Federated Authentication Service 2012

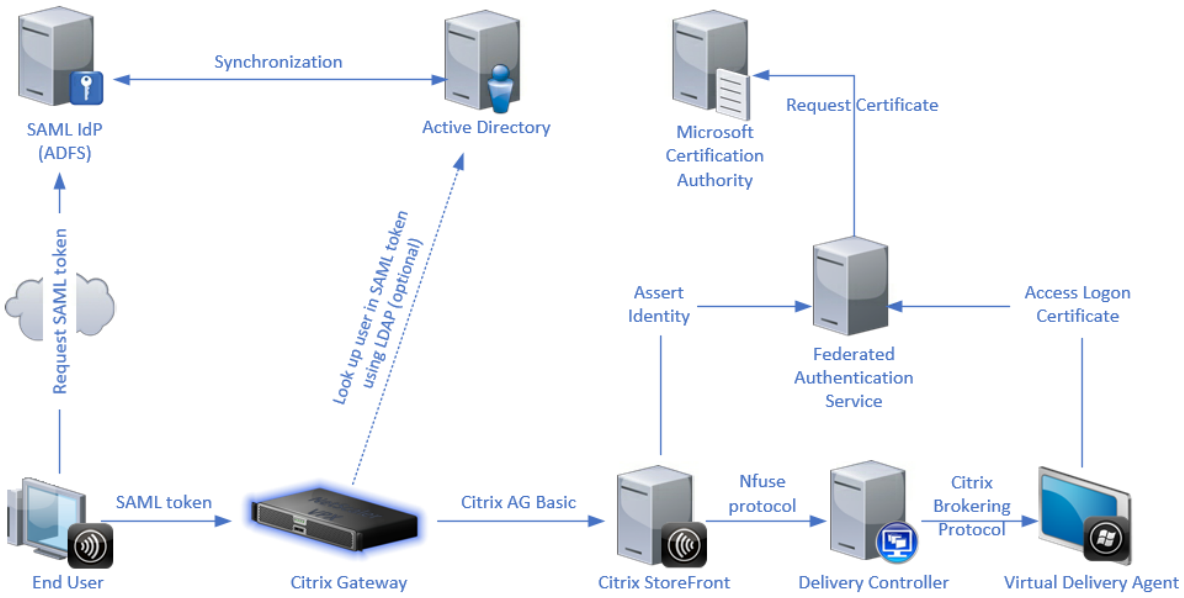
Contents

Federated Authentication Service 2012

December 11, 2020

Federated Authentication Service (FAS) is a privileged component designed to integrate with Active Directory Certificate Services. It dynamically issues certificates for users, allowing them to log on to an Active Directory environment as if they had a smart card. This allows StoreFront to use a broader range of authentication options, such as SAML (Security Assertion Markup Language) assertions. SAML is commonly used as an alternative to traditional Windows user accounts on the Internet.

The following diagram shows FAS integrating with a Microsoft Certification Authority and providing support services to StoreFront and Citrix Virtual Apps and Desktops Virtual Delivery Agents (VDAs).



Trusted StoreFront servers contact FAS as users request access to the Citrix environment. FAS grants a ticket that allows a single Citrix Virtual Apps or Citrix Virtual Desktops session to authenticate with a certificate for that session. When a VDA needs to authenticate a user, it connects to FAS and redeems the ticket. Only FAS has access to the user certificate's private key; the VDA must send each signing and decryption operation that it needs to perform with the certificate to FAS.

Federated Authentication Service 2012 is the latest Current Release version of FAS. This documentation reflects features and configurations in this latest release.

Earlier releases

For documentation on previous FAS releases, see:

- Federated Authentication Service 2009

- Federated Authentication Service 2006
- Federated Authentication Service 2003
- Federated Authentication Service 1912
- Federated Authentication Service 1909
- Citrix Virtual Apps and Desktops 7 1906
- Citrix Virtual Apps and Desktops 7 1903
- Earlier XenApp and XenDesktop Current Release versions
- XenApp and XenDesktop 7.15 Long Term Service Release

The product lifecycle strategy for Current Releases (CR) and Long Term Service Releases (LTSR) is described in Lifecycle Milestones.

References

- Active Directory Certificate Services Overview https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/hh831740(v=ws.11)
- Configuring Windows for Certificate Logon http://support.citrix.com/article/CTX206156

Federated Authentication Service 2012

November 18, 2020

There are no new features in Federated Authentication Service 2012. For information about bug fixes, see Fixed issues.

Fixed issues

December 11, 2020

This article describes fixed issues in Federated Authentication Service 2012.

- An interaction between the Microsoft Fast Reconnect feature on Windows Server 2019 and FAS can cause a user's account to be locked out during launch of, or reconnect to, a published Citrix Virtual Apps and Desktops resource. This issue is fixed in this release. Note: the fix is in the software installed on the Version 2012 of the Windows VDA. [AUTH-555]

- The FAS disconnect-on-lock feature, which allows the VDA session to be automatically disconnected if the user locks the session's screen, does not work in Citrix Virtual Apps and Desktops versions 2009, 2006, 2003. This issue is fixed in Citrix Virtual Apps and Desktops 2012. Note: the fix is in the software installed on the Version 2012 of the Windows VDA. [AUTH-787]

Known issues

November 18, 2020

There are no known issue in Federated Authentication Service 2012.

The following warning applies to any workaround that suggests changing a registry entry:

> **Warning:**
>
> Editing the registry incorrectly can cause serious problems that might require you to reinstall your operating system. Citrix cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk. Be sure to back up the registry before you edit it.

Third party notices

December 18, 2019

This release of Federated Authentication Service may include third-party software licensed under the terms defined in the following documents:

- Citrix Virtual Apps and Desktops Third Party Notices (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)

System requirements

September 8, 2020

Federated Authentication Service (FAS) is supported on all currently supported Windows Server versions, see Citrix Virtual Apps or Citrix Virtual Desktops system requirements.

- Citrix recommends installing FAS on a server that does not contain other Citrix components.
- The Windows Server should be secured. It will have access to a registration authority certificate and private key that allows it to automatically issue certificates for domain users, and it will have access to those user certificates and private keys.
- The FAS PowerShell cmdlets require Windows PowerShell 64-bit installed on the FAS server.
- A Microsoft Enterprise Certification Authority is required to issue user certificates.

In the Citrix Virtual Apps or Citrix Virtual Desktops Site:

- Delivery Controllers, Virtual Delivery Agents (VDAs), and StoreFront server must all be currently supported versions, see Citrix Virtual Apps or Citrix Virtual Desktops system requirements.

  > **Note:**
  >
  > FAS is not supported on XenApp and XenDesktop 7.6 Long Term Service Release (LTSR).

- Before creating the Machine Catalog, the Federated Authentication Service Group Policy configuration must be applied correctly to the VDAs. See the Configure Group Policy section for details.

When planning your deployment of this service, review the Security considerations section.

Install and configure

February 23, 2021

Install and setup sequence

1. Install the Federated Authentication Service (FAS)
2. Enable the FAS plug-in on StoreFront stores
3. Configure the Delivery Controller
4. Configure Group Policy
5. Use the FAS administration console to:
   a) Deploy certificate templates
   b) Set up certificate authorities
   c) Authorize FAS to use your certificate authorities
   d) Configure rules
   e) Connect FAS to Citrix Cloud (optional)

Install the Federated Authentication Service

For security, Citrix recommends that Federated Authentication Service (FAS) is installed on a dedicated server that is secured in a similar way to a domain controller or certificate authority. FAS can be installed from either:

- the Citrix Virtual Apps and Desktops installer (from the **Federated Authentication Service** button on the autorun splash screen when the ISO is inserted), or
- the stand-alone FAS installer file (available as an MSI file on Citrix Downloads).

These install the following components:

- Federated Authentication Service
- PowerShell snap-in cmdlets for advanced FAS configuration
- FAS administration console
- FAS Group Policy templates (CitrixFederatedAuthenticationService.admx/adml)
- Certificate template files
- Performance counters and event logs

Upgrading FAS

You can upgrade FAS to a newer version using an in-place upgrade. Before upgrading, consider the following:

- All FAS server settings are preserved when you perform an in-place upgrade.
- Ensure that the FAS administration console is closed before you upgrade FAS.
- Ensure that at least one FAS server is available at all times. If no server is reachable by a Federation Authentication Service-enabled StoreFront server, users cannot log on or start applications.

To start an upgrade, install FAS from the Citrix Virtual Apps and Desktops installer or from the stand-alone FAS installer file.

Enable the FAS plug-in on StoreFront stores

> **Note:**
>
> This step is not needed if you are using FAS only with Citrix Cloud.

To enable FAS integration on a StoreFront Store, run the following PowerShell cmdlets as an Administrator account. If the store has a different name, modify `$StoreVirtualPath`.

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

To stop using FAS, use the following PowerShell script:

```
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 ""
```

Configure the Delivery Controller

> **Note:**
>
> This step is not needed if you are using FAS only with Citrix Cloud.

To use FAS, configure the Citrix Virtual Apps or Citrix Virtual Desktops Delivery Controller to trust the StoreFront servers that can connect to it: run the **Set-BrokerSite -TrustRequestsSentToTheXmlServicePort $true** PowerShell cmdlet. This only needs to be done once per site, regardless of the number of Delivery Controllers in the site.

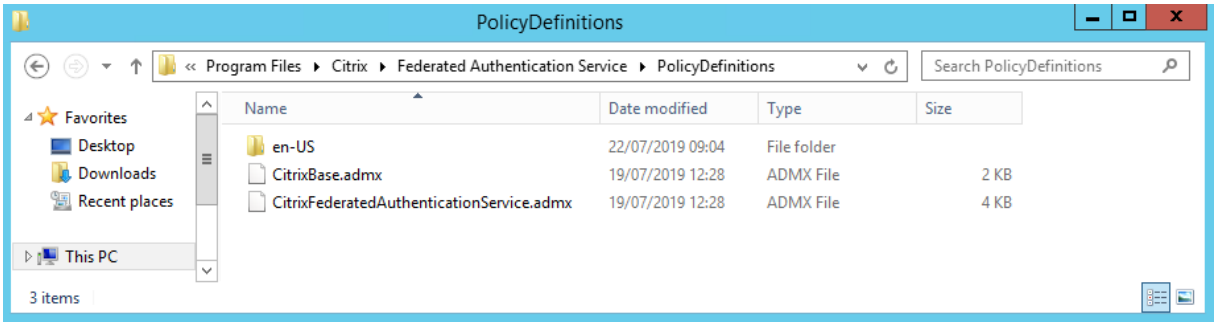
Configure Group Policy

After you install FAS, you must specify the fully qualified domain names (FQDNs) of the FAS servers in Group Policy using the Group Policy templates provided in the installation.

> **Important:**
>
> Ensure that the StoreFront servers requesting tickets and the Virtual Delivery Agents (VDAs) redeeming tickets have identical configuration of FQDNs, including the automatic server numbering applied by the Group Policy object.

For simplicity, the following examples configure a single policy at the domain level that applies to all machines; however, that is not required. FAS will function as long as the StoreFront servers, VDAs, and the machine running the FAS administration console see the same list of FQDNs. See Step 6.

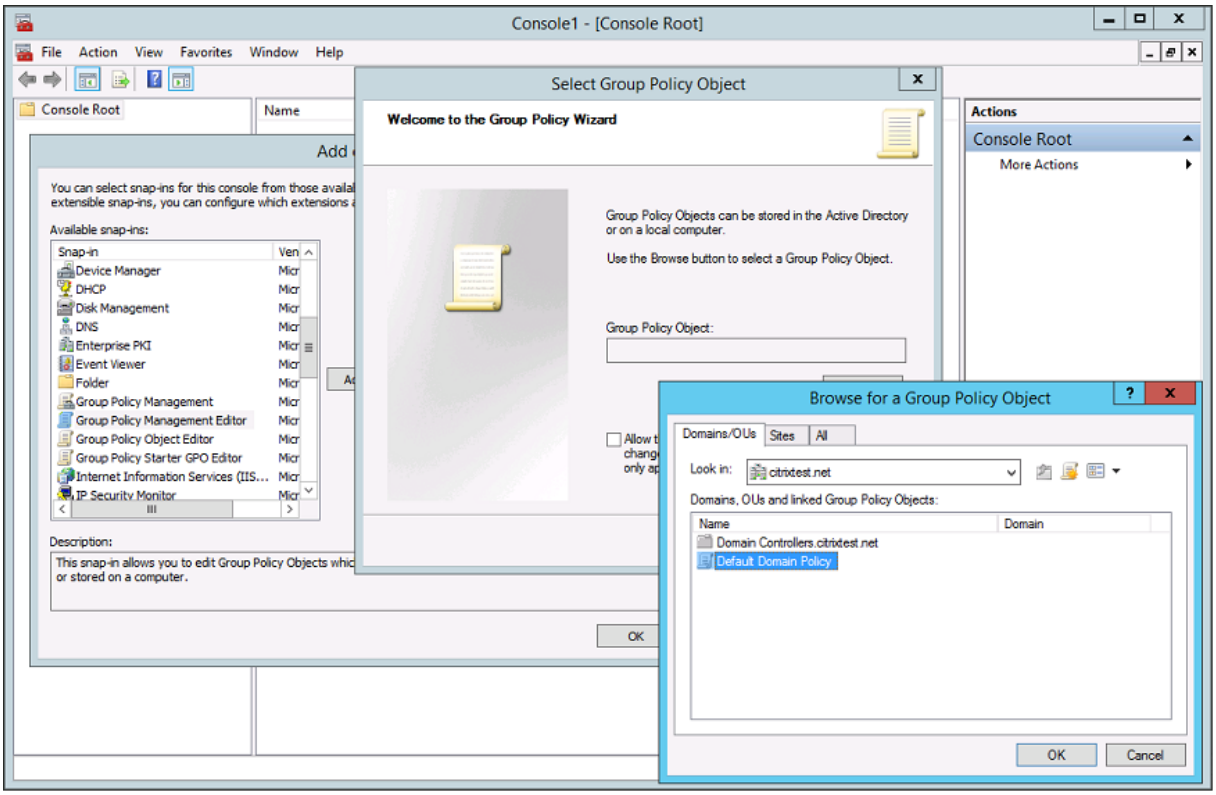
Step 1. On the server where you installed FAS, locate the C:\Program Files\Citrix\Federated Authentication Service\PolicyDefinitions\CitrixFederatedAuthenticationService.admx and CitrixBase.admx files, and the en-US folder.



Step 2. Copy these to your domain controllers and place them in the C:\Windows\PolicyDefinitions and en-US subfolder.

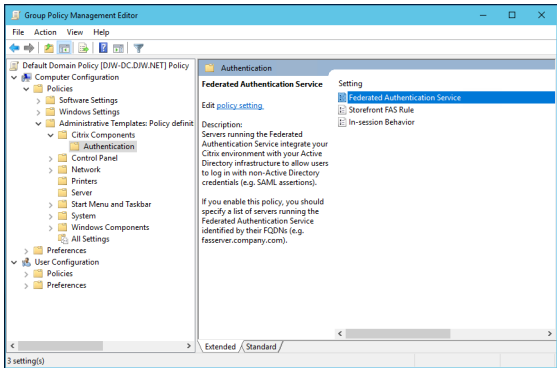
Step 3. Run the Microsoft Management Console (mmc.exe from the command line). From the menu bar, select **File > Add/Remove Snap-in**. Add the **Group Policy Management Editor**.

When prompted for a Group Policy Object, select **Browse** and then select **Default Domain Policy**. Alternatively, you can create and select an appropriate policy object for your environment, using the tools of your choice. The policy must be applied to all machines running affected Citrix software (VDAs, StoreFront servers, administration tools).



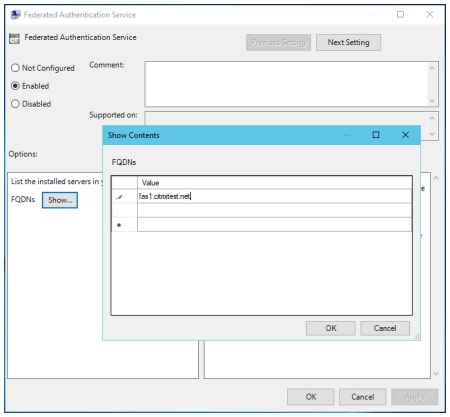
Step 4. Navigate to the *Federated Authentication Service* policy located in Computer Configura-

tion/Policies/Administrative Templates/Citrix Components/Authentication.



> **Note:**
>
> The Federated Authentication Service policy setting is only available on the domain GPO when you add the CitrixBase.admx/CitrixBase.adml template file to the PolicyDefinitions folder. After Step 3, the Federated Authentication Service policy setting is listed in the Administrative Templates > Citrix Components > Authentication folder.

Step 5. Open the Federated Authentication Service policy and select **Enabled**. This allows you to select the **Show** button, where you configure the FQDNs of your FAS servers.



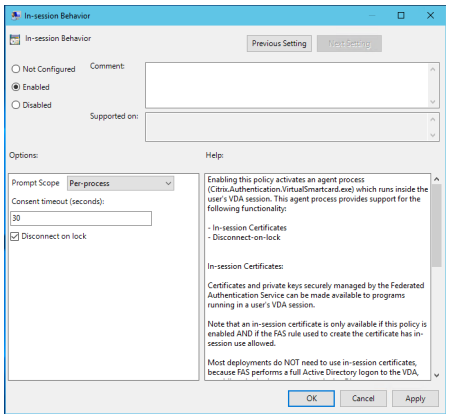
Step 6. Enter the FQDNs of the FAS servers.

> **Important:**
>
> If you enter multiple FQDNs, the order of the list must be consistent as seen by VDAs, StoreFront servers (if present), and FAS servers. See Group Policy settings.

Step 7. Click **OK** to exit the Group Policy wizard and apply the group policy changes. You may need to restart your machines (or run **gpupdate /force** from the command line) for the change to take effect.

In-session Behavior

This policy activates an agent process in the user's VDA session which supports in-session certificates, consent, and disconnect on lock. In-session certificates are only available if this policy is enabled *and* if the FAS rule used to create the certificate has in-session use allowed, see Configure rules.



Enable enables this policy and allows a FAS agent process to run in the user's VDA session.

Disable disables the policy and stops the FAS agent process from running.

Prompt Scope

If this policy is enabled, **Prompt Scope** controls how users are prompted for consent to allow an application to use an in-session certificate. There are three options:

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

Consent Timeout

If this policy is enabled, **Consent Timeout** controls how long (in seconds) the consent lasts. For example, with 300 seconds users see a prompt every five minutes. A value of zero prompts users for every private key operation.

Disconnect on lock

If this policy is enabled the user's session is automatically disconnected when they lock the screen. This functionality provides similar behaviour to the "disconnect on smart card removal" policy, and is useful for situations where users do not have Active Directory logon credentials.

> **Note:**
>
> The disconnect on lock policy applies to all sessions on the VDA.

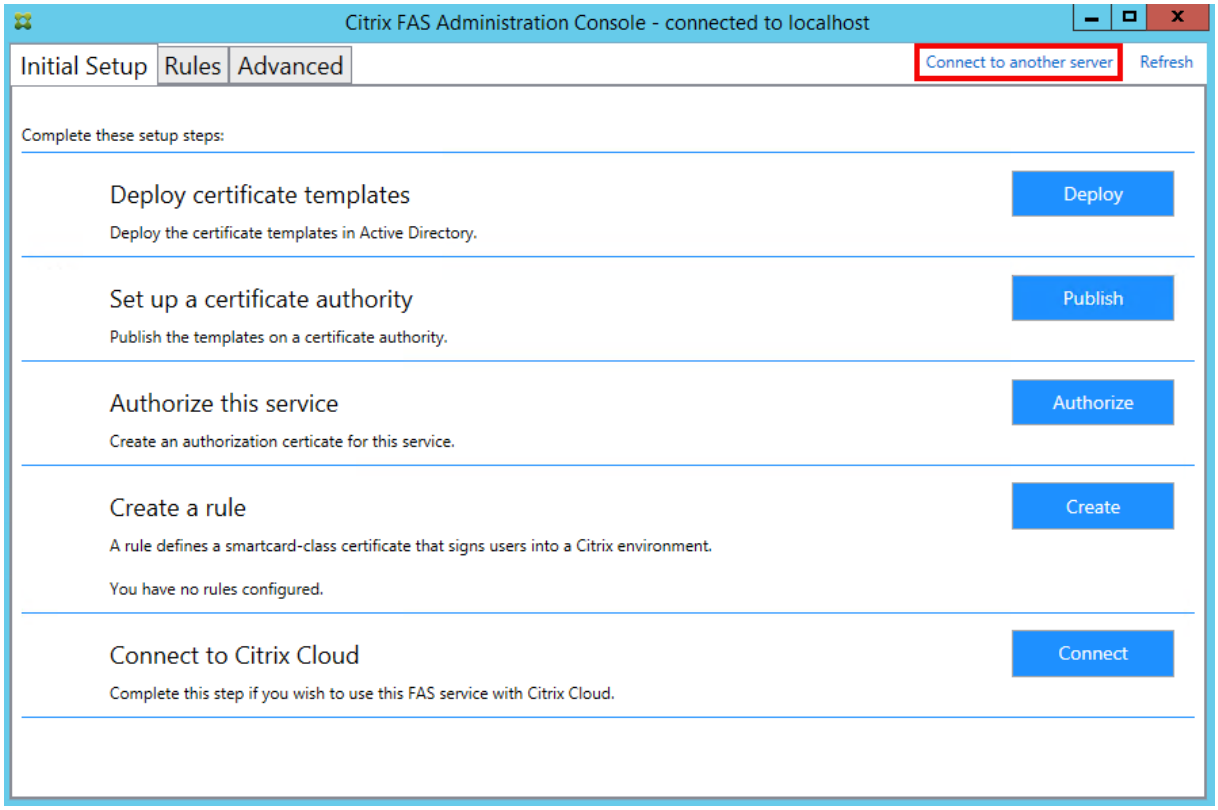
Using the Federated Authentication Service administration console

> **Note:**
>
> Although the FAS administration console is suitable for most deployments, the PowerShell interface offers more advanced options. For information on FAS PowerShell cmdlets, see PowerShell cmdlets.

The FAS administration console is installed as part of FAS. An icon (Citrix Federated Authentication Service) is placed in the Start Menu.

The first time the administration console is used, it guides you through a process that deploys certificate templates, sets up the certificate authority, and authorizes FAS to use the certificate authority. Some of the steps can alternatively be completed manually using OS configuration tools.

The FAS administration console connects to the local FAS service by default. If needed, you can connect to a remote service using **Connect to another server** in the top right of the console.

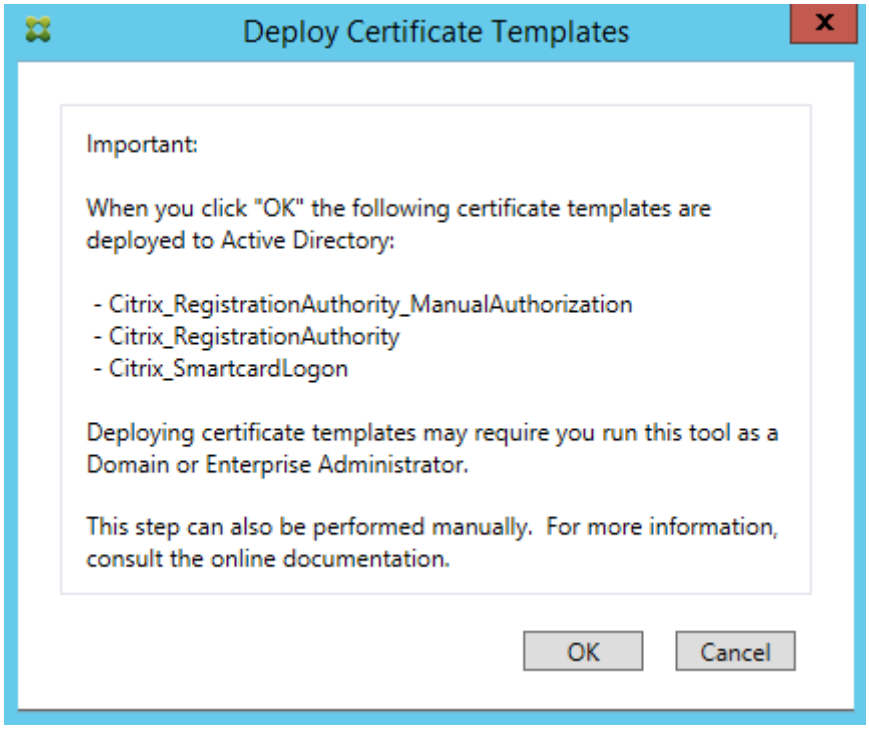


Deploy certificate templates

To avoid interoperability issues with other software, FAS provides three Citrix certificate templates for its own use.

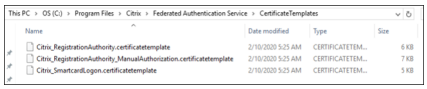
- Citrix_RegistrationAuthority_ManualAuthorization
- Citrix_RegistrationAuthority
- Citrix_SmartcardLogon

These templates must be registered with Active Directory. Click the **Deploy** button then click **OK**.



The configuration of the templates can be found in the XML files with extension .certificatetemplate that are installed with FAS in:

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



If you do not have permission to install these template files, give them to your Active Directory Administrator.

To manually install the templates, you can run the following PowerShell commands from the folder containing the templates:

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



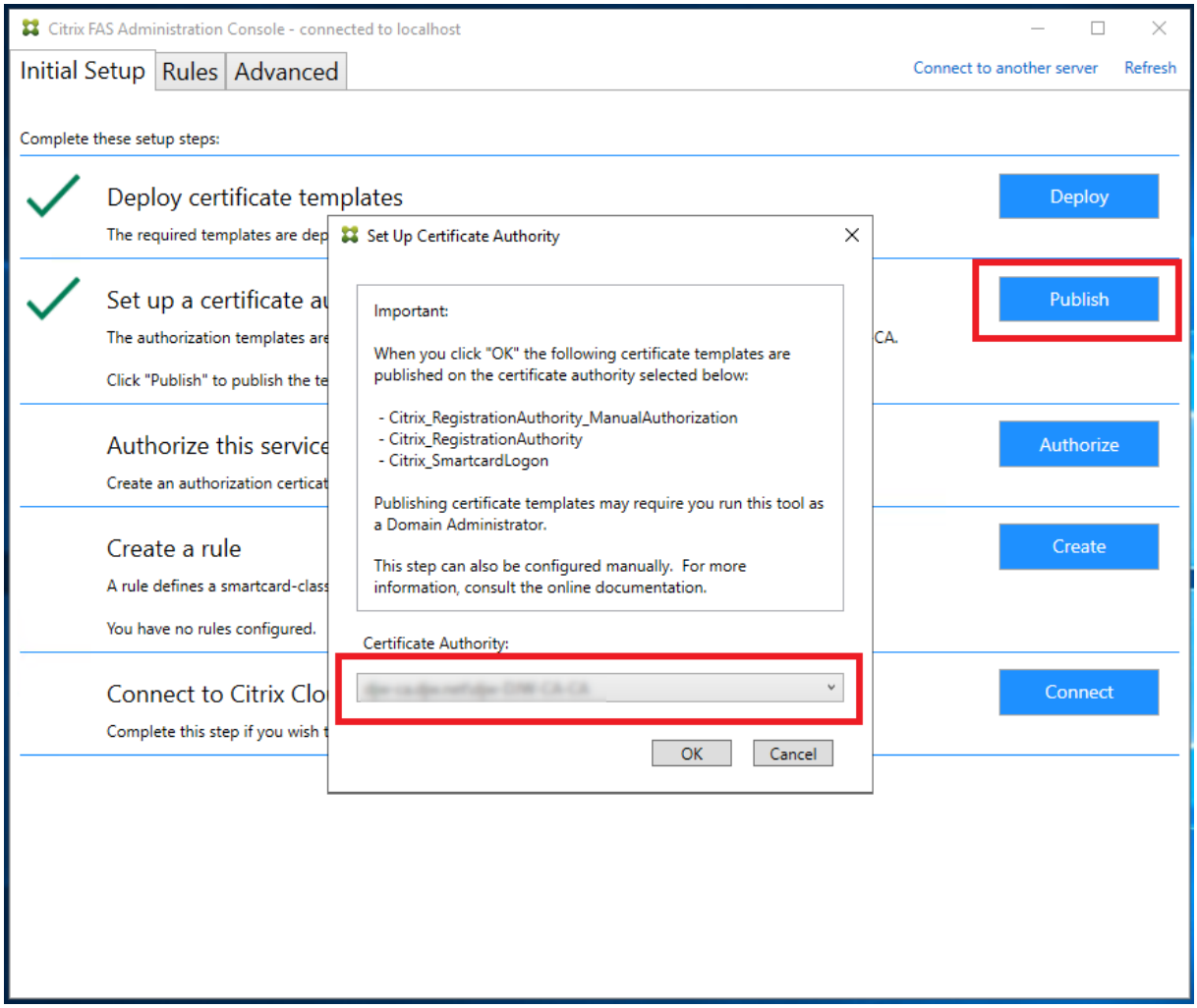
```
    $CertEnrol = New-Object -ComObject X509Enrollment.
        CX509EnrollmentPolicyWebService
    $CertEnrol.InitializeImport($template)
    $comtemplate = $CertEnrol.GetTemplates().ItemByIndex(0)
    $writabletemplate = New-Object -ComObject X509Enrollment.
        CX509CertificateTemplateADWritable
    $writabletemplate.Initialize($comtemplate)
    $writabletemplate.Commit(1, $NULL)
```

Set up Active Directory Certificate Services

After installing the Citrix certificate templates, they must be published on one or more Microsoft Enterprise Certification Authority servers. Refer to the Microsoft documentation on how to deploy Active Directory Certificate Services.

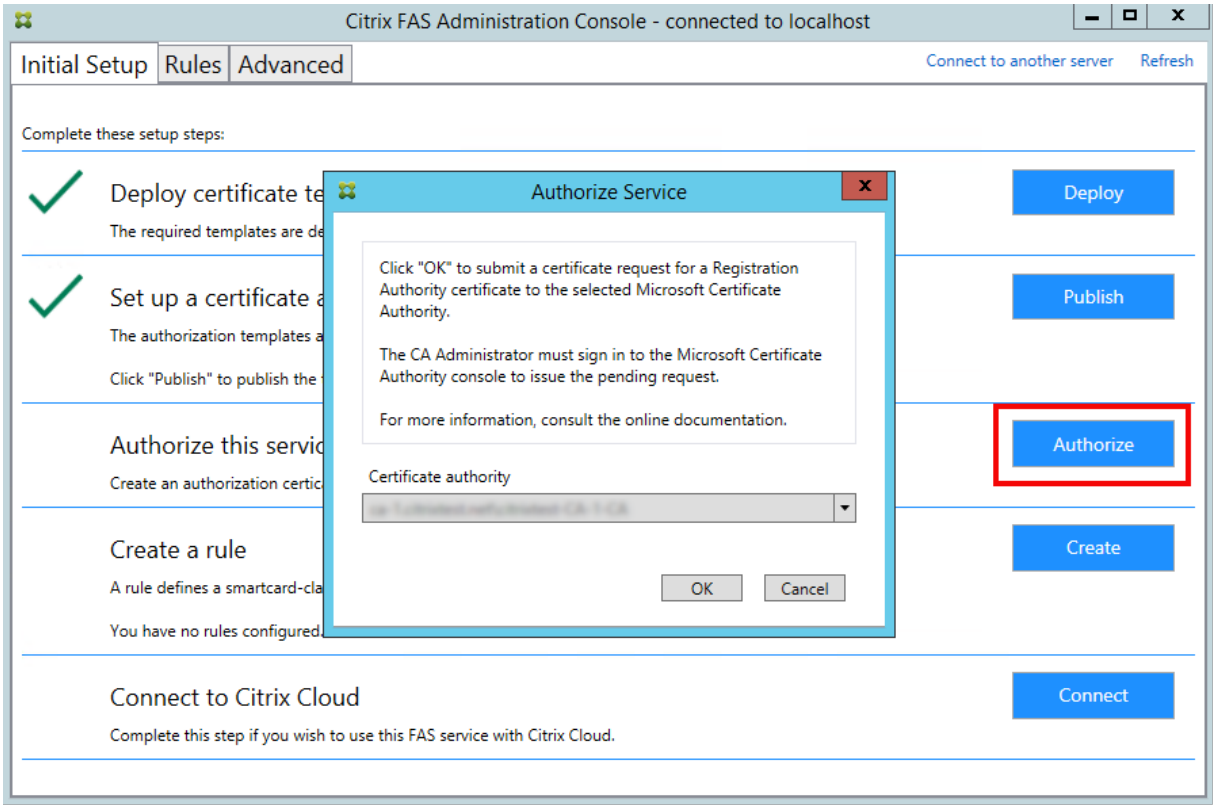
If the templates are not published on at least one server, use **Set Up Certificate Authority** to publish them. You must do this as a user that has permissions to administer the certificate authority.

(Certificate templates can also be published using the Microsoft Certification Authority console.)



Authorize Federated Authentication Service

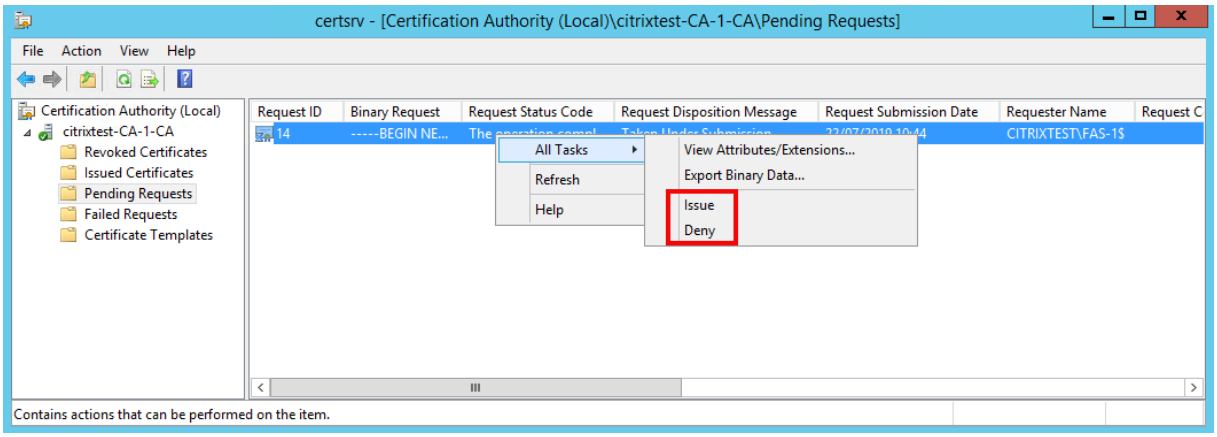
This step initiates the authorization of FAS. The administration console uses the Citrix_RegistrationAuthority_Manu template to generate a certificate request, and then sends it to one of the certificate authorities that are publishing that template.



After the request is sent, it appears in the **Pending Requests** list of the Microsoft Certification Authority console as a pending request from the FAS machine account. The certificate authority administrator must issue or deny the request before configuration of FAS can continue.

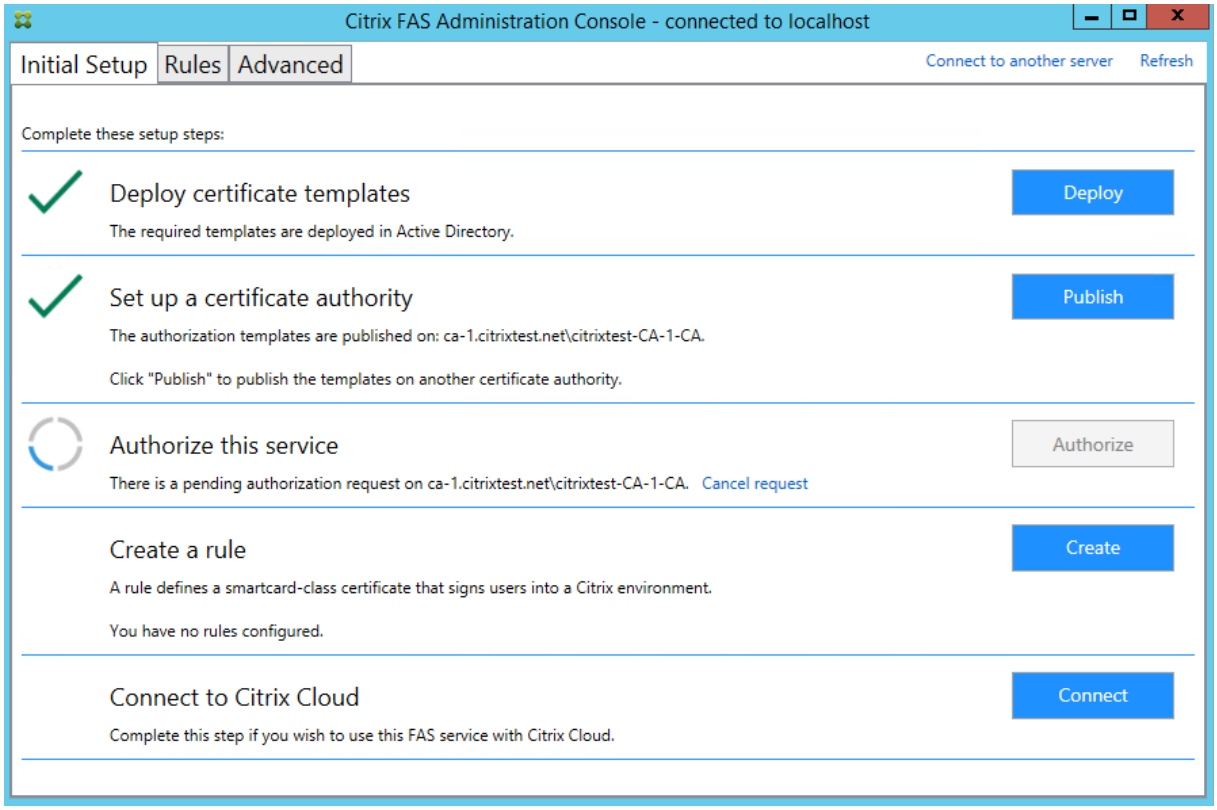
The FAS administration console displays a busy 'spinner' until the administrator chooses **Issue** or **Deny**.

In the Microsoft Certification Authority console, right-click **All Tasks** and then select **Issue** or **Deny** for the certificate request. If you choose **Issue**, the FAS administration console displays the authorisation certificate. If you choose **Deny**, the console shows an error message.



The FAS administration console automatically detects when this process completes. This can take a

couple of minutes.



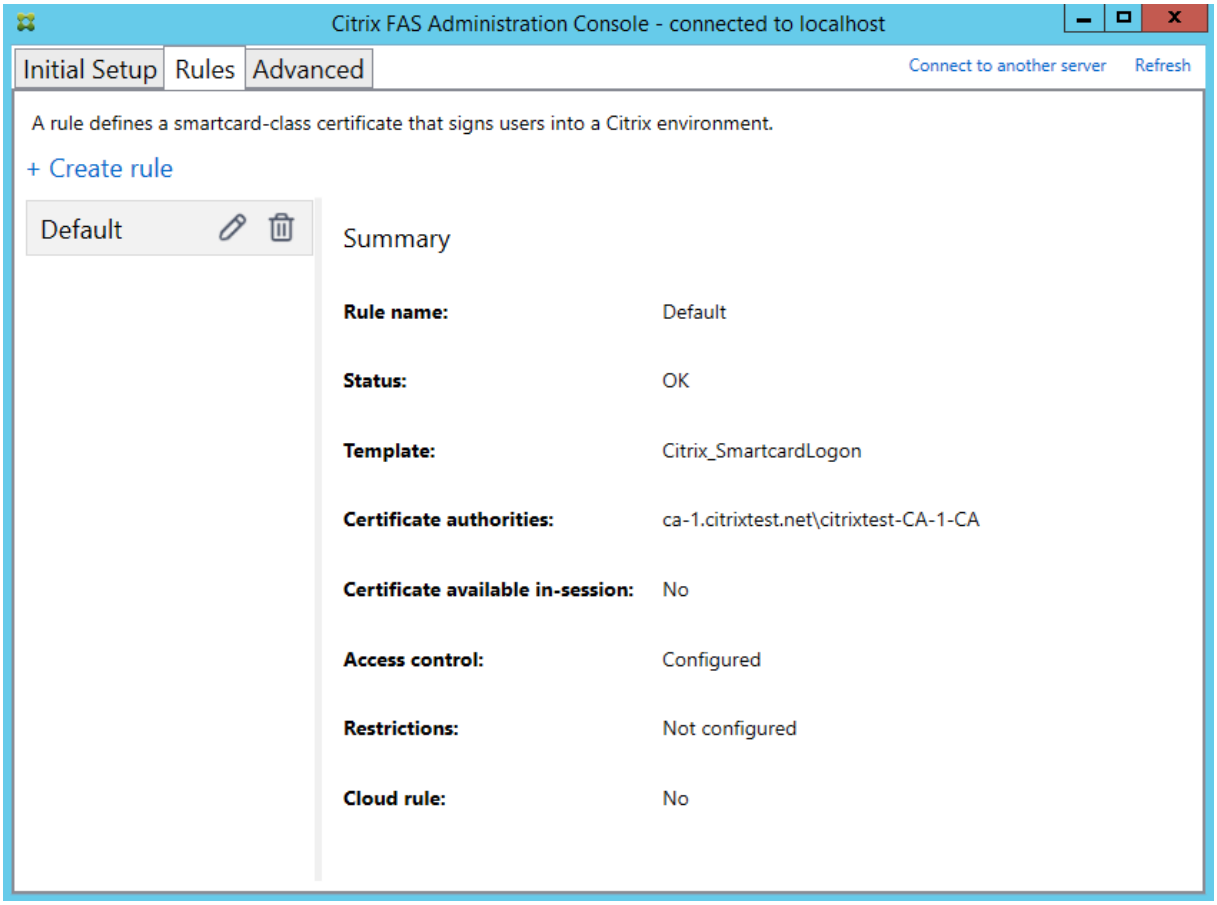
Configure rules

FAS uses rules to authorize the issuance of certificates for VDA logon and in-session use, as directed by StoreFront. Each rule specifies the StoreFront servers that are trusted to request certificates, the set of users for which they can be requested, and the set of VDA machines permitted to use them.

FAS needs at least one rule to be created and configured. We recommend that you create a rule named “default” because by default, StoreFront requests rule named “default” when contacting FAS.

You can create additional custom rules to reference different certificate templates and certificate authorities, and configure them to have different properties and permissions. These rules can be configured for use by different StoreFront servers or by Workspace. Configure StoreFront servers to request the custom rule by name using the Group Policy Configuration options.

Click **Create** (or **Create rule** on the “Rules” tab) to start the rule creation wizard which gathers information to create the rule. The “Rules” tab shows a summary of each rule.



The following information is gathered by the wizard:

Template: The certificate template that is used to issue user certificates. This should be the Citrix_SmartcardLogon template, or a modified copy of it (see Certificate templates).

Certificate Authority: The certificate authority that issues user certificates. The template must be published by the certificate authority. FAS supports adding multiple certificate authorities for failover and load balancing. Make sure the status shows "Template available" for the certificate authority you choose. See Certificate authority administration.

In-Session Use: The **Allow in-session use** option controls whether a certificate can be used after logon to the VDA.

- **Allow in-session use** not selected (default, *recommended*)—the certificate is only used only for logon or reconnection, and users do not have access to the certificate after authenticating.
- **Allow in-session use** selected—users have access to the certificate after authenticating. Most customers should not select this option. Resources accessed from within the VDA session, such as intranet websites or fileshares, can be accessed using Kerberos single sign-on, and therefore an in-session certificate is not required.

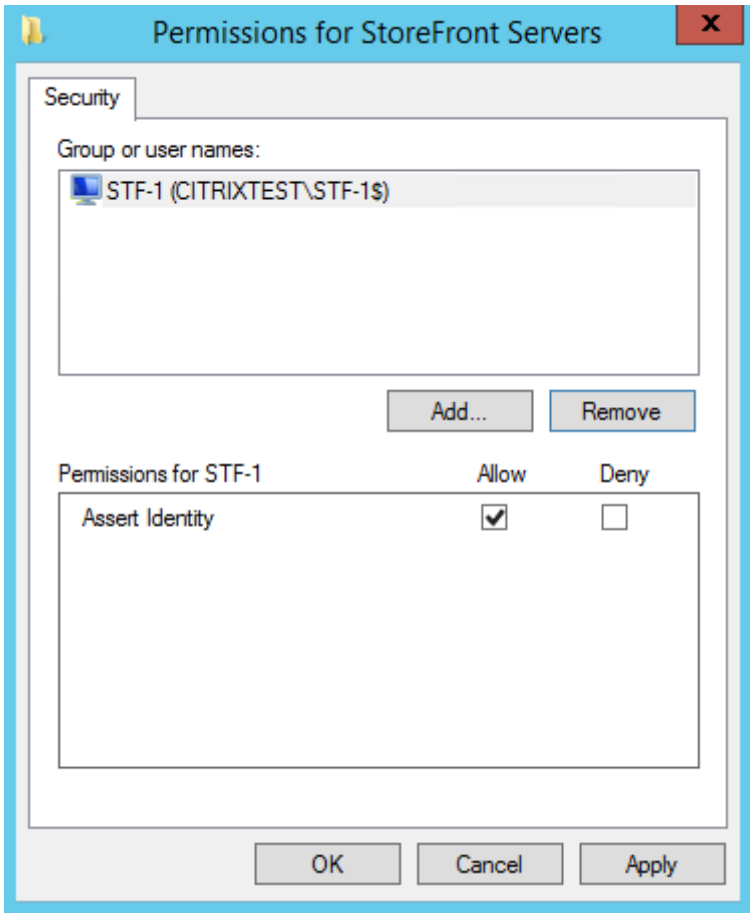
  If you select **Allow in-session use**, the In-session Behavior group policy must also be enabled

and applied to the VDA. Certificates are then placed in the user's personal certificate store after logon for application use. For example, if you require TLS authentication to web servers within the VDA session, the certificate can be used by Internet Explorer.

Access control: The list of trusted StoreFront server machines that are authorized to request certificates for logon or reconnection of users. For all these permissions you can add individual AD objects or groups.

> **Important:**
>
> The **Access control** setting is security critical, and must be managed carefully.
>
> **Note:**
>
> If you are using the FAS server only with Citrix Cloud you do not need to configure Access control. When a rule is used by Citrix Cloud, the StoreFront access permissions are ignored. You can use the same rule with Citrix Cloud and with an on-premises StoreFront deployment. StoreFront access permissions are still applied when the rule is used by an on-premises StoreFront.

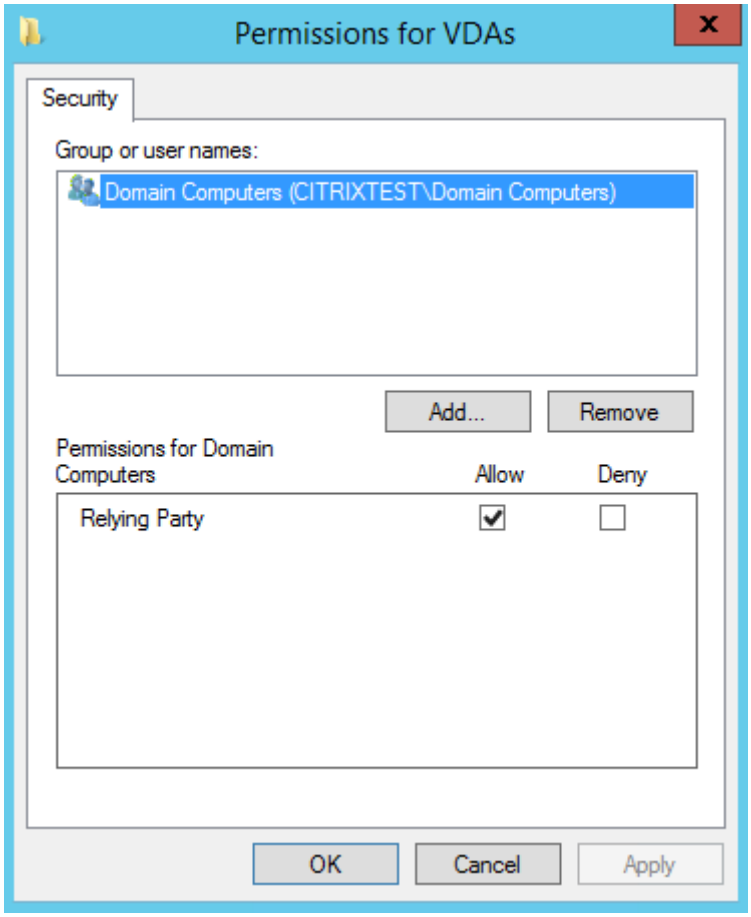
The default permission ("Assert Identity" allowed) denies everything. Therefore you must explicitly allow your Storefront servers.

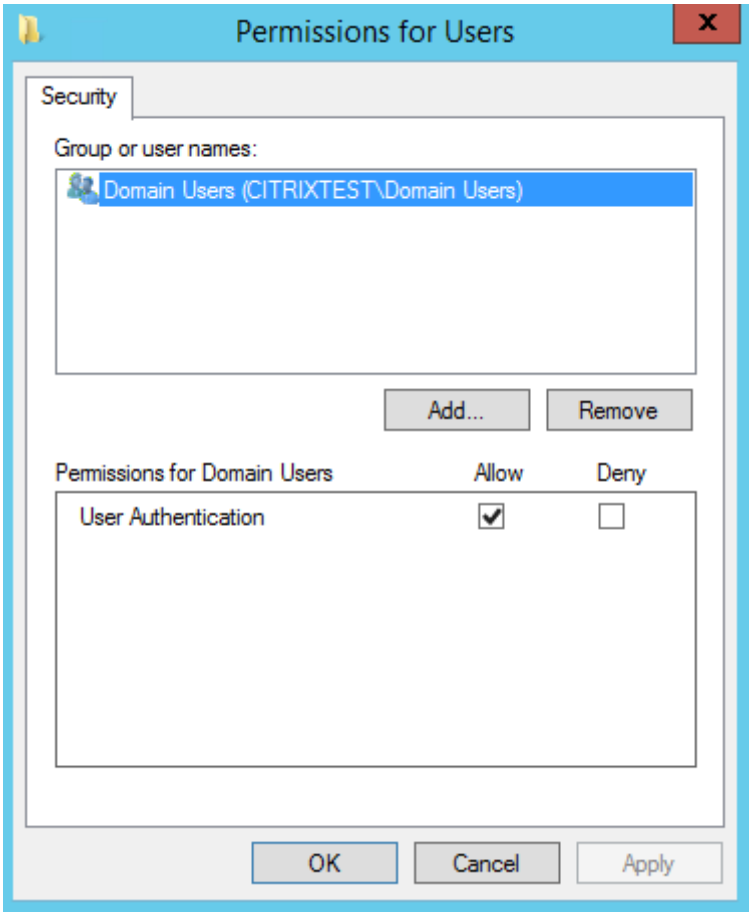


Restrictions: The list of VDA machines that can log users on using FAS and the list of users who can

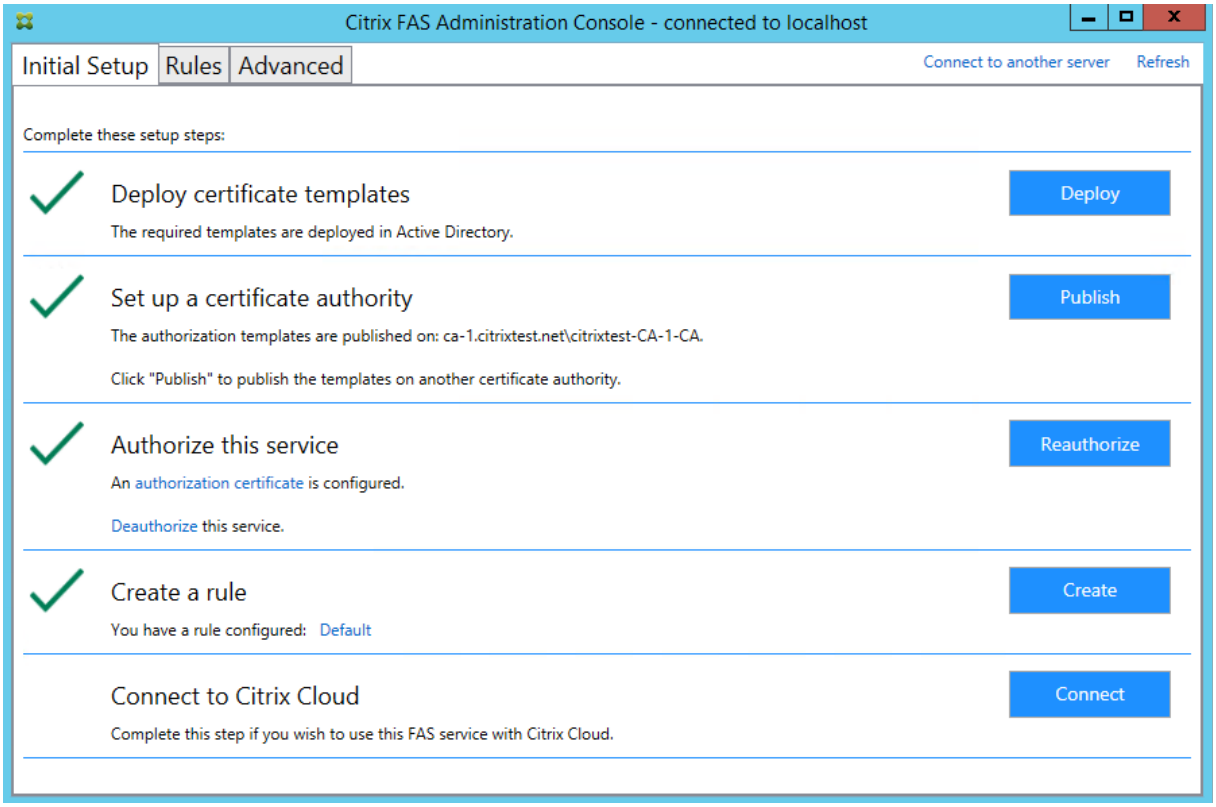
be issued certificates through FAS.

- **Manage VDA permissions** lets you specify which VDAs can use FAS to log the user on. The list of VDAs defaults to Domain Computers.
- **Manage user permissions** lets you specify which users can use FAS to sign in to a VDA. The list of users defaults to Domain Users.





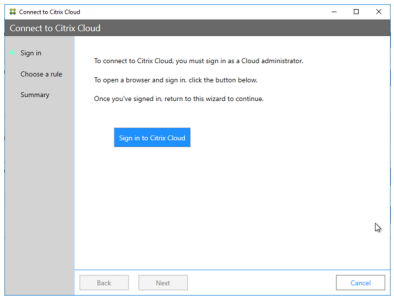
Cloud rule: Indicates if the rule is applied when identity assertions are received from Citrix Workspace. When you connect to Citrix Cloud, you choose which rule to use for Citrix Cloud. You can also change the rule after connecting to Citrix Cloud from a link in the **Connect to Citrix Cloud** section.



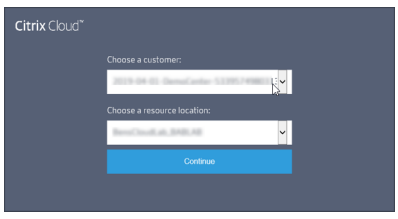
Connect to Citrix Cloud

You can connect the FAS server to Citrix Cloud with Citrix Workspace. See this Citrix Workspace article.

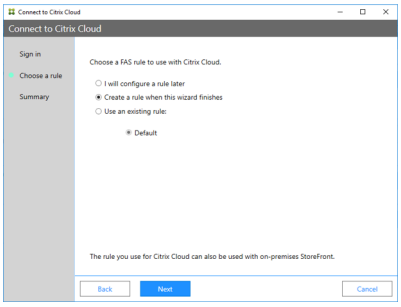
1. In the Initial Setup tab, under **Connect to Citrix Cloud** click **Connect**.



2. Click **Sign in to Citrix Cloud** then sign in to Citrix Cloud using admin credentials for the cloud customer you are connecting to.



3. Select the customer account, if applicable, and select the resource location where you want to connect the FAS server. Click **Continue** and then close the confirmation window.



4. In the FAS administration console, choose a rule to be applied when identity assertions are received from Citrix Workspace, or select **Create a rule** when this wizard finishes. (In the “Rules” tab, the Cloud rule value is “Yes” for the rule you select or create.)
5. In the “Summary” tab click **Finish** to complete Citrix Cloud connection.

Citrix Cloud registers the FAS server and displays it on the Resource Locations page in your Citrix Cloud account.

Disconnect from Citrix Cloud

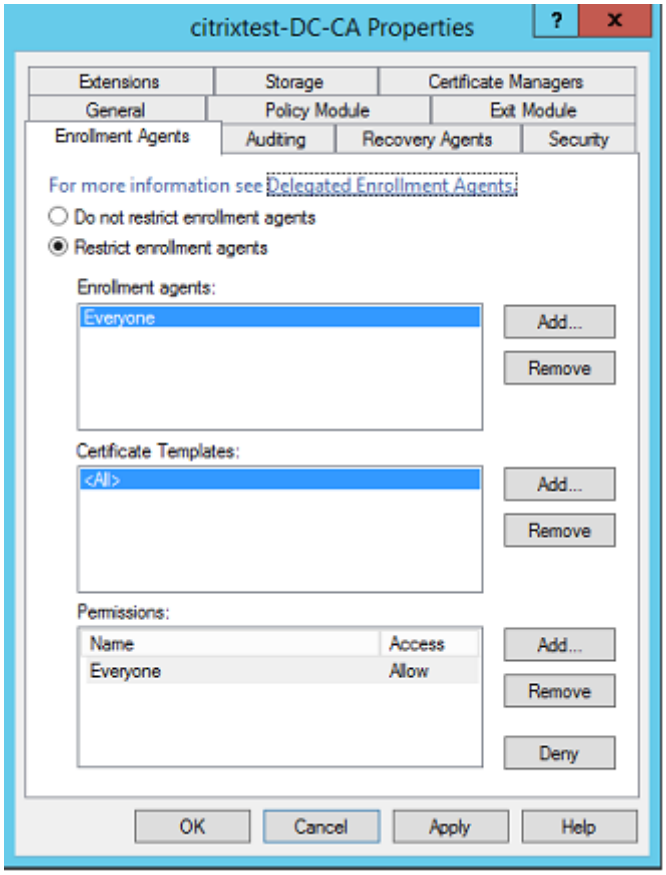
After removing the FAS server from your Citrix Cloud resource location, as described in this Citrix Workspace article, in **Connect to Citrix Cloud** select **Disable**.

Security considerations

FAS has a registration authority certificate that allows it to issue certificates autonomously on behalf of your domain users. As such, it is important to develop and implement a security policy to protect FAS servers, and to constrain their permissions.

Delegated enrollment agents

FAS issues user certificates by acting as an enrollment agent. The Microsoft Certification Authority allows you to restrict enrollment agents, certificate templates, and users which enrollment agents can issue certificates for.



You can use this dialog to ensure that:

- The *Enrollment agents* list contains only FAS servers.
- The *Certificate Templates* list contains only the FAS templates.
- The *Permissions* list contains only users who are permitted to use FAS. For example, it is good practice to prevent FAS from issuing certificates to users in an Administration or Protected Users group.

Access Control List configuration

As described in the Configure rules section, you must configure a list of StoreFront servers that are trusted to assert user identities to FAS when certificates are issued. Similarly, you can restrict which users will be issued certificates, and which VDA machines they can authenticate to. This is in addition to any standard Active Directory or certificate authority security features you configure.

Firewall settings

All communication to FAS servers uses mutually authenticated Windows Communication Foundation (WCF) Kerberos network connections over port 80.

Event log monitoring

FAS and the VDA write information to the Windows Event Log. This can be used for monitoring and auditing information. The Event logs section lists event log entries that may be generated.

Hardware security modules

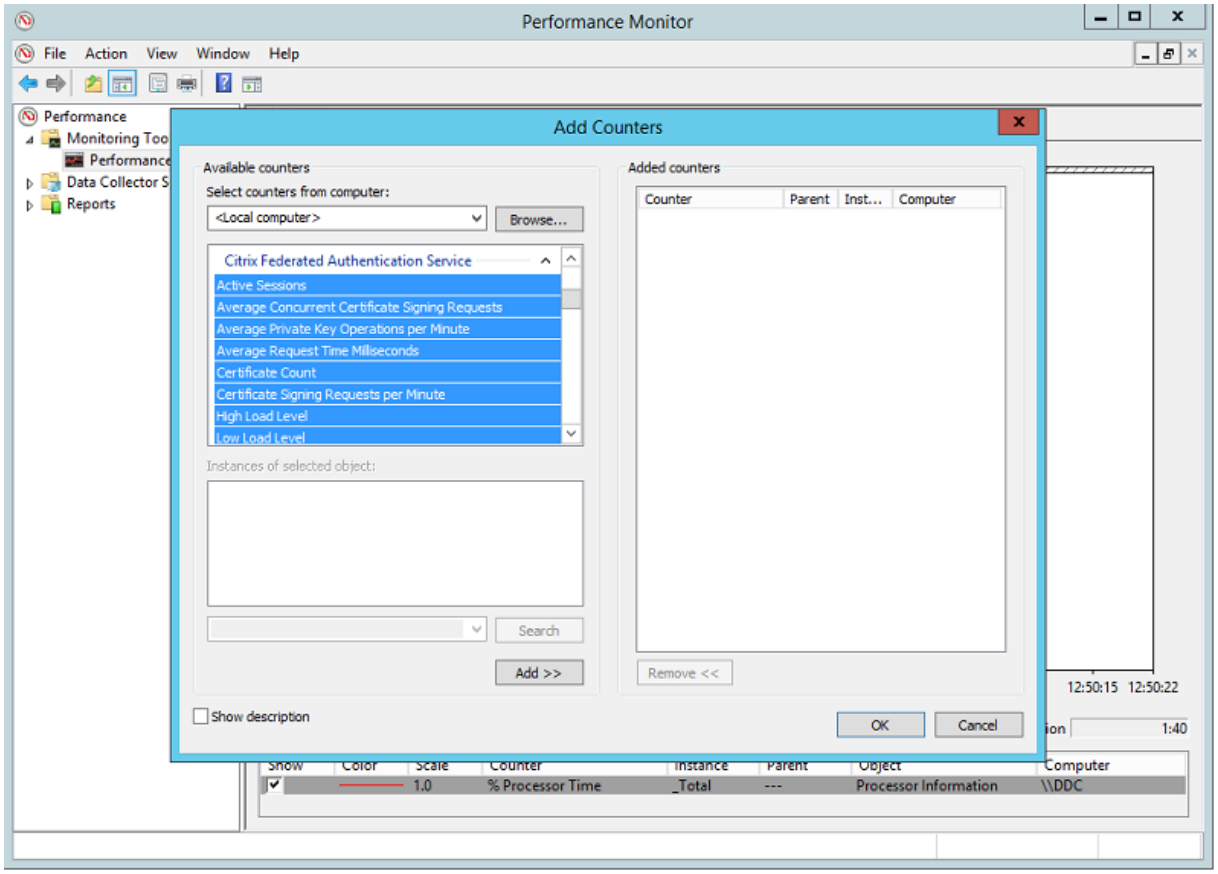
All private keys, including those of user certificates issued by FAS, are stored as non-exportable private keys by the Network Service account. FAS supports the use of a cryptographic hardware security module, if your security policy requires it.

Low-level cryptographic configuration is available in the FederatedAuthenticationService.exe.config file. These settings apply when private keys are first created. Therefore, different settings can be used for registration authority private keys (for example, 4096 bit, TPM protected) and runtime user certificates.

Parameter	Description
ProviderLegacyCsp	When set to true, FAS uses the Microsoft CryptoAPI (CAPI). Otherwise, FAS uses the Microsoft Cryptography Next Generation API (CNG).
ProviderName	Name of the CAPI or CNG provider to use.
ProviderType	Refers to Microsoft KeyContainerPermissionAccessEntry.ProviderType Property PROV_RSA_AES 24. Should always be 24 unless you are using an HSM with CAPI and the HSM vendor specifies otherwise.
KeyProtection	Controls the “Exportable” flag of private keys. Also allows the use of Trusted Platform Module (TPM) key storage, if supported by the hardware.
KeyLength	Key length for RSA private keys. Supported values are 1024, 2048 and 4096 (default: 2048).

Performance counters

FAS includes a set of performance counters for load tracking purposes.



The following table lists the available counters. Most counters are rolling averages over five minutes.

Name	Description
Active Sessions	Number of connections tracked by FAS.
Concurrent CSRs	Number of certificate requests processed at the same time.
Private Key ops	Number of private key operations performed per minute.
Request time	Length of time to generate and sign a certificate.
Certificate Count	Number of certificates cached in FAS.
CSR per minute	Number of certificate signing requests processed per minute.

Name	Description
Low/Medium/High	Estimates of the load that FAS can accept in terms of “CSRs per minute”. Exceeding the “High Load” threshold may result in session launches failing.

Event logs

The following tables list the event log entries generated by FAS.

Administration events [Federated Authentication Service]

[Event Source: Citrix.Authentication.FederatedAuthenticationService]

These events are logged in response to a configuration change in the FAS server.

Log Codes
[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}] enrolling with CA [{1}] templates [{2} and {3}]
[S005] Administrator [{0}] de-authorizing CA [{1}]
[S006] Administrator [{0}] creating new Certificate Definition [{1}]
[S007] Administrator [{0}] updating Certificate Definition [{1}]
[S008] Administrator [{0}] deleting Certificate Definition [{1}]
[S009] Administrator [{0}] creating new Role [{1}]
[S010] Administrator [{0}] updating Role [{1}]
[S011] Administrator [{0}] deleting Role [{1}]
[S012] Administrator [{0}] creating certificate [upn: {1} sid: {2} role: {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}]

Log Codes
[S050] Administrator [{0}] creating new cloud configuration: [{1}]
[S051] Administrator [{0}] updating cloud configuration: [{1}]
[S052] Administrator [{0}] removing cloud configuration

Log Codes
[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 occured 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 MinThreads adjusted from [workers: {0} completion: {1}] to: [workers: {2} completion: {3}]
[S410] Failed to adjust ThreadPool MinThreads from [workers: {0} completion: {1}] to: [workers: {2} completion: {3}]
[S411] Error starting the FAS service: [{0}]

Creating identity assertions [Federated Authentication Service]

[Event Source: Event Source: Citrix.Authentication.FederatedAuthenticationService]

These events are logged at runtime on the FAS server when a trusted server asserts a user logon.

Log Codes
[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}])

Log Codes
[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 [certifcate 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 [certifcate authority: {2}] [exception: {3}]

Acting as a relying party [Federated Authentication Service]

[Event Source: Event Source: Citrix.Authentication.FederatedAuthenticationService]

These events are logged at runtime on the FAS server when a VDA logs on a user.

Log Codes
[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] Calling account [{0}] is not a relying party in role [{1}]
[S206] Calling account [{0}] is not a relying party
[S208] Private Key operation failed [Operation: {0}][upn: {1} role: {2} certificateDefinition {3}][Error {4} {5}].

In-session certificate server [Federated Authentication Service]

[Event Source: Event Source: Citrix.Authentication.FederatedAuthenticationService]

These events are logged on the FAS server when a user uses an in-session certificate.

Log Codes
[S301] Access Denied: User [{0}] does not have access to a Virtual Smart Card
[S302] User [{0}] requested unknown Virtual Smart Card [thumbprint: {1}]

Log Codes
[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 plugin [Federated Authentication Service]

[Event Source: Event Source: Citrix.Authentication.FederatedAuthenticationService]

These events are logged by the FAS assertion plugin.

Log Codes
[S500] No FAS assertion plugin is configured
[S501] The configured FAS assertion plugin could not be loaded [exception:{0}]
[S502] FAS assertion plugin loaded [pluginId={0}] [assembly={1}] [location={2}]
[S503] Server [{0}] failed to assert UPN [{1}] (logon evidence was supplied but the plugin [{2}] does not support it)
[S504] Server [{0}] failed to assert UPN [{1}] (logon evidence was supplied but there is no configured FAS plugin)
[S505] Server [{0}] failed to assert UPN [{1}] (the plugin [{2}] rejected the logon evidence with status [{3}] and message [{4}])
[S506] The plugin [{0}] accepted logon evidence from server [{1}] for UPN [{2}] with message [{3}]
[S507] Server [{0}] failed to assert UPN [{1}] (the plugin [{2}] threw exception [{3}])
[S507] Server [{0}] failed to assert UPN [{1}] (the plugin [{2}] threw exception [{3}])
[S508] Server [{0}] failed to assert UPN [{1}] (access disposition was supplied but the plugin [{2}] does not support it)
[S509] Server [{0}] failed to assert UPN [{1}] (access disposition was supplied but there is no configured FAS plugin)
[S510] Server [{0}] failed to assert UPN [{1}] (the access disposition was deemed invalid by plugin [{2}]

Workspace-enabled FAS [Federated Authentication Service]

[Event Source: Event Source: Citrix.Fas.Cloud]

These events are logged when FAS is used in conjunction with Workspace.

Log Codes
[S001] Rotating Citrix Cloud service keys [fas id={0}]
[S002] The FAS cloud service 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 unregisted 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
[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 FAS cloud service failed to start. Exception: {0}
[S022] The FAS cloud service is stopping

Log on [VDA]

[Event Source: Citrix.Authentication.IdentityAssertion]

These events are logged on the VDA during the logon stage.

Log Codes
[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}]
[S106] Identity Assertion Logon. Logging in [Certificate: {0}]
[S107] Identity Assertion Logon failed. [Exception: {0}{1}]
[S108] Identity Assertion Subsystem. ACCESS_DENIED [Caller: {0}]

In-session certificates [VDA]

[Event Source: Citrix.Authentication.IdentityAssertion]

These events are logged on the VDA when a user attempts to use an in-session certificate.

Log Codes
[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

Certificate request and key pair generation [Federated Authentication Service]

[Event Source: Citrix.Fas.PkiCore]

These events are logged when the FAS server performs low-level cryptographic operations.

Log Codes
[S001] TrustArea::TrustArea: Installed certificate [TrustArea: {0}] [Certificate {1}][TrustAreaJoinParameters{2}
[S014] Pkcs10Request::Create: Created PKCS10 request [Distinguished Name {0}]

Log Codes
[S016] PrivateKey::Create [Identifier {0}][MachineWide: {1}][Provider: {2}][ProviderType: {3}][EllipticCurve: {4}][KeyLength: {5}][isExportable: {6}]
[S017] PrivateKey::Delete [CspName: {0}, Identifier {1}]

Log Codes
[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}]

Deployment architectures

March 26, 2020

Introduction

Federated Authentication Service (FAS) is a Citrix component that integrates with your Active Directory certificate authority, allowing users to be seamlessly authenticated within a Citrix environment. This document describes various authentication architectures that may be appropriate for your deployment.

When enabled, FAS delegates user authentication decisions to trusted StoreFront servers. StoreFront has a comprehensive set of built-in authentication options built around modern web technologies, and is easily extensible using the StoreFront SDK or third-party IIS plugins. The basic design goal is that any authentication technology that can authenticate a user to a web site can now be used to log in to a Citrix Virtual Apps or Citrix Virtual Desktops deployment.

This document describes example top-level deployment architectures, in increasing complexity.

- Internal deployment
- Citrix Gateway deployment
- ADFS SAML
- B2B account mapping

- Windows 10 Azure AD join

Links are provided to related FAS articles. For all architectures, the Install and configure article is the primary reference for setting up FAS.

How it works

FAS is authorized to issue smart card class certificates automatically on behalf of Active Directory users who are authenticated by StoreFront. This uses similar APIs to tools that allow administrators to provision physical smart cards.

When a user is brokered to a Citrix Virtual Apps or Citrix Virtual Desktops Virtual Delivery Agent (VDA), the certificate is attached to the machine, and the Windows domain sees the logon as a standard smart card authentication.

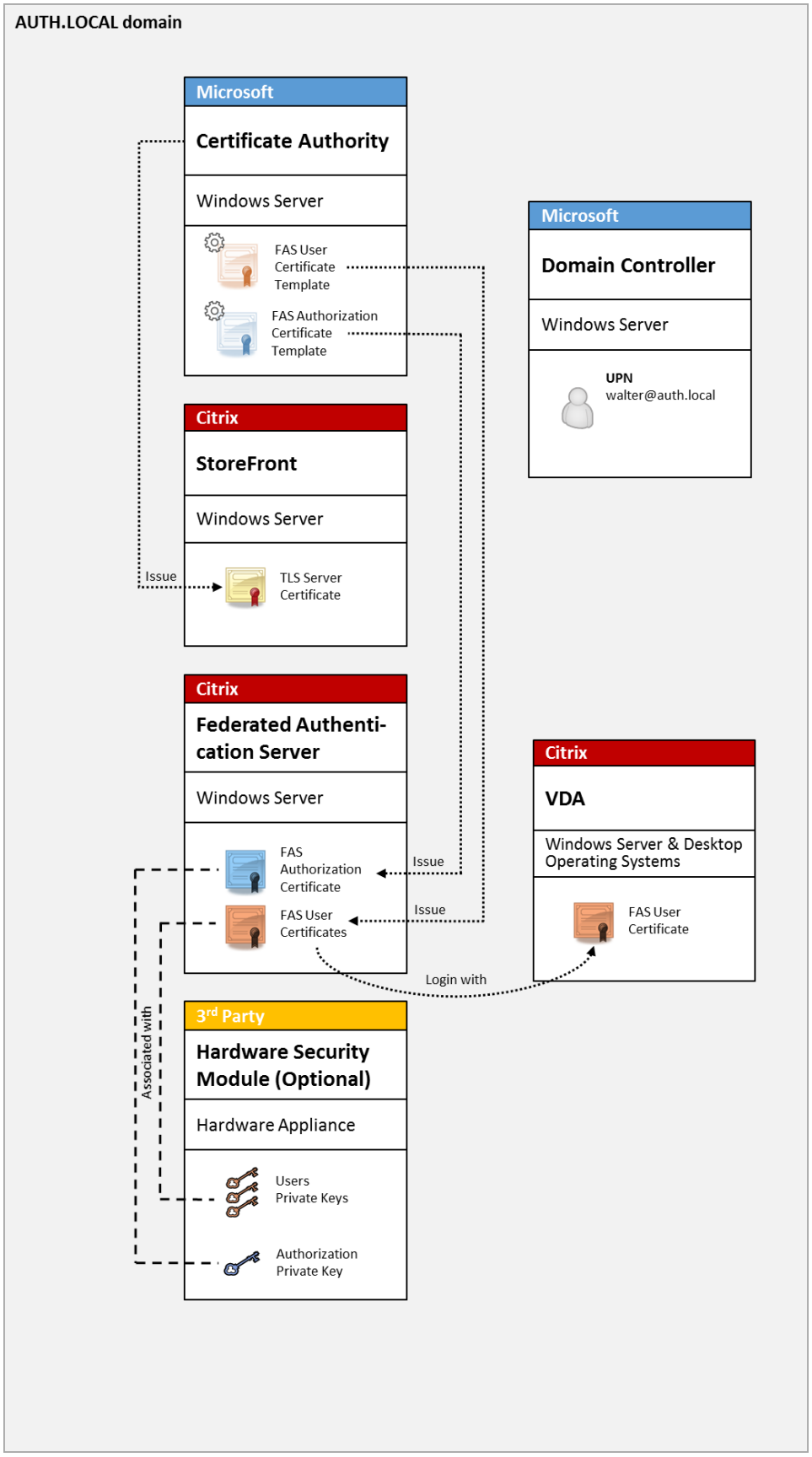
Internal deployment

FAS allows users to securely authenticate to StoreFront using a variety of authentication options (including Kerberos single sign-on) and connect through to a fully authenticated Citrix HDX session.

This allows Windows authentication without prompts to enter user credentials or smart card PINs, and without using “saved password management” features such as the Single Sign-on Service. This can be used to replace the Kerberos Constrained Delegation logon features available in earlier versions of Citrix Virtual Apps.

All users have access to public key infrastructure (PKI) certificates within their session, regardless of whether or not they log on to the endpoint devices with a smart card. This allows a smooth migration to two-factor authentication models, even from devices such as smartphones and tablets that do not have a smart card reader.

This deployment adds a new server running FAS, which is authorized to issue smart card class certificates on behalf of users. These certificates are then used to log on to user sessions in a Citrix HDX environment as if a smart card logon was used.



The Citrix Virtual Apps or Citrix Virtual Desktops environment must be configured in a similar manner as smart card logon, which is documented in CTX206156.

In an existing deployment, this usually involves only ensuring that a domain-joined Microsoft certificate authority is available, and that domain controllers have been assigned domain controller certificates. (See the "Issuing Domain Controller Certificates" section in CTX206156.)

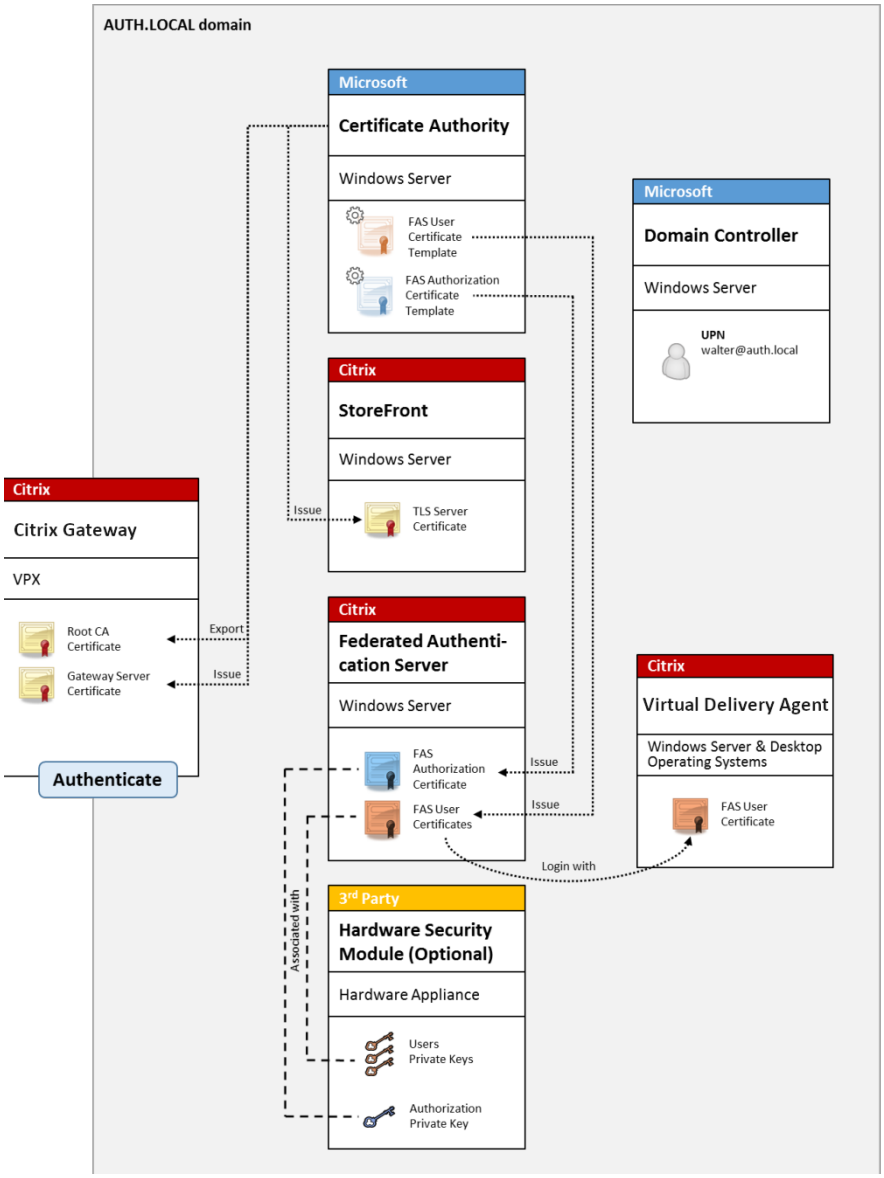
Related information:

- Keys can be stored in a Hardware Security Module (HSM) or built-in Trusted Platform Module (TPM). For details, see the Private key protection article.
- The Install and configure article describes how to install and configure FAS.

Citrix Gateway deployment

The Citrix Gateway deployment is similar to the internal deployment, but adds Citrix Gateway paired with StoreFront, moving the primary point of authentication to Citrix Gateway itself. Citrix Gateway includes sophisticated authentication and authorization options that can be used to secure remote access to a company's web sites.

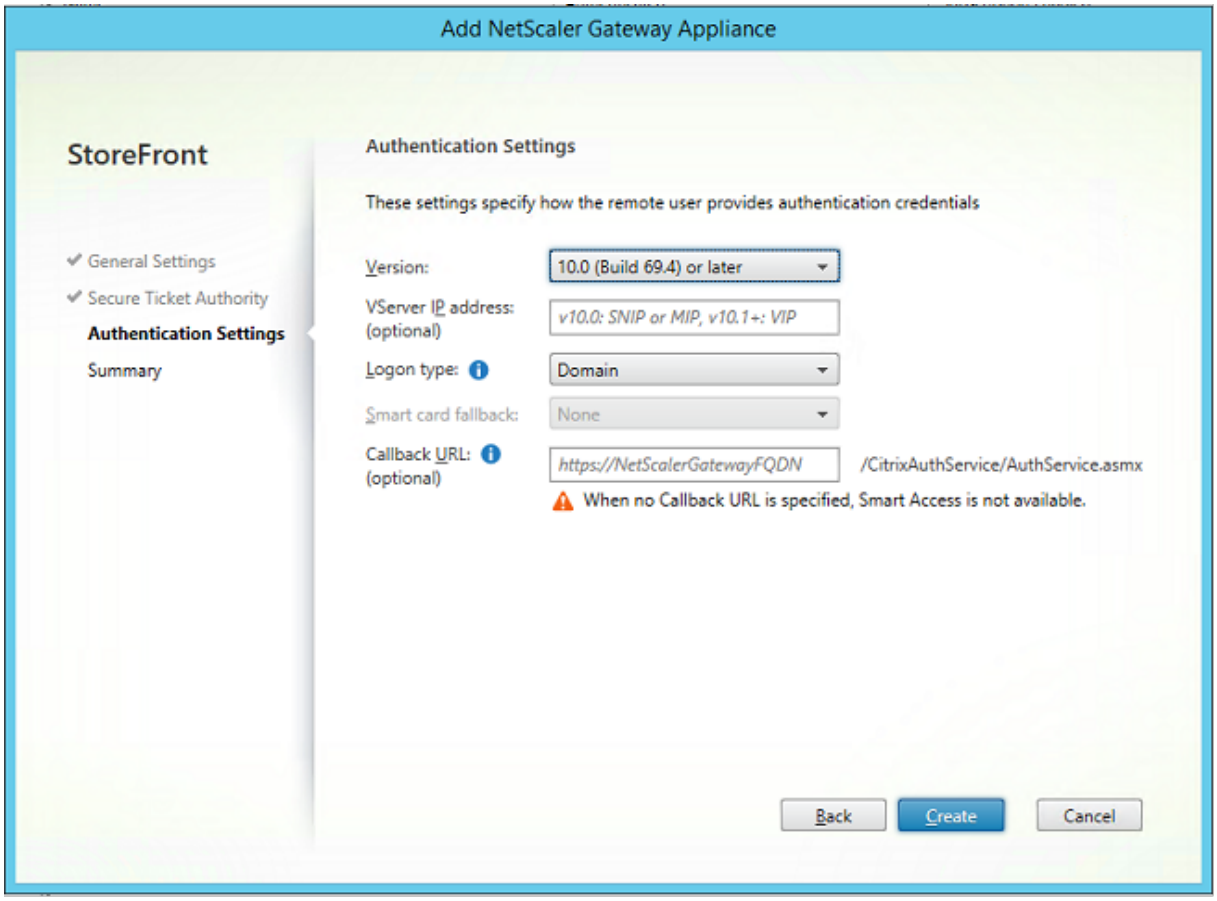
This deployment can be used to avoid multiple PIN prompts that occur when authenticating first to Citrix Gateway and then logging in to a user session. It also allows use of advanced Citrix Gateway authentication technologies without additionally requiring AD passwords or smart cards.



The Citrix Virtual Apps or Citrix Virtual Desktops environment must be configured in a similar manner as smart card logon, which is documented in CTX206156.

In an existing deployment, this usually involves only ensuring that a domain-joined Microsoft certificate authority is available, and that domain controllers have been assigned Domain Controller certificates. (See the “Issuing Domain Controller Certificates” section in CTX206156).

When configuring Citrix Gateway as the primary authentication system, ensure that all connections between Citrix Gateway and StoreFront are secured with TLS. In particular, ensure that the Callback Url is correctly configured to point to the Citrix Gateway server, as this can be used to authenticate the Citrix Gateway server in this deployment.

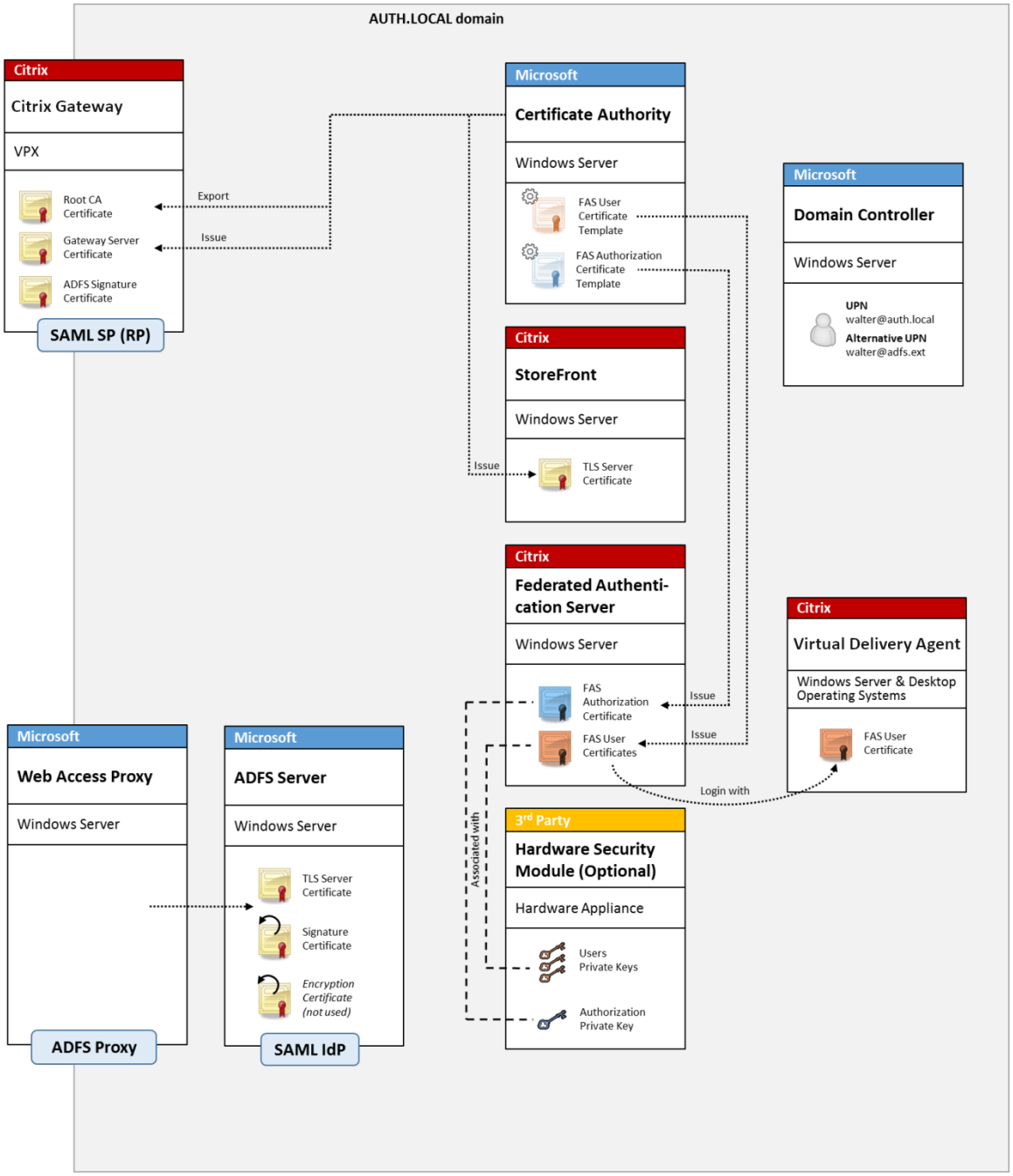


Related information:

- To configure Citrix Gateway, see "How to Configure NetScaler Gateway 10.5 to use with StoreFront 3.6 and Citrix Virtual Desktops 7.6."
- Install and configure describes how to install and configure FAS.

ADFS SAML deployment

A key Citrix Gateway authentication technology allows integration with Microsoft ADFS, which can act as a SAML Identity Provider (IdP). A SAML assertion is a cryptographically-signed XML block issued by a trusted IdP that authorizes a user to log on to a computer system. This means that the FAS server allows the authentication of a user to be delegated to the Microsoft ADFS server (or other SAML-aware IdP).



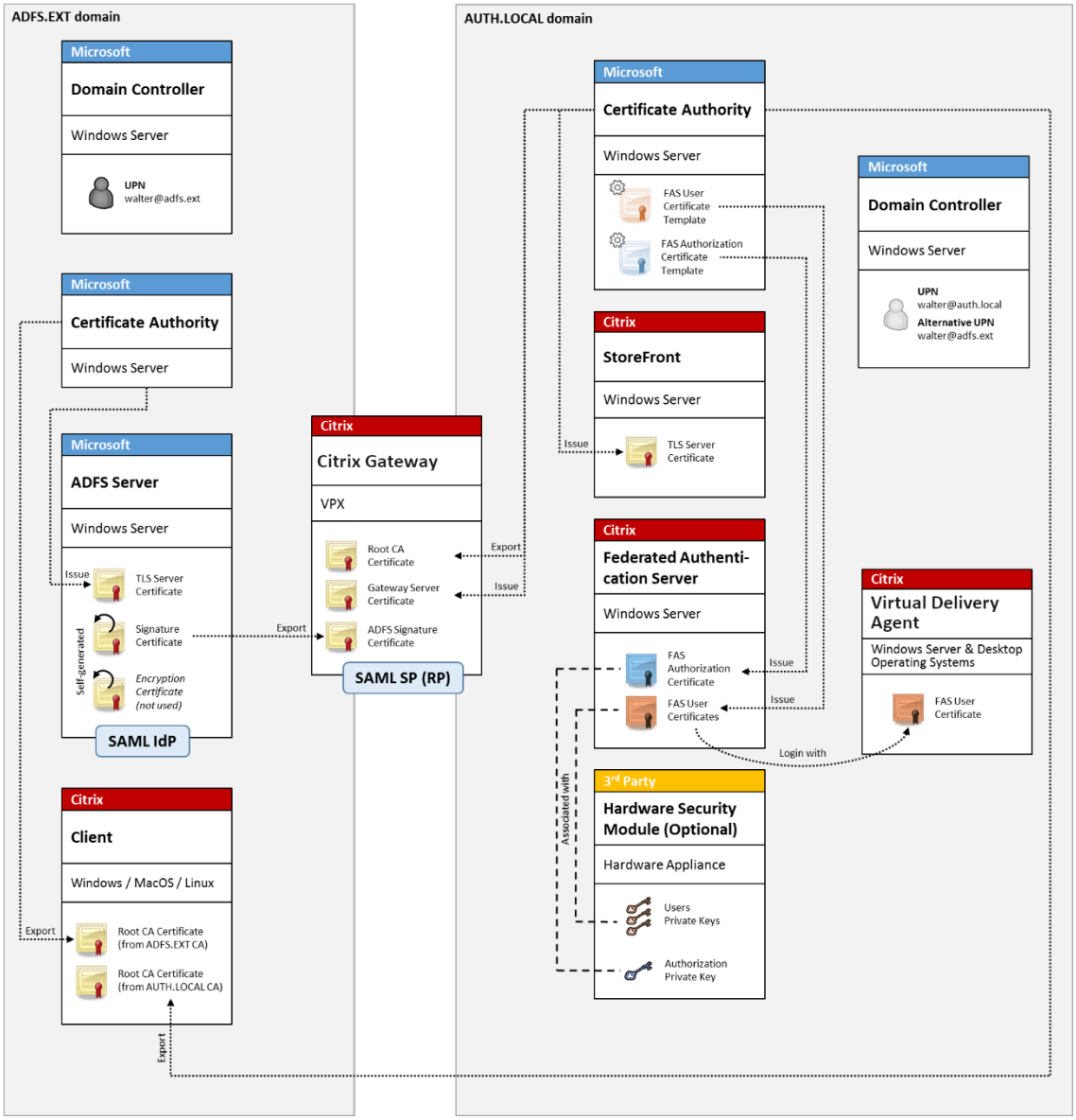
ADFS is commonly used to securely authenticate users to corporate resources remotely over the Internet; for example, it is often used for Office 365 integration.

Related information:

- The ADFS deployment article contains details.
- The Install and configure article describes how to install and configure FAS.
- The Citrix Gateway deployment section in this article contains configuration considerations.

B2B account mapping

If two companies want to use each other's computer systems, a common option is to set up an Active Directory Federation Service (ADFS) server with a trust relation. This allows users in one company to seamlessly authenticate into another company's Active Directory (AD) environment. When logging on, each user uses their own company logon credentials; ADFS automatically maps this to a "shadow account" in the peer company's AD environment.

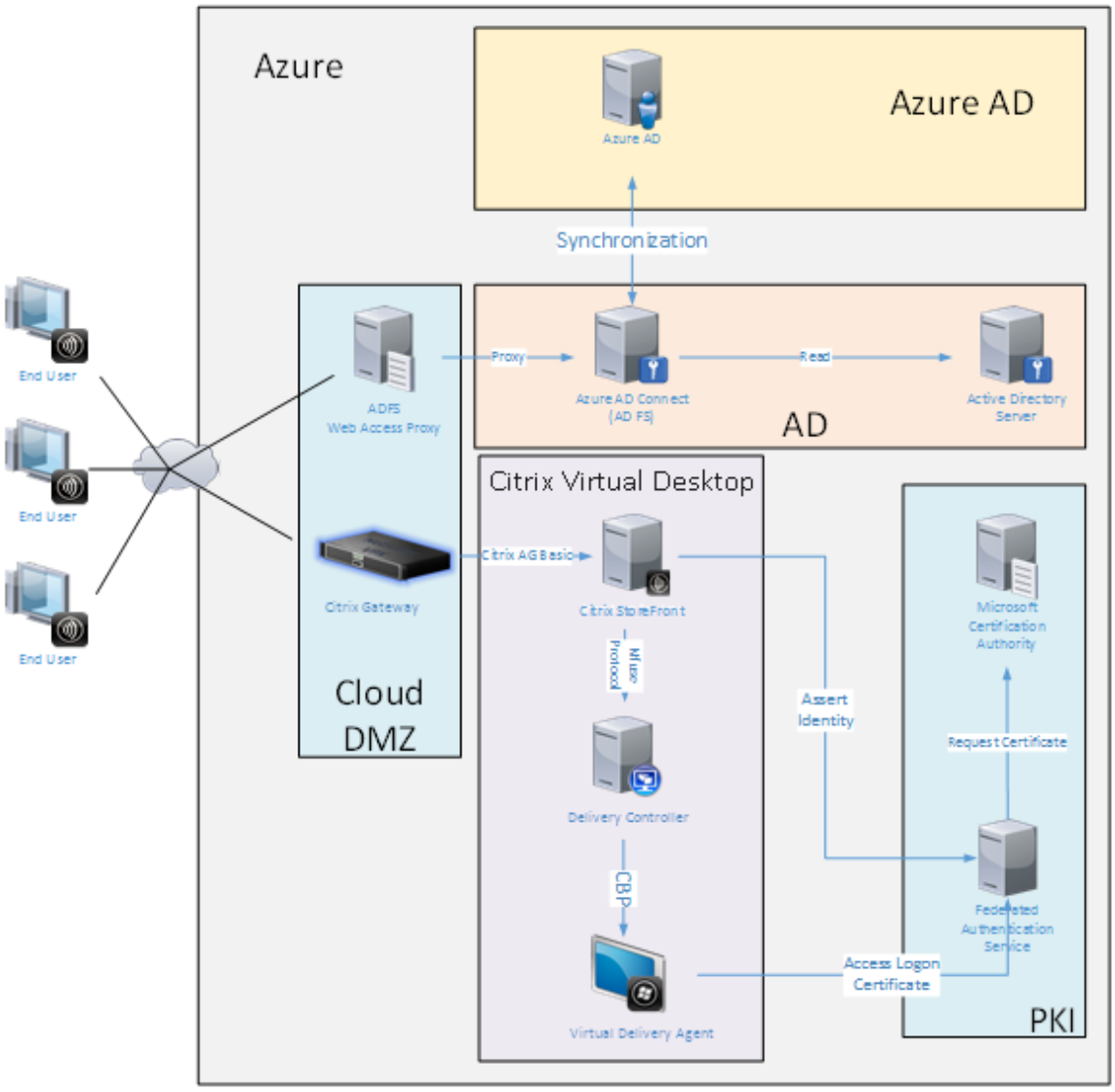


Related information:

- The Install and configure article describes how to install and configure FAS.

Windows 10 Azure AD Join

Windows 10 introduced the concept of “Azure AD Join,” which is conceptually similar to traditional Windows domain join but targeted at “over the internet” scenarios. This works well with laptops and tablets. As with traditional Windows domain join, Azure AD has functionality to allow single sign-on models for company websites and resources. These are all “Internet aware,” so will work from any Internet connected location, not just the office LAN.



This deployment is an example where there is effectively no concept of “end users in the office.” Laptops are enrolled and authenticate entirely over the Internet using modern Azure AD features.

Note that the infrastructure in this deployment can run anywhere an IP address is available: on-premises, hosted provider, Azure, or another cloud provider. The Azure AD Connect synchronizer will automatically connect to Azure AD. The example graphic uses Azure VMs for simplicity.

Related information:

- The Install and configure article describes how to install and configure FAS.
- The Azure AD integration article contains details.

ADFS deployment

September 11, 2019

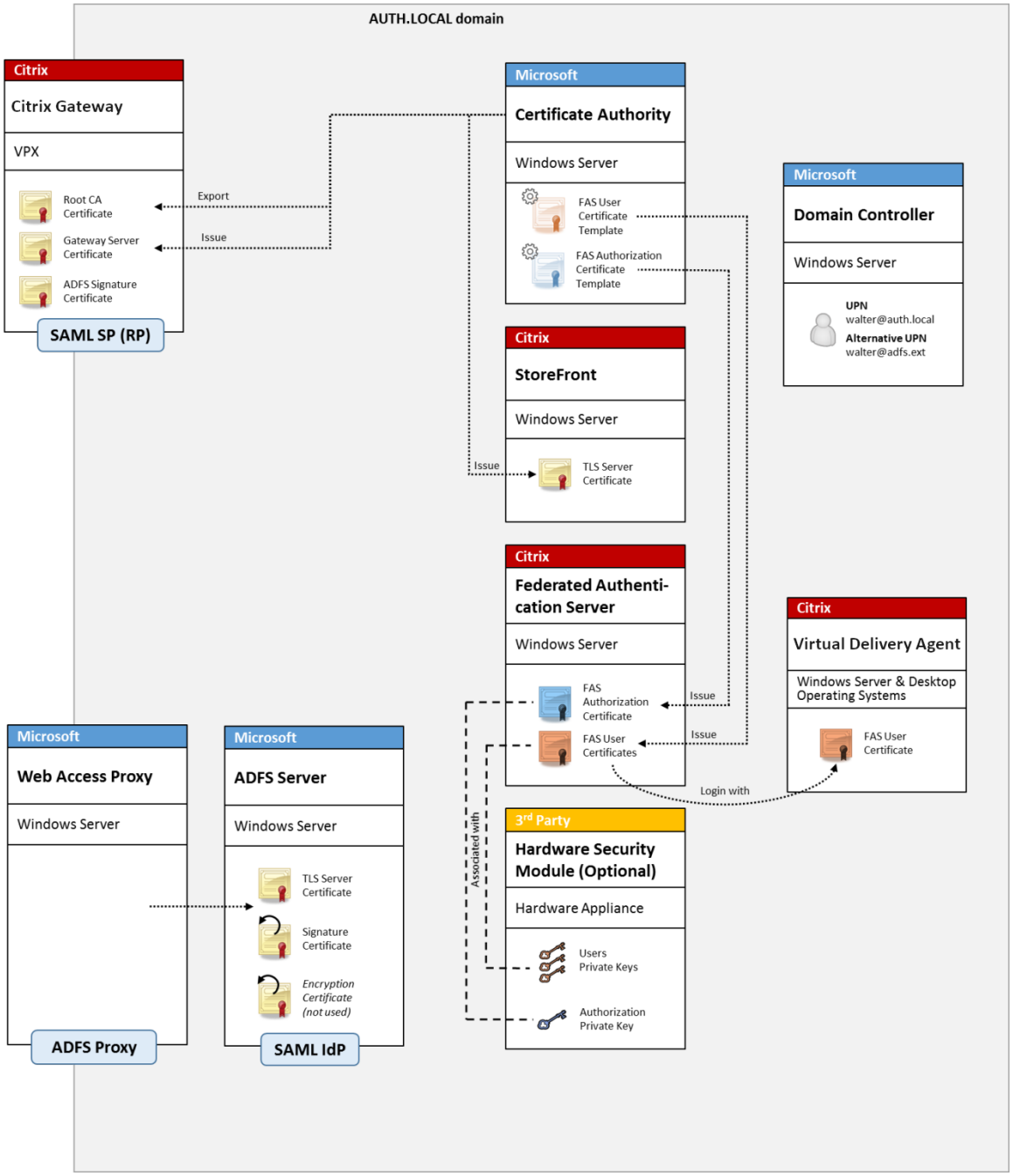
Introduction

This document describes how to integrate a Citrix environment with Microsoft ADFS.

Many organizations use ADFS to manage secure user access to web sites that require a single point of authentication. For example, a company may have additional content and downloads that are available to employees; those locations need to be protected with standard Windows logon credentials.

Federated Authentication Service (FAS) also allows Citrix Gateway and Citrix StoreFront to be integrated with the ADFS logon system, reducing potential confusion for the company's staff.

This deployment integrates Citrix Gateway as a relying party to Microsoft ADFS.



SAML overview

Security Assertion Markup Language (SAML) is a simple “redirect to a logon page” web browser logon system. Configuration includes the following items:

Redirect URL [Single Sign-on Service Url]

When Citrix Gateway discovers that a user needs to be authenticated, it instructs the user's web browser to do a HTTP POST to a SAML logon webpage on the ADFS server. This is usually an `https://` address of the form: `https://adfs.mycompany.com/adfs/ls`.

This web page POST includes other information, including the "return address" where ADFS will return the user when logon is complete.

Identifier [Issuer Name/EntityID]

The EntityId is a unique identifier that Citrix Gateway includes in its POST data to ADFS. This informs ADFS which service the user is trying to log on to, and to apply different authentication policies as appropriate. If issued, the SAML authentication XML will only be suitable for logging on to the service identified by the EntityId.

Usually, the EntityID is the URL of the Citrix Gateway server logon page, but it can generally be anything, as long as Citrix Gateway and ADFS agree on it: `https://ns.mycompany.com/application/logonpage`.

Return address [Reply URL]

If authentication is successful, ADFS instructs the user's web browser to POST a SAML authentication XML back to one of the Reply URLs that are configured for the EntityId. This is usually an `https://` address on the original Citrix Gateway server in the form: `https://ns.mycompany.com/cgi/samlauth`.

If there is more than one Reply URL address configured, Citrix Gateway can choose one in its original POST to ADFS.

Signing certificate [IDP Certificate]

ADFS cryptographically signs SAML authentication XML blobs using its private key. To validate this signature, Citrix Gateway must be configured to check these signatures using the public key included in a certificate file. The certificate file will usually be a text file obtained from the ADFS server.

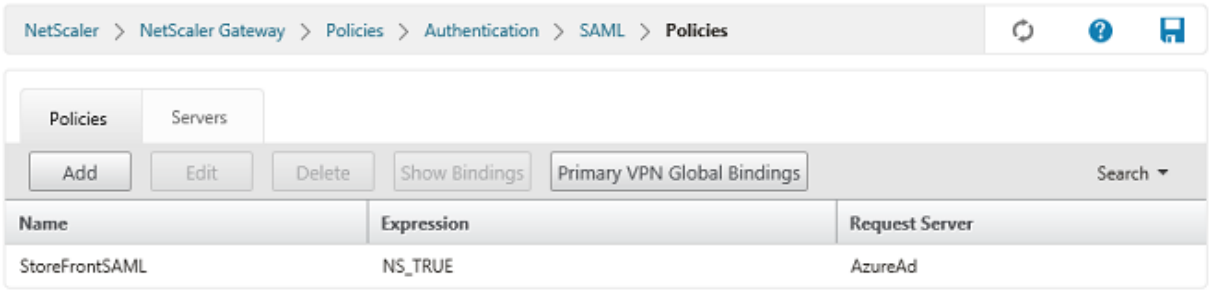
Single sign-out Url [Single Logout URL]

ADFS and Citrix Gateway support a "central logout" system. This is a URL that Citrix Gateway polls occasionally to check that the SAML authentication XML blob still represents a currently logged-on session.

This is an optional feature that does not need to be configured. It is usually an `https://` address in the form `https://adfs.mycompany.com/adfs/logout`. (Note that it can be the same as the Single Logon URL.)

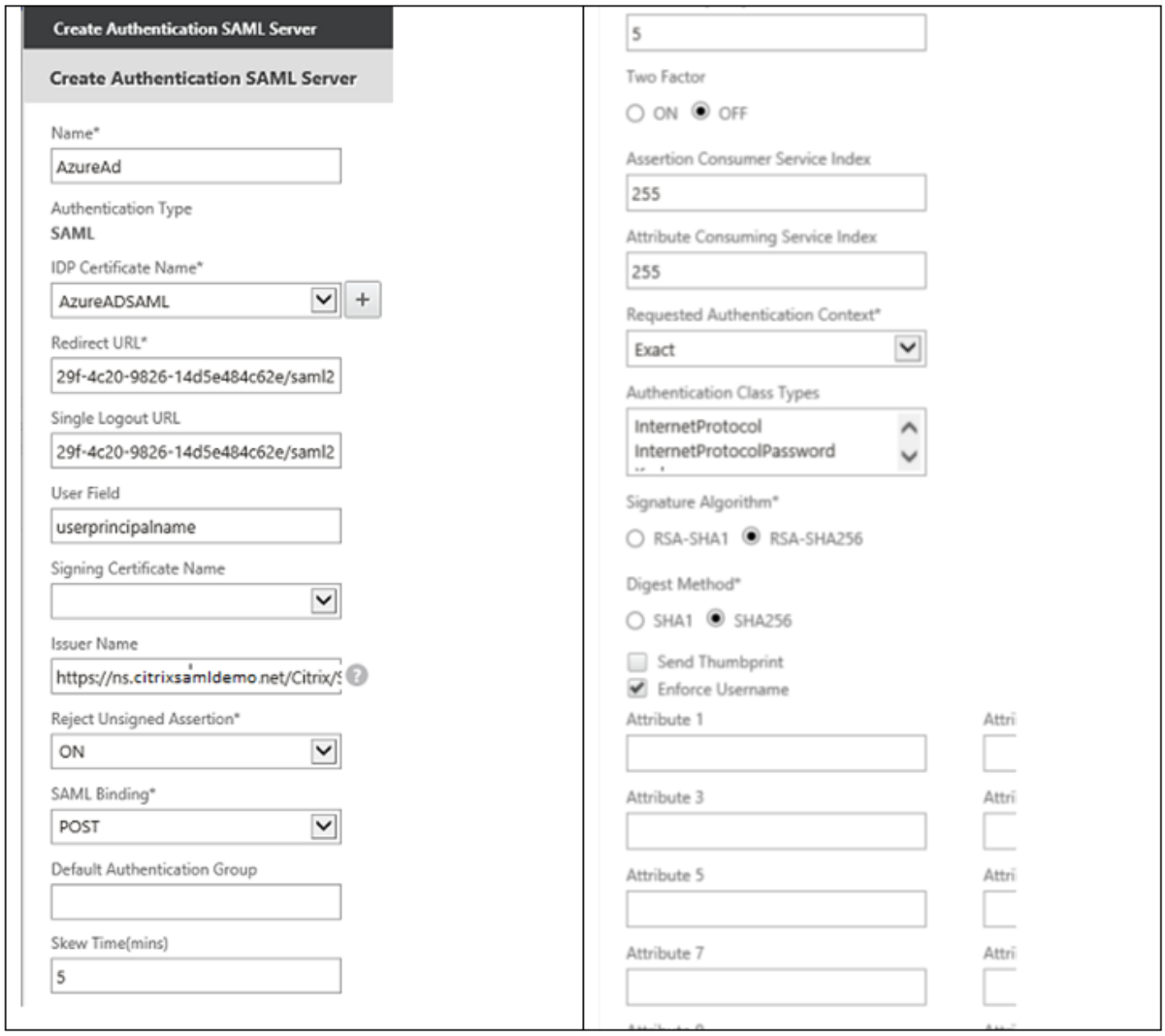
Configuration

The section Citrix Gateway deployment describes how to set up Citrix Gateway to handle standard LDAP authentication options. After that completes successfully, you can create a new authentication policy on Citrix Gateway that allows SAML authentication. This can then replace the default LDAP policy used by the Citrix Gateway wizard.



Fill in the SAML policy

Configure the new SAML IdP server using information taken from the ADFS management console earlier. When this policy is applied, Citrix Gateway redirects the user to ADFS for logon, and accepts an ADFS-signed SAML authentication token in return.



Related information

- Install and configure is the primary reference for FAS installation and configuration.
- The common FAS deployments are summarized in the Deployment architectures article.
- “How-to” articles are introduced in the Advanced configuration article.

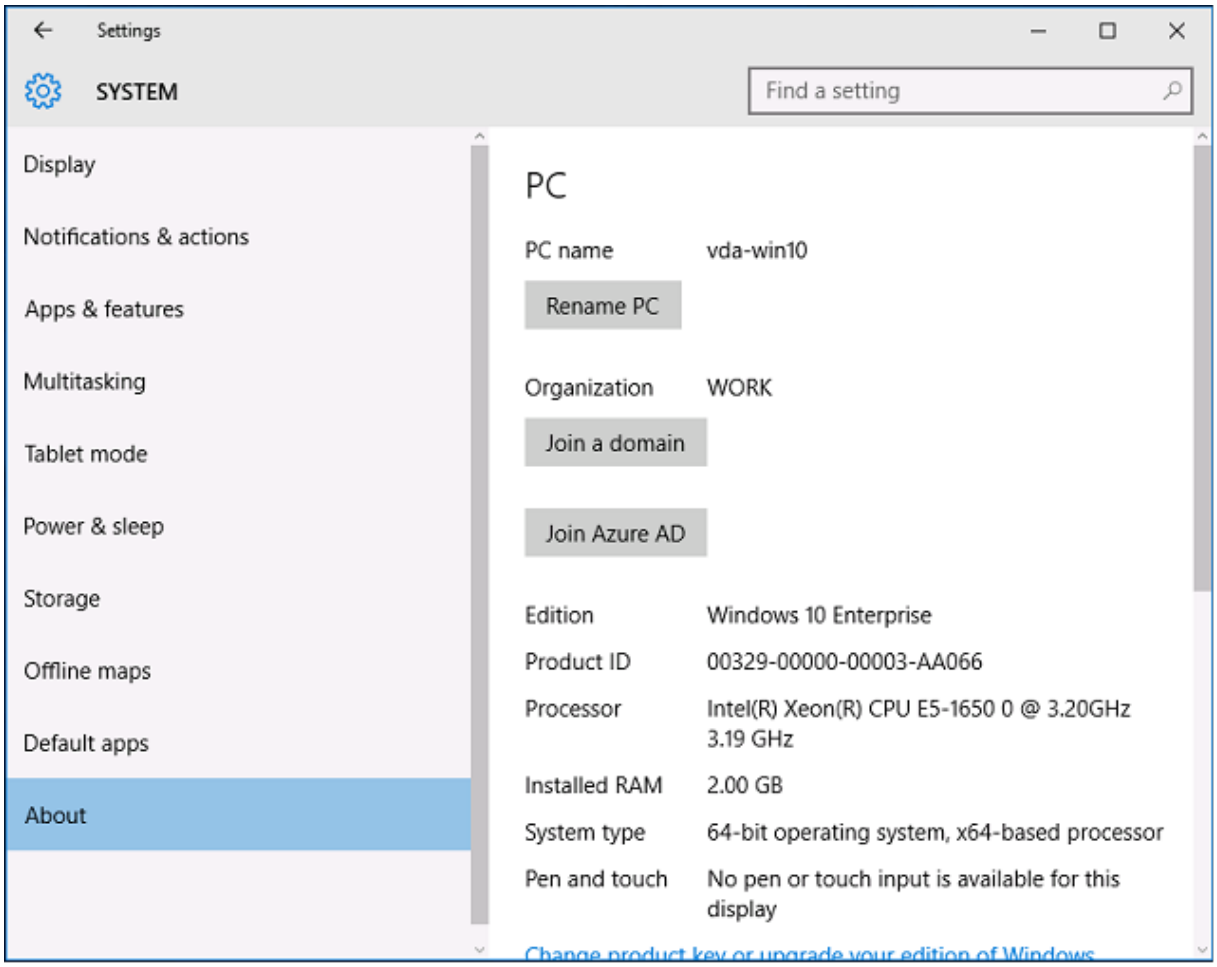
Azure AD integration

July 9, 2020

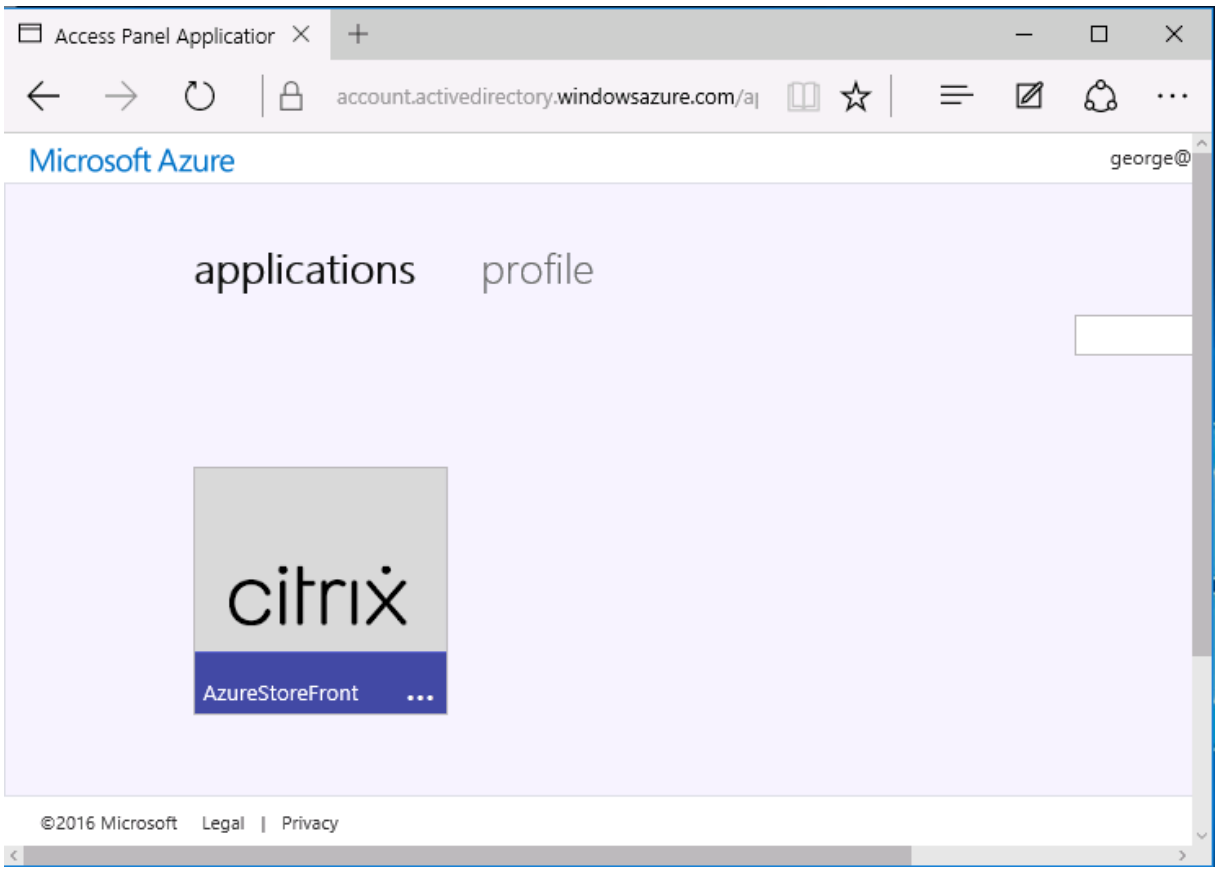
Introduction

This document describes how to integrate a Citrix environment with the Windows 10 Azure AD feature. Windows 10 introduced Azure AD, which is a new domain join model where roaming laptops can be joined to a corporate domain over the Internet for the purposes of management and single sign-on.

The example deployment in this document describes a system where IT provides new users with a corporate email address and enrollment code for their personal Windows 10 laptops. Users access this code through the **System > About > Join Azure AD** option in the **Settings** panel.



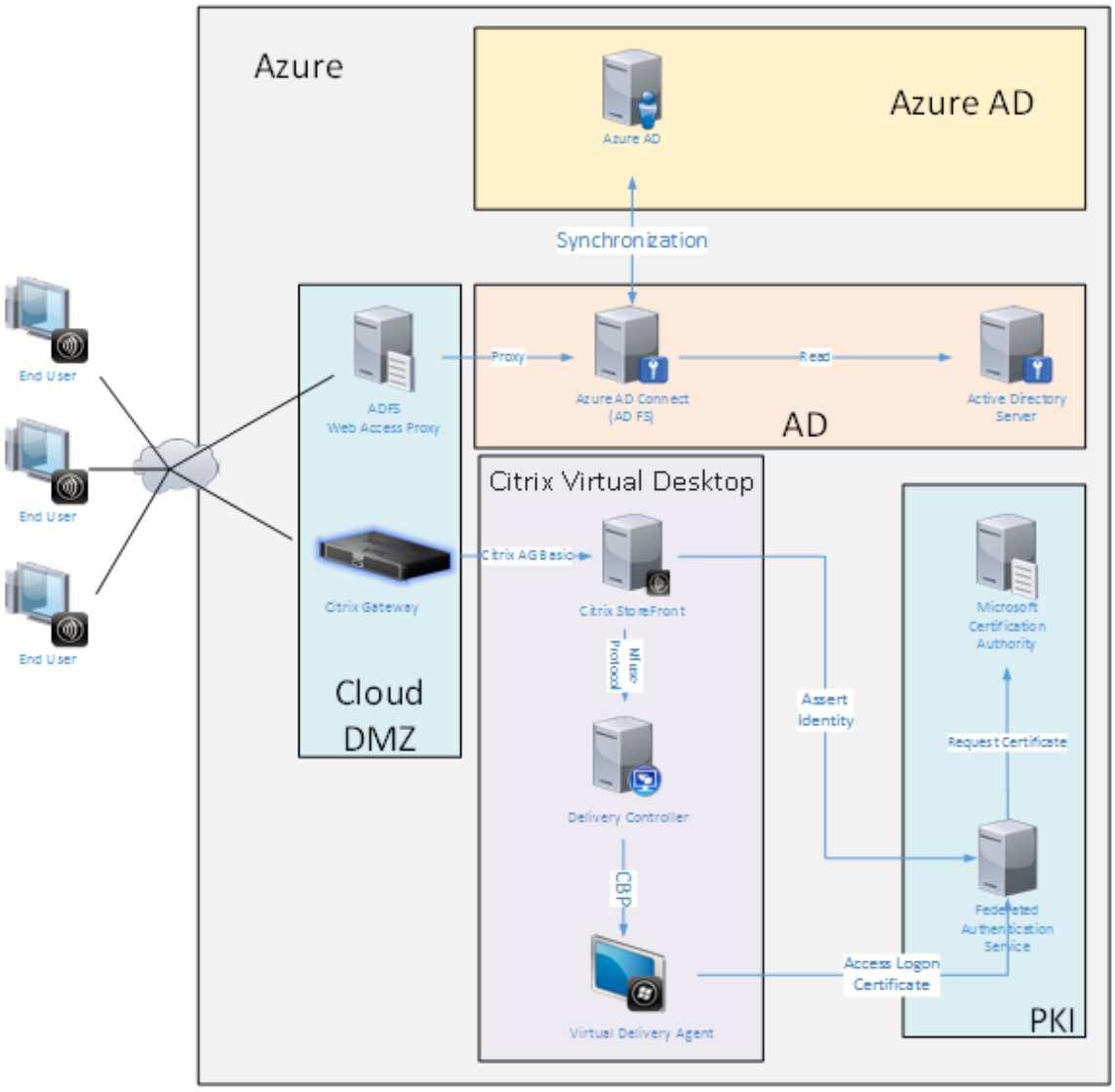
After the laptop is enrolled, the Microsoft Edge web browser automatically signs on to company web sites and Citrix published applications through the Azure SaaS applications web page, with other Azure applications such as Office 365.



Architecture

This architecture replicates a traditional company network completely within Azure, integrating with modern cloud technologies such as Azure AD and Office 365. End users are all considered remote workers, with no concept of being on an office intranet.

The model can be applied to companies with existing on premises systems, because the Azure AD Connect Synchronization can bridge to Azure over the Internet.



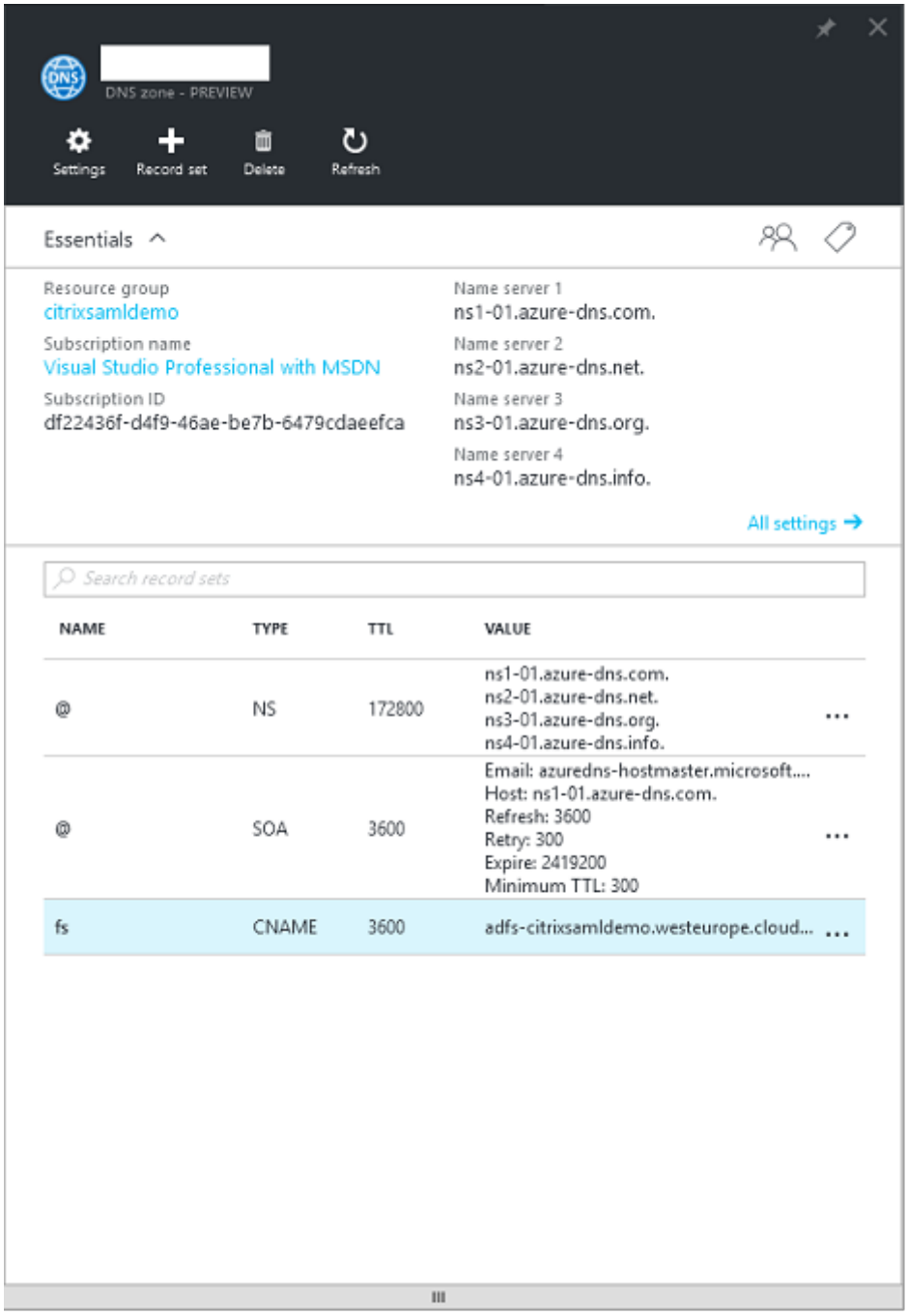
Secure connections and single sign-on, which would traditionally have been firewalled-LAN and Kerberos/NTLM authentication, are replaced in this architecture by TLS connections to Azure and SAML. New services are built as Azure applications joined to Azure AD. Existing applications that require Active Directory (such as a SQL Server database) can be run using a standard Active Directory Server VM in the IAAS portion of the Azure Cloud Service.

When a user launches a traditional application, they are accessed using Citrix Virtual Apps and Desktops published applications. The different types of applications are collated through the user's **Azure Applications** page, using the Microsoft Edge Single sign-on features. Microsoft also supplies Android and iOS apps that can enumerate and launch Azure applications.

Create a DNS zone

Azure AD requires that the administrator has registered a public DNS address and controls the delegation zone for the domain name suffix. To do this, the administrator can use the Azure DNS zone feature.

This example uses the DNS zone name *citrixsamldemo.net*.



The console shows the names of the Azure DNS name servers. These should be referenced in the DNS registrar's NS entries for the zone (for example, `citrixsamldemo.net. NS n1-01.azure-dns.`

com)

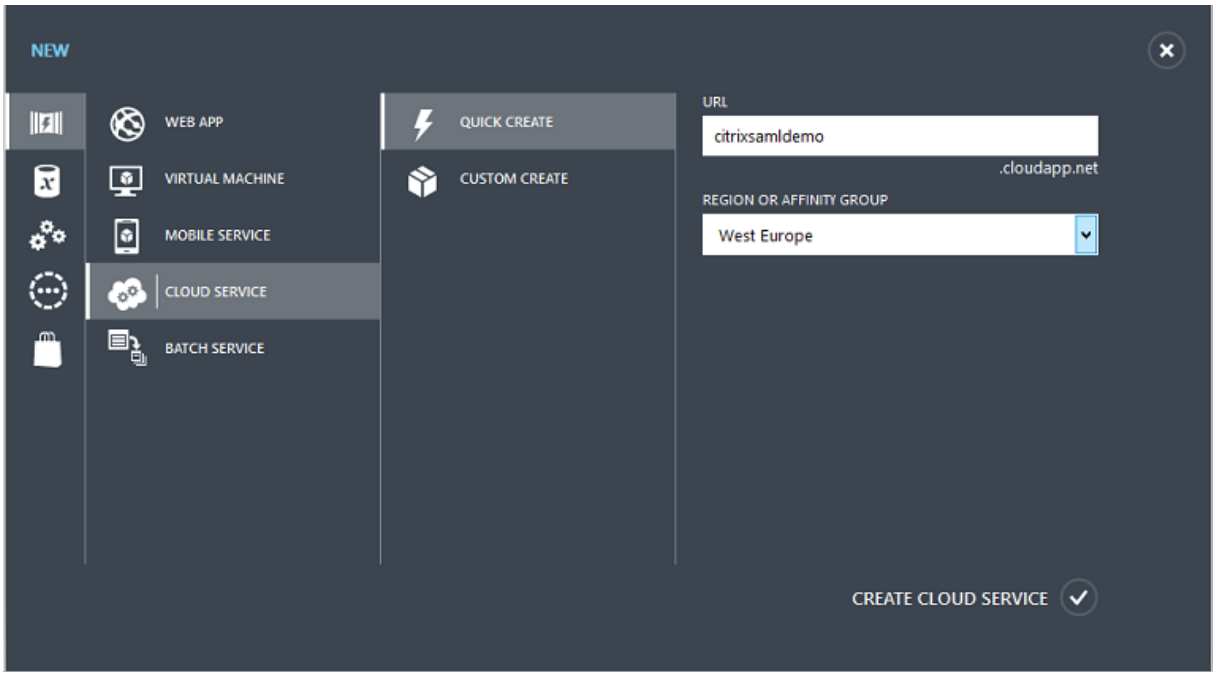
When adding references to VMs running in Azure, it is easiest to use a CNAME pointer to the Azure-managed DNS record for the VM. If the IP address of the VM changes, you will not need to manually update the DNS zone file.

Both internal and external DNS address suffixes will match for this deployment. The domain is citrixsamldemo.net, and uses a split DNS (10.0.0.* internally).

Add an “fs.citrixsamldemo.net” entry that references the Web Application Proxy server. This is the Federation Service for this zone.

Create a Cloud Service

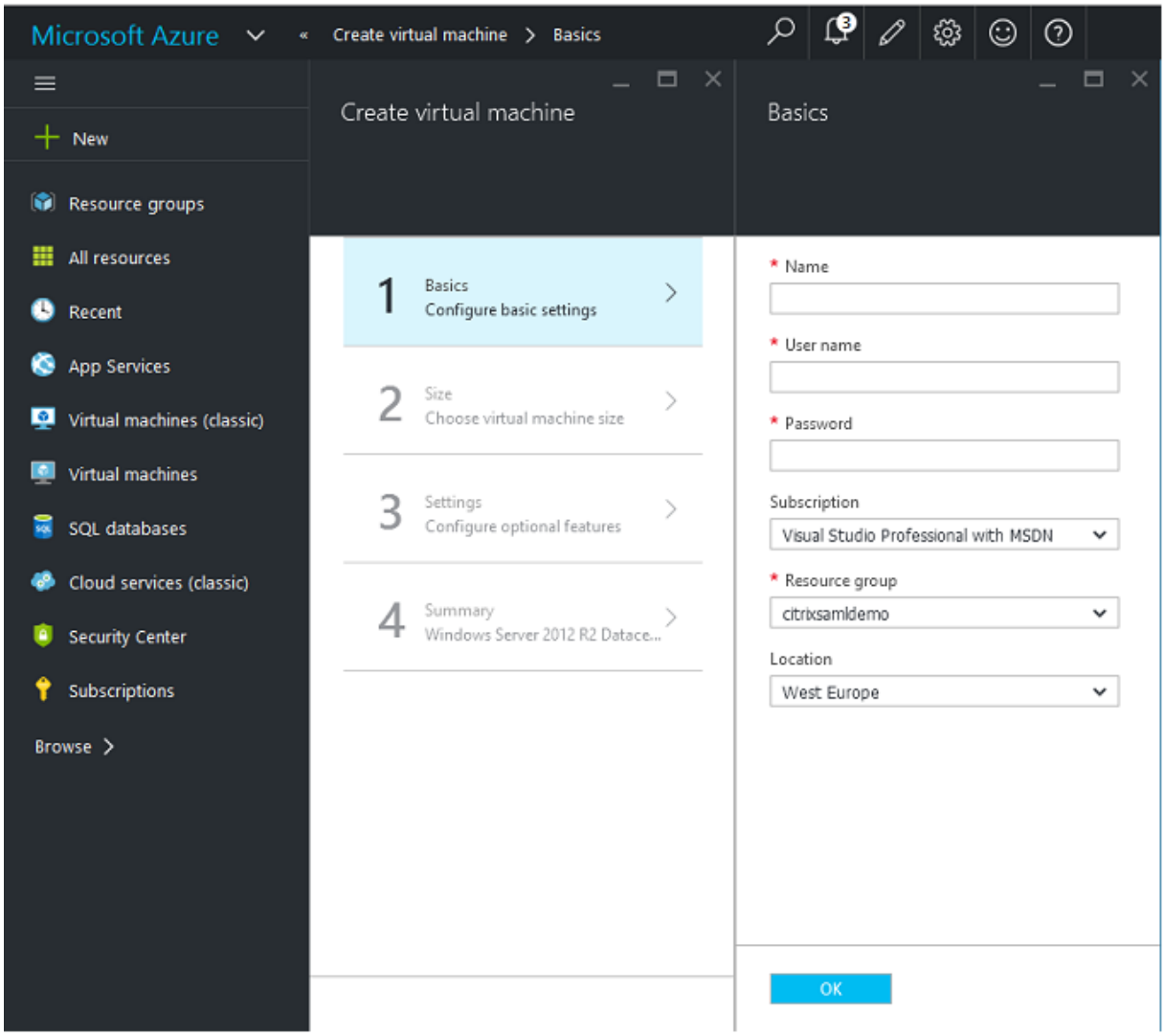
This example configures a Citrix environment, including an AD environment with an ADFS server running in Azure. A Cloud Service is created, named “citrixsamldemo.”



Create Windows virtual machines

Create five Windows VMs running in the Cloud Service:

- Domain controller (domaincontrol)
- Azure Connect ADFS server (adfs)
- ADFS web access proxy (Web Application Proxy, not domain joined)
- Citrix Virtual Apps and Desktops Delivery Controller
- Citrix Virtual Apps and Desktops Virtual Delivery Agent (VDA)



Domain Controller

- Add the **DNS Server** and **Active Directory Domain Services** roles to create a standard Active Directory deployment (in this example, citrixsamldemo. net). After domain promotion completes, add the **Active Directory Certification Services** role.
- Create a normal user account for testing (for example, George@citrixsamldemo.net).
- Since this server will be running internal DNS, all servers should refer to this server for DNS resolution. This can be done through the **Azure DNS settings** page. (For more information, see the Appendix in this document.)

ADFS controller and Web Application Proxy server

- Join the ADFS server to the citrixsamldemo domain. The Web Application Proxy server should remain in an isolated workgroup, so manually register a DNS address with the AD DNS.

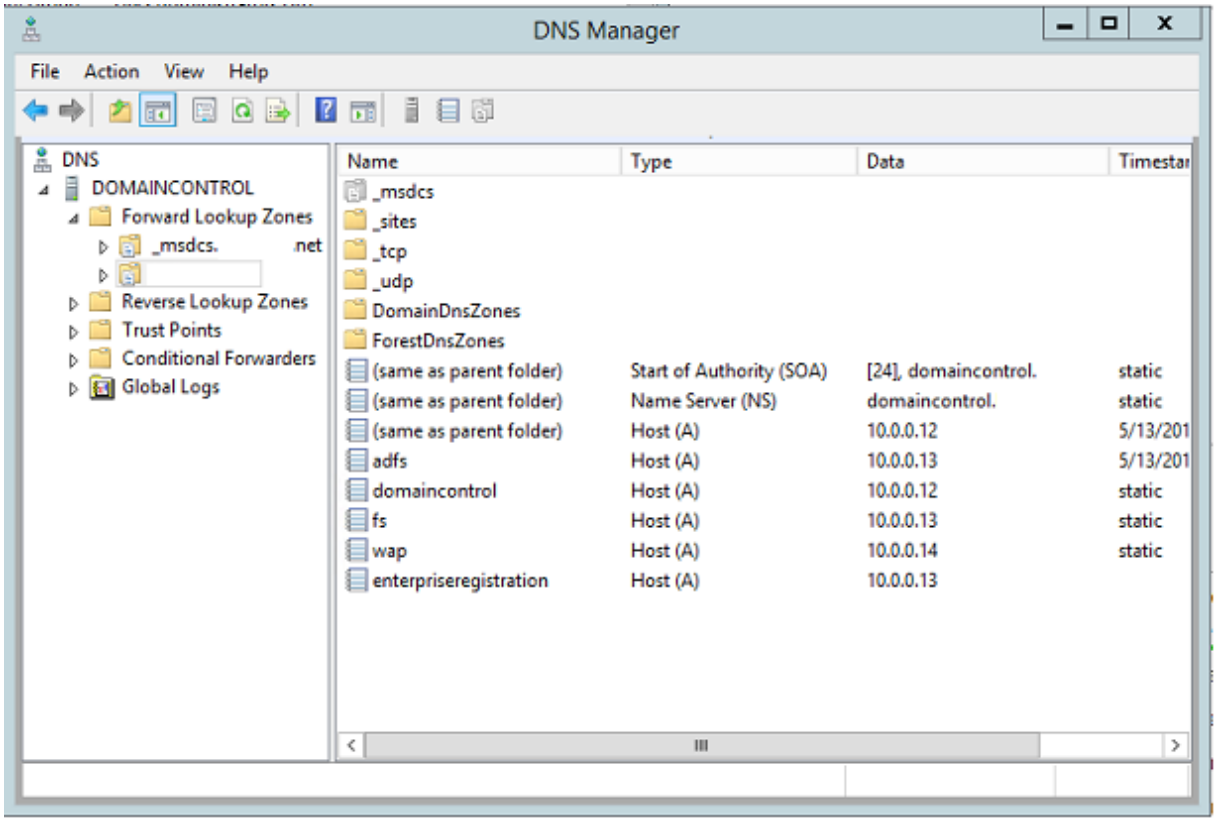
- Run the **Enable-PSRemoting –Force** cmdlet on these servers, to allow PS remoting through firewalls from the AzureAD Connect tool.

Citrix Virtual Desktops Delivery Controller and VDA

- Install the Citrix Virtual Apps or Citrix Virtual Desktops Delivery Controller and VDA on the remaining two Windows servers joined to citrixsamldemo.

Configure an internal DNS

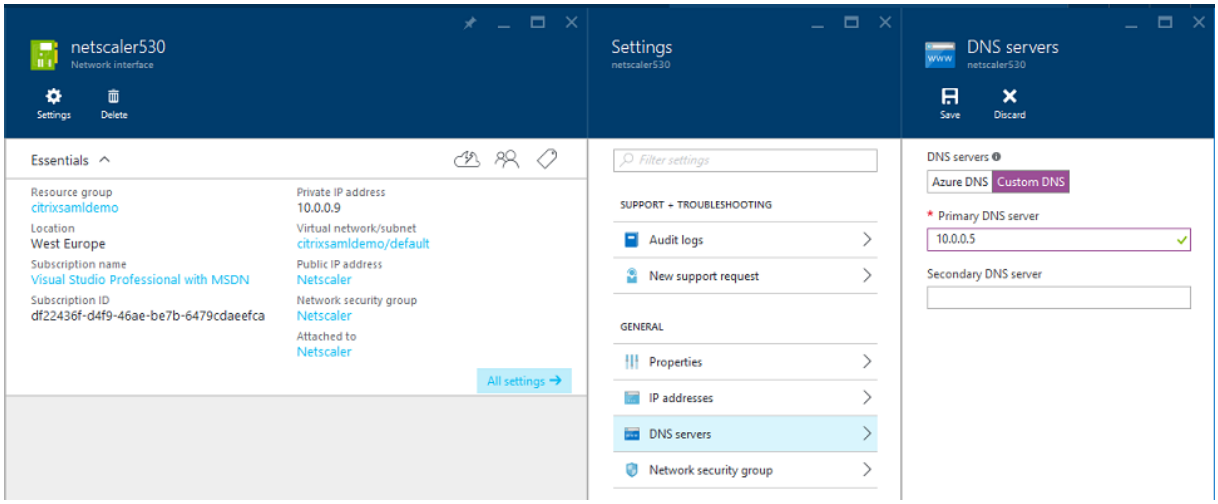
After the domain controller is installed, configure the DNS server to handle the internal view of citrixsamldemo.net, and act as a forwarder to an external DNS server (for example: 8.8.8.8).



Add a static record for:

- wap.citrixsamldemo.net [the Web Application Proxy VM will not be domain joined]
- fs.citrixsamldemo.net [internal federation server address]
- enterpriseregistration.citrixsaml.net [same as fs.citrixsamldemo.net]

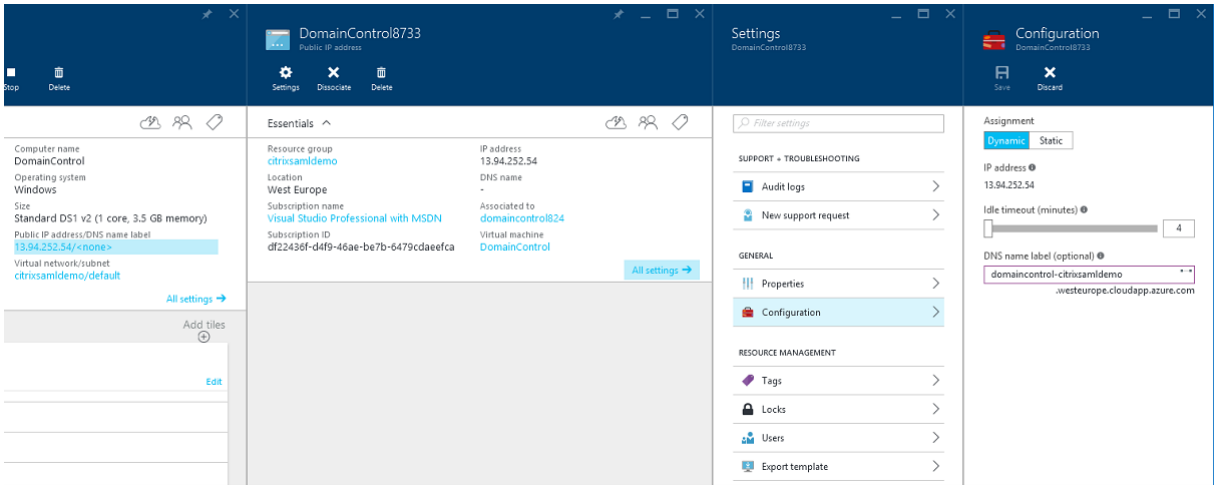
All VMs running in Azure should be configured to use only this DNS server. You can do this through the Network Interface GUI.



By default, the internal IP (10.0.0.9) address is dynamically allocated. You can use the IP addresses setting to permanently assign the IP address. This should be done for the Web Application Proxy server and the domain controller.

Configure an external DNS address

When a VM is running, Azure maintains its own DNS zone server that points to the current public IP address assigned to the VM. This is a useful feature to enable because Azure assigns IP addresses when each VM starts, by default.

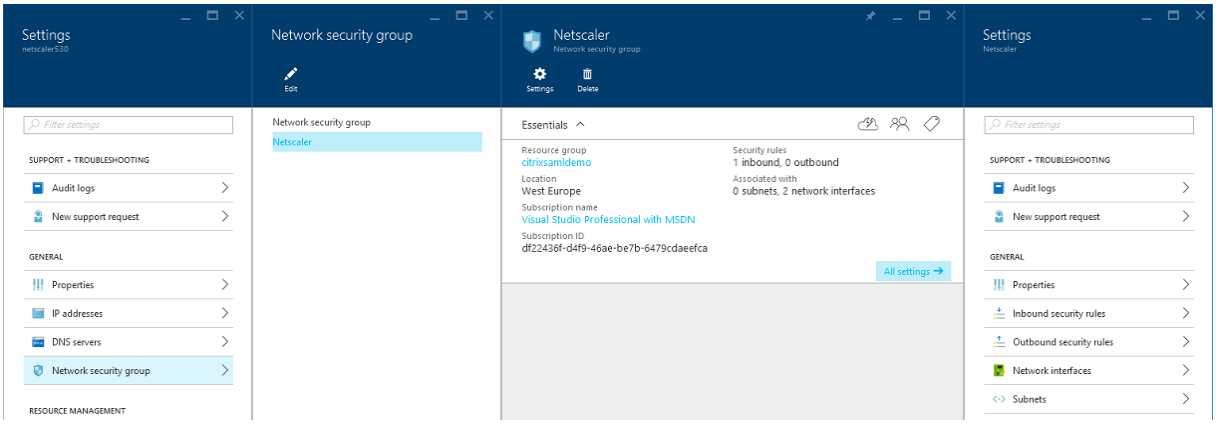


This example assigns a DNS address of domaincontrol-citrixsamldemo.westeurope.cloudapp.azure.com to the domain controller.

Note that when remote configuration is complete, only the Web Application Proxy and Citrix Gateway VMs should have public IP addresses enabled. (During configuration, the public IP address is used for RDP access to the environment).

Configure security groups

The Azure cloud manages firewall rules for TCP/UDP access into VMs from the Internet using security groups. By default, all VMs allow RDP access. The Citrix Gateway and Web Application Proxy servers should also allow TLS on port 443.

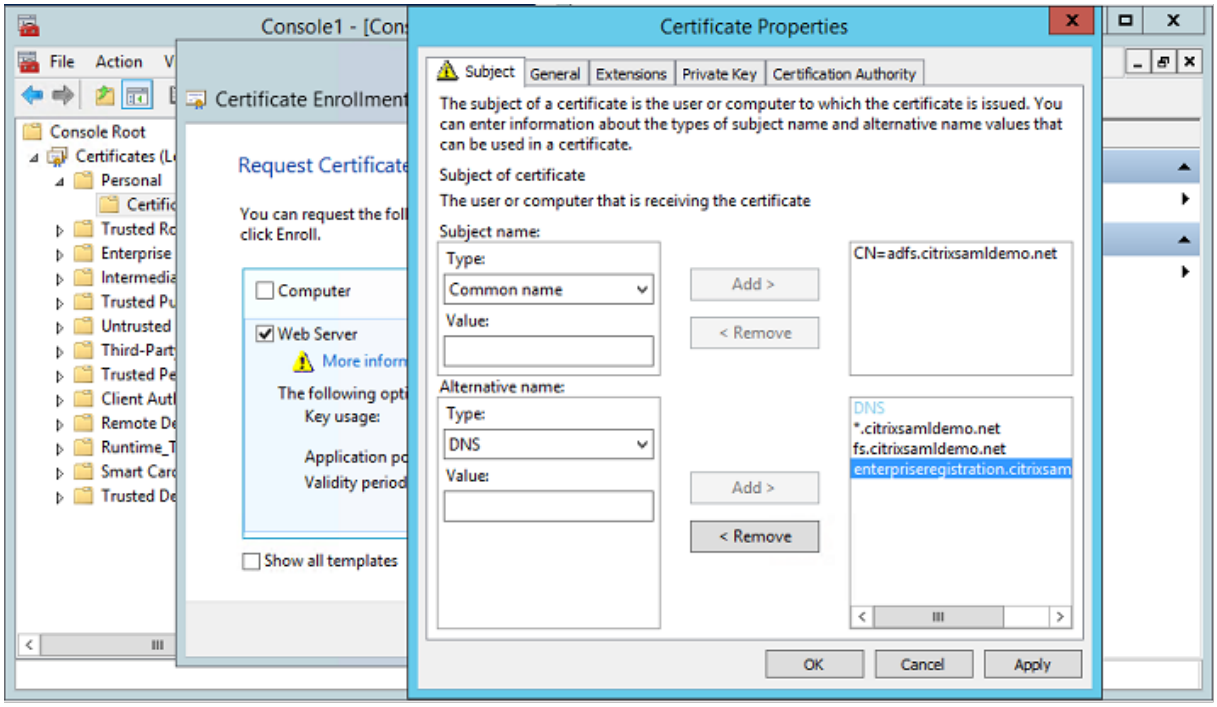


Create an ADFS certificate

Enable the **Web Server** certificate template on the Microsoft certificate authority. This allows creation of a certificate with custom DNS addresses that can be exported (including private key) to a pfx file. You must install this certificate on both the ADFS and Web Application Proxy servers, so the PFX file is the preferred option.

Issue a Web Server certificate with the following subject names:

- Commonname:
  - adfs.citrixsamldemo.net [name of computer]
- SubjectAltname:
  - *.citrixsamldemo.net [name of zone]
  - fs.citrixsamldemo. net [entry in DNS]
  - enterpriseregistration.citrixsamldemo.net



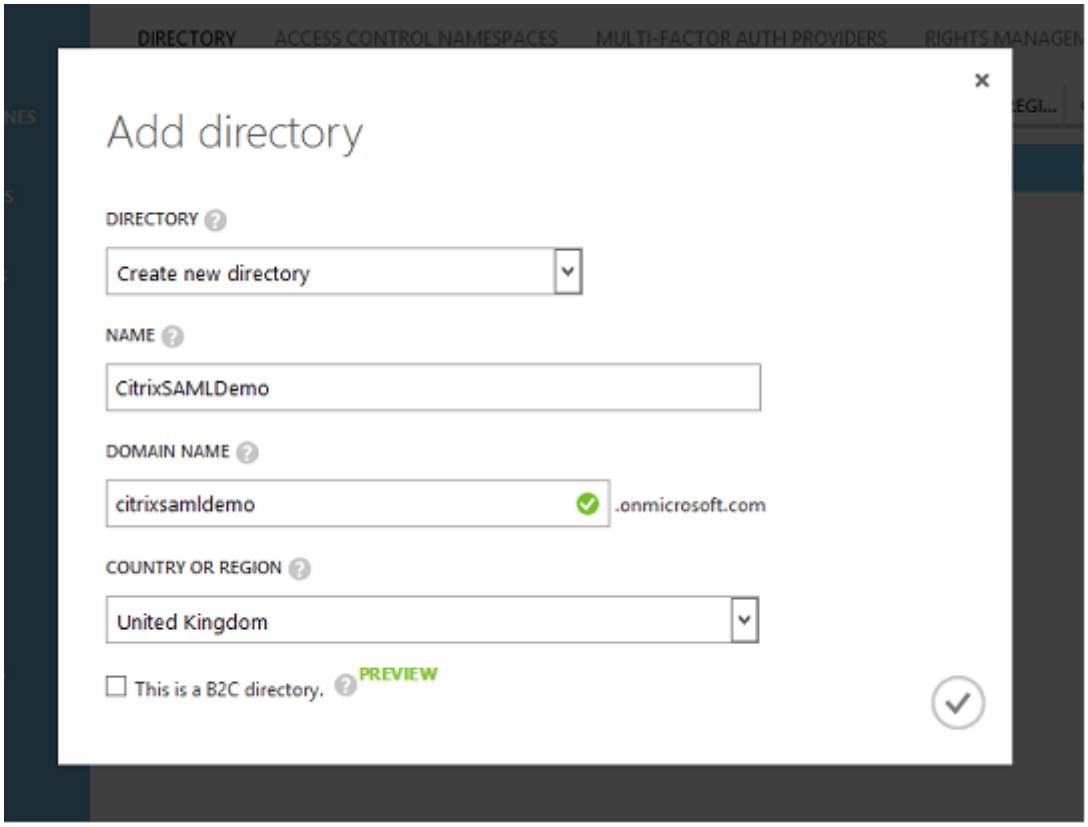
Export the certificate to a pfx file, including a password-protected private key.

Set up Azure AD

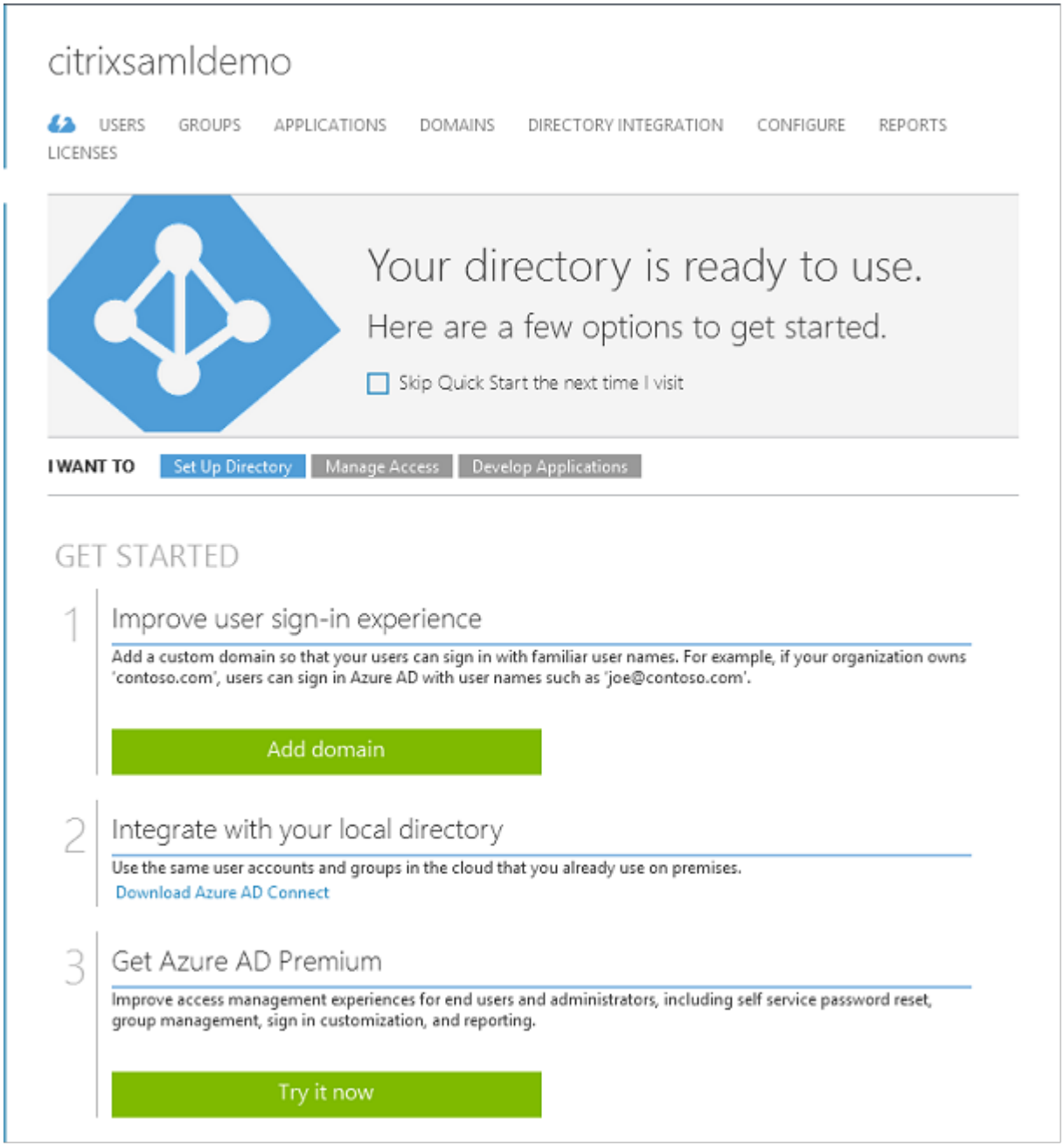
This section details the process of setting up a new Azure AD instance and creating user identities that can be used to join Windows 10 to Azure AD.

Create a new directory

Log on to the classic Azure portal and create a new directory.

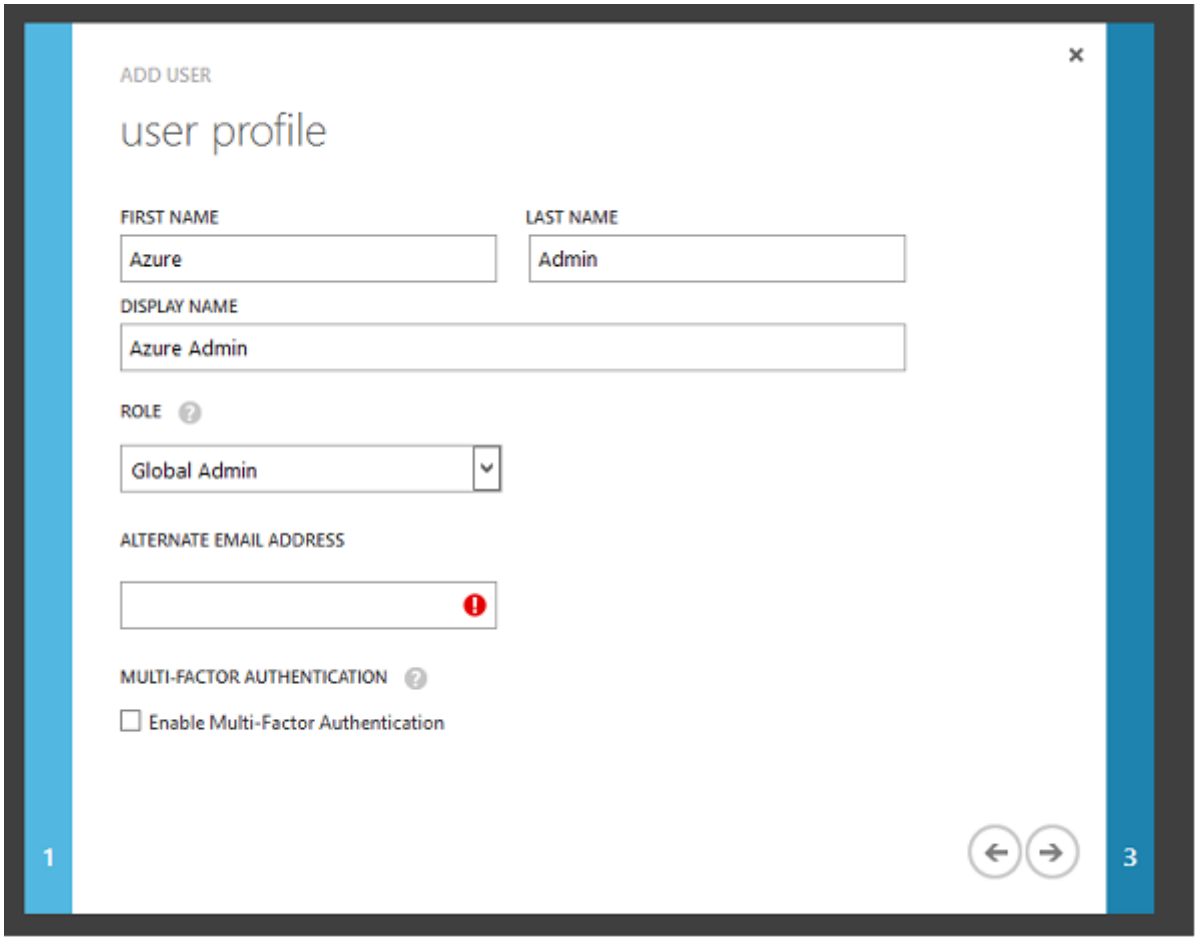


When complete, a summary page appears.



Create a global administrator user (AzureAdmin)

Create a global administrator in Azure (in this example, `AzureAdmin@citrixsamldemo.onmicrosoft.com`) and log on with the new account to set up a password.



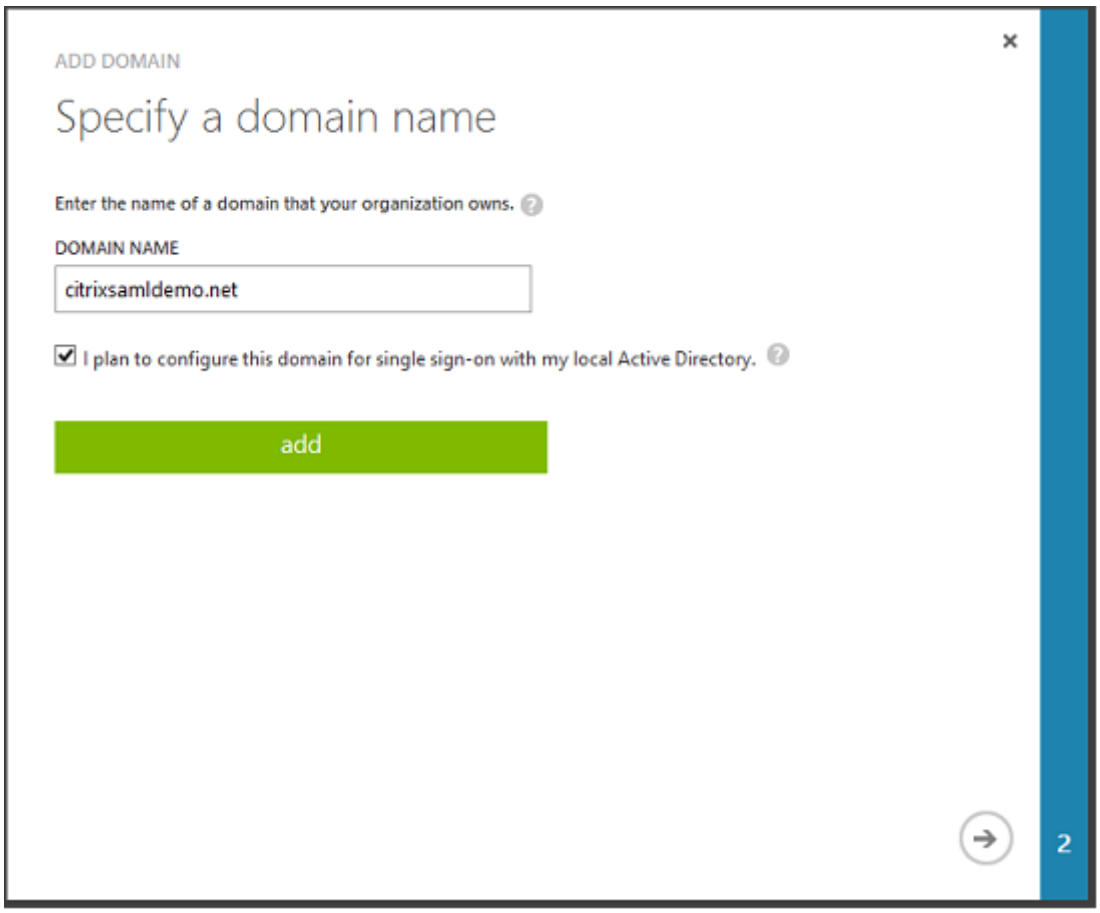
Register your domain with Azure AD

By default, users are identified with an email address in the form: `<user.name>@<company>.onmicrosoft.com`.

Although this works without further configuration, a standard format email address is better, preferably one that matches the email account of the end user: `<user.name>@<company>.com`.

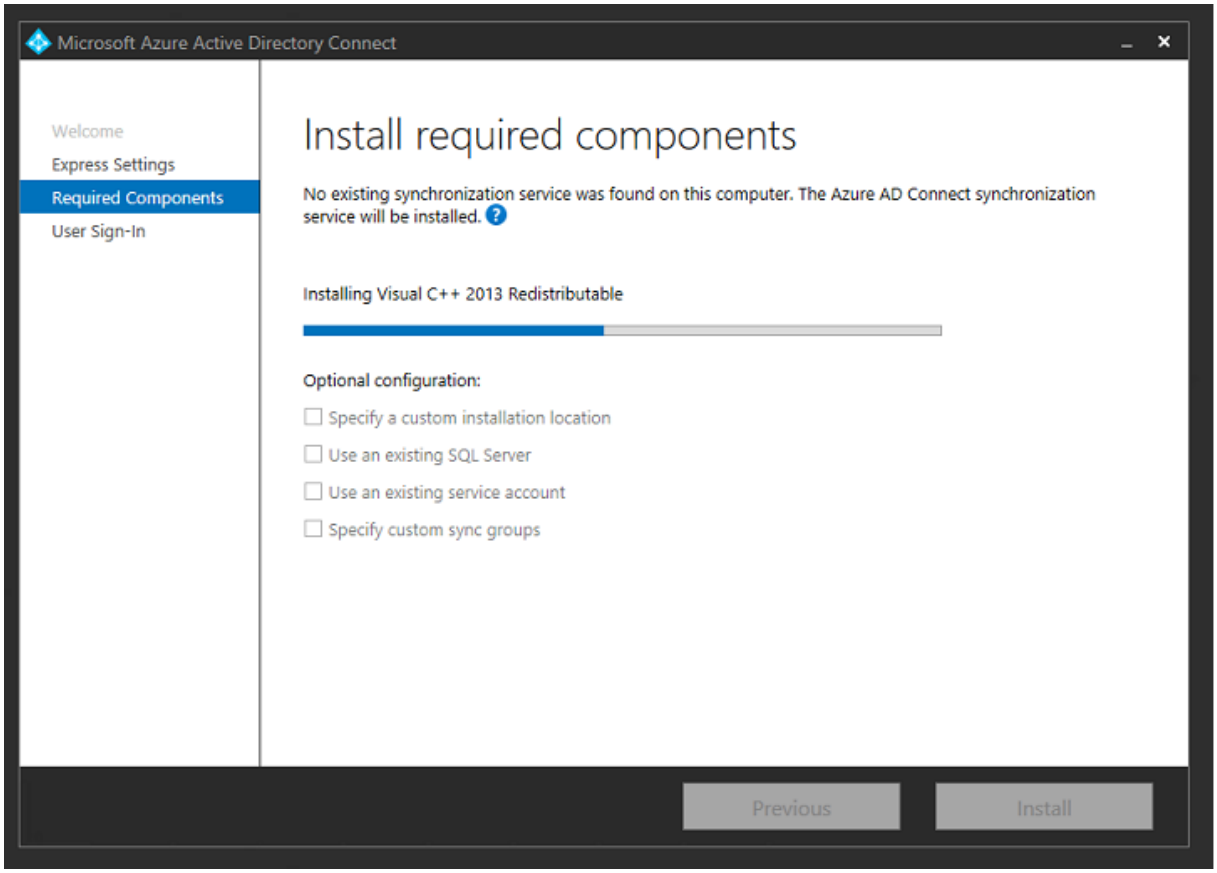
The **Add domain** action configures a redirect from your real company domain. The example uses `citrixsamldemo.net`.

If you are setting up ADFS for single sign-on, enable the check box.

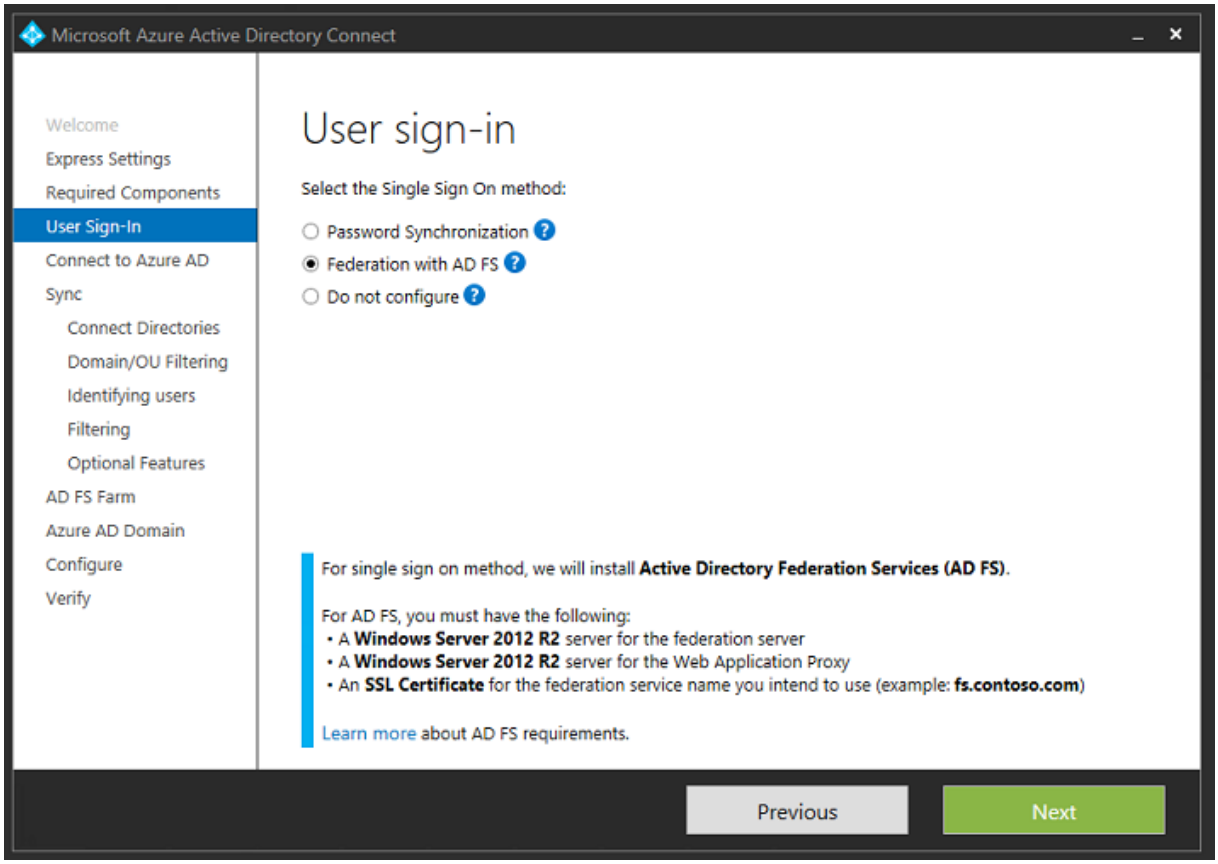


Install Azure AD Connect

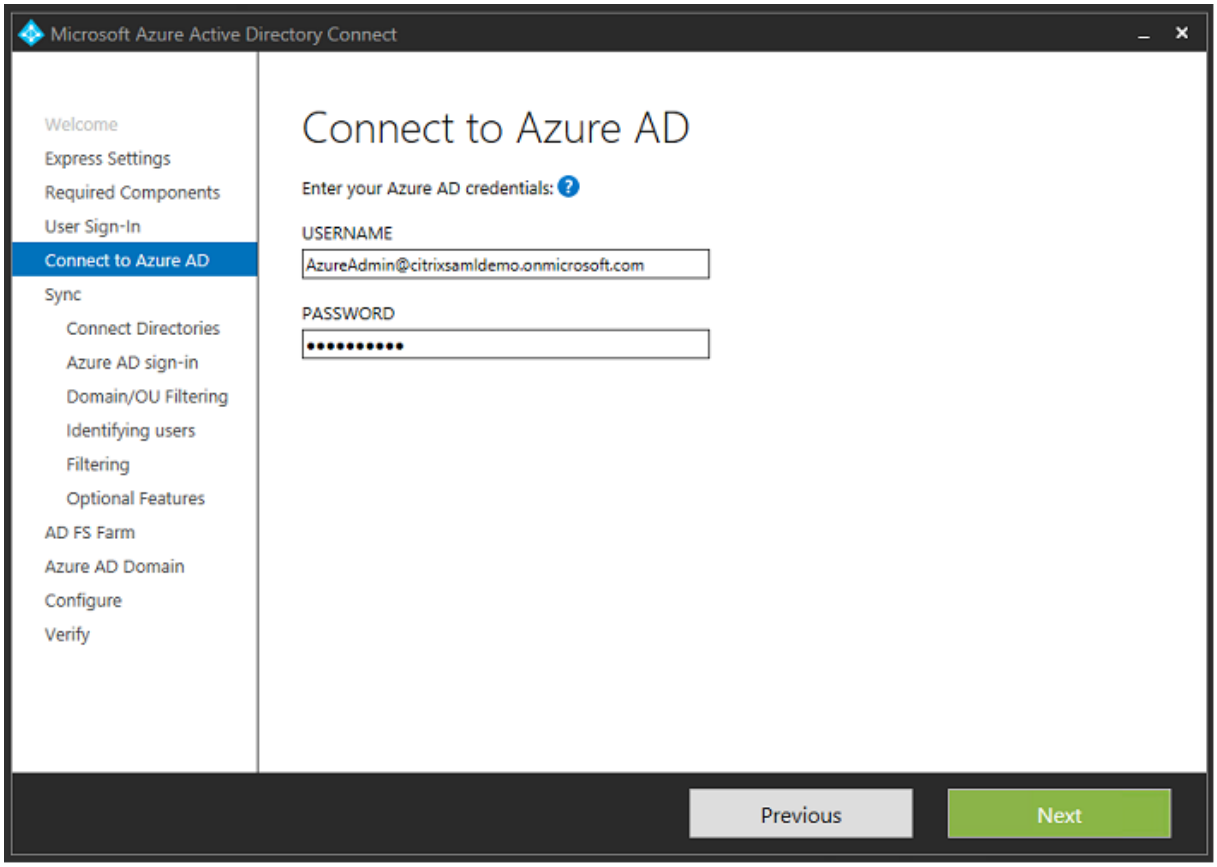
Step 2 of the Azure AD configuration GUI redirects to the Microsoft download page for Azure AD Connect. Install this on the ADFS VM. Use **Custom install**, rather than **Express Settings**, so that ADFS options are available.



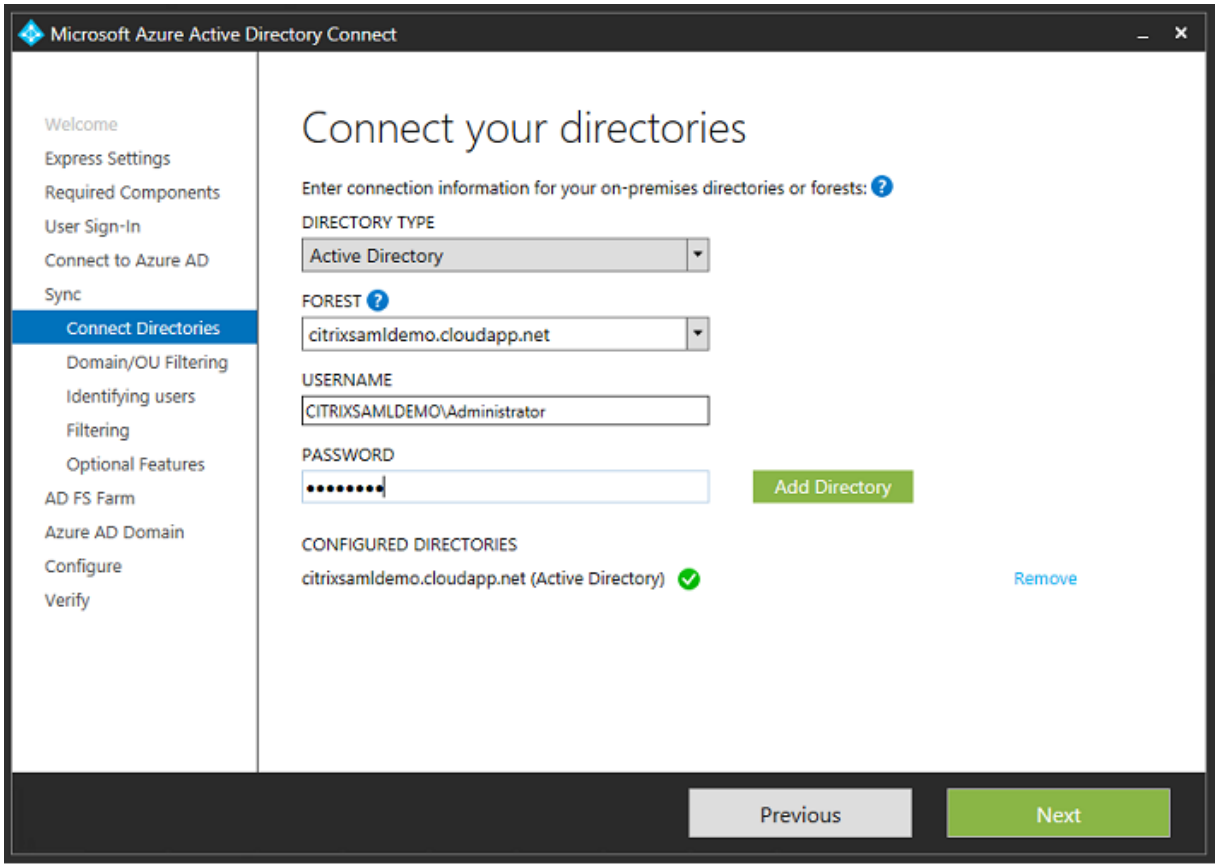
Select the **Federation with AD FS** Single sign-On option.



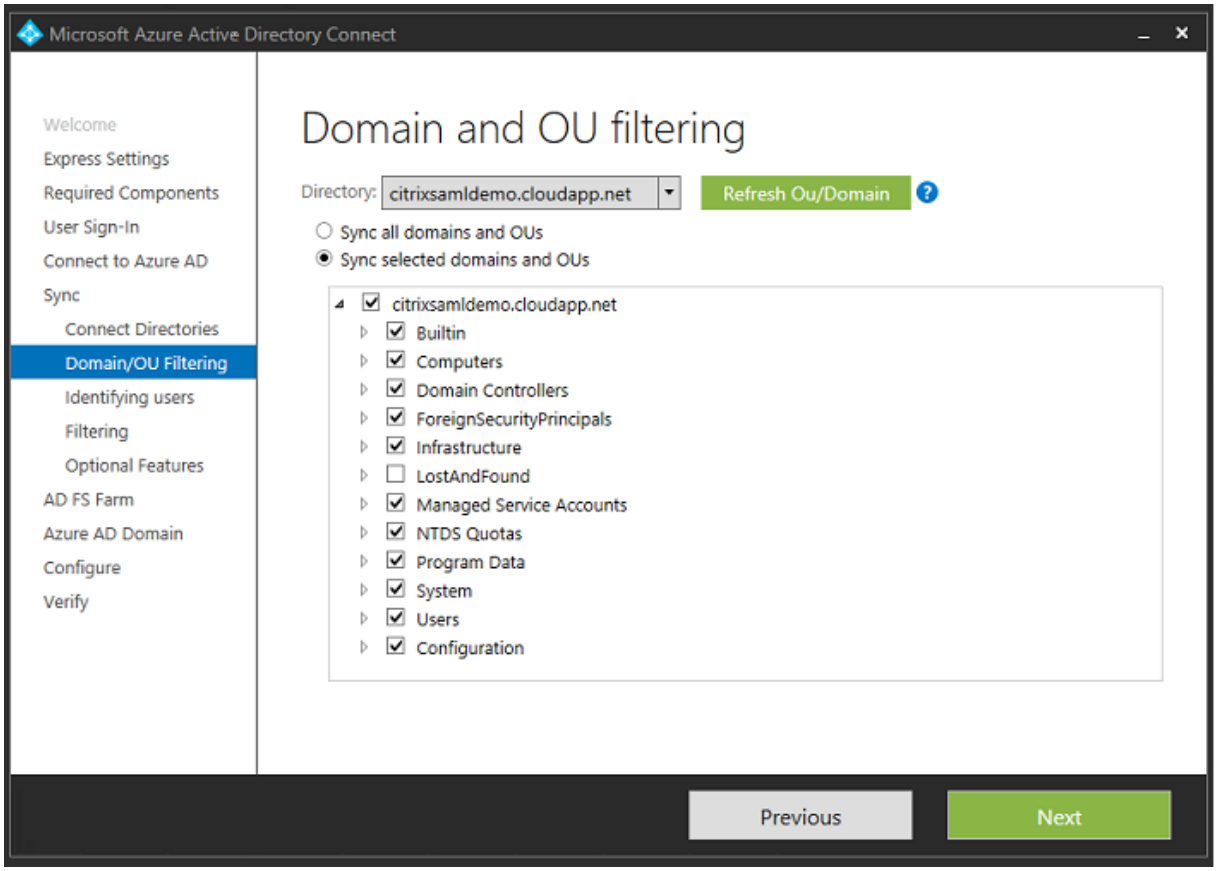
Connect to Azure with the administrator account you created earlier.



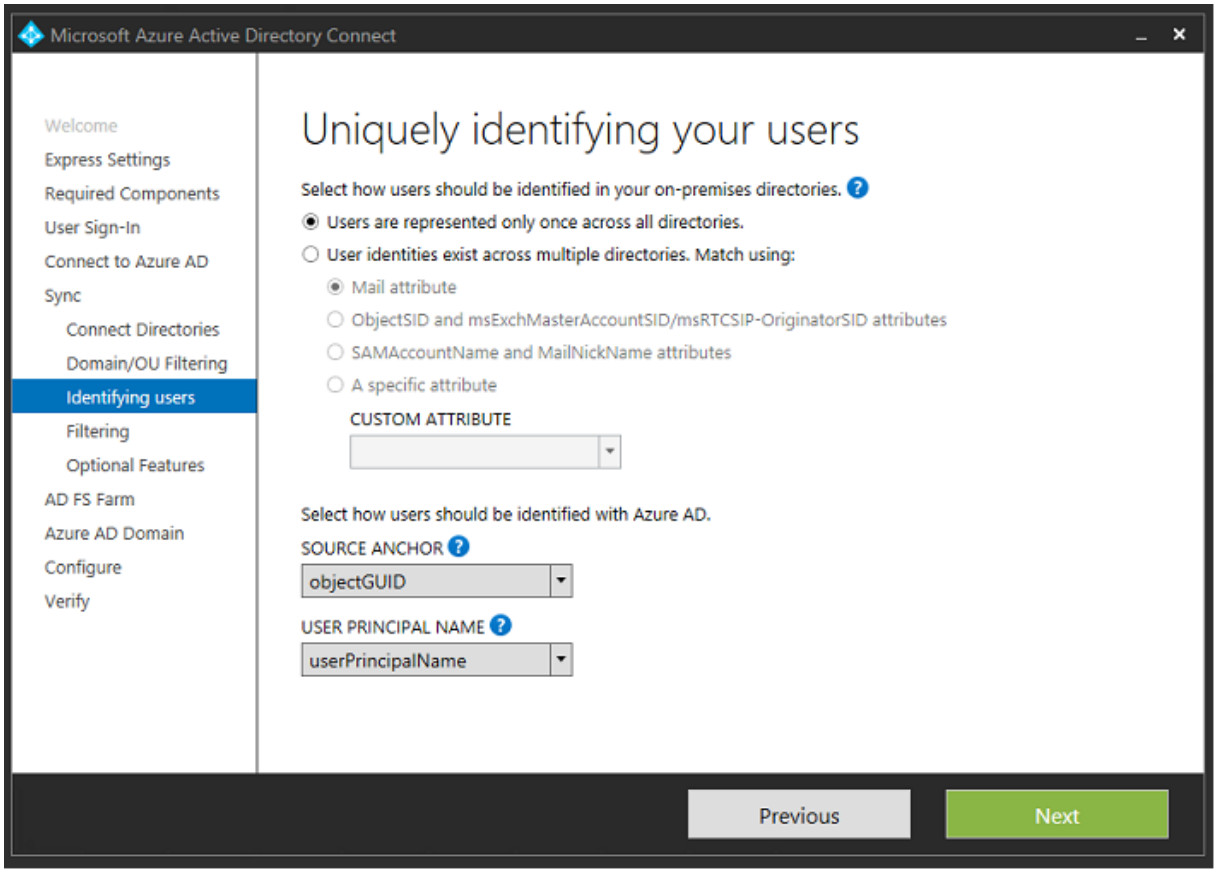
Select the internal AD forest.



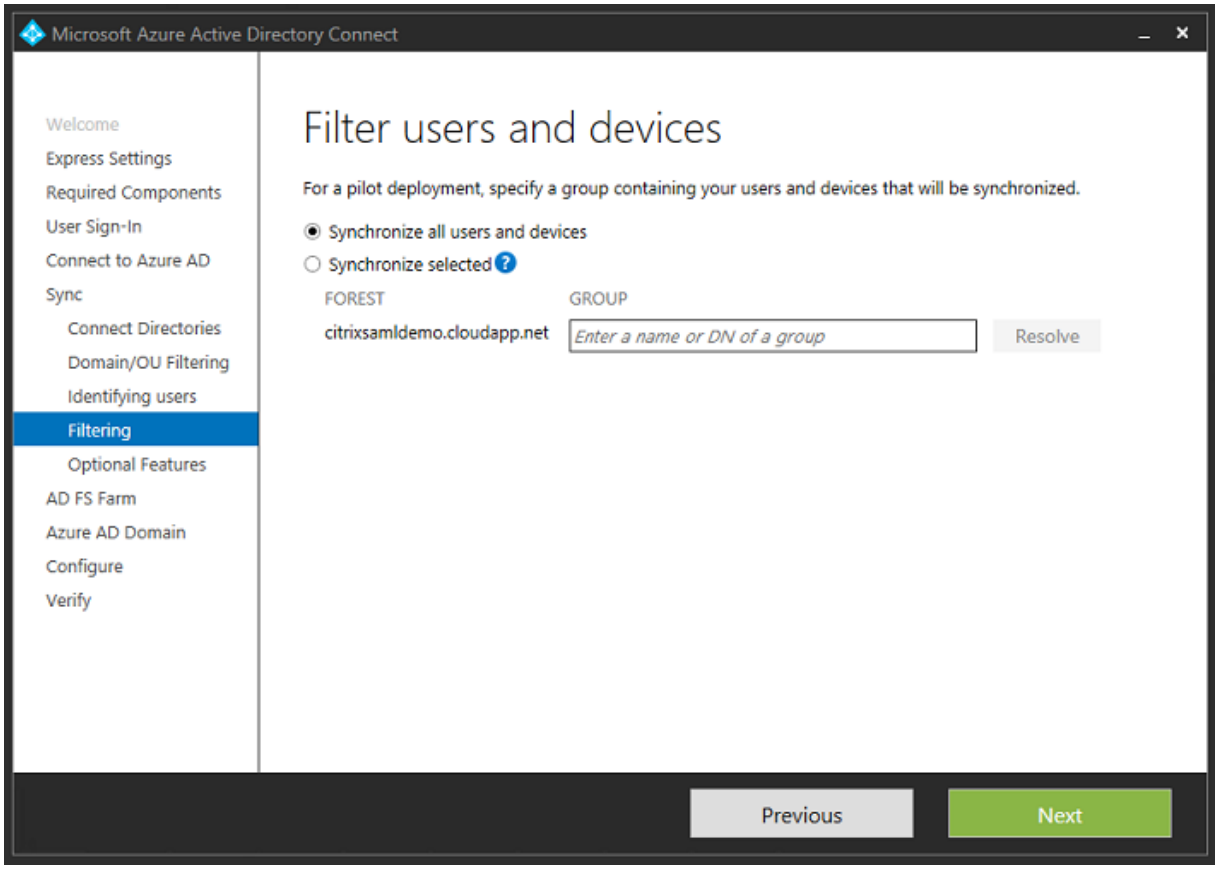
Synchronize all legacy Active Directory objects with Azure AD.



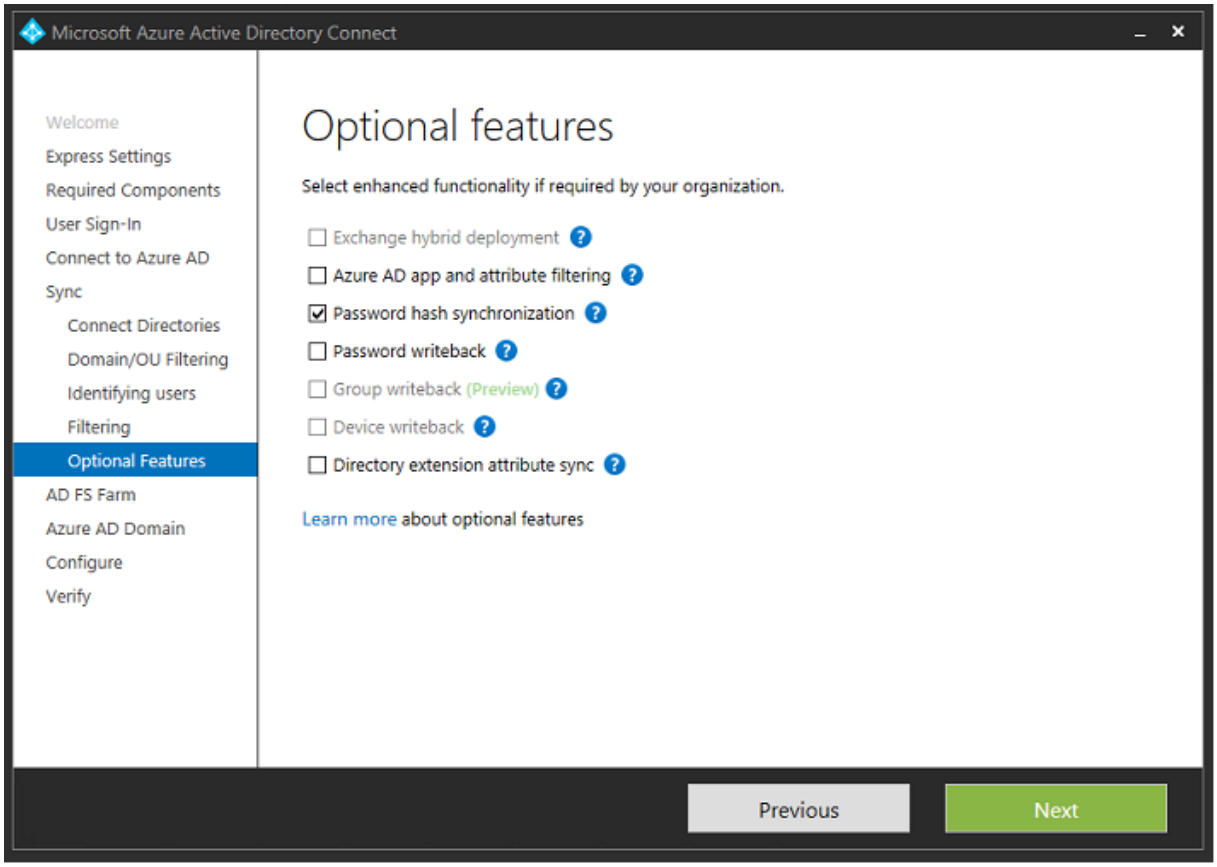
If the directory structure is simple, you can rely on the usernames being sufficiently unique to identify a user who logs on.



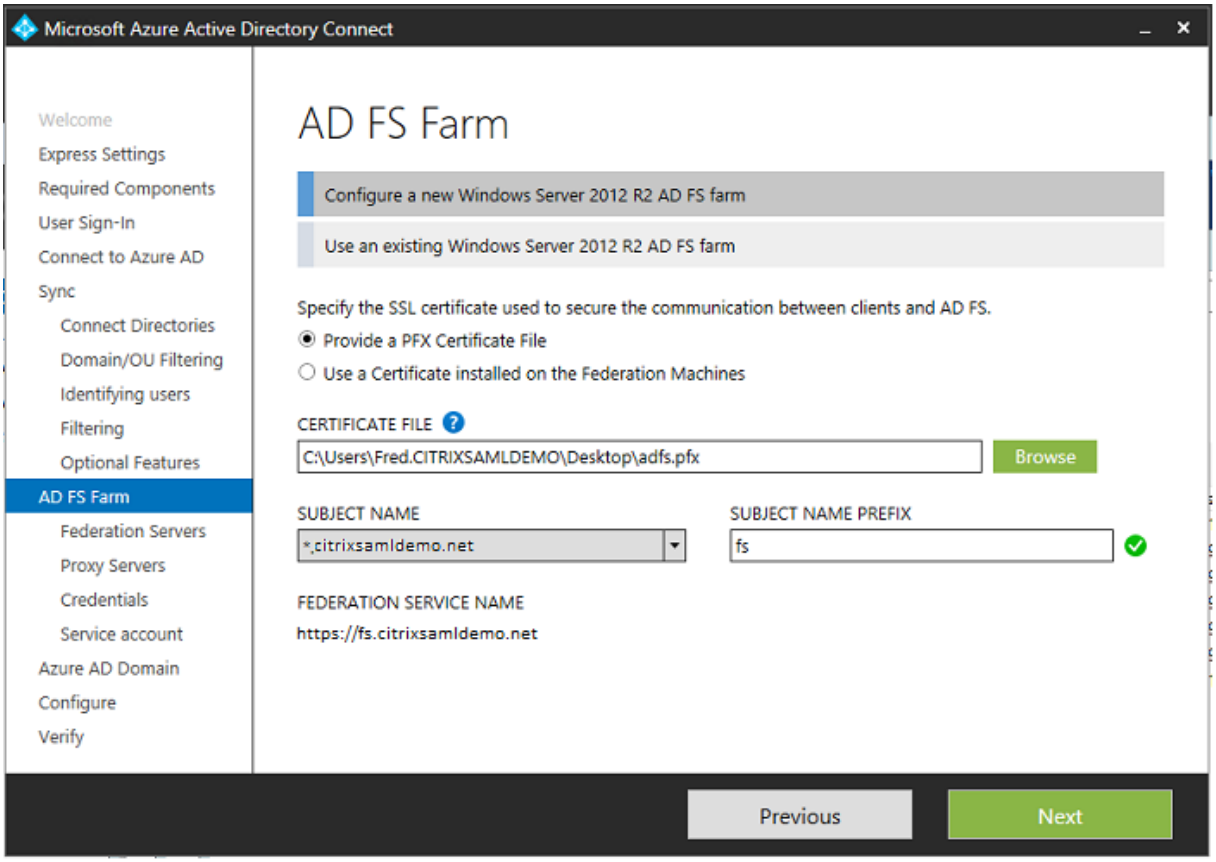
Accept the default filtering options, or restrict users and devices to a particular set of groups.



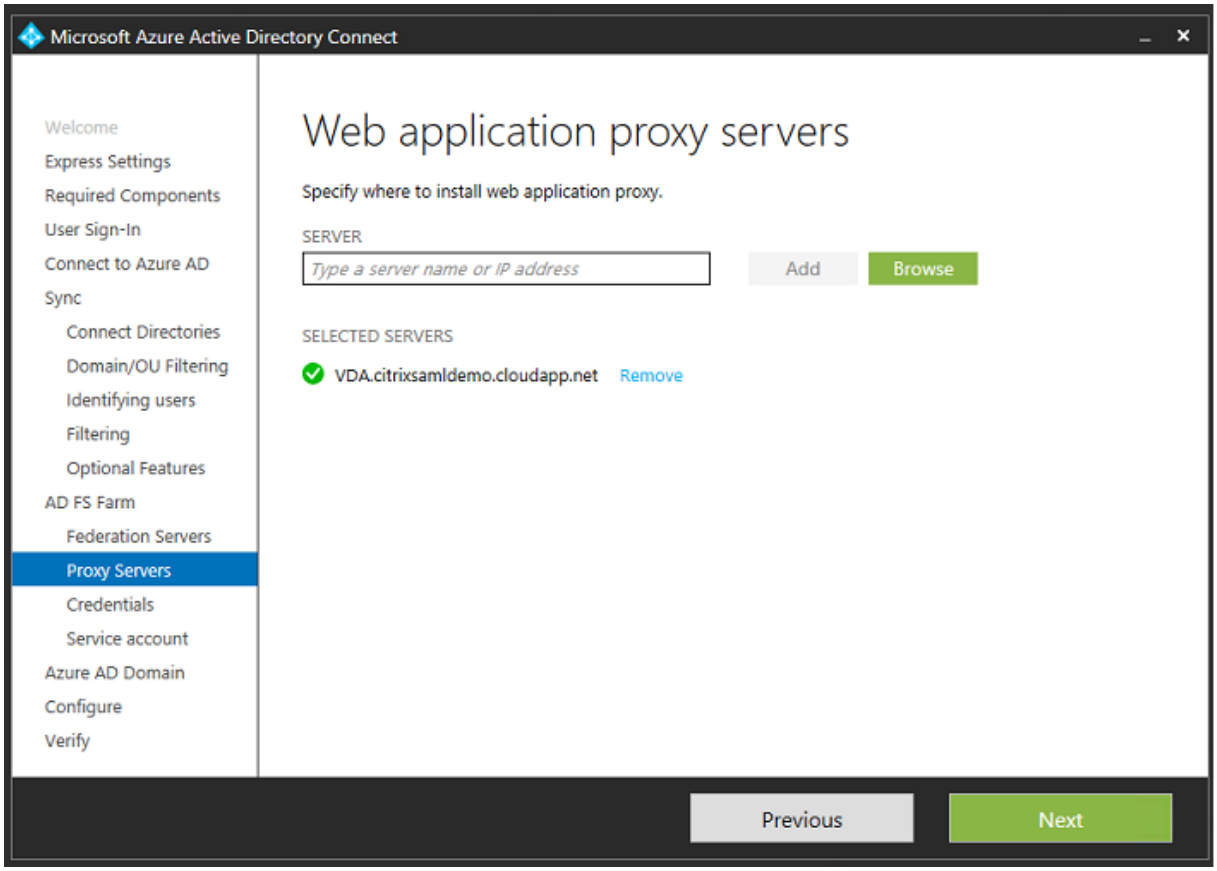
If desired, you can synchronize the Azure AD passwords with Active Directory. This is usually not required for ADFS-based authentication.



Select the certificate PFX file to use in AD FS, specifying fs.citrixsamldemo.net as the DNS name.

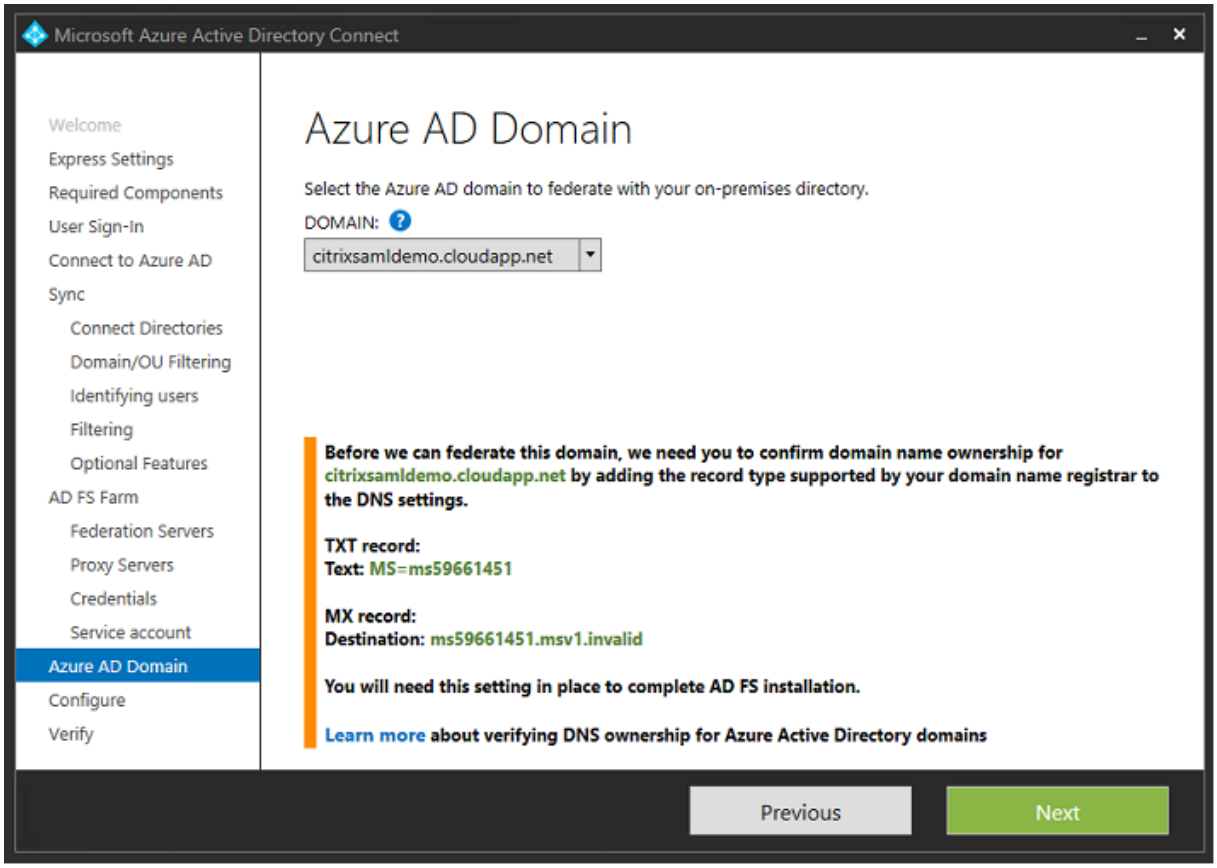


When prompted to select a proxy server, enter the address of the wap.citrixsamldemo.net server. You may need to run the **Enable-PSRemoting –Force** cmdlet as an administrator on the Web Application Proxy server, so that Azure AD Connect can configure it.

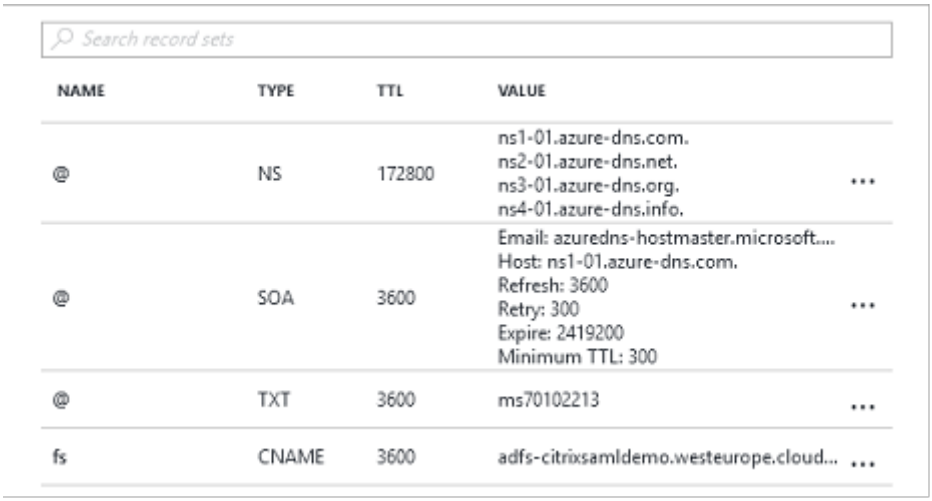


> **Note:**
>
> If this step fails due to Remote PowerShell trust problems, try joining the Web Application Proxy server to the domain.

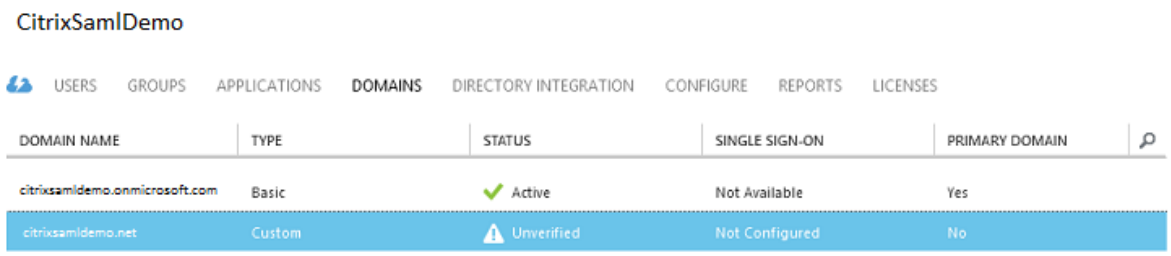
For the remaining steps of the wizard, use the standard administrator passwords, and create a service account for ADFS. Azure AD Connect will then prompt to validate the ownership of the DNS zone.



Add the TXT and MX records to the DNS address records in Azure.

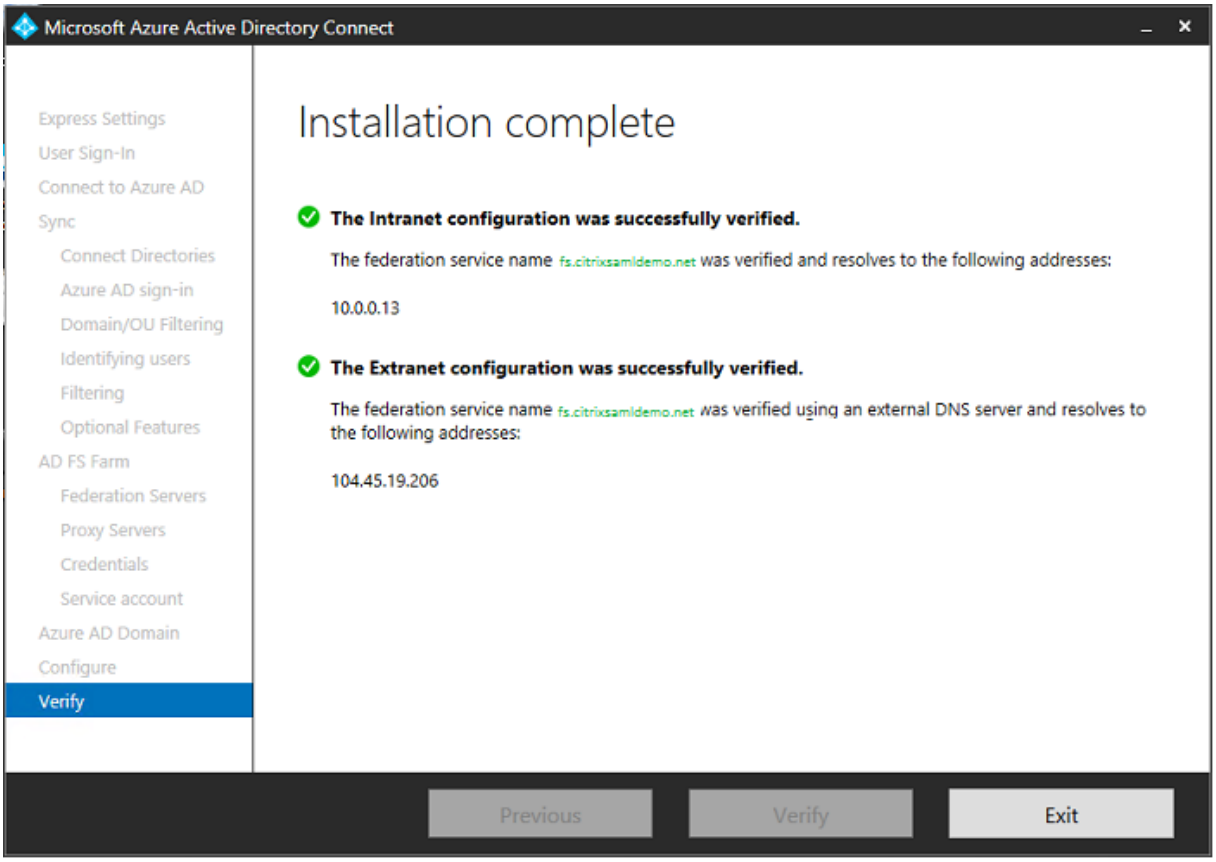


Click **Verify** in the Azure Management Console.



> **Note:**
>
> If this step fails, you can verify the domain before running Azure AD Connect.

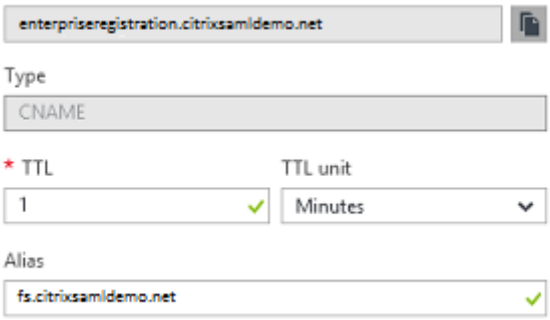
When complete, the external address fs.citrixsamldemo.net is contacted over port 443.



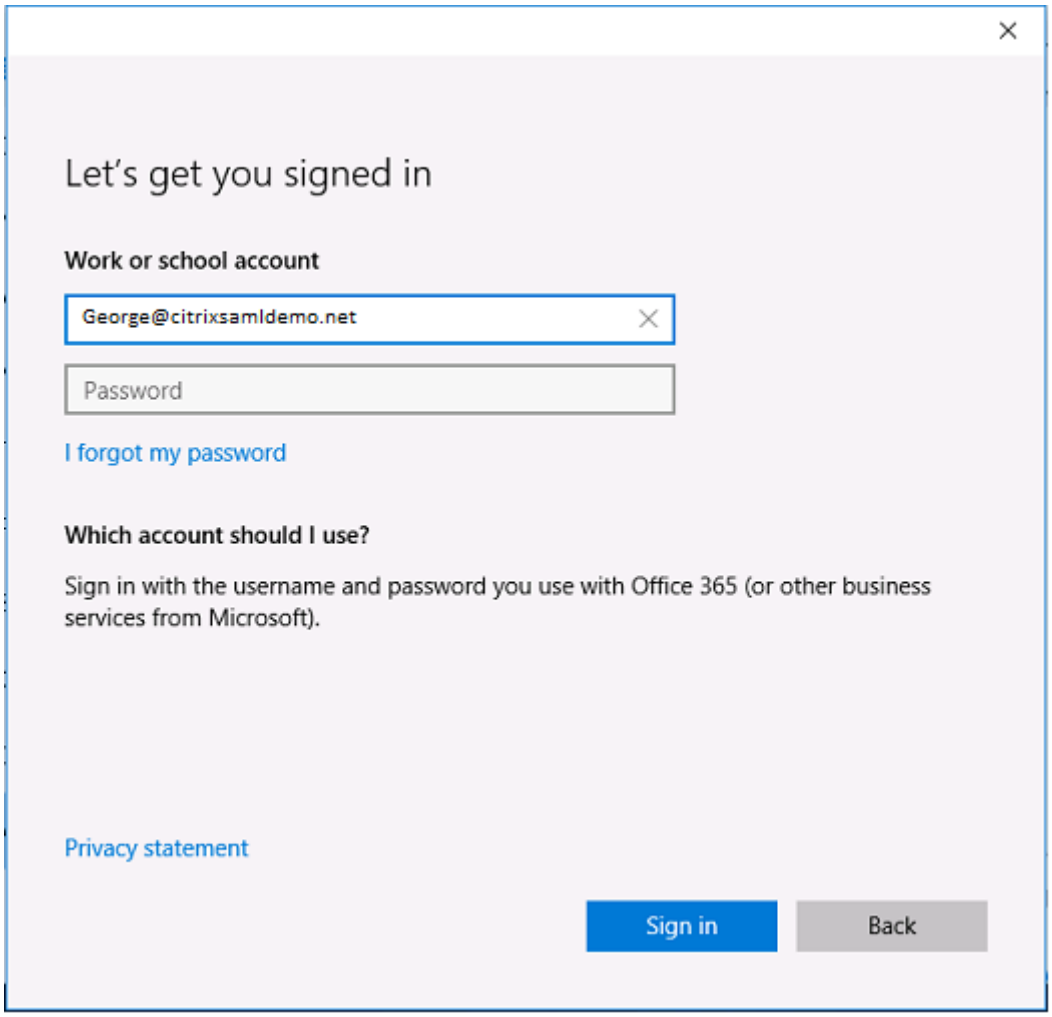
Enable Azure AD Join

When a user enters an email address so that Windows 10 can perform Azure AD join, the DNS suffix is used to construct a CNAME DNS record that should point to ADFS: enterpriseregistration.<*upnsuffix*>.

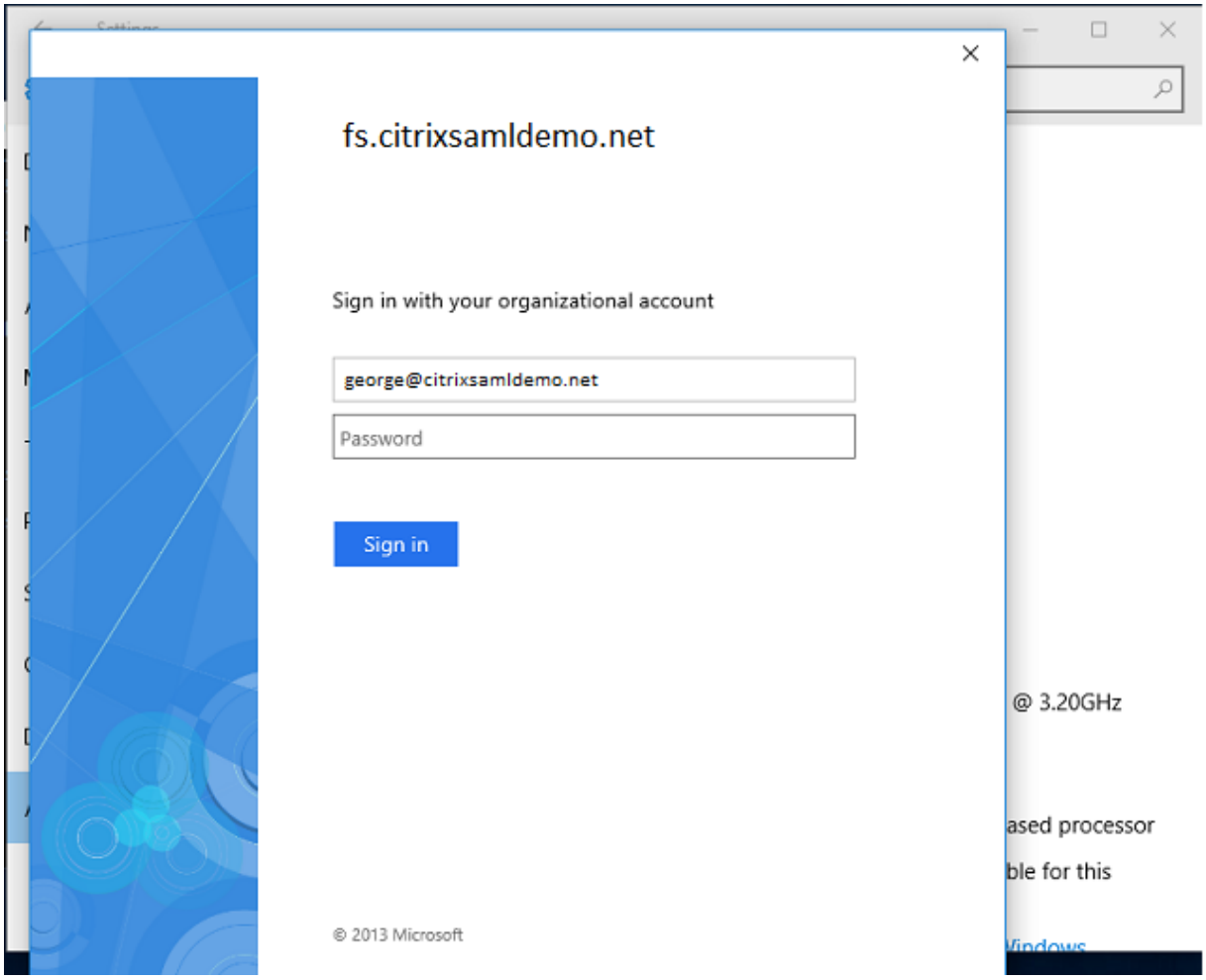
In the example, this is `fs.citrixsamldemo.net`.

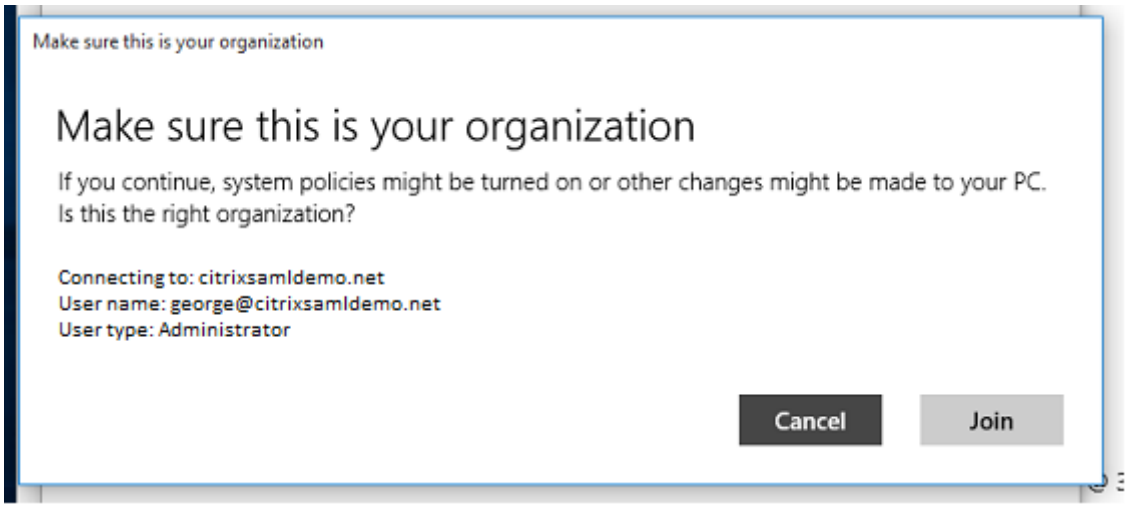


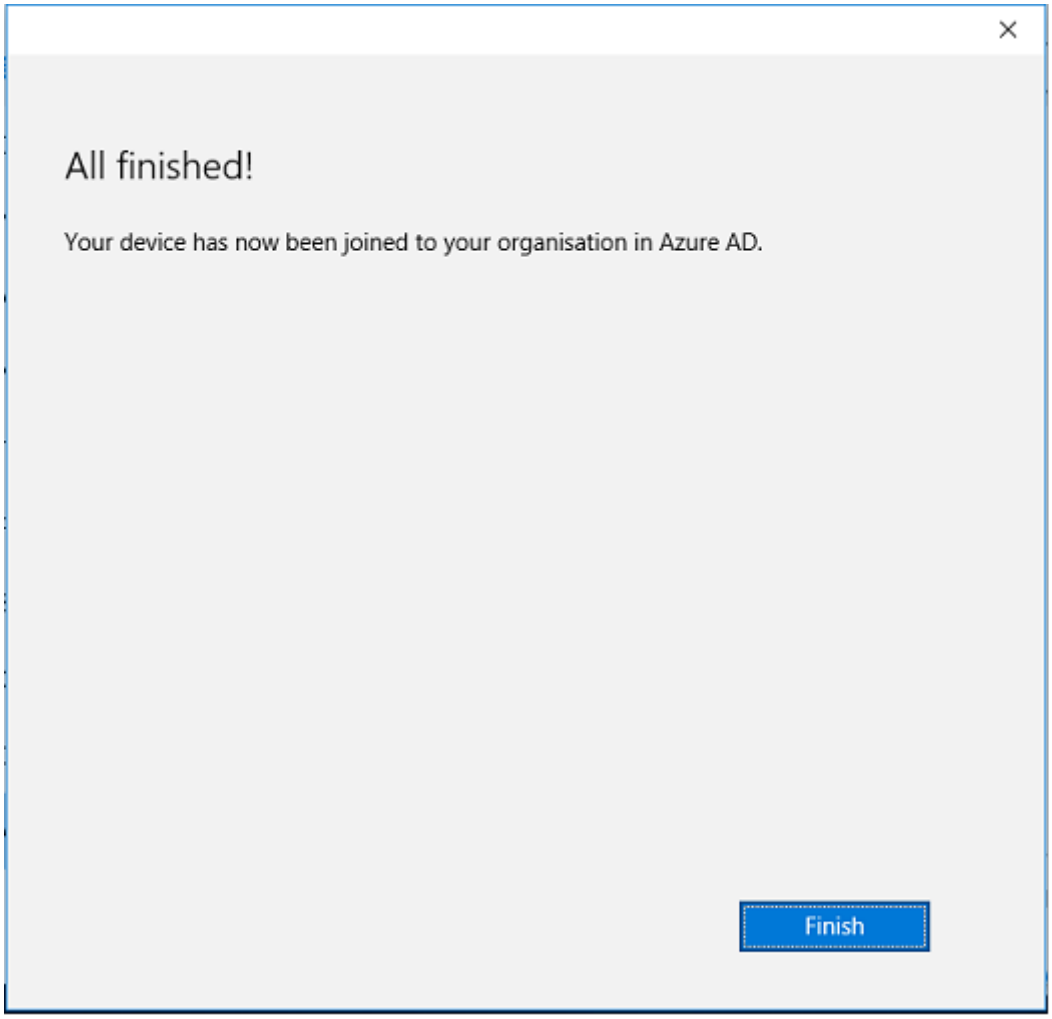
If you are not using a public certificate authority, ensure that the ADFS root certificate is installed on the Windows 10 computer so that Windows trusts the ADFS server. Perform an Azure AD domain join using the standard user account generated earlier.



Note that the UPN must match the UPN recognized by the ADFS domain controller.





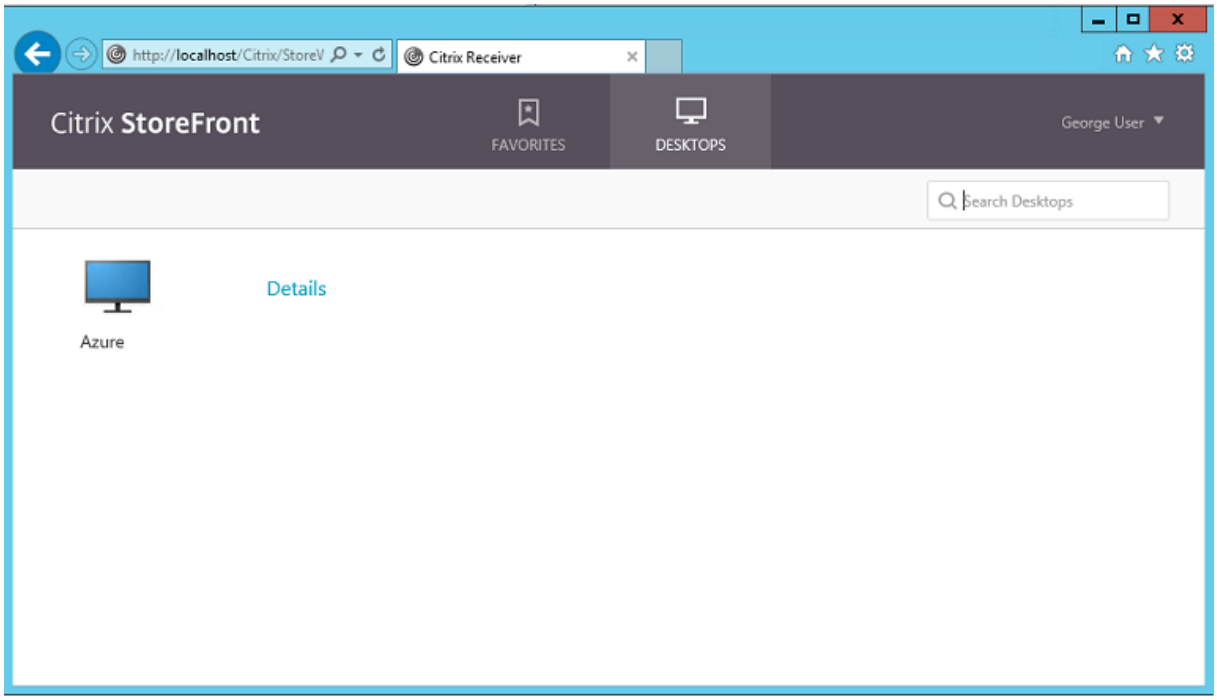


Verify that the Azure AD join was successful by restarting the machine and logging on, using the user's email address. When logged on, launch Microsoft Edge and connect to http://myapps.microsoft.com. The web site should use single sign-on automatically.

Install Citrix Virtual Apps or Citrix Virtual Desktops

You can install the Delivery Controller and VDA virtual machines in Azure directly from the Citrix Virtual Apps or Citrix Virtual Desktops ISO in the usual way.

In this example, StoreFront is installed on the same server as the Delivery Controller. The VDA is installed as a standalone Windows 2012 R2 RDS worker, without integrating with Machine Creation Services (although that can optionally be configured). Check that the user George@citrixsamldemo.net can authenticate with a password, before continuing.



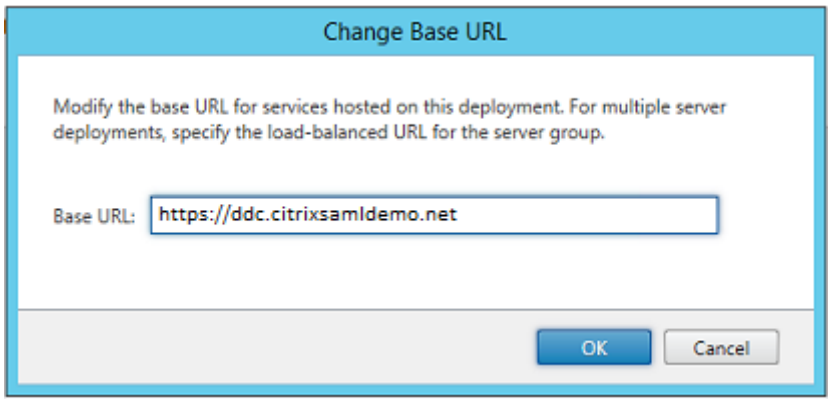
Run the **Set-BrokerSite –TrustRequestsSentToTheXmlServicePort $true** PowerShell cmdlet on the Controller to allow StoreFront to authenticate without the users' credentials.

Install Federated Authentication Service

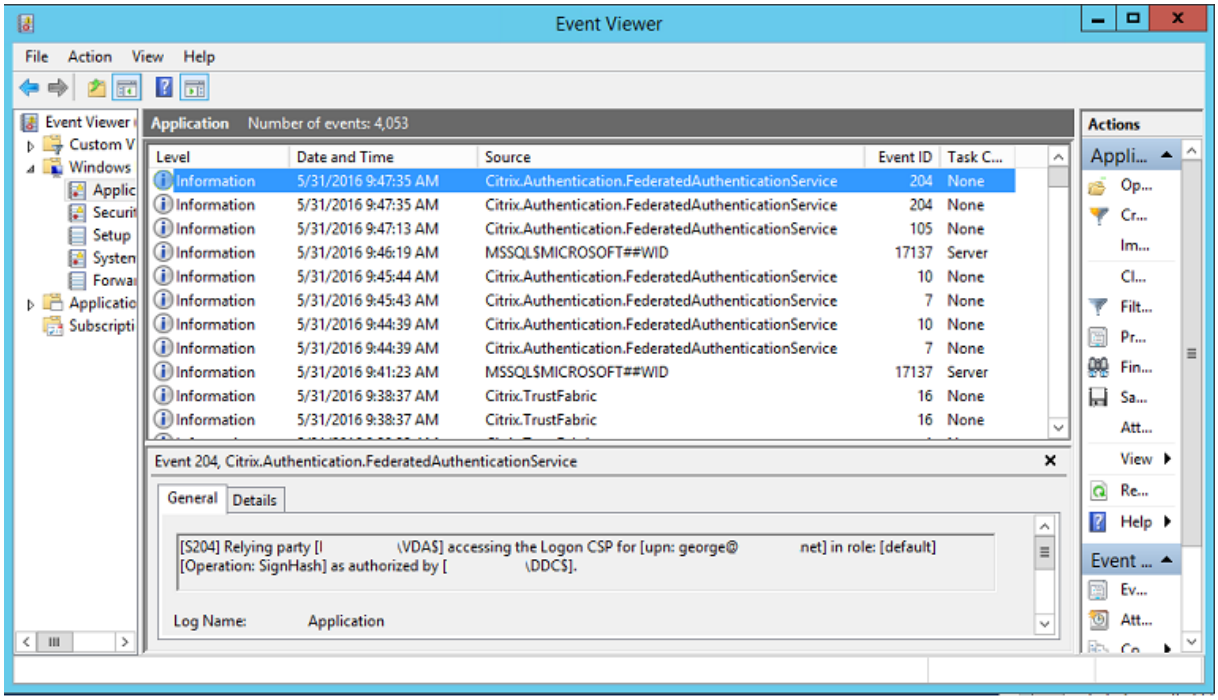
Install FAS on the ADFS server and configure a rule for the Delivery Controller to act as a trusted StoreFront (since, in this example, StoreFront is installed on the same VM as the Delivery Controller). See Install and configure.

Configure StoreFront

Request a computer certificate for the Delivery Controller, and configure IIS and StoreFront to use HTTPS by setting an IIS binding for port 443, and changing the StoreFront base address to https:.

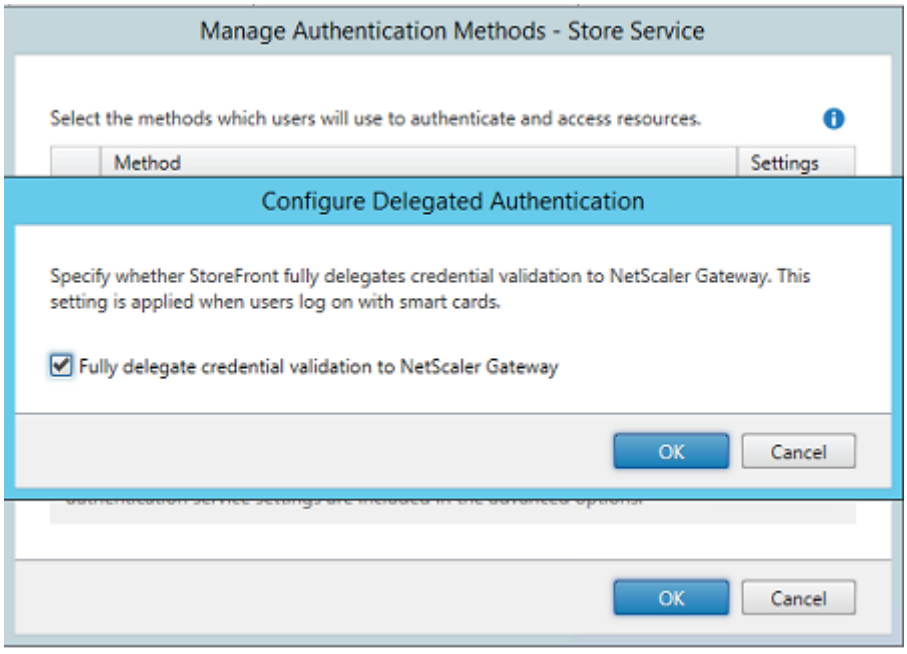


Configure StoreFront to use the FAS server (use the PowerShell script in Install and configure), and test internally within Azure, ensuring that the logon uses FAS by checking the event viewer on the FAS server.

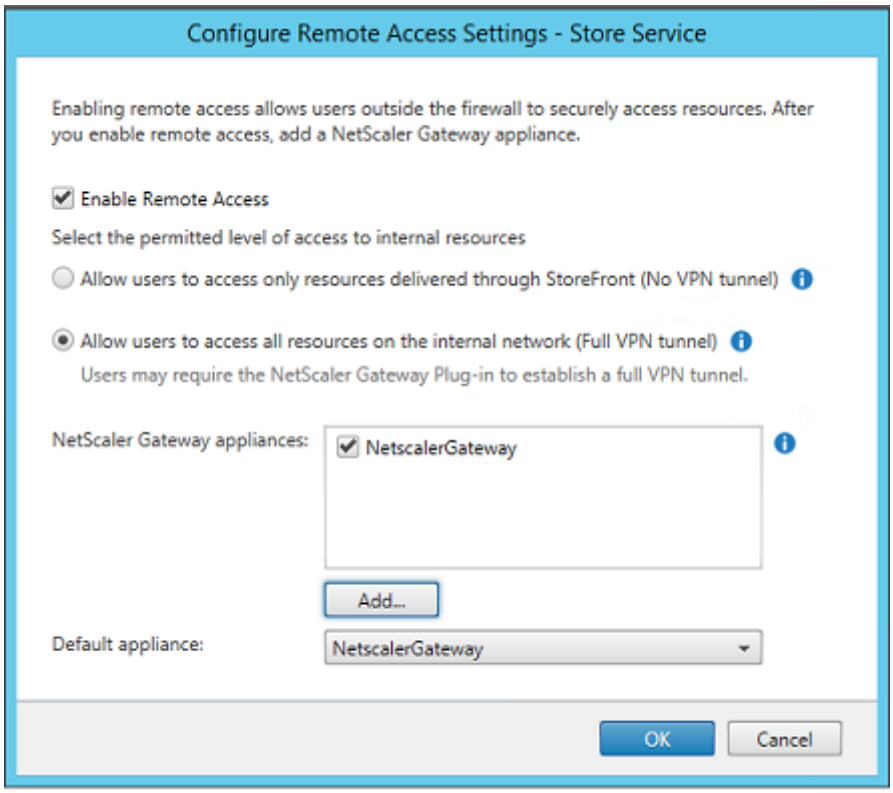


Configure StoreFront to use Citrix Gateway

Using the **Manage Authentication Methods** GUI in the StoreFront management console, configure StoreFront to use Citrix Gateway to perform authentication.

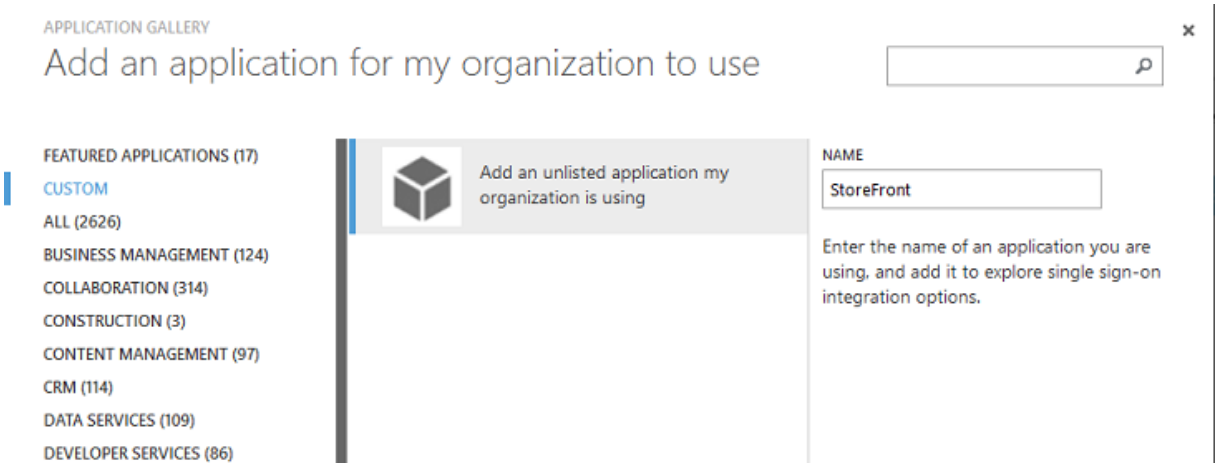


To integrate Citrix Gateway authentication options, configure a Secure Ticket Authority (STA) and configure the Citrix Gateway address.



Configure a new Azure AD application for Single Sign-on to StoreFront

This section uses the Azure AD SAML 2.0 Single Sign-on features, which currently require an Azure Active Directory Premium subscription. In the Azure AD management tool, select **New Application**, choosing **Add an application from the Gallery**.



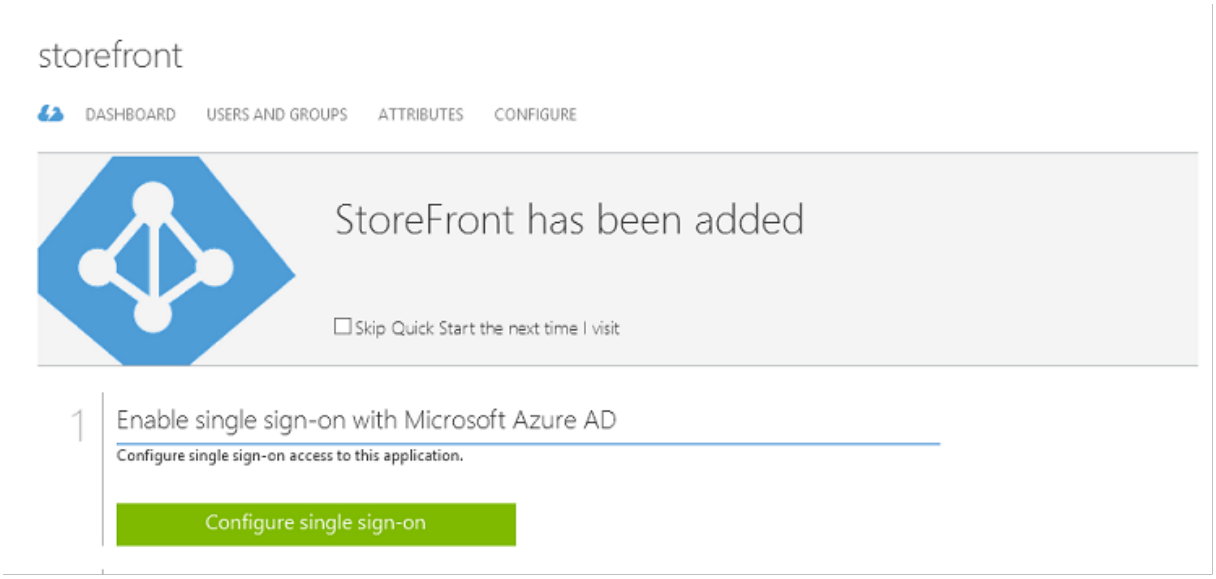
Select **CUSTOM > Add an unlisted application my organization is using** to create a new custom application for your users.

Configure an icon

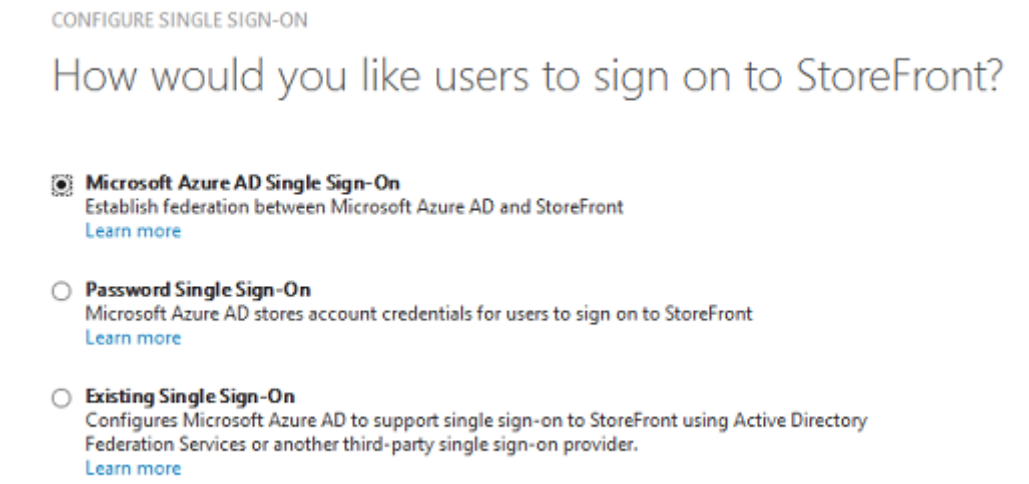
Create an image 215 by 215 pixels in size and upload it on the CONFIGURE page to use as an icon for the application.

Configure SAML authentication

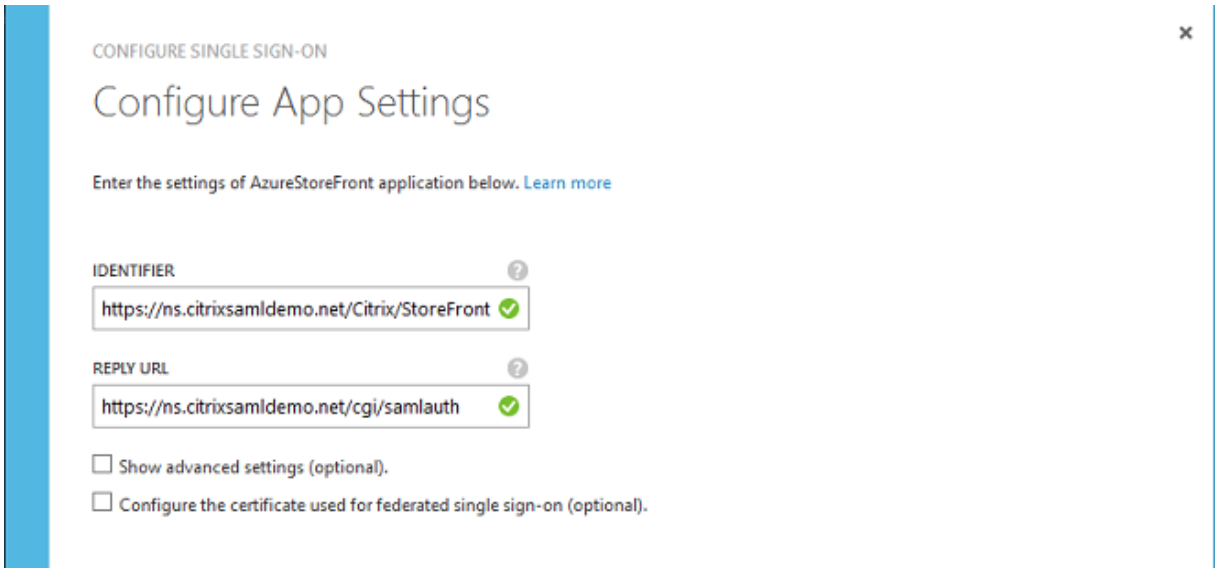
Return to the Application dashboard overview page and select **Configure Single sign-on**.



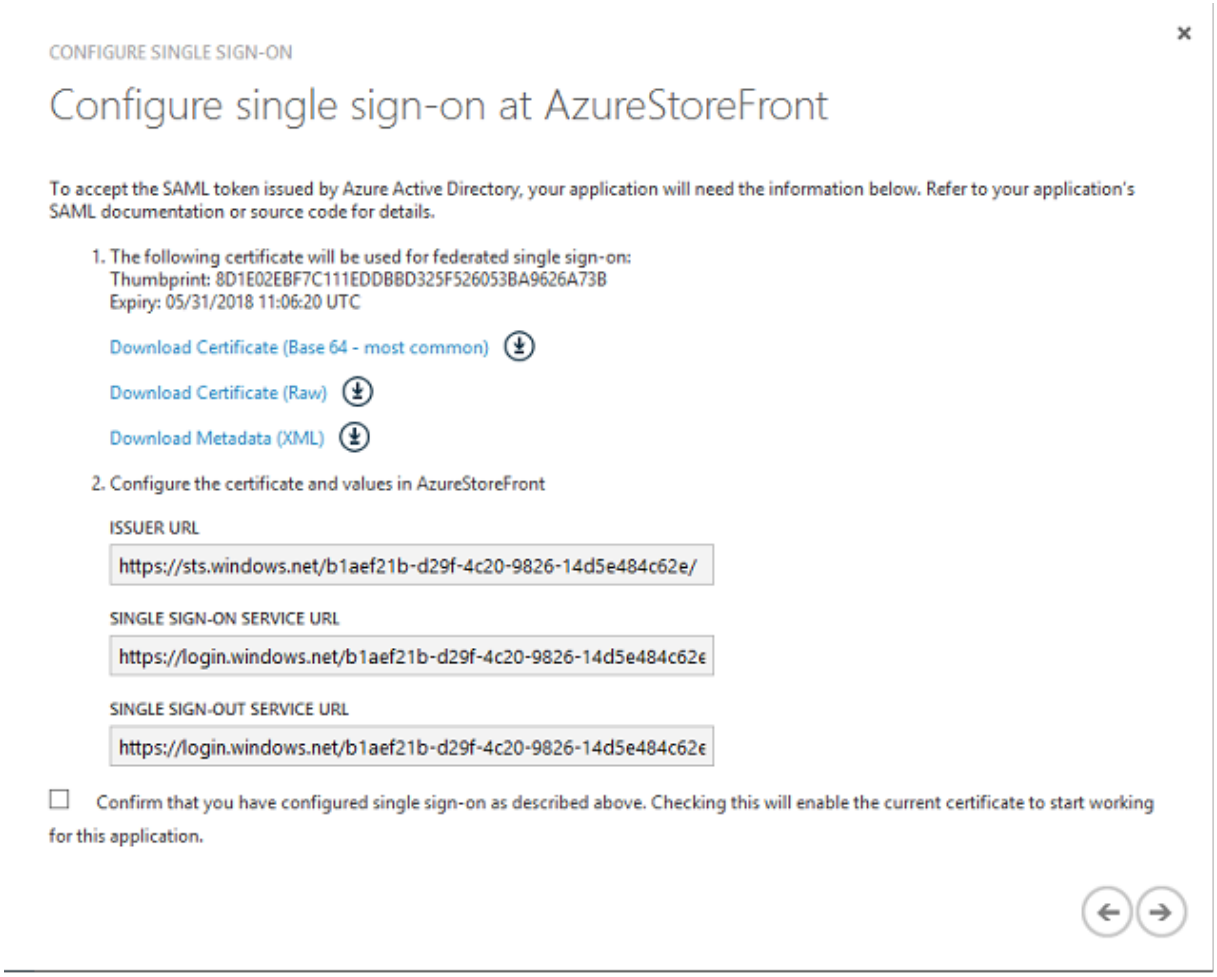
This deployment will use SAML 2.0 authentication, which corresponds to **Microsoft Azure AD Single Sign-On**.



The **Identifier** can be an arbitrary string (it must match the configuration provided to Citrix Gateway); in this example, the **Reply URL** is */cgi/samlauth* on the Citrix Gateway server.



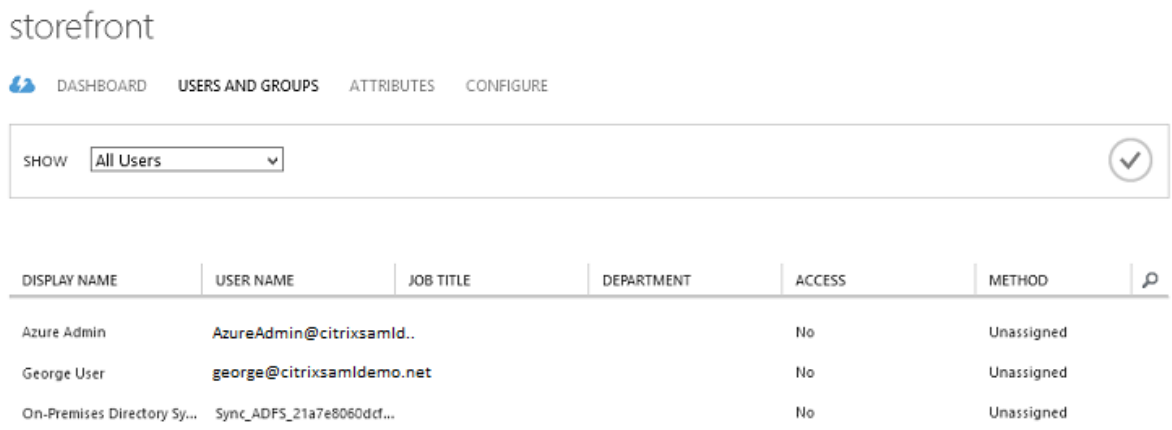
The next page contains information that is used to configure Citrix Gateway as a relying party to Azure AD.



Download the base 64 trusted signing certificate and copy the sign-on and sign-out URLs. You will paste these in Citrix Gateway configuration screens later.

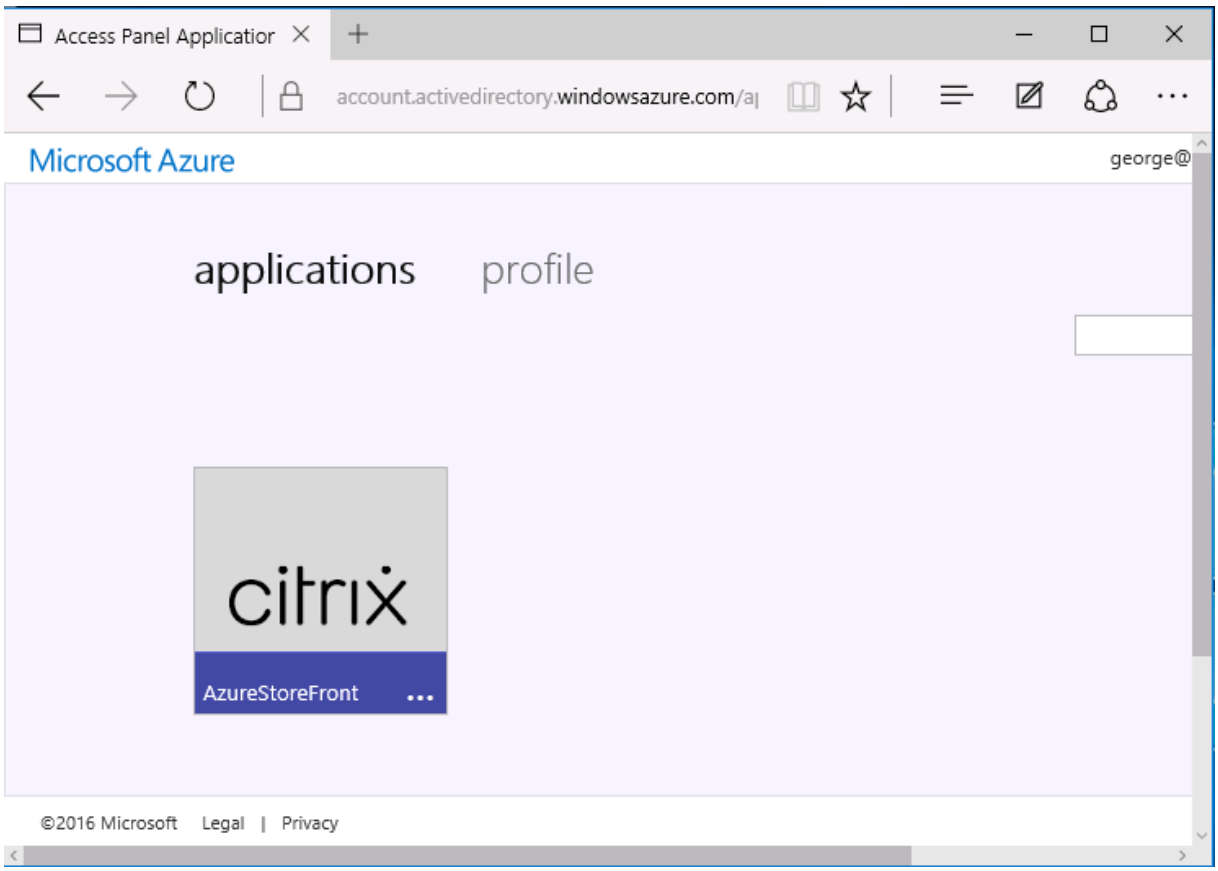
Assign the application to users

The final step is to enable the application so that it appears on users' "myapps.microsoft.com" control page. This is done on the USERS AND GROUPS page. Assign access for the domain users accounts synchronized by Azure AD Connect. Other accounts can also be used, but they must be explicitly mapped because they do not conform to the <user>@<domain> pattern.



MyApps page

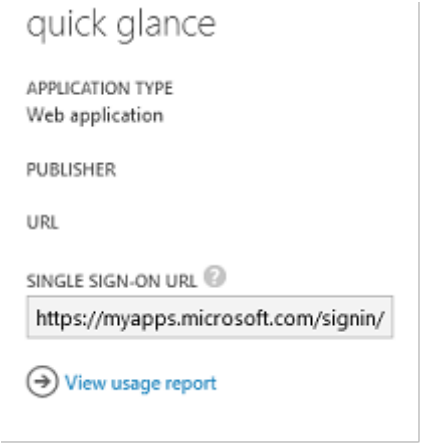
When the application has been configured, it appears on the users' lists of Azure applications when they visit https://myapps.microsoft.com.



When it is Azure AD joined, Windows 10 supports single sign-on to Azure applications for the user who logs on. Clicking the icon takes the browser to the SAML cgi/samlauth web page that was configured earlier.

Single sign-on URL

Return to the application in the Azure AD dashboard. There is now a single sign-on URL available for the application. This URL is used to provide web browser links or to create Start menu shortcuts that take users directly into StoreFront.



Paste this URL into a web browser to ensure that you are redirected by Azure AD to the Citrix Gateway cgi/samlauth web page configured earlier. This works only for users who have been assigned, and will provide single sign-on only for Windows 10 Azure AD-joined logon sessions. (Other users will be prompted for Azure AD credentials.)

Install and configure Citrix Gateway

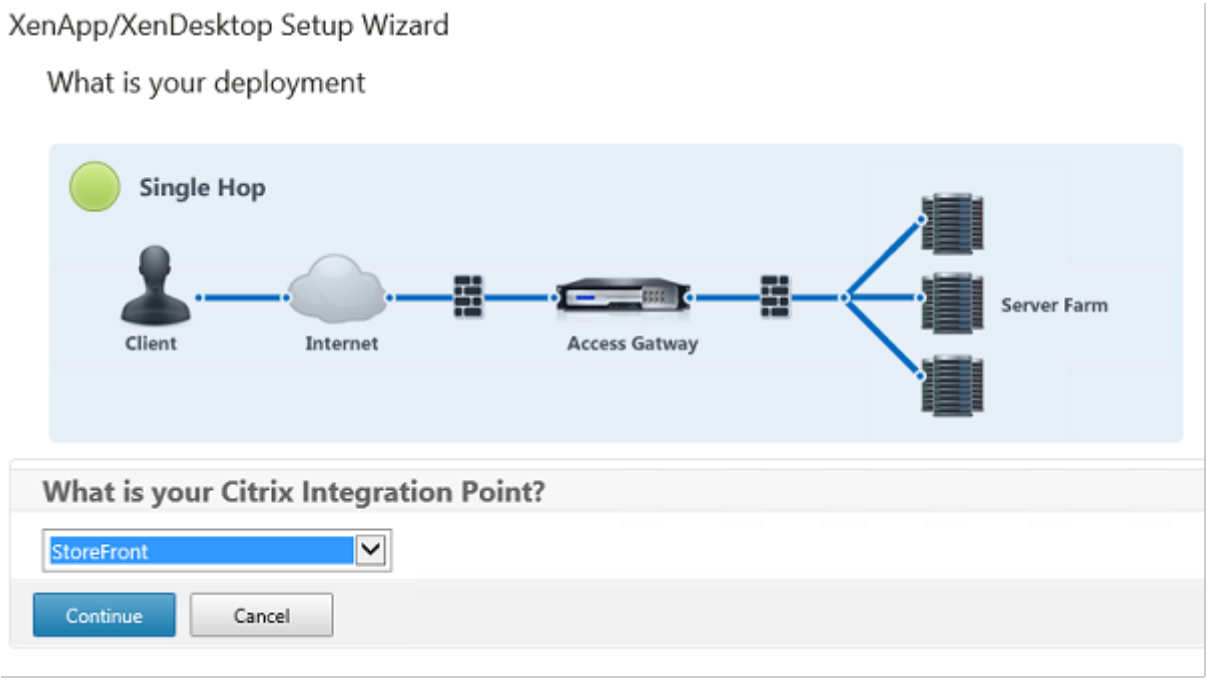
To remotely access the deployment, this example uses a separate VM running NetScaler (now Citrix Gateway). This can be purchased from the Azure Store. This example uses the "Bring your own License" version of NetScaler 11.0.

Log on to the NetScaler VM, pointing a web browser to the internal IP address, using the credentials specified when the user authenticated. Note that you must change the password of the nsroot user in an Azure AD VM.

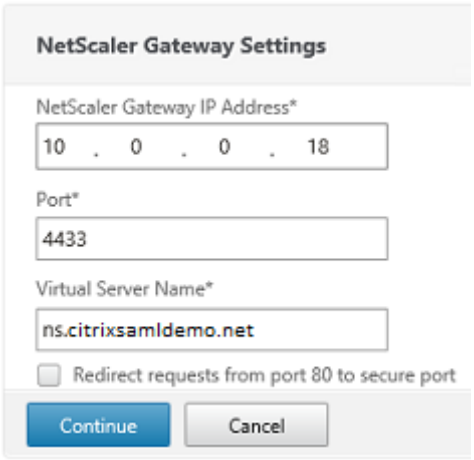
Add licenses, selecting **reboot** after each license file is added, and point the DNS resolver to the Microsoft domain controller.

Run the Citrix Virtual Apps and Desktops setup wizard

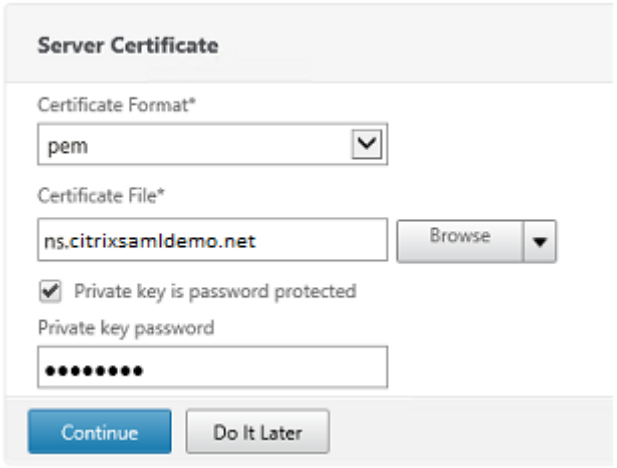
This example starts by configuring a simple StoreFront integration without SAML. After that deployment is working, it adds a SAML logon policy.



Select the standard Citrix Gateway StoreFront settings. For use in Microsoft Azure, this example configures port 4433, rather than port 443. Alternatively, you can port-forward or remap the Citrix Gateway administrative web site.

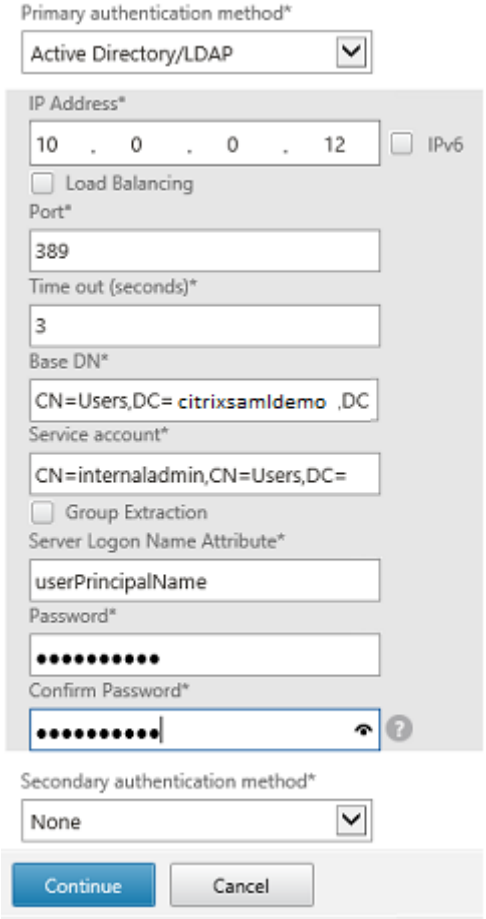


For simplicity, the example uploads an existing server certificate and private key stored in a file.



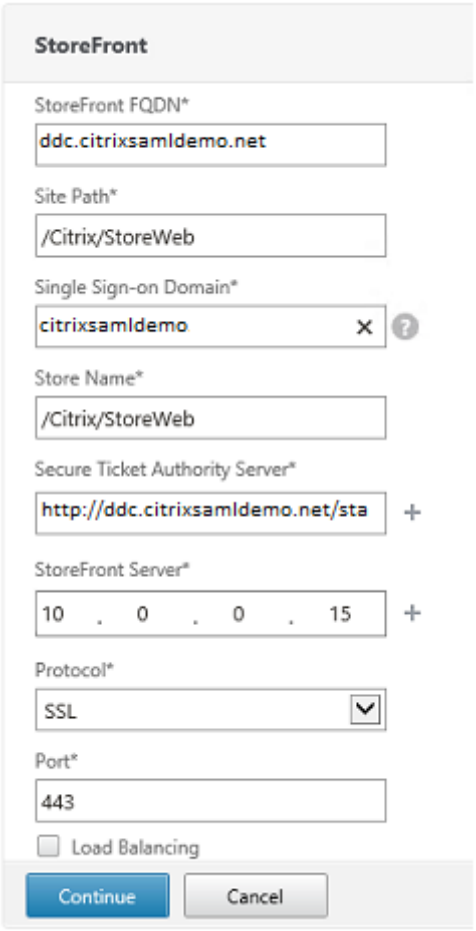
Configure the domain controller for AD account management

The domain controller will be used for account resolution, so add its IP address into the primary authentication method. Note the formats expected in each field in the dialog box.



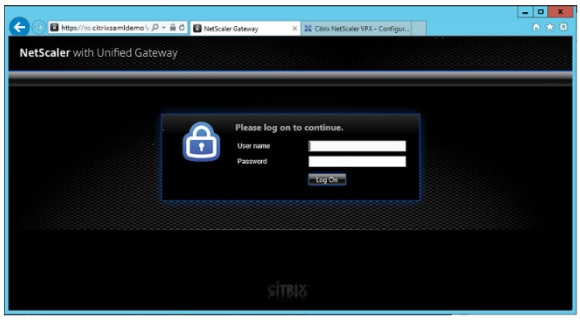
Configure the StoreFront address

In this example, StoreFront has been configured using HTTPS, so select the SSL protocol options.



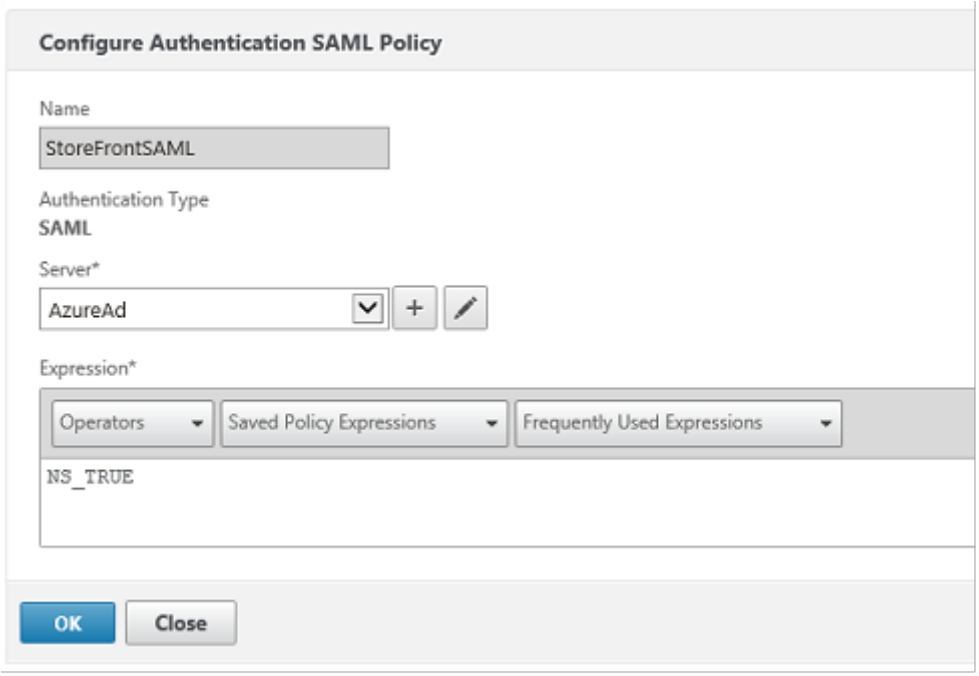
Verify the Citrix Gateway deployment

Connect to Citrix Gateway and check that authentication and launch are successful with the username and password.

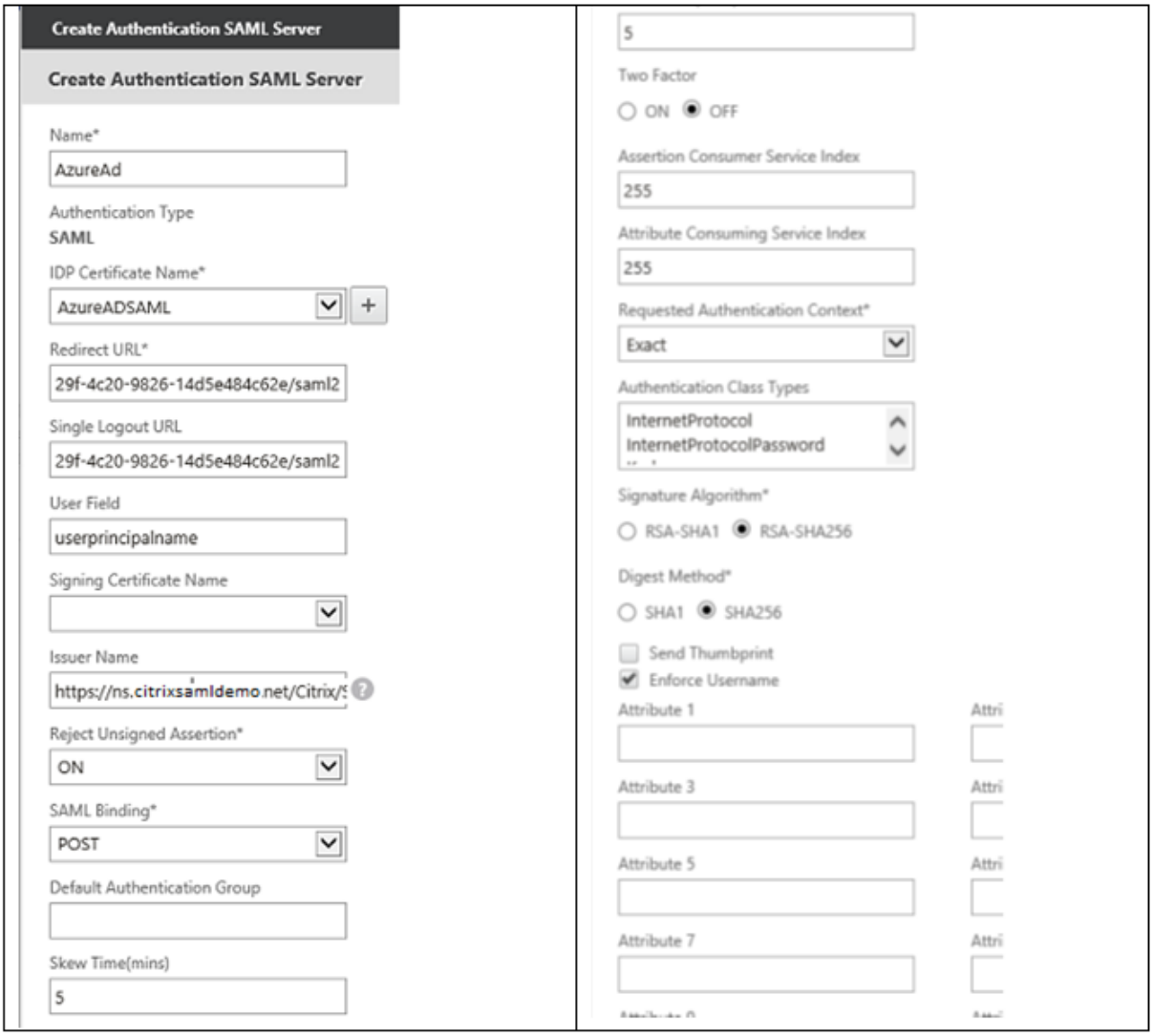


Enable Citrix Gateway SAML authentication support

Using SAML with StoreFront is similar to using SAMl with other web sites. Add a new SAML policy, with an expression of **NS_TRUE**.



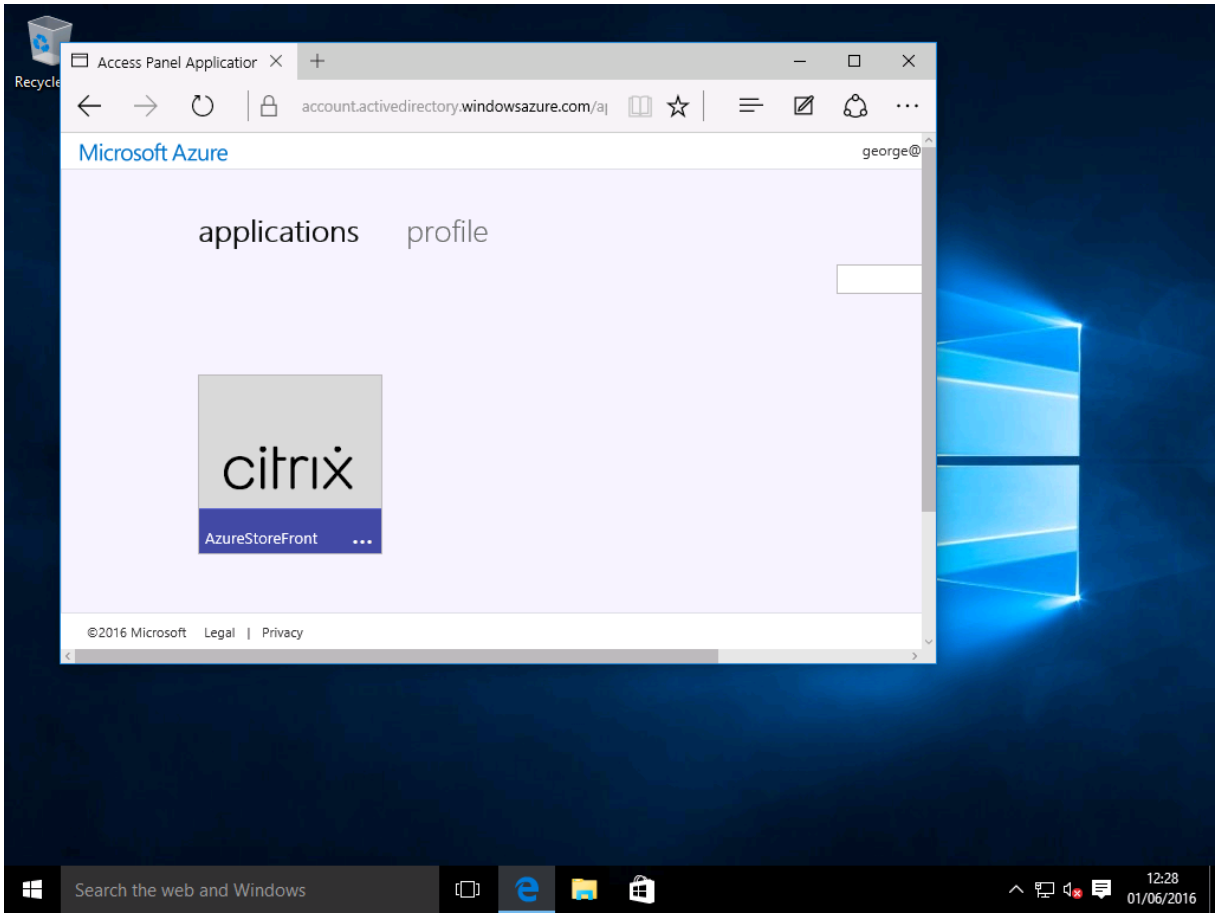
Configure the new SAML IdP server, using information obtained from Azure AD earlier.



Verify the end-to-end system

Log on to an Azure AD Joined Windows 10 desktop, using an account registered in Azure AD. Launch Microsoft Edge and connect to: https://myapps.microsoft.com.

The web browser should display the Azure AD applications for the user.



Verify that clicking the icon redirects you to an authenticated StoreFront server.

Similarly, verify that direct connections using the Single Sign-on URL and a direct connection to the Citrix Gateway site redirect you to Microsoft Azure and back.

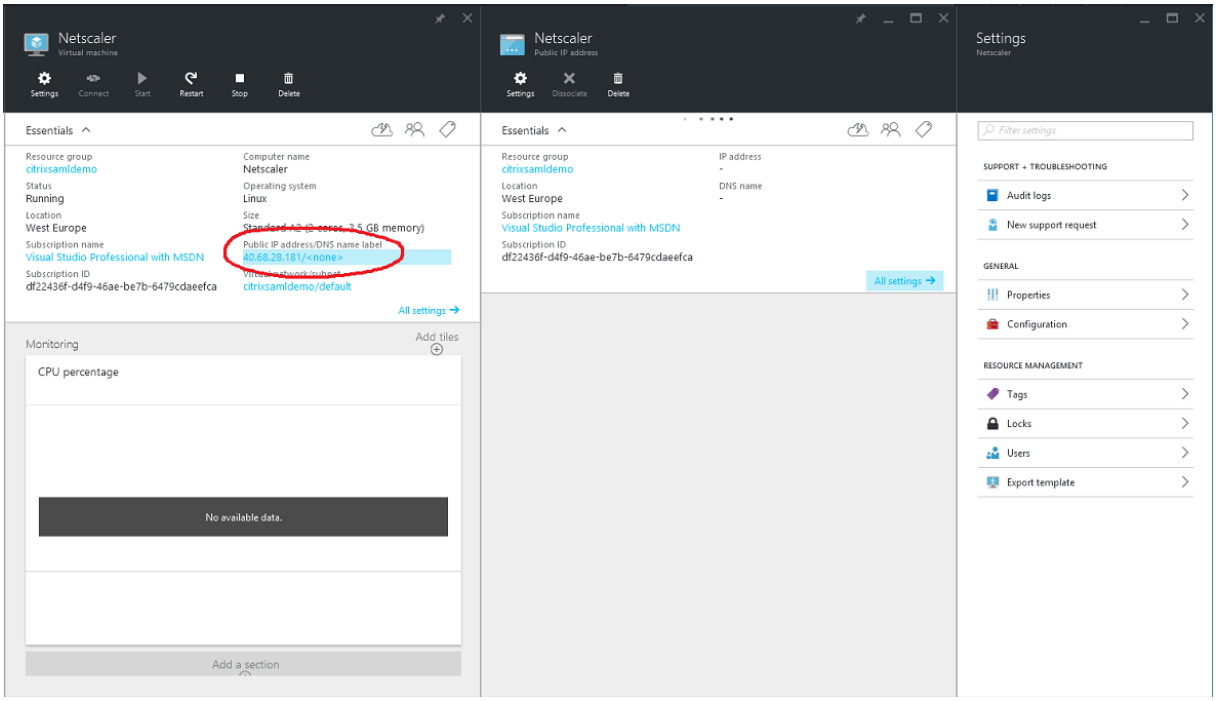
Finally, verify that non-Azure AD joined machines also function with the same URLs (although there will be a single explicit sign-on to Azure AD for the first connection).

Appendix

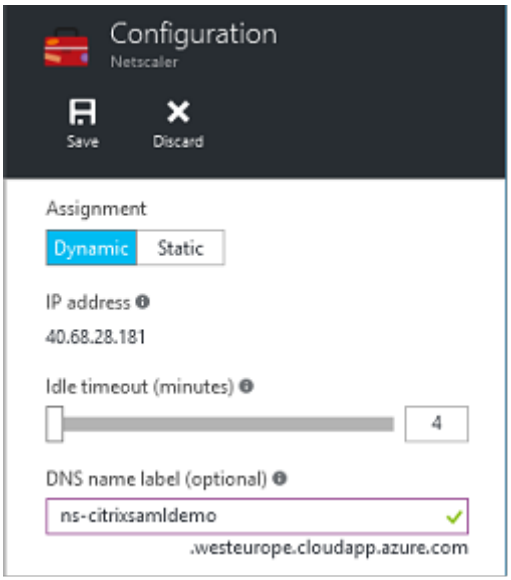
You should configure the following standard options when you are setting up a VM in Azure.

Provide a public IP address and DNS address

Azure gives all VMs an IP address on the internal subnet (10.*.*.* in this example). By default a public IP address is also supplied, which can be referenced by a dynamically updated DNS label.



Select **Configuration** of the **Public IP address/DNS name label**. Choose a public DNS address for the VM. This can be used for CNAME references in other DNS zone files, ensuring that all DNS records remain correctly pointing to the VM, even if the IP address is reallocated.

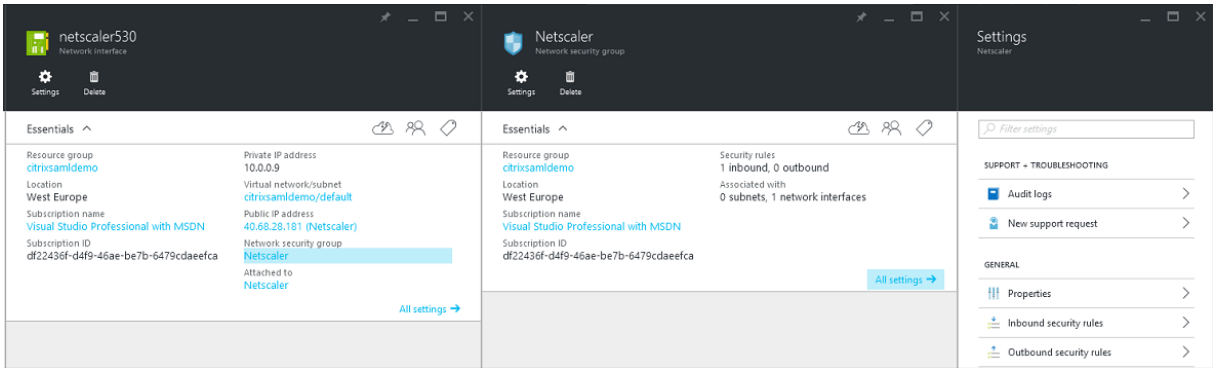


Set up firewall rules (security group)

Each VM in a cloud has a set of firewall rules applied automatically, known as the security group. The security group controls traffic forwarded from the public to the private IP address. By default, Azure allows RDP to be forwarded to all VMs. The Citrix Gateway and ADFS servers must also need to forward

TLS traffic (443).

Open **Network Interfaces** for a VM, and then click the **Network Security Group** label. Configure the **Inbound security rules** to allow appropriate network traffic.



Related information

- Install and configure is the primary reference for FAS installation and configuration.
- The common FAS deployments are summarized in the Deployment architectures article.
- “How-to” articles are introduced in the Advanced configuration article.

Advanced configuration

March 26, 2020

The “how-to” articles in this section provide advanced configuration and management guidance for Federated Authentication Service (FAS).

Related information

- The primary reference for FAS installation and initial setup is the Install and configure article.
- The Deployment architectures article provides summaries of the major FAS architectures, plus links to other articles about the more complex architectures.

Certificate authority configuration

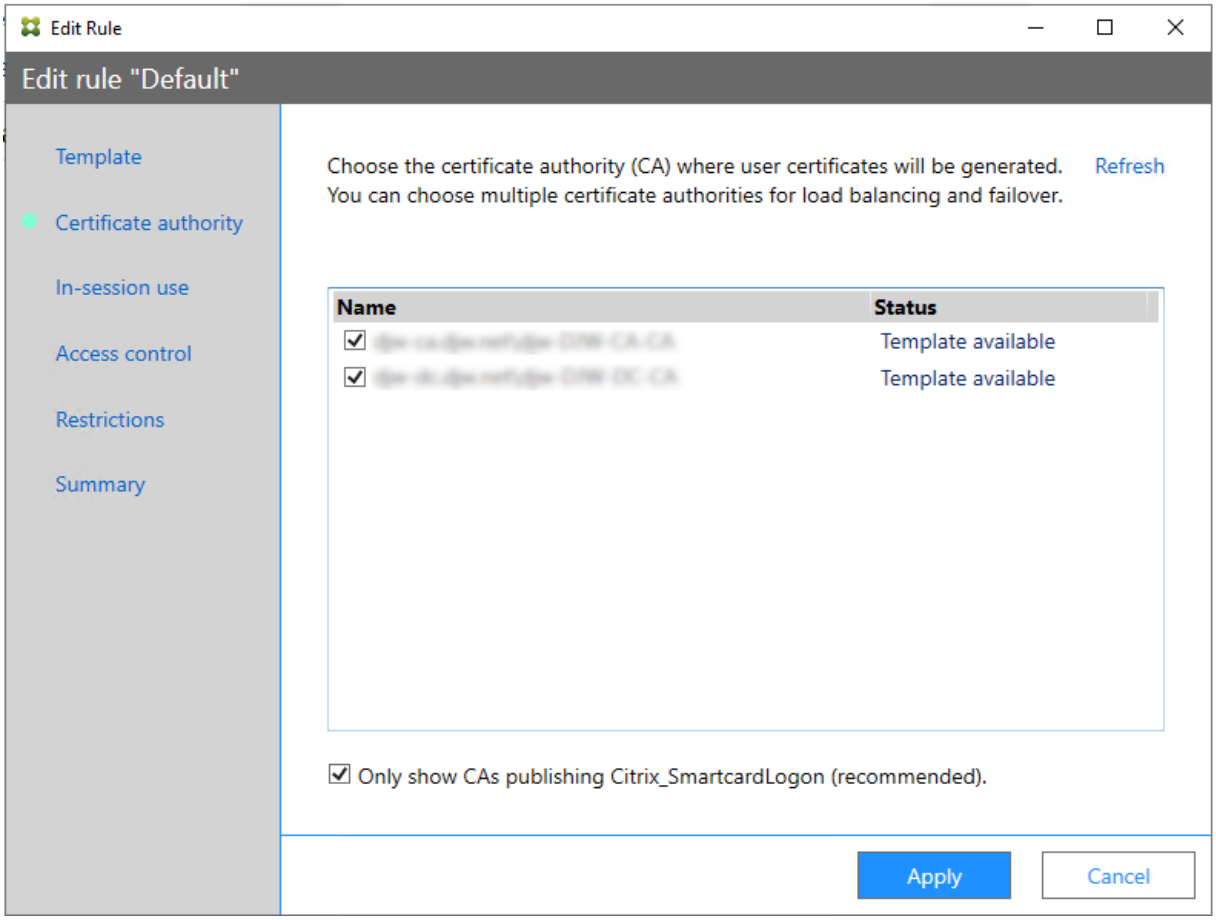
January 26, 2021

This article describes the advanced configuration of Federated Authentication Service (FAS) to integrate with certificate authority (CA) servers. Most of these configurations are not supported by the

FAS administration console. The instructions use PowerShell APIs provided by FAS. You should have a basic knowledge of PowerShell before executing any instructions in this article.

Set up multiple CA servers for use in FAS

You can use the FAS administration console to configure FAS with multiple CAs while creating or editing a rule:



All the CAs you select must be publishing the Citrix_SmartcardLogon certificate template (or whatever template you have chosen in your rule).

If one of the CAs you wish to use is not publishing the desired template, perform the Set up a certificate authority step for the CA.

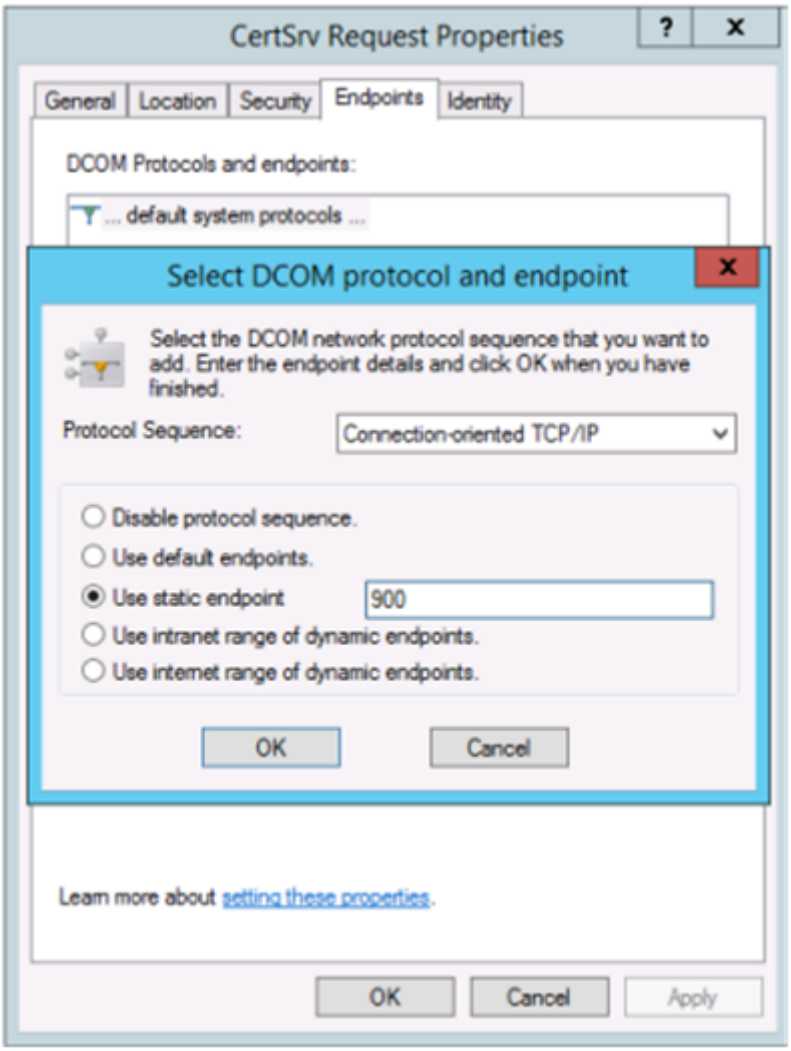
> **Note:**
>
> You do not have to perform the Authorize this service step for every CA, because the authorization certificate configured in this step can be used at any of your CAs.

Expected behavior changes

After you configure the FAS server with multiple CA servers, user certificate generation is distributed among all the configured CA servers. Also, if one of the configured CA servers fails, the FAS server will switch to another available CA server.

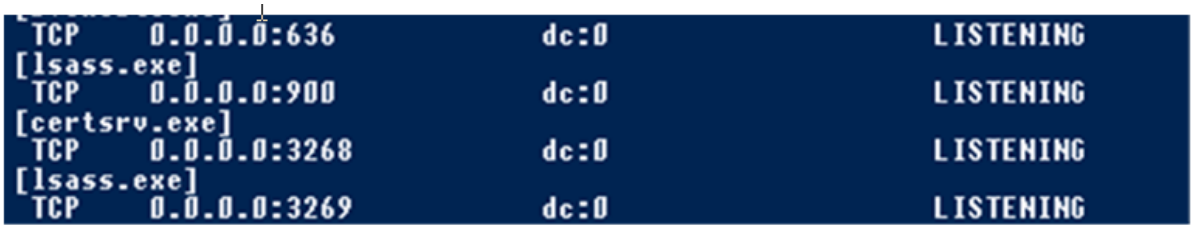
Configure the Microsoft certificate authority for TCP access

By default the Microsoft certificate authority uses DCOM for access. This can result in complexities when implementing firewall security, so Microsoft has a provision to switch to a static TCP port. On the Microsoft certificate authority, open the DCOM configuration panel and edit the properties of the "CertSrv Request" DCOM application:



Change the "Endpoints" to select a static endpoint and specify a TCP port number (900 in the graphic above).

Restart the Microsoft certificate authority and submit a certificate request. If you run `netstat -a -n -b` you should see that certsvr is now listening on port 900:



There is no need to configure the FAS server (or any other machines using the certificate authority), because DCOM has a negotiation stage using the RPC port. When a client needs to use DCOM, it connects to the DCOM RPC Service on the certificate server and requests access to a particular DCOM server. This triggers port 900 to be opened, and the DCOM server instructs the FAS server how to connect.

Pre-generate user certificates

The logon time for users will significantly improve when user certificates are pre-generated within the FAS server. The following sections describe how it can be done, either for single or multiple FAS servers.

Get a list of Active Directory users

You can improve certificate generation by querying the AD and storing the list of users into a file (for example, a .csv file), as shown in the following example.

```
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 {

```

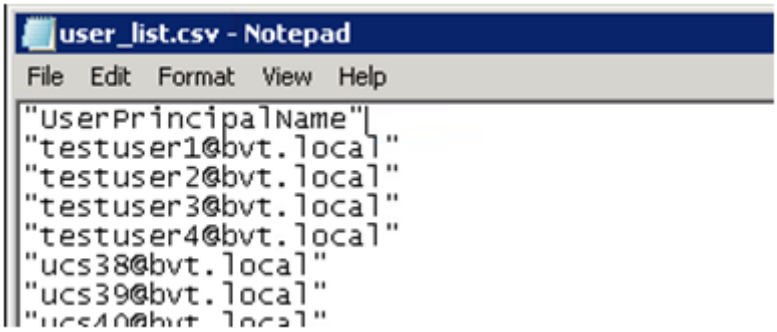


```
14      Get-ADUser -Filter {
15   (UserPrincipalName -ne ”null”) -and (Enabled -eq ”true”) }
16    -Properties UserPrincipalName | Select UserPrincipalName | Export-Csv
          -NoTypeInformation -Encoding utf8 -delimiter ”,” $filename
17   }
```

Get-ADUser is a standard cmdlet to query for a list of users. The example above contains a filter argument to list only users with a UserPrincipalName and an account status of ‘enabled.’

The SearchBase argument narrows which part of the AD to search for users. You can omit this if you want to include all users in AD. Note: This query might return a large number of users.

The CSV looks something like this:



FAS server

The following PowerShell script takes the previously-generated user list and creates a list of user certificates.

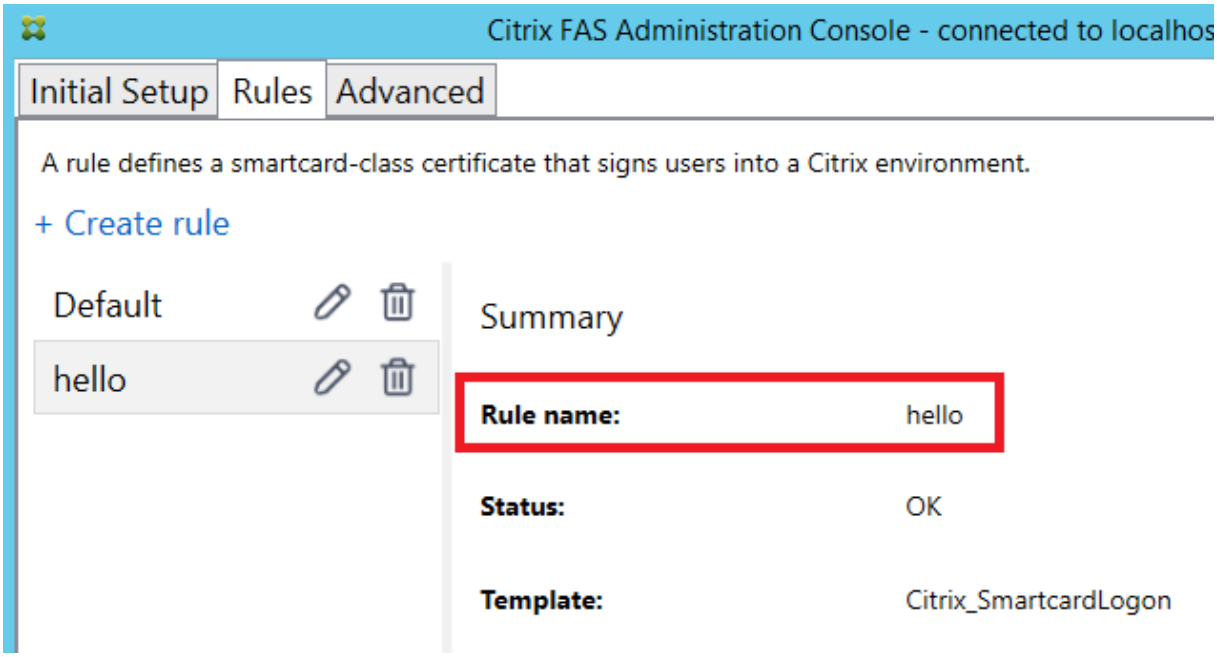
```
1  Add-PSSnapin Citrix.A*
2  $csv = ”user_list.csv”
3  $rule = ”default” # rule/role in your admin console
4  $users = Import-Csv -encoding utf8 $csv
5  foreach ( $user in $users )
6  {
7
8      $server = Get-FasServerForUser -UserPrincipalNames $user.
           UserPrincipalName
9      if( $server.Server -ne $NULL) {
10
11         New-FasUserCertificate -Address $server.Server -
               UserPrincipalName $user.UserPrincipalName -
               CertificateDefinition $rule”_Definition” -Rule $rule
```



```
12      }
13
14     if( $server.Failover -ne $NULL) {
15
16         New-FasUserCertificate -Address $server.Failover -
               UserPrincipalName $user.UserPrincipalName -
               CertificateDefinition $rule"_Definition" -Rule $rule
17      }
18
19  }
```

If you have more than one FAS server, a particular user's certificate will be generated twice: one in the main server, and the other in the failover server.

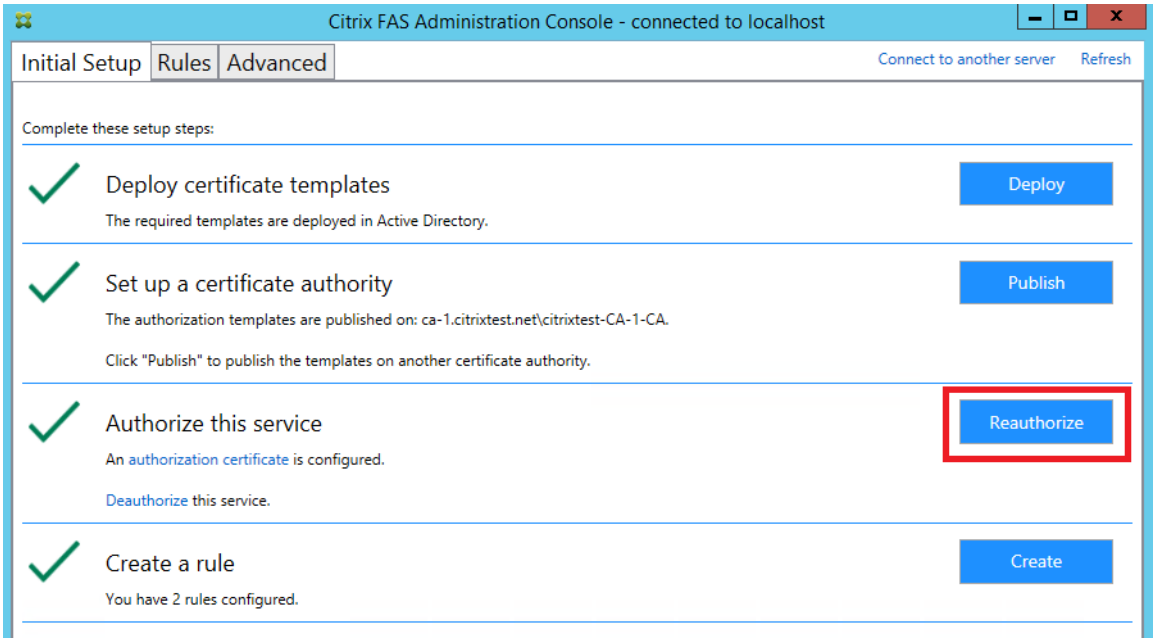
The script above is catered for a rule named 'default'. If you have a different rule name (for example, 'hello'), just change the $rule variable in the script.



Renew registration authority certificates

If more than one FAS server is in use, you can renew a FAS authorization certificate without affecting logged-on users.

> **Note:**
>
> You can also use the GUI to reauthorize FAS:



Complete the following sequence:

1. Create a new authorization certificate: `New-FasAuthorizationCertificate`
2. Note the GUID of the new authorization certificate, as returned by: `Get-FasAuthorizationCertificate`
3. Place the FAS server into maintenance mode: `Set-FasServer -Address <FAS server> -MaintenanceMode $true`
4. Swap the new authorization certificate: `Set-FasCertificateDefinition -AuthorizationCertifica <GUID>`
5. Take the FAS server out of maintenance mode: `Set-FasServer -Address <FAS server> -MaintenanceMode $false`
6. Delete the old authorization certificate: `Remove-FasAuthorizationCertificate`

Related information

- The Install and configure article is the primary reference for FAS installation and configuration.
- The common Federated Authentication Service deployments are summarized in the Deployment architectures article.
- Other “how-to” articles are introduced in the Advanced configuration article.

Private key protection

July 7, 2020

Introduction

Private keys are stored by means of the Network Service account and marked as non-exportable by default.

There are two types of private keys:

- The private key associated with the registration authority certificate, from the Citrix_RegistrationAuthority certificate template.
- The private keys associated with the user certificates, from the Citrix_SmartcardLogon certificate template.

There are actually two registration authority certificates: Citrix_RegistrationAuthority_ManualAuthorization (valid for 24 hours by default) and Citrix_RegistrationAuthority (valid for two years by default).

During step 3 of the **Initial Setup** tab in the Federated Authentication Service (FAS) administration console, when you click **Authorize** the FAS server generates a keypair and sends a certificate signing request to the certificate authority for the Citrix_RegistrationAuthority_ManualAuthorization certificate. This is a temporary certificate, valid for 24 hours by default. The certificate authority does not automatically issue this certificate; its issuance must be manually authorised on the certificate authority by an administrator. Once the certificate is issued to the FAS server, FAS uses the Citrix_RegistrationAuthority_ManualAuthorization certificate to automatically obtain the Citrix_RegistrationAuthority certificate (valid for two years by default). The FAS server deletes the certificate and key for Citrix_RegistrationAuthority_ManualAuthorization as soon as it obtains the Citrix_RegistrationAuthority certificate.

The private key associated with the registration authority certificate is particularly sensitive, because the registration authority certificate policy allows whoever possesses the private key to issue certificate requests for the set of users configured in the template. As a consequence, whoever controls this key can connect to the environment as any of the users in the set.

You can configure the FAS server to protect private keys in a way that fits your organization's security requirements, using one of the following:

- Microsoft Enhanced RSA and AES Cryptographic Provider or Microsoft Software Key Storage Provider for both the registration authority certificate and the user certificates' private keys.
- Microsoft Platform Key Storage Provider with a Trusted Platform Module (TPM) chip for the registration authority certificate's private key, and Microsoft Enhanced RSA and AES Cryptographic Provider or Microsoft Software Key Storage Provider for the user certificates' private keys.

- A Hardware Security Module (HSM) vendor's Cryptographic Service or Key Storage Provider with the HSM device for both the registration authority certificate and the user certificates' private keys.

Private key configuration settings

Configure FAS to use one of the three options. Use a text editor to edit the Citrix.Authentication.FederatedAuthentic file. The default location of the file is in the Program Files\Citrix\Federated Authentication Service folder on the 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>
```

FAS reads the config file only when the service starts. If any values are changed, FAS must be restarted before it reflects the new settings.

Set the relevant values in the Citrix.Authentication.FederatedAuthenticationService.exe.config file as follows:

Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.**ProviderLegacyCsp** (switch between CAPI and CNG APIs)

Value	Comment
true	Use CAPI APIs
false (default)	Use CNG APIs

Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.**ProviderName** (name of the provider to use)

Value	Comment
Microsoft Enhanced RSA and AES Cryptographic Provider	Default CAPI provider
Microsoft Software Key Storage Provider	Default CNG Provider
Microsoft Platform Key Storage Provider	Default TPM provider. Note that TPM is not recommended for user keys. Use TPM for the registration authority key only. If you plan to run your FAS server in a virtualized environment, check with your TPM and hypervisor vendor whether virtualization is supported.
HSM_Vendor CSP/Key Storage Provider	Supplied by HSM vendor. The value differs between vendors. If you plan to run your FAS server in a virtualized environment, check with your HSM vendor whether virtualization is supported.

Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.**ProviderType** (Required only in case of CAPI API)

Value	Comment
24	Default. Refers to Microsoft KeyContainerPermissionAccessEntry.ProviderType Property PROV_RSA_AES 24. Should always be 24 unless you are using an HSM with CAPI and the HSM vendor specifies otherwise.

Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.**KeyProtection** (When FAS needs to perform a private key operation, it uses the value specified here) Controls the “exportable” flag of private keys. Allows the use of TPM key storage, if supported by the hardware.

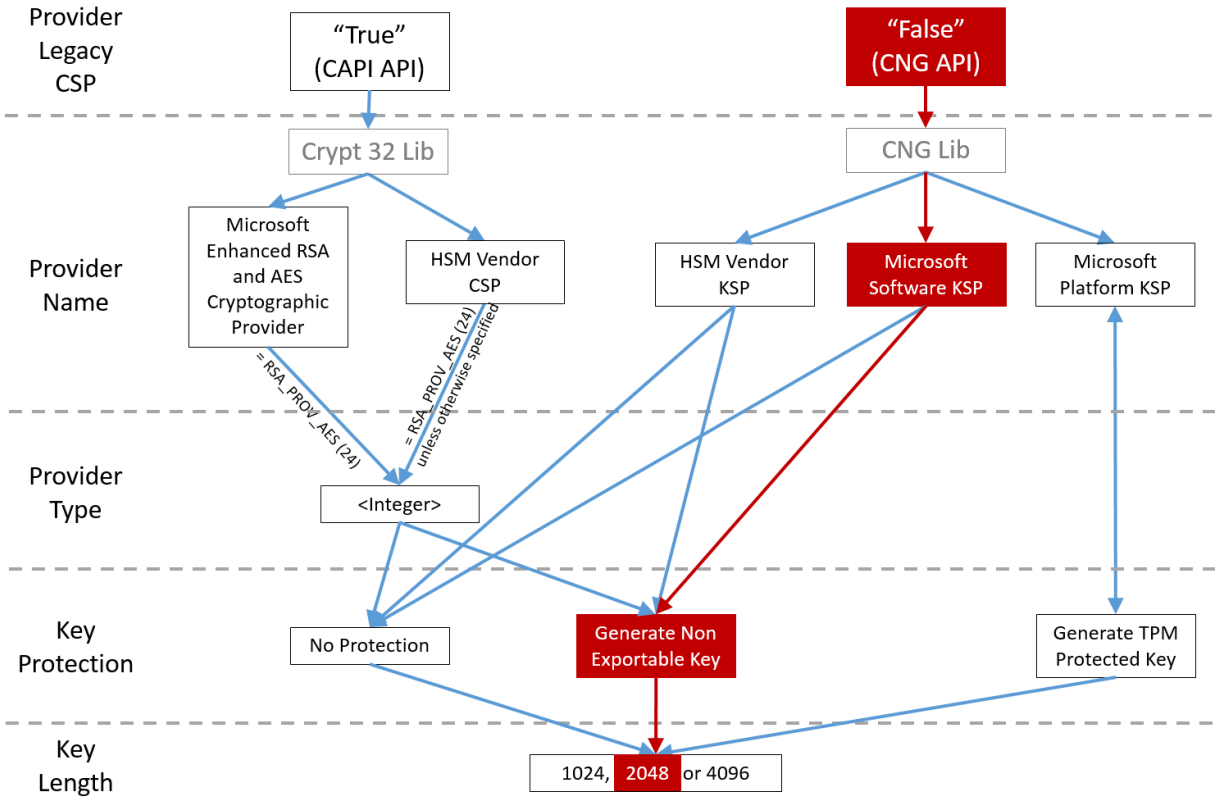
Value	Comment
NoProtection	Private key can be exported.
GenerateNonExportableKey	Default. Private key cannot be exported.

Value	Comment
GenerateTPMProtectedKey	Private key will be managed using the TPM. Private key is stored via the ProviderName you specified in ProviderName (for example, Microsoft Platform Key Storage Provider)

Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.**KeyLength** (Specify size of private key in bits)

Value	Comment
2048	Default. 1024 or 4096 can also be used.

The config file settings are represented graphically as follows (installation defaults are shown in red):



Configuration scenario examples

Example 1

This example covers the registration authority certificate private key and user certificates' private keys stored using the Microsoft Software Key Storage Provider

This is the default post-install configuration. No additional private key configuration is required.

Example 2

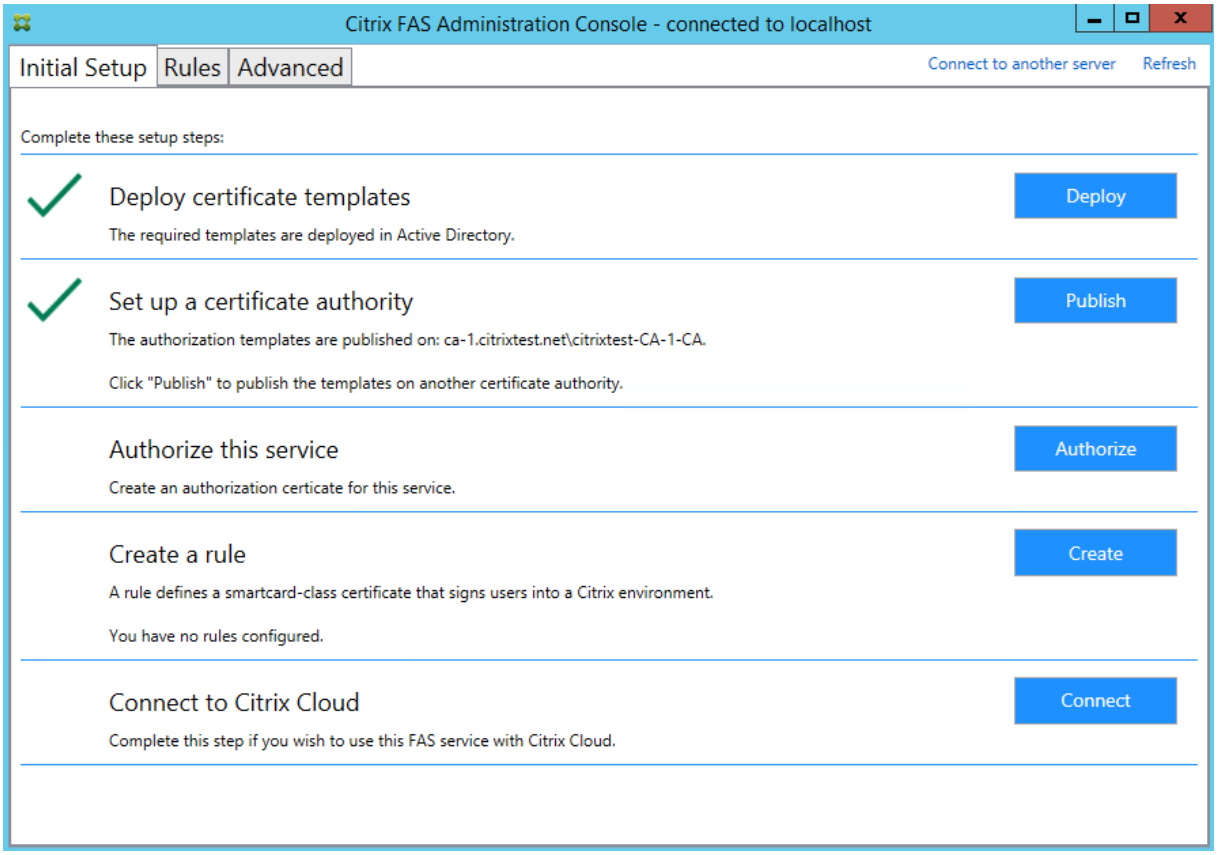
This example shows the registration authority certificate private key stored in the FAS server motherboard's hardware TPM via the Microsoft Platform Key Storage Provider, and user certificates' private keys stored using the Microsoft Software Key Storage Provider.

This scenario assumes that the TPM on your FAS server motherboard has been enabled in the BIOS according to the TPM manufacturer's documentation and then initialized in Windows; see https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-vista/cc749022(v=ws.10).

Using PowerShell (recommended)

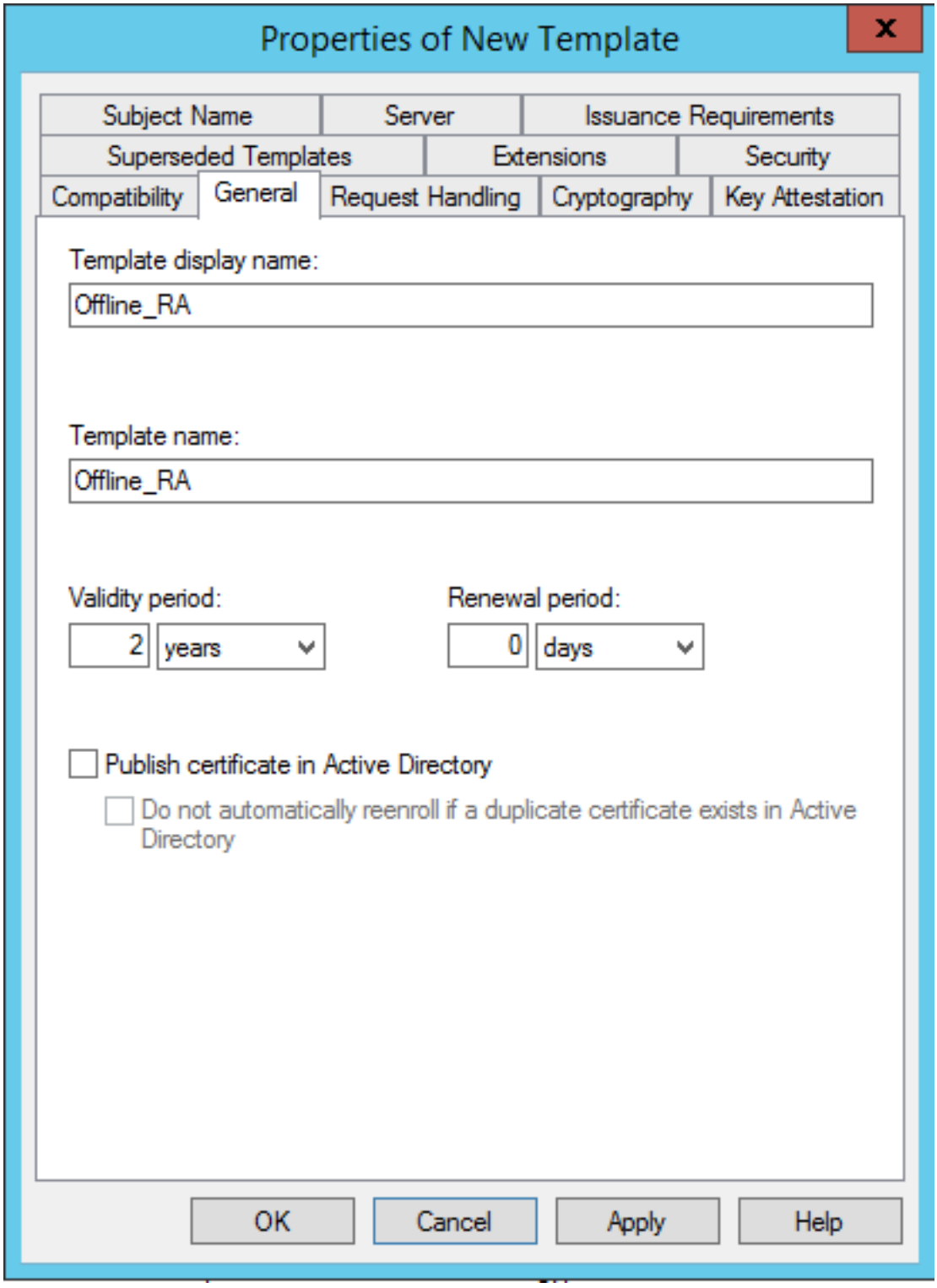
The registration authority certificate can be requested offline using PowerShell. This is recommended for organizations that do not want their certificate authority to issue a registration authority certificate through an online certificate signing request. An offline registration authority certificate signing request cannot be made using the FAS administration console.

Step 1: During the initial FAS configuration using the administration console, complete only the first two steps: "Deploy certificate templates" and "Set up a certificate authority."



Step 2: On your certificate authority server, add the Certificate Templates MMC snap-in. Right-click the **Citrix_RegistrationAuthority_ManualAuthorization** template and select **Duplicate Template**.

Select the **General** tab. Change the name and validity period. In this example, the name is *Offline_RA* and the validity period is 2 years:



Step 3: On your certificate authority server, add the certificate authority MMC snap-in. Right-click **Certificate Templates**. Select **New**, then click **Certificate Template to Issue**. Choose the template you just created.

Step 4: Load the following PowerShell cmdlets on the FAS server:


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

Step 5: Generate the RSA keypair inside the FAS server's TPM and create the certificate signing request by entering the following PowerShell cmdlet on the FAS server. **Note:** Some TPMs restrict key length. The default key length is 2048 bits. Be sure to specify a key length supported by your hardware.

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

For example:

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

The following is displayed:

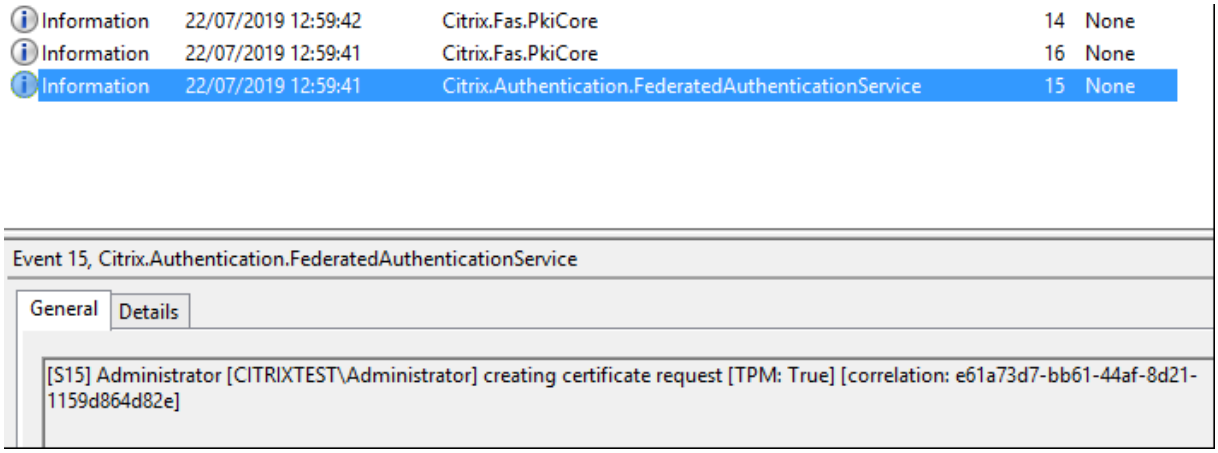
```
PS C:\Users\Administrator.AUTH> New-UcsAuthorizationCertificateRequest -UseTPM $true -address ucshsm.auth.local

Id                  : 5ac3d8bd-b484-4ebe-abf8-4b2cfd62ca39
Address             : [Offline CSR]
TrustArea           :
CertificateRequest  : -----BEGIN CERTIFICATE REQUEST-----
                      MIICaDCCAVACAQIwIzEhMB8GCgmSJomT8ixkARkWEUNpdHJpeFRydXNORmFicmljMIIBIjANBgkq
                      hkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAwAtwoCLXJuJ3yIscT8Y5v/7zuYqBhbHkhZV3wTNfROXW
                      1hCMwi7X4YpTE7CbJtgiFY/9SEBa9StGeTVpeJi66gKoZCdxydc2BwX6JNZrLi9hAf1bInFPgrz+
                      vbG3YjKuKtK35JpGqYWjUEDzKiQFaob3Dkh/pwP3V7OcEYthxB8CfbaN9MHOEFbepoSYOCAfunXW
                      snwIbXD9lc/fGyN/3f94P4fbNrjEIOHc+4Oy/WsPgPRgcq9XBwRjzpGj0gOWRoJS9g22DY5PwD77
                      7f7vZvoQkRy5NXXXATJ+xxYEPLp9JuJaElWXrTJG+XP3SnG/oCCPit7iUIIc9FjGa3qTUQIDAQAB
                      oAAwDQYJKoZIhvcNAQENBQADggEBAIJV8jR9XWHlvztpjxPeJzAVOsrLpOsCfNdvYn9u+I7J8Gsr
                      4tuLjuQ+An4Y2Rw7b6pZxEICV8rqd5Gy+wtPnUZoAf6eLg1Vht2RVfb6d7Ns6+Mc+F5bFegLHs8c
                      YlITHOtmcHFKt4Loz5O5E+tQw39MProEj3p7GwF7HrGY+QSbFD38rbL19Z5cfNYYqMbsgyMgdR8F
                      3SmagQjN3C8lyqT8z1iF4l32xlmQrP/4XQvr1F+TO15PM5Fxjj6PEKWopWTYZXGzSC1ufxevcD1K
                      +tTH9tQYJM6xw3+6TIcfuWDjrd8KJjTdC5SMu7LJuIajTNZ5Z+1eM61TATO3XG/AB7o=
                      -----END CERTIFICATE REQUEST-----
Status              : WaitingForApproval


PS C:\Users\Administrator.AUTH> _
```

Notes:

- The Id GUID (in this example, "5ac3d8bd-b484-4ebe-abf8-4b2cfd62ca39") is required in a subsequent step.
- Think of this PowerShell cmdlet as a one-time "override" that is used to generate the private key for the registration authority certificate.
- When running this cmdlet, the values that are read from the config file when FAS started are checked to determine the key length to use (the default is 2048).
- Because -UseTPM is set to $true in this manual PowerShell-initiated registration authority certificate private key operation, the system ignores values from the file that do not match the settings required to use a TPM.

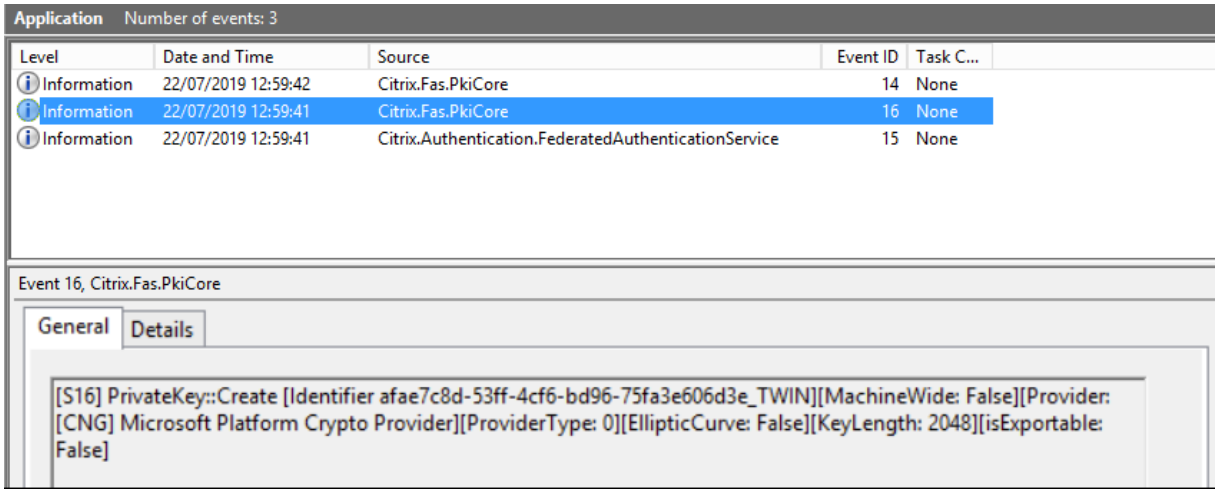
- Running this cmdlet does not change any settings in the config file.
- During subsequent automatic FAS-initiated user certificate private key operations, the values that were read from the file when FAS started are used.
- It is also possible to set the KeyProtection value in the config file to GenerateTPMProtectedKey when the FAS server is issuing user certificates to generate user certificate private keys protected by the TPM.

To verify that the TPM was used to generate the keypair, look in the application log in the Windows Event viewer on the FAS server, at the time that the keypair is generated.



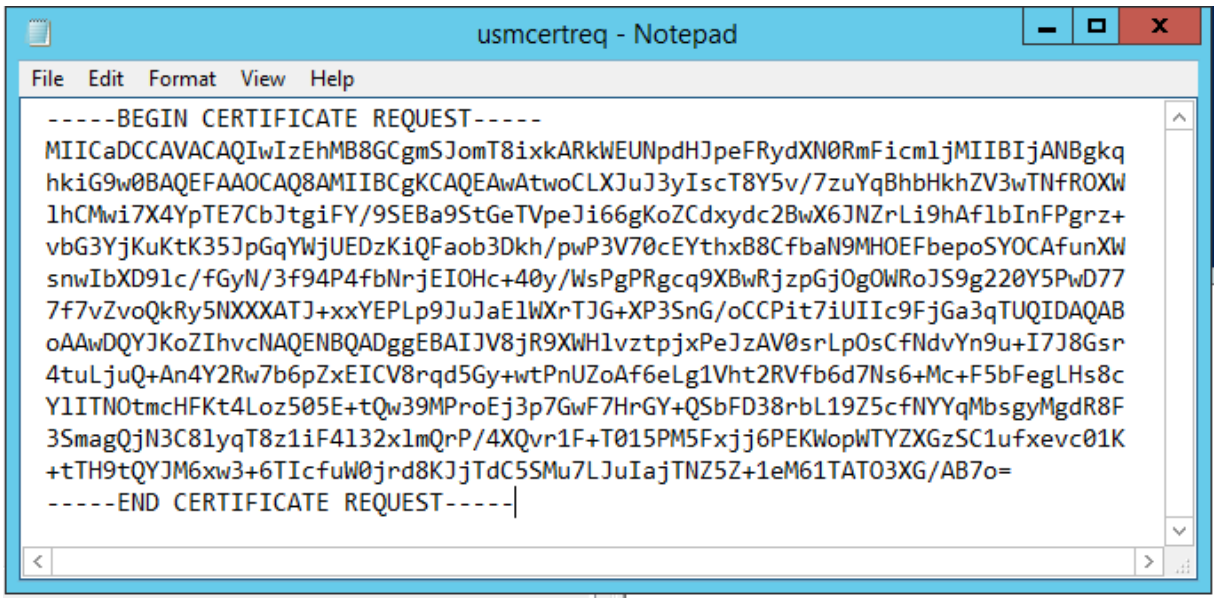
Note: “[TPM: True]”

Followed by:



Note: “Provider: [CNG] Microsoft Platform Crypto Provider”

Step 6: Copy the certificate request section into a text editor and save it to disk as a text file.



Step 7: Submit the certificate signing request to your certificate authority by typing the following into PowerShell on the FAS server:

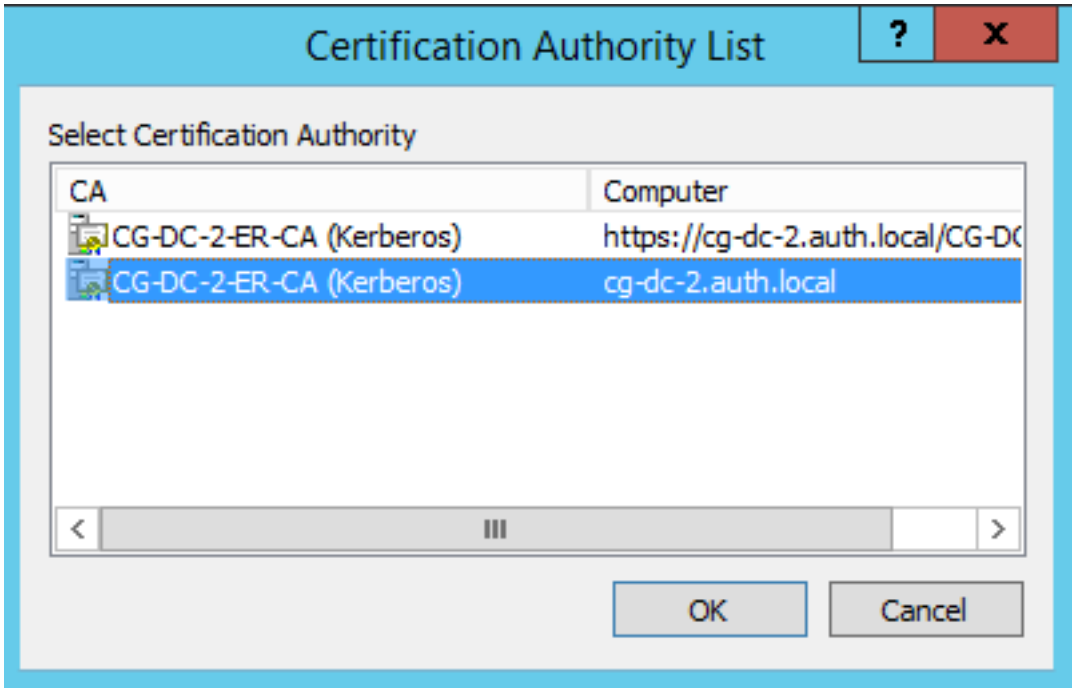
```
certreq -submit -attrib "certificatetemplate:\<certificate template
    from step 2>" \<certificate request file from step 6>
```

For example:

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

The following is displayed:

At this point a Certification Authority List window might appear. The certificate authority in this example has both http (top) and DCOM (bottom) enrolment enabled. Select the DCOM option, if available:

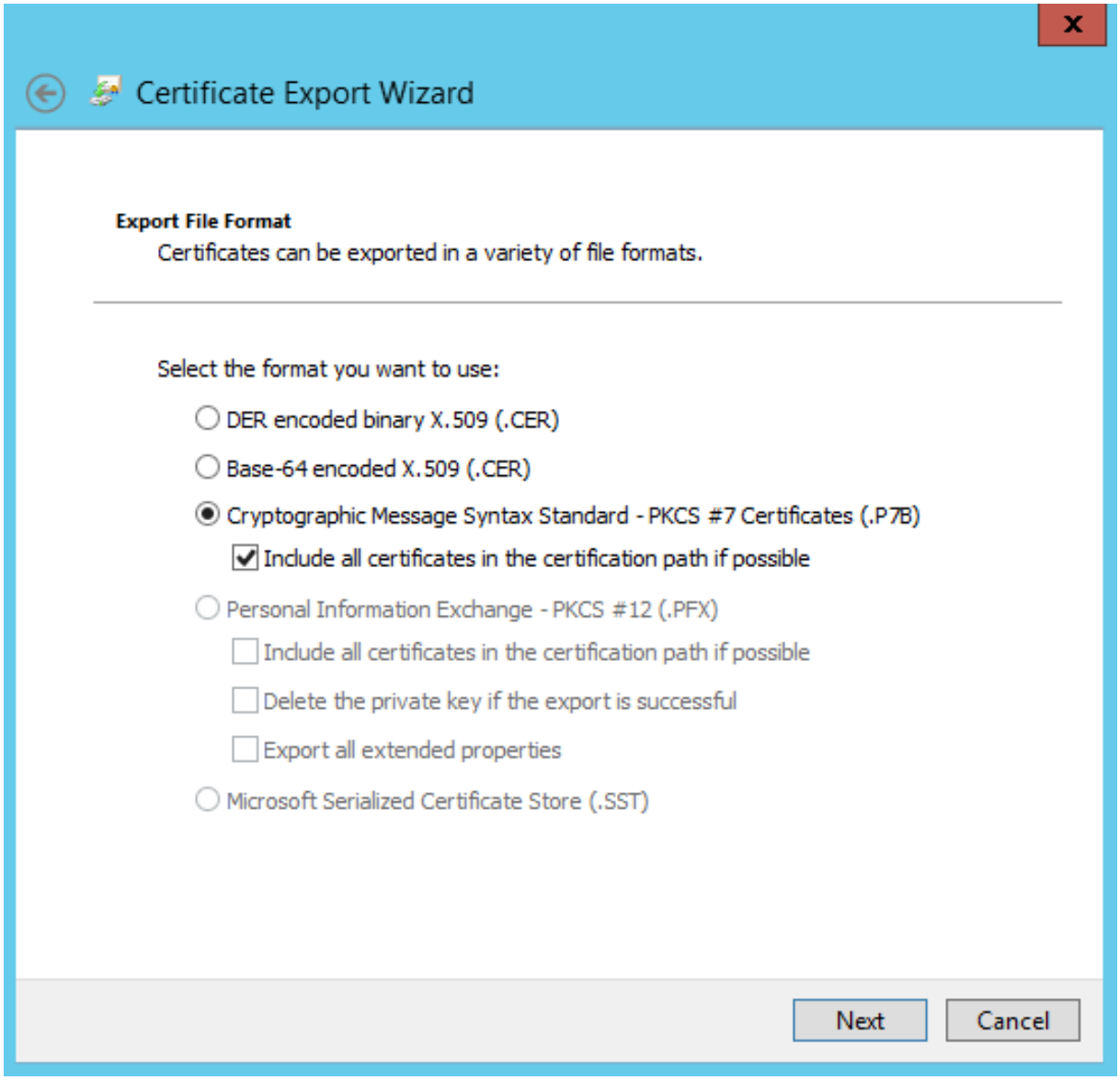


After the certificate authority has been specified, PowerShell displays the RequestID:

```
PS C:\Users\Administrator.AUTH> certreq -submit -attrib "certificatetemplate:Offline_RA" C:\Users\Administrator.AUTH\Des
ktop\usmcertreq.txt
Active Directory Enrollment Policy
  {4F7616DE-DB0C-4D21-A4FD-2E29502177C2}
  ldap:
RequestId: 106
RequestId: "106"
Certificate request is pending: Taken Under Submission (0)
PS C:\Users\Administrator.AUTH>
```

Step 8: On the certificate authority server, in the certificate authority MMC snap-in, click **Pending Requests**. Note the Request ID. Then right-click the request and choose **Issue**.

Step 9: Select the **Issued Certificates** node. Find the certificate that was just issued (the Request ID should match). Double-click to open the certificate. Select the **Details** tab. Click **Copy to File**. The Certificate Export Wizard launches. Click **Next.** Choose the following options for the file format:



The format must be "**Cryptographic Message Syntax Standard – PKCS #7 Certificates (.P7B)**" and "**Include all certificates in the certification path if possible**" must be selected.

Step 10: Copy the exported certificate file onto the FAS server.

Step 11: Import the registration authority certificate into the FAS server by entering the following PowerShell cmdlet on the FAS server:

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

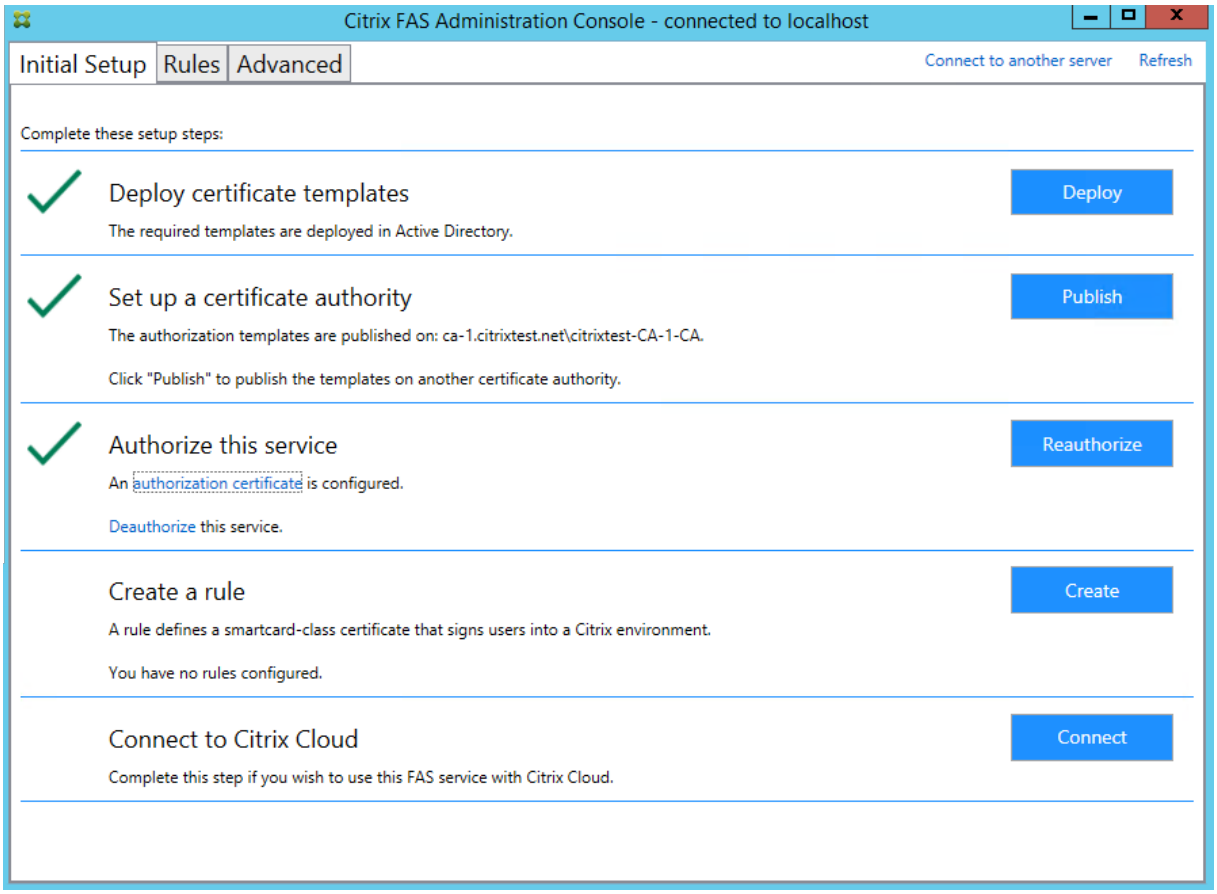
For example:

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


The following is displayed:

```
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
```

Step 12: Close the FAS administration console and then restart it.



Note: The step “Authorize this service” has a green tick.

Step 13: Select the **Rules** tab in the FAS administration console and edit the settings described in Install and configure.

Using the FAS management console

The FAS management console cannot perform offline certificate signing request, so using it is not recommended unless your organization allows online certificate signing request for registration authority certificates.

When performing initial FAS setup, after deploying certificate templates and setting up the certificate authority, but before authorizing the service (step 3 in the configuration sequence):

Step 1: Edit the config file by changing the following line as follows:

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

The file should now appear as follows:

```
<?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>
```

Some TPMs restrict key length. The default key length is 2048 bits. Ensure that you specify a key length supported by your hardware.

Step 2: Authorize the service.

Step 3: Manually issue the pending certificate request from the certificate authority server. After the registration authority certificate is obtained, step 3 in the setup sequence in the management console will be green. At this point, the registration authority certificate's private key will have generated in the TPM. The certificate will be valid for 2 years by default.

Step 4: Edit the config file back to the following:

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

> **Note:**
>
> Although FAS can generate user certificates with TPM protected keys, the TPM hardware may be too slow for large deployments.

Step 5: Restart FAS. This forces the service to re-read the config file and reflect the changed values. The subsequent automatic private key operations will affect user certificate keys; those operations will not store the private keys in the TPM, but use the Microsoft Software Key Storage Provider.

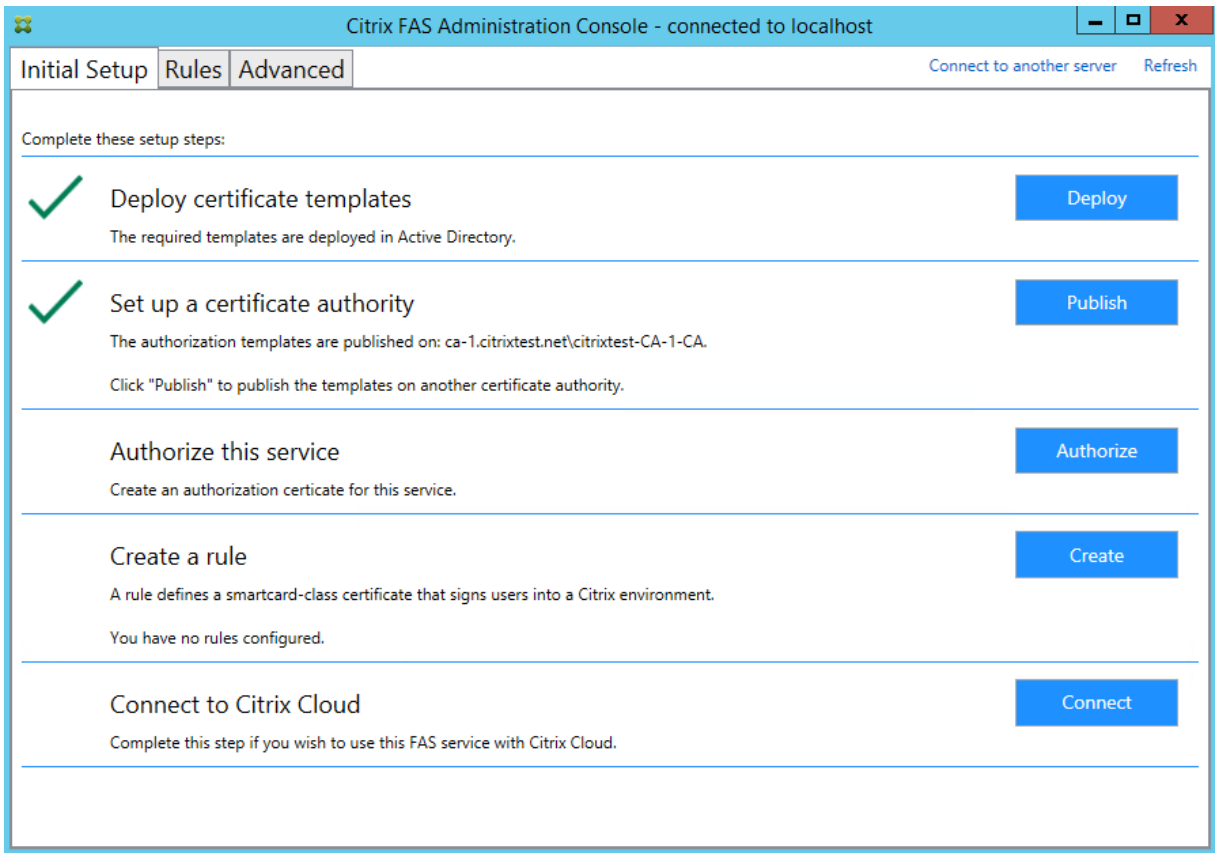
Step 6: Select the **Rules** tab in the FAS administration console and edit the settings as described in Install and configure.

Example 3

This example covers an registration authority certificate private key and user certificates' private keys stored in an HSM. This example assumes a configured HSM. Your HSM will have a provider name, for example "HSM_Vendor's Key Storage Provider."

If you plan to run your FAS server in a virtualized environment, check with your HSM vendor about hypervisor support.

Step 1. During initial setup of FAS using the administration console, complete only the first two steps: "Deploy certificate templates" and "Set up a certificate authority."



Step 2: Consult your HSM vendor's documentation to determine what your HSM's ProviderName value should be. If your HSM uses CAPI, the provider might be referred to in the documentation as a Cryptographic Service Provider (CSP). If your HSM uses CNG, the provider might be referred to as a Key Storage Provider (KSP).

Step 3: Edit the config file as follows:

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

The file should now appear as follows:


```
<?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>
```

This scenario assumes that your HSM uses CNG, so the ProviderLegacyCsp value is set to false. If your HSM uses CAPI, ProviderLegacyCsp value should be set to true. Consult your HSM vendor's documentation to determine whether your HSM uses CAPI or CNG. Also consult your HSM vendor's documentation on supported key lengths for asymmetric RSA key generation. In this example, the key length is set to the default of 2048 bits. Ensure that the key length you specify is supported by your hardware.

Step 4: Restart the Citrix Federated Authentication Service to read the values from the config file.

Step 5: Generate the RSA keypair inside the HSM and create the certificate signing request by clicking **Authorize** in the **Initial Setup** tab of FAS administration console.

Step 6: To verify that the keypair was generated in the HSM, check the application entries in the Windows Event log:

```
[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]
```

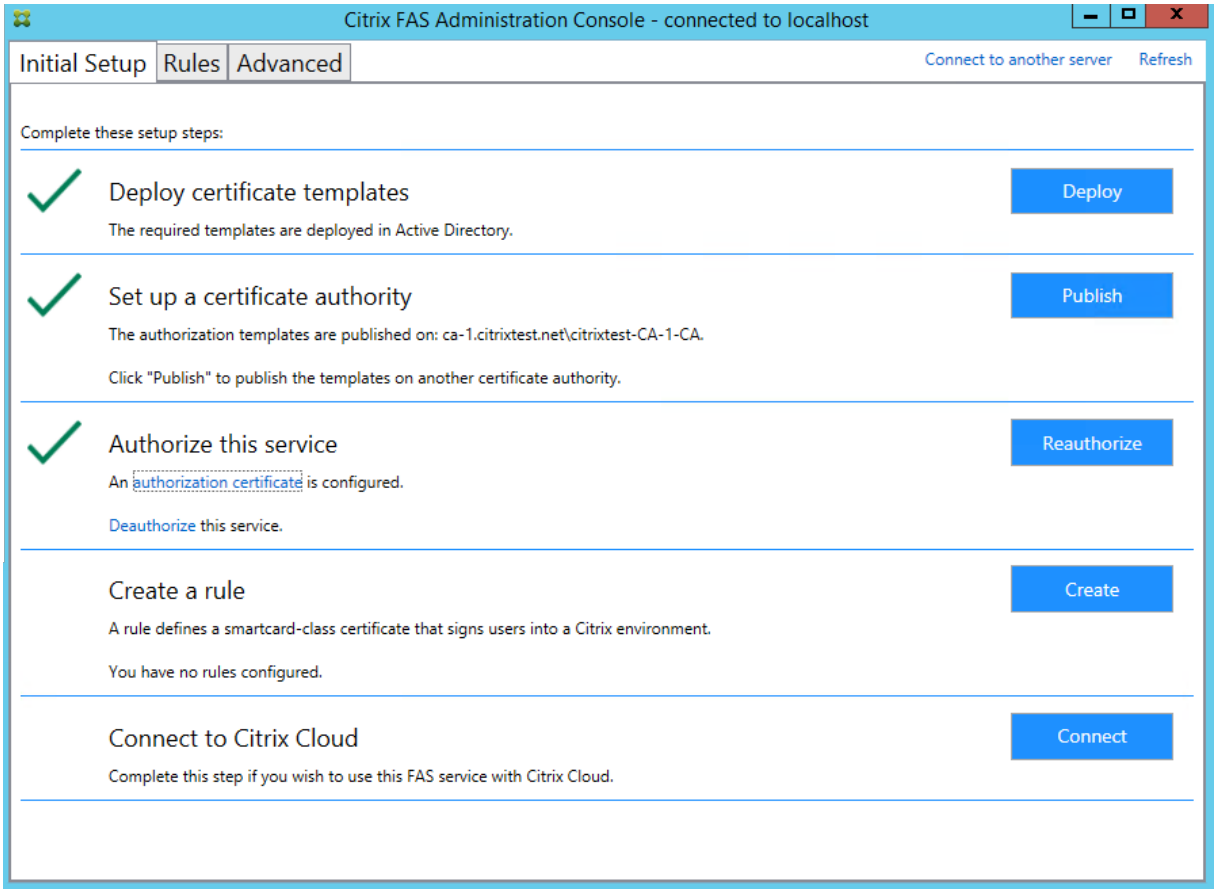
Note: [Provider: [CNG] HSM_Vendor's Key Storage Provider]

Step 7: On the certificate authority server, in the certificate authority MMC, select the **Pending Requests** node:

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$	

Right-click the request and select **Issue**.

Note: The step "Authorize this service" has a green tick.



Step 8: Select the **Rules** tab in FAS administration console and edit the settings as described in Install and configure.

FAS certificate storage

FAS does not use the Microsoft certificate store on the FAS server to store its certificates. It uses an embedded database.

To determine the GUID for the registration authority certificate, enter the following PowerShell cmdlets on the FAS server:

```
Add-pssnapin Citrix.a\*
Get-FasAuthorizationCertificate -address \<FAS server FQDN>
```

For example, **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+vdgWg86DFRVxTORholV86iazDZyOiYGgxe9/s8YZzCspVWN1nB1
                     zXOUJfo1qo9UsmImYr7MR/dhGAtkfsFUoPcd2+zcezmgOfq/4vmCIuerwqzRR5T/p4og7+IjR1se
                     ECz/CbXR0OuiDhW+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
```

To obtain a list of user certificates, enter:

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

For example, **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
```

Note:

When using an HSM to store private keys, HSM containers are identified with a GUID. The GUID for the private key in the HSM can be obtained using:

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

For example:

```
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
```

Related information

- Install and configure is the primary reference for FAS installation and configuration.
- The common FAS deployments are summarized in the Federated Authentication Services architectures overview article.
- Other "how-to" articles are introduced in the Advanced configuration article.

Security and network configuration

July 1, 2020

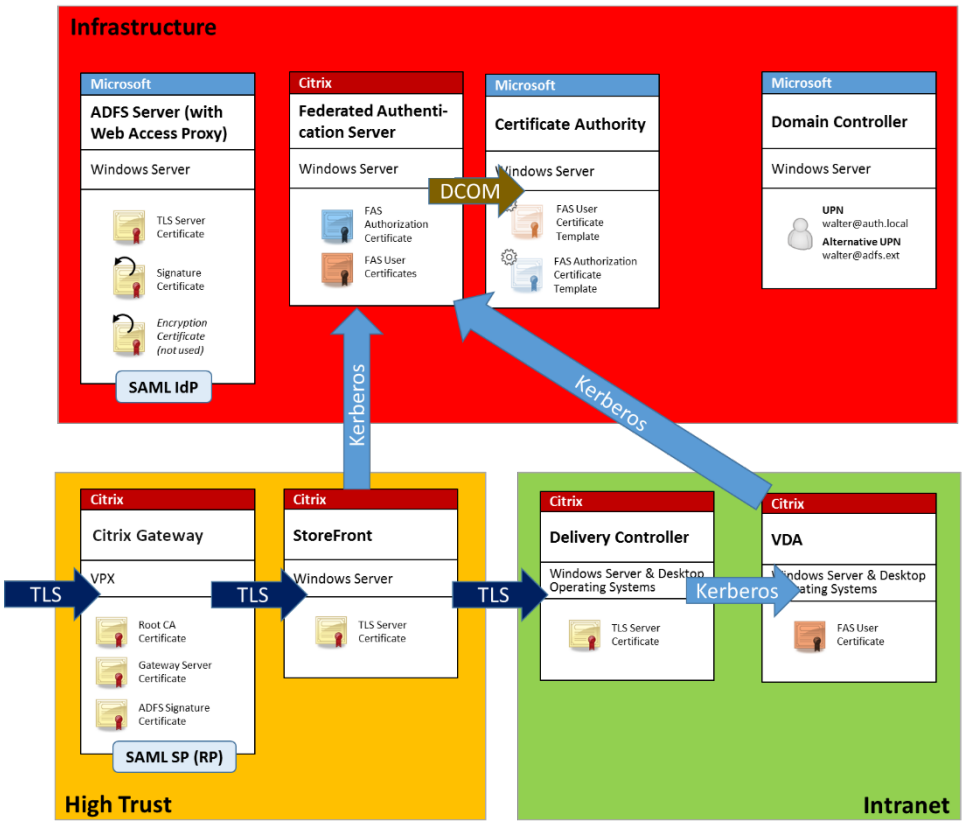
Federated Authentication Service (FAS) is tightly integrated with Microsoft Active Directory and the Microsoft certification authority. It is essential to ensure that the system is managed and secured appropriately, developing a security policy as you would for a domain controller or other critical infrastructure.

This document provides an overview of security issues to consider when deploying FAS. It also provides an overview of features available that may assist in securing your infrastructure.

Network architecture

The following diagram shows the main components and security boundaries used in a FAS deployment.

The FAS server should be treated as part of the security-critical infrastructure, along with the certificate authority and domain controller. In a federated environment, Citrix Gateway and Citrix StoreFront are components that are trusted to perform user authentication; other Citrix Virtual Apps and Desktops components are unaffected by introducing FAS.



Firewall and network security

Communication between Citrix Gateway, StoreFront and the Delivery Controller components should be protected by TLS over port 443. The StoreFront server performs only outgoing connections, and the Citrix Gateway should accept only connections over the Internet using HTTPS port 443.

The StoreFront server contacts the FAS server over port 80 using mutually authenticated Kerberos. Authentication uses the Kerberos HOST/fqdn identity of the FAS server, and the Kerberos machine account identity of the StoreFront server. This generates a single use “credential handle” needed by the Citrix Virtual Delivery Agent (VDA) to log on the user.

When an HDX session is connected to the VDA, the VDA also contacts the FAS server over port 80. Authentication uses the Kerberos HOST/fqdn identity of the FAS server, and the Kerberos machine identity of the VDA. Additionally, the VDA must supply the “credential handle” to access the certificate and private key.

The Microsoft certificate authority accepts communication using Kerberos authenticated DCOM, which can be configured to use a fixed TCP port. The certificate authority additionally requires that the FAS server supply a CMC packet signed by a trusted enrollment agent certificate.

Server	Firewall Ports
Federated Authentication Service	[in] Kerberos over HTTP from StoreFront and VDAs, [out] DCOM to Microsoft certificate authority
Citrix Gateway	[in] HTTPS from client machines, [in/out] HTTPS to/from StoreFront server, [out] HDX to VDA
StoreFront	[in] HTTPS from Citrix Gateway, [out] HTTPS to Delivery Controller, [out] Kerberos HTTP to FAS
Delivery Controller	[in] HTTPS from StoreFront server, [in/out] Kerberos over HTTP from VDAs
VDA	[in/out] Kerberos over HTTP from Delivery Controller, [in] HDX from Citrix Gateway, [out] Kerberos HTTP to FAS
Microsoft certificate authority	[in] DCOM & signed from FAS

Administration responsibilities

Administration of the environment can be divided into the following groups:

Name	Responsibility
Enterprise administrator	Install and secure certificate templates in the forest
Domain administrator	Configure Group Policy settings
Certificate authority administrator	Configure the certificate authority
FAS administrator	Install and configure the FAS server
StoreFront/Citrix Gateway administrator	Configure user authentication
Citrix Virtual Desktops administrator	Configure VDAs and Controllers

Each administrator controls different aspects of the overall security model, allowing a defense-in-depth approach to securing the system.

Group Policy settings

Trusted FAS machines are identified by a lookup table of "index number -> FQDN" configured through Group Policy. When contacting a FAS server, clients verify the FAS server's `HOST\<fqdn>` Kerberos identity. All servers that access the FAS server must have identical FQDN configurations for the same index; otherwise, StoreFront and VDAs may contact different FAS servers.

To avoid misconfiguration, Citrix recommends that a single policy be applied to all machines in the environment. Take care when modifying the list of FAS servers, especially when removing or reordering entries.

Control of this GPO should be limited to FAS administrators (and/or domain administrators) who install and decommission FAS servers. Take care to avoid reusing a machine FQDN name shortly after decommissioning a FAS server.

Certificate templates

If you do not want to use the Citrix_SmartcardLogon certificate template supplied with FAS, you can modify a copy of it. The following modifications are supported.

Rename a certificate template

If you want to rename the Citrix_SmartcardLogon to match your organizational template naming standard, you must:

- Create a copy of the certificate template and rename it to match your organizational template naming standard.
- Use FAS PowerShell commands to administer FAS, rather than the administrative user interface. (The administrative user interface is only intended for use with the Citrix default template names.)
  - Either use the Microsoft MMC Certificate Templates snap-in or the Publish-FasMsTemplate command to publish your template, and
  - Use the New-FasCertificateDefinition command to configure FAS with the name of your template.

Modify General properties

You can modify the Validity period in the certificate template.

Do not modify the Renewal period. FAS ignores this setting in the certificate template. FAS automatically renews the certificate halfway through its validity period.

Modify Request Handling properties

Do not modify these properties. FAS ignores these settings in the certificate template. FAS always deselects **Allow private key to be exported** and deselects **Renew with same key**.

Modify Cryptography properties

Do not modify these properties. FAS ignores these settings in the certificate template.

Refer to Private key protection for equivalent settings that FAS provides.

Modify Key Attestation properties

Do not modify these properties. FAS does not support key attestation.

Modify Superseded Templates properties

Do not modify these properties. FAS does not support superseding templates.

Modify Extensions properties

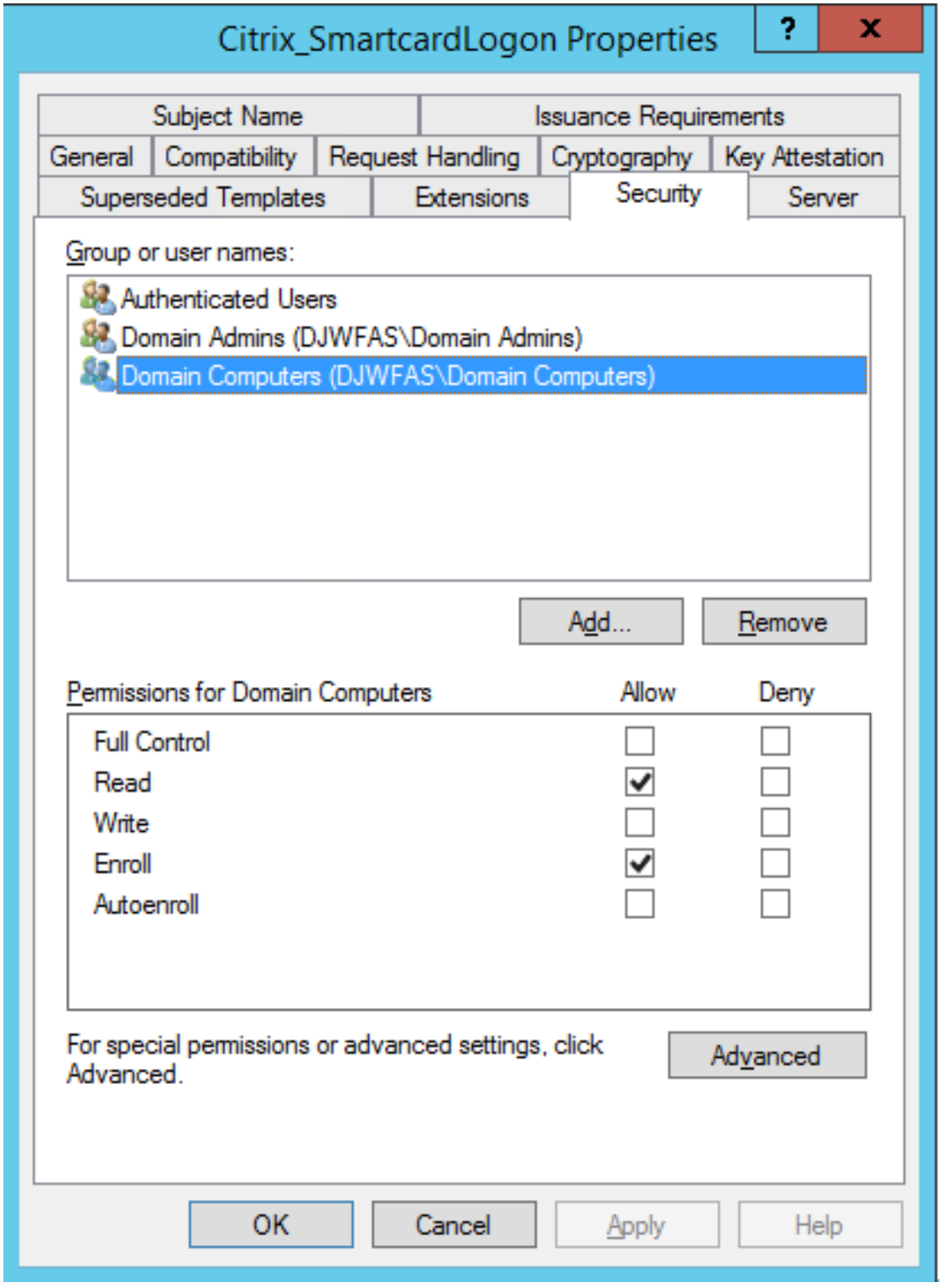
You can modify these settings to match your organizational policy.

Note: Inappropriate Extension settings may cause security issues, or result in unusable certificates.

Modify Security properties

Citrix recommends that you modify these settings to Allow the **Read** and **Enroll** permissions for only the machine accounts of the FAS servers. No other permissions are required by the FAS service. However, as with other certificate templates, you may want to:

- allow administrators to Read or Write the template
- allow authenticated users to Read the template



Modify Subject Name properties

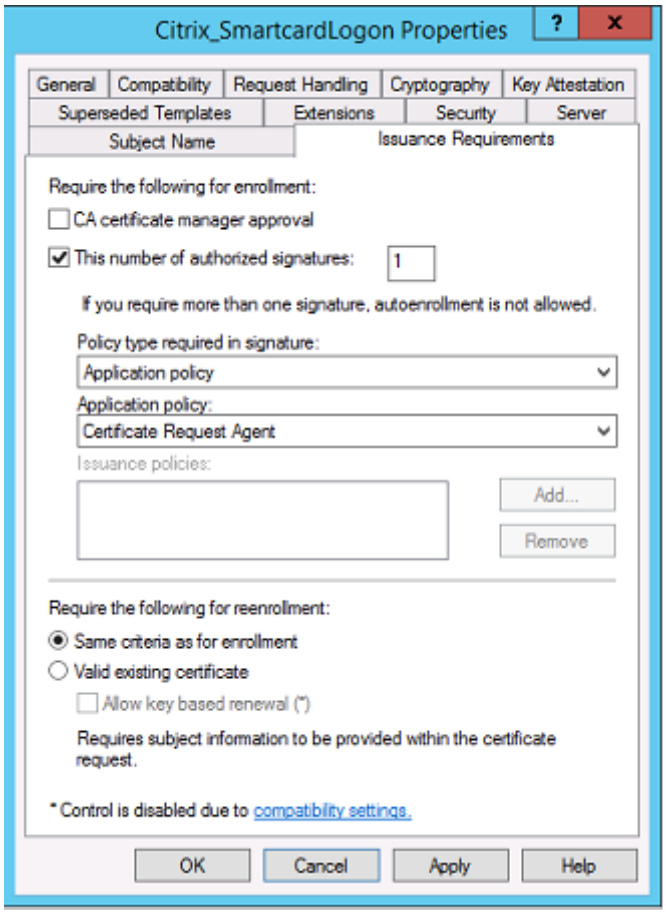
You can modify these settings to match your organizational policy, if needed.

Modify Server properties

Although Citrix does not recommend it, you can modify these settings to match your organizational policy, if needed.

Modify Issuance requirements properties

Do not modify these settings. These settings should be as shown:



Modify Compatibility properties

You can modify these settings. The setting must be at least **Windows Server 2003 CAs** (schema version 2). However, FAS supports only Windows Server 2008 and later CAs. Also, as explained above, FAS ignores the additional settings available by selecting **Windows Server 2008 CAs** (schema version 3) or **Windows Server 2012 CAs** (schema version 4).

Certificate authority administration

The certificate authority administrator is responsible for the configuration of the certificate authority server and the issuing certificate private key that it uses.

Publishing templates

For a certificate authority to issue certificates based on a template supplied by the enterprise administrator, the certificate authority administrator must choose to publish that template.

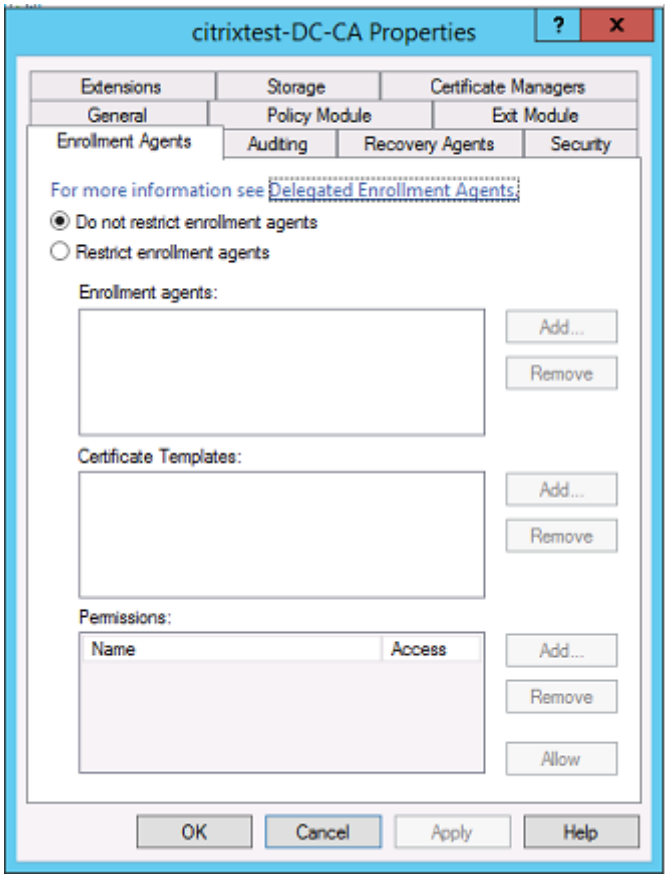
A simple security practice is to publish only the registration authority certificate templates when FAS servers are being installed, or to insist on a completely offline issuance process. In either case, the certificate authority administrator should maintain complete control over authorizing registration authority certificate requests, and have a policy for authorizing FAS servers.

Firewall settings

Generally, the certificate authority administrator will also have control of the network firewall settings of the certificate authority, allowing control over incoming connections. The certificate authority administrator can configure DCOM TCP and firewall rules so that only FAS servers can request certificates.

Restricted enrollment

By default any holder of an registration authority certificate can issue certificates to any user, using any certificate template that allows access. This should be restricted to a group of non-privileged users using the “Restrict enrollment agents” certificate authority property.



Policy modules and auditing

For advanced deployments, custom security modules can be used to track and veto certificate issuance.

FAS administration

FAS has several security features.

Restrict StoreFront, users, and VDAs through an ACL

At the center of the FAS security model is the control for which Kerberos accounts can access functionality:

Access Vector	Description
StoreFront [IdP]	These Kerberos accounts are trusted to declare that a user has been correctly authenticated. If one of these accounts is compromised, then certificates can be created and used for users allowed by the configuration of FAS.
VDAs [Relying party]	These are the machines that are allowed to access the certificates and private keys. A credential handle retrieved by the IdP is also needed, so a compromised VDA account in this group has limited scope to attack the system.
Users	This controls which users can be asserted by the IdP. Note that there is overlap with the "Restricted Enrollment Agent" configuration options at the certificate authority. In general, it is advisable to include only non-privileged accounts in this list. This prevents a compromised StoreFront account from escalating privileges to a higher administrative level. In particular, domain administrator accounts should not be allowed by this ACL.

Configure rules

Rules are useful if multiple independent Citrix Virtual Apps or Citrix Virtual Desktops deployments use the same FAS server infrastructure. Each rule has a separate set of configuration options; in particular, the ACLs can be configured independently.

Configure the certificate authority and templates

Different certificate templates and CAs can be configured for different access rights. Advanced configurations may choose to use less or more powerful certificates, depending on the environment. For example, users identified as "external" may have a certificate with fewer privileges than "internal" users.

In-session and authentication certificates

The FAS administrator can control whether the certificate used to authenticate is available for use in the user's session. For example, this could be used to have only "signing" certificates available in-session, with the more powerful "logon" certificate being used only at logon.

Private key protection and key length

The FAS administrator can configure FAS to store private keys in a Hardware Security Module (HSM) or Trusted Platform Module (TPM). Citrix recommends that at least the registration authority certificate private key is protected by storing it in a TPM; this option is provided as part of the "offline" certificate request process.

Similarly, user certificate private keys can be stored in a TPM or HSM. All keys should be generated as "non-exportable" and be at least 2048 bits in length.

Event logs

The FAS server provides detailed configuration and runtime event logs, which can be used for auditing and intrusion detection.

Administrative access and administration tools

FAS includes remote administration features (mutually authenticated Kerberos) and tools. Members of the "Local Administrators Group" have full control over FAS configuration. This list should be carefully maintained.

Citrix Virtual Apps, Citrix Virtual Desktops, and VDA administrators

In general, the use of FAS does not change the security model of the Delivery Controller and VDA administrators, as the FAS "credential handle" simply replaces the "Active Directory password." Controller and VDA administration groups should contain only trusted users. Auditing and event logs should be maintained.

General Windows server security

All servers should be fully patched and have standard firewall and anti-virus software available. Security-critical infrastructure servers should be kept in a physically secure location, with care taken over disk encryption and virtual machine maintenance options.

Auditing and event logs should be stored securely on a remote machine.

RDP access should be limited to authorized administrators. Where possible, user accounts should require smart card logon, especially for certificate authority and domain administrator accounts.

Related information

- Install and configure is the primary reference for FAS installation and configuration.
- FAS architectures are introduced in the Deployment architectures article.
- Other "how-to" articles are introduced in the Advanced configuration article.

Troubleshoot Windows logon issues

July 7, 2020

This article describes the logs and error messages Windows provides when a user logs on using certificates and/or smart cards. These logs provide information you can use to troubleshoot authentication failures.

Certificates and public key infrastructure

Windows Active Directory maintains several certificate stores that manage certificates for users logging on.

- **NTAuth certificate store**: To authenticate to Windows, the certificate authority immediately issuing user certificates (that is, no chaining is supported) must be placed in the NTAuth store. To see these certificates, from the certutil program, enter: certutil –viewstore –enterprise NTAuth.
- **Root and intermediate certificate stores:** Usually, certificate logon systems can provide only a single certificate, so if a chain is in use, the intermediate certificate store on all machines must include these certificates. The root certificate must be in the Trusted Root Store, and the penultimate certificate must be in the NTAuth store.
- **Logon certificate extensions and Group Policy:** Windows can be configured to enforce verification of EKUs and other certificate policies. See the Microsoft documentation: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/ff404287(v=ws.10).

Registry policy	Description
AllowCertificatesWithNoEKU	When disabled, certificates must include the smart card logon Extended Key Usage (EKU).

Registry policy	Description
AllowSignatureOnlyKeys	By default, Windows filters out certificates private keys that do not allow RSA decryption. This option overrides that filter.
AllowTimeInvalidCertificates	By default, Windows filters out expired certificates. This option overrides that filter.
EnumerateECCCerts	Enables elliptic curve authentication.
X509HintsNeeded	If a certificate does not contain a unique User Principal Name (UPN), or it could be ambiguous, this option allows users to manually specify their Windows logon account.
UseCachedCRLOnlyAnd, IgnoreRevocationUnknownErrors	Disables revocation checking (usually set on the domain controller).

- **Domain controller certificates**: To authenticate Kerberos connections, all servers must have appropriate "Domain Controller" certificates. These can be requested using the "Local Computer Certificate Personal Store" MMC snap-in menu.

UPN name and certificate mapping

It is recommended that user certificates include a unique User Principal Name (UPN) in the Subject Alternate Name extension.

UPN names in Active Directory

By default, every user in Active Directory has an implicit UPN based on the pattern <samUsername>@<domainNetB and <samUsername>@<domainFQDN>. The available domains and FQDNs are included in the RootDSE entry for the forest. Note that a single domain can have multiple FQDN addresses registered in the RootDSE.

Additionally, every user in Active Directory has an explicit UPN and altUserPrincipalNames. These are LDAP entries that specify the UPN for the user.

When searching for users by UPN, Windows looks first in the current domain (based on the identity of the process looking up the UPN) for explicit UPNs, then alterative UPNs. If there are no matches, it looks up the implicit UPN, which may resolve to different domains in the forest.

Certificate Mapping Service

If a certificate does not include an explicit UPN, Active Directory has the option to store an exact public certificate for each use in an "x509certificate" attribute. To resolve such a certificate to a user, a computer can query for this attribute directly (by default, in a single domain).

An option is provided for the user to specify a user account that speeds up this search, and also allows this feature to be used in a cross-domain environment.

If there are multiple domains in the forest, and the user does not explicitly specify a domain, the Active Directory rootDSE specifies the location of the Certificate Mapping Service. This is usually located on a global catalog machine, and has a cached view of all x509certificate attributes in the forest. This computer can be used to efficiently find a user account in any domain, based on only the certificate.

Control logon domain controller selection

When an environment contains multiple domain controllers, it is useful to see and restrict which domain controller is used for authentication, so that logs can be enabled and retrieved.

Control domain controller selection

To force Windows to use a particular Windows domain controller for logon, you can explicitly set the list of domain controllers that a Windows machine uses by configuring the lmhosts file: \Windows\System32\drivers\etc\lmhosts.

There is usually a sample file named "lmhosts.sam" in that location. Simply include a line:

1.2.3.4 dcnetbiosname #PRE #DOM:mydomai

Where "1.2.3.4" is the IP address of the domain controller named "dcnetbiosname" in the "mydomain" domain.

After a restart, the Windows machine uses that information to log on to mydomain. Note that this configuration must be reverted when debugging is complete.

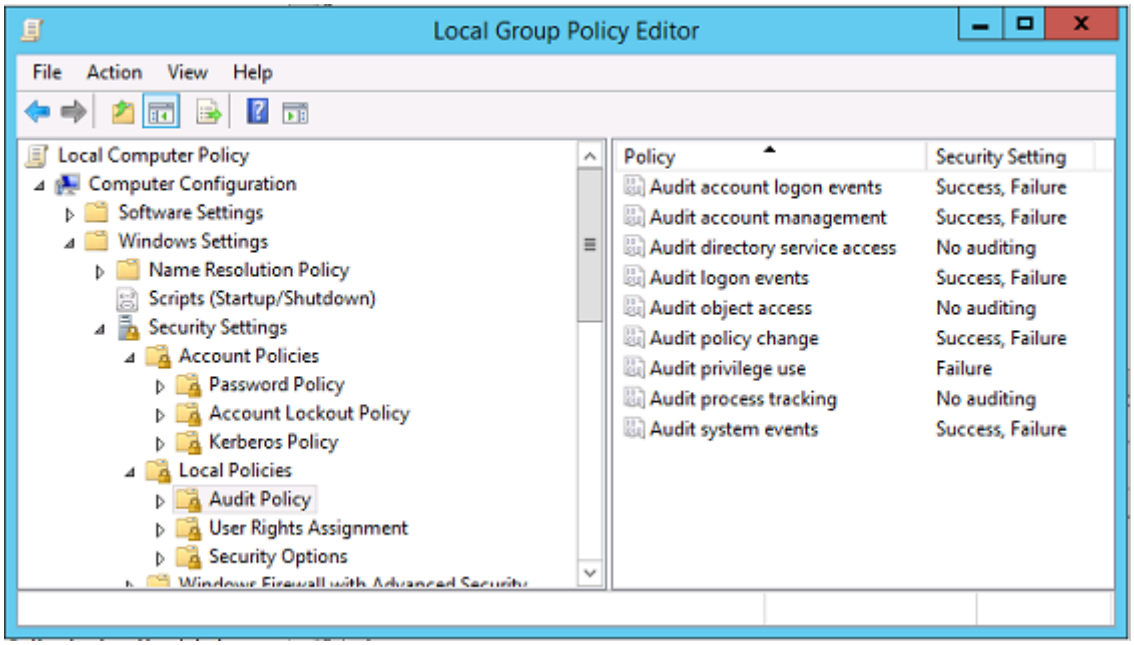
Identify the domain controller in use

At logon, Windows sets an MSDOS environment variable with the domain controller that logged the user on. To see this, start the command prompt with the command: **echo %LOGONSERVER%**.

Logs relating to authentication are stored on the computer returned by this command.

Enable account audit events

By default, Windows domain controllers do not enable full account audit logs. This can be controlled through audit policies in the security settings in the Group Policy editor. After they are enabled, the domain controller produces extra event log information in the security log file.



Certificate validation logs

Check certificate validity

If a smartcard certificate is exported as a DER certificate (no private key required), you can validate it with the command: certutil –verify user.cer

Enable CAPI logging

On the domain controller and users machine, open the event viewer and enable logging for Microsoft-/Windows/CAPI2/Operational Logs.

You can control CAPI logging with the registry keys at: CurrentControlSet\Services\crypt32.

Value	Description
DiagLevel (DWORD)	Verbosity level (0 to 5)
DiagMatchAnyMask (QUADWORD)	Event filter (use 0xffffff for all)
DiagProcessName (MULTI_SZ)	Filter by process name (for example, LSASS.exe)

CAPI logs

Message	Description
Build Chain	LSA called CertGetCertificateChain (includes result)
Verify Revocation	LSA called CertVerifyRevocation (includes result)
X509 Objects	In verbose mode, certificates and Certificate Revocation Lists (CRLs) are dumped to AppData\LocalLow\Microsoft\X509Objects
Verify Chain Policy	LSA called CertVerifyChainPolicy (includes parameters)

Error messages

Error code	Description
Certificate not trusted	The smart card certificate could not be built using certificates in the computer's intermediate and trusted root certificate stores.
Certificate revocation check error	The CRL for the smart card could not be downloaded from the address specified by the certificate CRL distribution point. If revocation checking is mandated, this prevents logon from succeeding. See the Certificates and public key infrastructure section.
Certificate Usage errors	The certificate is not suitable for logon. For example, it might be a server certificate or a signing certificate.

Kerberos logs

To enable Kerberos logging, on the domain controller and the end user machine, create the following registry values:

Hive	Value name	Value [DWORD]
CurrentControlSet\Control\Lsa	LogLevel	0x1
CurrentControlSet\Control\Lsa\Kerberos\Parameters		0xffffffff
CurrentControlSet\Services\Kd	KdcDebugLevel	0x1
CurrentControlSet\Services\Kdc	KdcExtraLogLevel	0x1f

Kerberos logging is output to the System event log.

- Messages such as “untrusted certificate” should be easy to diagnose.
- Two error codes are informational, and can be safely ignored:
  - KDC_ERR_PREAUTH_REQUIRED (used for backward compatibility with older domain controllers)
  - Unknown error 0x4b

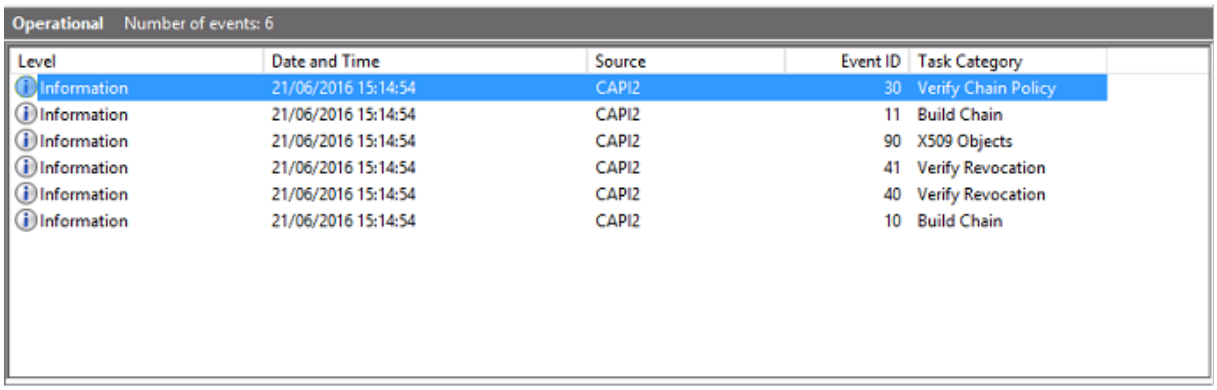
Event log messages

This section describes the expected log entries on the domain controller and workstation when the user logs on with a certificate.

- Domain controller CAPI2 log
- Domain controller security logs
- Virtual Delivery Agent (VDA) security log
- VDA CAPI log
- VDA system log

Domain controller CAPI2 log

During a logon, the domain controller validates the caller’s certificate, producing a sequence of log entries in the following form.



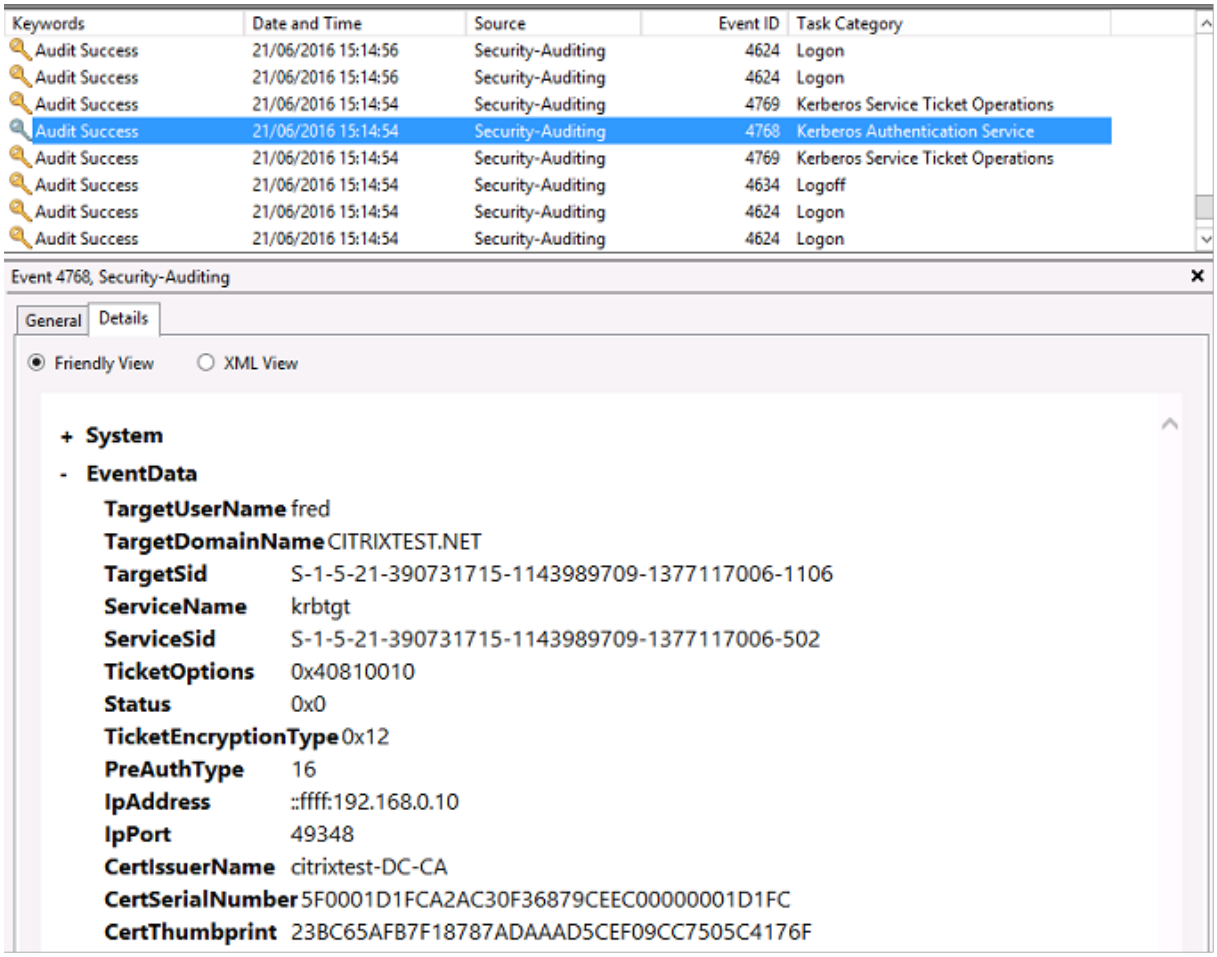
The final event log message shows lsass.exe on the domain controller constructing a chain based on the certificate provided by the VDA, and verifying it for validity (including revocation). The result is returned as “ERROR_SUCCESS”.

- **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

Domain controller security log

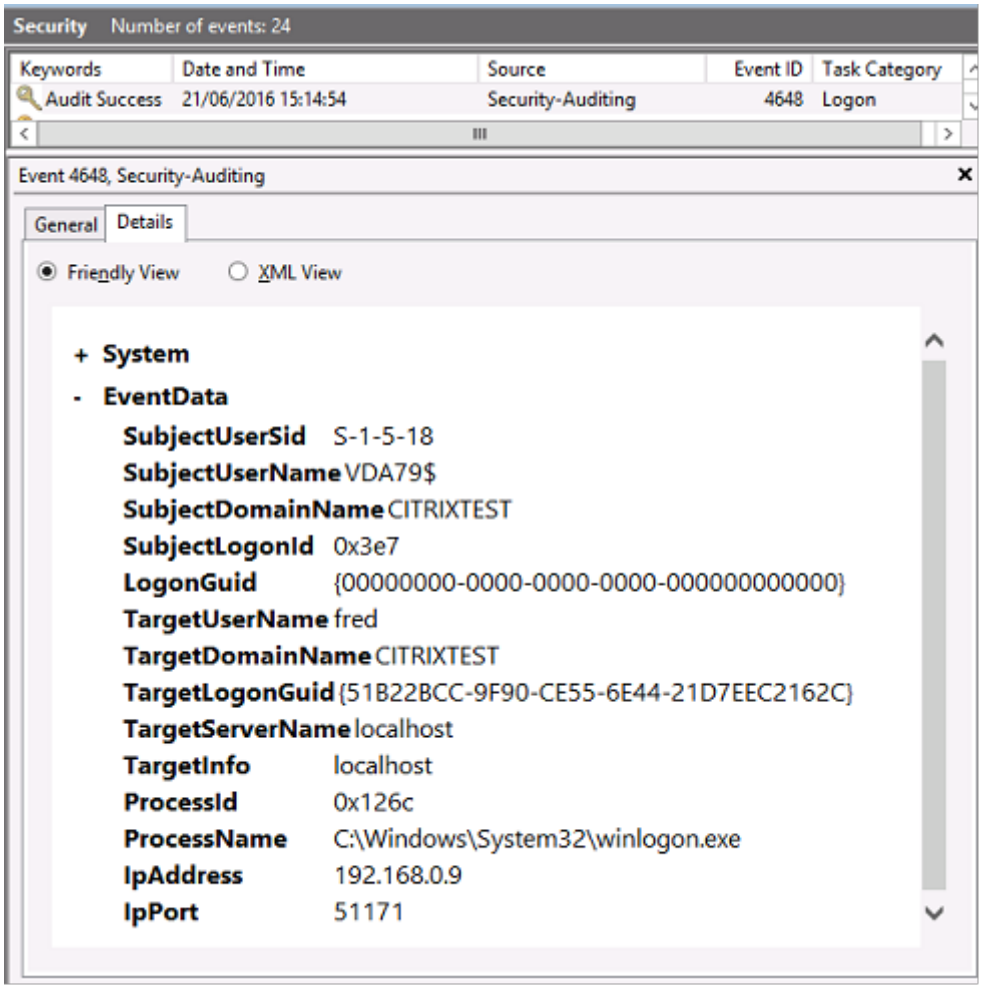
The domain controller shows a sequence of logon events, the key event being 4768, where the certificate is used to issue the Kerberos Ticket Granting Ticket (krbtgt).

The messages before this show the machine account of the server authenticating to the domain controller. The messages following this show the user account belonging to the new krbtgt being used to authenticate to the domain controller.



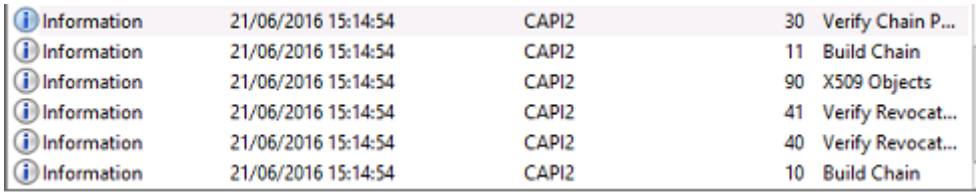
VDA security log

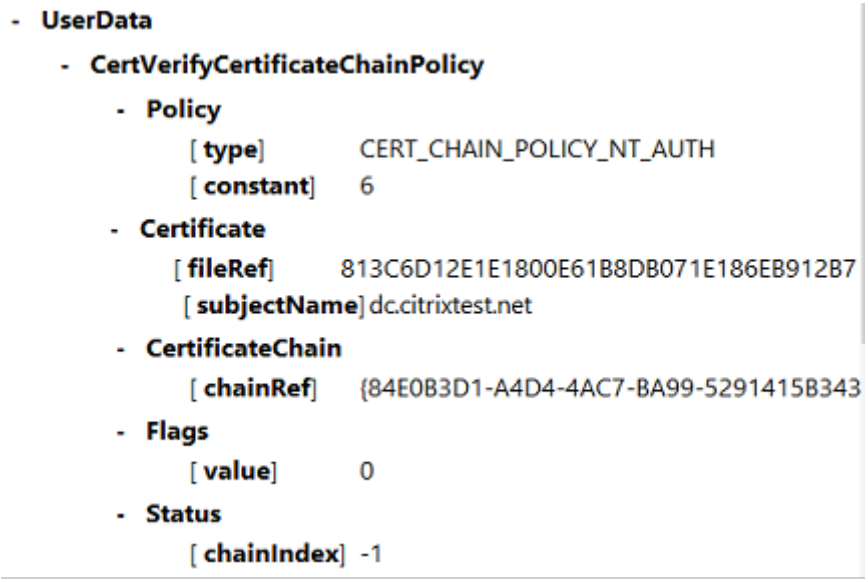
The VDA security audit log corresponding to the logon event is the entry with event ID 4648, originating from winlogon.exe.



VDA CAPI log

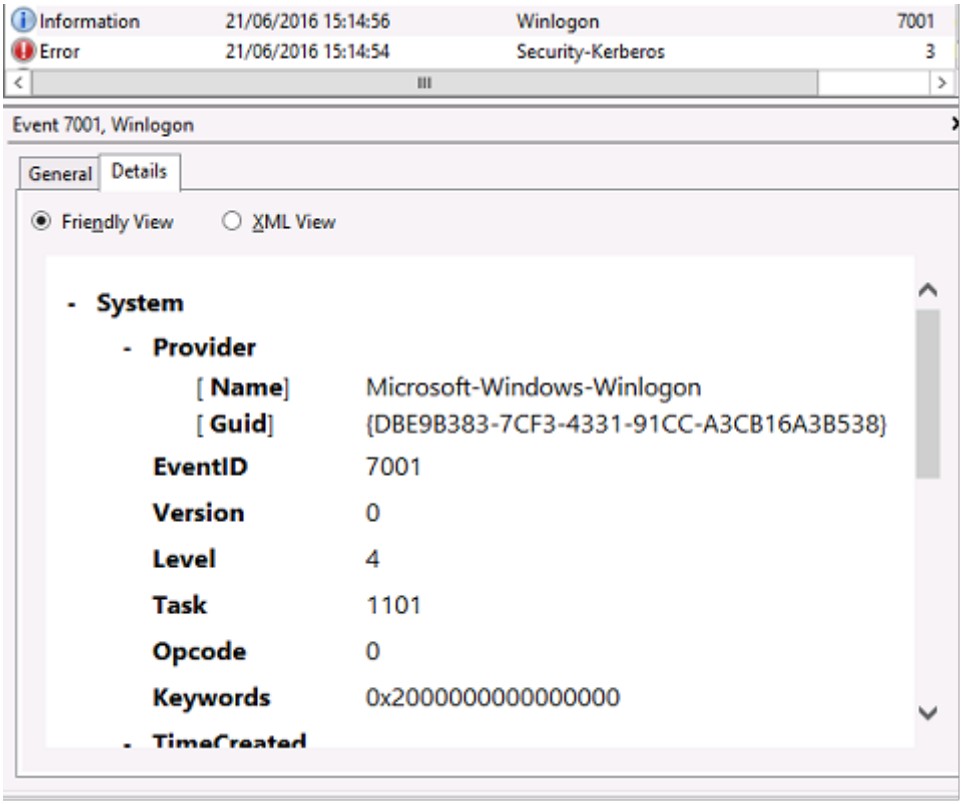
This example VDA CAPI log shows a single chain build and verification sequence from lsass.exe, validating the domain controller certificate (dc.citrixtest.net).





VDA system log

When Kerberos logging is enabled, the system log shows the error KDC_ERR_PREAUTH_REQUIRED (which can be ignored), and an entry from Winlogon showing that the Kerberos logon was successful.



End user error messages

This section lists common error messages displayed to a user on the Windows logon page.

Error message displayed	Description and reference
Invalid Username or Password	The computer believes that you have a valid certificate and private key, but the Kerberos domain controller has rejected the connection. See the *Kerberos logs* section of this article.
The system could not log you on. Your credentials could not be verified. / The request is not supported	The domain controller cannot be contacted, or the domain controller has not been configured with a certificate to support Smart Card authentication. Enroll the domain controller for a "Kerberos Authentication", "Domain Controller Authentication", or "Domain Controller" certificate. This is usually worth trying, even when the existing certificate appears to be valid.
The system could not log you on. The smartcard certificate used for authentication was not trusted.	The intermediate and root certificates are not installed on the local computer. See Certificates and public key infrastructure.
Bad Request	This usually indicates that the extensions on the certificate are not set correctly, or the RSA key is too short (<2048 bits).

Related information

- Configuring a domain for smart card logon: http://support.citrix.com/article/CTX206156
- Smartcard logon policies: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/ff404287(v=ws.10)
- Enabling CAPI logging: http://social.technet.microsoft.com/wiki/contents/articles/242.troubleshooting-pki-problems-on-windows.aspx
- Enabling Kerberos logging: https://support.microsoft.com/en-us/kb/262177
- Guidelines for enabling smart card logon with third-party certification authorities: https://support.microsoft.com/en-us/kb/281245

PowerShell cmdlets

December 3, 2019

You can use the Federated Authentication Service (FAS) administration console for simple deployments; however, the PowerShell interface offers more advanced options. If you plan to use options that are not available in the console, Citrix recommends using only PowerShell for configuration.

The following command adds the FAS PowerShell cmdlets:

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

In a PowerShell window, you can use Get-Help <*cmdlet name*> to display cmdlet help.

For more information on the FAS PowerShell SDK cmdlets, see https://developer-docs.citrix.com/projects/federated-authentication-service-powershell-cmdlets/en/latest/.

Locations
Corporate Headquarters | 851 Cypress Creek Road Fort Lauderdale, FL 33309, United States
Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054, United States