# Verbundauthentifizierungsdienst

# Contents



# Verbundauthentifizierungsdienst 2311

September 11, 2024

Dieses Release des Verbundauthentifizierungsdiensts enthält das folgende neue Feature:

- **Die Informationen Anforderung des Verbundauthentifizierungsdienst-Zertifikats wurden um SID erweitert.** Die Zertifikatsanforderung des Verbundauthentifizierungsdiensts an die Zertifizierungsstelle wurde um den SID-Parameter erweitert. Für Benutzer, die in den Eigenschaften des **Antragstellernamens** in der Vorlage `Citrix_SmartcardLogon` die Option **Informationen werden in der Anforderung angegeben** aktivieren, ermöglicht dieser Zusatz des FAS, mit den in KB5014754 beschriebenen Änderungen der Zertifikatsauthentifizierung zu arbeiten. Diese Authentifizierungsänderungen werden bereits für Benutzer unterstützt, die die Standardeinstellung **Aus diesen Active Directory-Informationen erstellen** verwenden.

Informationen zu Bugfixes finden Sie unter Behobene Probleme.

## Behobene Probleme

September 11, 2024

Es gibt keine behobenen Probleme im Verbundauthentifizierungsdienst 2311.

## Bekannte Probleme

September 11, 2024

Es gibt keine bekannten Probleme im Verbundauthentifizierungsdienst 2311.

Der folgende Warnhinweis gilt für alle Workarounds, bei denen ein Registrierungseintrag geändert werden muss:

> **Warnung:**
>
> Eine unsachgemäße Bearbeitung der Registrierung kann schwerwiegende Probleme verursachen und eine Neuinstallation des Betriebssystems erforderlich machen. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine unsachgemäße Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können. Die Verwendung des Registrierungs-Editors geschieht daher auf eigene Gefahr. Erstellen Sie auf jeden Fall ein Backup

> der Registrierung, bevor Sie sie bearbeiten.

## Hinweise zu Drittanbietern

September 11, 2024

Dieses Release des Verbundauthentifizierungsdiensts enthält ggf. Software von Drittanbietern, die gemäß den in den folgenden Dokumenten aufgeführten Bestimmungen lizenziert ist:

- Citrix Virtual Apps and Desktops –Hinweise zu Drittanbietern (PDF-Download)
- Non-Commercial Software Disclosures For FlexNet Publisher 2017 (11.15.0.0) (PDF Download)
- FlexNet Publisher Documentation Supplement Third Party and Open Source Software used in FlexNet Publisher 11.15.0 (PDF Download)

## Systemanforderungen

September 11, 2024

- Der Verbundauthentifizierungsdienst (Federated Authentication Service, FAS) wird unter folgenden Windows Server-Versionen unterstützt:
  - Windows Server 2022, Standard und Datacenter Edition
  - Windows Server 2019, Standard und Datacenter Edition und mit der Server Core-Option
  - Windows Server 2016, Standard und Datacenter Edition und mit der Server Core-Option
- Citrix empfiehlt die Installation des FAS auf einem Server, der keine anderen Citrix-Komponenten enthält.
- Der Windows-Server muss geschützt werden, da er Zugriff auf ein Zertifikat der Registrierungsstelle und einen privaten Schlüssel hat. Mithilfe des Zertifikats und des privaten Schlüssels kann der Server Zertifikate für Domänenbenutzer ausstellen. Der Server hat außerdem Zugriff auf die ausgestellten Zertifikate und privaten Schlüssel für Domänenbenutzer.
- Für die FAS-PowerShell-Cmdlets ist Windows PowerShell 64-Bit auf dem FAS-Server erforderlich.
- Für die Ausstellung von Benutzerzertifikaten ist eine Zertifizierungsstelle wie Microsoft Enterprise oder eine andere im Citrix Ready-Programm validierte Zertifizierungsstelle erforderlich.
- Stellen Sie für andere Zertifizierungsstellen als Microsoft Folgendes sicher:

  - Die Zertifizierungsstelle (ZS) ist im Active Directory als Registrierungsdienst registriert.
  - Das Zertifizierungsstellenzertifikat befindet sich im NTAuth-Store auf dem Domänencontroller. Weitere Informationen finden Sie unter Importieren von Zertifizierungsstellenzertifikaten von Drittanbietern in den Enterprise NTAuth-Speicher.

Citrix Virtual Apps- oder Citrix Virtual Desktops-Site:

- Delivery Controller, Virtual Delivery Agents (VDAs) und StoreFront Server müssen alle in unterstützten Versionen vorliegen.
- Bevor Sie den Maschinenkatalog erstellen, müssen Sie die Gruppenrichtlinienkonfiguration für den Verbundauthentifizierungsdienst auf die VDAs anwenden. Weitere Informationen finden Sie im Abschnitt Gruppenrichtlinie konfigurieren.

Konsultieren Sie bei der Planung der Bereitstellung dieses Diensts den Abschnitt Sicherheitsüberlegungen.

## Installation

September 11, 2024

### Reihenfolge der Schritte zur Installation und Einrichtung

1. Installieren des Verbundauthentifizierungsdiensts (FAS)
2. Aktivieren des FAS-Plug-Ins für StoreFront-Stores
3. Delivery Controller konfigurieren
4. Gruppenrichtlinie konfigurieren
5. Verwenden Sie die FAS-Verwaltungskonsole für Folgendes:

    a) Zertifikatvorlagen bereitstellen
    b) Einrichten von Zertifizierungsstellen
    c) Autorisierte Verwendung Ihrer Zertifizierungsstellen durch den FAS
    d) Konfigurieren von Regeln
    e) Verbinden des FAS mit Citrix Cloud (optional)

### Verbundauthentifizierungsdienst installieren

Citrix empfiehlt aus Sicherheitsgründen, den Verbundauthentifizierungsdienst (FAS) auf einem eigenen Server zu installieren. Dieser Server muss auf ähnliche Weise wie ein Domänencontroller oder eine Zertifizierungsstelle geschützt werden. Der FAS kann folgendermaßen installiert werden:

- Mit dem Citrix Virtual Apps and Desktops-Installationsprogramm (über die Schaltfläche **Verbundauthentifizierungsdienst** auf dem Begrüßungsbildschirm der automatischen Ausführung, wenn die ISO-Datei eingefügt wird) oder
- Mit der eigenständigen FAS-Installationsdatei (verfügbar als MSI-Datei unter Citrix Downloads).

Es werden folgende Komponenten installiert:

- Verbundauthentifizierungsdienst
- PowerShell-Snap-In-Cmdlets für die erweiterte FAS-Konfiguration
- FAS-Verwaltungskonsole
- FAS-Gruppenrichtlinienvorlagen (CitrixFederatedAuthenticationService.admx/adml)
- Zertifikatvorlagendateien
- Leistungsindikatoren und Ereignisprotokolle

#### Aktualisieren des Verbundauthentifzierungsdiensts

Sie können den FAS über ein direktes Upgrade aktualisieren. Berücksichtigen Sie vor dem Upgrade Folgendes:

- Alle FAS-Servereinstellungen bleiben erhalten, wenn Sie ein direktes Upgrade durchführen.
- Schließen Sie die FAS-Verwaltungskonsole, bevor Sie den FAS aktualisieren.
- Stellen Sie sicher, dass stets mindestens ein FAS-Server verfügbar ist. Wenn kein Server mit einem für den Verbundauthentifizierungsdienst aktivierten StoreFront-Server erreichbar ist, können die Benutzer sich nicht anmelden und keine Anwendungen starten.

Um ein Upgrade zu starten, installieren Sie den FAS mit dem Citrix Virtual Apps and Desktops-Installationsprogramm oder mit der eigenständigen FAS-Installationsdatei.

### Aktivieren des FAS-Plug-Ins für StoreFront-Stores

> **Hinweis:**
>
> Dieser Schritt ist nicht erforderlich, wenn Sie den FAS nur mit Citrix Cloud verwenden.

Zum Aktivieren der FAS-Integration auf einem StoreFront-Store führen Sie als Administrator folgende PowerShell-Cmdlets aus. Wenn der Store einen anderen Namen hat, ändern Sie `$StoreVirtualPath`.

```
1     Get-Module "Citrix.StoreFront.*" -ListAvailable | Import-Module
2     $StoreVirtualPath = "/Citrix/Store"
3     $store = Get-STFStoreService -VirtualPath $StoreVirtualPath
4     $auth = Get-STFAuthenticationService -StoreService $store
5     Set-STFClaimsFactoryNames -AuthenticationService $auth -
         ClaimsFactoryName "FASClaimsFactory"
```

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

Zum Beenden der Verwendung des FAS verwenden Sie folgendes PowerShell-Skript:

```
1     Get-Module "Citrix.StoreFront.*" -ListAvailable | Import-Module
2     $StoreVirtualPath = "/Citrix/Store"
3     $store = Get-STFStoreService -VirtualPath $StoreVirtualPath
4     $auth = Get-STFAuthenticationService -StoreService $store
5     Set-STFClaimsFactoryNames -AuthenticationService $auth -
          ClaimsFactoryName "standardClaimsFactory"
6     Set-STFStoreLaunchOptions -StoreService $store -
          VdaLogonDataProvider ""
```

### Delivery Controller konfigurieren

> **Hinweis:**
>
> Dieser Schritt ist nicht erforderlich, wenn Sie den FAS nur mit Citrix Cloud verwenden.

Zur Verwendung des FAS konfigurieren Sie den Citrix Virtual Apps- oder Citrix Virtual Desktops-Delivery Controller für eine Vertrauensstellung mit den StoreFront-Servern, die mit ihm verbunden werden. Führen Sie hierfür das PowerShell-Cmdlet **Set-BrokerSite -TrustRequestsSentToTheXmlServicePort $true** aus. Führen Sie diesen Befehl pro Site nur einmal aus, unabhängig von der Anzahl der Delivery Controller in der Site.

### Gruppenrichtlinie konfigurieren

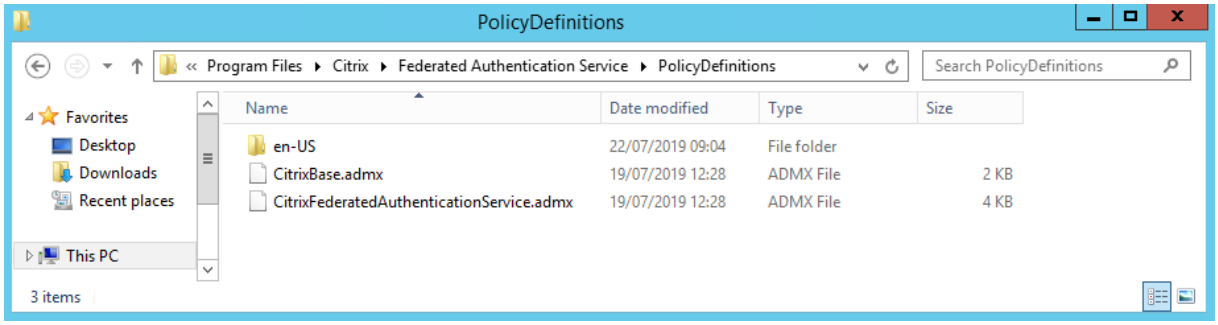
Nach der FAS-Installation geben Sie unter Verwendung der im Installationsprogramm enthaltenen Gruppenrichtlinienvorlagen den vollqualifizierten Domänennamen (FQDN) der FAS-Server in der Gruppenrichtlinie an.

> **Wichtig:**
>
> Die Tickets anfordernden StoreFront-Server und die Tickets auslösenden Virtual Delivery Agents (VDAs) müssen die gleiche FQDN-Konfiguration haben, einschließlich der automatischen Server-nummerierung, die vom Gruppenrichtlinienobjekt angewendet wird.

Der Einfachheit halber zeigen die folgenden Beispiele die Konfiguration einer Richtlinie auf Domänenebene für alle Maschinen. Dies ist jedoch nicht erforderlich. FAS funktioniert, wenn die Liste der FQDNs für die StoreFront-Server, die VDAs und die Maschine mit der FAS-Verwaltungskonsole identisch sind. Siehe Schritt 6.

**Schritt 1:** Suchen Sie auf dem Server, auf dem Sie den FAS installiert haben, die Dateien C:\Programme\Citrix\Federated Authentication Service\PolicyDefinitions\CitrixFederatedAuthenticationService.a und CitrixBase.admx und den Ordner “de-DE”.

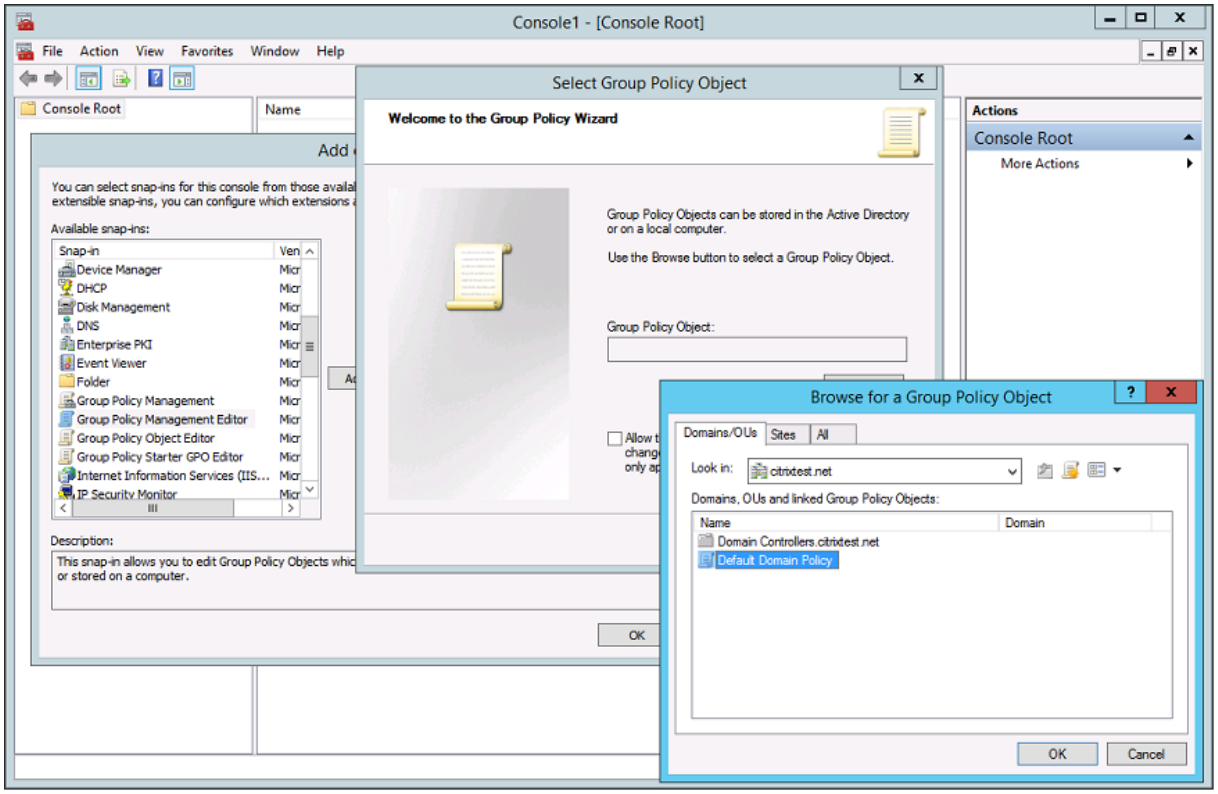
 




**Schritt 2:** Kopieren Sie diese Dateien auf die Domänencontroller in den Pfad C:\Windows\PolicyDefinitions.

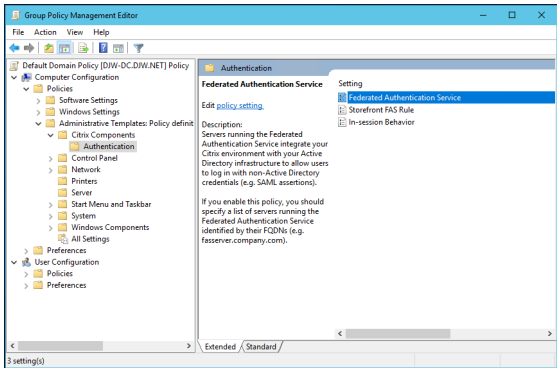
**Schritt 3:** Führen Sie Microsoft Management Console (Befehlszeile: "mmc.exe") aus. Wählen Sie auf der Menüleiste **Datei > Snap-In hinzufügen/entfernen**. Fügen Sie den **Gruppenrichtlinienverwaltungs-Editor** hinzu.

Wenn Sie nach einem Gruppenrichtlinienobjekt gefragt werden, wählen Sie **Durchsuchen** und dann **Standarddomänenrichtlinie**. Alternativ können Sie ein für Ihre Umgebung geeignetes Richtlinienobjekt mit einem Tool Ihrer Wahl erstellen und auswählen. Die Richtlinie muss auf alle Maschinen angewendet werden, auf denen relevante Citrix Software (VDAs, StoreFront-Server, Verwaltungstools) ausgeführt wird.



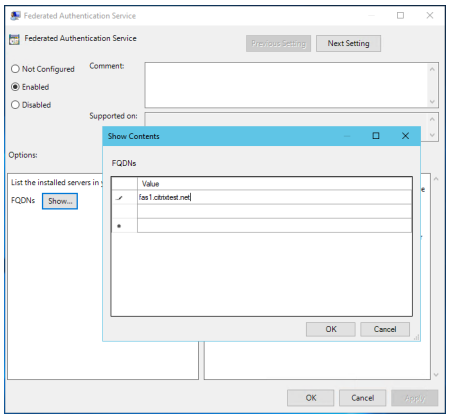

**Schritt 4:** Gehen Sie zur Richtlinie *Verbundauthentifizierungsdienst (Federated Authentication Service)* unter Configuration/Policies/Administrative Templates/Citrix Components/Authentication.




> **Hinweis:**
>
> Die Einstellung der Verbundauthentifizierungsdienst-Richtlinie ist nur im Gruppenrichtlinienobjekt der Domäne verfügbar, wenn Sie die Vorlagendatei CitrixBase.admx/CitrixBase.adml in den Ordner PolicyDefinitions einfügen. Nach Schritt 3 wird die Richtlinieneinstellung für den Verbundauthentifizierungsdienst im Ordner **Administrative Vorlagen > Citrix Komponenten > Authentifizierung** aufgeführt.

**Schritt 5:** Öffnen Sie die Verbundauthentifizierungsdienst-Richtlinie und wählen Sie **Aktiviert**. Dadurch wird die Schaltfläche **Anzeigen** wählbar, über die Sie die FQDNs der FAS-Server konfigurieren.




**Schritt 6:** Geben Sie die FQDNs der FAS-Server ein.

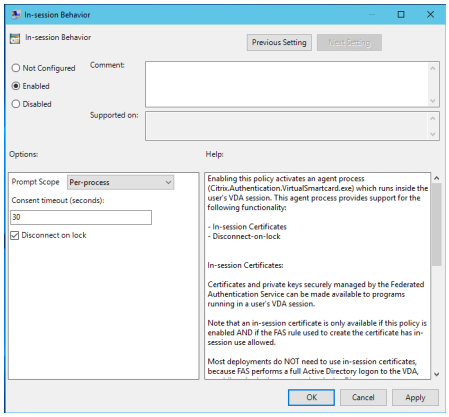
> **Wichtig:**
>
> Wenn Sie mehrere FQDNs eingeben, muss die Reihenfolge der Liste für VDAs, StoreFront-Server (falls vorhanden) und FAS-Server übereinstimmen. Siehe Gruppenrichtlinieneinstellungen.

**Schritt 7:** Klicken Sie auf **OK**, um den Gruppenrichtlinien-Assistenten zu beenden und die Änderungen der Gruppenrichtlinie anzuwenden. Sie müssen gegebenenfalls die Maschinen neu starten oder **gpupdate /force** an der Befehlszeile ausführen, damit die Änderungen wirksam werden.

### In-session Behavior

Diese Richtlinie aktiviert einen Agentprozess in der VDA-Sitzung des Benutzers, der sitzungsinterne Zertifikate, Zustimmung und Trennung bei Sperre unterstützt. Sitzungsinterne Zertifikate sind nur verfügbar, wenn diese Richtlinie aktiviert ist *und* wenn die zum Erstellen des Zertifikats verwendete FAS-Regel die sitzungsinterne Nutzung gestattet, siehe Konfigurieren von Regeln.




**Enable** aktiviert diese Richtlinie und ermöglicht die Ausführung eines FAS-Agentprozesses in der VDA-Sitzung des Benutzers.

**Disable** deaktiviert die Richtlinie und stoppt die Ausführung des FAS-Agentprozesses.

**Prompt Scope** Wenn diese Richtlinie aktiviert ist, steuert **Prompt Scope**, wie Benutzer aufgefordert werden zuzustimmen, damit eine Anwendung ein sitzungsinternes Zertifikat verwenden kann. Es gibt drei Optionen:

- **No consent required**: Diese Option deaktiviert die Sicherheitsaufforderung und private Schlüssel werden im Hintergrund verwendet.
- **Per-process consent**: Für jedes laufende Programm ist die separate Zustimmung erforderlich.
- **Per-session consent**: Sobald der Benutzer auf **OK** klickt, gilt diese Option für alle Programme in der Sitzung.

**Consent Timeout** Wenn diese Richtlinie aktiviert ist, definiert **Consent Timeout**, wie lange die Zustimmung gültig ist (in Sekunden). Bei einer Gültigkeit von 300 Sekunden müssen Benutzer beispielsweise alle fünf Minuten neu zustimmen. Beim Wert Null müssen Benutzer bei jedem Privatschlüsselvorgang zustimmen.

**Disconnect on lock** Wenn diese Richtlinie aktiviert ist, wird die Sitzung des Benutzers automatisch getrennt, wenn der Bildschirm gesperrt wird. Dieses Verhalten ähnelt der Richtlinie zum Trennen beim Entfernen von Smartcards. Verwenden Sie dieses Feature, wenn die Benutzer keine Active Directory-Anmeldeinformationen haben.

> **Hinweis:**
>
> Die Richtlinie zum Trennen der Verbindung beim Sperren gilt für alle Sitzungen auf dem VDA.

### Verwendung der FAS-Verwaltungskonsole

> **Hinweis:**
>
> Die FAS-Verwaltungskonsole eignet sich für die meisten Bereitstellungen, während die PowerShell erweiterte Optionen bietet. Informationen zu den FAS-PowerShell-Cmdlets finden Sie unter PowerShell-Cmdlets.

Die FAS-Verwaltungskonsole wird als Teil des FAS installiert. Ein Symbol (Citrix Verbundauthentifizierungsdienst) wird in das Startmenü eingefügt.

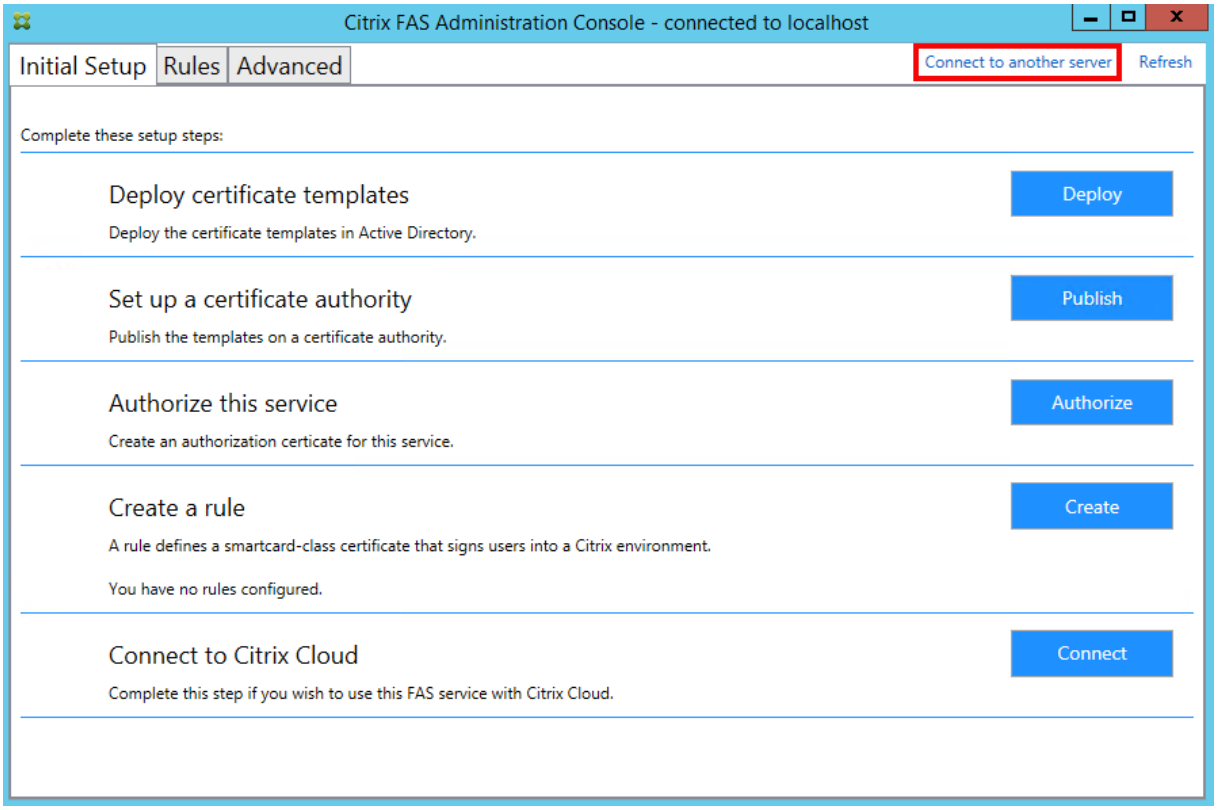
Wenn Sie die Verwaltungskonsole zum ersten Mal verwenden, werden Sie durch den folgenden Prozess geführt:

- Zertifikatvorlagen bereitstellen.
- Zertifizierungsstelle einrichten.
- Verwendung der Zertifizierungsstelle durch den FAS autorisieren.

Sie können auch die Konfigurationstools des Betriebssystems verwenden, um einige der Schritte manuell auszuführen.

Die FAS-Verwaltungskonsole stellt standardmäßig eine Verbindung zum On-Premises-Verbundauthentifizierungsdienst her. Bei Bedarf können Sie über **Connect to another Server** rechts oben in der Konsole eine Verbindung zu einem Remotedienst herstellen.



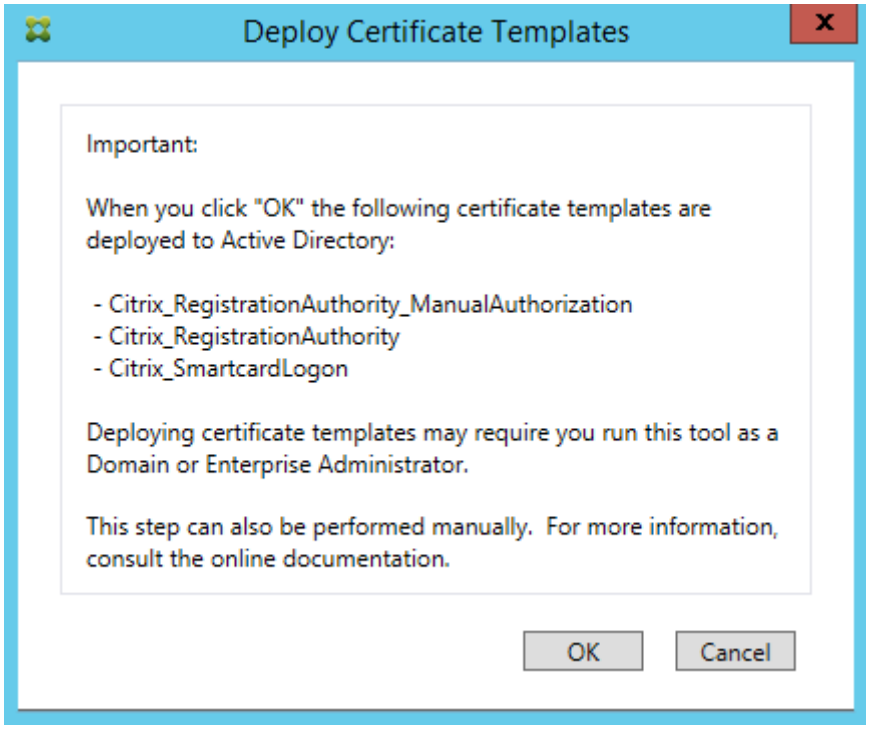

### Zertifikatvorlagen bereitstellen

Zur Vermeidung von Interoperabilitätsproblemen mit anderer Software bietet der FAS drei eigene Citrix Zertifikatvorlagen.

- Citrix_RegistrationAuthority_ManualAuthorization
- Citrix_RegistrationAuthority
- Citrix_SmartcardLogon

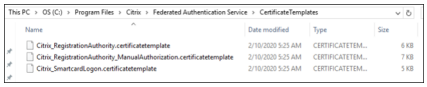
Diese Vorlagen müssen bei Active Directory registriert sein. Klicken Sie auf die Schaltfläche **Deploy** und dann auf **OK**.




Die Konfiguration der Vorlagen ist in den XML-Dateien mit der Erweiterung “certificatetemplate”zu finden. Diese werden mit dem FAS in folgenden Pfad installiert:

C:\Programme\Citrix\Federated Authentication Service\CertificateTemplates



Wenn Sie keine Berechtigung zum Installieren dieser Vorlagendateien haben, geben Sie sie dem Active Directory-Administrator.

Zur manuellen Installation der Vorlagen können Sie die folgenden PowerShell-Befehle verwenden, die sich im Ordner mit den Vorlagen befinden:

```
$template = [System.IO.File]::ReadAllBytes("$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)
```

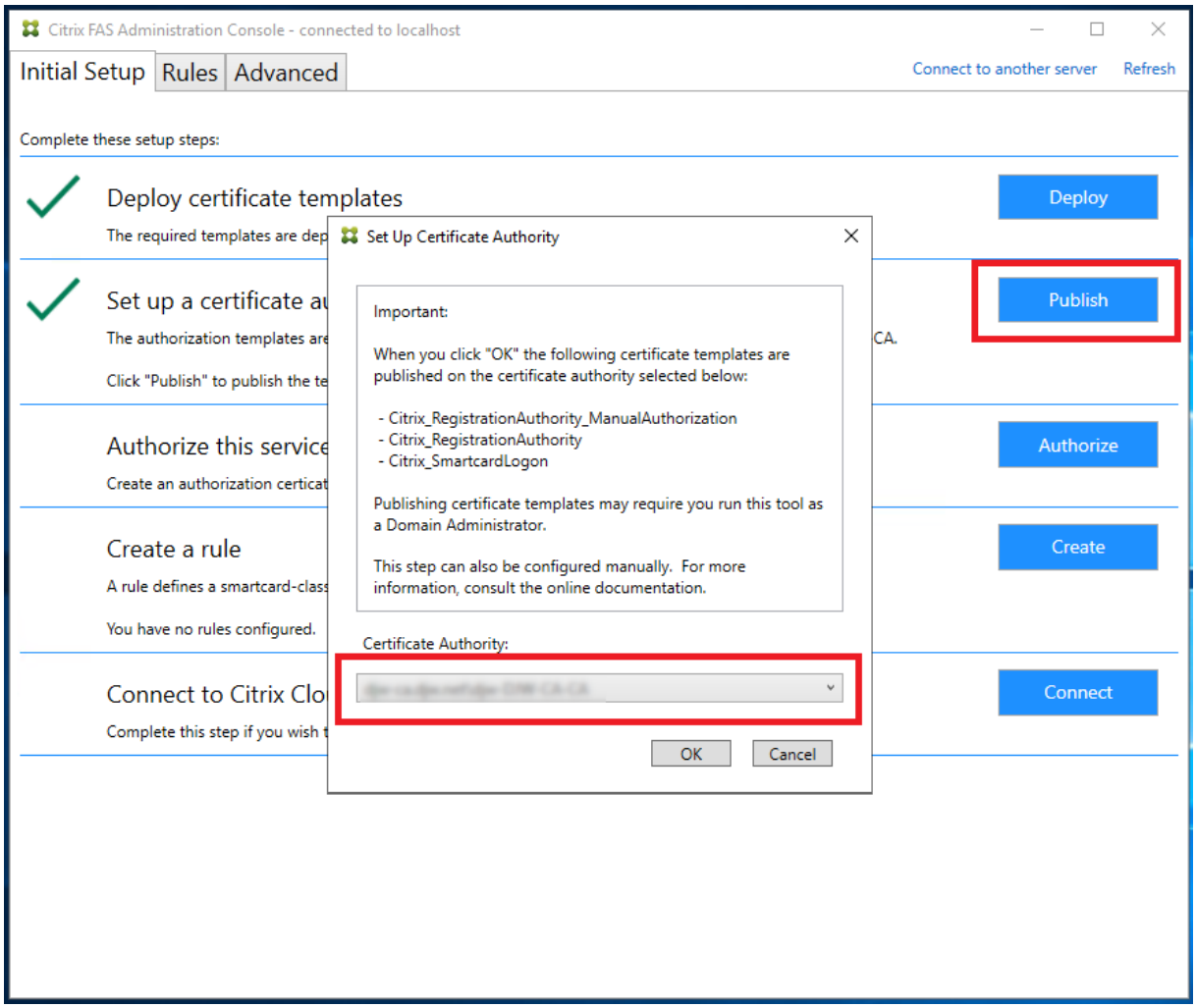
 

### Active Directory-Zertifikatdienste einrichten

Nach Installation der Citrix Zertifikatvorlagen müssen sie auf mindestens einem Microsoft Enterprise-Zertifizierungsstellenserver veröffentlicht werden. Informationen zur Bereitstellung von Active Directory-Zertifikatdienste finden Sie in der Dokumentation von Microsoft.

Ein Benutzer mit Berechtigung zum Verwalten der Zertifizierungsstelle muss die Vorlagen auf mindestens einem Server veröffentlichen. Verwenden Sie **Set Up Certificate Authority**, um sie zu veröffentlichen.

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

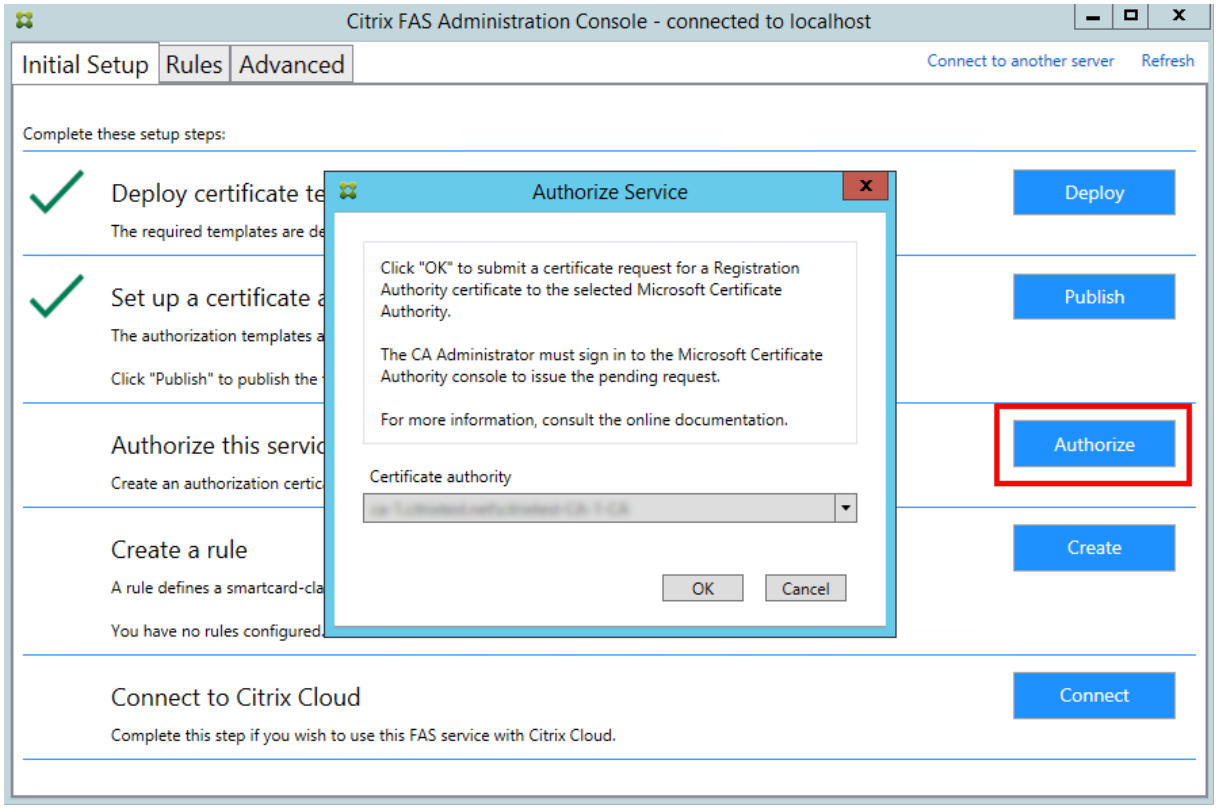



### Autorisieren des Verbundauthentifizierungsdiensts

Dieser Schritt leitet die Autorisierung des FAS ein. Von der Verwaltungskonsole wird die Vorlage “Citrix_RegistrationAuthority_ManualAuthorization”zum Erstellen einer Zertifikatanforderung

verwendet, die dann an eine der Zertifizierungsstellen gesendet wird, die das Zertifikat veröffentlichen.

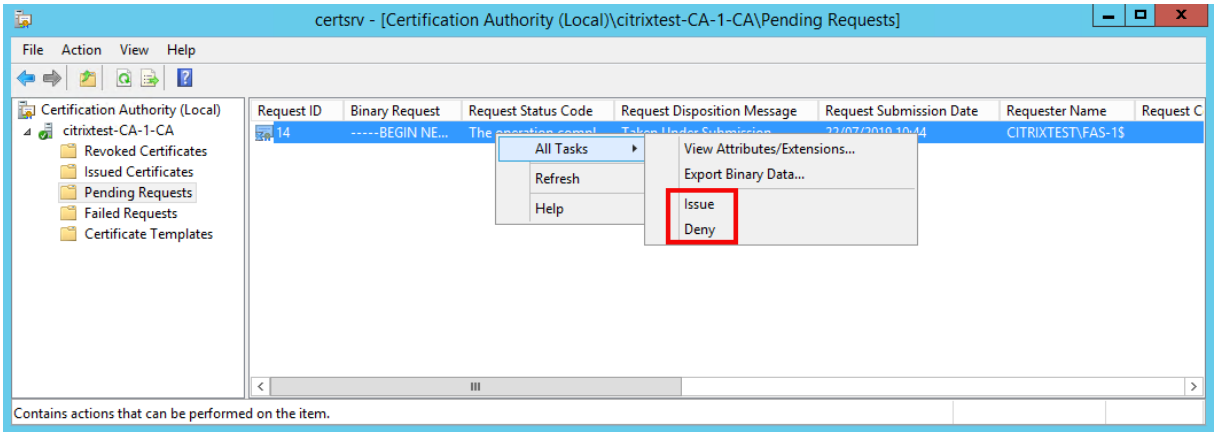



Nachdem die Anforderung gesendet wurde, wird sie in der Liste **Ausstehende Anforderungen** der Microsoft-Zertifizierungsstellenkonsole als ausstehende Anforderung des FAS-Maschinenkontos angezeigt. Der Administrator der Zertifizierungsstelle muss die Anforderung ausstellen oder ablehnen, damit die Konfiguration des FAS fortgesetzt werden kann.

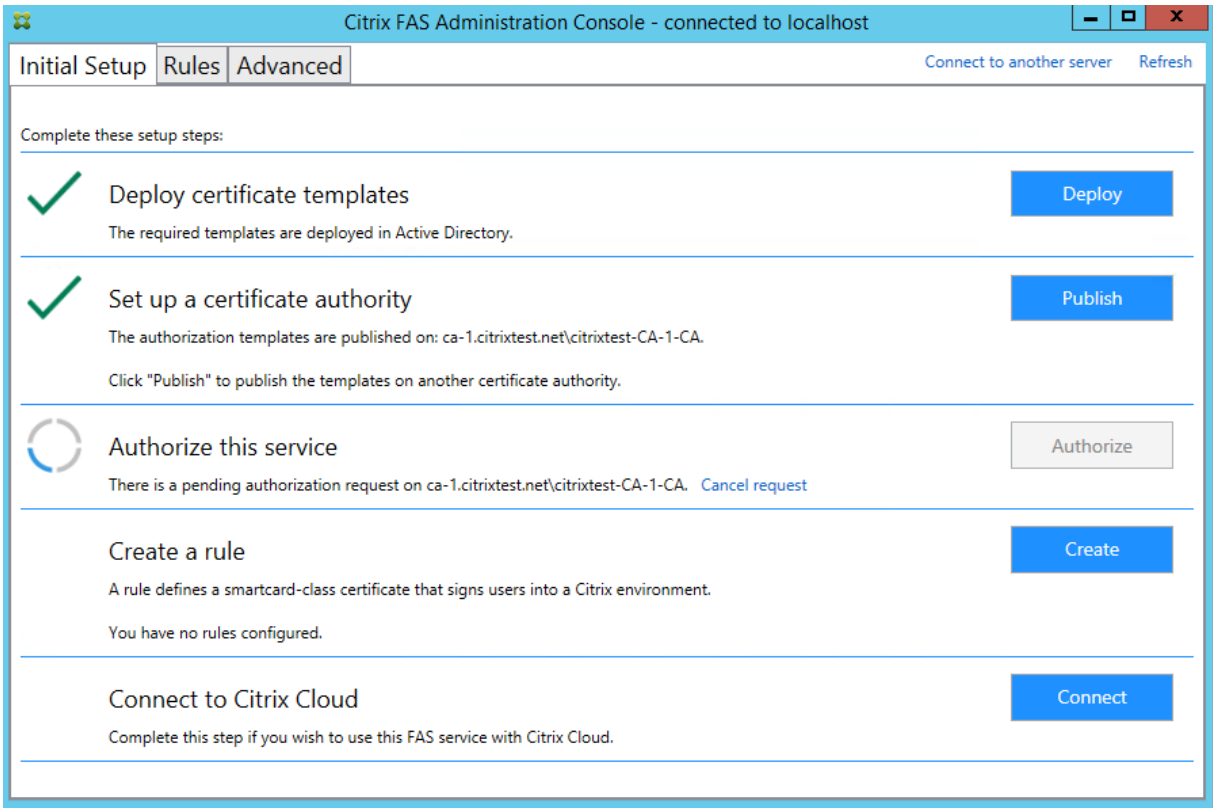
Die FAS-Verwaltungskonsole zeigt ein Drehfeld an, bis der Administrator **Ausstellen** oder **Verweigern** wählt.

Klicken Sie in der Konsole der Microsoft-Zertifizierungsstelle mit der rechten Maustaste auf **Alle Tasks** und wählen Sie für die Zertifikatsanforderung **Ausstellen** oder **Verweigern**. Wenn Sie **Ausstellen** wählen, zeigt die FAS-Verwaltungskonsole das Autorisierungszertifikat an. Wenn Sie **Verweigern** wählen, zeigt die Konsole eine Fehlermeldung an.




Die FAS-Verwaltungskonsole erkennt automatisch, wenn dieser Prozess abgeschlossen ist. Er kann einige Minuten dauern.




## Konfigurieren von Regeln

Der Verbundauthentifizierungsdienst (FAS) verwendet Regeln, um die Ausstellung von Zertifikaten für VDA-Anmeldungen und -Sitzungen nach Vorgabe von StoreFront zu autorisieren.

Jede Regel spezifiziert Folgendes:

- StoreFront-Server, denen zum Zweck des Anforderns der Zertifikate vertraut wird.

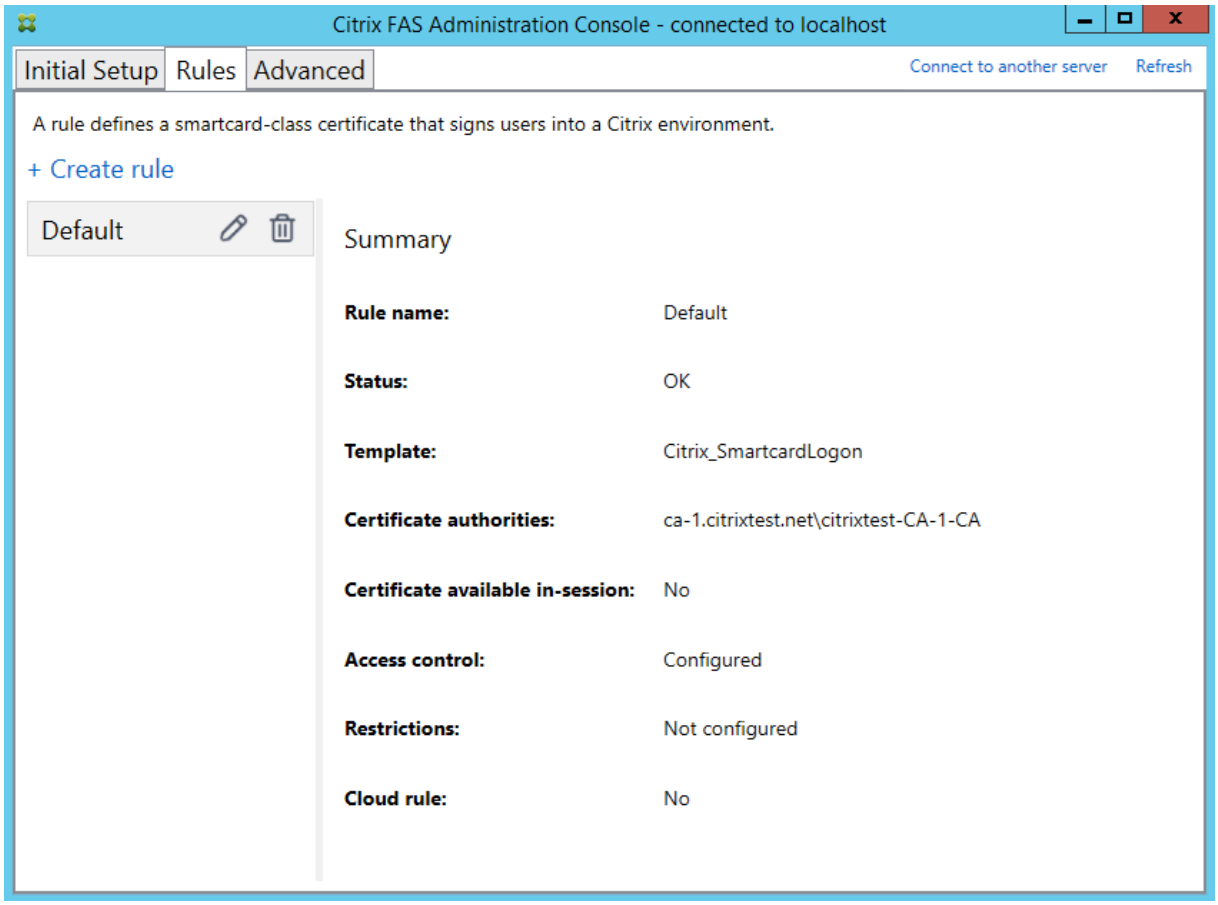
 

- Gruppe von Benutzern, für die die Zertifikate angefordert werden können.
- Gruppe von VDA-Maschinen, die die Zertifikate verwenden dürfen.

Citrix empfiehlt, eine Regel mit dem Namen "default"zu erstellen, da StoreFront bei der Kontaktaufnahme mit dem FAS eine Regel dieses Namens anfordert.

Sie können weitere benutzerdefinierte Regeln erstellen, um auf verschiedene Zertifikatvorlagen und Zertifizierungsstellen zu verweisen und für sie unterschiedliche Eigenschaften und Berechtigungen zu konfigurieren. Diese Regeln können für die Verwendung durch verschiedene StoreFront-Server oder von Workspace konfiguriert werden. Konfigurieren Sie die StoreFront-Server so, dass die benutzerdefinierte Regel über den Namen angefordert wird. Verwenden Sie dazu die Konfigurationsoptionen für die Gruppenrichtlinien.

Klicken Sie auf der Registerkarte "Rules"auf **Create** (oder **Create Rules**), um den Assistenten zur Regelerstellung zu starten, der Informationen zum Erstellen der Regel sammelt. Die Registerkarte "Rules" zeigt eine Zusammenfassung der einzelnen Regeln.




Der Assistent erfasst die folgenden Informationen:

**Template**: Die Zertifikatvorlage, die zum Ausstellen von Benutzerzertifikaten verwendet wird. Dies muss die Vorlage Citrix_SmartcardLogon oder eine modifizierte Kopie sein (siehe Zertifikatvorlagen).

**Certificate Authority**: Die Zertifizierungsstelle, die Benutzerzertifikate ausstellt und die Vorlage veröffentlicht. Für Failover und Lastausgleich können mehrere Zertifizierungsstellen hinzugefügt werden. Stellen Sie sicher, dass der Status für die gewählte Zertifizierungsstelle "Template available" anzeigt. Siehe Zertifizierungsstellenverwaltung.

**In-Session Use**: Mit der Option **Allow in-session use** legen Sie fest, ob ein Zertifikat nach der Anmeldung am VDA verwendet werden kann.

- **Allow in-session use** nicht ausgewählt (Standardeinstellung, *empfohlen*): Das Zertifikat wird nur für das Anmelden oder Wiederverbinden verwendet, und Benutzer haben nach der Authentifizierung keinen Zugriff auf das Zertifikat.
- **Allow in-session use** ist ausgewählt: Benutzer haben nach der Authentifizierung Zugriff auf das Zertifikat. Die meisten Kunden dürfen diese Option nicht wählen. Auf Ressourcen wie Intranet-Websites oder Datenfreigaben, auf die innerhalb der VDA-Sitzung zugegriffen wird, kann mit Kerberos Single Sign-On zugegriffen werden. Daher ist hier kein sitzungsinternes Zertifikat erforderlich.

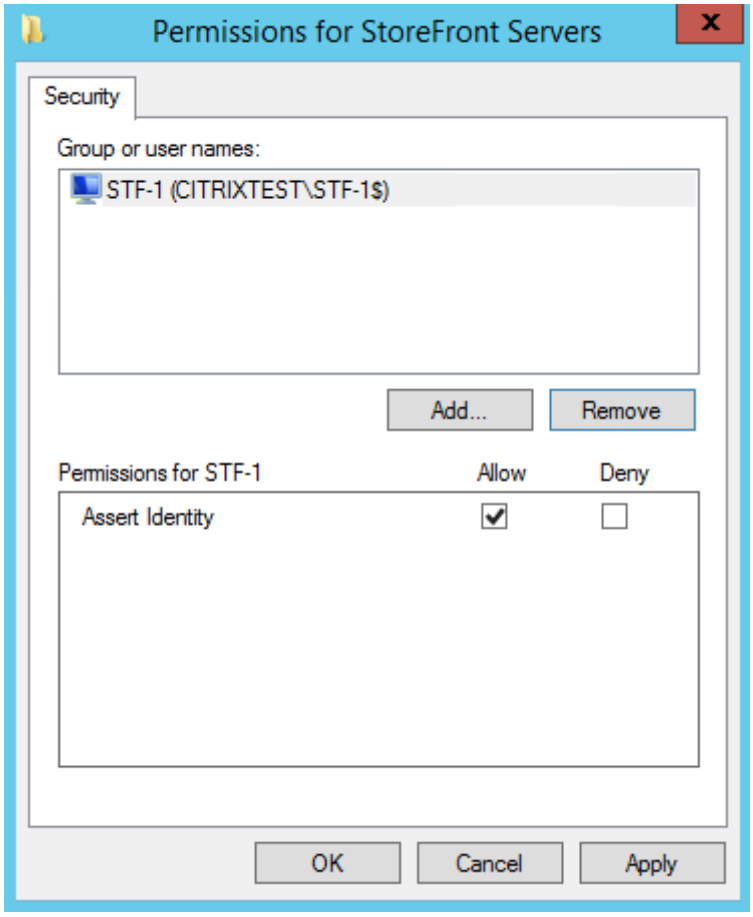
  Wenn Sie **Allow in-session use** auswählen, muss die Gruppenrichtlinie In-session Behavior auch aktiviert und auf den VDA angewendet werden. Zertifikate werden dann nach der Anmeldung eines Benutzers in dessen persönlichem Zertifikatspeicher abgelegt. Ein Zertifikat kann dann beispielsweise von Internet Explorer verwendet werden, wenn innerhalb der VDA-Sitzung eine TLS-Authentifizierung bei Webservern erforderlich ist.

**Access control**: Liste der vertrauenswürdigen StoreFront-Servermaschinen, die Zertifikate für die Anmeldung oder Wiederverbindung von Benutzern anfordern dürfen. Für all diese Berechtigungen können Sie einzelne AD-Objekte oder Gruppen hinzufügen.

> **Wichtig:**
>
> Die Einstellung **Access control** ist sicherheitsrelevant und muss mit großer Sorgfalt gewählt werden.
>
> **Hinweis:**
>
> Wenn Sie den FAS-Server nur mit Citrix Cloud verwenden, müssen Sie "Access control"nicht konfigurieren. Wenn eine Regel von Citrix Cloud verwendet wird, werden die StoreFront-Zugriffsberechtigungen ignoriert. Sie können dieselbe Regel mit Citrix Cloud und mit einer On-Premises-StoreFront-Bereitstellung verwenden. StoreFront-Zugriffsberechtigungen werden auch dann angewendet, wenn die Regel von einem On-Premises-StoreFront genutzt wird.

Die Standardberechtigung ("Assert Identity"zugelassen) verweigert alles. Daher müssen Sie Ihre StoreFront-Server explizit zulassen.

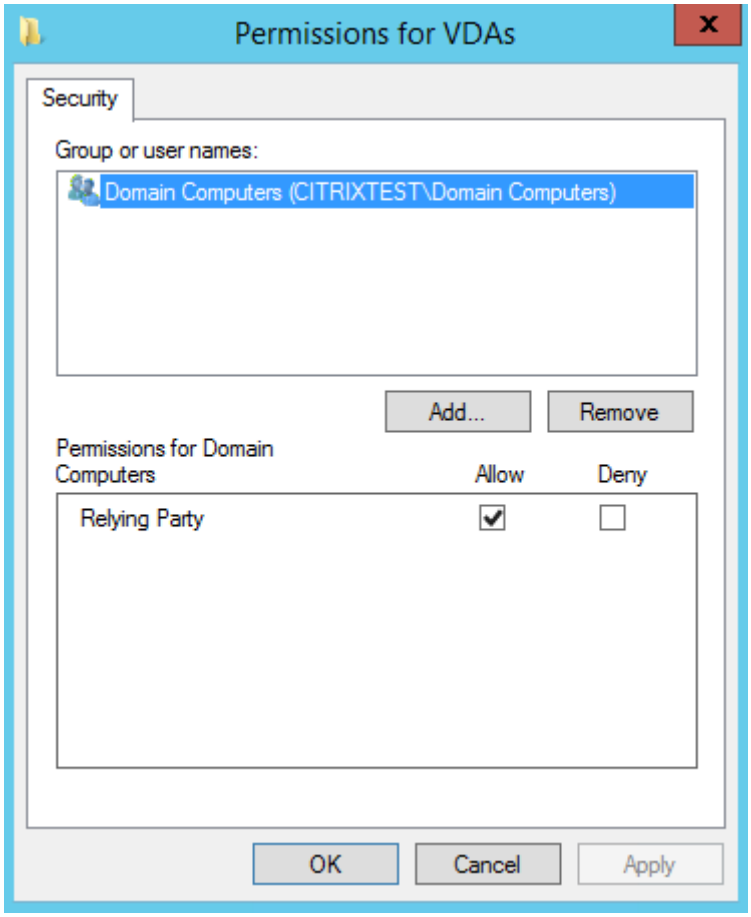



**Restrictions**: Liste der VDA-Maschinen, die Benutzer über den FAS anmelden können, und die Liste der Benutzer, für die Zertifikate über den FAS ausgestellt werden können.

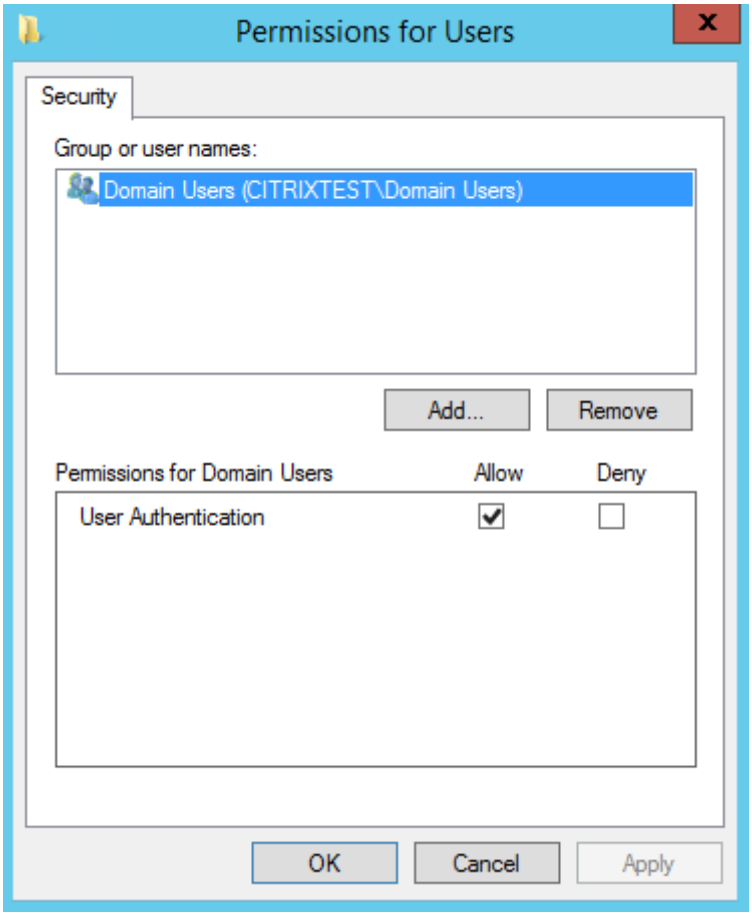
- Mit **Manage VDA permissions** können Sie angeben, auf welchen VDAs Benutzer sich über den FAS anmelden können. Die Liste der VDAs wird standardmäßig auf "Domain Computers"festgelegt.
- Mit **Manage user permissions** können Sie angeben, welche Benutzer sich über den FAS bei einem VDA anmelden können. Die Liste der Benutzer wird standardmäßig auf "Domain Users" festgelegt.

> **Hinweis:**
>
> Wenn die Domäne des FAS-Servers sich von der Domäne der VDAs und Benutzer unterscheidet, müssen die Standardeinschränkungen geändert werden.

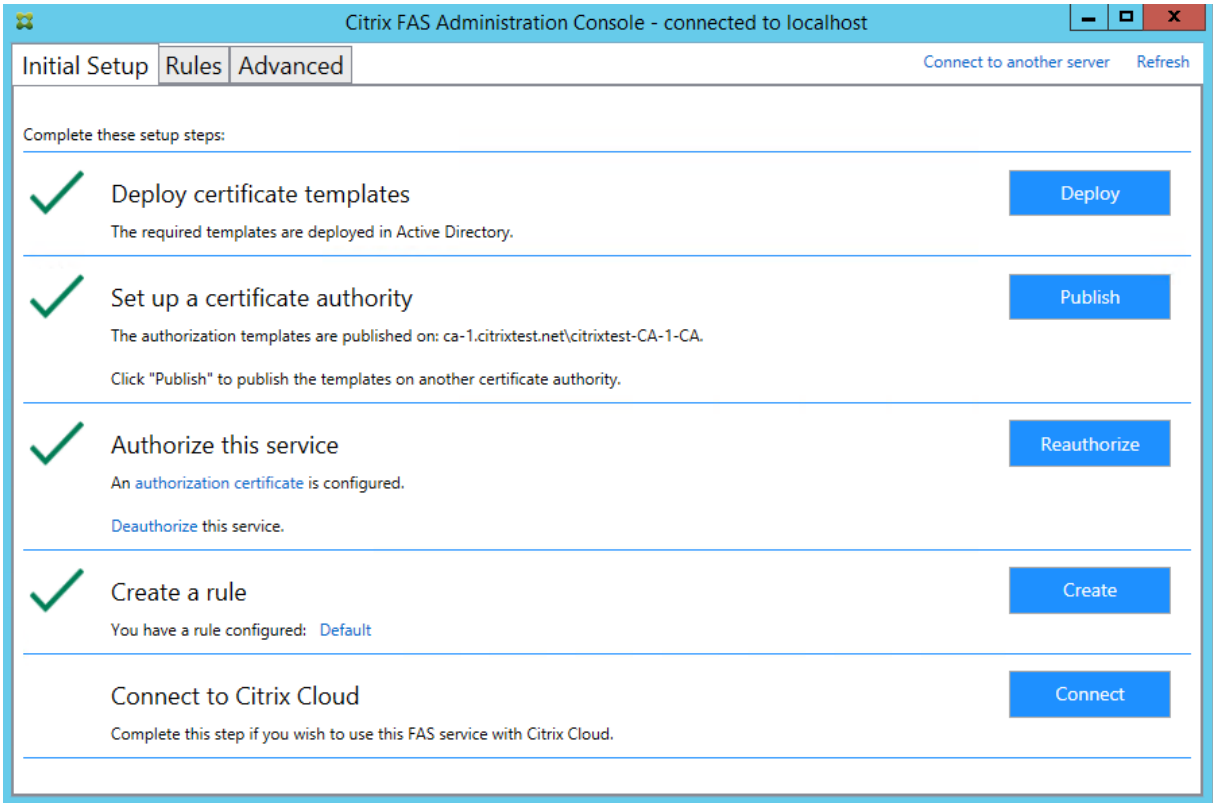





**Cloud rule**: Gibt an, ob die Regel angewendet wird, wenn Identitätsassertions von Citrix Workspace empfangen werden. Wenn Sie eine Verbindung mit Citrix Cloud herstellen, wählen Sie aus, welche Regel für Citrix Cloud zu verwenden ist. Nach dem Verbinden mit Citrix Cloud können Sie die Regel auch über einen Link im Abschnitt **Connect to Citrix Cloud** ändern.

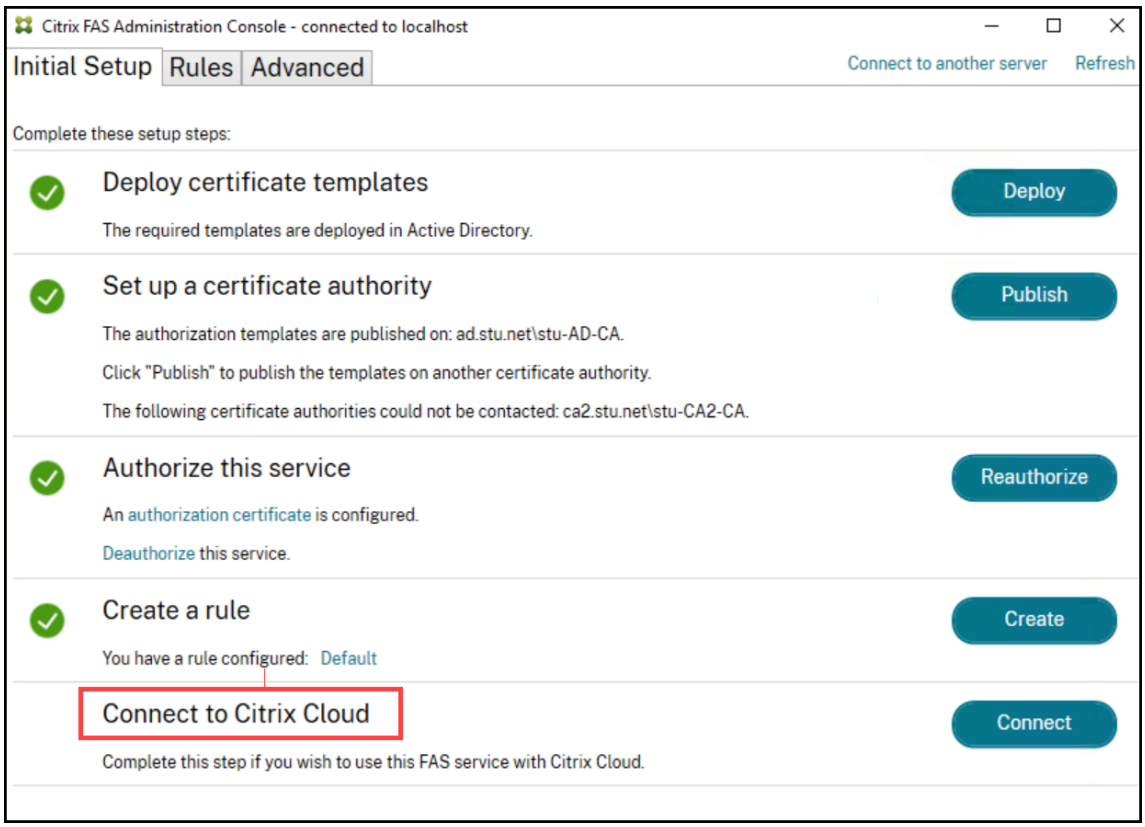



### Verbindung mit Citrix Cloud herstellen

Sie können den FAS-Server über Citrix Workspace mit Citrix Cloud verbinden. Weitere Informationen bietet dieser Citrix Workspace Artikel.

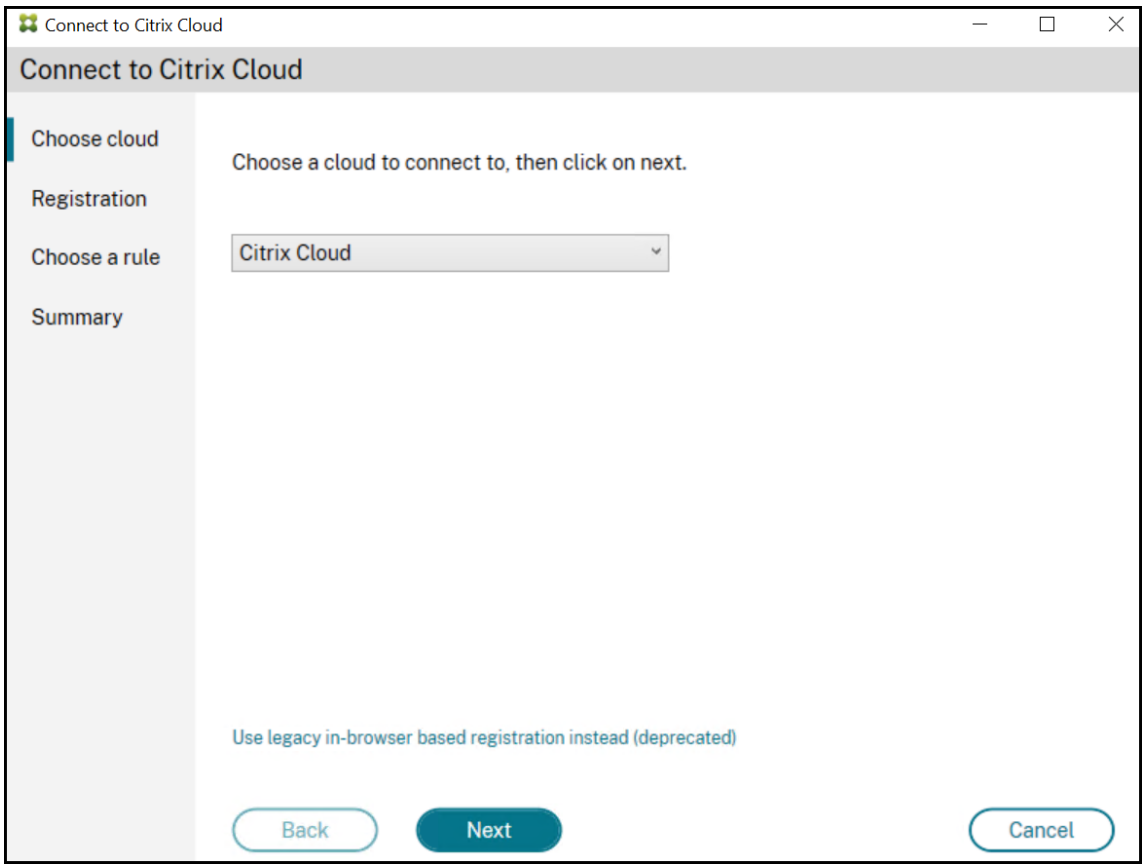
1. Klicken Sie auf der Registerkarte für die Ersteinrichtung unter **Connect to Citrix Cloud** auf **Connect**.




2. Wählen Sie die Cloud aus, mit der Sie sich verbinden möchten, und klicken Sie auf **Weiter**.

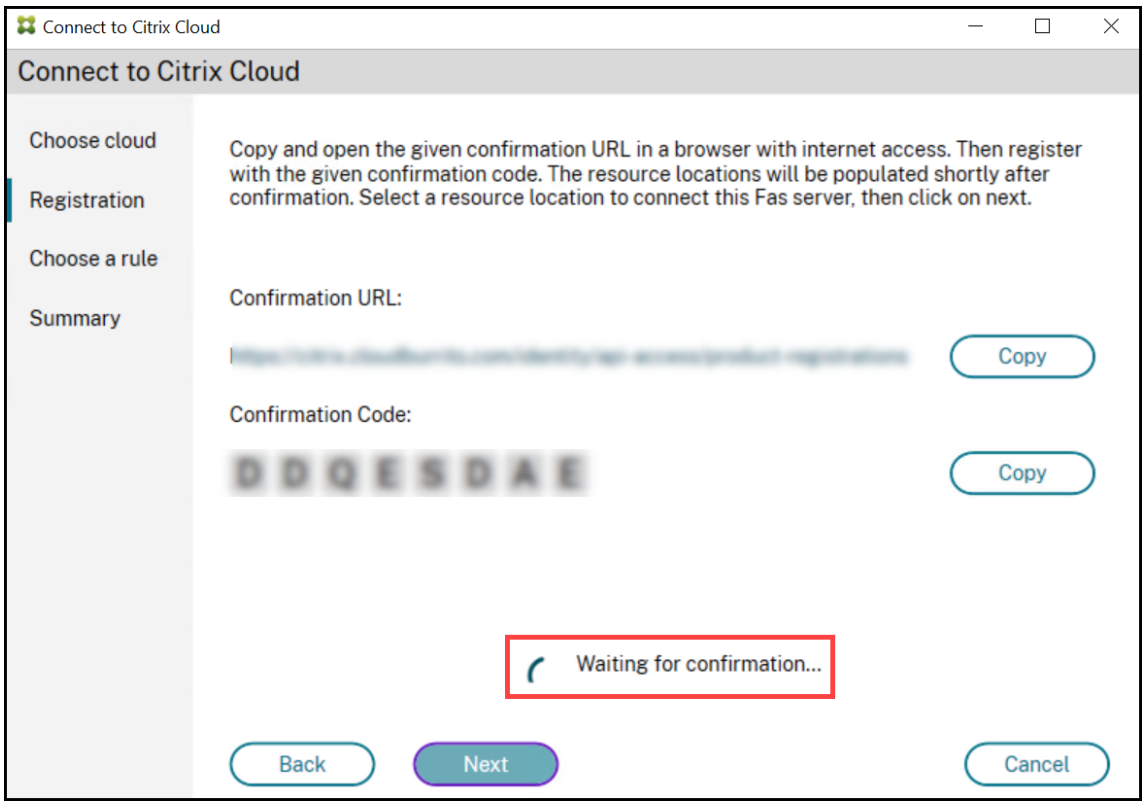
 




> **Hinweis**
>
> In der Vorschau ist nur **Citrix Cloud** verfügbar.

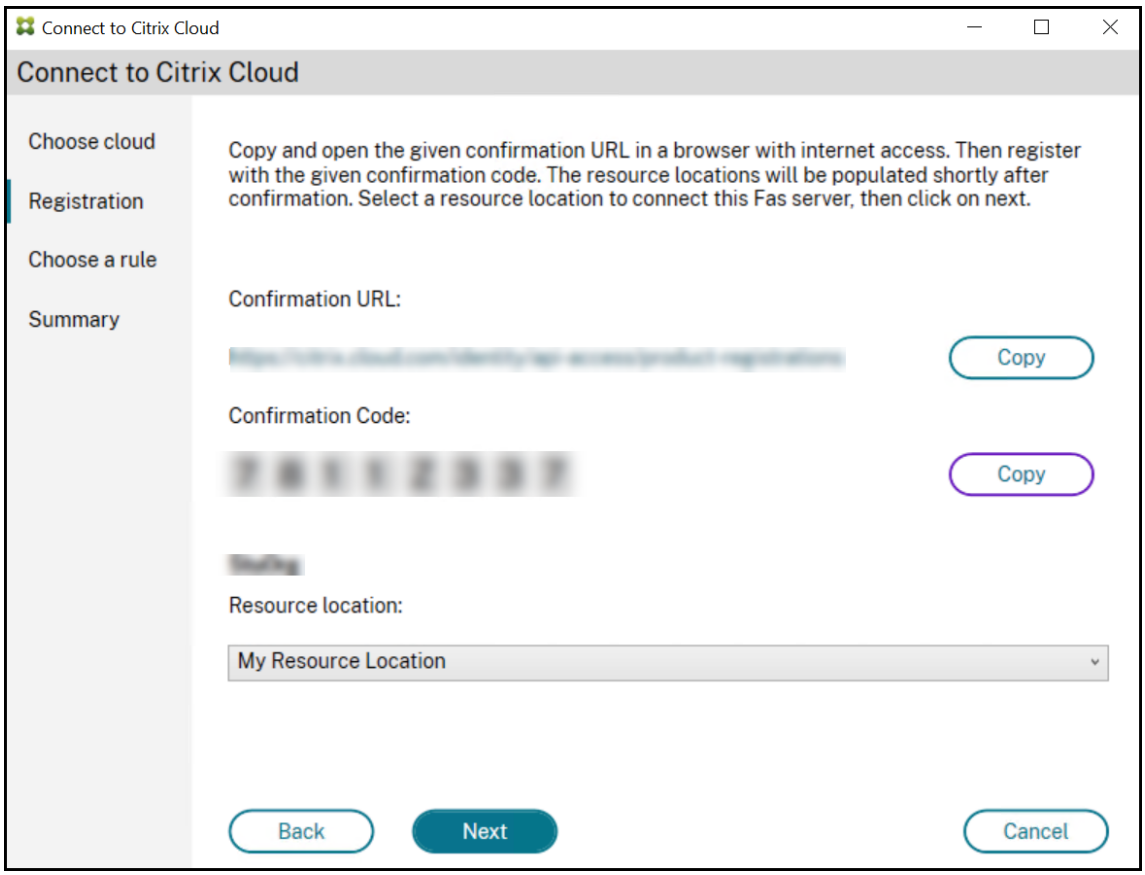
3. Das Fenster zeigt einen eindeutigen Registrierungscode an, der in Citrix Cloud genehmigt werden muss. Weitere Informationen finden Sie unter Registrieren von On-Premises-Produkten bei Citrix Cloud.



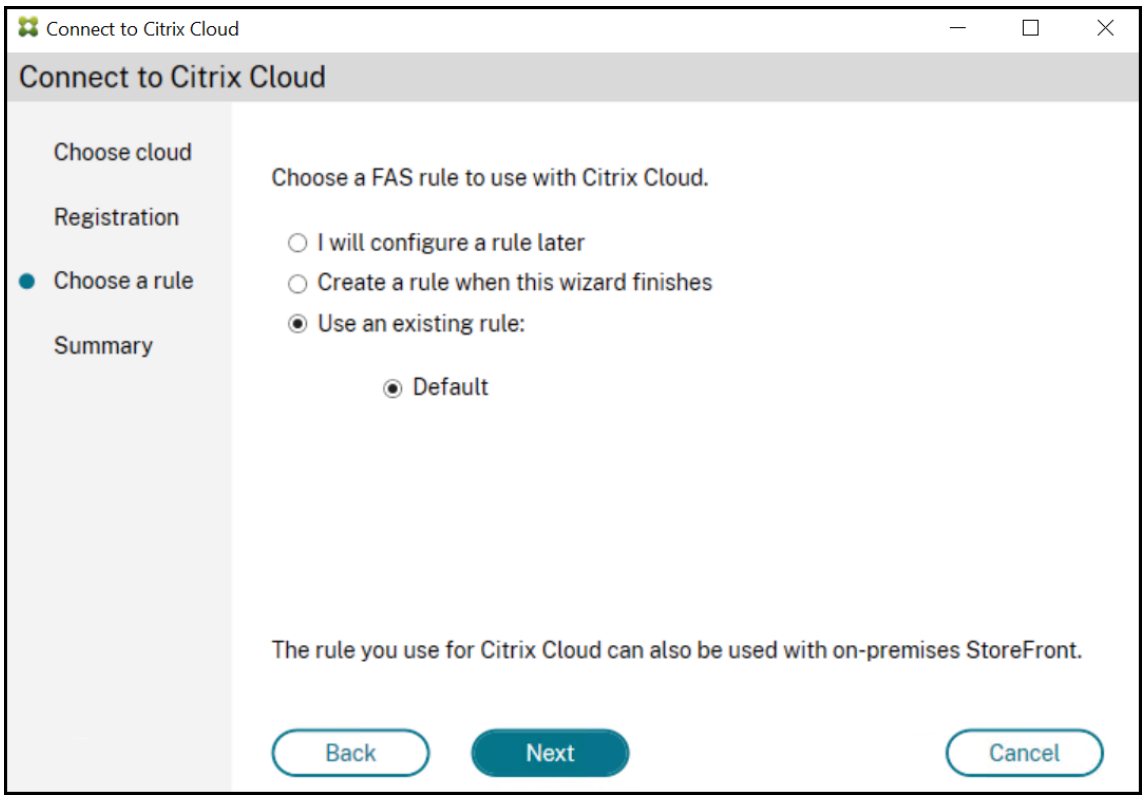

4. Wählen Sie nach der Bestätigung des Registrierungscodes den erforderlichen **Ressourcenstandort** aus der Dropdownliste.

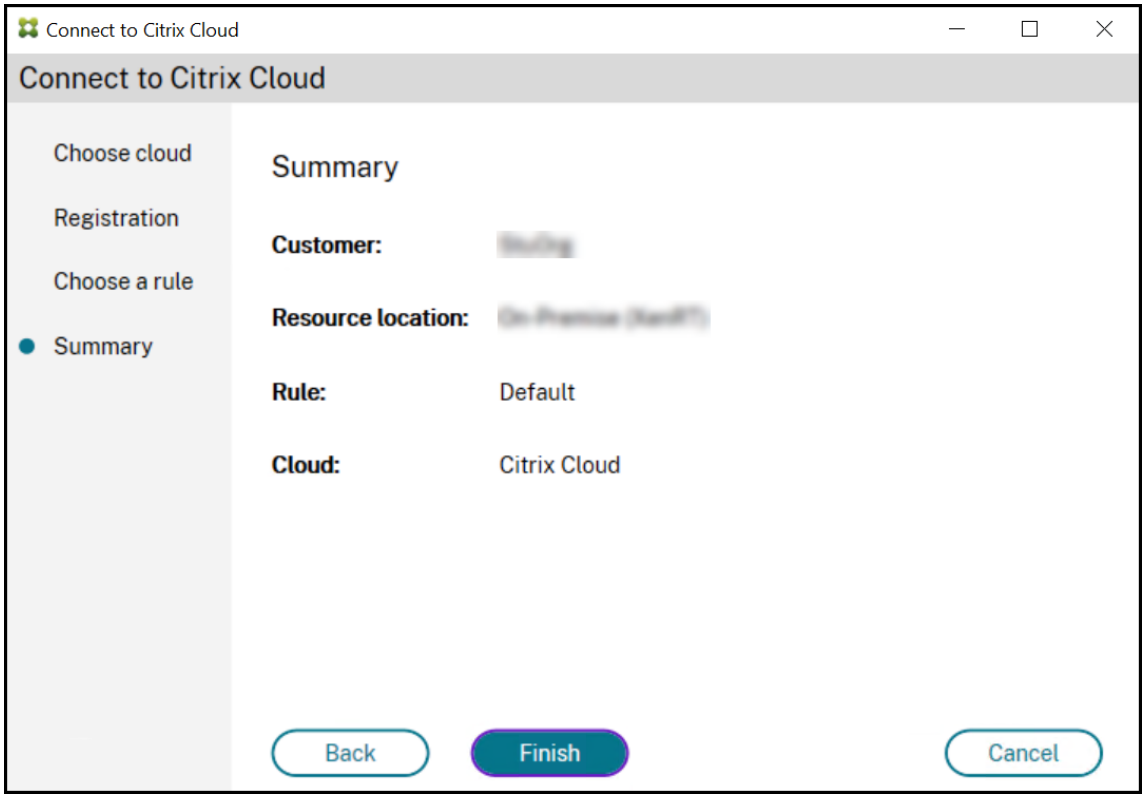



5. Wählen Sie ggf. das Kundenkonto und dann den Ressourcenstandort, an dem Sie den FAS-Server verbinden möchten. Klicken Sie auf **Continue** und schließen Sie das Bestätigungsfenster.
6. Verwenden Sie im Abschnitt **Choose a rule** eine vorhandene Regel, oder erstellen Sie eine Regel. Klicken Sie auf **Weiter**.




7. Klicken Sie auf der Registerkarte **Summary** auf **Finish**, um die Citrix Cloud-Verbindung herzustellen.



Citrix Cloud registriert den FAS-Server und zeigt ihn in Ihrem Citrix Cloud-Konto auf der Seite “Ressourcenstandorte”an.

> Hinweis
>
> Ein On-Premises-FAS-Server kann Benutzerzertifikate ausstellen, um den gleichzeitigen Zugriff auf Citrix Cloud und Citrix Virtual Apps and Desktops zu ermöglichen.

#### Trennen der Verbindung mit Citrix Cloud

Nachdem Sie den FAS-Server wie in diesem Citrix Workspace-Artikel beschrieben aus Ihrem Citrix Cloud-Ressourcenstandort entfernt haben, wählen Sie unter **Connect to Citrix Cloud** den Befehl **Disable**.

## Erweiterte Konfiguration

September 11, 2024

Die Anleitungen in diesem Abschnitt erläutern Konfiguration und Verwaltung des Verbundauthentifizierungsdiensts (FAS):

### Verwandte Informationen

- Primäre Referenz für die Installation und Ersteinrichtung des FAS ist der Artikel Installation und Konfiguration.
- Der Artikel Bereitstellungsarchitekturen enthält eine Übersicht über die gebräuchlichsten FAS-Architekturen sowie Links zu Artikeln über komplexere Architekturen.

## Verbundauthentifizierungsdienst für einen Mandantenkunden aktivieren

September 11, 2024

In diesem Artikel wird beschrieben, wie Sie den Verbundauthentifizierungsdienst (FAS) in Umgebungen mit Managed Service Provider (MSP) aktivieren. Weitere Informationen finden Sie unter Reference Architecture: Citrix Service Provider DaaS.

### Voraussetzungen

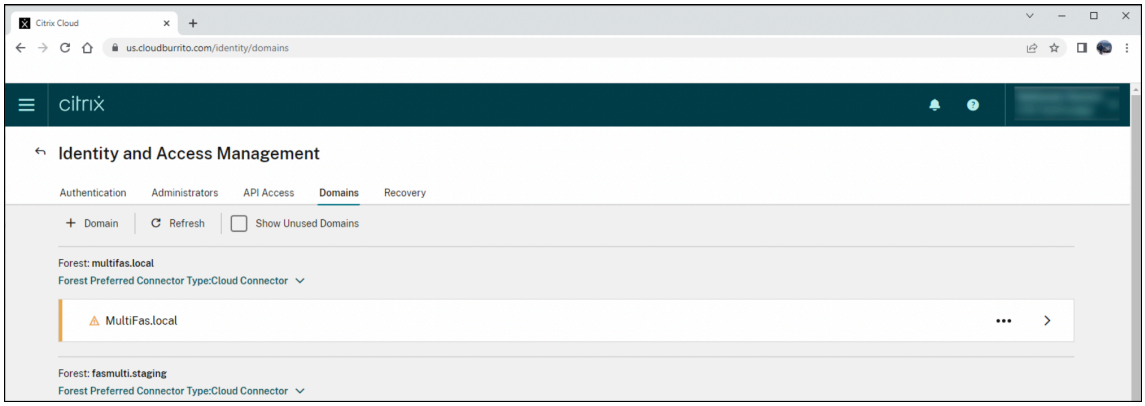
- Sie haben Administratorzugriff auf Domänen und Ressourcenstandort in Citrix Cloud. Weitere Hinweise finden Sie unter Ändern von Administratorberechtigungen.
- Sie haben eine Mandanten-MSP-Beziehung eingerichtet. Weitere Informationen finden Sie unter Citrix DaaS für Citrix Service Provider.

### MSP-Kunden konfigurieren

1. Verwenden Sie einen Cloud Connector, um Active Directory-Domänen für Citrix Cloud verfügbar zu machen.

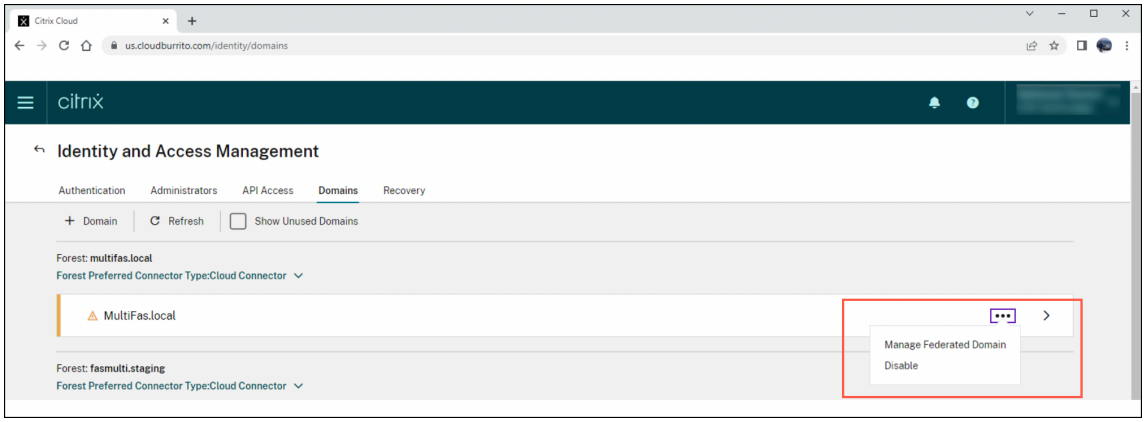
   Installieren Sie Cloud Connectors, um die On-Premises-Infrastruktur mit der Citrix Cloud zu verbinden.

   Überprüfen Sie unter **Identitäts- und Zugriffsverwaltung** > **Domänen**, ob die dem On-Premises-Domänencontroller zugeordneten Domänen verfügbar sind.



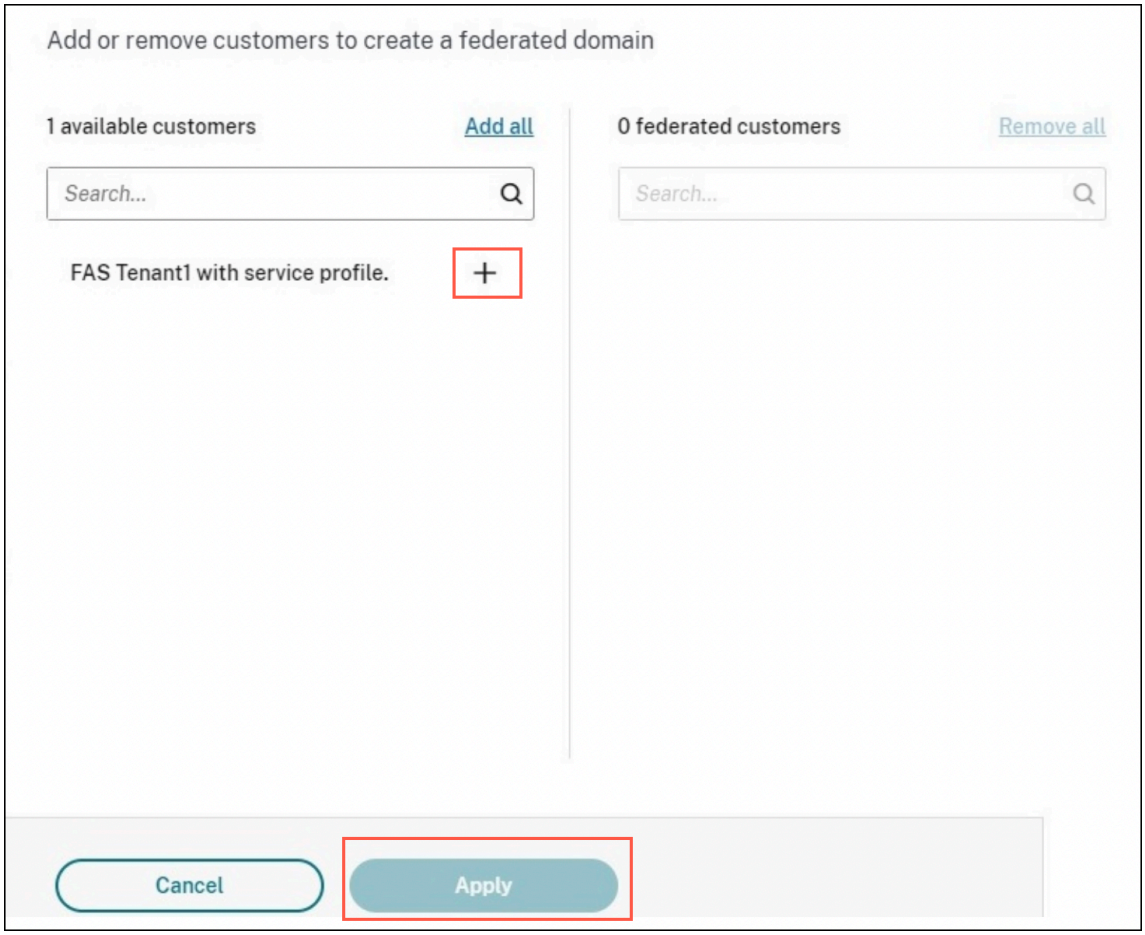

2. Stellen Sie einen Verbund zwischen Domäne und Mandanten her.

   Wählen Sie die Domäne aus, klicken Sie auf das Dropdownmenü (...) und klicken Sie auf **Verbunddomäne verwalten**.



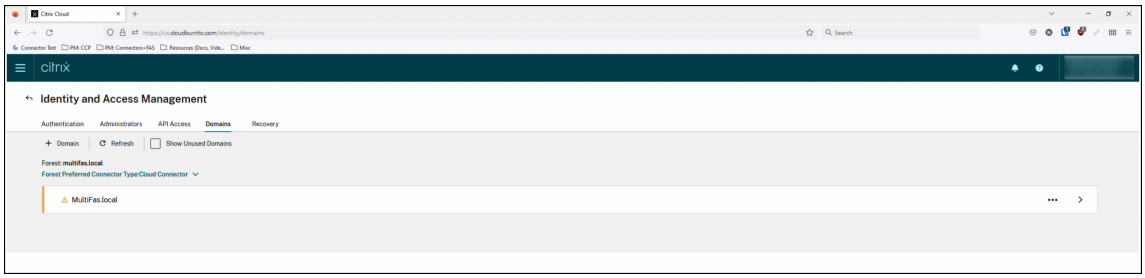

 

Suchen Sie den Mandanten und klicken Sie auf **+**. Klicken Sie dann auf **Anwenden**.




3. Stellen Sie sicher, dass die zugeordneten Domänen im Mandanten vorhanden sind.

   Dieser Schritt ist optional. Melden Sie sich bei der Konsole für die Mandantenkunden an und stellen Sie sicher, dass die Domänen unter **Identitäts- und Zugriffsverwaltung** > **Domänen** aufgeführt sind.




   Kehren Sie zum MSP-Kunden zurück.

4. Installieren und registrieren Sie einen FAS-Server bei Citrix Cloud.

   Installieren Sie den Verbundauthentifizierungsdienst (FAS) in der Active Directory (AD)-Gesamtstruktur, in der auch die Citrix Virtual Apps and Desktops-Ressourcen des Mandanten

sind. Verbinden Sie FAS mit dem Cloud-Ressourcenstandort, der der AD-Gesamtstruktur zugeordnet ist. Informationen zur Installation eines FAS-Servers finden Sie unter Installieren und Konfigurieren.

5. Mandantenkunden konfigurieren

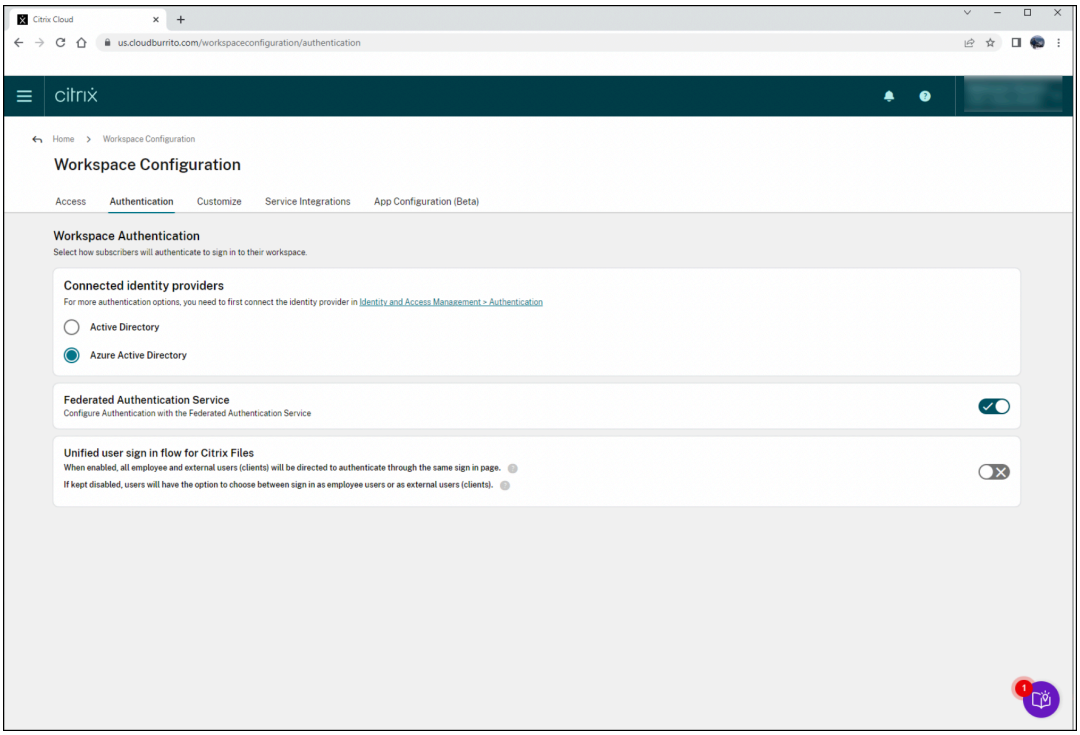
   FAS für den Mandantenkunden aktivieren

   - Identitätsanbieter (IdP) konfigurieren

     Wechseln Sie zum Mandantenkunden. Gehen Sie zu **Identitäts- und Zugriffsverwaltung** > **Authentifizierung**. Stellen Sie eine Verbindung zum IdP her und stellen Sie sicher, dass AD mit dem IdP synchronisiert ist.

   - FAS für einen Mandanten aktivieren

     Gehen Sie zu **Workspacekonfiguration** > **Authentifizierung**. Wählen Sie die von Ihnen eingerichtete Authentifizierung und aktivieren Sie FAS.




## Bekanntes Problem

Es gibt ein bekanntes Problem beim Löschen einer MSP-Domäne vor dem Entfernen der Verbunddomänen für Mandanten. Sie können FAS weiterhin für Mandanten aktivieren, FAS schlägt jedoch fehl, da die Domäne für MSP nicht mehr existiert.

## Single Sign-On mit Azure Active Directory

September 11, 2024

Der Citrix Verbundauthentifizierungsdienst (Federated Authentication Service, FAS) ermöglicht einen Single Sign-On für domänengebundene Virtual Delivery Agents (VDAs). Hierfür erhält der VDA von FAS ein Benutzerzertifikat und authentifiziert damit den Benutzer gegenüber Active Directory (AD). Sobald Sie sich bei der VDA-Sitzung angemeldet haben, können Sie dann ohne erneute Authentifizierung auf AD-Ressourcen zugreifen.

Es ist üblich, Azure Active Directory (AAD) mit Synchronisierung zwischen Ihrem AD und AAD zu implementieren, wodurch Hybrididentitäten für Benutzer und Maschinen entstehen. In diesem Artikel wird beschrieben, welche zusätzliche Konfiguration bei Verwendung von FAS erforderlich ist, um sich aus der VDA-Sitzung heraus per Single Sign-On bei AAD anzumelden und auf AAD-geschützte Anwendungen zuzugreifen, ohne sich erneut zu authentifizieren.

> **Hinweis:**
>
> - Sie benötigen keine spezielle FAS-Konfiguration, um Single Sign-On für AAD zu verwenden.
> - Sie benötigen keine sitzungsinternen Zertifikate für FAS.
> - Sie können jede beliebige Version von FAS verwenden.
> - Sie können jede VDA-Version verwenden, die FAS unterstützt.

Die Verfahren für den Single Sign-On für AAD sind in der folgenden Tabelle zusammengefasst:

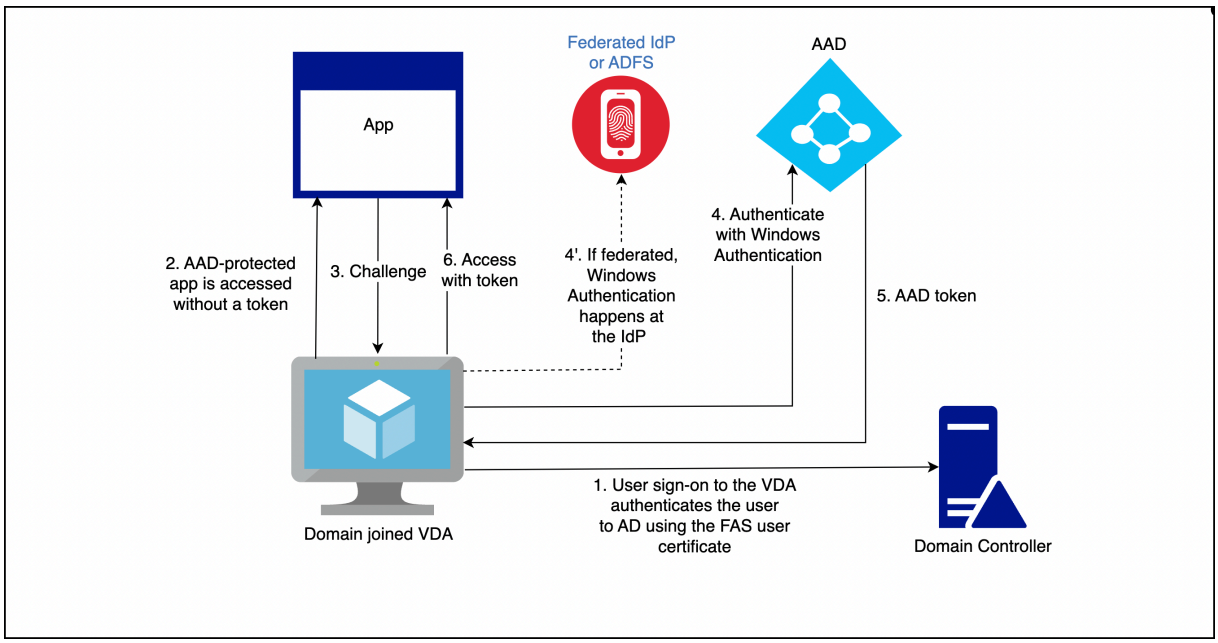
| AAD-Authentifizierungstyp | VDA ist domänengebunden | VDA mit Hybrideinbindung |
|---|---|---|
| Verwaltet | Seamless SSO AAD verwenden | AAD-zertifikatbasierte Authentifizierung verwenden |
| Verbunden mit Active Directory-Verbunddienste (AD FS) | Windows-Authentifizierung bei AD FS aktivieren | Sicherstellen, dass der WS-Trust-Endpunkt *certificatemixed* aktiviert ist |
| Verbunden mit einem externen Identitätsanbieter | Drittanbieter-Lösung verwenden | Drittanbieter-Lösung verwenden |

- Eine verwaltete AAD-Domäne ist eine Domäne, in der die Benutzerauthentifizierung bei AAD erfolgt. Dies wird auch als “native AAD-Authentifizierung”bezeichnet.
- Eine verbundene AAD-Domäne ist eine Domäne, in der AAD so konfiguriert ist, dass die Authentifizierung umgeleitet wird und an einem anderen Ort erfolgt. Zum Beispiel bei AD FS oder einem externen Identitätsanbieter.
- Ein VDA mit Hybrideinbindung ist mit AD und mit AAD verbunden.

### Domänengebundene VDAs

Bei domänengebundenen VDAs nutzen Sie Single Sign-On für AAD mittels Windows-Authentifizierung (traditionell als integrierte Windows-Authentifizierung oder Kerberos bezeichnet). Die Authentifizierung bei AAD erfolgt, wenn der Benutzer innerhalb der VDA-Sitzung auf eine AAD-geschützte Anwendung zugreift. Das folgende Diagramm zeigt den allgemeinen Authentifizierungsprozess:




Die genauen Details variieren je nachdem, ob die AAD-Domäne verwaltet oder verbunden ist.

Informationen zum Einrichten der verwalteten AAD-Domäne finden Sie unter Schnellstart: Nahtloses einmaliges Anmelden mit Azure Active Directory.

Bei einer mit AD FS verbundenen AAD-Domäne aktivieren Sie die Windows-Authentifizierung auf dem AD FS-Server.

Bei einer AAD-Domäne, die mit einem externen Identitätsanbieter verbunden ist, gibt es eine ähnliche Lösung. Wenden Sie sich an Ihren Identitätsanbieter, um weitere Hilfe zu erhalten.

> **Hinweis:**
>
> Sie können die aufgeführten Lösungen für domänengebundene VDAs auch für VDAs mit Hybrideinbindung verwenden. Bei Verwendung von FAS wird jedoch kein primärer Aktualisierungstoken (PRT) für AAD generiert.

### VDAs mit Hybrideinbindung

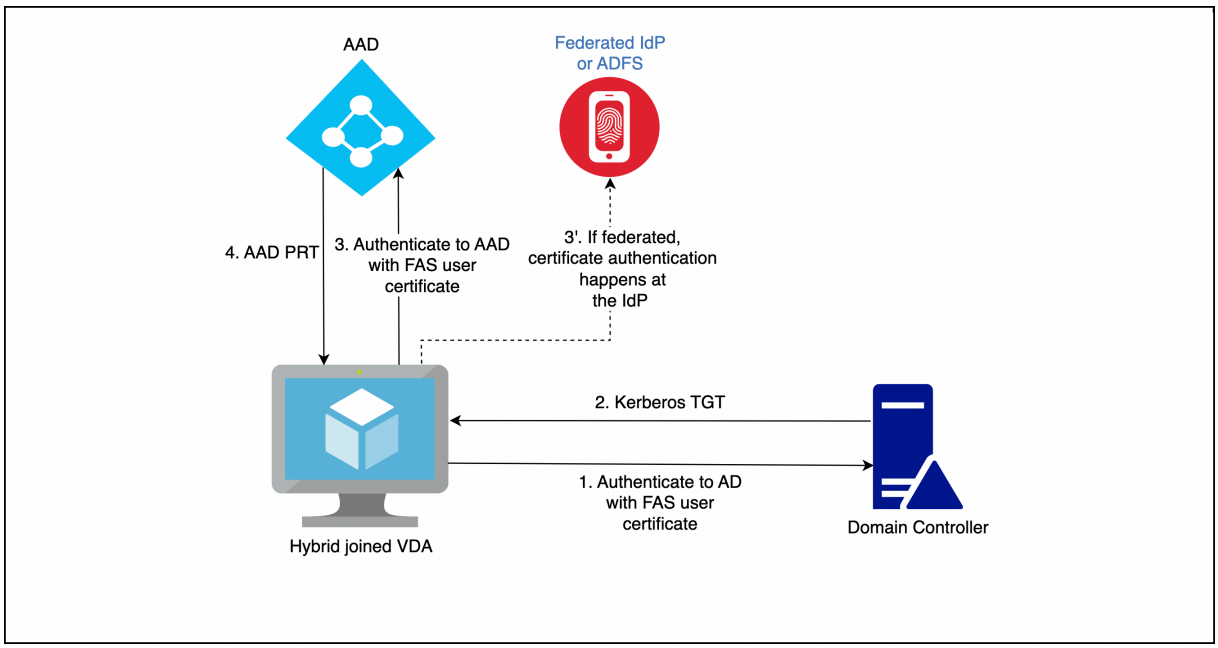
VDAs mit Hybrideinbindung sind gleichzeitig mit AD und AAD verbunden. Wenn der Benutzer sich beim VDA anmeldet, werden folgende Artefakte erstellt:

- Ein Kerberos Ticket Granting Ticket (TGT) zur Authentifizierung bei AD-Ressourcen
- Ein primärer Aktualisierungstoken (PRT) zur Authentifizierung bei AAD-Ressourcen

Der PRT enthält Informationen zum Benutzer und zur Maschine. Diese Informationen werden bei Bedarf in einer AAD-Richtlinie für bedingten Zugriff verwendet.

Da FAS zur Benutzerauthentifizierung ein Zertifikat für den VDA bereitstellt, muss die zertifikatbasierte Authentifizierung für AAD implementiert sein, damit ein PRT erstellt wird. Das folgende Diagramm zeigt den allgemeinen Authentifizierungsprozess:




Die genauen Details variieren je nachdem, ob die AAD-Domäne verwaltet oder verbunden ist.

Bei einer verwalteten AAD-Domäne konfigurieren Sie die zertifikatbasierte AAD-Authentifizierung. Weitere Informationen finden Sie unter Übersicht über die zertifikatbasierte Authentifizierung mit Azure AD. Der VDA verwendet die zertifikatbasierte AAD-Authentifizierung, um den Benutzer mit seinem FAS-Zertifikat bei AAD zu authentifizieren.

> **Hinweis:**
>
> In der Microsoft-Dokumentation wird die Anmeldung mit einem Smartcard-Zertifikat beschrieben; die zugrundeliegende Technik gilt aber auch bei der Anmeldung mit einem FAS-Benutzerzertifikat.

Für eine mit AD FS verbundene AAD-Domäne verwendet der VDA den WS-Trust-Endpunkt *certificatemixed* des AD FS-Servers, um den Benutzer mit seinem FAS-Zertifikat bei AAD zu authentifizieren. Dieser Endpunkt ist standardmäßig aktiviert.

Für eine AAD-Domäne, die mit einem externen Identitätsanbieter verbunden ist, gibt es möglicherweise eine ähnliche Lösung. Der Identitätsanbieter muss einen WS-Trust-Endpunkt *certificatemixed*

implementieren. Wenden Sie sich an Ihren Identitätsanbieter, um weitere Hilfe zu erhalten.

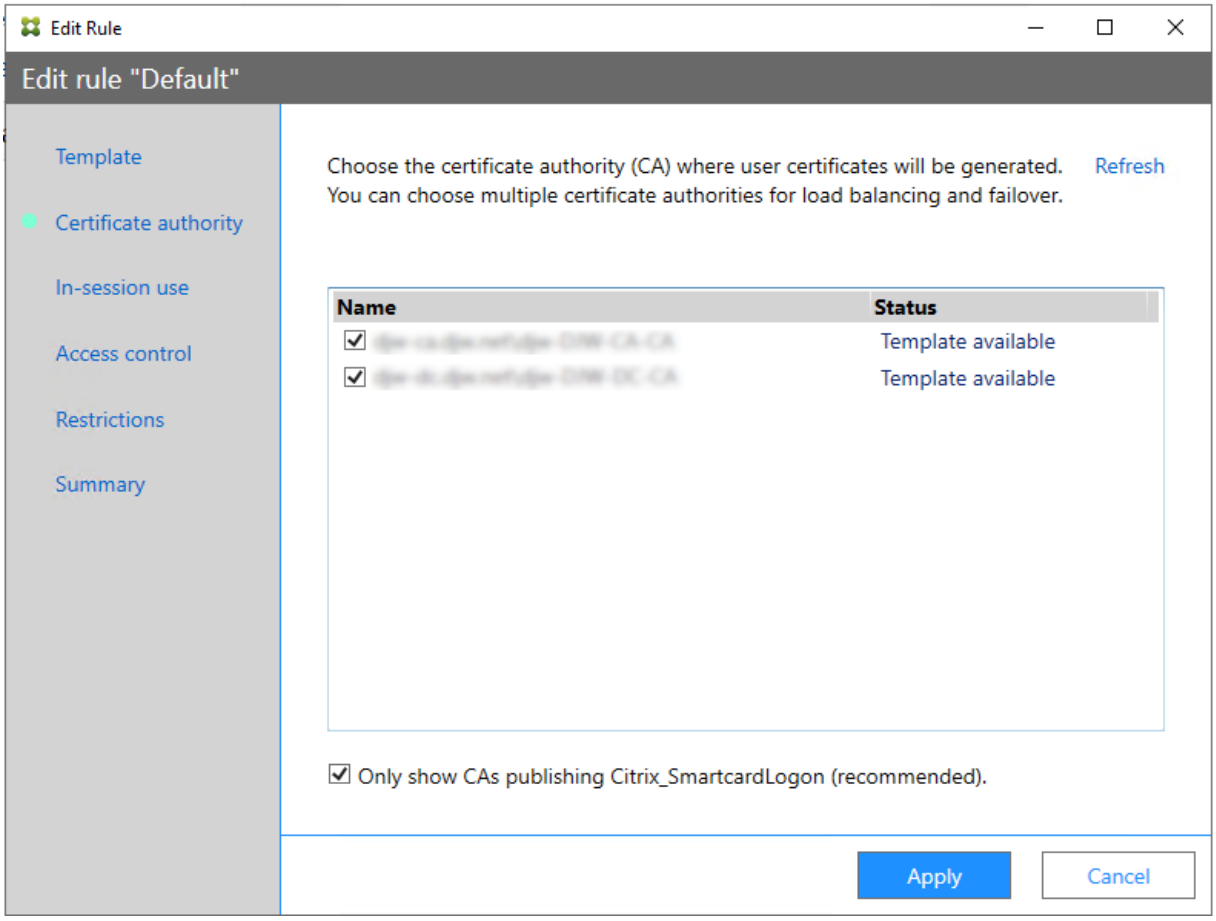
## Konfiguration der Zertifizierungsstelle

September 11, 2024

Dieser Abschnitt beschreibt die erweiterte Konfiguration des Verbundauthentifizierungsdiensts (Federated Authentication Service, FAS) für die Integration mit Zertifizierungsstellenservern. Die meisten dieser Konfigurationen werden von der FAS-Verwaltungskonsole nicht unterstützt. In den Anweisungen werden PowerShell-APIs verwendet, die der Verbundauthentifizierungsdienst bietet. Grundlegende Kenntnisse von PowerShell werden für die Ausführung der Anweisungen in diesem Abschnitt vorausgesetzt.

### Einrichten mehrerer Zertifizierungsstellenserver für die Verwendung im FAS

Sie können mit der FAS-Verwaltungskonsole den Verbundauthentifizierungsdienst mit mehreren Zertifizierungsstellen (ZS) konfigurieren, während Sie eine Regel erstellen oder bearbeiten:



Alle ausgewählten Zertifizierungsstellen müssen die Zertifikatvorlage Citrix_SmartcardLogon veröffentlichen (bzw. die in Ihrer Regel ausgewählte Vorlage).

Wenn eine Zertifizierungsstelle, die Sie verwenden möchten, die gewünschte Vorlage nicht veröffentlicht, führen Sie den Schritt Einrichten einer Zertifizierungsstelle für die Zertifizierungsstelle aus.

> **Hinweis:**
>
> Sie müssen den Schritt Autorisieren dieses Diensts nicht für jede Zertifizierungsstelle ausführen, da das in diesem Schritt konfigurierte Autorisierungszertifikat von allen Zertifizierungsstellen verwendet werden kann.

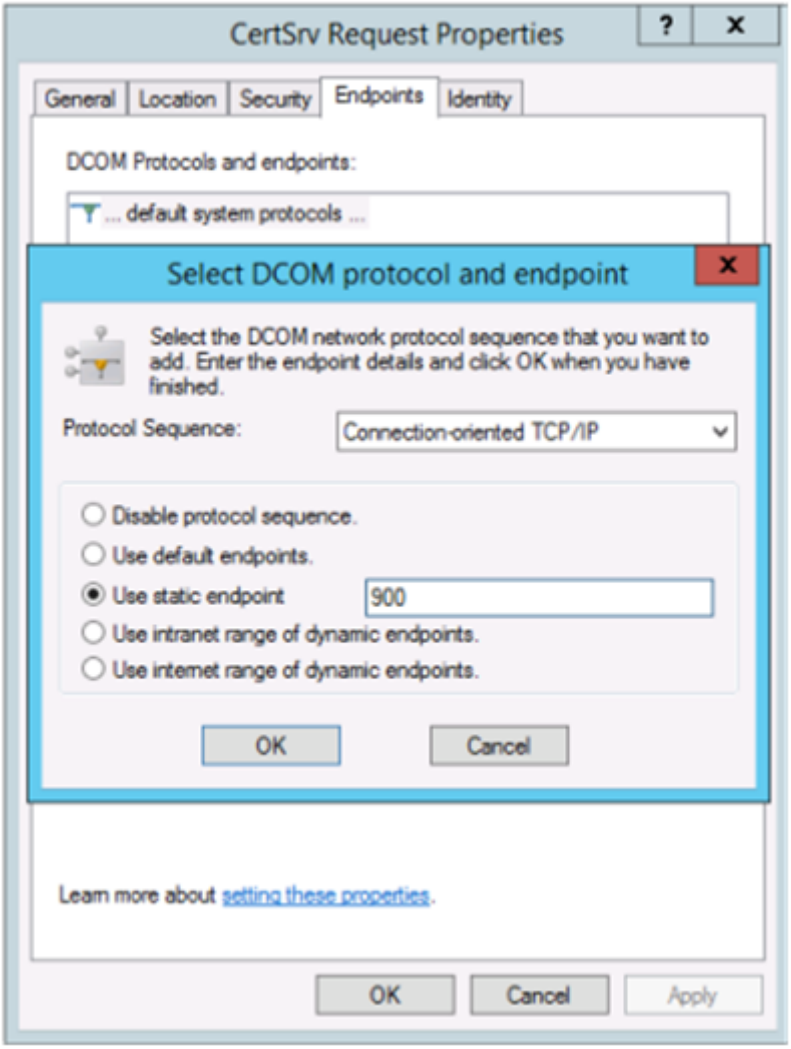
#### Erwartete Verhaltensänderungen

Wenn Sie den FAS-Server mit mehreren Zertifizierungsstellenservern konfiguriert haben, wird die Generierung von Benutzerzertifikaten auf alle konfigurierten Zertifizierungsstellenserver verteilt. Wenn einer der konfigurierten Zertifizierungsstellenserver ausfällt, wechselt der FAS-Server zu einem anderen verfügbaren Zertifizierungsstellenserver.

### Konfigurieren der Microsoft-Zertifizierungsstelle für TCP-Zugriff

Standardmäßig verwendet die Microsoft-Zertifizierungsstelle für den Zugriff DCOM. Beim Implementieren von Firewallsicherheit kann dies sehr komplex sein, daher bietet Microsoft die Möglichkeit, zu einem statischen TCP-Port zu wechseln. Verwenden Sie in der Microsoft-Zertifizierungsstelle **Start > Ausführen > dcomcnfg.exe**, um das DCOM-Konfigurationsfenster zu öffnen. Erweitern Sie *Computer > Arbeitsplatz > DCOM-Konfiguration*, um den Knoten **CertSrv Request** anzuzeigen, und bearbeiten Sie dann die Eigenschaften der Anwendung "CertSrv Request DCOM":




Ändern Sie die Endpunkte, indem Sie einen statischen Endpunkt auswählen, und geben Sie eine TCP-Portnummer ein (900 in der Abbildung oben).

Starten Sie die Microsoft-Zertifizierungsstelle neu und senden Sie eine Zertifikatanforderung. Wenn Sie `netstat –a –n –b` ausführen, müsste certsrv jetzt an Port 900 überwachen:

```
 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
```

Sie brauchen den FAS-Server (bzw. andere Maschinen, die die Zertifizierungsstelle verwenden) nicht zu konfigurieren, da DCOM durch Verwendung des RPC-Ports eine Aushandlungsphase 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. Dadurch wird Port 900 geöffnet

und der DCOM-Server gibt dem FAS-Server Anweisungen zum Herstellen der Verbindung.

### Vorabgenerieren von Benutzerzertifikaten

Die Anmeldung erfolgt für Benutzer erheblich schneller, wenn Benutzerzertifikate im FAS-Server vorab generiert werden. In den folgenden Abschnitten wird die erforderliche Vorgehensweise für einen oder mehrere FAS-Server beschrieben.

#### Abrufen einer Liste der Active Directory-Benutzer

Sie können die Zertifikatgenerierung verbessern, indem Sie eine Liste der Benutzer von Active Directory abrufen und als Datei (z. B. als CSV-Datei) speichern, wie im folgenden Beispiel dargestellt.

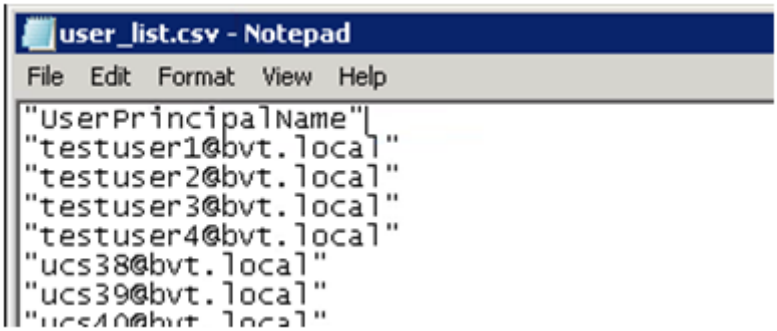
```
Import-Module ActiveDirectory

$searchbase = "cn=users,dc=bvt,dc=local" # AD User Base to Look for
   Users, leave it blank to search all
$filename = "user_list.csv" # Filename to save

if ($searchbase -ne ""){

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

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

Get-ADUser ist ein Standardcmdlet zum Abrufen einer Liste der Benutzer. Das obige Beispiel enthält ein Filterargument, damit nur Benutzer mit einem UserPrincipalName aufgelistet werden, deren Kontostatus “enabled”ist.

Mit dem Argument SearchBase können Sie den Teil von Active Directory einschränken, der nach Benutzern durchsucht wird. Wenn Sie alle Benutzer in AD durchsuchen möchten, lassen Sie das Argument aus. Hinweis: Die Abfrage gibt u. U. eine große Anzahl Benutzer zurück.

Die CSV-Datei sieht wie folgt aus:




**FAS-Server**

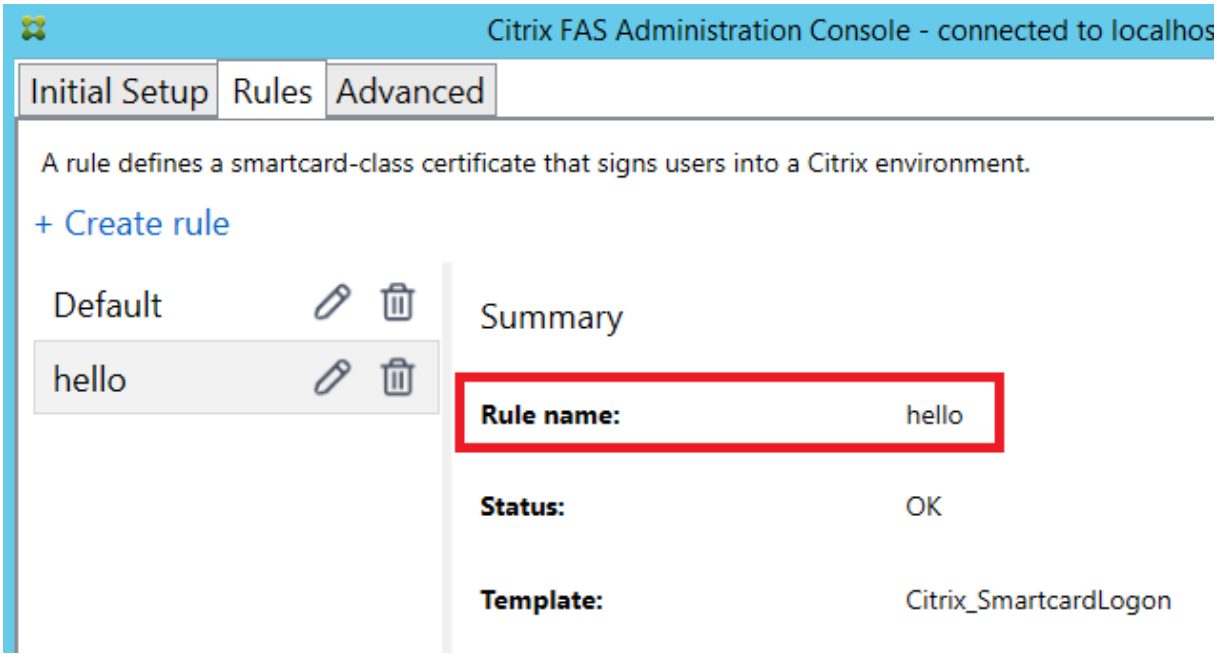
Das folgende PowerShell-Skript erstellt mit der generierten Benutzerliste eine Liste mit Benutzerzertifikaten.

```
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 -UserPrincipalNames $user.
       UserPrincipalName
    if( $server.Server -ne $NULL) {

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

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

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

 }
```

Wenn Sie mehr als einen FAS-Server haben, wird das Zertifikat für einen bestimmten Benutzer zweimal generiert: eins auf dem Hauptserver und das andere auf dem Failoverserver.

Das obige Skript wird durch die Regel “default”gesteuert. Wenn Ihre Regel einen anderen Namen hat (z. B. “hello”), ändern Sie im Skript die Variable $rule.

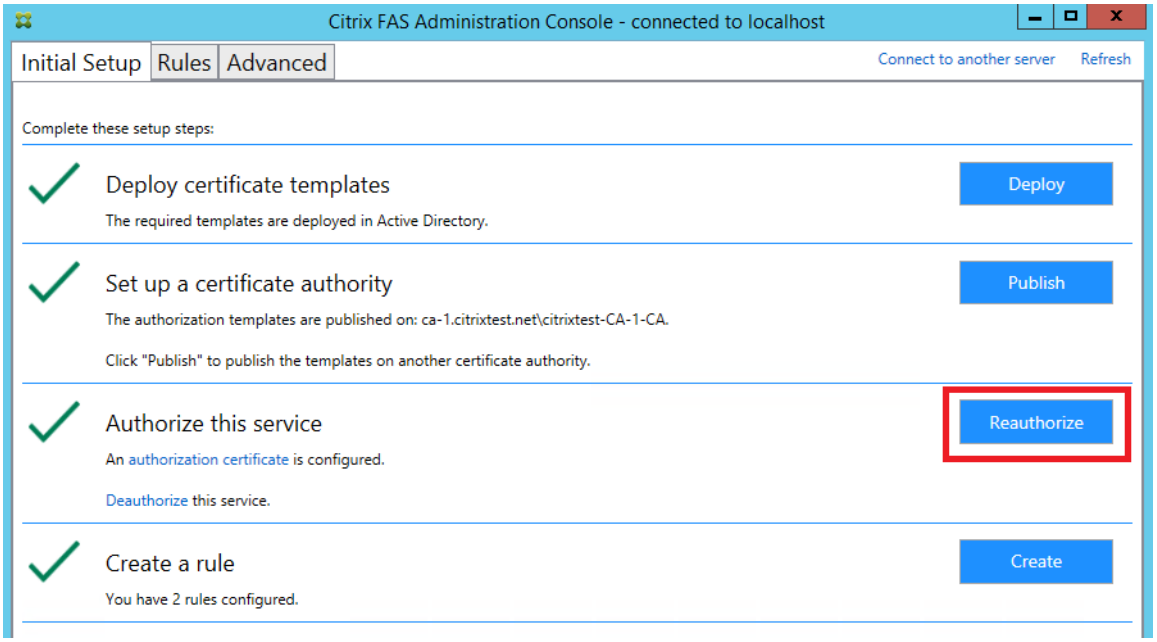



### Erneuern von Registrierungsstellenzertifikaten

Wenn mehrere FAS-Server verwendet werden, können Sie ein FAS-Registrierungsstellenzertifikat erneuern, ohne dass es Auswirkungen auf angemeldete Benutzer hat.

**Hinweis:**

Sie können den FAS auch über die grafische Benutzeroberfläche neu autorisieren:




Führen Sie die folgenden Schritte aus:

1. Erstellen Sie ein neues Autorisierungszertifikat: `New-FasAuthorizationCertificate`
2. Notieren Sie die GUID des neuen Autorisierungszertifikats, das mit folgendem Befehl zurückgegeben wird: `Get-FasAuthorizationCertificate`
3. Versetzen Sie den FAS-Server in den Wartungsmodus: `Set-FasServer –Address <FAS server> -MaintenanceMode $true`
4. Wechseln Sie zum neuen Autorisierungszertifikat: `Set-FasCertificateDefinition –AuthorizationCertificate <GUID>`
5. Heben Sie den Wartungsmodus für den FAS-Server auf: `Set-FasServer –Address <FAS server> -MaintenanceMode $false`
6. Löschen Sie das alte Autorisierungszertifikat: `Remove-FasAuthorizationCertificate`

### Verwandte Informationen

- Der Artikel Installation und Konfiguration ist die primäre Referenz für die Installation und Konfiguration des FAS.
- Der Artikel Bereitstellungsarchitekturen enthält eine Übersicht über die gebräuchlichen FAS-Architekturen.
- Der Artikel Erweiterte Konfiguration enthält Links zu weiteren Anleitungen.

## Schutz privater Schlüssel

September 11, 2024

### Einführung

Zertifikate werden in einer eingebetteten Datenbank auf dem FAS-Server gespeichert. Die zugehörigen privaten Schlüssel werden über das Netzwerkdienstkonto des FAS-Servers gespeichert und sind standardmäßig als nicht exportierbar markiert.

Es gibt zwei Arten privater Schlüssel:

- Der private Schlüssel des Registrierungsstellenzertifikats der Zertifikatvorlage Citrix_RegistrationAuthority.
- Die privaten Schlüssel der Benutzerzertifikate der Zertifikatvorlage Citrix_SmartcardLogon.

Es gibt zwei Registrierungsstellenzertifikate: Citrix_RegistrationAuthority_ManualAuthorization (24 Stunden gültig) und Citrix_RegistrationAuthority (zwei Jahre gültig).

Wenn Sie in der FAS-Verwaltungskonsole auf der Registerkarte **Initial Setup** in Schritt 3 auf **Authorize** klicken, generiert der FAS-Server ein Schlüsselpaar und sendet eine Zertifikatsignieranforderung für das Zertifikat Citrix_RegistrationAuthority_ManualAuthorization an die Zertifizierungsstelle. Dies ist ein temporäres Zertifikat, das standardmäßig 24 Stunden lang gültig ist. Die Zertifizierungsstelle stellt dieses Zertifikat nicht automatisch aus. Die Ausstellung muss bei der Zertifizierungsstelle manuell von einem Administrator genehmigt werden. Wenn das Zertifikat für den FAS-Server ausgestellt wurde, verwendet der Verbundauthentifizierungsdienst das Zertifikat Citrix_RegistrationAuthority_ManualAuthorization, um automatisch das Zertifikat Citrix_RegistrationAuthority (zwei Jahre gültig) abzurufen. Der FAS-Server löscht das Zertifikat und den Schlüssel für Citrix_RegistrationAuthority_ManualAuthorization, sobald er das Zertifikat Citrix_RegistrationAuthority erhält.

Der private Schlüssel des Registrierungsstellenzertifikats ist besonders vertraulich, da die Registrierungsstellenzertifikat-Richtlinie dem Besitzer des privaten Schlüssels das Ausstellen von Zertifikatanforderungen für die in der Vorlage konfigurierten Benutzer erlaubt. Wer also diesen Schlüssel hat, kann als einer der konfigurierten Benutzer eine Verbindung mit der Umgebung herstellen.

Mit einer der folgenden Optionen können Sie die Konfiguration des FAS-Servers so festlegen, dass private Schlüssel den Sicherheitsanforderungen Ihrer Organisation entsprechend geschützt sind:

- Microsoft Enhanced RSA und AES Cryptographic Provider oder Schlüsselspeicheranbieter für Microsoft-Software für die privaten Schlüssel von Registrierungsstellenzertifikaten und von Benutzerzertifikaten.
- Schlüsselspeicheranbieter der Microsoft-Plattform mit einem Trusted Platform Module (TPM)-Chip für den privaten Schlüssel des Registrierungsstellenzertifikats und Microsoft Enhanced RSA und AES Cryptographic Provider oder Schlüsselspeicheranbieter für Microsoft-Software für die privaten Schlüssel von Benutzern.
- Ein Hardwaresicherheitsmodul (HSM) mit dem Kryptografiedienst eines Anbieters oder ein Schlüsselspeicheranbieter mit dem HSM-Gerät für das Registrierungsstellenzertifikat und die privaten Schlüssel der Benutzerzertifikate.

### Konfigurationseinstellungen für private Schlüssel

Konfigurieren Sie den Verbundauthentifizierungsdienst, sodass er eine der drei Optionen verwendet. Bearbeiten Sie die Datei Citrix.Authentication.FederatedAuthenticationService.exe.config mit einem Text-Editor. Der Standardspeicherort der Datei ist unter Programme\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.Supress" value="" / -->

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

Der FAS liest die Konfigurationsdatei nur, wenn der Dienst gestartet wird. Wenn Sie Werte ändern, muss der FAS neu gestartet werden, damit die neuen Einstellungen wirksam 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 |
|---|---|
| true | CAPI-APIs verwenden |
| false (Standardwert) | CNG-APIs verwenden |

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

| Wert | Kommentar |
|---|---|
| Microsoft Enhanced RSA und AES Cryptographic Provider | CAPI-Standardanbieter |
| Schlüsselspeicheranbieter für Microsoft-Software | CNG-Standardanbieter |

| Wert | Kommentar |
| --- | --- |
| Schlüsselspeicheranbieter der Microsoft-Plattform | TPM-Standardanbieter TPM wird nicht für Benutzerschlüssel empfohlen. Verwenden Sie TPM nur für den Registrierungsstellenschlüssel. Wenn Sie beabsichtigen, den FAS-Server in einer virtualisierten Umgebung auszuführen, fragen Sie die TPM- und Hypervisor-Hersteller, ob Virtualisierung unterstützt wird. |
| HSM_Vendor CSP/Schlüsselspeicheranbieter | Bereitstellung durch HSM-Hersteller. Der Wert unterscheidet sich je nach Hersteller. Wenn Sie beabsichtigen, den FAS-Server in einer virtualisierten Umgebung auszuführen, fragen Sie den HSM-Hersteller, ob Virtualisierung unterstützt wird. |

Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.**ProviderType** (nur bei CAPI-API erforderlich)

| Wert | Kommentar |
| --- | --- |
| 24 | Standard. Bezieht sich auf Microsoft KeyContainerPermissionAccessEntry.ProviderType Property PROV_RSA_AES 24. Muss immer 24 lauten, es sei denn, Sie verwenden ein HSM mit CAPI und der HSM-Hersteller hat eine andere Spezifikation. |

Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.**KeyProtection** (wenn der FAS einen Privatschlüsselvorgang ausführen muss, wird der hier angegebene Wert verwendet) steuert das Flag "exportable"von privaten Schlüsseln. Ermöglicht außerdem die Verwendung eines TPM-Schlüsselspeichers, wenn die Hardware dies unterstützt.

| Wert | Kommentar |
| --- | --- |
| NoProtection | Privater Schlüssel kann exportiert werden. |
| GenerateNonExportableKey | Standard. Privater Schlüssel kann nicht exportiert werden. |

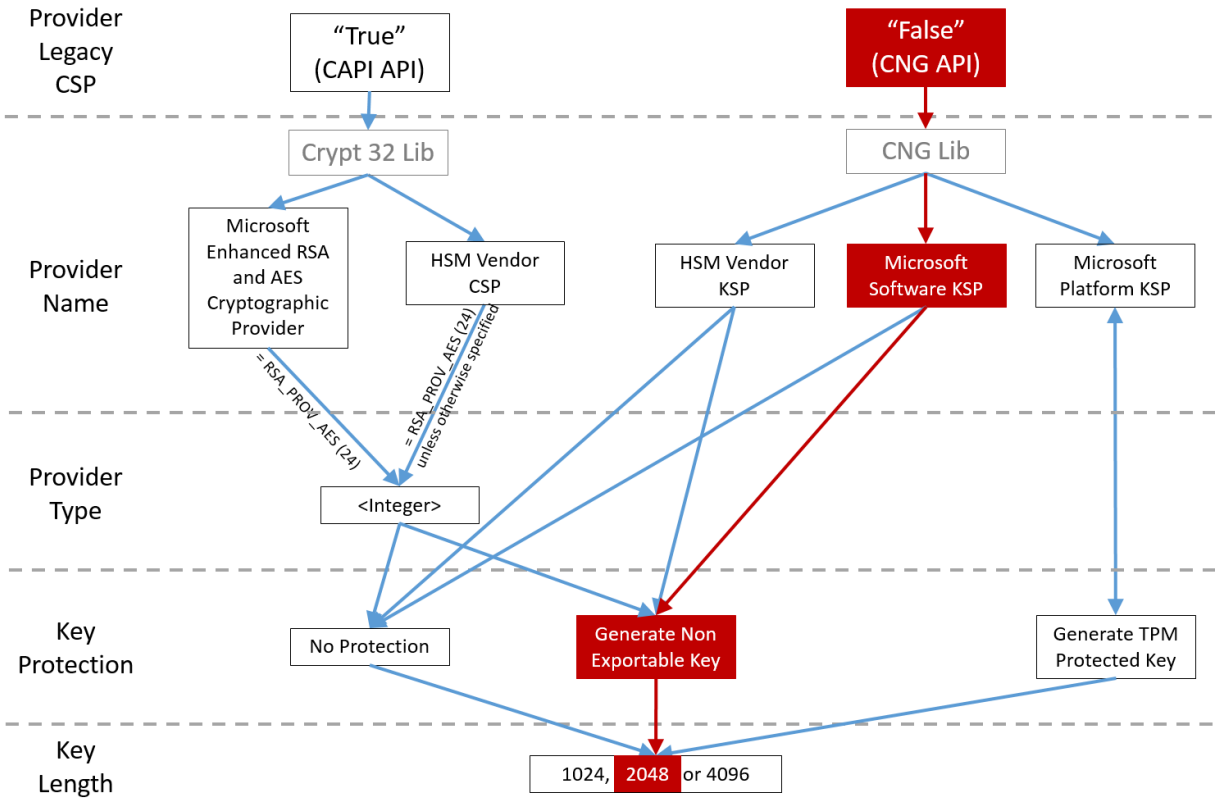
 

| Wert | Kommentar |
| --- | --- |
| GenerateTPMProtectedKey | Privater Schlüssel wird mit dem TPM verwaltet. Der private Schlüssel wird von dem Anbieter gespeichert, den Sie in ProviderName angegeben haben (z. B. Schlüsselspeicheranbieter der Microsoft-Plattform) |

Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.**KeyLength** (Größe des privaten Schlüssels in Bit eingeben)

| Wert | Kommentar |
| --- | --- |
| 2048 | 1024 oder 4096 können auch verwendet werden. |

Die Einstellungen für die Konfigurationsdatei werden grafisch wie folgt dargestellt (Installationsstandards sind rot markiert):



## Beispiele für Konfigurationsszenarios

### Beispiel 1

Dieses Beispiel gilt für den privaten Schlüssel des Registrierungsstellenzertifikats und die privaten Schlüssel der Benutzerzertifikate, die mit dem Schlüsselspeicheranbieter für Microsoft-Software gespeichert wurden.

Dies ist die Standardkonfiguration nach der Installation. Eine zusätzliche Konfiguration des privaten Schlüssels ist nicht erforderlich.

### Beispiel 2

Dieses Beispiel zeigt den privaten Schlüssel des Registrierungsstellenzertifikats, der auf dem FAS-Server auf der Hauptplatine im Hardware-TPM vom Schlüsselspeicheranbieter der Microsoft-Plattform gespeichert wurde, sowie die privaten Schlüssel der Benutzerzertifikate, die vom Schlüsselspeicheranbieter für Microsoft-Software gespeichert wurden.

In diesem Szenario wird angenommen, dass das TPM auf der Hauptplatine des FAS-Servers im BIOS entsprechend der TPM-Herstellerdokumentation aktiviert und dann in Windows initialisiert wurde. Weitere Informationen finden Sie unter https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-vista/cc749022(v=ws.10).

**Verwenden der FAS-Verwaltungskonsole** Die FAS-Verwaltungskonsole kann keine Offline-Zertifikatsignieranforderung ausstellen. Die Verwendung wird daher nur empfohlen, wenn Ihre Organisation Online-Zertifikatsignieranforderungen für Registrierungsstellenzertifikate erlaubt.

Führen Sie bei der Ersteinrichtung des FAS die folgenden Schritte aus, und zwar nach der Bereitstellung der Zertifikatvorlagen und der Einrichtung der Zertifizierungsstelle, aber bevor Sie den Dienst autorisieren (Schritt 3 in der Konfigurationsreihenfolge):

**Schritt 1:** Ändern Sie in der Config-Datei die u. a. Zeile wie folgt:

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

Daraufhin sollte die Datei 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.Supress" value="" / -->

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

Einige TPMs beschränken die Schlüssellänge. Die Standardschlüssellänge ist 2048 Bit. Achten Sie darauf, eine von der Hardware unterstützte Schlüssellänge anzugeben.

**Schritt 2:** Starten Sie den Citrix Verbundauthentifizierungsdienst neu, damit die Werte aus der Config-Datei gelesen werden.

**Schritt 3:** Autorisieren Sie den Dienst.

**Schritt 4:** Stellen Sie die ausstehende Zertifikatsanforderung manuell über den Zertifizierungsstellenserver aus. Nachdem Sie das Registrierungsstellenzertifikat erhalten haben, wird Schritt 3 der Einrichtungsreihenfolge in der Verwaltungskonsole grün angezeigt. Der private Schlüssel für das Registrierungsstellenzertifikat wurde nun im TPM generiert. Das Zertifikat gilt standardmäßig 2 Jahre.

Verwenden Sie die folgenden PowerShell-Befehle, um zu bestätigen, dass der private Schlüssel des Zertifikats der Registrierungsstelle korrekt im TPM gespeichert wird. Das Feld PrivateKeyProvider wird auf *Microsoft Platform Crypto Provider* festgelegt, wenn der private Schlüssel des Zertifikats der Registrierungsbehörde im TPM gespeichert ist:

```
1 Add-PSSnapin Citrix.Authentication.FederatedAuthenticationService.V1
2 Get-FasAuthorizationCertificate -FullCertInfo -Address localhost
```

**Schritt 5:** Ändern Sie die Config-Datei folgendermaßen zurück:

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

> **Hinweis:**
>
> Obwohl der Verbundauthentifizierungsdienst Benutzerzertifikate mit TPM-geschützten Schlüsseln generieren kann, ist die TPM-Hardware möglicherweise zu langsam für große Bereitstellungen.

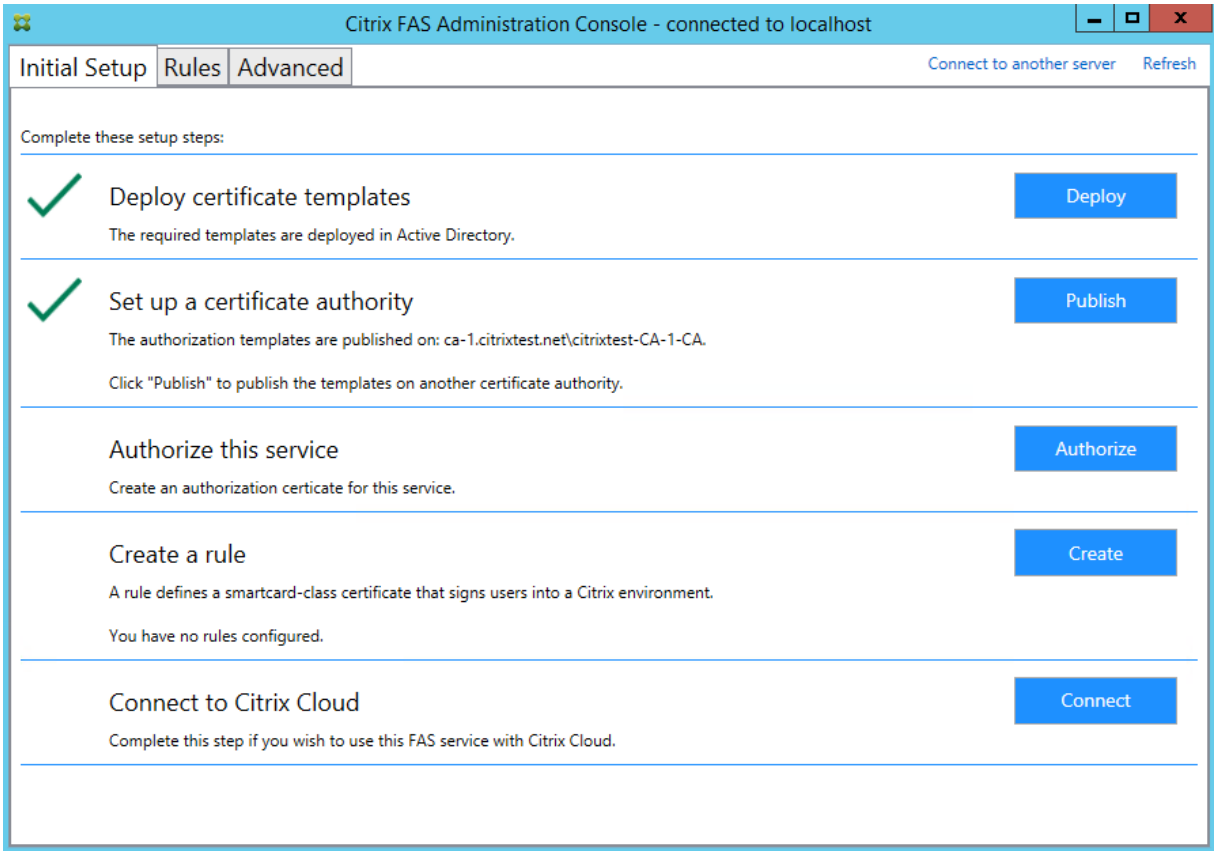
 

**Schritt 6:** Starten Sie den FAS neu. Dadurch wird der Dienst gezwungen, die Konfigurationsdatei erneut zu lesen und die geänderten Werte werden wirksam. Die nachfolgenden automatischen Privatschlüsselvorgänge wirken sich auf Benutzerzertifikatschlüssel aus. Bei diesen Vorgängen werden die privaten Schlüssel nicht im TPM, sondern mit dem Schlüsselspeicheranbieter für Microsoft-Software gespeichert.

**Schritt 7:** Wählen Sie in der FAS-Verwaltungskonsole die Registerkarte **Rules** und bearbeiten Sie die Einstellungen entsprechend den Anleitungen in Installation und Konfiguration.

**PowerShell verwenden** Das Registrierungsstellenzertifikat kann offline mit PowerShell angefordert werden. Dies ist für Organisationen geeignet, wenn die Zertifizierungsstellen keine Registrierungsstellenzertifikate über eine Online-Zertifikatsignieranforderung ausstellen dürfen. Sie können keine Zertifikatsignieranforderung bei einer Offline-Registrierungsstelle über die FAS-Verwaltungskonsole erstellen.

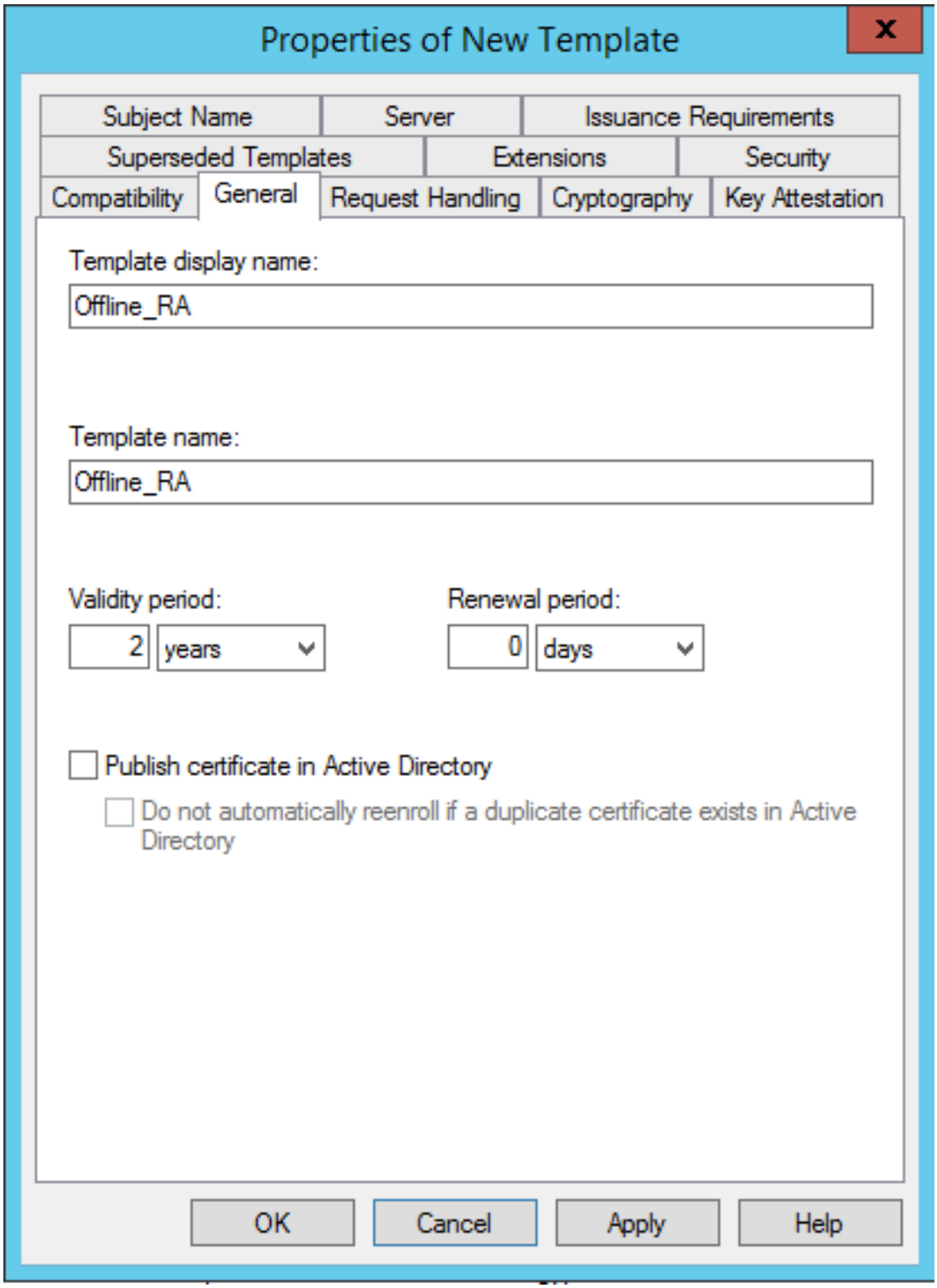
**Schritt 1:** Führen Sie während der Erstkonfiguration von FAS mit der Verwaltungskonsole nur die ersten zwei Schritte aus: “Deploy certificate templates”und “Set up a certificate authority”.




**Schritt 2:** Fügen Sie auf dem CA-Server das Zertifikatvorlagen-MMC-Snap-In hinzu. Klicken Sie mit der rechten Maustaste auf die Vorlage **Citrix_RegistrationAuthority_ManualAuthorization** und wählen Sie **Vorlage duplizieren**.

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




**Schritt 3:** Fügen Sie auf dem Zertifizierungsstellenserver das MMC-Snap-In der Zertifizierungsstelle hinzu. Klicken Sie mit der rechten Maustaste auf **Zertifikatvorlagen**. Wählen Sie **Neu** und klicken

Sie dann auf **Auszustellende Zertifikatvorlage**. Wählen Sie die Vorlage aus, die Sie soeben erstellt haben.

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

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

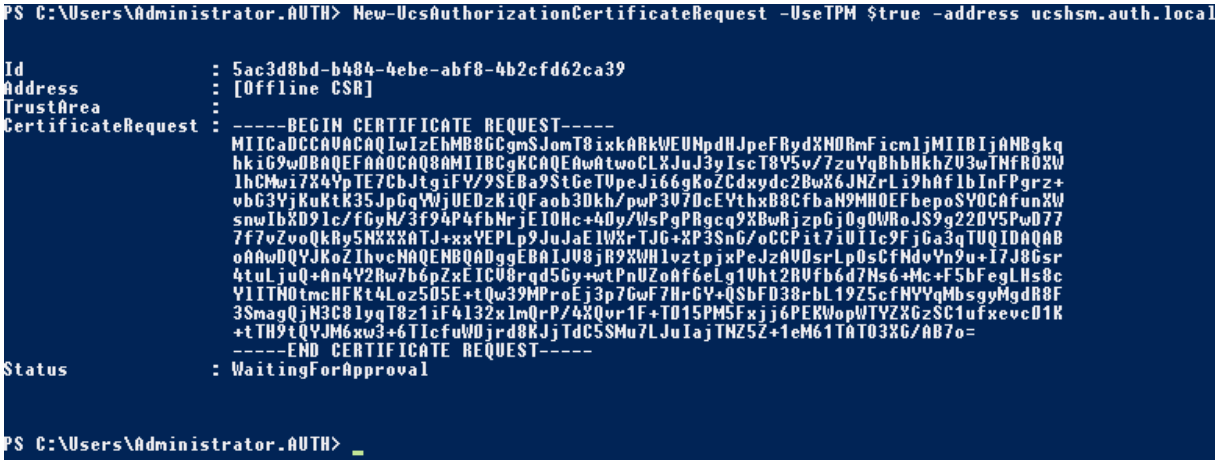
**Schritt 5:** Erstellen Sie das RSA-Schlüsselpaar im TPM des FAS-Servers und erstellen Sie die Zertifikatsignieranforderung durch Eingabe des folgenden PowerShell-Cmdlets auf dem FAS-Server. **Hinweis:** Einige TPMs beschränken die Schlüssellänge. Die Standardschlüssellänge ist 2048 Bit. Geben Sie eine Schlüssellänge an, die Ihre Hardware unterstützt.

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

Beispiel:

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

Folgendes wird angezeigt:

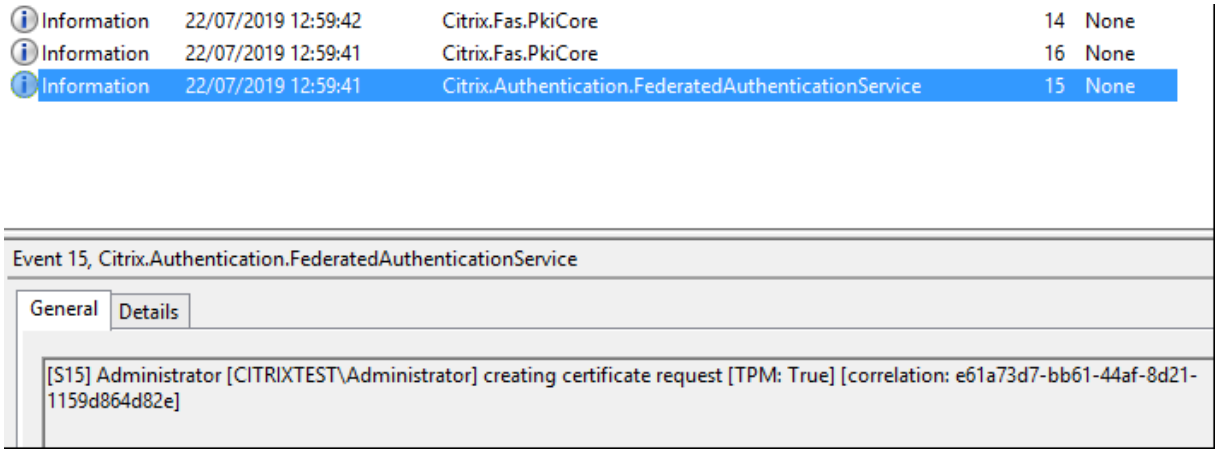



> **Hinweise:**
>
> - Die ID GUID (in diesem Beispiel "5ac3d8bd-b484-4ebe-abf8-4b2cfd62ca39") ist in einem der folgenden Schritte erforderlich.
> - Betrachten Sie das PowerShell-Cmdlet als einmalige Außerkraftsetzung zum Generieren des privaten Schlüssels für das Registrierungsstellenzertifikat.
> - Wenn dieses Cmdlet ausgeführt wird, wird die zu verwendende Schlüssellänge anhand der Werte bestimmt, die beim Start des FAS aus der Konfigurationsdatei gelesen wurden (der Standardwert ist 2048).
> - Da -UseTPM in diesem manuellen, mit PowerShell initiierten Privatschlüsselvorgang für das Registrierungsstellenzertifikat auf $true festgelegt ist, ignoriert das System Werte aus der

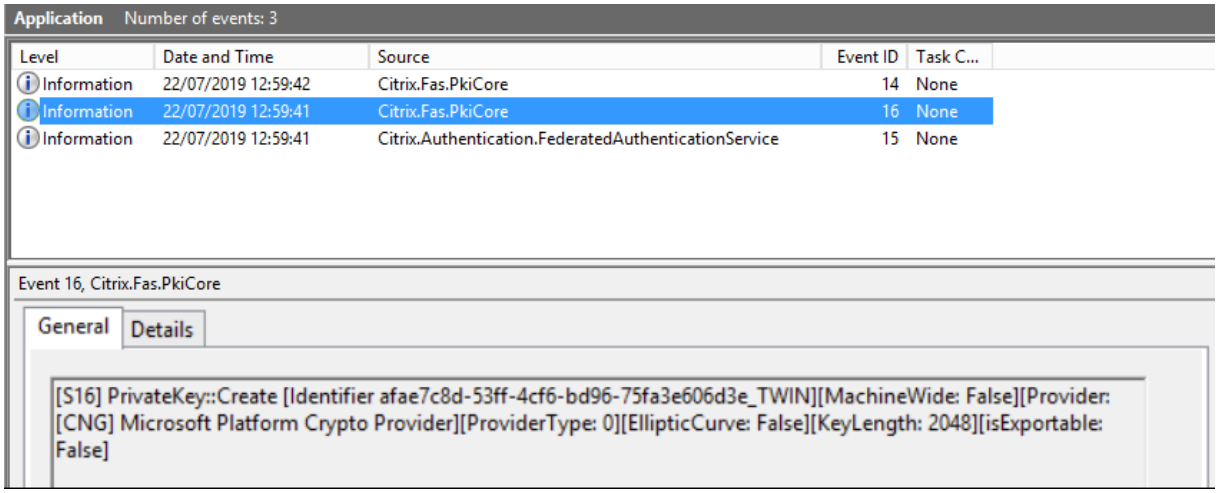
> Datei, die nicht mit den Einstellungen übereinstimmen, die zur Verwendung eines TPM erforderlich sind.
> - Durch das Ausführen des Cmdlets ändern sich keine Einstellungen in der Konfigurationsdatei.
> - Bei nachfolgenden automatischen, vom FAS initiierten Privatschlüsselvorgängen für Benutzerzertifikate werden die Werte verwendet, die beim Starten des FAS aus der Datei gelesen wurden.
> - Es ist auch möglich, den Wert KeyProtection in der Konfigurationsdatei auf GenerateTPMProtectedKey festzulegen, wenn der FAS-Server Benutzerzertifikate festlegt, damit durch das TPM geschützte private Schlüssel für Benutzerzertifikate generiert werden.

Um sicherzustellen, dass das TPM zum Generieren des Schlüsselpaars verwendet wurde, überprüfen Sie das Anwendungsprotokoll in der Windows-Ereignisanzeige auf dem FAS-Server auf die Zeit, zu der das Schlüsselpaar generiert wurde.




**Hinweis:** “[TPM: True]”

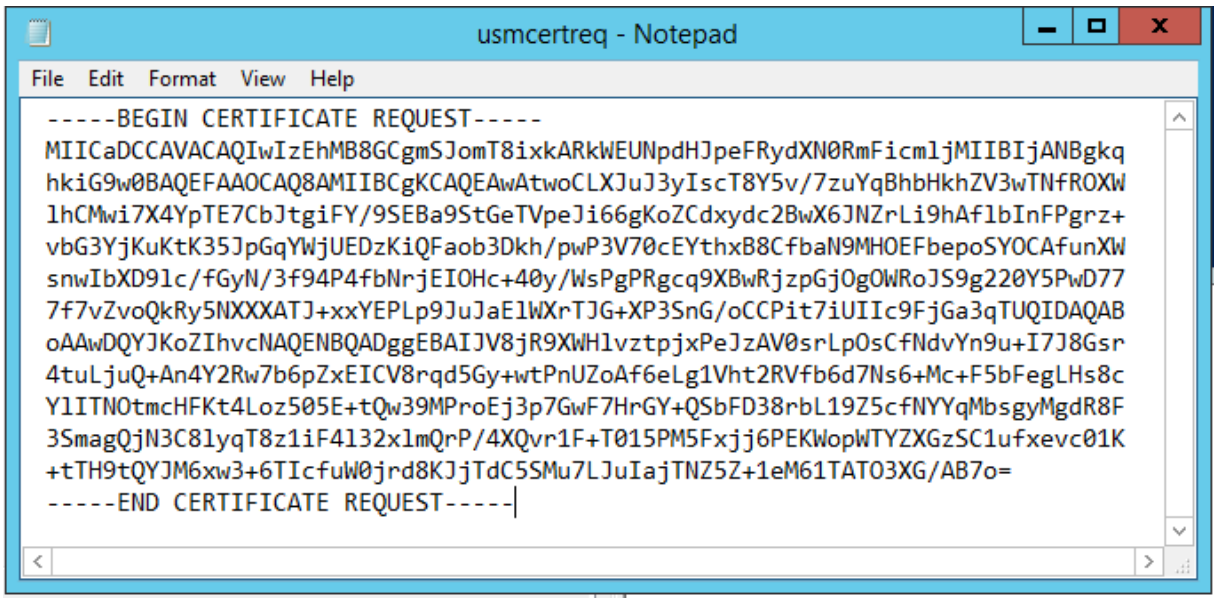
Gefolgt von:




**Hinweis:** “Provider: [CNG] Microsoft Platform Crypto Provider”

**Schritt 6:** Kopieren Sie den Zertifikatanforderungsabschnitt in einen Texteditor und speichern Sie ihn als Textdatei.




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

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

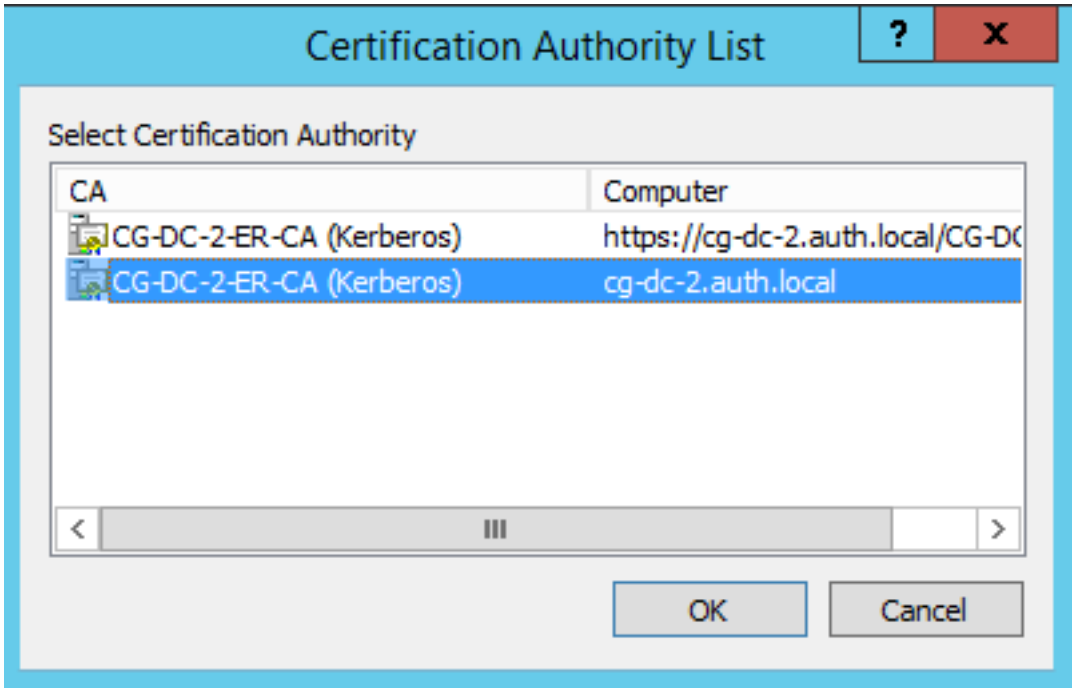
Beispiel:

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

Folgendes wird angezeigt:


An dieser Stelle wird u. U. ein Fenster mit einer Liste der Zertifizierungsstellen angezeigt. Für die Zertifizierungsstelle in diesem Beispiel sind http- (oben) und DCOM-Registrierung (unten) aktiviert. Wählen Sie ggf. die DCOM-Option:



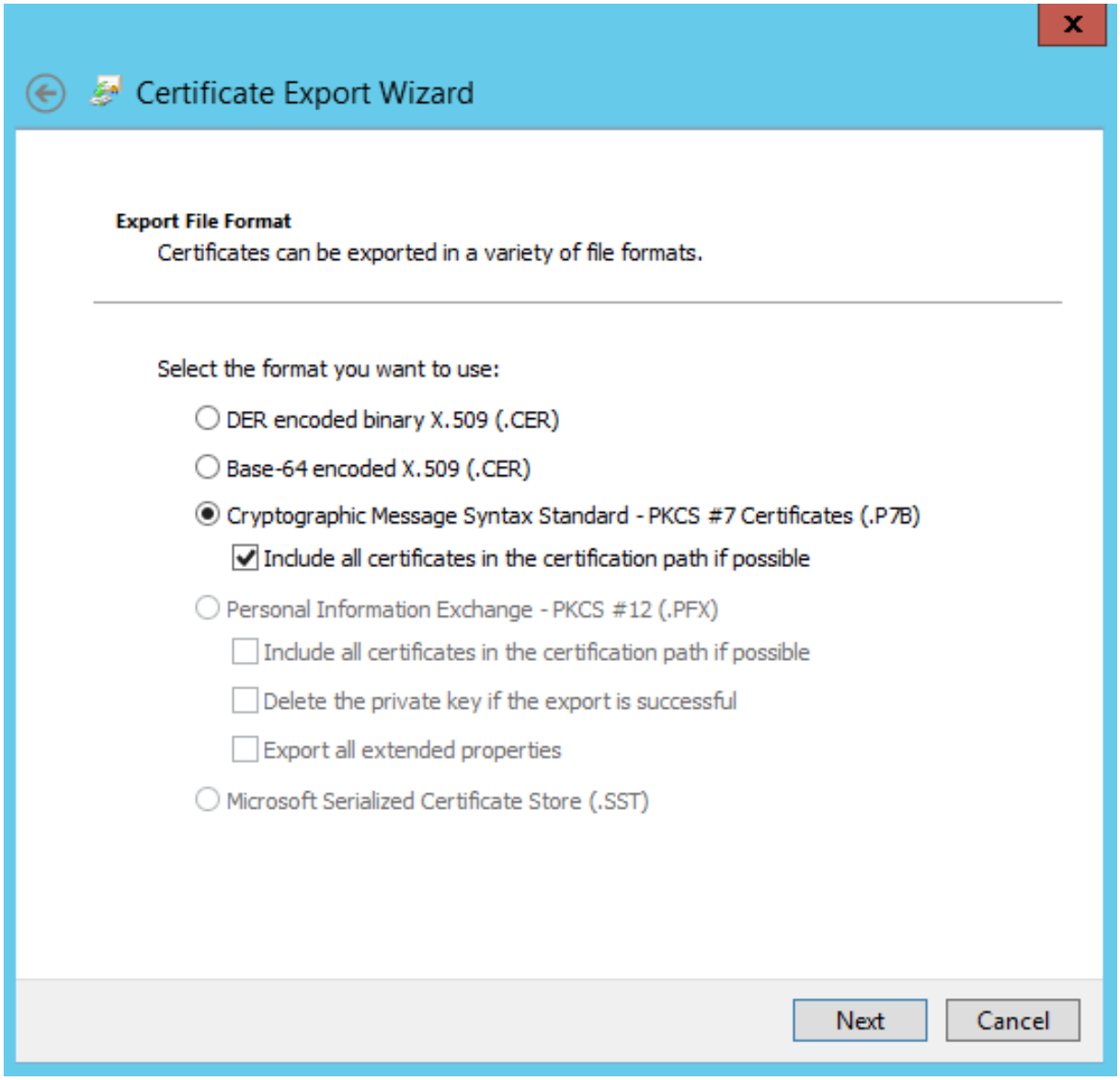

Nachdem die Zertifizierungsstelle angegeben wurde, zeigt PowerShell die RequestID an:

```
PS C:\Users\Administrator.AUTH> certreq -submit -attrib "certificatetemplate:Offline_RA" C:\Users\Administrator.AUTH\Des
ktop\usmcertreq.txt
Active Directory Enrollment Policy
  {4F7616DE-DB0C-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**. Suchen Sie die Anforderungs-ID (RequestID). Klicken Sie mit der rechten Maustaste auf die Anforderung und wählen Sie **Ausstellen**.

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




Format: **Cryptographic Message Syntax Standard –PKCS #7 Certificates (.P7B)** und **Wenn möglich, alle Zertifikate im Zertifizierungspfad einbeziehen muss** aktiviert sein.

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

**Schritt 11:** Importieren Sie das Registrierungsstellenzertifikat auf 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>
```

Beispiel:

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

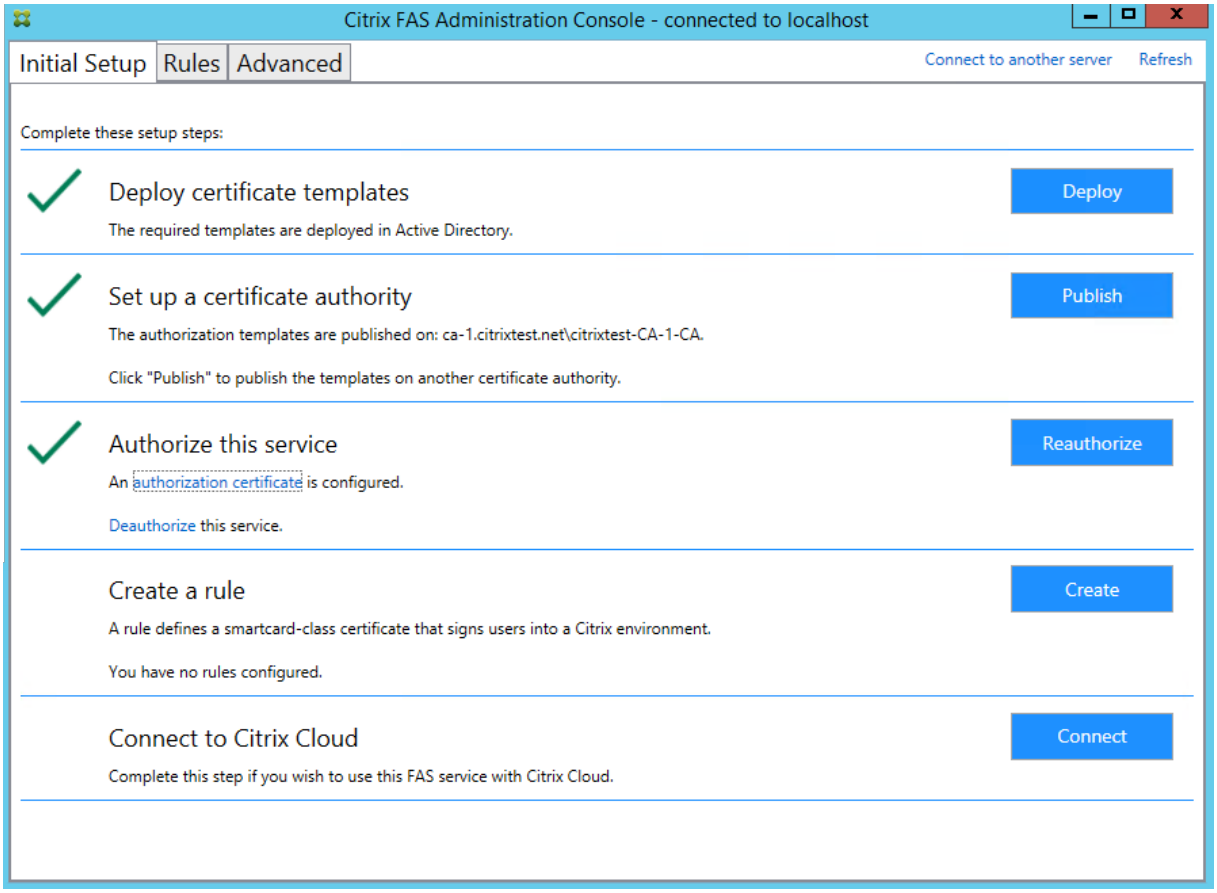
Folgendes wird angezeigt:

```
PS C:\Users\Administrator.AUTH> Import-UcsAuthorizationCertificateResponse -address ucshsm.auth.local -Id 5ac3d8bd-b484-4ebe-abf8-4b2cfd62ca39 -Pkcs7CertificateFile C:\Users\Administrator.AUTH\Desktop\TPM_UCS_Cert.p7b


Id                  : 5ac3d8bd-b484-4ebe-abf8-4b2cfd62ca39
Address             : [Offline CSR]
TrustArea           : a5c27fcc-1dd7-4c2b-8963-16ec31102dfc
CertificateRequest :
Status              : Ok
```

Verwenden Sie die folgenden PowerShell-Befehle, um zu bestätigen, dass der private Schlüssel des Zertifikats der Registrierungsstelle korrekt im TPM gespeichert wird. Das Feld PrivateKeyProvider wird auf *Microsoft Platform Crypto Provider* festgelegt, wenn der private Schlüssel des Zertifikats der Registrierungsbehörde im TPM gespeichert ist:

```
1 Add-PSSnapin Citrix.Authentication.FederatedAuthenticationService.V1
2 Get-FasAuthorizationCertificate -FullCertInfo -Address localhost
```

**Schritt 12:** Schließen Sie die FAS-Verwaltungskonsole und starten Sie sie neu.




**Hinweis:** Der Schritt “Authorize this Service”hat ein grünes Häkchen.

**Schritt 13:** Wählen Sie in der FAS-Verwaltungskonsole die Registerkarte **Rules** und bearbeiten Sie die Einstellungen entsprechend den Anleitungen in Installation und Konfiguration.

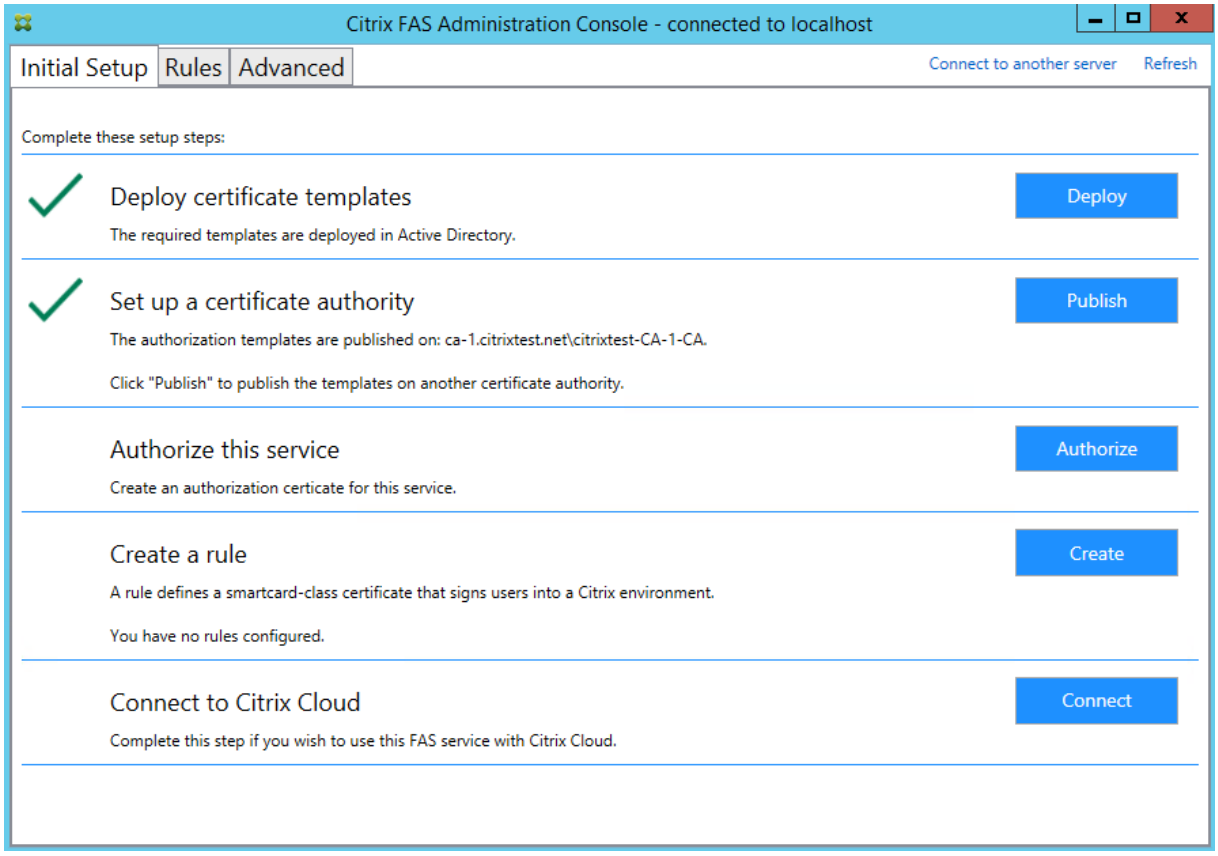
 

**Beispiel 3**

Dieses Beispiel gilt für einen privaten Schlüssel des Registrierungsstellenzertifikats und die privaten Schlüssel der Benutzerzertifikate, die in einem HSM gespeichert wurden. In diesem Beispiel wird ein konfiguriertes HSM vorausgesetzt. Das HSM hat einen Anbieternamen, z. B. "HSM_Vendor's Key Storage Provider".

Wenn Sie beabsichtigen, den FAS-Server in einer virtualisierten Umgebung auszuführen, fragen Sie den HSM-Hersteller nach Hypervisor-Unterstützung.

**Schritt 1:** Führen Sie während der Ersteinrichtung des FAS mit der Verwaltungskonsole nur die ersten zwei Schritte aus: "Deploy certificate templates"und "Set up a certificate authority".




**Schritt 2:** Aus der Dokumentation Ihres HSM erfahren Sie, welchen Wert der ProviderName Ihres HSM haben sollte. Wenn das HSM CAPI verwendet, wird der Anbieter in der Dokumentation möglicherweise als Kryptografiedienstanbieter (Cryptographic Service Provider, CSP) bezeichnet. Wenn das HSM CNG verwendet, wird der Anbieter möglicherweise als Schlüsselspeicheranbieter (Key Storage Provider, KSP) bezeichnet.

**Schritt 3:** Bearbeiten Sie die Config-Datei wie folgt:

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

Daraufhin sollte die Datei 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.Supress" value="" / -->

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

In diesem Szenario wird angenommen, dass Ihr HSM CNG verwendet, daher ist der Wert von ProviderLegacyCsp “false”. Wenn das HSM CAPI verwendet, sollte der Wert für ProviderLegacyCsp auf “true” festgelegt sein. Sie erfahren aus der Dokumentation des HSM-Herstellers, ob das HSM CAPI oder CNG verwendet. Außerdem erfahren Sie aus der Dokumentation, welche Schlüssellängen für die Generierung eines asymmetrischen RSA-Schlüssels das HSM unterstützt. In diesem Beispiel ist die Schlüssellänge auf den Standardwert von 2048 Bit festgelegt. Stellen Sie sicher, dass die von Ihnen festgelegte Schlüssellänge von der Hardware unterstützt wird.

**Schritt 4:** Starten Sie den Citrix Verbundauthentifizierungsdienst neu, damit die Werte aus der Config-Datei gelesen werden.

**Schritt 5:** Generieren Sie das RSA-Schlüsselpaar im HSM und erstellen Sie die Zertifikatsignieranforderung, indem Sie auf der Registerkarte **Initial Setup** der FAS-Verwaltungskonsole auf **Authorize** 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: [Provider: [CNG] HSM_Vendor’s Key Storage Provider]

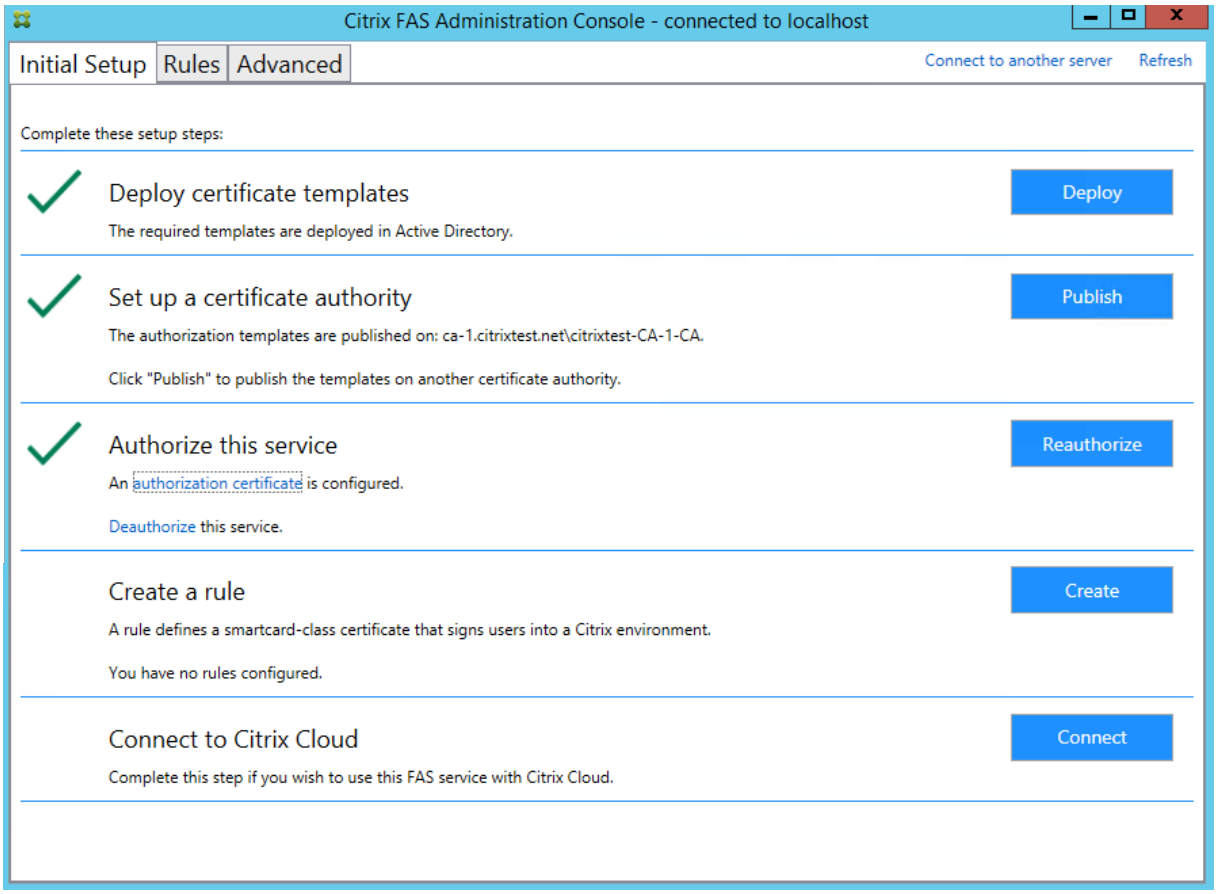
**Schritt 7:** Wählen Sie auf dem Zertifizierungsstellenserver in der MMC der Zertifizierungsstelle den Knoten **Ausstehende Anforderungen**:

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

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

**Hinweis:** Der Schritt “Authorize this Service”hat ein grünes Häkchen.




**Schritt 8:** Wählen Sie in der FAS-Verwaltungskonsole die Registerkarte **Rules** und bearbeiten Sie die Einstellungen entsprechend den Anleitungen in Installation und Konfiguration.

### FAS-Zertifikatspeicher

Der Verbundauthentifizierungsdienst verwendet nicht den Microsoft Zertifikatspeicher auf dem FAS-Server, um Zertifikate zu speichern. Er 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\*
Get-FasAuthorizationCertificate –address \<FAS server FQDN>
```

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

```
PS C:\Users\Administrator.AUTH> Get-UcsAuthorizationCertificate -address cg-ucs-2.auth.local


Id                  : a3958424-b8c3-4cac-ba0d-7eb3ce24591c
Address             : cg-dc-2.auth.local\CG-DC-2-ER-CA
TrustArea           : 3df77088-00e0-4dca-a47a-28060dc16986
CertificateRequest  :
Status              : MaintenanceDue

Id                  : fcb185f9-5069-4e34-8625-a333ac126535
Address             : [Offline CSR]
TrustArea           :
CertificateRequest  : -----BEGIN CERTIFICATE REQUEST-----
                      MIICaDCCAVACAQIwIzEhMB8GCgmSJomT8ixkARkWEUNpdHJpeFRydXN0RmFicmljMIIBIjANBgkq
                      hkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAxyNzaiWX8DhUnOZMS2YVSDhr36AV5BGeIYOGVCFKvZPe
                      Rmm/xOVM6cNKsLbew3dYlbo+vdgWg86DFRVxTORhollV86iazDZyOiYGgxe9/s8YZzCspVWN1nB1
                      zXOUJfo1qo9UsmImYr7MR/dhGAtkfsFUoPcd2+zcezmgOfq/4vmCIuerwqzRR5T/p4og7+IjR1se
                      ECz/CbXROOuiDhW+VWbjcsgklcavzvC/jR33F9dZSXNgKRiGHgfd/lBb3elZKA4OOoi90u64Q916
                      3ba9BnihqxIgvwWILOmyUfiJmCgbhLJV4TPBopOdKz/axZEIO5p5XYVjCcpXqhqL7Ppn1wIDAQAB
                      oAAwDQYJKoZIhvcNAQENBQADggEBAJhdvw6yrLGBMtAgo3oPL6o8/at+IqHjHKqgcJNJO/MU7/7X
                      bZB46drLPFzpzF88DkmfoCEgOxlbzFX9waaiFs9CHC/AcEzblN925y1gqljsfC3l5TCKBAeLFoMl
                      PSEkfYMQUOSBYCuLlkFn1LXLSeQ3qJTzSvptYROawFmUMQLffwLSR1vOuS8DJSrpASrwdXJk3TOa
                      Glo/xJo/NRMOwMH+AvGbBsgp3l+jnDjXED5RudqARfgVgcW714JP+XIeFrE1TZmUL2skNIXEPNHC
                      H8eAHdYD26caFigydfefbjx4fbaJDFHJs5+1tnrTZ9knCrawhUiIyOMLGZOOaiER+z8=
                      -----END CERTIFICATE REQUEST-----
Status              : WaitingForApproval
```

Geben Sie zum Abrufen einer Liste mit Benutzerzertifikaten Folgendes ein:

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

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

```
PS C:\Users\Administrator.AUTH> Get-UcsUserCertificate -address cg-ucs-2.auth.local


ThumbPrint            : 7BA22879F40EE92125A2F96E7DD2D52C73820459
UserPrincipalName     : walter@adfs.ext
Role                  : default
CertificateDefinition : default_Definition
ExpiryDate            : 05/04/2016 12:02:13
```

> **Hinweis:**
>
> Wenn Sie ein HSM zum Speichern der privaten Schlüssel verwenden, werden die HSM-Container durch GUIDs identifiziert. Die GUID für den privaten Schlüssel im HSM erhalten Sie über:
>
> ```
> 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
```

### Verwandte Informationen

- Installation und Konfiguration ist die primäre Referenz für die Installation und Konfiguration des FAS.
- Der Artikel Übersicht über die Architekturen des Verbundauthentifizierungsdiensts enthält eine Übersicht über die gebräuchlichen FAS-Architekturen.
- Der Artikel Erweiterte Konfiguration enthält Links zu weiteren Anleitungen.

## Sicherheits- und Netzwerkkonfiguration

September 11, 2024

Der Verbundauthentifizierungsdienst (Federated Authentication Service, FAS) ist eng in Microsoft Active Directory und die Microsoft-Zertifizierungsstelle integriert. Das System muss richtig verwaltet und geschützt werden. Hierfür muss, wie bei Domänencontrollern oder anderen wichtigen Infrastrukturkomponenten auch, eine geeignete Sicherheitsrichtlinie entwickelt werden.

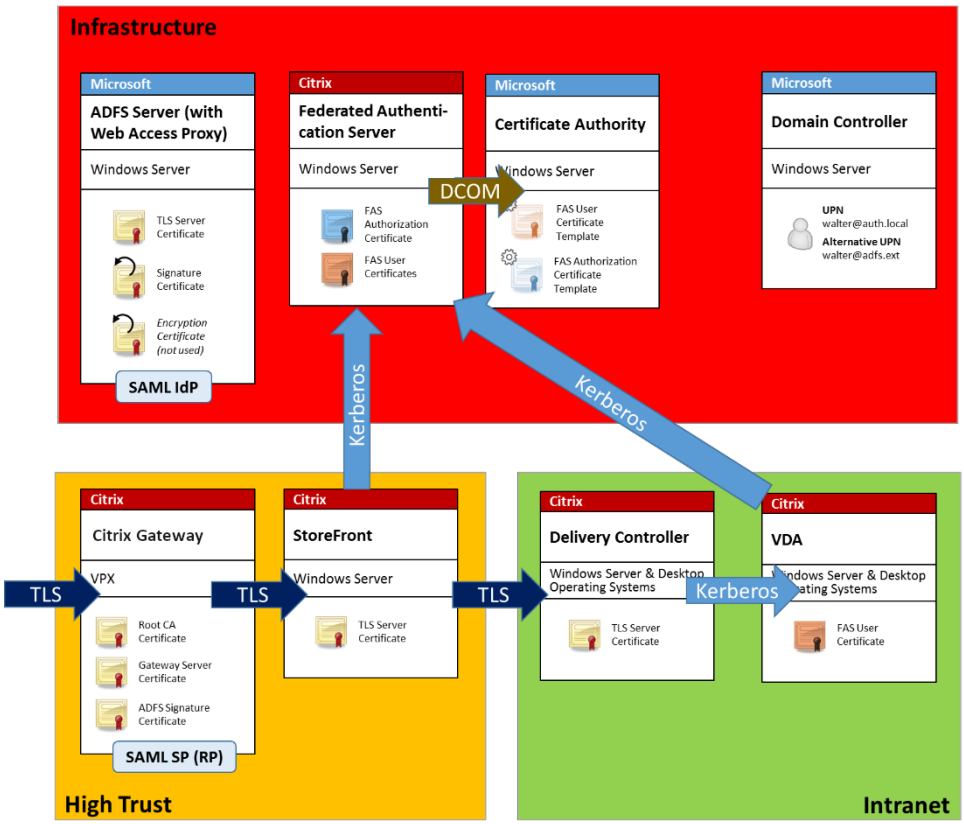
Dieses Dokument enthält eine Übersicht über die Sicherheitsfragen, die Sie bei der FAS-Bereitstellung berücksichtigen sollten. Außerdem finden Sie hier eine Übersicht über die Features, die Ihnen beim Schutz der Infrastruktur helfen können.

### Netzwerkarchitektur

Die folgende Abbildung zeigt die wichtigsten Komponenten und Sicherheitsgrenzen einer FAS-Bereitstellung.

Der FAS-Server ist zusammen mit der Zertifizierungsstelle und dem Domänencontroller Teil der sicherheitskritischen Infrastruktur. In einer Verbundumgebung übernehmen Citrix Gateway und Citrix StoreFront die Benutzerauthentifizierung. Andere Komponenten von Citrix Virtual Apps and Desktops sind von der Einführung von FAS nicht betroffen.




## Firewall und Netzwerksicherheit

TLS über Port 443 schützt die Kommunikation zwischen Citrix Gateway, StoreFront und den Delivery Controller-Komponenten. Der StoreFront-Server führt nur ausgehende Verbindungen durch und Citrix Gateway akzeptiert nur Verbindungen über das Internet mit HTTPS-Port 443.

Der StoreFront-Server kontaktiert den FAS-Server über Port 80 unter Verwendung von beidseitig authentifiziertem Kerberos. Bei der Authentifizierung werden die Kerberos-HOST/fqdn-Identität des FAS-Servers und die Kerberos-Computerkontoidentität des StoreFront-Servers verwendet. Diese Authentifizierungsmethode generiert ein Anmeldehandle für die einmalige Verwendung, das der Citrix Virtual Delivery Agent (VDA) zur Anmeldung des Benutzers benötigt.

Wenn eine HDX-Sitzung mit dem VDA verbunden wird, kontaktiert der VDA außerdem den FAS-Server über Port 80. Bei der Authentifizierung werden die Kerberos-HOST/fqdn-Identität des FAS-Servers und die Kerberos-Computeridentität des VDAs verwendet. Außerdem muss der VDA das Anmeldeinformations-Handle übergeben, um auf Zertifikat und privaten Schlüssel zugreifen zu können.

Die Microsoft-Zertifizierungsstelle akzeptiert Kommunikation mit einem Kerberos-authentifizierten DCOM, das zur Verwendung eines festen TCP-Ports konfiguriert werden kann. Die Zertifizierungsstelle

erfordert, dass der FAS-Server ein durch ein vertrauenswürdiges Enrollment Agent-Zertifikat signiertes CMC-Paket übergibt.

| Server | Firewallports |
|---|---|
| Verbundauthentifizierungsdienst | [in] Kerberos über HTTP von StoreFront und VDAs, [out] DCOM zur Microsoft-Zertifizierungsstelle |
| Citrix Gateway | [in] HTTPS von Clientmaschinen, [in/out] HTTPS zum/vom StoreFront-Server, [out] HDX zum VDA |
| StoreFront | [in] HTTPS von Citrix Gateway, [out] HTTPS an Delivery Controller, [out] Kerberos HTTP an 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 an FAS |
| Microsoft-Zertifizierungsstelle | (eingehend) DCOM und signiert von FAS |

### Verbindungen zwischen dem Citrix Verbundauthentifizierungsdienst (FAS) und Citrix Cloud

Die Konsole und FAS greifen über das Benutzerkonto bzw. das Netzwerkdienstkonto auf folgende Adressen zu.

- FAS-Verwaltungskonsole, unter dem Benutzerkonto
  - `*.cloud.com`
  - `*.citrixworkspacesapi.net`
  - Adressen, die von einem externen Identitätsanbieter benötigt werden (sofern dieser in Ihrer Umgebung verwendet wird)
- FAS-Dienst, über das Netzwerkdienstkonto:
  - `*.citrixworkspacesapi.net`
  - `*.citrixnetworkapi.net`

Wenn Ihre Umgebung Proxyserver enthält, konfigurieren Sie den Benutzerproxy mit den Adressen für die FAS-Verwaltungskonsole. Die Adresse für das Netzwerkdienstkonto ist zudem mit netsh oder einem ähnlichen Tool zu konfigurieren.

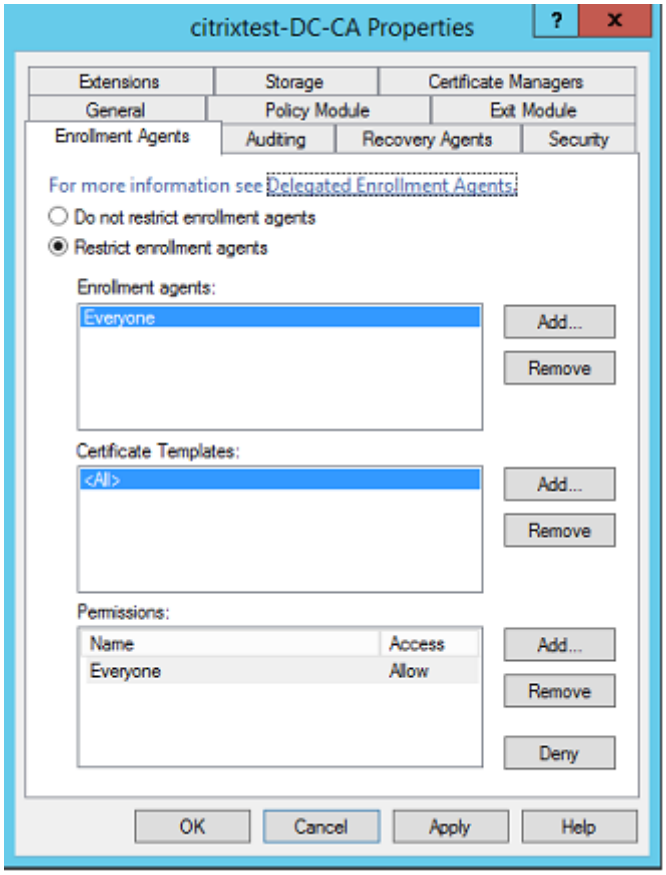
 

## Sicherheitsüberlegungen

Der FAS hat ein RA-Zertifikat, mit dem er selbständig Zertifikate für Ihre Domänenbenutzer ausstellen kann. Es hilft bei der Entwicklung und Implementierung einer Sicherheitsrichtlinie zum Schutz von FAS-Servern und zur Einschränkung der zugehörigen Berechtigungen.

### Delegierte Registrierungsagents

FAS stellt Benutzerzertifikate als Registrierungsagent aus. Mit der Microsoft-Zertifizierungsstelle können Sie Registrierungsagents, Zertifikatvorlagen und Benutzer einschränken, für die Registrierungsagents Zertifikate ausstellen können.




In dem Dialogfeld können Sie Folgendes sicherstellen:

- Die Liste der *Registrierungsagents* enthält nur FAS Server.
- Die Liste der *Zertifikatvorlagen* enthält nur die FAS-Vorlagen.
- Die Liste der *Berechtigungen* enthält Benutzer, die FAS verwenden dürfen. Es wird beispielsweise empfohlen, keine Zertifikate für Administratoren oder die Gruppe der geschützten Benutzer auszustellen.

### Zugriffssteuerungsliste konfigurieren

Wie im Abschnitt Regeln konfigurieren beschrieben, müssen Sie eine Liste von StoreFront-Servern konfigurieren. Diese StoreFront-Server mache bei dem FAS Benutzeridentitäten geltend, wenn Zertifikate ausgestellt werden. Sie können außerdem festlegen, welchen Benutzern Zertifikate ausgestellt werden dürfen und bei welchen VDA-Maschinen sie sich authentifizieren können. Dieses Feature versteht sich zusätzlich zu den von Ihnen konfigurierten Active Directory- bzw. Zertifizierungsstellen-Standardsicherheitsfeatures.

### Firewalleinstellungen

Für die gesamte Kommunikation mit FAS-Servern werden gegenseitig authentifizierte Kerberos-Netzwerkverbindungen gemäß Windows Communication Foundation über Port 80 verwendet.

### Ereignisprotokollüberwachung

FAS und VDA schreiben Informationen in das Windows-Ereignisprotokoll. Dieses Protokoll kann zur Überwachung und Überprüfung verwendet werden. Der Abschnitt Ereignisprotokolle enthält eine Liste möglicher Ereignisprotokolleinträge.

### Hardwaresicherheitsmodule

Alle privaten Schlüssel (einschließlich der vom FAS ausgestellten Benutzerzertifikatschlüssel) werden als nicht exportierbare private Schlüssel vom Netzwerkdienstkonto gespeichert. Der FAS unterstützt die Verwendung eines kryptographischen Hardwaresicherheitsmoduls, sollte eine Sicherheitsrichtlinie dies erfordern.

Eine detaillierte Kryptographiekonfiguration ist über die Datei FederatedAuthenticationService.exe.config verfügbar. Diese Einstellungen gelten für die Ersterstellung privater Schlüssel. Daher können verschiedene Einstellungen für private Registrierungsstellenschlüssel (z. B. 4096 Bit, TPM-geschützt) und Laufzeit-Benutzerzertifikate verwendet werden.

| Parameter | Beschreibung |
|---|---|
| ProviderLegacyCsp | Bei der Einstellung “true”verwendet der FAS die Microsoft CryptoAPI (CAPI). Andernfalls verwendet der FAS die Microsoft Cryptography Next Generation-API (CNG). |
| ProviderName | Name des CAPI- oder CNG-Anbieters, der verwendet werden soll. |

| Parameter | Beschreibung |
| --- | --- |
| ProviderType | Bezieht sich auf Microsoft KeyContainerPermissionAccessEntry.ProviderType Property PROV_RSA_AES 24. Muss immer 24 lauten, es sei denn, Sie verwenden ein HSM mit CAPI und der HSM-Hersteller hat eine andere Spezifikation. |
| KeyProtection | Steuert das Flag "Exportable"privater Schlüssel. Ermöglicht außerdem die Verwendung eines TPM-Schlüsselspeichers (Trusted Platform Module), wenn die Hardware dies unterstützt. |
| KeyLength | Schlüssellänge privater RSA-Schlüssel. Zulässige Werte sind 1024, 2048 und 4096 (Standard = 2048). |

### Verwaltungsaufgaben

Die Verwaltung der Umgebung lässt sich in folgende Zuständigkeiten aufgliedern:

| Name | Aufgaben |
| --- | --- |
| Unternehmensadministrator | Installation und Schutz von Zertifikatvorlagen in der Gesamtstruktur |
| Domänenadministrator | Konfiguration der Gruppenrichtlinieneinstellungen |
| Zertifizierungsstellenadministrator | Konfigurieren der Zertifizierungsstelle |
| FAS-Administrator | Installieren und konfigurieren des FAS-Servers |
| StoreFront-/Citrix Gateway-Administrator | Konfigurieren der Benutzerauthentifizierung |
| Citrix Virtual Desktops-Administrator | Konfigurieren von VDAs und Controllern |

Jeder Administrator ist für verschiedene Aspekte des allgemeinen Sicherheitsmodells zuständig, sodass ein Defense-in-Depth-Schutz des Systems möglich ist.

### Gruppenrichtlinieneinstellungen

Vertrauenswürdige FAS-Maschinen werden anhand einer über die Gruppenrichtlinie konfigurierten Nachschlagetabelle mit Indexnummer -> FQDN identifiziert. Beim Herstellen einer Verbindung mit

dem FAS-Server prüfen Clients dessen HOST\<fqdn> Kerberos-Identität. Alle Server, die auf den FAS-Server zugreifen, müssen die gleiche FQDN-Konfiguration für denselben Index haben, ansonsten können StoreFront und VDAs eine Verbindung mit verschiedenen FAS-Servern herstellen.

Citrix empfiehlt, eine Richtlinie auf alle Maschinen in der Umgebung anzuwenden, um Fehlkonfigurationen zu vermeiden. Vorsicht beim Bearbeiten der Liste der FAS-Server, insbesondere wenn Sie Einträge entfernen oder umsortieren.

Die Steuerung dieses Gruppenrichtlinienobjekts muss auf FAS-Administratoren (und/oder Domänenadministratoren) beschränkt werden, die FAS-Server installieren und außer Betrieb nehmen. Die Wiederverwendung von Maschinen-FQDNs kurz nach der Außerbetriebnahme eines FAS-Servers ist zu vermeiden.

## Zertifikatvorlagen

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

### Umbenennen der Zertifikatvorlage

Wenn Sie die Zertifikatvorlage "Citrix_SmartcardLogon"entsprechend dem Benennungsstandard Ihres Unternehmens umbenennen möchten, müssen Sie folgende Schritte ausführen:

- Erstellen Sie eine Kopie der Zertifikatvorlage und benennen Sie sie gemäß Ihrem Benennungsstandard.
- Verwenden Sie zum Verwalten von FAS nicht die Verwaltungsbenutzeroberfläche, sondern die FAS-PowerShell-Befehle. (Die Verwaltungsbenutzeroberfläche ist nur zur Verwendung mit den Citrix Standardvorlagennamen vorgesehen.)
  - Veröffentlichen Sie die Vorlage mit dem Microsoft MMC-Zertifikatvorlagen-Snap-In oder mit dem Befehl "Publish-FasMsTemplate".
  - Konfigurieren Sie FAS mit dem Befehl "New-FasCertificateDefinition"für den Namen der Vorlage.

### Ändern allgemeiner Eigenschaften

Standardmäßig gilt ein Benutzerzertifikat für sieben Tage. Sie können die Gültigkeitsdauer der Zertifikatvorlage ändern.

Ändern Sie nicht den Verlängerungszeitraum. FAS ignoriert diese Einstellung in der Zertifikatvorlage. FAS aktualisiert das Zertifikat automatisch nach Ablauf der halben Gültigkeitsdauer.

#### Ändern der Anforderungsverarbeitung

Ändern Sie diese Eigenschaften nicht. FAS ignoriert diese Einstellungen in der Zertifikatvorlage. FAS deaktiviert immer die Einstellungen **Exportieren von privatem Schlüssel zulassen** und **Mit gleichem Schlüssel erneuern**.

#### Ändern der Kryptographieeigenschaften

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

Informationen zu gleichwertigen Einstellungen in FAS finden Sie unter Schutz privater Schlüssel.

#### Ändern der Schlüsselnachweiseigenschaften

Ändern Sie diese Eigenschaften nicht. FAS unterstützt keinen Schlüsselnachweis.

#### Ändern der Eigenschaften für abgelöste Vorlagen

Ändern Sie diese Eigenschaften nicht. FAS unterstützt keine Vorlagenablösung.

#### Ändern der Erweiterungseigenschaften

Sie können diese Einstellungen entsprechend den Richtlinien Ihres Unternehmens ändern.

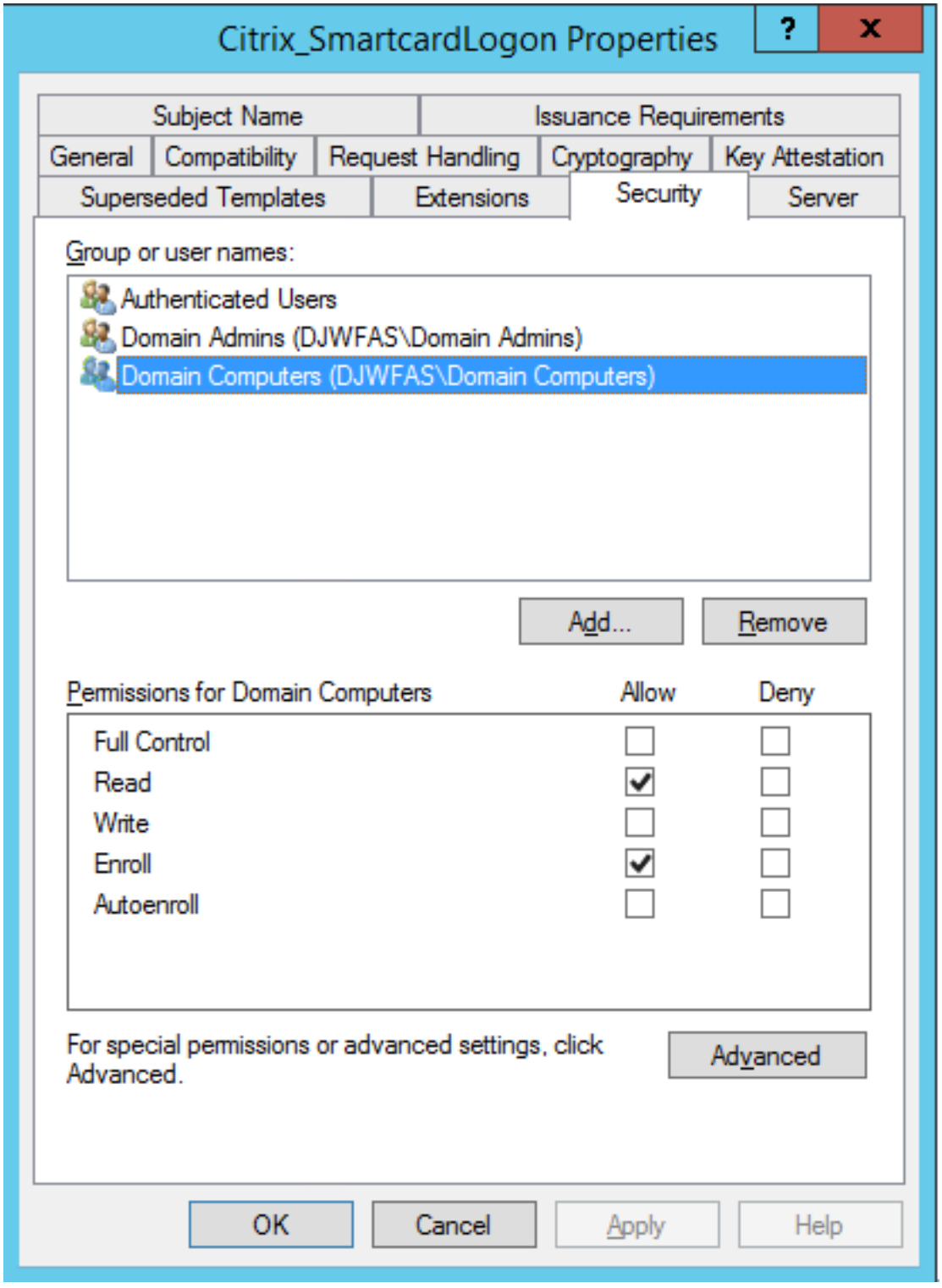
Hinweis: Ungeeignete Erweiterungseinstellungen können Sicherheitsprobleme verursachen oder zur Unbrauchbarkeit von Zertifikaten führen.

#### Ändern der Sicherheitseigenschaften

Citrix empfiehlt die Änderung dieser Einstellungen, sodass die Berechtigungen **Lesen** und **Registrieren** ausschließlich für Maschinenkonten der FAS-Server zugelassen werden. Für den FAS-Dienst sind keine weiteren Berechtigungen erforderlich. Wie bei anderen Zertifikatvorlagen können Sie jedoch Folgendes tun:

- Administratoren erlauben, die Vorlage zu lesen und schreiben
- Authentifizierten Benutzern erlauben, die Vorlage zu lesen




**Ändern der Eigenschaften des Antragstellernamens**

Citrix empfiehlt, diese Eigenschaften nicht zu ändern.

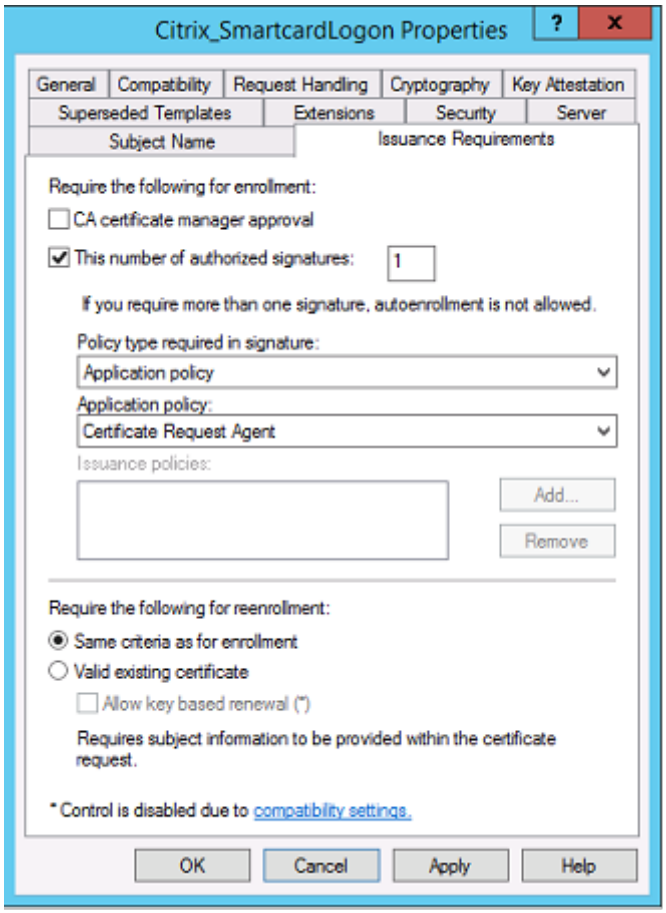
In der Vorlage ist *Build from this Active Directory information* ausgewählt, wodurch die Zertifizierungsstelle die SID des Benutzers in eine Zertifikatserweiterung einschließt und eine sichere Zuordnung zum Active Directory-Konto des Benutzers gewährleistet wird.

### Ändern von Servereigenschaften

Falls erforderlich, können Sie diese Einstellung entsprechend den Richtlinien Ihres Unternehmens ändern. Citrix rät davon ab.

### Ändern der Ausstellungsvoraussetzungen

Ändern Sie diese Einstellungen nicht. Es müssen folgende Einstellungen gelten:




### Ändern der Kompatibilitätseigenschaften

Sie können diese Einstellungen ändern. Die Mindesteinstellung ist **Windows Server 2003 CAs** (Schemaversion 2). FAS unterstützt jedoch nur Zertifizierungsstellen für Windows Server 2008 und

höher. Wie oben erläutert ignoriert FAS außerdem die zusätzlichen Einstellungen für **Windows Server 2008 CAs** (Schemaversion 3) und **Windows Server 2012 CAs** (Schemaversion 4).

## Zertifizierungsstellenverwaltung

Der Zertifizierungsstellenadministrator ist für die Konfiguration des Zertifizierungsstellenservers und des von ihm verwendeten privaten Schlüssels des ausstellenden Zertifikats verantwortlich.

### Veröffentlichen von Vorlagen

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

Eine einfache Sicherheitsmaßnahme besteht darin, bei der Installation der FAS-Server nur die Vorlagen für Registrierungsstellenzertifikate zu veröffentlichen oder ein Ausstellungsverfahren vorzuschreiben, das komplett offline ist. In beiden Fällen darf nur der Zertifizierungsstellenadministrator Registrierungsstellenzertifikate autorisieren und er muss eine Richtlinie für die Autorisierung von FAS-Servern haben.

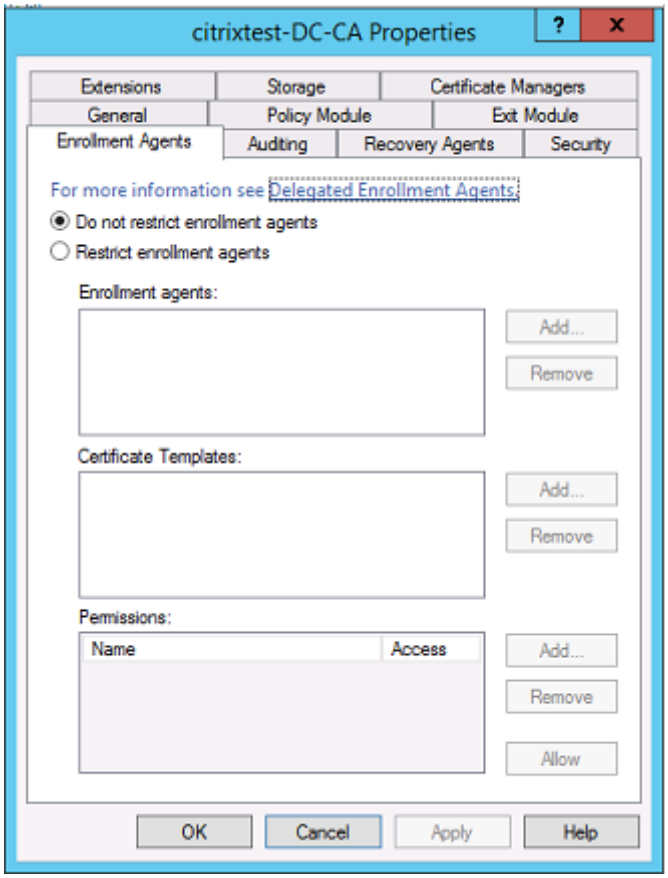
### Firewalleinstellungen

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

### Eingeschränkte Registrierung

Standardmäßig kann jeder Eigentümer eines Registrierungsstellenzertifikats beliebigen Benutzern ein Zertifikat auf der Basis einer Zertifikatvorlage, die Zugriff ermöglicht, ausstellen. Diese Zertifikatausstellung muss auf eine Gruppe von Benutzern ohne Privilegien über die Zertifizierungsstelleneigenschaft “Restrict enrollment agents”eingeschränkt werden.




### Richtlinienmodule und Überwachung

In komplexeren Bereitstellungen können benutzerdefinierte Sicherheitsmodule verwendet werden, um die Zertifikatausstellung zu verfolgen und zu unterbinden.

## FAS-Verwaltung

Der FAS hat mehrere Sicherheitsfeatures.

### Beschränken von StoreFront, Benutzern und VDAs über eine ACL

Im Zentrum des FAS-Sicherheitsmodells liegt die Steuerung des Zugriffs auf Funktionen durch Kerberos-Konten:

| Zugriffsvektor | Beschreibung |
| --- | --- |
| StoreFront (IdP) | Diese Kerberos-Konten können deklarieren, dass ein Benutzer korrekt authentifiziert wurde. Bei Gefährdung eines dieser Konten können Zertifikate erstellt und für durch die FAS-Konfiguration zugelassene Benutzer verwendet werden. |
| VDAs (vertrauende Seite) | Dies sind die Maschinen, die auf Zertifikate und private Schlüssel zugreifen dürfen. Zusätzlich ist ein vom IdP abgerufenes Anmelde-Handle erforderlich, sodass ein gefährdetes VDA-Konto in dieser Gruppe nur geringe Möglichkeiten für einen Angriff auf das System hat. |
| Benutzer | Durch diese Option wird gesteuert, welche Benutzer vom IdP bestätigt werden können. Es besteht eine Überschneidung mit den Zertifizierungsstellenoptionen "Restrict enrollment agents". Im Allgemeinen sollten nur nicht-privilegierte Benutzerkonten in diese Liste aufgenommen werden. Dies verhindert, dass ein gefährdetes StoreFront-Konto Privilegien auf eine höhere Verwaltungsebene übertragen kann. Vor allem Domänenadministratorkonten dürfen keine Berechtigung durch diese ACL erhalten. |

**Konfigurieren von Regeln**

Regeln sind nützlich, wenn mehrere eigenständige Citrix Virtual Apps- oder Citrix Virtual Desktops-Bereitstellungen die gleiche FAS-Serverinfrastruktur verwenden. Jede Regel hat eigene Konfigurationsoptionen, wobei insbesondere separate Kerberos Zugriffssteuerungslisten (ACLs) konfiguriert werden können.

**Konfigurieren von Zertifizierungsstelle und Vorlagen**

Für verschiedene Zugriffsrechte können verschiedene Zertifikatvorlagen und Zertifizierungsstellen konfiguriert werden. In komplexen Konfigurationen können abhängig von der Umgebung weniger oder leistungsfähigere Zertifikate verwendet werden. Beispiel: Als "extern"identifizierte Benutzer können ein Zertifikat mit weniger Berechtigungen als interne Benutzer haben.

#### Sitzungsinterne und Authentifizierungszertifikate

Der FAS-Administrator kann festlegen, ob das für die Authentifizierung verwendete Zertifikat in der Sitzung eines Benutzers verwendet werden kann.
Damit kann beispielsweise ein Benutzer Signaturzertifikate nur sitzungsintern zur Verfügung haben und die leistungsfähigeren Anmeldezertifikate nur bei der Anmeldung.

#### Schutz privater Schlüssel und Schlüssellänge

Der FAS-Administrator kann den FAS so konfigurieren, dass private Schlüssel in einem Hardwaresicherheitsmodul (HSM) oder einem Trusted Platform Module (TPM) gespeichert werden. Citrix empfiehlt, zumindest den privaten Schlüssel des Registrierungsstellenzertifikats in einem TPM zu speichern. Der FAS bietet die Möglichkeit, den privaten Schlüssel als Teil der Offline-Zertifikatanforderung in einem TPM zu speichern.

Auch die privaten Schlüssel für Benutzerzertifikate können in einem TPM oder HSM gespeichert werden. Alle Schlüssel müssen als nicht exportierbar generiert werden und eine Länge von mindestens 2048 Bit haben.

#### Ereignisprotokolle

Der FAS-Server bietet detaillierte Konfigurations- und Laufzeit-Ereignisprotokolle, die für die Überwachung und Angriffserkennung verwendet werden können.

#### Verwaltungszugriff und Verwaltungstools

Der FAS umfasst Features und Tools zur Remoteverwaltung (unter gegenseitiger Kerberos-Authentifizierung). Mitglieder der lokalen Administratorgruppe haben Vollzugriff auf die FAS-Konfiguration. Die FAS-Konfiguration muss ordnungsgemäß gepflegt werden.

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

Die Verwendung des FAS ändert nichts am Sicherheitsmodell für Delivery Controller- und VDA-Administratoren, da das FAS-Anmeldeinformations-Handle direkt das Active Directory-Kennwort ersetzt. Controller- und VDA-Administratorgruppen dürfen nur vertrauenswürdige Benutzer enthalten. Es müssen Überwachungs- und Ereignisprotokolle geführt werden.

### Allgemeine Windows-Serversicherheit

Für alle Server müssen sämtliche Patches installiert sein und Standardfirewall- und Antivirensoftware zur Verfügung stehen. Sicherheitskritische Infrastrukturserver müssen an einem sicheren physischen Standort sein, Optionen für Datenträgerverschlüsselung und die Wartung virtueller Maschinen müssen sorgfältig gewählt werden.

Überwachungs- und Ereignisprotokolle müssen sicher auf einem Remotecomputer gespeichert werden.

Der RDP-Zugriff muss auf autorisierte Administratoren beschränkt werden. Citrix empfiehlt, die Smartcard-Anmeldung für Benutzerkonten. Dies gilt insbesondere für Zertifizierungsstellen- und Domänenadministratorkonten.

### Verwandte Informationen

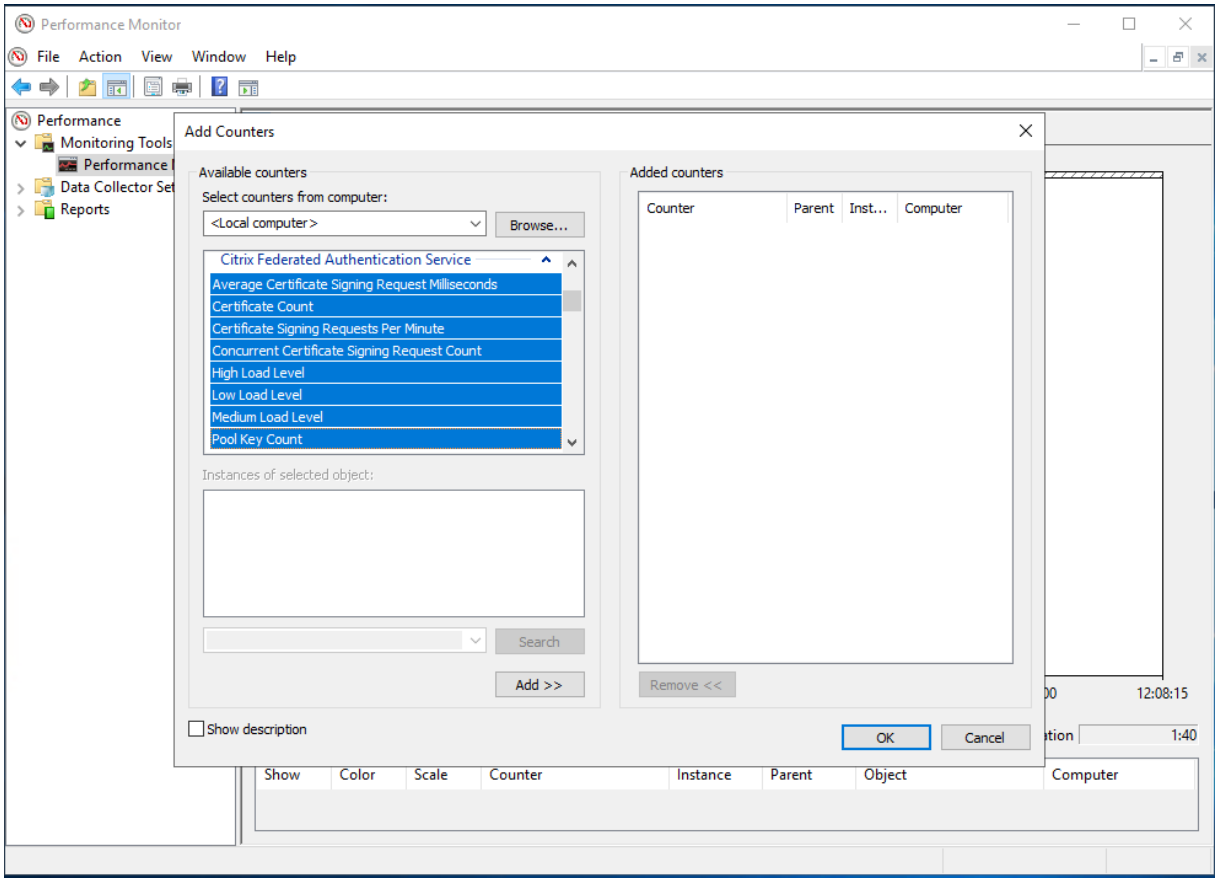
- Installation und Konfiguration ist die primäre Referenz für die Installation und Konfiguration des FAS.
- Eine Einführung in FAS-Architekturen finden Sie unter Bereitstellungsarchitekturen.
- Der Artikel Erweiterte Konfiguration enthält Links zu weiteren Anleitungen.

## Leistungsindikatoren

September 11, 2024

Der FAS enthält eine Reihe von Leistungsindikatoren zur Lastnachverfolgung.




In der folgenden Tabelle werden die Leistungsindikatoren aufgelistet. Sofern nicht anders angegeben, wird jeder Zähler alle 10 Sekunden aktualisiert.

| Name | Beschreibung |
| --- | --- |
| Average Certificate Signing Request Milliseconds | Die durchschnittliche Dauer (in Millisekunden) von Zertifikatsignieranforderungen, berechnet anhand von Daten aus der vorherigen Minute. |
| Certificate Count | Die Anzahl der Zertifikate, die vom Verbundauthentifizierungsdienst verwaltet werden. |
| Certificate Signing Requests Per Minute | Die Anzahl der vom Verbundauthentifizierungsdienst ausgestellten Zertifikatsignieranfragen pro Minute, berechnet anhand von Daten aus der vorherigen Minute. |
| Concurrent Certificate Signing Request Count | Die Anzahl der gleichzeitigen Zertifikatsignieranforderungen, die vom Verbundauthentifizierungsdienst bearbeitet werden. |

| Name | Beschreibung |
| --- | --- |
| Pool Key Count | Die Anzahl der vorgenerierten Schlüsselpaare im Schlüsselpool, die für Zertifikatsignieranforderungen verwendet werden können. |
| Private Key Operations Per Minute | Die Anzahl der Vorgänge für private Zertifikatschlüssel, die vom Verbundauthentifizierungsdienst pro Minute ausgeführt werden, berechnet anhand von Daten aus der vorherigen Minute. |
| Sitzungsanzahl | Die Anzahl der VDA-Sitzungen, die vom Verbundauthentifizierungsdienst verfolgt werden. |
| Low/Medium/High Load Level | Schätzungen der Last, die der Verbundauthentifizierungsdienst für Zertifikatsignieranfragen pro Minute akzeptieren kann. Die Schätzungen werden jede Minute unter Verwendung von Daten aus der vorherigen Minute aktualisiert. Die Überschreitung des Schwellenwerts “High Load”kann dazu führen, dass Starts von veröffentlichten Apps oder Desktops fehlschlagen. |

## Behandlung von Windows-Anmeldeproblemen

September 11, 2024

In diesem Artikel werden die Protokolle und Fehlermeldungen beschrieben, die in Windows verfügbar sind, wenn sich Benutzer mit Zertifikaten oder Smartcards oder mit beidem anmelden. Die Protokolle enthalten Informationen, die bei der Problembehandlung von Authentifizierungsfehlern hilfreich sein können.

### Zertifikate und Public Key-Infrastruktur

Windows Active Directory unterhält mehrere Zertifikatspeicher, in denen Zertifikate für Benutzer verwaltet werden, die sich anmelden.

- **NTAuth-Zertifikatspeicher:** Für die Authentifizierung bei Windows muss die Zertifizierungsstelle, die Benutzerzertifikate sofort ausstellt (Verkettung wird nicht unterstützt), im NTAuth-Speicher platziert werden. Geben Sie zum Anzeigen dieser Zertifikate im certutil-Programm Folgendes ein: `certutil –viewstore –enterprise NTAuth`
- **Speicher für Stamm- und Zwischenzertifikate:** Normalerweise können Zertifikatanmeldesysteme nur ein einzelnes Zertifikat zur Verfügung stellen. Wenn eine Kette verwendet wird, muss daher der Zwischenzertifikatspeicher auf allen Maschinen diese Zertifikate enthalten. Das Stammzertifikat muss im vertrauenswürdigen Stammspeicher und das vorletzte Zertifikat muss im NTAuth-Speicher sein.
- **Anmeldezertifikat-Erweiterungen und Gruppenrichtlinie:** Windows kann so konfiguriert werden, dass die Überprüfung von EKUs und anderen Zertifikatrichtlinien erzwungen wird. Informationen finden Sie in der Microsoft-Dokumentation auf https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/ff404287(v=ws.10).

| Registrierungsrichtlinie | Beschreibung |
|---|---|
| AllowCertificatesWithNoEKU | Wenn deaktiviert, müssen Zertifikate die Smartcard-Anmeldung “Erweiterte Schlüsselverwendung”(Enhanced Key Usage, EKU) enthalten. |
| AllowSignatureOnlyKeys | Standardmäßig filtert Windows die privaten Schlüssel aus Zertifikaten heraus, die RSA-Entschlüsselung nicht zulassen. Diese Option setzt den Filter außer Kraft. |
| AllowTimeInvalidCertificates | Standardmäßig filtert Windows abgelaufene Zertifikate heraus. Diese Option setzt den Filter außer Kraft. |
| EnumerateECCCerts | Aktiviert die Authentifizierung mit elliptischen Kurven. |
| X509HintsNeeded | Mit dieser Option können Benutzer ihr Windows-Anmeldekonto manuell angeben, wenn ein Zertifikat keinen eindeutigen Benutzerprinzipalnamen (UPN) enthält oder der Name mehrdeutig ist. |
| UseCachedCRLOnlyAnd, IgnoreRevocationUnknownErrors | Deaktiviert die Überprüfung von Sperrlisten (auf dem Domänencontroller festgelegt). |

- **Domänencontrollerzertifikate:** Zum Authentifizieren von Kerberos-Verbindungen müssen alle Server entsprechende Domänencontrollerzertifikate haben. Diese können mit dem MMC-Snap-In-Menü “Local Computer Certificate Personal Store”angefordert werden.

## Zuordnung von UPN-Namen und Zertifikaten

Es wird empfohlen, dass die Erweiterung des alternativen Antragstellernamens in Benutzerzertifikaten einen eindeutigen UPN (Benutzerprinzipalname) enthält.

### UPN-Namen in Active Directory

Standardmäßig hat jeder Benutzer in Active Directory eine implizite UPN entsprechend den Mustern <samUsername>@<domainNetBios> und <samUsername>@<domainFQDN>. Die verfügbaren Domänen und FQDNs sind im RootDSE-Eintrag für die Gesamtstruktur enthalten. Für eine einzelne Domäne können mehrere FQDN-Adressen im RootDSE registriert sein.

Darüber hinaus hat jeder Benutzer in Active Directory eine explizite UPN und altUserPrincipalNames. Dies sind LDAP-Einträge, die den UPN für den Benutzer angeben.

Wenn Benutzer anhand der UPN gesucht werden, sucht Windows zuerst in der aktuellen Domäne (basierend auf der Identität des Prozesses bei der Suche nach der UPN) nach expliziten UPNs und dann nach alternativen UPNs. Wenn keine Übereinstimmungen gefunden werden, wird nach der impliziten UPN gesucht, die möglicherweise in anderen Domänen in der Gesamtstruktur aufgelöst wird.

### Zertifikatszuordnungsdienst

Wenn ein Zertifikat keine explizite UPN enthält, kann Active Directory für jede Verwendung ein genaues öffentliches Zertifikat in einem “x509certificate”-Attribut speichern. Um ein solches Zertifikat in einen Benutzer aufzulösen, kann ein Computer eine direkte Abfrage für dieses Attribut durchführen (standardmäßig in einer einzelnen Domäne).

Der Benutzer hat die Option, ein Benutzerkonto anzugeben, das die Suche beschleunigt. Dieses Feature kann außerdem in einer domänenübergreifenden Umgebung verwendet werden.

Wenn die Gesamtstruktur mehrere Domänen enthält und der Benutzer eine Domäne nicht explizit angibt, kann der Speicherort des Zertifikatzuordnungsdiensts mit Active Directory rootDSE angegeben werden. Dies ist auf einer Maschine des globalen Katalogs und umfasst die zwischengespeicherte Anzeige aller x509certificate-Attribute in der Gesamtstruktur. Mit diesem Computer kann ein Benutzerkonto basierend auf dem Zertifikat effizient in jeder Domäne gesucht werden.

## Steuern der Domänencontrollerauswahl für die Anmeldung

Wenn eine Umgebung mehrere Domänencontroller umfasst, ist es sinnvoll einzuschränken, welcher Domänencontroller für die Authentifizierung verwendet wird, damit Protokolle aktiviert und abgerufen werden können.

#### Steuern der Domänencontrollerauswahl

Sie können Windows zur Verwendung eines bestimmten Windows-Domänencontrollers für die Anmeldung zwingen, indem Sie durch Konfigurieren der Datei lmhosts eine explizite Liste mit Domänencontrollern festlegen, die eine Windows-Maschine verwendet: \Windows\System32\drivers\etc\lmhosts.

In diesem Speicherort ist normalerweise eine Beispieldatei namens "lmhosts.sam". Fügen Sie einfach eine Zeile hinzu:

1.2.3.4 dcnetbiosname #PRE #DOM:mydomai

"1.2.3.4"ist die IP-Adresse des Domänencontrollers "dcnetbiosname"in der Domäne "mydomain".

Nach einem Neustart verwendet die Windows-Maschine diese Informationen, um sich bei "mydomain"anzumelden. Diese Konfiguration muss zurückgesetzt werden, wenn das Debuggen abgeschlossen ist.

#### Identifizieren des verwendeten Domänencontrollers

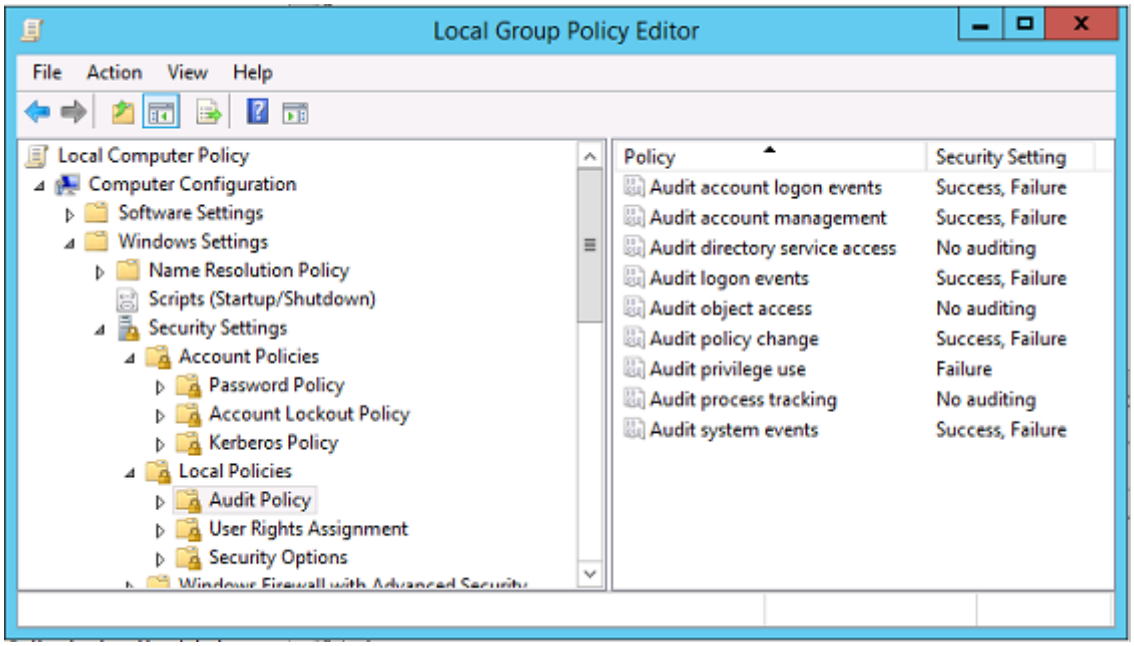
Bei der Anmeldung platziert Windows eine MSDOS-Umgebungsvariable in dem Domänencontroller, der den Benutzer angemeldet hat. Zum Anzeigen starten Sie die Befehlszeile mit dem folgenden Befehl: **echo %LOGONSERVER%**.

Authentifizierungsprotokolle werden auf dem Computer gespeichert, den dieser Befehl zurückgibt.

### Aktivieren von Kontoüberwachungsereignissen

Standardmäßig aktivieren Windows-Domänencontroller keine vollständigen Überwachungsprotokolle für Konten. Überwachungsprotokolle können mit Überwachungsrichtlinien in den Sicherheitseinstellungen im Gruppenrichtlinien-Editor gesteuert werden. Führen Sie auf dem Domänencontroller den Befehl `gpedit.msc` aus, um den Gruppenrichtlinien-Editor zu öffnen. Wenn die Überwachungsrichtlinien aktiviert sind, schreibt der Domänencontroller zusätzliche Ereignisprotokollinformationen in das Sicherheitsprotokoll.




## Zertifikatüberprüfungsprotokolle

### Überprüfen der Zertifikatgültigkeit

Wenn ein Smartcardzertifikat als DER-Zertifikat (kein privater Schlüssel erforderlich) exportiert wird, können Sie es mit folgendem Befehl überprüfen: certutil –verify user.cer

### Aktivieren der CAPI-Protokollierung

Öffnen Sie auf dem Domänencontroller und den Benutzermaschinen die Ereignisanzeige und aktivieren Sie die Protokollierung für Microsoft/Windows/CAPI2/Operational Logs.

Öffnen Sie auf dem Domänencontroller und der VDA-Maschine die Ereignisanzeige und navigieren Sie zu **Anwendungs- und Dienstprotokolle** > **Microsoft** > **Windows** > **CAPI2** > **Betriebsbereit**. Klicken Sie mit der rechten Maustaste auf **Betriebsbereit** und wählen Sie **Protokoll aktivieren**.

Optimieren Sie zusätzlich die CAPI-Protokollierung anhand der Registrierungswerte unter: *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\crypt32*. Die folgenden Werte sind standardmäßig nicht vorhanden, sondern müssen von Ihnen erstellt werden. Löschen Sie die Werte, um zu den Standardeinstellungen der CAPI2-Protokollierung zurückzukehren.

| Wert | Beschreibung |
|---|---|
| DiagLevel (DWORD) | Ausführlichkeitsgrad (0 bis 5) |

| Wert | Beschreibung |
| --- | --- |
| DiagMatchAnyMask (QUADWORD) | Ereignisfilter (0xffffff für alle) |
| DiagProcessName (MULTI_SZ) | Nach Prozessname filtern (z. B. LSASS.exe) |

**CAPI-Protokolle**

| Meldung | Beschreibung |
| --- | --- |
| Build Chain | LSA-Aufruf: CertGetCertificateChain (einschließlich Ergebnis) |
| Verify Revocation | LSA-Aufruf: CertVerifyRevocation (einschließlich Ergebnis) |
| X509 Objects | Im ausführlichen Modus werden Zertifikate und Zertifikatsperrlisten (CRLs) im Verzeichnis \AppData\LocalLow Microsoft\X509Objects ausgegeben |
| Verify Chain Policy | LSA-Aufruf: CertVerifyChainPolicy (einschließlich Parameter) |

**Fehlermeldungen**

| Fehlercode | Beschreibung |
| --- | --- |
| Zertifikat ist nicht vertrauenswürdig | Das Smartcardzertifikat konnte nicht mit Zertifikaten aus den Speichern für Zwischenzertifikate und vertrauenswürdige Stammzertifikate erstellt werden. |
| Certificate revocation check error | Die Zertifikatsperrliste für die Smartcard konnte nicht von der Adresse heruntergeladen werden, die vom Zertifikatsperrlisten-Verteilungspunkt angegeben wurde. Wenn die Zertifikatsperrüberprüfung obligatorisch ist, schlagen Anmeldungen fehl. Weitere Informationen finden Sie im Abschnitt Zertifikate und Public Key-Infrastruktur. |

| Fehlercode | Beschreibung |
|---|---|
| Certificate Usage errors | Das Zertifikat ist nicht für Anmeldungen geeignet. Es ist möglicherweise ein Serverzertifikat oder ein Signaturzertifikat. |

### Kerberos-Protokolle

Erstellen Sie folgende Registrierungswerte, um Kerberos-Protokollierung auf dem Domänencontroller und der Maschine des Endbenutzers zu aktivieren:

| Struktur | 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 aufgezeichnet.

- Meldungen wie “untrusted certificate”sind in der Regel einfach zu diagnostizieren.
- Zwei Fehlercodes sind nur zur Information und können ignoriert werden:
  - KDC_ERR_PREAUTH_REQUIRED (für die Abwärtskompatibilität bei älteren Domänencontrollern)
  - Unknown error 0x4b

### Domänencontroller und Arbeitsstationsprotokolle

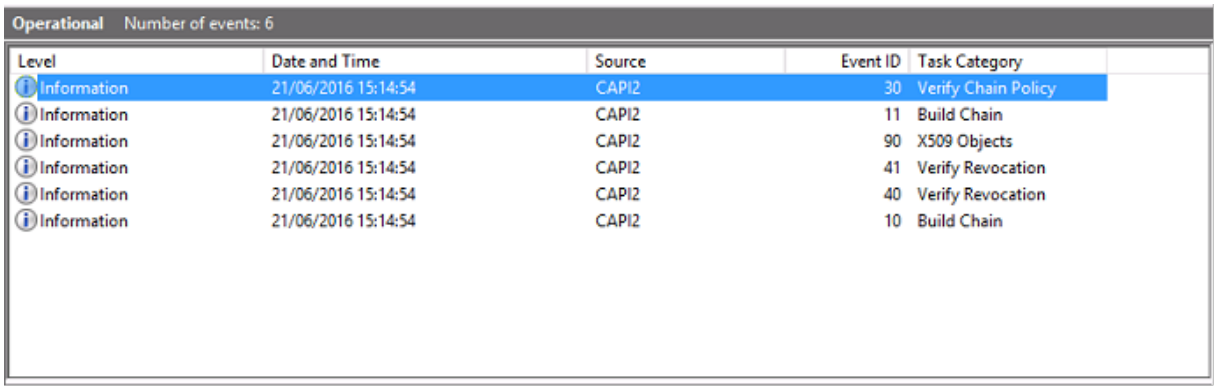
Dieser Abschnitt beschreibt die auf dem Domänencontroller und der Arbeitsstation erwarteten Protokolleinträge, wenn Benutzer sich mit einem Zertifikat anmelden.

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

### CAPI2-Protokoll des Domänencontrollers

Bei einer Anmeldung überprüft der Domänencontroller das Zertifikat des Aufrufenden, wodurch eine Sequenz von Protokolleinträgen wie nachfolgend dargestellt erstellt wird.



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 letzte Meldung zeigt, dass lsass.exe auf dem Domänencontroller basierend auf dem vom VDA bereitgestellten Zertifikat eine Kette erstellt und sie auf Gültigkeit überprüft (einschließlich Sperrung). Das zurückgegebene Ergebnis ist "ERROR_SUCCESS".

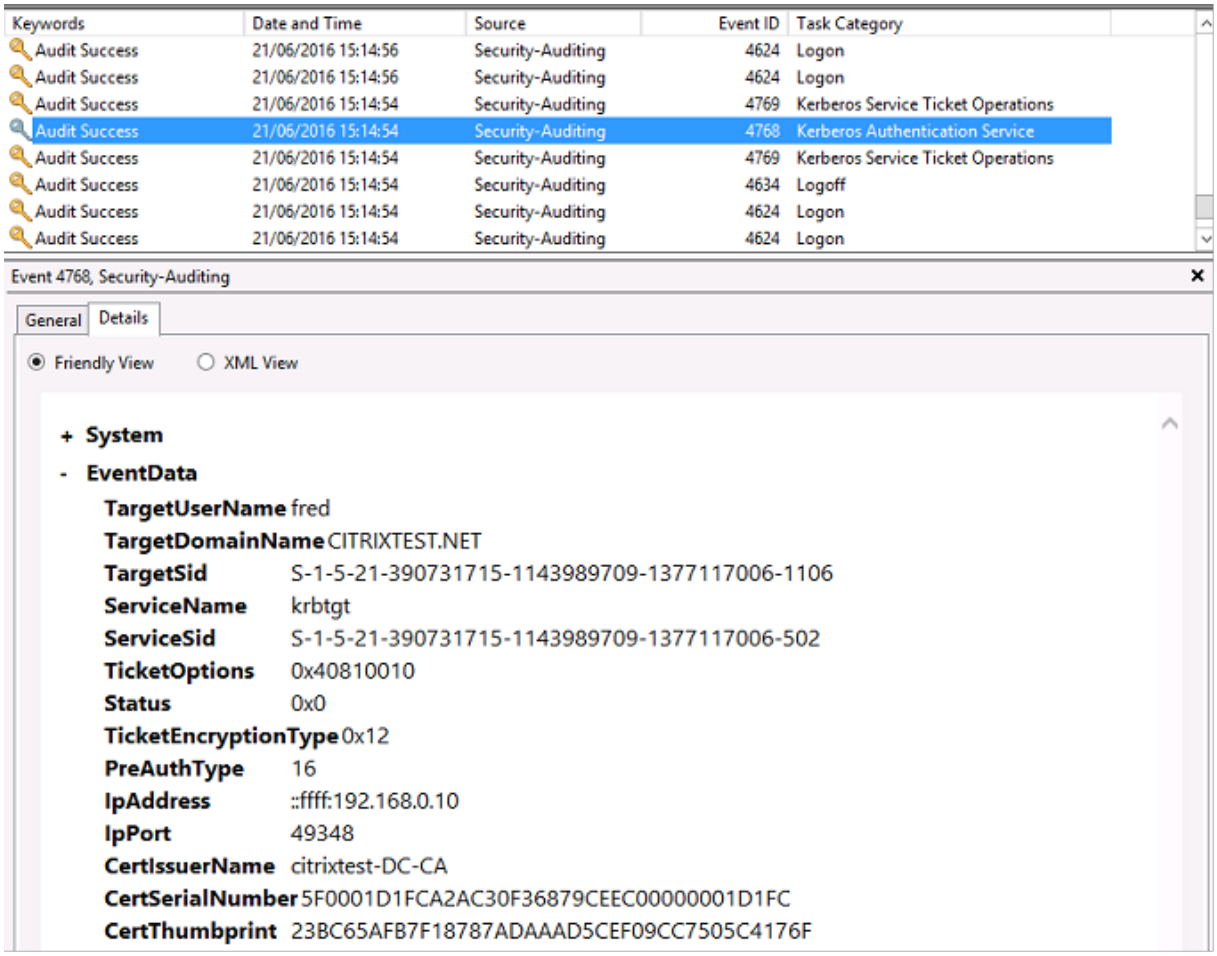
- **CertVerifyCertificateChainPolicy**
  - **Policy**
    - [ **type**] CERT_CHAIN_POLICY_NT_AUTH
    - [ **constant**] 6
  - **Certificate**
    - [ **fileRef**] 23BC65AFB7F18787ADAAAD5CEF09CC7505C4176F.cer
    - [ **subjectName**] fred
  - **CertificateChain**
    - [ **chainRef**] {FF03F79B-52F8-4C93-877A-5DFFE40B9574}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

### Sicherheitsprotokoll des Domänencontrollers

Der Domänencontroller zeigt eine Reihe von Anmeldeereignissen an, wobei das Ereignis 4768, die Verwendung des Zertifikats zum Ausstellen des Kerberos Ticket Granting Ticket (krbtgt), das wichtigste ist.

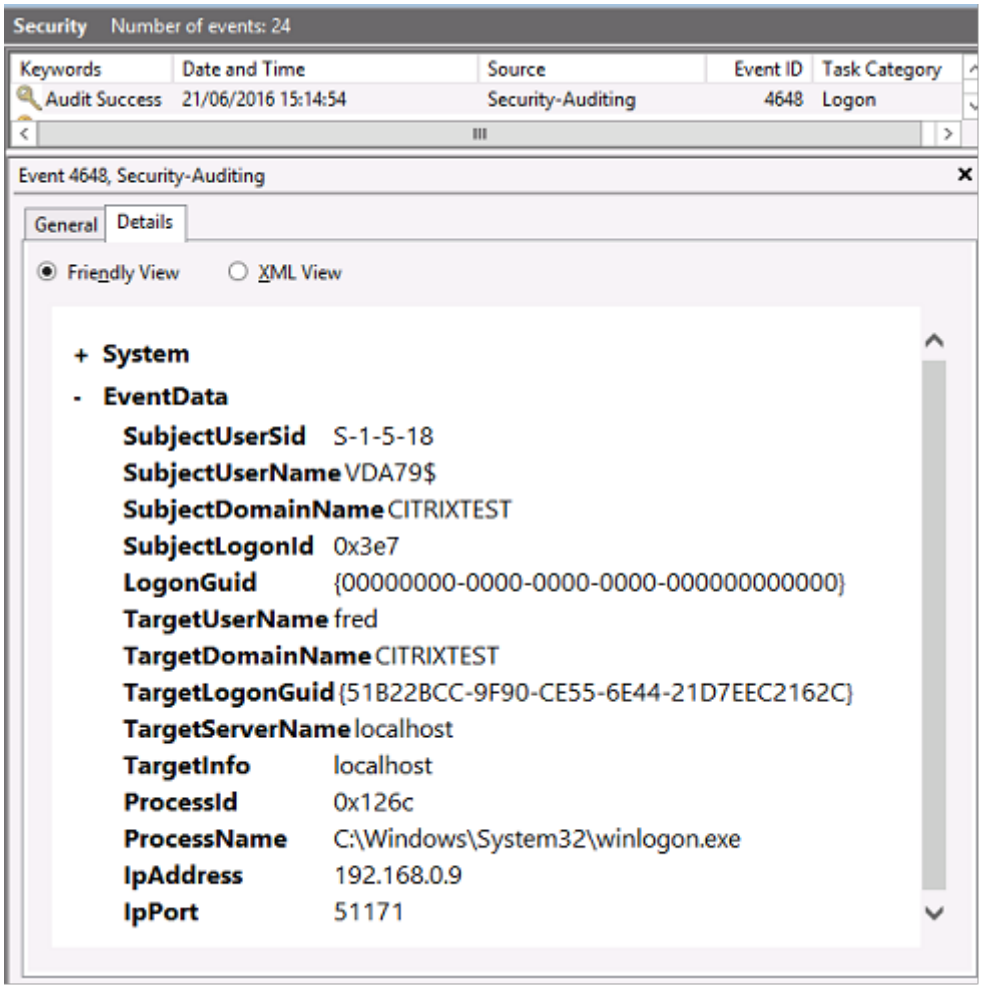
Die vorhergehenden Meldungen zeigen, wie sich das Maschinenkonto des Servers beim Domänencontroller authentifiziert. Die darauffolgenden Meldungen zeigen, wie mit dem Benutzerkonto, das nun zum neuen krbtgt gehört, die Authentifizierung beim Domänencontroller durchgeführt wird.




### VDA-Sicherheitsprotokoll

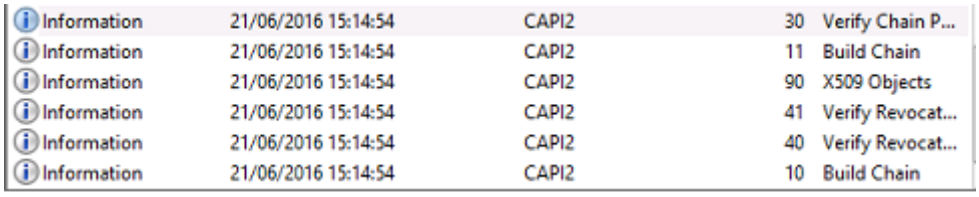
Die VDA-Sicherheitsüberwachungsprotokolle, die der Anmeldung entsprechen, sind der Eintrag mit der Ereignis-ID 4648, der von winlogon.exe verursacht wurde.




**VDA-CAPI-Protokoll**

Dieses VDA-CAPI-Beispielprotokoll zeigt eine erstellte Kette und eine Überprüfungssequenz von lsass.exe, mit der das Domänencontrollerzertifikat (dc.citrixtest.net) überprüft wurde.

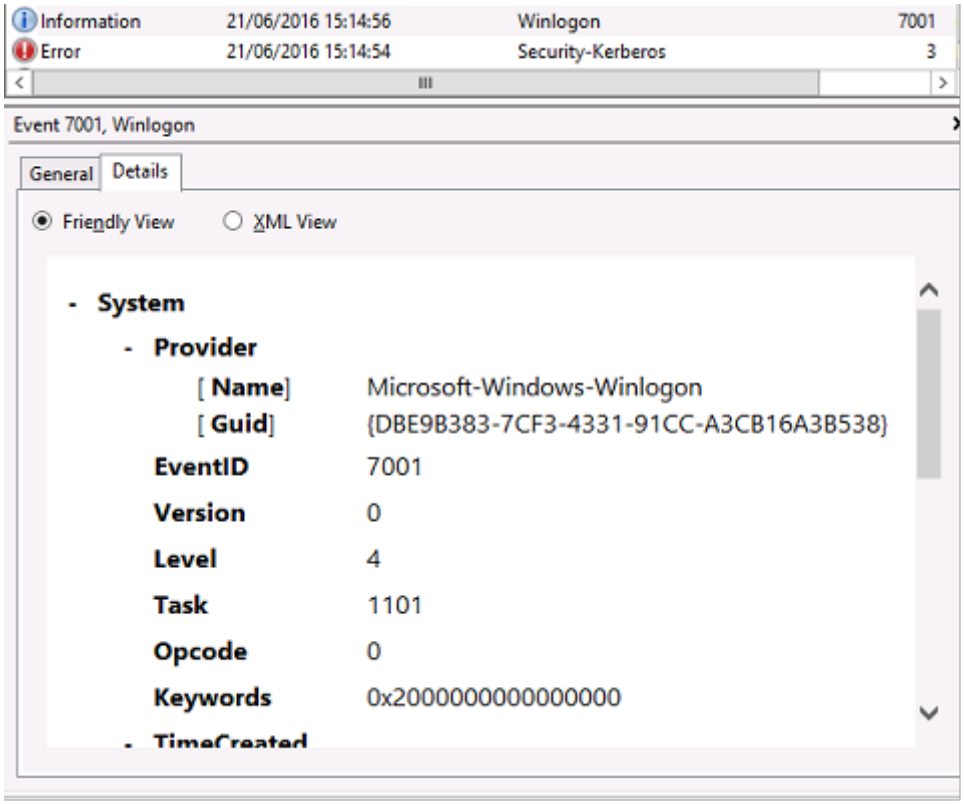


- **UserData**
  - **CertVerifyCertificateChainPolicy**
    - **Policy**
      - [ **type**] CERT_CHAIN_POLICY_NT_AUTH
      - [ **constant**] 6
    - **Certificate**
      - [ **fileRef**] 813C6D12E1E1800E61B8DB071E186EB912B7
      - [ **subjectName**] dc.citrixtest.net
    - **CertificateChain**
      - [ **chainRef**] {84E0B3D1-A4D4-4AC7-BA99-5291415B343
    - **Flags**
      - [ **value**] 0
    - **Status**
      - [ **chainIndex**] -1

**VDA-Systemprotokoll**

Wenn die Kerberos-Protokollierung aktiviert ist, enthält das Systemprotokoll die Fehlermeldung KDC_ERR_PREAUTH_REQUIRED, die ignoriert werden kann, und einen Eintrag von Winlogon zur erfolgreichen Kerberos-Anmeldung.



## Überwachen von FAS mit dem Windows-Ereignisprotokoll

Alle FAS-Ereignisse werden in das Windows-Anwendungsereignisprotokoll geschrieben. Sie können Produkte wie System Center Operations Manager (SCOM) verwenden, um den Zustand Ihres FAS-Dienstes mit den hier beschriebenen Prozessen und Ereignissen zu überwachen.

### Wird der FAS-Dienst ausgeführt?

Um festzustellen, ob der FAS-Dienst ausgeführt wird, überwachen Sie den Prozess Citrix.Authentication.FederatedA

In diesem Abschnitt werden nur die wichtigsten Ereignisse zur Überwachung des FAS-Dienstes beschrieben. Eine vollständige Liste der FAS-Ereigniscodes finden Sie unter FAS-Ereignisprotokolle.

### FAS-Integritätsereignisse

Die folgenden Ereignisse zeigen, ob Ihr FAS-Dienst fehlerfrei ist.

Die Ereignisquelle ist **Citrix.Authentication.FederatedAuthenticationService**.

| Ereignis | Ereignistext | Erläuterung | Hinweise |
|---|---|---|---|
| [S003] | Administrator [{0}] setting Maintenance Mode to [{1}] | Für den FAS-Dienst wurde der Wartungsmodus aktiviert oder deaktiviert. | Im Wartungsmodus kann der FAS-Server nicht für Single Sign-On verwendet werden. |
| [S022] | Administrator [{0}] setting Maintenance Mode to Off | Der FAS-Dienst wurde aus dem Wartungsmodus genommen. | Ab FAS 10.7/Citrix Virtual Apps and Desktops 2109 verfügbar. |
| [S023] | Administrator [{0}] setting Maintenance Mode to On | Der FAS-Dienst wurde in den Wartungsmodus versetzt. | Ab FAS 10.7/Citrix Virtual Apps and Desktops 2109 verfügbar. |

| Ereignis | Ereignistext | Erläuterung | Hinweise |
| --- | --- | --- | --- |
| [S123] | Failed to issue a certificate for [upn: {0} role: {1}] [exception: {2}] | Dieses Ereignis tritt nach [S124] ein, wenn keine der Zertifizierungsstellen für FAS mit einem erfolgreich ausgestelltem Benutzerzertifikat konfiguriert wurde. Single Sign-on schlägt für diesen Benutzer fehl. | Dieses Ereignis weist darauf hin, dass alle konfigurierten Zertifizierungsstellen nicht funktionieren. Wenn die FAS-Konfiguration ein HSM verwendet, kann dies auch darauf hinweisen, dass das HSM nicht funktioniert. |
| [S124] | Failed to issue a certificate for [upn: {0} role: {1}] at [certificate authority: {2}] [exception: {3}] | Ein Fehler ist aufgetreten, als FAS versuchte, ein Benutzerzertifikat von der angegebenen Zertifizierungsstelle anzufordern. Wenn FAS mit mehr als einer Zertifizierungsstelle konfiguriert ist, versucht FAS die Anforderung von einer anderen Zertifizierungsstelle. | Dieses Ereignis kann darauf hinweisen, dass die Zertifizierungsstelle nicht funktioniert oder nicht erreichbar ist. Wenn die FAS-Konfiguration ein HSM verwendet, kann dies auch darauf hinweisen, dass das HSM nicht funktioniert. Die Ausnahme kann verwendet werden, um die Ursache des Problems zu ermitteln. |

| Ereignis | Ereignistext | Erläuterung | Hinweise |
|---|---|---|---|
| [S413] | Authorization certificate expiring soon ({0} days left). Certificate details: {1} | Dieses Ereignis wird in Abständen generiert, wenn das FAS-Autorisierungszertifikat kurz vor dem Ablauf steht. Standardmäßig wird das Ereignis täglich generiert, wenn das Berechtigungszertifikat innerhalb von 30 Tagen abläuft. | Die Standardeinstellungen können mit dem Cmdlet **Set-FasRaCertificateMonitor** angepasst werden; siehe PowerShell-Cmdlets. |
| [S414] | Authorization certificate has expired. Certificate details: {0} | Dieses Ereignis wird in Abständen generiert, wenn das FAS-Autorisierungszertifikat abgelaufen ist. Standardmäßig wird das Ereignis täglich generiert. | Nach Ablauf ist FAS nicht in der Lage, neue Benutzerzertifikate zu generieren, und Single Sign-On schlägt fehl. |

#### Cloud-bezogene FAS-Ereignisse

Wenn Sie FAS mit Citrix Cloud verwenden, zeigen die folgenden Ereignisse, ob Ihr FAS-Dienst fehlerfrei ist.

Die Ereignisquelle ist **Citrix.Fas.Cloud**.

| Ereignis | Ereignistext | Erläuterung | Hinweise |
|---|---|---|---|
| [S012] | The FAS service is available for single sign-on from Citrix Cloud | Dieses Ereignis weist darauf hin, dass Single Sign-On von Workspace (d. h. Citrix Cloud) funktionieren sollte. | Vor der Ausgabe dieses Ereignisses prüft FAS (1), ob es konfiguriert ist, (2) sich nicht im Wartungsmodus befindet und (3) mit Citrix Cloud verbunden ist. |

| Ereignis | Ereignistext | Erläuterung | Hinweise |
|---|---|---|---|
| [S013] | The FAS service is not available for single sign-on from Citrix Cloud. [{0}] Further details can be found in the admin console. | Dieses Ereignis weist darauf hin, dass FAS kein Single Sign-On von Workspace (d. h. Citrix Cloud) aus bereitstellen kann. Die Meldung enthält den Grund, warum Single Sign-On nicht funktioniert. | FAS hält eine dauerhafte Verbindung zu Citrix Cloud aufrecht. Von Zeit zu Zeit kann diese Verbindung aus verschiedenen Gründen beendet werden (z. B. ein Netzwerkausfall oder eine Verbindungslebens-dauerrichtlinie auf einem Proxyserver). In diesem Fall enthält der Ereignistext "Service is not connected to the cloud". **Dies ist ein normales Verhalten, und FAS versucht sofort, die Verbindung zu Citrix Cloud wiederherzustellen**. |

**Sicherheitsereignisse**

Die folgenden Ereignisse deuten darauf hin, dass eine nicht autorisierte Einheit versucht hat, FAS zu verwenden.

Die Ereignisquelle ist **Citrix.Authentication.FederatedAuthenticationService**.

| Ereignis | Ereignistext | Erläuterung |
|---|---|---|
| [S001] | ACCESS DENIED: User [{0}] is not a member of the Administrators group | Es wurde versucht, die Konfiguration von FAS anzuzeigen oder zu ändern, aber es war kein FAS-Administrator. |
| [S002] | ACCESS DENIED: User [{0}] is not an Administrator of Role [{1}] | Es wurde versucht, die Konfiguration einer FAS-Regel anzuzeigen oder zu ändern, aber es war kein FAS-Administrator. |
| [S101] | Server [{0}] is not authorized to assert identities in role [{1}] | Es wurde versucht, ein Assert von Benutzeridentitäten durchzuführen, aber das Konto ist dazu nicht berechtigt. Nur StoreFront-Server, die in der FAS-Regelkonfiguration (und Workspace, falls zutreffend) als zulässig eingestellt wurden, dürfen ein Assert von Benutzeridentitäten durchführen. |
| [S104] | Server [{0}] failed to assert UPN [{1}] (UPN not allowed by role [{2}]) | Es wurde versucht, ein Assert von Benutzeridentitäten durchzuführen, aber das Konto des Benutzers ist gemäß der Konfiguration der FAS-Regel nicht zulässig. |
| [S205] | Relying party access denied - the calling account [{0}] is not a permitted relying party of the rule [{1}] | Ein VDA hat versucht, Single Sign-On mit FAS durchzuführen, aber der VDA ist gemäß der FAS-Regelkonfiguration nicht zulässig. |

### FAS-Ereignisprotokolle

Die folgenden Tabellen enthalten die vom FAS generierten Ereignisprotokolleinträge.

**Administrationsereignisse [Verbundauthentifizierungsdienst]**

[Ereignisquelle: Citrix.Authentication.FederatedAuthenticationService]

Diese Ereignisse werden bei einer Konfigurationsänderung des FAS-Servers protokolliert.

Protokollcodes

[S001] ACCESS DENIED: User [{0}] is not a member of Administrators group

[S002] ACCESS DENIED: User [{0}] is not an Administrator of Role [{1}]

[S003] Administrator [{0}] setting Maintenance Mode to [{1}]

[S004] Administrator [{0}] requesting authorization certificate from CA [{1}] using templates [{2} and {3}]

[S005] Administrator [{0}] de-authorizing CA [{1}]

[S006] Administrator [{0}] creating Certificate Definition [{1}]

[S007] Administrator [{0}] updating Certificate Definition [{1}]

[S008] Administrator [{0}] deleting Certificate Definition [{1}]

[S009] Administrator [{0}] creating Rule [{1}]

[S010] Administrator [{0}] updating Rule [{1}]

[S011] Administrator [{0}] deleting Rule [{1}]

[S012] Administrator [{0}] creating certificate [upn: {1} sid: {2} rule: {3}]Certificate Definition: {4} Security Context: {5}]

[S013] Administrator [{0}] deleting certificates [upn: {1} role: {2} Certificate Definition: {3} Security Context: {4}]

[S015] Administrator [{0}] creating certificate request [TPM: {1}]

[S016] Administrator [{0}] importing Authorization certificate [Reference: {1}]

[S022] Administrator [{0}] setting Maintenance Mode to Off

[S023] Administrator [{0}] setting Maintenance Mode to On

[S024] Administrator [{0}] setting system health monitor

[S025] Administrator [{0}] setting system health monitor

[S026] Administrator [{0}] setting RA Certificate Monitor

[S027] Administrator [{0}] resetting RA certificate monitor

[S050] Administrator [{0}] creating cloud configuration: [{1}]

[S051] Administrator [{0}] updating cloud configuration: [{1}]

Protokollcodes

[S052] Administrator [{0}] removing cloud configuration

[S060] Administrator [{0}] Requesting Cloud Registration. Instance: {1}

[S060] Administrator [{0}] Requesting Direct Trust Cloud Registration. Instance: {1} CloudServiceUrlFormat: {2}

[S061] Administrator [{0}] Completing Cloud Registration. Resource location: {1}, Rule name: {2}

[S062] Administrator [{0}] Completed Cloud Registration. Resource location: {1} ({2}), Rule name: {3}, Customer: {4} ({5})

[S063] A KRS error occurred during cloud registration. The exception was {0}

[S064] An unknown error occurred during cloud registration. The exception was {0}

Logcodes

[S401] Performing configuration upgrade - [From version {0} to version {1}]

[S402] ERROR: The Citrix Federated Authentication Service must be run as Network Service [currently running as: {0}]

[S404] Forcefully erasing the Citrix Federated Authentication Service database

[S405] An error occurred while migrating data from the registry to the database: [{0}]

[S406] Migration of data from registry to database is complete (note: user certificates are not migrated)

[S407] Registry-based data was not migrated to a database since a database already existed

[S408] Cannot downgrade the configuration –[From version {0} to version {1}]

[S409] ThreadPool configuration succeeded - MinThreads adjusted from [workers: {0} completion: {1}] to: [workers: {2} completion: {3}]

[S410] ThreadPool configuration failed - failed to adjust MinThreads from [workers: {0} completion: {1}] to: [workers: {2} completion: {3}]; this may impact the scalability of the FAS server

[S411] Error starting the FAS service: [{0}]

[S412] Configuration upgrade complete –[From version {0} to version {1}]

[S413] Authorization certificate expiring soon ({0} days left). Certificate details: {1}

[S414] Authorization certificate has expired. Certificate details: {0}

[S415] Authorization certificate checks completed. {0} issues were logged. Next check is due in {1}

### Erstellen von Identitätsassertions [Verbundauthentifizierungsdienst]

[Ereignisquelle: Citrix.Authentication.FederatedAuthenticationService]

Diese Ereignisse werden zur Laufzeit auf dem FAS-Server protokolliert, wenn von einem vertrauenswürdigen Server eine Benutzeranmeldung bestätigt wird.

| Logcodes |
| --- |
| [S101] Server [{0}] is not authorized to assert identities in role [{1}] |
| [S102] Server [{0}] failed to assert UPN [{1}] (Exception: {2}{3}) |
| [S103] Server [{0}] requested UPN [{1}] SID {2}, but lookup returned SID {3} |
| [S104] Server [{0}] failed to assert UPN [{1}] (UPN not allowed by role [{2}]) |
| [S105] Server [{0}] issued identity assertion [upn: {1}, role {2}, Security Context: [{3}]] |
| [S120] Issuing certificate to [upn: {0} role: {1} Security Context: [{2}]] |
| [S121] Certificate issued to [upn: {0} role: {1}] by [certificate authority: {2}] |
| [S122] Warning: Server is overloaded [upn: {0} role: {1}][Requests per minute {2}]. |
| [S123] Failed to issue a certificate for [upn: {0} role: {1}] [exception: {2}] |
| [S124] Failed to issue a certificate for [upn: {0} role: {1}] at [certificate authority: {2}] [exception: {3}] |

### Bei Agieren als vertrauende Seite [Verbundauthentifizierungsdienst]

[Ereignisquelle: Citrix.Authentication.FederatedAuthenticationService]

Diese Ereignisse werden zur Laufzeit auf dem FAS-Server protokolliert, wenn von einem VDA ein Benutzer angemeldet wird.

| Logcodes |
| --- |
| [S201] Relying party [{0}] does not have access to a password. |
| [S202] Relying party [{0}] does not have access to a certificate. |
| [S203] Relying party [{0}] does not have access to the Logon CSP |
| [S204] Relying party [{0}] accessing the Logon CSP for [upn: {1}] in role: [{2}] [Operation: {3}] as authorized by [{4}] |
| [S205] Relying party access denied - the calling account [{0}] is not a permitted relying party of the rule [{1}] |
| [S206] Calling account [{0}] is not a relying party |

| Logcodes |
| --- |
| [S208] Private Key operation failed [Operation: {0} upn: {1} role: {2} certificateDefinition {3} Error {4} {5}]. |

**Server für sitzungsinterne Zertifikate [Verbundauthentifizierungsdienst]**

[Ereignisquelle: Citrix.Authentication.FederatedAuthenticationService]

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

| Logcodes |
| --- |
| [S301] Access Denied: User [{0}] does not have access to a Virtual Smart Card |
| [S302] User [{0}] requested unknown Virtual Smart Card [thumbprint: {1}] |
| [S303] Access Denied: User [{0}] does not match Virtual Smart Card [upn: {1}] |
| [S304] User [{0}] running program [{1}] on computer [{2}] using Virtual Smart Card [upn: {3} role: {4} thumbprint: {5}] for private key operation [{6}] |
| [S305] Private Key operation failed [Operation: {0}] [upn: {1} role: {2} containerName {3} Error {4} {5}]. |

**FAS-Assertion-Plug-In [Verbundauthentifizierungsdienst]**

[Ereignisquelle: Citrix.Authentication.FederatedAuthenticationService]

Diese Ereignisse werden vom FAS-Assertion-Plug-In protokolliert.

| Logcodes |
| --- |
| [S500] No FAS assertion plug-in is configured |
| [S501] The configured FAS assertion plug-in could not be loaded [exception:{0}] |
| [S502] FAS assertion plug-in loaded [pluginId={0}] [assembly={1}] [location={2}] |
| [S503] Server [{0}] failed to assert UPN [{1}] (logon evidence was supplied but the plug-in [{2}] does not support it) |
| [S504] Server [{0}] failed to assert UPN [{1}] (logon evidence was supplied but there is no configured FAS plug-in) |
| [S505] Server [{0}] failed to assert UPN [{1}] (the plug-in [{2}] rejected the logon evidence with status [{3}] and message [{4}]) |

| Logcodes |
| --- |
| [S506] The plug-in [{0}] accepted logon evidence from server [{1}] for UPN [{2}] with message [{3}] |
| [S507] Server [{0}] failed to assert UPN [{1}] (the plug-in [{2}] threw exception [{3}] during method [{4}]) |
| [S507] Server [{0}] failed to assert UPN [{1}] (the plug-in [{2}] threw exception [{3}]) |
| [S508] Server [{0}] failed to assert UPN [{1}] (access disposition was supplied but the plug-in [{2}] does not support it) |
| [S509] Server [{0}] failed to assert UPN [{1}] (access disposition was supplied but there is no configured FAS plug-in) |
| [S510] Server [{0}] failed to assert UPN [{1}] (the access disposition was considered invalid by plug-in [{2}] |

**Workspace mit FAS [Verbundauthentifizierungsdienst]**

[Event Source: Citrix.Fas.Cloud]

Diese Ereignisse werden protokolliert, wenn FAS mit Workspace verwendet wird.

| Logcodes |
| --- |
| [S001] Rotated Citrix Cloud authorization key [fas id: {0}] [old key id:{1}] [new key id:{2}] |
| [S002] The cloud support module is starting. FasHub cloud service URL: {0} |
| [S003] FAS registered with the cloud [fas id: {0}] [transaction id: {1}] |
| [S004] FAS failed to register with the cloud [fas id: {0}] [transaction id: {1}] [exception: {2}] |
| [S005] FAS sent its current configuration to the cloud [fas id: {0}] [transaction id: {1}] |
| [S006] FAS failed to send its current configuration to the cloud [fas id: {0}] [transaction id: {1}] [exception: {2}] |
| [S007] FAS unregistered from the cloud [fas id: {0}] [transaction id: {1}] |
| [S009] FAS failed to unregister from the cloud [fas id: {0}] [transaction id: {1}] [exception: {2}] |
| [S010] The FAS service is connected to the cloud messaging URL: {0} |
| [S011] The FAS service is not connected to the cloud |
| [S012] The FAS service is available for single sign-on from Citrix Cloud |
| [S013] The FAS service is not available for single sign-on from Citrix Cloud. [{0}] Further details can be found in the admin console |

| Logcodes |
| --- |
| [S014] A call to the cloud service <service name> failed [fas id: {0}] [transaction id: {1}] [exception: {2}] |
| [S015] A message from Citrix Cloud was blocked because the caller is not permitted [message ID {0}] [transaction ID {1}] [caller {2}] |
| [S016] A call to the cloud service <service name> succeeded [fas id: {0}] [transaction id: {1}] |
| [S019] FAS downloaded its configuration from the cloud [fas id: {0}] [transaction id: {1}] |
| [S020] FAS failed to download its configuration from the cloud [fas id: {0}] [transaction id: {1}] [exception: {2}] |
| [S021] The cloud support module failed to start. Exception: {0} |
| [S022] The cloud support module is stopping |
| [S023] Failed to rotate Citrix Cloud authorization key [fas id: {0}] [current key id:{1}] [new key id:{2}] [keys in cloud:{3}] |
| [S024] Initiating rotation of Citrix Cloud authorization key [fas id: {0}] [current key id:{1}] [new key id:{2}] |
| [S025] This service's authorization key is present in the Citrix Cloud [current key: {0}] [keys in cloud: {1}] |
| [S026] This service's authorization key is not present in the Citrix Cloud [current key: {0}] [keys in cloud: {1}] |
| [S027] Upgraded the Citrix Cloud authorization key storage format [fas id: {0}] |

**Anmeldung [VDA]**

[Ereignisquelle: Citrix.Authentication.IdentityAssertion]

Diese Ereignisse werden bei der Anmeldung auf dem VDA protokolliert.

| Logcodes |
| --- |
| [S101] Identity Assertion Logon failed. Unrecognised Federated Authentication Service [id: {0}] |
| [S102] Identity Assertion Logon failed. Could not lookup SID for {0} [Exception: {1}{2}] |
| [S103] Identity Assertion Logon failed. User {0} has SID {1}, expected SID {2} |
| [S104] Identity Assertion Logon failed. Failed to connect to Federated Authentication Service: {0} [Error: {1} {2}] |
| [S105] Identity Assertion Logon. Logging in [Username: {0} Domain: {1}] |

| Logcodes |
| --- |
| [S106] Identity Assertion Logon.\n\nFederated Authentication Service: {0}\n\nLogging in [Certificate: {1}] |
| [S107] Identity Assertion Logon failed. [Exception: {0}{1}] |
| [S108] Identity Assertion Subsystem. ACCESS_DENIED [Caller: {0}] |

**Sitzungsinterne Zertifikate [VDA]**

[Ereignisquelle: Citrix.Authentication.IdentityAssertion]

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

| Logcodes |
| --- |
| [S201] Virtual smart card access authorized by [{0}] for [PID: {1} Program Name: {2}Certificate thumbprint: {3}] |
| [S203] Virtual Smart Card Subsystem. Access Denied [caller: {0}, session {1}] |
| [S204] Virtual Smart Card Subsystem. Smart card support disabled |

**Zertifikatanforderung und Schlüsselpaargenerierung [Verbundauthentifizierungsdienst]**

[Event Source: Citrix.Fas.PkiCore]

Diese Ereignisse werden protokolliert, wenn der FAS-Server low-level kryptographische Vorgänge durchführt.

| Logcodes |
| --- |
| [S001] TrustArea::TrustArea: Installed certificate [TrustArea: {0} Certificate {1}TrustAreaJoinParameters {2}] |
| [S014] Pkcs10Request::Create: Created PKCS10 request [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}] |

| Logcodes |
| --- |
| [S104] MicrosoftCertificateAuthority::GetCredentials: Authorized to use {0} |
| [S105] MicrosoftCertificateAuthority::SubmitCertificateRequest Error submit response [{0}] |
| [S106] MicrosoftCertificateAuthority::SubmitCertificateRequest Issued certificate [{0}] |
| [S112] MicrosoftCertificateAuthority::SubmitCertificateRequest - Waiting for approval [CR_DISP_UNDER_SUBMISSION] [Reference: {0}] |

### Endbenutzerfehlermeldungen

In diesem Abschnitt finden Sie allgemeine Fehlermeldungen, die Benutzern auf der Windows-Anmeldeseite angezeigt werden.

| Angezeigte Fehlermeldung | Beschreibung und Referenz |
| --- | --- |
| Benutzername oder Kennwort ist ungültig | Der Computer glaubt, dass Sie ein gültiges Zertifikat und einen gültigen privaten Schlüssel haben, aber der Kerberos-Domänencontroller hat die Verbindung zurückgewiesen. Weitere Informationen finden unter ***Kerberos-Protokolle***. |
| Sie konnten nicht angemeldet werden. 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 Smartcardauthentifizierung konfiguriert. Registrieren Sie den Domänencontroller für ein Zertifikat “Kerberos-Authentifizierung”, “Domänencontrollerauthentifizierung”oder “Domänencontroller”. Dies ist einen Versuch wert, selbst wenn die vorhandenen Zertifikate anscheinend gültig sind. |
| Das System meldet Sie möglicherweise nicht an. Das für die Authentifizierung verwendete Smartcardzertifikat ist nicht vertrauenswürdig. | Die Zwischen- und Stammzertifikate sind nicht auf dem lokalen Computer installiert. Siehe Zertifikate und Public Key-Infrastruktur |
| Ungültige Anforderung | Dies weist meist darauf hin, dass die Erweiterungen des Zertifikats nicht ordnungsgemäß festgelegt sind oder dass der RSA-Schlüssel zu kurz ist. (<2048 Bits). |

### Verwandte Informationen

- Configuring a domain for Smart Card Logon
- Smart Card Logon policies
- Enabling CAPI logging
- Aktivieren der Kerberos-Ereignisprotokollierung
- Richtlinien zum Aktivieren der Smartcardanmeldung bei Zertifizierungsstellen von Drittanbietern

## PowerShell-Cmdlets

September 11, 2024

Die Verwaltungskonsole des Verbundauthentifizierungsdiensts (FAS) eignet sich für einfache Bereitstellungen, während die PowerShell-Oberfläche erweiterte Optionen bietet. Wenn Sie Optionen verwenden möchten, die in der Konsole nicht verfügbar sind, empfiehlt Citrix, ausschließlich PowerShell für die Konfiguration zu verwenden.

Mit dem folgenden Befehl werden die FAS-PowerShell-Cmdlets hinzugefügt:

```
1 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/.

## Bereitstellungsarchitekturen

September 11, 2024

### Einführung

Der Verbundauthentifizierungsdienst (Federated Authentication Service, FAS) ist eine Citrix Komponente zur Integration in die Active Directory-Zertifizierungsstelle, die eine nahtlose Benutzerauthentifizierung in einer Citrix Umgebung ermöglicht. In diesem Dokument werden die verschiedenen Authentifizierungsarchitekturen beschrieben, die für diverse Bereitstellungen geeignet sein können.

Wenn der FAS aktiviert ist, delegiert er die Entscheidung über die Benutzerauthentifizierung an vertrauenswürdige StoreFront-Server. StoreFront hat umfassende integrierte Authentifizierungsoptionen, die auf modernen Internet-Technologien aufbauen. Es kann problemlos mit dem StoreFront-SDK oder IIS-Plug-Ins anderer Hersteller erweitert werden. Das grundlegende Designziel besteht darin, dass jede Technologie zur Authentifizierung von Benutzern bei einer Website nun auch für die Anmeldung bei einer Citrix Virtual Apps- oder Citrix Virtual Desktops-Bereitstellung verwendet werden kann.

In diesem Dokument werden die Beispiele einiger Bereitstellungsarchitekturen in der Reihenfolge zunehmender Komplexität vorgestellt.

- Interne Bereitstellung
- Citrix Gateway-Bereitstellung
- ADFS SAML
- B2B-Kontozuordnung
- Einbindung in Azure AD unter Windows 10

Das Dokument enthält außerdem Links zu verwandten FAS-Artikeln. Für alle Architekturen gilt der Artikel Installation und Konfiguration als primäre Referenz für das Einrichten des FAS.

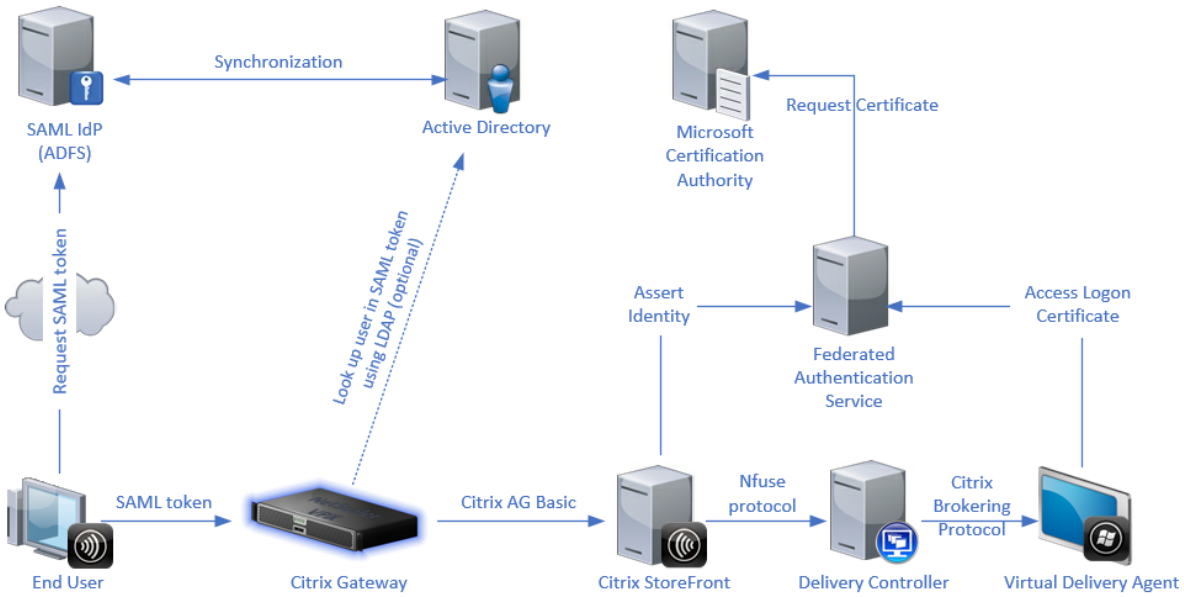
### Architektur im Überblick

Der FAS kann für Active Directory-Benutzer, die von StoreFront authentifiziert werden, automatisch Zertifikate der Smartcardklasse ausstellen. Dabei werden ähnliche APIs verwendet, wie bei Tools zum Bereitstellen physischer Smartcards. Wenn ein Benutzer an einen Citrix Virtual Apps- oder Citrix Virtual Desktops-VDA vermittelt wird, wird das Zertifikat der Maschine angehängt und die Anmeldung wird von der Windows-Domäne als normale Smartcardauthentifizierung behandelt.

Vertrauenswürdige StoreFront-Server kontaktieren den FAS, wenn Benutzer Zugriff auf die Citrix Umgebung anfordern. Der FAS stellt ein Ticket aus, mit dem eine einzelne Citrix Virtual Apps- oder Citrix Virtual Desktops-Sitzung sich mit einem Zertifikat für die Sitzung authentifizieren kann. Wenn ein VDA einen Benutzer authentifizieren muss, stellt er eine Verbindung mit dem FAS her und löst das Ticket aus. Nur der FAS hat Zugriff auf den privaten Schlüssel des Benutzerzertifikats. Der VDA muss jeden erforderlichen Signier- und Entschlüsselungsvorgang mit dem Zertifikat an den FAS senden.

Die folgende Abbildung zeigt das Zusammenwirken des FAS mit einer Microsoft-Zertifizierungsstelle und die Bereitstellung entsprechender Dienste für StoreFront und Citrix Virtual Apps and Desktops-VDAs.




## Interne Bereitstellung

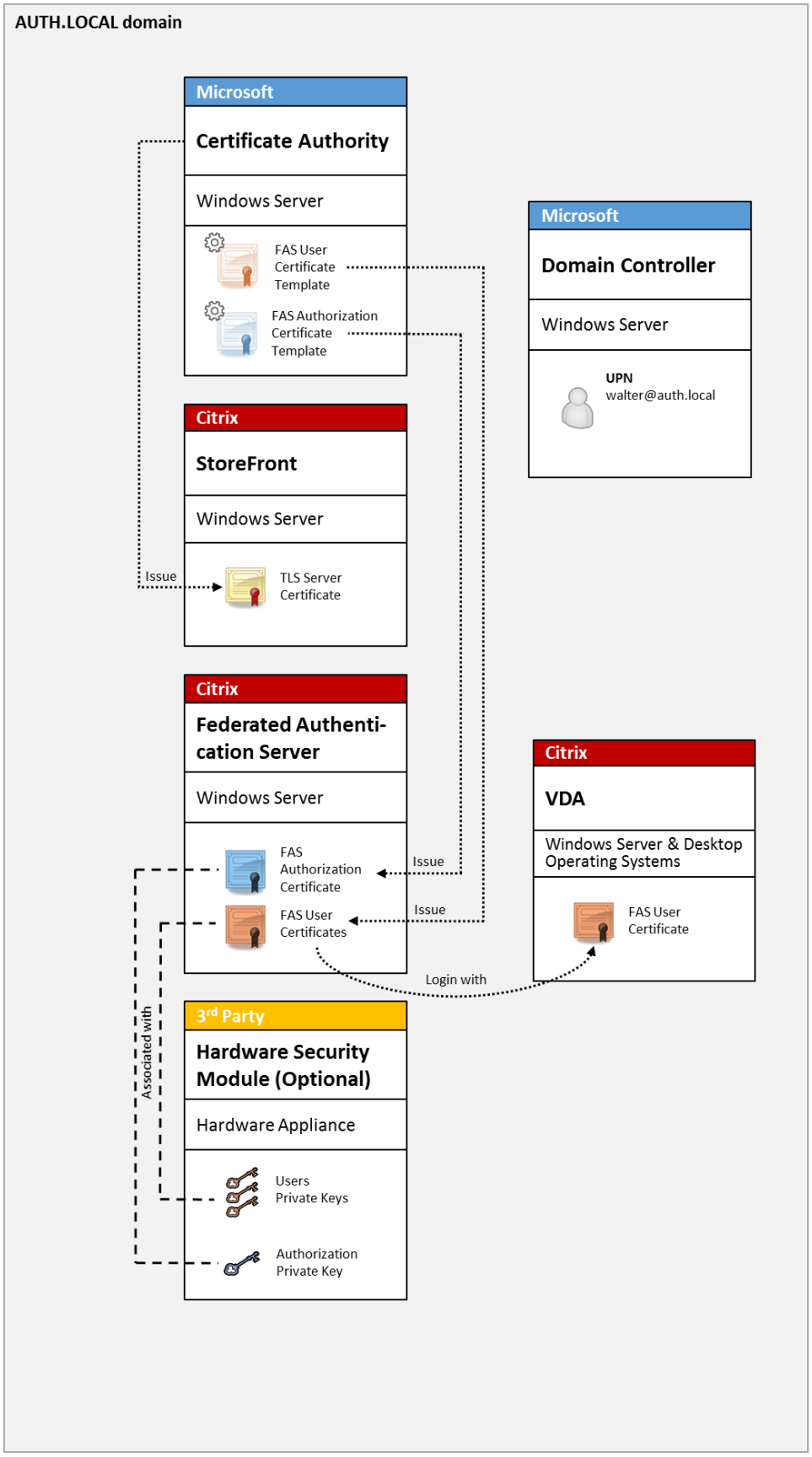
Der FAS ermöglicht die sichere Authentifizierung der Benutzer bei StoreFront mit einer Reihe von Authentifizierungsoptionen (einschließlich Kerberos-Single Sign-On) und die Verbindung mit einer vollauthentifizierten Citrix HDX-Sitzung.

Dies ermöglicht die Windows-Authentifizierung ohne Aufforderungen zur Eingabe von Anmeldeinformationen oder Smartcard-PINs und ohne Verwaltung gespeicherter Kennwörter wie beim Single Sign-On-Dienst. Der Service kann die Anmeldefeatures der eingeschränkten Kerberos-Delegierung älterer Versionen von Citrix Virtual Apps ersetzen.

Alle Benutzer haben Zugriff auf Public Key-Infrastruktur-Zertifikate in ihrer Sitzung, unabhängig davon, ob sie sich bei Endpunktgeräten mit einer Smartcard angemeldet haben. Dies ermöglicht eine reibungslose Migration zur zweistufigen Authentifizierung, und zwar selbst bei Smartphones, Tablets und ähnlichen Geräten ohne Smartcardleser.

Bei dieser Bereitstellung gibt es einen neuen Server, auf dem der FAS ausgeführt wird und der Zertifikate der Smartcardklasse für Benutzer ausstellen darf. Die Zertifikate werden dann zur Anmeldung bei Benutzersitzungen in einer Citrix HDX-Umgebung verwendet, die wie eine klassische Smartcard-Anmeldung verarbeitet wird.



Die Citrix Virtual Apps- oder Citrix Virtual Desktops-Umgebung muss ähnlich konfiguriert werden wie für die Smartcard-Anmeldung (siehe CTX206156).

In einer bestehenden Bereitstellung muss hierfür in der Regel nur sichergestellt werden, dass eine in die Domäne eingebundene Microsoft-Zertifizierungsstelle verfügbar ist und den Domänencontrollern Domänencontrollerzertifikate zugewiesen wurden. (Weitere Informationen finden Sie unter CTX206156 im Abschnitt zum Ausstellen von Domänencontrollerzertifikaten .)

Verwandte Informationen

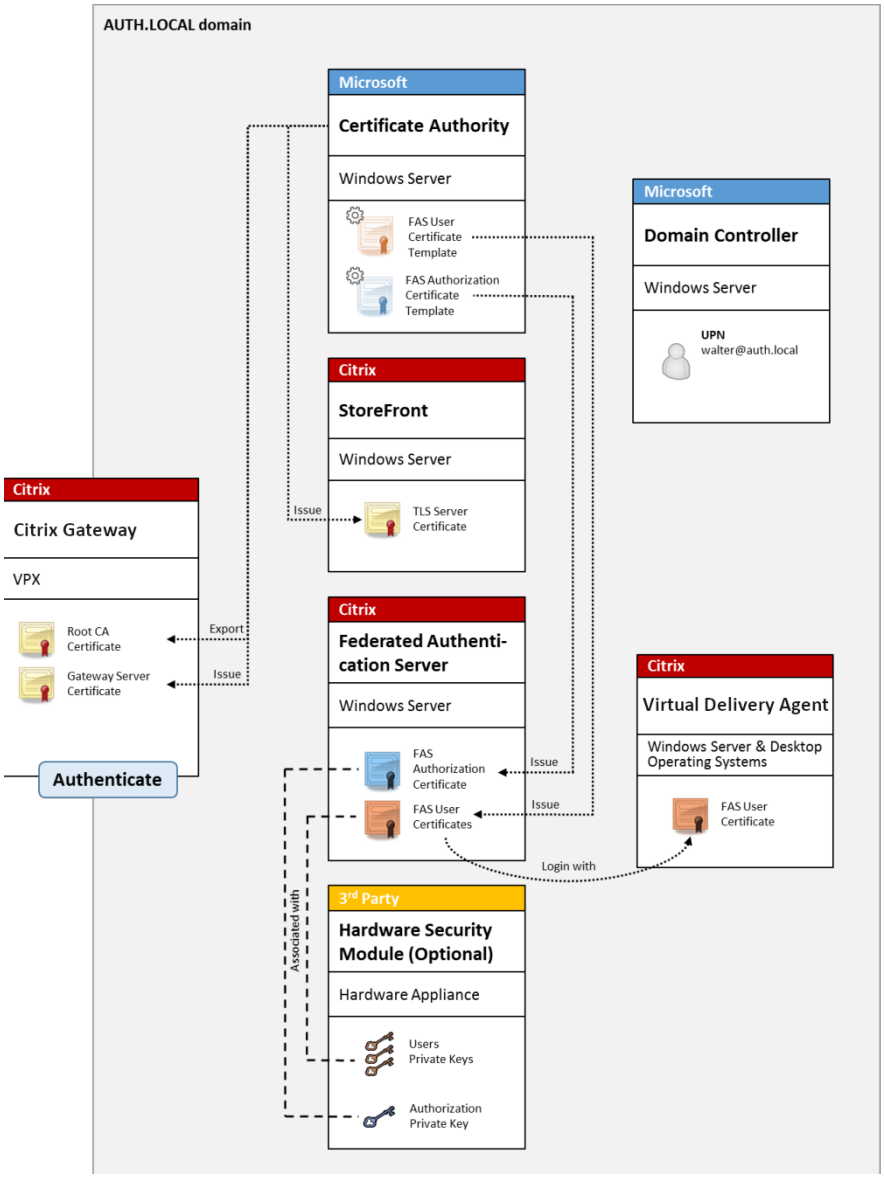
- Schlüssel können in einem Hardwaresicherheitsmodul (HSM) oder einem integrierten Trusted Platform Module (TPM) gespeichert werden. Weitere Informationen finden Sie unter Schutz privater Schlüssel.
- Im Artikel Installation und Konfiguration wird beschrieben, wie der FAS installiert und konfiguriert wird.

### Citrix Gateway-Bereitstellung

Die Citrix Gateway-Bereitstellung ähnelt der internen Bereitstellung, wobei zusätzlich ein mit StoreFront gekoppeltes Citrix Gateway verwendet wird und die primäre Authentifizierung in Citrix Gateway erfolgt. Citrix Gateway bietet intelligente Optionen für Authentifizierung und Autorisierung, mit denen der Remotezugriff auf die Websites eines Unternehmens gesichert werden kann.

Diese Bereitstellung kann verwendet werden, um mehrere PIN-Eingabeaufforderungen zu vermeiden, wie sie bei der Authentifizierung bei Citrix Gateway und anschließender Anmeldung bei einer Benutzersitzung auftreten. Außerdem können erweiterte Citrix Gateway-Authentifizierungstechnologien ohne zusätzliche Active Directory-Kennwörter oder Smartcards genutzt werden.



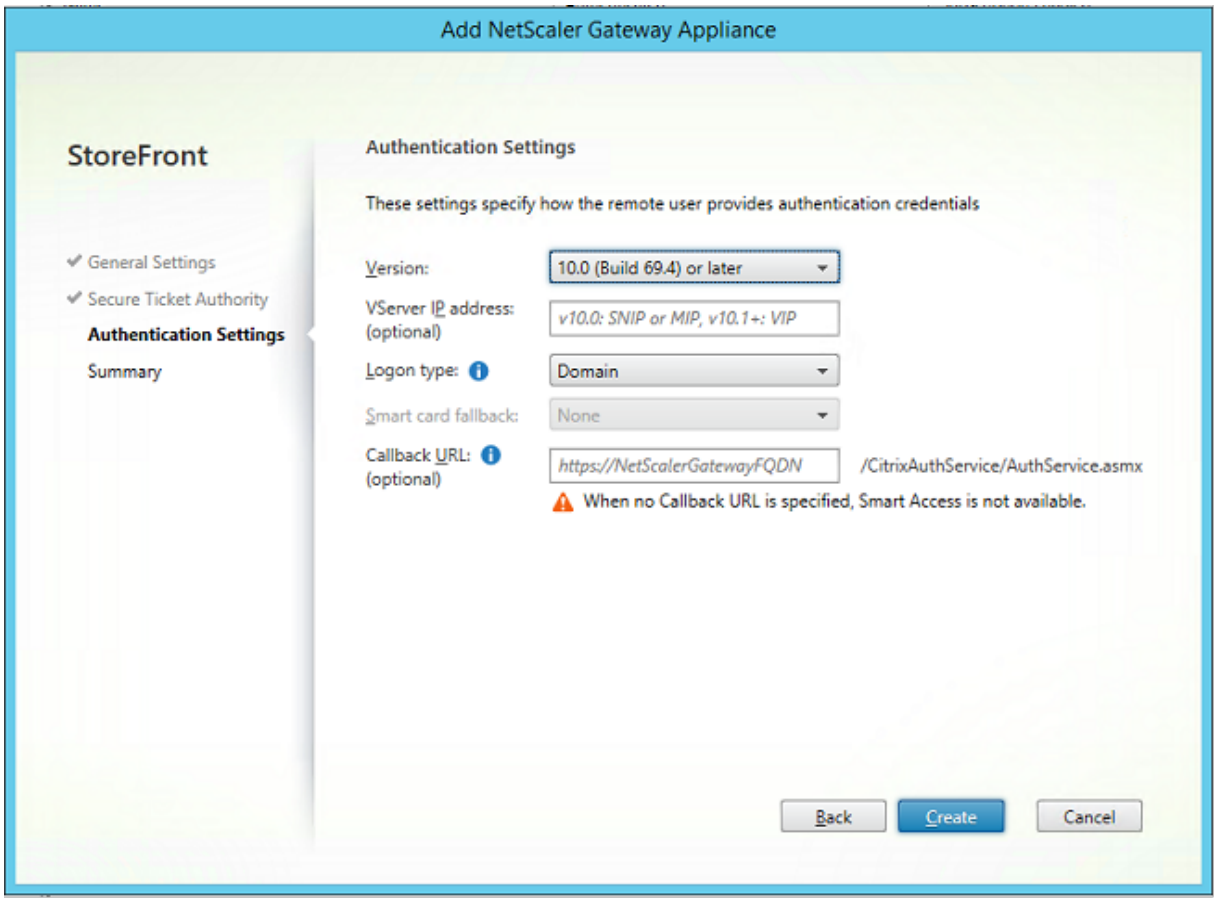

Die Citrix Virtual Apps- oder Citrix Virtual Desktops-Umgebung muss ähnlich konfiguriert werden wie für die Smartcard-Anmeldung (siehe CTX206156).

In einer bestehenden Bereitstellung muss hierfür in der Regel nur sichergestellt werden, dass eine in die Domäne eingebundene Microsoft-Zertifizierungsstelle verfügbar ist und den Domänencontrollern Domänencontrollerzertifikate zugewiesen wurden. (Weitere Informationen finden Sie unter CTX206156 im Abschnitt zum Ausstellen von Domänencontrollerzertifikaten .)

Bei der Konfiguration von Citrix Gateway als primäres Authentifizierungssystem müssen alle Verbindungen zwischen Citrix Gateway und StoreFront mit TLS geschützt werden. Sorgen Sie vor allem dafür, dass die Callback-URL richtig auf den Citrix Gateway-Server zeigt, denn sie kann zur

Authentifizierung des Citrix Gateway-Servers in dieser Bereitstellung verwendet werden.



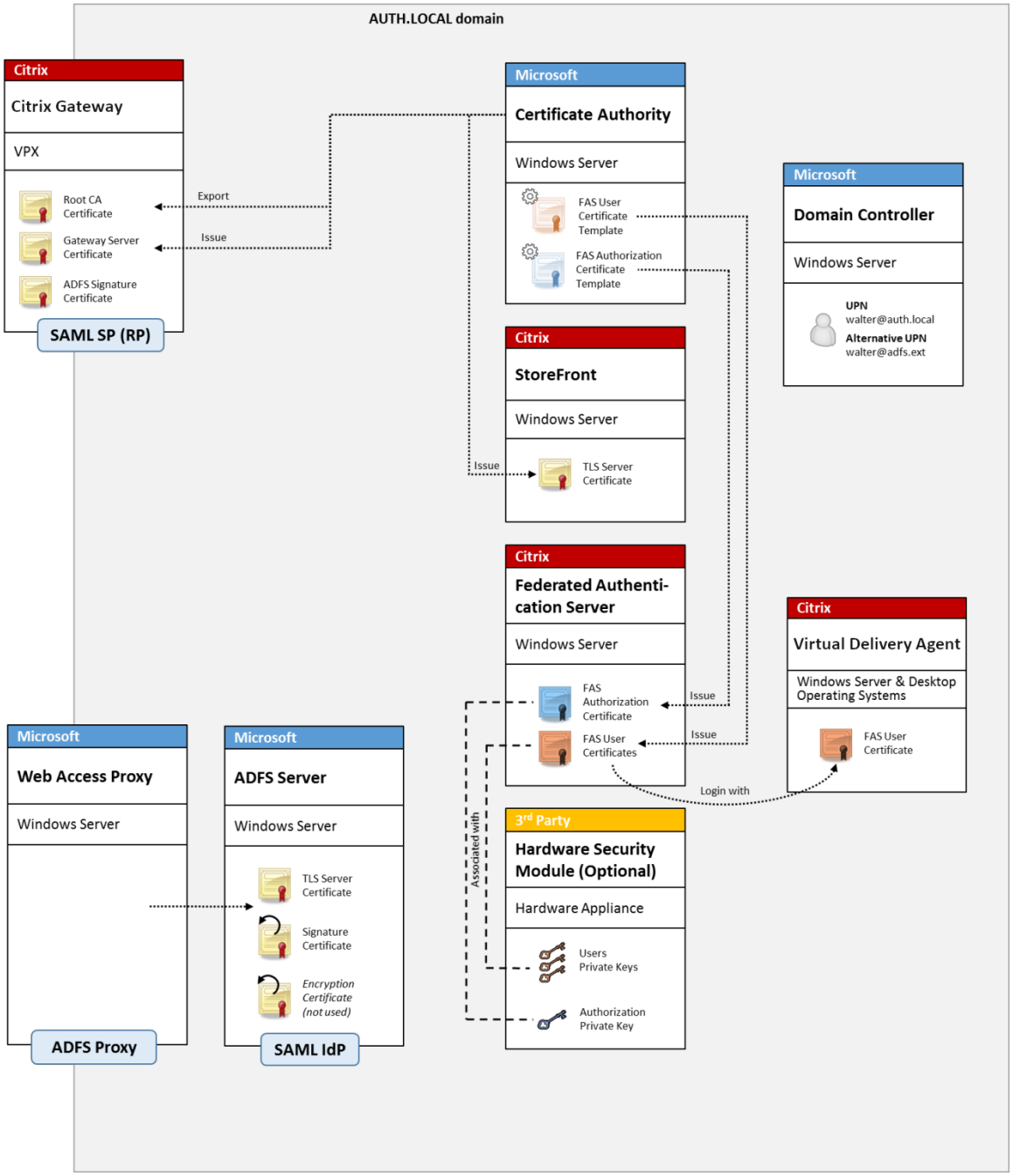

Verwandte Informationen

- 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.
- Im Artikel Installation und Konfiguration wird beschrieben, wie der FAS installiert und konfiguriert wird.

### AD FS SAML-Bereitstellung

Eine wichtige Citrix Gateway-Authentifizierungstechnologie ermöglicht die Integration in Microsoft AD FS zur Verwendung als SAML-Identitätsanbieter (IdP). Eine SAML-Assertion ist ein kryptografisch signierter XML-Block, der von einem vertrauenswürdigen IdP ausgestellt wird und einen Benutzer zur Anmeldung bei einem Computersystem autorisiert. Der FAS-Server gestattet die Delegation der Authentifizierung eines Benutzers an den Microsoft AD FS-Server (oder einen anderen SAML-fähigen IdP).




AD FS wird häufig zur sicheren Authentifizierung von Benutzern bei Unternehmensressourcen remote über das Internet verwendet (z. B. bei einer Office 365-Integration).

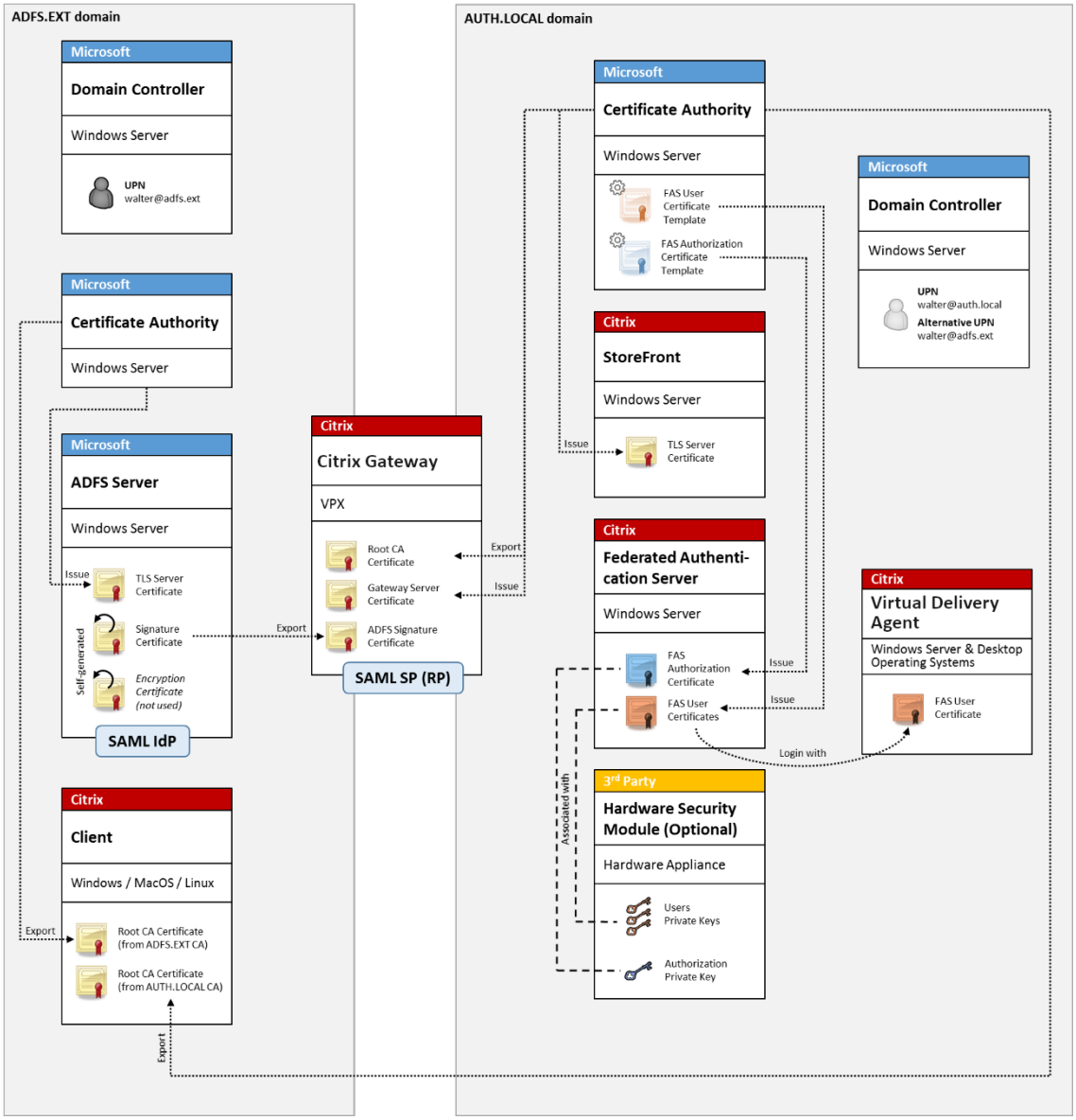
Verwandte Informationen

- Der Artikel AD FS-Bereitstellung enthält Details.
- Im Artikel Installation und Konfiguration wird beschrieben, wie der FAS installiert und konfiguriert wird.
- Der Abschnitt Citrix Gateway-Bereitstellung enthält Hinweise zur Konfiguration.

## B2B-Kontozuordnung

Wenn zwei Unternehmen ihre Computersysteme gemeinsam verwenden möchten, wird häufig ein Active Directory-Verbunddienste-Server (AD FS) mit einer Vertrauensstellung eingerichtet. Dadurch können Benutzer in einem Unternehmen sich nahtlos bei dem Active Directory (AD) des zweiten authentifizieren. Die Benutzer verwenden bei der Anmeldung die Anmeldeinformationen ihres eigenen Unternehmens, die von AD FS automatisch einem Schattenkonto in der AD-Umgebung des zweiten Unternehmens zugewiesen wird.



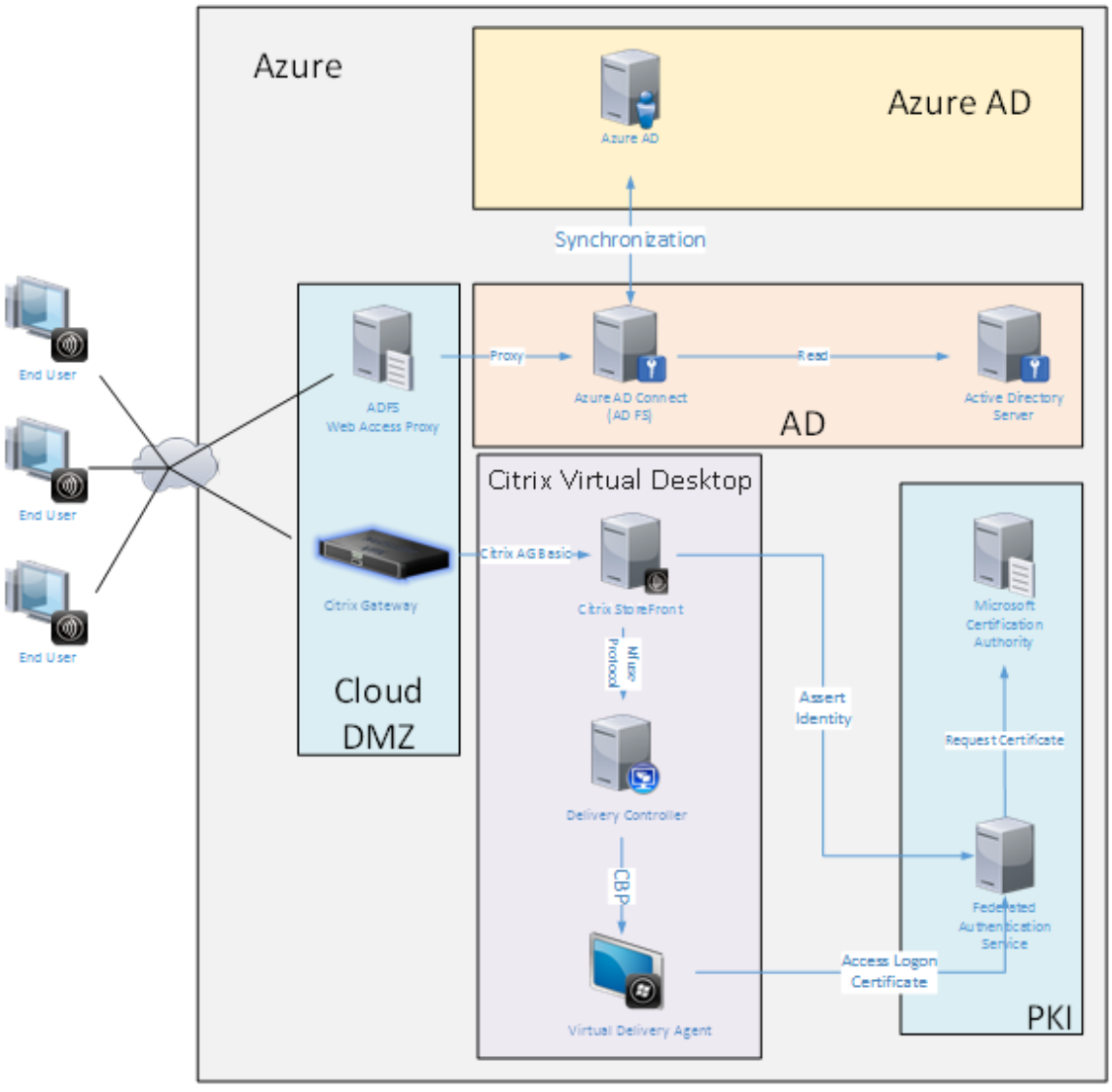

Verwandte Informationen

- Im Artikel Installation und Konfiguration wird beschrieben, wie der FAS installiert und konfiguriert wird.

### Einbindung in Azure AD unter Windows 10

Mit Windows 10 wurde das Konzept der Azure AD-Einbindung eingeführt. Im Konzept entspricht dies dem herkömmlichen Beitritt zu einer Windows-Domäne, zielt jedoch auf Verbindungen über das Internet ab. Es funktioniert gut mit Laptops und Tablets. Genau wie der herkömmliche Windows-Domänenbeitritt bietet Azure AD Funktionen, die Single Sign-On-Modelle für Unternehmenswebsites und -ressourcen zulassen. Diese sind allesamt Internet-fähig und können daher auch außerhalb des Unternehmens-LANs an jedem Standort mit Internet-Verbindung verwendet werden.




Diese Bereitstellung ist ein Beispiel, bei dem das Konzept "Endbenutzer im Büro"effektiv nicht existiert. Die Registrierung und Authentifizierung von Laptops erfolgt vollständig über das Internet mit modernen Azure AD-Features.

Die Infrastruktur dieser Bereitstellung kann überall dort ausgeführt werden, wo eine IP-Adresse

verfügbar ist: lokal, bei einem Hostinganbieter, in Azure oder in einer anderen Cloud. Die Synchronisierung von Azure AD Connect stellt automatisch eine Verbindung mit Azure AD her. In der Beispielabbildung werden der Einfachheit halber Azure-VMs verwendet.

Verwandte Informationen

- Im Artikel Installation und Konfiguration wird beschrieben, wie der FAS installiert und konfiguriert wird.
- Der Artikel Integration in Azure Active Directory enthält detaillierte Informationen.

## AD FS-Bereitstellung

September 11, 2024

### Einführung

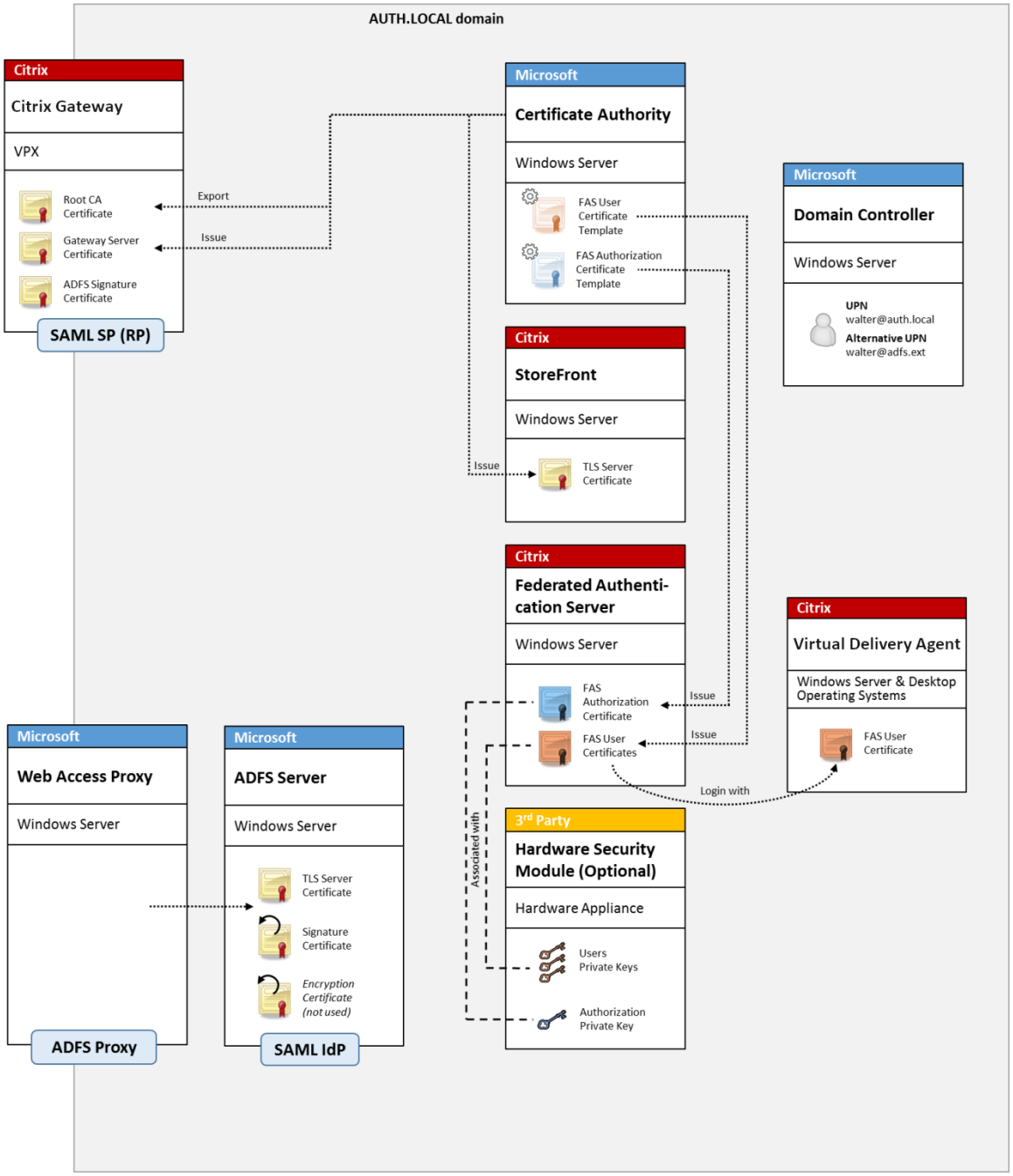
In diesem Dokument wird beschrieben, wie Sie eine Citrix Umgebung in Microsoft Active Directory-Verbunddienste integrieren.

In vielen Organisationen wird AD FS zum Verwalten des sicheren Benutzerzugriffs auf Websites verwendet, die einen einzelnen Authentifizierungspunkt erfordern. Wenn beispielsweise Mitarbeitern zusätzliche Inhalte und Downloads zur Verfügung stehen, müssen diese durch standardmäßige Windows-Anmeldeinformationen geschützt werden.

Der Verbundauthentifizierungsdienst (Federated Authentication Service, FAS) ermöglicht zudem die Integration von Citrix Gateway und Citrix StoreFront in das AD FS-Anmeldesystem und vereinfacht so die Anmeldung für die Mitarbeiter.

Bei einer solchen Bereitstellung wird Citrix Gateway als vertrauende Seite für Microsoft AD FS integriert.




> **Hinweis:**
>
> Es macht keinen Unterschied, ob die Back-End-Ressource Windows VDA oder Linux VDA ist.

## Übersicht über SAML

SAML (Security Assertion Markup Language) ist eine einfaches System für die Webbrowser-Anmeldung, durch das eine Umleitung auf eine Anmeldeseite vorgenommen wird. Die Konfiguration

umfasst folgende Elemente:

**Umleitungs-URL (URL des Single Sign-On-Diensts)**

Wenn Citrix Gateway erkennt, dass ein Benutzer authentifiziert werden muss, weist es den Webbrowser zur Durchführung eines HTTP POST an eine SAML-Anmeldeseite auf dem AD FS-Server an. Dies ist normalerweise eine `https://`-Adresse des Formats `https://adfs.mycompany.com/adfs/ls`.

Der Webseiten-POST umfasst weitere Informationen, darunter eine Rückleitungsadresse, an die der Benutzer nach der Anmeldung zurückgeleitet wird.

**Bezeichner (Ausstellername/EntityID)**

Die EntityID ist ein eindeutiger Bezeichner, der von Citrix Gateway in den POST-Daten an AD FS verwendet wird. Durch ihn wird AD FS darüber informiert, bei welchem Dienst der Benutzer versucht, sich anzumelden und welche Authentifizierungsrichtlinien anzuwenden sind. Wenn eine SAML-Authentifizierungs-XML ausgestellt wird, kann diese nur für die Anmeldung bei dem durch die EntityID bezeichneten Dienst verwendet werden.

Normalerweise ist die EntityID die URL der Anmeldeseite des Citrix Gateway-Servers. Es kann jedoch eine beliebige andere EntityID verwendet werden, sofern Citrix Gateway und AD FS sie beide als gültig interpretieren: `https://ns.mycompany.com/application/logonpage`.

**Rückleitungsadresse (Antwort-URL)**

Wenn die Authentifizierung erfolgreich ist, weist AD FS den Webbrowser des Benutzers an, einen POST einer SAML-Authentifizierungs-XML an eine der Antwort-URLs vorzunehmen, die für die EntityID konfiguriert wurden. Das ist normalerweise eine `https://`-Adresse auf dem ursprünglichen Citrix Gateway-Server im Format `https://ns.mycompany.com/cgi/samlauth`.

Sind mehrere Antwort-URLs konfiguriert, kann Citrix Gateway eine aus dem ursprünglichen POST an AD FS wählen.

**Signaturzertifikat (IDP-Zertifikat)**

SAML-Authentifizierungs-XML-Blobs werden von AD FS kryptografisch mit seinem privaten Schlüssel signiert. Zur Überprüfung der Signatur muss die Prüfung solcher Signaturen mit dem öffentlichen Schlüssel in der Zertifikatdatei in Citrix Gateway konfiguriert sein. Die Zertifikatdatei ist normalerweise eine vom AD FS-Server erhaltene Textdatei.

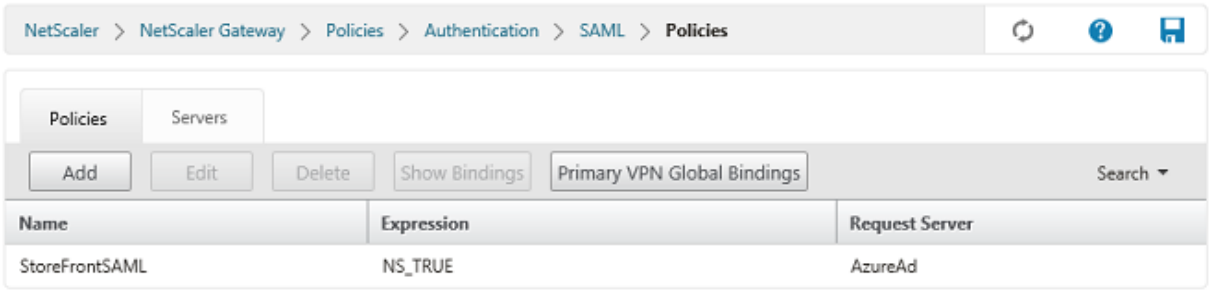
### URL für Single Sign-Out (URL für einmaliges Abmelden)

AD FS und Citrix Gateway unterstützen ein zentrales Abmeldesystem. Das ist eine URL, die von Citrix Gateway regelmäßig abgefragt wird, um zu prüfen, ob das SAML-Authentifizierungs-XML-Blob immer noch die aktuell angemeldete Sitzung repräsentiert.

Dies ist ein optionales Feature, das nicht konfiguriert werden muss. Dies ist normalerweise eine `https://`-Adresse des Formats `https://adfs.mycompany.com/adfs/logout`. (Die Adresse darf nicht mit der URL für die einmalige Anmeldung identisch sein.)

## Konfiguration

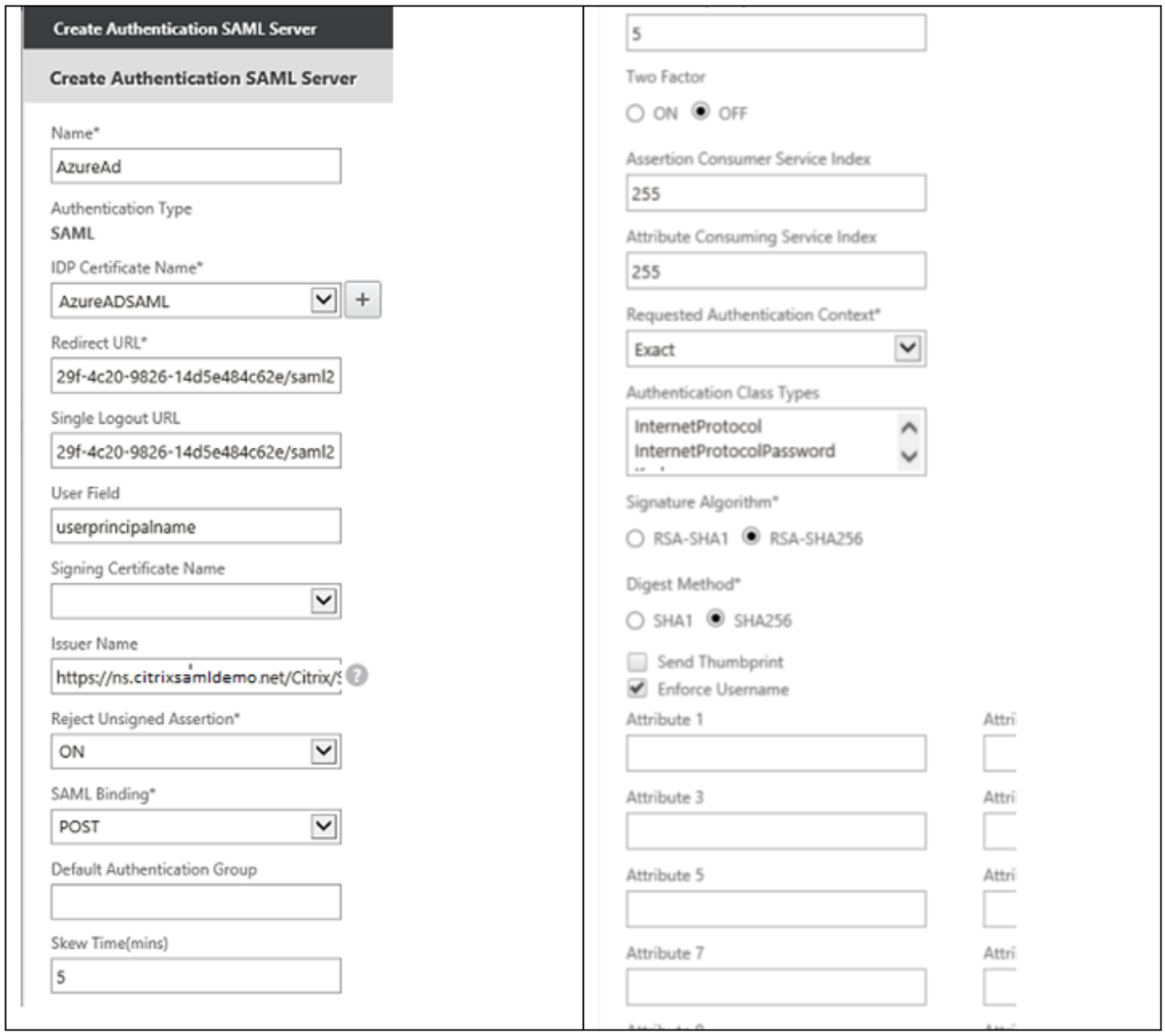
Unter Citrix Gateway-Bereitstellung wird beschrieben, wie Citrix Gateway für die Standard-LDAP-Authentifizierungsoptionen konfiguriert wird. Nach diesem Arbeitsgang können Sie eine neue Authentifizierungsrichtlinie in Citrix Gateway für die SAML-Authentifizierung erstellen. Diese kann dann die von dem Citrix Gateway-Assistenten verwendete Standard-LDAP-Richtlinie ersetzen.




### Ausfüllen der SAML-Richtlinie

Konfigurieren Sie den neuen SAML-IdP-Server mit den zuvor der AD FS-Verwaltungskonsole entnommenen Informationen. Wenn diese Richtlinie angewendet wird, leitet Citrix Gateway Benutzer zur Anmeldung an AD FS um und akzeptiert das zurückgegebene, von AD FS signierte SAML-Authentifizierungstoken.




### Verwandte Informationen

- Installation und Konfiguration ist die primäre Referenz für die Installation und Konfiguration des FAS.
- Der Artikel Bereitstellungsarchitekturen enthält eine Übersicht über die gebräuchlichen FAS-Architekturen.
- Der Artikel Erweiterte Konfiguration enthält Links zu weiteren Anleitungen.

## Integration in Azure Active Directory

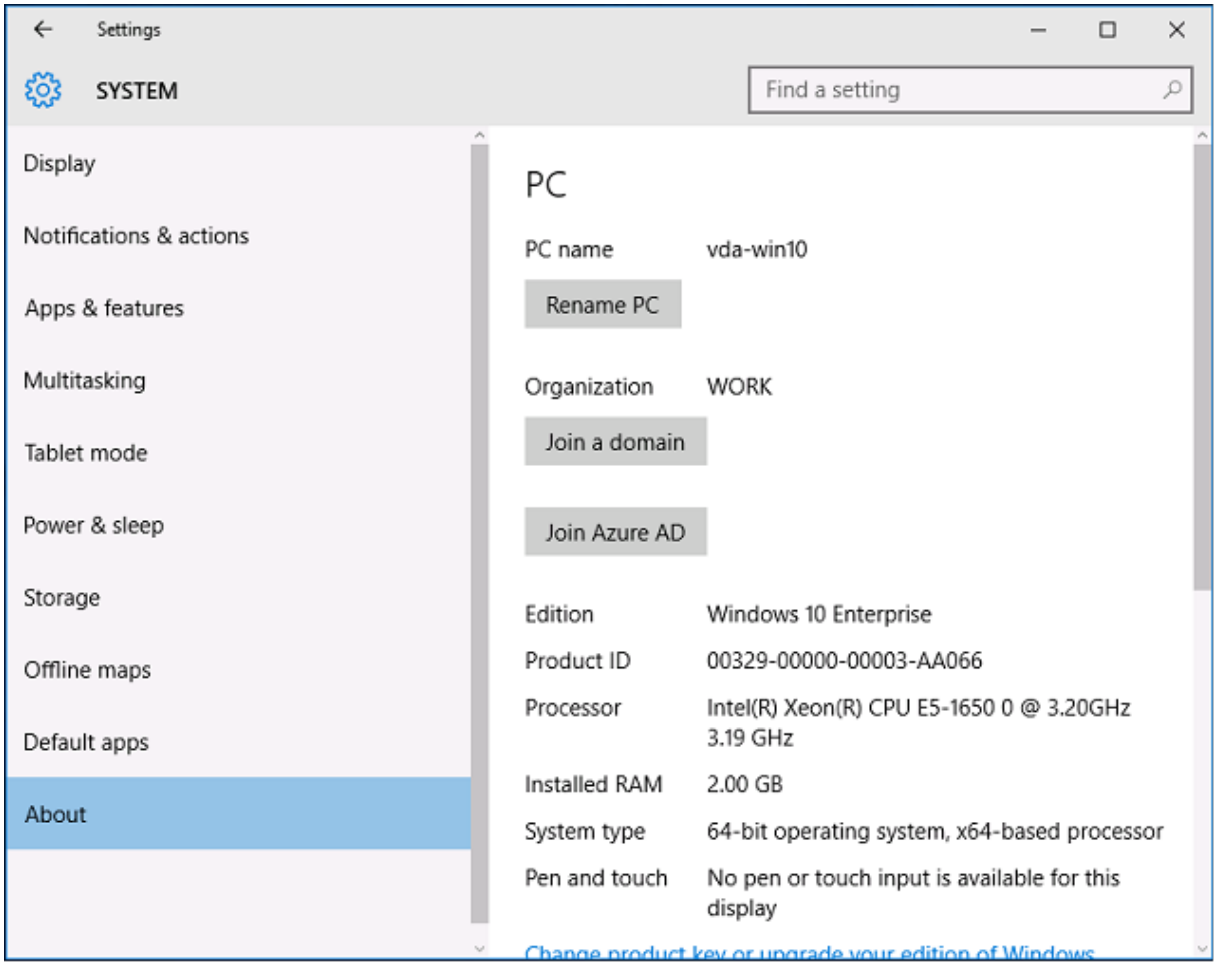
September 11, 2024

## Einführung

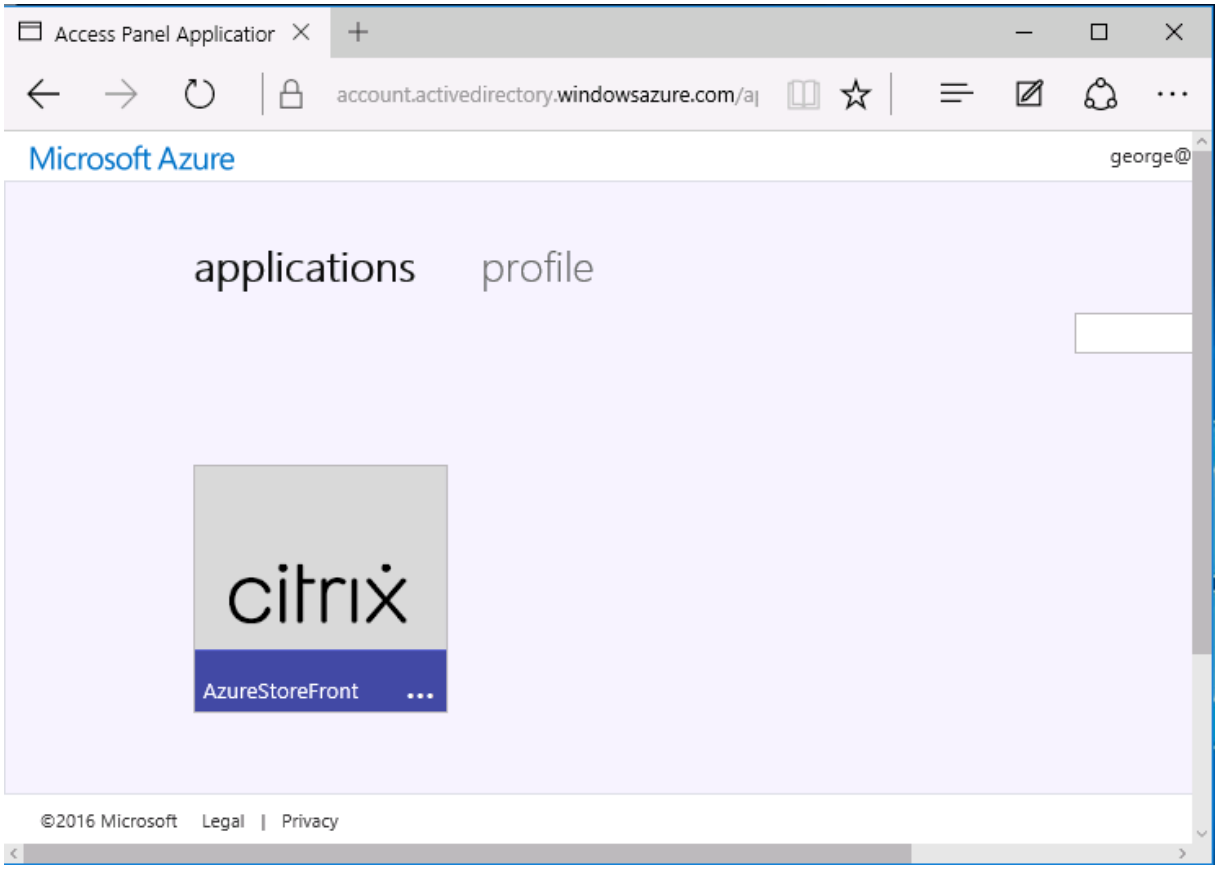
In diesem Dokument wird beschrieben, wie Sie eine Citrix Umgebung in Azure Active Directory unter Windows 10 integrieren. Azure Active Directory wurde mit Windows 10 eingeführt und repräsentiert ein neues Modell für den Domänenbeitritt, bei dem Laptops im Roamingbetrieb über das Internet einer Unternehmensdomäne für Verwaltungszwecke und zum Single Sign-On beitreten können.

Die hier vorgestellte Beispielbereitstellung ist ein System, bei dem die IT neuen Benutzern eine Unternehmens-E-Mail-Adresse und einen Registrierungscode für ihre privaten Windows 10-Laptops zuteilt. Die Benutzer greifen auf diesen Code über die Option **System > Info > Azure AD beitreten** im Bereich **Einstellungen** zu.




Nach der Registrierung eines Laptops führt der Microsoft Edge-Webbrowser automatisch die Anmeldung bei Unternehmenswebsites und veröffentlichten Citrix Anwendungen über die Azure-SaaS-Anwendungswebsite durch, die auch andere Azure-Anwendungen, wie Office 365, bietet.

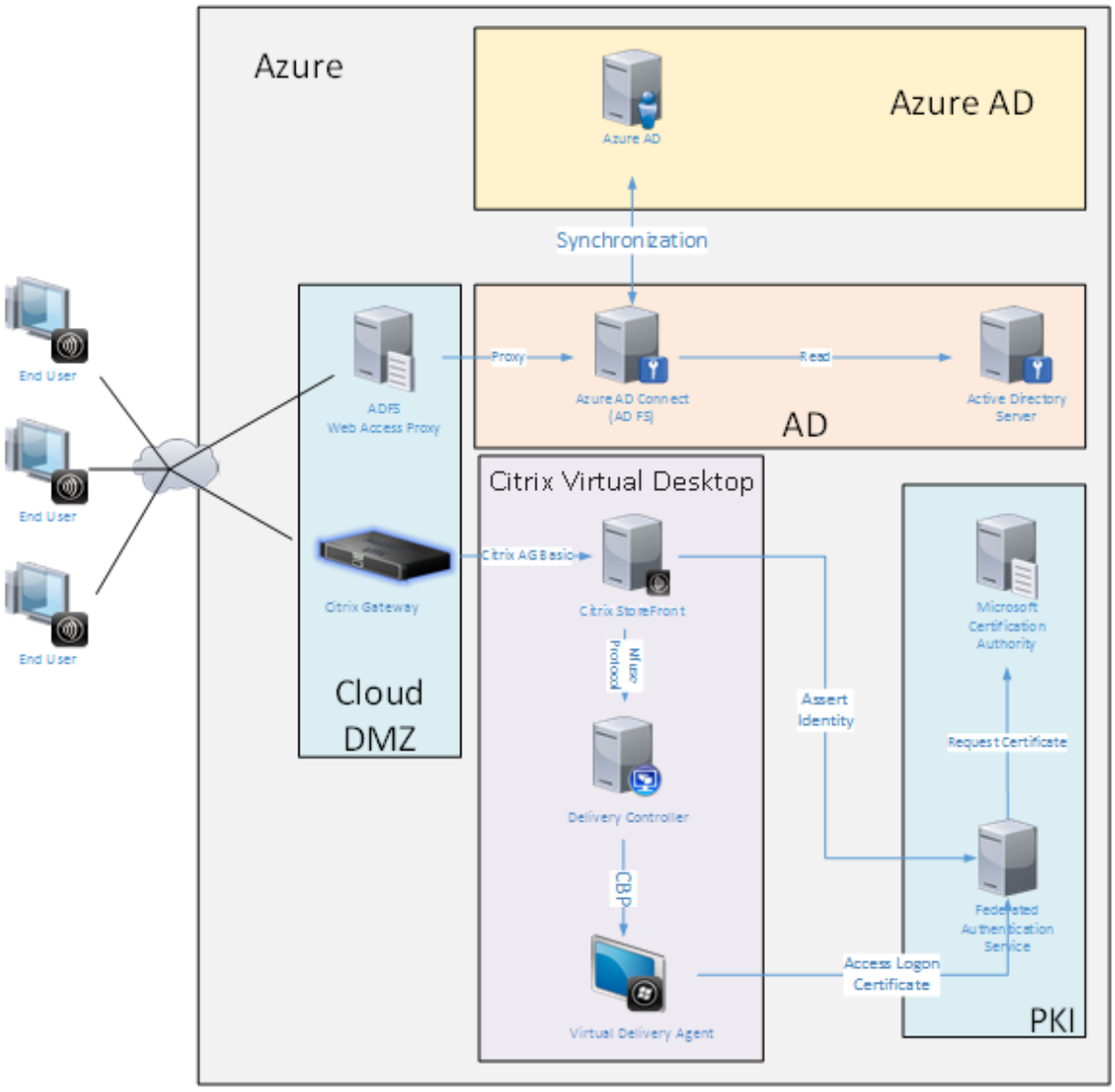



### Architektur

Diese Architektur repliziert innerhalb von Azure ein herkömmliches Unternehmensnetzwerk unter Integration moderner Cloudtechnologien, wie Azure Active Directory und Office 365. Die Endbenutzer werden alle als Remotebenutzer angesehen, das Konzept eines Büro-Intranets kommt nicht zur Anwendung.

Das Modell kann auch in Unternehmen mit lokalen Systemen verwendet werden, da die Azure AD Connect-Synchronisierung eine Verbindung mit Azure über das Internet herstellen kann.




Sichere Verbindungen und Single Sign-On, wie sie konventionell per LAN mit Firewall und Kerberos/NTLM-Authentifizierung realisiert wurden, werden in dieser Architektur durch TLS-Verbindungen mit Azure und SAML ersetzt. Neue Dienste werden als Azure-Anwendungen, die Mitglied von Azure AD sind, erstellt. Vorhandene Anwendungen, die Active Directory erfordern (z. B. eine SQL Server-Datenbank), können mit einer Standard-AD-Server-VM im IAAS-Teil des Azure-Clouddiensts ausgeführt werden.

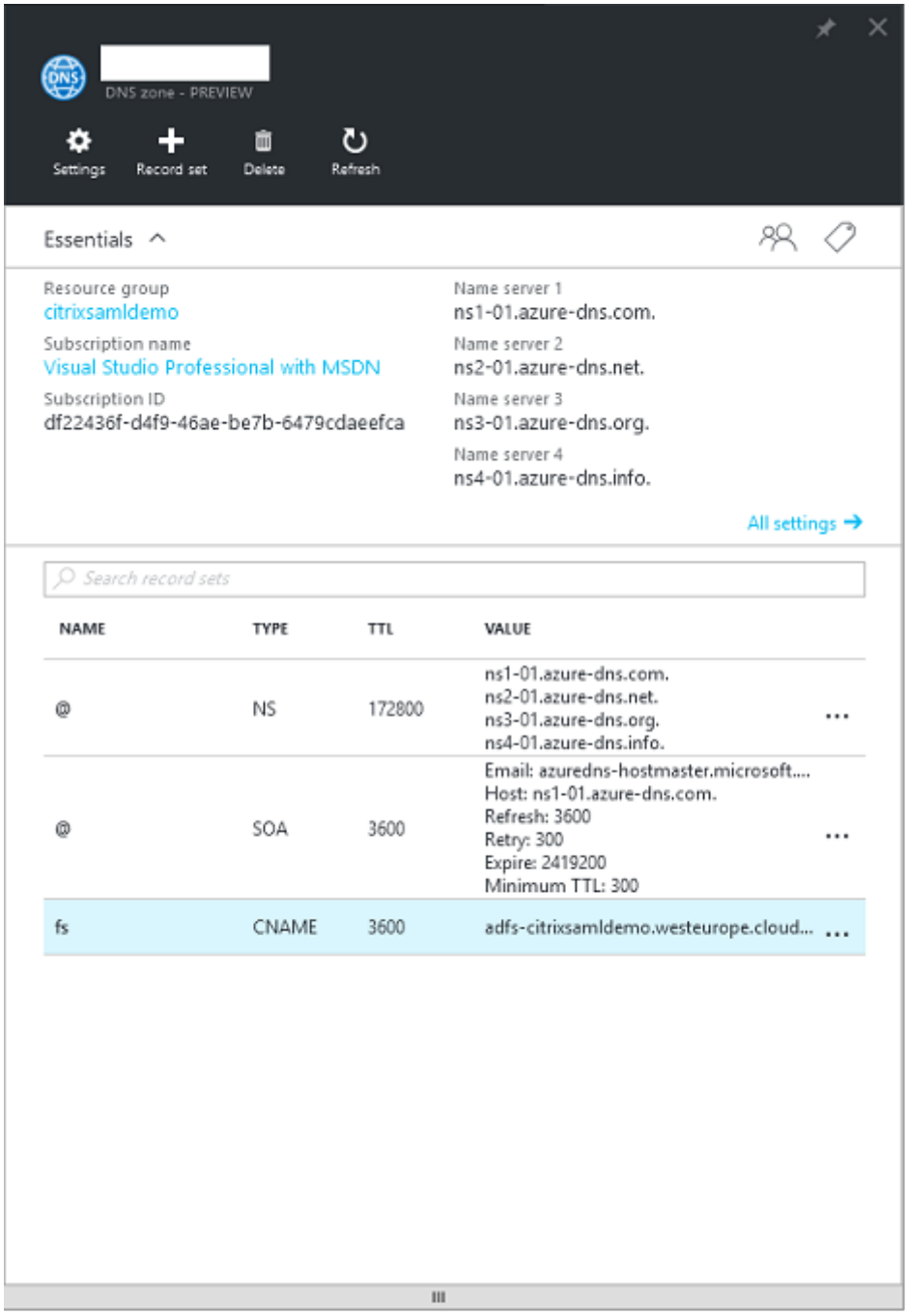
Wenn ein Benutzer eine herkömmliche Anwendung startet, erfolgt der Zugriff über die mit Citrix Virtual Apps and Desktops veröffentlichte Anwendung. Die verschiedenen Anwendungstypen werden auf der Seite **Azure-Anwendungen** unter Verwendung der Microsoft Edge-Single Sign-On-Features sortiert. Microsoft stellt außerdem Android- und iOS-Apps zur Verfügung, die Azure-Anwendungen aufzählen und starten können.

### Erstellen einer DNS-Zone

Für Azure AD muss der Administrator eine öffentliche DNS-Adresse registrieren und die Delegierungszone für das Domänennamensuffix steuern. Hierfür kann das Azure-Feature "DNS-Zone"verwendet werden.

Im vorliegenden Beispiel lautet der Name der DNS-Zone *citrixsamldemo.net*.




In der Konsole werden die Namen der Azure-DNS-Namensserver angezeigt. Auf diese muss in den

NS-Einträgen der DNS-Registrierungsstelle für die Zone verwiesen werden (z. B. `citrixsamldemo.net. NS n1-01.azure-dns.com`).

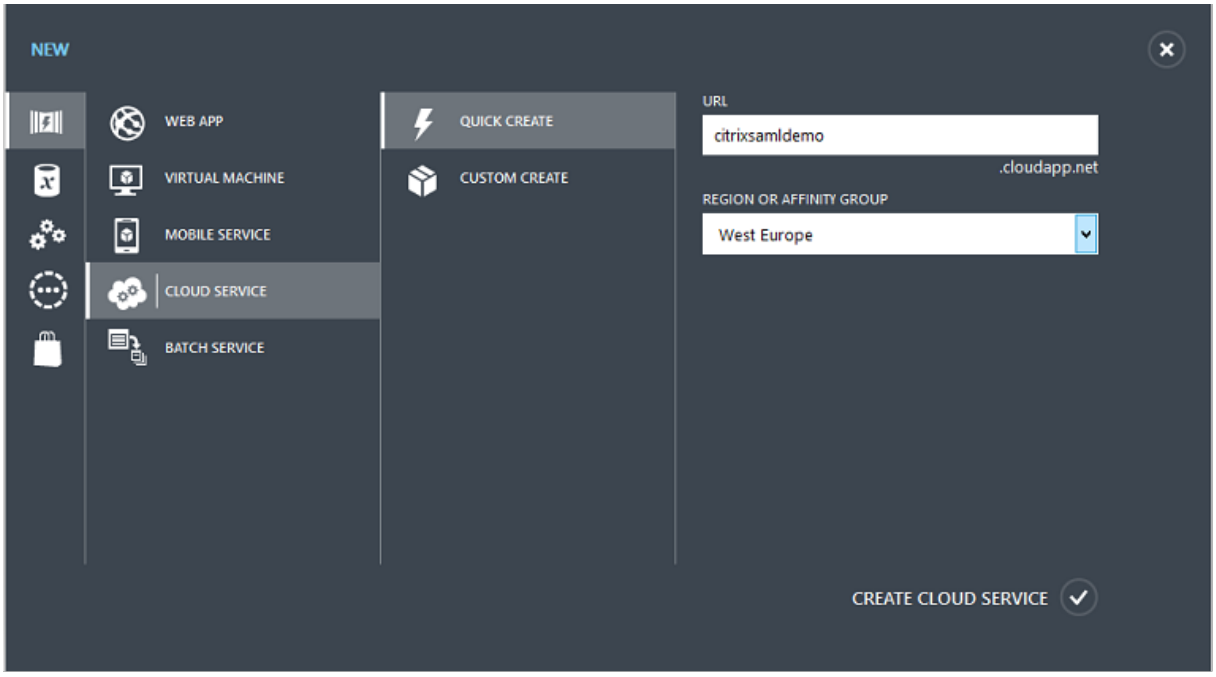
Beim Hinzufügen von Verweisen auf VMs, die in Azure ausgeführt werden, verwendet man am einfachsten den CNAME-Zeiger auf den in Azure verwalteten DNS-Eintrag für die jeweilige VM. Wenn sich die IP-Adresse der VM ändert, müssen Sie dann die DNS-Zonendatei nicht manuell aktualisieren.

In dieser Bereitstellung stimmen internes und externes DNS-Adresssuffix überein. Die Domäne ist citrixsamldemo.net und verwendet Split DNS (10.0.0.* intern).

Fügen Sie den Eintrag "fs.citrixsamldemo.net"hinzu, der auf den Webanwendungsproxyserver verweist. Dies ist der Verbunddienst für diese Zone.

### Erstellen eines Clouddiensts

In diesem Beispiel wird eine Citrix Umgebung einschließlich einer AD-Umgebung mit einem in Azure ausgeführten AD FS-Server konfiguriert. Ein Clouddienst wird unter dem Namen "citrixsamldemo" erstellt.



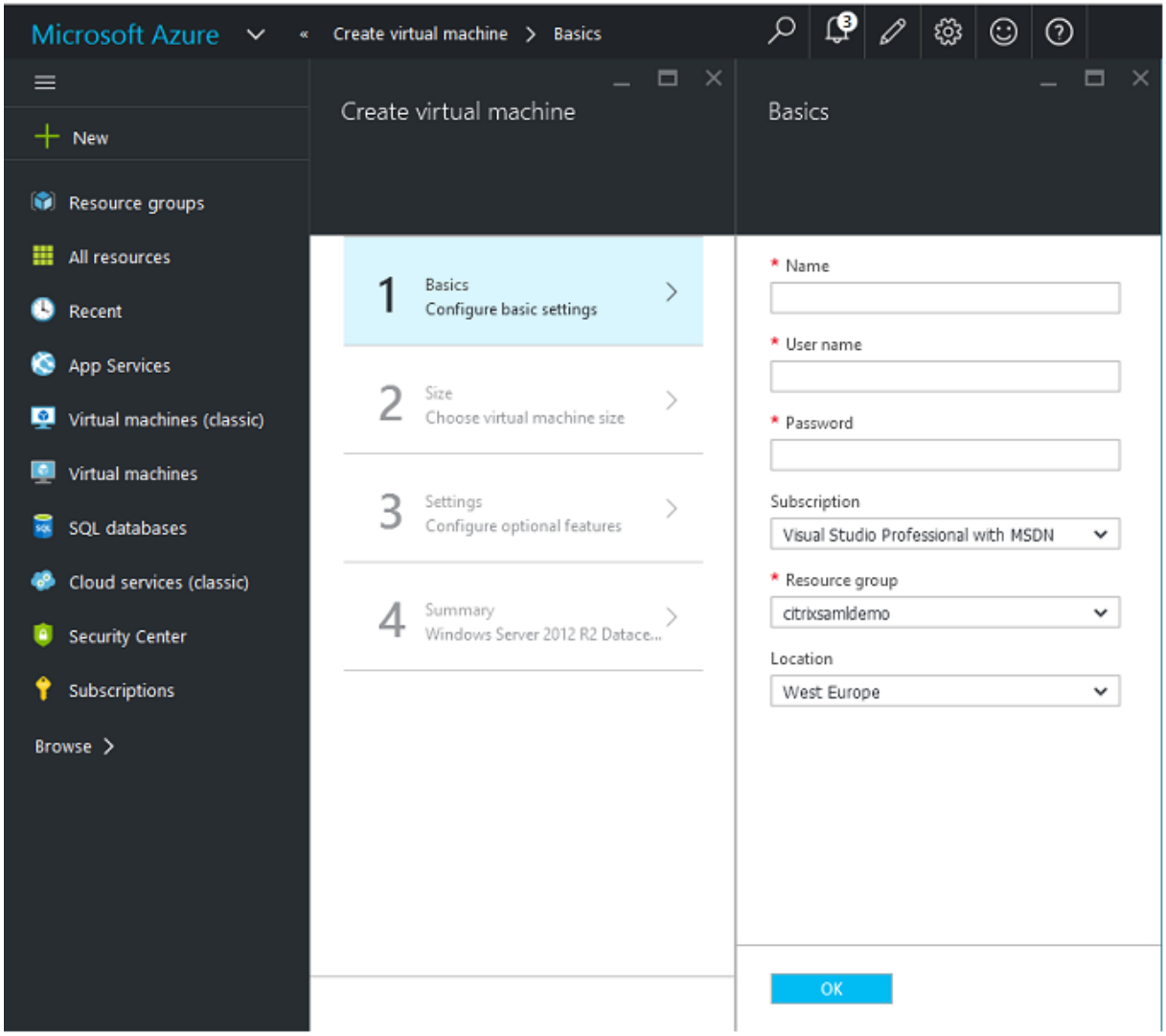

### Erstellen virtueller Windows-Maschinen

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

- Domänencontroller (domaincontrol)
- Azure Connect AD FS-Server (adfs)
- AD FS-Proxy für den Webzugriff (Webanwendungsproxy, kein Mitglied einer Domäne)

- Citrix Virtual Apps and Desktops-Delivery Controller
- Citrix Virtual Apps and Desktops Virtual Delivery Agent (VDA)




**Domänencontroller**

- Fügen Sie die Rollen **DNS-Server** und **Active Directory-Domänendienste** hinzu, um eine Active Directory-Standardbereitstellung zu erstellen (in diesem Beispiel citrixsamldemo.net). Nach Abschluss der Domänenpromotion fügen Sie die Rolle **Active Directory-Zertifikatdienste** hinzu.
- Erstellen Sie ein normales Benutzerkonto für Tests (z. B. George@citrixsamldemo.net).
- Da auf diesem Server DNS intern ausgeführt wird, müssen alle Server zur DNS-Auflösung auf diesem Server verweisen. Sie tun dies auf der Seite **Azure-DNS-Einstellungen**. (Weitere Informationen finden Sie im Anhang).

#### AD FS-Controller und Webanwendungsproxyserver

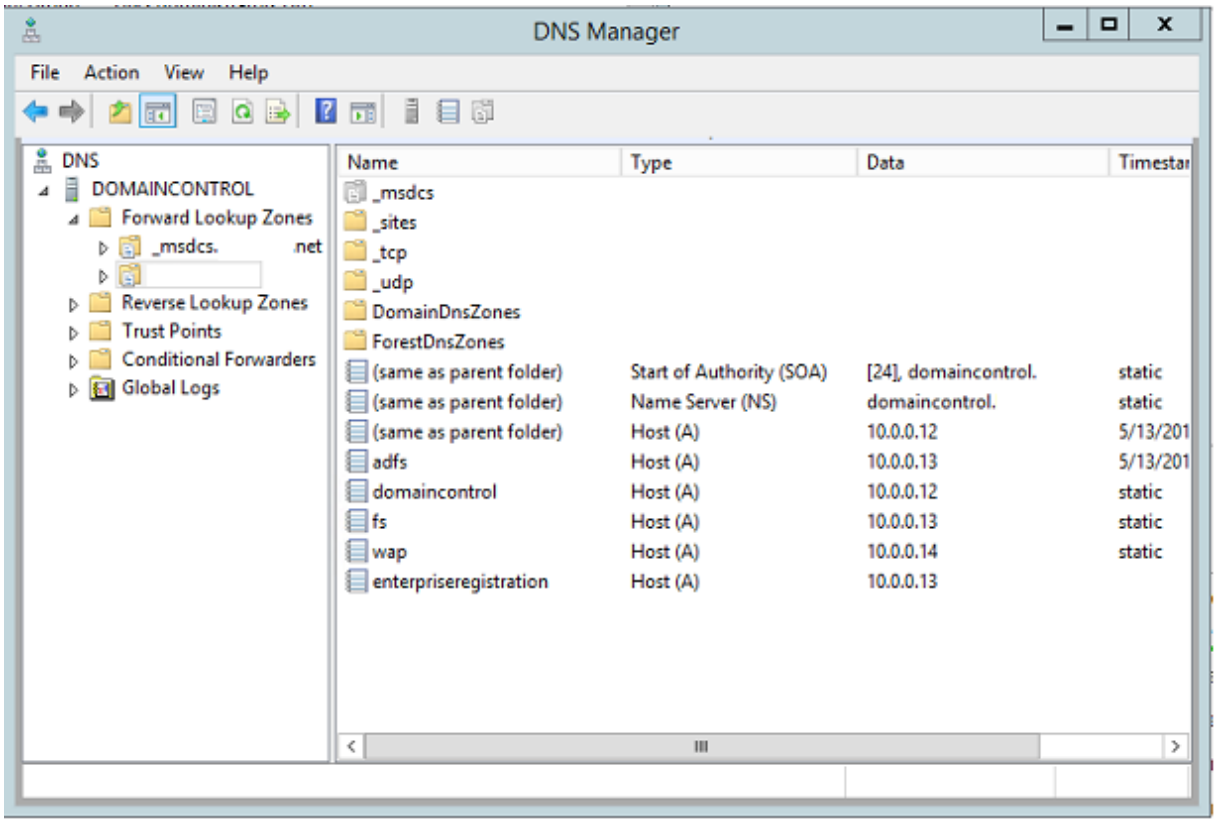
- Fügen Sie den AD FS-Server der Domäne citrixsamldemo hinzu. Der Webanwendungsproxy-server muss in einer isolierten Arbeitsgruppe bleiben. Registrieren Sie daher manuell eine DNS-Adresse beim AD-DNS.
- Führen Sie an diesen Servern das Cmdlet **Enable-PSRemoting** –**Force** aus, um PS-Remoting aus dem Azure AD Connect-Tool über Firewalls zuzulassen.

#### Citrix Virtual Desktops-Delivery Controller und -VDA

- Installieren Sie den Citrix Virtual Apps- oder Citrix Virtual Desktops-Delivery Controller und -VDA auf den verbleibenden beiden Windows-Servern, die zur Domäne “citrixsamldemo”gehören.

### Konfigurieren eines internen DNS

Nach Installation des Domänencontrollers konfigurieren Sie den DNS-Server für die interne citrixsamldemo.net-Dimension und als Weiterleiter an einen externen DNS-Server (z. B.: 8.8.8.8).



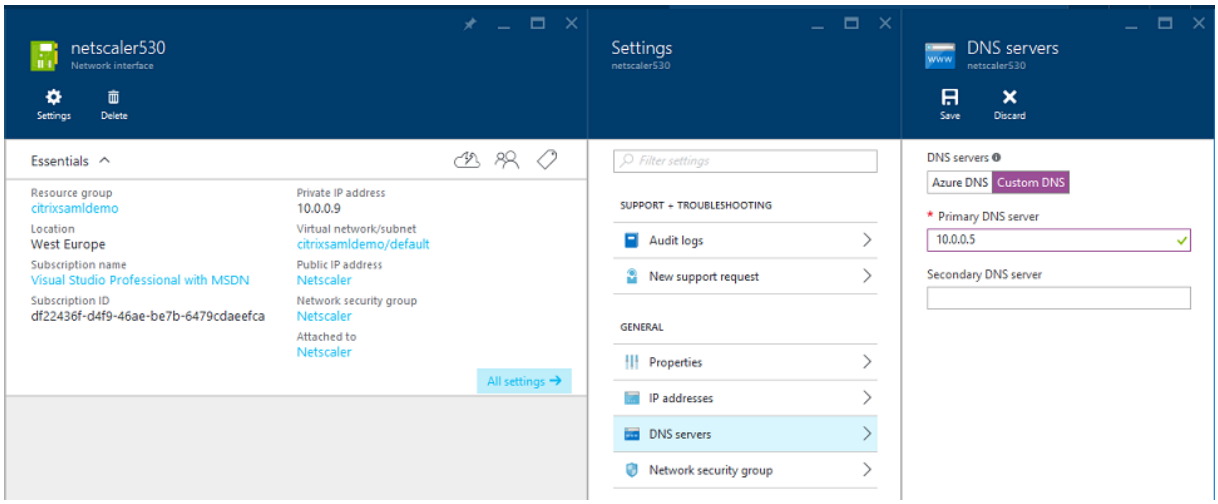

Fügen Sie für folgende Elemente einen statischen Eintrag hinzu:

- wap.citrixsamldemo.net (die Webanwendungsproxy-VM wird nicht der Domäne hinzugefügt)

- fs.citrixsamldemo.net (Adresse des internen Verbundservers)
- enterpriseregistration.citrixsaml.net (identisch mit fs.citrixsamldemo.net)

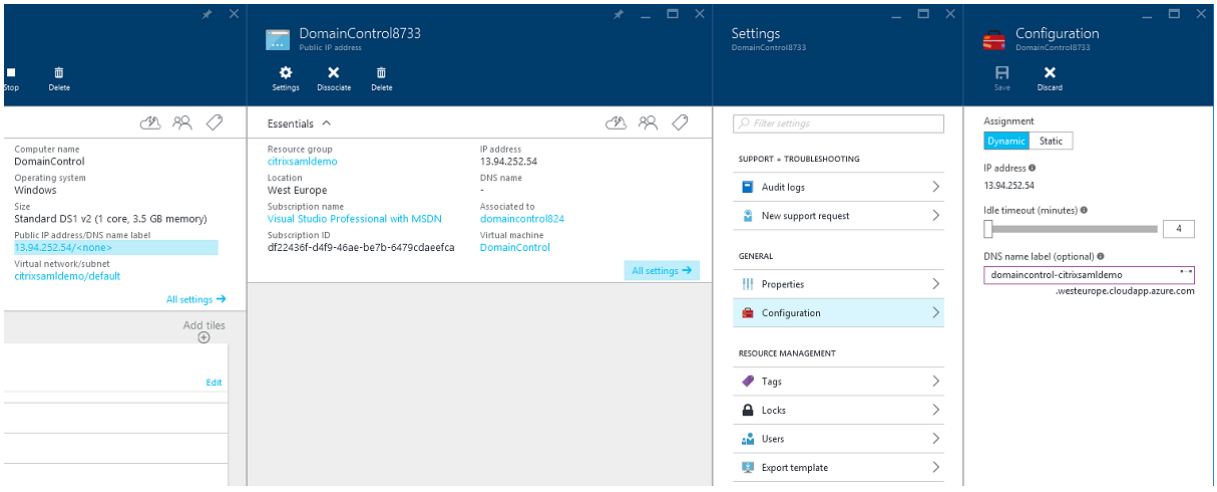
Alle in Azure ausgeführten VMs müssen zur ausschließlichen Verwendung dieses DNS-Servers konfiguriert werden. Sie können diese Konfiguration über die Netzwerkschnittstellen-GUI durchführen.




Standardmäßig wird die interne IP-Adresse (10.0.0.9) dynamisch zugewiesen. Sie können die IP-Adresse über die zugehörige Einstellung bleibend zuweisen. Diesen Schritt müssen Sie für den Webanwendungsproxyserver und den Domänencontroller durchführen.

### Konfigurieren einer externen DNS-Adresse

Wenn eine virtuelle Maschine ausgeführt wird, verwendet Azure seinen eigenen DNS-Zonenserver, der auf die aktuelle, der VM zugewiesene, öffentliche IP-Adresse verweist. Dies kann als nützliches Feature aktiviert werden, da Azure standardmäßig IP-Adressen bei jedem VM-Start zuweist.



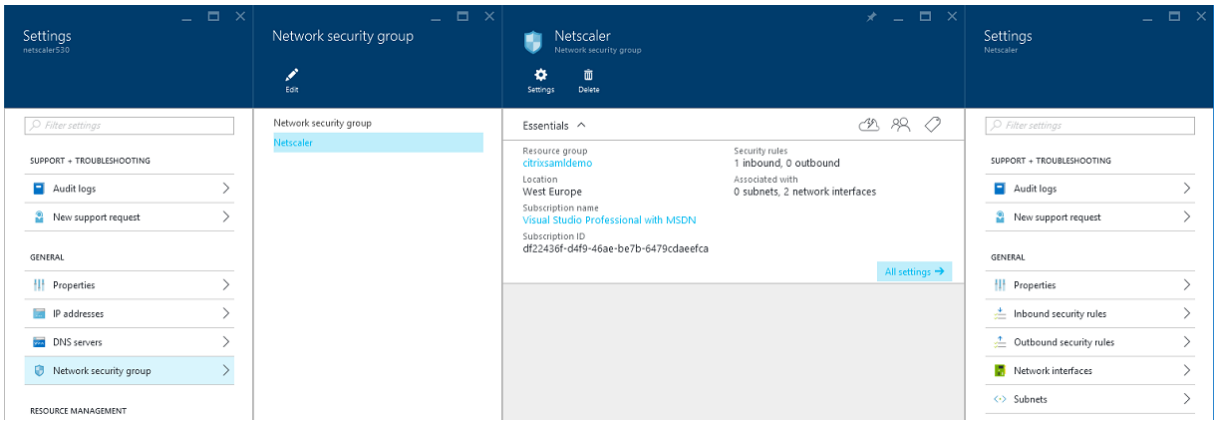

In diesem Beispiel wird dem Domänencontroller die DNS-Adresse “domaincontrol-citrixsamldemo.westeurope.clo
zugewiesen.

Nach Abschluss der Remotekonfiguration dürfen öffentliche IP-Adressen nur für die Webanwendungsproxy- und die Citrix Gateway-VMs aktiviert sein. (Während der Konfiguration wird die öffentliche IP-Adresse für den RDP-Zugriff auf die Umgebung verwendet).

### Konfigurieren von Sicherheitsgruppen

Von der Azure-Cloud werden Firewall-Regeln für den TCP/UDP-Zugriff auf VMs aus dem Internet mit Sicherheitsgruppen verwaltet. Standardmäßig lassen alle VMs RDP-Zugriff zu. Der Citrix Gateway-Server und der Webanwendungsproxyserver müssen außerdem TLS an Port 443 zulassen.



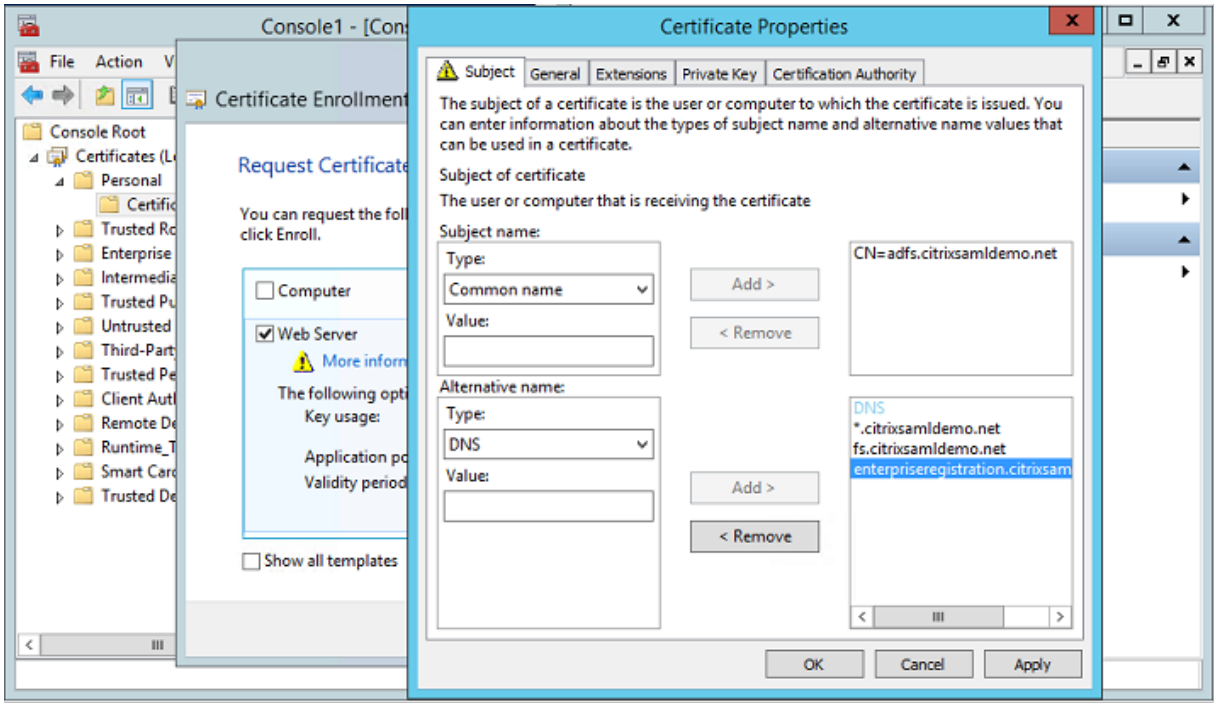

### Erstellen eines AD FS-Zertifikats

Aktivieren Sie die Zertifikatvorlage **Webserver** in 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 auf dem AD FS-Server und dem Webanwendungsproxyserver installieren, damit die PFX-Datei bevorzugte Option ist.

Stellen Sie ein Webserverzertifikat mit folgenden Antragstellernamen aus:

- Commonname:
  - adfs.citrixsamldemo.net (Computername)
- SubjectAltname:
  - *.citrixsamldemo.net [Zonenname]
  - fs.citrixsamldemo. net [Eintrag in DNS]
  - enterpriseregistration.citrixsamldemo.net




Exportieren Sie das Zertifikat mitsamt einem kennwortgeschützten privaten Schlüssel in eine PFX-Datei.

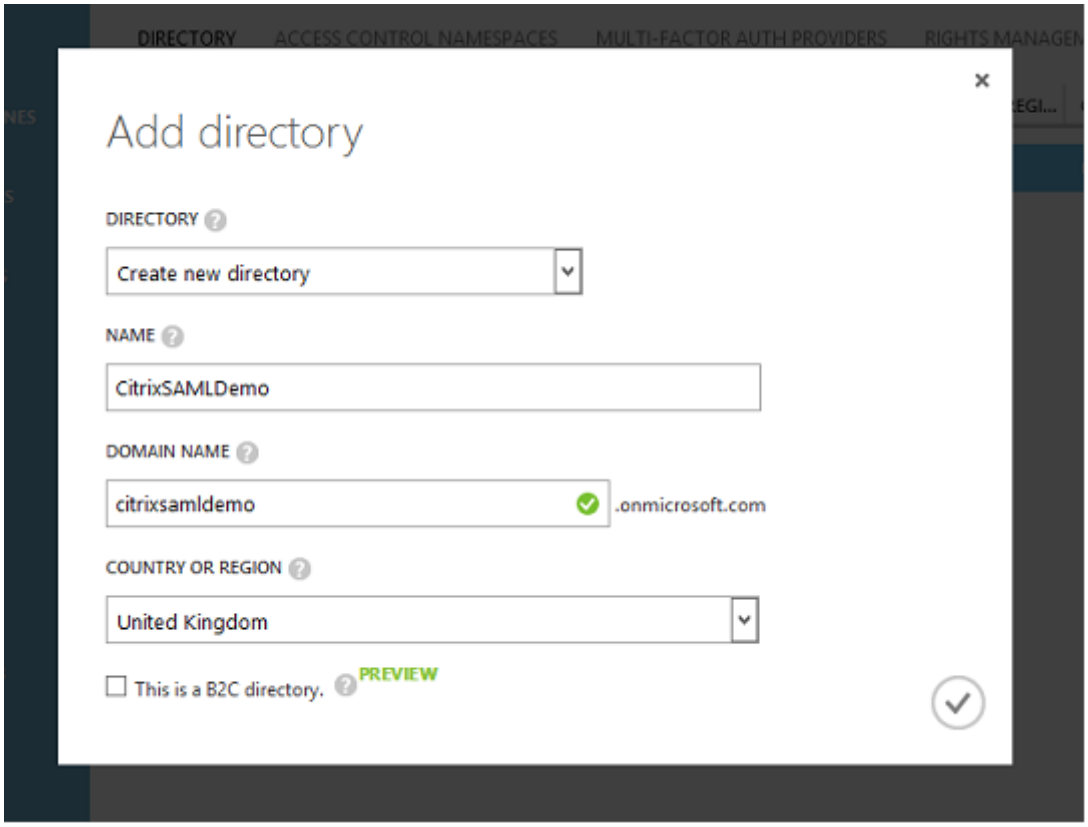
## Einrichten von Azure Active Directory

In diesem Abschnitt wird erläutert, wie eine neue Instanz von Azure AD eingerichtet und Benutzeridentitäten für die Windows 10-Einbindung in Azure AD erstellt werden.

### Erstellen eines Verzeichnisses

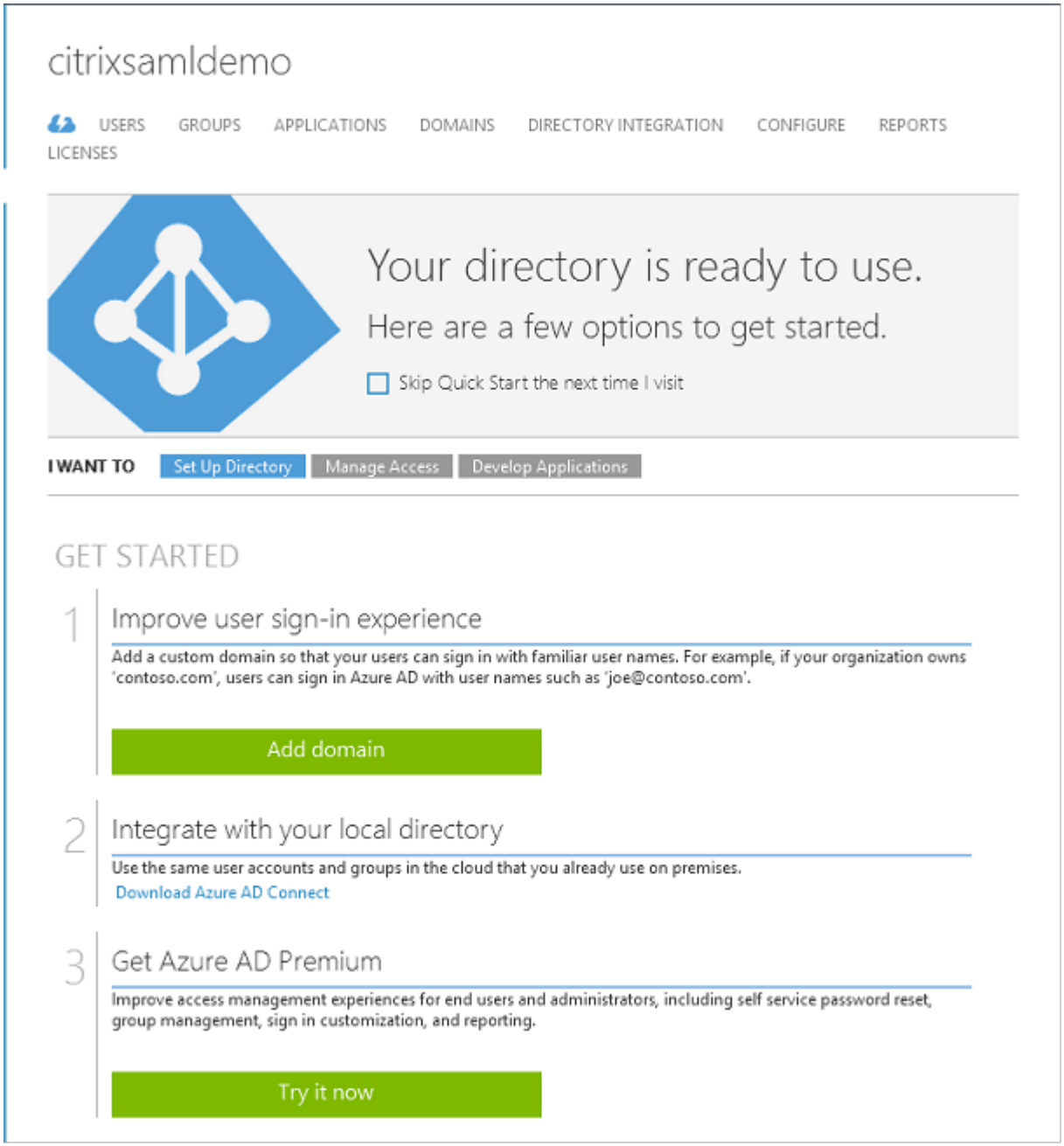
Melden Sie sich beim Azure-Portal an und erstellen Sie ein Verzeichnis.




Zum Abschluss wird die Seite “Zusammenfassung”angezeigt.

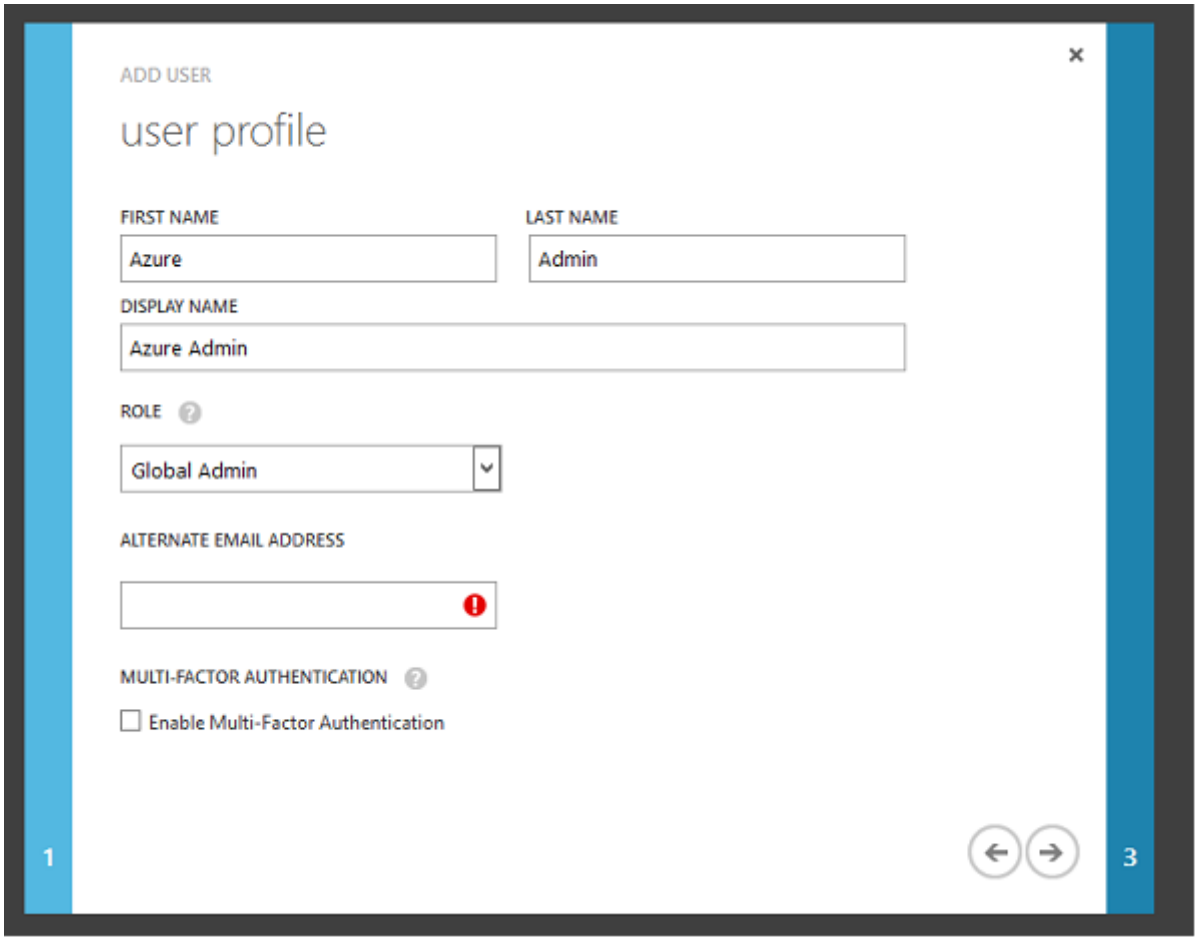
 




**Erstellen eines globalen Administrators (AzureAdmin)**

Erstellen Sie einen globalen Administrator in Azure (in diesem Beispiel `AzureAdmin@citrixsamldemo.onmicrosoft.com`) und melden Sie sich mit dem neuen Konto an, um ein Kennwort einzurichten.




**Registrieren der Domäne bei Azure AD**

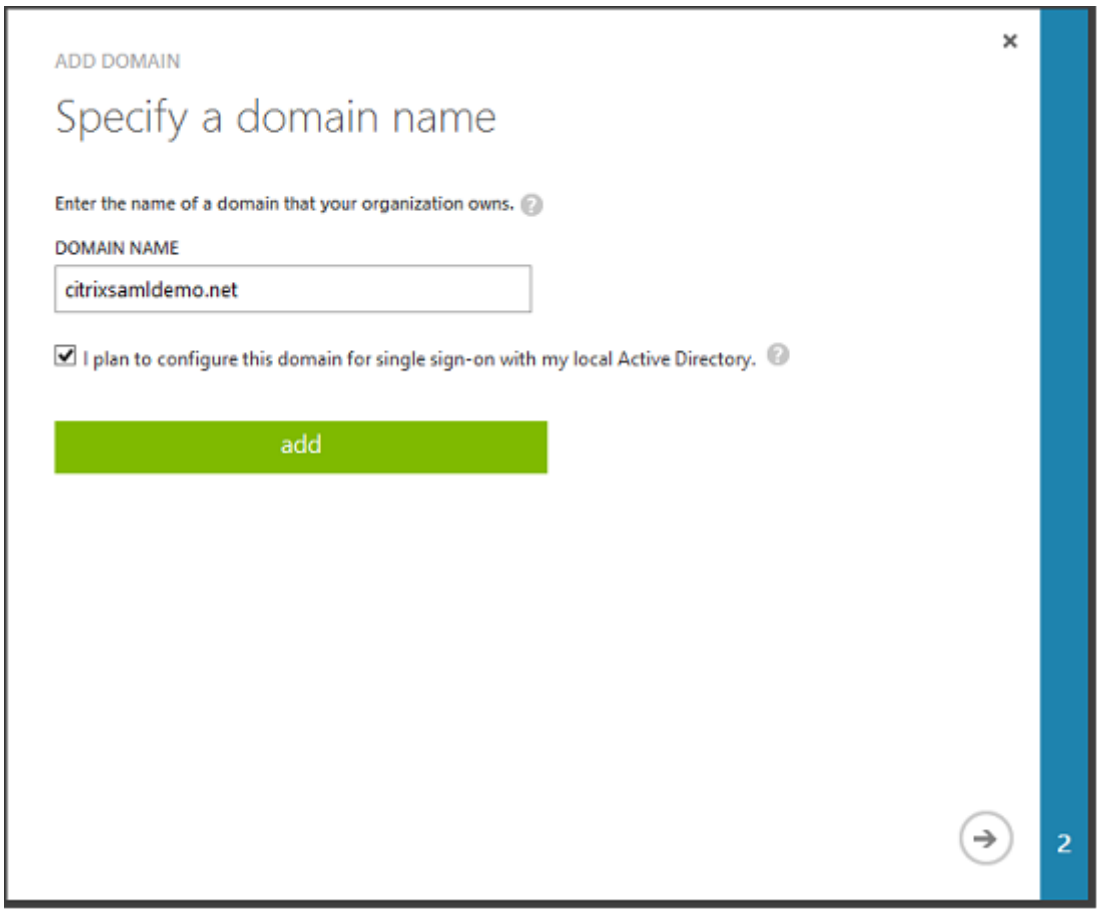
Standardmäßig werden Benutzer anhand einer E-Mail-Adresse im Format `<user.name>@<company>.onmicrosoft.com` identifiziert.

Dies funktioniert zwar ohne weitere Konfiguration, eine E-Mail-Adresse im Standardformat ist jedoch besser; sie sollte möglichst dem E-Mail-Konto des Endbenutzers entsprechen: `<user.name>@<company>.com`.

Die Aktion **Domäne hinzufügen** dient zum Konfigurieren der Umleitung von der tatsächlichen Unternehmensdomäne. Im vorliegenden Beispiel ist dies `citrixsamldemo.net`.

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

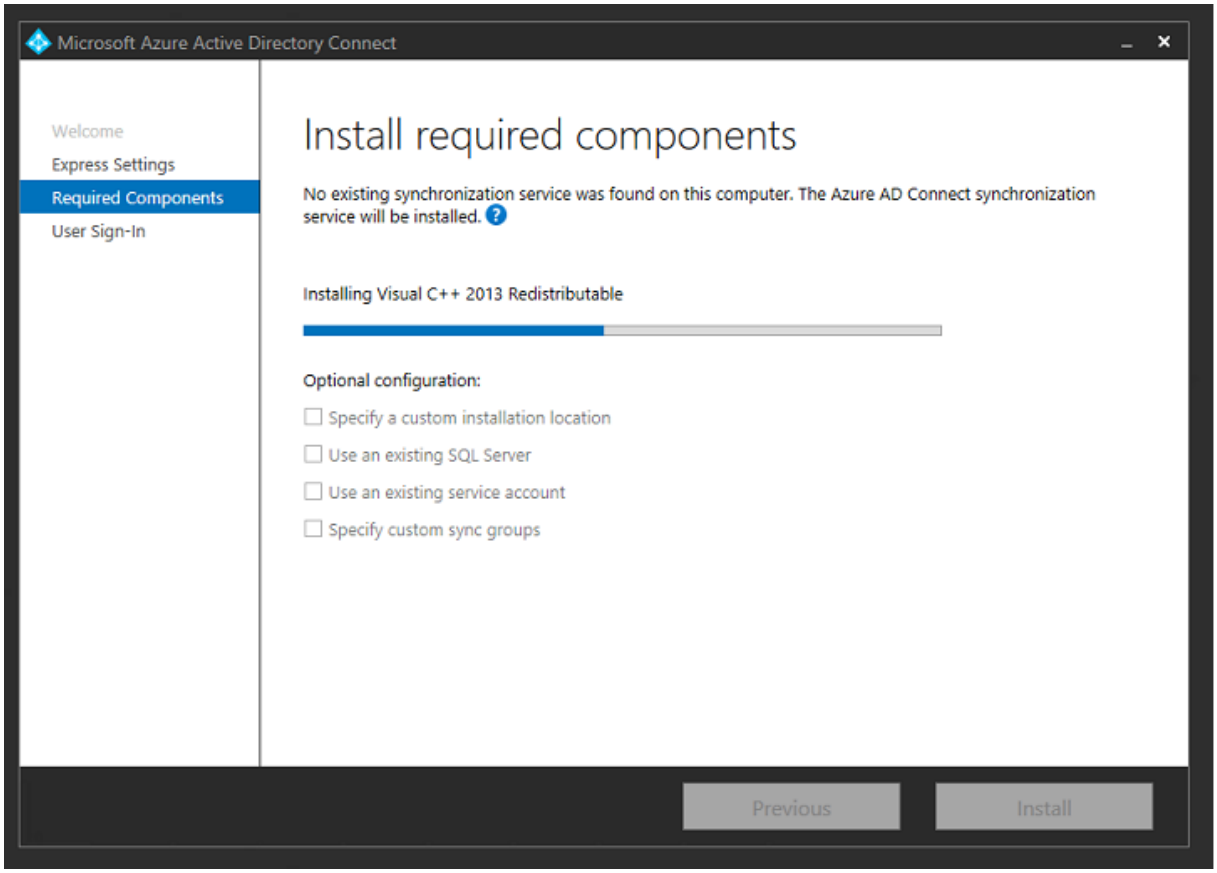
 




**Installieren von Azure AD Connect**

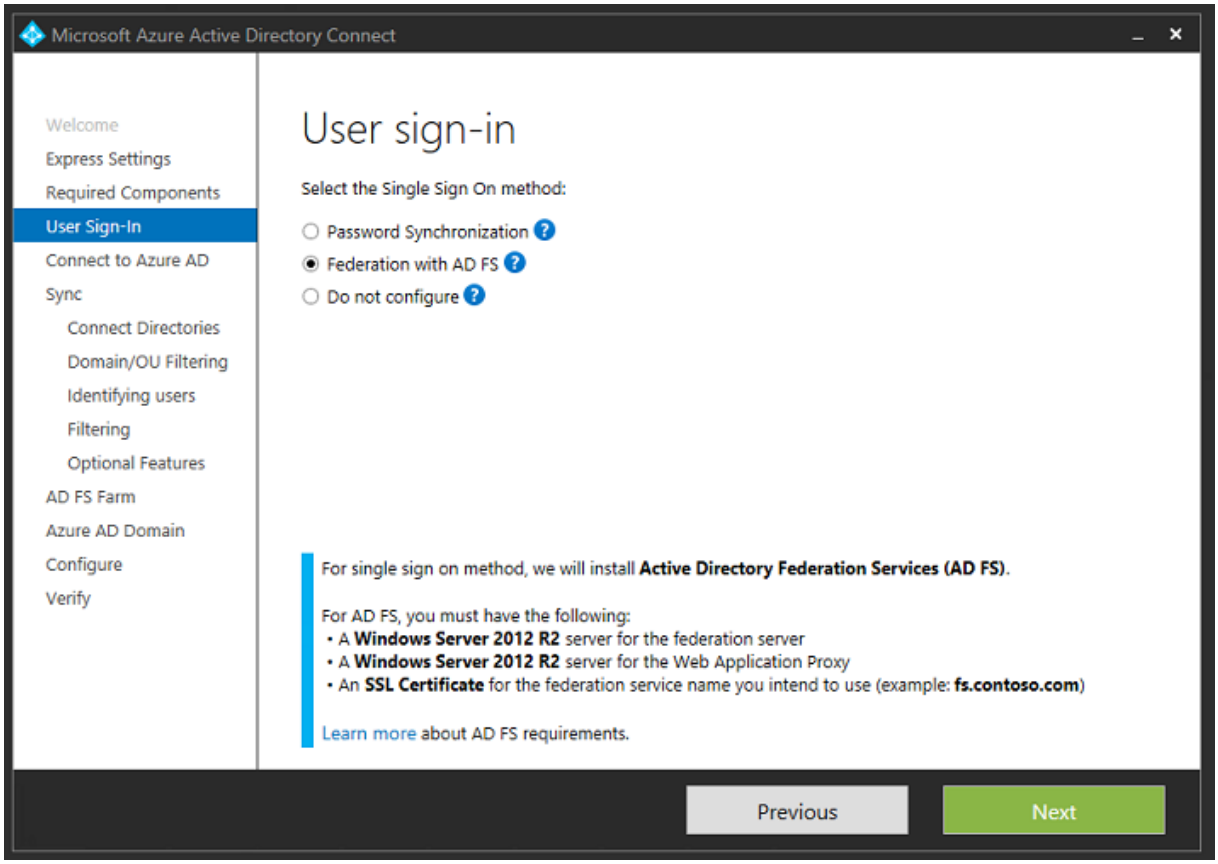
In Schritt 2 der Azure AD-Konfiguration werden Sie auf die Downloadseite für Azure AD Connect umgeleitet. Installieren Sie dieses Tool auf der AD FS-VM. Verwenden Sie **Benutzerdefinierte Installation** anstelle von **Express-Einstellungen**, damit AD FS-Optionen verfügbar sind.



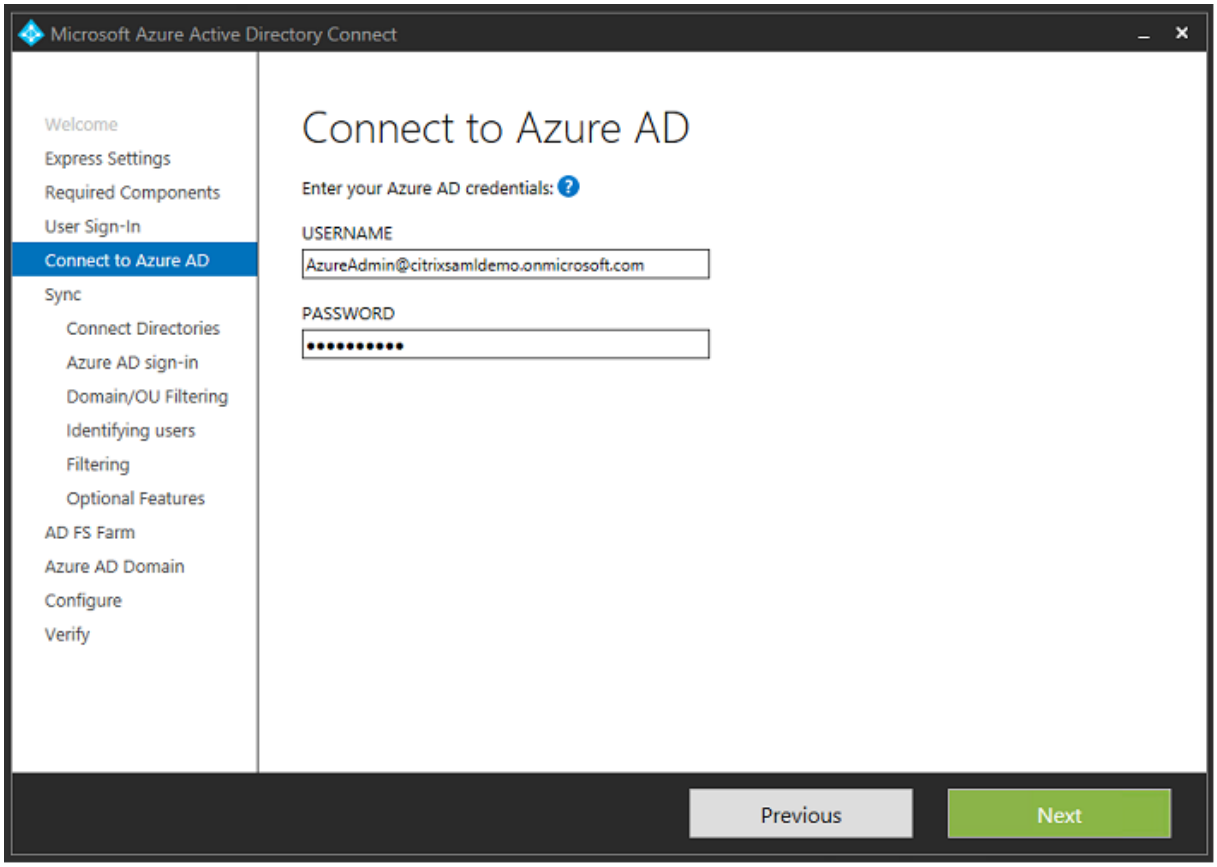

Wählen Sie die Single Sign-On-Option **Verbund mit AD FS**.



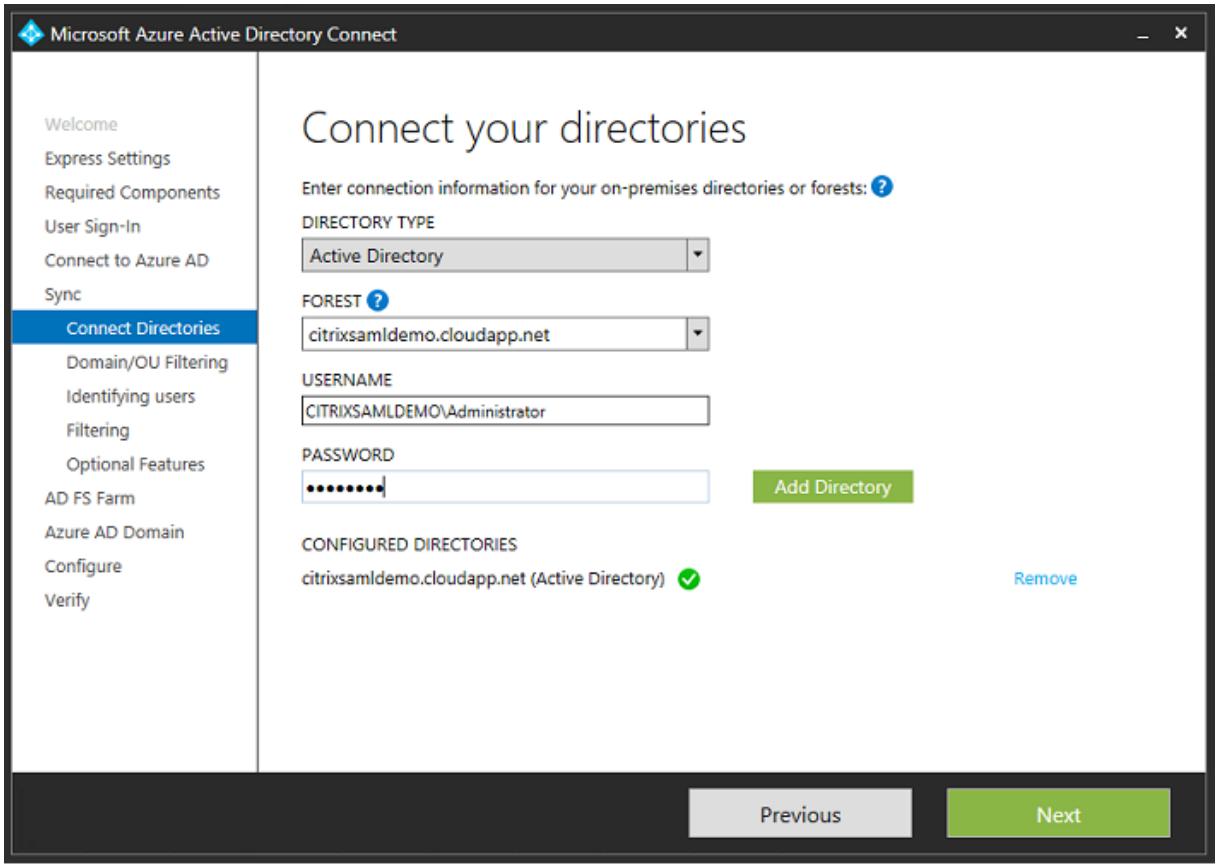

Stellen Sie eine Verbindung mit Azure unter Verwendung des zuvor erstellten Administratorkontos her.



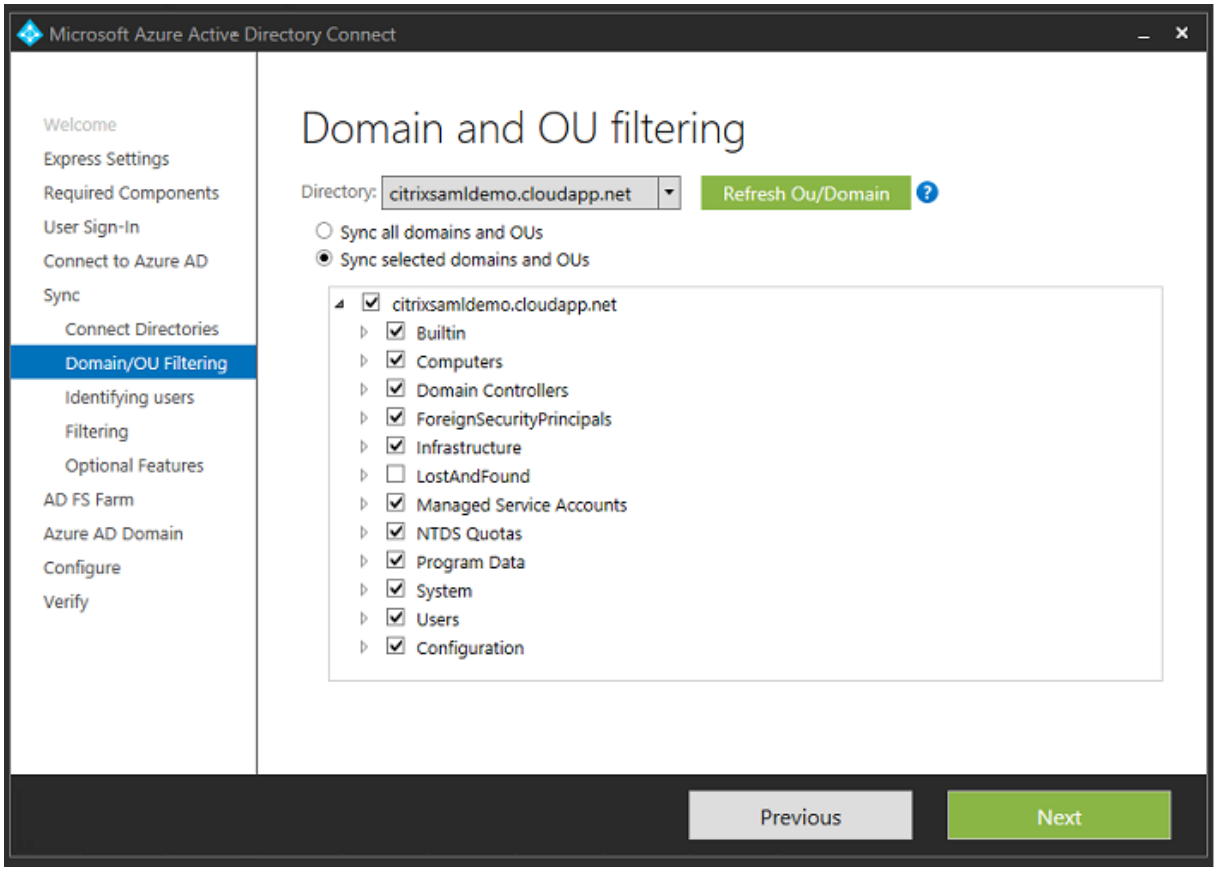

Wählen Sie die interne AD-Gesamtstruktur.



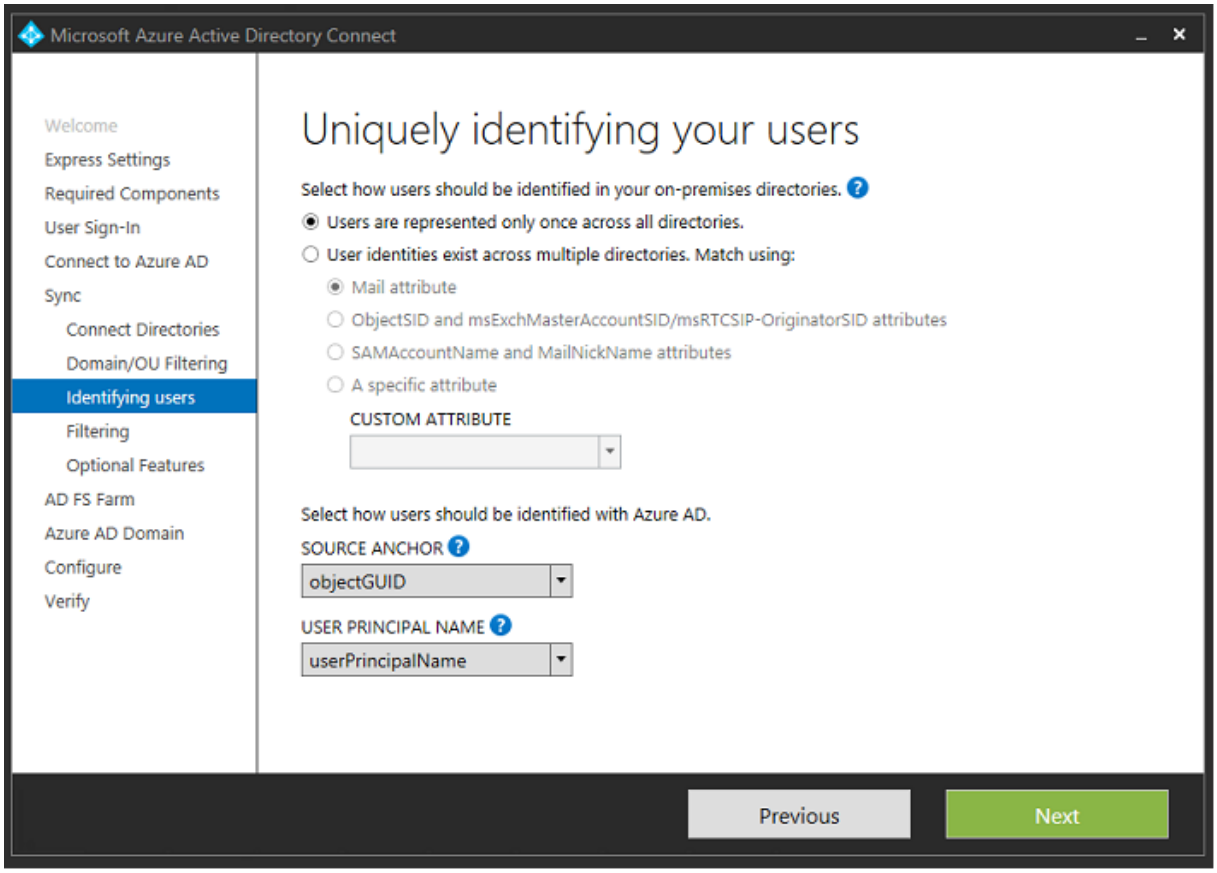

Synchronisieren Sie alle alten Active Directory-Objekte mit Azure AD.



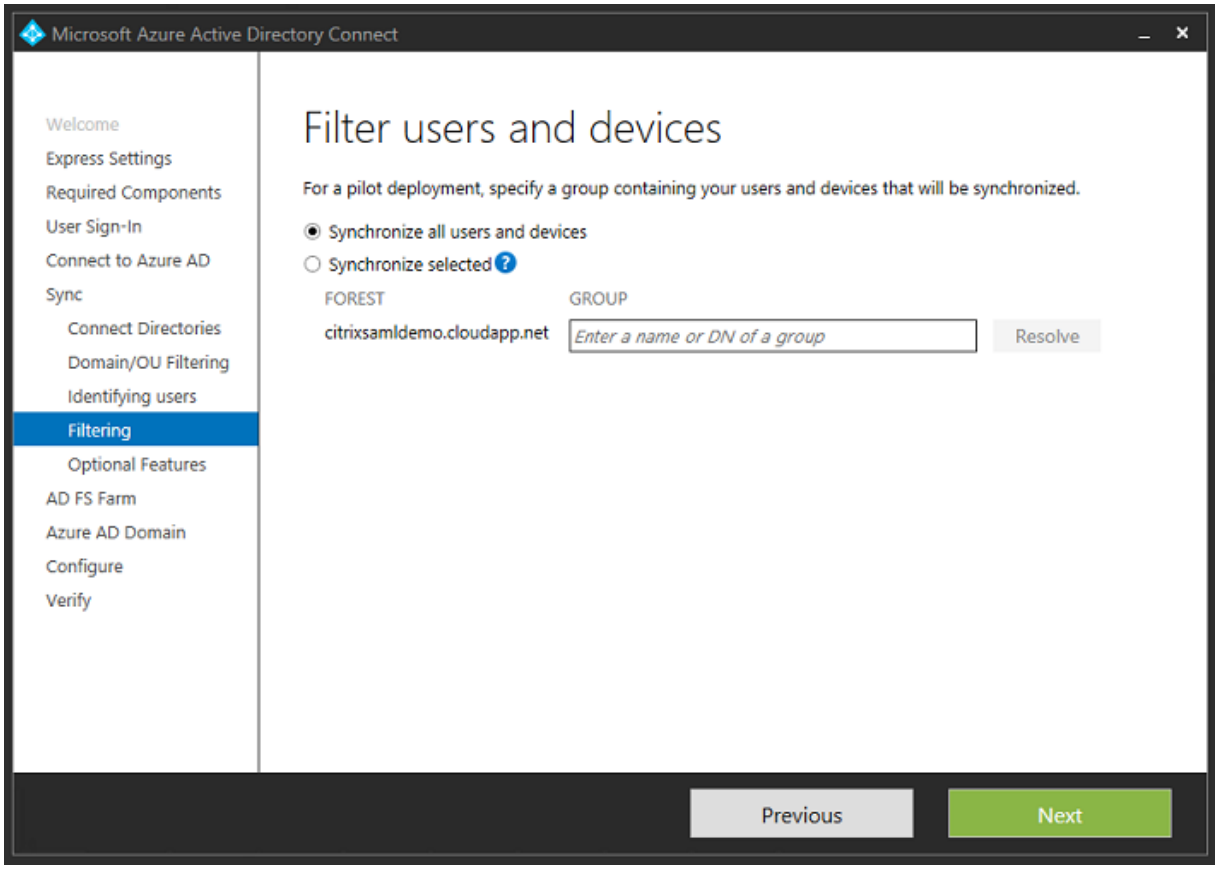

Bei einer einfachen Verzeichnisstruktur sind die Benutzernamen ausreichend eindeutig zur Identifizierung von Benutzern, die sich anmelden.



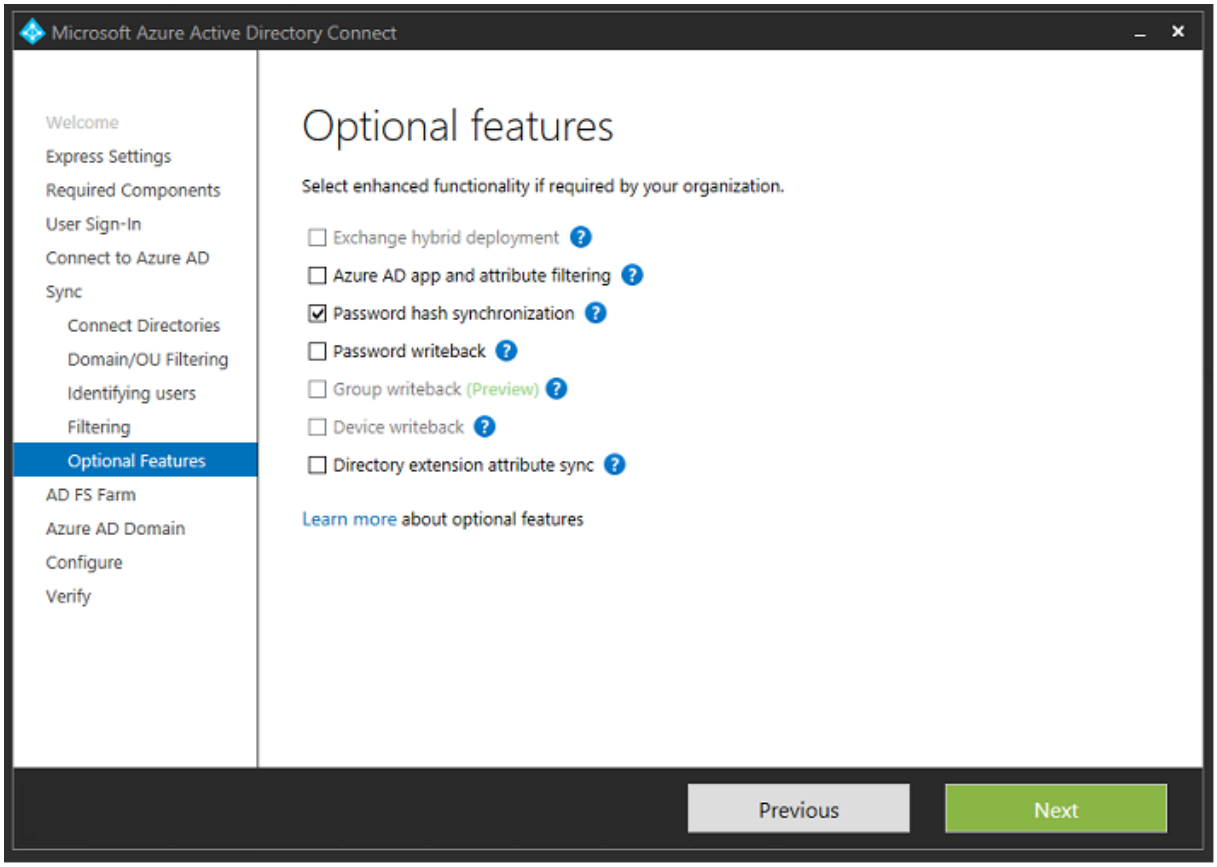

Akzeptieren Sie die Standardfilteroptionen oder schränken Sie Benutzer und Geräte auf bestimmte Gruppen ein.



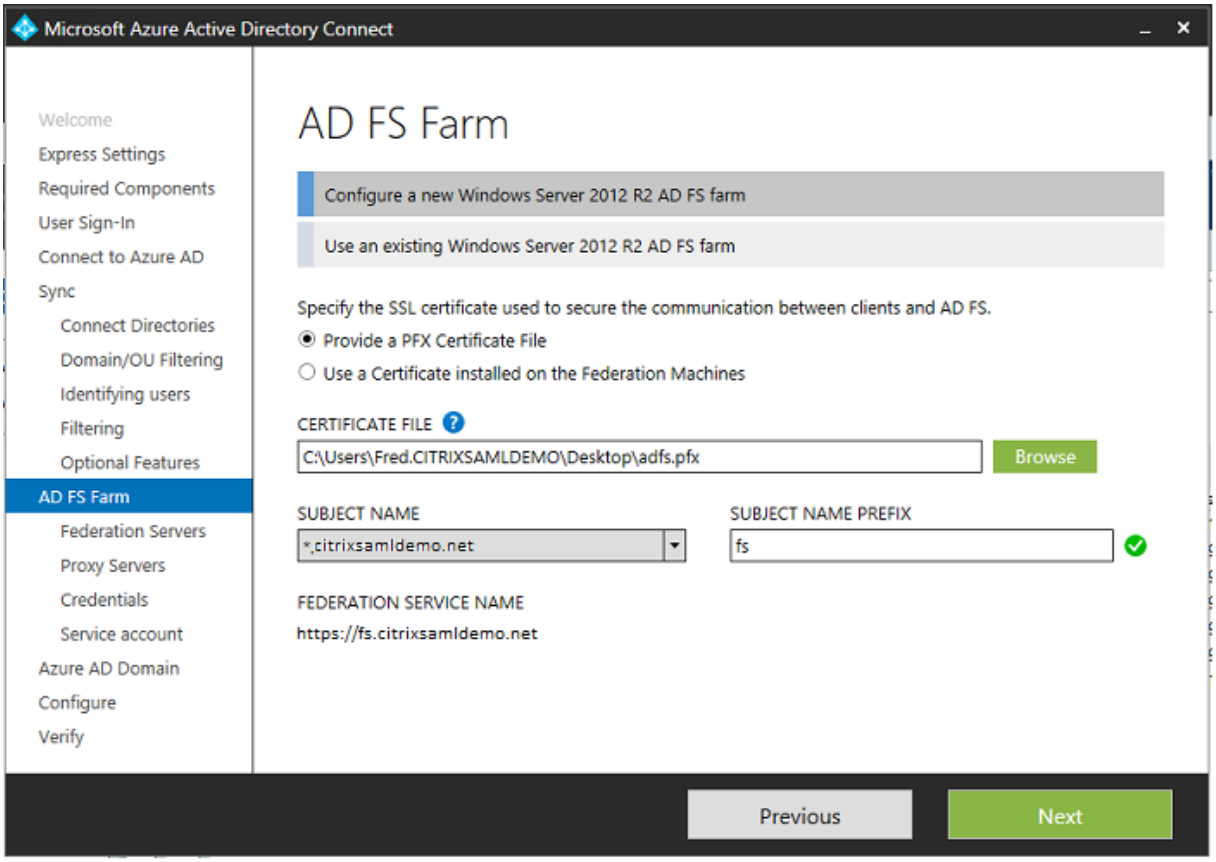

Falls gewünscht können Sie die Azure AD-Kennwörter mit Active Directory synchronisieren. Das ist für die AD FS-basierte Authentifizierung normalerweise nicht nötig.



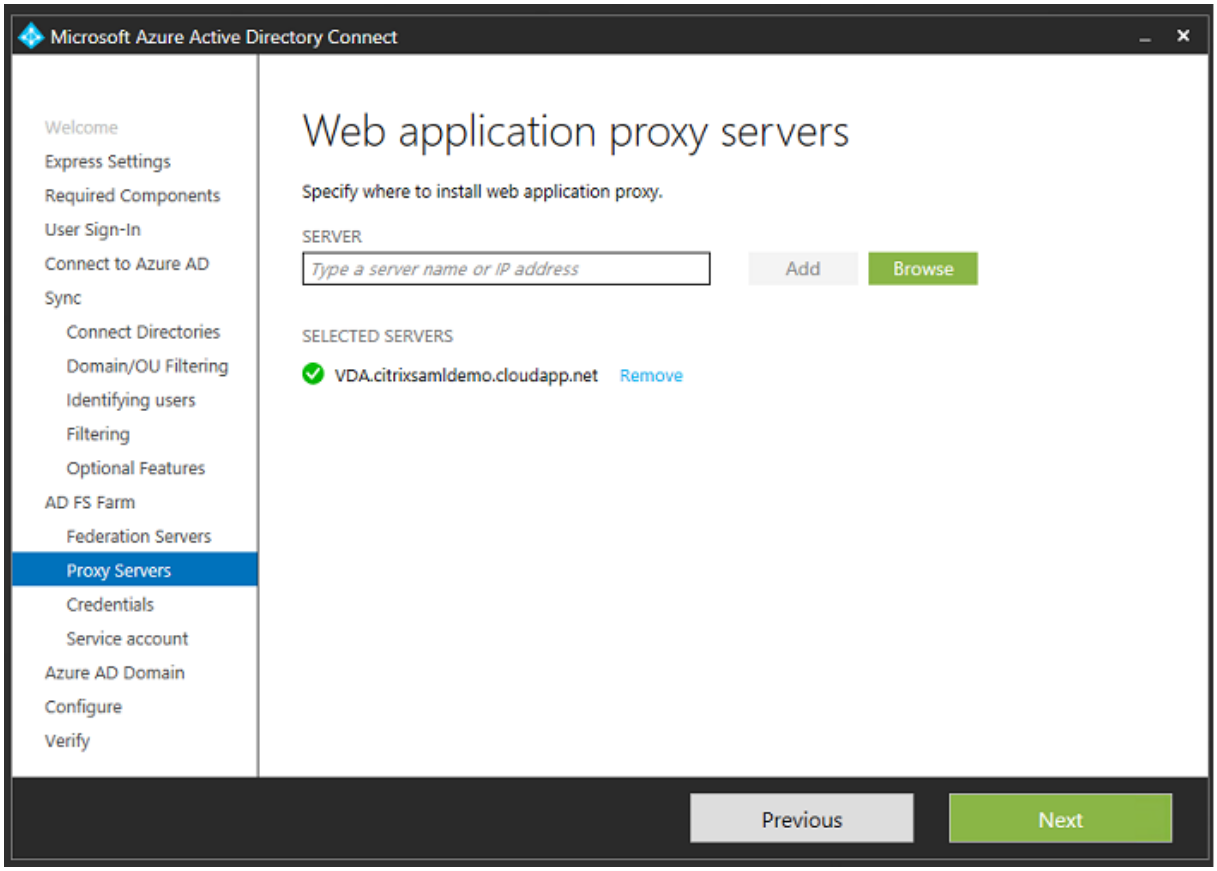

Wählen Sie die Zertifikat-PFX-Datei für AD FS unter Angabe von “fs.citrixsamldemo.net”als DNS-Namen aus.




Wenn Sie zur Auswahl eines Proxyservers aufgefordert werden, geben Sie die Adresse des wap.citrixsamldemo.net-Servers ein. Sie müssen u. U. das Cmdlet **Enable-PSRemoting** –**Force** als Administrator auf dem Webanwendungsproxyserver ausführen, damit Azure AD diesen konfigurieren kann.

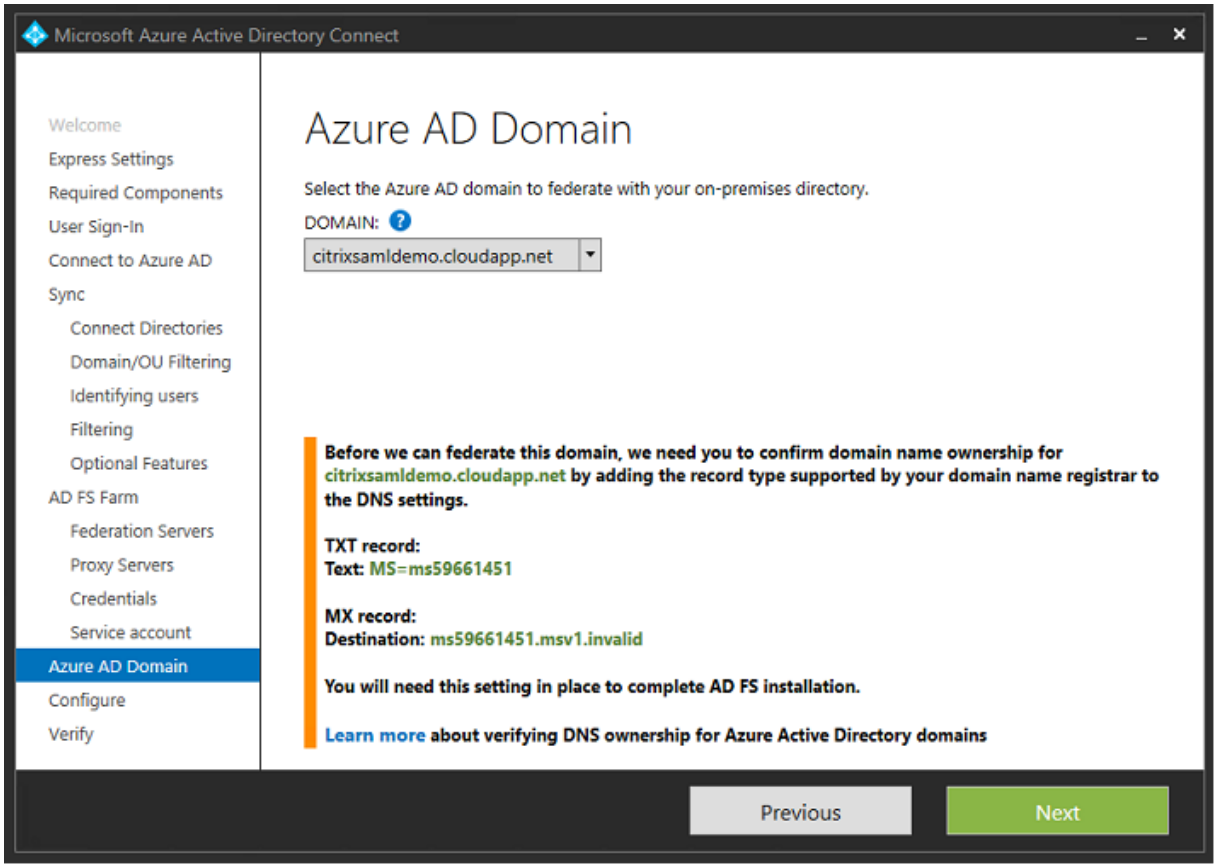
 



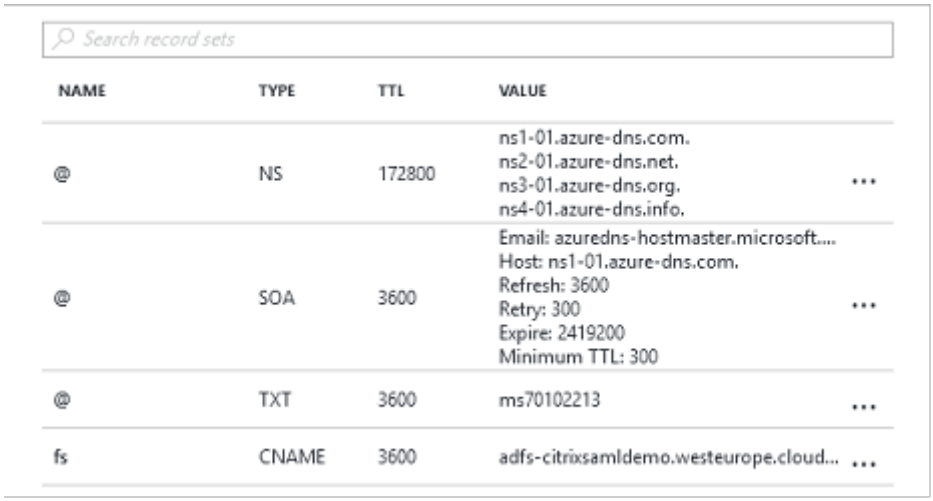

> **Hinweis:**
>
> Wenn dieser Schritt aufgrund von Problemen mit der Remote PowerShell-Vertrauensstellung fehlschlägt, versuchen Sie den Beitritt des Webanwendungsproxyservers zur Domäne.

Verwenden Sie für die restlichen Schritte des Assistenten die Standardadministratorkennwörter und erstellen Sie ein Dienstkonto für AD FS. Von Azure AD Connect wird dann zur Überprüfung der Eigentümerschaft der DNS-Zone aufgefordert.

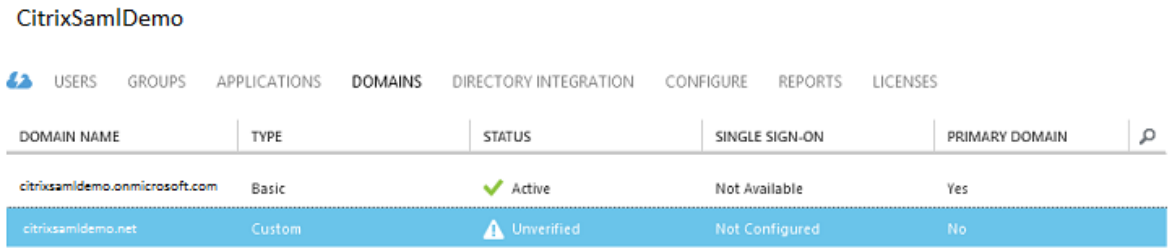



Fügen Sie die TXT- und MX-Einträge den DNS-Adresseinträgen in Azure hinzu.



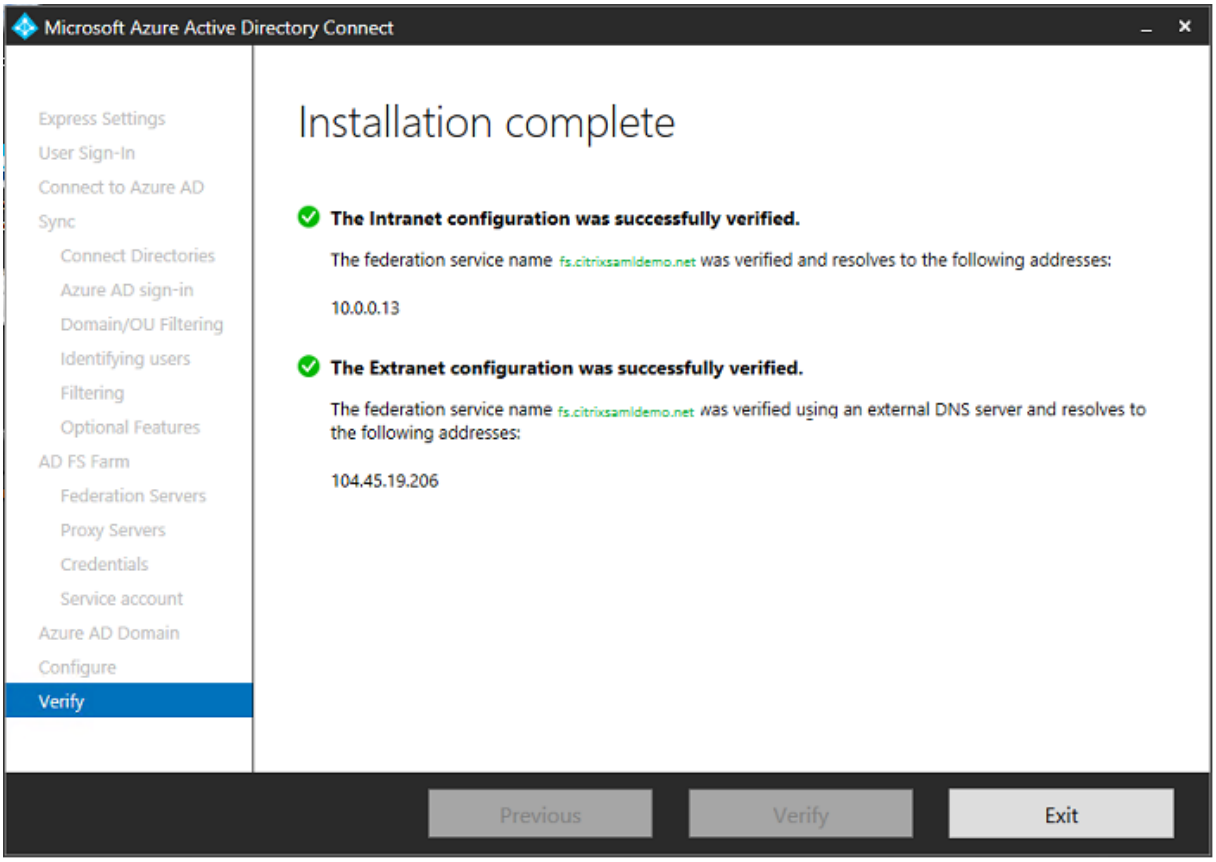

Klicken Sie in der Azure-Verwaltungskonsole auf **Überprüfen**.




> **Hinweis:**
>
> Wenn dieser Schritt fehlschlägt, können Sie die Domäne vor Ausführung von Azure AD Connect überprüfen.

Nach Anschluss wird die externe Adresse fs.citrixsamldemo.net über Port 443 angesprochen.

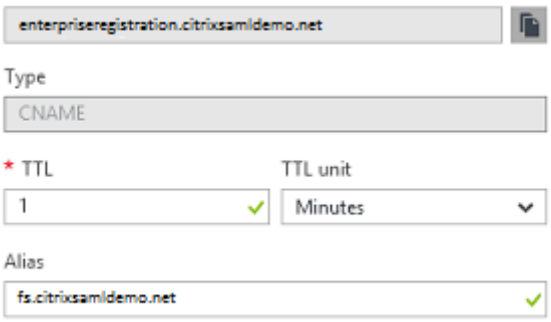



### Aktivieren der Azure AD-Einbindung

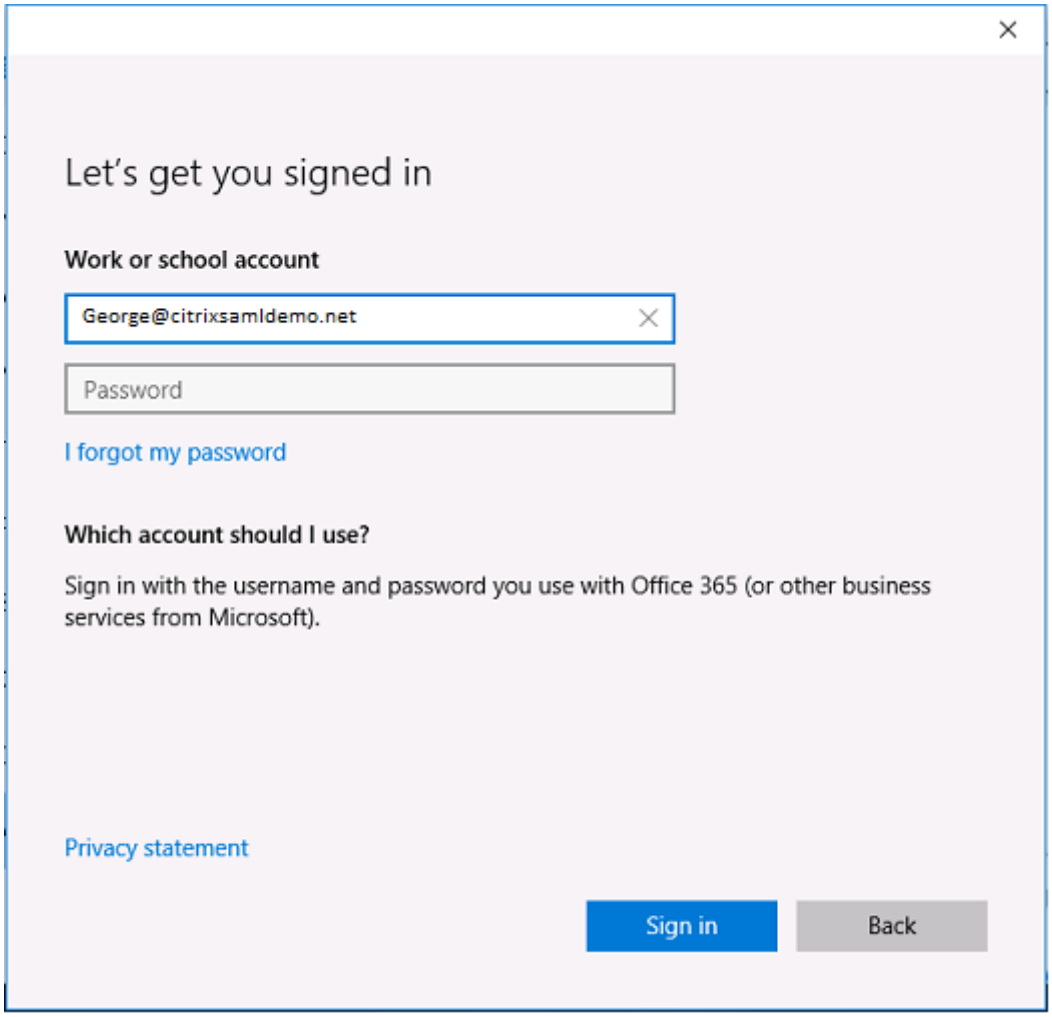
Wenn ein Benutzer eine E-Mail-Adresse eingibt, sodass Windows 10 einen Beitritt zu Azure AD durchführen kann, wird das DNS-Suffix zur Erstellung eines CNAME-DNS-Eintrags verwendet, der auf ADFS: enterpriseregistration.<*upnsuffix*> verweisen muss.

Im Beispiel ist dies `fs.citrixsamldemo.net`.

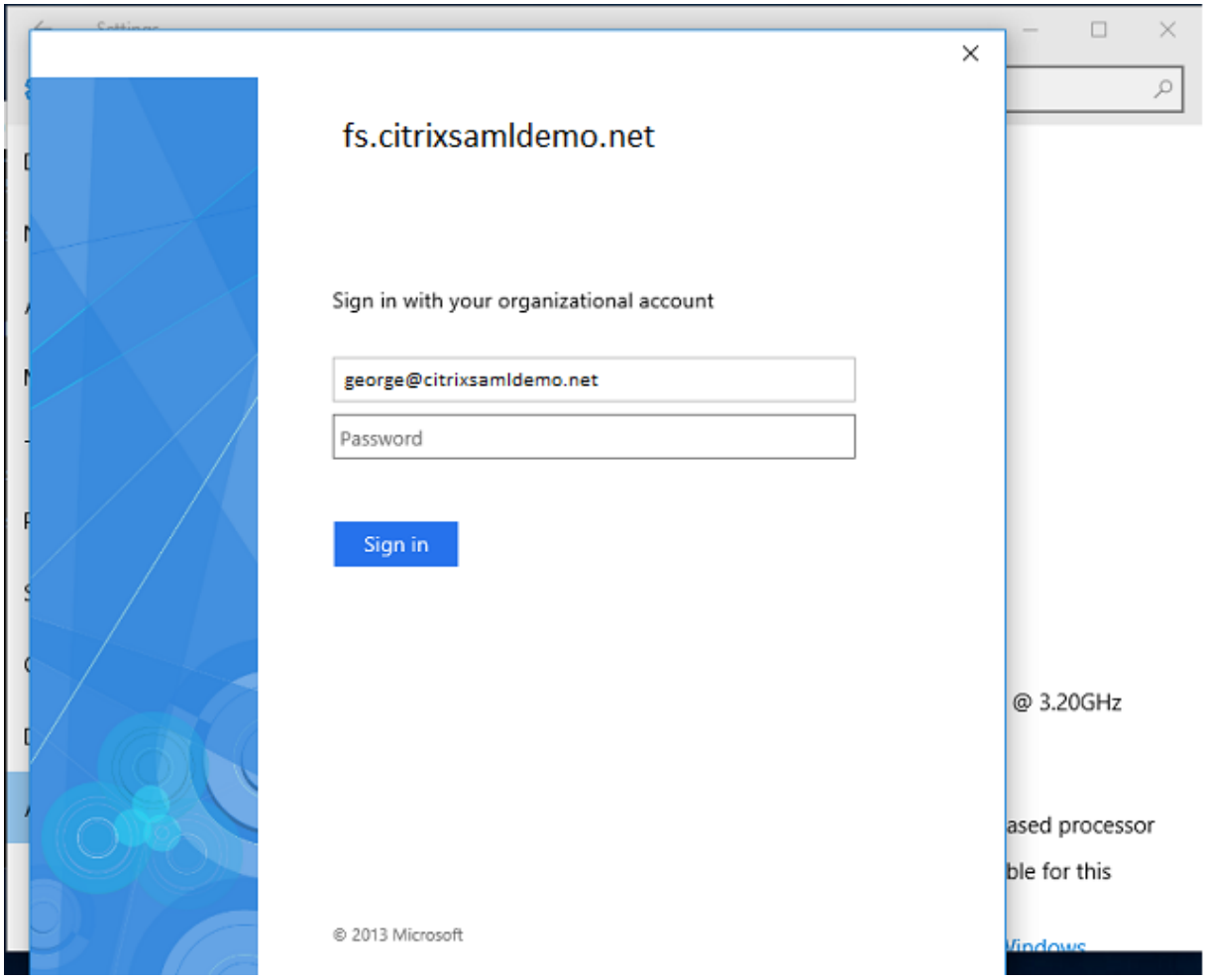


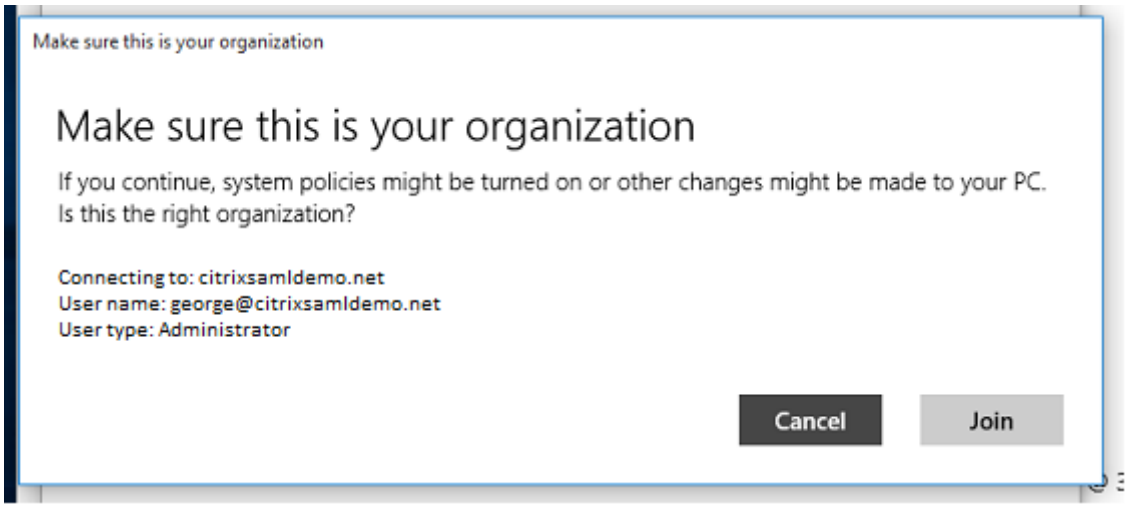

Wenn Sie keine öffentliche Zertifizierungsstelle verwenden, installieren Sie das AD FS-Stammzertifikat auf dem Windows 10-Computer, damit Windows dem AD FS-Server vertraut. Führen Sie einen Azure AD-Domänenbeitritt unter Verwendung des zuvor erstellten Standardbenutzerkontos durch.



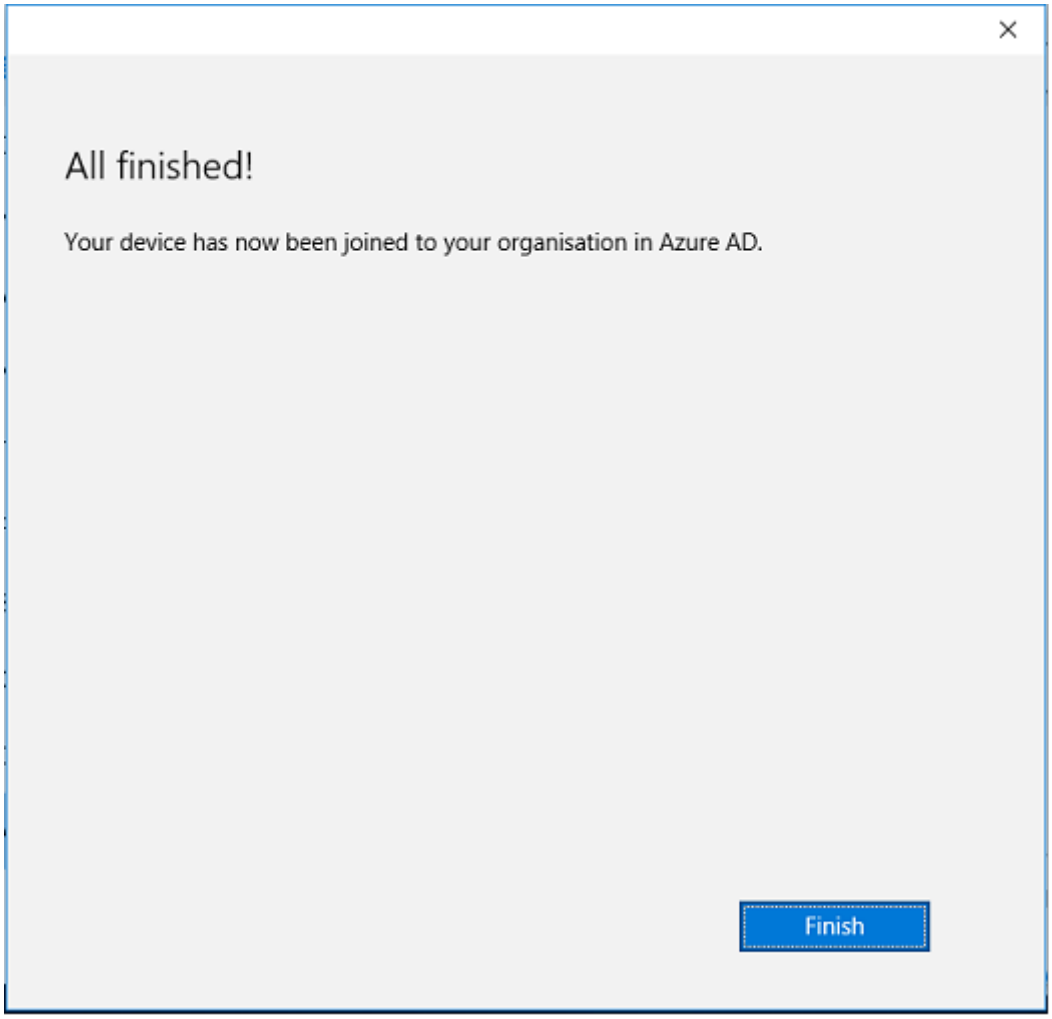

Der UPN muss mit dem von dem AD FS-Domänencontroller erkannten UPN übereinstimmen.





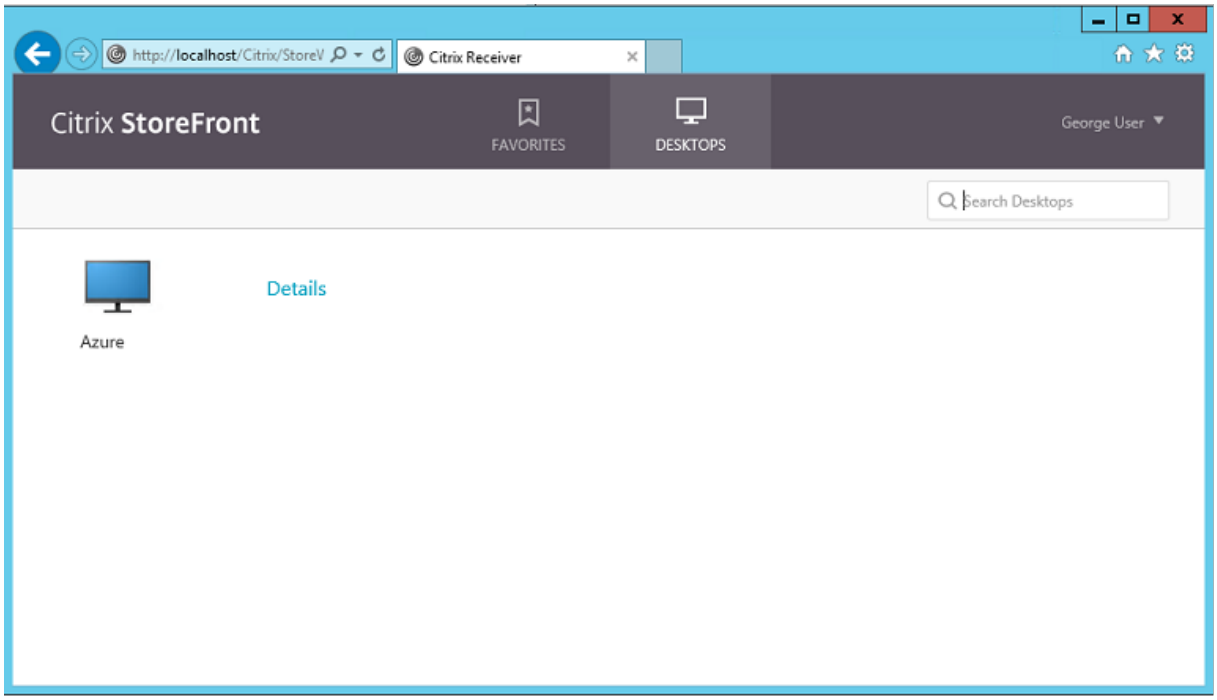

Prüfen Sie den Erfolg der Azure AD-Einbindung, indem Sie die Maschine neu starten und sich mit der E-Mail-Adresse des Benutzers anmelden. Nach der Anmeldung starten Sie Microsoft Edge und stellen Sie eine Verbindung mit http://myapps.microsoft.com her. Die Website müsste Single Sign-On automatisch verwenden.

### Installieren von Citrix Virtual Apps oder Citrix Virtual Desktops

Sie können die virtuellen Maschinen für Delivery Controller und VDA in Azure direkt vom Citrix Virtual Apps- oder Citrix Virtual Desktops-ISO-Image wie gewohnt installieren.

In diesem Beispiel wird StoreFront auf demselben Server wie der Delivery Controller installiert. Der VDA wird als eigenständiger Windows 2012 R2 RDS-Worker ohne Integration in Maschinenerstellungsdienste installiert (optional könnte dies aber konfiguriert werden). Vergewissern Sie sich bevor Sie fortfahren, dass der Benutzer George@citrixsamldemo.net sich mit einem Kennwort authentifizieren kann.




Führen Sie das PowerShell-Cmdlet **Set-BrokerSite –TrustRequestsSentToTheXmlServicePort $true** auf dem Controller aus, damit StoreFront eine Authentifizierung ohne Anmeldeinformationen des Benutzers durchführen kann.

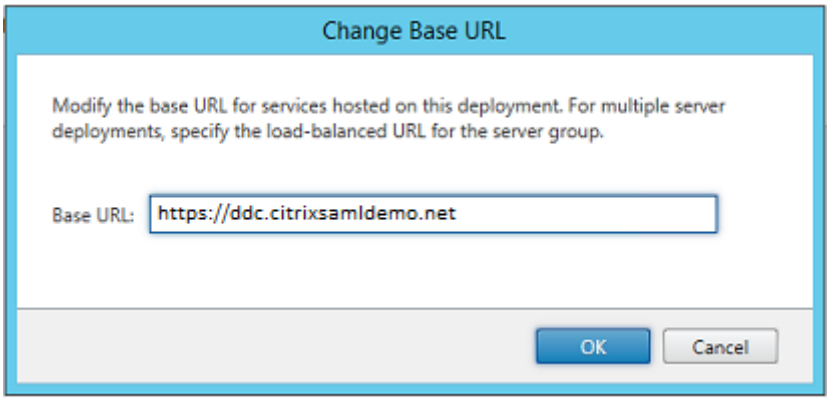
### Verbundauthentifizierungsdienst installieren

Installieren Sie den FAS auf dem AD FS-Server und konfigurieren Sie eine Regel, durch die der Controller als vertrauenswürdiges StoreFront agiert (da in diesem Beispiel StoreFront auf derselben VM wie der Delivery Controller installiert ist). Siehe Installation und Konfiguration.

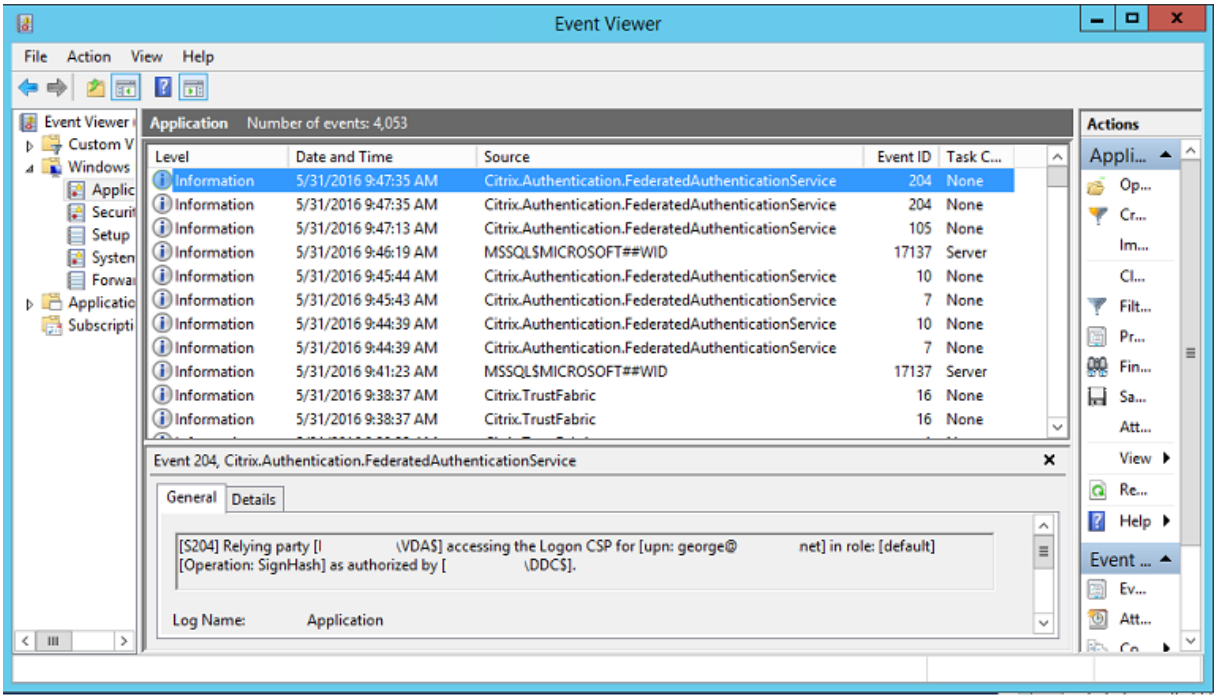
### Konfigurieren von StoreFront

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



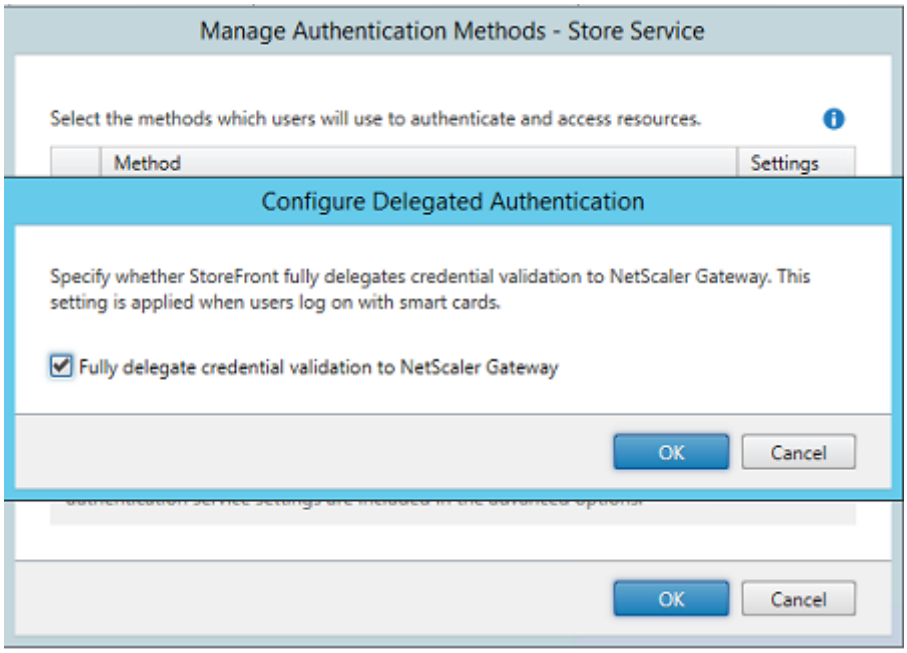

Konfigurieren Sie die Verwendung des FAS-Servers durch StoreFront (mit dem PowerShell-Skript in Installation und Konfiguration) und führen Sie in Azure einen Test durch. Prüfen Sie in der Ereignisanzeige des FAS-Servers, dass die Anmeldung über den FAS erfolgt.



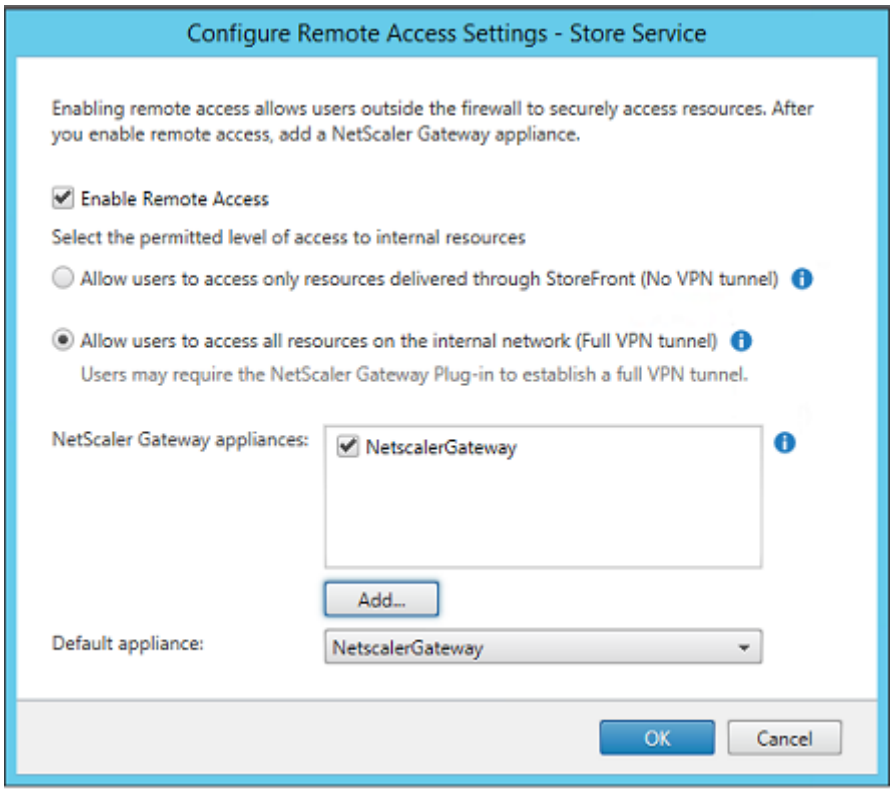

**Konfigurieren von StoreFront für die Verwendung von Citrix Gateway**

Konfigurieren Sie im Bereich **Authentifizierungsmethoden verwalten** der StoreFront-Verwaltungskonsole die Authentifizierung über Citrix Gateway.



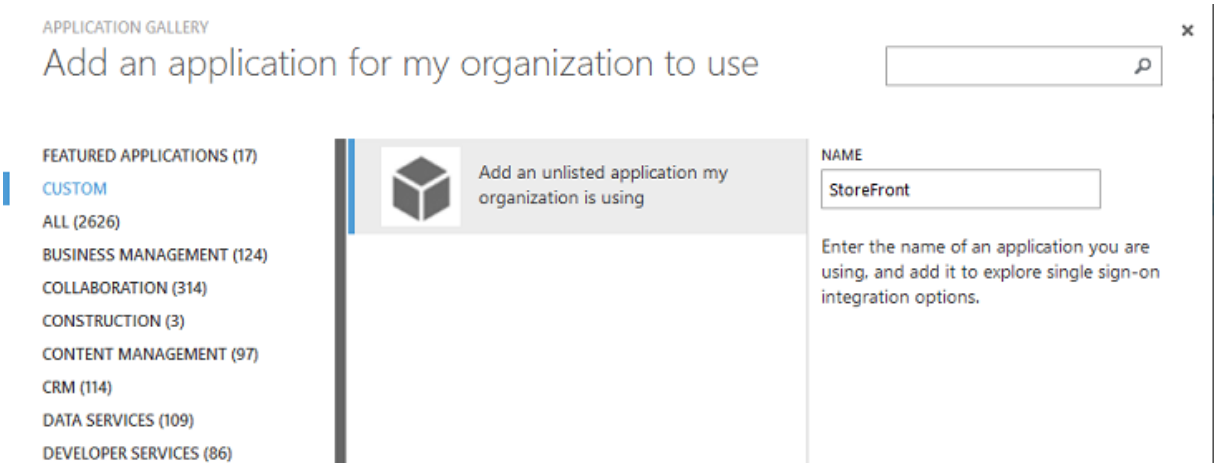

Zum Integrieren der Citrix Gateway-Authentifizierungsoptionen konfigurieren Sie eine Secure Ticket Authority (STA) und die Citrix Gateway-Adresse.



### Konfigurieren einer neuen Azure-Anwendung für das Single Sign-On bei StoreFront

In diesem Abschnitt werden die Single Sign-On-Features von Azure AD SAML 2.0 verwendet, die zurzeit ein Azure Active Directory Premium-Abonnement erfordern. Wählen Sie in der Azure AD-Verwaltung **Neue Anwendung** und **Anwendung aus dem Katalog hinzufügen**.




Wählen Sie **BENUTZERDEFINIERT > Eine nicht aufgeführte von meiner Organisation eingesetzte Anwendung hinzufügen**, um eine neue benutzerdefinierte Anwendung für die Benutzer zu erstellen.

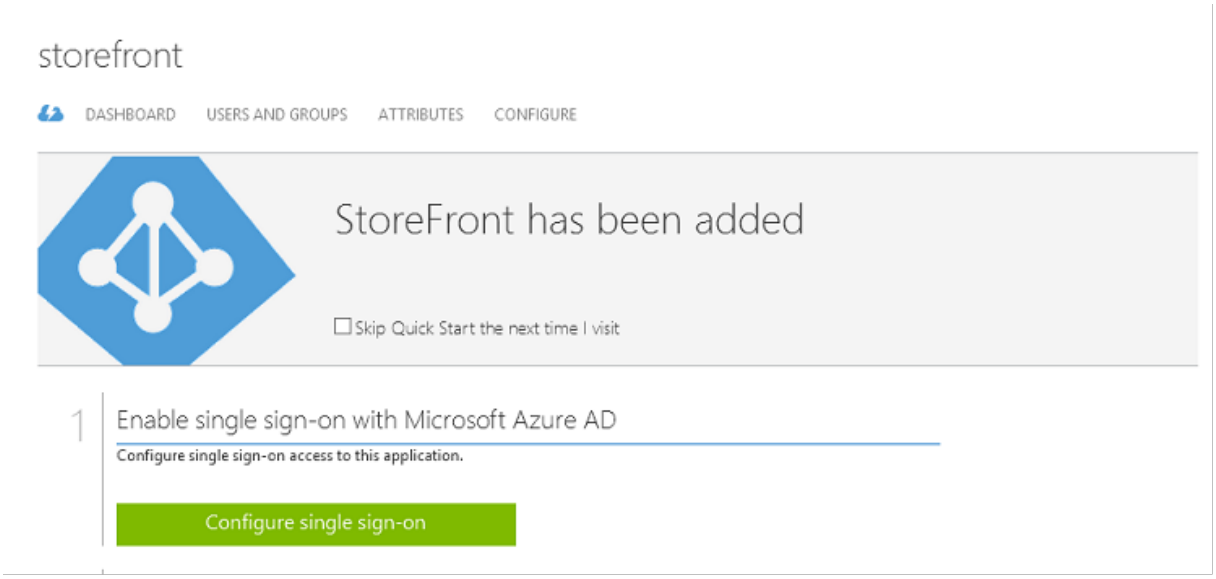
#### Konfigurieren eines Symbols

Erstellen Sie ein 215 x 215 Pixel großes Bild und laden Sie es auf der Seite KONFIGURIEREN hoch, um es als Symbol für die Anwendung zu verwenden.

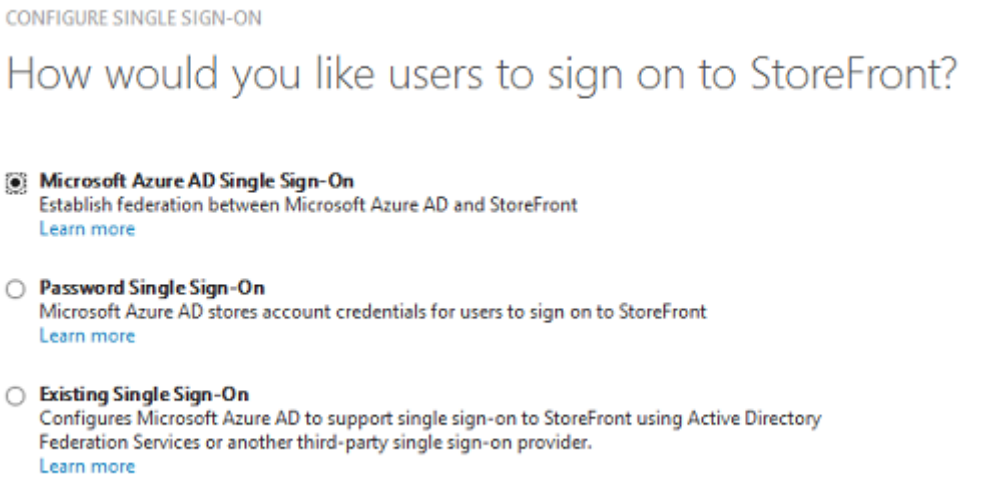

 

### Konfigurieren der SAML-Authentifizierung

Kehren Sie auf die Dashboard-Übersichtsseite zurück und wählen Sie **Single Sign-On konfigurieren**.

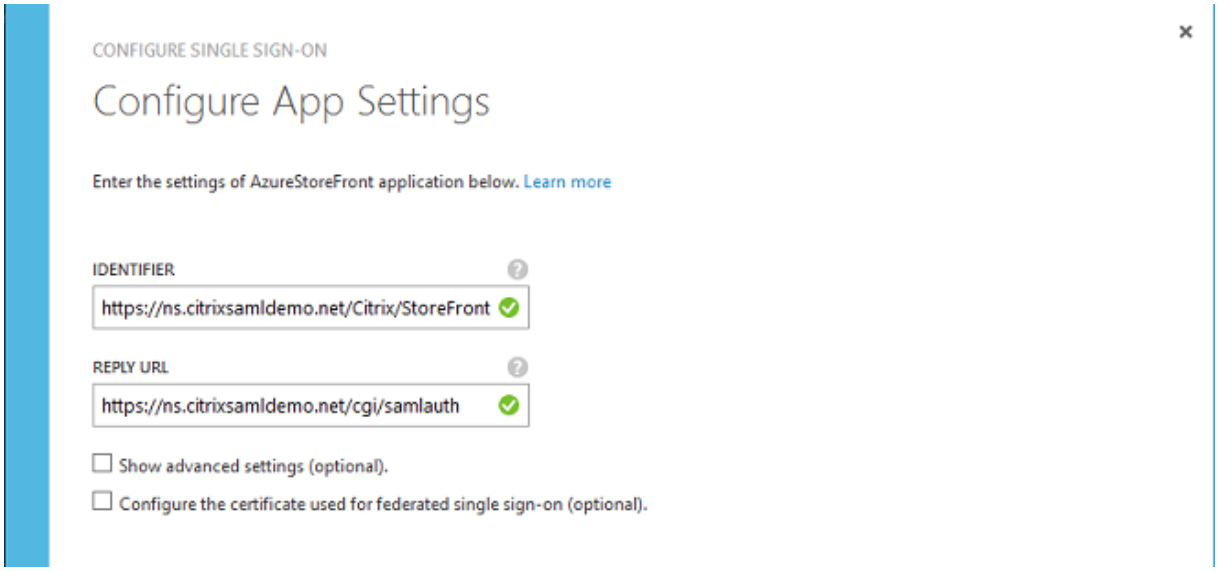



In dieser Bereitstellung wird die SAML 2.0-Authentifizierung verwendet. Dies entspricht **Single Sign-On** in Microsoft Azure AD.

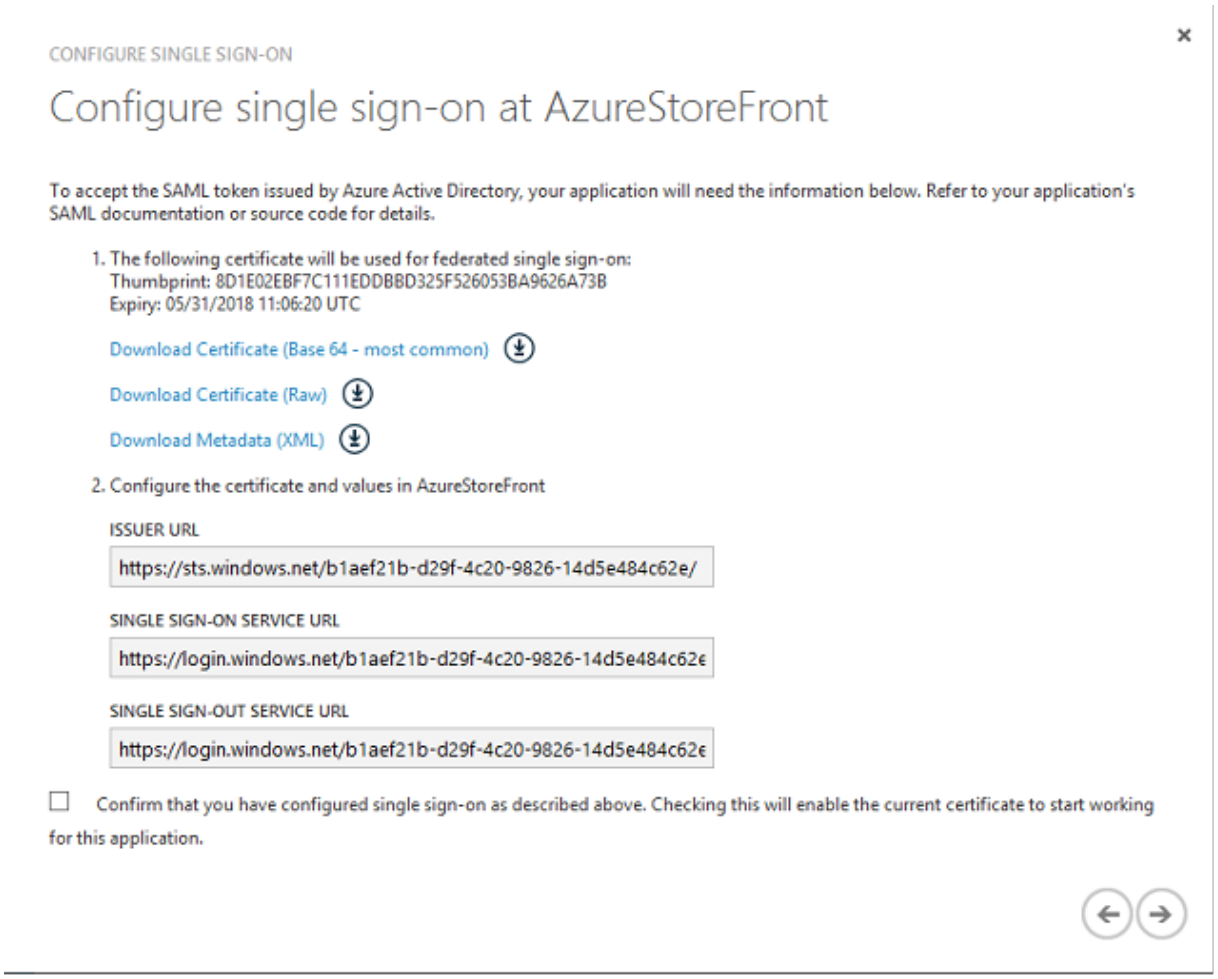



Die **Kennung** darf eine beliebige Zeichenfolge sein (sie muss mit der für Citrix Gateway bereitgestellten Konfiguration übereinstimmen). Im vorliegenden Beispiel ist die **Antwort-URL** auf dem Citrix Gateway-Server */cgi/samlauth*.




Die nächste Seite enthält Informationen zum Konfigurieren von Citrix Gateway als vertrauende Seite für Azure AD.



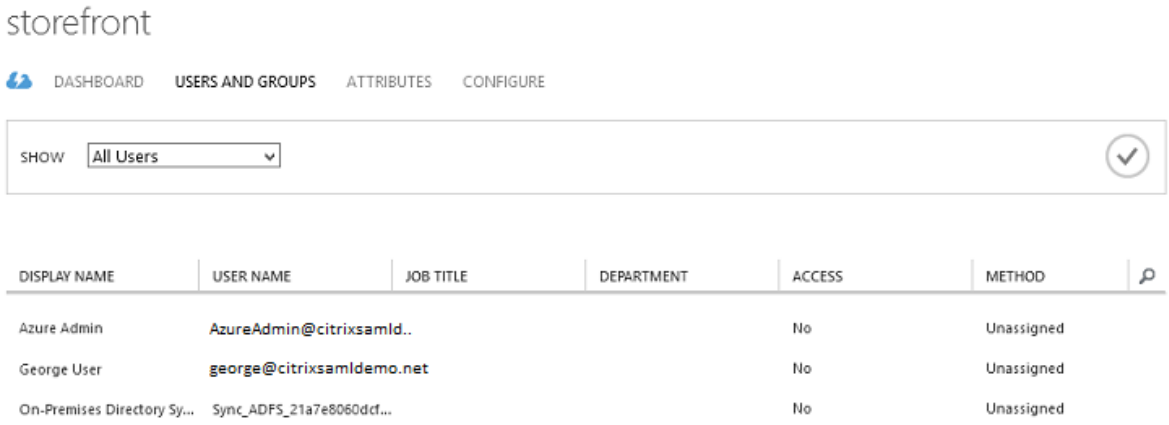

Laden Sie das vertrauenswürdige Base-64-Signaturzertifikat herunter und kopieren Sie die Sign-On-

und die Sign-Out-URL. Diese fügen Sie später bei der Citrix Gateway-Konfiguration ein.

### Zuweisen der Anwendung zu Benutzern

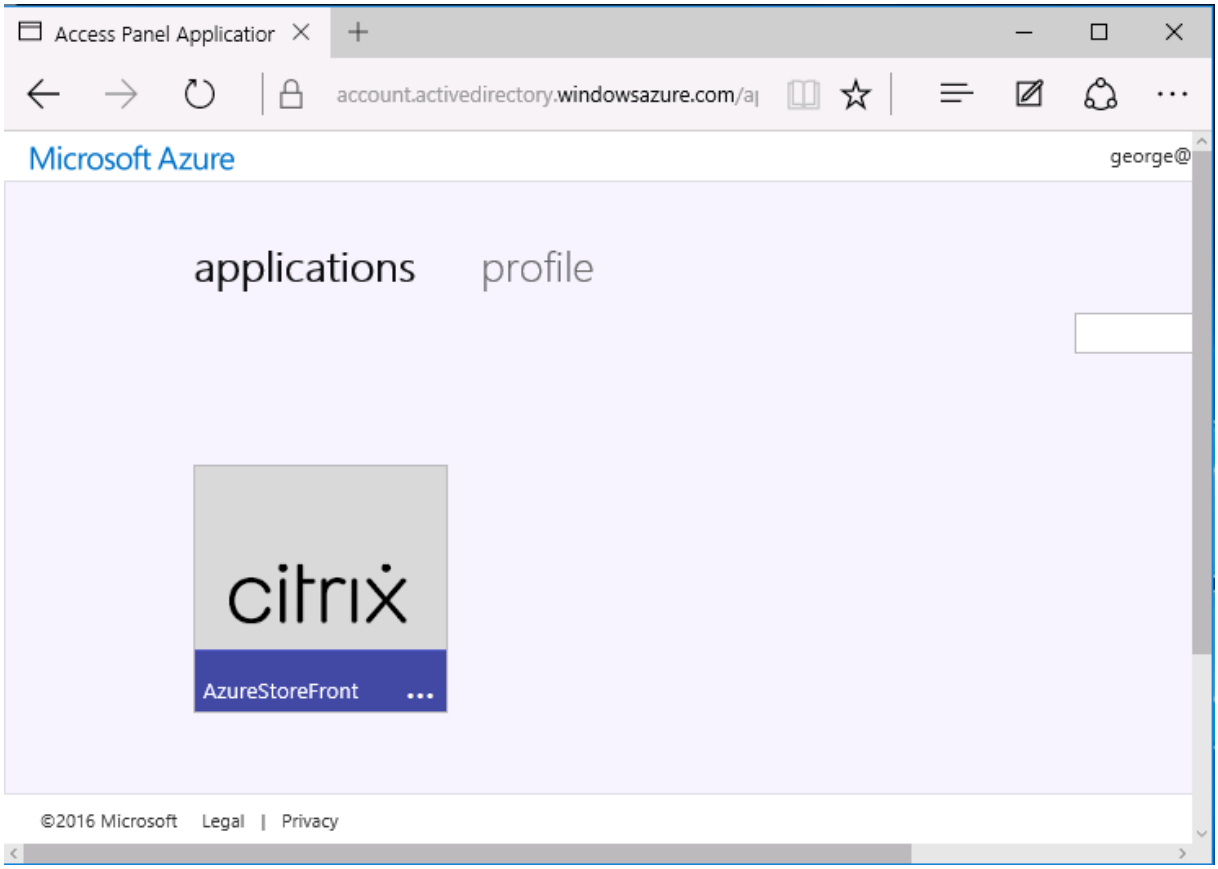
Der letzte Schritt besteht in der Aktivierung der Anwendung, damit sie für die Benutzer auf der Steuerungsseite "myapps.microsoft.com"angezeigt wird. Dafür wird die Seite BENUTZER UND GRUPPEN verwendet. Weisen Sie Zugriff für die über Azure AD Connect synchronisierten Domänenbenutzerkonten zu. Andere Konten können ebenfalls verwendet werden, sie müssen jedoch explizit zugeordnet werden, da sie nicht dem Muster <user>@<domain> entsprechen.




### Seite "MyApps"

Wenn die Anwendung konfiguriert wurde, wird sie in der Azure-Anwendungsliste angezeigt, wenn die Benutzer https://myapps.microsoft.com besuchen.

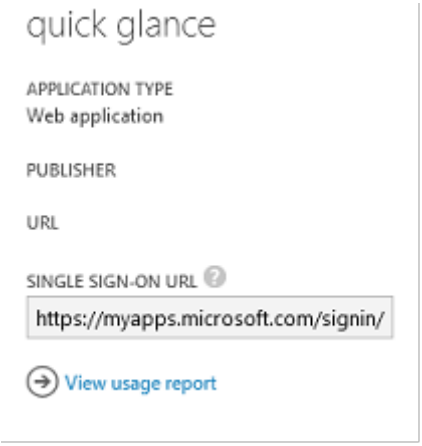



Wenn Windows 10 Azure AD beigetreten ist, unterstützt es Single Sign-On für Azure-Anwendungen. Bei einem Klick auf das Symbol wird der Browser an die zuvor konfigurierte SAML-Webseite cgi/samlauth umgeleitet.

**URL für Single Sign-On**

Kehren Sie zu der Anwendung im Azure AD-Dashboard zurück. Es gibt jetzt eine Single Sign-On-URL für die Anwendung. Diese URL wird zur Erstellung von Browserlinks und Startmenüverknüpfungen verwendet, die die Benutzer direkt an StoreFront umleiten.




Fügen Sie diese URL in einen Webbrowser ein, um sicherzustellen, dass Sie von Azure AD an die zuvor konfigurierte Citrix Gateway-Webseite cgi/samlauth umgeleitet werden. Dies funktioniert nur dann, wenn ein Benutzer zugewiesen wurde, zudem ist Single Sign-On nur bei Anmeldungssitzungen möglich, wenn Windows 10 Azure AD beigetreten ist. (Andere Benutzer werden aufgefordert, ihre Azure AD-Anmeldeinformationen einzugeben.)

## Installieren und Konfigurieren von Citrix Gateway

Für den Remote-Zugriff auf die Bereitstellung wird in diesem Beispiel eine separate VM mit NetScaler (jetzt Citrix Gateway) verwendet. Diese kann im Azure-Store erworben werden. In diesem Beispiel wird die "Bring your own License"-Lizenzversion für NetScaler 11.0 verwendet.

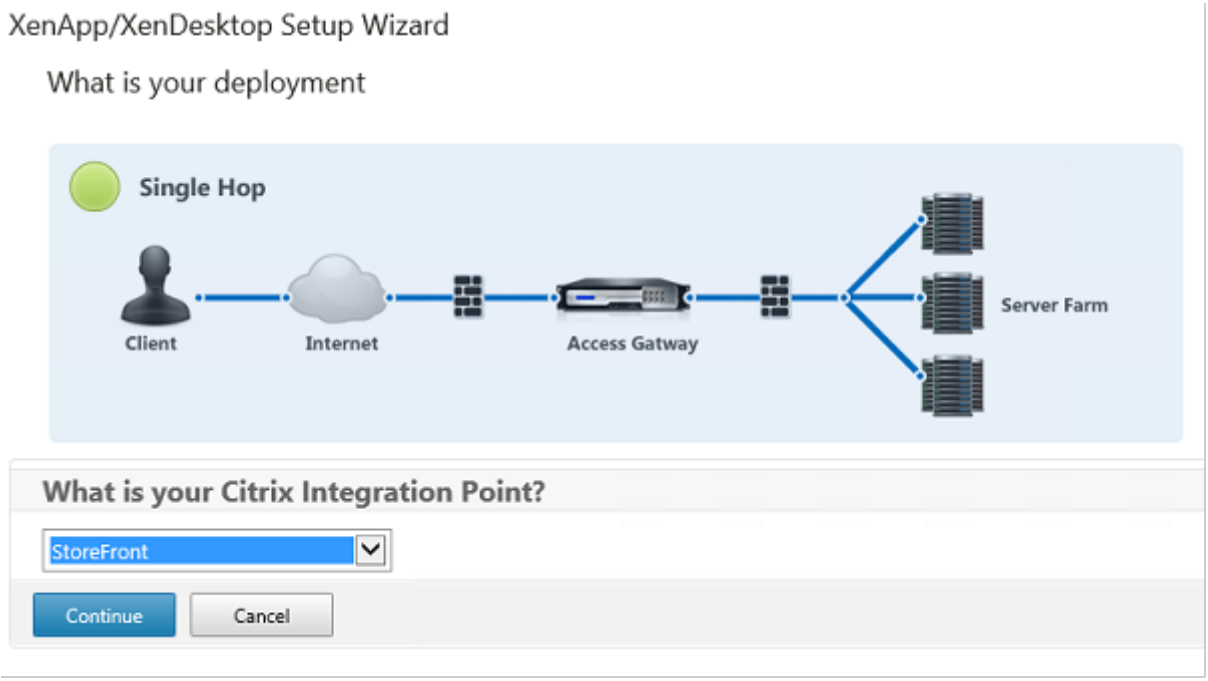
Melden Sie sich bei der NetScaler-VM an, indem Sie im Webbrowser die interne IP-Adresse und die bei der Benutzerauthentifizierung angegebenen Anmeldeinformationen eingeben. Sie müssen das Kennwort des nsroot-Benutzers in einer Azure AD-VM ändern.

Fügen Sie Lizenzen hinzu (führen Sie nach dem Hinzufügen jeder Lizenz einen **Neustart** durch) und verweisen Sie die DNS-Auflösung an den Microsoft-Domänencontroller.

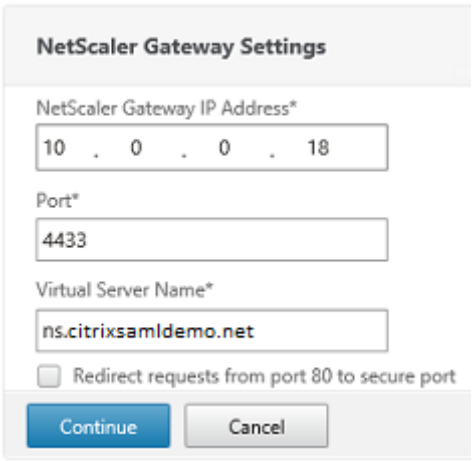
### Ausführen des Citrix Virtual Apps and Desktops-Setupassistenten

In diesem Beispiel wird zunächst eine einfache StoreFront-Integration ohne SAML konfiguriert. Wenn diese Bereitstellung betriebsbereit ist, wird eine SAML-Anmelderichtlinie hinzugefügt.

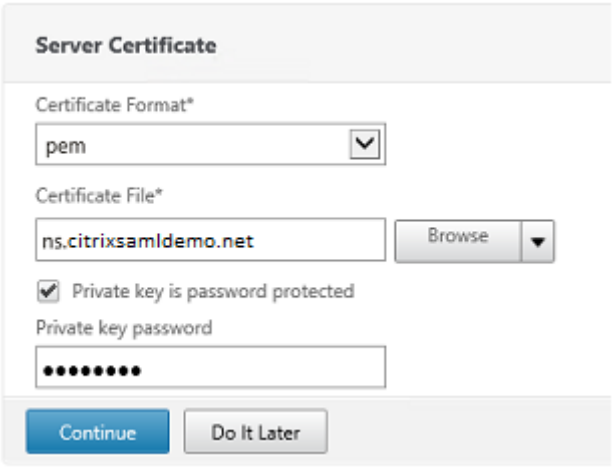



Wählen Sie die StoreFront-Standardeinstellungen für Citrix Gateway. Zur Verwendung in Microsoft Azure wird in diesem Beispiel Port 4433 anstelle von Port 443 konfiguriert. Alternativ können Sie eine Portweiterleitung einrichten oder die Zuweisung der Verwaltungswebsite von Citrix Gateway ändern.



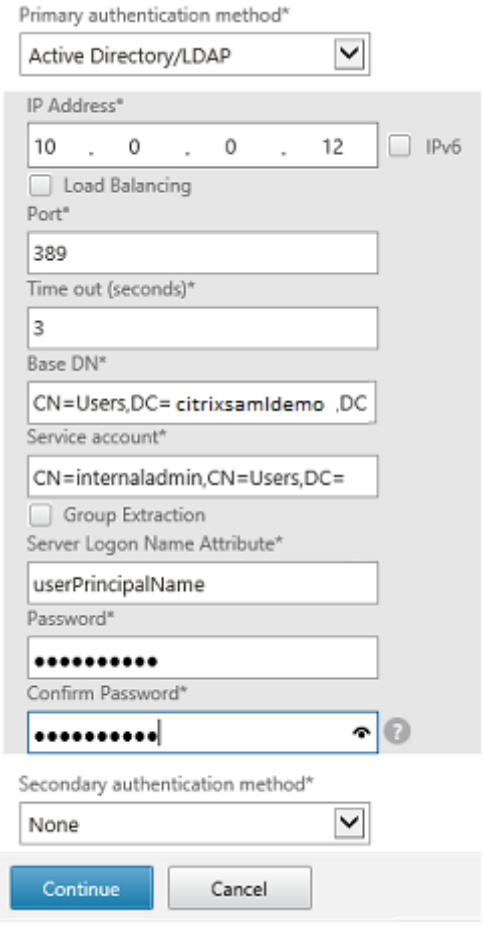

Der Einfachheit halber wird in diesem Beispiel ein in einer Datei gespeichertes, vorhandenes Serverzertifikat mit privatem Schlüssel hochgeladen.




### Konfigurieren des Domänencontrollers für die AD-Kontoverwaltung

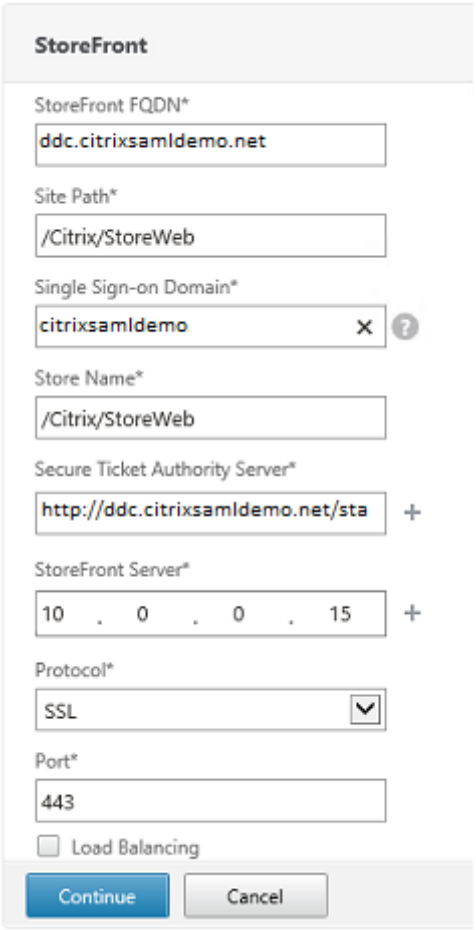
Der Domänencontroller wird zur Kontoauflösung verwendet. Fügen Sie daher seine IP-Adresse in die primäre Authentifizierungsmethode ein. Beachten Sie die in den einzelnen Feldern im Dialogfeld erforderlichen Formate.



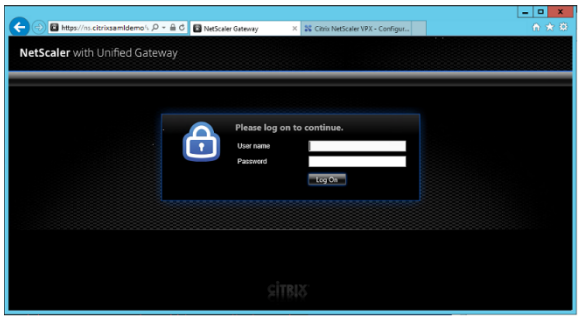
### Konfigurieren der StoreFront-Adresse

In diesem Beispiel wurde StoreFront für HTTPS konfiguriert. Wählen Sie daher die SSL-Protokolloptionen.




### Überprüfen der Citrix Gateway-Bereitstellung

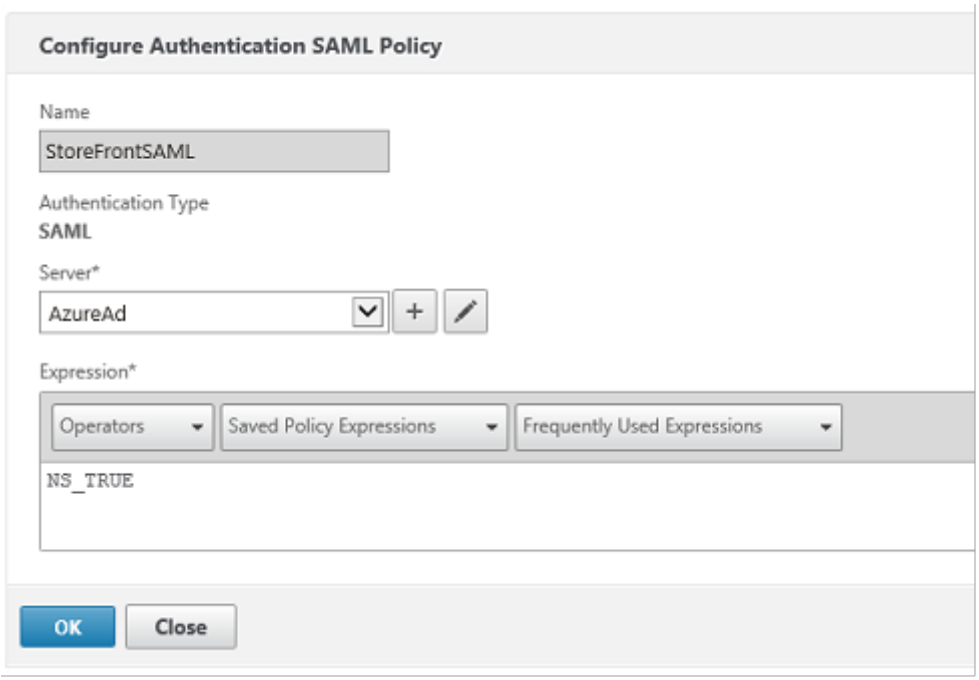
Stellen Sie eine Verbindung mit Citrix Gateway her und überprüfen Sie, ob Authentifizierung und Start mit den Anmeldeinformationen funktionieren.



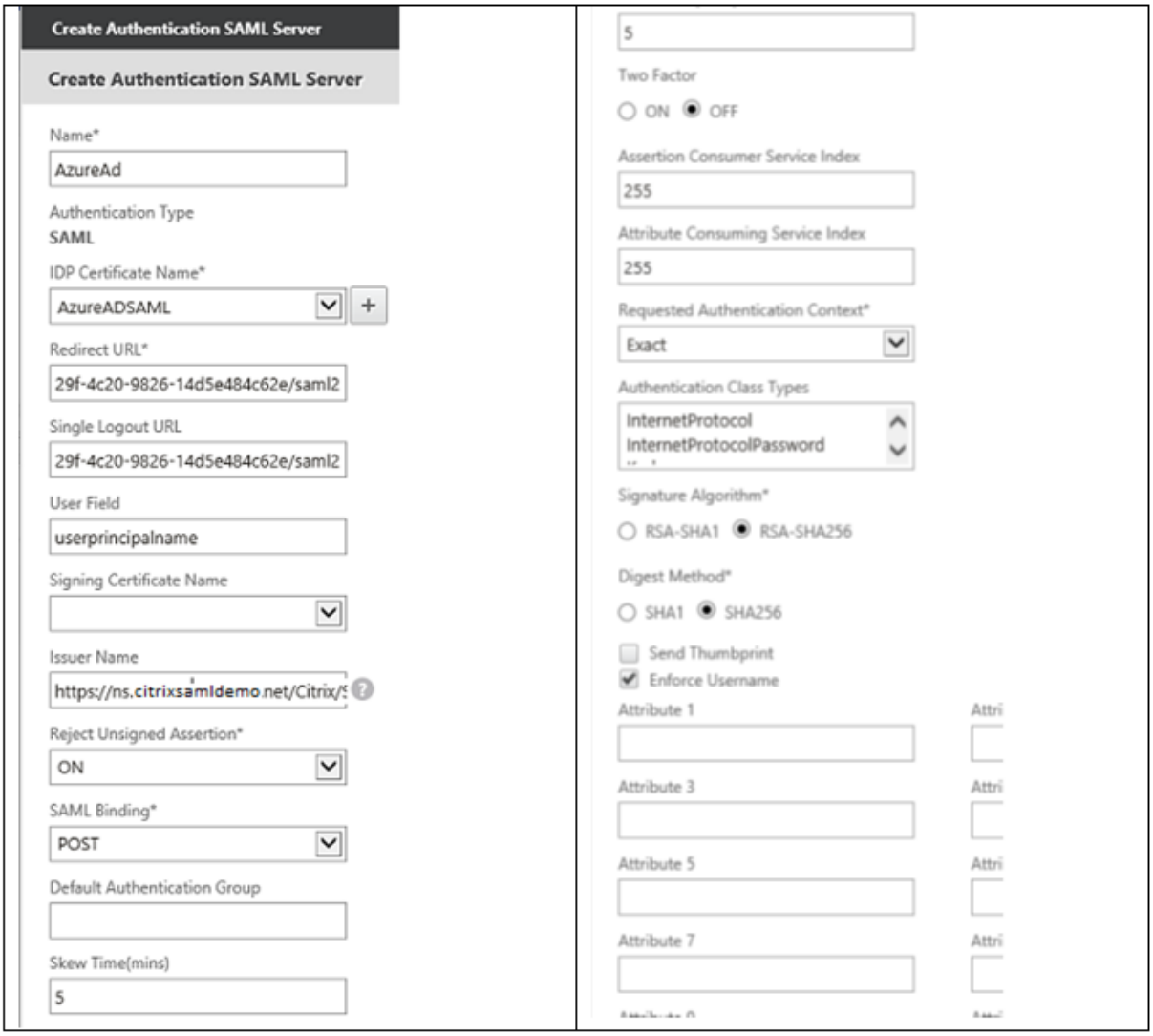
### Aktivieren der SAML-Authentifizierung in Citrix Gateway

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




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

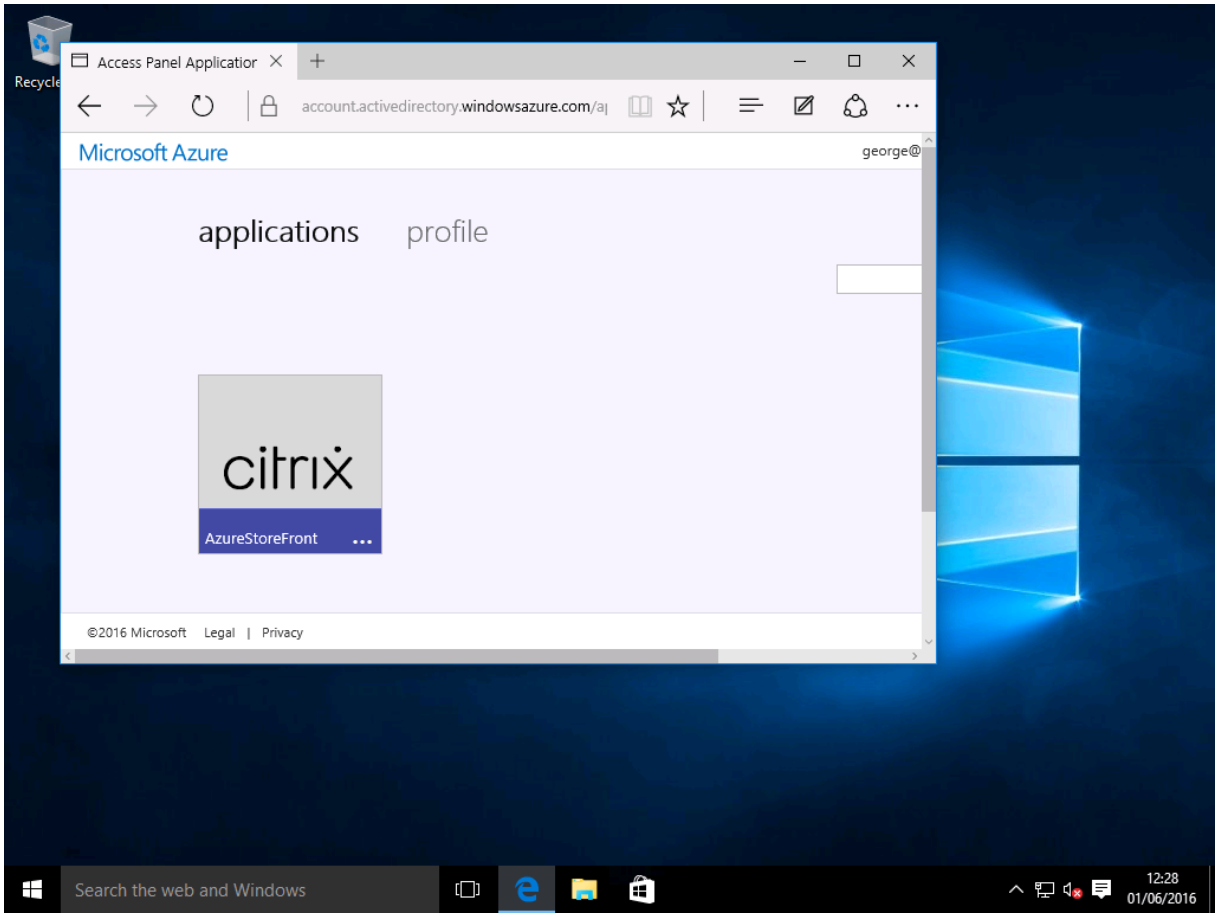



## Überprüfen des Gesamtsystems

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

Im Webbrowser müssten nun die Azure AD-Anwendungen für den Benutzer angezeigt werden.




Vergewissern Sie sich, dass bei einem Klick auf das Symbol eine Umleitung an einen authentifizierten StoreFront-Server erfolgt.

Prüfen Sie außerdem, ob bei direkten Verbindungen mit der Single Sign-On-URL und mit der Citrix Gateway-Site eine Umleitung an Microsoft Azure und zurück erfolgt.

Vergewissern Sie sich zuletzt, dass dieselben URLs auch bei nicht Azure AD beigetretenen Maschinen funktionieren (allerdings ist hier bei der ersten Verbindung ein Sign-On bei Azure AD erforderlich).

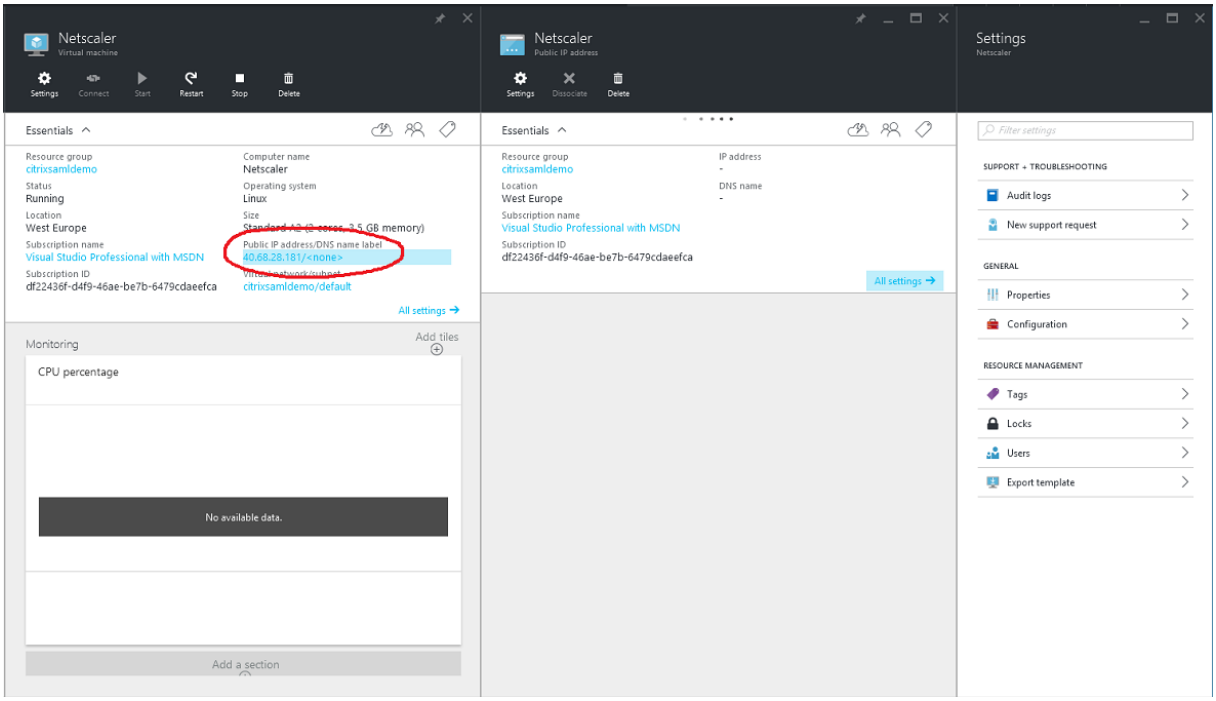
## Anhang

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

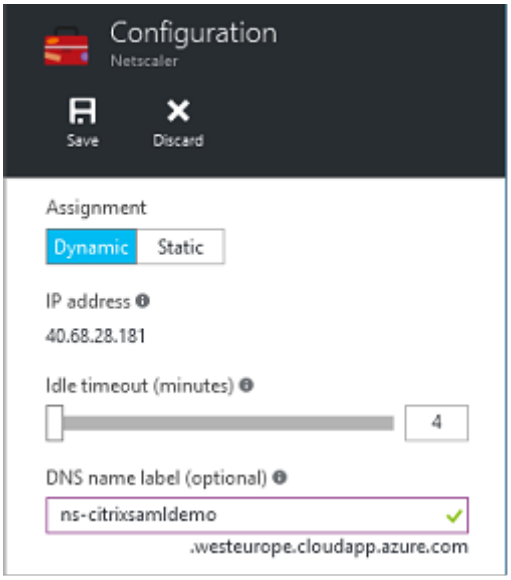
### Angeben einer öffentlichen IP-Adresse und einer DNS-Adresse

Azure weist allen VMs eine IP-Adresse im internen Subnetz zu (in diesem Beispiel 10.*.*.*). Standardmäßig wird auch eine öffentliche IP-Adresse angegeben, auf die durch eine dynamisch aktualisierte DNS-Bezeichnung verwiesen werden kann.




Wählen Sie **Configuration** für **Public IP address/DNS name label**. Wählen Sie eine öffentliche DNS-Adresse für die VM. Diese kann für CNAME-Verweise in anderen DNS-Zonendateien verwendet werden, damit alle DNS-Einträge richtig auf die VM verweisen, selbst wenn die IP-Adresse neu zugewiesen wird.



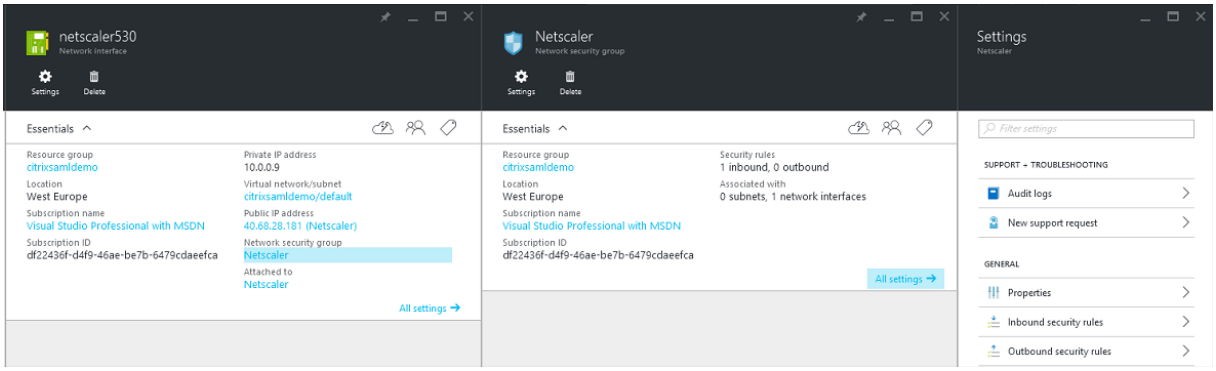

### Einrichten von Firewallregeln (Sicherheitsgruppe)

Auf jede VM in einer Cloud werden automatisch einige Firewallregeln angewendet, die als Sicherheitsgruppe bezeichnet werden. Die Sicherheitsgruppe steuert den Datenverkehr von der öffentlichen an

die private IP-Adresse. Standardmäßig lässt Azure die RDP-Weiterleitung an alle VMs zu. Der Citrix Gateway- und der AD FS-Server müssen ebenfalls TLS-Datenverkehr (443) weiterleiten.

Öffnen Sie **Network Interfaces** für eine VM und klicken Sie dann auf **Network Security Group**. Konfigurieren Sie **Inbound security rules** zum Zulassen des erforderlichen Datenverkehrs im Netzwerk.




## Verwandte Informationen

- Installation und Konfiguration ist die primäre Referenz für die Installation und Konfiguration des FAS.
- Der Artikel Bereitstellungsarchitekturen enthält eine Übersicht über die gebräuchlichen FAS-Architekturen.
- Der Artikel Erweiterte Konfiguration enthält Links zu weiteren Anleitungen.