Versión 1912 LTSR del Servicio de autenticación federada

Contents

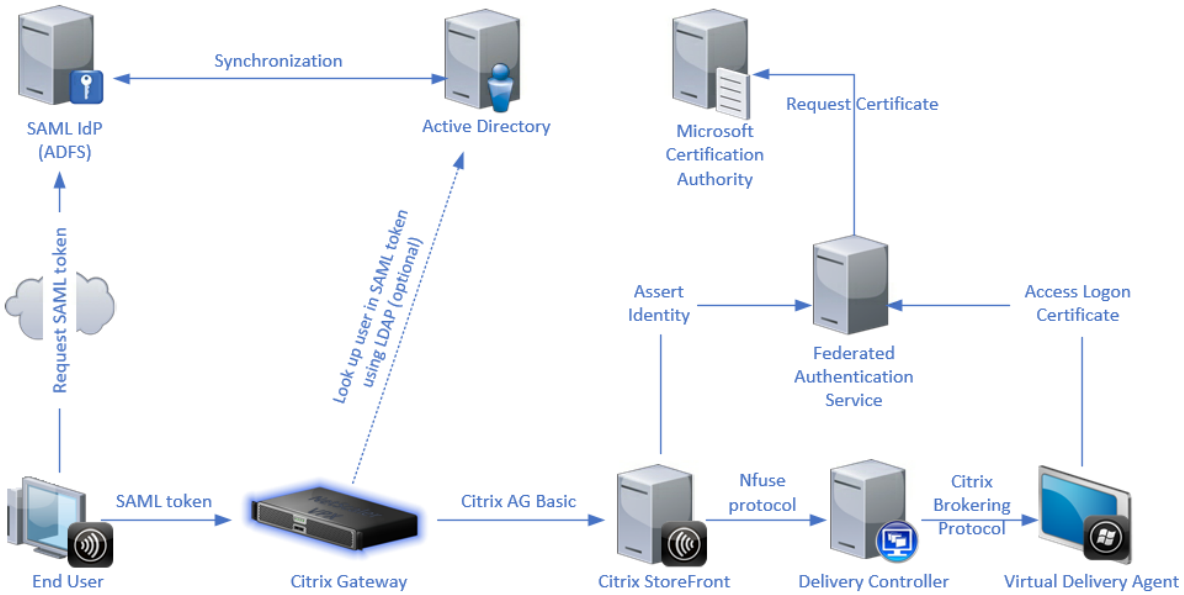
Versión 1912 LTSR del Servicio de autenticación federada

March 30, 2023

> Nota:
>
> Esta documentación admite la versión **1912 del Servicio de autenticación federada**, un componente básico para Citrix Virtual Apps and Desktops 7 1912 LTSR. Para obtener el contenido actualizado más recientemente, consulte la documentación de la versión actual del Servicio de autenticación federada. La estrategia de ciclos de vida para las versiones Current Release (CR) y las versiones Long Term Service (LTSR) del producto se describe en Hitos del ciclo de vida.

El Servicio de autenticación federada (Federated Authentication Service) es un componente con privilegios diseñado para integrarlo con el Servicio de certificados de Active Directory. Emite certificados para los usuarios de forma dinámica, lo que les permite iniciar sesiones en un entorno de Active Directory como si tuvieran una tarjeta inteligente. Esto permite a StoreFront usar una gama más amplia de opciones de autenticación, tales como aserciones SAML (Security Assertion Markup Language). SAML se usa normalmente como alternativa a las cuentas de usuario tradicionales de Windows en Internet.

El siguiente diagrama muestra FAS integrado con una entidad de certificación de Microsoft y que ofrece servicios de compatibilidad con StoreFront y los agentes Virtual Delivery Agent (VDA) de Citrix Virtual Apps and Desktops.



Los servidores de StoreFront de confianza contactan con FAS cuando los usuarios solicitan acceso a los entornos Citrix. FAS concede un tíquet que permite que una sola de sesión de Citrix Virtual Apps o

Citrix Virtual Desktops se autentique con un certificado para esa sesión. Cuando un agente VDA debe autenticar a un usuario, se conecta a FAS y canjea el tíquet. Solo FAS tiene acceso a la clave privada del certificado del usuario; el VDA debe enviar a FAS cada operación de firma y descifrado que necesita llevar a cabo con el certificado.

Referencias

- Servicios de certificados de Active Directoryhttps://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/hh831740(v=ws.11)
- Configuración de Windows para el inicio de sesión con certificadoshttp://support.citrix.com/article/CTX206156

Versión 1912 LTSR del Servicio de autenticación federada

March 30, 2023

En esta versión del Servicio de autenticación federada se resolvieron varios problemas para ayudar a mejorar el rendimiento y la estabilidad generales. No se agregaron nuevas funciones.

Para ver las correcciones de errores, consulte Problemas resueltos.

Problemas resueltos

March 30, 2023

Problemas resueltos en la versión 1912

Comparado con: Versión 1909 del Servicio de autenticación federada

La versión 1912 del Servicio de autenticación federada contiene las siguientes correcciones:

- En las propiedades de la plantilla de certificado Citrix_SmartcardLogon, la descripción de la extensión Uso de clave debe contener solo “Firma digital”y “Cifrado de clave”, pero muestra otros elementos adicionales. Sin embargo, los certificados emitidos con esta plantilla son correctos. [CVADHELP-14040]
- Cuando se utiliza la consola de administración de FAS para implementar plantillas de certificado en Active Directory, los permisos de seguridad de las plantillas ya no incluyen el permiso de

"inscripción automática". Este permiso no es necesario para el correcto funcionamiento de FAS; provocaba intentos de inscripción no deseados por parte de equipos de dominio en algunas implementaciones de clientes. [AUTH-224]

Problemas conocidos

March 30, 2023

La versión 1912 del Servicio de autenticación federada no contiene problemas conocidos.

Esta advertencia se aplica a cualquier solución temporal que sugiera cambiar una entrada del Registro:

> **Advertencia:**
>
> Si se modifica el Registro de forma incorrecta, pueden producirse problemas graves que obliguen a reinstalar el sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del Registro puedan resolverse. Si utiliza el Editor del Registro, será bajo su propia responsabilidad. Haga una copia de seguridad del Registro antes de modificarlo.

Avisos legales de terceros

March 30, 2023

Esta versión del Servicio de autenticación federada puede incluir software de terceros con licencias definidas en los términos de los siguientes documentos:

- Avisos de terceros sobre Citrix Virtual Apps and Desktops (Descargar PDF)
- Avisos de software para uso no comercial de FlexNet Publisher 2017 (11.15.0.0) (Descargar PDF)
- Software de terceros de FlexNet Publisher Documentation Supplement y software Open Source utilizados en FlexNet Publisher 11.15.0 (Descargar PDF)

Requisitos del sistema

March 30, 2023

- El Servicio de autenticación federada (FAS) es compatible con estas versiones de Windows Server:
  - Windows Server 2019, ediciones Standard y Datacenter, y con la opción Server Core
  - Windows Server 2016, ediciones Standard y Datacenter, y con opción Server Core
  - Windows Server 2012 R2, ediciones Standard y Datacenter, y Server Core para Windows Server 2012 R2
- Citrix recomienda la instalación de FAS en un servidor que no contenga ningún otro componente de Citrix.
- El servidor de Windows debe ser seguro. Este servidor tendrá acceso a un certificado de autorización de registro y una clave privada que permitirá emitir certificados para los usuarios del dominio y tendrá acceso a esos certificados de usuario y sus claves privadas.
- Los cmdlets de PowerShell de FAS requieren que Windows PowerShell de 64 bits esté instalado en el servidor FAS.
- Se requiere una entidad de certificación empresarial de Microsoft para emitir certificados de usuario.

En el sitio de Citrix Virtual Apps o Citrix Virtual Desktops:

- Los Delivery Controller, Virtual Delivery Agents (VDA) y el servidor StoreFront deben ser de versiones compatibles.

  > **Nota:**
  >
  > El servicio FAS no se admite en XenApp y XenDesktop 7.6 Long Term Service Release (LTSR).

- Antes de crear el catálogo de máquinas, compruebe que la configuración de directiva de grupo del Servicio de autenticación federada se ha aplicado correctamente a los VDA. Consulte la sección Configurar la directiva de grupo para obtener más información.

Al planificar la implementación de este servicio, revise la sección Consideraciones de seguridad.

Instalación y configuración

March 30, 2023

Secuencia de instalación y configuración

1. Instalar el Servicio de autenticación federada (FAS)
2. Habilitar el plug-in de FAS en servidores de StoreFront

3. Configurar la directiva de grupo
4. Use la consola de administración de FAS para: (a) Implementar las plantillas suministradas, (b) Configurar entidades de certificación y (c) Autorizar FAS a usar su entidad de certificación.
5. Configurar reglas de usuario

Instalar el Servicio de autenticación federada

Por motivos de seguridad, Citrix recomienda que el servicio de autenticación federada (FAS) esté instalado en un servidor dedicado que sea seguro, y esté protegido del mismo modo que un controlador de dominio o una entidad de certificación. FAS se puede instalar con el botón **Servicio de autenticación federada** en la pantalla de presentación que se autoejecuta cuando se abre la imagen ISO.

Se instalarán los siguientes componentes:

- Servicio de autenticación federada
- Cmdlets del complemento de PowerShell para configurar FAS de forma remota
- Consola de administración de FAS
- Plantillas de directiva de grupo de FAS (CitrixFederatedAuthenticationService.admx/adml)
- Archivos de plantilla de certificado para una configuración simple de las entidades de certificación
- Contadores de rendimiento y registros de eventos

Habilitar el plug-in de FAS en servidores de StoreFront

Para habilitar la integración de FAS en un almacén de StoreFront, ejecute los siguientes cmdlets de PowerShell con una cuenta de administrador. Si tiene más de un almacén, o si el almacén tiene otro nombre, la ruta indicada aquí puede ser distinta de la suya.

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

Para dejar de usar FAS, utilice el siguiente script de PowerShell:

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



```
    Set-STFClaimsFactoryNames -AuthenticationService $auth -
        ClaimsFactoryName "standardClaimsFactory"
    Set-STFStoreLaunchOptions -StoreService $store -
        VdaLogonDataProvider ""
<!--NeedCopy-->
```

Configurar el Delivery Controller

Para usar FAS, configure el Delivery Controller de Citrix Virtual Apps o Citrix Virtual Desktops para que confíe en los servidores de StoreFront que pueden conectarse a él: Ejecute el cmdlet de PowerShell **Set-BrokerSite -TrustRequestsSentToTheXmlServicePort $true**.

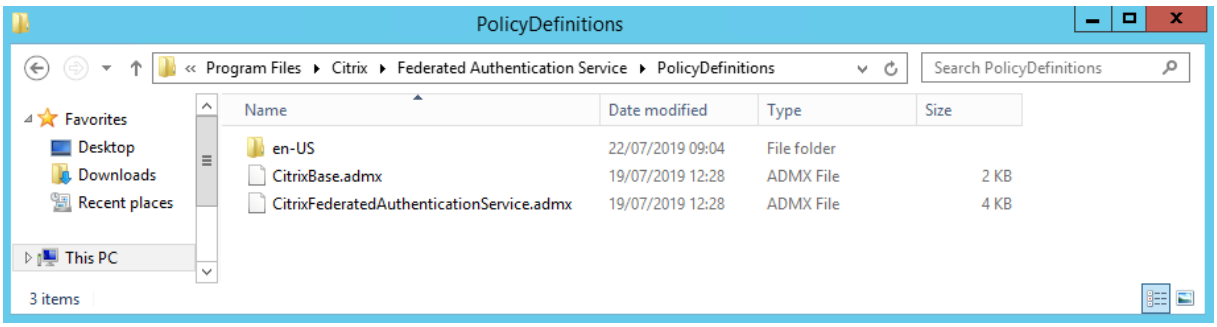
Configurar la directiva de grupo

Después de instalar FAS, se deben especificar las direcciones DNS completas de los servidores del servicio FAS en Directiva de grupo mediante las plantillas de directiva de grupo suministradas en la instalación.

> **Importante:**
>
> Compruebe que los servidores de StoreFront que solicitan tíquets y los agentes Virtual Delivery Agent (VDA) que canjean los tíquets tienen una configuración idéntica de direcciones DNS, incluida la numeración automática de los servidores que aplica el objeto de directiva de grupo.

Para simplificar la tarea, los siguientes ejemplos configuran una sola directiva en el nivel de dominio que se aplica a todas las máquinas; sin embargo, esto no es necesario. FAS funcionará siempre que los servidores de StoreFront, los VDA y la máquina que ejecuta la consola de administración de FAS vean la misma lista de direcciones DNS. Tenga en cuenta que el objeto de directiva de grupo agrega un número de índice a cada entrada, que también debe coincidir cuando se usan varios objetos.

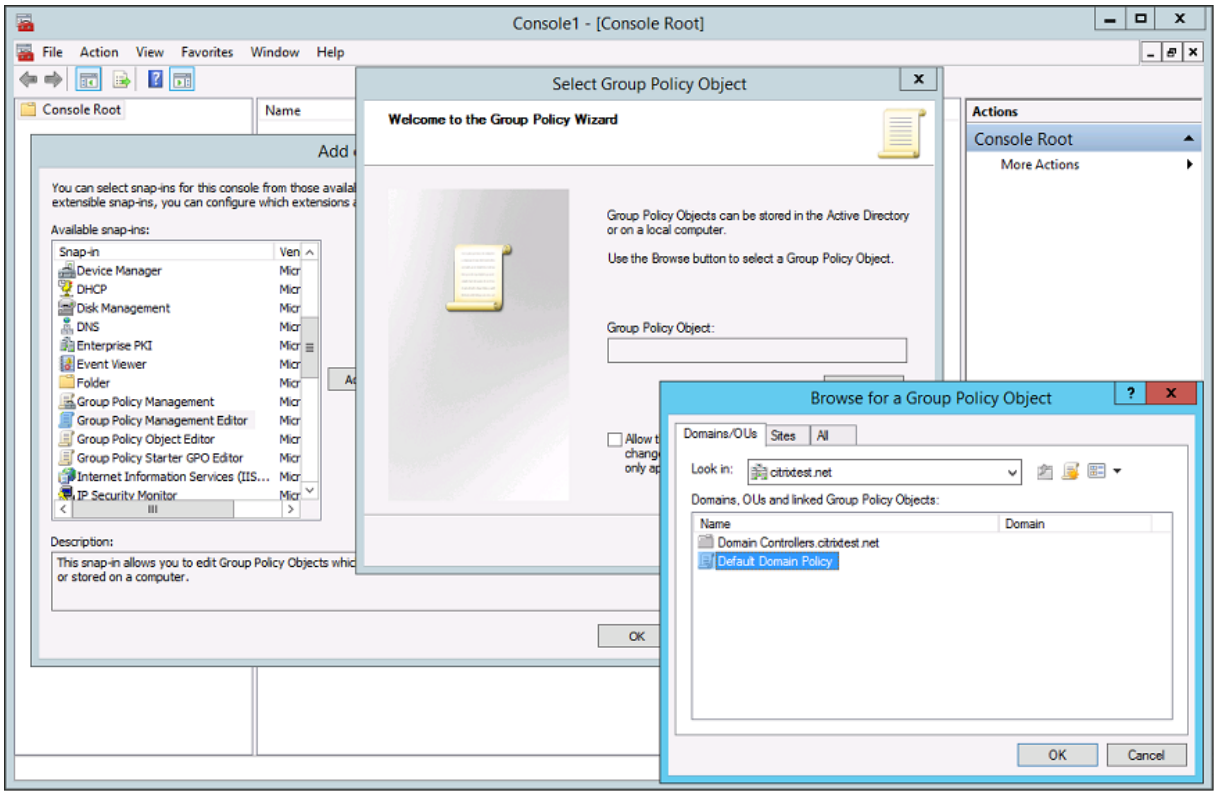
Paso 1. En el servidor donde instaló FAS, busque los archivos C:\Archivos de programa\Citrix\Federated Authentication Service\PolicyDefinitions\CitrixFederatedAuthenticationService.admx y CitrixBase.admx, y la carpeta en-US.



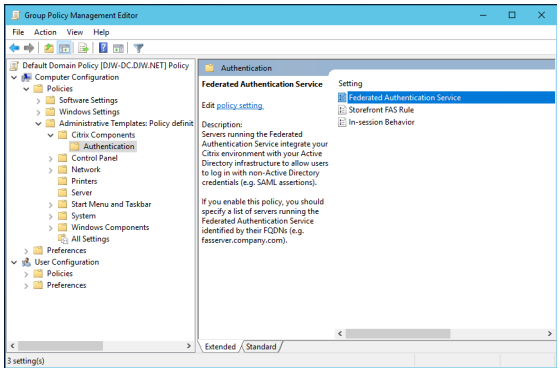
Paso 2. Cópielos en el controlador de dominio y colóquelos en la unidad C:\Windows\PolicyDefinitions y en la subcarpeta en-US.

Paso 3. Ejecute Microsoft Management Console (mmc.exe desde la línea de comandos). En la barra de menús, seleccione **Archivo > Agregar o quitar complemento**. Agregue el **Editor de administración de directivas de grupo**.

Cuando se le solicite un objeto de directiva de grupo, seleccione **Examinar** y, a continuación, seleccione **Directiva predeterminada de dominio**. De forma alternativa, puede crear y seleccionar un objeto de directiva adecuado para el entorno, mediante las herramientas de su elección. La directiva debe aplicarse a todas las máquinas que ejecutan el software de Citrix afectado (VDA, servidores de StoreFront, herramientas de administración).

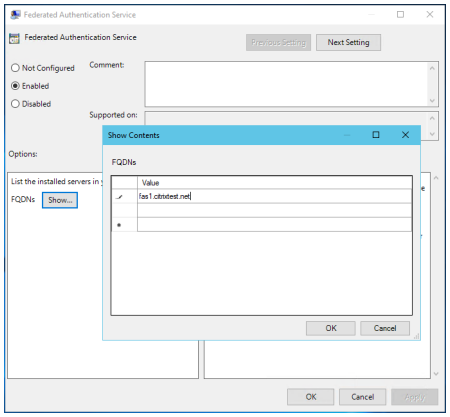


Paso 4. Vaya a la directiva de *Servicio de autenticación federada (Federated Authentication Service)* en Configuración del equipo/Directivas/Plantillas administrativas/Componentes de Citrix/Autenticación.



> **Nota:**
>
> La configuración de directiva del Servicio de autenticación federada solo está disponible en el GPO del dominio cuando agrega el archivo de plantilla CitrixBase.admx o CitrixBase.adml a la carpeta PolicyDefinitions. Una vez agregada, la configuración de directiva del Servicio de autenticación federada aparece en la carpeta Plantillas administrativas > Componentes Citrix > Autenticación.

Paso 5. Abra la directiva Federated Authentication Service y seleccione **Habilitada**. Esto le permite seleccionar el botón **Mostrar** con el que puede configurar las direcciones DNS de servidores del servicio FAS.

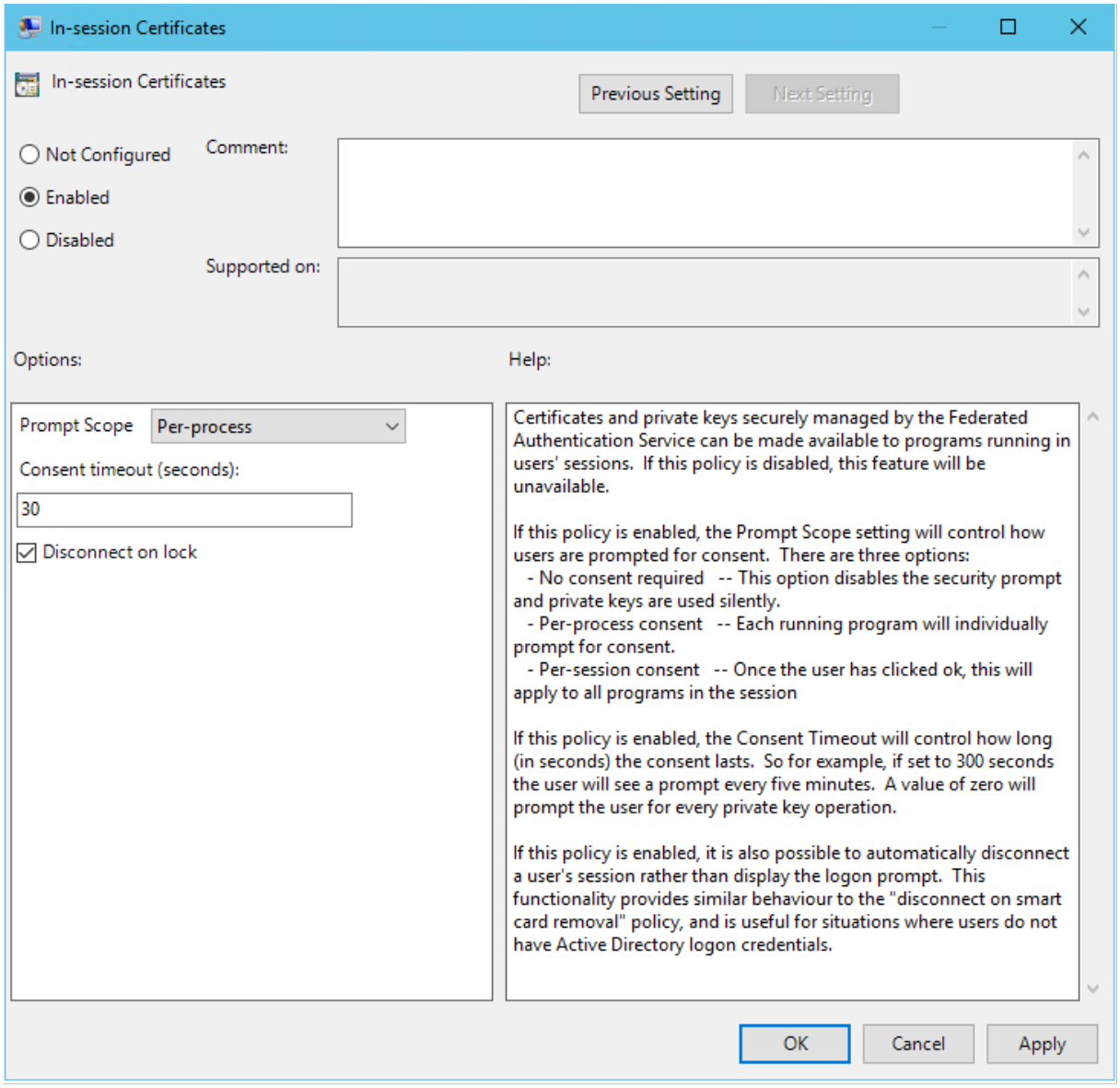


Paso 6. Introduzca los nombres de dominio completos (FQDN) de los servidores que alojan FAS.

Recuerde: Si escribe varios nombres FQDN, el orden de la lista debe ser coherente entre los servidores de StoreFront y los VDA. Esto incluye las entradas en blanco y las entradas de no utilizadas de la lista.

Paso 7. Haga clic en **Aceptar** para salir del asistente de directivas de grupo y aplicar los cambios de la directiva de grupo. Es posible que tenga que reiniciar las máquinas (o ejecutar **gpupdate /force** desde la línea de comandos) para que el cambio surta efecto.

Compatibilidad con certificados en la sesión y desconexión por bloqueo



Funcionalidad de certificados en la sesión De forma predeterminada, los VDA no permiten el acceso a los certificados después de iniciar la sesión. Si es necesario, puede utilizar la plantilla de directivas de grupo con el fin de configurar el sistema para certificados en la sesión. Esto coloca los certificados en el almacén de certificados personal del usuario después del inicio de sesión para el uso de aplicaciones. Por ejemplo, si necesita usar autenticación TLS en los servidores web dentro de la sesión de VDA, Internet Explorer puede usar el certificado.

Desconexión por bloqueo Si esta directiva está habilitada, la sesión del usuario se desconecta automáticamente cuando este bloquea la pantalla. Esta funcionalidad ofrece un comportamiento simi-

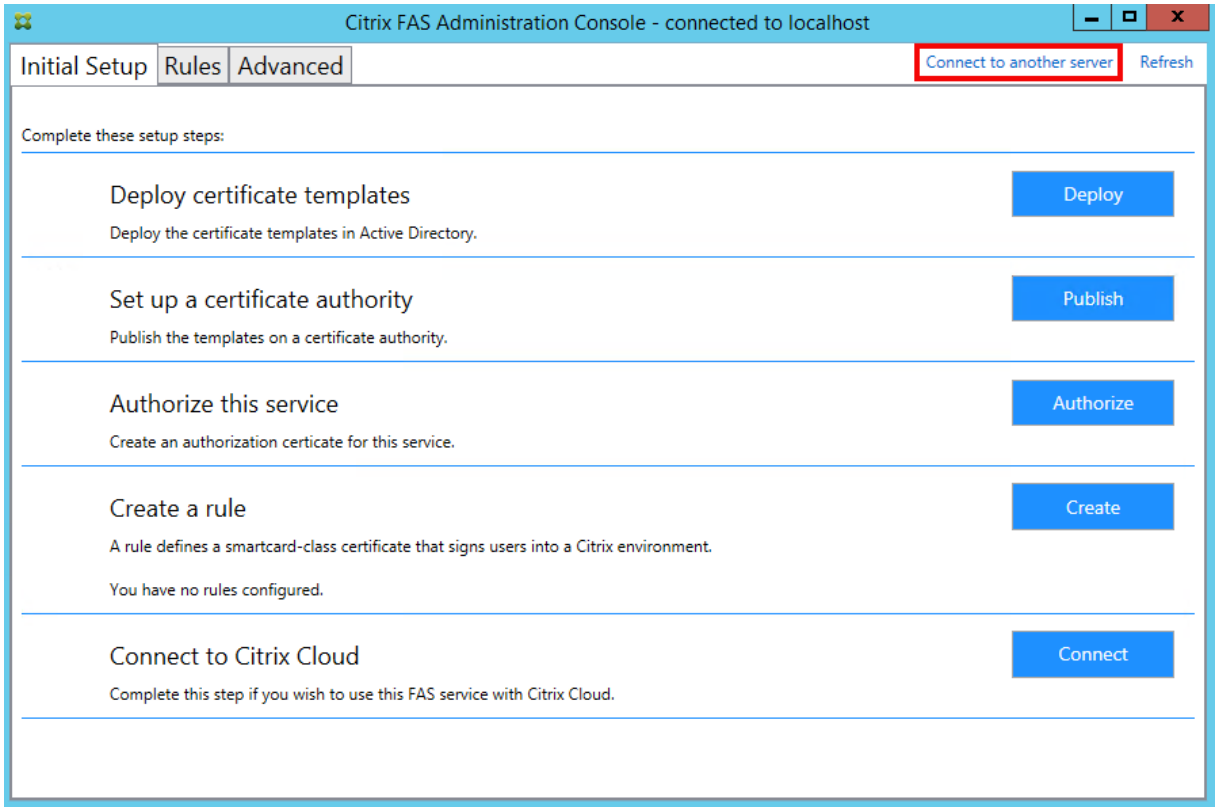
lar al de la directiva de "desconexión por extracción de tarjeta inteligente"y es útil en situaciones en las que los usuarios no tienen credenciales de inicio de sesión de Active Directory.

> **Nota:**
>
> La directiva de desconexión por bloqueo se aplica a todas las sesiones del VDA.

Usar la consola de administración de los Servicios de autenticación federada

La consola de administración de FAS se instala como parte de FAS. Se coloca el icono Citrix Federated Authentication Service en el menú Inicio.

La primera vez que se utiliza la consola de administración, se le guiará a través de un proceso que implementa las plantillas de certificado, establece la entidad de certificación y autoriza a FAS para usar la entidad de certificación. Algunos de los pasos pueden completarse manualmente mediante herramientas de configuración del sistema operativo.

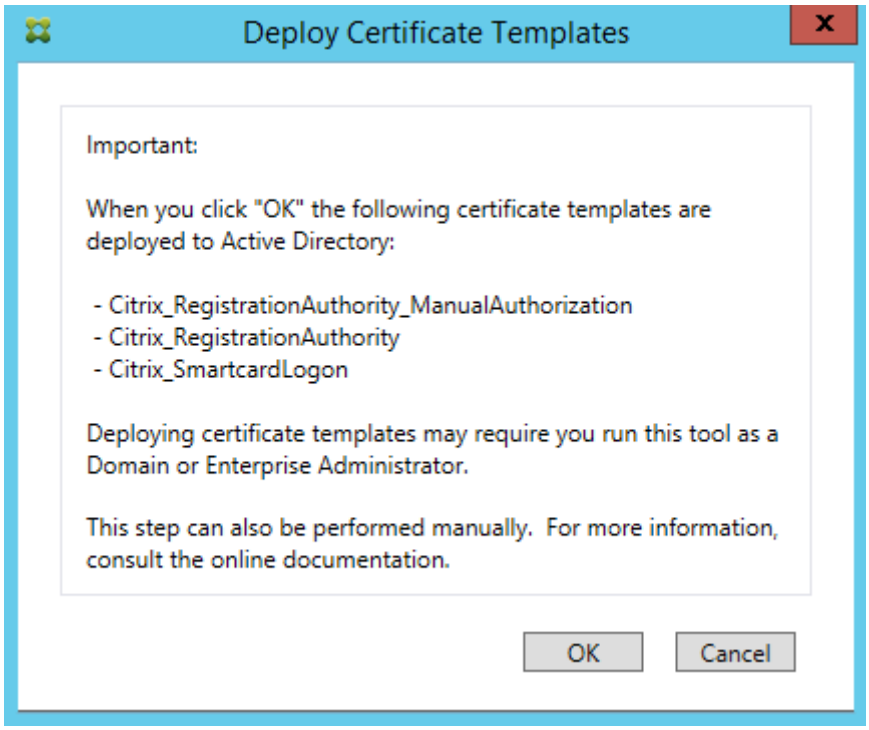


Implementar plantillas de certificado

Para evitar problemas de interoperabilidad con otros programas de software, FAS proporciona tres plantillas de certificado de Citrix para su propio uso.

- Citrix_RegistrationAuthority_ManualAuthorization
- Citrix_RegistrationAuthority
- Citrix_SmartcardLogon

Estas plantillas deben registrarse en Active Directory. Si la consola no puede encontrarlas, se pueden instalar con la herramienta **Implementar plantillas de certificado**. Esta herramienta debe ejecutarse con una cuenta que tenga permisos para administrar el bosque de AD de su empresa.



La configuración de las plantillas se encuentra en los archivos XML con la extensión .certificatetemplate. Estos archivos se instalan con FAS en:

C:\Archivos de programa\Citrix\Federated Authentication Service\CertificateTemplates

Si no dispone de permiso para instalar estos archivos de plantilla, déselas al administrador de Active Directory.

Para instalar manualmente las plantillas, pueden usar los siguientes comandos de PowerShell:

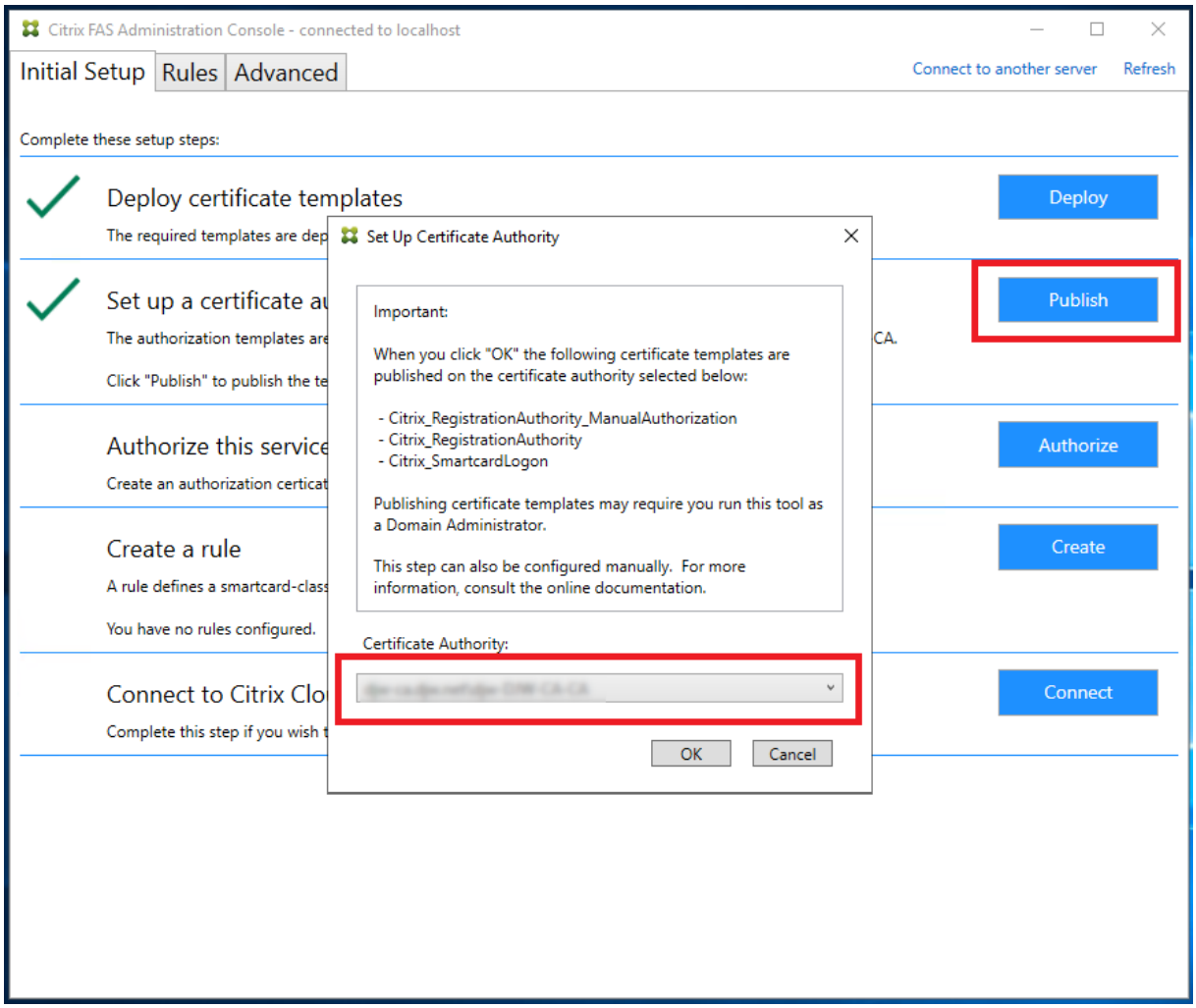
```
1      $template = [System.IO.File]::ReadAllBytes("$Pwd\
          Citrix_SmartcardLogon.certificatetemplate")
2      $CertEnrol = New-Object -ComObject X509Enrollment.
          CX509EnrollmentPolicyWebService
3      $CertEnrol.InitializeImport($template)
4      $comtemplate = $CertEnrol.GetTemplates().ItemByIndex(0)
5      $writabletemplate = New-Object -ComObject X509Enrollment.
          CX509CertificateTemplateADWritable
6      $writabletemplate.Initialize($comtemplate)
7      $writabletemplate.Commit(1, $NULL)
8  <!--NeedCopy-->
```


Configurar los Servicios de certificados de Active Directory

Después de instalar las plantillas de certificado de Citrix, deben publicarse en uno o varios servidores de entidad de certificación de Microsoft. Consulte la documentación de Microsoft acerca de cómo implementar Servicios de certificados de Active Directory.

Si las plantillas no se publican en, al menos, un servidor, la herramienta **Setup certificate authority** solicita publicarlas. Debe ejecutar esta herramienta como un usuario que tenga permisos para administrar la entidad de certificación.

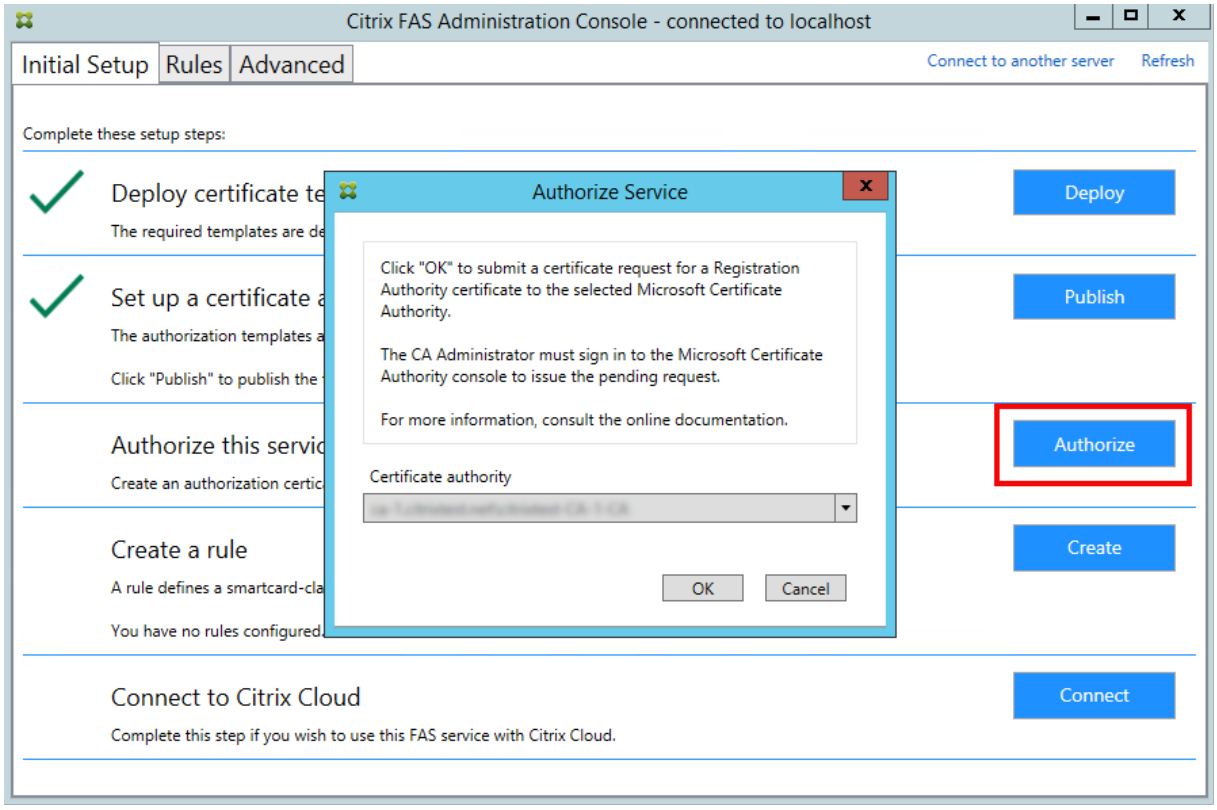
(También se pueden publicar plantillas de certificado mediante la consola de Entidad de certificación de Microsoft.)



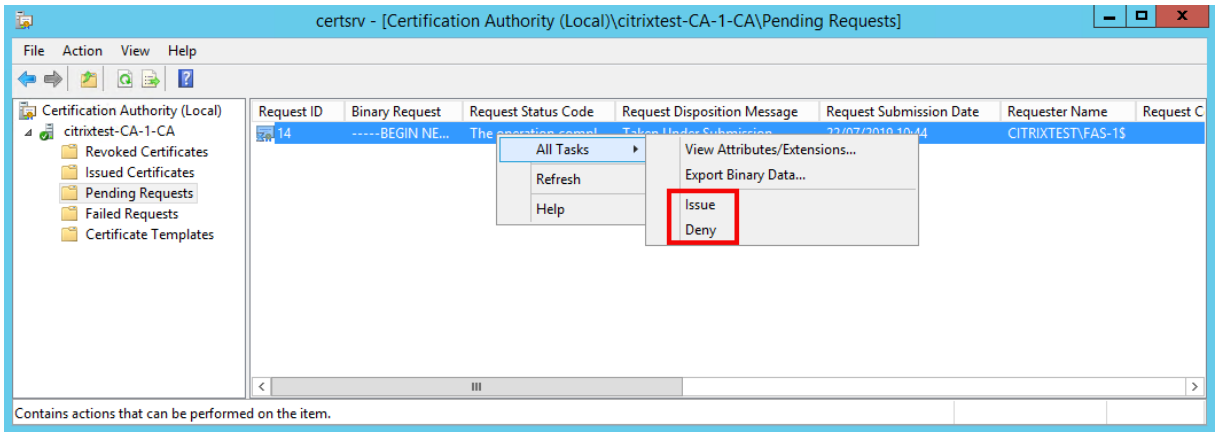
Autorizar el Servicio de autenticación federada

Este paso inicia la autorización de FAS. La consola de administración utiliza la plantilla Citrix_RegistrationAuthority_ManualAuthorization para generar una solicitud de certificado y, a

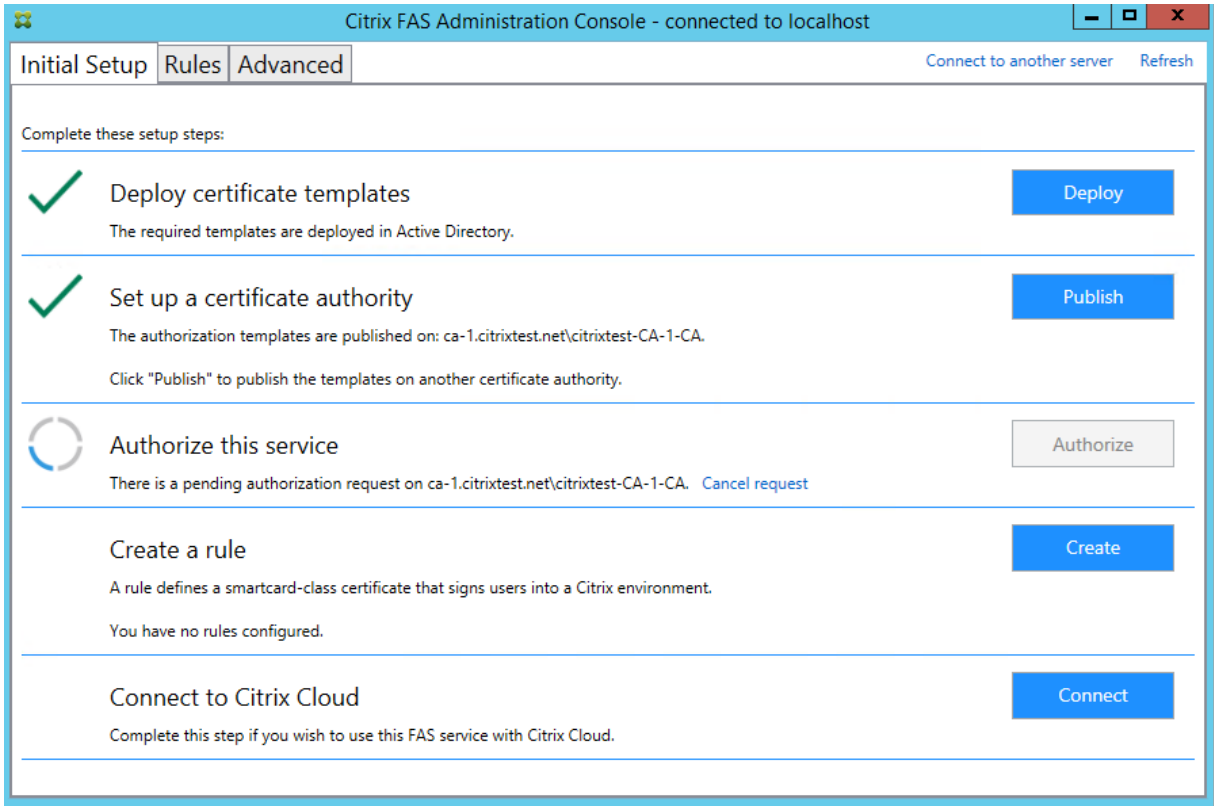
continuación, lo envía a una de las entidades de certificación que publican esa plantilla.



Después de enviarse la solicitud, aparecerá en la lista de **Solicitudes pendientes** de la consola de la entidad de certificación de Microsoft. El administrador de la entidad de certificación debe elegir entre **Emitir** o **Rechazar** la solicitud antes de que la configuración de FAS pueda continuar. Tenga en cuenta que la solicitud de autorización se muestra como una **Solicitud pendiente** desde la cuenta de equipo de FAS.



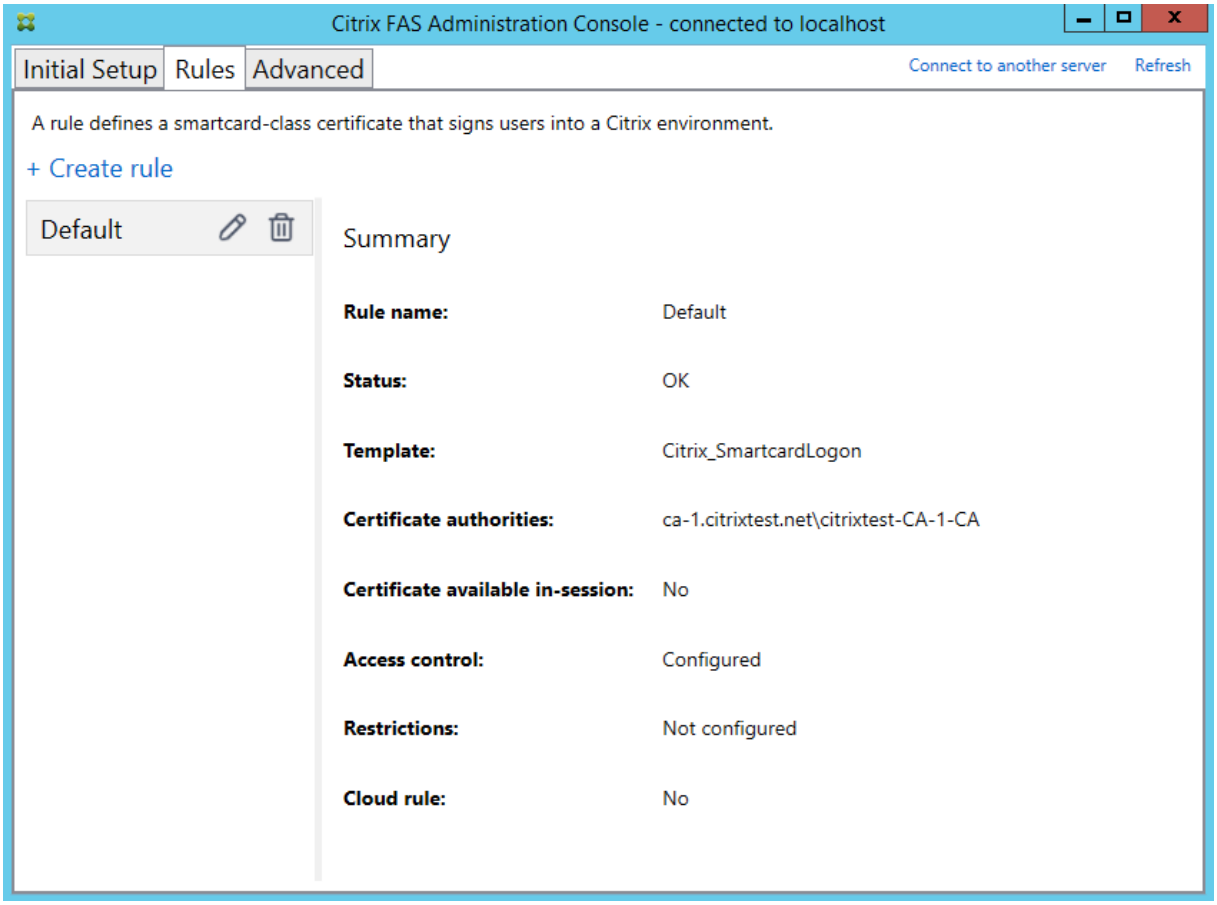
Haga clic con el botón secundario en **Todas las tareas** y, a continuación, seleccione **Emitir** o **Rechazar** la solicitud de certificado. La consola de administración de FAS detecta automáticamente cuando se completa el proceso. Esto puede tardar unos minutos.



Configurar reglas de usuario

Una regla de usuario autoriza la emisión de certificados para el inicio de sesión en los VDA y uso dentro de sesiones, según lo indique StoreFront. Cada regla especifica los servidores de StoreFront que son de confianza para solicitar certificados, el conjunto de usuarios para los que pueden ser solicitados y el conjunto de máquinas VDA a las que se les permite usarlos.

Para completar la configuración de FAS, debe definir la regla predeterminada. Haga clic en **Crear** para crear una regla o vaya a la ficha "Reglas"y haga clic en **Crear regla**. El asistente recopila la información necesaria para definir una regla.



El asistente recopila la siguiente información:

Template: La plantilla de certificado que se utiliza para emitir certificados de usuario. Debe ser la plantilla Citrix_SmartcardLogon, o una copia modificada de la misma.

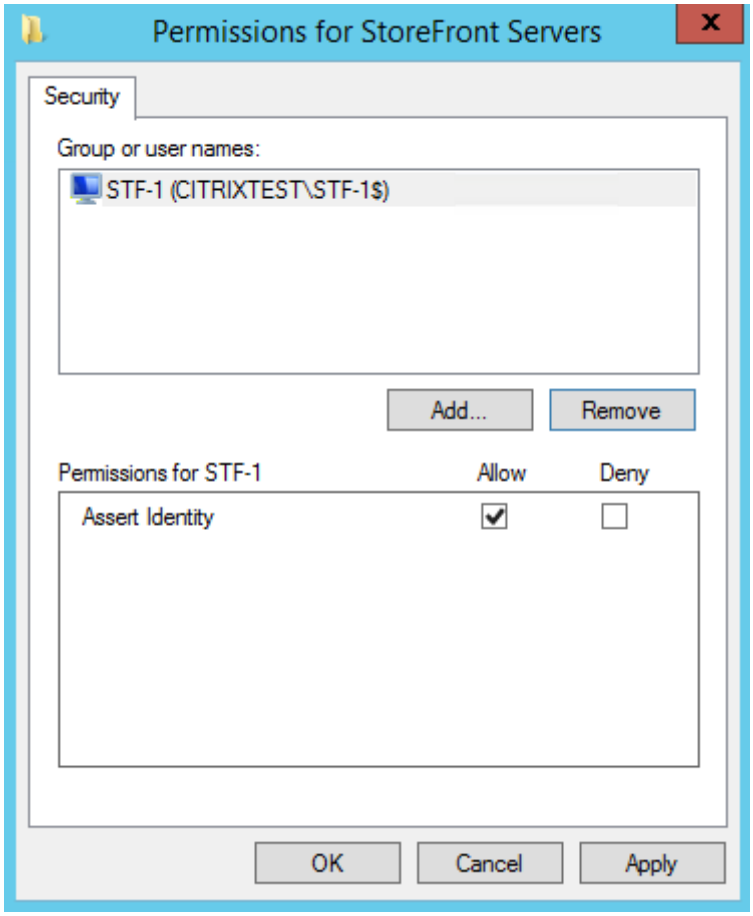
Certificate Authority: La entidad de certificación que emite los certificados de usuario. La entidad de certificación es la que debe publicar la plantilla. FAS admite varias entidades de certificación para la conmutación por error y el equilibrio de carga.

In-Session Use: La opción **Allow in-session use** controla si se puede utilizar un certificado después de iniciar sesión en el VDA. Seleccione esta opción solo si quiere que los usuarios tengan acceso al certificado después de la autenticación. Si esta opción no está seleccionada, el certificado se usará solamente para iniciar sesión o reconectarse, y el usuario no tendrá acceso al certificado después de autenticarse.

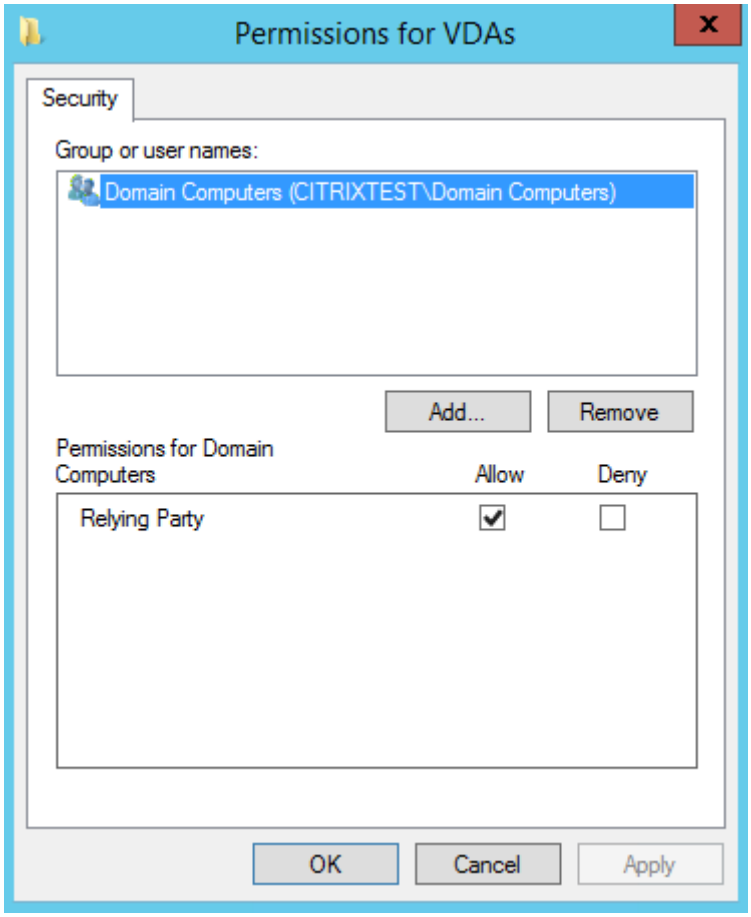
Access control: La lista de máquinas de servidor de StoreFront de confianza que están autorizadas para solicitar certificados para el inicio de sesión o la reconexión de usuarios.

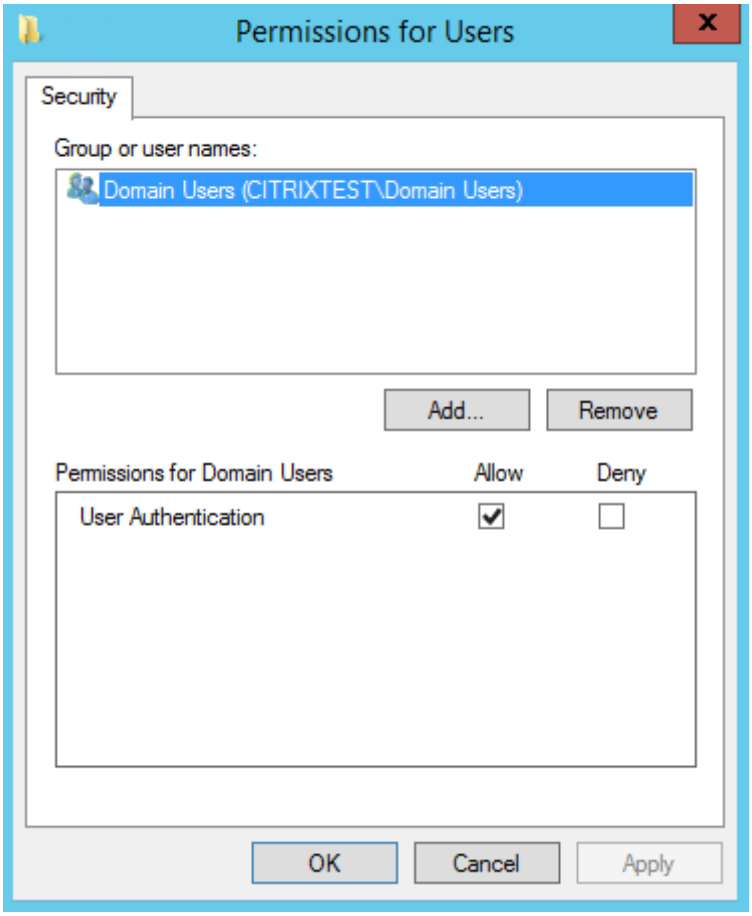
> **Importante:**
>
> Tenga en cuenta que el parámetro **Access control** es fundamental para la seguridad y es nece-

> sario configurarlo cuidadosamente.



Restrictions: La lista de máquinas VDA que pueden iniciar sesión para los usuarios mediante FAS y la lista de usuarios a los que se pueden emitir certificados a través de FAS. La lista de VDA incluye de forma predeterminada los Equipos del dominio y la lista de usuario incluye de forma predeterminada los Usuarios del dominio, pero esto puede cambiarse si estos valores predeterminados no son los adecuados.





Cloud rule: Actualmente no disponible.

Uso avanzado

Puede crear reglas adicionales para hacer referencia a otras plantillas de certificado y entidades de certificación, que pueden haberse configurado con propiedades y permisos diferentes. Estas reglas se pueden configurar para ser utilizadas por distintos servidores de StoreFront, que a su vez deberán configurarse para solicitar la nueva regla por su nombre. De forma predeterminada, StoreFront solicita la regla predeterminada **default** al contactar con FAS. Esto se puede cambiar mediante las opciones de configuración de la directiva de grupo.

Para crear una nueva plantilla de certificado, cree un duplicado de la plantilla Citrix_SmartcardLogon en la consola de la entidad de certificación de Microsoft, cámbiele el nombre (por ejemplo, Citrix_SmartcardLogon2) y modifíquela según sea necesario. Cree una nueva regla, haciendo clic en **Add** para que haga referencia a la nueva plantilla de certificado.

Consideraciones sobre la actualización

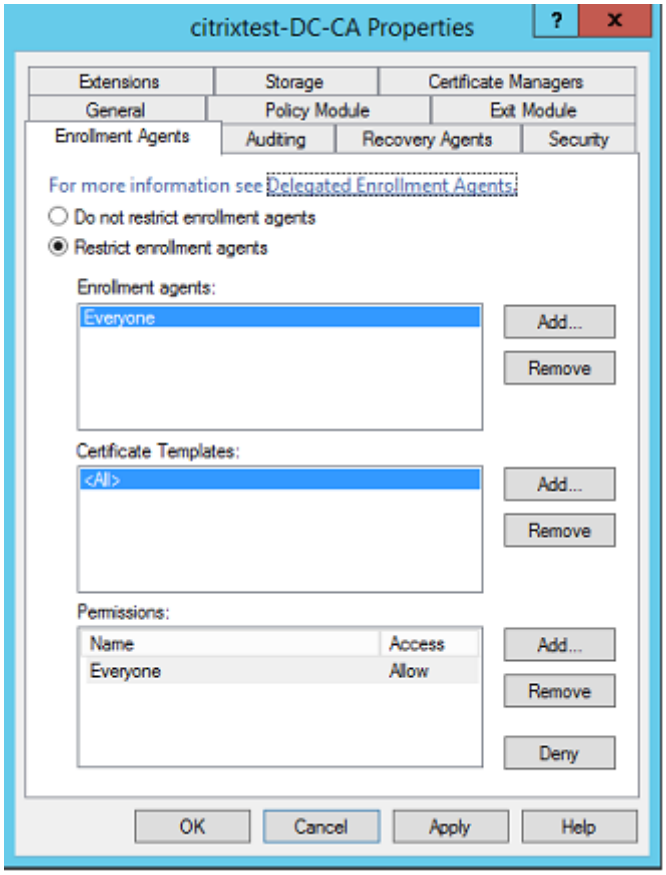
- Todos los parámetros de servidor de FAS se conservan cuando se realiza una actualización en contexto.
- Actualice FAS mediante el instalador de producto completo de Virtual Apps and Desktops.
- Antes de actualizar FAS, actualice el Controller y los VDA (y otros componentes principales) a la versión requerida.
- Compruebe que la consola de administración de FAS esté cerrada antes de actualizar FAS.
- Al menos un servidor de FAS debe estar disponible en todo momento. Si un servidor de StoreFront habilitado para el Servicio de autenticación federada no puede establecer contacto con ningún servidor, los usuarios no podrán iniciar sesión ni iniciar aplicaciones.

Consideraciones sobre seguridad

FAS tiene un certificado de autorización de registro que le permite emitir certificados de forma autónoma en nombre de los usuarios de dominio. Como consecuencia, es muy importante desarrollar e implementar una directiva de seguridad para proteger los servidores de FAS y restringir sus permisos.

Agentes de inscripción delegada

El servicio FAS emite certificados de usuario y, así, actúa como agente de inscripción. La entidad de certificación de Microsoft permite controlar qué plantillas puede usar el servidor del servicio FAS, así como limitar para qué usuarios puede emitir certificados dicho servidor.



Citrix recomienda configurar estas opciones de modo que FAS solo pueda emitir certificados para los usuarios apropiados. Por ejemplo, se recomienda impedir que FAS emita certificados para los usuarios incluidos en un grupo de administración o de usuarios protegidos.

Configurar una lista de control de acceso

Como se describe en la sección Configurar reglas de usuario, debe configurar una lista de servidores de StoreFront con la confianza necesaria para la aserción de identidades de usuario de cara a FAS cuando se emiten certificados. Del mismo modo, puede restringir para qué usuarios se pueden emitir certificados y en qué máquinas VDA se pueden autenticar. Esto es adicional a las funciones de seguridad estándar de la entidad de certificación o de Active Directory.

Parámetros de firewall

Todas las comunicaciones con los servidores de FAS usan conexiones de red de Windows Communication Foundation (WCF) a través del puerto 80 mediante autenticación mutua con Kerberos.

Supervisar el registro de eventos

FAS y el VDA escriben información en el registro de eventos de Windows. Esto se puede utilizar para ver información de supervisión y auditoría. En la sección Registros de eventos, se ofrece una lista de las entradas del Registro de eventos que pueden generarse.

Módulo de seguridad de hardware

Todas las claves privadas, incluidas las de los certificados de usuario emitidos por FAS, se almacenan como claves privadas no exportables con la cuenta de Servicio de red. FAS admite el uso de un módulo de seguridad de hardware de cifrado, si su directiva de seguridad así lo requiere.

La configuración criptográfica de bajo nivel está disponible en el archivo FederatedAuthenticationService.exe.config. Estos parámetros se aplican cuando las claves privadas se crean por primera vez. Por lo tanto, se pueden usar parámetros diferentes para las claves privadas de autoridad de registro (por ejemplo, 4096 bits, protegido por TPM) y de los certificados de usuario en tiempo de ejecución.

Parámetro	Descripción
ProviderLegacyCsp	Cuando tiene el valor True, FAS usará CryptoAPI (CAPI) de Microsoft. De lo contrario, FAS usará la API Cryptography Next Generation (CNG) de Microsoft.
ProviderName	Nombre del proveedor de CAPI o CNG que se va a usar.
ProviderType	Se refiere a Microsoft KeyContainerPermissionAccessEntry.ProviderType Property PROV_RSA_AES 24. Debe ser siempre 24 a menos que esté usando un HSM con CAPI y el proveedor de HSM especifique otra cosa.
KeyProtection	Controla la marca “Exportable”de las claves privadas. También permite el uso del almacenamiento de claves TPM (Trusted Platform Module), si lo admite el hardware.
KeyLength	Longitud de clave para las claves privadas de RSA. Los valores admitidos son 1024, 2048 y 4096 (predeterminado: 2048).

SDK de PowerShell

Aunque la consola de administración de FAS es adecuada para implementaciones simples, la interfaz de PowerShell ofrece opciones más avanzadas. Cuando use opciones que no estén disponibles en la consola, Citrix recomienda utilizar solo PowerShell para la configuración.

El siguiente comando agrega los cmdlets de PowerShell:

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

Use **Get-Help** <*nombre del cmdlet*> para ver la ayuda de uso de los cmdlet. La siguiente tabla muestra algunos comandos donde * representa un verbo estándar de PowerShell (tales como New, Get, Set, Remove).

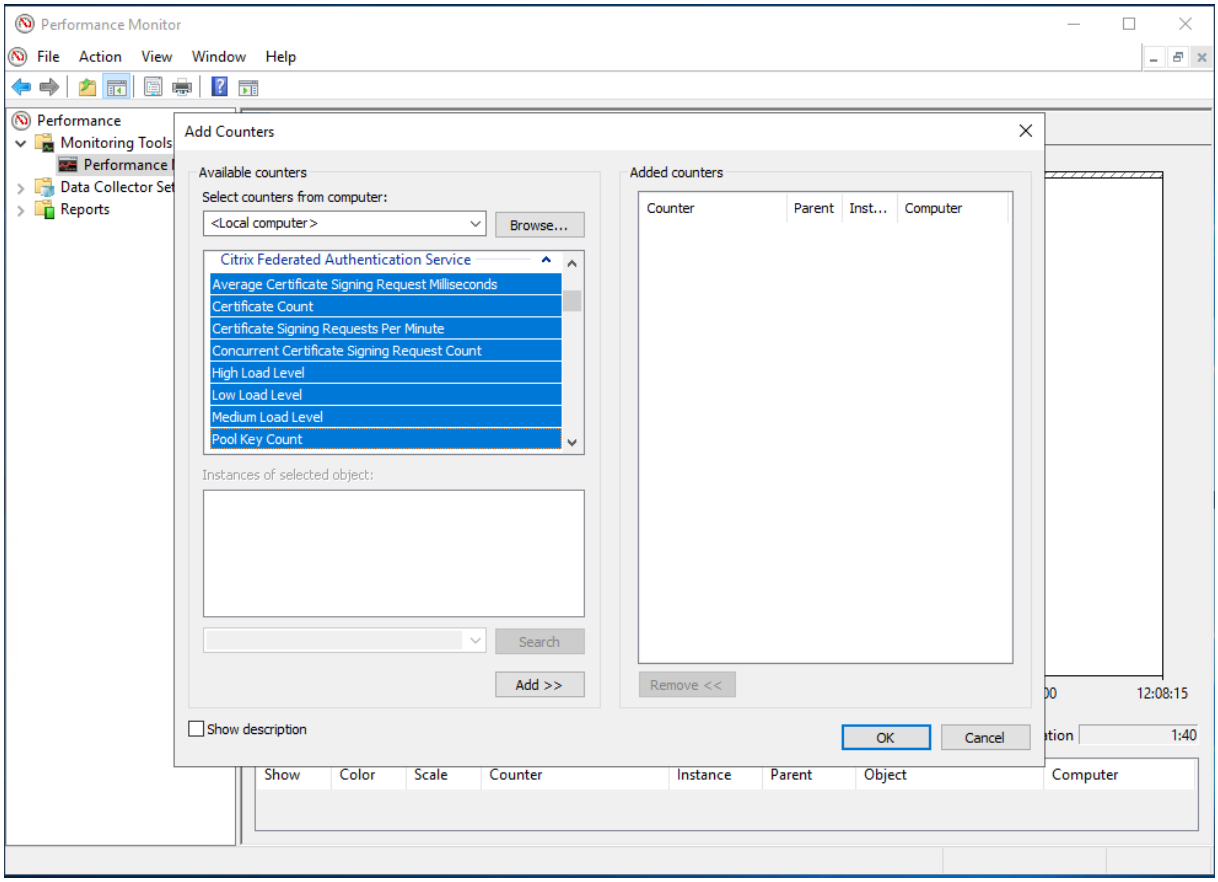
Comandos	Información general
*-FasServer	Muestra y reconfigura los servidores del servicio FAS en el entorno actual.
*-FasAuthorizationCertificate	Administra el certificado de autoridad de registro.
*-FasCertificateDefinition	Controla los parámetros que usa FAS para generar certificados.
*-FasRule	Administra las reglas de usuario configuradas en FAS.
*-FasUserCertificate	Ofrece una lista y administra los certificados que FAS almacena en caché.

Se pueden usar cmdlets de PowerShell de forma remota especificando la dirección de un servidor del servicio FAS.

Para obtener información sobre los cmdlets de PowerShell de FAS, consulte Cmdlets de PowerShell.

Contadores de rendimiento

FAS incluye un conjunto de contadores de rendimiento para el rastreo de la carga.



En la siguiente tabla se muestran los contadores disponibles. La mayoría de estos contadores muestran la media calculada cada cinco minutos.

Name	Descripción
Sesiones activas	Cantidad de conexiones que rastrea FAS.
Concurrent CSRs (Solicitudes de firma de certificado simultáneas)	Cantidad de solicitudes de certificado procesadas al mismo tiempo.
Private Key ops (Operaciones de clave privada)	Cantidad de operaciones de clave privada realizadas por minuto.
Request time (Tiempo de la solicitud)	Tiempo tomado para generar y firmar un certificado.
Certificate Count (Recuento de certificados)	Cantidad de certificados que se almacenan en caché en FAS.
CSR per minute (CSR por minuto)	Cantidad de solicitudes de firma de certificado procesadas por minuto.

Name	Descripción
Low/Medium/High (Baja, media o alta)	Estimaciones de la carga que FAS puede aceptar en las solicitudes de certificado (CSR) por minuto. Si se supera el umbral "Carga alta", el lanzamiento de sesiones puede fallar.

Registros de eventos

Las siguientes tablas contienen las entradas de registro de eventos generadas por FAS.

Eventos de administración [Servicio de autenticación federada]

[Origen del evento: Citrix.Authentication.FederatedAuthenticationService]

Estos eventos se registran como respuesta a un cambio de configuración en el servidor de FAS.

Códigos de registros
[S001] ACCESS DENIED: User [{0}] is not a member of Administrators group
[S002] ACCESS DENIED: User [{0}] is not an Administrator of Role [{1}]
[S003] Administrator [{0}] setting Maintenance Mode to [{1}]
[S004] Administrator [{0}] enrolling with CA [{1}] templates [{2} and {3}]
[S005] Administrator [{0}] de-authorizing CA [{1}]
[S006] Administrator [{0}] creating new Certificate Definition [{1}]
[S007] Administrator [{0}] updating Certificate Definition [{1}]
[S008] Administrator [{0}] deleting Certificate Definition [{1}]
[S009] Administrator [{0}] creating new Role [{1}]
[S010] Administrator [{0}] updating Role [{1}]
[S011] Administrator [{0}] deleting Role [{1}]
[S012] Administrator [{0}] creating certificate [upn: {1} sid: {2} role: {3} Certificate Definition: {4} Security Context: {5}]
[S013] Administrator [{0}] deleting certificates [upn: {1} role: {2} Certificate Definition: {3} Security Context: {4}]
[S015] Administrator [{0}] creating certificate request [TPM: {1}]
[S016] Administrator [{0}] importing Authorization certificate [Reference: {1}]

Códigos de registros

Códigos de registros
[S401] Performing configuration upgrade –[From version {0} to version {1}]
[S402] ERROR: The Citrix Federated Authentication Service must be run as Network Service [currently running as: {0}]
[S404] Forcefully erasing the Citrix Federated Authentication Service database
[S405] An error occured while migrating data from the registry to the database: [{0}]
[S406] Migration of data from registry to database is complete (note: user certificates are not migrated)
[S407] Registry-based data was not migrated to a database since a database already existed
[S408] Cannot downgrade the configuration –[From version {0} to version {1}]
[S409] ThreadPool MinThreads adjusted from [workers: {0} completion: {1}] to: [workers: {2} completion: {3}]
[S410] Failed to adjust ThreadPool MinThreads from [workers: {0} completion: {1}] to: [workers: {2} completion: {3}]

Creación de aserciones de identidad [Servicio de autenticación federada]

[Origen del evento: Origen del evento: Citrix.Authentication.FederatedAuthenticationService]

Estos eventos se registran en tiempo de ejecución en el servidor de FAS cuando un servidor de confianza declara un inicio de sesión de usuario.

Códigos de registros
[S101] Server [{0}] is not authorized to assert identities in role [{1}]
[S102] Server [{0}] failed to assert UPN [{1}] (Exception: {2}{3})
[S103] Server [{0}] requested UPN [{1}] SID {2}, but lookup returned SID {3}
[S104] Server [{0}] failed to assert UPN [{1}] (UPN not allowed by role [{2}])
[S105] Server [{0}] issued identity assertion [upn: {1}, role {2}, Security Context: [{3}]]
[S120] Issuing certificate to [upn: {0} role: {1} Security Context: [{2}]]
[S121] Certificate issued to [upn: {0} role: {1}] by [certifcate authority: {2}]

Códigos de registros
[S122] Warning: Server is overloaded [upn: {0} role: {1}][Requests per minute {2}].
[S123] Failed to issue a certificate for [upn: {0} role: {1}] [exception: {2}]
[S124] Failed to issue a certificate for [upn: {0} role: {1}] at [certifcate authority: {2}] [exception: {3}]

Actuando como usuario de confianza [Servicio de autenticación federada]

[Origen del evento: Origen del evento: Citrix.Authentication.FederatedAuthenticationService]

Estos sucesos se registran durante el tiempo de ejecución en el servidor de FAS cuando un VDA inicia la sesión de un usuario.

Códigos de registros
[S201] Relying party [{0}] does not have access to a password.
[S202] Relying party [{0}] does not have access to a certificate.
[S203] Relying party [{0}] does not have access to the Logon CSP
[S204] Relying party [{0}] accessing the Logon CSP for [upn: {1}] in role: [{2}] [Operation: {3}] as authorized by [{4}]
[S205] Calling account [{0}] is not a relying party in role [{1}]
[S206] Calling account [{0}] is not a relying party
[S208] Private Key operation failed [Operation: {0} upn: {1} role: {2} certificateDefinition {3} Error {4} {5}].

Servidor de certificados de sesión [Servicio de autenticación federada]

[Origen del evento: Origen del evento: Citrix.Authentication.FederatedAuthenticationService]

Estos sucesos se registran en el servidor de FAS cuando un usuario utiliza un certificado de sesión.

Códigos de registros
[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}]

Códigos de registros
[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}].

Plug-in de aserción de FAS [Servicio de autenticación federada]

[Origen del evento: Origen del evento: Citrix.Authentication.FederatedAuthenticationService]

El plug-in de la aserción de FAS registra estos eventos.

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

Inicio de sesión [VDA]

[Origen del evento: Citrix.Authentication.IdentityAssertion]

Estos sucesos se registran en el VDA durante la fase de inicio de sesión.

Códigos de registros
[S101] Identity Assertion Logon failed. Unrecognised Federated Authentication Service [id: {0}]
[S102] Identity Assertion Logon failed. Could not lookup SID for {0} [Exception: {1}{2}]
[S103] Identity Assertion Logon failed. User {0} has SID {1}, expected SID {2}
[S104] Identity Assertion Logon failed. Failed to connect to Federated Authentication Service: {0} [Error: {1} {2}]
[S105] Identity Assertion Logon. Logging in [Username: {0} Domain: {1}]
[S106] Identity Assertion Logon. Logging in [Certificate: {0}]
[S107] Identity Assertion Logon failed. [Exception: {0}{1}]
[S108] Identity Assertion Subsystem. ACCESS_DENIED [Caller: {0}]

Certificados de sesión [VDA]

[Origen del evento: Citrix.Authentication.IdentityAssertion]

Estos sucesos se registran en el VDA cuando un usuario intenta usar un certificado de sesión.

Códigos de registros
[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

Generación de pares de claves y solicitudes de certificados [Servicio de autenticación federada]

[Origen del evento: Citrix.Fas.PkiCore]

Estos eventos se registran cuando el servidor de FAS realiza operaciones criptográficas de bajo nivel.

Códigos de registros
[S001] TrustArea::TrustArea: Installed certificate [TrustArea: {0}] [Certificate {1} TrustAreaJoinParameters{2}

Códigos de registros
[S014] Pkcs10Request::Create: Created PKCS10 request [Distinguished Name {0}]
[S016] PrivateKey::Create [Identifier {0} MachineWide: {1} Provider: {2} ProviderType: {3}EllipticCurve: {4} KeyLength: {5} isExportable: {6}]
[S017] PrivateKey::Delete [CspName: {0}, Identifier {1}]

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

Información relacionada

- Las implementaciones más comunes de FAS se resumen en Arquitecturas de implementación.
- En Configuración avanzada, se presentan artículos de procedimientos.

Arquitecturas de implementación

March 30, 2023

Introducción

El Servicio de autenticación federada FAS (Federated Authentication Service) es un componente de Citrix que se integra con su entidad de certificación de Active Directory, lo que permite a los usuarios autenticarse de manera imperceptible dentro de un entorno Citrix. Este documento describe diversas arquitecturas de autenticación que pueden ser apropiadas para su implementación.

Cuando está habilitado, FAS delega las decisiones de autenticación de usuarios en servidores de StoreFront de confianza. StoreFront tiene un amplio conjunto de opciones de autenticación integrado con tecnologías Web modernas y es fácilmente ampliable con el SDK de StoreFront o complementos de IIS de terceros. El objetivo básico del diseño es conseguir que cualquier tecnología de autenticación

que pueda autenticar a un usuario en un sitio web se pueda usar para iniciar sesión en una implementación de Citrix Virtual Apps o Citrix Virtual Desktops.

Este documento contiene algunos ejemplos de implementación de nivel superior, con una complejidad cada vez mayor.

- Implementación interna
- Implementación de Citrix Gateway
- SAML de ADFS
- Asignación de cuentas B2B
- Unión a Azure AD de Windows 10

Se proporcionan enlaces a artículos relativos al servicio FAS. Para todas las arquitecturas, el artículo Instalación y configuración es la referencia principal para la instalación y la configuración de FAS.

Funcionamiento

FAS tiene autorización para emitir automáticamente certificados de tarjeta inteligente de parte de los usuarios de Active Directory que StoreFront autentica. Esto usa interfaces API similares a las herramientas que permiten a los administradores aprovisionar tarjetas inteligentes físicas.

Cuando un broker gestiona el acceso de un usuario a un Virtual Delivery Agent (VDA) de Citrix Virtual Apps o Citrix Virtual Desktops, el certificado se conecta a la máquina, y el dominio de Windows detecta el inicio de sesión como una acción de autenticación con tarjeta inteligente estándar.

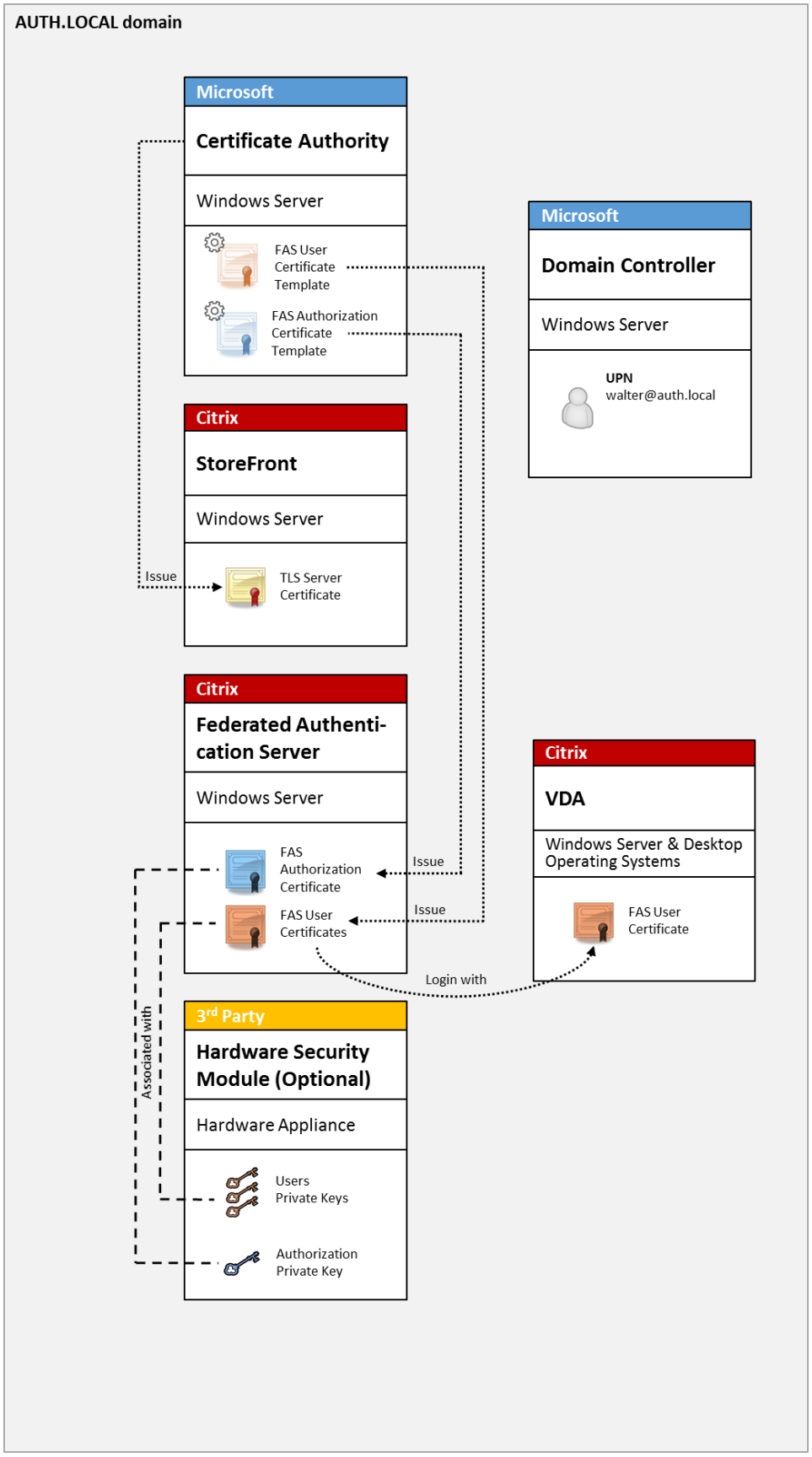
Implementación interna

FAS permite que los usuarios se autentiquen de forma segura en StoreFront con una gran variedad de opciones de autenticación (incluido el inicio de sesión Single Sign-On de Kerberos) y se conecten con una sesión de Citrix HDX con autenticación completa.

Esto permite la autenticación de Windows sin diálogos para introducir las credenciales de usuario o el PIN de tarjeta inteligente, y sin tener que usar la función del tipo "administración de contraseñas guardadas", tales como Single Sign-On Service. Puede utilizarse para reemplazar las funciones de inicio de sesión que ofrezca la Delegación limitada de Kerberos, disponible en versiones anteriores de Citrix Virtual Apps.

Todos los usuarios tienen acceso a certificados de infraestructura de clave pública (PKI) dentro de su sesión, independientemente de si inician sesión en los dispositivos de punto final con una tarjeta inteligente o no. Esto permite una migración sin problemas a modelos de autenticación de dos factores, incluso desde dispositivos como smartphones y tabletas que no tienen un lector de tarjeta inteligente.

Esta implementación agrega un nuevo servidor en el que se ejecuta FAS, que tiene autorización para emitir certificados de clase de tarjeta inteligente en nombre de los usuarios. Estos certificados se utilizan después para conectar con sesiones de usuario en un entorno de Citrix HDX como si se estuviera utilizando un inicio de sesión con tarjeta inteligente.



El entorno de Citrix Virtual Apps o Citrix Virtual Desktops debe estar configurado de manera similar al inicio de sesión con tarjeta inteligente, que se describe en CTX206156.

En una implementación existente, esto normalmente solo implica asegurarse de que haya una entidad de certificación de Microsoft disponible y de que los controladores de dominio tengan asignados certificados de controlador de dominio (consulte la sección "Issuing Domain Controller Certificates" en el artículo CTX206156).

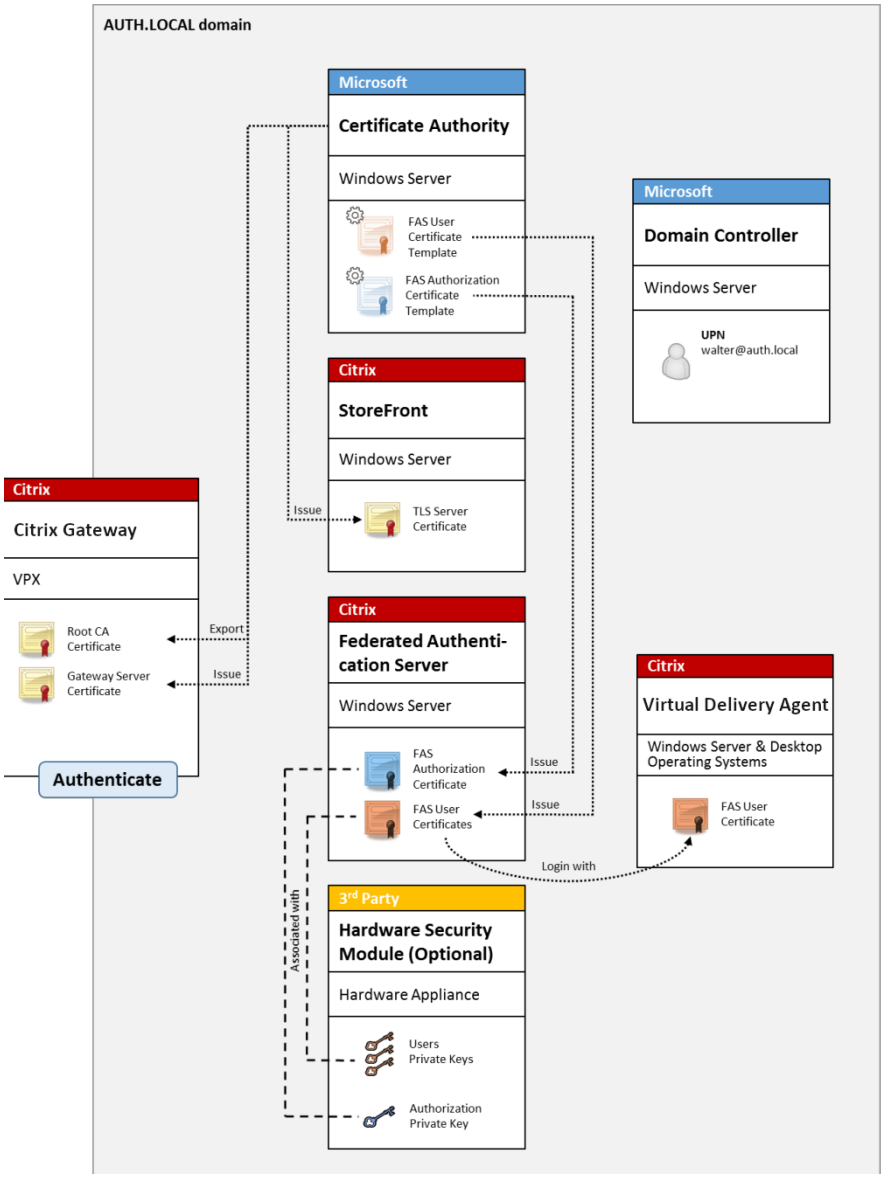
Información relacionada:

- Las claves se pueden almacenar en un módulo de seguridad de hardware (HSM) o en un módulo de plataforma de confianza (TPM) integrado. Para obtener más información, consulte el artículo Protección de claves privadas.
- En el artículo Instalación y configuración se describe cómo instalar y configurar el servicio FAS.

Implementación de Citrix Gateway

La implementación de Citrix Gateway es similar a la implementación interna, pero agrega Citrix Gateway emparejado con StoreFront, moviendo el punto principal de autenticación a Citrix Gateway. Citrix Gateway incluye opciones muy sofisticadas de autenticación y autorización que se pueden usar para el acceso remoto seguro a los sitios web de una empresa.

Esta implementación se puede utilizar para evitar la aparición de varias solicitudes de PIN que ocurren al autenticarse primero en Citrix Gateway y, a continuación, iniciar sesión en una sesión de usuario. También permite el uso de las tecnologías avanzadas de autenticación de Citrix Gateway, sin necesidad de pedir adicionalmente contraseñas de Active Directory o tarjetas inteligentes.

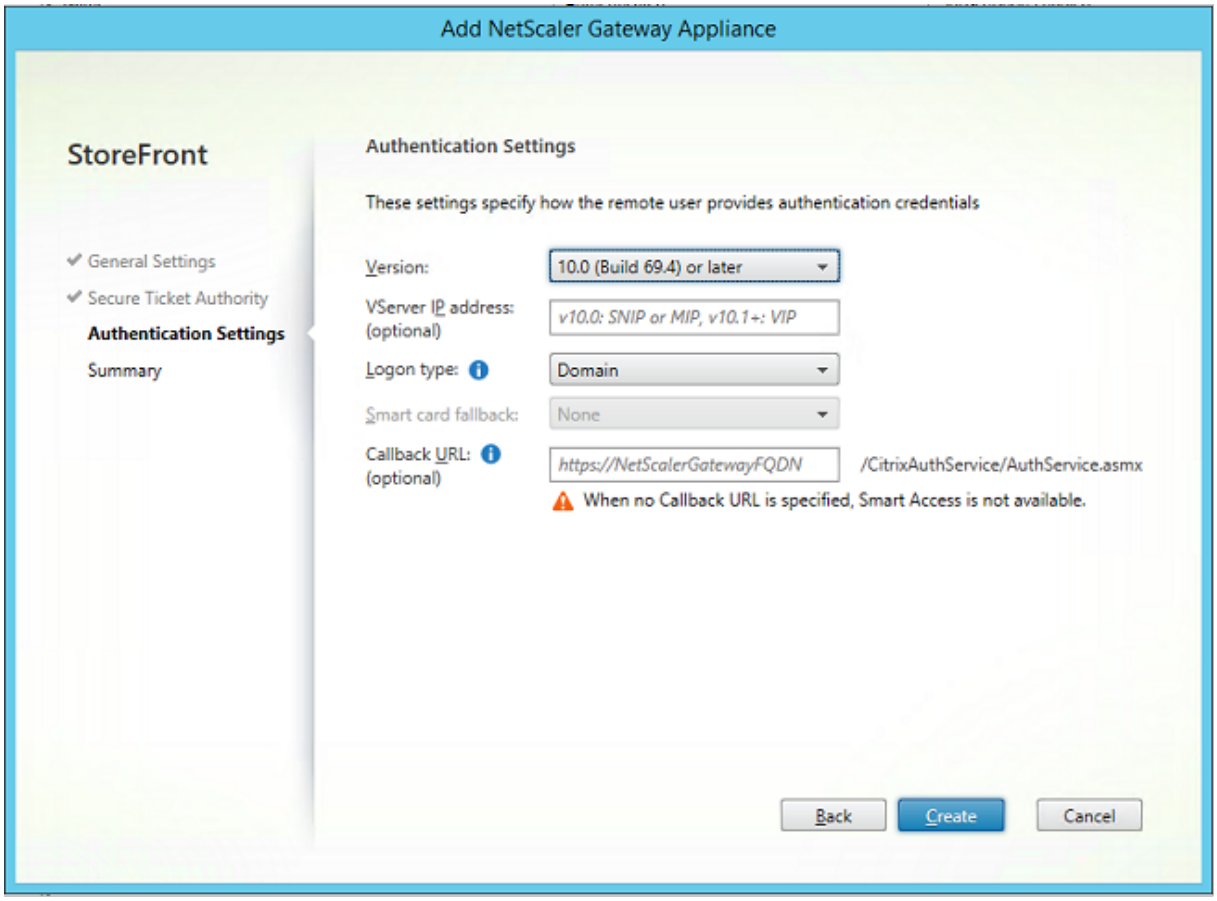


El entorno de Citrix Virtual Apps o Citrix Virtual Desktops debe estar configurado de manera similar al inicio de sesión con tarjeta inteligente, que se describe en CTX206156.

En una implementación existente, esto normalmente solo implica asegurarse de que haya una entidad de certificación de Microsoft disponible y de que los controladores de dominio tengan asignados certificados de controlador de dominio (consulte la sección "Issuing Domain Controller Certificates" del artículo CTX206156).

Al configurar Citrix Gateway como el sistema de autenticación principal, compruebe que todas las conexiones entre Citrix Gateway y StoreFront estén protegidas con TLS. En concreto, compruebe que la URL de respuesta está configurada para que apunte al servidor Citrix Gateway, ya que puede usarse

para autenticar el servidor Citrix Gateway en esta implementación.

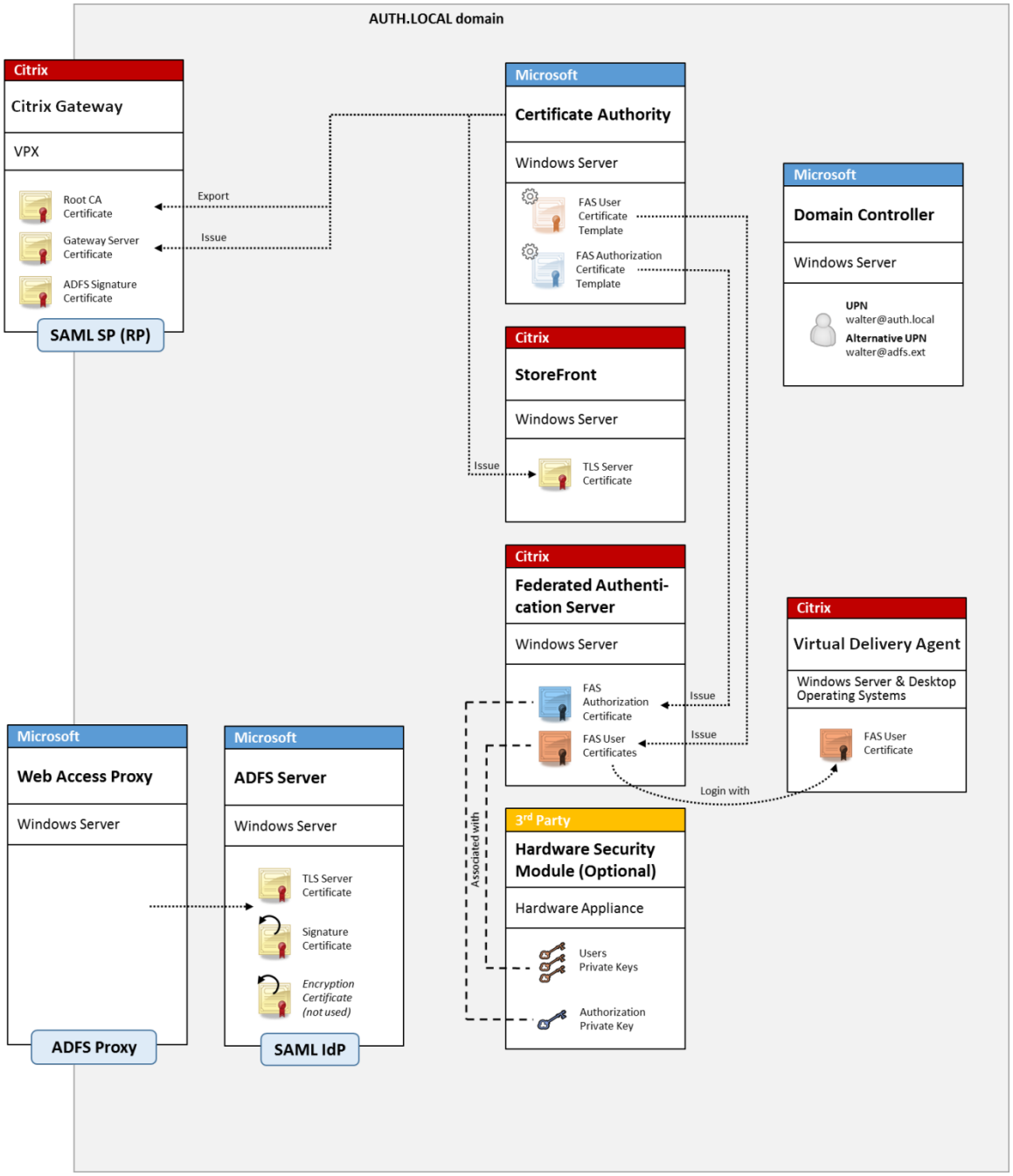


Información relacionada:

- Para configurar Citrix Gateway, consulte "Cómo configurar NetScaler Gateway 10.5 para usarlo con StoreFront 3.6 y Citrix Virtual Desktops 7.6".
- En Instalación y configuración se describe cómo instalar y configurar el servicio FAS.

Implementación de SAML de ADFS

Una tecnología de autenticación clave de Citrix Gateway permite la integración en Microsoft ADFS, que puede funcionar como un proveedor de identidades (IdP) SAML. Una aserción SAML es un bloque XML firmado criptográficamente, emitido por un IdP de confianza, que autoriza a un usuario a iniciar sesión en un sistema informático. Eso significa que el servidor de FAS permite delegar la autenticación de un usuario al servidor de ADFS de Microsoft (o a otro IdP habilitado para SAML).



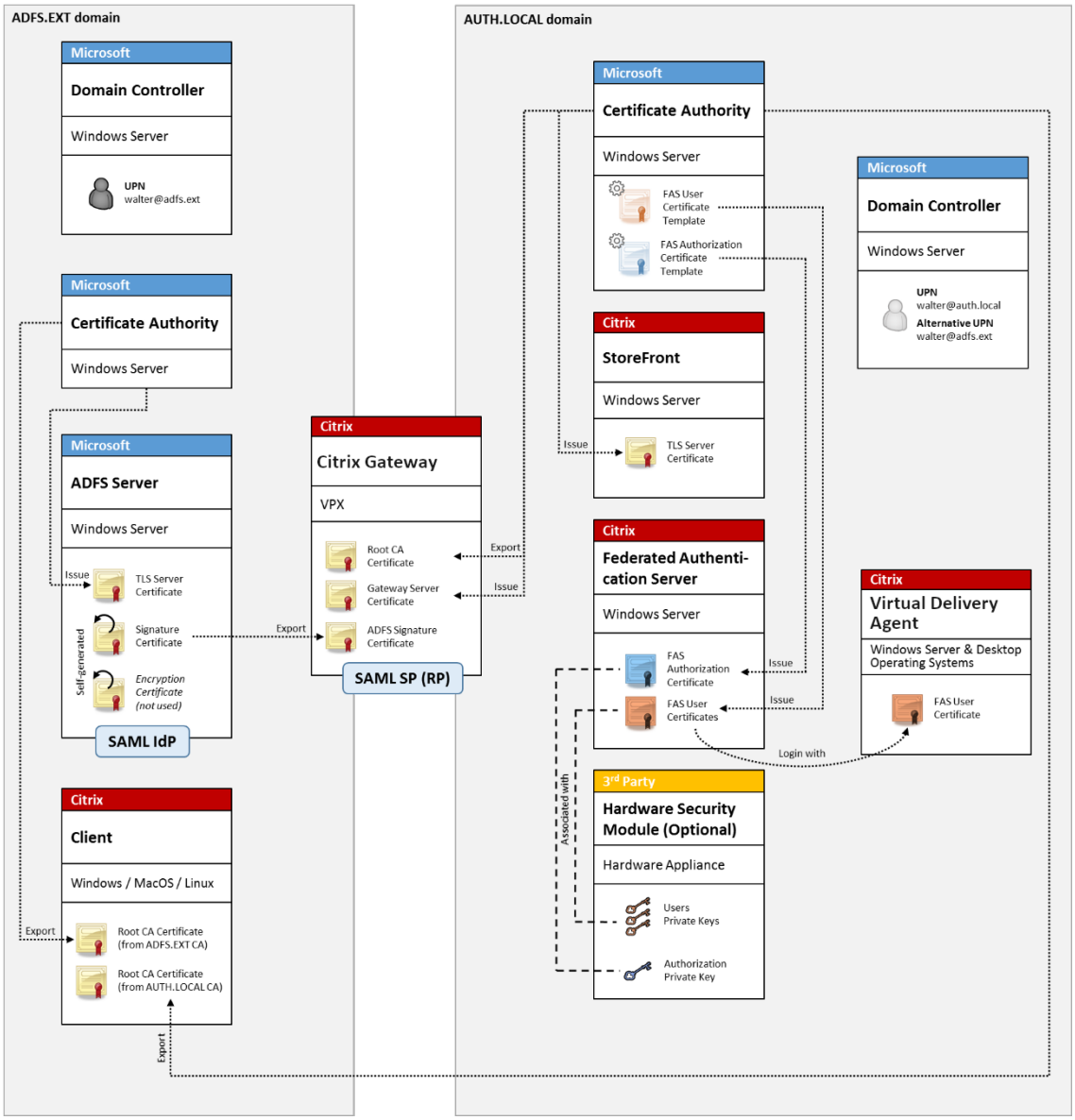
ADFS se usa normalmente para autenticar a los usuarios con seguridad de forma remota en los recursos de la empresa a través de Internet, por ejemplo, se usa para la integración de Office 365.

Información relacionada:

- El artículo Implementación ADFS contiene información detallada.
- En el artículo Instalación y configuración se describe cómo instalar y configurar el servicio FAS.
- La sección Implementación de Citrix Gateway en este artículo contiene información acerca de la configuración.

Asignación de cuentas B2B

Si dos empresas desean usar los sistemas informáticos de la otra, una opción común es configurar un servidor de ADFS (Servicio de federación de Active Directory) con una relación de confianza. Eso permite que los usuarios de una empresa se autentiquen en el entorno de Active Directory (AD) de la otra, de manera imperceptible. Al iniciar sesión, cada usuario utiliza las credenciales de su propia empresa; ADFS las asigna automáticamente a una "cuenta sombra"en el entorno de AD de la otra empresa.

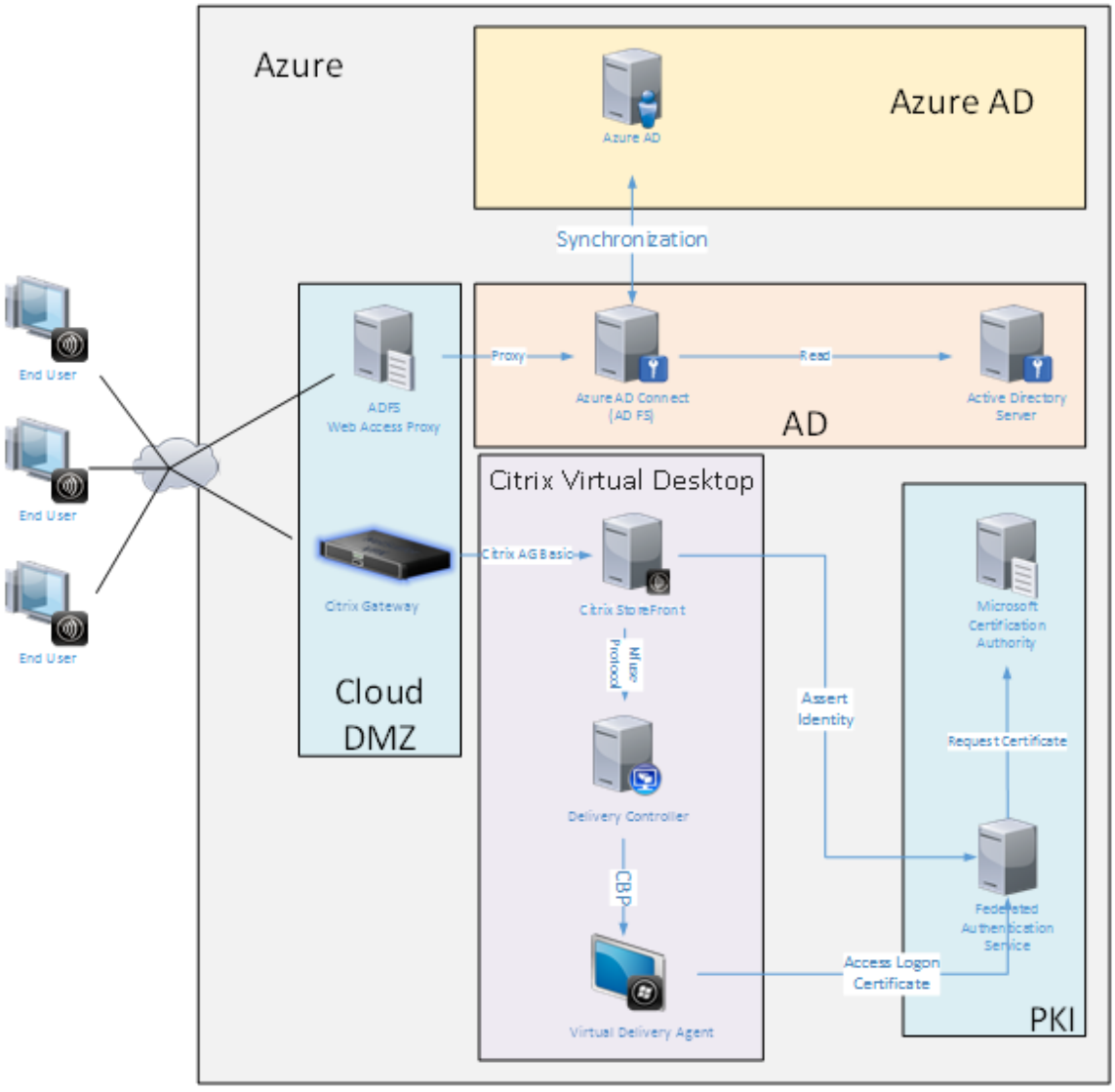


Información relacionada:

- En el artículo Instalación y configuración se describe cómo instalar y configurar el servicio FAS.

Unión a Azure AD de Windows 10

Windows 10 introdujo el concepto de "Unión a Azure AD", que es conceptualmente similar a la unión a un dominio Windows tradicional, solo que destinado a casos a través de Internet. Este sistema funciona bien con equipos portátiles y tabletas. Al igual que al unirse a un dominio de Windows tradicional, Azure AD tiene funciones para permitir modelos de inicio de sesión Single Sign-On en recursos y sitios Web de la empresa. Estos pueden funcionar con Internet, por lo que funcionarán desde cualquier ubicación que esté conectada a Internet, no solo la red LAN de la oficina.



Esta implementación es un ejemplo donde no existe el concepto de "usuarios finales en la oficina". Los equipos portátiles se inscriben y se autentican totalmente en Internet con las funciones modernas de Azure AD.

Tenga en cuenta que la infraestructura de esta implementación se puede ejecutar en cualquier lugar

en que haya disponible una dirección IP: local, proveedor alojado, Azure u otro proveedor de la nube. El sincronizador de Azure AD Connect se conectará automáticamente a Azure AD. El gráfico de ejemplo utiliza máquinas virtuales de Azure para simplificar la tarea.

Información relacionada:

- En el artículo Instalación y configuración se describe cómo instalar y configurar el servicio FAS.
- El artículo Integración de Azure AD contiene información detallada.

Implementación ADFS

March 30, 2023

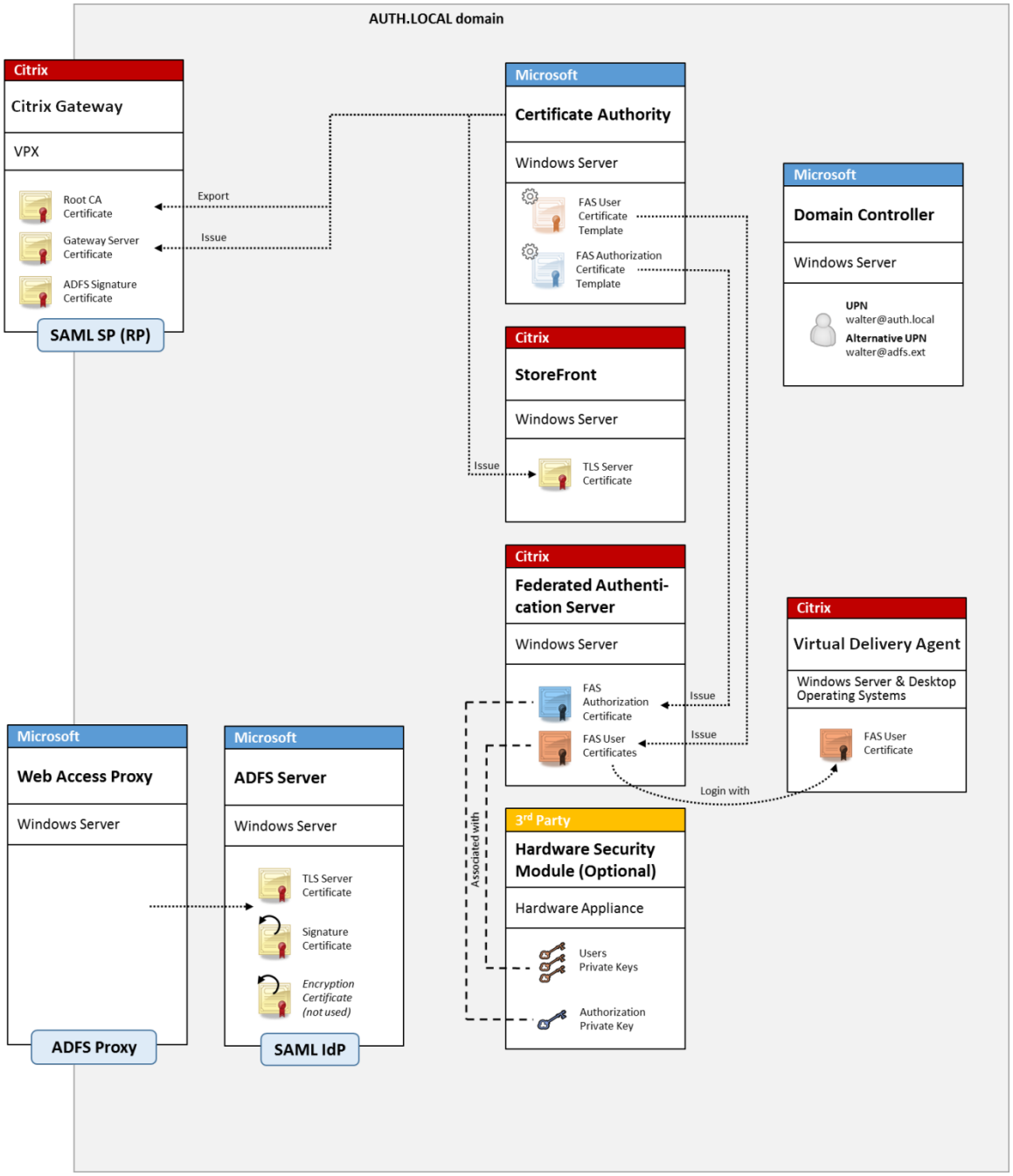
Introducción

Este documento describe cómo integrar un entorno de Citrix con Microsoft ADFS.

Muchas organizaciones usan ADFS para administrar el acceso seguro de los usuarios a los sitios web que requieren un único punto de autenticación. Por ejemplo, una empresa puede tener descargas y contenido adicionales disponibles para los empleados; estas ubicaciones deben estar protegidas con credenciales de inicio de sesión estándar de Windows.

El Servicio de autenticación federada (FAS) también permite integrar Citrix Gateway y Citrix StoreFront en el sistema de inicio de sesión de ADFS, lo que disminuye el riesgo de confusión para el personal de la empresa.

Esta implementación integra Citrix Gateway como una entidad de confianza en Microsoft ADFS.



> **Nota:**
>
> No hay ninguna diferencia si el recurso del back-end es Windows VDA o Linux VDA.

Descripción general de SAML

Security Assertion Markup Language (SAML) es un sistema sencillo de inicio de sesión con explorador web para "redirigir a la página de inicio de sesión". La configuración incluye los siguientes elemen-

tos:

Dirección URL de redireccionamiento [URL del servicio Single Sign-On]

Cuando Citrix Gateway detecta que un usuario tiene que autenticarse, indica al explorador web del usuario que haga un envío HTTP POST a la página web de inicio de sesión de SAML en el servidor de ADFS. Esta suele ser una dirección `https://` en el formato: `https://adfs.mycompany.com/adfs/ls`.

Este POST a la página web incluye información adicional, incluida la dirección de devolución adonde ADFS llevará al usuario cuando se complete el inicio de sesión.

Identificador [Nombre del emisor/ID de entidad]

El ID de entidad (EntityId) es un identificador único que Citrix Gateway incluye en los datos de POST enviados a ADFS. Eso informa al servicio ADFS acerca del servicio en el que intenta iniciar sesión el usuario, para aplicar distintas directivas de autenticación según corresponda. Si se emite, el XML de autenticación de SAML solo servirá para iniciar sesión en el servicio identificado por EntityId.

EntityID suele ser la dirección URL de la página de inicio de sesión del servidor Citrix Gateway, pero puede ser cualquier otra cosa, siempre y cuando Citrix Gateway y ADFS lo acuerden: `https://ns.mycompany.com/application/logonpage`.

Dirección de devolución [dirección URL de respuesta]

Si la autenticación se realiza correctamente, ADFS indica al explorador web del usuario que envíe con POST un XML de autenticación de SAML de vuelta a una de las URL de respuesta que están configuradas para EntityId. Esta suele ser una dirección `https://` en el servidor Citrix Gateway original con el formato: `https://ns.mycompany.com/cgi/samlauth`.

Si hay más de una URL de respuesta configurada, Citrix Gateway puede elegir una en su POST original para ADFS.

Certificado de firma [Certificado IDP]

ADFS firma criptográficamente los objetos blob (Binary Large Object) de XML de autenticación de SAML mediante su clave privada. Para validar la firma, Citrix Gateway debe estar configurado para comprobar las firmas mediante una clave pública que se incluye en un archivo de certificado. El archivo de certificado suele ser un archivo de texto obtenido del servidor de ADFS.

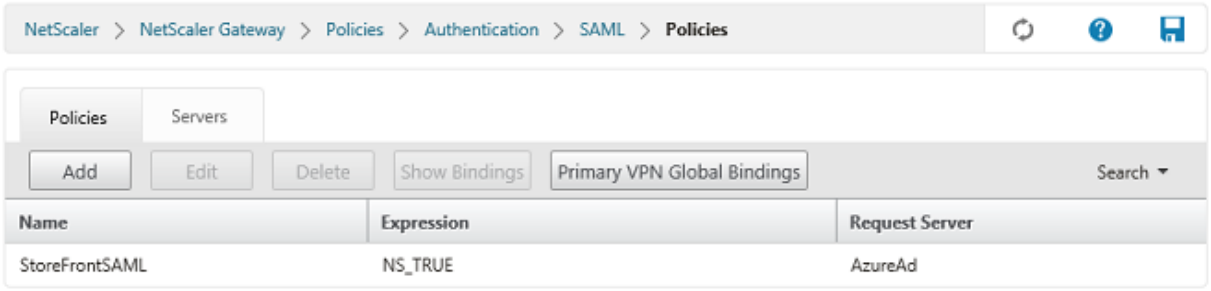
URL de Single Sign-Out [URL de cierre de sesión único]

ADFS y Citrix Gateway ofrecen un sistema de "cierre de sesión central". Se trata de una dirección URL que Citrix Gateway sondea ocasionalmente para comprobar que el blob XML de autenticación SAML aún representa una sesión conectada.

Esta es una función opcional; no es necesario que esté configurada. Esta suele ser una dirección `https://` en el formato: `https://adfs.mycompany.com/adfs/logout`. (Tenga en cuenta que puede ser la misma que la dirección URL de inicio de sesión único.)

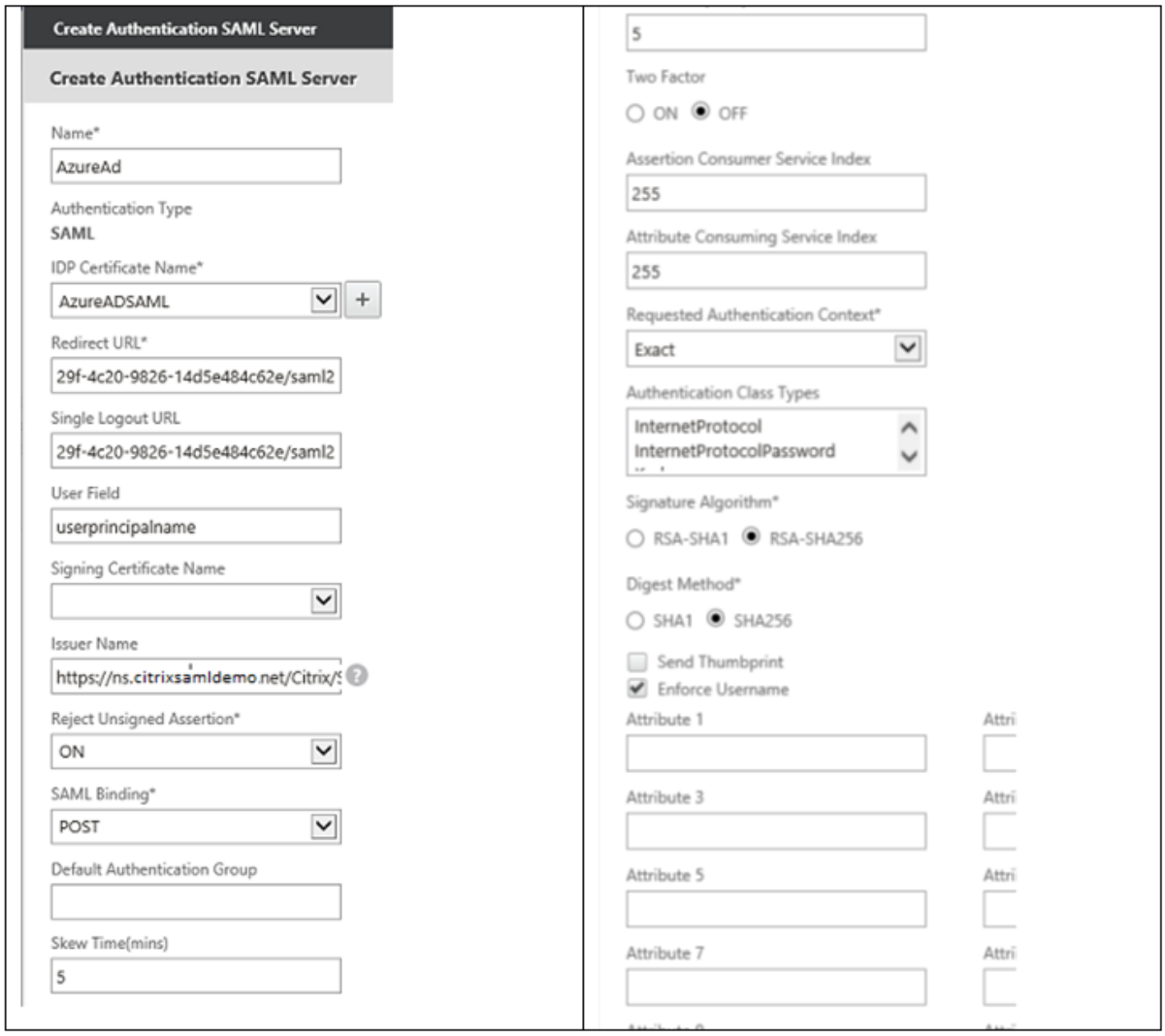
Configuración

En la sección Implementación de Citrix Gateway se describe cómo configurar Citrix Gateway para gestionar las opciones de autenticación LDAP estándar. Una vez completado correctamente, se puede crear una nueva directiva de autenticación en Citrix Gateway que permita la autenticación SAML. Después, esto puede reemplazar la directiva LDAP predeterminada utilizada en el asistente de instalación de Citrix Gateway.



Rellenar la directiva de SAML

Configure el nuevo servidor de proveedor de identidades SAML mediante la información tomada anteriormente de la consola de administración de ADFS. Cuando se aplica esta directiva, Citrix Gateway redirige al usuario a ADFS para el inicio de sesión y a su vez acepta el token de autenticación de SAML firmado por ADFS.



Información relacionada

- Instalación y configuración es la referencia principal para la instalación y la configuración de este servicio.
- Las implementaciones más comunes de FAS se resumen en el artículo Arquitecturas de implementación.
- En Configuración avanzada, se presentan artículos de "procedimientos".

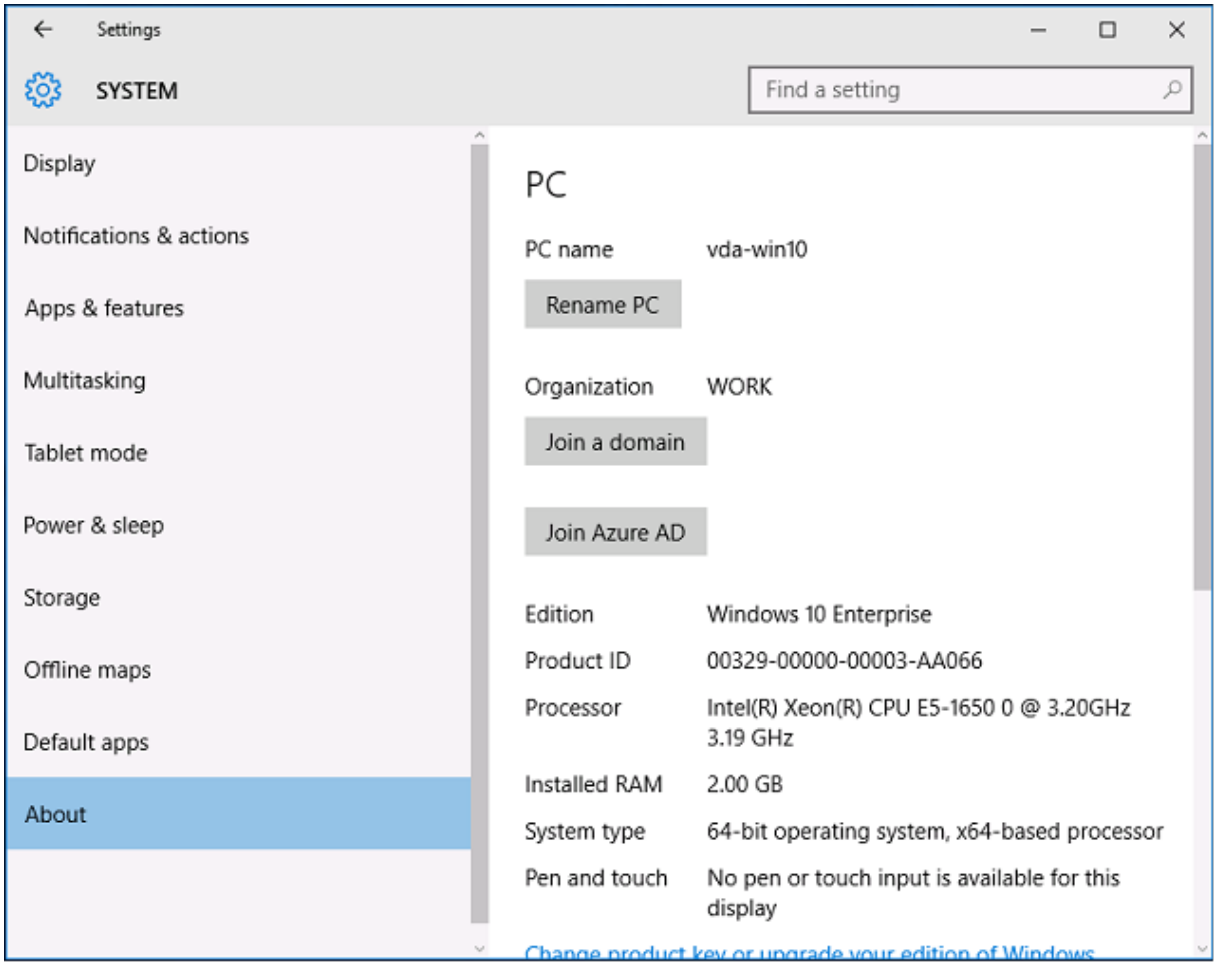
Integración de Azure AD

March 30, 2023

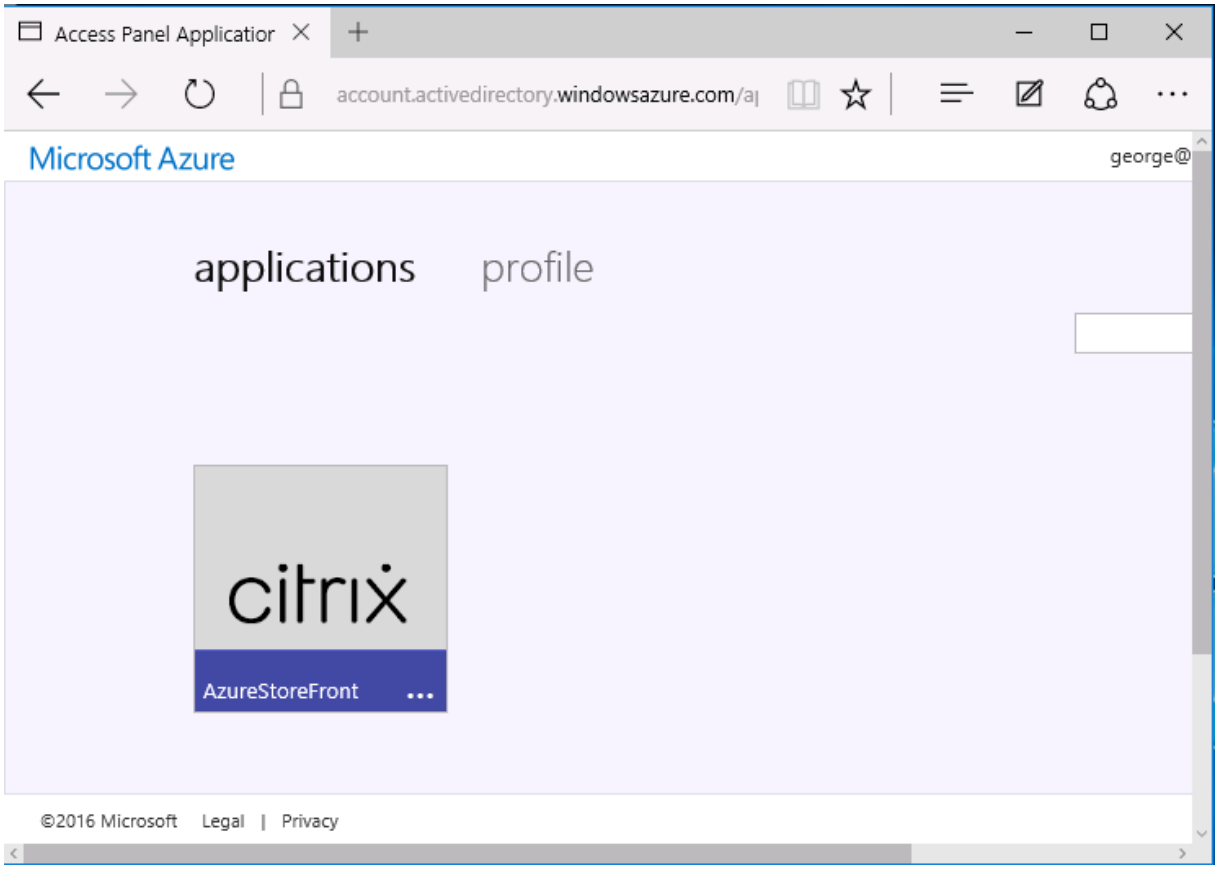
Introducción

Este documento describe cómo integrar un entorno de Citrix con la funcionalidad de Azure AD de Windows 10. Windows 10 introdujo Azure AD, que es un nuevo modelo para unirse a dominios, por el cual los portátiles móviles pueden unirse a un dominio de empresa a través de Internet con fines de administración y Single Sign-On.

El ejemplo de implementación en este documento describe un sistema donde TI proporciona a los nuevos usuarios una dirección de correo electrónico de la empresa y un código de inscripción para sus portátiles Windows 10 personales. Los usuarios acceden a este código mediante la opción **Sistema > Acerca de > Unirse a Azure AD** del panel **Configuración**.



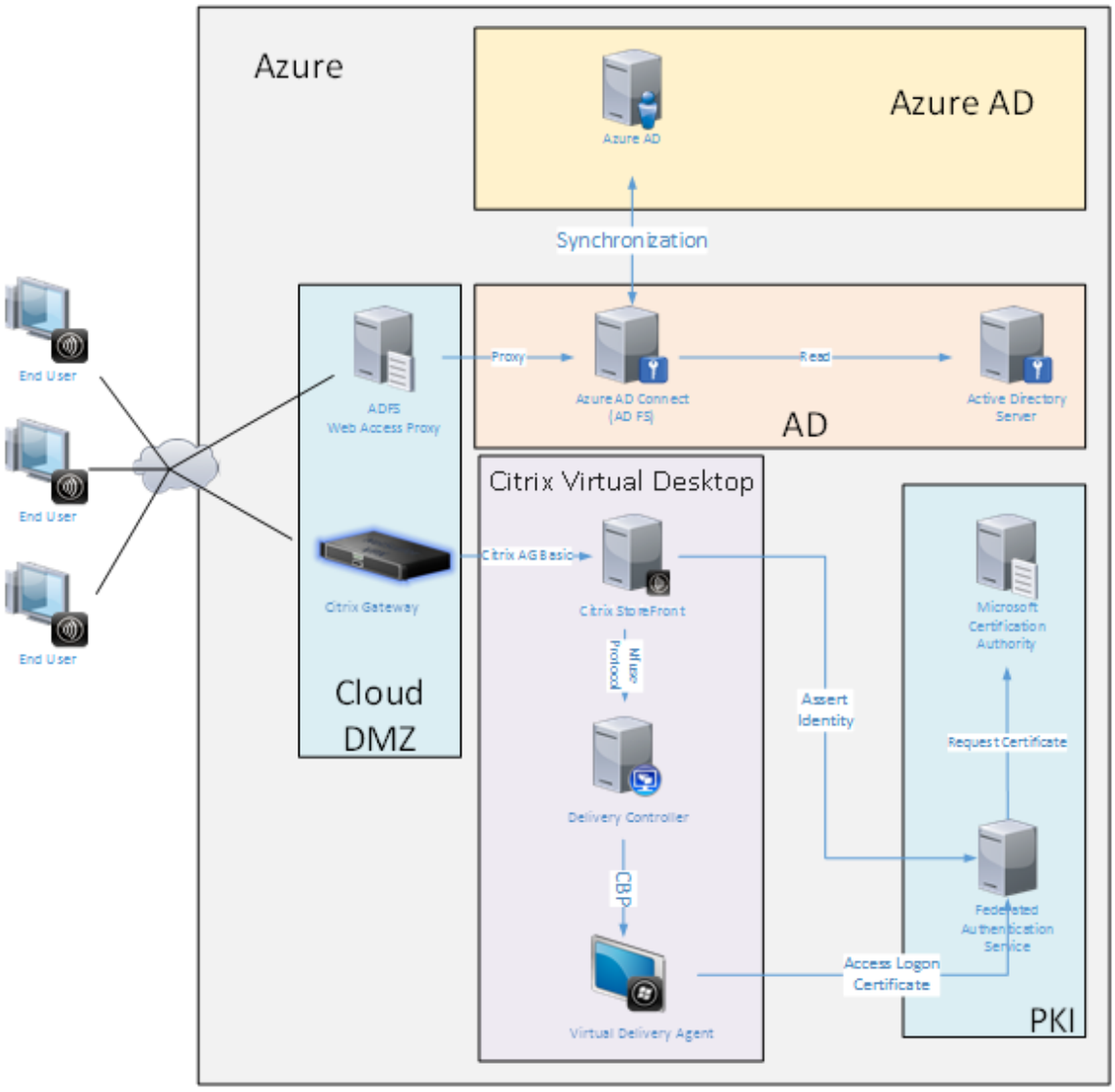
Una vez inscrito el portátil, el explorador web Microsoft Edge inicia sesión automáticamente en los sitios web de la empresa y las aplicaciones publicadas de Citrix a través de la página web de aplicaciones SaaS de Azure, con otras aplicaciones de Azure, como Office 365.



Arquitectura

Esta arquitectura replica una red de empresa tradicional incluida totalmente dentro de Azure, integrada con tecnologías de nube modernas, tales como Azure AD y Office 365. Los usuarios finales se consideran todos trabajadores remotos, sin concepto de estar en una intranet de la oficina.

El modelo se puede aplicar a las empresas con sistemas existentes en las propias sedes, porque Azure Connect Synchronization puede establecer un puente con Azure a través de Internet.



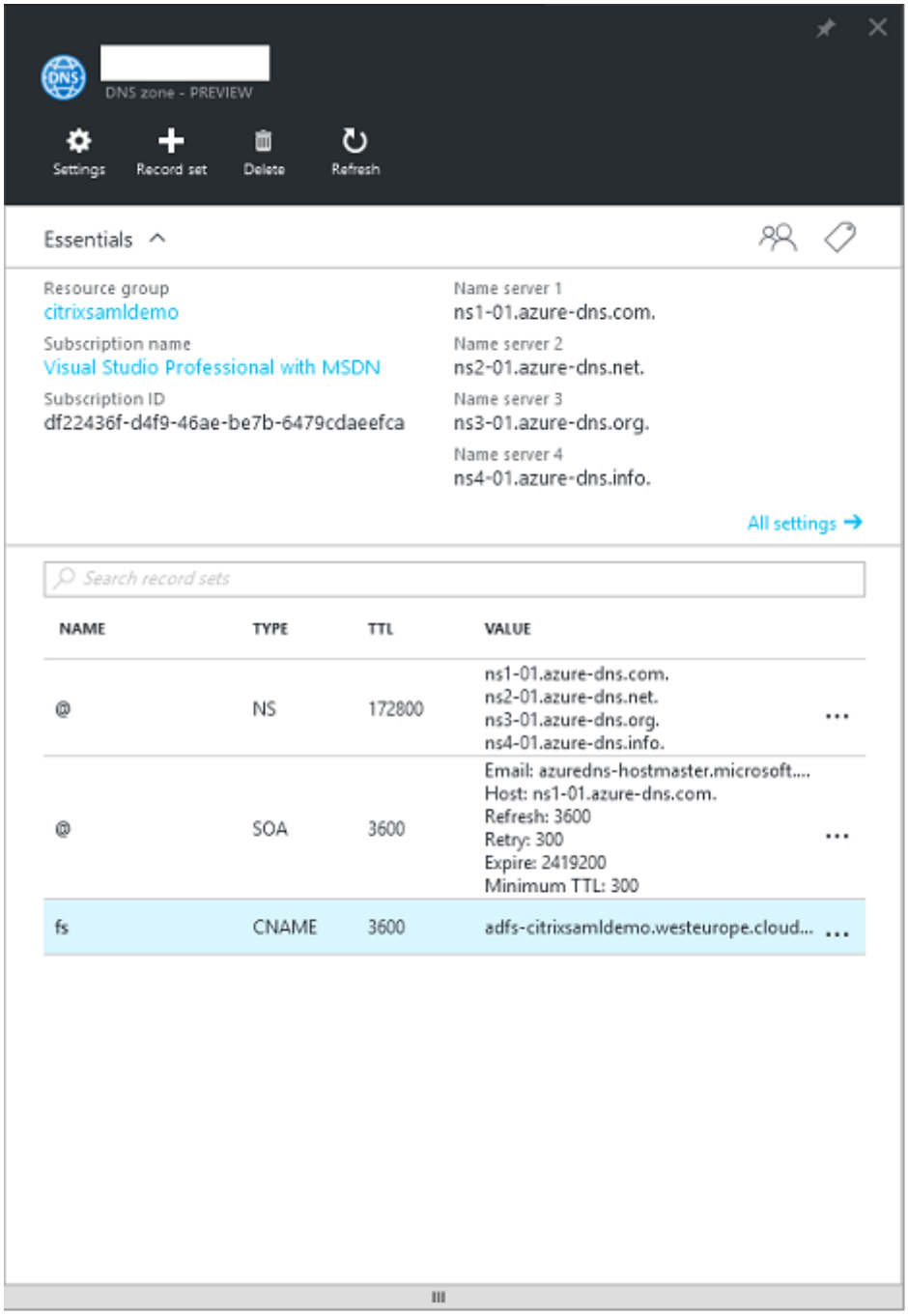
Las conexiones seguras y Single Sign-On, que tradicionalmente se habrían establecido con autenticación Kerberos/NTLM y LAN con firewall, se sustituyen en esta arquitectura con conexiones TLS hacia Azure y SAML. Se crean nuevos servicios a medida que nuevas aplicaciones de Azure se unen a Azure AD. Las aplicaciones que requieren Active Directory (por ejemplo, una base de datos de SQL Server) se pueden ejecutar mediante una VM estándar de servidor de Active Directory en la porción de IAAS del Servicio de nube de Azure.

Cuando un usuario inicia una aplicación tradicional, el acceso tiene lugar mediante aplicaciones publicadas de Citrix Virtual Apps and Desktops. Los diferentes tipos de aplicaciones se intercalan a través de la página **Aplicaciones de Azure** del usuario con la ayuda de las funciones Single Sign-On de Microsoft Edge. Microsoft también proporciona aplicaciones de iOS y Android que pueden enumerar e iniciar aplicaciones de Azure.

Crear una zona DNS

Azure AD requiere que el administrador haya registrado una dirección DNS pública y controla la zona de delegación para el sufijo de nombre de dominio. Para realizar esta acción, el administrador puede usar la función de zona DNS en Azure.

En este ejemplo, se usa la zona DNS con el nombre *citrixsamldemo.net*.



La consola muestra los nombres de los servidores DNS de Azure. Estos deben constar en las entradas

NS del registrador DNS de la zona (por ejemplo: `citrixsamldemo.net. NS n1-01.azure-dns.com`).

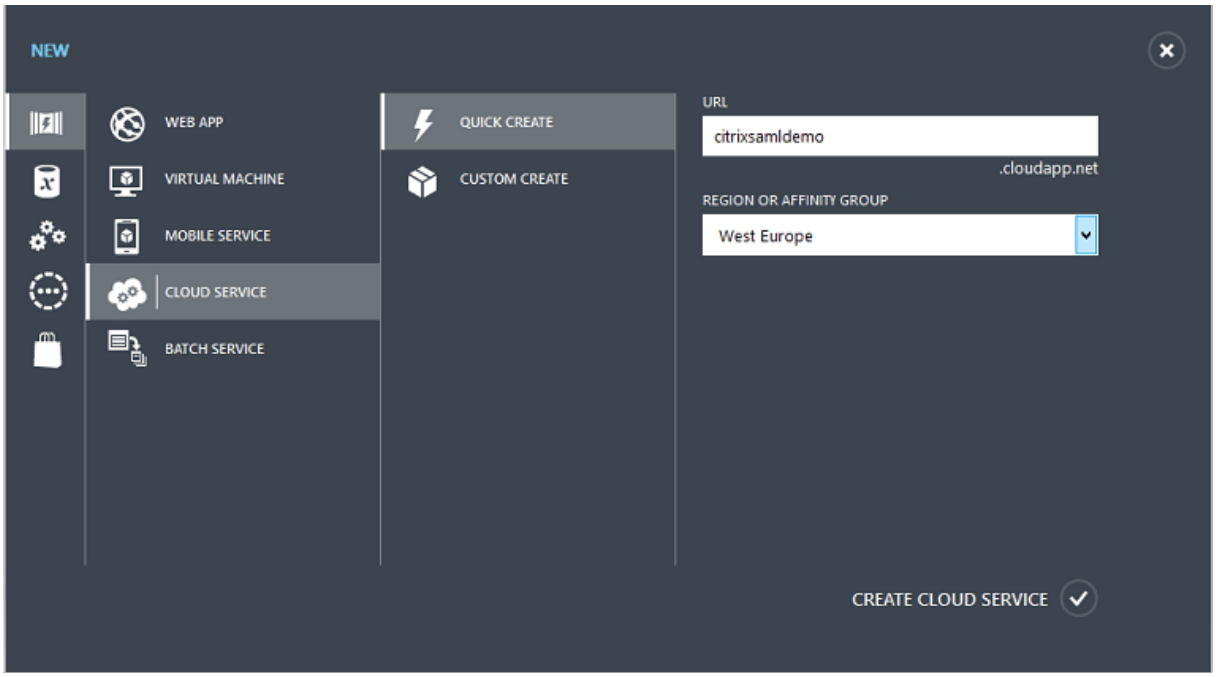
Al agregar referencias a las VM ejecutadas en Azure, lo más sencillo es usar un puntero CNAME que apunte al registro DNS administrado por Azure para la VM. Si la dirección IP de la VM cambia, no será necesario actualizar manualmente el archivo de zona DNS.

Los sufijos de ambas direcciones DNS interna y externa coincidirán en esta implementación. El dominio es citrixsamldemo.net y usan DNS dividido (10.0.0.* internamente).

Agregue una entrada "fs.citrixsamldemo.net"que haga referencia al servidor Proxy de aplicación web. Este es el Servicio de federación para esta zona.

Crear un servicio de nube

En este ejemplo se configura un entorno Citrix, incluido un entorno de AD con un servidor de ADFS activo en Azure. Se crea un servicio de nube llamado "citrixsamldemo".

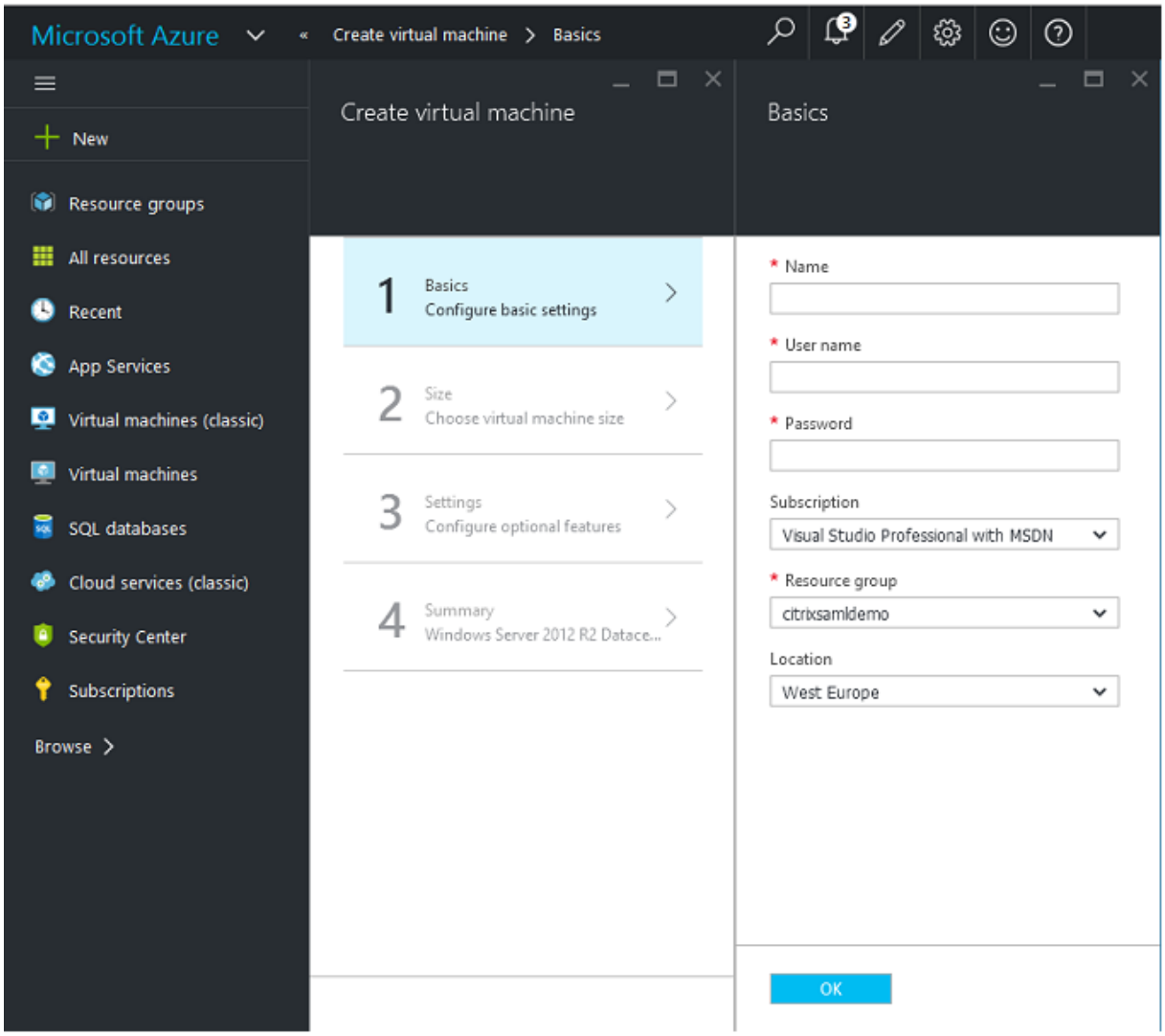


Crear máquinas virtuales de Windows

Cree cinco máquinas virtuales Windows ejecutándose en el servicio de nube:

- Controlador de dominio (domaincontrol)
- Servidor de ADFS de Azure Connect (adfs)
- Proxy de acceso web de ADFS (proxy de aplicación web, no unido a dominio)
- Delivery Controller de Citrix Virtual Apps and Desktops

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



Controlador de dominio

- Agregue los roles **Servidor DNS** y **Servicios de dominio de Active Directory** para crear una implementación estándar de Active Directory (en este ejemplo, citrixsamldemo.net). Una vez completada la promoción de dominio, agregue el rol **Servicios de certificados de Active Directory**.
- Cree una cuenta de usuario normal para las pruebas (por ejemplo, Jorge@citrixsamldemo.net).
- Dado que este servidor ejecutará DNS interno, todos los servidores deben hacer referencia a este servidor para la resolución de DNS. Esto se puede hacer desde la página de **configuración de Azure DNS** (para obtener más información, consulte el Apéndice en este documento).

Controlador ADFS y servidor proxy de aplicaciones web

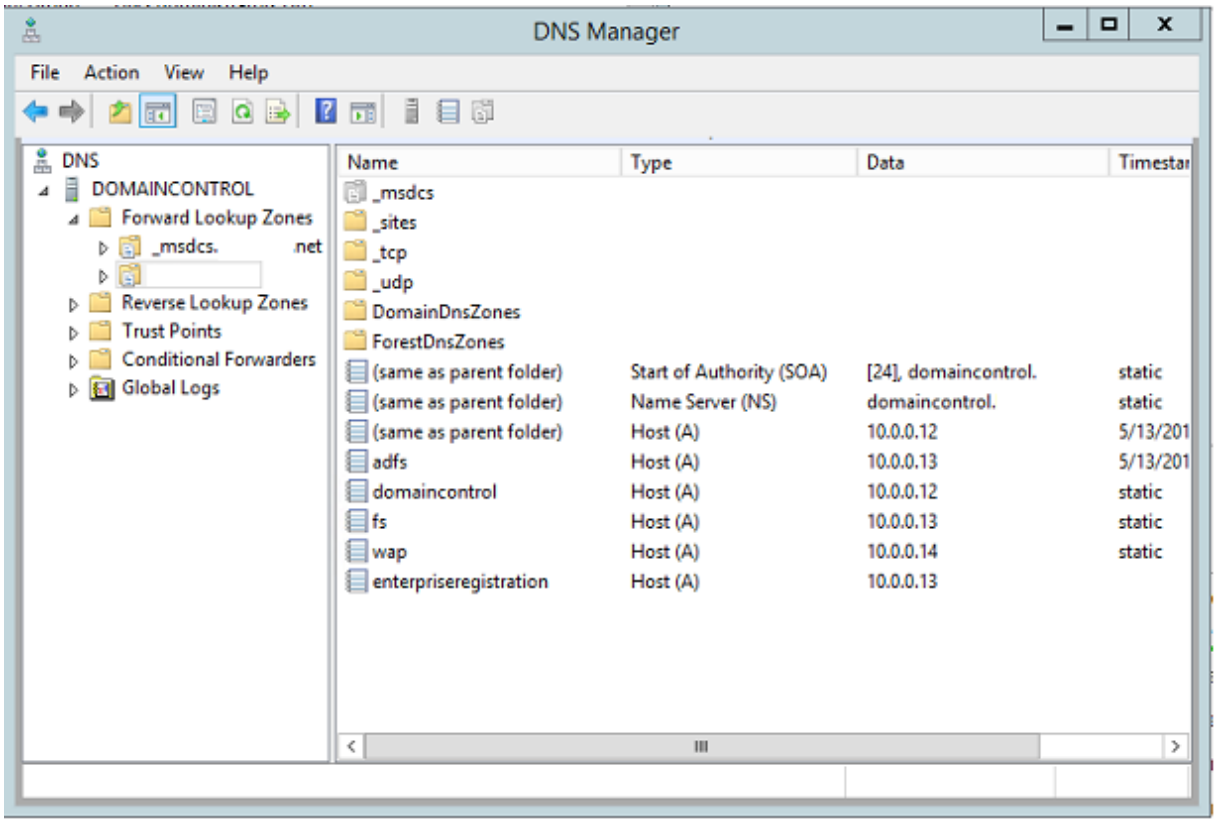
- Una el servidor de ADFS al dominio citrixsamldemo. El servidor proxy de aplicaciones web debe estar en un grupo de trabajo aislado, por lo que debe registrar manualmente una dirección DNS con el DNS de AD.
- Ejecute el cmdlet **Enable-PSRemoting** –**Force** en estos servidores, para permitir la comunicación remota de PS a través de firewalls desde la herramienta Azure AD Connect.

VDA y Delivery Controller de Citrix Virtual Desktops

- Instale el Delivery Controller y el VDA de Citrix Virtual Apps o Citrix Virtual Desktops en los dos servidores Windows restantes unidos a citrixsamldemo.

Configurar un DNS interno

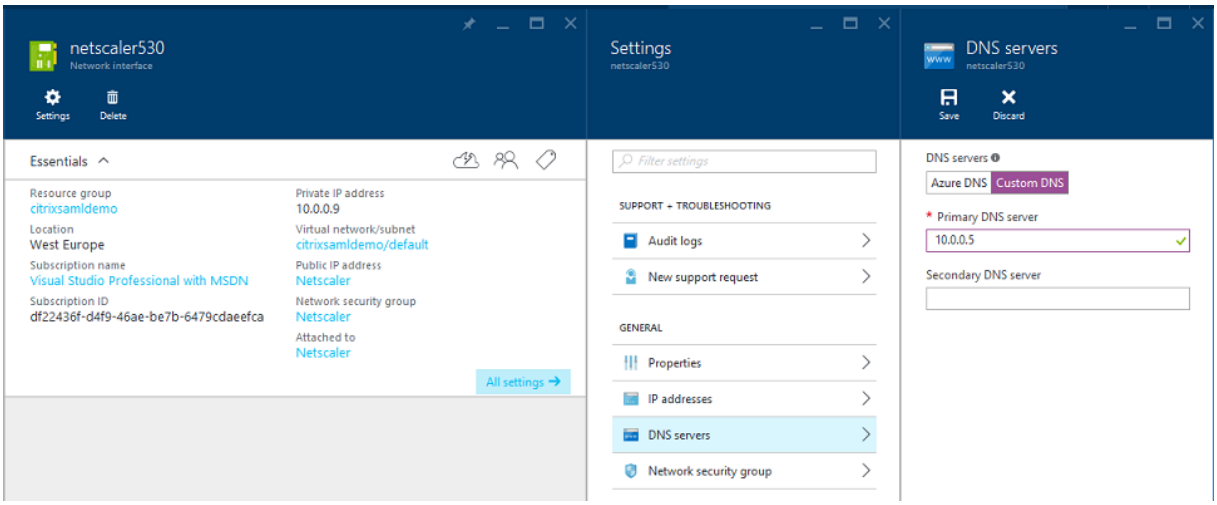
Después de que el controlador de dominio está instalado, configure el servidor DNS para controlar la vista de citrixsamldemo.net y actuar como un reenviador a un servidor DNS externo (por ejemplo: 8.8.8.8).



Agregue un registro estático para:

- wap.citrixsamldemo.net [la VM de proxy de aplicaciones web no estará unidad a un dominio]
- fs.citrixsamldemo.net [dirección de servidor de federación interno]
- enterpriseregistration.citrixsaml.net [lo mismo que fs.citrixsamldemo.net]

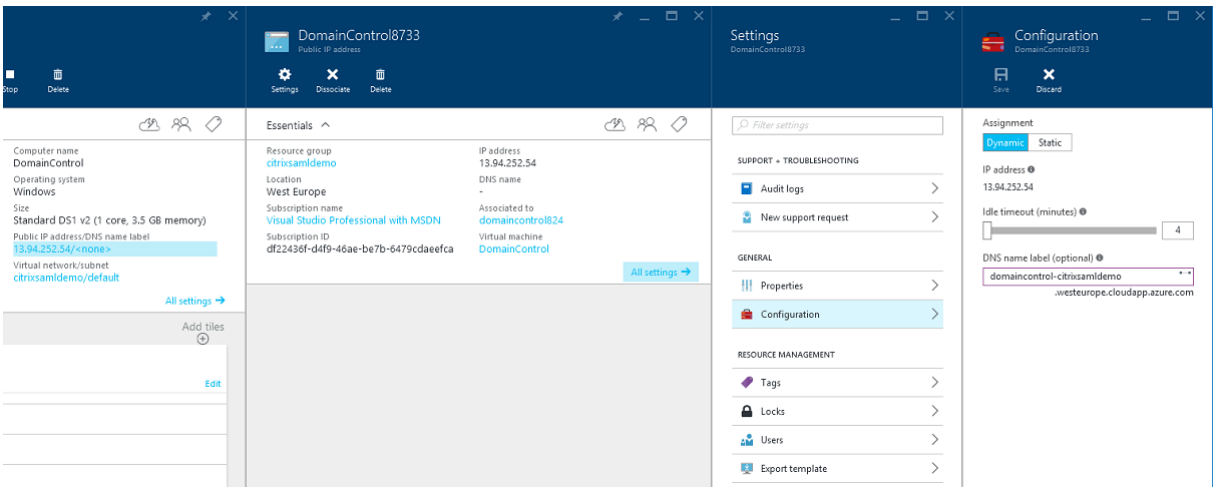
Todas las VM que se ejecutan en Azure deben estar configuradas para usar solo este servidor DNS. Puede hacerlo a través de la GUI de interfaz de red.



De forma predeterminada, la dirección IP interna (10.0.0.9) se asigna dinámicamente. Puede usar el parámetro de direcciones IP para asignar permanentemente la dirección IP. Esto debe hacerse para el servidor proxy de aplicaciones web y el controlador de dominio.

Configurar una dirección DNS externa

Cuando se está ejecutando una VM, Azure mantiene su propio servidor de zona DNS que apunta a la dirección IP pública actual asignada a la VM. Habilitar esta función resulta muy útil porque Azure asigna direcciones IP cuando cada VM se inicia, de manera predeterminada.

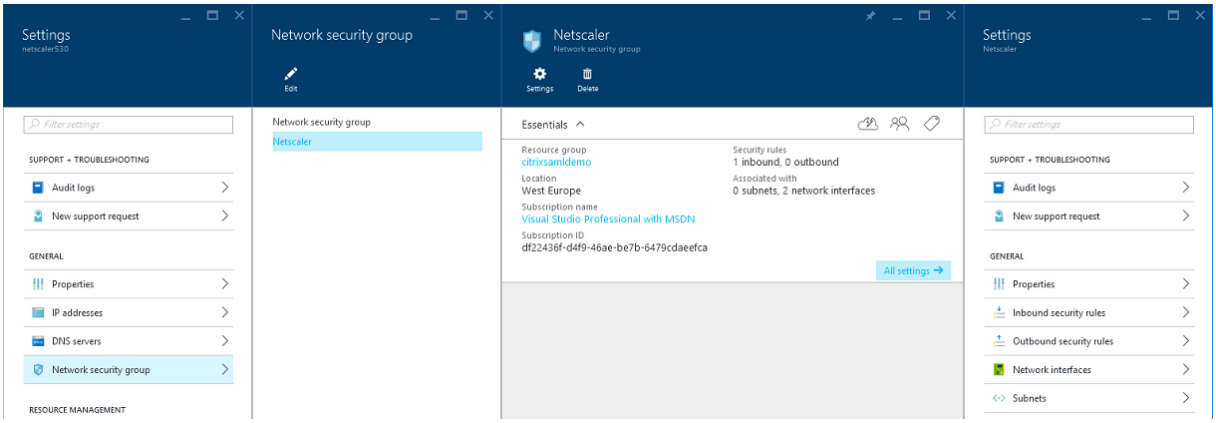


Este ejemplo asigna una dirección DNS de domaincontrol-citrixsamldemo.westeurope.cloudapp.azure.com al controlador de dominio.

Tenga en cuenta que, cuando se complete la configuración remota, solo las VM del proxy de aplicaciones web y de Citrix Gateway deben tener direcciones IP públicas habilitadas. (Durante la configuración, la dirección IP pública se usa para el acceso RDP al entorno).

Configurar grupos de seguridad

La nube de Azure administra las reglas de firewall para el acceso TCP/UDP en las VM desde Internet mediante grupos de seguridad. De forma predeterminada, todas las VM permiten el acceso RDP. Los servidores de Citrix Gateway y el proxy de aplicaciones web también deben permitir TLS en el puerto 443.

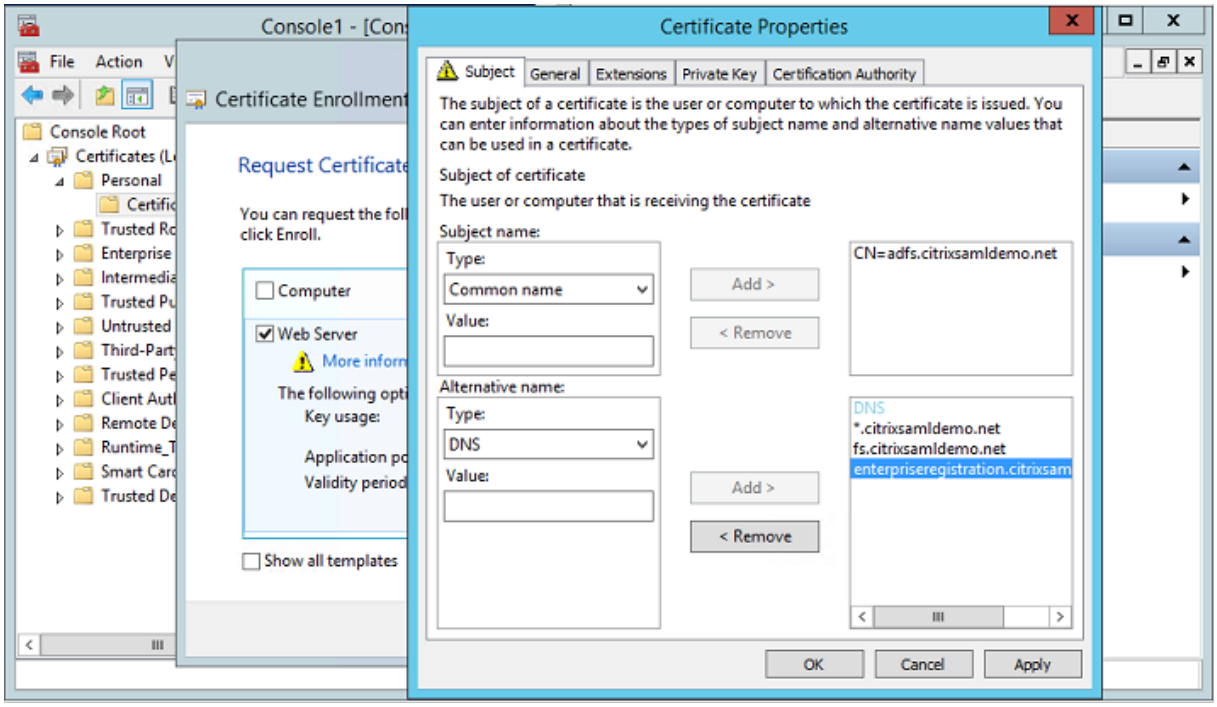


Crear un certificado ADFS

Habilite la plantilla de certificado **Servidor web** en la entidad de certificación de Microsoft. Esto permite la creación de un certificado con direcciones DNS personalizadas que se pueden exportar (incluida la clave privada) a un archivo .pfx. Debe instalar este certificado tanto en el servidor proxy de aplicaciones web como en el servidor de ADFS, por lo que un archivo PFX es la opción preferida.

Emita un certificado de servidor web con los siguientes nombres de sujeto:

- Commonname:
  - adfs.citrixsamldemo.net [nombre del equipo]
- SubjectAltname:
  - *.citrixsamldemo.net [nombre de la zona]
  - fs.citrixsamldemo. net [entrada en DNS]
  - enterpriseregistration.citrixsamldemo.net



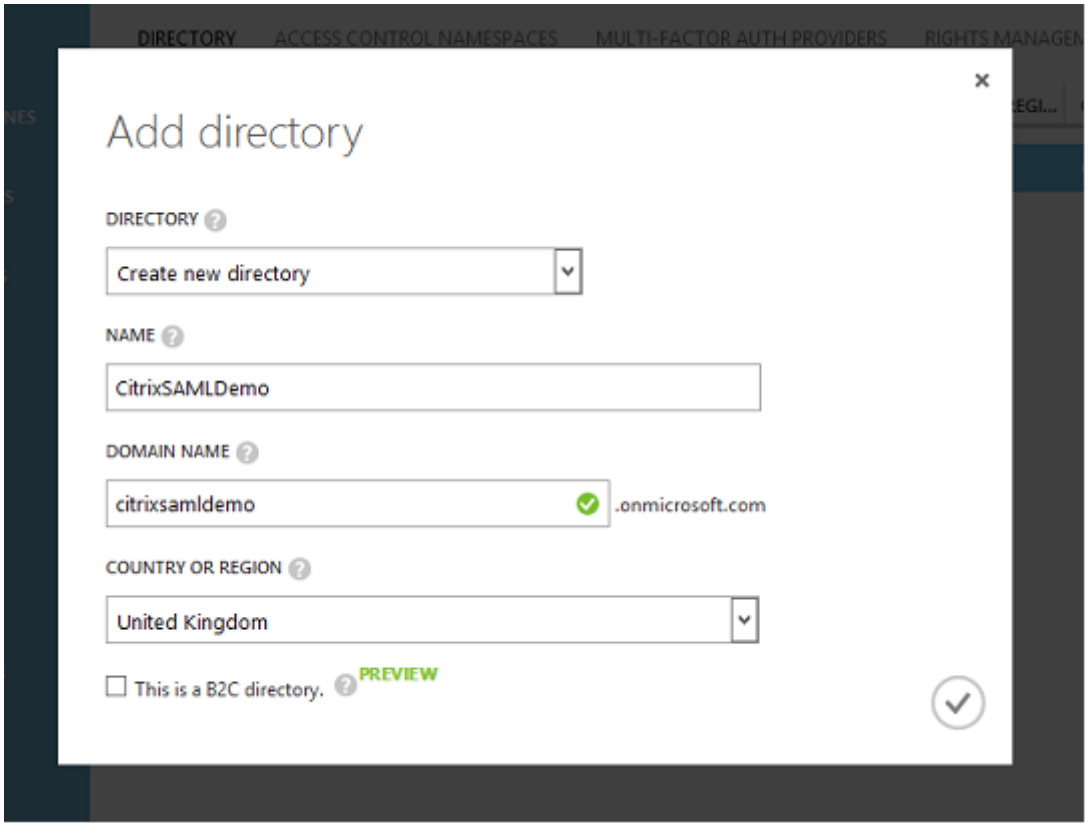
Exporte el certificado a un archivo PFX, incluida una clave privada protegida por contraseña.

Configurar Azure AD

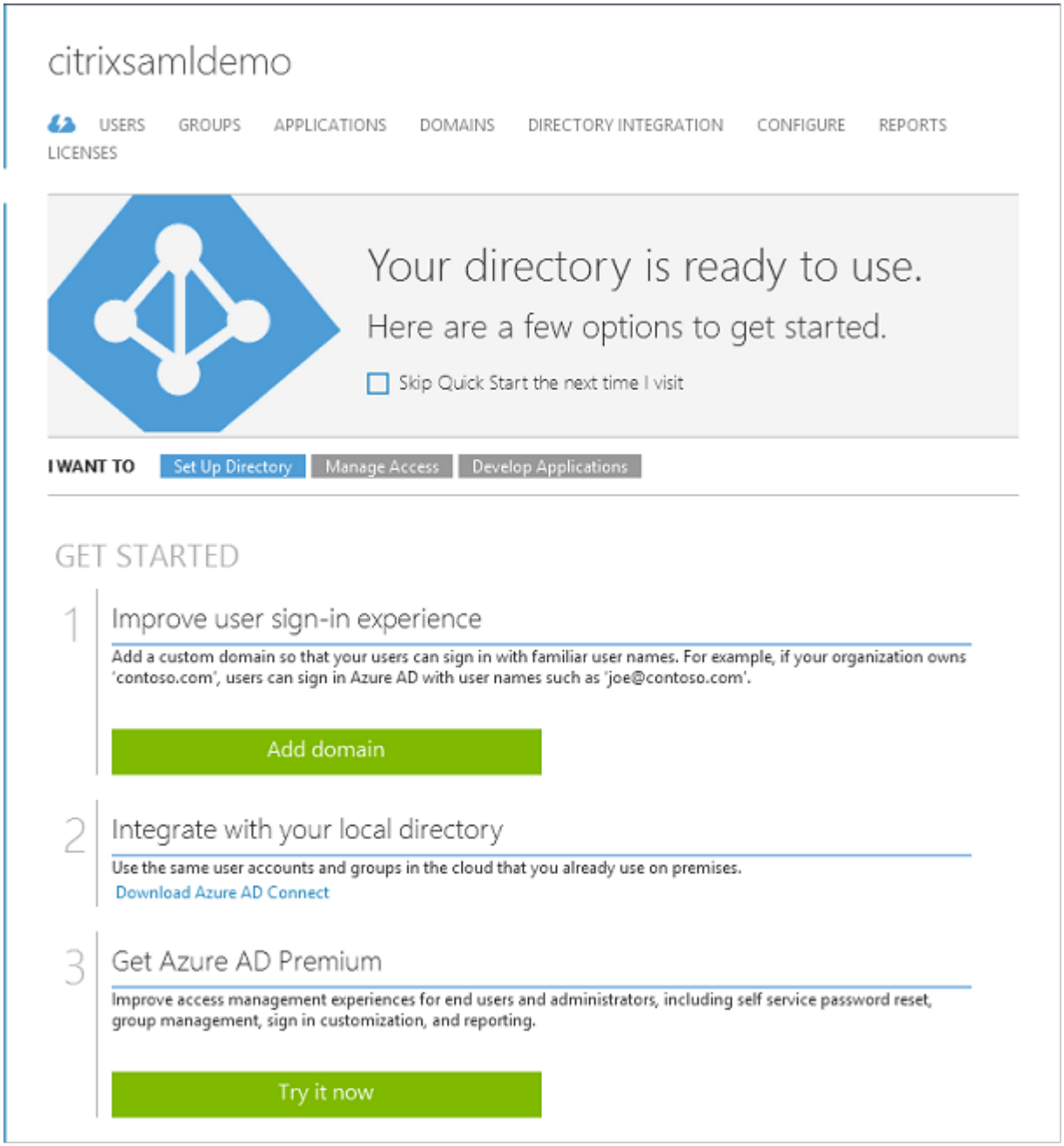
Esta sección detalla el proceso de configuración de una nueva instancia de Azure AD y la creación de identidades de usuario que se pueden usar para unir Windows 10 a Azure AD.

Crear un directorio nuevo

Inicie sesión en el portal Azure clásico y cree un directorio nuevo.

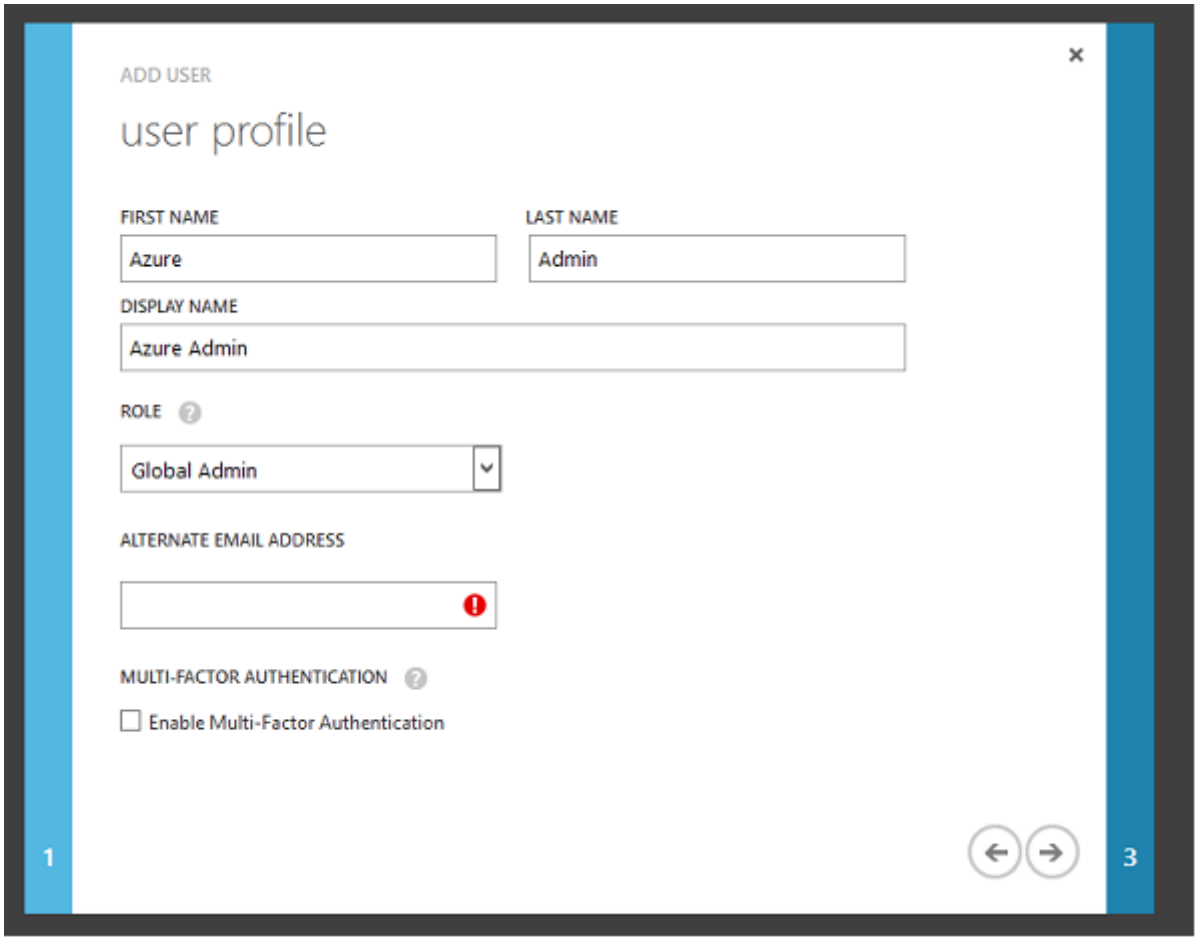


Una vez completado, aparece una página de resumen.



Crear un usuario administrador global (AzureAdmin)

Cree un administrador global en Azure (en este ejemplo, `AzureAdmin@citrixsamldemo.onmicrosoft.com`) e inicie sesión con la nueva cuenta para configurar una contraseña.



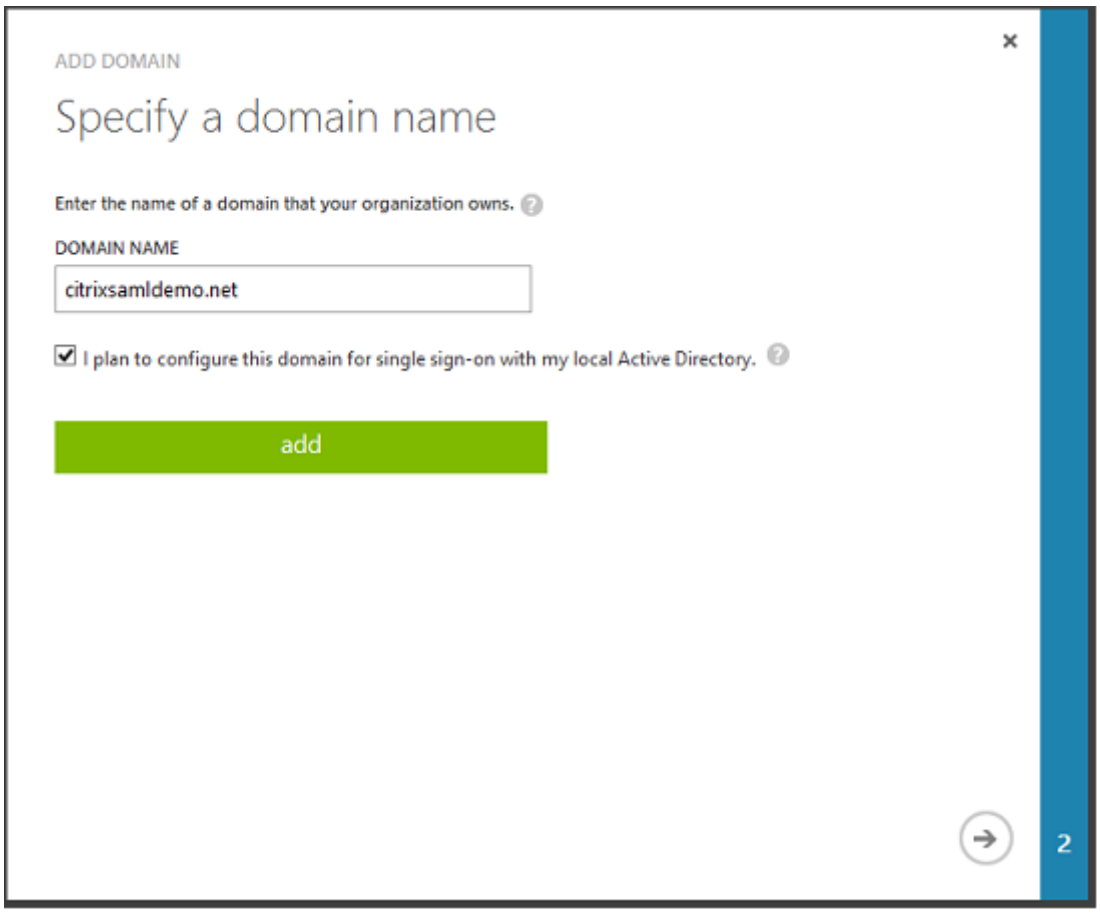
Registrar su dominio en Azure AD

De forma predeterminada, los usuarios se identifican mediante una dirección de correo electrónico en el formato: `<user.name>@<company>.onmicrosoft.com`.

Aunque esto funciona sin configuración adicional, se prefiere un formato estándar para la dirección de correo electrónico; preferiblemente, es mejor que coincida con el formato de la cuenta de correo electrónico del usuario final: `<user.name>@<company>.com`.

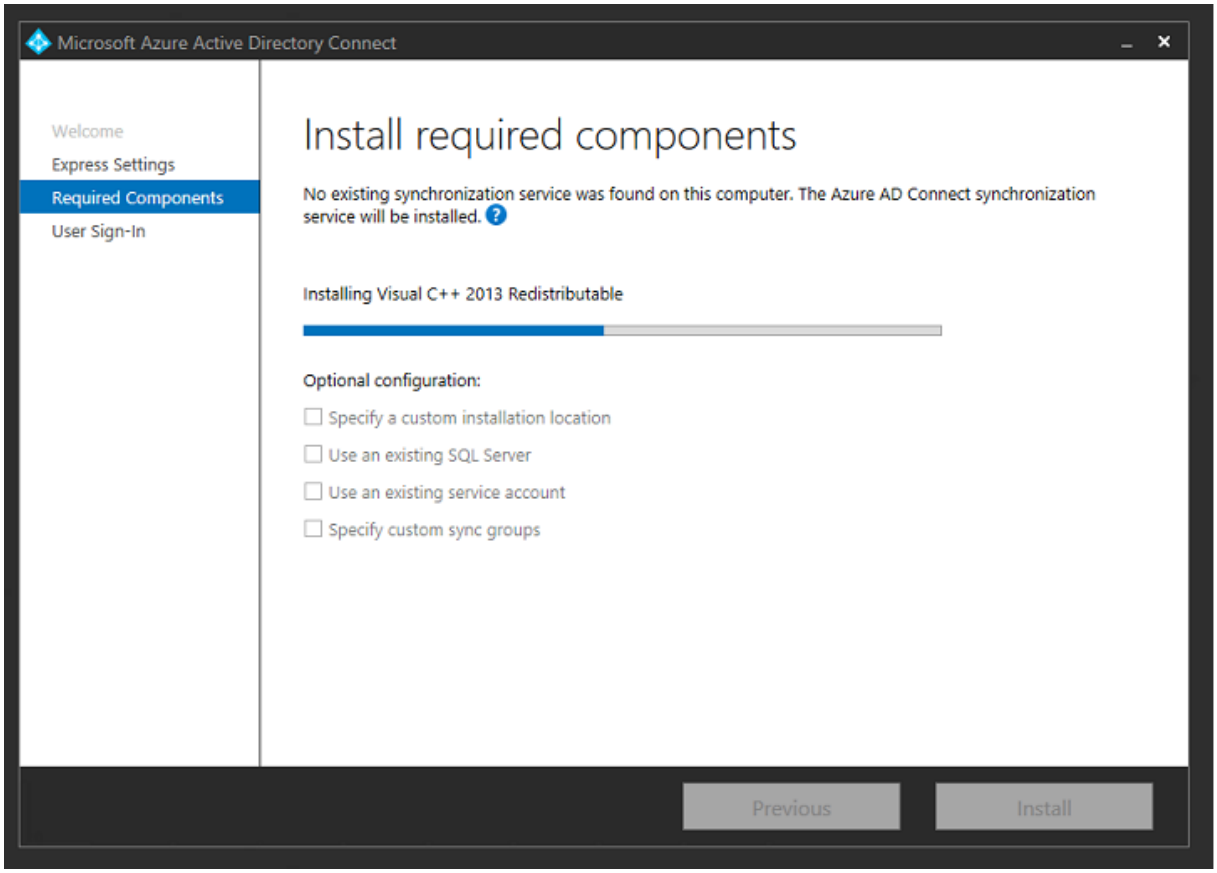
La acción **Agregar dominio** configura una redirección desde el dominio real de su empresa. En el ejemplo se usa `citrixsamldemo.net`.

Si quiere configurar ADFS para el inicio de sesión único Single Sign-On, marque la casilla correspondiente.

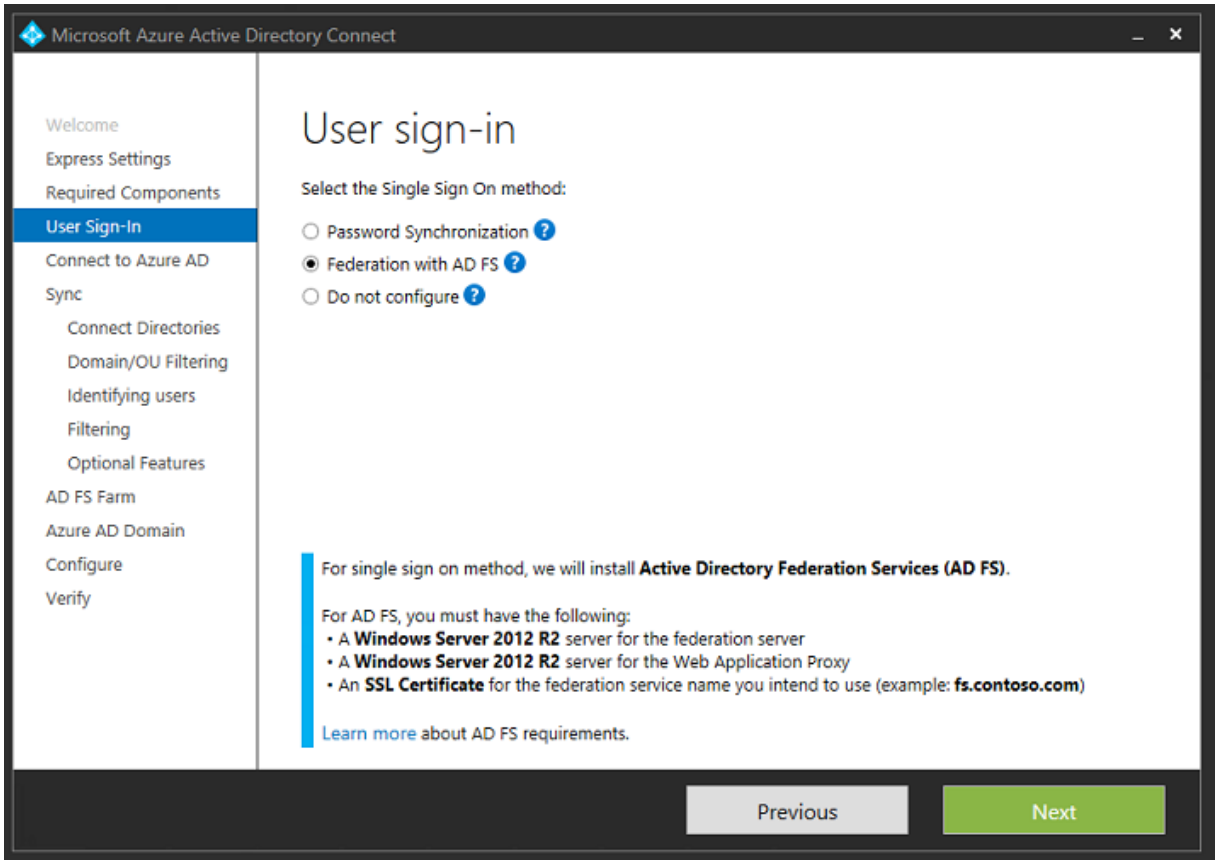


Instalar Azure AD Connect

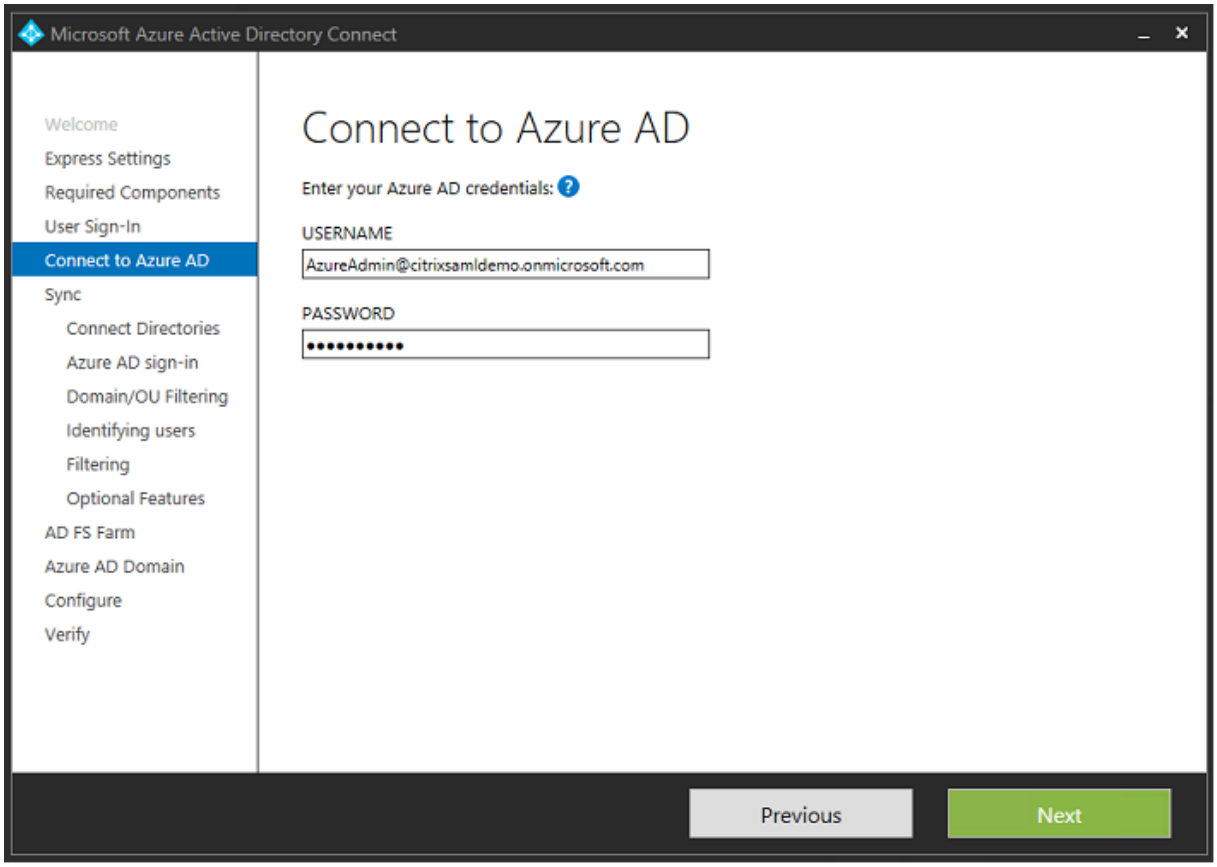
El paso 2 de la interfaz de usuario de configuración de Azure AD le redirige a la página de descarga de Microsoft de Azure AD Connect. Instale esto en la VM de ADFS. Use **Instalación personalizada**, en lugar de **Configuración rápida**, para poder acceder a las opciones de ADFS.



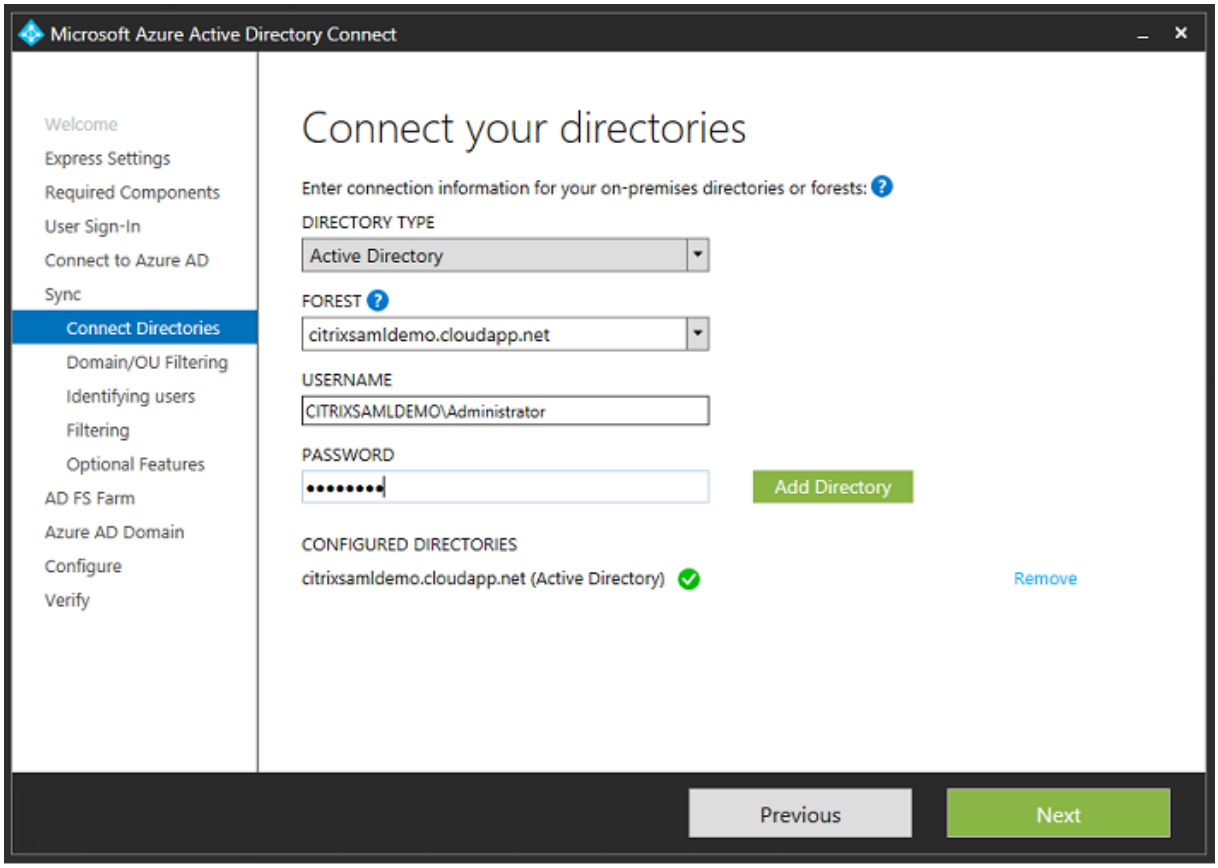
Seleccione la opción **Federación con AD FS** como método SSO.



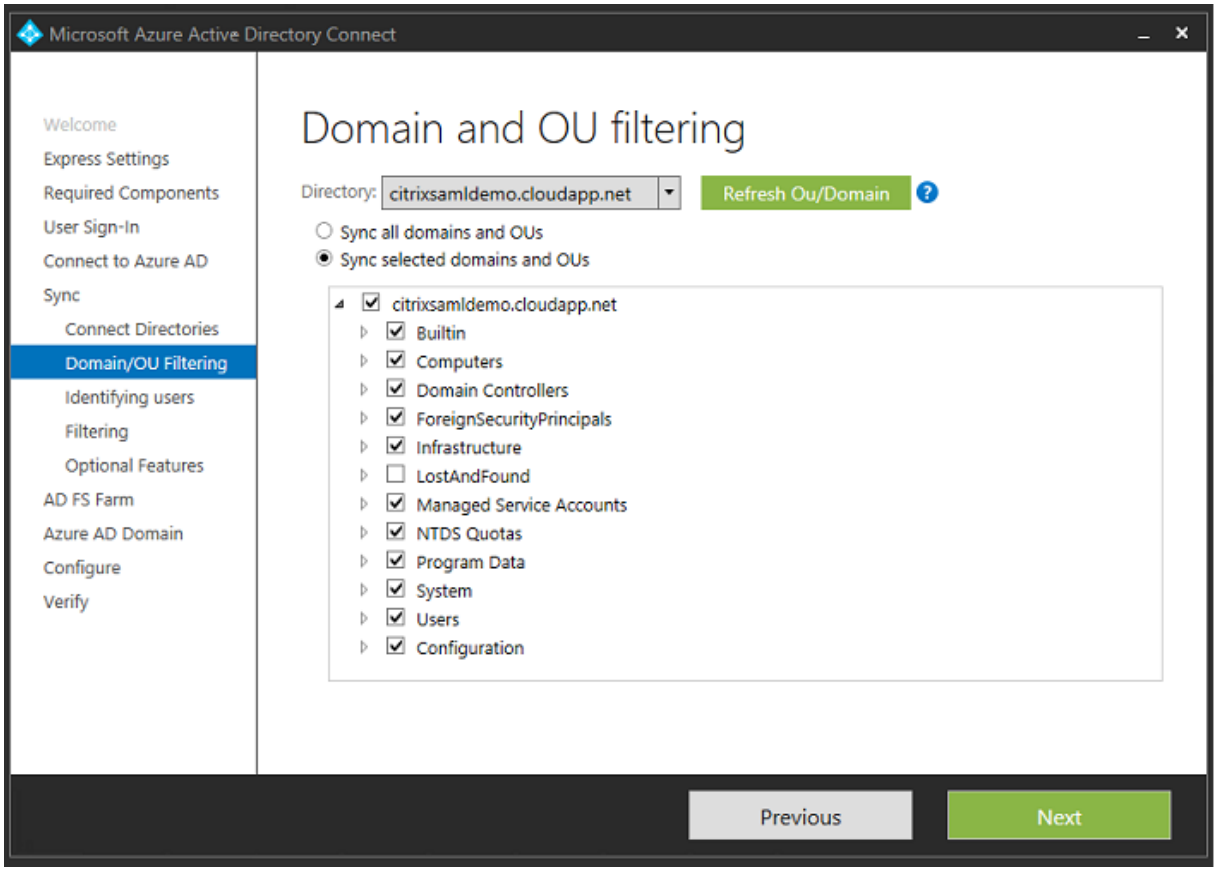
Conéctese a Azure con la cuenta de administrador que ha creado anteriormente.



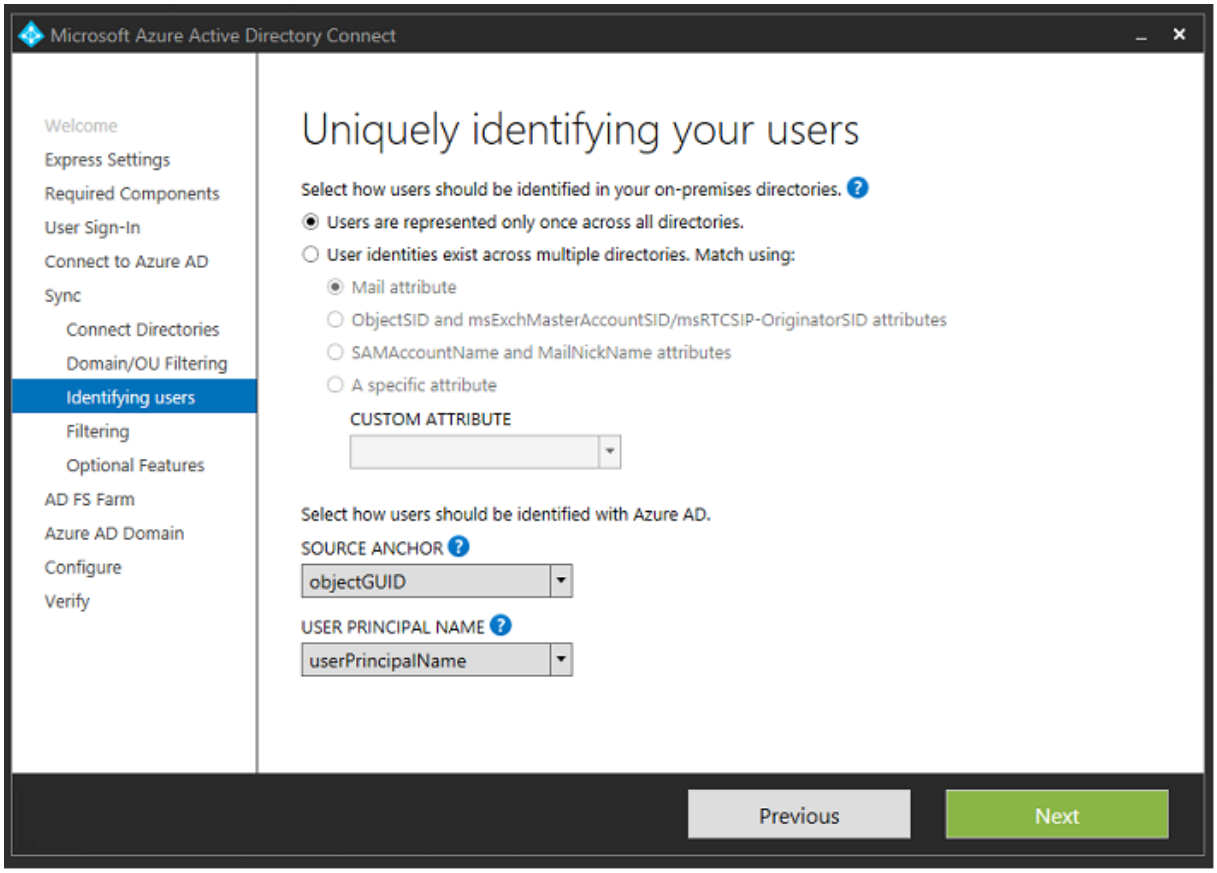
Seleccione el bosque de AD interno.



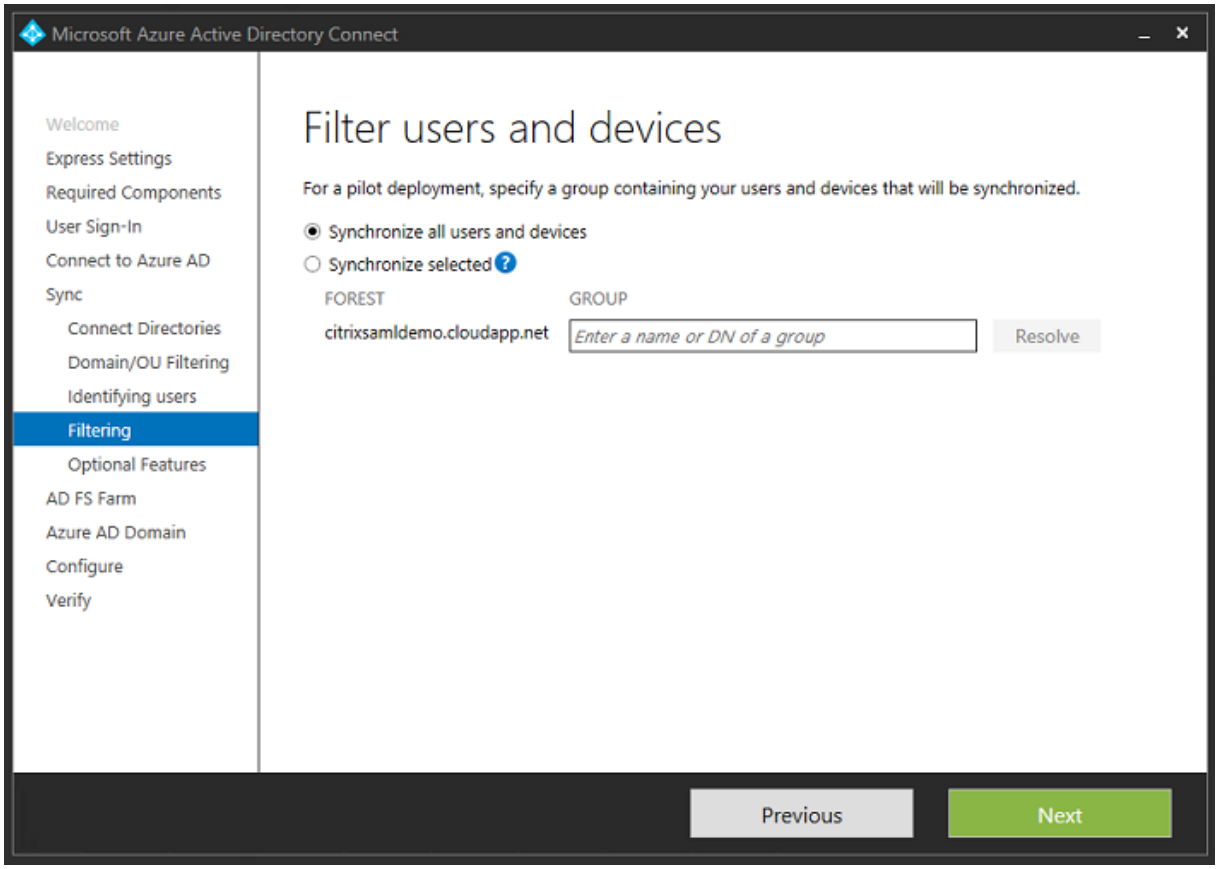
Sincronice todos los objetos de Active Directory antiguos con Azure AD.



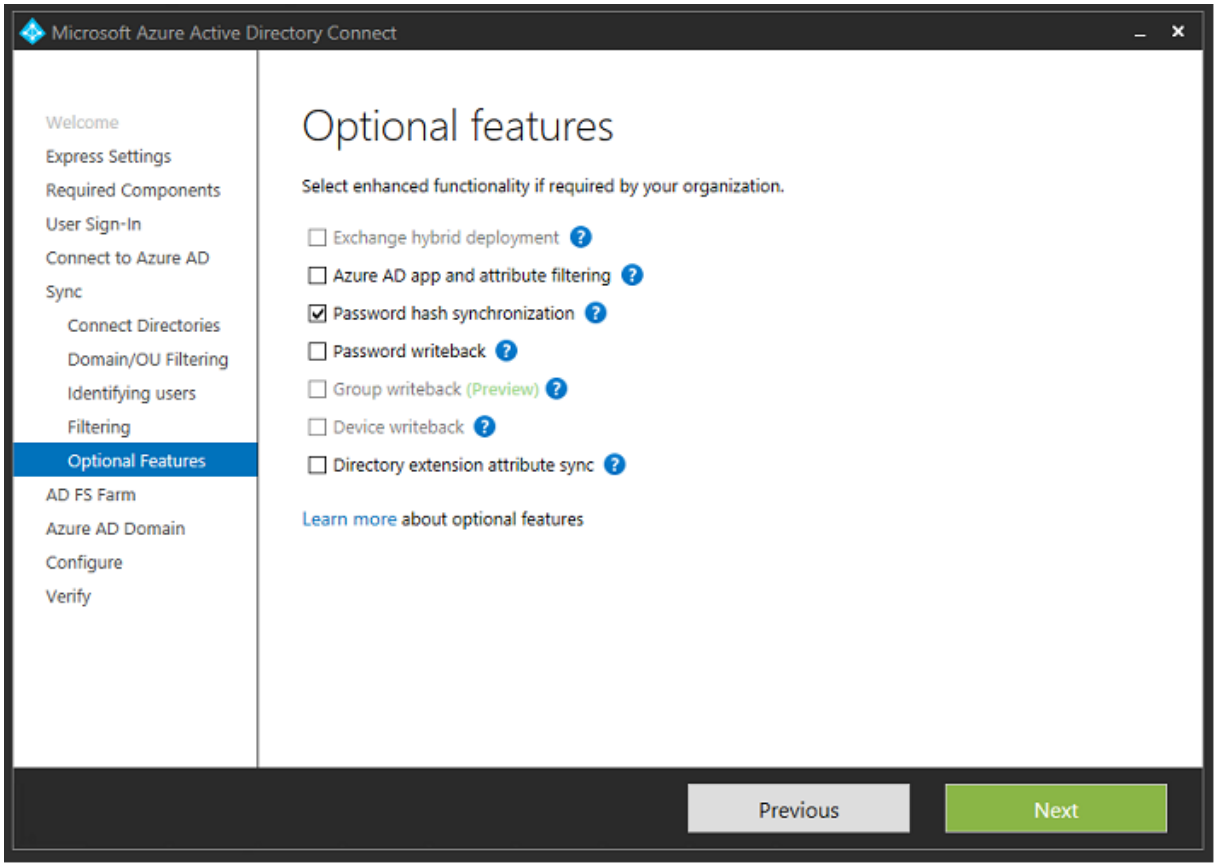
Si la estructura de directorio es sencilla, puede asumir que los nombres de usuario serán lo suficientemente únicos para identificar al usuario que inicia una sesión.



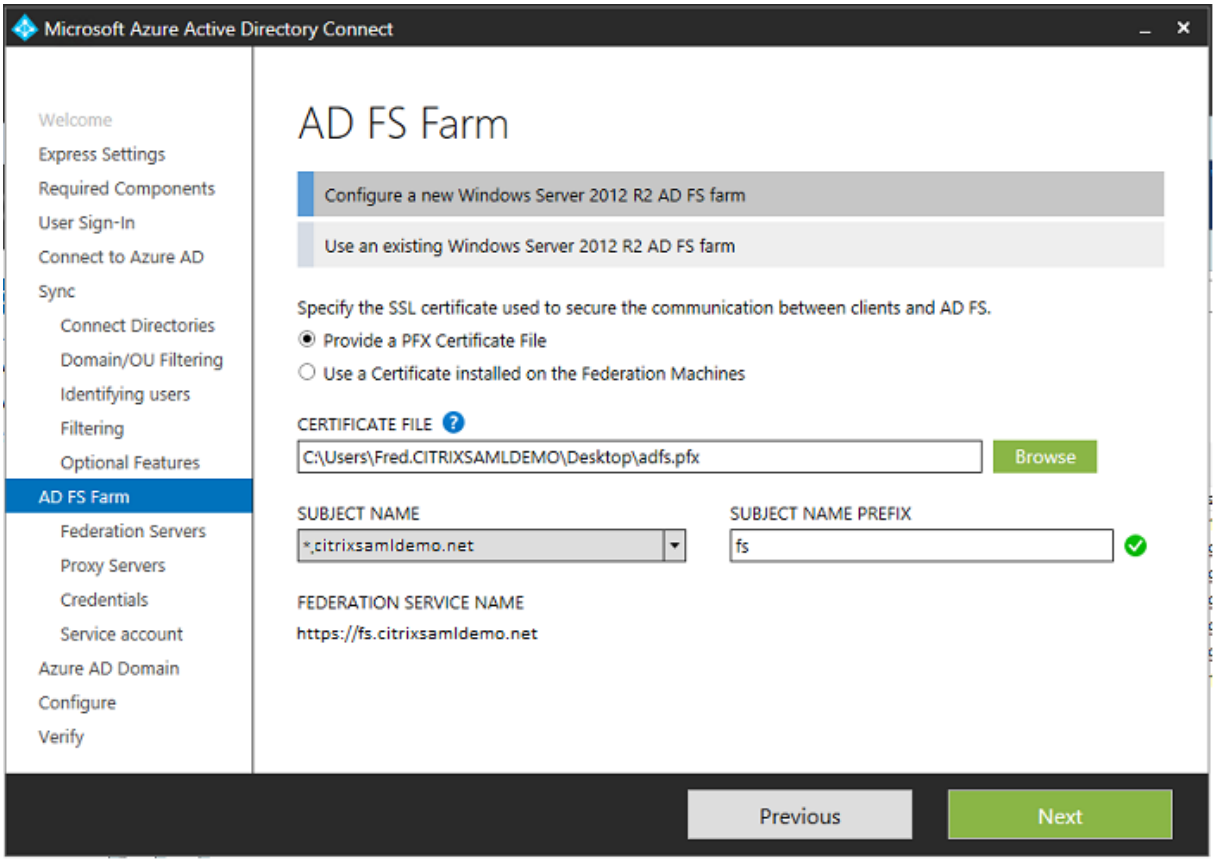
Acepte las opciones de filtrado predeterminadas, o restrinja usuarios y dispositivos a un conjunto de grupos determinado.



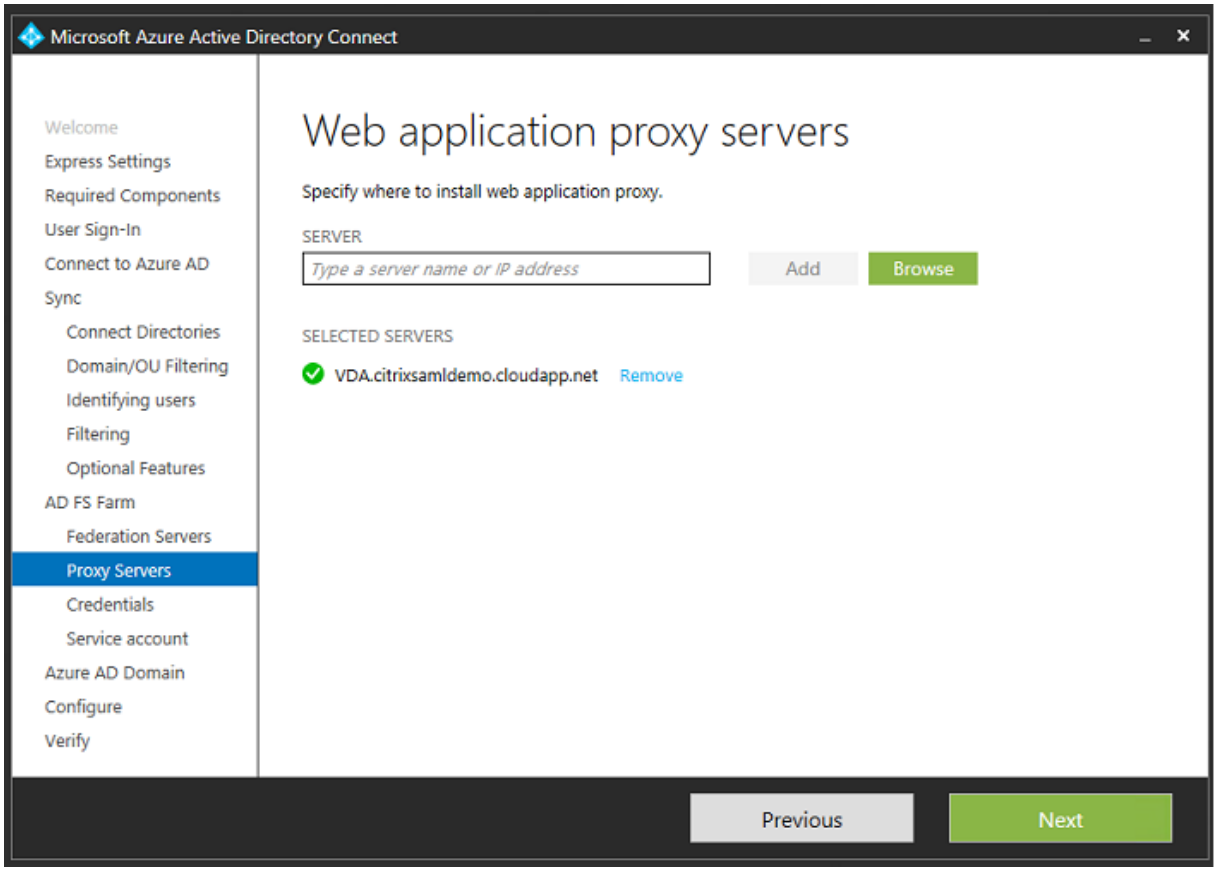
Si lo desea, puede sincronizar las contraseñas de Azure AD con Active Directory. Esto normalmente no es necesario para la autenticación basada en ADFS.



Seleccione el archivo de certificado PFX que se va a usar en ADFS y especifique fs.citrixsamldemo.net como nombre DNS.

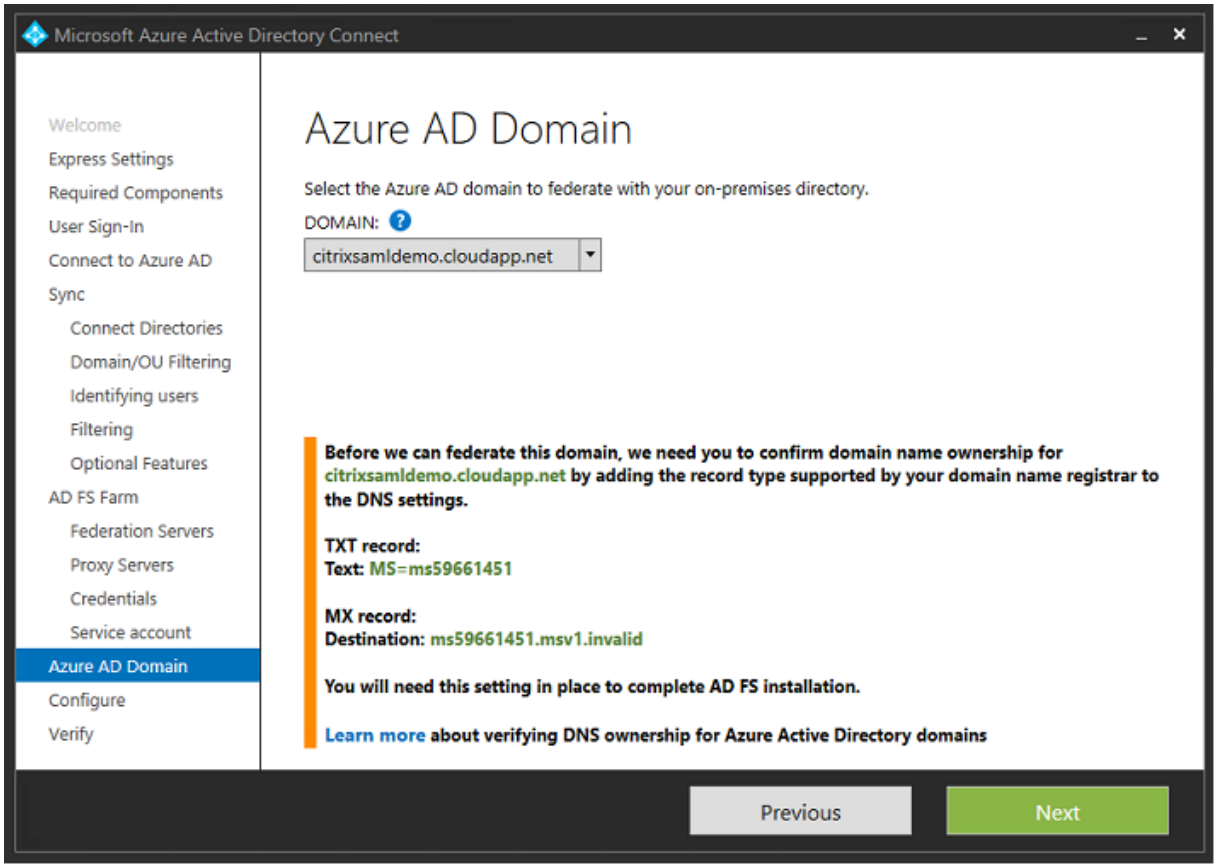


Cuando se le pida seleccionar un servidor proxy, escriba la dirección del servidor wap.citrixsamldemo.net. Puede que deba ejecutar el cmdlet **Enable-PSRemoting** –**Force** como administrador en el servidor proxy de aplicaciones web, para que Azure AD Connect pueda configurarlo.

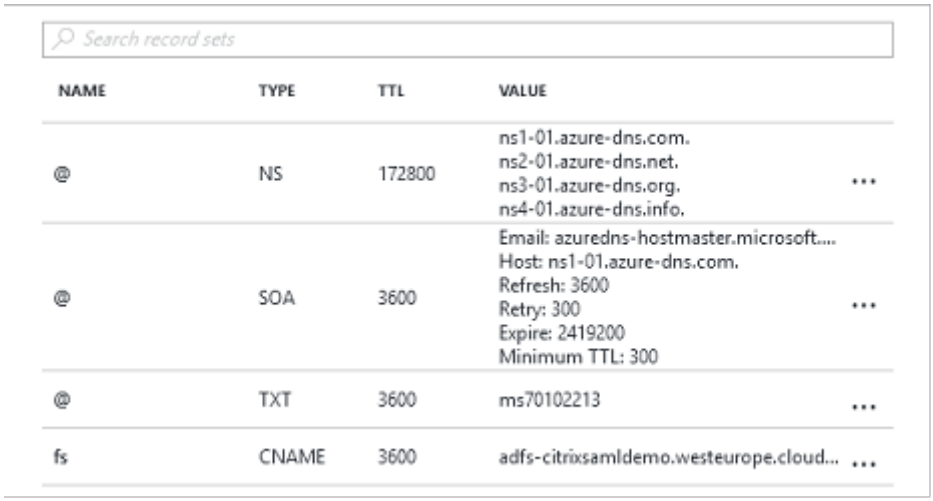


> **Nota:**
>
> Si este paso falla debido a problemas de confianza con el PowerShell remoto, una el servidor proxy de aplicaciones web al dominio.

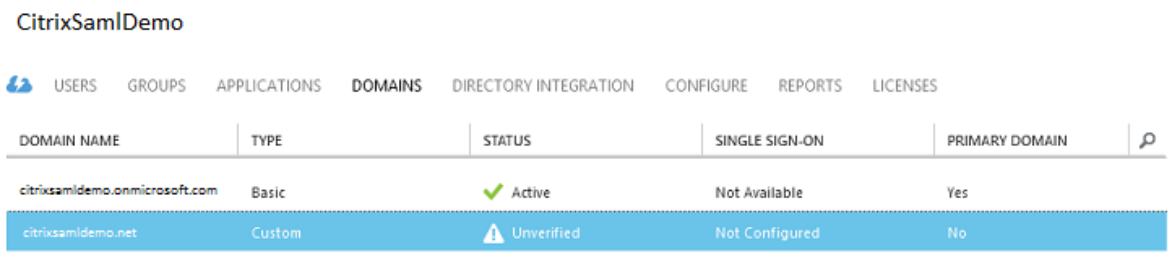
Para los pasos restantes del asistente, use las contraseñas estándar de administrador y cree una cuenta de servicio de ADFS. Azure AD Connect pedirá validar el propietario de la zona DNS.



Agregue los registros TXT y MX a los registros de direcciones DNS en Azure.

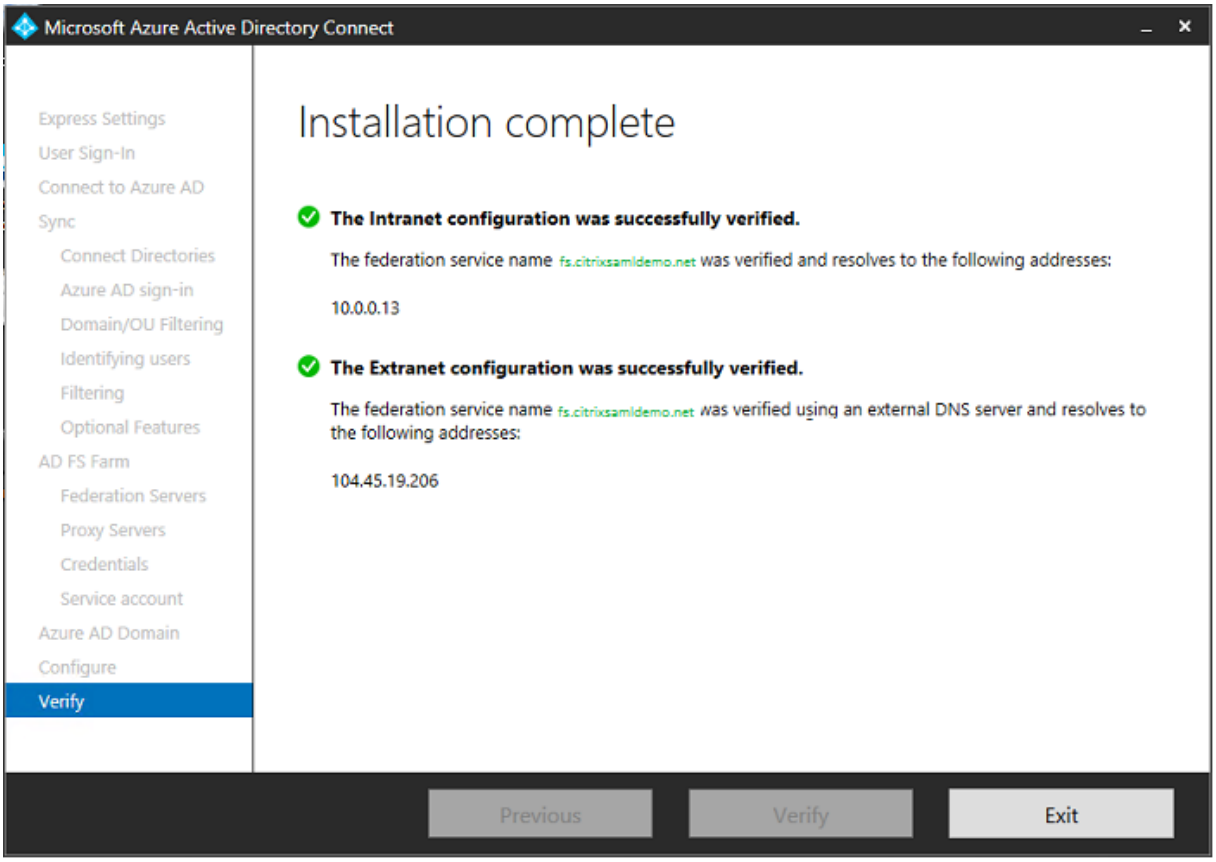


Haga clic en **Verificar** en la consola de administración de Azure.



> **Nota:**
>
> Si este paso falla, puede verificar el dominio antes de ejecutar Azure AD Connect.

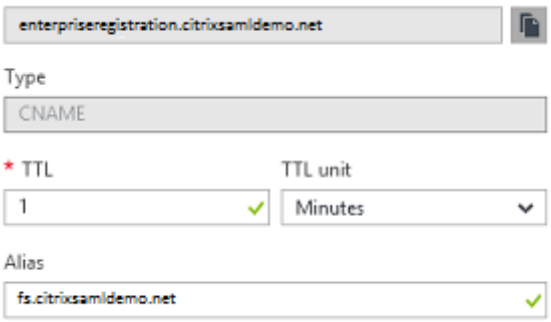
Una vez completado, se contacta con la dirección externa fs.citrixsamldemo.net a través del puerto 443.



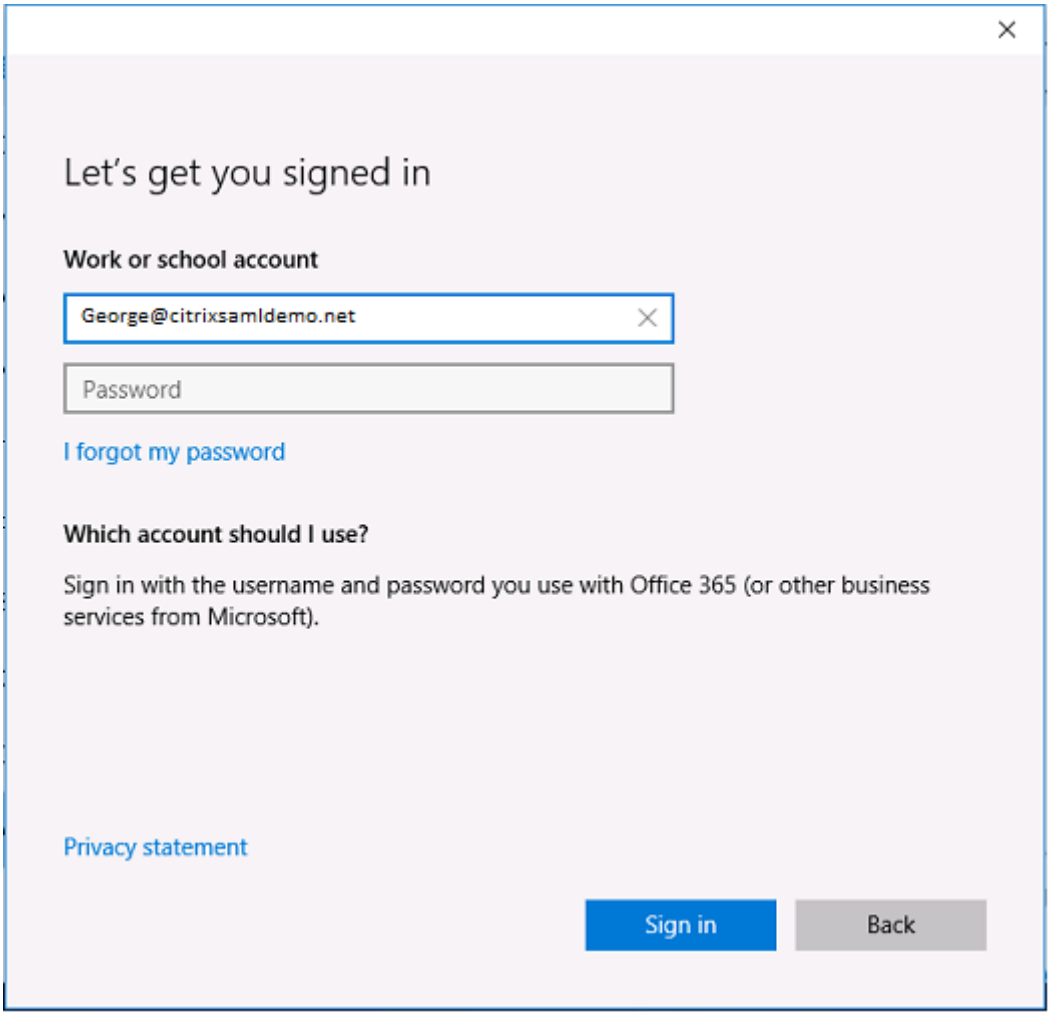
Habilitar la función Unirse a Azure AD

Cuando un usuario introduce una dirección de correo electrónico para que Windows 10 pueda unirse a Azure AD, se usa el sufijo DNS para crear un registro DNS CNAME que debe apuntar a ADFS: enterpriseregistration.<*sufijoUPN*>.

En el ejemplo, es `fs.citrixsamldemo.net`.

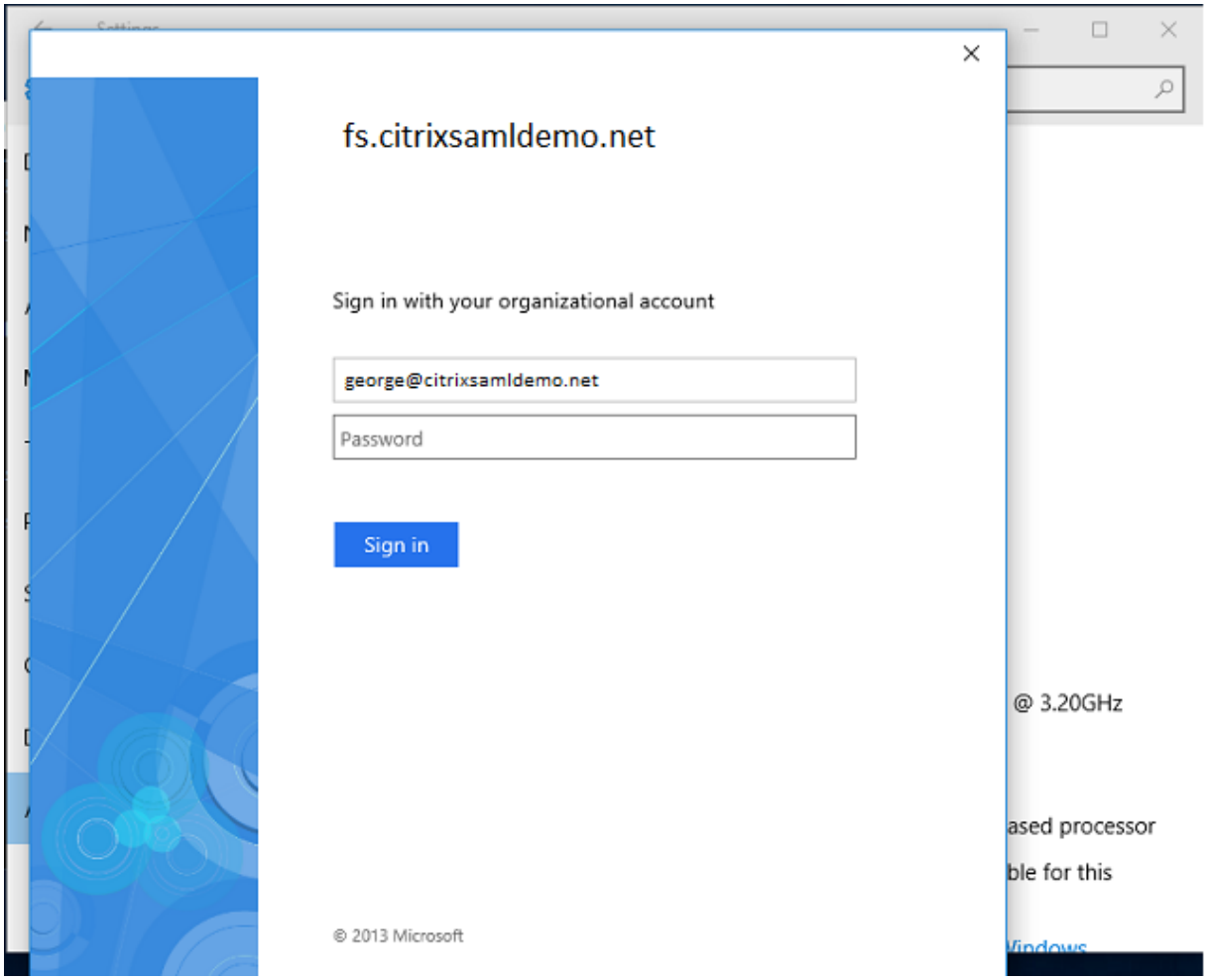


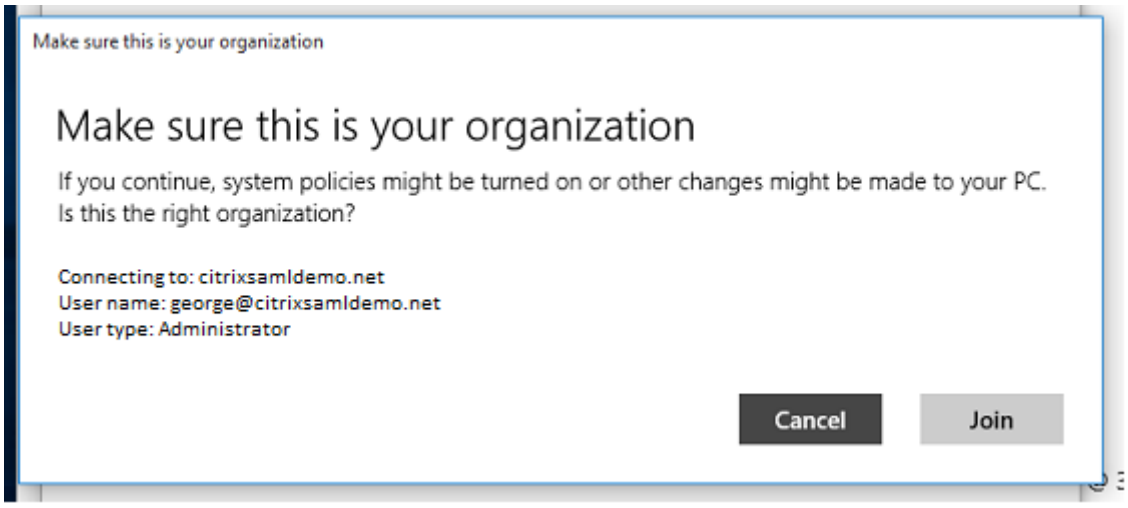
Si no está usando una entidad de certificación pública, asegúrese de que el certificado raíz de ADFS está instalado en el equipo con Windows 10 de modo que Windows confíe en el servidor de ADFS. Realice la unión con el dominio de Azure AD mediante la cuenta de usuario estándar generada anteriormente.

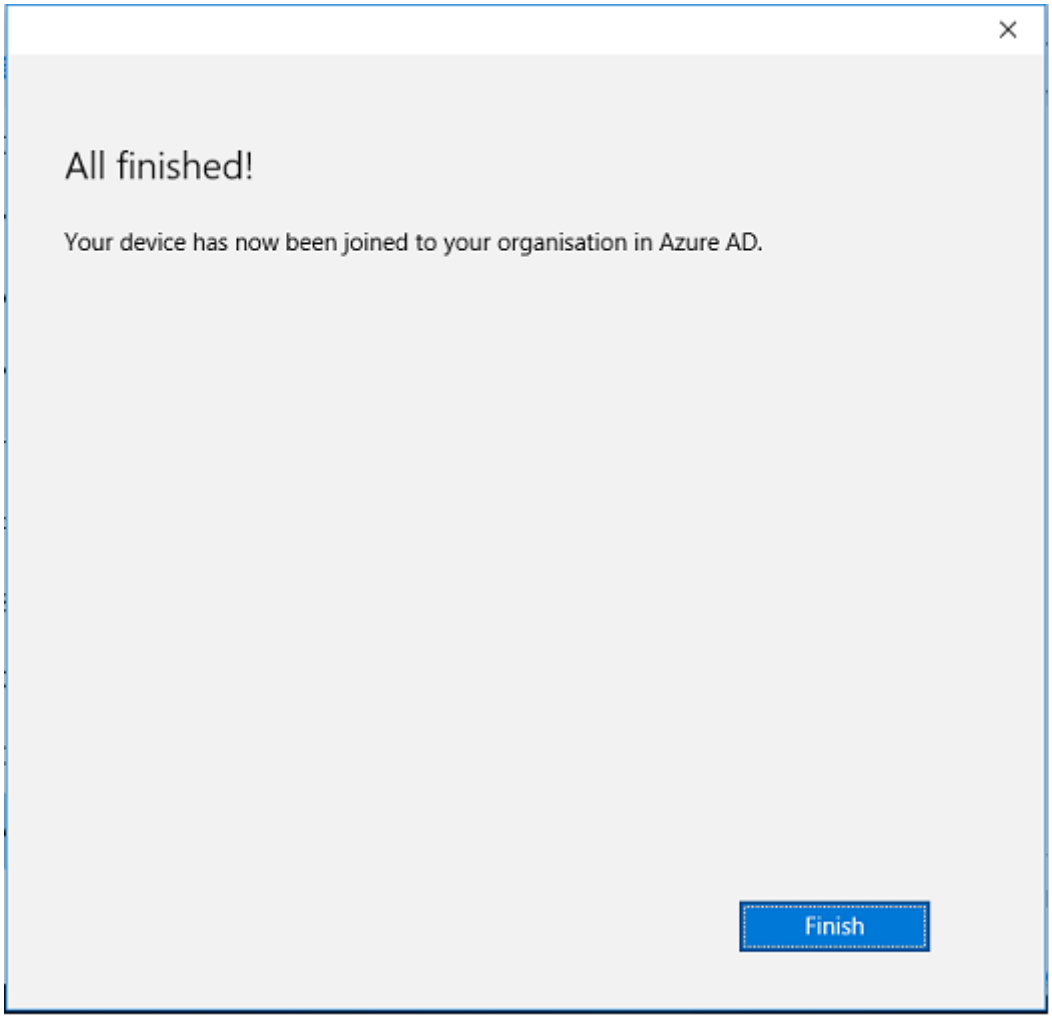


Tenga en cuenta que el nombre UPN debe coincidir con el nombre UPN reconocido por el controlador

de dominio de ADFS.





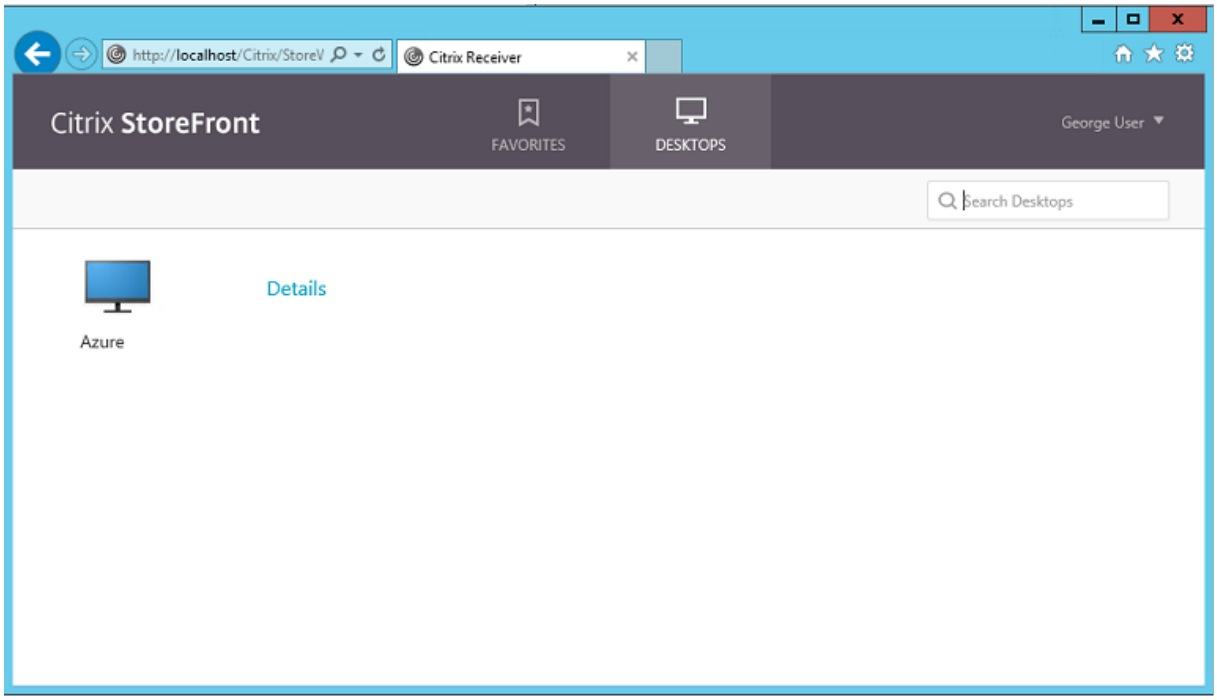


Verifique que la máquina se ha unido al dominio de Azure AD. Para ello, reinicie la máquina e inicie sesión con la dirección de correo electrónico del usuario. Una vez iniciada la sesión, abra Microsoft Edge y conéctese a http://myapps.microsoft.com. El sitio web debe utilizar Single Sign-On automáticamente.

Instalar Citrix Virtual Apps o Citrix Virtual Desktops

Puede instalar las máquinas virtuales del Delivery Controller y los VDA directamente en Azure desde la imagen ISO de Citrix Virtual Apps o Citrix Virtual Desktops de la forma habitual.

En este ejemplo, StoreFront se instala en el mismo servidor que el Delivery Controller. El VDA se instala como una máquina de trabajo Windows 2012 R2 RDS independiente, sin integración con Machine Creation Services (aunque esto puede configurarse si se prefiere). Compruebe que el usuario Jorge@citrixsamldemo.net se puede autenticar con una contraseña, antes de continuar.



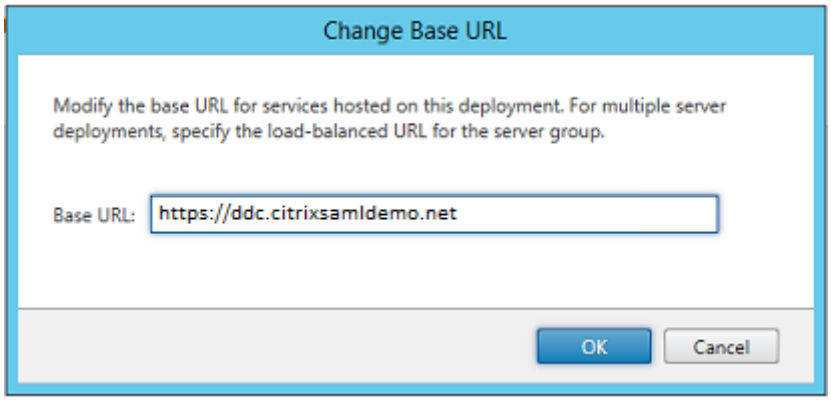
Ejecute el cmdlet **Set-BrokerSite –TrustRequestsSentToTheXmlServicePort $true** de PowerShell en el Controller para permitir que StoreFront se autentique sin las credenciales de los usuarios.

Instalar el Servicio de autenticación federada

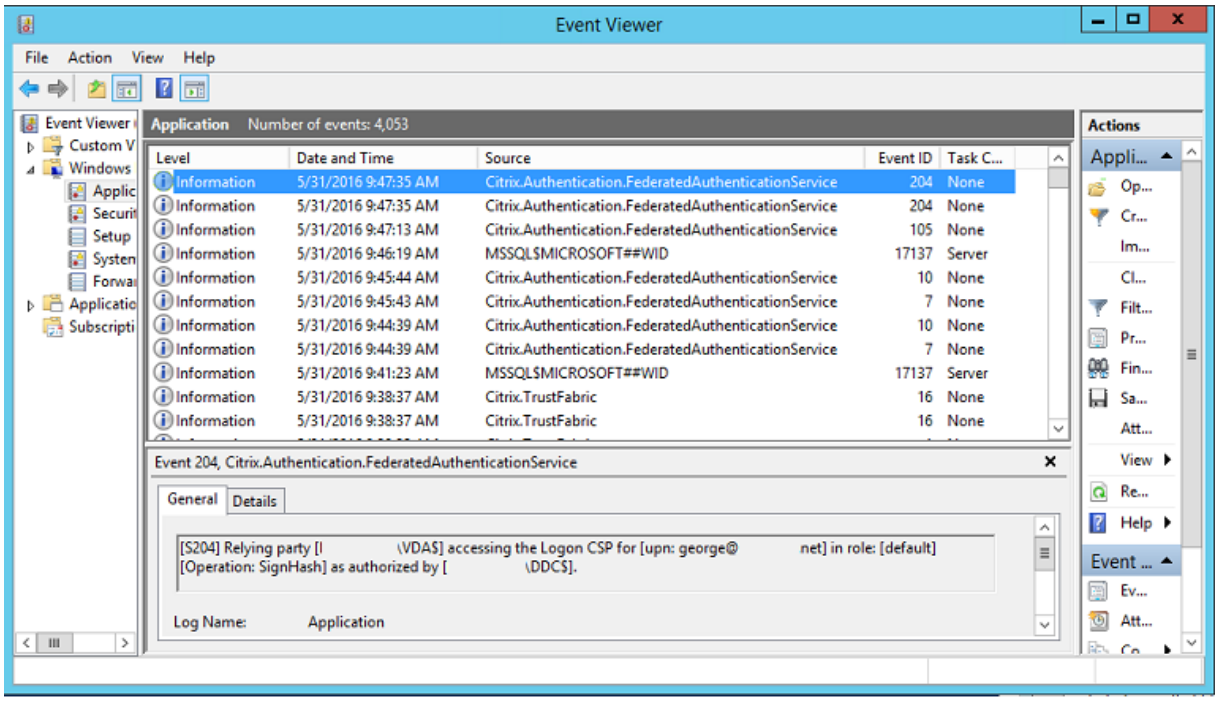
Instale FAS en el servidor de ADFS y configure una regla para que el Delivery Controller actúe como StoreFront de confianza (ya que, en este ejemplo, StoreFront está instalado en la misma máquina virtual que el Delivery Controller). Consulte Instalar y configurar.

Configurar StoreFront

Solicite un certificado de equipo para el Delivery Controller y configure IIS y StoreFront para usar HTTPS estableciendo un enlace de IIS para el puerto 443 y cambiando la dirección de base de datos de StoreFront a https:.

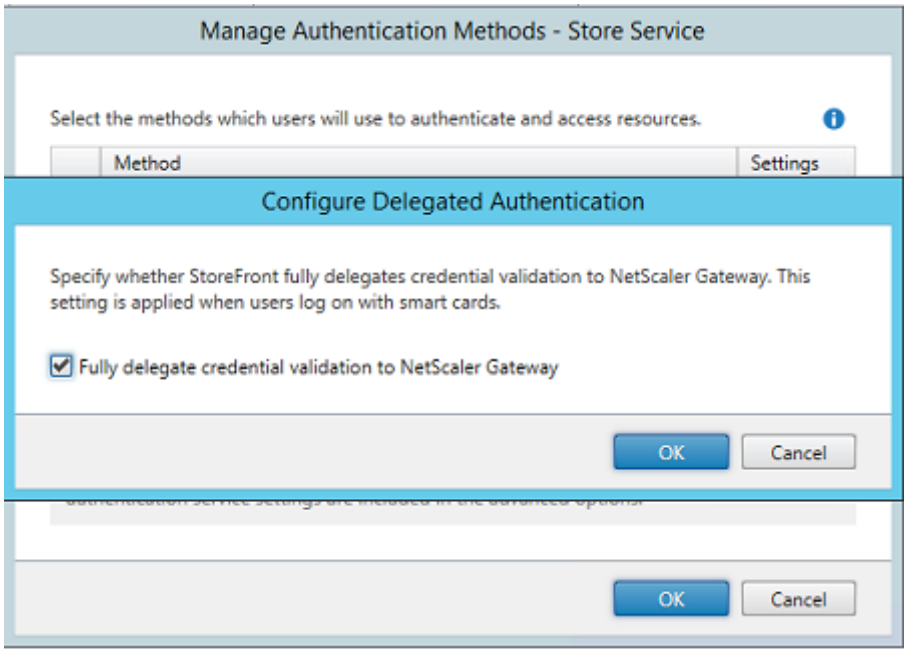


Configure StoreFront para usar el servidor de FAS (use el script de PowerShell que hay en Instalación y configuración) y haga pruebas internas dentro de Azure para asegurarse de que el inicio de sesión consulta el visor de eventos en el servidor de FAS para usar FAS.

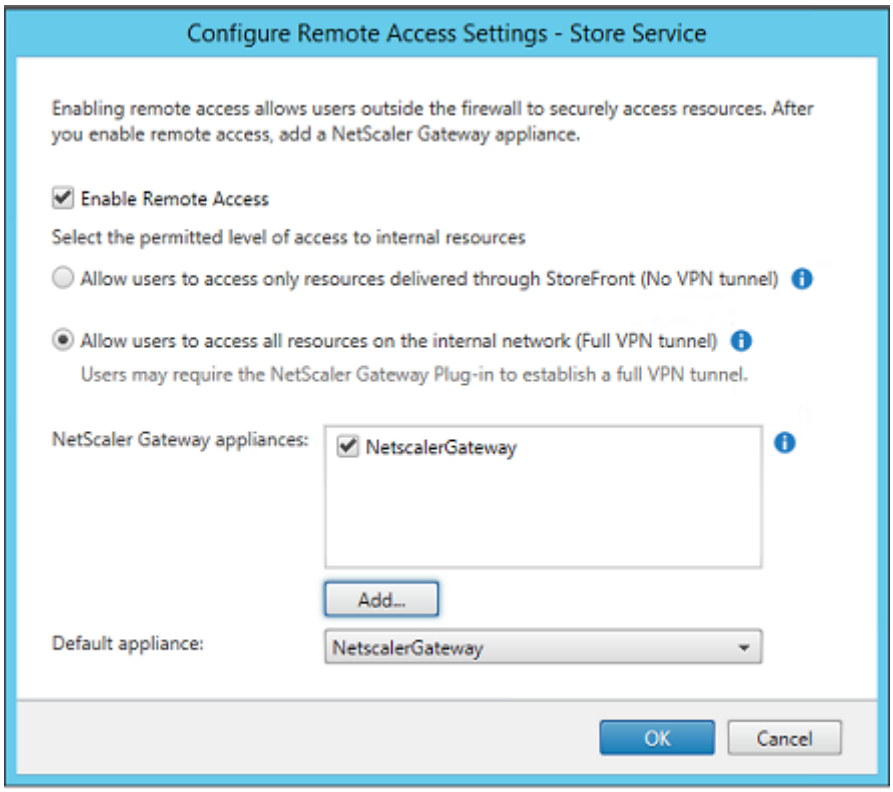


Configurar StoreFront para usar Citrix Gateway

Mediante la interfaz de usuario de **Administrar métodos de autenticación** en la consola de administración de StoreFront, configure StoreFront de modo que utilice Citrix Gateway para realizar la autenticación.

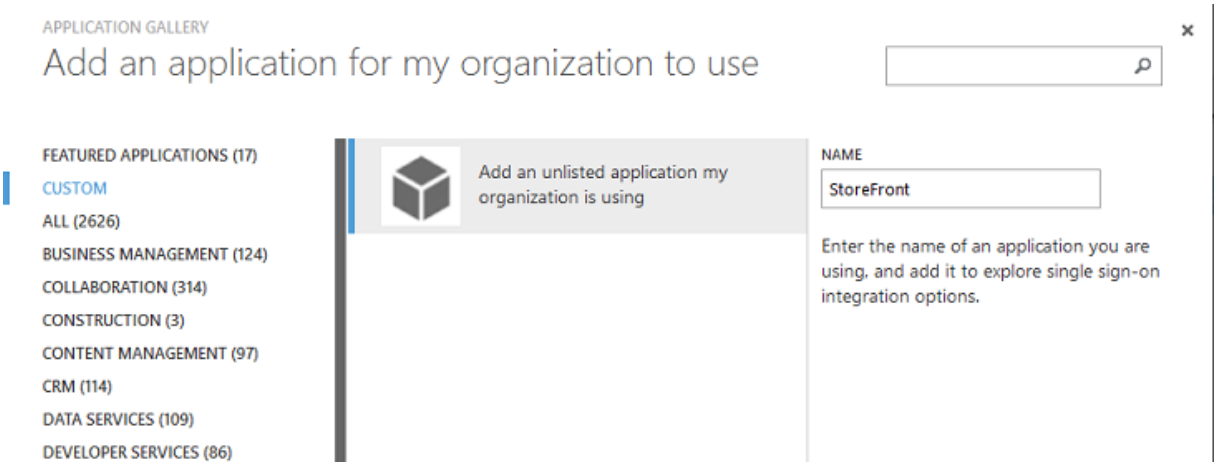


Para integrar las opciones de autenticación de Citrix Gateway, configure Secure Ticket Authority (STA) y la dirección de Citrix Gateway.



Configurar una nueva aplicación de Azure AD para inicios Single Sign-On en StoreFront

En esta sección se usan las funciones de Single Sign-On de Azure AD SAML 2.0, que actualmente requieren una suscripción de Azure Active Directory Premium. En la herramienta de administración de Azure AD, seleccione **Nueva aplicación** y elija **Agregar una aplicación de la galería**.



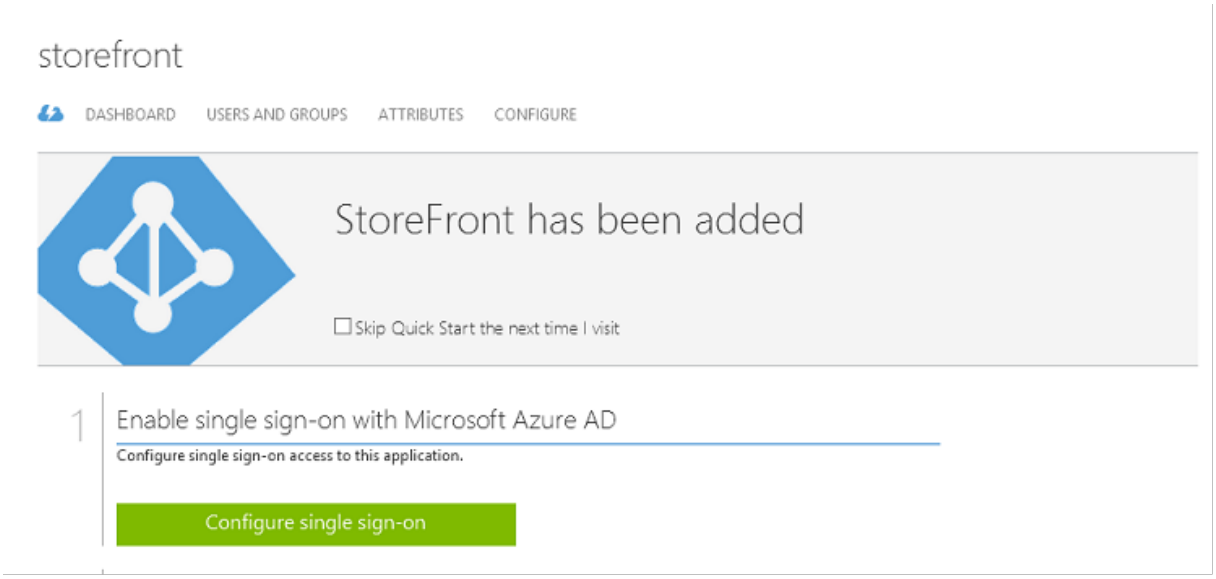
Seleccione **Personalizado > Agregar una aplicación que no figura en la lista que mi organización está usando** para crear una nueva aplicación personalizada para los usuarios.

Configurar un icono

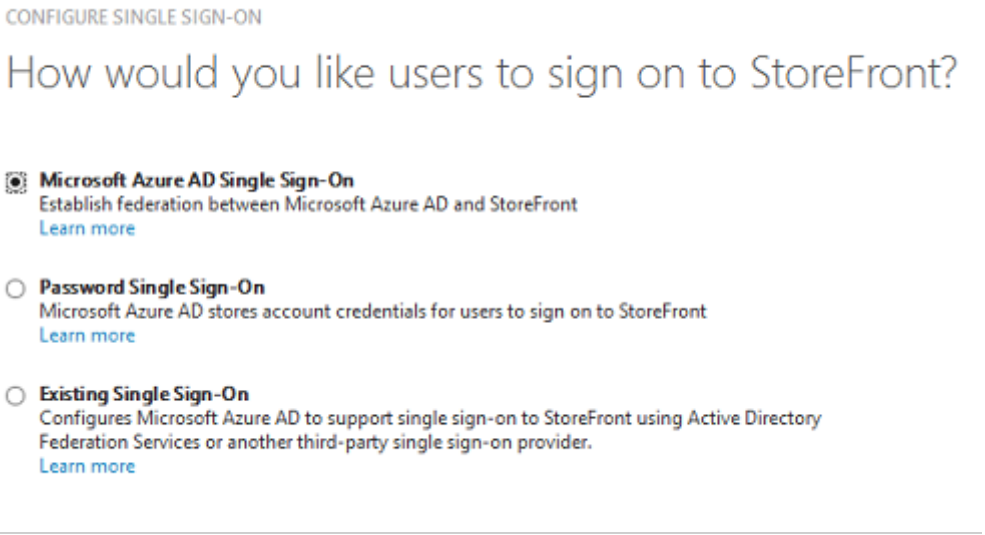
Cree una imagen de 215 x 215 píxeles de tamaño y cárguela en la página CONFIGURAR para usarla como icono de la aplicación.

Configurar la autenticación SAML

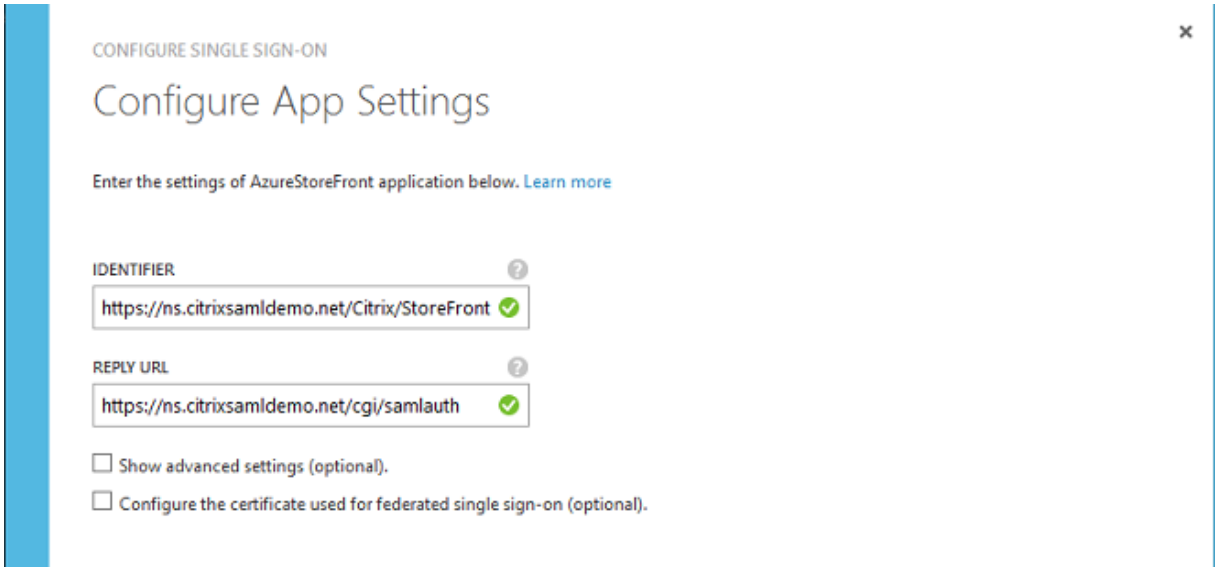
Vuelva a la página introductoria Panel de la aplicación y seleccione **Configurar Single Sign-On**.



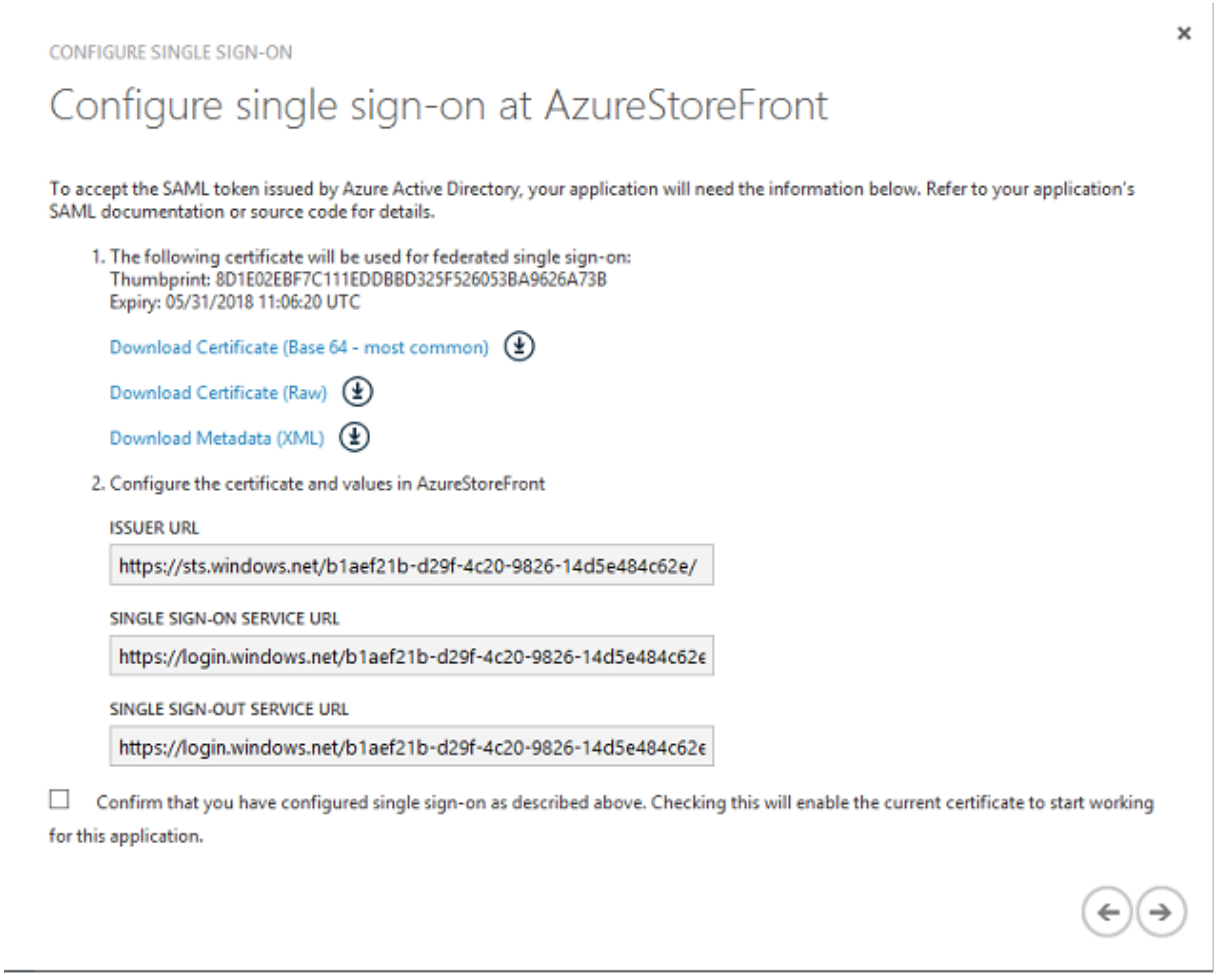
Esta implementación utilizará la autenticación SAML 2.0, que corresponde a **Microsoft Azure AD Single Sign-On**.



La cadena de identificación **Identifier** puede ser una arbitraria (debe coincidir con la configuración suministrada a Citrix Gateway); en este ejemplo, la **URL de respuesta**, Reply URL, es */cgi/samlauth* en el servidor Citrix Gateway.



La siguiente página contiene información que se usa para configurar Citrix Gateway como una entidad de confianza para Azure AD.

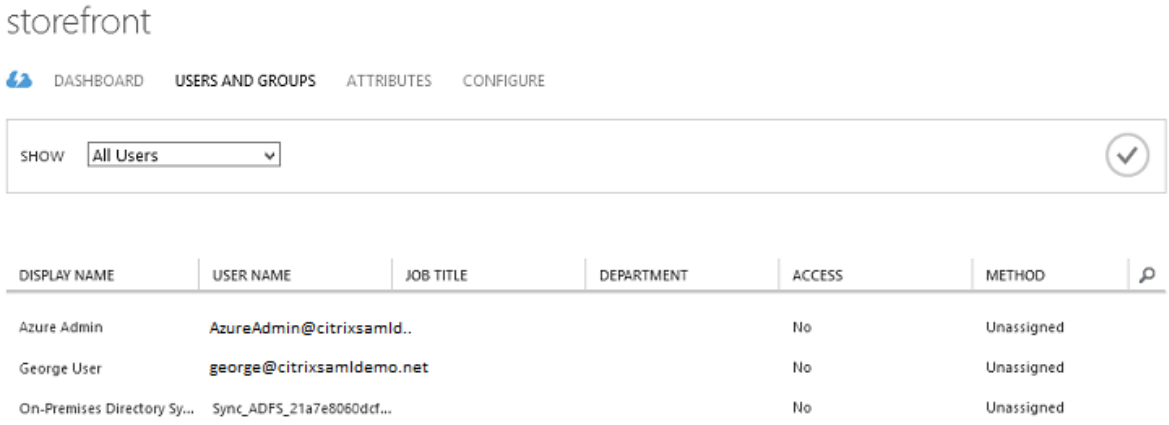


Descargue el certificado de firma de confianza de base 64 y copie las URL de inicio y cierre de sesión.

Pegará estas URL en las pantallas de configuración de Citrix Gateway más adelante.

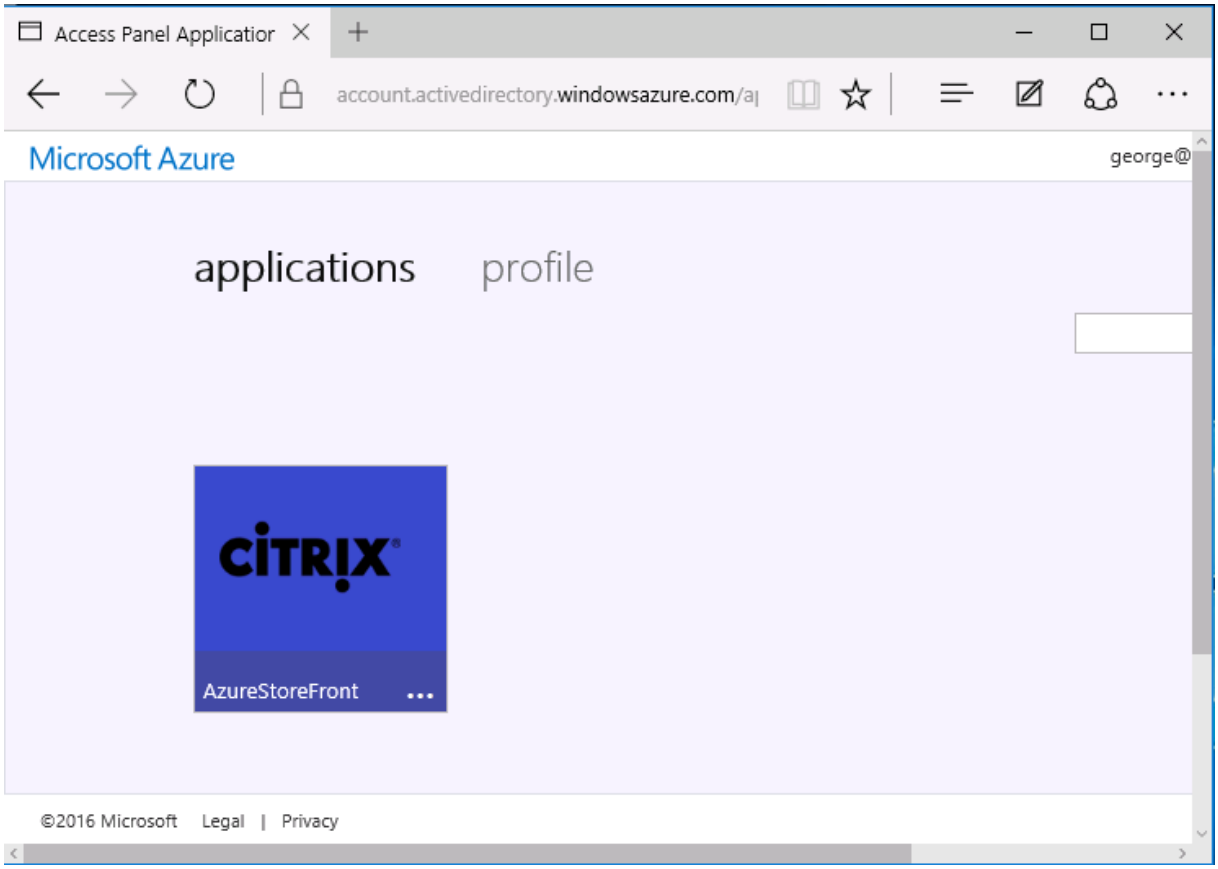
Asignar la aplicación a los usuarios

El paso final es habilitar la aplicación de modo que aparezca en la página de control "myapps.microsoft.com" de los usuarios. Esto se realiza en la página Usuarios y grupos. Asigne acceso para las cuentas de usuarios de domino sincronizadas por Azure AD Connect. También puede usar otras cuentas, pero deben estar explícitamente asignadas, porque no cumplen el formato <usuario>@<dominio>.



Página MyApps

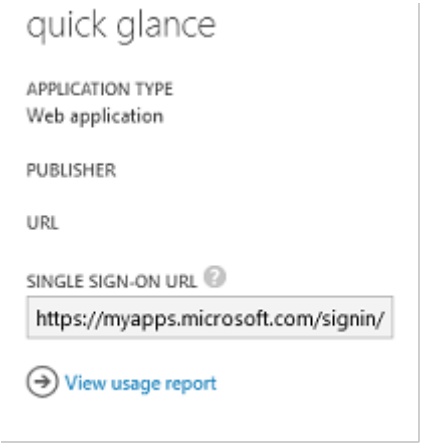
Cuando la aplicación se ha configurado, aparece en las listas de los usuarios de las aplicaciones de Azure cuando visitan https://myapps.microsoft.com.



Cuando está unido a Azure AD, Windows 10 admite el inicio de sesión único Single Sign-On en las aplicaciones de Azure para el usuario que inicie sesión. Al hacer clic en el icono, el explorador va a la página de SAML cgi/samlauth que se configuró anteriormente.

URL de Single Sign-On

Vuelva a la aplicación en el panel de mandos de Azure AD. Ahora hay una URL de Single Sign-On disponible para la aplicación. Esta dirección URL se utiliza para proporcionar enlaces de explorador web o crear accesos directos del menú Inicio que llevan a los usuarios directamente a StoreFront.



Pegue la dirección URL en un explorador web para asegurarse de que Azure AD le redirige a la página web de Citrix Gateway cgi/samlauth configurada anteriormente. Este sistema funciona solamente para los usuarios que se han asignado y ofrecerá inicio de sesión único Single Sign-On solo para sesiones de inicio de sesión en Windows 10 unido a Azure AD. (A otros usuarios se les pedirán credenciales de Azure AD.)

Instalar y configurar Citrix Gateway

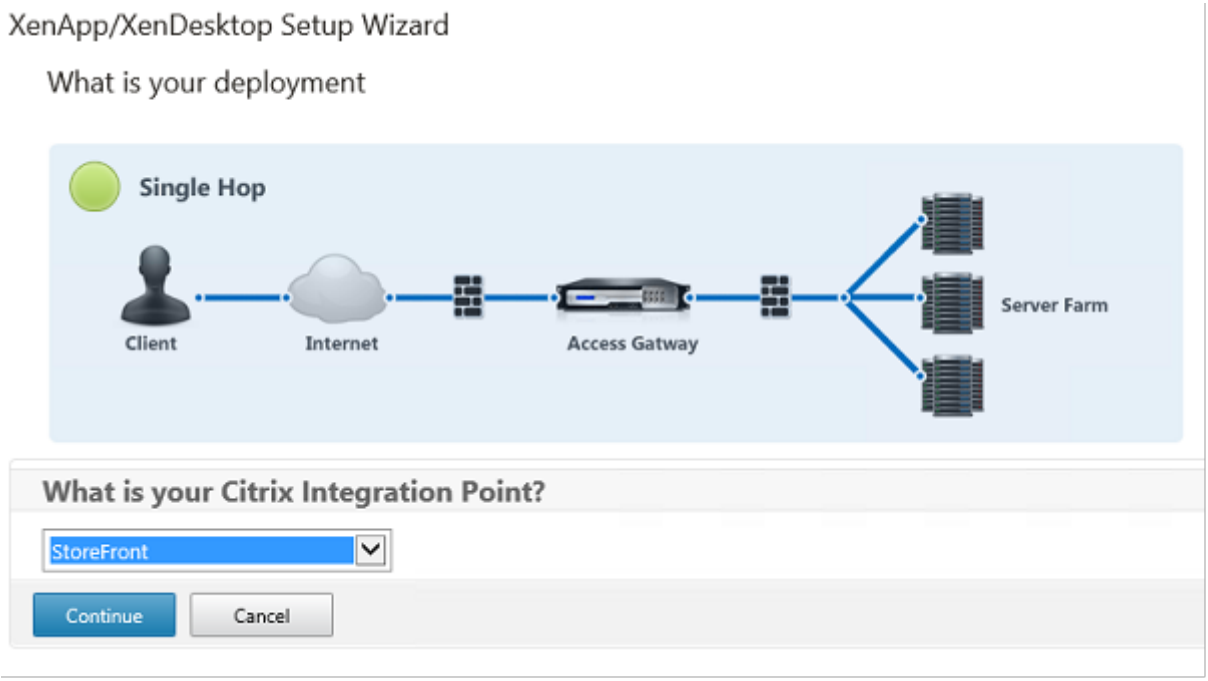
Para acceder de manera remota a la implementación, en este ejemplo se utiliza una VM independiente que ejecuta NetScaler (ahora Citrix Gateway). Esta VM se puede adquirir en Azure Store. En este ejemplo, se usa la opción "Bring your own License"de NetScaler 11.0.

Inicie sesión en la VM de NetScaler y apunte el explorador web a la dirección IP interna con las credenciales especificadas cuando el usuario se autenticó. Tenga en cuenta que se debe cambiar la contraseña del usuario nsroot en una VM de Azure AD.

Agregue licencias, seleccionando **reboot** después de agregar cada una de ellas, y apunte la resolución DNS al controlador de dominio de Microsoft.

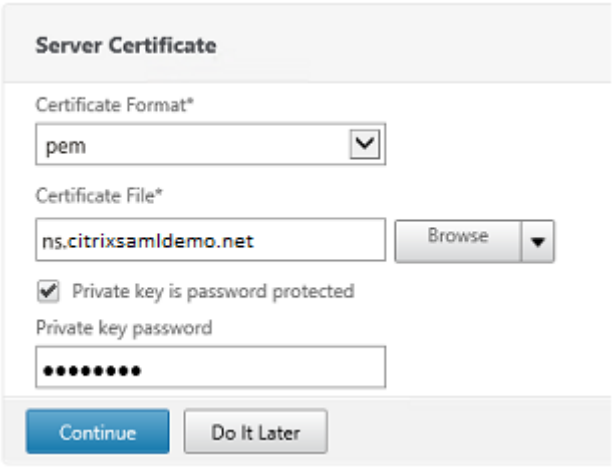
Ejecutar el asistente de configuración de Citrix Virtual Apps and Desktops

Este ejemplo empieza configurando una integración simple de StoreFront sin SAML. Una vez que esta implementación está funcionando, agrega una directiva de inicio de sesión de SAML.



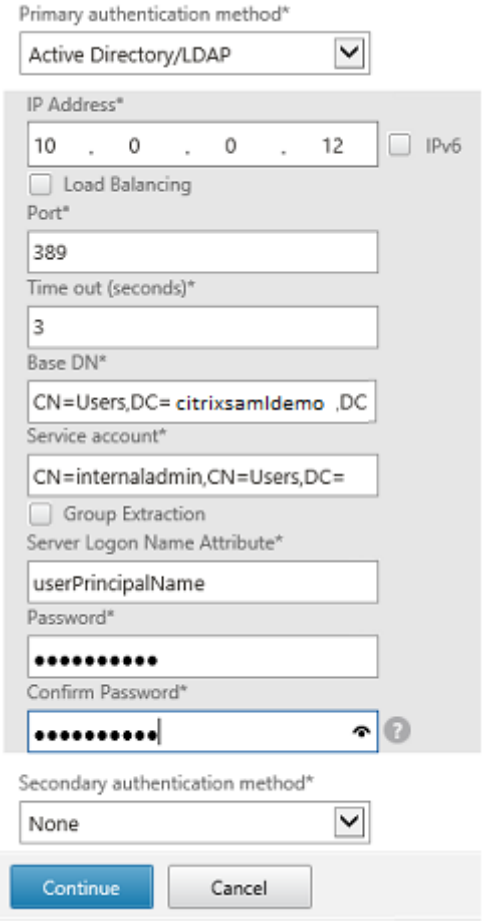
Seleccione la configuración estándar de Citrix Gateway para StoreFront. Para usarlo en Microsoft Azure, en este ejemplo se configura el puerto 4433, en lugar del puerto 443. De forma alternativa, puede redirigir el puerto o reasignar el sitio web de administración de Citrix Gateway.

Para simplificar las tareas, el ejemplo carga un certificado de servidor existente y una clave privada guardada en un archivo.



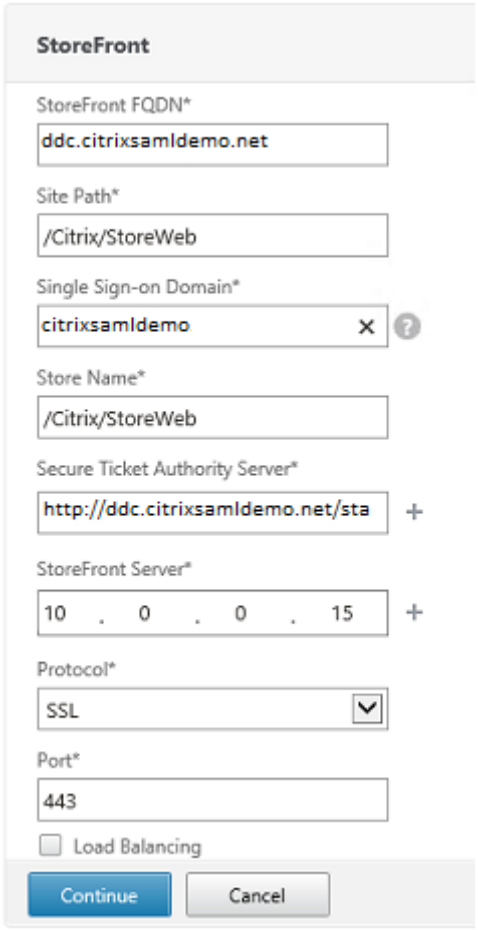
Configurar el controlador de dominio para la administración de cuentas de AD

El controlador de dominio se usará para la resolución de cuentas, por lo que hay que agregar su dirección IP en el método de autenticación principal. Tenga en cuenta el formato esperado en cada campo en el cuadro de diálogo.



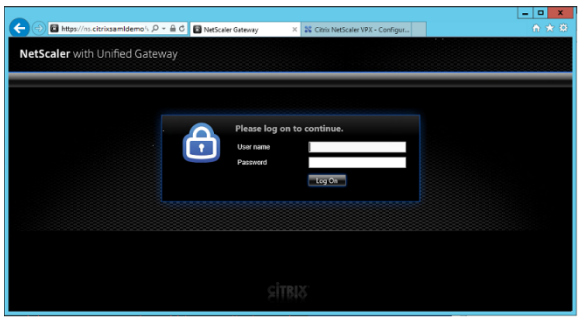
Configurar la dirección de StoreFront

En este ejemplo, StoreFront se ha configurado con HTTPS; por lo tanto, seleccione las opciones de protocolo SSL.



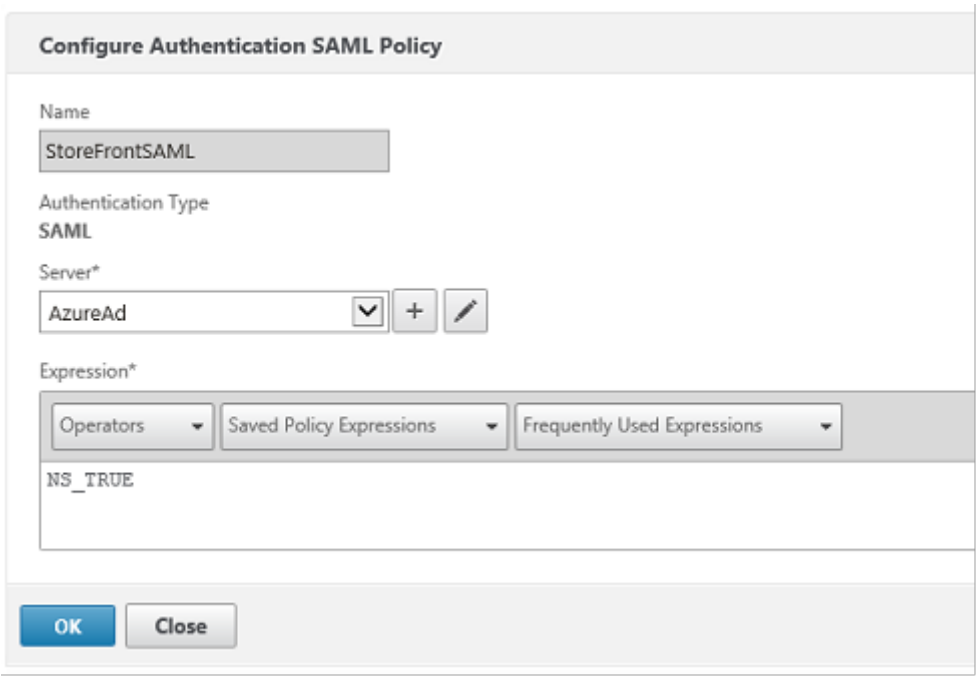
Verificar la implementación de Citrix Gateway

Conéctese a Citrix Gateway y compruebe que la autenticación y el inicio se realizan correctamente con el nombre de usuario y la contraseña.

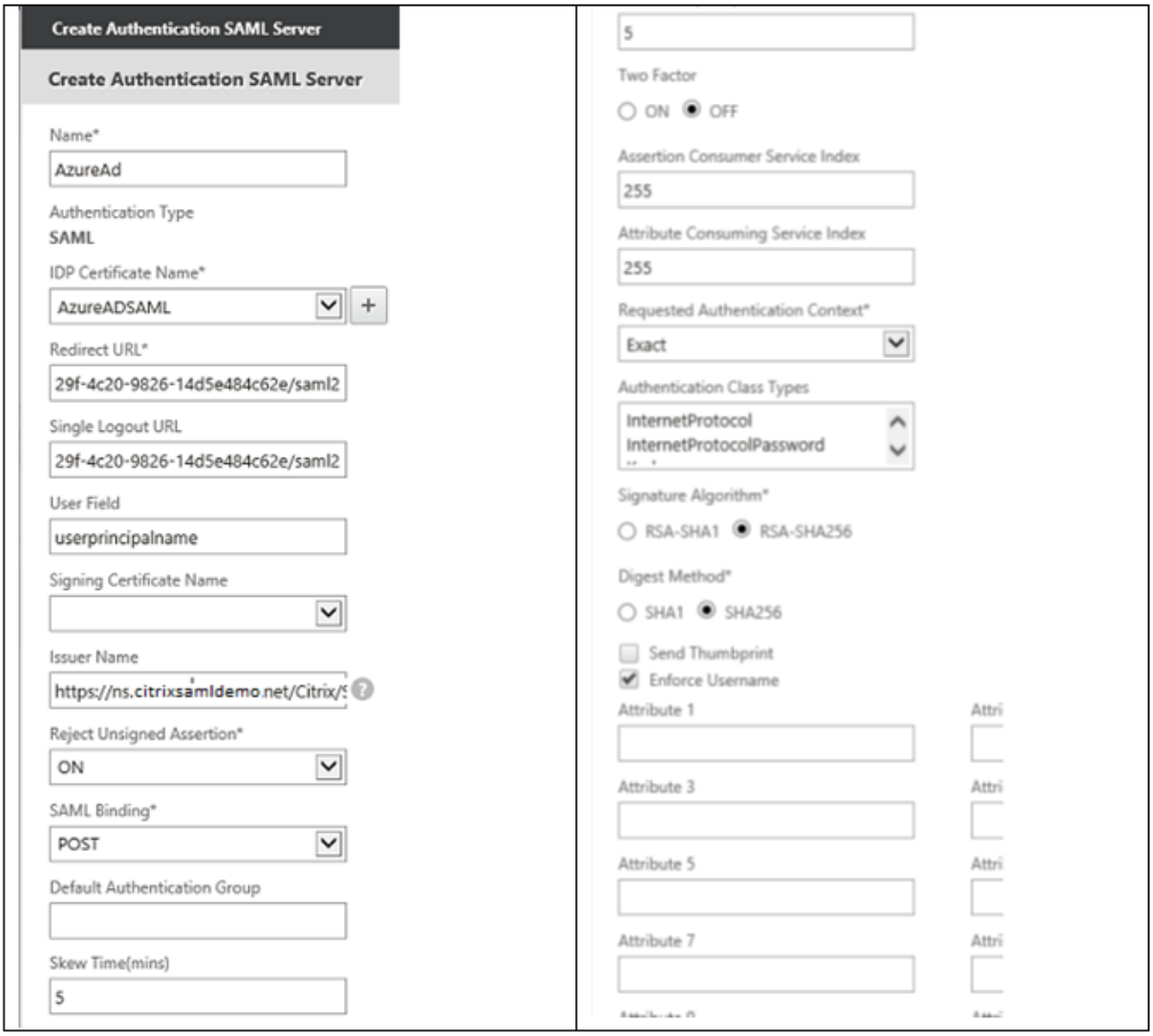


Habilitar la compatibilidad con la autenticación SAML de Citrix Gateway

El uso de SAML con StoreFront es similar al uso de SAML con otros sitios web. Agregue una nueva directiva de SAML con una expresión de **NS_TRUE**.



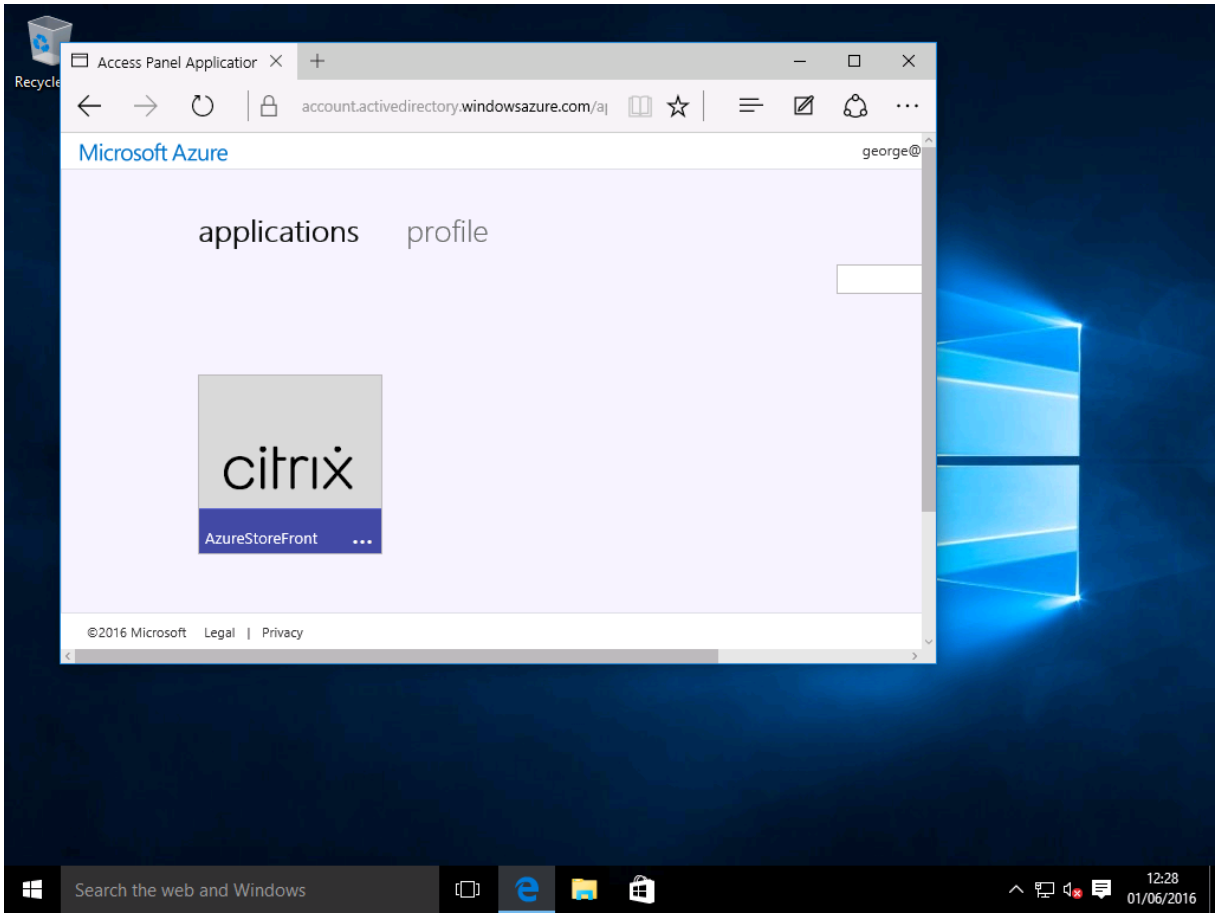
Configurar el servidor de identidades SAML, mediante la información obtenida de Azure AD previamente.



Verificar el sistema de extremo a extremo

Inicie sesión en un escritorio de Windows 10 unido a Azure AD con una cuenta registrada en Azure AD. Inicie Microsoft Edge y conéctese a: https://myapps.microsoft.com.

El explorador web debe mostrar las aplicaciones de Azure AD para el usuario.



Compruebe que hacer clic en el icono que se le redirige a un servidor de StoreFront autenticado.

Del mismo modo, compruebe que las conexiones directas a través de la URL de Single Sign-On y una conexión directa con el sitio de Citrix Gateway le redirigen a Microsoft Azure y viceversa.

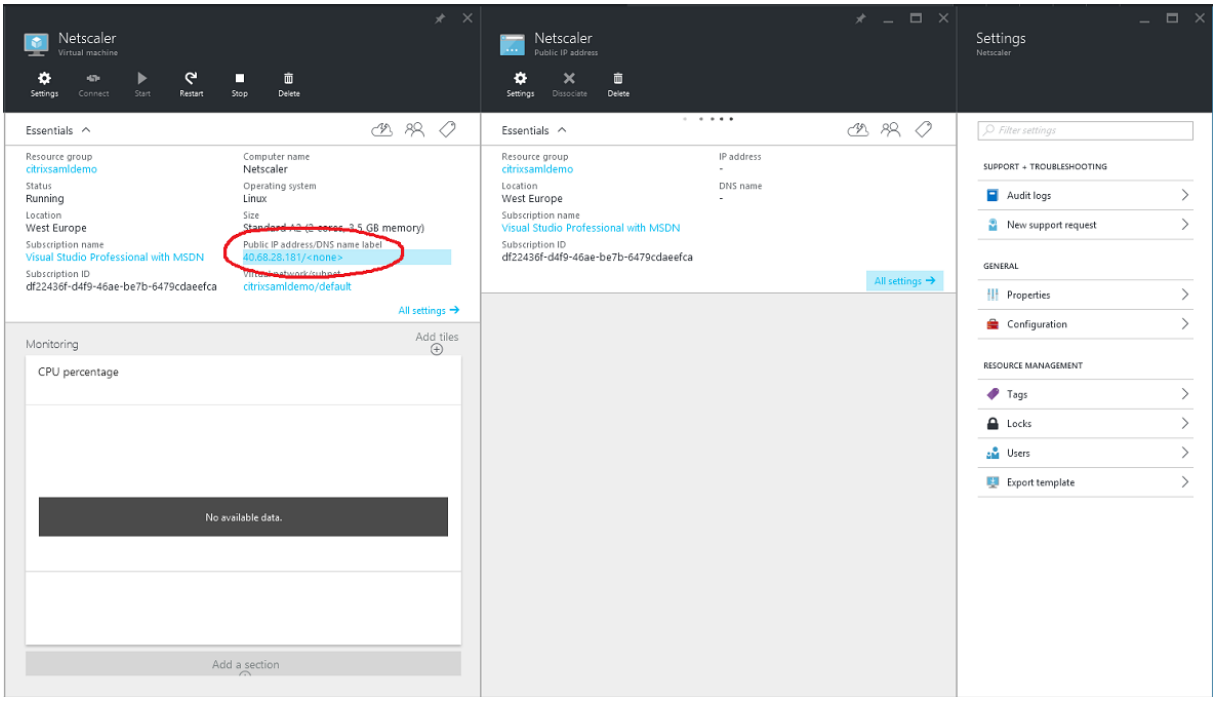
Finalmente, compruebe que las máquinas que no están unidas a Azure AD también funcionan con las mismas direcciones URL (aunque habrá un único inicio de sesión explícito a Azure AD para la primera conexión).

Apéndice

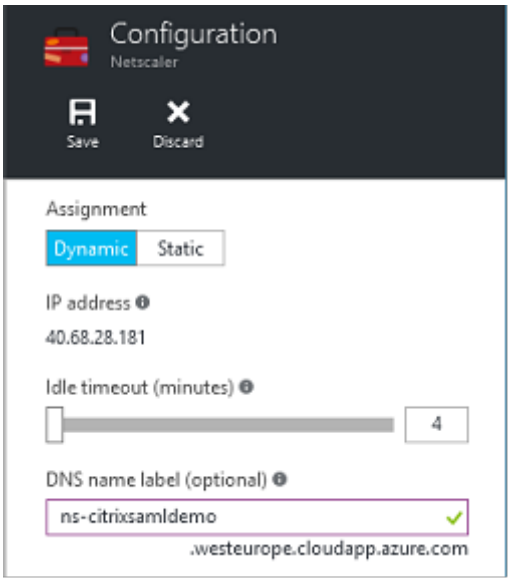
Debe configurar las siguientes opciones estándar cuando configure una máquina virtual en Azure.

Proporcionar una dirección IP pública y una dirección DNS

Azure da a todas las VM una dirección IP en la subred interna (10.*.*.* en este ejemplo). De forma predeterminada, también se proporciona una dirección IP pública a la que se puede hacer referencia mediante una etiqueta DNS actualizada dinámicamente.



Seleccione **Configuration** en **Public IP address/DNS name label**. Elija una dirección DNS pública para la VM. Se puede usar para las referencias de CNAME en otros archivos de zona DNS, asegurándose de que todos los registros DNS quedan apuntando correctamente a la VM incluso aunque la dirección IP se reasigne.

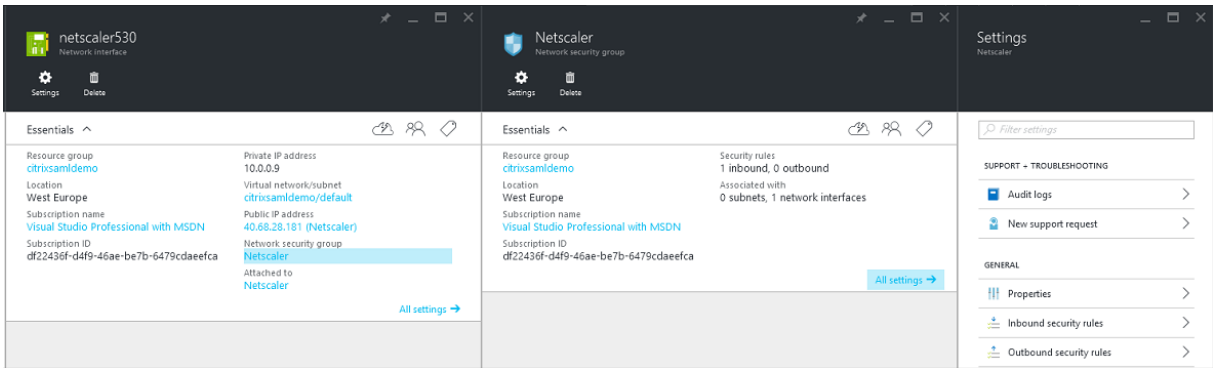


Configurar las reglas de firewall (grupo de seguridad)

Cada VM en una nube tiene un conjunto de reglas de firewall que se aplican automáticamente, lo que se conoce como el grupo de seguridad. El grupo de seguridad controla el tráfico reenviado desde la

dirección IP privada a la pública. De forma predeterminada, Azure permite el reenvío de RDP a todas las VM. Los servidores Citrix Gateway y ADFS también deben reenviar el tráfico TLS (443).

Abra **Network Interfaces** en una VM, y luego haga clic en la etiqueta **Network Security Group**. Configure **Inbound security rules** para permitir el tráfico de red apropiado.



Información relacionada

- Instalación y configuración es la referencia principal para la instalación y la configuración de este servicio.
- Las implementaciones más comunes de FAS se resumen en el artículo Arquitecturas de implementación.
- En Configuración avanzada, se presentan artículos de "procedimientos".

Configuración avanzada

March 30, 2023

Los artículos de procedimientos de esta sección contienen instrucciones para la configuración y administración avanzadas del servicio de autenticación federada (FAS).

Información relacionada

- El artículo Instalación y configuración es la referencia principal para la instalación y la configuración inicial de FAS.
- En el artículo Arquitecturas de implementación, se ofrece un resumen de las principales arquitecturas de FAS, además de enlaces a otros artículos sobre arquitecturas más complejas.

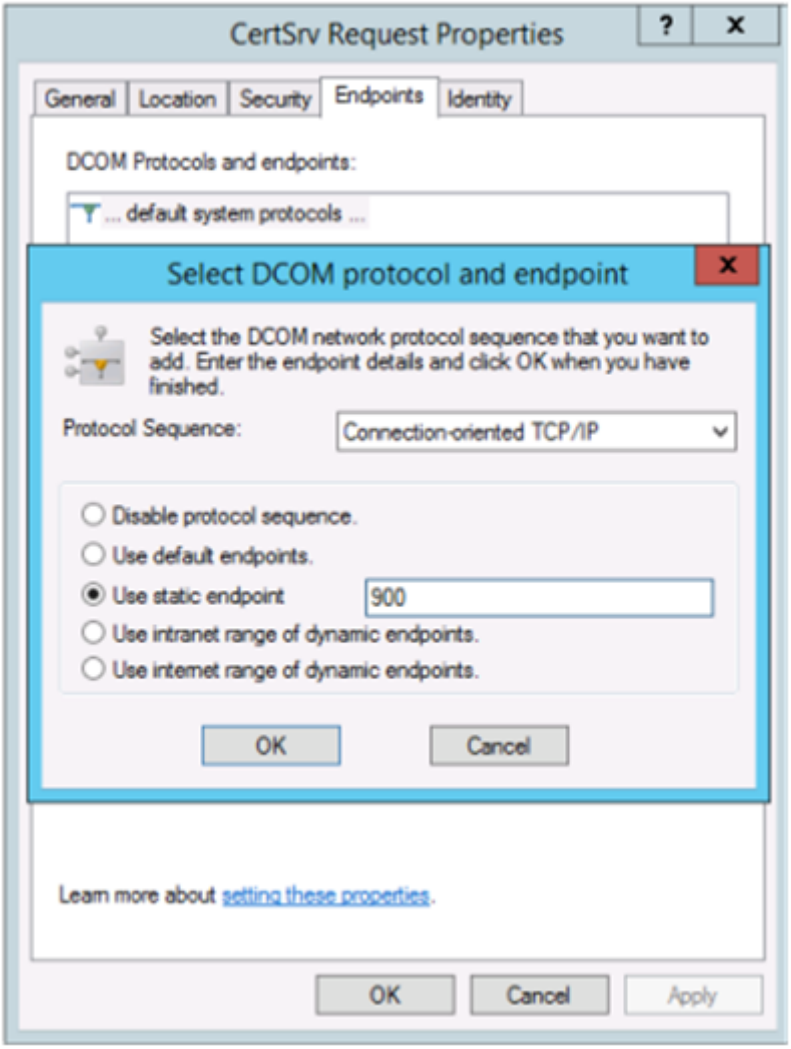
Configuración de entidades de certificación

March 30, 2023

En este artículo, se describe la configuración avanzada del Servicio de autenticación federada (FAS) para que se integre con los servidores de la entidad de certificación que no admite la consola de administración de FAS. En las instrucciones, se usan las API de PowerShell que suministra el servicio FAS. Debe tener conocimientos básicos de PowerShell para poder ejecutar las instrucciones de este artículo.

Configurar la entidad de certificación de Microsoft para el acceso por TCP

De forma predeterminada, la entidad de certificación de Microsoft utiliza DCOM para el acceso. Esto puede provocar complicaciones cuando se implemente la seguridad del firewall, por lo que Microsoft puede cambiar a un puerto TCP estático. En la entidad de certificación de Microsoft, abra el panel de configuración de DCOM y modifique las propiedades de "CertSrv Request":



Cambie los "puntos finales"para seleccionar un dispositivo de punto final estático y especifique un número de puerto TCP (900 en la imagen de arriba).

Reinicie la entidad de certificación de Microsoft y envíe una solicitud de certificado. Si ejecuta `netstat –a –n –b`, debería ver que ahora certsvr escucha en el puerto 900:

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

No es necesario configurar el servidor del servicio FAS (o cualquier otra máquina que use la entidad de certificación) porque DCOM tiene una fase de negociación que usa el puerto RPC. Cuando un cliente quiere usar DCOM, se conecta al servicio de RPC de DCOM que está presente en el certificado de servidor y solicita acceso a un servidor DCOM determinado. Esta acción abre el puerto 900, y el servidor

DCOM indica al servidor de FAS cómo conectarse.

Generar previamente los certificados de usuario

El tiempo de inicio de sesión mejora significativamente para los usuarios si los certificados de usuario se generan previamente en el servidor de FAS. En las siguientes secciones, se describe cómo hacerlo con uno o varios servidores de FAS.

Obtener una lista de usuarios de Active Directory

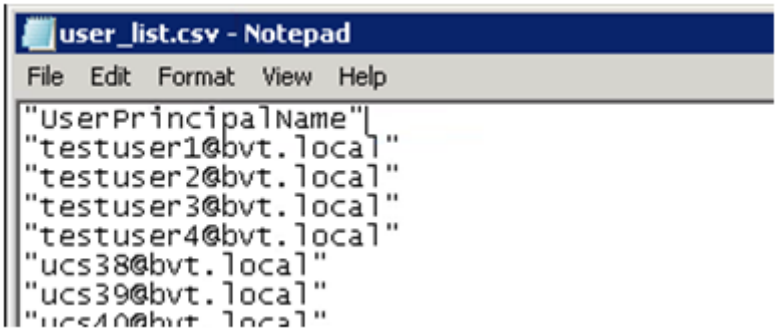
Puede mejorar la generación de certificados si consulta AD y almacena la lista de usuarios en un archivo (por ejemplo, un archivo CSV), como se muestra en el siguiente ejemplo.

```
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
 }

<!--NeedCopy-->
```

Get-ADUser es un cmdlet estándar para consultar una lista de usuarios. El ejemplo anterior contiene un argumento de filtro para incluir en la lista solo a los usuarios con un UserPrincipalName y un estado de cuenta “enabled”(habilitado).

El argumento SearchBase limita la parte de Active Directory en que buscar usuarios. Puede omitirlo si quiere incluir a todos los usuarios de AD. Nota: Es posible que esta consulta devuelva una gran cantidad de usuarios.

El archivo CSV tiene un aspecto similar a:



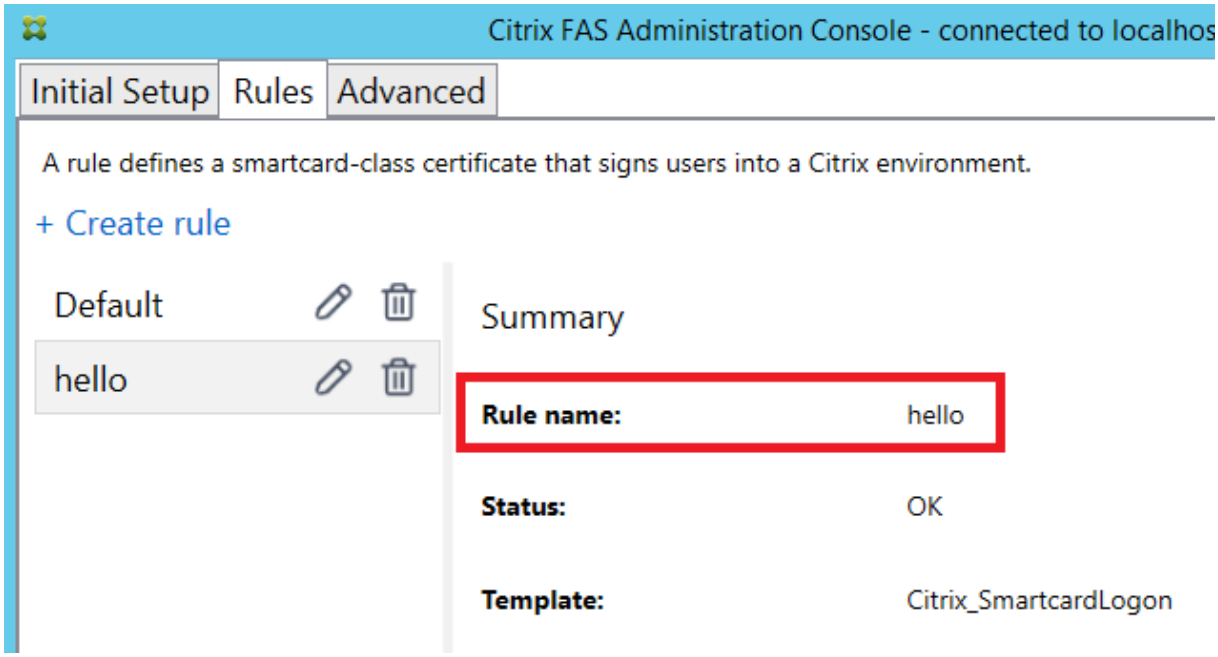
Servidor de FAS

El siguiente script de PowerShell utiliza la lista de usuarios previamente generada y crea a partir de ella una lista de los certificados de usuario.

```
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
     }

 }

<!--NeedCopy-->
```

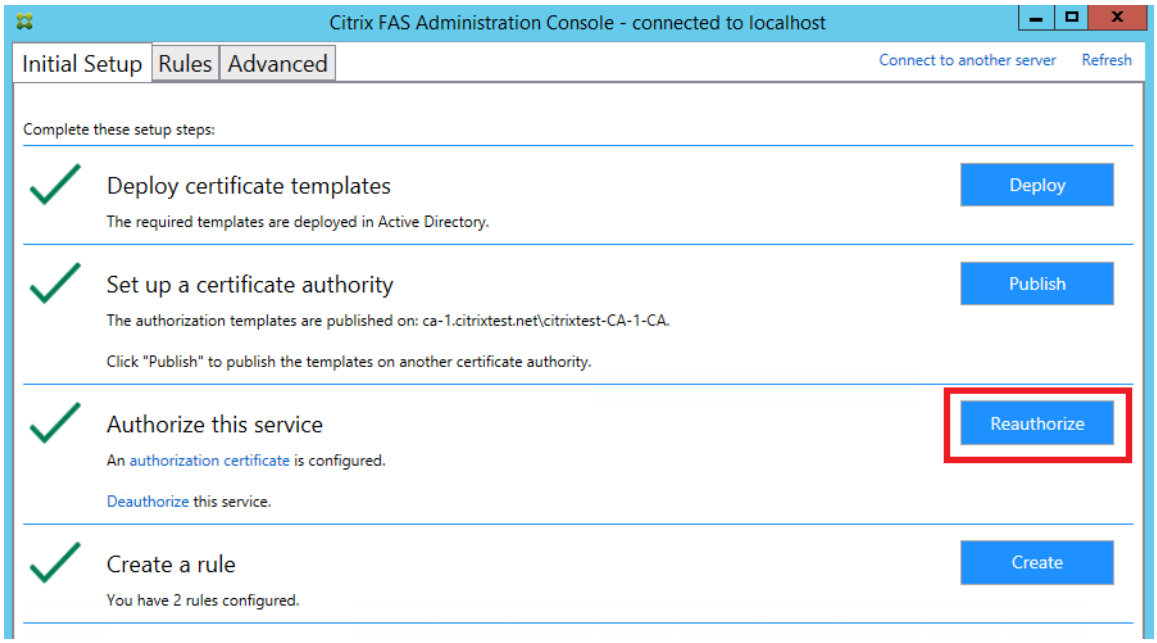
Si dispone de varios servidores de FAS, el certificado de un usuario concreto se generará dos veces: uno en el servidor principal y otro en el servidor de conmutación por error.

El script anterior está orientado a una regla denominada “default”. Si tiene otro nombre de regla (por ejemplo, “hola”), cambie la variable $rule en el script.



Renovar certificados de la entidad de registro

Si utiliza más de un servidor de FAS, puede renovar un certificado de autorización de FAS sin que ello afecte a los usuarios con sesión iniciada.

> **Nota:**
>
> También puede usar la interfaz gráfica de usuario para volver a autorizar FAS:
>
> 
>

Lleve a cabo los siguientes pasos:

1. Cree un nuevo certificado de autorización: `New-FasAuthorizationCertificate`
2. Escriba el GUID del nuevo certificado de autorización que devuelve: `Get-FasAuthorizationCertific`
3. Coloque el servidor de FAS en el modo de mantenimiento: `Set-FasServer –Address <FAS server> -MaintenanceMode $true`
4. Cambie el nuevo certificado de autorización: `Set-FasCertificateDefinition –AuthorizationCertificate <GUID>`
5. Desactive el modo de mantenimiento del servidor de FAS: `Set-FasServer –Address <FAS server> -MaintenanceMode $false`
6. Elimine el certificado anterior de autorización: `Remove-FasAuthorizationCertificate`

Información relacionada

- El artículo Instalación y configuración es la referencia principal para la instalación y la configuración de este servicio.
- Las implementaciones más comunes del Servicio de autenticación federada se resumen en el artículo Arquitecturas de implementación.
- En Configuración avanzada, se presentan otros artículos de "procedimientos".

Protección de claves privadas

March 30, 2023

Introducción

Las claves privadas se almacenan por medio de la cuenta de servicio de red y, de forma predeterminada, se marcan como elementos que no se pueden exportar.

Hay dos tipos de claves privadas:

- La clave privada asociada al certificado de la autoridad de registro, procedente de la plantilla de certificado Citrix_RegistrationAuthority.
- La clave privada asociada a los certificados de usuario, procedente de la plantilla de certificado Citrix_SmartcardLogon.

En realidad, existen dos certificados de autoridad de registro: Citrix_RegistrationAuthority_ManualAuthorization (válido durante 24 horas de forma predeterminada) y Citrix_RegistrationAuthority (válido durante dos años de forma predeterminada).

En el paso 3 de la ficha **Instalación inicial** en la consola de administración del servicio de autenticación federada, cuando al hacer clic en **Autorizar**, el servidor de FAS genera un par de claves y envía una solicitud de firma de certificado a la entidad de certificación para el certificado Citrix_RegistrationAuthority_ManualAuthorization. Se trata de un certificado temporal, válido durante 24 horas de forma predeterminada. La entidad de certificación no emite automáticamente el certificado, por lo que un administrador debe autorizar manualmente la emisión en ella. Una vez emitido el certificado al servidor de FAS, el servicio FAS utiliza el certificado Citrix_RegistrationAuthority_ManualAuthorization para obtener automáticamente el certificado Citrix_RegistrationAuthority (cuya validez predeterminada es de dos años). El servidor de FAS elimina el certificado y la clave de Citrix_RegistrationAuthority_ManualAuthorization tan pronto como obtiene el certificado Citrix_RegistrationAuthority.

La clave privada asociada al certificado de la autoridad de registro debe ser especialmente confidencial, porque la directiva de certificados de autoridad de registro permite a quien posea la clave privada emitir solicitudes de certificado para el conjunto de usuarios configurados en la plantilla. Como consecuencia, quien posea esta clave puede conectarse al entorno como ninguno de los usuarios del conjunto.

Puede configurar el servidor de FAS para que proteja las claves privadas según los requisitos de seguridad de la empresa. Para ello, elija una de las siguientes opciones:

- El proveedor de servicios de cifrado RSA y AES mejorado de Microsoft o el proveedor de almacenamiento de claves (KSP) de software de Microsoft para las claves privadas del certificado de la autoridad de registro y de los certificados de usuario.
- El proveedor de almacenamiento de claves de la plataforma Microsoft con un chip del módulo de plataforma segura (TPM) para la clave privada del certificado de la autoridad de registro, y el proveedor de servicios de cifrado RSA y AES mejorado de Microsoft o el proveedor de almacenamiento de claves (KSP) de software de Microsoft para las claves privadas de los certificados de usuario.
- El proveedor de almacenamiento de claves o el servicio de cifrado del distribuidor, ambos con el módulo de seguridad de hardware (HSM), para las claves privadas del certificado de autoridad de registro y de los certificados de usuario.

Parámetros de configuración de claves privadas

Configure el servicio de autenticación federada (FAS) para usar una de las tres opciones. En un editor de texto, modifique el archivo Citrix.Authentication.FederatedAuthenticationService.exe.config. La

ubicación predeterminada del archivo es la carpeta Archivos de programa\Citrix\Federated Authentication Service que se encuentra en el servidor de FAS.

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

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

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

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

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

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

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

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

FAS lee el archivo de configuración solo cuando se inicia el servicio. Si se cambian los valores, el servicio FAS debe reiniciarse para que se vea la nueva configuración.

Establezca los valores correspondientes en el archivo Citrix.Authentication.FederatedAuthenticationService.exe.co como se muestra a continuación:

Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.**ProviderLegacyCsp** (cambie entre CAPI y las API de CNG)

Valor	Comentario
true	Usar las API de CAPI
false (opción predeterminada)	Usar las API de CNG

Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.**ProviderName** (nombre del proveedor que se va a usar)

Valor	Comentario
Microsoft Enhanced RSA and AES Cryptographic Provider	Proveedor predeterminado de CAPI
Microsoft Software Key Storage Provider	Proveedor predeterminado de CNG

Valor	Comentario
Microsoft Platform Key Storage Provider	Proveedor predeterminado de TPM. Tenga en cuenta que TPM no se recomienda para las claves de usuario. Utilice TPM solamente para la clave de autoridad de registro. Si quiere ejecutar el servidor de FAS en entornos virtualizados, consulte al distribuidor de TPM y del hipervisor si se admite la virtualización.
HSM_Vendor CSP/Proveedor de almacenamiento de claves	Facilitado por el distribuidor de HSM. El valor difiere de un distribuidor a otro. Si quiere ejecutar el servidor de FAS en entornos virtualizados, consulte al distribuidor de HSM si se admite la virtualización.

Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.**ProviderType** (obligatorio solo en caso de API de CAPI)

Valor	Comentario
24	Predeterminado. Se refiere a Microsoft KeyContainerPermissionAccessEntry.ProviderType Property PROV_RSA_AES 24. Debe ser siempre 24 a menos que esté usando un HSM con CAPI y el proveedor de HSM especifique otra cosa.

Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.**KeyProtection** (Cuando se necesita que el servicio FAS realice una operación de clave privada, este utiliza el valor especificado aquí) Controla el indicador "exportable"de las claves privadas. Permite el uso del almacenamiento de claves de TPM, si lo admite el hardware.

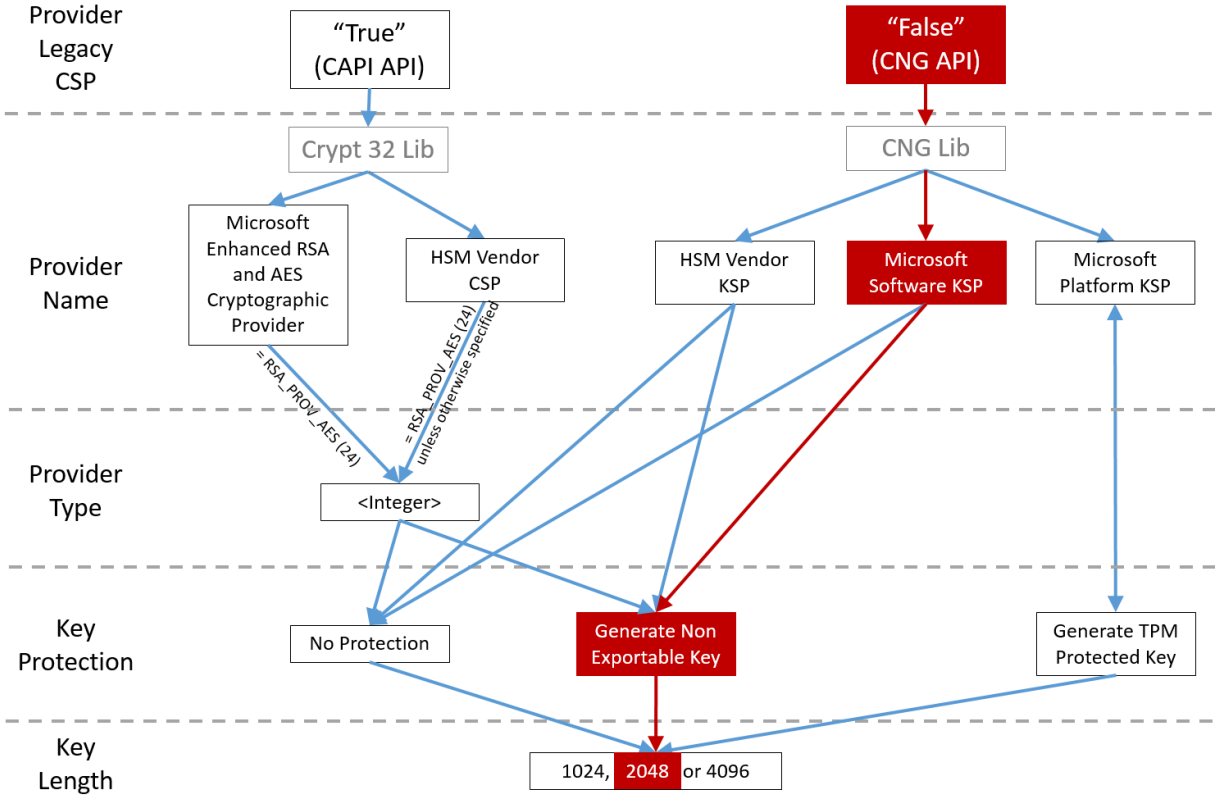
Valor	Comentario
NoProtection	Se puede exportar la clave privada.
GenerateNonExportableKey	Predeterminado. No se puede exportar la clave privada.

Valor	Comentario
GenerateTPMProtectedKey	La clave privada se administrará mediante TPM. La clave privada se almacena mediante el nombre de proveedor que especifique en ProviderName (por ejemplo, el proveedor de almacenamiento de claves de la plataforma Microsoft).

Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.**KeyLength** (especifique el tamaño de la clave privada en bits)

Valor	Comentario
2048	Valor predeterminado. También se puede usar 1024 o 4096.

A continuación, se muestran los parámetros del archivo de configuración representados gráficamente (las opciones de instalación predeterminadas aparecen en rojo):



Ejemplos de configuración

Ejemplo 1

En este ejemplo, la clave privada del certificado de autoridad de registro y las claves privadas de los certificados de usuario se almacenan con el proveedor de almacenamiento de claves de software de Microsoft.

Esta es la configuración predeterminada tras la instalación. No se necesita configurar ninguna clave privada adicional.

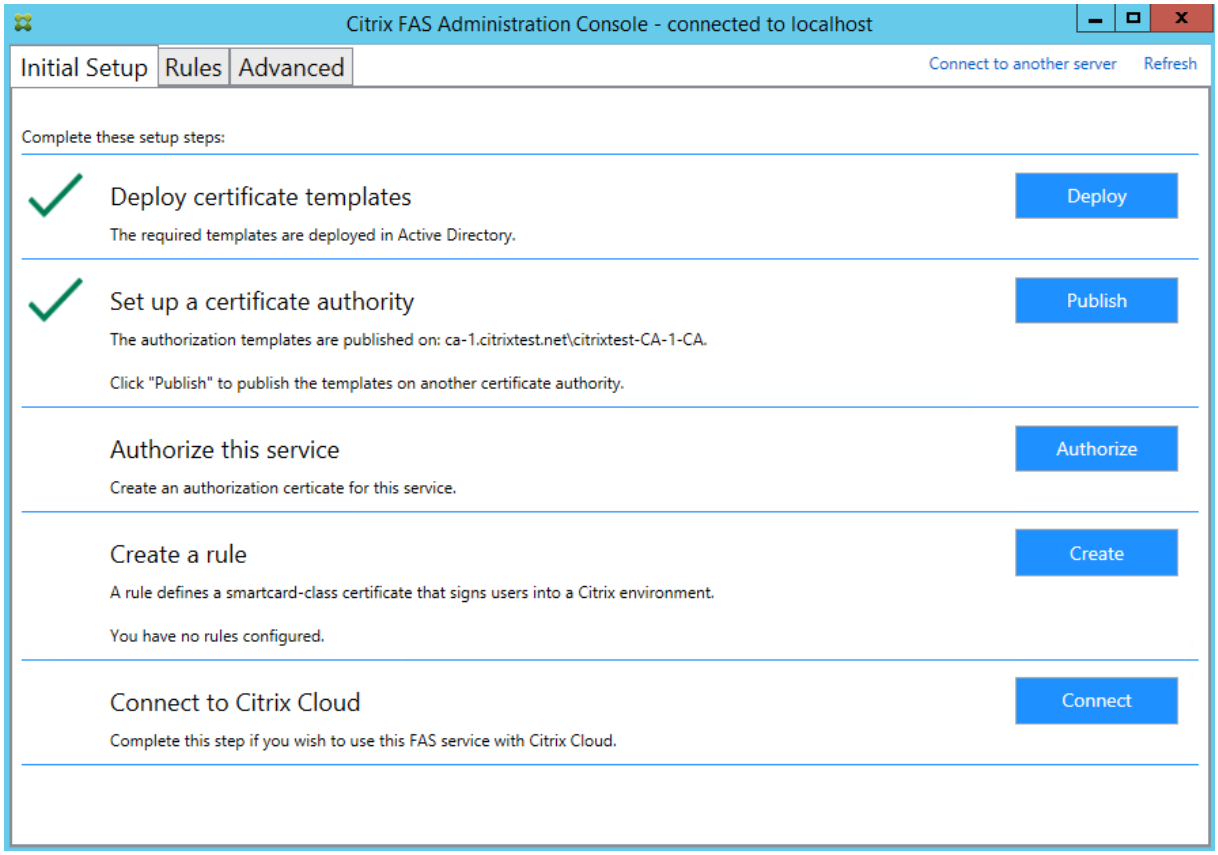
Ejemplo 2

En este ejemplo, la clave privada del certificado de autoridad de registro se almacena en el hardware TPM de la placa base del servidor de FAS con el proveedor de almacenamiento de claves de la plataforma Microsoft, mientras que las claves privadas de los certificados de usuario se almacenan con el proveedor de almacenamiento de claves (KSP) de software de Microsoft.

En este caso, se presupone que el TPM de la placa madre del servidor de FAS se ha habilitado en BIOS (siguiendo la documentación del fabricante del TPM) y, a continuación, se ha inicializado en Windows; consulte https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-vista/cc749022(v=ws.10).

Mediante la consola de administración de FAS La consola de administración de FAS no puede realizar solicitudes de firma de certificado sin conexión, por lo que no se recomienda utilizarla a menos que su organización permita la solicitud de firma de certificado en línea para certificados de autoridad de registro.

Durante la configuración inicial de FAS con la consola de administración, complete solo los primeros dos pasos; es decir, **implemente las plantillas de certificado** y **configure la entidad de certificación**, y siga estos pasos:



Paso 1: Modifique la siguiente línea del archivo de configuración como se muestra a continuación:

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

Ahora, el archivo debería aparecer como se muestra a continuación:

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

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

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

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

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

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

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

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

Algunos TPM limitan la longitud de la clave. La longitud predeterminada de la clave es de 2048 bits.

Compruebe que el hardware admite la longitud de clave especificada.

Paso 2: Reinicie el servicio de autenticación federada de Citrix para que este lea los nuevos valores del archivo de configuración.

Paso 3: Autorice el servicio.

Paso 4: Emita manualmente la solicitud de certificado pendiente desde el servidor de la entidad de certificación. Una vez obtenido el certificado de autoridad de registro, el paso 3 de la secuencia de configuración que aparece en la consola de administración pasará a ser verde. En este punto, la clave privada del certificado de autoridad de registro se habrá generado en el TPM. De forma predeterminada, el certificado será válido durante 2 años.

Para confirmar que la clave privada del certificado de la autoridad de registro se almacena correctamente en el TPM, utilice estos comandos de PowerShell. El campo PrivateKeyProvider se establecerá en *Microsoft Platform Crypto Provider* si la clave privada del certificado de la autoridad de registro se almacena en el TPM:

```
1 Add-PSSnapin Citrix.Authentication.FederatedAuthenticationService.V1
2 Get-FasAuthorizationCertificate -FullCertInfo -Address localhost
3 <!--NeedCopy-->
```

Paso 5: Modifique el archivo de configuración de nuevo a lo siguiente:

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

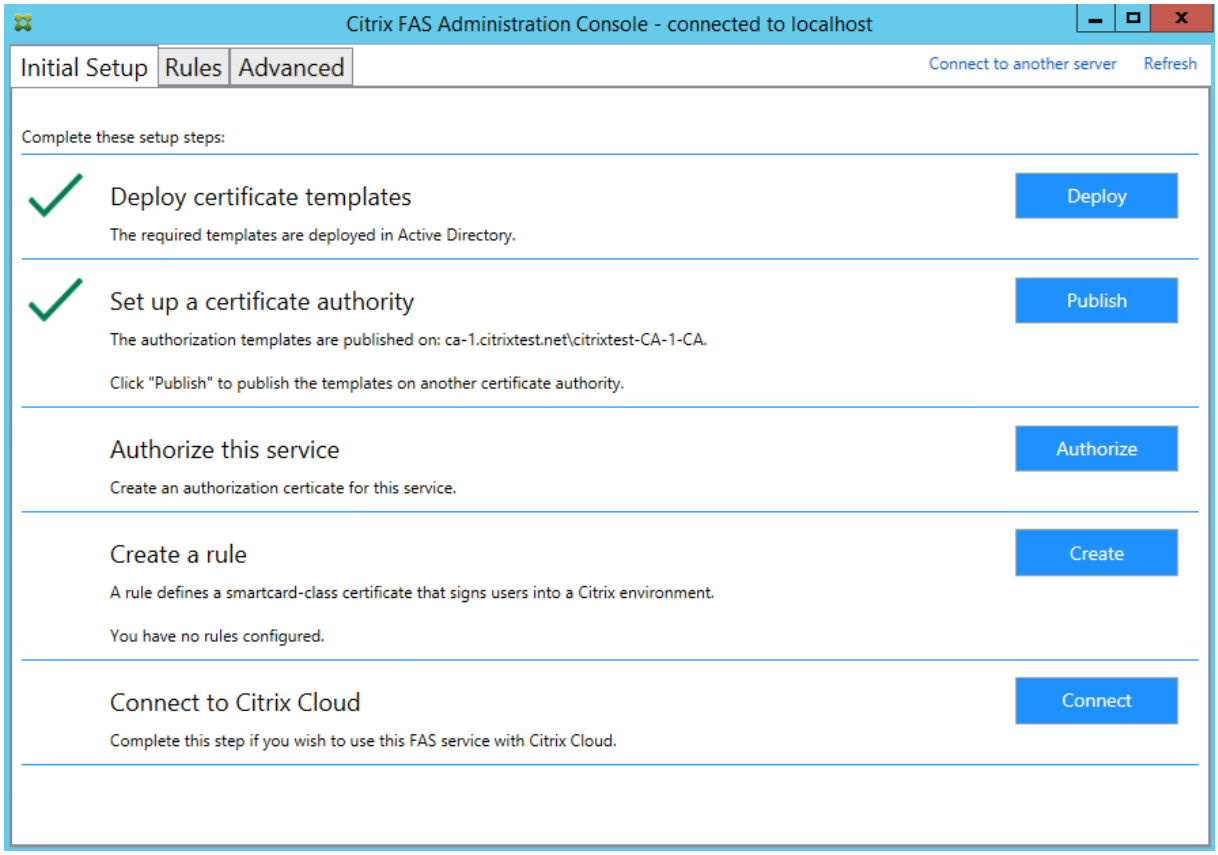
> **Nota:**
>
> Aunque FAS puede generar certificados de usuario con las claves protegidas de TPM, el hardware de TPM puede ser demasiado lento para implementaciones de gran tamaño.

Paso 6: Reinicie FAS. Ello obliga al servicio a volver a leer el archivo de configuración y procesar los valores cambiados. Las siguientes operaciones automáticas de clave privada afectarán a las claves de certificado de usuario; las operaciones se almacenarán las claves privadas en el TPM, sino que usarán el proveedor de almacenamiento de claves (KSP) de software de Microsoft.

Paso 7: Seleccione la **ficha Reglas** en la consola de administración de FAS y modifique la configuración como se describe en Instalación y configuración.

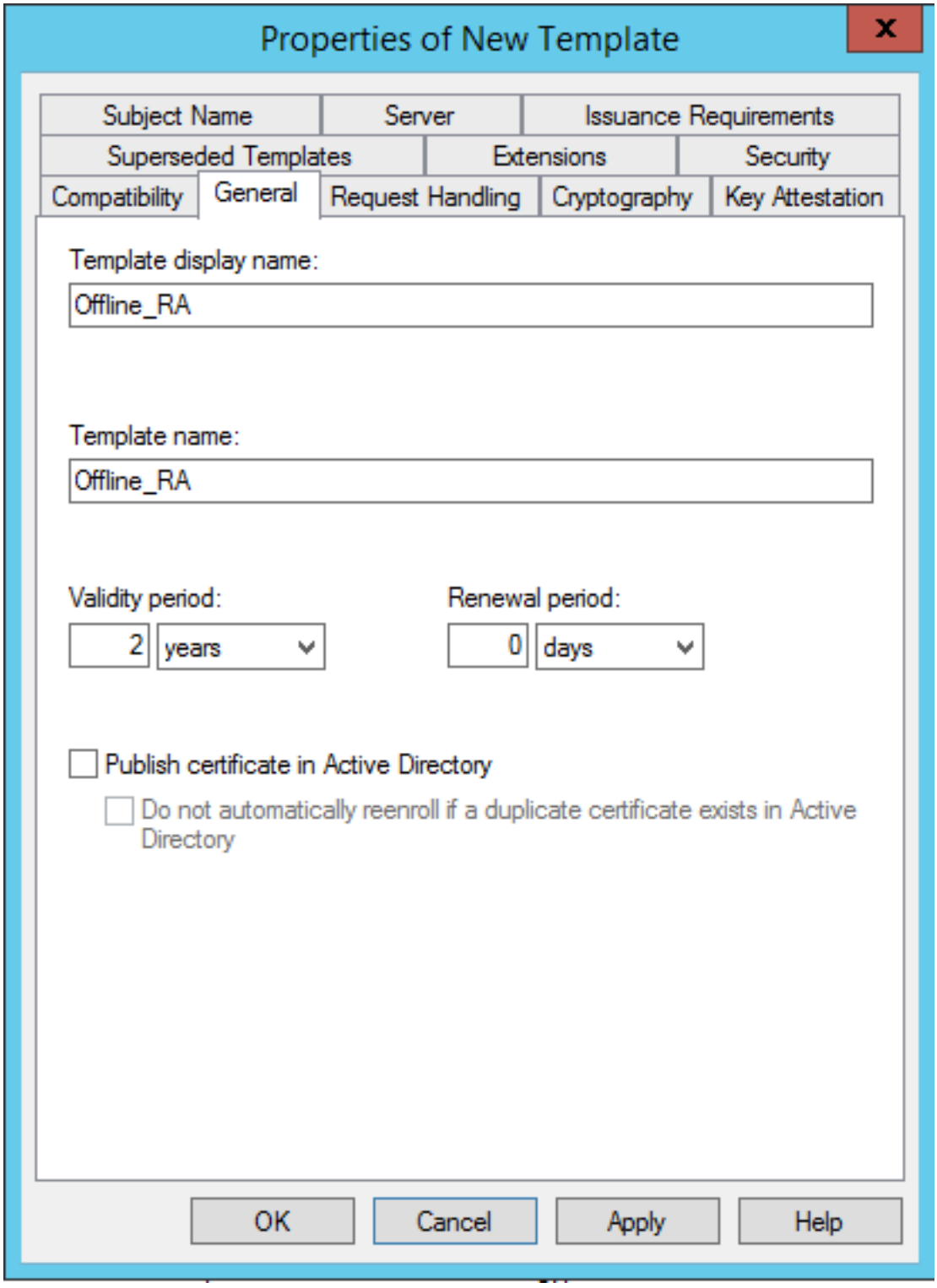
Mediante PowerShell El certificado de autoridad de registro se puede solicitar sin conexión mediante PowerShell. Esto es adecuado para organizaciones que no quieran que su entidad de certificación emita un certificado de autoridad de registro a través de una solicitud de firma de certificado en línea. No puede realizar solicitudes de firma de certificados de autoridad de registro sin conexión mediante la consola de administración de FAS.

Paso 1: Durante la configuración inicial de FAS con la consola de administración, complete solo los primeros dos pasos; es decir, implemente las plantillas de certificado y configure la entidad de certificación.



Paso 2: En el servidor de la entidad de certificación, agregue el complemento MMC de las plantillas de certificados. Haga clic con el botón secundario en la plantilla **Citrix_RegistrationAuthority_ManualAuthorizatio** y seleccione **Duplicar plantilla**.

Seleccione la ficha **General**. Cambie el nombre y el período de validez. En este ejemplo, el nombre es *Offline_RA* y el período de validez es de 2 años:



Paso 3: En el servidor de la entidad de certificación, agregue el complemento MMC de la entidad de certificación. Haga clic con el botón secundario en **Plantillas de certificado**. Seleccione **Nueva** y, a continuación, haga clic en **Plantilla de certificado que se va a emitir**. Elija la plantilla que acaba de crear.

Paso 4: Cargue los siguientes cmdlets de PowerShell en el servidor de FAS:

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

Paso 5: Genere el par de claves RSA en el TPM del servidor de FAS y cree la solicitud de firma de certificado con el siguiente cmdlet de PowerShell en el servidor de FAS. **Nota:** Algunos TPM limitan la longitud de la clave. La longitud predeterminada de la clave es de 2048 bits. Especifique una longitud de clave que su hardware admita.

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

Por ejemplo:

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

Aparecerá lo siguiente:

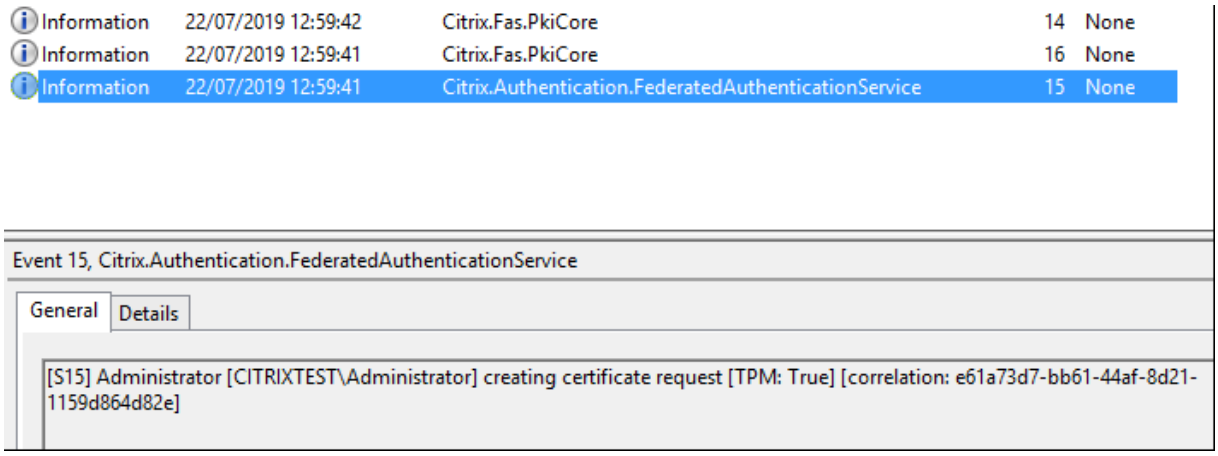
```
PS C:\Users\Administrator.AUTH> New-UcsAuthorizationCertificateRequest -UseTPM $true -address ucshsm.auth.local

Id                  : 5ac3d8bd-b484-4ebe-abf8-4b2cfd62ca39
Address             : [Offline CSR]
TrustArea           :
CertificateRequest  : -----BEGIN CERTIFICATE REQUEST-----
                      MIICaDCCAVACAQIwIzEhMB8GCgmSJomT8ixkARkWEUNpdHJpeFRydXNORmFicmljMIIBIjANBgkq
                      hkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAwAtwoCLXJuJ3yIscT8Y5v/7zuYqBhbHkhZV3wTNfRORW
                      lhCMwi7X4YpTE7CbJtgiFY/9SEBa9StGeTVpeJi66gKoZCdxydc2BwX6JNZrLi9hAflbInFPgrz+
                      vbG3YjKuKtK35JpGqYWjUEDzKiQFaob3Dkh/pwP3V7OcEYthxB8CfbaM9MHOEFbepoSYOCAfunXW
                      snwIbXD91c/fGyM/3f94P4fbNrjEIOHc+4Dy/WsPgPRgcq9XBwRjzpGjOgOWRoJS9g22DY5PwD77
                      7f7vZvoQkRy5NXXXATJ+xxYEPLp9JuJaElWXrTJG+XP3SnG/oCCPit7iUIIc9FjGa3qTUQIDAQAB
                      oAAwDQYJKoZIhvcNAQENBQADggEBAIJV8jR9XWHlvztpjxPeJzAVOsrLpOsCfNdvYn9u+I7J8Gsr
                      4tuLjuQ+An4Y2Rw7b6pZxEICV8rqd5Gy+wtPnUZoAf6eLg1Vht2RVfb6d7Ns6+Mc+F5bFegLHs8c
                      YlITNOtmcHFKt4Loz5D5E+tQw39MProEj3p7GwF7HrGY+QSbFD38rbL19Z5cfNYYqMbsgyMgdR8F
                      3SmagQjN3C8lyqT8z1iF4l32xlmQrP/4XQvr1F+TD15PM5Fxjj6PEKWopWTYZXGzSC1ufxevcO1K
                      +tTH9tQYJM6xw3+6TIcfuWDjrd8KJjTdC5SMu7LJuIajTNZ5Z+1eM61TATO3XG/AB7o=
                      -----END CERTIFICATE REQUEST-----
Status              : WaitingForApproval


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

Notas:

- En uno de los siguientes pasos, se necesita el identificador GUID (en este ejemplo, “5ac3d8bd-b484-4ebe-abf8-4b2cfd62ca39”).
- Este cmdlet de PowerShell se puede entender como una “invalidación”puntual que se usa para generar la clave privada del certificado de la autoridad de registro.
- Cuando se ejecuta este cmdlet, se comprueban los valores del archivo de configuración, leídos en el inicio del servicio FAS, para determinar la longitud de la clave que se va a usar (la longitud predeterminada es de 2048).
- Como -UseTPM está establecido en $true en esta operación manual de clave privada de certificado de autoridad de registro que se ha iniciado con PowerShell, el sistema ignora los valores del archivo que no coincidan con la configuración necesaria para usar un TPM.
- Ejecutar este cmdlet no cambia los parámetros del archivo de configuración.

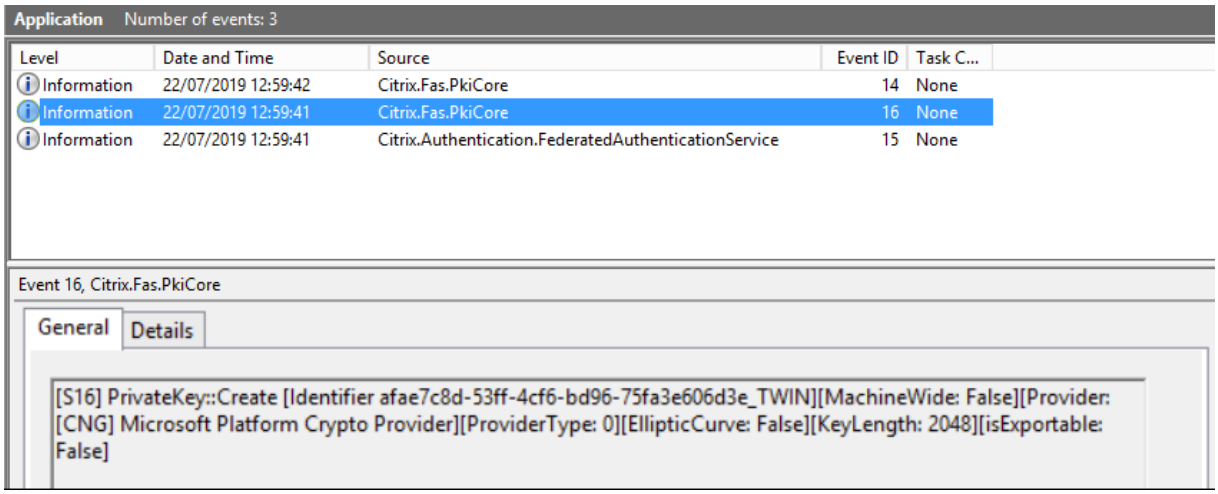
- En las siguientes operaciones automáticas de clave privada para los certificados de usuario que se inicien con FAS, se utilizan los valores que se hayan leído del archivo cuando se inicia FAS.
- También se puede establecer el valor de KeyProtection del archivo de configuración en GenerateTPMProtectedKey cuando el servidor de FAS emita certificados. De este modo, se generarán claves privadas de certificados de usuario protegidas por el TPM.

Para verificar que se haya utilizado el TPM para generar el par de claves, abra el registro de la aplicación en el visor de eventos de Windows que está presente en el servidor de FAS y consulte el momento en que se generó el par de claves.



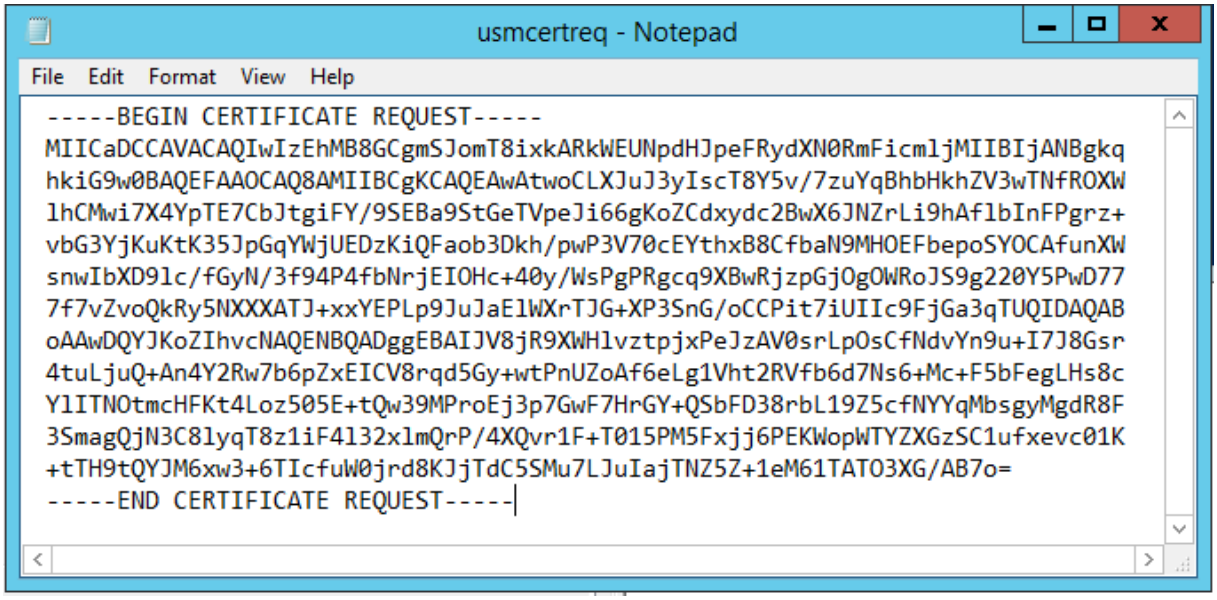
Nota: "[TPM: True]"

Seguido de:



Nota: "Provider: [CNG] Microsoft Platform Crypto Provider"

Paso 6: Copie la sección de la solicitud de certificado a un editor de texto y guárdela en el disco como un archivo de texto.



Paso 7: Envíe la solicitud de firma de certificado a la entidad de certificación. Para ello, escriba lo siguiente en la instancia de PowerShell presente en el servidor de FAS:

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

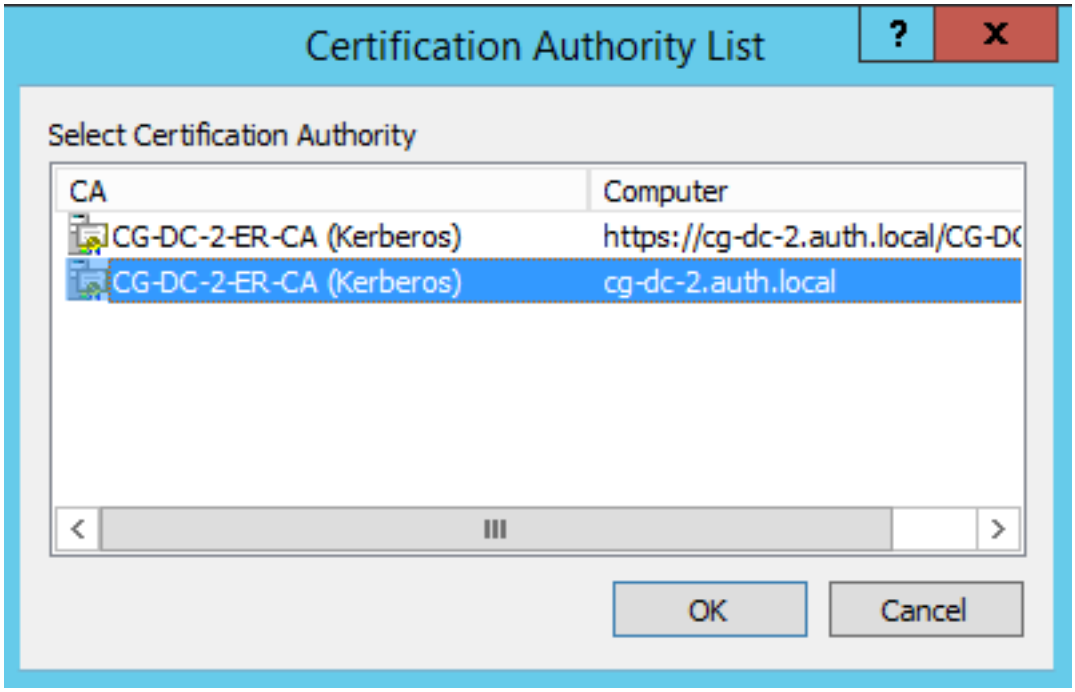
Por ejemplo:

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

Aparecerá lo siguiente:

```
PS C:\Users\Administrator.AUTH> certreq -submit -attrib "certificatetemplate:Offline_RA" C:\Users\Administrator.AUTH\Des
ktop\usmcertreq.txt
Active Directory Enrollment Policy
  {4F7616DE-DB0C-4D21-A4FD-2E29502177C2}
  ldap:
```

En este punto, es posible que aparezca una ventana con la lista de entidades de certificación. En este ejemplo, la entidad de certificación tiene habilitadas las inscripciones HTTP (hilera superior) y DCOM (hilera inferior). Seleccione la opción DCOM, si está disponible:

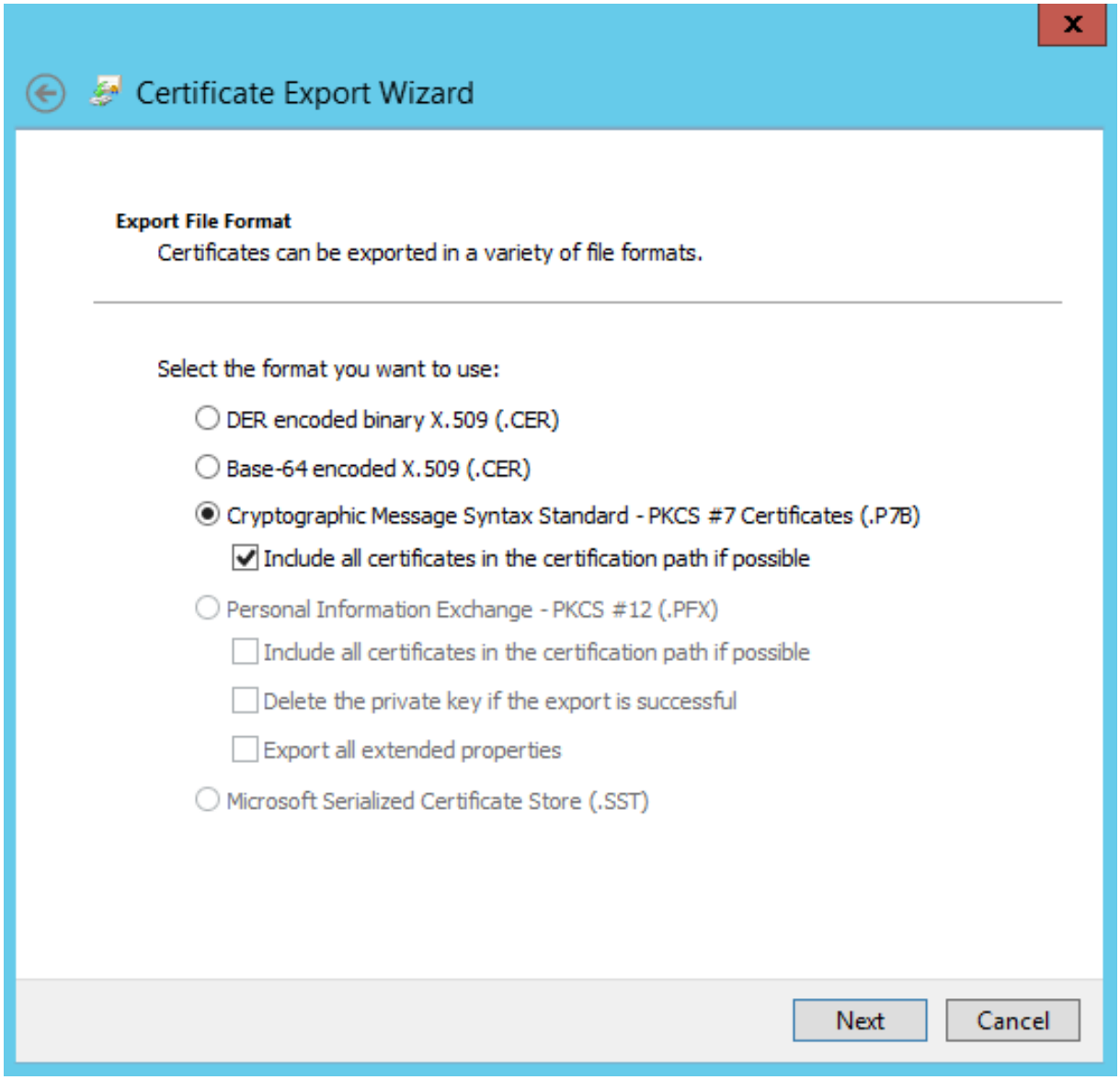


Tras especificar la entidad de certificación, PowerShell pide el ID de la solicitud mediante RequestID:

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

Paso 8: En el servidor de la entidad de certificación, en el complemento MMC de esta, haga clic en **Solicitudes pendientes**. Tome nota del identificador de la solicitud. A continuación, haga clic con el botón secundario en la solicitud y elija **Emitir**.

Paso 9: Seleccione el nodo **Certificados emitidos**. Busque el certificado que se acaba de emitir (el ID de solicitud debe coincidir). Haga doble clic para abrir el certificado. Seleccione la ficha **Detalles**. Haga clic en **Copiar a archivo**. Se iniciará el Asistente para exportación de certificados. Haga clic en **Siguiente.** Seleccione las siguientes opciones para el formato de archivo:



El formato debe ser "**Estándar de sintaxis de cifrado de mensajes: certificados PKCS #7 (.P7B)**"y se debe marcar "**Si es posible, incluir todos los certificados en la ruta de acceso de certificación**" .

Paso 10: Copie el archivo del certificado exportado al servidor de FAS.

Paso 11: Debe importar el certificado de autoridad de registro en el servidor de FAS. Para ello, introduzca los siguientes cmdlets de PowerShell en el servidor de FAS:

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

Por ejemplo:


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

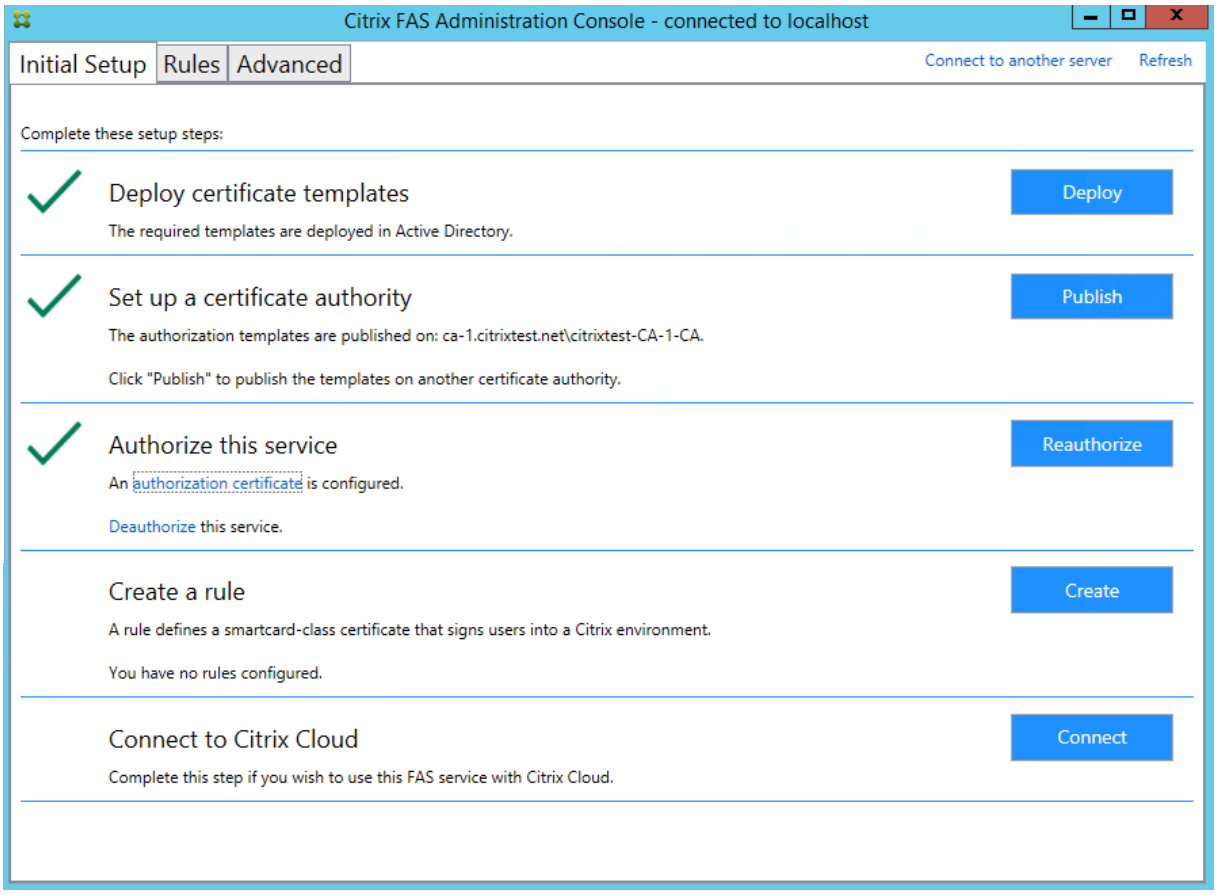
Aparecerá lo siguiente:

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


Id                  : 5ac3d8bd-b484-4ebe-abf8-4b2cfd62ca39
Address             : [Offline CSR]
TrustArea           : a5c27fcc-1dd7-4c2b-8963-16ec31102Dfc
CertificateRequest :
Status              : Ok
```

Para confirmar que la clave privada del certificado de la autoridad de registro se almacena correctamente en el TPM, utilice estos comandos de PowerShell. El campo PrivateKeyProvider se establecerá en *Microsoft Platform Crypto Provider* si la clave privada del certificado de la autoridad de registro se almacena en el TPM:

```
1 Add-PSSnapin Citrix.Authentication.FederatedAuthenticationService.V1
2 Get-FasAuthorizationCertificate -FullCertInfo -Address localhost
3 <!--NeedCopy-->
```

Paso 12: Cierre la consola de administración de FAS y reiníciela.



Nota: El paso "Authorize this Service"tiene una marca de verificación verde.

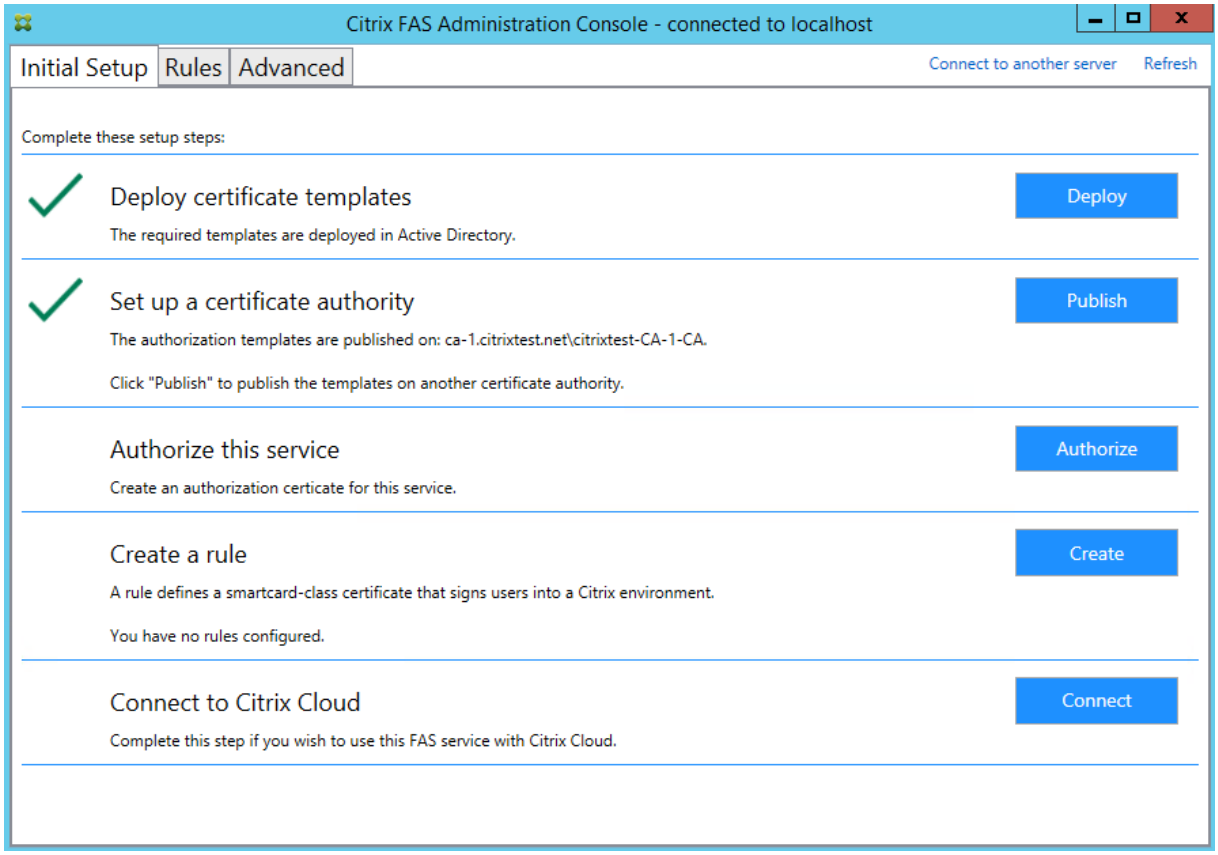
Paso 13: Seleccione la ficha **Reglas** en la consola de administración de FAS y modifique la configuración como se describe en Instalación y configuración.

Ejemplo 3

En este ejemplo, la clave privada del certificado de autoridad de registro y las claves privadas de los certificados de usuario se almacenan en un módulo de seguridad de hardware (HSM). En este ejemplo, se presupone que el lector tiene configurado un módulo HSM. El módulo HSM tendrá un nombre de proveedor; por ejemplo, "Proveedor de almacenamiento de claves de HSM_Vendor".

Si quiere ejecutar el servidor de FAS en entornos virtualizados, consulte al distribuidor de HSM si admite el hipervisor.

Paso 1. Durante la configuración inicial de FAS con la consola de administración, complete solo los primeros dos pasos; es decir, implemente las plantillas de certificado y configure la entidad de certificación.



Paso 2: Consulte la documentación del distribuidor de HSM para determinar el valor de ProviderName que debe tener el módulo HSM. Si el módulo HSM utiliza CAPI, es posible que, en la documentación, el proveedor se conozca como proveedor de servicios de cifrado (CSP). En cambio, si el módulo HSM utiliza CNG, es posible que el proveedor se conozca como proveedor de almacenamiento de claves (KSP).

Paso 3: Modifique el archivo de configuración como se indica a continuación:

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

Ahora, el archivo debería aparecer como se muestra a continuación:

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

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

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

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

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

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

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

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

En este caso, se presupone que el módulo HSM utiliza CNG, por lo que el valor de ProviderLegacyCsp se establece en false. Si el módulo HSM utiliza CAPI, el valor de ProviderLegacyCsp debe establecerse en true. Consulte la documentación del distribuidor de HSM para determinar si el módulo HSM utiliza CAPI o CNG. Asimismo, consulte la documentación del distribuidor de HSM para saber las longitudes de clave que admite en la generación de claves asimétricas de RSA. En este ejemplo, la longitud de la clave se ha establecido en el valor predeterminado de 2048 bits. Compruebe que el hardware admite la longitud de clave especificada.

Paso 4: Reinicie el servicio de autenticación federada de Citrix para que este lea los nuevos valores del archivo de configuración.

Paso 5: Genere el par de claves RSA en el HSM y cree la solicitud de firma de certificado; para ello, haga clic en **Authorize** en la ficha **Initial Setup** de la consola de administración de FAS.

Paso 6: Para verificar que el par de claves se ha generado en el HSM, consulte las entradas de la aplicación en el registro de eventos de Windows:

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

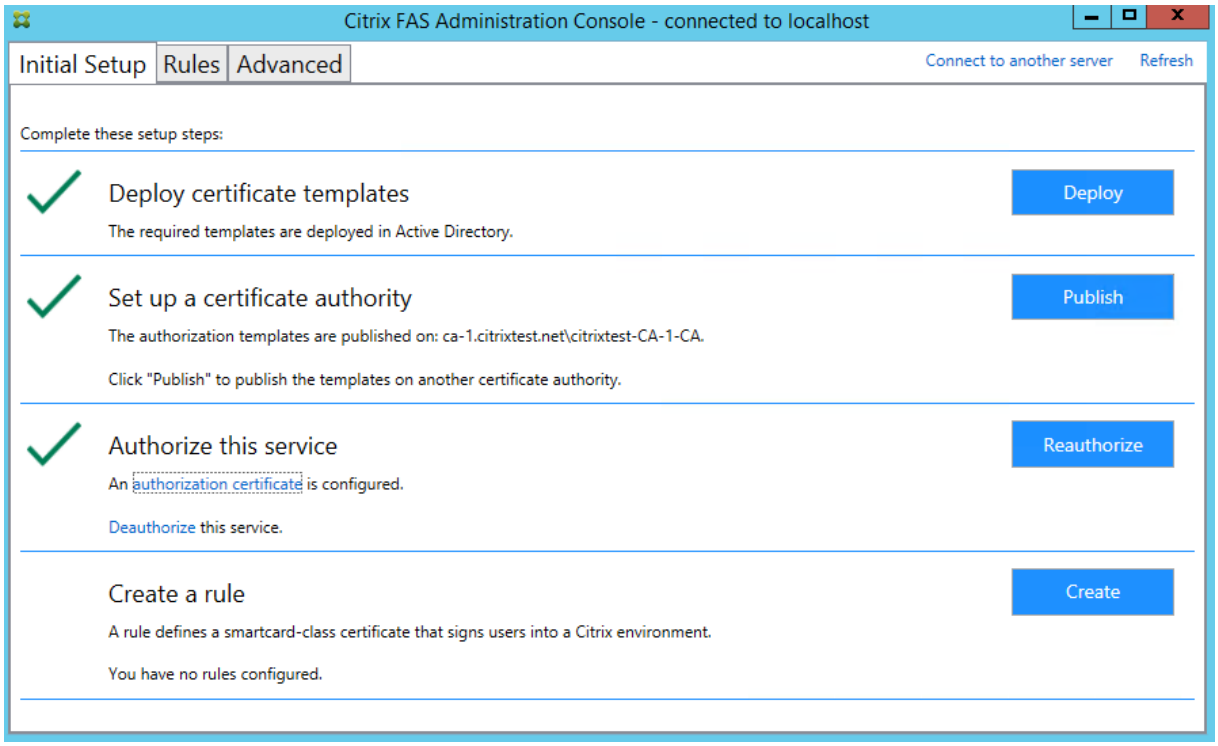
Nota: [Provider: [CNG] HSM_Vendor's Key Storage Provider]

Paso 7: En el servidor de la entidad de certificación, en el complemento MMC de esta, seleccione el nodo **Solicitudes pendientes**:

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

Haga clic con el botón secundario en la solicitud y seleccione **Emitir**.

Nota: El paso "Authorize this Service"tiene una marca de verificación verde.



Paso 8: Seleccione la ficha **Reglas** en la consola de administración de FAS y modifique la configuración como se describe en Instalación y configuración.

Almacenamiento de certificados del servicio de autenticación federada (FAS)

El servicio de autenticación federada (FAS) no utiliza el almacén de certificados de Microsoft que haya en el servidor de FAS para almacenar en él sus certificados. Utiliza una base de datos integrada.

Para determinar el GUID del certificado de autoridad de registro, introduzca los siguientes cmdlets de PowerShell en el servidor de FAS:

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

Por ejemplo, **Get-FasAuthorizationCertificate –address cg-fas-2.auth.net**:


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


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

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

Para obtener una lista de certificados de usuario, escriba:

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

Por ejemplo, **Get-FasUserCertificate –address cg-fas-2.auth.net**

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


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

> **Nota:**
>
> Al usar un HSM para almacenar las claves privadas, los contenedores de HSM se identifican con un GUID. El GUID para la clave privada en el HSM se puede obtener con:
>
> ```
> Get-FasUserCertificate –address \<FAS server FQDN> -KeyInfo $true
> ```
>
> Por ejemplo:
>
> ```
> Get-FasUserCertificate –address fas3.djwfas.net -KeyInfo $true
> ```

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


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


Información relacionada

- Instalación y configuración es la referencia principal para la instalación y la configuración de este servicio.
- Las implementaciones más comunes del servicio FAS se resumen en el artículo Introducción a las arquitecturas del Servicio de autenticación federada.
- En Configuración avanzada, se presentan otros artículos de "procedimientos".

Seguridad y configuración de red

March 30, 2023

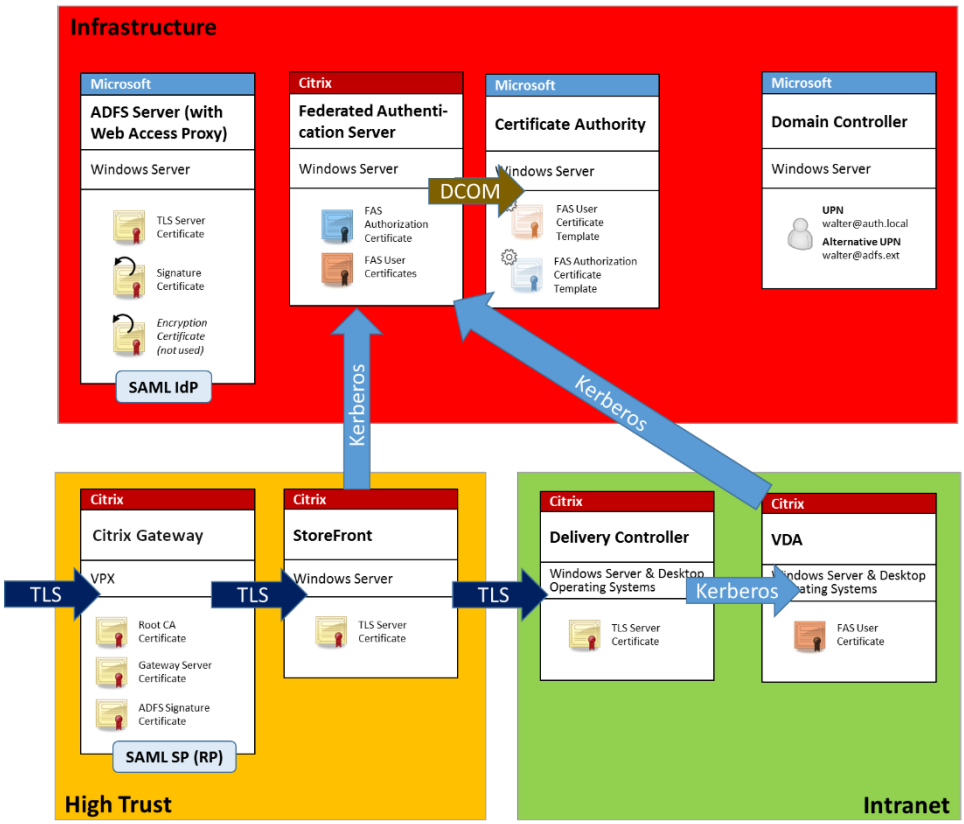
El Servicio de autenticación federada (FAS) está estrechamente integrado con Microsoft Active Directory y con la entidad de certificación de Microsoft. Es fundamental asegurarse de que el sistema está administrado y protegido correctamente mediante el desarrollo de una directiva de seguridad del mismo modo que lo haría para un controlador de dominio o para otra parte importante de la infraestructura.

Este documento presenta un resume de las cuestiones de seguridad que se deben tener en cuenta al implementar FAS. También proporciona una visión general de las funciones disponibles que pueden ayudarle a proteger su infraestructura.

Arquitectura de red

El diagrama siguiente muestra los componentes principales y los límites de seguridad usados en una implementación de FAS.

El servidor de FAS debe tratarse como una parte de la infraestructura fundamental para la seguridad, junto con la entidad de certificación y el controlador de dominio. En un entorno federado, Citrix Gateway y Citrix StoreFront son componentes de confianza para realizar la autenticación de usuarios; otros componentes de Citrix Virtual Apps and Desktops no se ven afectados por la introducción de FAS.



Seguridad de red y firewalls

La comunicación entre Citrix Gateway, StoreFront y los componentes de Delivery Controller debe estar protegida con TLS a través del puerto 443. El servidor de StoreFront realiza únicamente conexiones salientes y Citrix Gateway debe aceptar solo conexiones a través de Internet que usen HTTPS en el puerto 443.

El servidor de StoreFront contacta con el servidor de FAS a través del puerto 80 mediante autenticación mutua con Kerberos. En la autenticación se utiliza la identidad Kerberos HOST/FQDN del servidor de FAS y la identidad Kerberos de la cuenta de máquina del servidor de StoreFront. Eso genera un identificador de credenciales de un solo uso, necesario para que Citrix Virtual Delivery Agent (VDA) inicie la sesión del usuario.

Cuando una sesión HDX se conecta al VDA, el VDA también se comunica con el servidor de FAS en el puerto 80. En la autenticación, se utiliza la identidad Kerberos HOST/FQDN del servidor de FAS y la identidad Kerberos de máquina del VDA. Además, el VDA debe proporcionar el identificador de credenciales para acceder al certificado y la clave privada.

La entidad de certificación de Microsoft acepta la comunicación con DCOM autenticado con Kerberos, que se puede configurar para usar un puerto TCP fijo. La entidad de certificación también requiere que

el servidor de FAS proporcione un paquete CMC firmado por un certificado de agente de inscripción de confianza.

Servidor	Puertos de firewall
Servicio de autenticación federada	[entrada] Kerberos por HTTP desde StoreFront y los VDA, [salida] DCOM hacia la entidad de certificación de Microsoft
Citrix Gateway	[entrada] HTTPS desde las máquinas cliente, [entrada o salida] HTTPS hacia o desde el servidor de StoreFront, [salida] HDX a VDA
StoreFront	[entrada] HTTPS desde Citrix Gateway, [salida] HTTPS a Delivery Controller, [salida] Kerberos HTTP a FAS
Delivery Controller	[entrada] HTTPS desde el servidor de StoreFront, [entrada o salida] Kerberos por HTTP desde VDA
VDA	[entrada o salida] Kerberos por HTTP desde Delivery Controller, [entrada] HDX desde Citrix Gateway, [salida] Kerberos HTTP a FAS
Entidad de certificación de Microsoft	[entrada] DCOM y firmado desde FAS

Conexiones entre el Servicio de autenticación federada de Citrix y Citrix Cloud

La consola y FAS acceden a estas direcciones con la cuenta del usuario y la cuenta del servicio de red, respectivamente.

- Consola de administración de FAS, bajo la cuenta del usuario
  - `*.cloud.com`
  - `*.citrixworkspacesapi.net`
  - Direcciones requeridas por un proveedor de identidades tercero, si se utiliza uno en su entorno
- Servicio FAS, en la cuenta del servicio de red: `*.citrixworkspacesapi.net`

Si su entorno incluye servidores proxy, configure el proxy de usuario con las direcciones de la consola de administración FAS. Además, asegúrese de que la dirección de la cuenta de servicio de red esté configurada mediante “netsh”o una herramienta similar.

Responsabilidades de administración

La administración del entorno se puede dividir en los siguientes grupos:

Name	Responsabilidad
Administrador de la organización	Instalar y proteger las plantillas de certificado en el bosque
Administrador del dominio	Configurar parámetros de directivas de grupo
Administrador de entidades de certificación	Configurar la entidad de certificación
Administrador de FAS	Instalar y configurar el servidor de FAS
Administrador de StoreFront/Citrix Gateway	Configurar la autenticación de usuarios
Administrador de Citrix Virtual Desktops	Configurar los VDA y los Controllers

Cada administrador controla diferentes aspectos del modelo de seguridad global, lo que permite aplicar un enfoque de defensa en profundidad para proteger el sistema.

Configuración de directivas de grupo

Las máquinas FAS de confianza se identifican en una tabla de búsqueda por "número de índice -> FQDN"configurada mediante Directiva de grupo. Al contactar con un servidor de FAS, los clientes verifican la identidad Kerberos `HOST\<fqdn>` del servidor de FAS. Todos los servidores que tienen acceso al servidor de FAS deben tener configuraciones idénticas de FQDN con el mismo índice; de lo contrario, StoreFront y los VDA pueden contactar con servidores de FAS distintos.

Para evitar errores de configuración, Citrix recomienda aplicar una única directiva a todas las máquinas del entorno. Ponga cuidado a la hora de modificar la lista de servidores de FAS, especialmente al quitar o reordenar las entradas.

El control de este objeto de directiva de grupo debe estar limitado a los administradores de FAS (y/o los administradores de dominio) encargados de instalar y retirar servidores de FAS. No reutilice nombres de dominio completo (FQDN) de máquinas al poco tiempo de retirar servidores de FAS.

Plantillas de certificado

Si no quiere utilizar la plantilla de certificado Citrix_SmartcardLogon suministrada con FAS, puede modificar una copia de ella. Se admiten las siguientes modificaciones.

Cambiar el nombre de una plantilla de certificado

Si quiere cambiar el nombre de Citrix_SmartcardLogon para que coincida con la nomenclatura de nombramiento de plantillas que estipula la organización, debe:

- Crear una copia de la plantilla de certificado y cambiarle el nombre para que coincida con la nomenclatura de la denominación de la organización.
- Use comandos de PowerShell FAS para administrar FAS, en lugar de la interfaz del usuario administrador. (La interfaz del usuario administrador se diseñó para usarla únicamente con los nombres de plantilla predeterminados de Citrix.)
  - Utilice el complemento Plantillas de certificados de MMC de Microsoft o el comando Publish-FasMsTemplate para publicar la plantilla, y
  - Utilice el comando New-FasCertificateDefinition para configurar FAS con el nombre de su plantilla.

Modificar propiedades generales

Puede modificar el período de validez de la plantilla de certificado.

No modifique el período de renovación. FAS ignora este parámetro en la plantilla de certificado. FAS renovará automáticamente el certificado a mitad de su período de validez.

Modificar propiedades de gestión de peticiones

No modifique estas propiedades. FAS ignora esta configuración en la plantilla de certificado. FAS siempre desmarca **Permitir que la clave privada se pueda exportar** y **Renovar con la misma clave**.

Modificar propiedades de criptografía

No modifique estas propiedades. FAS ignora esta configuración en la plantilla de certificado.

Consulte Protección de claves privadas para conocer los parámetros equivalentes que ofrece FAS.

Modificar propiedades de atestación de clave

No modifique estas propiedades. FAS no admite la atestación de claves.

Modificar propiedades de plantillas reemplazadas

No modifique estas propiedades. FAS no admite la sustitución de plantillas.

Modificar propiedades de extensiones

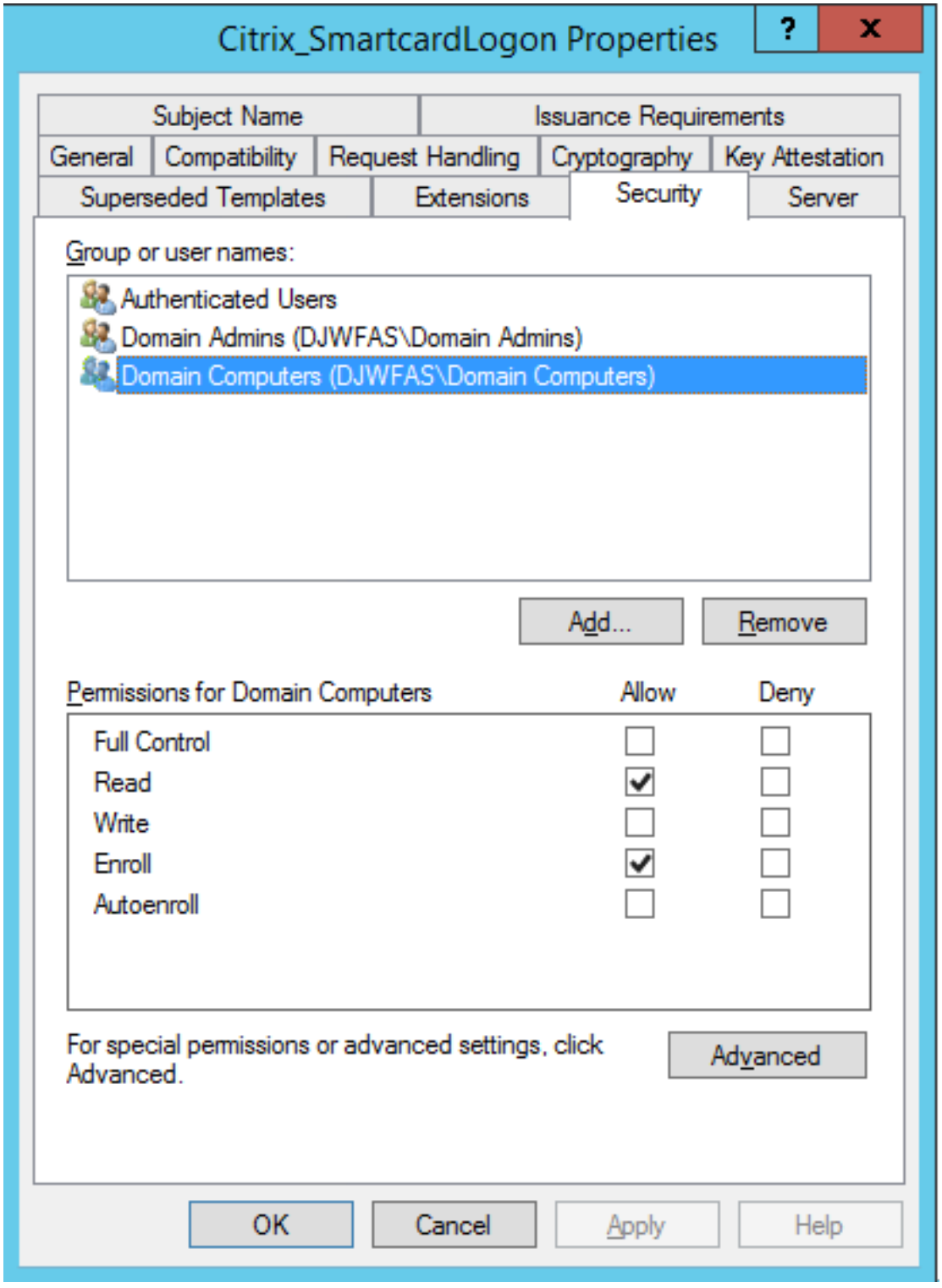
Puede modificar estas opciones de configuración para que coincidan con la directiva de la organización.

Nota: Una configuración inadecuada de las extensiones puede causar problemas de seguridad o resultar en certificados inutilizables.

Modificar propiedades de seguridad

Citrix recomienda modificar estas opciones de configuración para conceder los permisos de **lectura** y de **inscripción** solo a las cuentas de máquina de los servidores de FAS. El servicio FAS no requiere otros permisos. Sin embargo, al igual que con otras plantillas de certificado, es posible que quiera:

- Conceder a los administradores permisos de lectura o escritura en la plantilla
- Conceder a los usuarios autenticados permisos de lectura en la plantilla



Modificar propiedades de nombre del sujeto

Citrix recomienda no modificar estas propiedades.

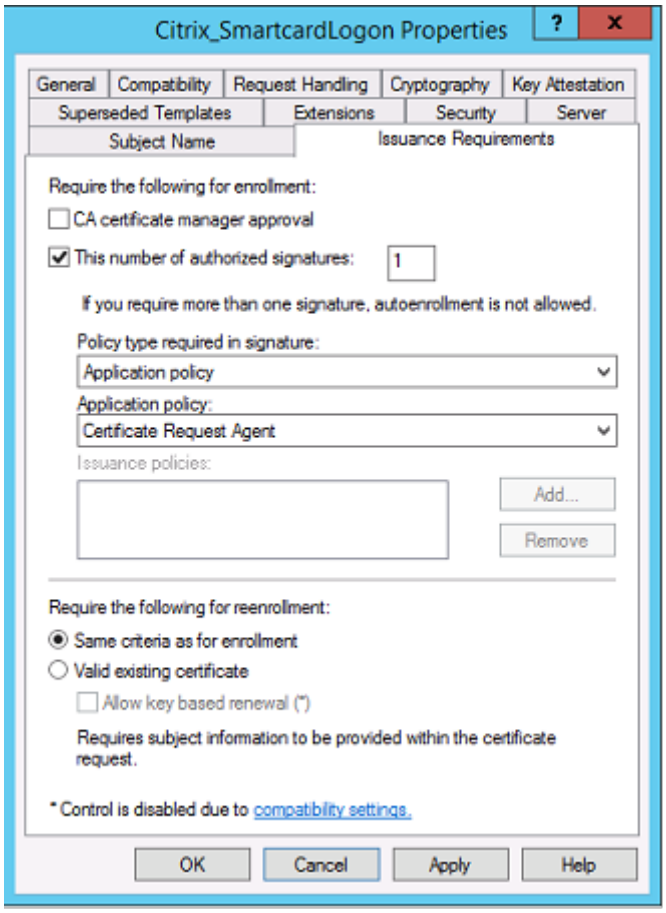
La plantilla tiene seleccionada la opción *Build from this Active Directory information*, lo que hace que la entidad de certificación incluya el SID del usuario en una extensión de certificado. Esto proporciona una asignación sólida a la cuenta de Active Directory del usuario.

Modificar propiedades de servidor

Aunque Citrix no lo recomienda, puede modificar estas opciones de configuración para que coincidan con la directiva de la organización si fuera necesario.

Modificar propiedades de requisitos de emisión

No modifique estos parámetros. Estos parámetros deben ser como se muestra a continuación:



Modificar propiedades de compatibilidad

Puede modificar estos parámetros. El valor debe ser al menos **Windows Server 2003 CAs** (versión 2 del esquema). Sin embargo, FAS solo admite entidades emisoras de certificados Windows Server

2008 y posterior. Además, como se ha explicado anteriormente, FAS pasa por alto la configuración adicional disponible si se selecciona **Windows Server 2008 CAs** (versión 3 del esquema) o **Windows Server 2012 CAs** (versión 4 del esquema).

Administrar la entidad de certificación

El administrador de la entidad de certificación es responsable de la configuración del servidor de la entidad de certificación y de la clave privada de emisión de certificados que se usa.

Publicar plantillas

Para que una entidad de certificación emita certificados basados en una plantilla proporcionada por el administrador de la empresa, el administrador de la entidad de certificación debe elegir publicar esa plantilla.

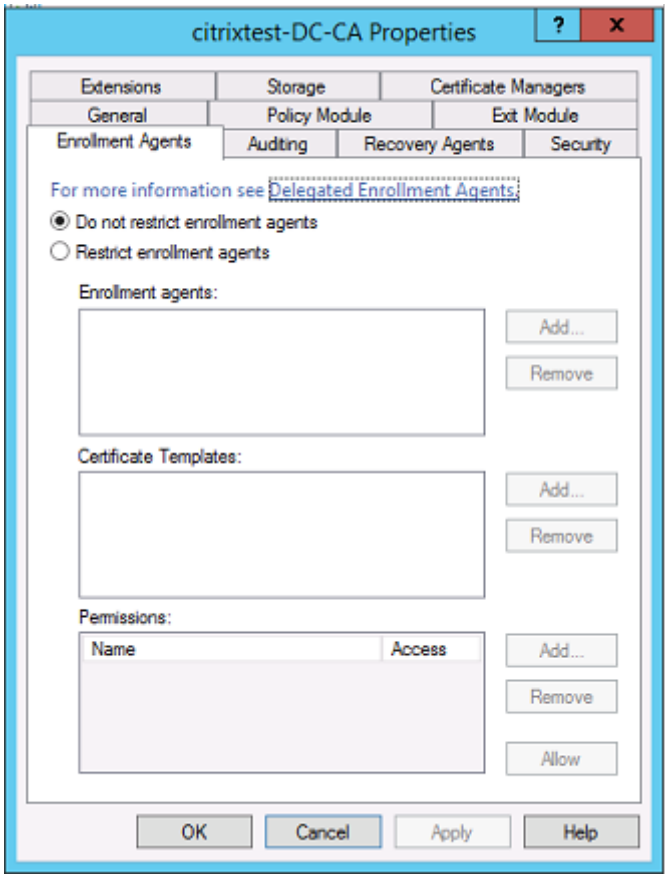
Una sencilla medida de seguridad consiste en publicar solo las plantillas de autoridad de registro cuando se están instalando los servidores de FAS, o insistir en un proceso de emisión que tenga lugar completamente sin conexión. En ambos casos, el administrador de la entidad de certificación debe mantener el control total de la autorización de las solicitudes de certificados de autoridad de registro, y tener una directiva para autorizar los servidores de FAS.

Parámetros de firewall

Por lo general, el administrador de la entidad de certificación también tiene el control de los parámetros de firewall de red de la entidad de certificación, lo que permite controlar las conexiones entrantes. El administrador de la entidad de certificación puede configurar reglas de firewall y DCOM TCP para que solo los servidores de FAS puedan solicitar certificados.

Inscripción restringida

De forma predeterminada, cualquier titular de un certificado de autoridad de registro puede emitir certificados a cualquier usuario mediante cualquier plantilla de certificado que permita el acceso. Debe restringirse a un grupo de usuarios sin privilegios con la ayuda de la propiedad “Restringir agentes de inscripción”de la entidad de certificación.



Módulos de directiva y auditoría

Para implementaciones avanzadas, se pueden usar módulos de seguridad personalizados con los que se puede hacer un rastreo y vetar la emisión de certificados.

Administrar FAS

FAS tiene varias funciones de seguridad.

Restringir StoreFront, usuarios y VDA mediante una lista de control de acceso

En el centro del modelo de seguridad de FAS está el control del acceso a la funcionalidad para las cuentas de Kerberos:

Vector de acceso	Descripción
StoreFront [IdP]	Estas cuentas de Kerberos son de confianza para declarar que un usuario se ha autenticado correctamente. Si una de estas cuentas está en situación de riesgo, se pueden crear y usar certificados para los usuarios permitidos por la configuración de FAS.
VDA [entidad de confianza]	Estas son las máquinas a las que se permite acceder a los certificados y las claves privadas. Se necesita también un identificador de credencial obtenido por el IdP, de modo que una cuenta de VDA de este grupo que esté en situación de riesgo tendrá un ámbito muy limitado para atacar el sistema.
Usuarios	Esto controla qué usuarios pueden ser objeto de aserciones de proveedor de identidades (IdP). Tenga en cuenta que esto se solapa con las opciones de configuración de Agente de inscripción restringido (Restricted Enrollment Agent) en la entidad de certificación. En general, se recomienda incluir solo cuentas sin privilegios en esta lista. Esto evita que una cuenta de StoreFront que esté en situación de riesgo pueda aumentar sus privilegios a un nivel administrativo superior. En concreto, las cuentas de administrador de dominio no deben permitirse en esta lista de control de acceso.

Configurar reglas

Las reglas son útiles cuando hay varias implementaciones de Citrix Virtual Apps o Citrix Virtual Desktops independientes que usan la misma infraestructura de servidor de FAS. Cada regla tiene un conjunto de opciones de configuración aparte; en concreto, las listas de control de acceso se pueden configurar de forma independiente.

Configurar la entidad de certificación y las plantillas

Se pueden configurar plantillas de certificados y entidades de certificación diferentes para distintos derechos de acceso. En configuraciones avanzadas, se puede elegir usar certificados más o menos potentes en función del entorno. Por ejemplo, los usuarios identificados como "externos"pueden tener un certificado con menos privilegios que los usuarios "internos".

Certificados de sesión y de autenticación

El administrador de FAS puede controlar si el certificado usado para autenticar está disponible para su uso también dentro de la sesión del usuario. Por ejemplo, puede tener solo certificados de "firma" disponibles durante la sesión, y usar el certificado más potente de "inicio de sesión"solo para iniciar sesión.

Protección de claves privadas y longitud de las claves

El administrador de FAS puede configurar FAS para almacenar las claves privadas en un módulo de seguridad de hardware (HSM) o en un módulo de plataforma de confianza (TPM). Citrix recomienda que se almacene, por lo menos, la clave privada del certificado de autoridad de registro en un módulo TPM para protegerla; esta opción se ofrece como parte del proceso de solicitud de certificado "sin conexión".

Del mismo modo, las claves privadas de certificado de usuario se pueden guardar en un módulo TPM o HSM. Todas las claves deben generarse como "no-exportables"y deben tener una longitud mínima de 2048 bits.

Registros de eventos

El servidor de FAS proporciona registros de eventos detallados sobre configuración y tiempo de ejecución, que se pueden utilizar para la auditoría y la detección de intrusiones.

Acceso administrativo y herramientas de administración

FAS incluye herramientas y funciones de administración remota (autenticación mutua con Kerberos). Los miembros del grupo "Administradores locales"tienen control total sobre la configuración de FAS. Esta lista se debe mantener con cuidado.

Administradores de VDA, Citrix Virtual Apps y Citrix Virtual Desktops

En general, el uso de FAS no cambia el modelo de seguridad de Delivery Controller y los administradores de VDA, ya que el "identificador de credenciales"de FAS simplemente reemplaza la "contraseña de Active Directory". Los grupos de administración de Controller y VDA deben contener solo usuarios de confianza. Deben mantenerse registros de eventos y auditoría.

Seguridad general de los servidores Windows

Todos los servidores deben contar con las revisiones disponibles y tener instalado un software de firewall y antivirus estándar. Los servidores de la infraestructura de importancia crítica para la seguridad deben ubicarse en un lugar protegido físicamente, y hay que poner especial cuidado en las opciones de cifrado de los discos y el mantenimiento de las máquinas virtuales.

Los registros de eventos y auditoría deben almacenarse de forma segura en una máquina remota.

El acceso RDP debe limitarse solo a administradores autorizados. Cuando sea posible, las cuentas de usuario deben requerir el inicio de sesión con tarjeta inteligente, especialmente para las cuentas de administradores de dominio y de entidad de certificación.

Información relacionada

- Instalación y configuración es la referencia principal para la instalación y la configuración de este servicio.
- Las arquitecturas de FAS se presentan en el artículo Arquitecturas de implementación.
- En Configuración avanzada, se presentan otros artículos de "procedimientos".

Solucionar problemas de inicio de sesión en Windows

March 30, 2023

En este artículo, se describen los registros y los mensajes de error que Windows muestra cuando un usuario inicia sesión con certificados y/o tarjetas inteligentes. Estos registros ofrecen información que se puede utilizar para solucionar fallos de autenticación.

Certificados e infraestructura de clave pública

Active Directory de Windows mantiene varios almacenes de certificados que administran certificados para los usuarios que inician sesión.

- **Almacén de certificados NTAuth:** Para autenticarse en Windows, la entidad de certificación que acaba de emitir los certificados de usuario (es decir, no se admiten entidades de certificación en cadena) debe colocarse en el almacén NTAuth. Para ver los certificados, desde el programa CertUtil, escriba: certutil –viewstore –enterprise NTAuth.
- **Almacén de certificados raíz e intermedios:** Por lo general, los sistemas de inicios de sesión con certificados pueden proporcionar solo un certificado, de modo que, si se utilizan certificados en cadena, el almacén de certificados intermedios de todas las máquinas debe incluir esos certificados. El certificado raíz debe estar en el almacén raíz de confianza y el penúltimo certificado debe estar en el almacén NTAuth.
- **Extensiones del certificado de inicio de sesión y directivas de grupo**. Windows se puede configurar para aplicar la verificación de EKU y otras directivas de certificados. Consulte la documentación de Microsoft: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/ff404287(v=ws.10).

Directiva de Registro	Descripción
AllowCertificatesWithNoEKU	Cuando está inhabilitada, los certificados deben incluir la propiedad Uso mejorado de clave (EKU) para el inicio de sesión con tarjeta inteligente.
AllowSignatureOnlyKeys	De forma predeterminada, Windows filtra y excluye las claves privadas de los certificados que no permiten el descifrado RSA. Esta opción anula ese filtro.
AllowTimeInvalidCertificates	De forma predeterminada, Windows filtra y excluye los certificados caducados. Esta opción anula ese filtro.
EnumerateECCCerts	Habilita la autenticación de curva elíptica.
X509HintsNeeded	Si un certificado no contiene un nombre principal de usuario (UPN) único o contiene uno que puede ser ambiguo, esta opción permite a los usuarios especificar manualmente su cuenta de inicio de sesión en Windows.
UseCachedCRLOnlyAnd, IgnoreRevocationUnknownErrors	Inhabilita la comprobación de revocación (normalmente establecida en el controlador de dominio).

- **Certificados de controlador de dominio:** Para la autenticación de conexiones Kerberos, todos los servidores deben tener los certificados "Domain Controller"(Controlador de dominio) que corresponden. Se pueden solicitar desde el menú de complemento MMC "Local Computer Certificate Personal Store"(Almacén personal de certificados del equipo local).

Nombre UPN y asignación de certificados

Se recomienda que los certificados de usuario contengan un nombre principal de usuario (UPN) único en la extensión Nombre alternativo del firmante.

Nombres UPN en Active Directory

De forma predeterminada, en Active Directory todos los usuarios tienen un UPN implícito que se forma siguiendo el formato <samUsername>@<domainNetBIOS> y <samUsername>@<domainFQDN>, es decir, <nombre de usuario SAM>@<NetBIOS del dominio> y <nombre de usuario SAM>@<FQDN de dominio>. Los dominios y los nombres FQDN disponibles se incluyen en la entrada RootDSE del bosque. Tenga en cuenta que un solo dominio puede tener varias direcciones FQDN registradas en el RootDSE.

Además, todo usuario en Active Directory tiene un nombre UPN explícito y altUserPrincipalNames. Son las entradas de LDAP que especifican el nombre UPN para el usuario.

Cuando se buscan usuarios por nombre UPN, Windows examina primero el dominio actual (basado en la identidad del proceso que busca el nombre UPN) para buscar nombres UPN explícitos y luego busca nombres UPN alternativos. Si no hay coincidencias, busca el nombre UPN implícito, lo que puede resultar en varios dominios en el bosque.

Servicio de asignaciones de certificado

Si un certificado no incluye un nombre UPN explícito, Active Directory tiene la opción de almacenar un certificado público exacto para cada uso en un atributo "x509certificate". Para resolver un certificado así para un usuario, el sistema puede consultar ese atributo directamente (de forma predeterminada, en un único dominio).

Se ofrece una opción para que el usuario especifique una cuenta de usuario que acelere la búsqueda, lo que también permite que esta funcionalidad se utilice en un entorno de varios dominios.

Si hay varios dominios en el bosque y el usuario no especifica explícitamente un dominio, rootDSE de Active Directory especifica la ubicación del servicio de asignaciones de certificado. Por regla general, este servicio se encuentra en una máquina del catálogo global y tiene una vista en caché de todos los atributos "x509certificate"del bosque. Ese equipo resulta eficaz para buscar cuentas de usuario en cualquier dominio basándose solamente en el certificado.

Controlar la selección del controlador de dominio para iniciar sesión

Cuando un entorno contiene varios controladores de dominio, es muy útil ver y precisar el controlador de dominio concreto (restringir los demás) que debe utilizarse para la autenticación, de modo que los

registros se puedan habilitar y recuperar.

Controlar la selección del controlador de dominio

Para forzar Windows a usar un controlador de dominio Windows concreto para el inicio de sesión, puede establecer explícitamente la lista de los controladores de dominio que una máquina Windows puede utilizar. Para ello, debe configurar el archivo lmhosts: \Windows\System32\drivers\etc\lmhosts.

Por regla general, hay un archivo de muestra denominado "lmhosts.sam"en esa ubicación. Solo necesita incluir una línea:

1.2.3.4 cnetbiosname #PRE #DOM:mydomain

Donde "1.2.3.4"es la dirección IP del controlador de dominio llamado "dcnetbiosname"en el dominio "mydomain".

Después de reiniciarse, la máquina Windows usará esa información para iniciar sesión en "mydomain" . Tenga en cuenta que esta configuración debe revertirse cuando la depuración se complete.

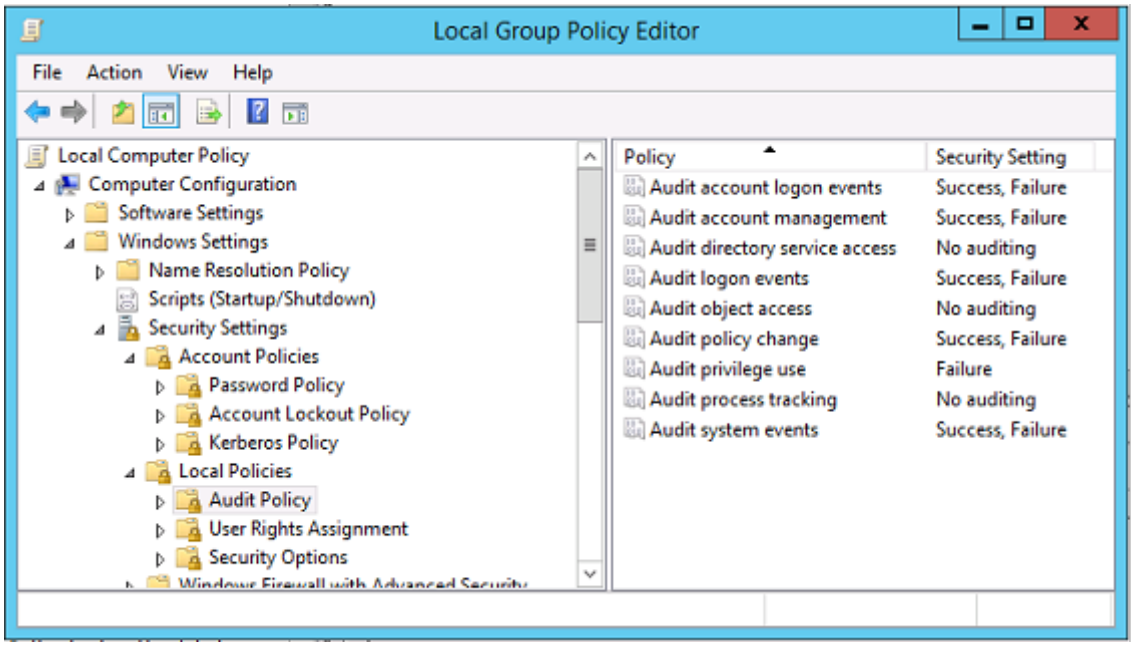
Identificar el controlador de dominio en uso

Durante el inicio de sesión, Windows aplica una variable de entorno MS-DOS con el controlador de dominio que inició la sesión del usuario. Para verlo, inicie el símbolo del sistema con el comando: **echo %LOGONSERVER%**.

Los registros relacionados con la autenticación se almacenan en el equipo que devuelva este comando.

Habilitar eventos de auditoría de cuentas

De forma predeterminada, los controladores de dominio de Windows no habilitan los registros de auditoría completa de la cuenta. La captura de registros se puede controlar mediante directivas de auditoría, ubicadas en la configuración de seguridad del Editor de directivas de grupo. Una vez habilitadas, el controlador de dominio genera más información de registro de sucesos que se guarda en el archivo del registro de seguridad.



Registros de validación de certificados

Comprobar la validez del certificado

Si un certificado de tarjeta inteligente se exporta como certificado DER (sin clave privada requerida), se puede validar con el comando: certutil –verify user.cer

Habilitar la captura de registros de CAPI

En el controlador de dominio y la máquina de usuarios, abra el visor de eventos y habilite la captura de registros de Microsoft/Windows/CAPI2/Operational Logs.

Puede gestionar la captura de registros CAPI con las claves de Registro en: CurrentControlSet\Services\crypt32.

Valor	Descripción
DiagLevel (DWORD)	Nivel de detalle (de 0 a 5)
DiagMatchAnyMask (QUADWORD)	Filtro de eventos (use 0xffffff para todo)
DiagProcessName (MULTI_SZ)	Filtrar por nombre del proceso (por ejemplo, LSASS.exe)

Registros de CAPI

Mensaje	Descripción
Compilar cadena	LSA llamado CertGetCertificateChain (incluye resultado)
Comprobar revocación	LSA llamado CertVerifyRevocation (incluye resultado)
Objetos X509	En el modo detallado, los certificados y las listas de revocación de certificados (CRL) se vuelcan en AppData\LocalLow\Microsoft\X509Objects
Comprobar directiva de cadena	LSA llamado CertVerifyChainPolicy (incluye parámetros)

Mensajes de error

Código de error	Descripción
Certificate not trusted (El certificado no es de confianza)	El certificado de tarjeta inteligente no se ha podido crear con certificados provenientes de los almacenes de certificados intermedios y certificados raíz de confianza alojados en el equipo.
Certificate revocation check error (Error en la comprobación de revocaciones de certificados)	La lista de revocación de certificados de la tarjeta inteligente no se ha podido descargar desde la dirección que especifica el punto de distribución de la CRL del certificado. Si la comprobación de revocación de certificados es obligatoria, este error impide el inicio de sesión. Consulte la sección Certificados e infraestructura de clave pública.
Certificate Usage errors (Errores de uso de certificados)	El certificado no es adecuado para el inicio de sesión. Por ejemplo, puede tratarse de un certificado de servidor o un certificado de firma.

Registros Kerberos

Para habilitar captura de registros Kerberos, en el controlador de dominio y la máquina del usuario final, cree los siguientes valores de Registro:

Subárbol de Registro	Nombre del valor	Valor [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

El registro Kerberos se guarda en el registro de eventos del sistema.

- Los mensajes del tipo "El certificado no es de confianza"deberían ser fáciles de diagnosticar.
- Hay dos códigos de error que son informativos y se pueden ignorar sin consecuencias negativas:
  - KDC_ERR_PREAUTH_REQUIRED (utilizado para la compatibilidad con versiones anteriores de controladores de dominio)
  - Error desconocido 0x4b

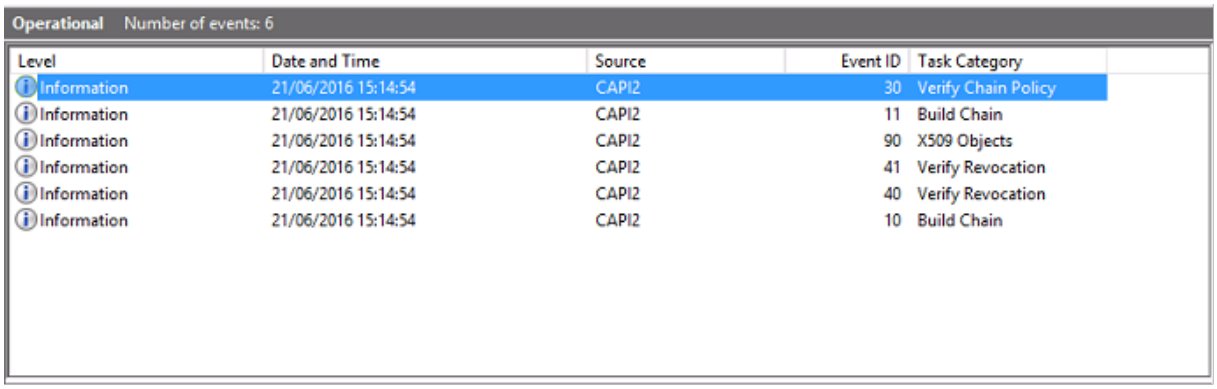
Mensajes del registro de sucesos

En esta sección, se describen entradas de registro previstas en el controlador de dominio y en la estación de trabajo cuando el usuario inicia sesión con un certificado.

- Registro de CAPI2 del controlador de dominio
- Registros de seguridad del controlador de dominio
- Registro de seguridad de Virtual Delivery Agent (VDA)
- Registro de CAPI del VDA
- Registro del sistema del VDA

Registro de CAPI2 del controlador de dominio

Durante el inicio de sesión, el controlador de dominio valida el certificado del autor de llamada, con lo que genera la siguiente secuencia de entradas de registro.



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

El último mensaje del registro de eventos muestra lsass.exe en el controlador de dominio creando una cadena basada en el certificado proporcionado por el agente VDA y comprobando la validez de ese certificado (incluida la revocación). El resultado se devuelve como "ERROR_SUCCESS".

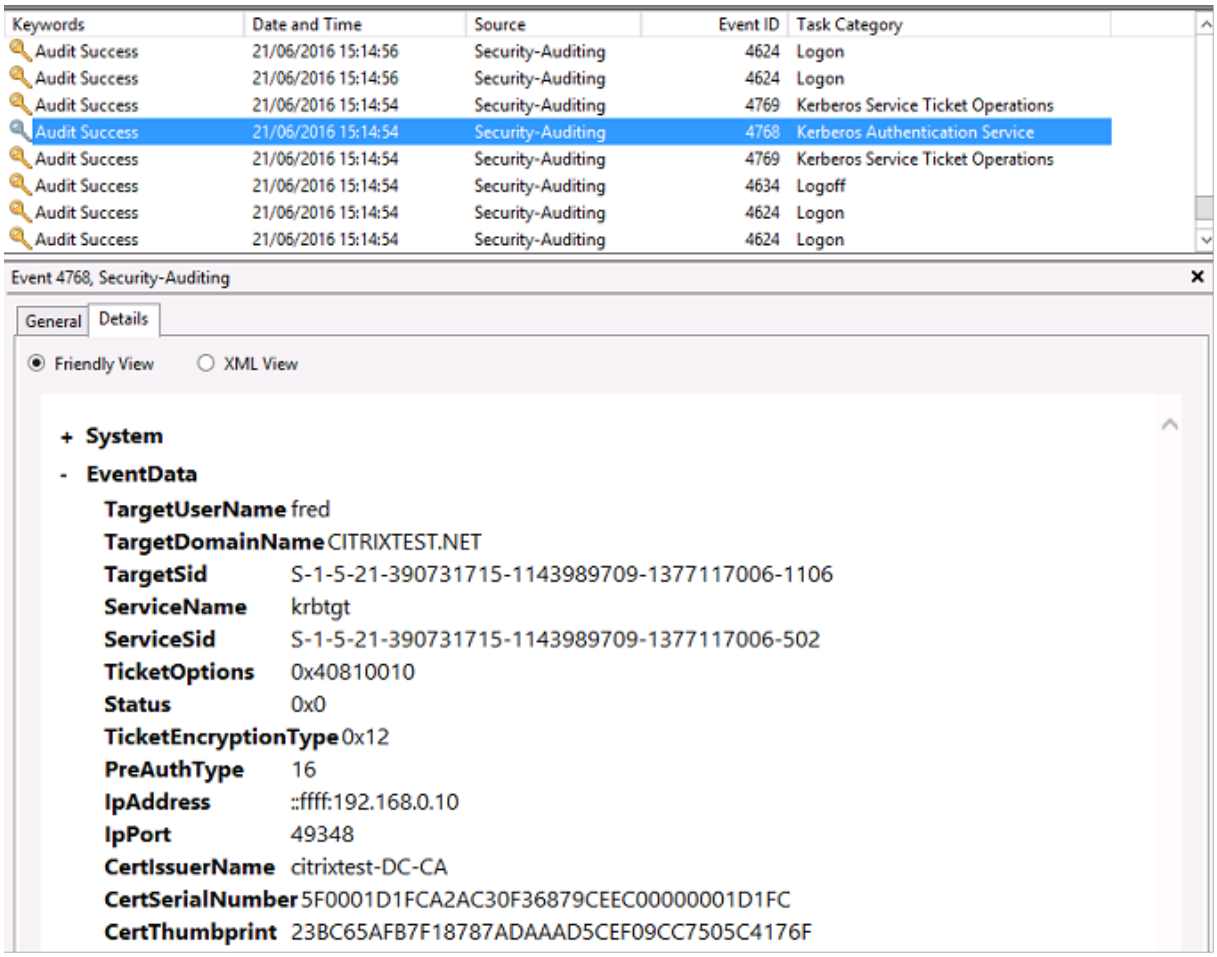
- **CertVerifyCertificateChainPolicy**
  - **Policy**
    - [**type**] CERT_CHAIN_POLICY_NT_AUTH
    - [**constant**] 6
  - **Certificate**
    - [**fileRef**] 23BC65AFB7F18787ADAAAD5CEF09CC7505C4176F.cer
    - [**subjectName**] fred
  - **CertificateChain**
    - [**chainRef**] {FF03F79B-52F8-4C93-877A-5DFFE40B9574}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

Registro de seguridad del controlador de dominio

El controlador de dominio muestra una secuencia de eventos de inicio de sesión (la clave es 4768), donde el certificado se usa para emitir el vale de concesión de vales Kerberos (krbtgt).

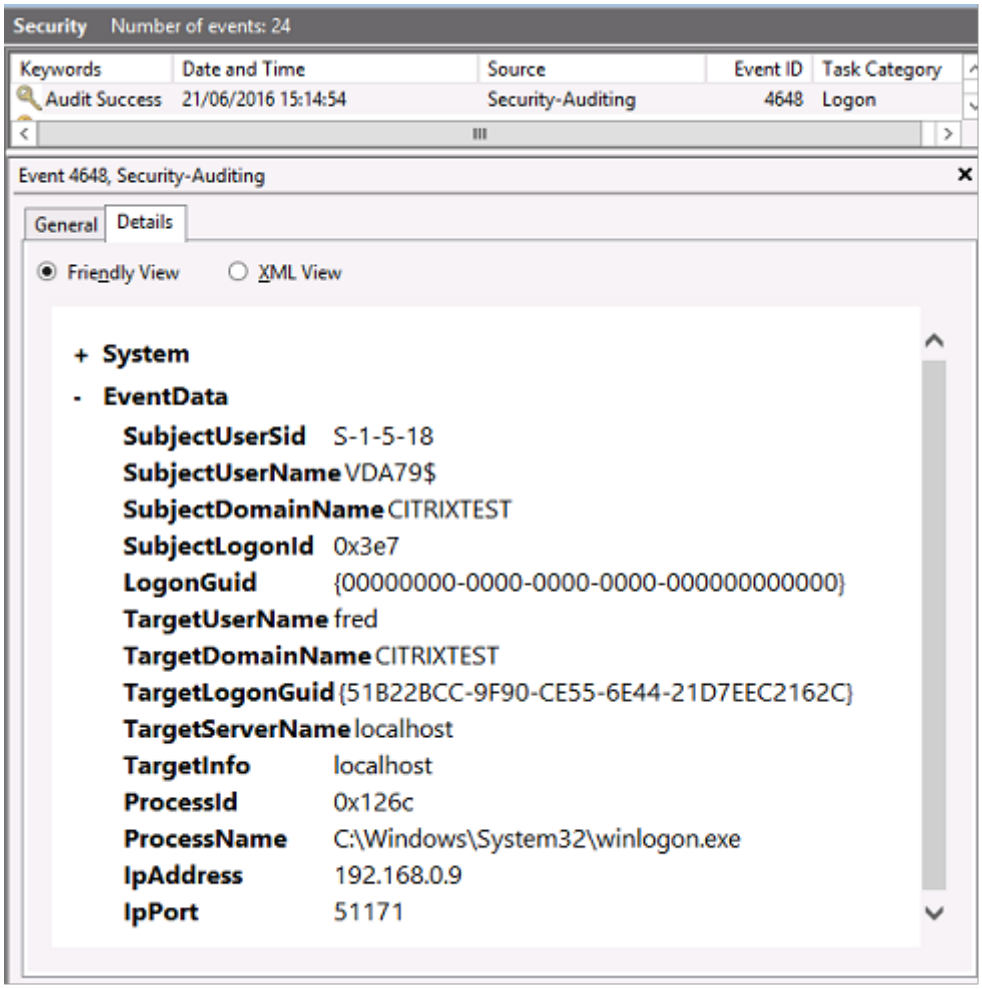
Los mensajes anteriores a este muestran la cuenta de máquina del servidor que se autentica en el

controlador de dominio. Los mensajes siguientes muestran la cuenta de usuario que pertenece al nuevo vale krbtgt que se usa para autenticarse en el controlador de dominio.



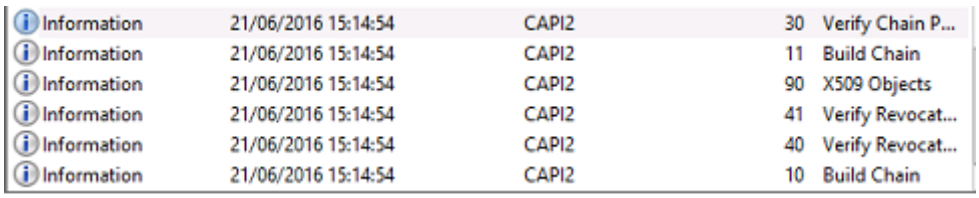
Registro de seguridad del VDA

El registro de auditoría de seguridad del VDA que corresponde al evento de inicio de sesión es la entrada cuyo ID de evento es 4648, originado de winlogon.exe.



Registro de CAPI del VDA

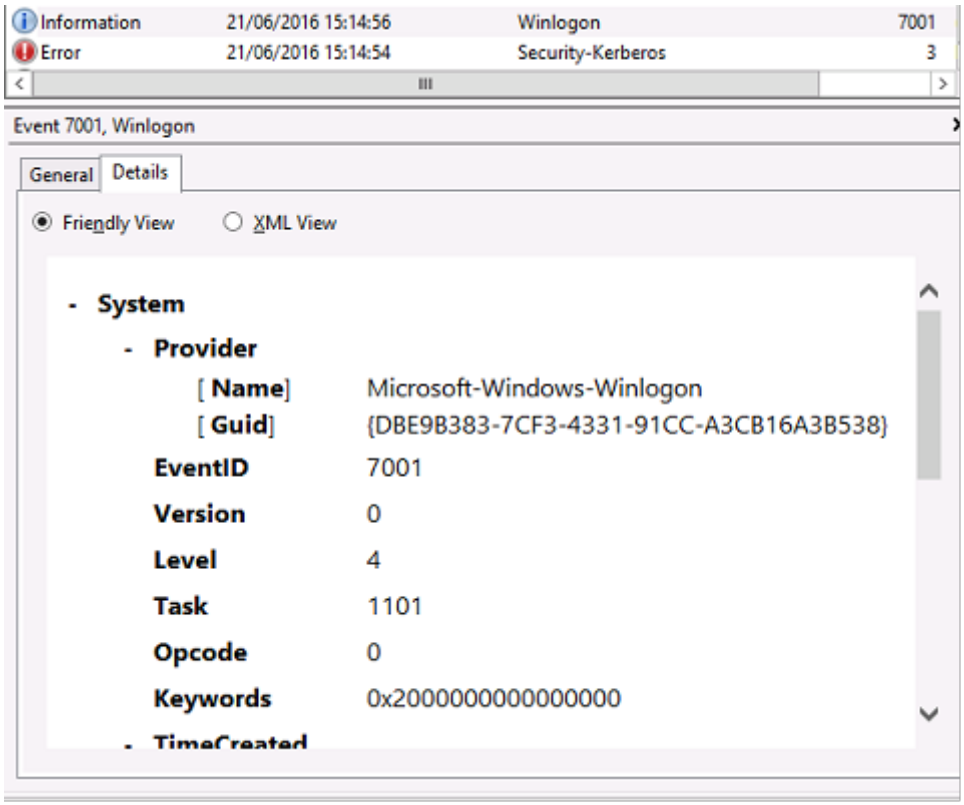
En este ejemplo, el registro de CAPI del VDA muestra una sola secuencia de compilación de cadena y comprobación desde lsass.exe, que valida el certificado del controlador de dominio (dc.citrixtest.net).



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

Registro del sistema del VDA

Si la captura de registros Kerberos está habilitada, el registro del sistema muestra el error KDC_ERR_PREAUTH_REQUIRED (que se puede ignorar) y una entrada de Winlogon con el mensaje de que el inicio de sesión con Kerberos se realizó correctamente.



Mensajes de error del usuario final

En esta sección, se ofrece una lista de los mensajes de error comunes que ve un usuario en la página de inicio de sesión de Windows.

Mensaje de error mostrado	Descripción y referencia
Nombre de usuario o contraseña no válidos.	El equipo cree que usted tiene un certificado y una clave privada válidos, pero el controlador de dominio Kerberos ha rechazado la conexión. Consulte la sección *Registros Kerberos* de este artículo.
El sistema no pudo iniciar sesión. No se pudieron comprobar las credenciales. / La solicitud no se admite.	No se puede establecer contacto con el controlador de dominio o no se ha configurado el controlador de dominio con un certificado que admite la autenticación de tarjeta inteligente. Inscriba el controlador de dominio para un certificado de "autenticación Kerberos", de "autenticación de controlador de dominio"o de "controlador de dominio". Suele valer la pena intentarlo incluso cuando el certificado existente parezca válido.
El sistema no pudo iniciar sesión. No se puede determinar el estado de revocación del certificado de la tarjeta inteligente usado para la autenticación.	Los certificados intermedios y de raíz no están instalados en el equipo local. Consulte Certificados e infraestructura de clave pública.
Solicitud incorrecta.	Normalmente, esto indica que las extensiones del certificado no están configuradas correctamente o la clave RSA es demasiado corta (<2048 bits).

Información relacionada

- Configuración de un dominio para el inicio de sesión con tarjeta inteligente: http://support.citrix.com/article/CTX206156
- Directivas de inicio de sesión de tarjeta inteligente: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/ff404287(v=ws.10)
- Habilitación del registro de CAPI: http://social.technet.microsoft.com/wiki/contents/articles/242.troubleshooting-pki-problems-on-windows.aspx
- Habilitación del registro de Kerberos: https://support.microsoft.com/en-us/kb/262177

- Instrucciones para habilitar el inicio de sesión mediante tarjeta inteligente con entidades externas de certificación: https://support.microsoft.com/en-us/kb/281245

Cmdlets de PowerShell

March 30, 2023

Aunque la consola de administración del Servicio de autenticación federada (FAS) es adecuada para implementaciones simples, la interfaz de PowerShell ofrece opciones más avanzadas. Si va a usar opciones que no están disponibles en la consola, Citrix recomienda utilizar solo PowerShell para la configuración.

El siguiente comando agrega los cmdlets de PowerShell para FAS:

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

En una ventana de PowerShell, use Get-Help <*nombre del cmdlet*> para ver la ayuda del cmdlet.

Para obtener más información sobre los cmdlets de FAS PowerShell SDK, consulte https://developer-docs.citrix.com/projects/federated-authentication-service-powershell-cmdlets/en/latest/.