Federated Authentication Service 2603

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.

Federated Authentication Service 2603 is the latest Current Release version of FAS.

Earlier releases

For documentation of earlier FAS releases, see:

- Federated Authentication Service 2511
- Federated Authentication Service 2507 LTSR
- Federated Authentication Service 2503
- Federated Authentication Service 2411
- Federated Authentication Service 2407
- Federated Authentication Service 2402 LTSR
- Federated Authentication Service 2311
- Federated Authentication Service 2308
- Federated Authentication Service 2305
- Federated Authentication Service 2303
- Federated Authentication Service 2212
- Federated Authentication Service 2209
- Federated Authentication Service 2206
- Federated Authentication Service 2203 LTSR
- Federated Authentication Service 2112
- Federated Authentication Service 2109

- Federated Authentication Service 2106
- Federated Authentication Service 2103
- Federated Authentication Service 1912 LTSR
- 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
- Configuring Windows for Certificate Logon

Federated Authentication Service 2603

This release of Federated Authentication Service (FAS) includes no new features.

Fixed issues

There are no fixed issues in Federated Authentication Service 2603.

Known issues

The following actions delete the registry-based FAS Group Policies on the VDA, causing single sign-on failures:

- Upgrade the VDA from Citrix Virtual Apps and Desktops 2411 to any future version
- Upgrade the VDA from Citrix Virtual Apps and Desktops 2503 to any future version
- Uninstall Citrix Virtual Apps and Desktops 2411 from the VDA
- Uninstall Citrix Virtual Apps and Desktops 2503 from the VDA

Run the following command on the VDA to restore the FAS Group Policies:

```
gpupdate /force
```

Third party notices

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

- Federated Authentication Service (FAS) is supported on the following Windows Server versions:
  - Windows Server 2025, Standard, and Datacenter Editions
  - Windows Server 2022, Standard, and Datacenter Editions
  - Windows Server 2019, Standard and Datacenter Editions, and with the Server Core option
- Citrix recommends installing FAS on a server that does not have any other Citrix components.
- The Windows Server must be secured since it has access to a registration authority certificate and a private key. The certificate and private key allow the server to issue certificates for domain users. The server also has access to the issued domain user certificates and private keys.
- The FAS PowerShell cmdlets require Windows PowerShell 64-bit installed on the FAS server.
- A Microsoft Enterprise Certificate Authority or other validated Certificate Authority (CA) is required to issue user certificates. The following non-Microsoft PKI providers have validated their solutions for use with FAS. For support with these validations reach out to the vendor:
  - Keyfactor Command
  - Sectigo Certificate Manager
  - Venafi Zero-Touch PKI
  - HDI PKIaaS (Venafi)
  - Entrust WNES
  - AppViewX
  - Evertrust Horizon CLM
  - Opentrust PKI
  - IDnomic PKI-3
  - DigiCert Autoenrollment Server
- For support and guidance to use FAS with non-Microsoft CA, you can reach out to the relevant PKI provider.

- For certificate authorities other than Microsoft, ensure the following:
  - The certificate authority (CA) is registered in the Active Directory as an enrollment service.
  - The CA certificate is in the NTAuth store on the Domain Controller. For more information, see How to import third-party certificate authority (CA) certificates into the Enterprise NTAuth store.
- For more information, see the Deployment Guide: Citrix Federated Authentication Service and Sectigo MS Agent.

In the Citrix Virtual Apps or Citrix Virtual Desktops™ Site:

- Delivery Controllers, Virtual Delivery Agents (VDAs), and StoreFront™ servers must all be supported versions.

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

Install and configure

Install and set up 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 installing the Federated Authentication Service (FAS) on a dedicated server. This server must be secured in a similar way to a domain controller or certificate authority. FAS can be installed from either of the following:

- the Citrix Virtual Apps and Desktops™ installer, from the **Federated Authentication Service** button on the autorun splash screen when the ISO is inserted
- `XenDesktopFasSetup.exe` located on the Citrix Virtual Apps and Desktops ISO at `x64\XenDesktop Setup\XenDesktopFasSetup.exe`
- `FasSetup_xxxx.exe`, the stand-alone FAS installer file, available from the stand-alone FAS installer file (available on Citrix Downloads)

Any of 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 or CitrixFederatedAuthenticationService.adml)
- Certificate template files
- Performance counters and event logs
- Citrix Telemetry Service, which provides support for FAS Always-on Tracing
- Citrix Scout, an application, which can be used to collect diagnostics such as always-on tracing

For more information about the installers, seeCommand-line options for installing FAS.

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 do an in-place upgrade.
- Ensure to close the FAS administration console before you upgrade FAS.
- Ensure that at least one FAS server is available always. 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:**
>
> You do not need this step if you're using FAS only with Citrix Cloud.

> For more details on how to enable the FAS plug-in on StoreFront stores, see `<https://docs.citrix.com/en-us/storefront/current-release/configure-authentication-and-delegation/fas>`.

Configure the Delivery Controller™

Note:

You do not need this step if you're 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 connects to it: run the **Set-BrokerSite -TrustRequestsSentToTheXmlServicePort $true** PowerShell cmdlet. Run this command once per site, regardless of the number of Delivery Controllers on the site.

Configure Group Policy

Note:

If all your FAS servers and VDAs are version 2511 or later, the Group Policy FQDN list on the VDA is no longer needed. See FAS V2 ticketing and the registry address list

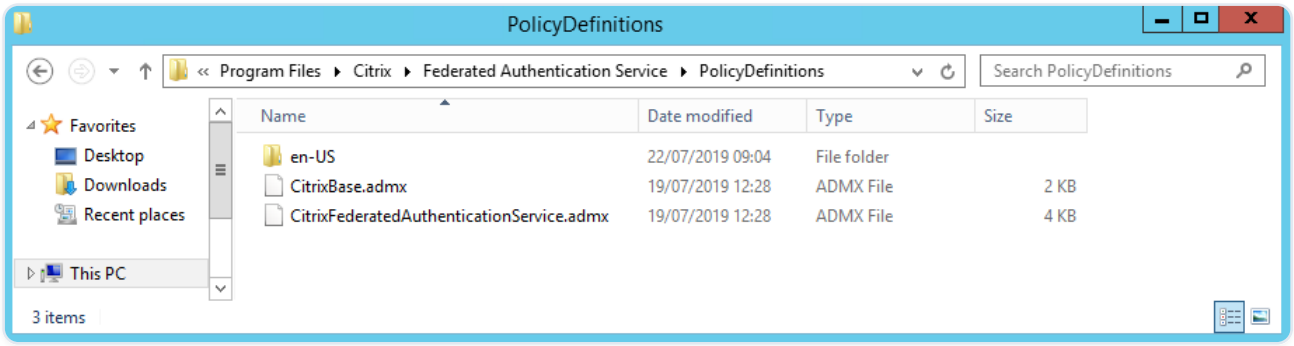
After you install FAS, use the Group policy templates provided in the installation to specify the fully qualified domain names (FQDNs) of the servers in the Group Policy.

Important:

Ensure that the StoreFront servers requesting tickets and the Virtual Delivery Agents (VDAs) redeeming tickets have an 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 functions as long as the StoreFront servers, VDAs, and the machine running the FAS administration console see the same list of FQDNs. See Step 6.

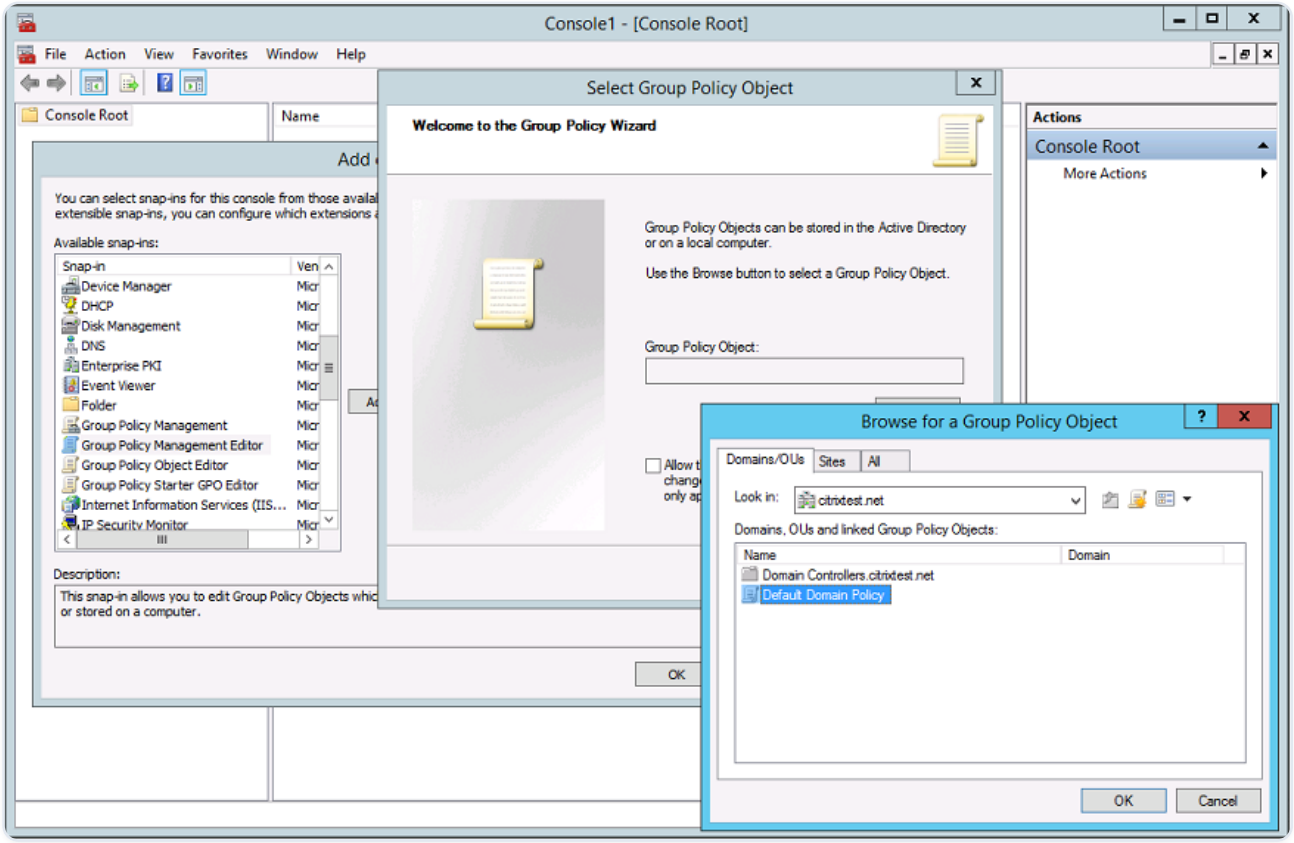
Step 1. On the server where you installed FAS, locate the C:\Program Files\Citrix\Federated Authentication Service\PolicyDefinitions\CitrixFederatedAuthenticationService.admx and CitrixBase.admx files, and the en-US folder.



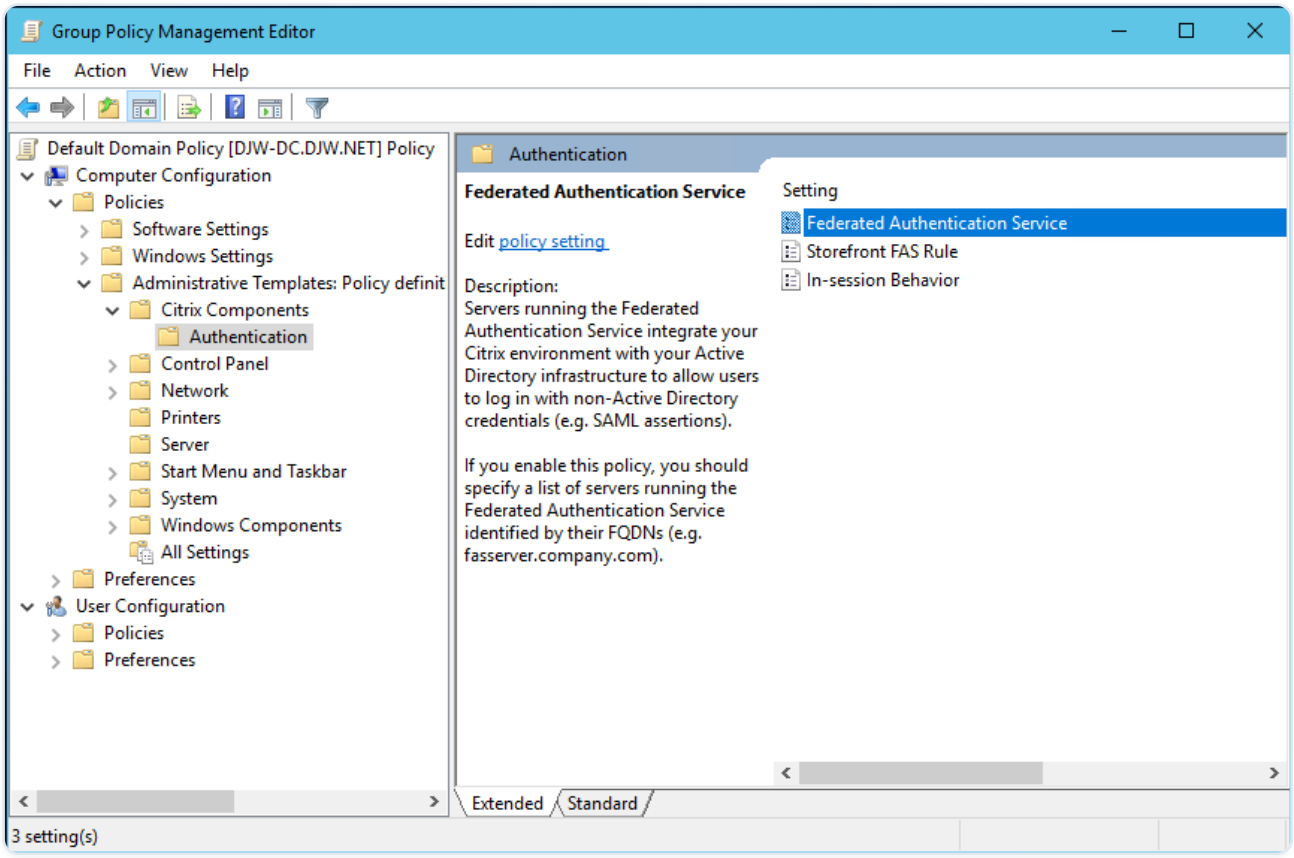
Step 2. Copy these files to your domain controllers and place them in the C:\Windows\PolicyDefinitions and en-US subfolder.

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).



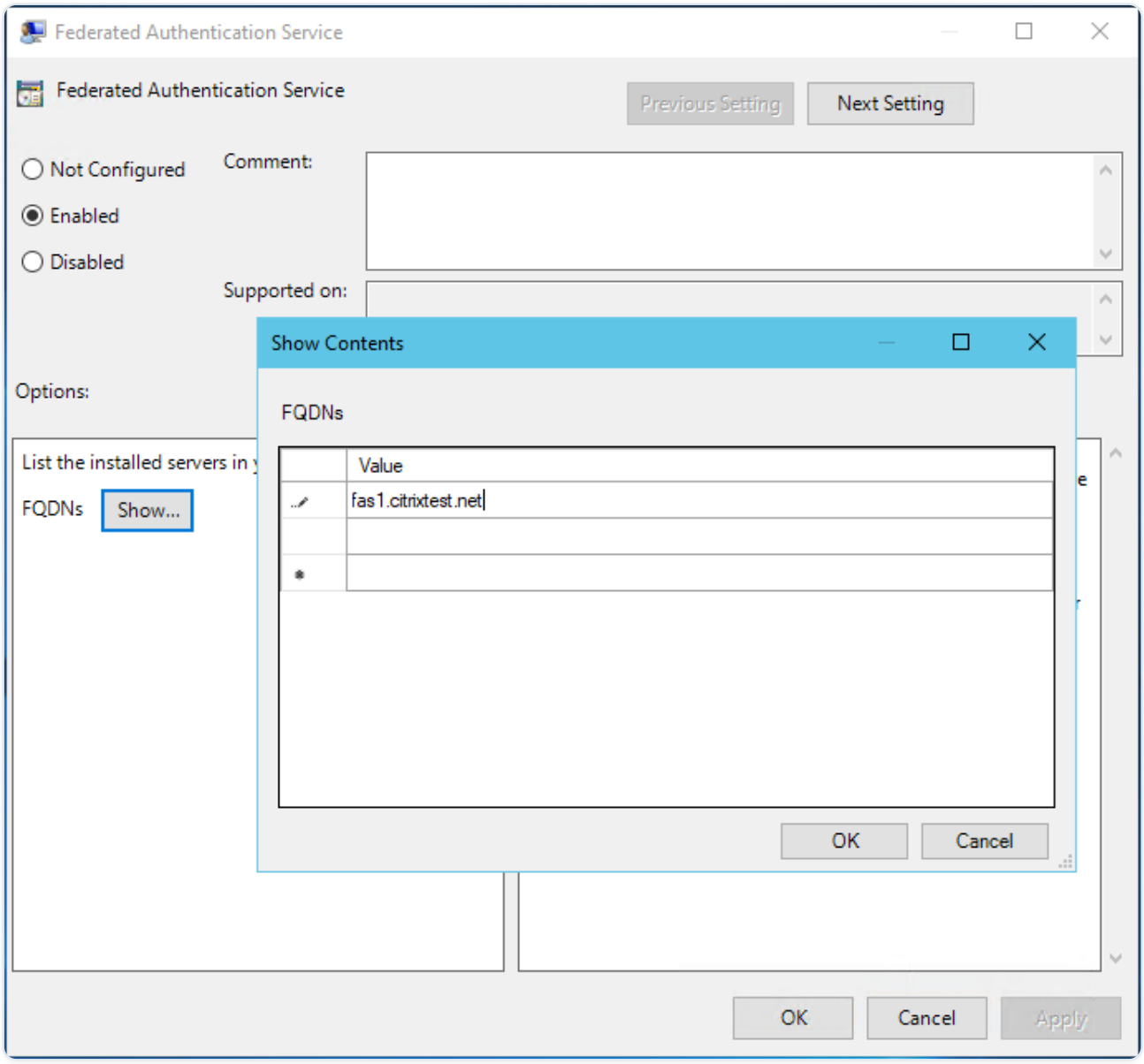
Step 4. Navigate to the *Federated Authentication Service* policy in Computer Configuration/ Policies/Administrative Templates/Citrix Components/Authentication.



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.

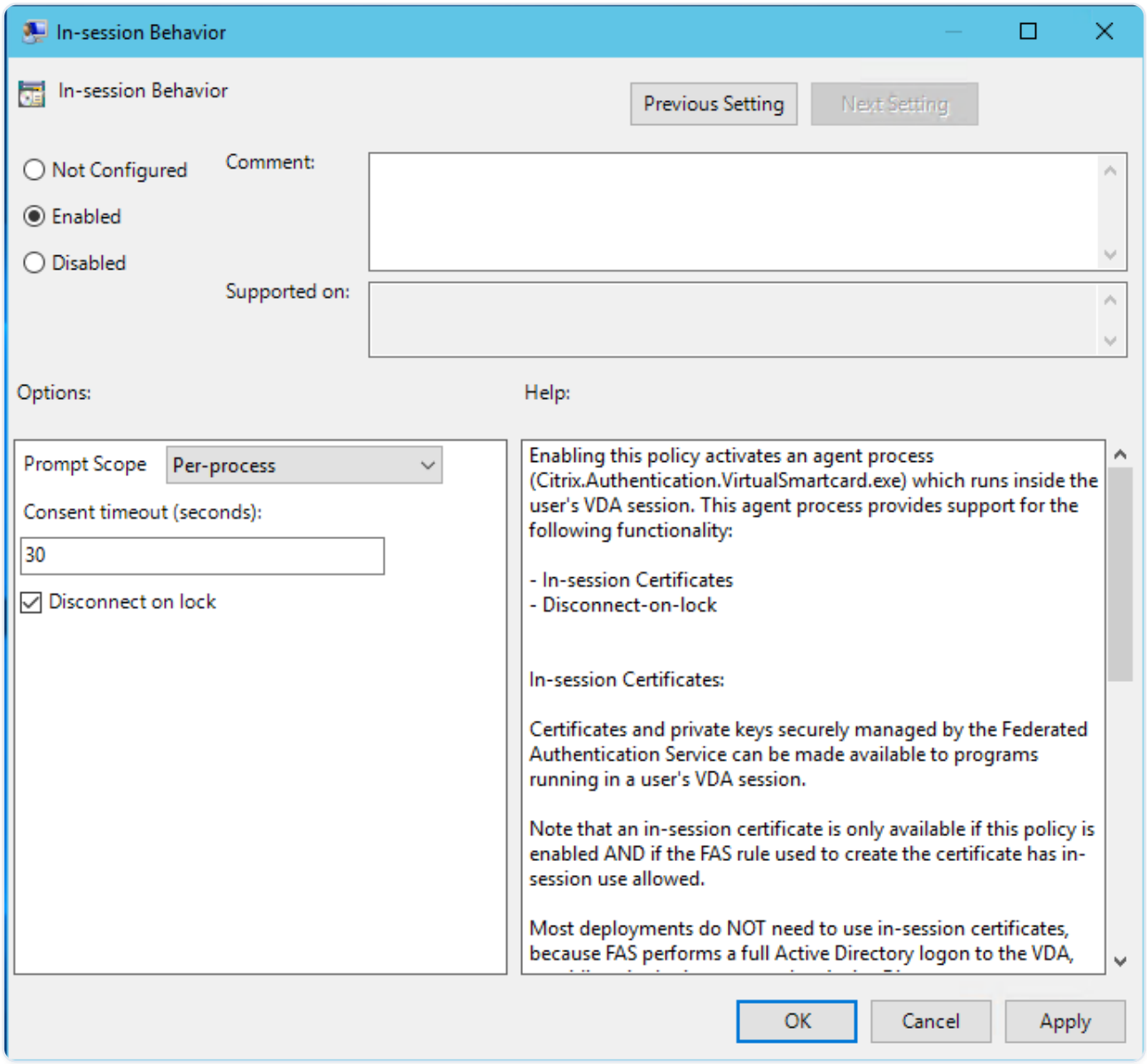
Important:

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 might 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 option 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 behavior is similar to the "disconnect on smart card removal" policy. Use this feature when the 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.

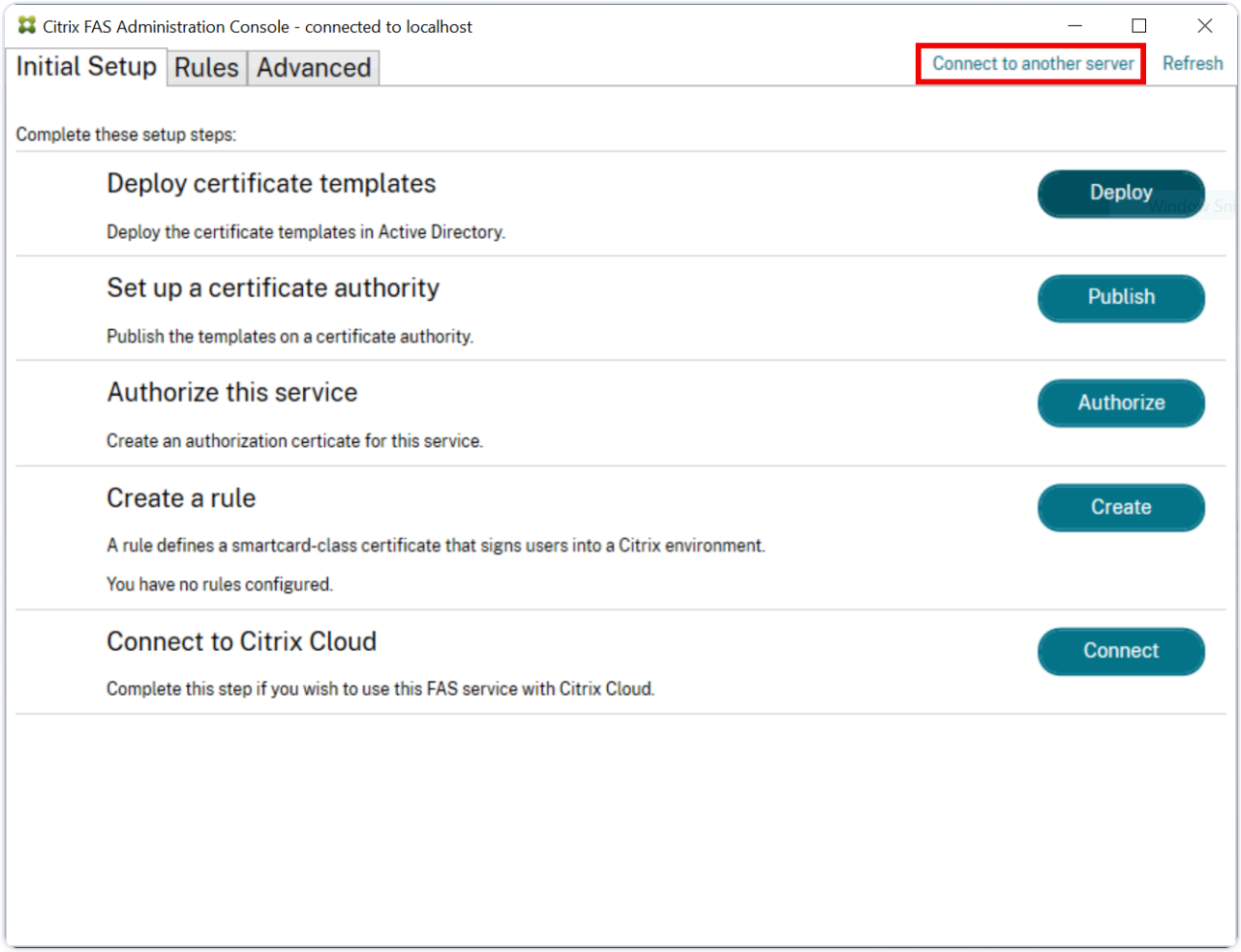
The first time you use the administration console, it guides you through the following processes to:

- Deploy certificate templates.

- Set up the certificate authority.
- Authorize FAS to use the certificate authority.

You can also use OS configuration tools to complete some of the steps manually.

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.

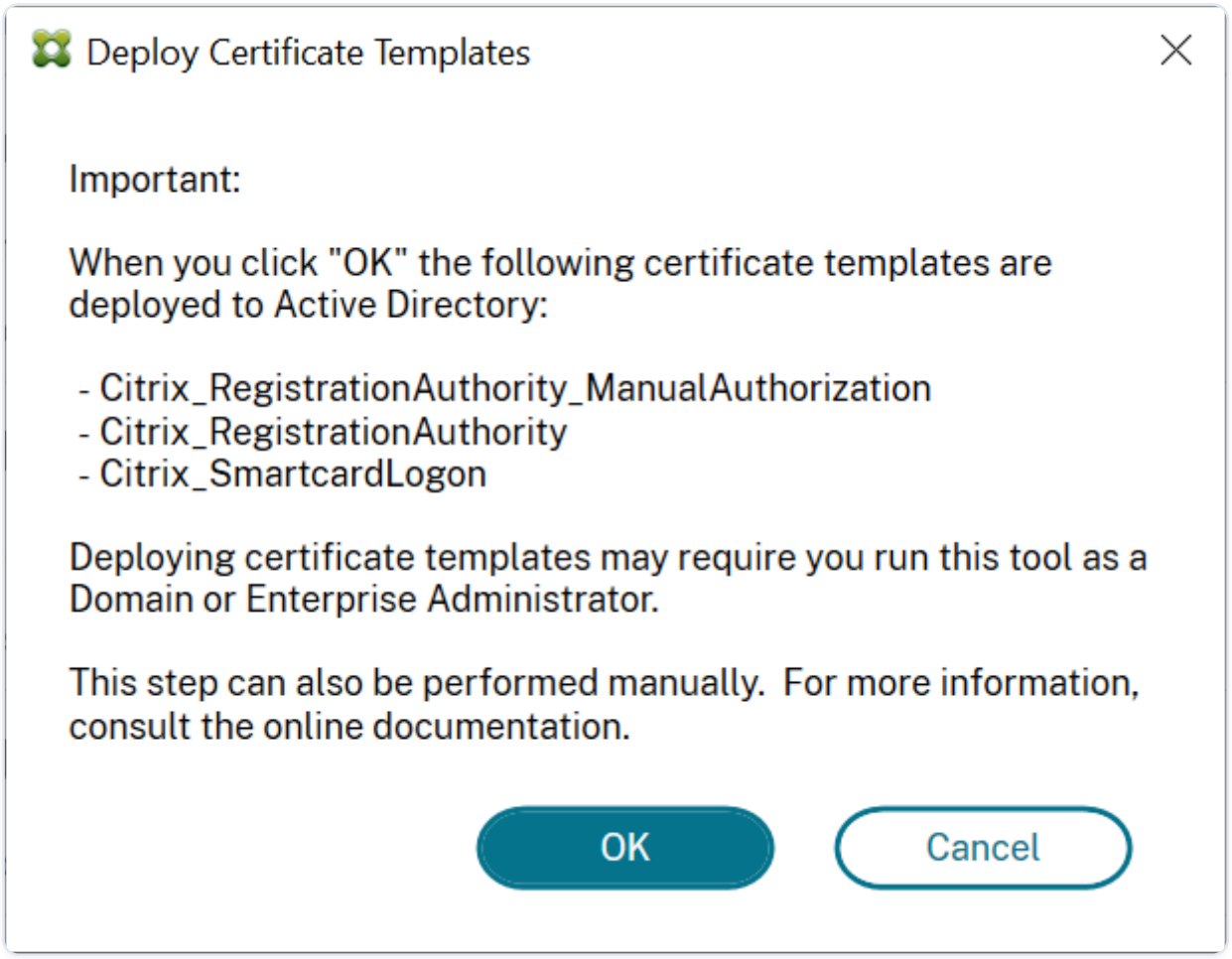


Deploy certificate templates

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

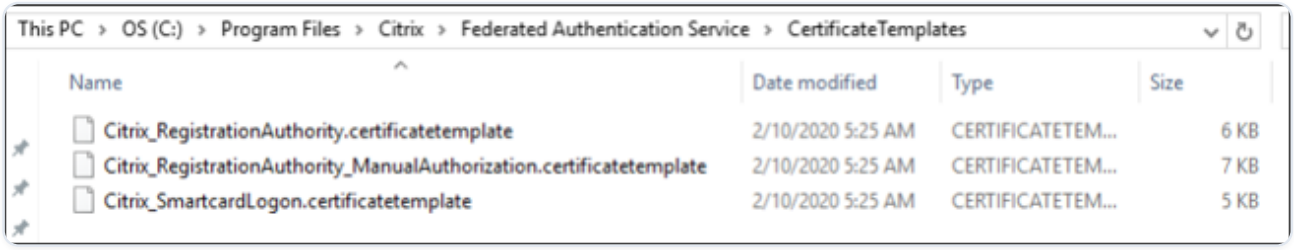
- Citrix_RegistrationAuthority_ManualAuthorization
- Citrix_RegistrationAuthority
- Citrix_SmartcardLogon

These templates must be registered with the 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:

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

$CertEnrol = New-Object -ComObject
```

```
X509Enrollment.CX509EnrollmentPolicyWebService

$CertEnrol.InitializeImport($template)

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

$writabletemplate = New-Object -ComObject
X509Enrollment.CX509CertificateTemplateADWritable

$writabletemplate.Initialize($comtemplate)

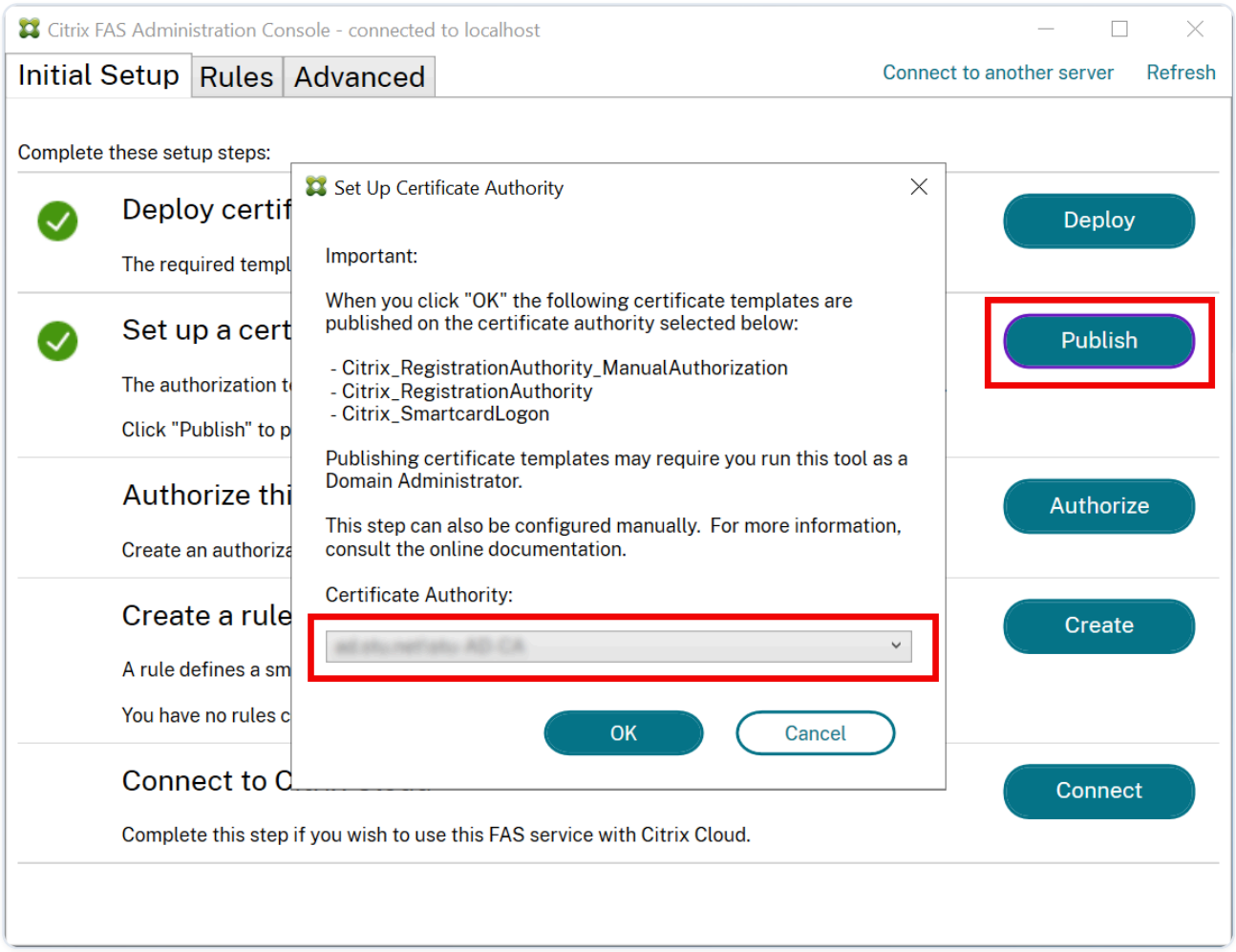
$writabletemplate.Commit(1, $NULL)
```

Set up Active Directory Certificate Services

After you install 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.

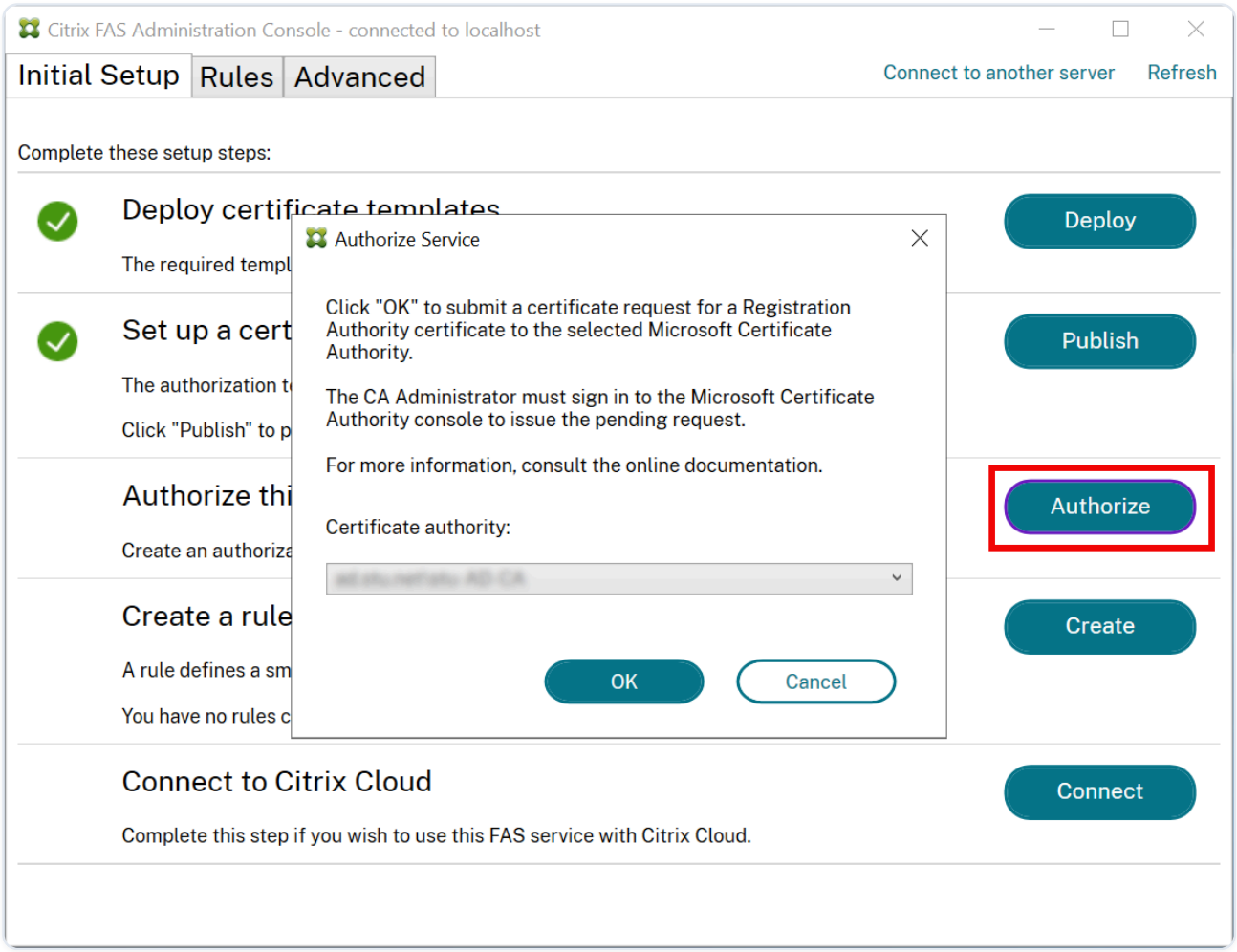
A user who has permissions to administer the certificate authority must publish the templates on at least one server. Use **Set Up Certificate Authority** to publish them.

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



Authorize Federated Authentication Service

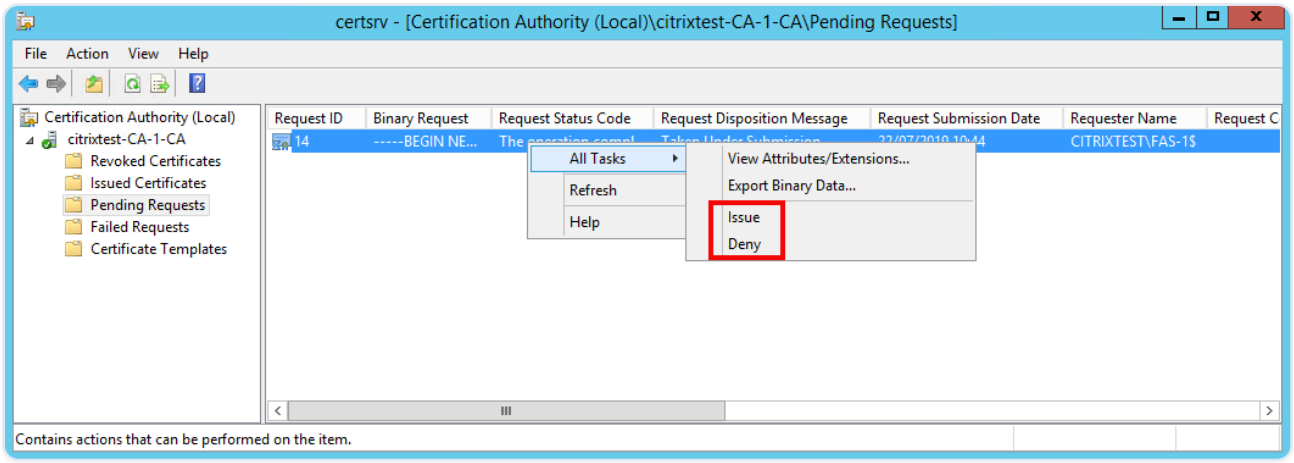
This step initiates the authorization of FAS. The administration console uses the Citrix_RegistrationAuthority_ManualAuthorization template to generate a certificate request, and then sends it to one of the certificate authorities that are publishing that template.



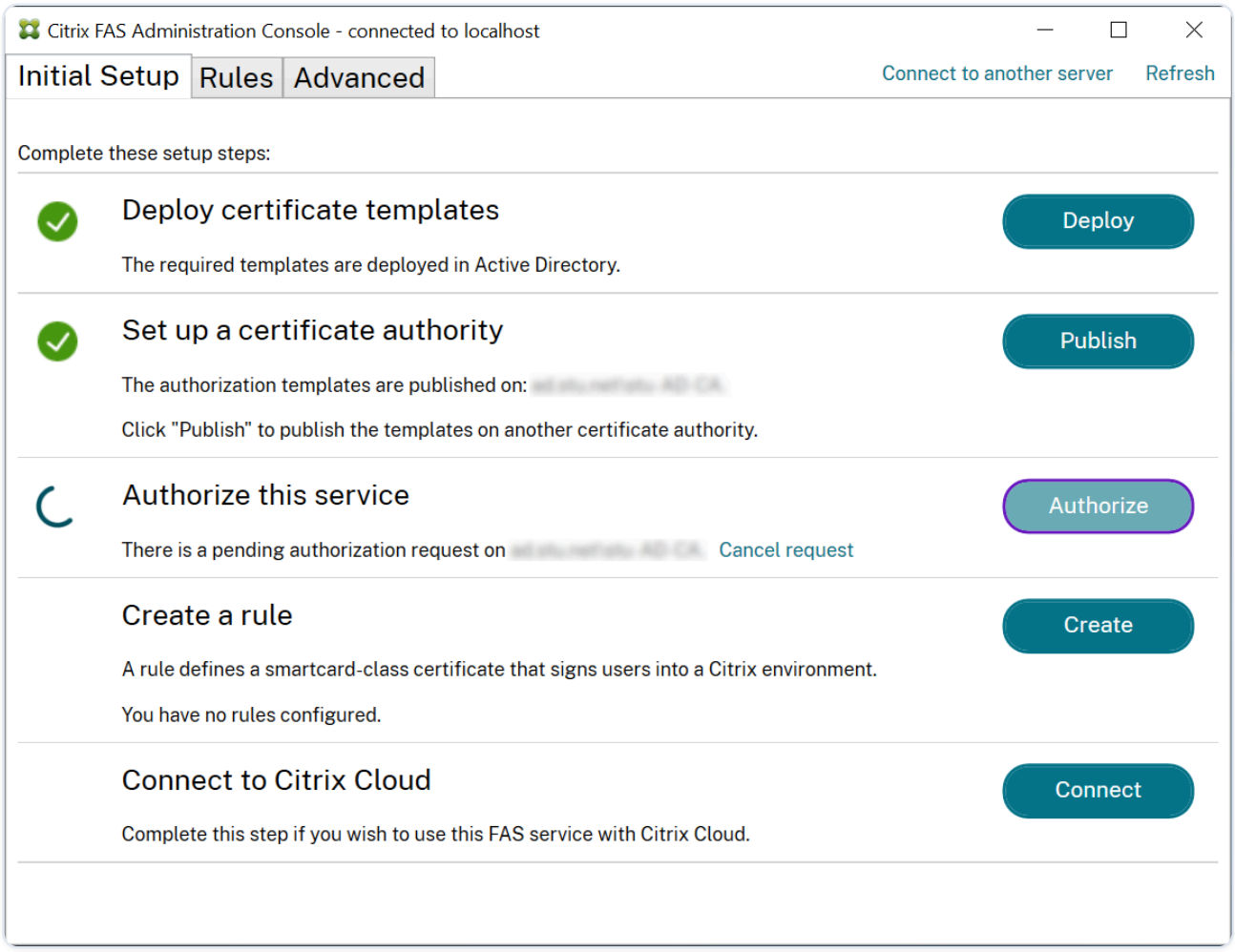
After the request is sent, it appears in the **Pending Requests** list of the Microsoft Certification Authority console as a pending request from the FAS machine account. The certificate authority administrator must issue or deny the request before the configuration of FAS can continue.

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 authorization 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 the rules to authorize the issuance of certificates for VDA logon and in-session use, as directed by StoreFront.

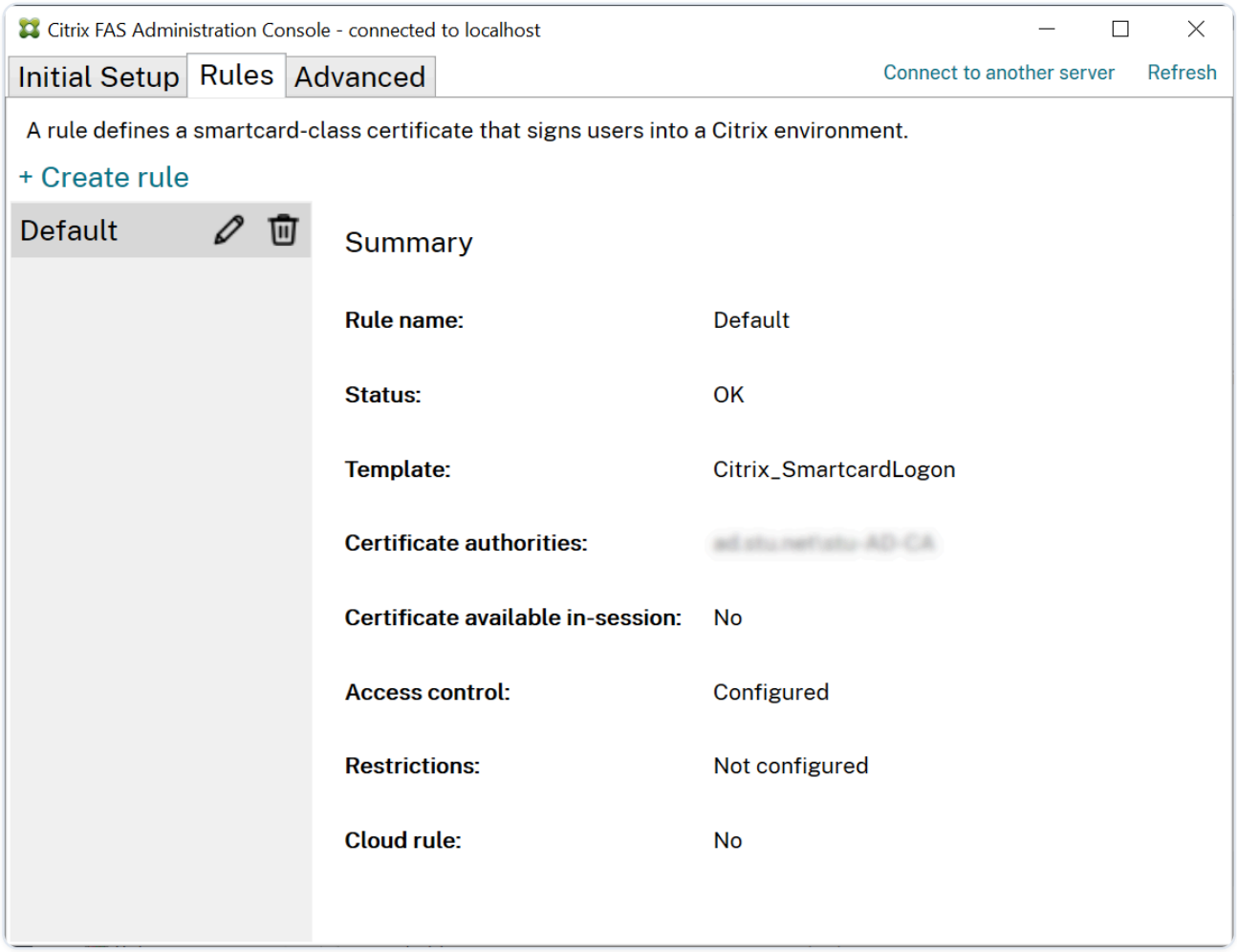
Each rule specifies the following:

- StoreFront servers that are trusted to request the certificates.
- Set of users for whom the certificates are requested.
- Set of VDA machines allowed to use the certificates.

Citrix recommends creating a rule with the name "default" as the StoreFront requests for a rule with the same name while contacting FAS.

You can create more 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 the information to create the rule. The "Rules" tab shows a summary of each rule.



The wizard gathers the following information:

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

Certificate Authority: The certificate authority that issues user certificates and publishes the template. FAS supports adding multiple certificate authorities for failover and load balancing. Make sure that 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 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 must 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.

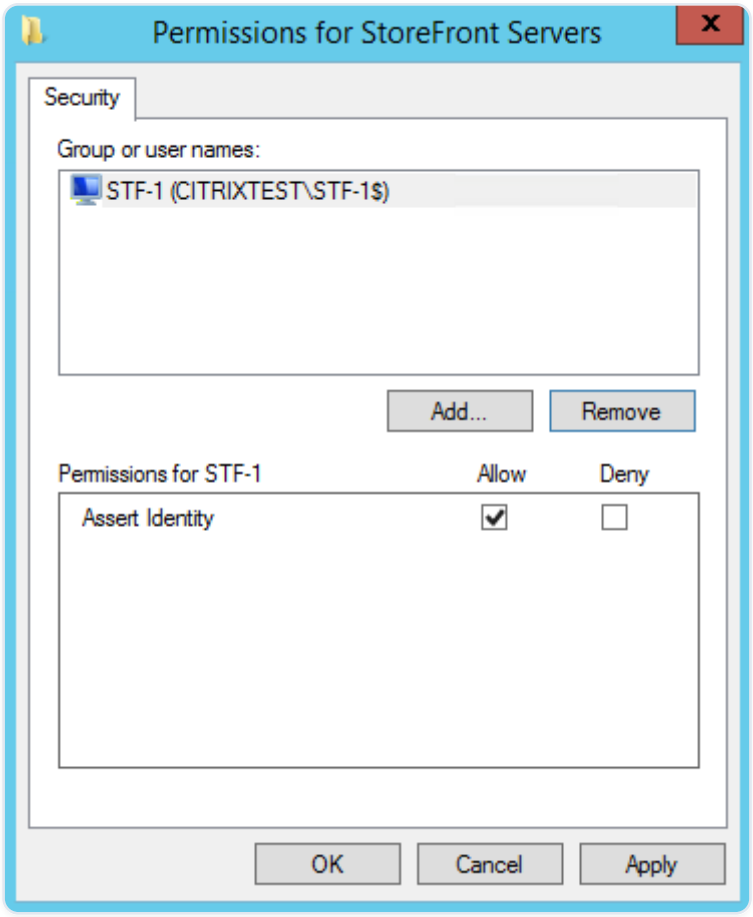
  If you select **Allow in-session use**, the In-session Behavior group policy must also be enabled and applied to the VDA. Certificates are then placed in the user's personal certificate store after logon for application use. For example, if you require TLS authentication to web servers within the VDA session, the Internet Explorer can use the certificate.

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.

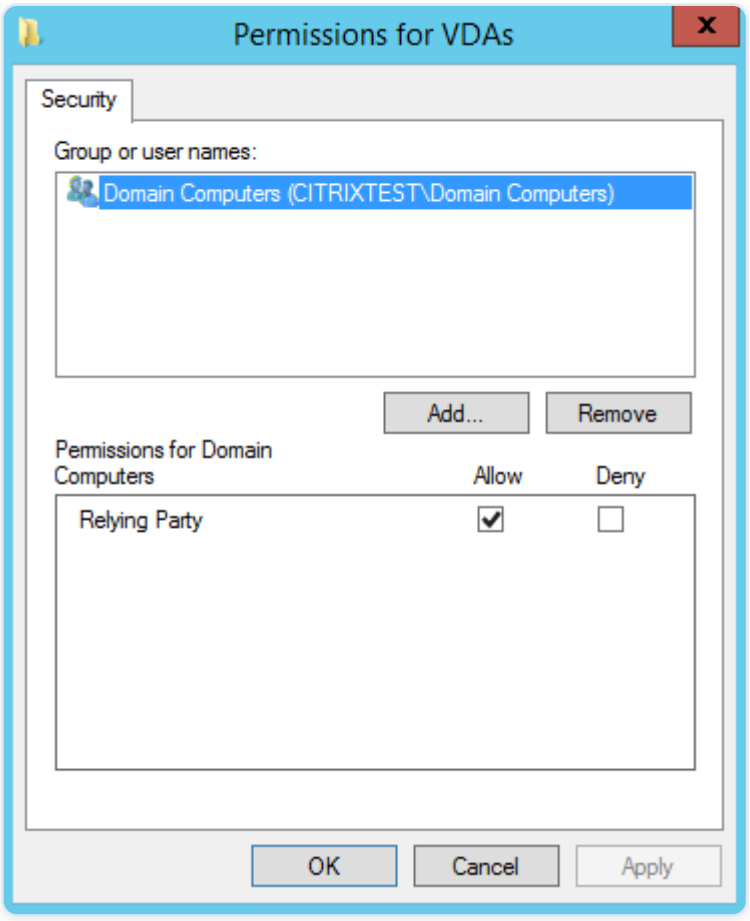
> The default permission ("Assert Identity" allowed) denies everything. Therefore you must explicitly allow your StoreFront servers.

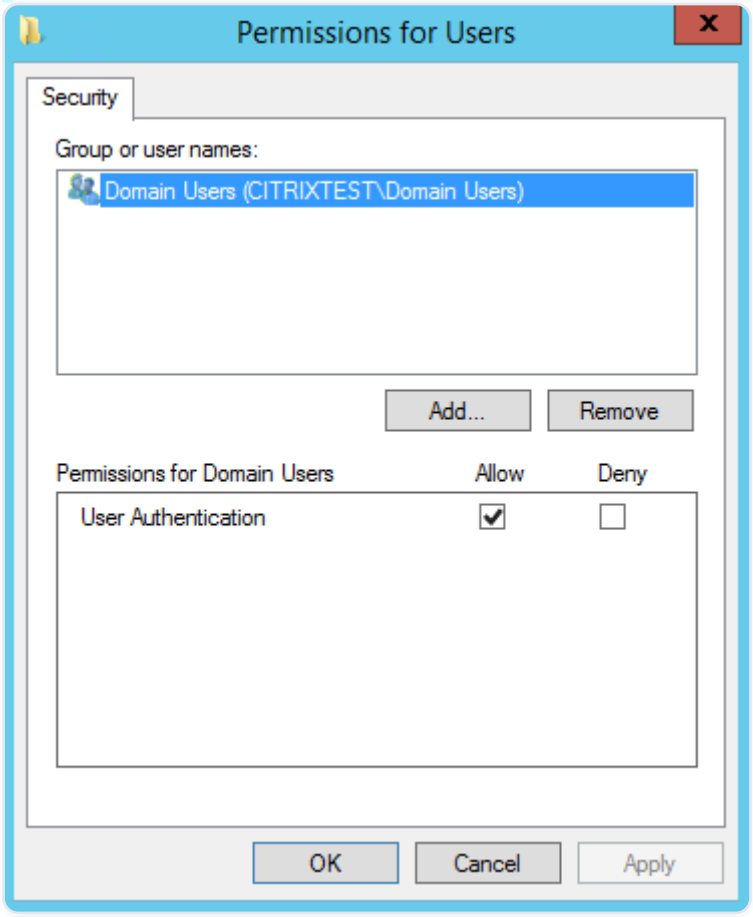


Restrictions: The list of VDA machines that can log users on using FAS and the list of users who can be issued certificates through FAS.

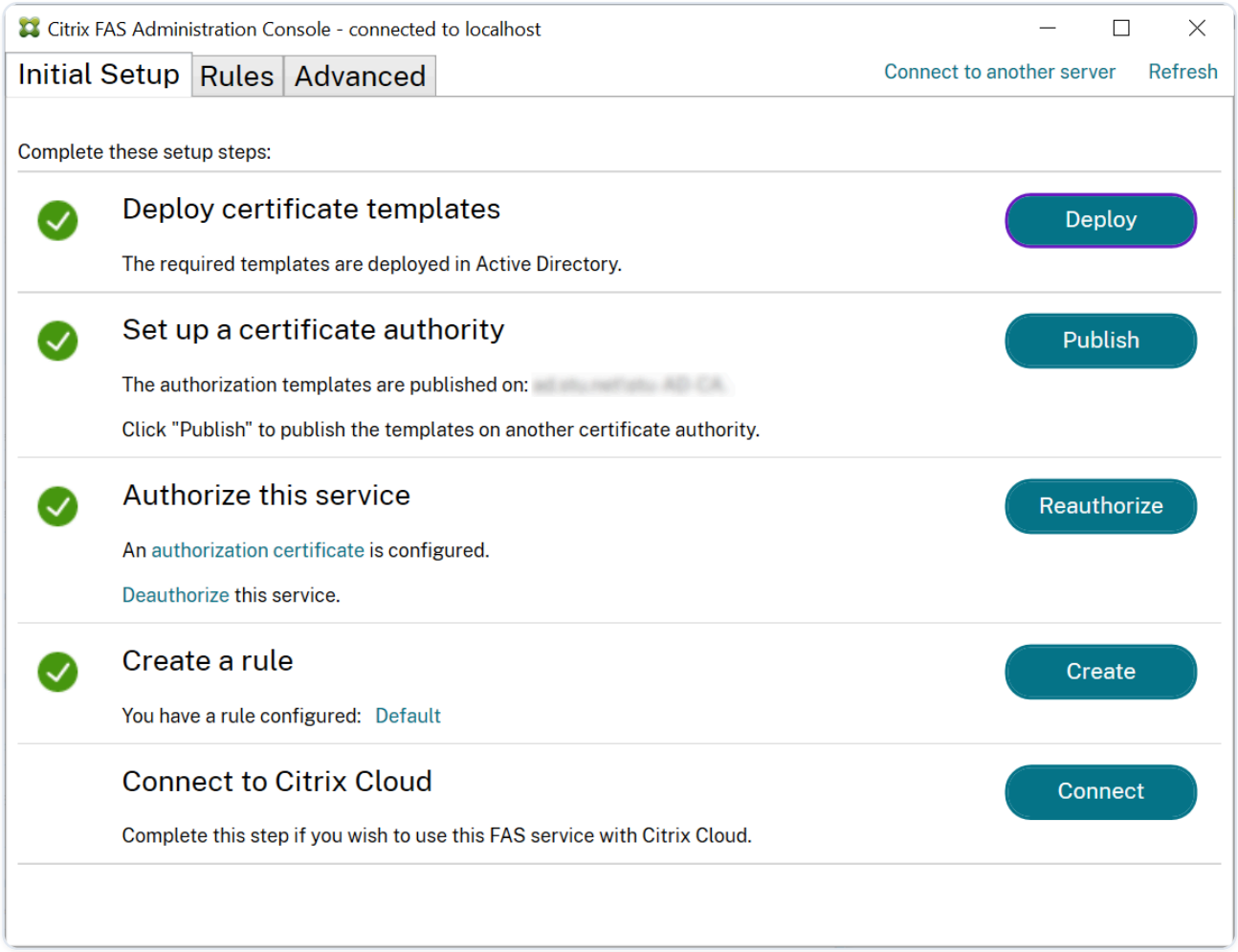
- **Manage VDA permissions** lets you specify which VDAs can use FAS to log the user on. The list of VDAs defaults to Domain Computers.
- **Manage user permissions** lets you specify which users can use FAS to sign in to a VDA. The list of users defaults to Domain Users.

> **Note:**
>
> If the domain of the FAS server differs from that of the VDAs and users, the default restrictions must be modified.


Permissions for VDAs
Security
Group or user names:
Domain Computers (CITRIXTEST\Domain Computers)
Add...
Remove
Permissions for Domain Computers
Allow
Deny
Relying Party
OK
Cancel
Apply


Permissions for Users
Security
Group or user names:
Domain Users (CITRIXTEST\Domain Users)
Add...
Remove
Permissions for Domain Users
Allow
Deny
User Authentication
OK
Cancel
Apply

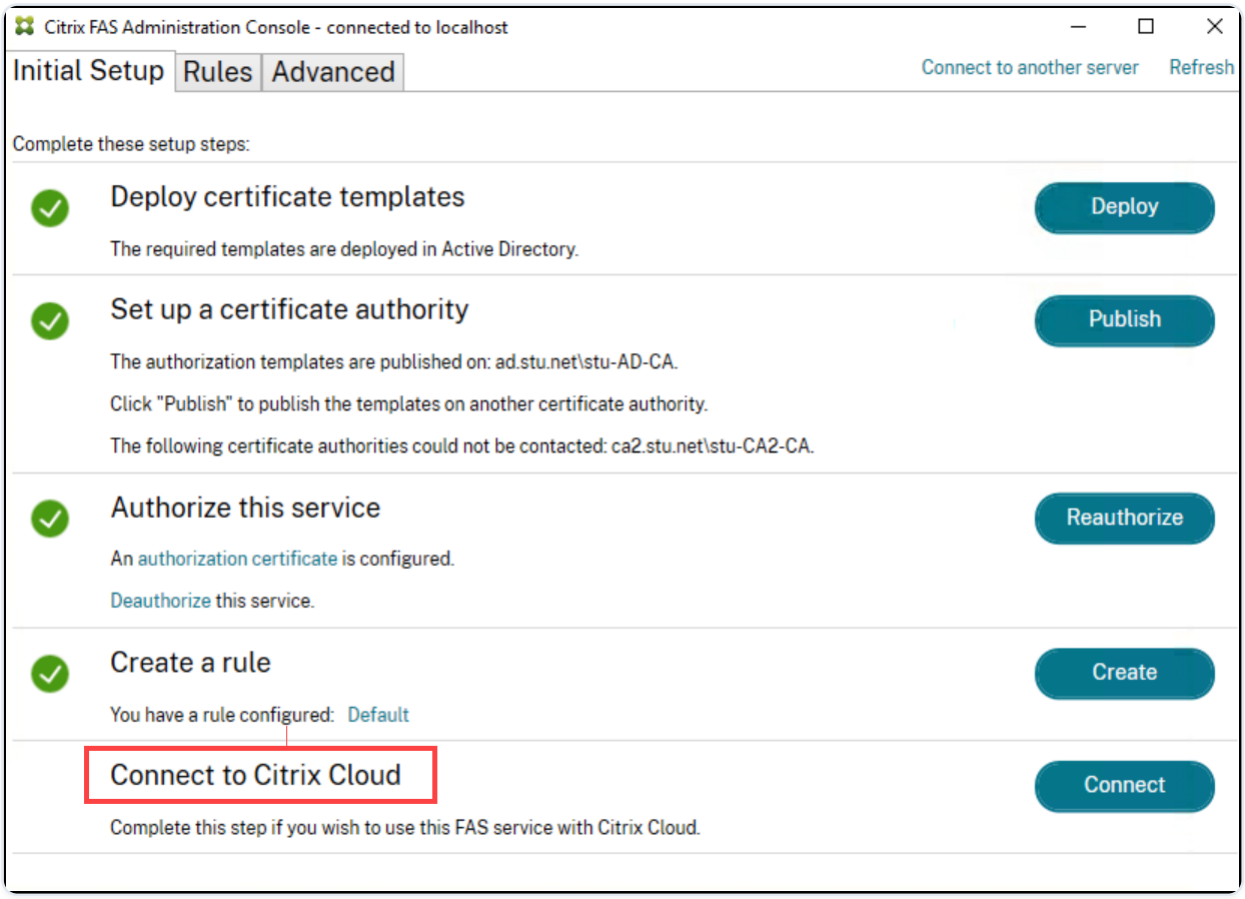
Cloud rule: Indicates if the rule is applied when identity assertions are received from Citrix Workspace. When you connect to Citrix Cloud, you choose which rule to use for Citrix Cloud. You can also change the rule after connecting to Citrix Cloud from a link in the **Connect to Citrix Cloud** section.



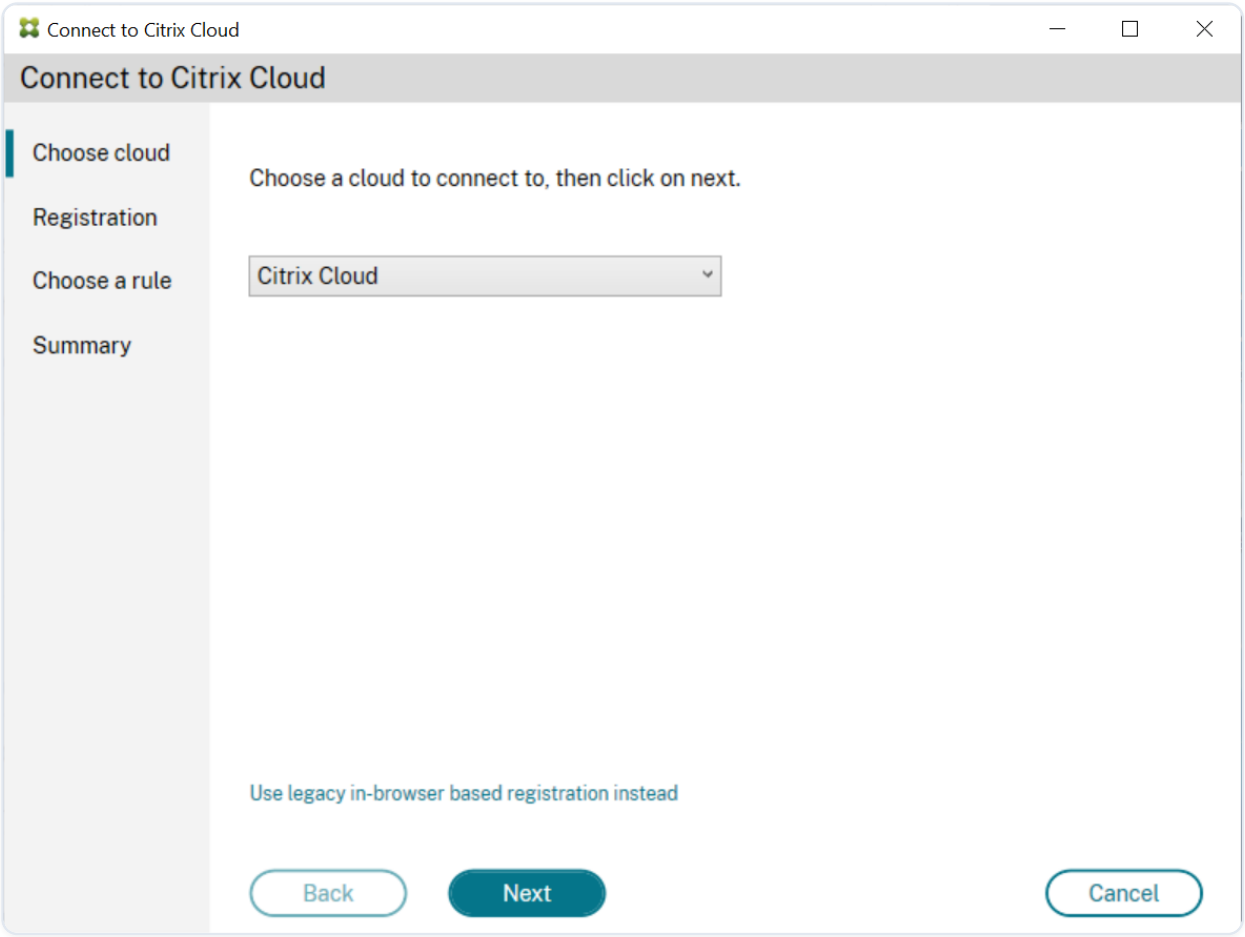
Connect to Citrix Cloud

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

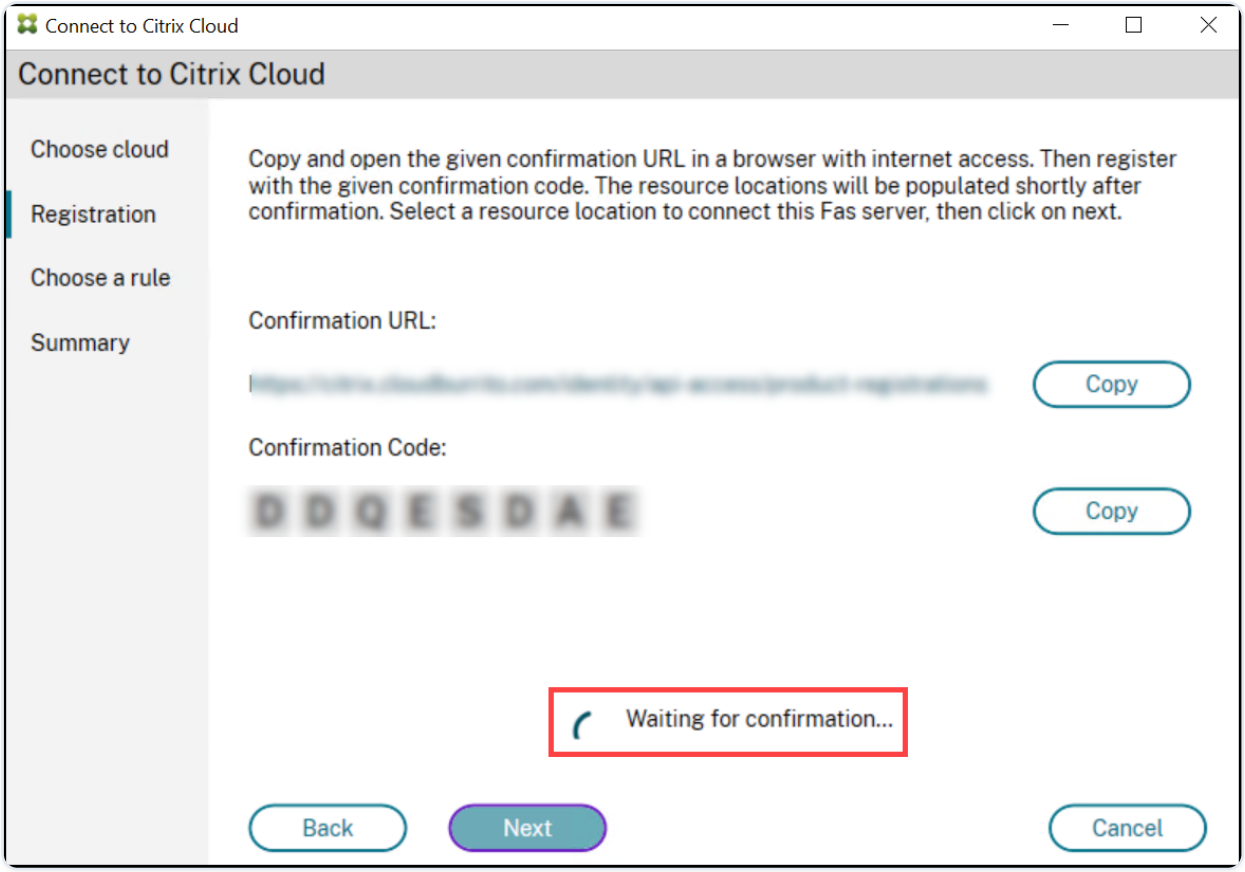
1. In the Initial Setup tab, under **Connect to Citrix Cloud** click **Connect**.



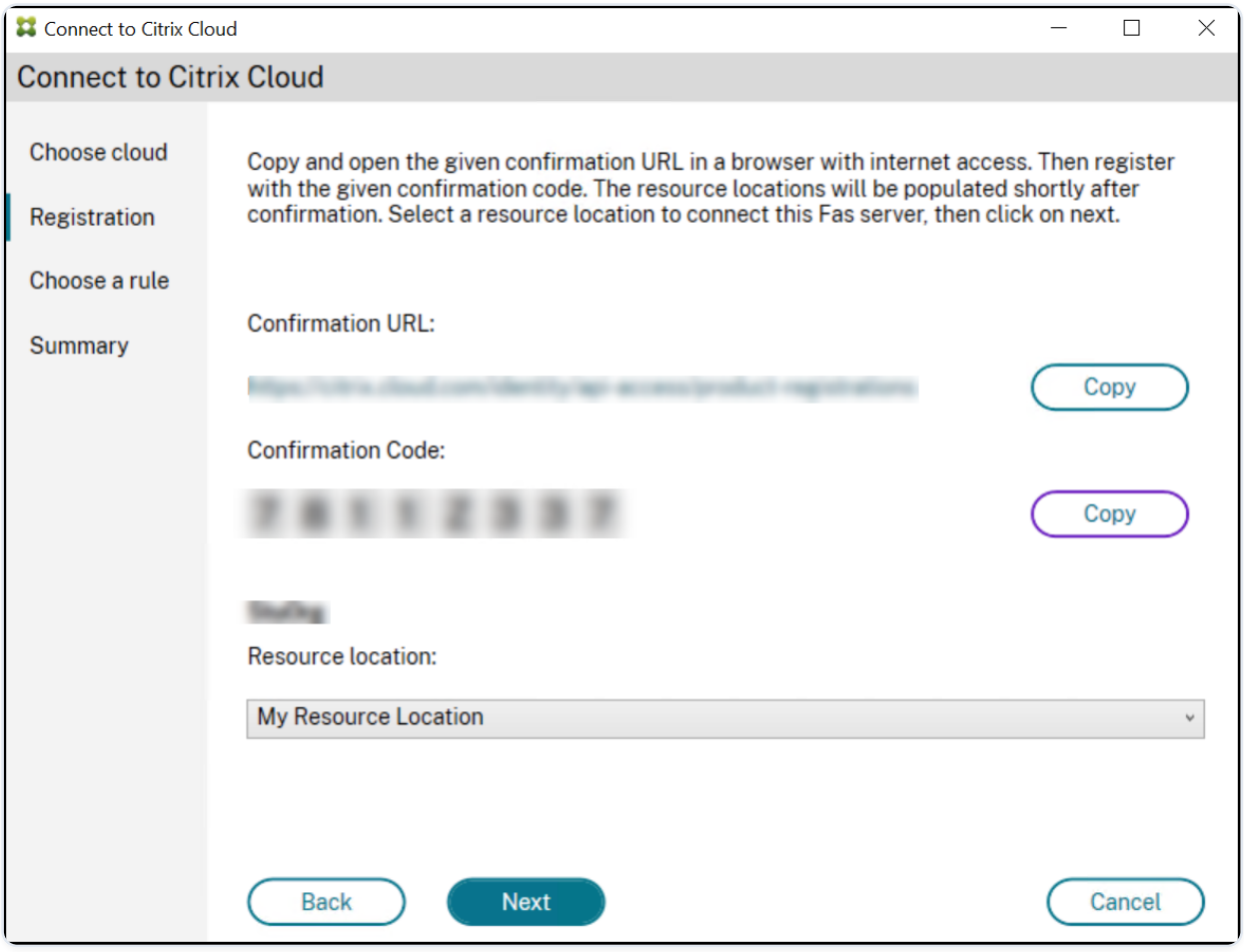
2. Select the cloud that you want to connect to and click **Next**.



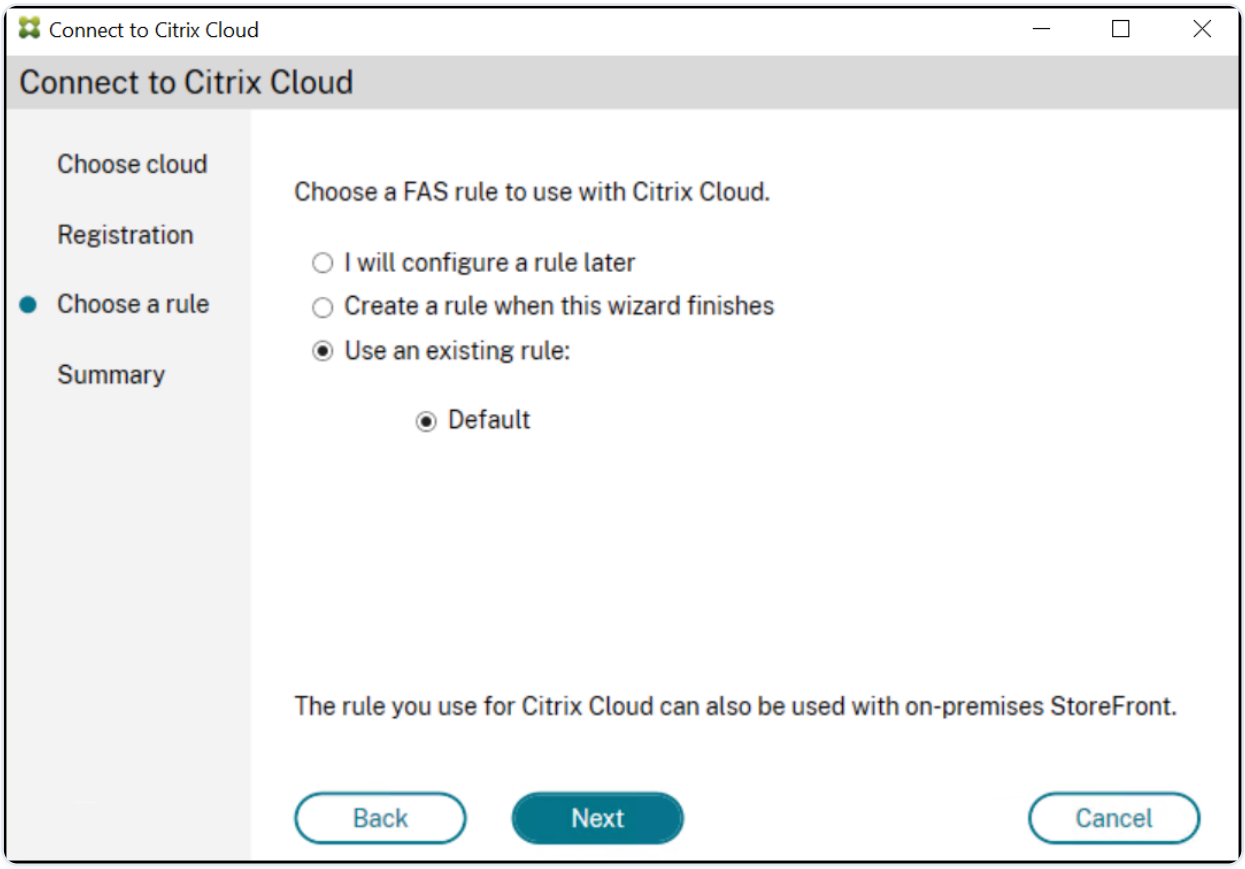
3. The window displays a unique registration code, which must be approved in Citrix Cloud. For more information, see Register on-premises products with Citrix Cloud.



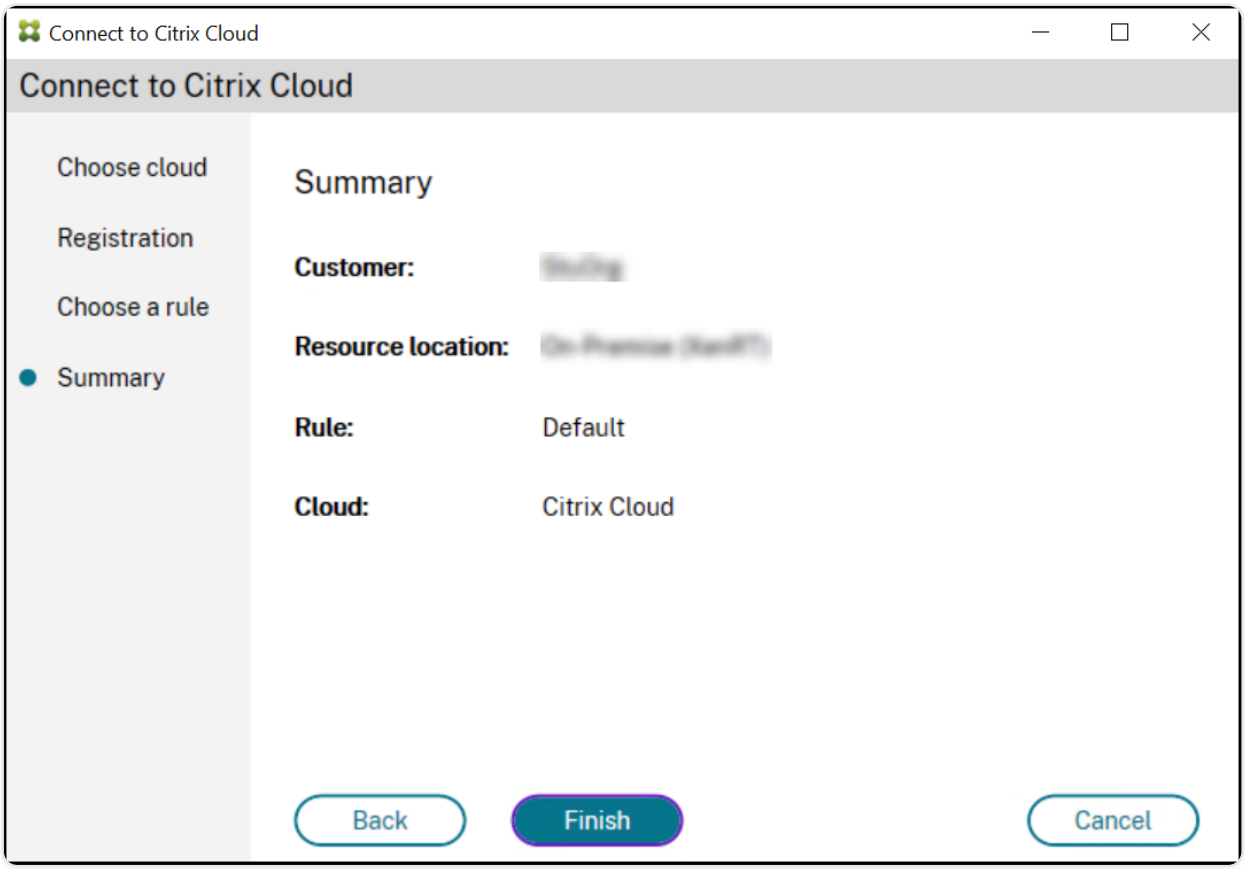
4. Once the registration code is validated, select the required **Resource location** from the drop-down list.



5. 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.
6. In the **Choose a rule** section, use an existing rule or create a rule. Click **Next**.



7. In the **Summary** section, 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.

> **Note:**
>
> An on-prem FAS server can issue user certificates to allow access to Citrix Cloud and Citrix Virtual Apps and Desktops at the same time.

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**.

Advanced configuration

The 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.

FAS V2 ticketing and the registry address list

Prior to FAS 2511, FAS created **V1** (version 1) format tickets, which start with an index byte. The VDA needs to determine which FAS server issued the ticket. It does this by using the index byte to look up the FAS address from the list of FAS addresses in its registry.

GPO generally configures the list of FAS addresses on the VDA. On Windows VDAs, the registry location of the address list is `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\Authentication\UserCredentialService\Addresses`

The address list on the VDA must exactly match the address list on StoreFront, otherwise single-sign on fails. This requirement was a significant source of configuration errors for customers, especially ones with complex deployments.

FAS 2511 introduces **V2** (version 2) format tickets. The address (that is, FQDN and port) of the FAS server is written into the ticket itself, thus the VDA does not need to consult the registry address list.

Compatibility

From 2511 onwards, FAS generates V2 tickets by default. V2 tickets are compatible with all Windows and Linux VDA versions.

VDAs prior to version 2511 continue to consult the registry address list, using the index byte as described in the previous section.

Only 2511 and later Windows and Linux VDAs are able to parse V2 tickets, and therefore do not need the registry address list.

V2 tickets are compatible with any version of StoreFront, and a StoreFront upgrade is not necessary.

If you experience issues with V2 tickets, you can configure FAS to generate V1 tickets using this PowerShell command:

```
Set-FasServer -Address localhost -TicketVersion 1
```

To revert to V2 tickets generation, use this PowerShell command:

```
Set-FasServer -Address localhost -TicketVersion 2
```

FAS ticket version the VDA understands

Only VDA 2511 and above can parse V2 tickets. Previous versions treat the V2 ticket as if it were a V1 ticket.

To confirm whether a VDA understands the V2 ticket version, inspect the event log on the FAS server.

If FAS and your VDA is 2511 or later, you must see an event log entry similar to the following during VDA launch. The event is in the **Windows Logs > Application log** on your FAS server:

```
Level: Information


Source: Citrix.Authentication.FederatedAuthenticationService


EventId: 204


Text: [S204] Relying party [VDA machine name] accessing the Logon Provider
```

```
for [User UPN] in role: [FAS Role] [Operation: XXXX] as authorized by
[StoreFront machine name]. Caller ticket version: 2. [correlation: XXXX]
```

In this event, the caller ticket version is **2**. This indicates that the VDA doesn't need to be configured with a registry FAS address list.

Conversely, if your VDA does not support V2 tickets, the event log entry have caller ticket version **1**:

```
Level: Information

Source: Citrix.Authentication.FederatedAuthenticationService

EventId: 204

Text: [S204] Relying party [VDA machine name] accessing the Logon Provider
for [User UPN] in role: [FAS Role] [Operation: XXXX] as authorized by
[StoreFront machine name]. Caller ticket version: 1. [correlation: XXXX]
```

Configure FAS V2 tickets with StoreFront

Any version of StoreFront can be used, since the FAS ticket is opaque to StoreFront, and no special configuration is required.

Configuration of FAS server addresses on StoreFront continues to use the registry address list, supplied using a GPO.

Configure FAS V2 tickets with Citrix Cloud Workspace

When FAS is connected to Citrix Cloud, FAS requires that its address is present in its own registry address list. This behavior is to support V1 tickets. If not found, the FAS admin console displays a warning, and FAS doesn't provide a single sign-on for Citrix Cloud Workspace launches.

However, if your entire deployment is using V2 tickets (that is, your FAS server and VDAs are 2511 or later), then there is no need for the registry address list on the FAS server.

You can use the following PowerShell to prevent a cloud-connected FAS from requiring the registry address list:

```
Set-FasCloudConfig -Address localhost -SkipGpoCheck $true
```

Other PowerShell changes

In addition to the commands noted above, the following changes have been made in FAS 2511's PowerShell.

Display the FAS server's FQDN and port

The following PowerShell command now returns the FQDN and listening port of the FAS server. This is the FAS address information encoded into V2 tickets.

```
Get-FasServer -Address localhost
```

Address parameter of cmdlets

Prior to 2511, any Address parameter of a FAS PowerShell command (other than "localhost") was checked against the FAS server's registry address list. To change this behavior, it was necessary to use the following command:

```
Set-FasAdministrationPolicy -CheckAddressAgainstGpo $false
```

From 2511 onwards, FAS PowerShell commands don't check the Address parameter against the address list. To revert to the previous behavior, run the following PowerShell command:

```
Set-FasAdministrationPolicy -CheckAddressAgainstGpo $true
```

Enable Federated Authentication Service for a tenant customer

This article describes the steps to enable Federated Authentication Service (FAS) in multitenant Managed Service Provider (MSP) environments. For more information, see Reference Architecture: Citrix Service Provider DaaS.

Prerequisites

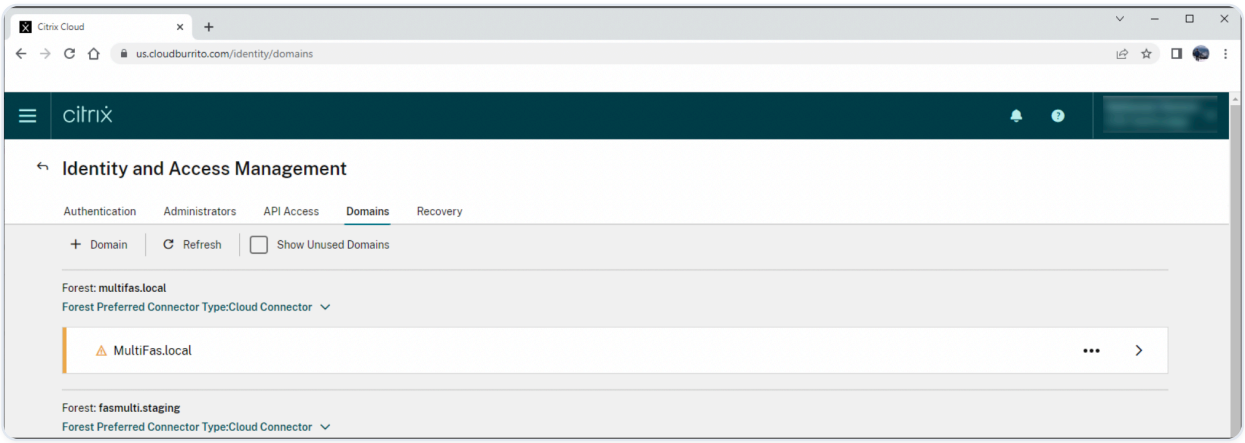
- You have administrator access to Domains and Resource Location on Citrix Cloud. For more information, see Modify administrator permissions.
- You have set up a tenant-MSP relationship. For more information, see Citrix DaaS for Citrix Service Providers.

Configure the MSP Customer

1. Use a Cloud Connector to make active directory domains available to Citrix Cloud.

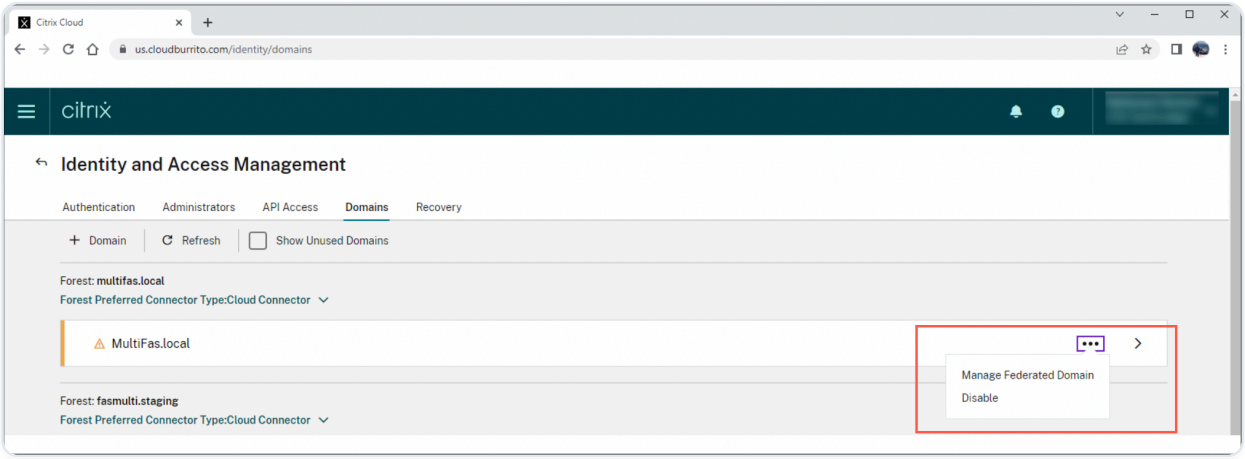
   Connect the on-prem infrastructure to the Citrix Cloud by installing cloud connectors.

   Verify that the domains associated with the on-prem domain controller are available under **Identity and Access Management** > **Domains**.

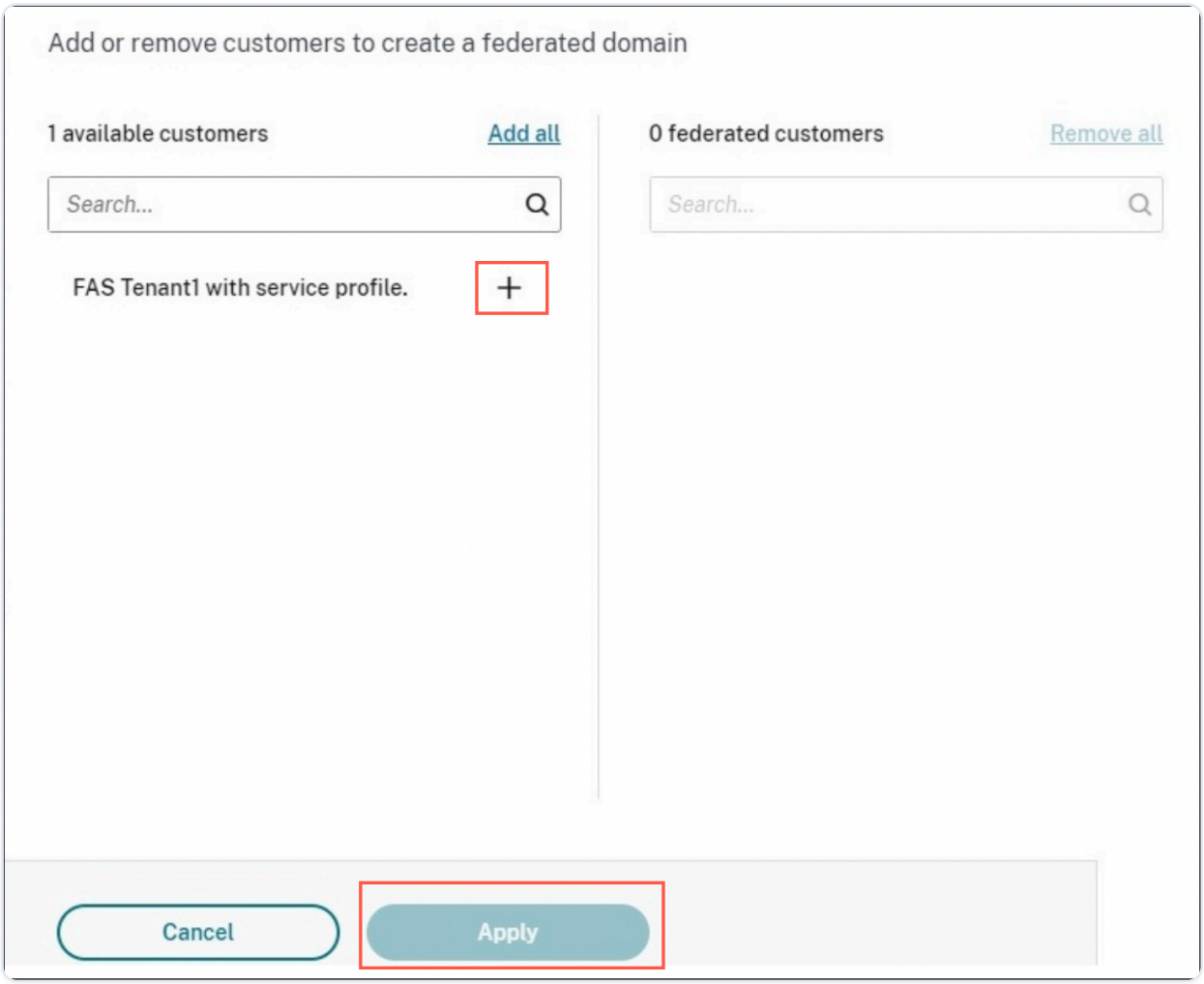


2. Federate the domain to the tenant.

   Select the domain and click the drop-down menu (**...**) and click **Manage Federated Domains**.

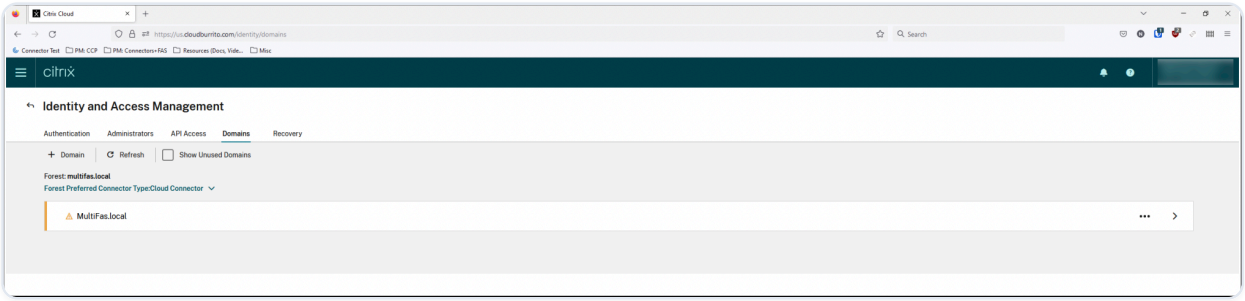


   Find the tenant and click **+**. Then click **Apply**.



3. Verify that the domains associated are present in the tenant.

   This step is an optional. Sign in to the console for the tenant customers and verify that the domains are listed under **Identity and Access Management** > **Domains**.



   Return to the MSP customer.

4. Install and register a FAS server with Citrix Cloud.

   Install FAS in the Active Directory (AD) forest where the tenant's Citrix Virtual Apps and Desktops resources are located. Connect FAS to the cloud resource location associated with that AD forest. To install a FAS server, see Install and configure.

5. Configure the tenant customer

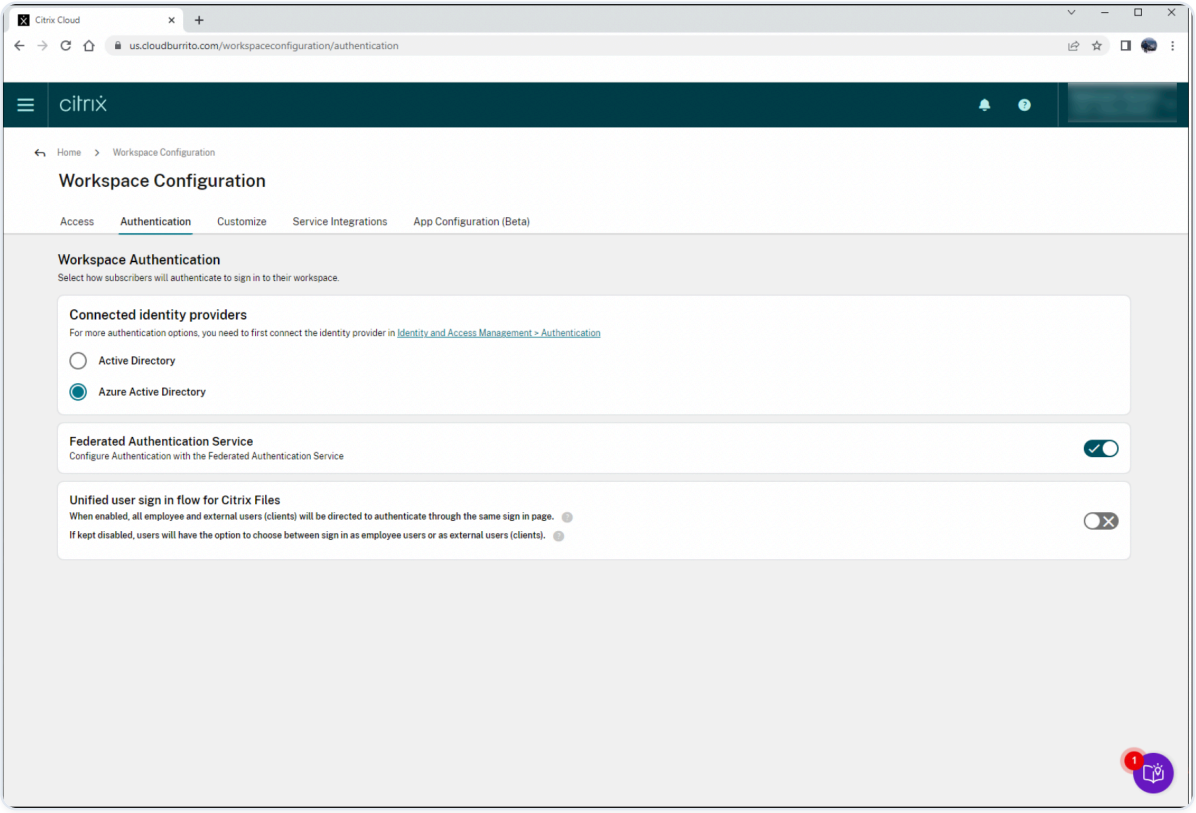
Enable FAS for the tenant customer

- Configure your Identity Provider (IdP)

  Switch to the tenant customer. Go to **Identity and Access Management** > **Authentication**. Connect to your IdP and ensure that AD is synchronized with the IdP.

- Enable FAS for a tenant

  Go to **Workspace Configuration** > **Authentication**. Select the authentication that you've set up and enable FAS.



Known issue

There's a known problem with deleting a MSP domain before removing the federated domains for tenants. You can still enable FAS for the tenants, but FAS fails since the domain doesn't exist for MSP anymore.

Azure Active Directory single sign-on

> **Note:**

> Since July 2023, Microsoft has renamed Azure Active Directory (Azure AD) to Microsoft Entra ID. In this document, any reference to Azure Active Directory, Azure AD, or AAD now refers to Microsoft Entra ID.

> Citrix Federated Authentication Service (FAS) provides single sign-on (SSO) to domain-joined Virtual Delivery Agents (VDAs). FAS achieves SSO by supplying the VDA with a user certificate, which the VDA uses to authenticate the user to Active Directory (AD). Once you sign on to the VDA session, you can access AD resources without reauthentication.

It's common to implement Microsoft Entra ID (ME-ID) with synchronization between your AD and Microsoft Entra ID, which creates hybrid identities for both users and computers. This article describes the additional configuration required to achieve SSO to Microsoft Entra ID from within your VDA session when using FAS, which allows the user to access Microsoft Entra ID-protected applications without reauthentication.

> **Note:**
>
> - You don't require any special configuration for FAS to use SSO for Microsoft Entra ID.
> - You don't require the FAS in-session certificates.
> - You can use any version of FAS.
> - You can use any version of the VDA that supports FAS.

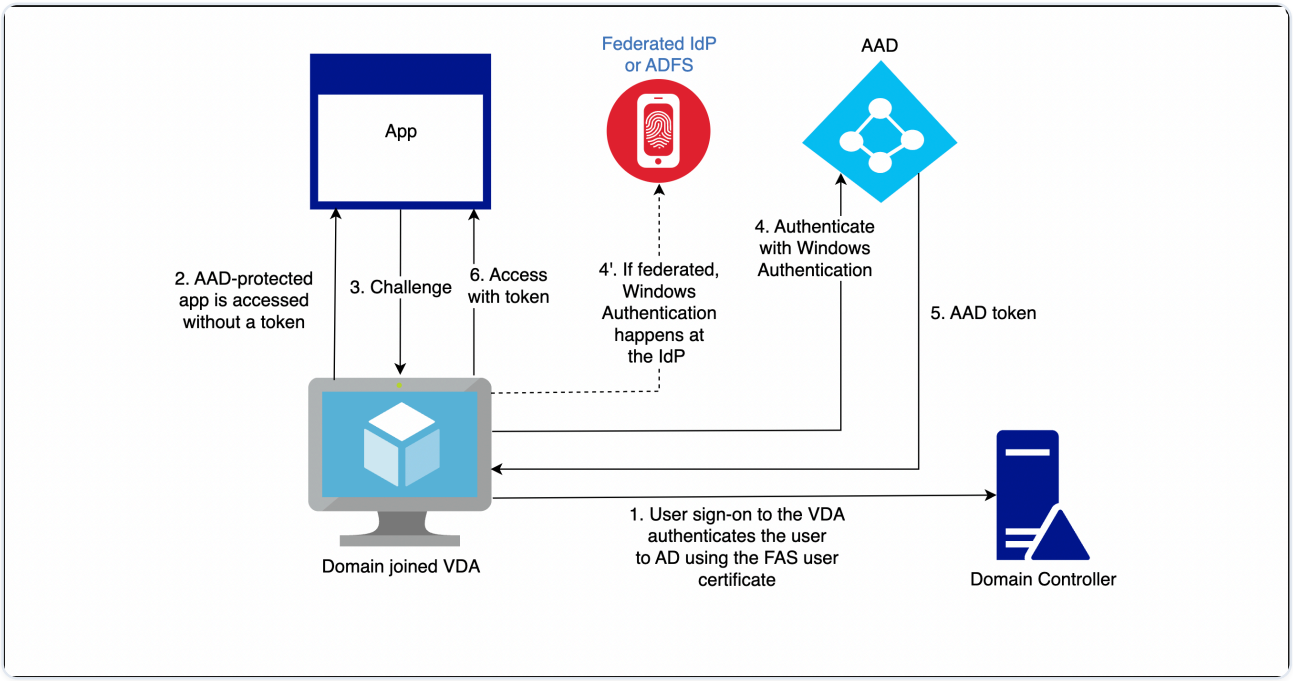
> The techniques for Microsoft Entra ID SSO are summarized in the following table:

ME-ID AUTHENTICATION TYPE	VDA IS DOMAIN JOINED	VDA IS HYBRID JOINED
Managed	Use ME-ID seamless SSO	Use ME-ID Certificate Based Authentication
Federated to Active Directory Federation Services (ADFS)	Enable Windows Authentication at ADFS	Ensure that the WS-Trust *certificatemixed* endpoint is enabled
Federated to a third party identity provider	Use a third party solution	Use a third party solution

- A managed Microsoft Entra ID domain is one where the user authentication happens at Microsoft Entra ID, sometimes referred to as native Microsoft Entra ID authentication.
- A federated Microsoft Entra ID domain is one where Microsoft Entra ID is configured to redirect authentication elsewhere. For example, to ADFS or to a third party identity provider.
- A hybrid joined VDA is AD joined and Microsoft Entra ID joined.

Domain-joined VDAs

For domain-joined VDAs, achieve SSO to Microsoft Entra ID using Windows Authentication (traditionally called Integrated Windows Authentication, or Kerberos). Authentication to Microsoft Entra ID happens when the user accesses an Microsoft Entra ID-protected application from within the VDA session. The following diagram shows the authentication process on a high-level:



The exact details vary depending on whether the Microsoft Entra ID domain is managed or federated.

For information on the managed Microsoft Entra ID domain setup, see Seamless single sign-on.

For an Microsoft Entra ID domain federated to ADFS, enable Windows Authentication at the ADFS server.

For an Microsoft Entra ID domain federated to a third party identity provider, a similar solution exists. Contact your identity provider for help.

> **Note:**

> You can also use the solutions listed for the domain-joined VDAs for hybrid-joined VDAs. But an Microsoft Entra ID Primary Refresh Token (PRT) isn't generated when using FAS.

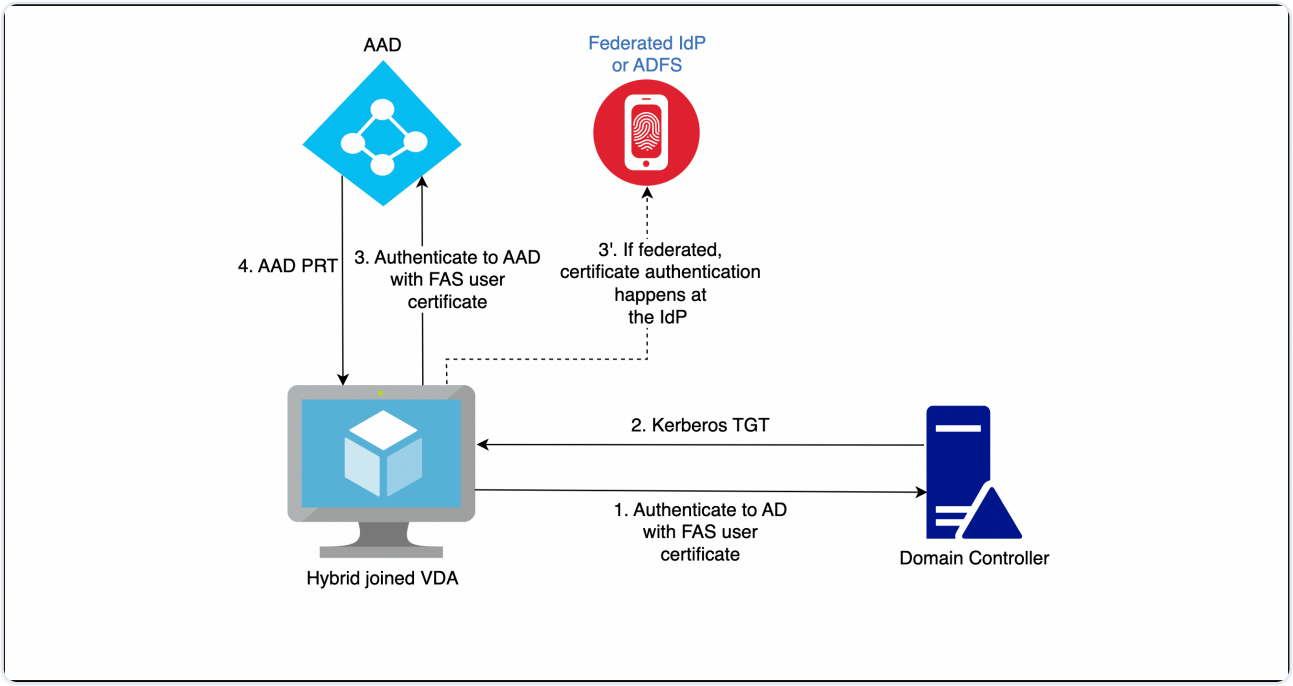
Hybrid-joined VDAs

Hybrid-joined VDAs are joined to AD and Microsoft Entra ID at the same time. When the user signs in to the VDA, the following artifacts are created:

- A Kerberos Ticket Granting Ticket (TGT), to authenticate to AD resources
- A Primary Refresh Token (PRT), to authenticate to Microsoft Entra ID resources

The PRT contains information about both the user and the computer. This information is used in an Microsoft Entra ID conditional access policy if necessary.

Since FAS authenticates the user by supplying a certificate to the VDA, a PRT can only be created if certificate-based authentication for Microsoft Entra ID is implemented. The following diagram shows the authentication process on a high-level:



The exact details vary depending on whether the Microsoft Entra ID domain is managed or federated.

For a managed Microsoft Entra ID domain, configure Microsoft Entra ID CBA. For more information, see Overview of Azure AD certificate-based authentication. The VDA uses Microsoft Entra ID CBA to authenticate the user to Microsoft Entra ID with the user's FAS certificate.

> **Note:**

> The Microsoft documentation describes sign in with a smart card certificate, but the underlying technique applies when signing in with a FAS user certificate.

> For an Microsoft Entra ID domain federated to ADFS, the VDA uses the ADFS server's WS-Trust *certificatemixed* endpoint to authenticate the user to Microsoft Entra ID with the user's FAS certificate. This endpoint is enabled by default.

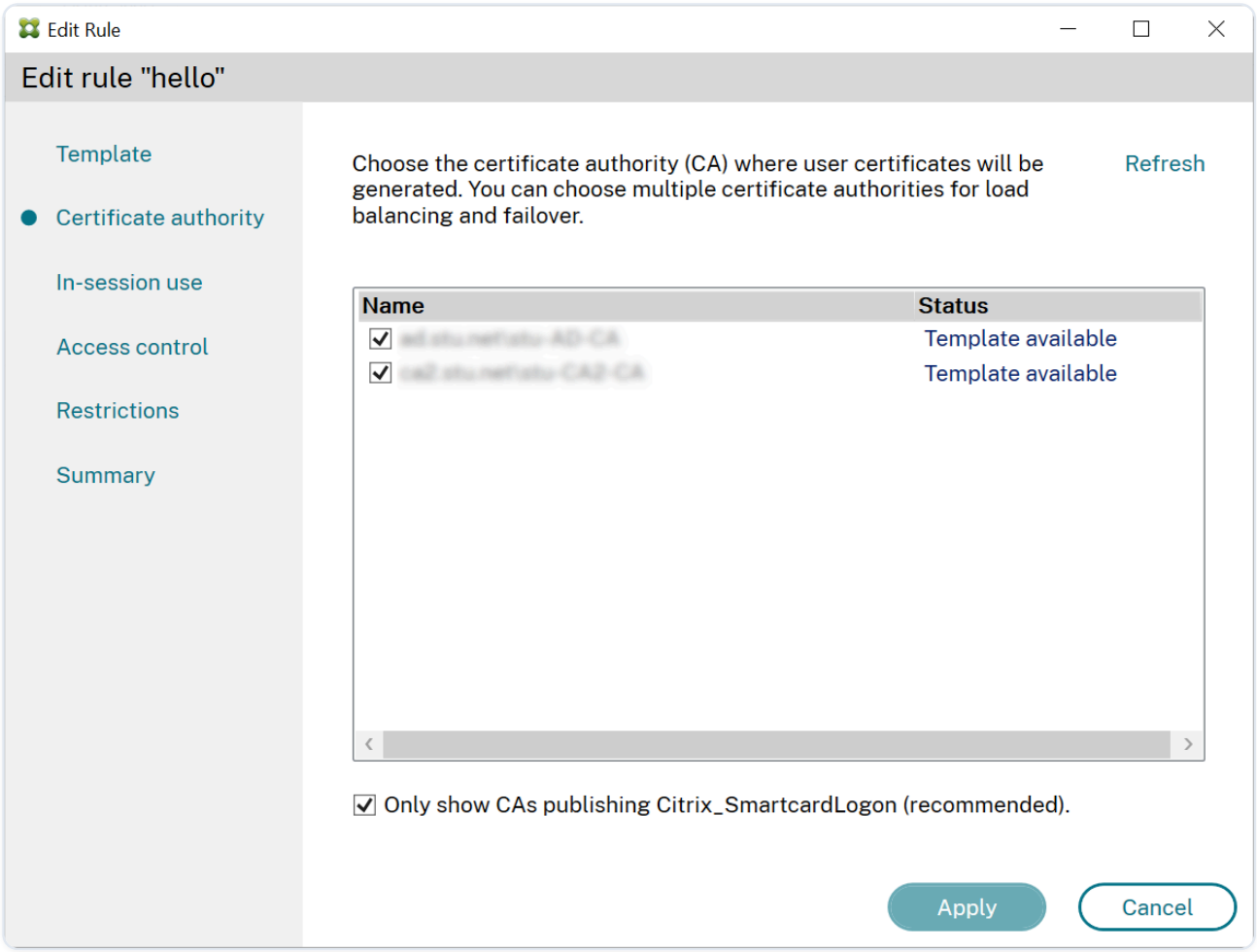
For an Microsoft Entra ID domain federated to a third party identity provider, a similar solution may exist. The identity provider must implement a WS-Trust *certificatemixed* endpoint. Contact your identity provider for help.

Certificate authority configuration

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 must have a basic knowledge of PowerShell before running 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 that you want to use is not publishing the desired template, perform the Setup a certificate authority step for the CA.

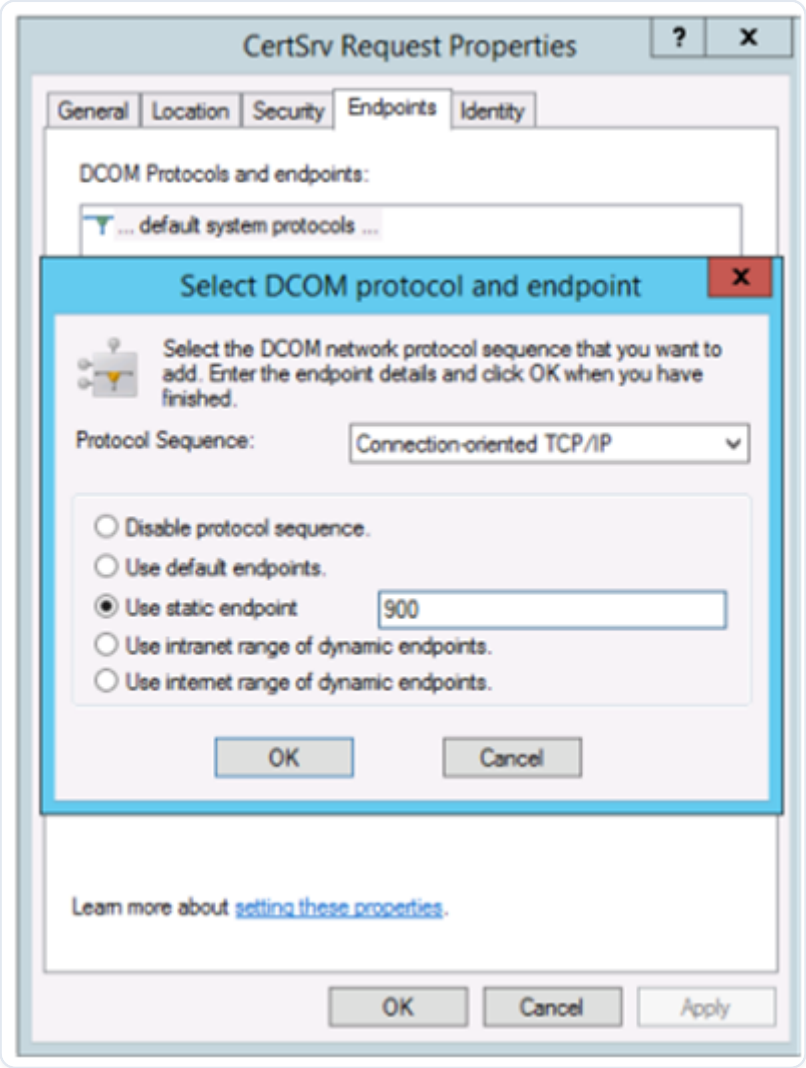
> **Note:**
>
> You do not have to perform the Authorize this service step for every CA, because the authorization certificate configured in this step can be used at any of your CAs.

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 switches to another available CA server.

Configure the Microsoft certificate authority for TCP access

FAS accesses the Microsoft CA using DCOM. DCOM uses port 135 to discover the port on which the service is listening. By default, the listening port is allocated dynamically. This can result in complexities when implementing firewall security. Therefore, Microsoft has a provision to configure a static port. To configure a static port on Microsoft CA, select **Start** > **Run** > `dcomcnfg.exe` to open the **DCOM configuration** panel. Expand **Computers** > **My computer** > **DCOM Config** to show the CertSrv Request node. Then, 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 preceding graphic).

In this example, the firewall needs to allow port 135 and port 900.

Restart the Microsoft certificate authority to apply the change.

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 135. When a client needs to use

DCOM, it connects to the DCOM RPC Service on the server and requests access to a particular DCOM server. This triggers port 900 (in this example) to be opened, and the DCOM server instructs the client to connect to that port.

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 {

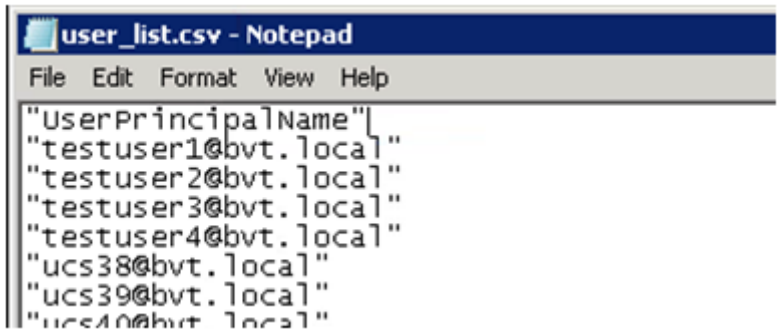
    Get-ADUser -Filter {(UserPrincipalName -ne "null") -and (Enabled -eq
"true")} -Properties UserPrincipalName | Select UserPrincipalName |
Export-Csv -NoTypeInformation -Encoding utf8 -delimiter "," $filename

}
```

`Get-ADUser` is a standard cmdlet to query for a list of users. The preceding example 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 leave 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.

```
Add-PSSnapin Citrix.A*

$csv = "user_list.csv"

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

$users = Import-Csv -encoding utf8 $csv

foreach ( $user in $users )

{

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

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

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

    }

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

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

    }

}
```

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

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

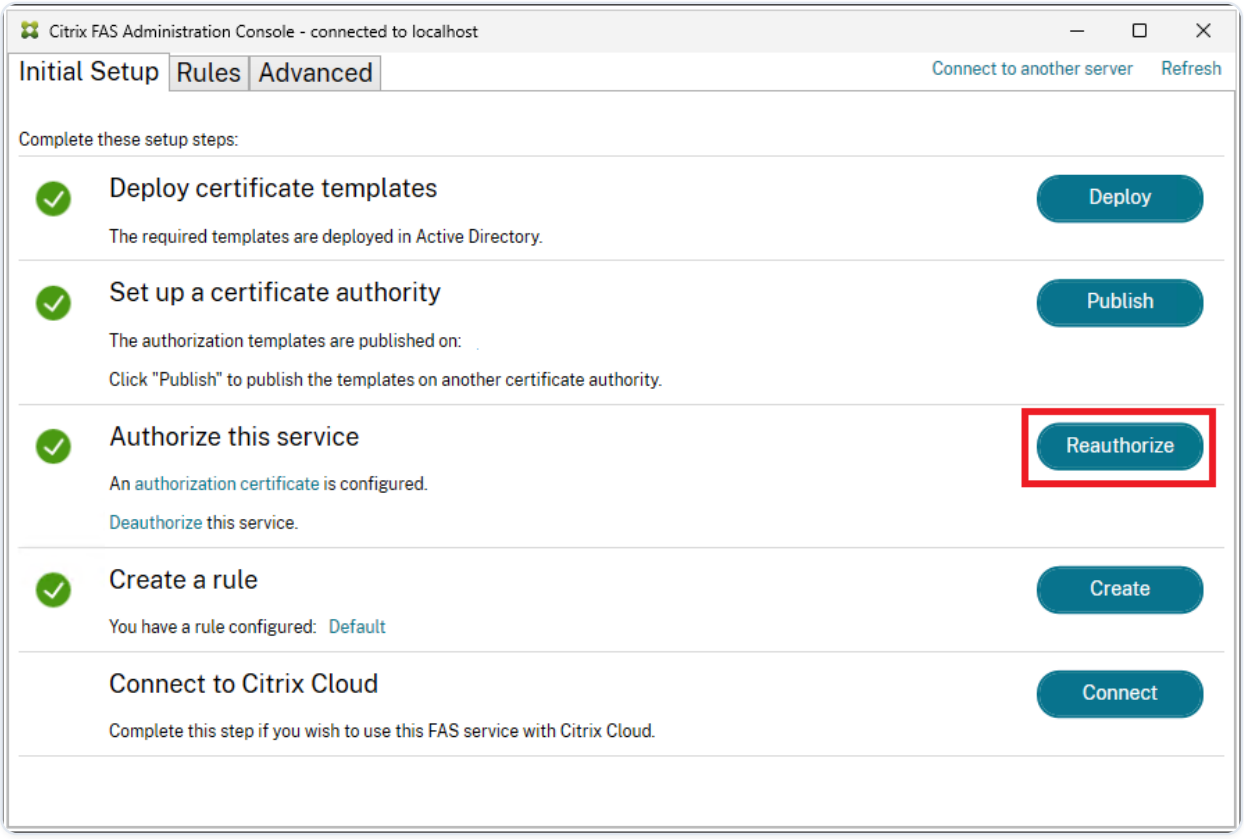


Renew FAS authorization certificate

You can renew a FAS authorization certificate without disrupting FAS users.

Using the FAS administration console

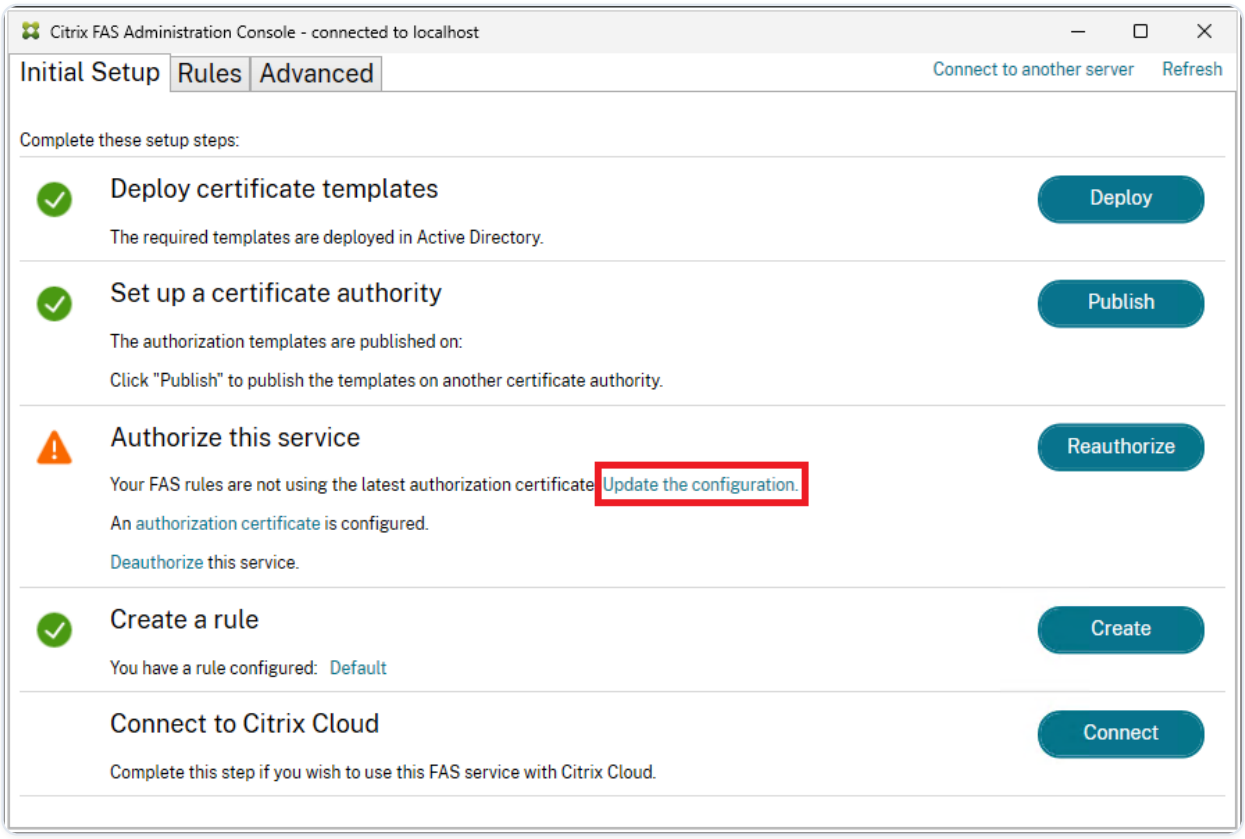
- Click **Reauthorize** to generate a new FAS authorization certificate request:



You need to manually approve the request at the CA. For more information, see Authorize Federated Authentication Service.

- Once a new authorization certificate has been generated, FAS provides an indication that it is not yet associated with your rules. Click **Update the configuration** to associate the new

authorization certificate with your rules.



Using PowerShell

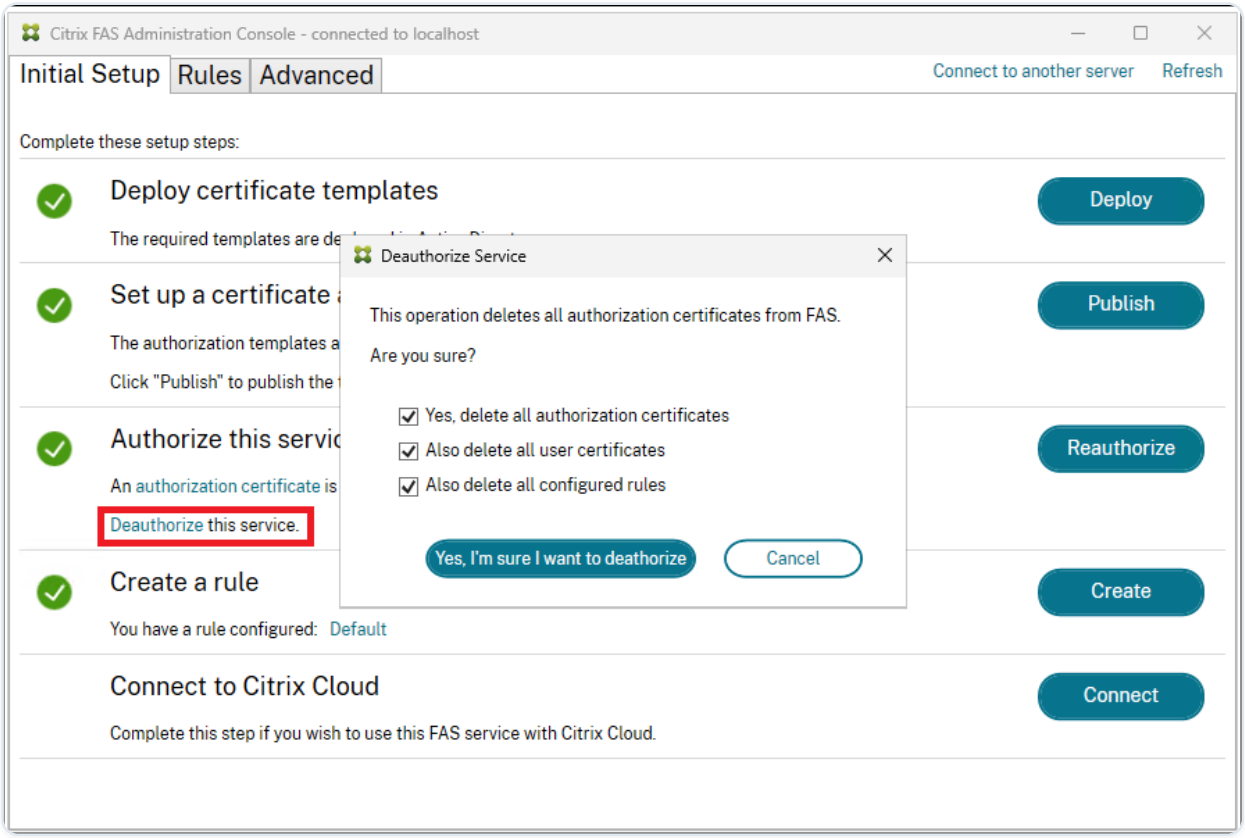
Complete the following sequence:

1. Create an authorization certificate: `New-FasAuthorizationCertificate`
2. Note the GUID of the new authorization certificate, as returned by: `Get-FasAuthorizationCertificate`
3. Swap the new authorization certificate: `Set-FasCertificateDefinition –AuthorizationCertificate <GUID>`
4. Delete the old authorization certificate: `Remove-FasAuthorizationCertificate`. Ensure to use the `DeleteUserCerts $false option`, so that the user activity is not disrupted.

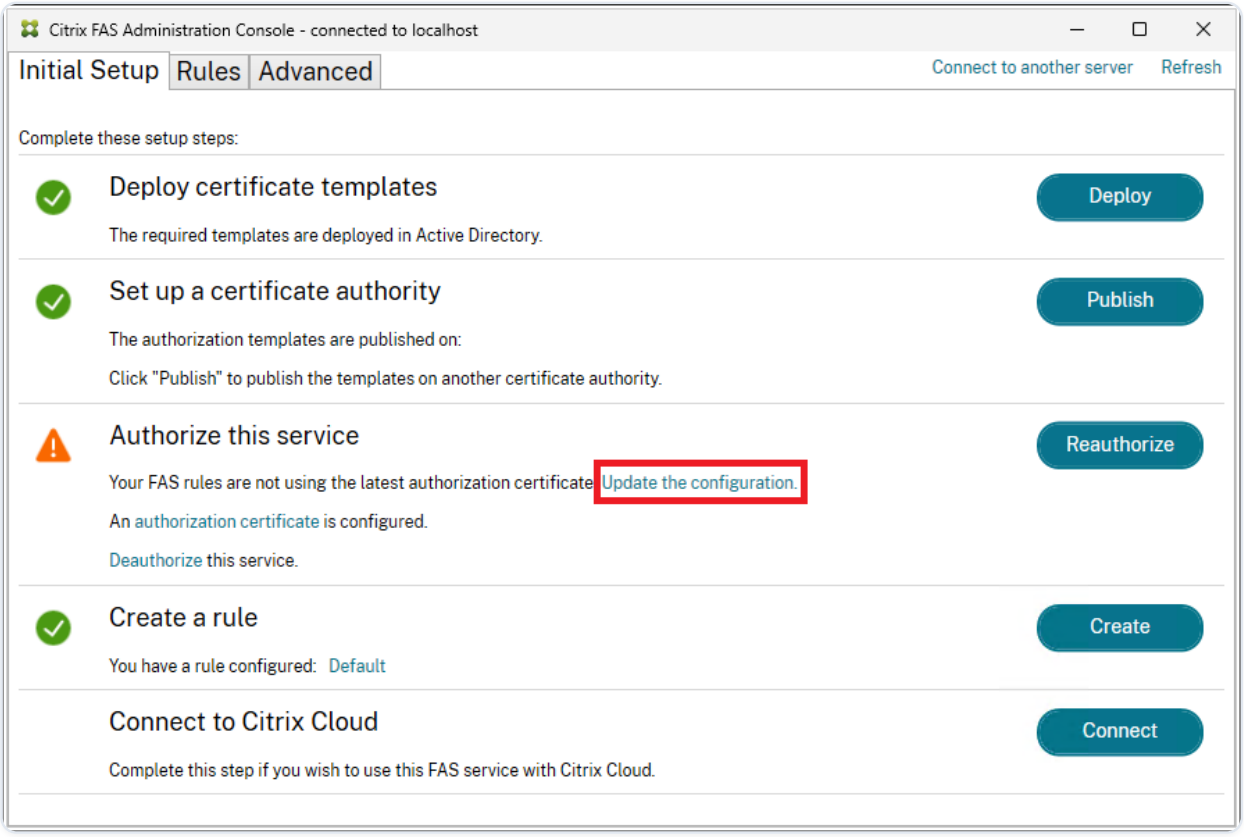
Deauthorizing FAS and deleting FAS certificates

Using the FAS administration console

- Click the **Deauthorize** link and delete the authorization certificates. You can delete all user certificates and all the rules (though it is not necessary for clearing out certificates).



- If you do not delete the rules, when you later authorize FAS you get a warning:



The warning indicates that the authorization certificate is not yet associated with your rules. Click **Update the configuration** to associate the new authorization certificate with your rules.

Using PowerShell

Use the following PowerShell command to delete the authorization certificate and user certificates:

```
$AuthCert = Get-FasAuthorizationCertificate -Address localhost

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

Note:

`Get-FasAuthorizationCertificate` returns a list of authorization certificates and pending authorization certificate requests, for you to inspect the value of `$AuthCert` before proceeding with `Remove-FasAuthorizationCertificate`.

You can remove the authorization certificate, but retain the user certifcates, by setting the `DeleteUserCerts` parameter to false:

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

The remaining user certificates can still be usable by FAS for VDA sign-in and in-session certificates, which is useful when renewing FAS authorization. For more details, see Renew FAS authorization certificate.

- You can remove user certificates thus:

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

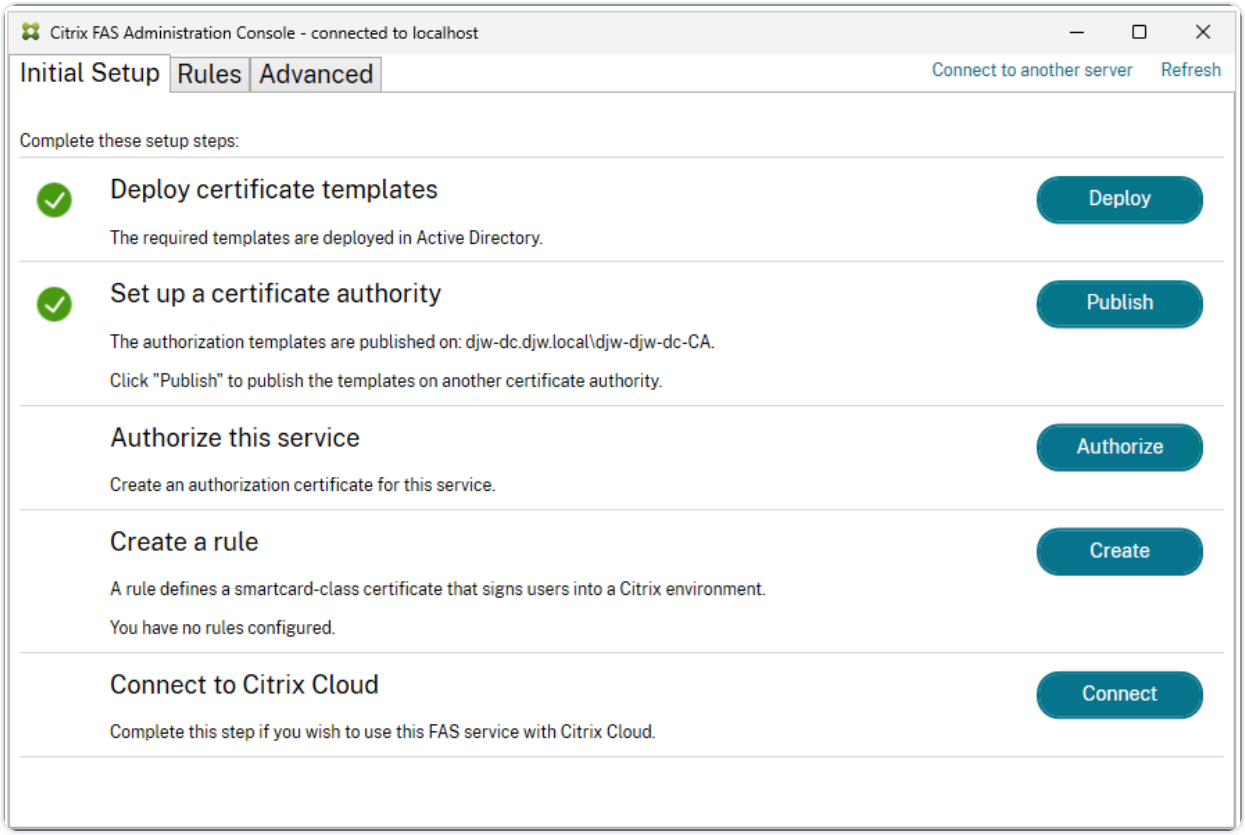
This command removes all user certificate from the FAS server. The command has options to filter the set of certificates removed.

> **Note:**
>
> When FAS removes an authorization or user certificate from its internal storage, it also deletes the associated keypair.

Offline authorization

The FAS authorization certificate can be requested offline using PowerShell. This is suitable for organizations that do not want their certificate authority to issue an authorization certificate through an online certificate signing request.

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**.



2. Load the following PowerShell cmdlets on the FAS server:

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

3. Generate the keypair and create the certificate signing request by entering the following PowerShell cmdlet on the FAS server:

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

This results in:



> **Note:**
>
> The properties of the keypair generated are determined by the FAS authorization key configuration. For more details, see Private key protection.

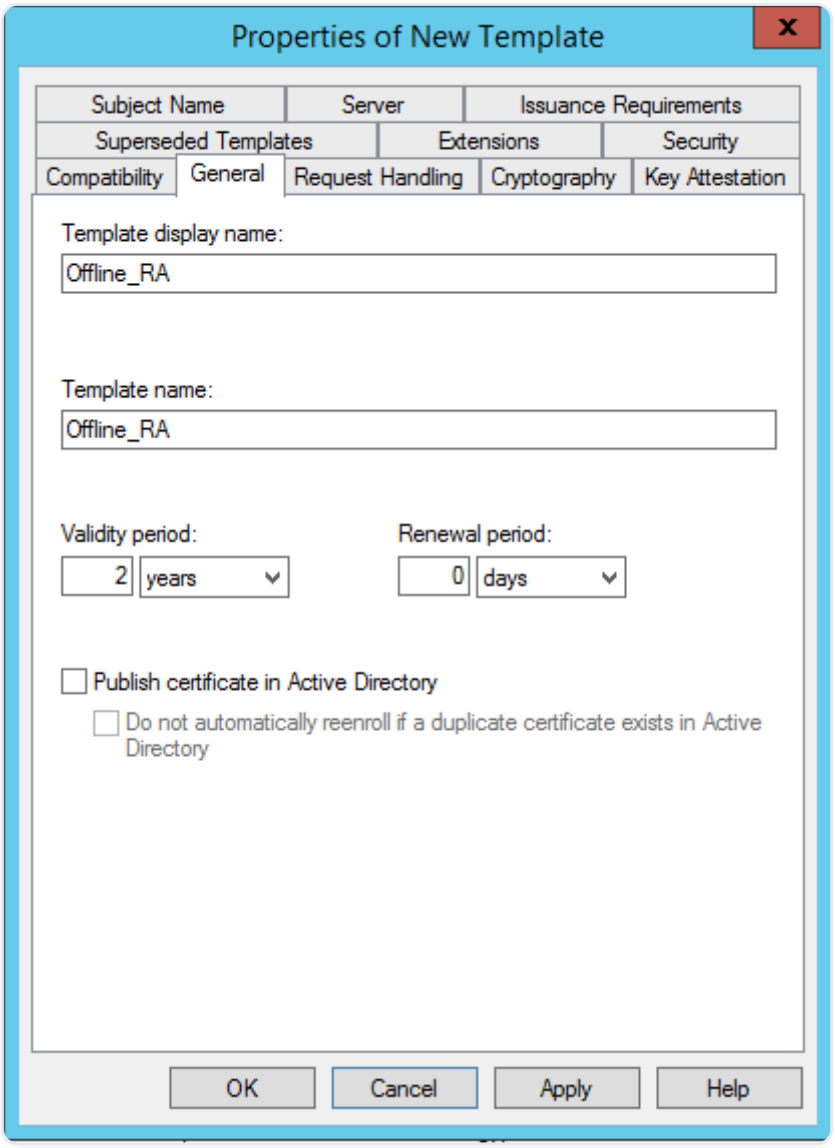
4. Copy the certificate request to disk:

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

5. Present the certificate request file (in this example, authcert.csr) to your certificate authority, approve the request, and obtain a certificate response.

   The following five steps are specific to using a Microsoft Enterprise Certification Authority; for other CAs, contact your CA vendor for help.

   - 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 two years:



- 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 that you created.
- Submit the certificate signing request to your certificate authority by typing the following into a PowerShell command prompt on the FAS server:

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

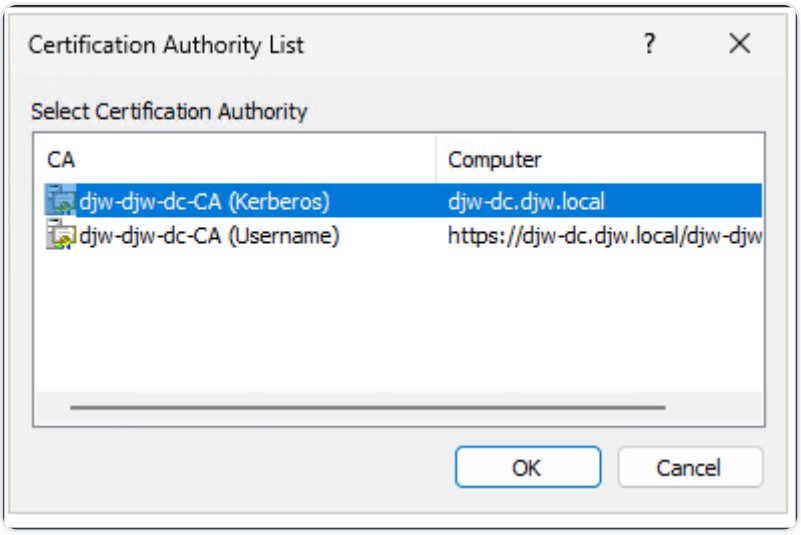
For example:

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

Running the preceding command results in:

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

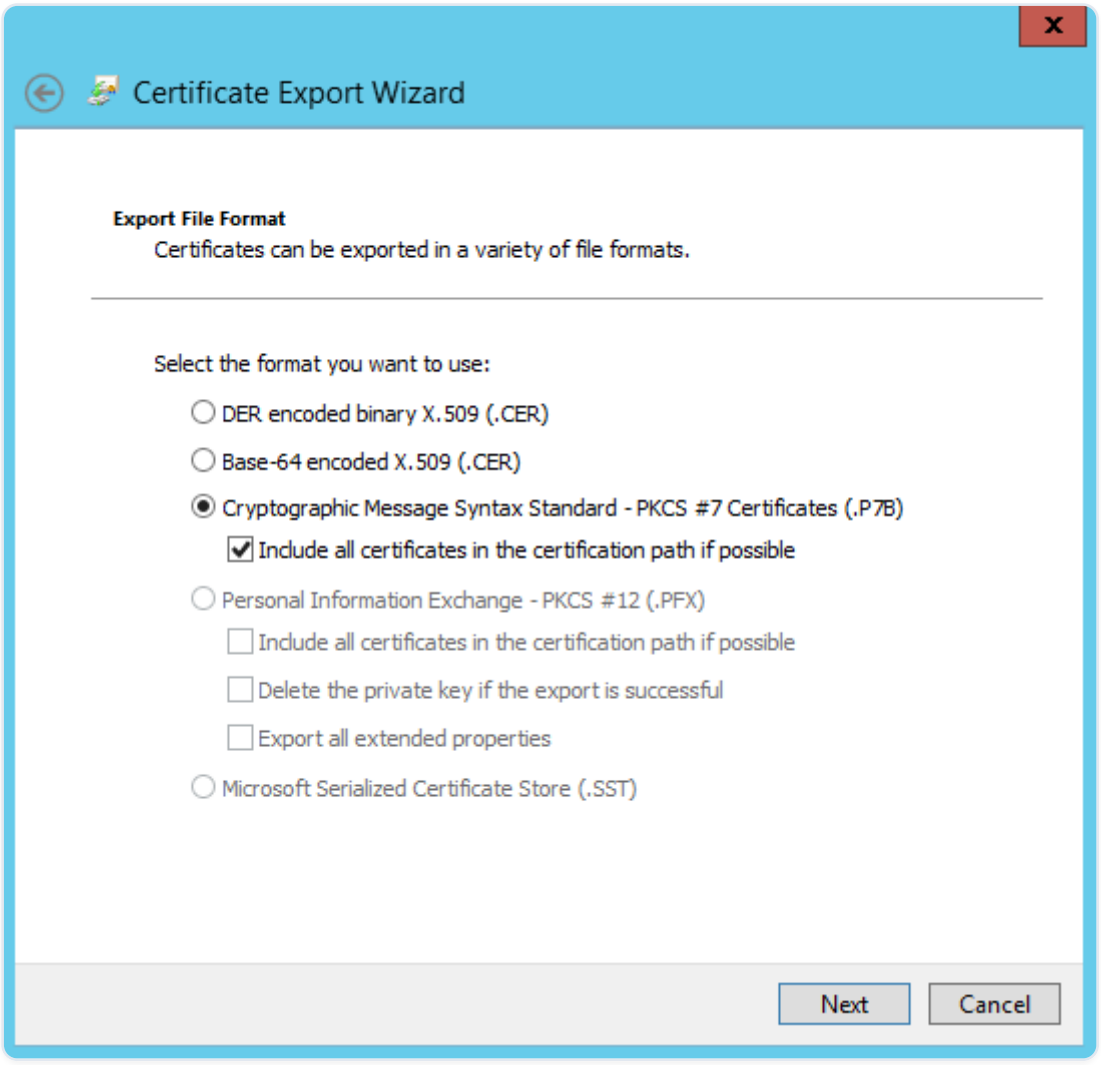
At this point a **Certification Authority List** window might appear. The certificate authority in this example has both DCOM (top) and HTTP (bottom) enrollment enabled. Select **DCOM**, if available, then click **OK**:



After the certificate authority has been specified, the command completes and displays the RequestID:

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

- On the certificate authority server, in the certificate authority MMC snap-in, click **Pending Requests**. Find the Request ID. Then right-click the request and choose **Issue**.
- Select the **Issued Certificates** node. Find the certificate that was issued (the Request ID must 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.

6. Copy the exported certificate file onto the FAS server.
7. Import the registration authority certificate into the FAS server by entering the following PowerShell cmdlet on the FAS server:

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

For example:

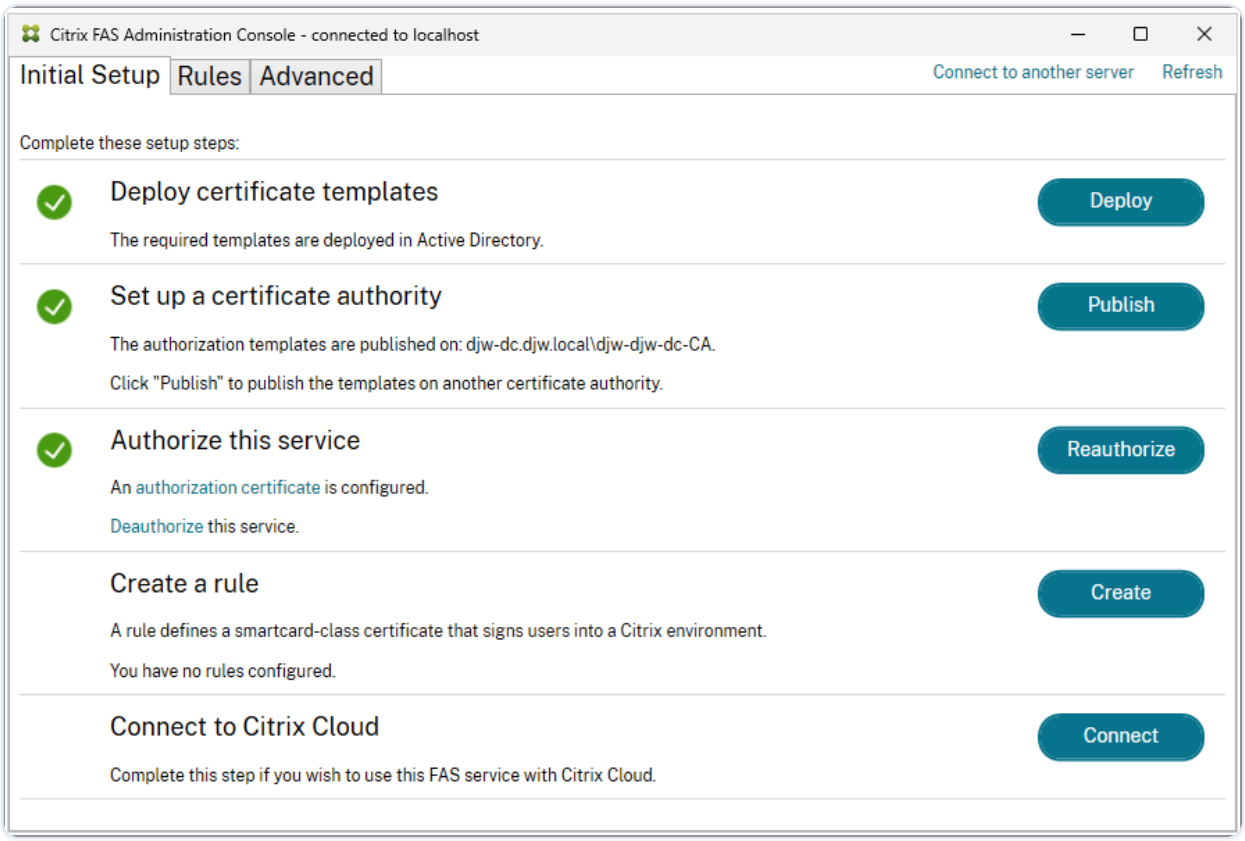
```
Import-FasAuthorizationCertificateResponse -Address localhost -Id
$AuthCertRequest.Id -Pkcs7CertificateFile C:\temp\response.p7b
```

Running this command results in:

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


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

8. Check the FAS admin console. It must show that FAS is now authorized.



> **Note:**
>
> The step **Authorize this service** has a green check mark next to it.

9. Continue configuration by creating a rule. For more details, see Configure rules.

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

Introduction

FAS certificates are stored in an embedded database on the FAS server. The private keys associated with FAS certificates are stored under the Network Service account of the FAS server. By default, the keys are non-exportable, 2048-bit RSA, created and stored in the Microsoft Software Key Storage Provider.

Using FAS PowerShell commands PowerShell cmdlets, it's possible to change the properties and storage location of the private keys.

Note:

FAS configuration and certificates are stored locally on the FAS server. The data is not shared between FAS servers.

In FAS releases before Citrix Virtual Apps and Desktops 2411, private key properties were configured by editing the XML file at `%programfiles%\Citrix\Federated Authentication Service\Citrix.Authentication.FederatedAuthenticationService.exe.config.` This has been superseded by PowerShell commands, which provide more flexibility and can be applied without restarting the FAS server. Additionally, unlike the XML file settings, configuration made using PowerShell is retained when the FAS server is upgraded. Therefore, configuration using the XML file for the following settings is no longer supported:

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

See the section, Upgrading from versions of FAS before Citrix Virtual Apps and Desktops™ 2411.

Information about FAS certificates and templates

There are two types of certificates held by FAS: the authorization certificate, of which there is normally one instance, and the user certificates.

> **Note:**
>
> The FAS authorization certificate is also sometimes referred to as an **Registration Authority** or **Request Agent** (RA) certificate.

> FAS uses certificate templates when requesting certificates, as described in the following section. While FAS does specify the name of a template in certificate requests, it does not read the content of the template. Therefore changing the template's settings does not influence the certificate requests made by FAS. Changing certain properties of the template affects the certificate generated by the CA. For example, you can change the validity period using the template.

FAS authorization certificate

This certificate is created when you configure FAS. You can use the FAS administration console's **Authorize** or **Reauthorize** button to request a new authorization certificate.

It's also possible to use PowerShell commands, which provide more flexibility:

- `New-FasAuthorizationCertificate`: This command behaves similarly to the FAS administration console, except it's possible to specify the certificate templates to use in the authorization process.
- `New-FasAuthorizationCertificateRequest`: This command creates an *offline* request for an authorization certificate; Offline authorization.

The authorization certificate is also sometimes referred to as an RA certificate, because FAS is acting as a registration authority, that is requesting certificates on behalf of a user. The certificate has the enhanced key usage **Certificate Request Agent**, that allows it to be used as an authorization credential when requesting FAS user certificates.

By default, the authorization process uses the following templates:

- `Citrix_RegistrationAuthority_ManualAuthorization`: The certificate created using this template is temporary and short lived, used to *bootstrap* the authorization process;

- `Citrix_RegistrationAuthority`: The certificate created using this template has a long validity, and is stored by the FAS server.

Authorizing FAS results in the following steps:

1. FAS creates a keypair, and sends a **Certificate Signing Request** (CSR) to the CA, specifying the public key of the keypair and the template `Citrix_RegistrationAuthority_ManualAuthorization`.
2. The template's issuance requirements specify that the CSR must be manually approved by the CA administrator.
3. Once the CA administrator has approved the CSR, the CA creates a certificate which FAS retrieves. This certificate has a short validity of one day and is only used for the following step. Once used, FAS destroys the certificate and its keypair.
4. FAS creates another keypair, and sends a second CSR to the CA, specifying the public key of this keypair and the template `Citrix_RegistrationAuthority`. The request is authorized by and signed with the certificate from the previous step.
5. The CA automatically issues the certificate, FAS retrieves the certificate, and FAS is now **Authorized**. By default, this authorization certificate has a validity of two years.

The settings used to create the keypairs mentioned before can be viewed using this PowerShell command:

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

FAS user certificates

FAS creates user certificates to sign users in to VDAs.

When FAS creates a user certificate, the following steps occur:

- FAS creates a key pair, and sends a CSR to the CA, specifying the public key of the keypair, the identity of the user, and by default, the template `Citrix_SmartcardLogon` (the template used is configurable).
- The CSR is signed using the FAS authorization certificate.
- `Citrix_SmartcardLogon` template has issuance requirement `Application Policy: Certificate Request Agent`. As this attribute is present in the FAS authorization certificate, the CA issues the user certificate automatically.
- FAS retrieves the certificate, and stores it in an embedded database on the FAS server.
- By default, the certificate has a validity of one week.

Later, the user certificate is made available to the VDA to sign the user in.

The settings used to create the keypair mentioned before can be viewed using the following PowerShell command:

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

Private key storage options

FAS can be configured to create and store keypairs in three categories of storage:

- Software: Normally using **Microsoft Software Key Storage Provider**, which is secured by software only; the data is stored on the disk.
- **Trusted Platform Module** (TPM): The TPM can be physical hardware on the computer, or a virtual TPM provided by a hypervisor.
- **Hardware Security Module** (HSM): This is a hardware peripheral or network device designed to securely store cryptographic keys.

> **Note:**
>
> There is a trade-off to consider. Hardware storage may be more secure, but is often less performant, especially when creating and storing a large number of user certificate keypairs.

> The private key associated with the FAS authorization certificate is particularly sensitive, as the certificate's policy allows whoever possesses the private key to authorize certificate requests, for any user. As a consequence, whoever controls this key can connect to the environment as any user.

> **Note:**
>
> Microsoft CAs can be configured to restrict the power of the FAS authorization certificate, including the set of users for whom certificates can be issued. See Delegated enrollment agents.

> For this reason, FAS allows you to configure the private key properties for authorization and user certificates independently.

Some typical configurations are as follows:

AUTHORIZATION CERTIFICATE KEY	USER CERTIFICATE KEYS	COMMENT
Software	Software	Default configuration
TPM	Software	Authorization certificate has hardware protection
HSM	HSM	All certificates have hardware protection

> **Note:**
>
> A hardware TPM is not recommended for user keys. Use TPM for the authorization certificate key only. If you plan to run your FAS server in a virtualized environment, check with your hypervisor vendor whether TPM virtualization is supported.

Key configuration PowerShell commands

The commands relating to the configuration of private keys are as follows:

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

For more information, see PowerShell cmdlets.

The key configuration for authorization and user certificates is independent, specified by the `CertificateType` argument. For example, to get the private key configuration used when requesting an authorization certificate (RA certificate):

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

To get the private key configuration used when requesting a user certificate:

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

You can use **Set-FasKeyConfig** and **Get-FasKeyConfig** to set and inspect the following private key properties:

PROPERTY	DEFAULT	COMMENT
Length	2048	Key length in bits. Note that, in the Microsoft template GUI, the **Cryptograhy** tab specifies the *minimum* key size. The CSR is rejected by the CA if the key length configured in FAS is less than the minimum key size specified in the template. For RSA keys, lengths can be 1024 bits, 2048 bits or 4096 bits. For ECC keys, lengths can be 256 bits, 384 bits or 521 bits.
Exportable	false	Whether the private key can be exported from its provider.
Prefix	none	Specifies a prefix to add to the identifier of private keys generated by FAS. The identifiers generated are comprised of the prefix and a GUID. For example,

PROPERTY	DEFAULT	COMMENT
		`MyPrefix70277985-6908-4C6F-BE59-B08691456804`.
EllipticCurve	false	If true an ECC keypair is generated, otherwise an RSA keypair is generated.
Key Storage Provider (KSP)	**true**	If true, FAS uses the modern Windows CNG API, and a KSP must be specified in the **Provider** property. If false, FAS uses the legacy CAPI API, and a Cryptographic Service Provider (CSP) must be specified in the Provider property. Citrix recommends using a KSP.
Provider	**Microsoft Software Key Storage Provider**	The name of the provider where keypairs are created and stored. You can change this property to specify a TPM or HSM. An HSM's KSP (or CSP) is provided by the HSM vendor. They provide instructions on how to install their

PROPERTY	DEFAULT	COMMENT
		software, and the name of the provider.
CSPType	24	Only relevant if the **KSP** property is set to **false**. Refers to `Microsoft KeyContainerPermissionAccessEntry.ProviderType Property PROV_RSA_AES 24`. Must always be 24 unless you are using an HSM with a CSP, and the HSM vendor specifies otherwise.

In addition, **Set-FasKeyConfig** can be used with the following switches, provided for convenience:

FLAG	DESCRIPTION
-UseDefaultSoftwareProvider	Sets the **Provider** property to **Microsoft Software Key Storage Provider** and the **KSP** field to **true**.
-UseDefaultTpmProvider	Sets the **Provider** property to **Microsoft Platform Crypto Provider** and the **KSP** field to **true**.

Microsoft Software Key Storage Provider is the provider usually used to create and store keys on disk.

Microsoft Platform Crypto Provider is the provider usually used to create and store keys in a TPM.

Get-FasKeyConfig also provides fields, which help confirm which provider and algorithm are being used:

FIELD	MEANING
IsDefaultSoftwareProvider	If true, indicates that the provider is set to **Microsoft Software Key Storage Provider** and the **KSP** field is set to **true**.
IsDefaultTpmProvider	If true, indicates that the provider is set to **Microsoft Platform Crypto Provider** and the **KSP** field is set to **true**.
Algorithm	**RSA** indicates that RSA keys will be created (the **EllipticCurve** property is **false**). **ECC** indicates that ECC keys will be created (the **EllipticCurve** property is **true**).

You can restore the settings to the defaults using `Reset-FasKeyConfig`.

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

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

Note:

Changes made to the Private key configuration (using `Set-FasKeyConfig` or `Reset-FasKeyConfig`) apply immediately to newly created certificates. However, existing authorization and user certificates with a different configuration are not affected.

> You can remove existing certificates by deauthorizing your FAS service from the administration console, or by using PowerShell commands in Deauthorizing FAS and deleting FAS certificates.

> Any pre-generated keys in the key pool which do not conform to the current user key configuration are discarded.

Configuration scenario examples

In each example, set the key configuration using the PowerShell provided before authorizing your FAS service, as the existing certificates are unaffected by any configuration change.

If you already have authorization or user certificates with the wrong key configuration you can remove them by Inspecting FAS certificates and Deauthorizing FAS and deleting FAS certificates.

If your FAS server is in a *live* deployment, consider putting it into maintenance mode while making configuration changes Maintenance mode.

Example 1 - Store all keys in Microsoft Software Key Storage Provider

As this is by default, no additional configuration is required.

If you have changed your key configuration previously, you can revert to using **Microsoft Software Key Storage Provider** with the following commands:

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

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

You can use `Reset-FasKeyConfig` to revert to **Microsoft Software Key Storage Provider** and additionally restore all the other key configuration settings to the defaults.

Example 2 - Store the authorization certificate key in a TPM

This example illustrates storing the FAS authorization certificate key in a TPM (real or virtual), while the user certificate keys are stored in the **Microsoft Software Key Storage Provider**.

Although FAS can generate user certificates with TPM protected keys, the TPM hardware may be too slow or size constrained for large deployments.

Use the following PowerShell commands:

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

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

Example 3 - Store all keys in an HSM

This example illustrates using an HSM to store both authorization certificate and user certificate private keys. This example assumes a configured HSM. Your HSM will have a provider name. For example, **HSM Vendor Key Storage Provider**.

Use the following PowerShell commands (replace the example text with the actual name of your HSM's Provider):

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

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

Example 4 - Use Elliptic Curve keys

By default, FAS generates RSA keys. In this example, Elliptic curve (ECC) keys are configured for both the authorization certificate and user certificates.

The example uses different key lengths. The authorization certificate is configured with a 384-bit key, and user certificates are configured with a 256-bit key.

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

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

At this point, authorization and user certificate requests may be rejected by the CA because the minimum key size in the FAS certificate templates is set to 1024 bits by default.

Therefore, for this example, it's necessary to change the minimum key size in the templates as follows:

- `Citrix_RegistrationAuthority_ManualAuthorization` and `Citrix_RegistrationAuthority`: Change the minimum key size to 384 (or smaller)
- `Citrix_SmartcardLogon`: Change the minimum key size to 256 (or smaller)

To edit the templates, run `mmc.exe`, and add the **Certificate Templates** snap-in. Locate the template, and open its properties. The minimum key size setting is located in the **Cryptography** tab of the template's properties.

> **Note:**
>
> User certificates with ECC keys are only supported on Windows VDAs running Citrix Virtual Apps and Desktops 2411 or later. ECC keys are not supported on Linux VDAs.

Testing the private key configuration

Although the `Set-FasKeyConfig` command does some validation, it's still possible to set an invalid key configuration. For example, you may make a mistake in the Provider name of your HSM, or the key length you specify may not be supported by your hardware.

The command `Test-FasKeyConfig` can help. It attempts to create a keypair using the current key configuration, and reports **success** or **failure**. If a failure occurs, an indication of the failure reason is provided. If successful, the keypair is immediately destroyed.

The following PowerShell commands test the authorization and user key configuration respectively:

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

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

Once you've authorized your FAS server and created a rule, you can additionally make a test CSR for a user certificate as follows:

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

Replace <mailto:user@example.com/> with a real UPN from your Active Directory deployment. The FAS rule is normally named **default**. But, if you prefer to test another rule that you have configured, specify that name instead.

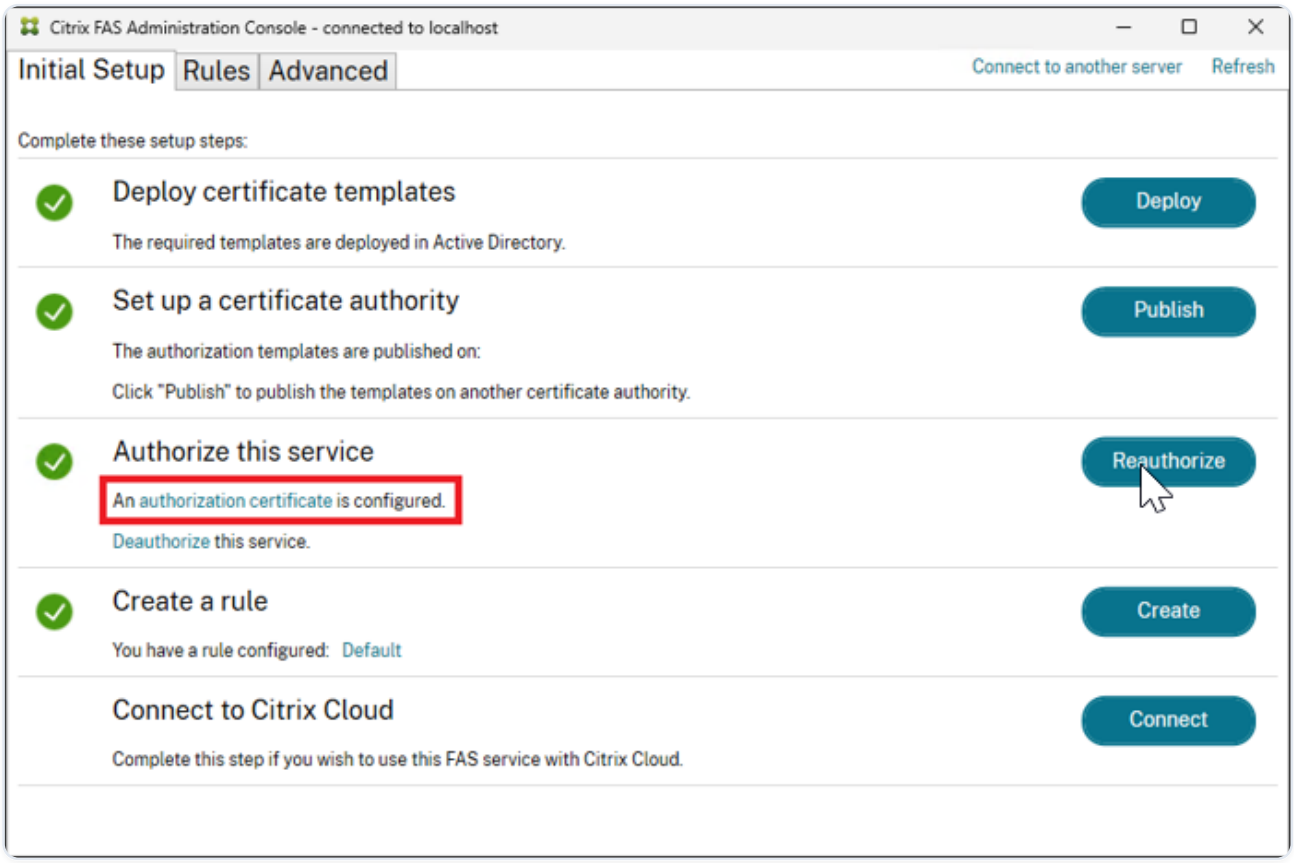
If the CSR succeeds, FAS discards the resulting certificate.

Inspecting FAS certificates

You can use PowerShell to inspect a certificate's properties and determine where the associated private key is stored.

Inspecting the authorization certificate

You can see the authorization certificate by clicking the **authorization certificate** link in the FAS administration console:



However, for more detailed information use PowerShell:

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

Several fields are returned, including **PrivateKeyProvider**, which contains an indication of the provider where the certificate was created and stored.

PRIVATEKEYPROVIDER	WHERE THE KEY IS STORED
Microsoft Software Key Storage Provider	The key is stored on-disk, protected by Microsoft's software provider.
Microsoft Platform Crypto Provider	The key is stored in a TPM (real or virtual).
HSM Vendor Key Storage Provider (example only)	The key is stored in an HSM (in this example, the vendor's provider is named **HSM Vendor Key Storage Provider**)

Inspecting user certifcates

You can get a list of all user certificates cached on the FAS server as follows:

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

The *KeyInfo* parameter causes the output to contain further information about the private key associated with the certificate. In particular, the **PrivateKeyProvider** field indicates where the keypair associated with the certificate is stored (see the previous section for interpreting this value).

You can filter the set of certificates returned using various optional parameters, such as `-UserPrincipalName`.

The certificate field of the command output is a PEM encoded user certificate. Copy the text to a `.crt` file to display the certificate using the Windows certificate GUI as follows:

COMMAND	DESCRIPTION
`$CertInfos = Get-FasUserCertificate -Address localhost`	There may be multiple user certificates in this list
`$CertInfo = $CertInfos[0]`	In this example, we select the very first user certificate
`$CertInfo.Certificate > c:\temp\user.crt`	Pipe the PEM data to a `.crt` file
`c:\temp\user.crt`	Open the `.crt` file in the Windows **GUI**

Upgrading from versions of FAS before Citrix Virtual Apps and Desktops 2411

In FAS releases before Citrix Virtual Apps and Desktops 2411, private key properties were configured by editing the XML file at

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

This has been superseded by the PowerShell commands described in this document, which provide more flexibility and can be applied without restarting the FAS server.

Additionally, unlike the XML file settings, configuration done using PowerShell is retained when the FAS server is upgraded.

The XML file settings relevant to private key configuration are listed as follows, with their corresponding PowerShell parameters (as used in `Get-FasKeyConfig` and `Set-FasKeyConfig`):

XML FILE SETTING	DEFAULT VALUE IN XML FILE	POWERSHELL EQUIVALENT	COMMENT
`Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.KeyLength`	2048	-Length	-
`Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.KeyProtection`	GenerateNonExportableKey	`-Exportable` `-UseDefaultTpmProvider`	• NoProtection is achieved by setting `-Exportable` to `$true` `-GenerateNonExportableKey`

XML FILE SETTING	DEFAULT VALUE IN XML FILE	POWERSHELL EQUIVALENT	COMMENT	
			is achieved by setting `-Exportable` to `$false` `-GenerateTPMProtectedKey` is achieved by specifying the `-UseDefaultTpmProvider` switch	
`Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderLegacyCsp`	false	-Ksp	`-ProviderLegacyCsp` false is achieved by setting `-Ksp` to `$true` `-ProviderLegacyCsp` true is achieved by setting `-Ksp` to `$false`	
`Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameter`	-	-Provider	-	

XML FILE SETTING	DEFAULT VALUE IN XML FILE	POWERSHELL EQUIVALENT	COMMENT
`s.ProviderName`			
`Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderType`	-	-CspType	-

The XML configuration defaults and the PowerShell defaults are functionally equivalent. That is, by default, properties of keypairs generated by FAS in this version and in versions before Citrix Virtual Apps and Desktops 2411 are the same.

Therefore, if you have not changed any of the preceding settings in the XML configuration file, you need not take any action when upgrading FAS.

However, if you have changed any of the preceding settings, upgrade FAS as follows:

- Place FAS into maintenance mode; Maintenance mode.
- Upgrade FAS **in place** simply by running the FAS installer; once upgrade, all previous settings will not be present in the XML file, and they cannot be configured in the XML file.
- Use the PowerShell command `Set-FasKeyConfig`, as described in Key configuration PowerShell commands, to set the FAS private key configuration as desired; consider the settings you need for your authorization and user certificates.
- Test your configuration, as described in Testing the private key configuration
- Take the FAS server out of maintenance mode

Next time you upgrade, the FAS private key configuration settings is retained, and there is no need to take any special action.

Cryptographic remoting

Private keys associated with FAS user certificates are never transfered to the VDA. Instead, when the VDA needs to use a user's FAS certificate, either for signing in to the VDA, or for in-session

use, the cryptographic request is remoted back to the FAS server. This improves security, because the private keys never leave FAS key storage (whether they are software storage, TPM, or HSM).

On Windows VDAs, this is achieved by using a pair of providers on the VDA. The application or operating system code making the cryptographic request is unaware that the operation is being remoted back to the FAS server.

Before Citrix Virtual Apps and Desktops 2411, the providers were **Cryptographic Service Providers** (CSPs) where applications and operating system code access was through the older Windows CAPI API. The providers were:

- `CitrixLogonCsp.dll`: for single sign-on to the VDA
- `CitrixVirtualSmartcardCsp.dll`: for in-session certificates

From Citrix Virtual Apps and Desktops 2411 onwards, additional Key Storage Providers (KSPs) are supplied on the VDA. Applications and operation system code access these with the newer Windows CNG API. The new providers are:

- `CitrixLogonKsp.dll`: for single sign-on to the VDA
- `CitrixVirtualSmartcardKsp.dll`: for in-session certificates

KSP is a more up-to-date way of exposing cryptographic operations to Windows applications, which provides more capabilities. For example:

- Certificates with ECC keys are supported
- Probabilistic Signature Scheme (PSS) padding is supported

KSP remoting is used (that is, remoting through the new KSPs) if both FAS and the VDA are running Citrix Virtual Apps and Desktops 2411 or later. Otherwise, the system falls back to use the older CSPs for remoting.

Disabling KSP remoting

In case of any compatibility issues, it's possible to disable KSP remoting so that the older CSP remoting can always be used.

Use the following PowerShell:

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

Maintenance mode

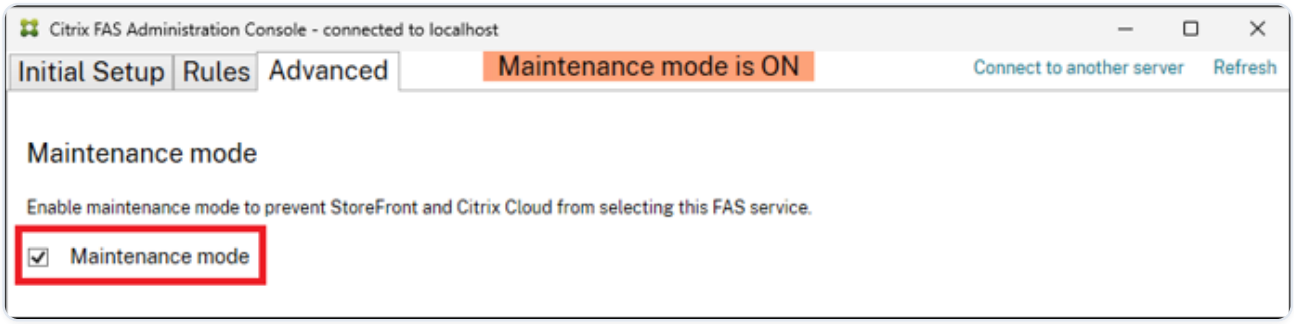
When performing changes to the configuration of a *live* FAS server, consider putting it in maintenance mode.

When FAS is in maintenance mode, the following holds true:

- When **Workspace** or **StoreFront™** call FAS as part of the published application or desktop launch sequence, FAS indicates that it is in maintenance mode; the caller must react to this by choosing a different FAS server.
- As an extra precaution, FAS does not allow automatic creation of user certificates when in maintenance mode. Thus inadvertent creation of user certificates with unintended settings is avoided.
- However, activities involving existing user certificates, such as VDA sign-in or in-session usage, are still permitted.

Although automatic user certificate creation is not allowed, administrators can still create user certificates using PowerShell commands such as `New-FasUserCertificate` or `Test-FasCertificateSigningRequest`.

Using the administration console



Using PowerShell

Place a FAS server into maintenance mode as follows:

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

Take a FAS server out of maintenance mode (and back into normal operation) as follows:

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

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

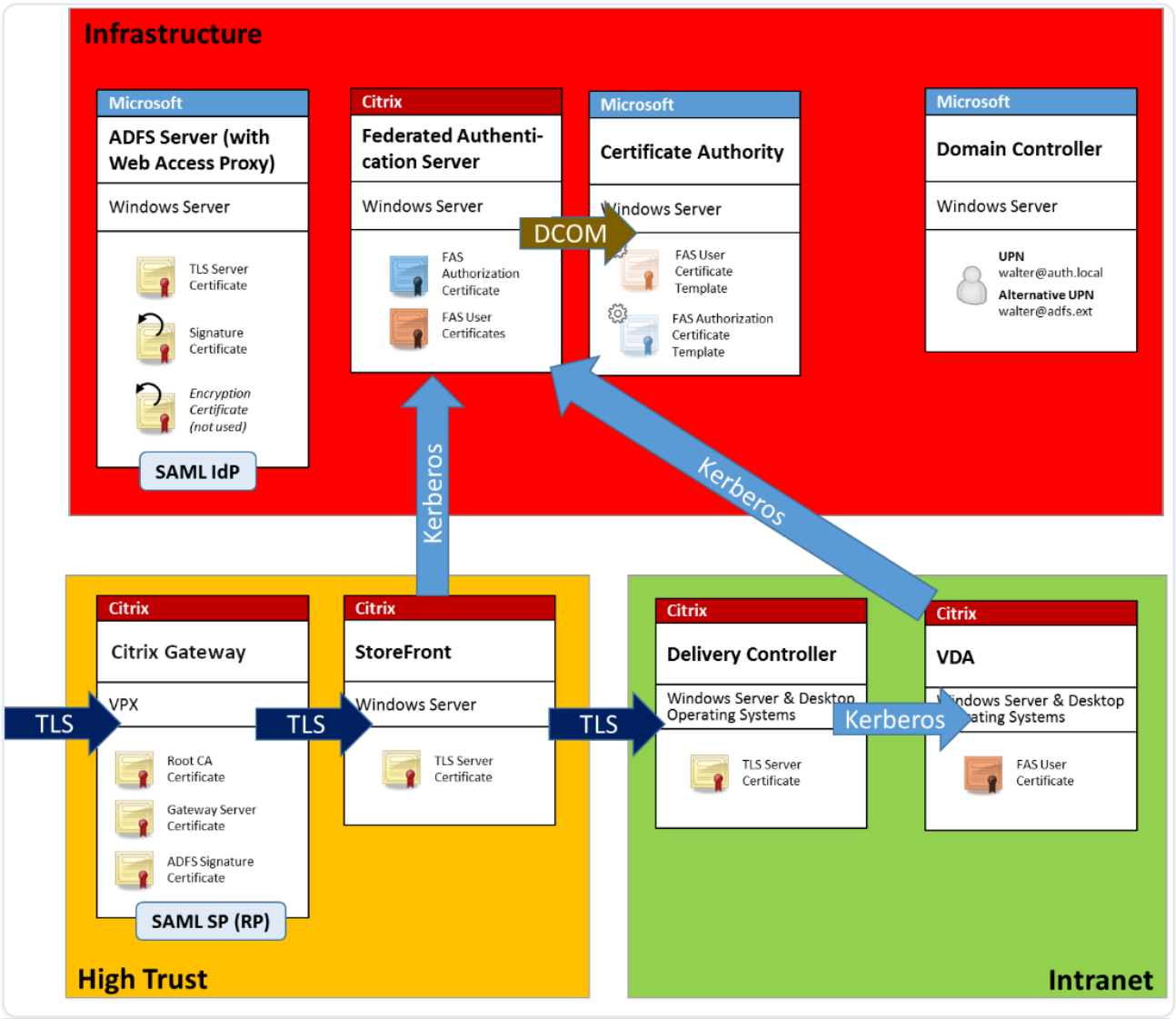
Federated Authentication Service (FAS) is tightly integrated with Microsoft Active Directory and the Microsoft certification authority. Ensure that the system is managed and secured appropriately, developing a security policy as you would for a domain controller or other critical infrastructure.

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

Network architecture and security

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

The FAS server is 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 perform user authentication. Other Citrix Virtual Apps and Desktops™ components are unaffected by introducing FAS.



SERVER	CONNECTIONS
Federated Authentication Service	[in] HTTP with Kerberos security 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] HTTP with kerberos security to FAS
Delivery Controller	[in] HTTPS from StoreFront server, [in/out] HTTP with kerberos security from VDAs

FEDERATED AUTHENTICATION SERVICE

SERVER	CONNECTIONS
VDA	[in/out] HTTP with Kerberos security from Delivery Controller, [in] HDX from Citrix Gateway, [out] HTTP with Kerberos security to FAS
Microsoft certificate authority	[in] DCOM from FAS

Communication between StoreFront and FAS

- When launching a VDA, the StoreFront server contacts the FAS server to get a single-use ticket which is needed by the Citrix Virtual Delivery Agent (VDA) to sign in the user.
- StoreFront connects to FAS using SOAP over HTTP. By default it uses port 80.
- It authenticates using mutual Kerberos with the Kerberos HOST/fqdn identity of the FAS server, and the Kerberos machine account identity of the StoreFront server.
- Data is encrypted by using message level security. No additional configuration is required to enable encryption.

Communication between VDA and FAS

When an HDX™ session is connected to the VDA, the VDA contacts the FAS server to request a certificate.

- The VDA connects to the FAS server using SOAP over HTTP. By default it uses port 80.
- It authenticates using mutual Kerberos with the Kerberos HOST/fqdn identity of the FAS server, and the Kerberos machine identity of the VDA. Also, the VDA must supply the "credential handle" to access the certificate and private key.
- Data is encrypted by using message level security. No additional configuration is required to enable encryption.

Communication between FAS and Microsoft certificate authority

When a user launches a VDA, if the FAS server does not already have a certificate for the user, then it communicates with the certificate authority to request a certificate. The certificate authority requires the FAS server to supply a CMC packet signed by a trusted enrollment agent certificate.

- The FAS server communicates with the Microsoft certificate authority using DCOM. For information on required ports, see Microsoft documentation.
- It authenticates using Kerberos.

Connections between Citrix Federated Authentication Service and Citrix Cloud™

If you are connecting FAS to Citrix Cloud, then your FAS servers must be able to access the following addresses over HTTPS port 443.

Citrix Cloud:

- FAS administration console that runs under the user's account
  - `*.cloud.com`
  - `*.citrixworkspacesapi.net`
  - Addresses required by a third-party identity provider, if one is used in your environment
- FAS service that runs under the Network Service account:
  - `*.citrixworkspacesapi.net`
  - `*.citrixnetworkapi.net`

Citrix Cloud Japan:

- FAS administration console, under the user’s account
  - `*.citrixcloud.jp`
  - `*.citrixworkspacesapi.jp`
  - Addresses required by a third party identity provider, if one is used in your environment
- FAS service, under the Network Service account:
  - `*.citrixworkspacesapi.jp`
  - `*.citrixnetworkapi.jp`

If your environment includes proxy servers, configure the user proxy with the addresses for the FAS administration console. Also, ensure that the address for the Network Service account is configured using netsh or a similar tool.

Further information

For information on securing communication between other Citrix components, see the following articles:

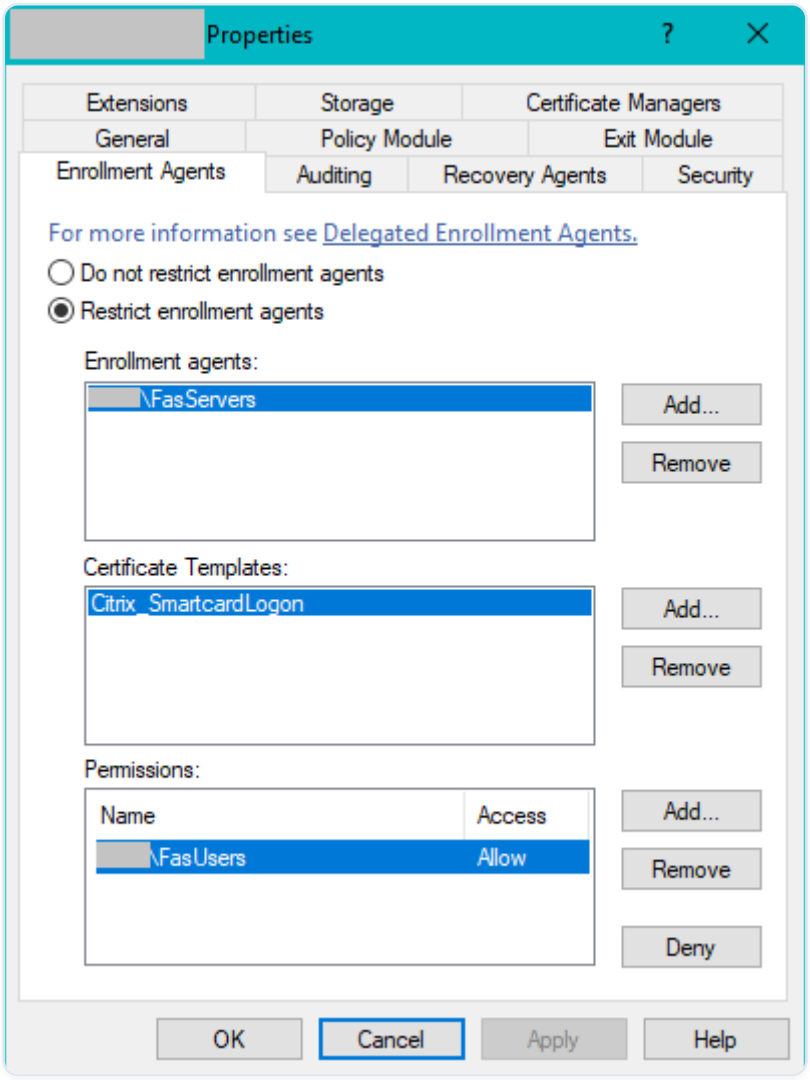
- Citrix Virtual Apps and Desktops - Security considerations and best practices.
- Secure your StoreFront deployment.

Security considerations

FAS has a registration authority certificate that allows it to issue certificates autonomously for your domain users. It helps in developing and implementing 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 for whom the enrollment agents can issue certificates for.



You can use the given dialog to ensure that:

- The *Enrollment agents* list contains only FAS servers (assuming that there are no other enrollment agents required in your Active Directory deployment).
- The *Certificate Templates* list contains only the FAS templates used to issue user certificates. By default this is the `Citrix_SmartcardLogon` template.

- The *Permissions* list contains users who are permitted to use FAS. For example, it is recommended not to issue certificates to Administrators or Protected Users group.

> **Note:**
>
> Any changes to the Active Directory group membership of a computer account do not take effect until the computer is rebooted.

Access Control List configuration

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

Firewall settings

The FAS server must accept incoming connections from StoreFront and VDAs, using port 80 unless otherwise configured. For more information on network communication, see Network architecture and security.

The FAS installer can optionally configure the Windows firewall. For more information, see FAS installer options.

Change FAS server port

The FAS server uses port 80 by default. You can customize the port:

> **Note:**
>
> You can change the FAS server port to port 443, but it doesn't change the protocol used by FAS. FAS doesn't use HTTPS even if configured on port 443.

1. Run the following command line on your FAS server:

```
"C:\Program Files\Citrix\Federated Authentication
Service\Citrix.Authentication.FederatedAuthenticationService.exe" /
SVCPORT [port] /CONFIGUREFIREWALL
```

Replacing `[port]` with the port number you wish to use.

The `/CONFIGUREFIREWALL` switch causes it to update the Windows firewall to allow incoming connections on the specified port.

2. Restart the FAS service.
3. In your FAS group policy object, update the list of FAS servers to include the port (e.g. `fas.example.com:[port]`).
4. Propagate the change to the FAS server, StoreFront and the VDA (e.g. using `gpupdate /force`)

Event log monitoring

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

Hardware security modules

All private keys, including user certificate keys 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 using the **PowerShell** commands. Different settings can be used for FAS authorization certificate private keys and user certificate keys. For more details, see Private key protection

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

NAME	RESPONSIBILITY
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

> **Note:**
>
> If all your FAS servers and VDAs are version 2511 or later, the Group Policy FQDN list on the VDA is no longer needed. See FAS V2 ticketing and the registry address list.

> 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 can contact different FAS servers. Additionally, if the FAS server is connected to Citrix Cloud, the Group Policy must also be applied to the FAS server itself.

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

Control of this GPO must 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.

FAS Group Policy settings appear in the registry at `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\Authentication`. The list of FAS FQDNs from the Group Policy appears at the subkey `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\Authentication\UserCredentialService\Addresses`

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

By default, the lifespan of a user certificate is seven days. 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.

See Private key protection for the settings that FAS provides.

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 can cause security issues, or result in unusable certificates.

Modify Security properties

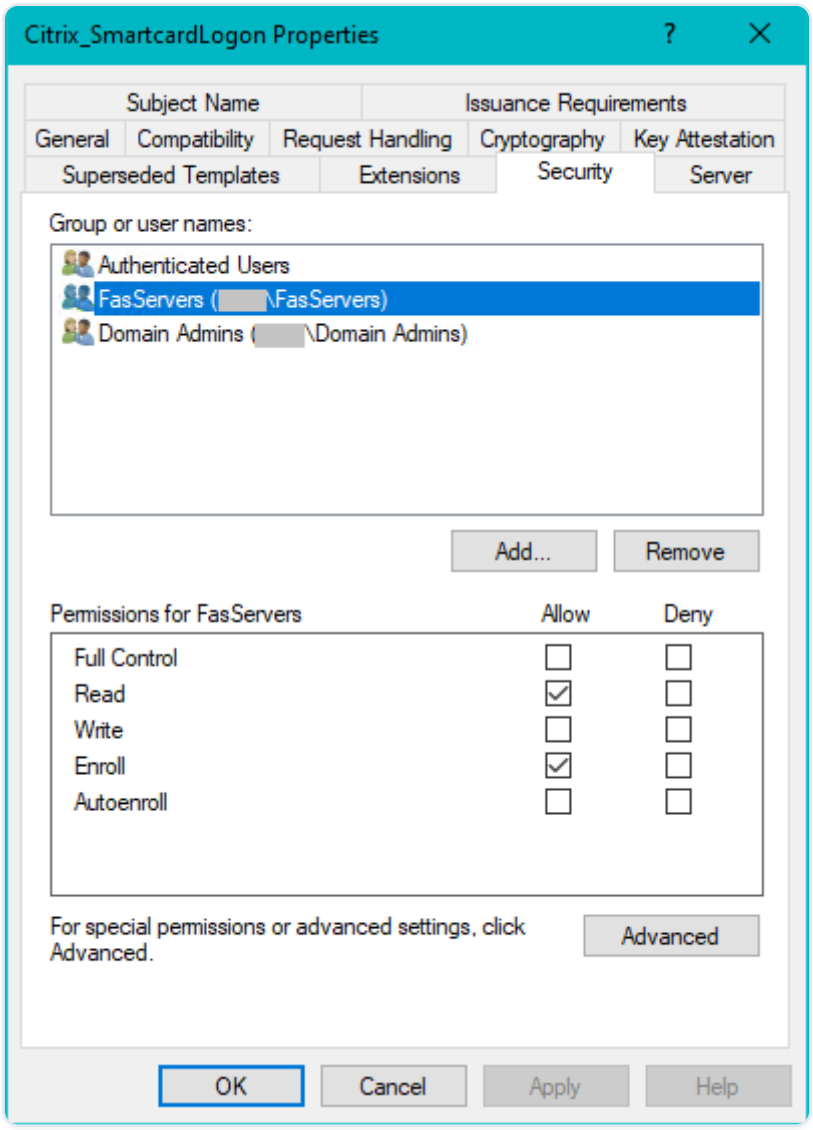
Citrix recommends that you modify these settings to allow the **Read** and **Enroll** permissions for only the machine accounts of the FAS servers. The FAS service does not require any other permissions.

Additionally:

- allow **Authenticated Users** to **Read** the template. This is necessary, because the Certificate Authorities themselves need to be able to read the template.
- allow your Certificate Authority administrators to **Read** and **Write** the template.

The recommendation applies to all three FAS templates:

- `Citrix_SmartcardLogon`
- `Citrix_RegistrationAuthority`
- `Citrix_RegistrationAuthority_ManualAuthorization`



Note:

Any changes to the Active Directory group membership of a computer account do not take effect until the computer is rebooted.

Modify Subject Name properties

Citrix recommends that you don't modify these properties.

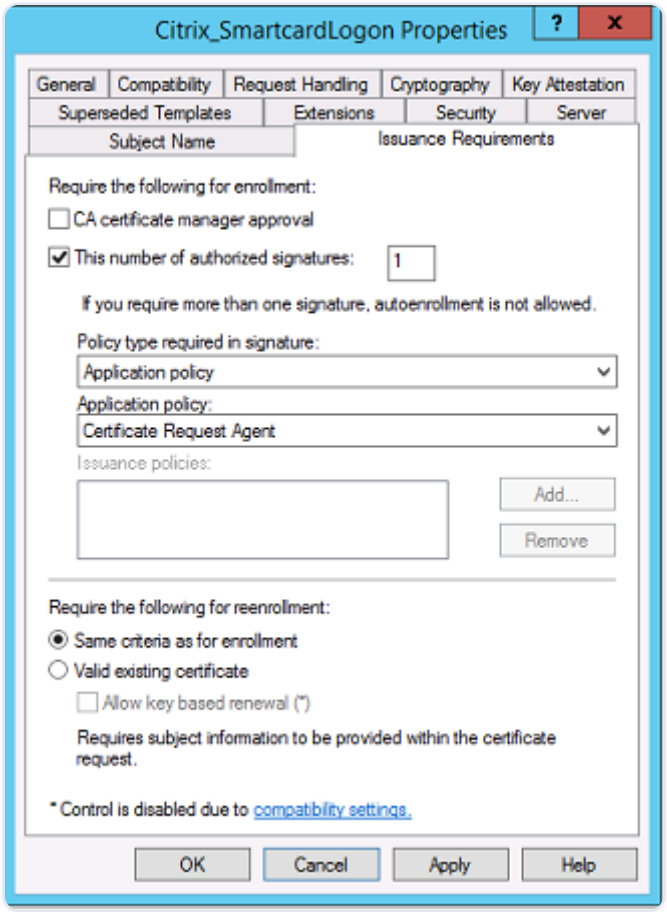
The template has *Build from this Active Directory information* selected, causing the certificate authority to include the user's SID in a certificate extension, which provides a strong mapping to the user's Active Directory account.

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 must 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 must maintain complete control over authorizing registration authority certificate requests, and have a policy for authorizing FAS servers.

Firewall settings

The certificate authority administrator has the 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 a registration authority certificate can issue certificates to any user, using any certificate template that allows access. Citrix recommends that issuance of certificates is restricted to a group of non-privileged users using the **Restrict enrollment agents** certificate authority property. See Delegated enrollment agents.

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

ACCESS VECTOR	DESCRIPTION
	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 option 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 must 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 Kerberos access control lists (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 can choose to use less or more powerful certificates, depending on the environment. For example, users identified as "external" can 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, a user can have only "signing" certificates available in-session, with the more powerful "logon" certificate 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 FAS authorization certificate private key is protected by storing it in a TPM.

Similarly, user certificate private keys can be stored in a TPM or HSM. All keys must be generated as *non-exportable* and be at least 2048 bits in length if RSA is used.

> **Note:**
>
> Although FAS can generate and store user certificate keys in a TPM or HSM, the hardware may be too slow or size constained for large deployments.

> For more details, see Private key protection.

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. FAS configuration must be properly maintained.

Citrix Virtual Apps, Citrix Virtual Desktops, and VDA administrators

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 must contain only trusted users. Auditing and event logs must be maintained.

General Windows server security

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

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

RDP access must be limited to authorized administrators. Citrix recommends smart card logon for user accounts, especially for certificate authority and domain administrator accounts.

Federal Information Processing Standard (FIPS) support

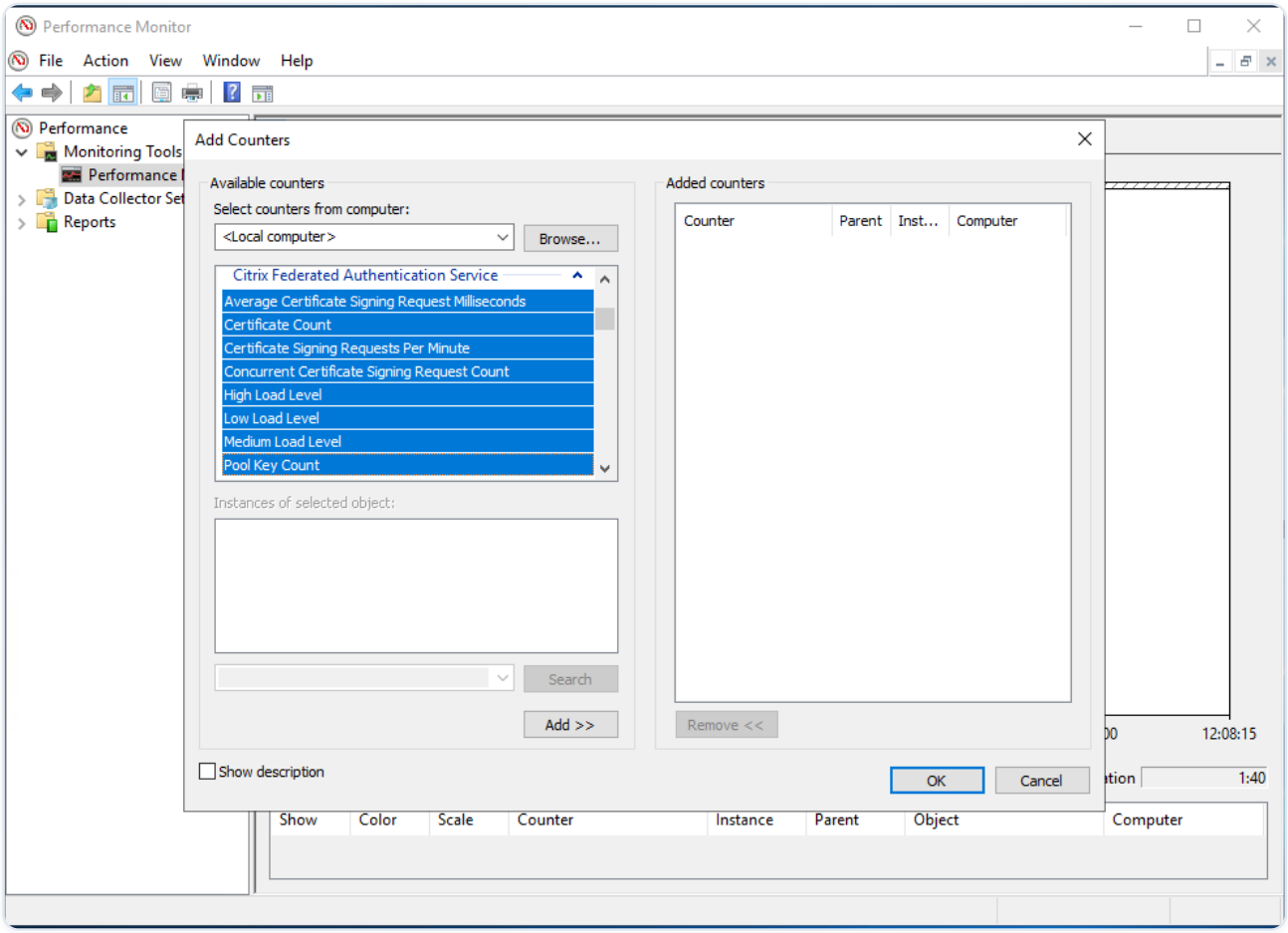
FAS uses the FIPS-validated cryptographic algorithms on FIPS-enabled Windows computers. If you configure FAS to use a TPM or HSM for key storage, consult your hardware vendor for FIPS compliance information.

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.

Performance counters

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



The following table lists the available counters. Unless otherwise stated, each counter is updated every 10 seconds.

FEDERATED AUTHENTICATION SERVICE

NAME	DESCRIPTION
Average Certificate Signing Request Milliseconds	The average duration (in milliseconds) of certificate signing requests, calculated using data from the previous minute.
Certificate Count	The number of certificates being managed by the Federated Authentication Service.
Certificate Signing Requests Per Minute	The number of certificate signing requests issued by the Federated Authentication Service per minute, calculated using data from the previous minute.
Concurrent Certificate Signing Request Count	The number of concurrent certificate signing requests being serviced by the Federated Authentication Service.
Pool Key Count	The number of pre-generated key pairs in the key pool that can be used for certificate signing requests.
Private Key Operations Per Minute	The number of certificate private key operations being performed by the Federated Authentication Service per minute, calculated using data from the previous minute.
Session Count	The number of VDA sessions being tracked by the Federated Authentication Service.
Low/Medium/High Load Level	Estimates of the load that the Federated Authentication Service can accept in terms of certificate signing requests per minute. The estimates are updated every minute, using data from the previous minute. Exceeding the “High Load” threshold may result in published app or desktop launches failing.

Troubleshoot Windows Logon issues

This article describes the logs and error messages Windows provides when a user logs on using certificates or smart cards, or both. These logs provide information that 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).
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's ambiguous, this

REGISTRY POLICY	DESCRIPTION
	option allows users to manually specify their Windows Logon account.
UseCachedCRLOnlyAnd, IgnoreRevocationUnknownErrors	Disables revocation checking (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 the Active Directory has an implicit UPN based on the pattern \<samUsername>@\<domainNetBios> and \<samUsername>@\<domainFQDN>. The available domains and FQDNs are included in the **RootDSE** entry for the forest. A single domain can have multiple FQDN addresses registered in the RootDSE.

Also, every user in the 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 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 log on 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**. This configuration must be reverted when debugging is complete.

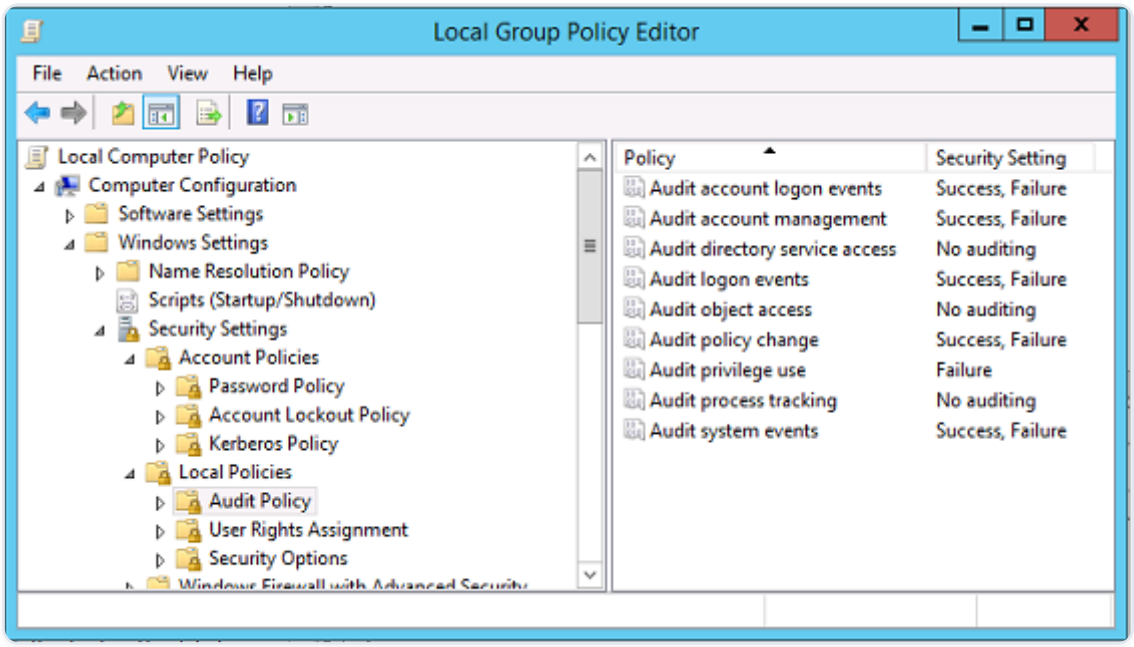
Identify the domain controller in use

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. To open the Group Policy editor, run `gpedit.msc` on the Domain Controller. After the audit policies are enabled, the domain controller produces extra event log information in the security log.



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.

On the domain controller and VDA machine, open the event viewer and navigate to **Applications and Services Logs** > **Microsoft** > **Windows** > **CAPI2** > **Operational**. Right-click **Operational** and select **Enable Log**.

Additionally, fine-tune the CAPI logging with the registry values at: *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\crypt32*. The following values don't exist by default. You have to create them. Delete the values if you want to revert to the default CAPI2 logging settings.

VALUE	DESCRIPTION
DiagLevel (DWORD)	Verbosity level (0 to 5)
DiagMatchAnyMask (QUADWORD)	Event filter (use 0xffffff for all)

VALUE	DESCRIPTION
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 the 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\Kerberos\Parameters	LogLevel	0x1
CurrentControlSet\Control\Lsa\Kerberos\Parameters	KerbDebuglevel	0xffffffff
CurrentControlSet\Services\Kdc	KdcDebugLevel	0x1
CurrentControlSet\Services\Kdc	KdcExtraLogLevel	0x1f

Kerberos logging is output to the System event log.

- Messages such as **untrusted certificate** must 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

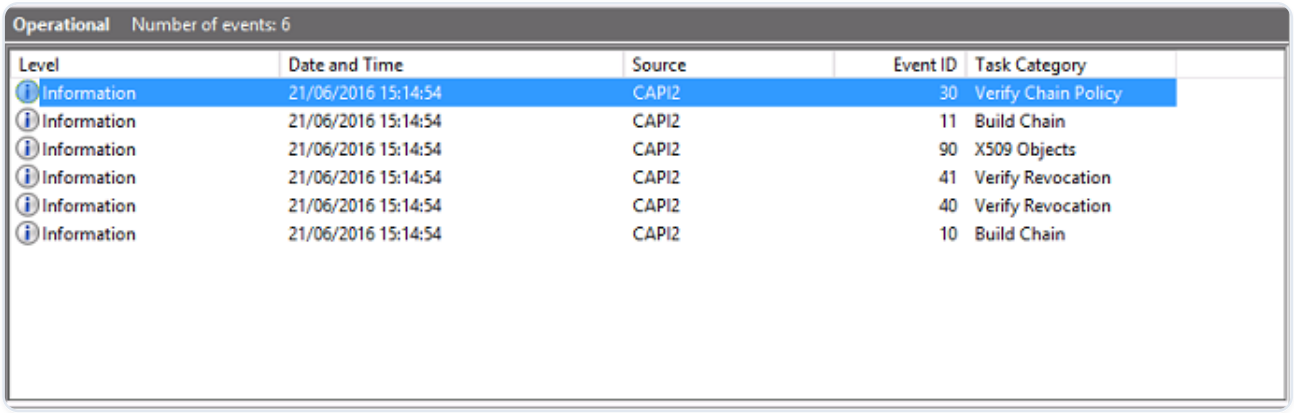
Domain controller and workstation logs

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.



Operational Number of events: 6

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

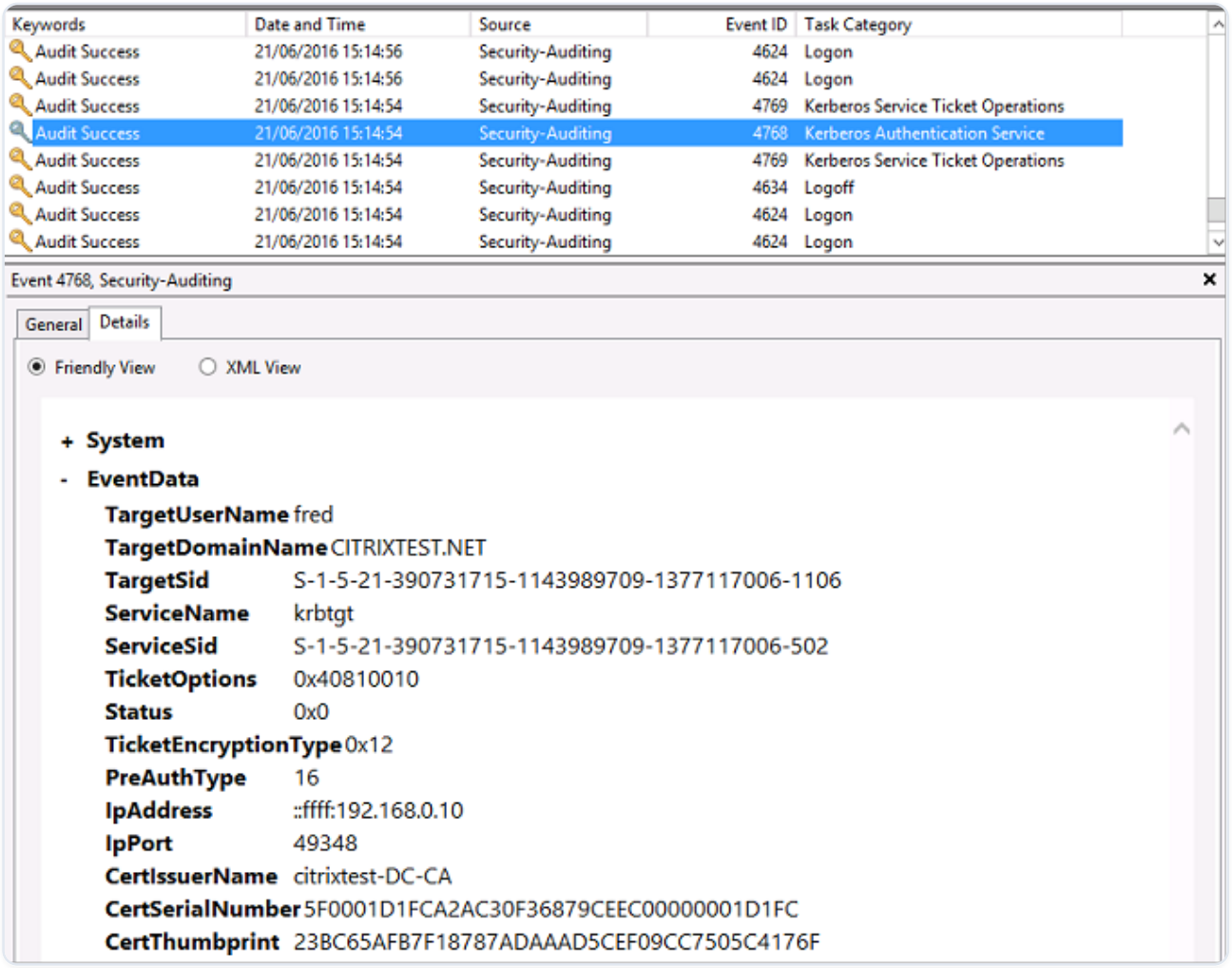
The final event log message shows lsass.exe on the domain controller constructing a chain based on the certificate provided by the VDA, and verifying it for validity (including revocation). The result is returned as "ERROR_SUCCESS".

- **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

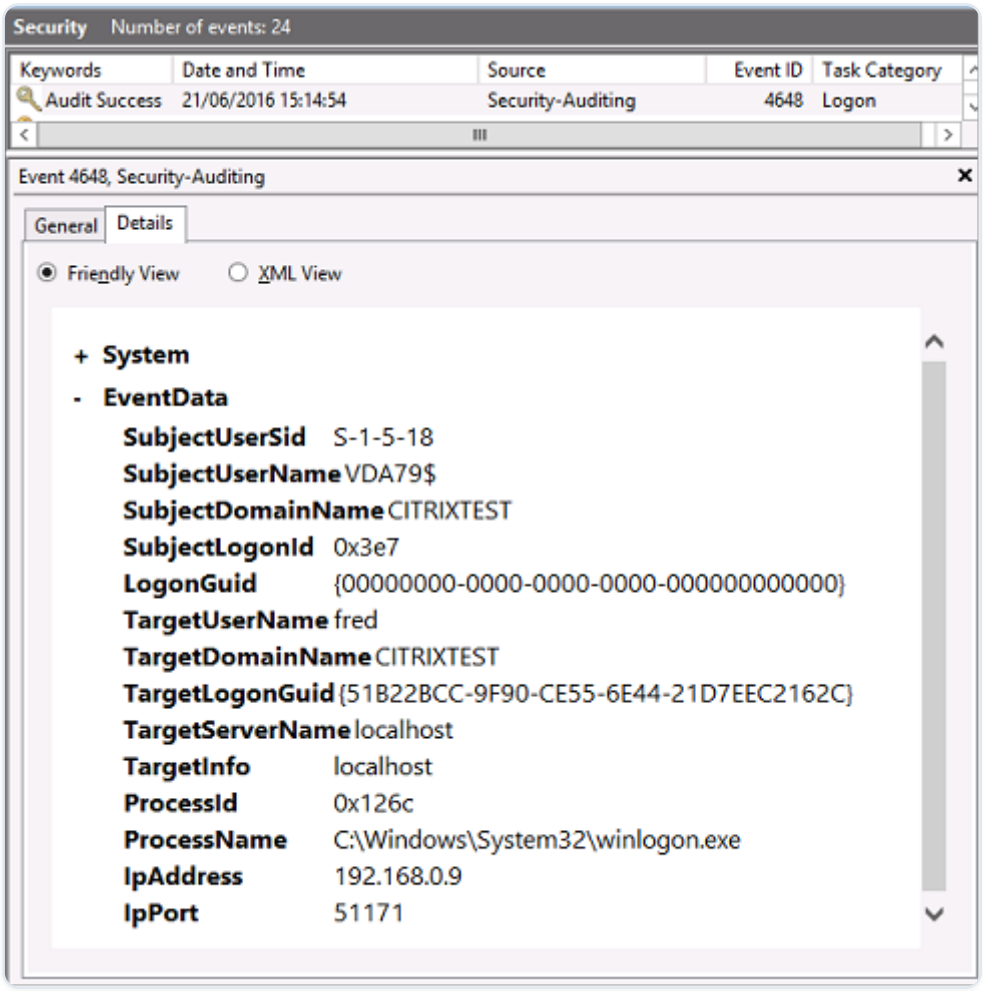
The domain controller shows a sequence of logon events, the key event being 4768, where the certificate is used to issue the Kerberos Ticket Granting Ticket (krbtgt).

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.



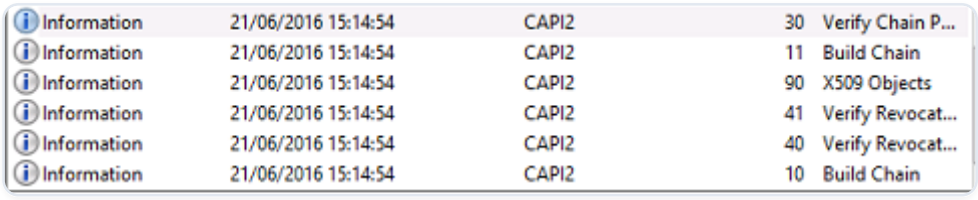
VDA security log

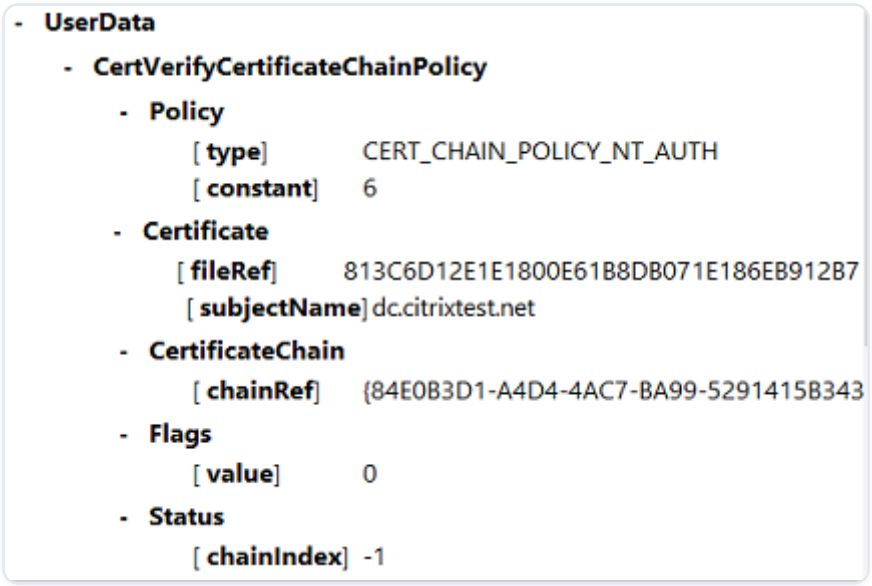
The VDA security audit logs corresponding to the logon event is the entry with event ID 4648, originating from winlogon.exe.



VDA CAPI log

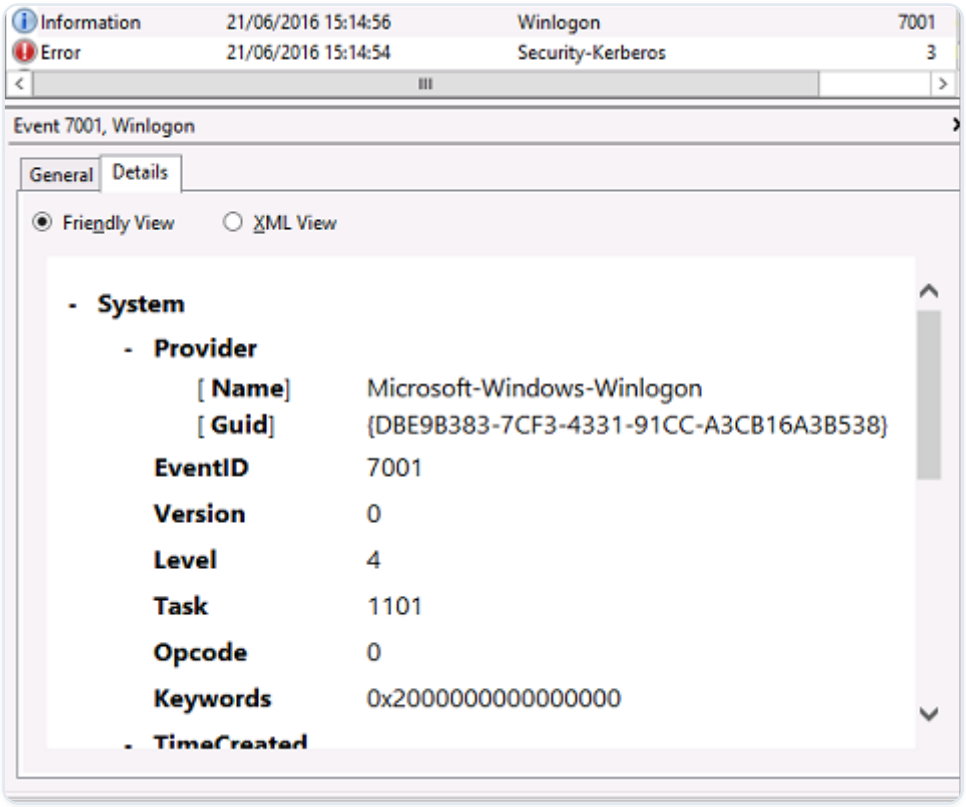
This example VDA CAPI log shows a single chain build and verification sequence from lsass.exe, validating the domain controller certificate (dc.citrixtest.net).





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 Windows Logon showing that the Kerberos logon was successful.



Monitoring FAS using Windows event log

All FAS events are written to the Windows **Application event log**. You can use products such as System Center Operations Manager (SCOM) to monitor the health of your FAS service using the processes and events described here.

Is the FAS service running?

To determine if the FAS service is running, monitor the process Citrix.Authentication.FederatedAuthenticationService.exe.

Only the most important events for monitoring the FAS service are described in this section. For the full list of FAS event codes, see FAS event logs.

FAS health events

The following events show whether your FAS service is healthy.

The event source is **Citrix.Authentication.FederatedAuthenticationService**.

EVENT	EVENT TEXT	EXPLANATION	NOTES
[S003]	Administrator [{0}] setting Maintenance Mode to [{1}]	The FAS service was put into, or taken out of, maintenance mode.	While in maintenance mode, the FAS server is not usable for single sign-on.
[S022]	Administrator [{0}] setting Maintenance Mode to Off	The FAS service was taken out of maintenance mode.	Available from FAS 10.7 / Citrix Virtual Apps and Desktops 2109.
[S023]	Administrator [{0}] setting Maintenance Mode to On	The FAS service was put into maintenance mode.	Available from FAS 10.7 / Citrix Virtual Apps and Desktops 2109.
[S123]	Failed to issue a certificate for at any CA for [upn: {0} role: {1}] [exception: {2}]	This event happens after [S124] if none of the CAs FAS is configured with successfully issued a user certificate. Single sign-on will fail for that user.	This event indicates that all configured CAs are not working. If FAS is configured to use an HSM, it may also indicate that the HSM is not working.
[S124]	Failed to issue a certificate for [upn: {0} role: {1}] at	A failure occurred when FAS attempted to request a user	This event may indicate that the CA is not working, or is

EVENT	EVENT TEXT	EXPLANATION	NOTES
	[certificate authority: {2}] [exception: {3}]	certificate from the given CA. If FAS is configured with more than one CA, FAS tries the request at another CA.	not contactable. If FAS is configured to use an HSM, it may also indicate that the HSM is not working. The exception can be used to help identify the cause of the problem.
[S413]	Authorization certificate expiring soon ({0} days left). Certificate details: {1}	This event is generated periodically when the FAS authorization certificate is close to expiry. By default, the event is generated every day if the authorization certificate is within 30 days of expiry.	The default settings can be adjusted using the cmdlet **Set-FasRaCertificateMonitor**; see PowerShell cmdlets.
[S414]	Authorization certificate has expired. Certificate details: {0}	This event is generated periodically when the FAS authorization certificate has expired. By default, the event is generated every day.	Once expired, FAS is not able to generate new user certificates and single-sign-on begins to fail.

Cloud-connected FAS events

If you are using FAS with Citrix Cloud™, the following events show whether your FAS service is healthy.

The event source is **Citrix.Fas.Cloud**.

EVENT	EVENT TEXT	EXPLANATION	NOTES
[S012]	The FAS service is available for single sign-on from Citrix Cloud	This event indicates that the single sign-on from Workspace (that is, Citrix Cloud) should be working.	Before issuing this event, FAS checks (1) that it is configured, (2) is not in maintenance mode, and (3) is connected to 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.	This event indicates that FAS is not able to provide a single sign-on from Workspace (that is, Citrix Cloud). The message includes the reason why the single sign-on is not working.	FAS maintains a persistent connection to Citrix Cloud. From time-to-time, this connection may terminate for various reasons (such as a network glitch, or a connection lifetime policy on a proxy server). When this happens, the event text contains "Service is not connected to the cloud". **This is normal behaviour, and FAS immediately attempts to re-establish a connection to Citrix Cloud**.

Security events

The following events indicate that an unauthorized entity attempted to use FAS.

The event source is **Citrix.Authentication.FederatedAuthenticationService**.

EVENT	EVENT TEXT	EXPLANATION
[S001]	ACCESS DENIED: User [{0}] is not a member of the Administrators group	An attempt was made to view or change te configuration of FAS, but the caller was not a FAS administrator.
[S002]	ACCESS DENIED: User [{0}] is not an Administrator of Role [{1}]	An attempt was made to view or change the configuration of a FAS rule, but the caller was not a FAS administrator.
[S101]	Server [{0}] is not authorized to assert identities in role [{1}]	An attempt was made to assert user identities, but the caller is not permitted to do so. Only StoreFront™ servers, which have been permitted in the FAS rule configuration (and Workspace if applicable) are allowed to assert user identities.
[S104]	Server [{0}] failed to assert UPN [{1}] (UPN not allowed by rule [{2}])	An attempt was made to assert a user identity, but the user's account is not permitted according to the FAS rule configuration.
[S205]	Relying party access denied - the calling account [{0}] is not a permitted relying party of the rule [{1}]	A VDA attempted to perform single sign-on with FAS, but the VDA is not permitted according to the FAS rule configuration.

FAS event logs

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

Administration events

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}] requesting authorization certificate from CA [{1}] using templates [{2} and {3}]
[S005] Administrator [{0}] removing FAS authorization [RA cert id: {1}]
[S006] Administrator [{0}] creating Certificate Definition [{1}]
[S007] Administrator [{0}] updating Certificate Definition [{1}]
[S008] Administrator [{0}] deleting Certificate Definition [{1}]
[S009] Administrator [{0}] creating Rule [{1}]
[S010] Administrator [{0}] updating Rule [{1}]
[S011] Administrator [{0}] deleting Rule [{1}]
[S012] Administrator [{0}] creating certificate [upn: {1} sid: {2} rule: {3}]Certificate Definition: {4} Security Context: {5}]
[S013] Administrator [{0}] deleting certificates [upn: {1} role: {2} Certificate Definition: {3} Security Context: {4}]
[S015] Administrator [{0}] creating certificate request [TPM: {1}]
[S016] Administrator [{0}] importing Authorization certificate [Reference: {1}]
[S022] Administrator [{0}] setting Maintenance Mode to Off
[S023] Administrator [{0}] setting Maintenance Mode to On
[S024] Administrator [{0}] setting system health monitor
[S025] Administrator [{0}] setting system health monitor
[S026] Administrator [{0}] setting RA Certificate Monitor

LOG CODES
[S027] Administrator [{0}] resetting RA certificate monitor
[S028] Administrator [{0}] setting key configuration for [{1}] certificate to [{2}]
[S029] Administrator [{0}] resetting key configuration for [{1}] certificate to default values [{2}]
[S030] Administrator [{0}] setting Service Properties to [{1}]
[S031] Administrator [{0}] de-authorizing CA [RA cert id: {1}]
[S050] Administrator [{0}] creating cloud configuration: [{1}]
[S051] Administrator [{0}] updating cloud configuration: [{1}]
[S052] Administrator [{0}] removing cloud configuration
[S060] Administrator [{0}] Requesting Cloud Registration. Instance: {1}
[S060] Administrator [{0}] Requesting Direct Trust Cloud Registration. Instance: {1} CloudServiceUrlFormat: {2}
[S061] Administrator [{0}] Completing Cloud Registration. Resource location: {1}, Rule name: {2}
[S062] Administrator [{0}] Completed Cloud Registration. Resource location: {1} ({2}), Rule name: {3}, Customer: {4} ({5})
[S063] A KRS error occurred during cloud registration. The exception was {0}
[S064] An unknown error occurred during cloud registration. The exception was {0}
[S065] Administrator [{0}] Requesting Direct Trust Cloud Registration. Instance: {1} CloudServiceUrlFormat: {2}

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

LOG CODES
[S405] An error occurred while migrating data from the registry to the database: [{0}]
[S406] Migration of data from registry to database is complete (note: user certificates are not migrated)
[S407] Registry-based data was not migrated to a database since a database already existed
[S408] Cannot downgrade the configuration -- [From version {0} to version {1}]
[S409] ThreadPool configuration succeeded - MinThreads adjusted from [workers: {0} completion: {1}] to: [workers: {2} completion: {3}]
[S410] ThreadPool configuration failed - failed to adjust MinThreads from [workers: {0} completion: {1}] to: [workers: {2} completion: {3}]; this may impact the scalability of the FAS server
[S411] Error starting the FAS service: [{0}]
[S412] Configuration upgrade complete -- [From version {0} to version {1}]
[S413] Authorization certificate expiring soon ({0} days left). Certificate details: {1}
[S414] Authorization certificate has expired. Certificate details: {0}
[S415] Authorization certificate checks completed. {0} issues were logged. Next check is due in {1}

Creating identity assertions

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 is not allowed by rule [{2}])
[S105] Server [{0}] issued identity assertion [upn: {1}, role {2}, Security Context: [{3}]]
[S120] Issuing certificate to [upn: {0} role: {1} Security Context: [{2}]]

LOG CODES
[S121] Certificate issued to [upn: {0} role: {1}] by [certificate authority: {2}]
[S122] Warning: Server is overloaded [upn: {0} role: {1}][Requests per minute {2}].
[S123] Failed to issue a certificate at any CA for [upn: {0} role: {1}] [exception: {2}]
[S124] Failed to issue a certificate for [upn: {0} role: {1}] at [certificate authority: {2}] [exception: {3}]
[S125] Call timed out after {0} seconds waiting for pending certificate request to complete [upn: {1} role: {2} Security Context: [{3}]]
[S126] Server [{0}] attempted to assert an identity using an undefined rule [{1}]
[S127] FAS could not request a certificate for [upn: {0} role: {1} definition: {2}] because the server is in maintenance mode; use PowerShell cmdlet Set-FasServer to change the behavior while in maintenance mode

Acting as a relying party

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 Provider
[S204] Relying party [{0}] accessing the Logon Provider for [upn: {1}] in role: [{2}] [Operation: {3}] as authorized by [{4}]
[S205] Relying party access denied - the calling account [{0}] is not a permitted relying party of the rule [{1}]
[S206] Calling account [{0}] is not a relying party
[S208] Private Key operation failed [Operation: {0} upn: {1} role: {2} certificateDefinition {3} Error {4} {5}].
[S209] Cached certificate not found. [Caller: {0}] [upn: {1}] [role: {2}] [cert definition: {3}] [Operation: {4}]

In-session certificate server

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}]
[S303] Access Denied: User [{0}] does not match Virtual Smart Card [upn: {1}]
[S304] User [{0}] running program [{1}] on computer [{2}] using Virtual Smart Card [upn: {3} role: {4} thumbprint: {5}] for private key operation [{6}]
[S305] Private Key operation failed [Operation: {0}] [upn: {1} role: {2} containerName {3} Error {4} {5}].

FAS assertion plug-in

These events are logged by the FAS assertion plug-in.

LOG CODES
[S500] No FAS assertion plug-in is configured
[S501] The configured FAS assertion plug-in could not be loaded [exception:{0}]
[S502] FAS assertion plug-in loaded [pluginId={0}] [assembly={1}] [location={2}]
[S503] Server [{0}] failed to assert UPN [{1}] (logon evidence was supplied but the plug-in [{2}] does not support it)
[S504] Server [{0}] failed to assert UPN [{1}] (logon evidence was supplied but there is no configured FAS plug-in)
[S505] Server [{0}] failed to assert UPN [{1}] (the plug-in [{2}] rejected the logon evidence with status [{3}] and message [{4}])
[S506] The plug-in [{0}] accepted logon evidence from server [{1}] for UPN [{2}] with message [{3}]
[S507] Server [{0}] failed to assert UPN [{1}] (the plug-in [{2}] threw exception [{3}] during method [{4}])

LOG CODES
[S507] Server [{0}] failed to assert UPN [{1}] (the plug-in [{2}] threw exception [{3}])
[S508] Server [{0}] failed to assert UPN [{1}] (access disposition was supplied but the plug-in [{2}] does not support it)
[S509] Server [{0}] failed to assert UPN [{1}] (access disposition was supplied but there is no configured FAS plug-in)
[S510] Server [{0}] failed to assert UPN [{1}] (the access disposition was considered invalid by plug-in [{2}]

Workspace-enabled FAS

These events are logged when FAS is used with Workspace.

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

LOG CODES
[S014] A call to the cloud service `<service name>` failed [fas id: {0}] [transaction id: {1}] [exception: {2}]
[S015] A message from Citrix Cloud was blocked because the caller is not permitted [message ID {0}] [transaction ID {1}] [caller {2}]
[S016] A call to the cloud service `<service name>` succeeded [fas id: {0}] [transaction id: {1}]
[S019] FAS downloaded its configuration from the cloud [fas id: {0}] [transaction id: {1}]
[S020] FAS failed to download its configuration from the cloud [fas id: {0}] [transaction id: {1}] [exception: {2}]
[S021] The cloud support module failed to start. Exception: {0}
[S022] The cloud support module is stopping
[S023] Failed to rotate Citrix Cloud authorization key [fas id: {0}] [current key id:{1}] [new key id:{2}] [keys in cloud:{3}]
[S024] Initiating rotation of Citrix Cloud authorization key [fas id: {0}] [current key id:{1}] [new key id: {2}]
[S025] This service's authorization key is present in the Citrix Cloud [current key: {0}] [keys in cloud: {1}]
[S026] This service's authorization key is not present in the Citrix Cloud [current key: {0}] [keys in cloud: {1}]
[S027] Upgraded the Citrix Cloud authorization key storage format [fas id: {0}]
[S028] FAS sent its current telemetry to the cloud [fas id: {0}] [transaction id: {1}]
[S029] FAS failed to send its current telemetry to the cloud [fas id: {0}] [transaction id: {1}] [exception: {2}]

Log on

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

LOG CODES
[S101] Identity Assertion Logon failed. Unrecognised Federated Authentication Service GPO index [index: {0}] [registry name: {1}]
[S102] Identity Assertion Logon failed. SID lookup failed for {0} [Exception: {1}{2}]
[S103] Identity Assertion Logon failed. User {0} has SID {1}, but the expected SID is {2}
[S104] Identity Assertion Logon failed. Call to {0} returned [Error: {1} {2}]
[S105] Identity Assertion Logon. Logging in [Username: {0} Domain: {1}]
[S106] Identity Assertion Logon.\n\nFederated Authentication Service: {0}\n\nLogging in [Certificate: {1}]
[S107] Identity Assertion Logon failed. [Exception: {0}{1}]
[S108] Identity Assertion Subsystem. ACCESS_DENIED [Caller: {0}]

In-session certificates

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

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}] [Reason: {1}]

LOG CODES
[S016] PrivateKey::Create [Identifier: {0}] [MachineWide: {1}] [Provider: {2}] [ProviderType: {3}] [EllipticCurve: {4}] [KeyLength: {5}] [isExportable: {6}] [CreateReason: {7}]
[S017] PrivateKey::Delete [Provider: {0}] [Identifier {1}] [Twin: {2}]
[S018] PrivateKey::Create failed [Identifier: {0}] [MachineWide: {1}] [Provider: {2}] [ProviderType: {3}] [EllipticCurve: {4}] [KeyLength: {5}] [isExportable: {6}] [CreateReason: {7}] [Exception: {8}]

LOG CODES
[S104] FAS received an authorization certificate from CA {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}]

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 user name 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 worth trying, even when the existing certificate appears to be valid.

ERROR MESSAGE DISPLAYED	DESCRIPTION AND REFERENCE
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).

FAS Always-on Tracing

With always-on tracing, FAS logs its activity to the filesystem. This can help with troubleshooting, potentially eliminating the need to reproduce an incident that has occurred.

Always-on tracing is enabled when you install or upgrade FAS using any of these methods:

- The Citrix Virtual Apps and Desktops™ installer: from the **Federated Authentication Service** button on the autorun splash screen when the ISO is inserted
- `XenDesktopFasSetup.exe`: Located on the Citrix Virtual Apps and Desktops ISO at `x64\XenDesktop Setup\XenDesktopFasSetup.exe`
- `FasSetup_xxxx.exe`: the stand-alone FAS installer file, available from Citrix Downloads.

> **Note:**
>
> Always-on tracing is not available if you install or upgrade using the **FAS installer MSI** file, `FederatedAuthenticationService_x64.msi`.

Collecting always-on tracing

Use Citrix Scout to collect always-on tracing and other diagnostic data from your FAS server. **Citrix Scout** is installed when you install FAS using any of the preceeding methods.

Disabling always-on tracing

If for any reason you wish to disable always-on tracing, stop and disable **Citrix Telemetry Service** on your FAS server.

Sending always-on tracing to a central logging server

For more information and configuration steps, see the Always-on tracing (AOT) article.

Related information

- ConfigurRun the following PowerShell command on the FAS server to configure FAS toing a domain for Smart Card Logon
- Smart Card Logon policies
- Enabling CAPI logging
- Enabling Kerberos logging
- Guidelines for enabling Smart Card Logon with third-party certification authorities

PowerShell cmdlets

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/>`.

FAS Installer Options

Command-line options for installing FAS

The following options are valid with both:

1. `XenDesktopFasSetup.exe` file located on the Citrix Virtual Apps and Desktops ISO at `x64\XenDesktop Setup\XenDesktopFasSetup.exe`
2. FasSetup_xxxx.exe, where xxxx is the release available from Citrix Downloads

    - `/configure_firewall`

Opens all ports in the Windows firewall used by the components being installed, if the Windows Firewall Service is running, even if the firewall is not enabled. If you are using a third-party firewall or no firewall, you must manually open the ports. FAS requires inbound TCP port 80.

- `/help or /h or /?`

  Displays command help.

- `/noreboot`

  Prevents a restart after installation.

- `/quiet` or `/passive`

  No user interface appears during the installation. The only evidence of the installation and configuration process is in Windows Task Manager. If this option is omitted, the graphical interface launches.

- `/remove`

  Removes FAS.

- `/installdir`

  Specifies the installation folder.

For information about how Citrix reports the result of component installations, see Citrix installation return codes.

Installing FAS on Windows Server Core

Citrix Virtual Apps and Desktops ISO or the stand-alone FAS installer exe (`FasSetup_xxxx.exe`) are the preferred ways to install FAS. However, depending on what OS features are enabled, you may not be able to use them to install on Windows Server Core.

Instead, use the following MSI files from the Citrix Virtual Apps and Desktops™ ISO:

MSI FILE	LOCATION ON ISO	COMMENT
`FederatedAuthenticationService_x64.msi`	`x64\Federated Authentication Service`	Required
`TelemetryServiceInstaller_x64.msi`	`x64\Virtual Desktop Components`	Recommended, provides support for Always-on Tracing

As a prerequisite, `.net4.8` must be installed.

To install or upgrade, use the following commands:

```
msiexec /i FederatedAuthenticationService_x64.msi [/quiet]
CONFIGUREFIREWALL=[YES|NO]

msiexec /i TelemetryServiceInstaller_x64.msi [/quiet]

net start "Citrix Telemetry Service"
```

The options are:

- `/quiet`: Does not display any user interface
- CONFIGUREFIREWALL: Specifies **YES** to configure the firewall to allow incoming connections on port 80. The default if this option is omitted is **NO**

To remove FAS, use the following commands:

```
msiexec /x FederatedAuthenticationService_x64.msi [/quiet]

msiexec /x TelemetryServiceInstaller_x64.msi [/quiet]
```

FAS Administration on Windows Server Core

You can configure and administer FAS locally or from another computer that has FAS installed using either:

- The FAS PowerShell cmdlets
- The FAS Administration Console GUI

When using PowerShell cmdlets, set the `-Address` parameter to the target FAS server's FQDN. Alternatively, you can set the variable `$CitrixFasAddress` to the FQDN. You can specify **localhost** if you want to administer the local FAS.

When using the FAS administration console, click the **Connect to another server** link in the top right-hand corner.

Deployment architectures

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

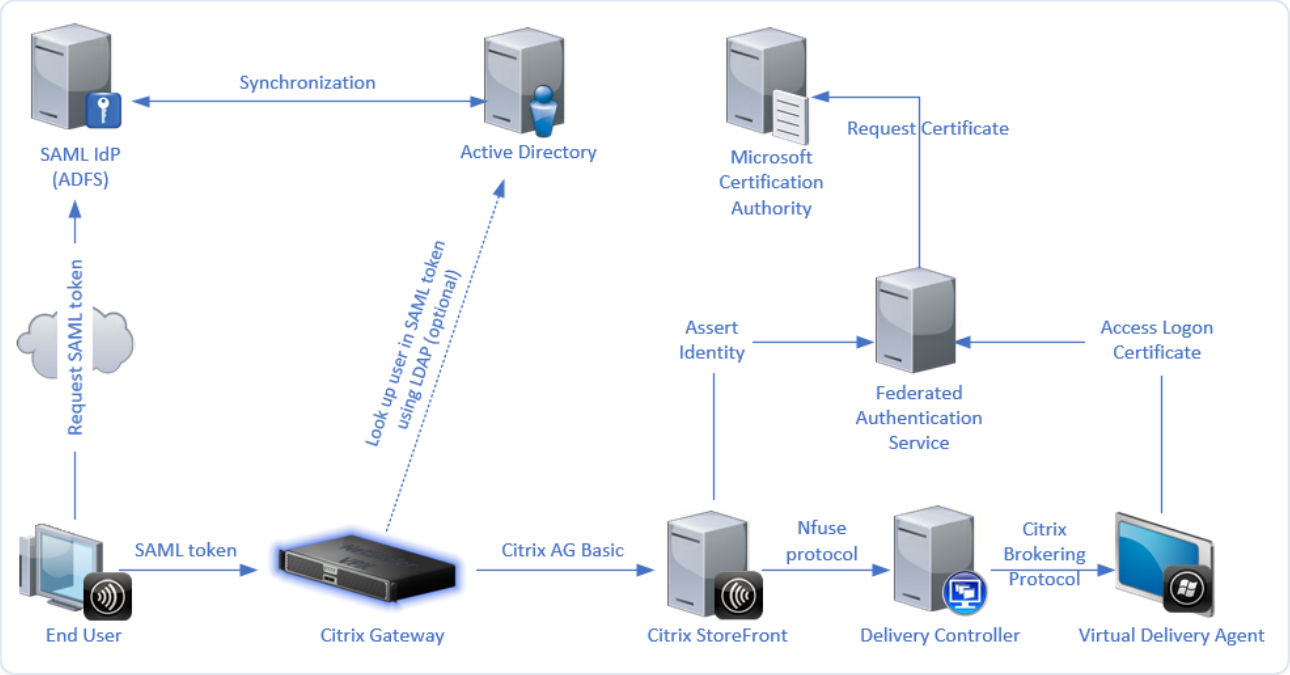
Links are provided to related FAS articles. For all architectures, the Install and configure article is the primary reference for setting up FAS.

Architectural overview

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.

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.

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).



Internal deployment

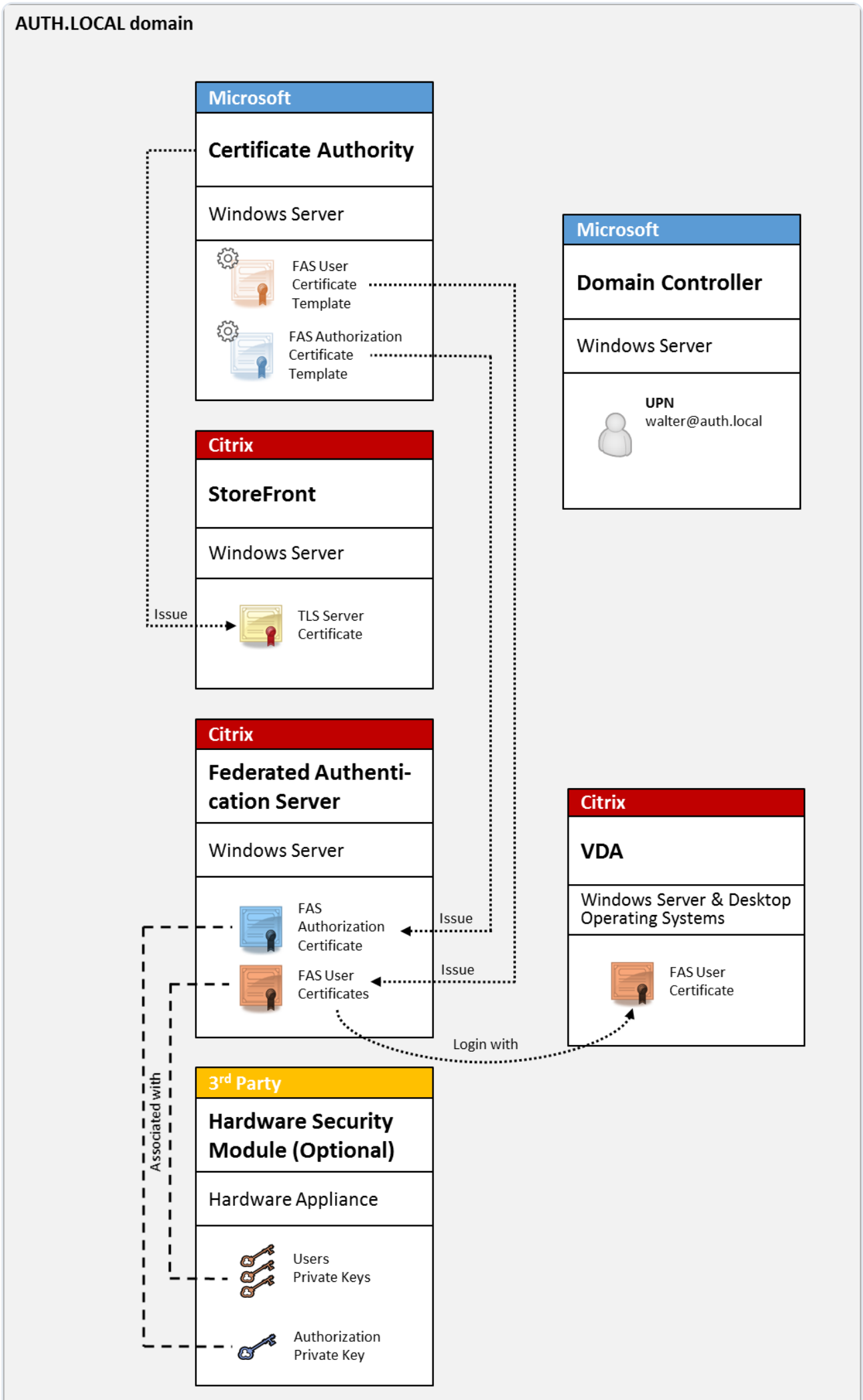
FAS allows users to securely authenticate to StoreFront using a variety of authentication options (including Kerberos single sign-on) and connect through to a fully authenticated Citrix HDX™ session.

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.


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

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.)

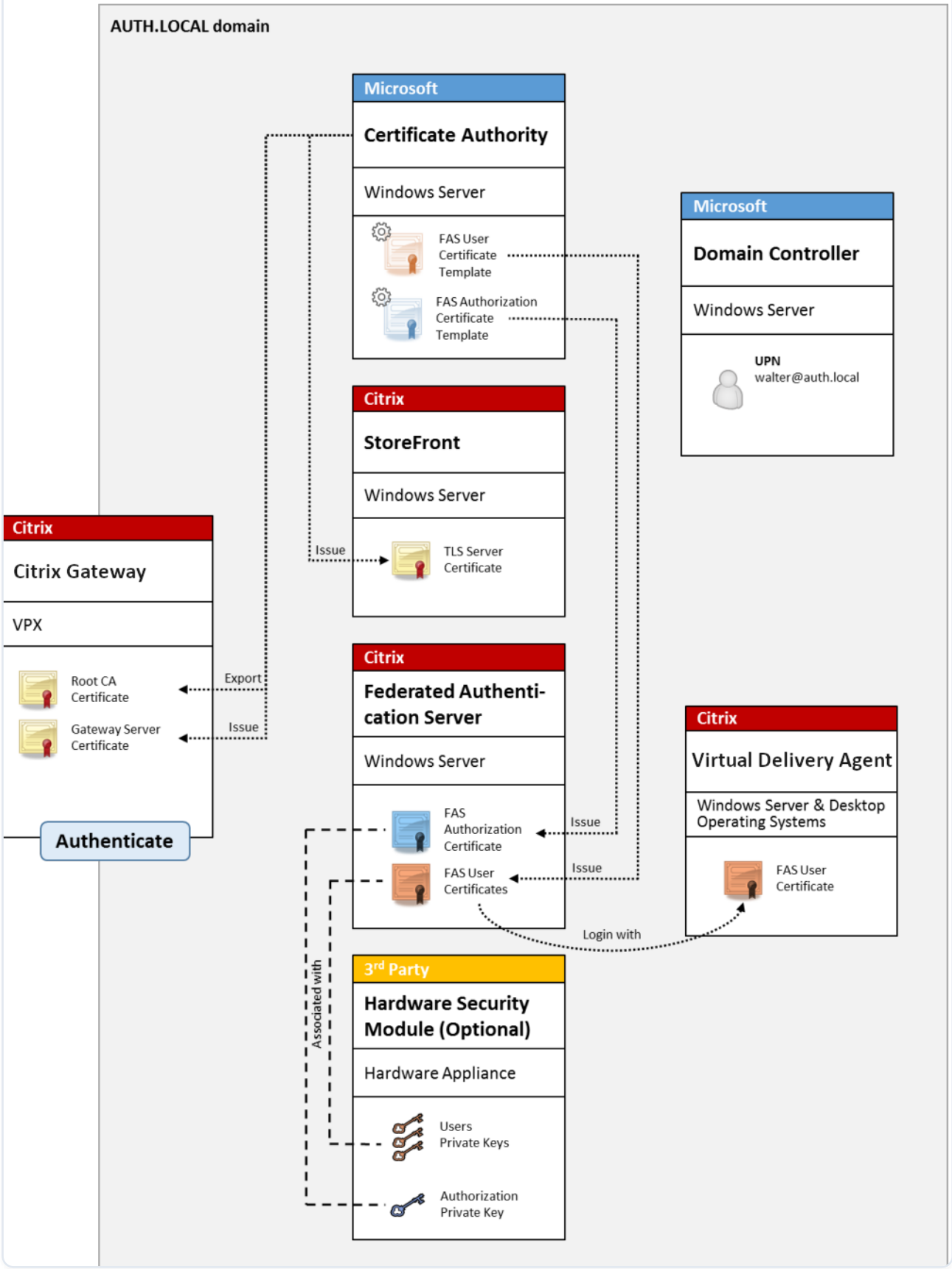
Related information:

- 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.

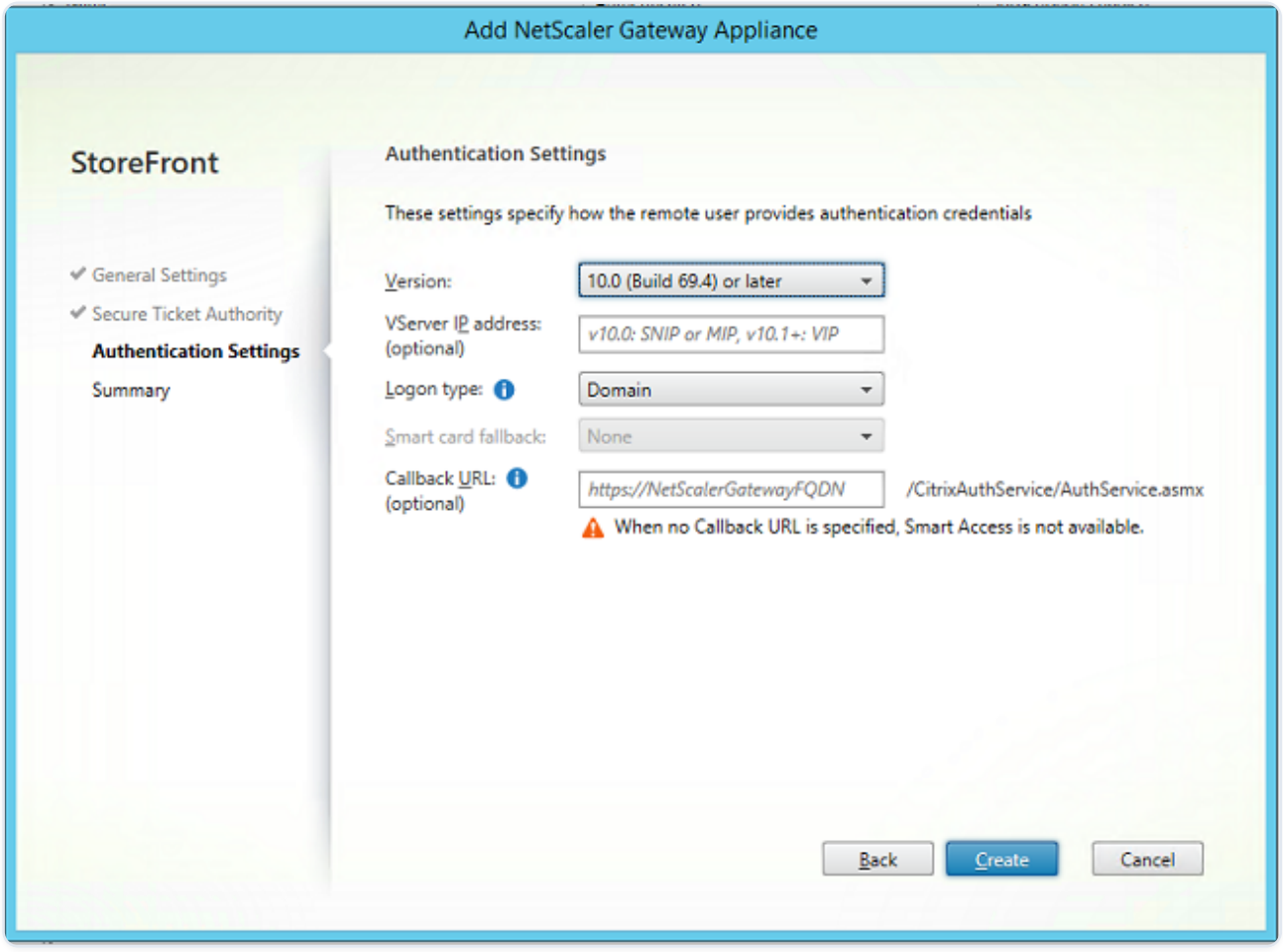
This deployment can be used to avoid multiple PIN prompts that occur when authenticating first to Citrix Gateway and then logging in to a user session. It also allows use of advanced Citrix Gateway authentication technologies without additionally requiring AD passwords or smart cards.


AUTH.LOCAL domain
Microsoft
Certificate Authority
Windows Server
FAS User Certificate Template
FAS Authorization Certificate Template
Microsoft
Domain Controller
Windows Server
UPN
walter@auth.local
Citrix
StoreFront
Windows Server
Issue
TLS Server Certificate
Citrix
Citrix Gateway
VPX
Root CA Certificate
Gateway Server Certificate
Export
Issue
Authenticate
Citrix
Federated Authentication Server
Windows Server
FAS Authorization Certificate
FAS User Certificates
Issue
Issue
Citrix
Virtual Delivery Agent
Windows Server & Desktop Operating Systems
FAS User Certificate
Login with
3rd Party
Hardware Security Module (Optional)
Hardware Appliance
Users Private Keys
Authorization Private Key
Associated with

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.

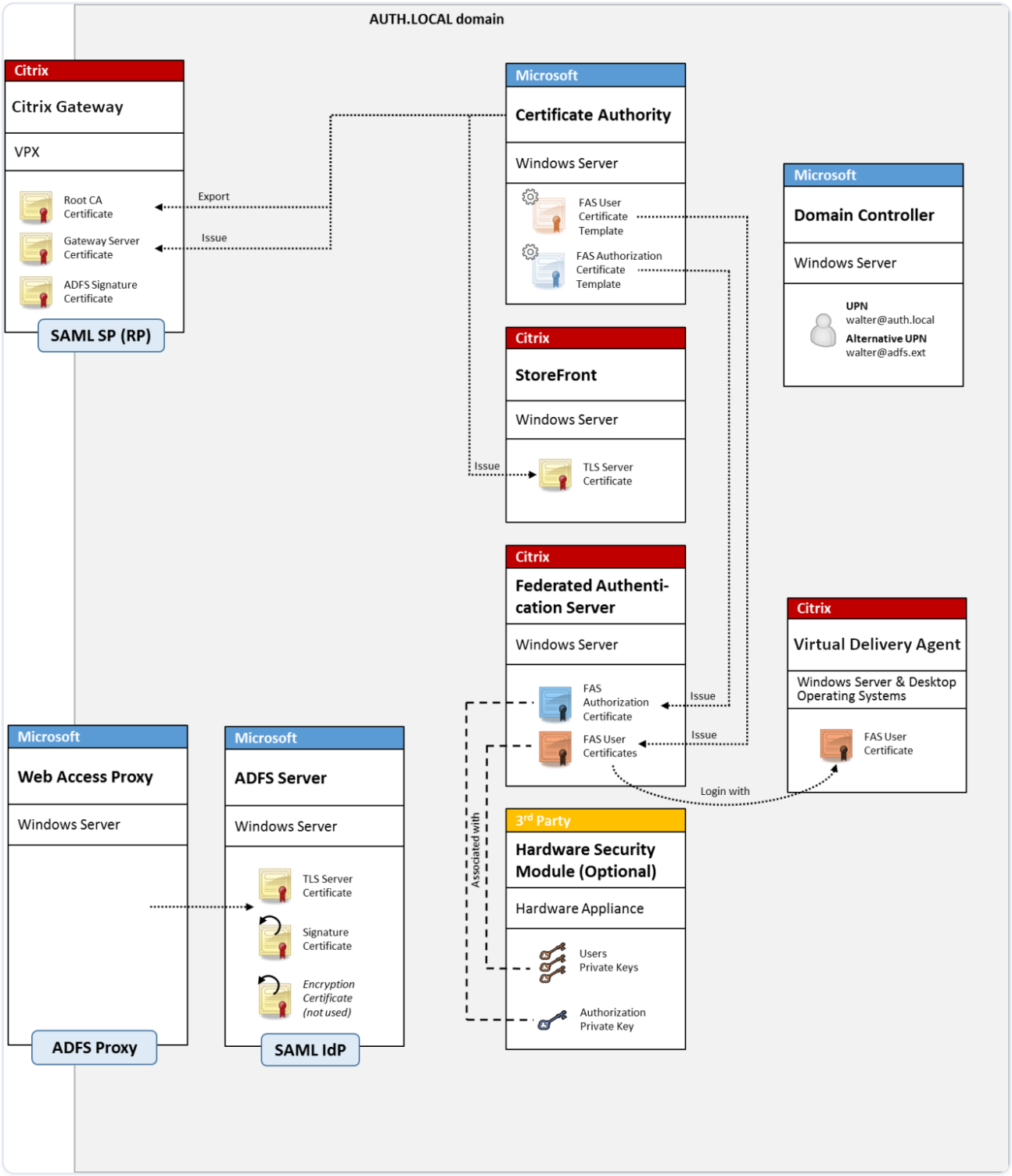


Related information:

- 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).



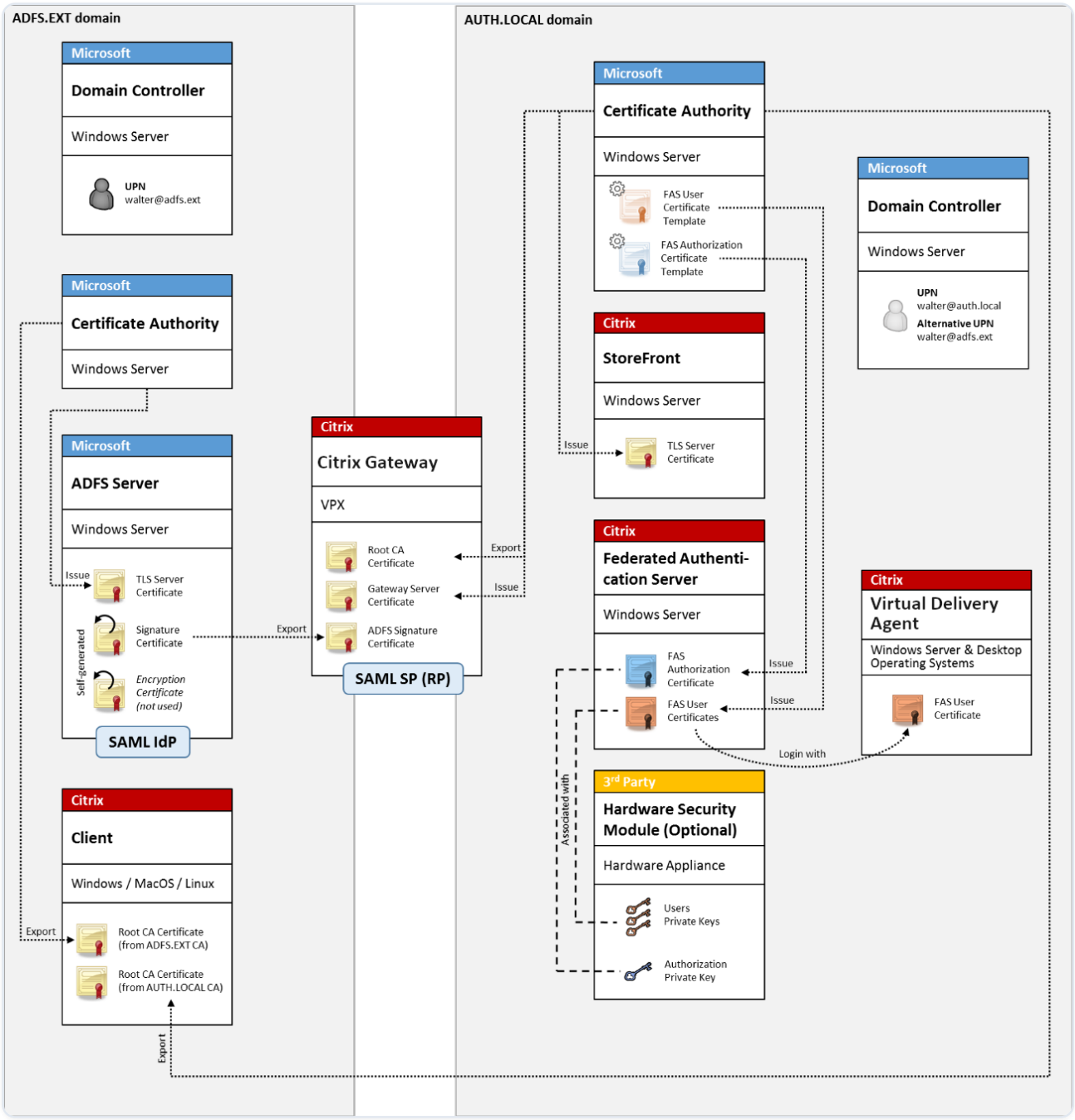
ADFS is commonly used to securely authenticate users to corporate resources remotely over the Internet; for example, it is often used for Office 365 integration.

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.

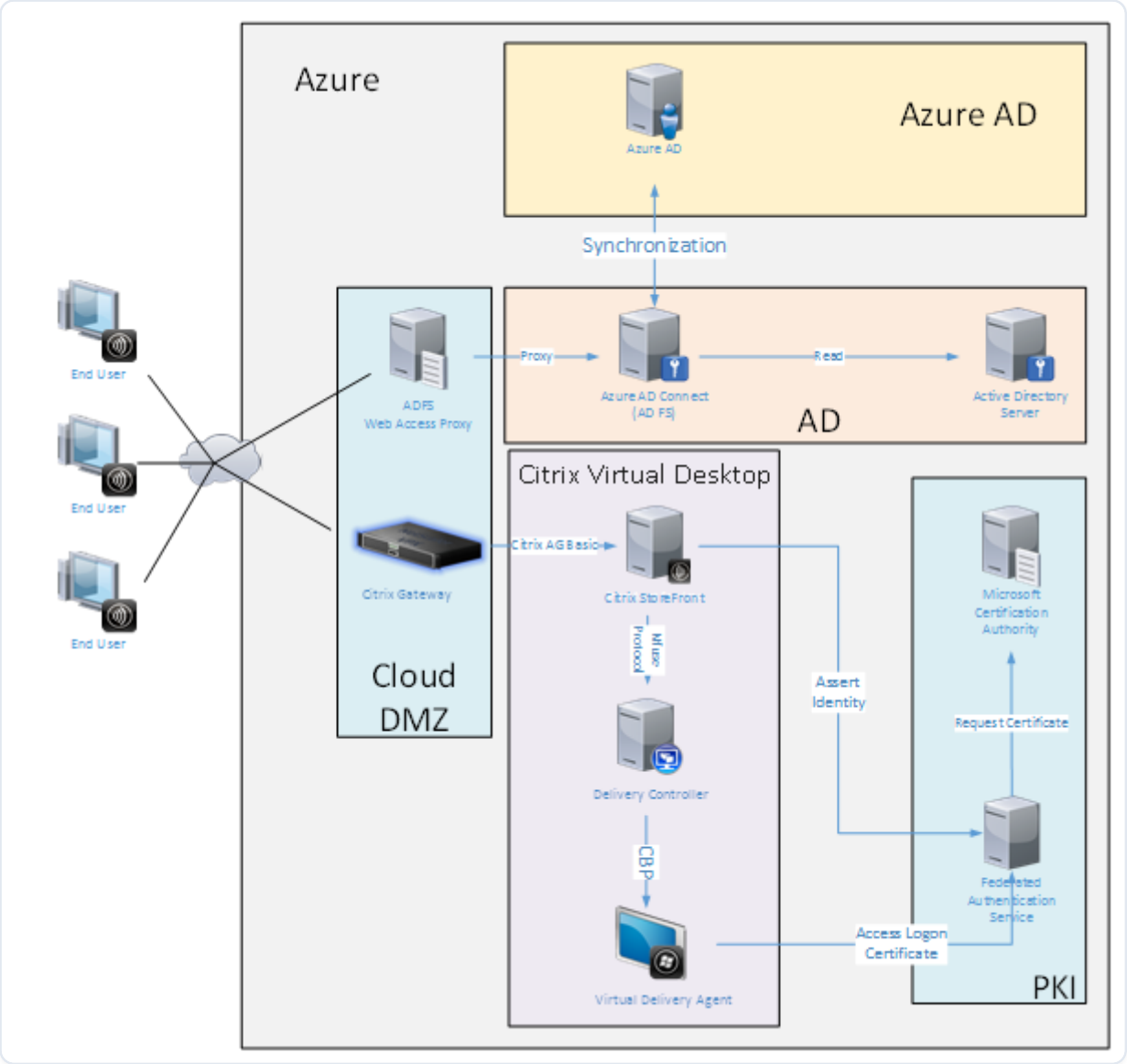


Related information:

- 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.

ADFS deployment

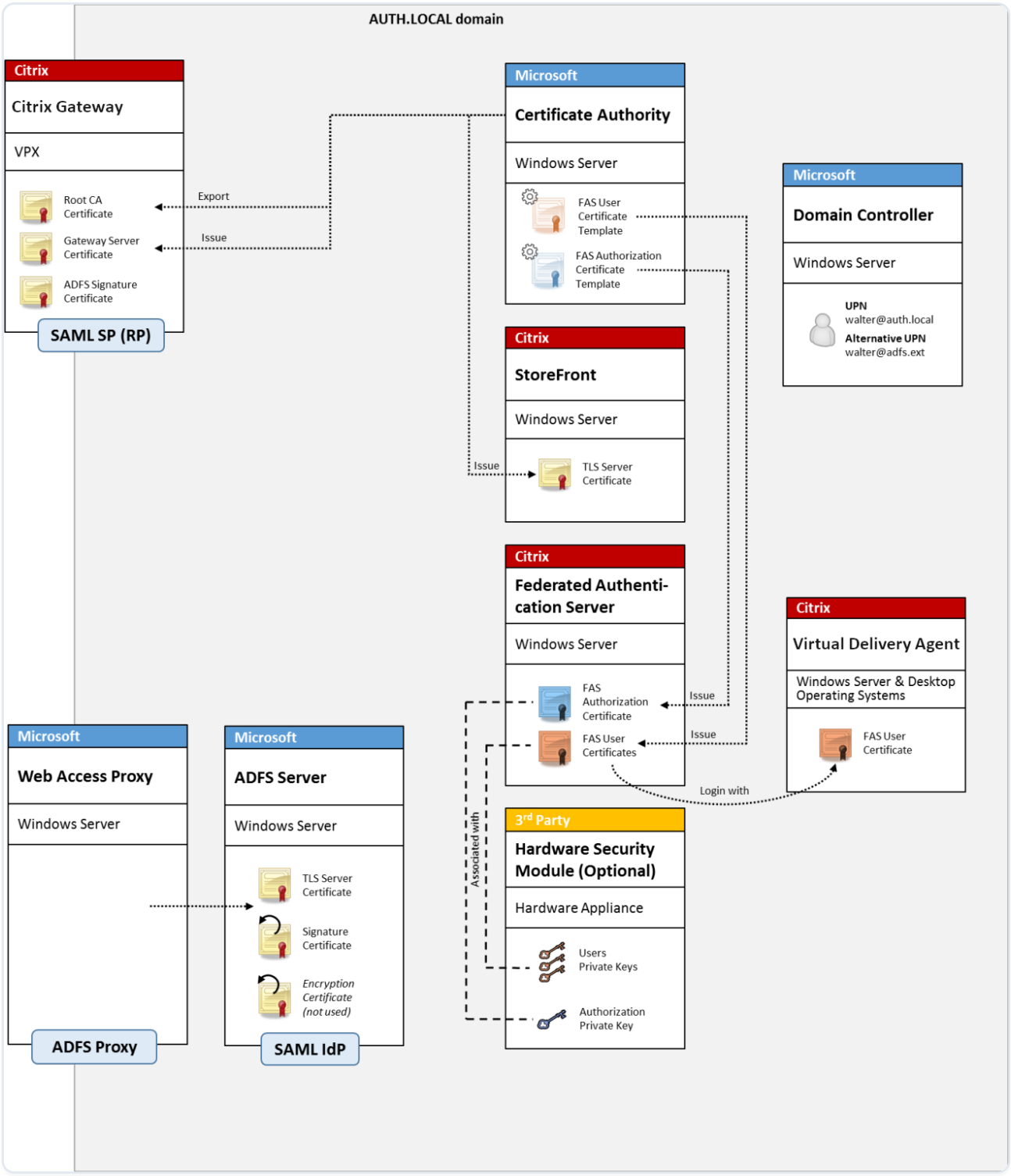
Introduction

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 employees.

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



Note:

There are no differences if the back end resource is either Windows VDA or Linux VDA.

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

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

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

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

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.

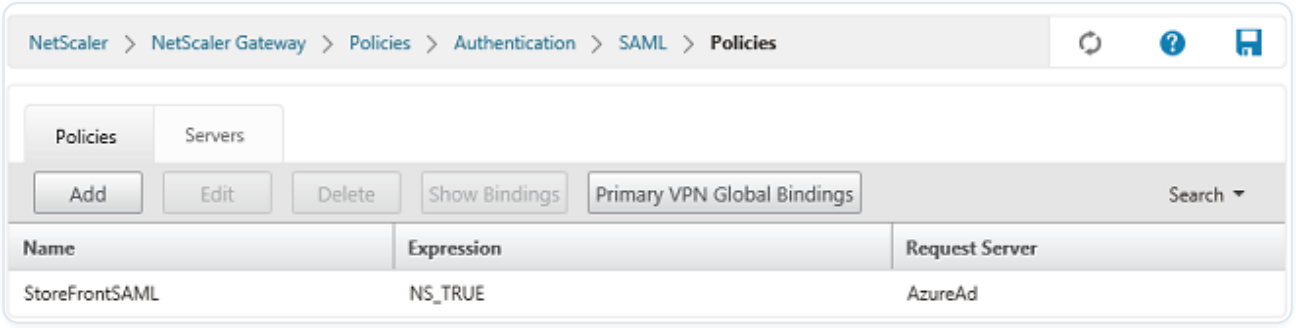
Single sign-out Url

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.)

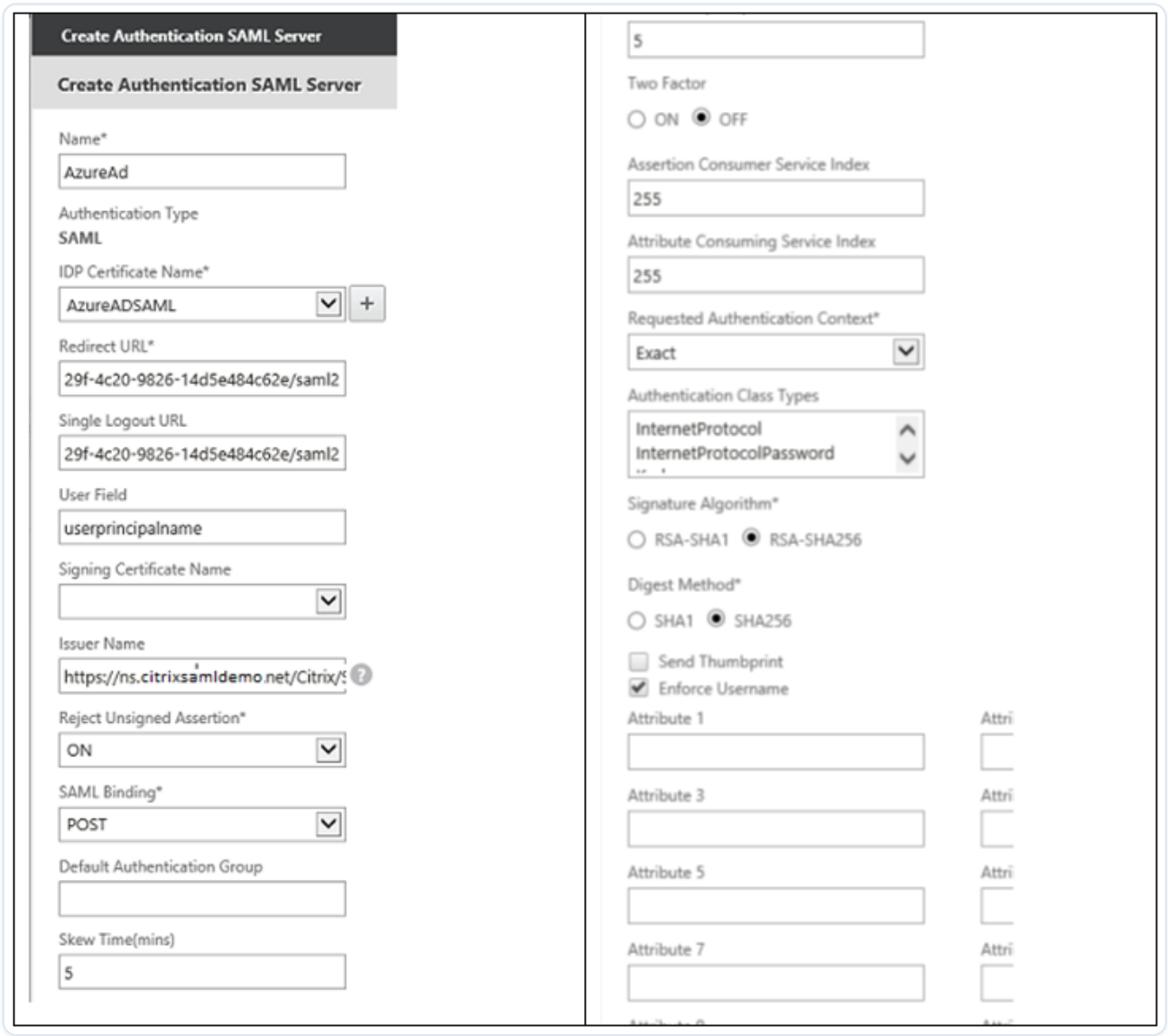
Configuration

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.

Federated Authentication Service 2603 Document History

The following table describes important changes to the Federated Authentication Service 2603 documentation. To receive notifications about these updates, subscribe to the RSS feed.

DATE	CHANGE	DESCRIPTION
30 Apr 2026	Initial release of Federated Authentication Service 2603	For more information, see What'new.