Standardmäßig aktivieren Windows-Domänencontroller keine vollständigen Überwachungsprotokolle für Konten. Dies kann über Überwachungsrichtlinien in den Sicherheitseinstellungen des Gruppenrichtlinien-Editors gesteuert werden. Nach der Aktivierung erzeugt der Domänencontroller zusätzliche Ereignisprotokollinformationen in der Sicherheitsereignisprotokolldatei.



Zertifikatsvalidierungsprotokolle

Zertifikatsgültigkeit prüfen

Wenn ein Smartcard-Zertifikat als DER-Zertifikat (kein privater Schlüssel erforderlich) exportiert wird, können Sie es mit dem Befehl validieren: `certutil -verify user.cer`

CAP-Protokollierung aktivieren

Auf dem Domänencontroller und dem Computer des Benutzers öffnen Sie die Ereignisanzeige und aktivieren die Protokollierung für Microsoft/Windows/CAP/Operational Logs.

Sie können die CAP-Protokollierung mit den Registrierungsschlüsseln unter steuern: `CurrentControlSet\Services\crypt32`.

WERT	BESCHREIBUNG
DiagLevel (DWORD)	Ausführlichkeitsgrad (0 bis 5)
DiagMatchAnyMask (QUADWORD)	Ereignisfilter (verwenden Sie 0xffffffff für alle)
DiagProcessName (MULTI_SZ)	Nach Prozessname filtern (zum Beispiel LSASS.exe)

CAPI-Protokolle

MELDUNG	BESCHREIBUNG
Kette erstellen	LSA hat CertGetCertificateChain aufgerufen (enthält Ergebnis)
Sperrung überprüfen	LSA hat CertVerifyRevocation aufgerufen (enthält Ergebnis)
X509-Objekte	Im ausführlichen Modus werden Zertifikate und Zertifikatssperrlisten (CRLs) in AppData\LocalLow\Microsoft\X509Objects abgelegt.
Kettenrichtlinie überprüfen	LSA hat CertVerifyChainPolicy aufgerufen (enthält Parameter)

Fehlermeldungen

FEHLERCODE	BESCHREIBUNG
Zertifikat nicht vertrauenswürdig	Das Smartcard-Zertifikat konnte nicht unter Verwendung von Zertifikaten in den Zwischen- und vertrauenswürdigen Stammzertifikatspeichern des Computers erstellt werden.
Fehler bei der Zertifikatssperrprüfung	Die CRL für die Smartcard konnte nicht von der Adresse heruntergeladen werden, die vom CRL-Verteilungspunkt des Zertifikats angegeben wurde. Wenn die Sperrprüfung vorgeschrieben ist, verhindert dies eine

FEHLERCODE	BESCHREIBUNG
	erfolgreiche Anmeldung. Siehe den Abschnitt Zertifikate und Public Key Infrastruktur .
Fehler bei der Zertifikatsverwendung	Das Zertifikat ist nicht für die Anmeldung geeignet. Es könnte sich zum Beispiel um ein Serverzertifikat oder ein Signaturzertifikat handeln.

Kerberos-Protokolle

Um die Kerberos-Protokollierung zu aktivieren, erstellen Sie auf dem Domänencontroller und dem Endbenutzercomputer die folgenden Registrierungswerte:

HIVE	WERTNAME	WERT [DWORD]
CurrentControlSet\Control\LSa\Kerberos\Parameters	LogLevel	0x1
CurrentControlSet\Control\LSa\Kerberos\Parameters	KerbDebuglevel	0xffffffff
CurrentControlSet\Services\Kdc	KdcDebugLevel	0x1
CurrentControlSet\Services\Kdc	KdcExtraLogLevel	0x1f

Die Kerberos-Protokollierung wird im Systemereignisprotokoll ausgegeben.

- Meldungen wie „nicht vertrauenswürdiges Zertifikat“ sollten leicht zu diagnostizieren sein.
- Zwei Fehlercodes sind informativ und können bedenkenlos ignoriert werden:
 - KDC_ERR_PREAUTH_REQUIRED (wird zur Abwärtskompatibilität mit älteren Domänencontrollern verwendet)
 - Unbekannter Fehler 0x4b

Ereignisprotokollmeldungen

Dieser Abschnitt beschreibt die erwarteten Protokolleinträge auf dem Domänencontroller und der Workstation, wenn sich der Benutzer mit einem Zertifikat anmeldet.

- CAPI2-Protokoll des Domänencontrollers
- Sicherheitsprotokolle des Domänencontrollers
- Sicherheitsprotokoll des Virtual Delivery Agent (VDA)
- VDA CAPI-Protokoll
- VDA-Systemprotokoll

CAPI2-Protokoll des Domänencontrollers

Während einer Anmeldung validiert der Domänencontroller das Zertifikat des Aufrufers und erstellt eine Abfolge von Protokolleinträgen in der folgenden Form.

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

Die endgültige Ereignisprotokollmeldung zeigt, dass lsass.exe auf dem Domänencontroller eine Kette basierend auf dem vom VDA bereitgestellten Zertifikat erstellt und diese auf Gültigkeit (einschließlich Sperrung) überprüft. Das Ergebnis wird als „ERROR_SUCCESS“ zurückgegeben.

```
- 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
```

Sicherheitsprotokoll des Domänencontrollers

Der Domänencontroller zeigt eine Abfolge von Anmeldeereignissen, wobei das Schlüsselereignis 4768 ist, bei dem das Zertifikat zur Ausstellung des Kerberos Ticket Granting Ticket (krbtgt) verwendet wird.

Die Meldungen davor zeigen, dass das Computerkonto des Servers sich beim Domänencontroller authentifiziert. Die Meldungen danach zeigen, dass das Benutzerkonto, das zum neuen krbtgt gehört, zur Authentifizierung beim Domänencontroller verwendet wird.

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

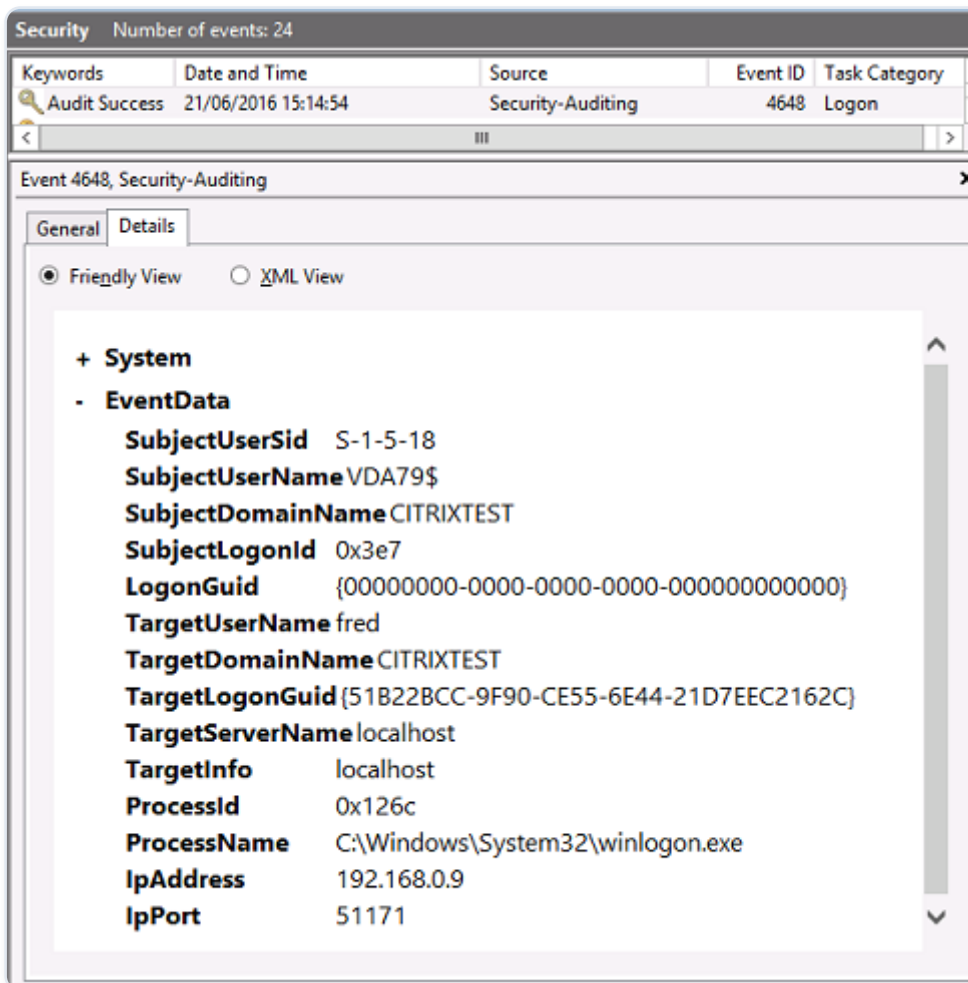
General Details

☒ 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-Sicherheitsprotokoll

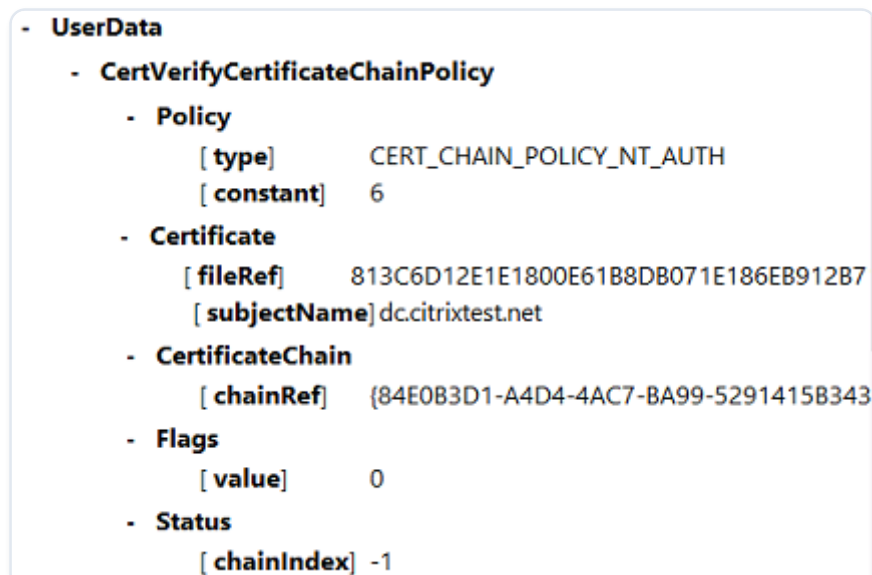
Das VDA-Sicherheitsüberwachungsprotokoll, das dem Anmeldeereignis entspricht, ist der Eintrag mit der Ereignis-ID 4648, der von winlogon.exe stammt.



VDA CAPI-Protokoll

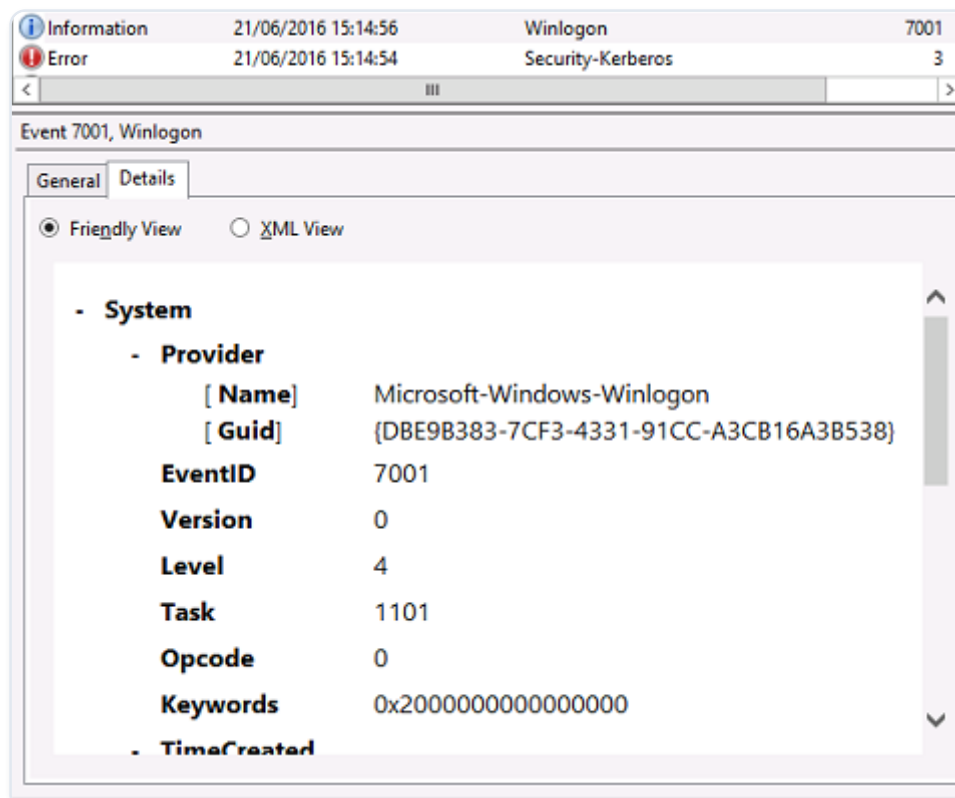
Dieses Beispiel-VDA-CAPI-Protokoll zeigt eine einzelne Kettenaufbau- und Verifizierungssequenz von lsass.exe, die das Domänencontroller-Zertifikat (dc.citrixtest.net) validiert.

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



VDA-Systemprotokoll

Wenn die Kerberos-Protokollierung aktiviert ist, zeigt das Systemprotokoll den Fehler KDC_ERR_PREAUTH_REQUIRED (der ignoriert werden kann) und einen Eintrag von Winlogon, der anzeigt, dass die Kerberos-Anmeldung erfolgreich war.



Fehlermeldungen für Endbenutzer

Dieser Abschnitt listet häufige Fehlermeldungen auf, die einem Benutzer auf der Windows-Anmeldeseite angezeigt werden.

ANGEZEIGTE FEHLERMELDUNG	BESCHREIBUNG UND REFERENZ
Ungültiger Benutzername oder ungültiges Kennwort	Der Computer geht davon aus, dass Sie ein gültiges Zertifikat und einen privaten Schlüssel besitzen, aber der Kerberos-Domänencontroller hat die Verbindung abgelehnt. Siehe den Abschnitt <i>Kerberos-Protokolle</i> dieses Artikels.
Das System konnte Sie nicht anmelden. Ihre Anmeldeinformationen konnten nicht überprüft werden. / Die Anforderung wird nicht unterstützt	Der Domänencontroller kann nicht kontaktiert werden, oder der Domänencontroller wurde nicht mit einem Zertifikat zur Unterstützung der Smartcard-Authentifizierung konfiguriert. Registrieren Sie den Domänencontroller für ein „Kerberos-Authentifizierungs“- , „Domänencontroller-Authentifizierungs“- oder „Domänencontroller“-Zertifikat. Dies ist normalerweise einen Versuch wert, auch wenn das vorhandene Zertifikat gültig zu sein scheint.
Das System konnte Sie nicht anmelden. Das zur Authentifizierung verwendete Smartcard-Zertifikat wurde nicht als vertrauenswürdig eingestuft.	Die Zwischen- und Stammzertifikate sind nicht auf dem lokalen Computer installiert. Siehe Zertifikate und Public Key-Infrastruktur .
Ungültige Anforderung	Dies deutet normalerweise darauf hin, dass die Erweiterungen des Zertifikats nicht korrekt eingestellt sind, oder der RSA-Schlüssel zu kurz ist (<2048 Bit).

Verwandte Informationen

- Konfigurieren einer Domäne für die Smartcard-Anmeldung: <http://support.citrix.com/article/CTX206156>
- Smartcard-Anmelderichtlinien: [https://docs.microsoft.com/de-de/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/ff404287\(v=ws.10\)](https://docs.microsoft.com/de-de/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/ff404287(v=ws.10))
- CAPI-Protokollierung aktivieren: <http://social.technet.microsoft.com/wiki/contents/articles/242.troubleshooting-pki-problems-on-windows.aspx>
- Kerberos-Protokollierung aktivieren: <https://support.microsoft.com/de-de/kb/262177>

- Richtlinien zum Aktivieren der Smartcard-Anmeldung mit Zertifizierungsstellen von Drittanbietern: <https://support.microsoft.com/de-de/kb/281245>

PowerShell-Cmdlets

Sie können die Verwaltungskonsole des Federated Authentication Service (FAS) für einfache Bereitstellungen verwenden; die PowerShell-Schnittstelle bietet jedoch erweiterte Optionen. Wenn Sie Optionen verwenden möchten, die in der Konsole nicht verfügbar sind, empfiehlt Citrix®, für die Konfiguration ausschließlich PowerShell zu verwenden.

Der folgende Befehl fügt die FAS PowerShell-Cmdlets hinzu:

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

In einem PowerShell-Fenster können Sie `Get-Help \<cmdlet name>` verwenden, um die Cmdlet-Hilfe anzuzeigen.

Weitere Informationen zu den FAS PowerShell SDK-Cmdlets finden Sie unter <https://developer-docs.citrix.com/projects/federated-authentication-service-powershell-cmdlets/en/latest/>.

Dokumentationshistorie des Federated Authentication Service 1912

Die folgende Tabelle beschreibt wichtige Änderungen an der Dokumentation des Federated Authentication Service 1912. Um Benachrichtigungen über diese Updates zu erhalten, abonnieren Sie den RSS-Feed.

DATUM	ÄNDERUNG	BESCHREIBUNG
18 Dec 2019	Erste Veröffentlichung des Federated Authentication Service 1912	Erste Veröffentlichung des Federated Authentication Service 1912. Weitere Informationen finden Sie unter Neuerungen .