



# Servicio de autenticación federado

# Contents

|                                                                         |    |
|-------------------------------------------------------------------------|----|
| Servicio de autenticación federada 2308                                 | 9  |
| Versiones anteriores                                                    | 9  |
| Referencias                                                             | 10 |
| Federated Authentication Service 2308                                   | 11 |
| Problemas resueltos                                                     | 11 |
| Problemas conocidos                                                     | 11 |
| Avisos de terceros                                                      | 11 |
| Requisitos del sistema                                                  | 12 |
| Instalar y configurar                                                   | 13 |
| Secuencia de instalación y configuración                                | 13 |
| Instalar el Servicio de autenticación federada                          | 13 |
| Actualización de FAS                                                    | 14 |
| Habilitar el complemento de FAS en los almacenes de StoreFront          | 14 |
| Configurar el Delivery Controller™                                      | 15 |
| Configurar la directiva de grupo                                        | 15 |
| Comportamiento en la sesión                                             | 19 |
| Ámbito de la solicitud                                                  | 20 |
| Tiempo de espera de consentimiento                                      | 21 |
| desconectar al bloquear                                                 | 21 |
| Uso de la consola de administración de Federated Authentication Service | 21 |
| Implementar plantillas de certificados                                  | 22 |
| Configurar Servicios de certificados de Active Directory                | 24 |
| Autorizar Servicio de autenticación federada                            | 25 |
| Configurar reglas                                                       | 27 |
| Conectarse a Citrix Cloud                                               | 32 |
| desconectar de Citrix Cloud                                             | 37 |

|                                                                              |    |
|------------------------------------------------------------------------------|----|
| Configuración avanzada                                                       | 38 |
| Información relacionada                                                      | 38 |
| Habilitar el Servicio de autenticación federada para un cliente de inquilino | 38 |
| Requisitos previos                                                           | 38 |
| Configurar el cliente MSP                                                    | 38 |
| Problema conocido                                                            | 41 |
| Inicio de sesión único de Azure Active Directory                             | 41 |
| VDA unidos a un dominio                                                      | 43 |
| VDA unidos de forma híbrida                                                  | 43 |
| Configuración de la autoridad de certificación                               | 45 |
| Configurar varios servidores CA para su uso en FAS                           | 45 |
| Cambios de comportamiento esperados                                          | 46 |
| Configurar la autoridad de certificación de Microsoft para el acceso TCP     | 46 |
| Generar previamente certificados de usuario                                  | 48 |
| Obtener una lista de usuarios de Active Directory                            | 48 |
| Servidor FAS                                                                 | 49 |
| Renovar certificados de la autoridad de registro                             | 50 |
| Información relacionada                                                      | 51 |
| Protección de claves privadas                                                | 52 |
| Introducción                                                                 | 52 |
| Configuración de claves privadas                                             | 53 |
| Ejemplos de escenarios de configuración                                      | 56 |
| Ejemplo 1                                                                    | 56 |
| Ejemplo 2                                                                    | 56 |
| Ejemplo 3                                                                    | 67 |
| Almacenamiento de certificados de FAS                                        | 69 |
| Información relacionada                                                      | 71 |
| Configuración de seguridad y red                                             | 71 |

|                                                                          |    |
|--------------------------------------------------------------------------|----|
| Arquitectura de red                                                      | 71 |
| Firewall y seguridad de red                                              | 72 |
| Conexiones entre Citrix Federated Authentication Service y Citrix Cloud™ | 73 |
| Consideraciones de seguridad                                             | 74 |
| Agentes de inscripción delegados                                         | 74 |
| Configuración de la lista de control de acceso                           | 75 |
| Configuración del firewall                                               | 75 |
| Supervisión del registro de eventos                                      | 75 |
| Módulos de seguridad de hardware                                         | 75 |
| Responsabilidades de administración                                      | 76 |
| Configuración de directivas de grupo                                     | 77 |
| Plantillas de certificado                                                | 77 |
| Cambiar el nombre de una plantilla de certificado                        | 77 |
| Modificar las propiedades generales                                      | 78 |
| Modificar las propiedades de control de solicitudes                      | 78 |
| Modificar las propiedades de criptografía                                | 78 |
| Modificar las propiedades de atestación de clave                         | 78 |
| Modificar las propiedades de las plantillas reemplazadas                 | 78 |
| Modificar las propiedades de las extensiones                             | 78 |
| Modificar las propiedades de seguridad                                   | 78 |
| Modificar las propiedades del nombre del sujeto                          | 79 |
| Modificar las propiedades del servidor                                   | 79 |
| Modificar las propiedades de requisitos de emisión                       | 79 |
| Modificar las propiedades de compatibilidad                              | 80 |
| Administración de la entidad de certificación                            | 80 |
| Publicación de plantillas                                                | 80 |
| Configuración del firewall                                               | 81 |
| Inscripción restringida                                                  | 81 |

|                                                                       |    |
|-----------------------------------------------------------------------|----|
| Módulos de directivas y auditoría                                     | 81 |
| Administración de FAS                                                 | 82 |
| Restringir StoreFront, usuarios y VDA a través de una ACL             | 82 |
| Configurar reglas                                                     | 82 |
| Configurar la autoridad de certificación y las plantillas             | 83 |
| Certificados en sesión y de autenticación                             | 83 |
| Protección de clave privada y longitud de clave                       | 83 |
| Registros de eventos                                                  | 83 |
| Acceso administrativo y herramientas de administración                | 83 |
| Administradores de Citrix Virtual Apps, Citrix Virtual Desktops y VDA | 84 |
| Seguridad general del servidor Windows                                | 84 |
| Información relacionada                                               | 84 |
| Contadores de rendimiento                                             | 84 |
| Solucionar problemas de inicio de sesión de Windows                   | 86 |
| Certificados e infraestructura de clave pública                       | 86 |
| Asignación de nombres UPN y certificados                              | 87 |
| Nombres UPN en Active Directory                                       | 88 |
| Servicio de asignación de certificados                                | 88 |
| Controlar la selección del controlador de dominio de inicio de sesión | 88 |
| Controlar la selección del controlador de dominio                     | 88 |
| Identificar el controlador de dominio en uso                          | 89 |
| Habilitar eventos de auditoría de cuenta                              | 89 |
| Registros de validación de certificados                               | 89 |
| Comprobar la validez del certificado                                  | 89 |
| Habilitar el registro de CAPI                                         | 89 |
| Registros CAPI                                                        | 90 |
| Mensajes de error                                                     | 90 |
| Registros de Kerberos                                                 | 91 |

|                                                                  |     |
|------------------------------------------------------------------|-----|
| Registros del controlador de dominio y de la estación de trabajo | 92  |
| Registro CAPI2 del controlador de dominio                        | 92  |
| Registro de seguridad del controlador de dominio                 | 93  |
| Registro de seguridad del VDA                                    | 94  |
| Registro CAPI de VDA                                             | 95  |
| Registro del sistema de VDA                                      | 96  |
| Supervisión de FAS mediante el registro de eventos de Windows    | 96  |
| ¿Se está ejecutando el servicio FAS?                             | 97  |
| Eventos de estado de FAS                                         | 97  |
| Eventos de FAS conectados a la nube                              | 99  |
| Eventos de seguridad                                             | 100 |
| Registros de eventos de FAS                                      | 101 |
| Eventos de administración                                        | 101 |
| Creación de aserciones de identidad                              | 104 |
| Actuando como parte que confía                                   | 104 |
| Servidor de certificados en sesión                               | 105 |
| Complemento de aserción de FAS                                   | 105 |
| FAS habilitado para Workspace                                    | 106 |
| Inicio de sesión                                                 | 108 |
| Certificados en sesión                                           | 108 |
| Solicitud de certificado y generación de par de claves           | 109 |
| Mensajes de error para el usuario final                          | 109 |
| Información relacionada                                          | 110 |
| Cmdlets de PowerShell                                            | 111 |
| Arquitecturas de implementación                                  | 112 |
| Introducción                                                     | 112 |
| Descripción general de la arquitectura                           | 112 |
| Implementación interna                                           | 113 |

|                                                          |     |
|----------------------------------------------------------|-----|
| Implementación de Citrix Gateway                         | 116 |
| Implementación de ADFS SAML                              | 119 |
| Asignación de cuentas B2B                                | 120 |
| Unión a Azure AD en Windows 10                           | 121 |
| Implementación de ADFS                                   | 123 |
| Introducción                                             | 123 |
| Información general de SAML                              | 125 |
| URL de redirección                                       | 125 |
| Identificador                                            | 125 |
| Dirección de retorno                                     | 125 |
| Certificado de firma                                     | 125 |
| URL de cierre de sesión único                            | 126 |
| Configuración                                            | 126 |
| Rellenar la política SAML                                | 126 |
| Información relacionada                                  | 127 |
| Integración de Azure AD                                  | 127 |
| Introducción                                             | 127 |
| Arquitectura                                             | 129 |
| Crear una zona DNS                                       | 131 |
| Crear un servicio en la nube                             | 132 |
| Crear máquinas virtuales Windows                         | 132 |
| Controlador de dominio                                   | 133 |
| Controlador ADFS y servidor proxy de aplicación web      | 134 |
| Controlador de entrega y VDA de Citrix Virtual Desktops™ | 134 |
| Configurar un DNS interno                                | 134 |
| Configurar una dirección DNS externa                     | 135 |
| Configurar grupos de seguridad                           | 136 |
| Crear un certificado ADFS                                | 136 |

|                                                                                          |     |
|------------------------------------------------------------------------------------------|-----|
| Configurar Azure AD                                                                      | 137 |
| Crear un nuevo directorio                                                                | 137 |
| Crear un usuario administrador global (AzureAdmin)                                       | 139 |
| Registrar su dominio con Azure AD                                                        | 140 |
| Instalar Azure AD Connect                                                                | 141 |
| Habilitar la unión a Azure AD                                                            | 151 |
| Instalar Citrix Virtual Apps o Citrix Virtual Desktops                                   | 154 |
| Instalar el Servicio de autenticación federada                                           | 155 |
| Configurar StoreFront                                                                    | 155 |
| Configurar StoreFront para usar Citrix Gateway                                           | 156 |
| Configurar una nueva aplicación de Azure AD para el inicio de sesión único en StoreFront | 157 |
| Configurar un icono                                                                      | 158 |
| Configurar la autenticación SAML                                                         | 158 |
| Asignar la aplicación a los usuarios                                                     | 160 |
| Página de MyApps                                                                         | 161 |
| URL de inicio de sesión único                                                            | 162 |
| Instalar y configurar Citrix Gateway                                                     | 162 |
| Ejecute el asistente de configuración de Citrix Virtual Apps and Desktops                | 162 |
| Configurar el controlador de dominio para la administración de cuentas de AD             | 164 |
| Configurar la dirección de StoreFront                                                    | 164 |
| verificar la implementación de Citrix Gateway                                            | 165 |
| Habilitar la compatibilidad con la autenticación SAML de Citrix Gateway                  | 166 |
| verificar el sistema de extremo a extremo                                                | 167 |
| Apéndice                                                                                 | 168 |
| Proporcione una dirección IP pública y una dirección DNS                                 | 168 |
| Configurar reglas de firewall (grupo de seguridad)                                       | 169 |
| Información relacionada                                                                  | 170 |
| Historial de la documentación de Federated Authentication Service 2308                   | 171 |

# Servicio de autenticación federada 2308

---

El Servicio de autenticación federada (FAS) es un componente privilegiado diseñado para integrarse con los Servicios de certificados de Active Directory. Emite certificados dinámicamente para los usuarios, lo que les permite iniciar sesión en un entorno de Active Directory como si tuvieran una tarjeta inteligente. Esto permite a StoreFront™ utilizar una gama más amplia de opciones de autenticación, como las aserciones SAML (Security Assertion Markup Language). SAML se utiliza habitualmente como alternativa a las cuentas de usuario tradicionales de Windows en Internet.

**Federated Authentication Service 2308** es la versión más reciente de Current Release de FAS. Este artículo refleja las funciones y configuraciones de esta última versión.

## Versiones anteriores

Para obtener documentación sobre versiones anteriores de FAS, consulte:

- [Servicio de autenticación federada 2305](#)
- [Servicio de autenticación federada 2303](#)
- [Servicio de autenticación federada 2212](#)
- [Servicio de autenticación federada 2209](#)
- [Servicio de autenticación federada 2206](#)
- [Servicio de autenticación federada 2203 LTSR](#)
- [Servicio de autenticación federada 2112](#)
- [Servicio de autenticación federada 2109](#)
- [Servicio de autenticación federada 2106](#)
- [Servicio de autenticación federada 2103](#)
- [Servicio de autenticación federada 1912 LTSR\(/es-es/federated-authentication-service/1912-ltsr.html\)](#)
- [XenApp y XenDesktop 7.15 Long Term Service Release\(/es-es/xenapp-and-xendesktop/7-15-ltsr.html\)](#)

La estrategia del ciclo de vida del producto para las versiones actuales (CR) y las versiones de servicio a largo plazo (LTSR) se describe en [Hitos del ciclo de vida](#).

## Referencias

- Información general de los Servicios de certificados de Active Directory([https://docs.microsoft.com/es-es/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/hh831740\(v=ws.11\)](https://docs.microsoft.com/es-es/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/hh831740(v=ws.11)))
- Configuración de Windows para el inicio de sesión con certificado(<http://support.citrix.com/article/CTX206156>)

# Federated Authentication Service 2308

---

Esta versión de Federated Authentication Service no incluye nuevas funciones.

Para obtener información sobre las correcciones de errores, consulte [Problemas resueltos](#).

## Problemas resueltos

No hay problemas resueltos en Federated Authentication Service 2308.

## Problemas conocidos

No hay problemas conocidos en Federated Authentication Service 2308.

La siguiente advertencia se aplica a cualquier solución alternativa que sugiera cambiar una entrada del Registro:

### ADVERTENCIA:

La modificación incorrecta del Registro puede causar problemas graves que pueden obligarle a reinstalar el sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización incorrecta del Editor del Registro puedan resolverse. Utilice el Editor del Registro bajo su propia responsabilidad. Asegúrese de hacer una copia de seguridad del Registro antes de modificarlo.

## Avisos de terceros

Esta versión de Federated Authentication Service puede incluir software de terceros con licencia bajo los términos definidos en los siguientes documentos:

- [Avisos de terceros de Citrix Virtual Apps and Desktops](#) (Descarga de PDF)
- [Divulgaciones de software no comercial para FlexNet Publisher 2017 \(11.15.0.0\)](#) (Descarga de PDF)
- [Suplemento de documentación de FlexNet Publisher: Software de terceros y de código abierto utilizado en FlexNet Publisher 11.15.0](#) (Descarga de PDF)

# Requisitos del sistema

---

- Federated Authentication Service (FAS) es compatible con las siguientes versiones de Windows Server:
  - Windows Server 2022, ediciones Standard y Datacenter
  - Windows Server 2019, ediciones Standard y Datacenter, y con la opción Server Core
  - Windows Server 2016, ediciones Standard y Datacenter, y con la opción Server Core
- Citrix recomienda instalar FAS en un servidor que no tenga ningún otro componente de Citrix.
- El servidor Windows debe estar protegido, ya que tiene acceso a un certificado de autoridad de registro y a una clave privada. El certificado y la clave privada permiten al servidor emitir certificados para los usuarios del dominio. El servidor también tiene acceso a los certificados de usuario de dominio emitidos y a las claves privadas.
- Los (</es-es/federated-authentication-service/2308/config-manage/ps-sdk.html>) de FAS requieren Windows PowerShell de 64 bits instalado en el servidor FAS.
- Se requiere una entidad de certificación empresarial de Microsoft (raíz o subordinada) para emitir certificados de usuario.

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

- Los Delivery Controllers, los Virtual Delivery Agents (VDA) y los servidores StoreFront™ deben ser todas versiones compatibles.
- Antes de crear el Catálogo de máquinas, la configuración de la directiva de grupo de Federated Authentication Service debe aplicarse correctamente a los VDA. Consulte la sección (</es-es/federated-authentication-service/2308/install-configure.html#configure-group-policy>) para obtener más detalles.

Al planificar la implementación de este servicio, revise la sección (</es-es/federated-authentication-service/2308/config-manage/security.html#security-considerations>).

# Instalar y configurar

---

## Secuencia de instalación y configuración

1. [Instalar el Servicio de autenticación federada \(FAS\)](#)
2. [Habilitar el complemento de FAS en los almacenes de StoreFront](#)
3. [Configurar el Delivery Controller](#)
4. [Configurar la Directiva de grupo](#)
5. Utilice la consola de administración de FAS para:
  - a. [Implementar plantillas de certificado](#)
  - b. [Configurar autoridades de certificación](#)
  - c. [Autorizar a FAS a usar sus autoridades de certificación](#)
  - d. [Configurar reglas](#)
  - e. [Conectar FAS a Citrix Cloud](#) (opcional)

## Instalar el Servicio de autenticación federada

Por motivos de seguridad, Citrix recomienda instalar el Servicio de autenticación federada (FAS) en un servidor dedicado. Este servidor debe protegerse de forma similar a un controlador de dominio o una autoridad de certificación. FAS se puede instalar desde:

- el instalador de Citrix Virtual Apps and Desktops™ (desde el botón **Federated Authentication Service** en la pantalla de inicio automático cuando se inserta la ISO), o
- el archivo de instalación independiente de FAS (disponible como archivo MSI en [Citrix Downloads](#)).

Estos instalan los siguientes componentes:

- Servicio de autenticación federada
- [Cmdlets de complemento de PowerShell](#) para la configuración avanzada de FAS
- [Consola de administración de FAS](#)
- Plantillas de directiva de grupo de FAS (CitrixFederatedAuthenticationService.admx/adml)

- Archivos de plantilla de certificado
- [Contadores de rendimiento y registros de eventos](#)

## Actualización de FAS

Puede actualizar FAS a una versión más reciente mediante una actualización in situ. Antes de actualizar, tenga en cuenta lo siguiente:

- Todas las configuraciones del servidor FAS se conservan al realizar una actualización in situ.
- Asegúrese de cerrar la consola de administración de FAS antes de actualizar FAS.
- Asegúrese de que al menos un servidor FAS esté siempre disponible. Si ningún servidor StoreFront™ habilitado para el Servicio de autenticación federada puede acceder a un servidor, los usuarios no podrán iniciar sesión ni iniciar aplicaciones.

Para iniciar una actualización, instale FAS desde el instalador de Citrix Virtual Apps and Desktops o desde el archivo de instalación independiente de FAS.

## Habilitar el complemento de FAS en los almacenes de StoreFront

### NOTA:

No necesita este paso si usa FAS solo con Citrix Cloud.

Para habilitar la integración de FAS en un almacén de StoreFront, ejecute los siguientes cmdlets de PowerShell como una cuenta de administrador. Si el almacén tiene un nombre diferente, modifique `$StoreVirtualPath`.

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

$StoreVirtualPath = "/Citrix/Store"

$store = Get-STFStoreService -VirtualPath $StoreVirtualPath

$auth = Get-STFAuthenticationService -StoreService $store

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

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

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

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

## Configurar el Delivery Controller™

### NOTA:

No necesita este paso si usa FAS solo con Citrix Cloud.

Para usar FAS, configure el Delivery Controller de Citrix Virtual Apps o Citrix Virtual Desktops™ para que confíe en los servidores de StoreFront que se conectan a él: ejecute el cmdlet de PowerShell **Set-BrokerSite -TrustRequestsSentToTheXmlServicePort \$true**. Ejecute este comando una vez por sitio, independientemente del número de Delivery Controllers en el sitio.

## Configurar la directiva de grupo

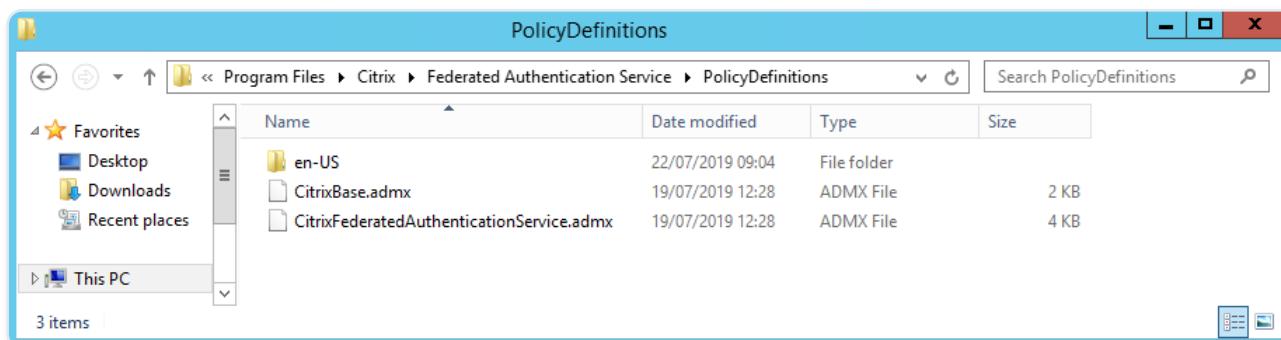
Después de instalar FAS, use las plantillas de directiva de grupo proporcionadas en la instalación para especificar los nombres de dominio completos (FQDN) de los servidores en la directiva de grupo.

**IMPORTANTE:**

Asegúrese de que los servidores de StoreFront que solicitan tickets y los Virtual Delivery Agents (VDA) que canjean tickets tengan una configuración idéntica de FQDN, incluida la numeración automática de servidores aplicada por el objeto de directiva de grupo.

Para simplificar, los siguientes ejemplos configuran una única directiva a nivel de dominio que se aplica a todas las máquinas. Sin embargo, esto no es obligatorio. FAS funciona siempre que los servidores de StoreFront, los VDA y la máquina que ejecuta la consola de administración de FAS vean la misma lista de FQDN. Consulte el paso 6.

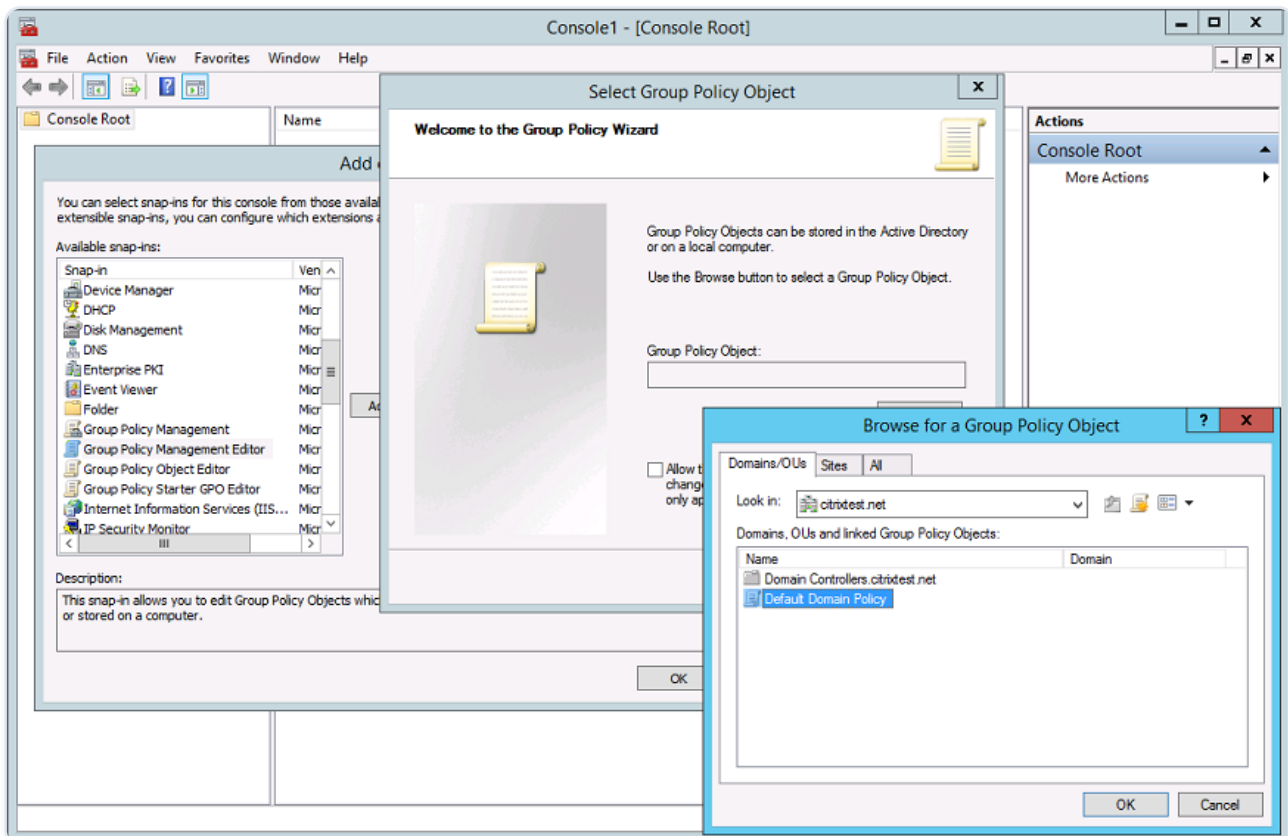
**Paso 1.** En el servidor donde instaló FAS, busque los archivos C:\Program Files\Citrix\Federated Authentication Service\PolicyDefinitions\CitrixFederatedAuthenticationService.admx y CitrixBase.admx, y la carpeta en-US.



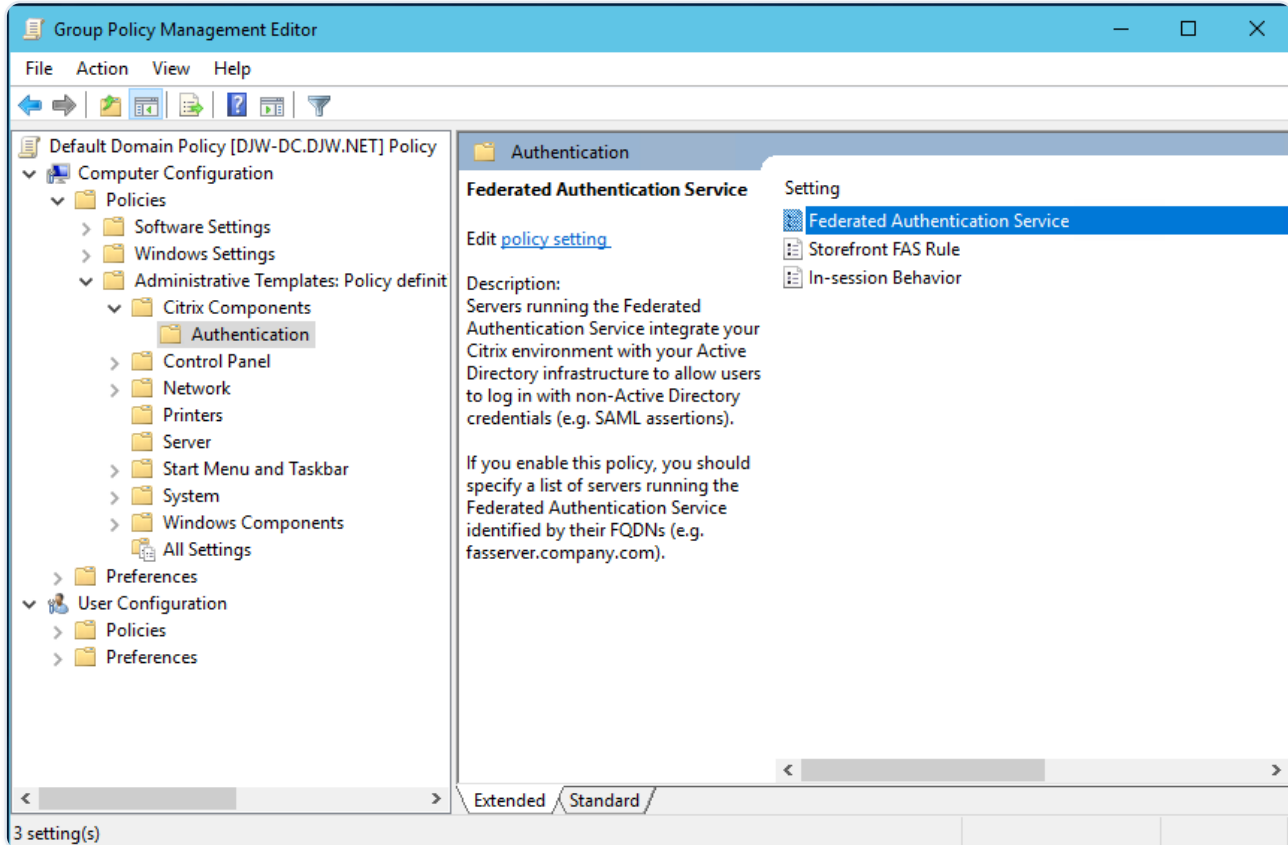
**Paso 2.** Copie estos archivos en sus controladores de dominio y colóquelos en la subcarpeta C:\Windows\PolicyDefinitions y en-US.

**Paso 3.** Ejecute Microsoft Management Console (mmc.exe desde la línea de comandos). En la barra de menú, 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 de dominio predeterminada**. De forma alternativa, puede crear y seleccionar un objeto de directiva adecuado para su entorno, utilizando las herramientas de su elección. La directiva debe aplicarse a todas las máquinas que ejecuten el software de Citrix afectado (VDAs, servidores StoreFront, herramientas de administración).



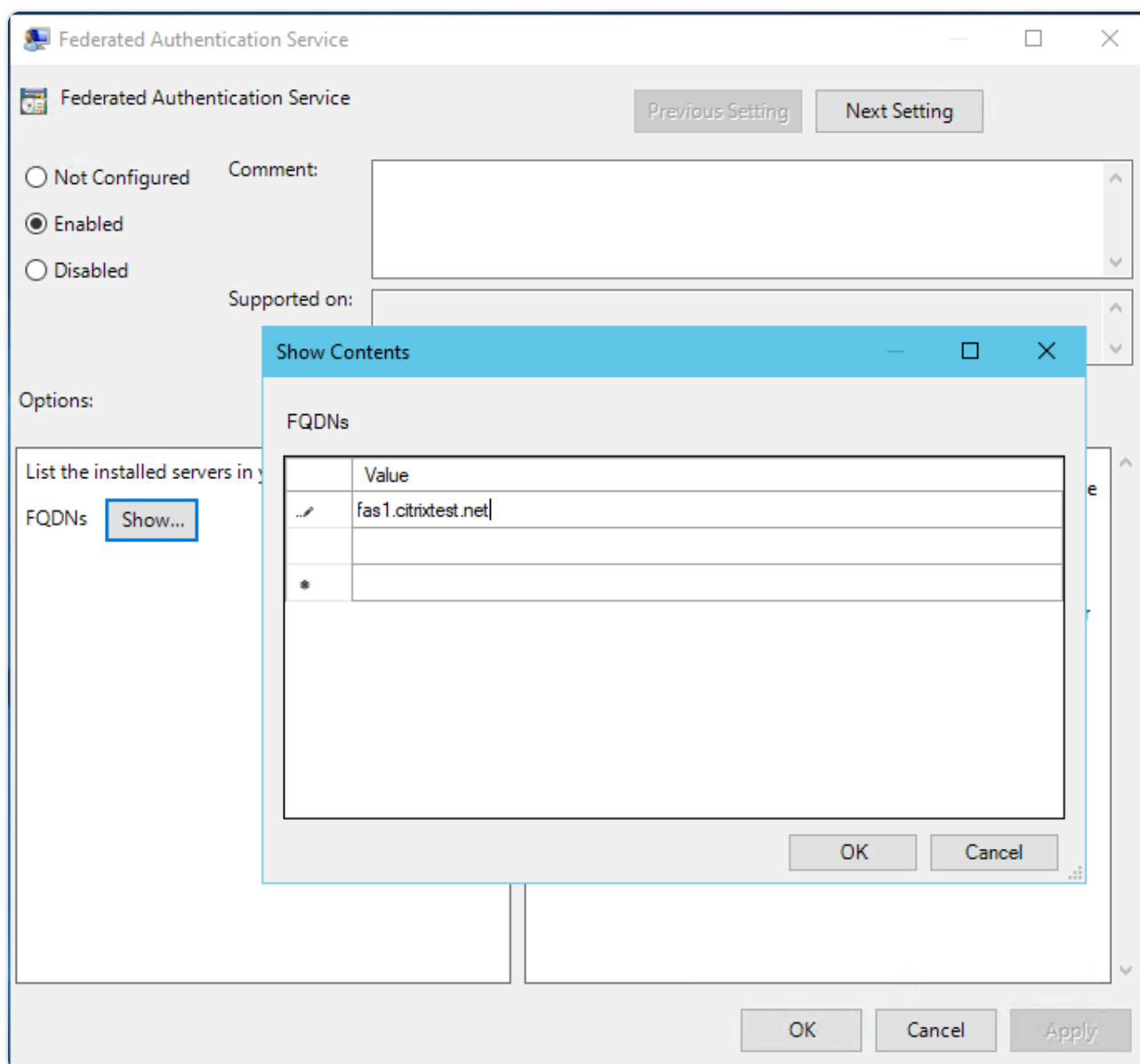
**Paso 4.** Vaya a la directiva *Federated Authentication Service* en Configuración del equipo/Directivas/Plantillas administrativas/Componentes de Citrix/Autenticación.



**NOTA:**

La configuración de la directiva de Federated Authentication Service solo está disponible en la GPO de dominio cuando se agrega el archivo de plantilla CitrixBase.admx/CitrixBase.adml a la carpeta PolicyDefinitions. Después del Paso 3, la configuración de la directiva de Federated Authentication Service aparece en la carpeta **Plantillas administrativas > Componentes de Citrix > Autenticación**.

**Paso 5.** Abra la directiva de Federated Authentication Service y seleccione **Habilitada**. Esto le permite seleccionar el botón **Mostrar**, donde configura los FQDN de sus servidores FAS.



**Paso 6.** Introduzca los FQDN de los servidores FAS.

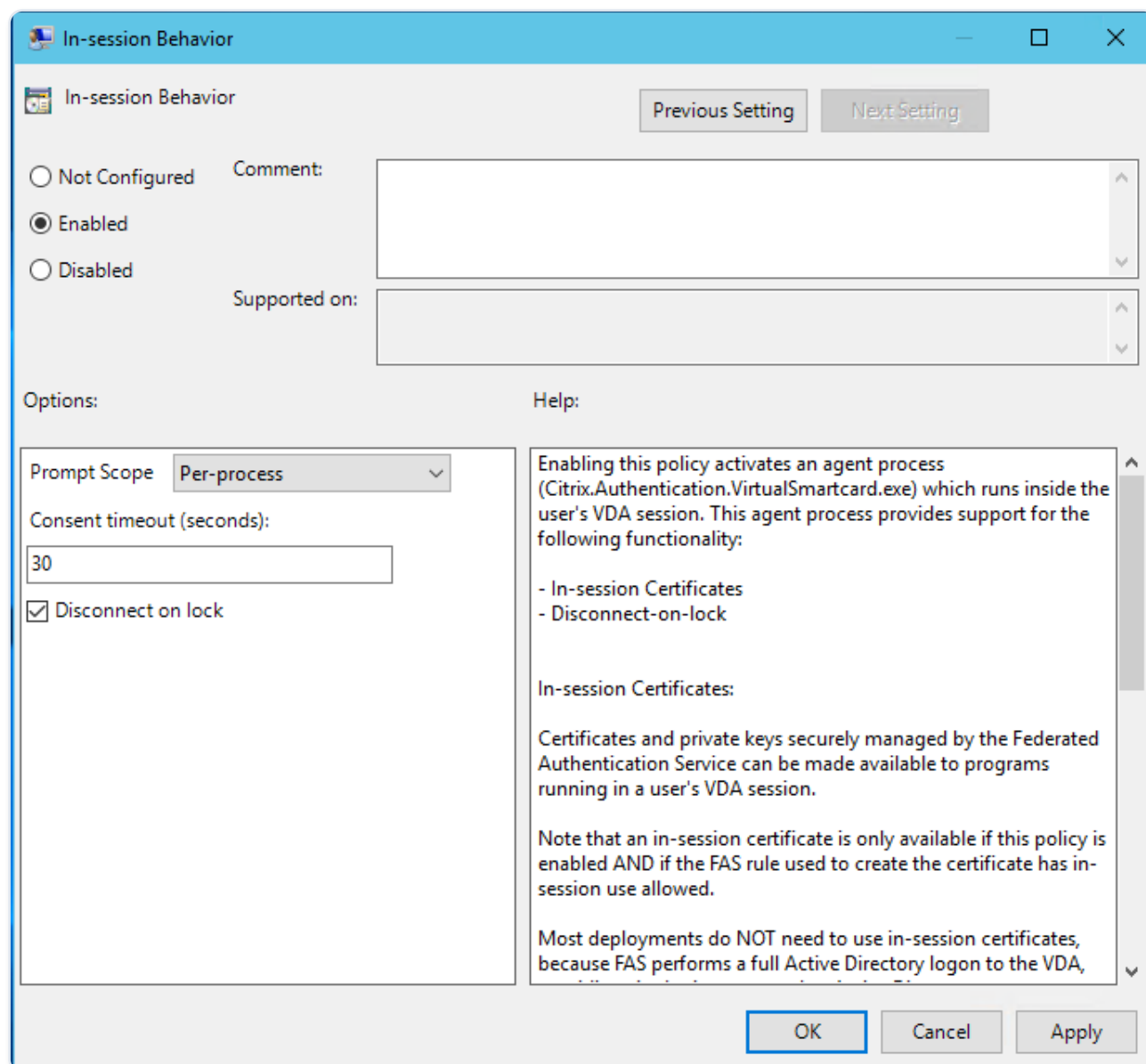
**IMPORTANTE:**

Si introduce varios FQDN, el orden de la lista debe ser coherente tal y como lo ven los VDAs, los servidores StoreFront (si están presentes) y los servidores FAS. Consulte [Configuración de directivas de grupo](#).

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

## Comportamiento en la sesión

Esta directiva activa un proceso de agente en la sesión VDA del usuario que admite certificados en la sesión, consentimiento y desconectar al bloquear. Los certificados en la sesión solo están disponibles si esta directiva está habilitada y si la regla de FAS utilizada para crear el certificado permite el uso en la sesión, consulte [Configurar reglas](#).



**Habilitar** activa esta directiva y permite que un proceso de agente de FAS se ejecute en la sesión VDA del usuario.

**Deshabilitar** desactiva la directiva e impide que se ejecute el proceso de agente de FAS.

### Ámbito de la solicitud

Si esta directiva está habilitada, **Ámbito de la solicitud** controla cómo se solicita a los usuarios su consentimiento para permitir que una aplicación utilice un certificado en la sesión. Hay tres opciones:

- **No se requiere consentimiento**—Esta opción deshabilita la solicitud de seguridad y las claves privadas se utilizan de forma silenciosa.
- **Consentimiento por proceso**—Cada programa en ejecución solicita el consentimiento individualmente.

- **Consentimiento por sesión**—Una vez que el usuario ha hecho clic en **Aceptar**, esta opción se aplica a todos los programas de la sesión.

### Tiempo de espera de consentimiento

Si esta directiva está habilitada, **Tiempo de espera de consentimiento** controla la duración (en segundos) del consentimiento. Por ejemplo, con 300 segundos, los usuarios ven una solicitud cada cinco minutos. Un valor de cero solicita a los usuarios cada operación de clave privada.

### desconectar al bloquear

Si esta directiva está habilitada, la sesión del usuario se desconecta automáticamente cuando bloquea la pantalla. Este comportamiento es similar a la directiva de "desconectar al quitar la tarjeta inteligente". Utilice esta función cuando los usuarios no tengan credenciales de inicio de sesión de Active Directory.

#### NOTA:

La directiva de desconectar al bloquear se aplica a todas las sesiones del VDA.

## Uso de la consola de administración de Federated Authentication Service

#### NOTA:

Aunque la consola de administración de FAS es adecuada para la mayoría de las implementaciones, la interfaz de PowerShell ofrece opciones más avanzadas. Para obtener información sobre los cmdlets de PowerShell de FAS, consulte [Cmdlets de PowerShell](#).

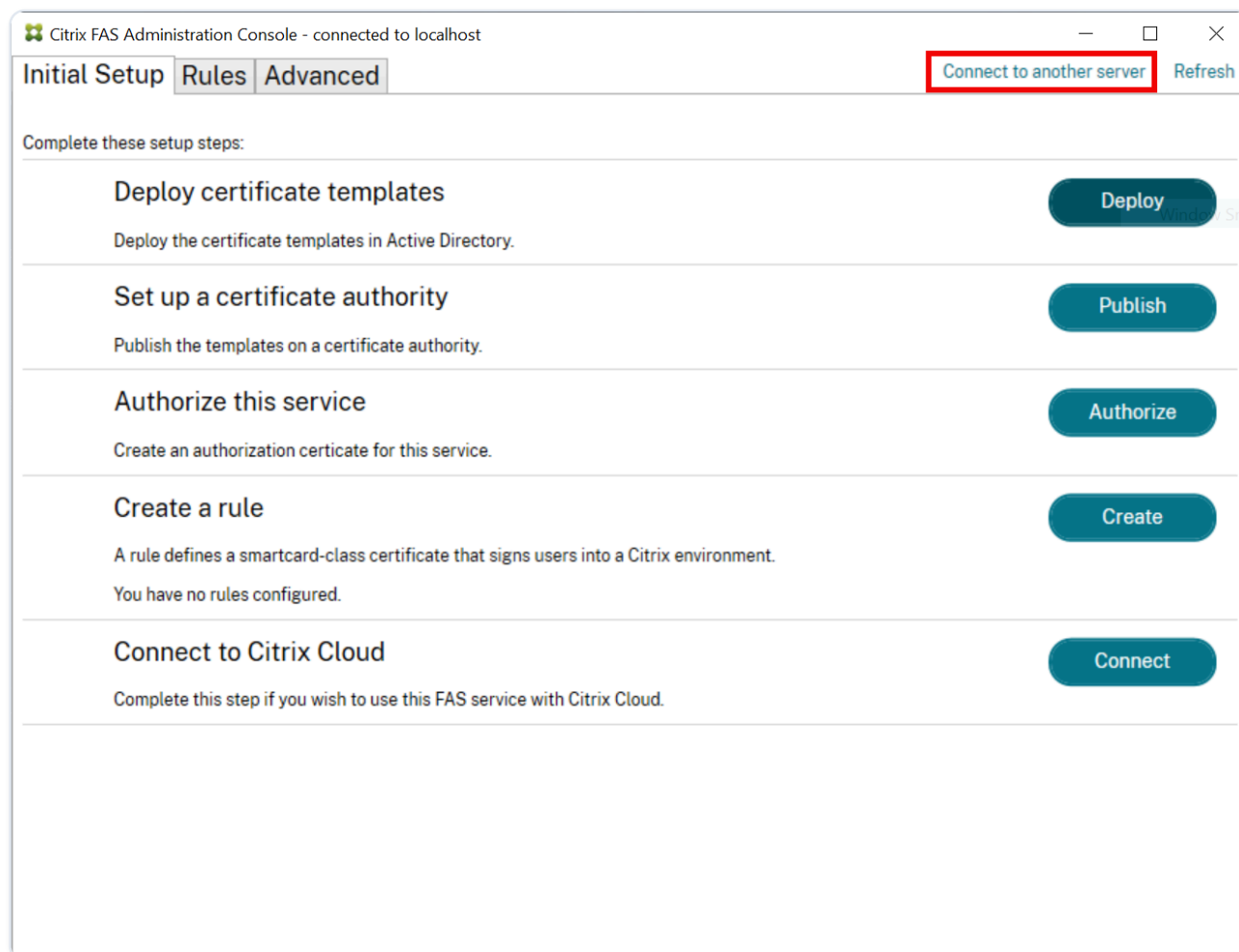
La consola de administración de FAS se instala como parte de FAS. Se coloca un icono (Citrix Federated Authentication Service) en el menú Inicio.

La primera vez que utiliza la consola de administración, esta le guía a través de los siguientes procesos para:

- Implementar plantillas de certificados.
- Configurar la entidad de certificación.
- Autorizar a FAS para que utilice la entidad de certificación.

También puede utilizar las herramientas de configuración del sistema operativo para completar algunos de los pasos manualmente.

La consola de administración de FAS se conecta al servicio FAS local de forma predeterminada. Si es necesario, puede conectarse a un servicio remoto mediante **Conectarse a otro servidor** en la parte superior derecha de la consola.

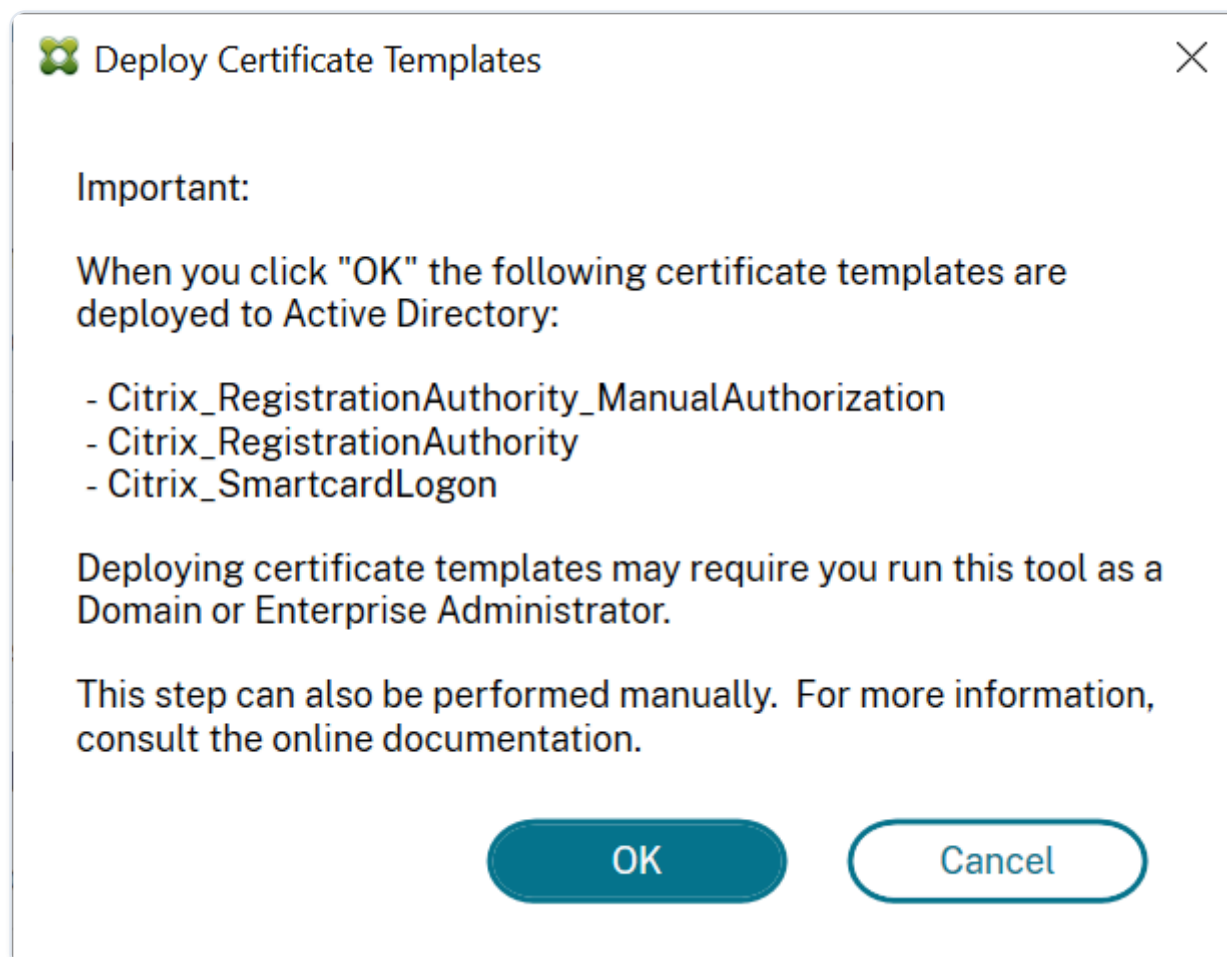


## Implementar plantillas de certificados

Para evitar problemas de interoperabilidad con otro software, FAS proporciona tres plantillas de certificados de Citrix para su propio uso.

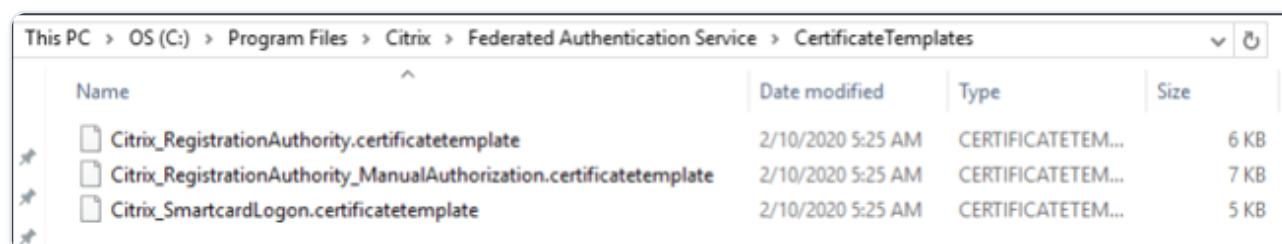
- Citrix\_RegistrationAuthority\_ManualAuthorization
- Citrix\_RegistrationAuthority
- Citrix\_SmartcardLogon

Estas plantillas deben registrarse con Active Directory. Haga clic en el botón **Implementar** y luego haga clic en **Aceptar**.



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

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



Si no tiene permiso para instalar estos archivos de plantilla, déselos a su administrador de Active Directory.

Para instalar manualmente las plantillas, puede ejecutar los siguientes comandos de PowerShell desde la carpeta que contiene las plantillas:

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

$CertEnrol = New-Object -ComObject
```

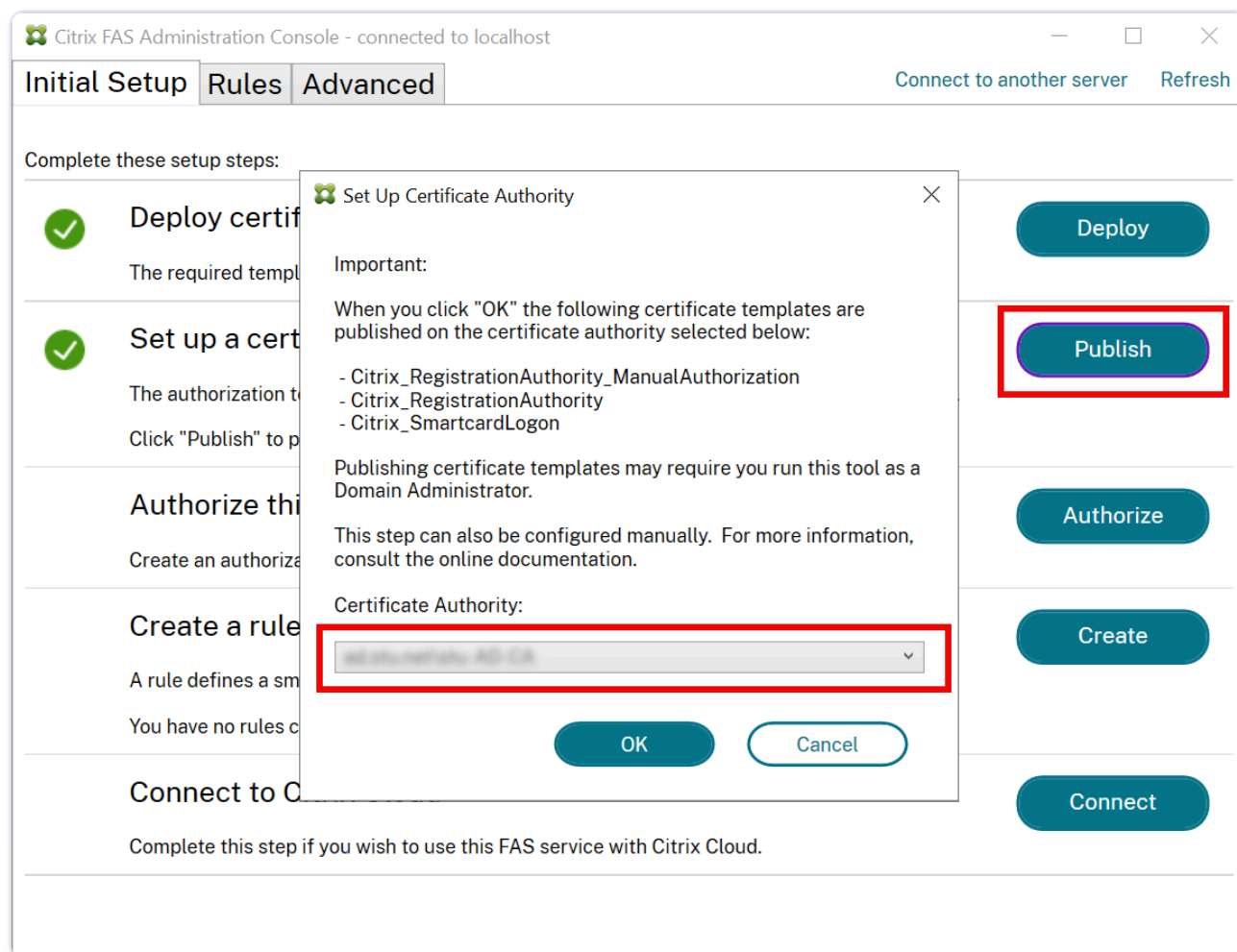
```
X509Enrollment.CX509EnrollmentPolicyWebService  
  
$CertEnrol.InitializeImport($template)  
  
$comtemplate = $CertEnrol.GetTemplates().ItemByIndex(0)  
  
$writabletemplate = New-Object -ComObject  
X509Enrollment.CX509CertificateTemplateADWritable  
  
$writabletemplate.Initialize($comtemplate)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

## Configurar Servicios de certificados de Active Directory

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

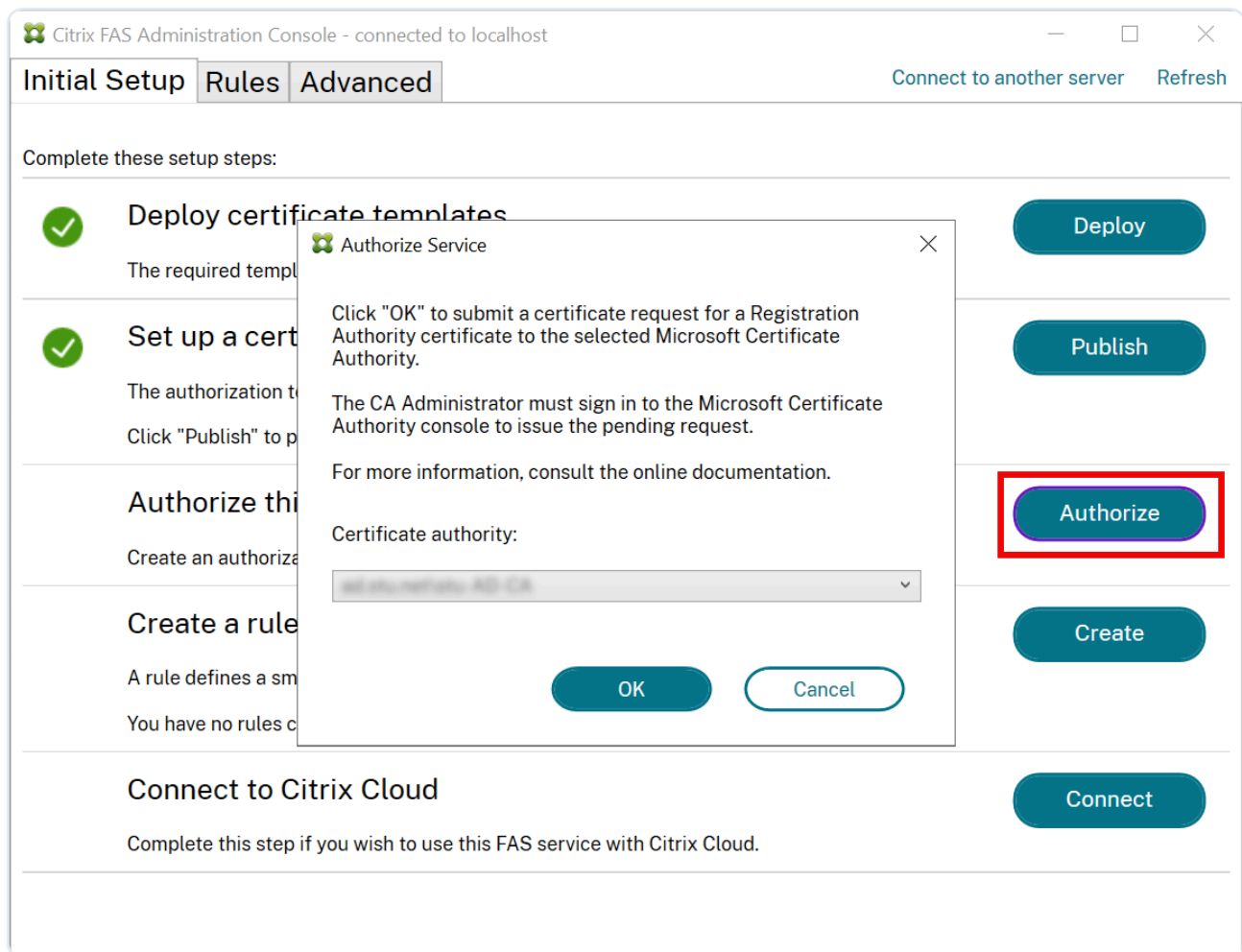
Un usuario que tenga permisos para administrar la entidad de certificación debe publicar las plantillas en al menos un servidor. Utilice **Configurar entidad de certificación** para publicarlas.

(Las plantillas de certificados también se pueden publicar mediante la consola de la entidad de certificación de Microsoft).



## Autorizar Servicio de autenticación federada

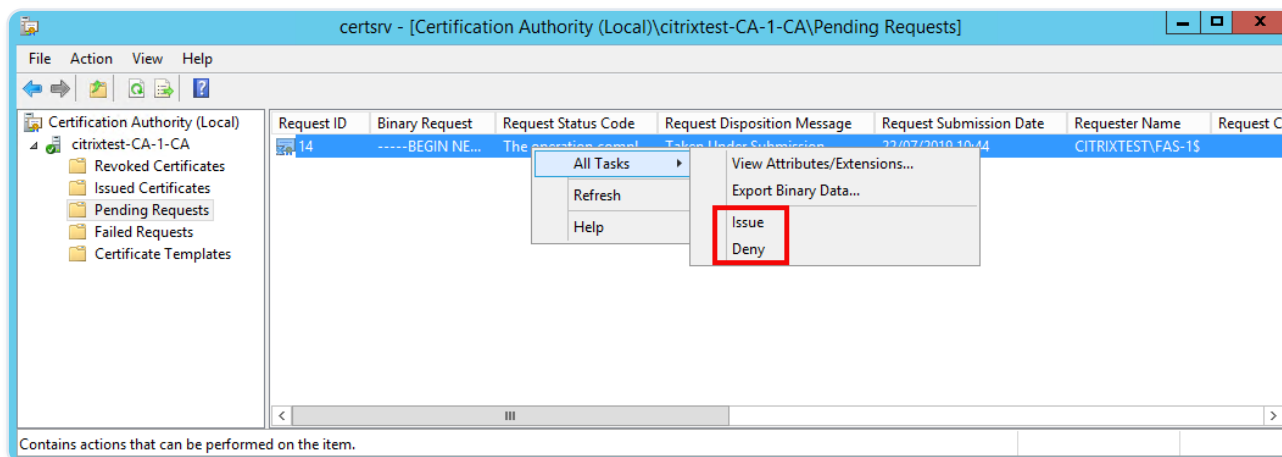
Este paso inicia la autorización de FAS. La consola de administración utiliza la plantilla Citrix\_RegistrationAuthority\_ManualAuthorization para generar una solicitud de certificado y luego la envía a una de las entidades de certificación que publican esa plantilla.



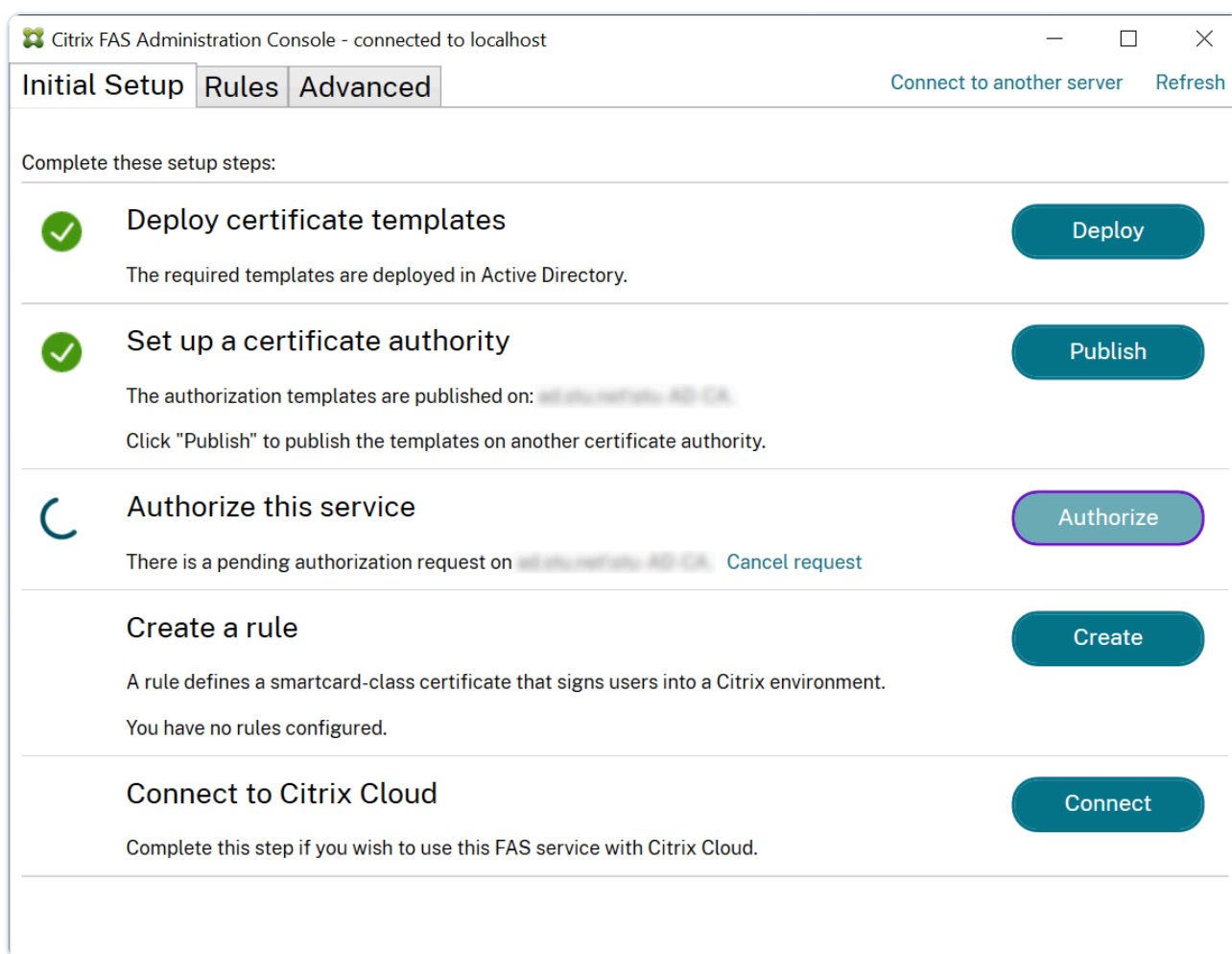
Una vez enviada la solicitud, aparece en la lista de **Solicitudes pendientes** de la consola de la entidad de certificación de Microsoft como una solicitud pendiente de la cuenta de máquina de FAS. El administrador de la entidad de certificación debe emitir o denegar la solicitud antes de que pueda continuar la configuración de FAS.

La consola de administración de FAS muestra un "indicador de progreso" ocupado hasta que el administrador elija **Emitir** o **Denegar**.

En la consola de la entidad de certificación de Microsoft, haga clic con el botón secundario en **Todas las tareas** y, a continuación, seleccione **Emitir** o **Denegar** para la solicitud de certificado. Si elige **Emitir**, la consola de administración de FAS muestra el certificado de autorización. Si elige **Denegar**, la consola muestra un mensaje de error.



La consola de administración de FAS detecta automáticamente cuándo finaliza este proceso. Esto puede tardar un par de minutos.



## Configurar reglas

FAS utiliza las reglas para autorizar la emisión de certificados para el inicio de sesión de VDA y el uso en la sesión, según lo indique StoreFront.

Cada regla especifica lo siguiente:

- Servidores StoreFront de confianza para solicitar los certificados.
- Conjunto de usuarios para los que se solicitan los certificados.
- Conjunto de máquinas VDA autorizadas para usar los certificados.

Citrix recomienda crear una regla con el nombre "default", ya que StoreFront solicita una regla con el mismo nombre al ponerse en contacto con FAS.

Puede crear más reglas personalizadas para hacer referencia a diferentes plantillas de certificado y entidades de certificación, y configurarlas para que tengan diferentes propiedades y permisos. Estas reglas se pueden configurar para su uso por diferentes servidores StoreFront o por Workspace. Configure los servidores StoreFront para solicitar la regla personalizada por nombre mediante las opciones de Configuración de directivas de grupo.

Haga clic en **Crear** (o en **Crear regla** en la ficha "Reglas") para iniciar el asistente de creación de reglas, que recopila la información necesaria para crear la regla. La ficha "Reglas" muestra un resumen de cada regla.

Citrix FAS Administration Console - connected to localhost

Initial Setup Rules Advanced [Connect to another server](#) [Refresh](#)

A rule defines a smartcard-class certificate that signs users into a Citrix environment.

[+ Create rule](#)

| Default | Summary                                           |
|---------|---------------------------------------------------|
|         | <b>Rule name:</b> Default                         |
|         | <b>Status:</b> OK                                 |
|         | <b>Template:</b> Citrix_SmartcardLogon            |
|         | <b>Certificate authorities:</b> ad-00000000-AD-CA |
|         | <b>Certificate available in-session:</b> No       |
|         | <b>Access control:</b> Configured                 |
|         | <b>Restrictions:</b> Not configured               |
|         | <b>Cloud rule:</b> No                             |

El asistente recopila la siguiente información:

**Plantilla:** La plantilla de certificado que se utiliza para emitir certificados de usuario. Debe ser la plantilla Citrix\_SmartcardLogon o una copia modificada de ella (consulte [Plantillas de certificado](#)).

**Entidad de certificación:** La entidad de certificación que emite certificados de usuario y publica la plantilla. FAS admite la adición de varias entidades de certificación para la conmutación por error y el equilibrio de carga. Asegúrese de que el estado muestre "Plantilla disponible" para la entidad de certificación que elija. Consulte [Administración de entidades de certificación](#).

**Uso en la sesión:** La opción **Permitir uso en la sesión** controla si se puede usar un certificado después de iniciar sesión en el VDA.

- **Permitir uso en la sesión** no seleccionada (predeterminado, *recomendado*)—el certificado se utiliza solo para el inicio de sesión o la reconexión, y los usuarios no tienen acceso al certificado después de autenticarse.
- **Permitir uso en la sesión** seleccionada—los usuarios tienen acceso al certificado después de autenticarse. La mayoría de los clientes no deben seleccionar esta opción. Se puede acceder a los recursos a los que se accede desde la sesión de VDA, como sitios web de intranet o recursos compartidos de archivos, mediante el inicio de sesión único de Kerberos, por lo que no se requiere un certificado en la sesión.

Si selecciona **Permitir uso en la sesión**, la directiva de grupo [Comportamiento en la sesión](#) también debe estar habilitada y aplicada al VDA. Los certificados se colocan entonces en el almacén de certificados personal del usuario después de iniciar sesión para su uso en aplicaciones. Por ejemplo, si necesita autenticación TLS en servidores web dentro de la sesión de VDA, Internet Explorer puede usar el certificado.

**Control de acceso:** La lista de máquinas de servidor StoreFront de confianza que están autorizadas a solicitar certificados para el inicio de sesión o la reconexión de usuarios. Para todos estos permisos, puede agregar objetos o grupos de AD individuales.

#### IMPORTANTE:

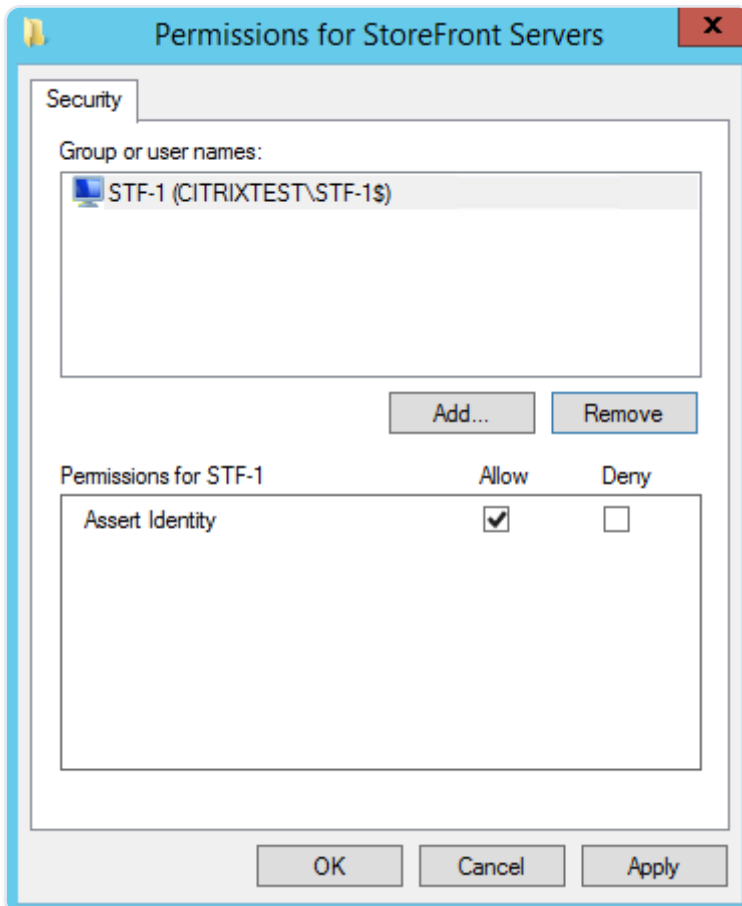
La configuración de **Control de acceso** es crítica para la seguridad y debe administrarse con cuidado.

#### Nota:

Si utiliza el servidor FAS solo con Citrix Cloud, no es necesario configurar el Control de acceso. Cuando Citrix Cloud utiliza una regla, se ignoran los permisos de acceso de StoreFront. Puede utilizar la misma regla con Citrix Cloud y con una implementación de StoreFront local. Los

permisos de acceso de StoreFront se siguen aplicando cuando la regla es utilizada por un StoreFront local.

El permiso predeterminado ("Afirmar identidad" permitido) deniega todo. Por lo tanto, debe permitir explícitamente sus servidores StoreFront.

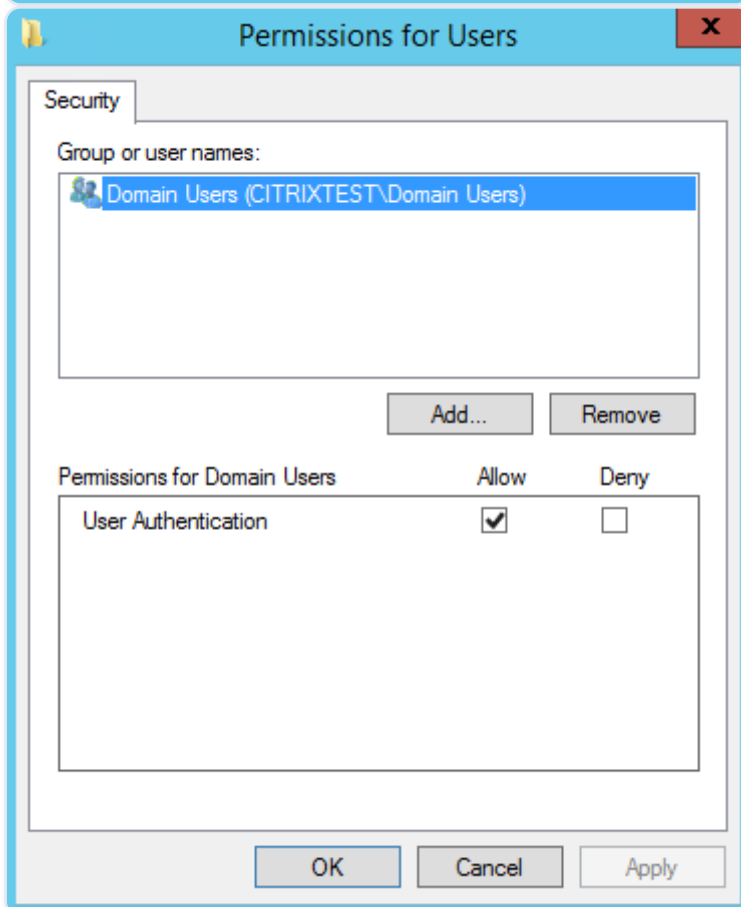
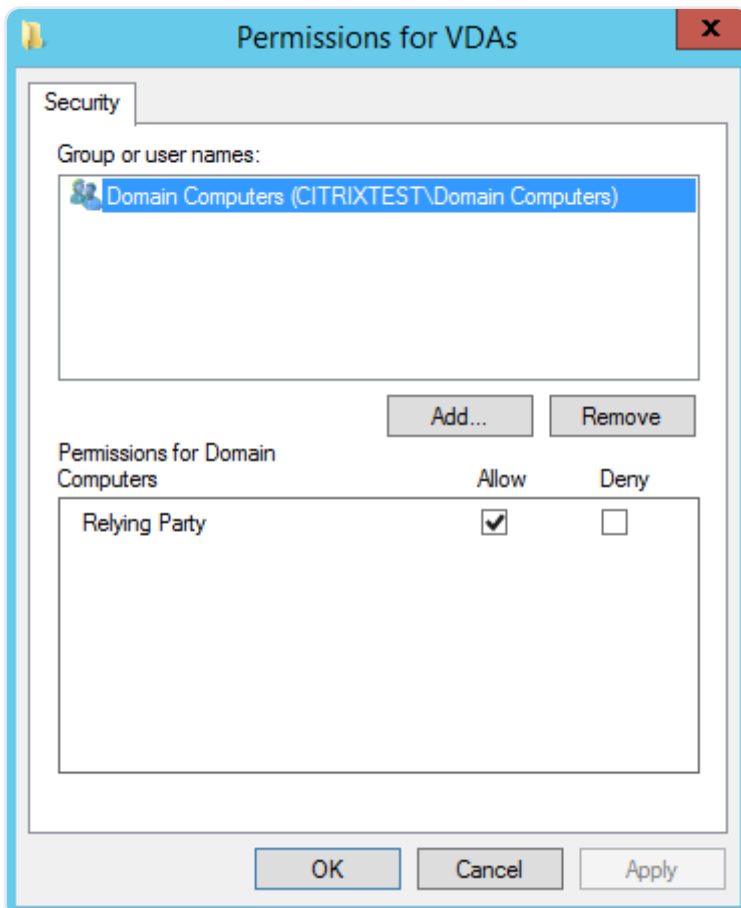


**Restricciones:** La lista de máquinas VDA que pueden iniciar sesión de usuarios mediante FAS y la lista de usuarios a los que se les pueden emitir certificados a través de FAS.

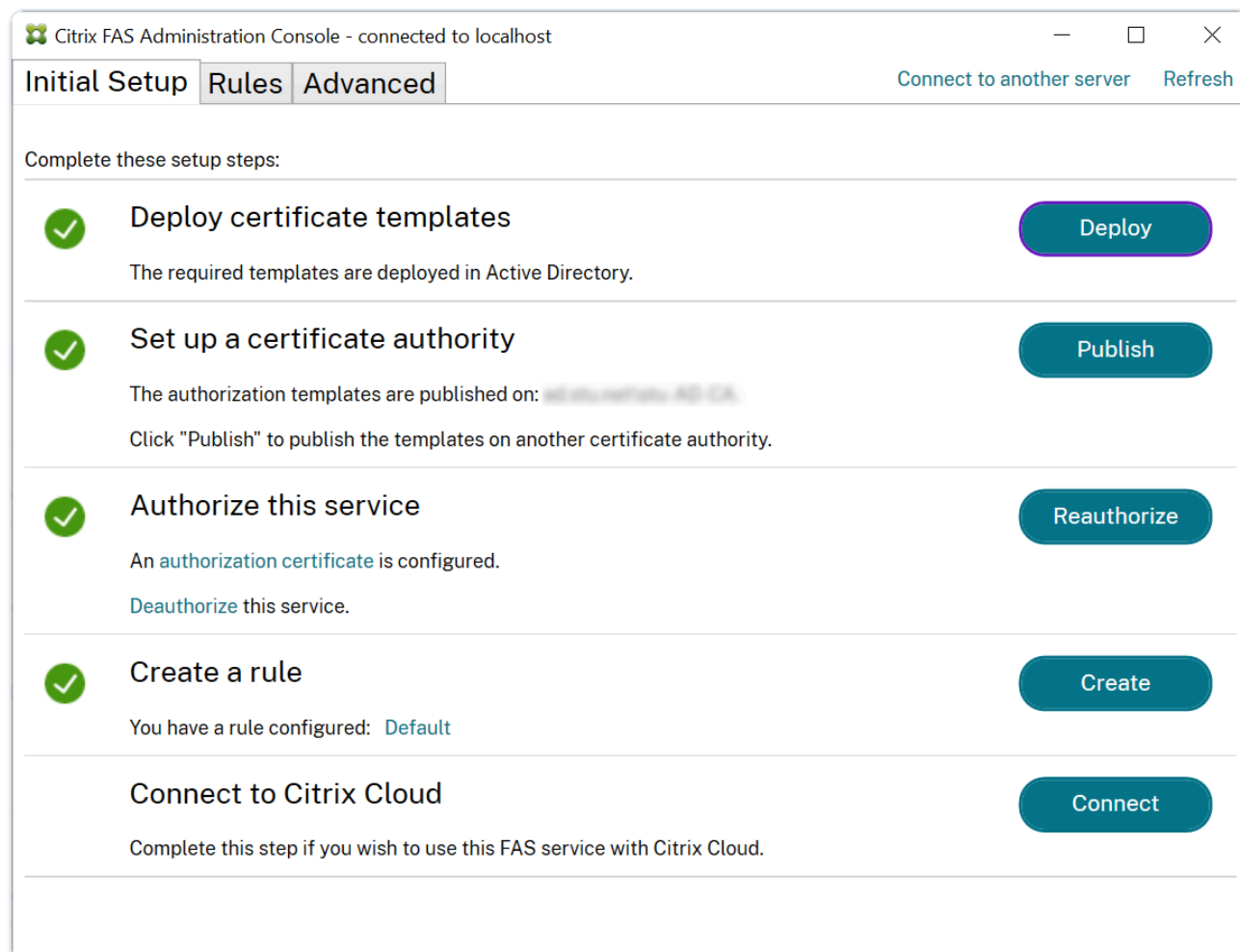
- **Administrar permisos de VDA** permite especificar qué VDA pueden usar FAS para iniciar sesión del usuario. La lista de VDA predeterminada es Domain Computers.
- **Administrar permisos de usuario** permite especificar qué usuarios pueden usar FAS para iniciar sesión en un VDA. La lista de usuarios predeterminada es Domain Users.

**NOTA:**

Si el dominio del servidor FAS difiere del de los VDA y los usuarios, las restricciones predeterminadas deben modificarse.



**Regla de la nube:** Indica si la regla se aplica cuando se reciben aserciones de identidad de Citrix Workspace. Al conectarse a Citrix Cloud, se elige qué regla usar para Citrix Cloud. También puede cambiar la regla después de conectarse a Citrix Cloud desde un enlace en la sección **Conectarse a Citrix Cloud**.



Citrix FAS Administration Console - connected to localhost

Initial Setup Rules Advanced [Connect to another server](#) [Refresh](#)

Complete these setup steps:

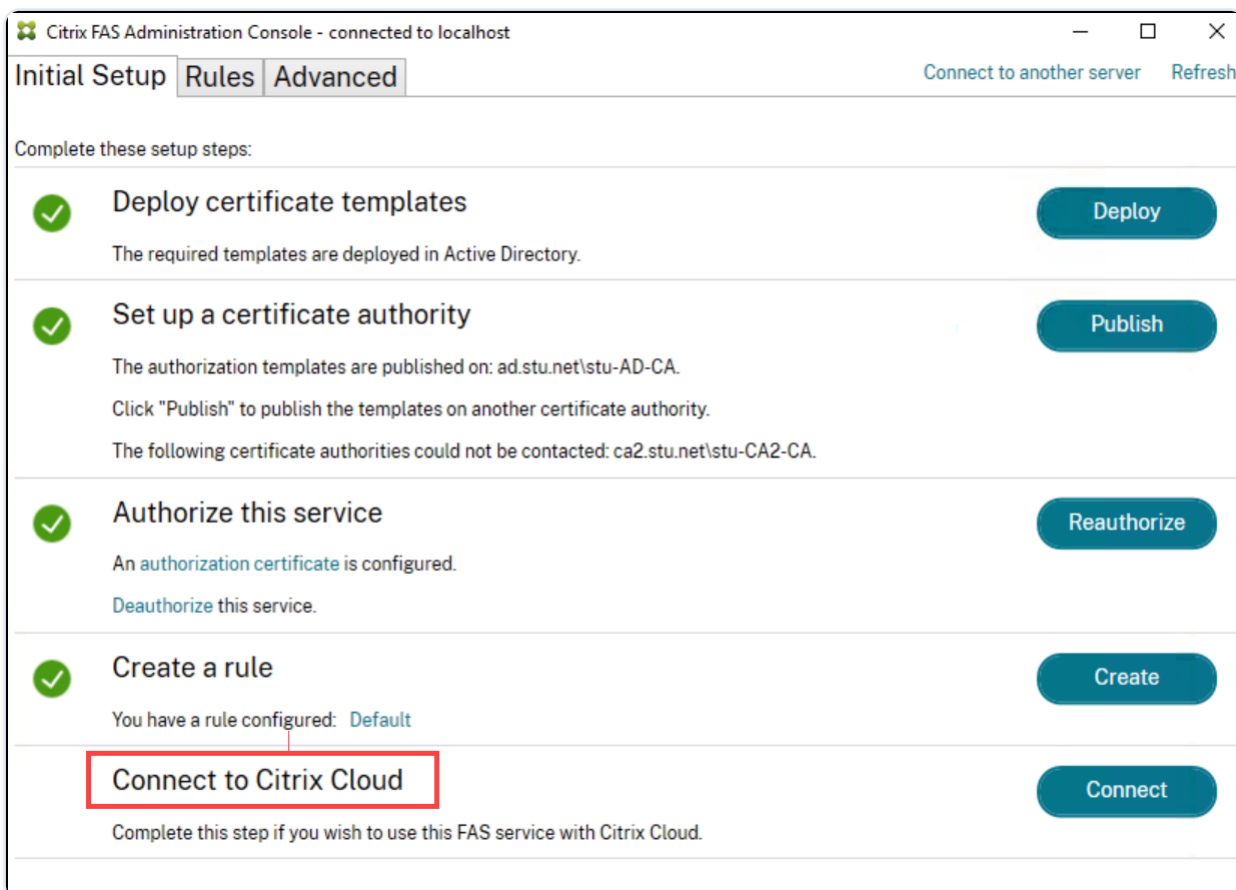
- ☒ **Deploy certificate templates** [Deploy](#)  
The required templates are deployed in Active Directory.
- ☒ **Set up a certificate authority** [Publish](#)  
The authorization templates are published on: [adfs.adfs.net:80 CA](#).  
Click "Publish" to publish the templates on another certificate authority.
- ☒ **Authorize this service** [Reauthorize](#)  
An [authorization certificate](#) is configured.  
[Deauthorize](#) this service.
- ☒ **Create a rule** [Create](#)  
You have a rule configured: [Default](#)

**Connect to Citrix Cloud** [Connect](#)  
Complete this step if you wish to use this FAS service with Citrix Cloud.

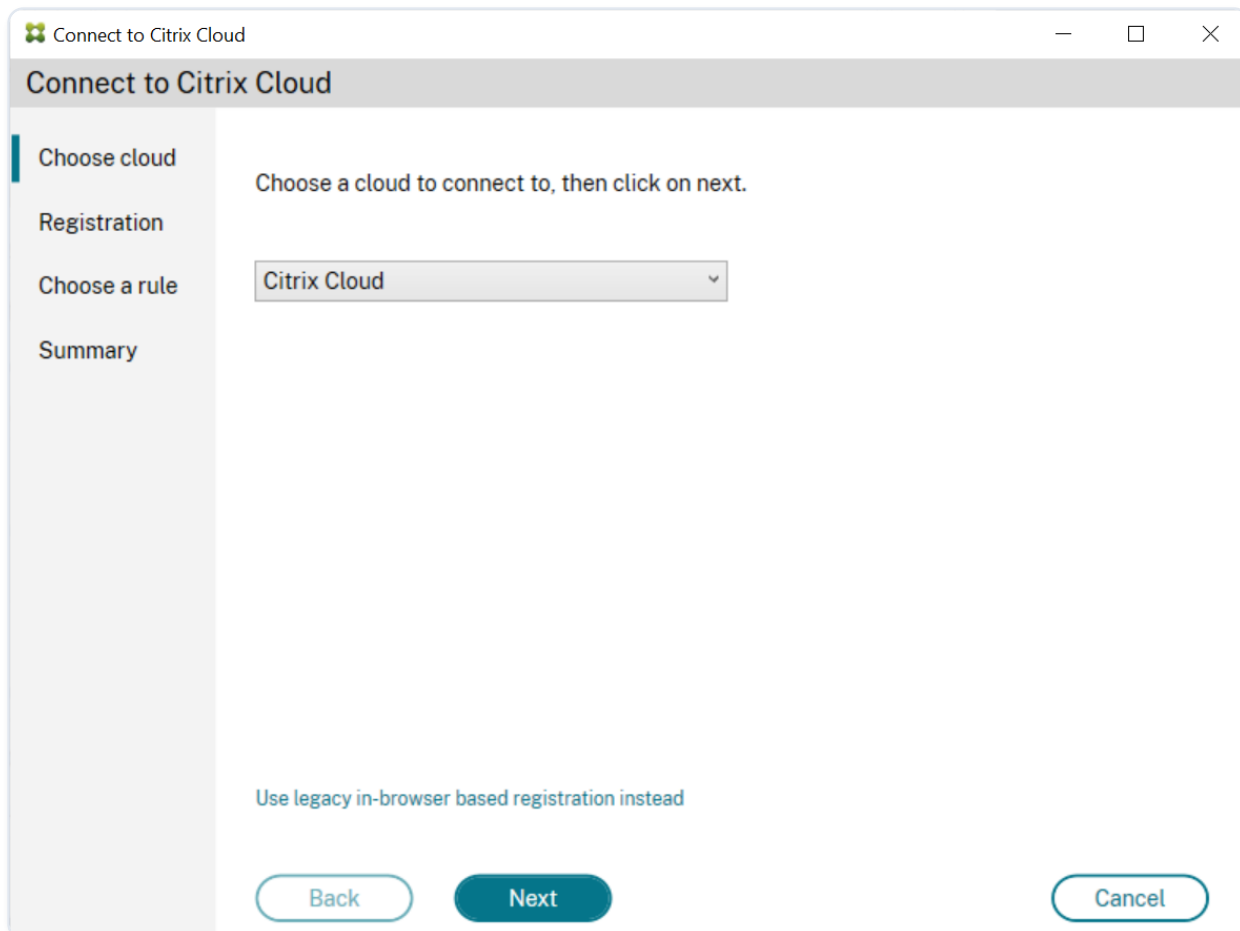
## Conectarse a Citrix Cloud

Puede conectar el servidor FAS a Citrix Cloud con Citrix Workspace. Consulte este (</es-es/citrix-workspace/workspace-federated-authentication.html>).

1. En la ficha Configuración inicial, en **Conectarse a Citrix Cloud**, haga clic en **Conectar**.



2. Seleccione la nube a la que quiere conectarse y haga clic en **Siguiente**.



**NOTA**

Solo **Citrix Cloud** está disponible en la vista previa.

3. La ventana muestra un código de registro único, que debe aprobarse en Citrix Cloud. Para obtener más información, consulte [Registrar productos locales con Citrix Cloud](#).

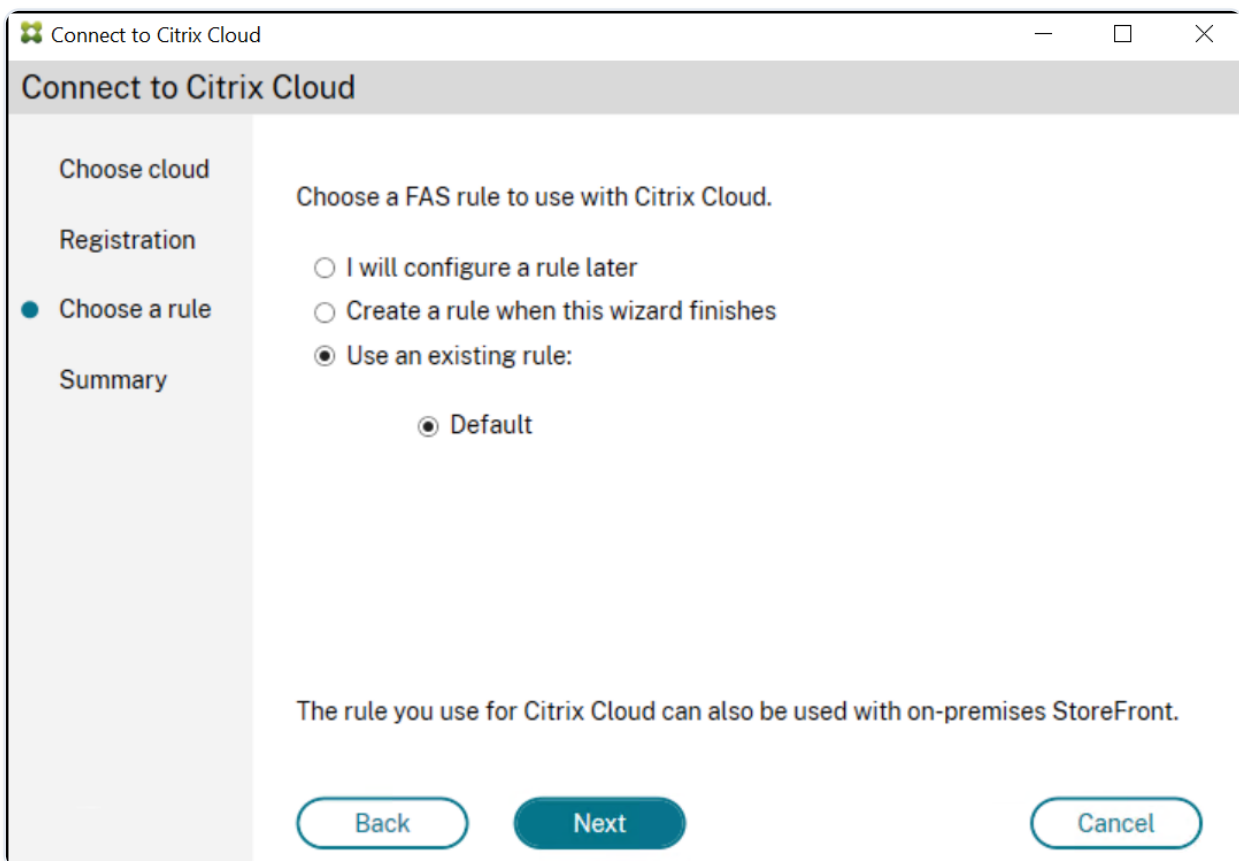
The screenshot shows a window titled "Connect to Citrix Cloud" with a sidebar on the left containing the following menu items: "Choose cloud", "Registration" (highlighted), "Choose a rule", and "Summary". The main content area contains the following text: "Copy and open the given confirmation URL in a browser with internet access. Then register with the given confirmation code. The resource locations will be populated shortly after confirmation. Select a resource location to connect this Fas server, then click on next." Below this text, there are two fields: "Confirmation URL:" with a blurred URL and a "Copy" button, and "Confirmation Code:" with a blurred code "DDQESDAE" and a "Copy" button. At the bottom center, there is a red-bordered box containing a circular arrow icon and the text "Waiting for confirmation...". At the bottom of the window, there are three buttons: "Back", "Next" (highlighted), and "Cancel".

4. Una vez validado el código de registro, seleccione la **Ubicación de recursos** necesaria en la lista desplegable.

The screenshot shows a window titled "Connect to Citrix Cloud" with a sidebar on the left containing four options: "Choose cloud", "Registration" (which is selected and highlighted with a blue bar), "Choose a rule", and "Summary". The main area of the window contains the following elements:

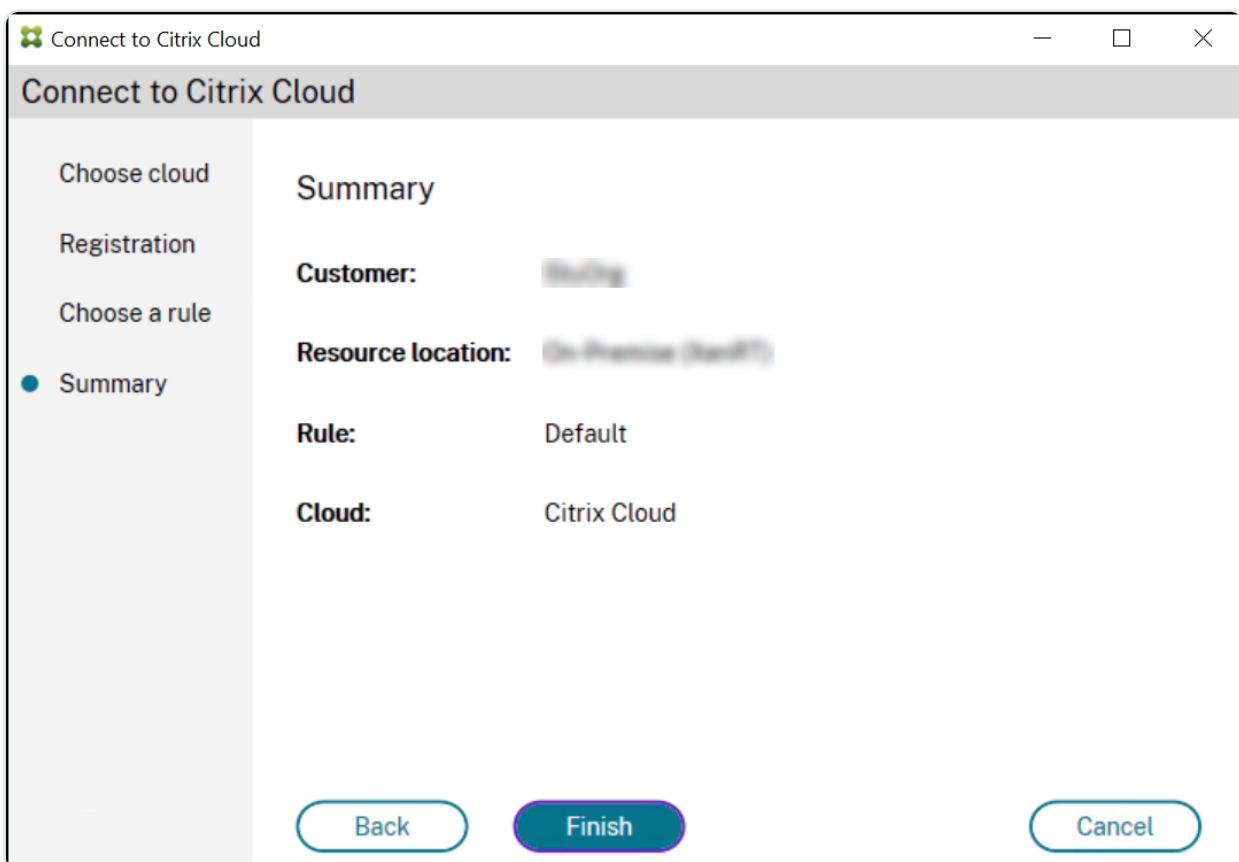
- Instructions:** "Copy and open the given confirmation URL in a browser with internet access. Then register with the given confirmation code. The resource locations will be populated shortly after confirmation. Select a resource location to connect this Fas server, then click on next."
- Confirmation URL:** A text field containing a blurred URL, followed by a blue "Copy" button.
- Confirmation Code:** A text field containing the code "78552997", followed by a blue "Copy" button.
- Resource location:** A dropdown menu with the text "My Resource Location" and a downward arrow.
- Navigation buttons:** At the bottom, there are three buttons: a blue "Back" button, a dark blue "Next" button, and a blue "Cancel" button.

5. Seleccione la cuenta de cliente, si corresponde, y seleccione la ubicación de recursos donde desea conectar el servidor FAS. Haga clic en **Continuar** y, a continuación, cierre la ventana de confirmación.
6. En la sección **Elegir una regla**, utilice una regla existente o cree una. Haga clic en **Siguiente**.



The screenshot shows the 'Connect to Citrix Cloud' wizard window. The title bar says 'Connect to Citrix Cloud'. The left sidebar has four steps: 'Choose cloud', 'Registration', 'Choose a rule' (which is selected with a blue dot), and 'Summary'. The main area is titled 'Choose a FAS rule to use with Citrix Cloud.' and contains three radio button options: 'I will configure a rule later', 'Create a rule when this wizard finishes', and 'Use an existing rule:'. Under 'Use an existing rule:', there is a sub-option 'Default' which is selected. At the bottom, there is a note: 'The rule you use for Citrix Cloud can also be used with on-premises StoreFront.' and three buttons: 'Back', 'Next' (highlighted in blue), and 'Cancel'.

7. En la sección **Resumen**, haga clic en **Finalizar** para completar la conexión a Citrix Cloud.



The screenshot shows the 'Connect to Citrix Cloud' wizard window at the 'Summary' step. The left sidebar now has 'Summary' selected with a blue dot. The main area is titled 'Summary' and displays the following configuration details: 'Customer: Citrix', 'Resource location: On-Premise (Self?)', 'Rule: Default', and 'Cloud: Citrix Cloud'. At the bottom, there are three buttons: 'Back', 'Finish' (highlighted in blue), and 'Cancel'.

Citrix Cloud registra el servidor FAS y lo muestra en la página Ubicaciones de recursos de su cuenta de Citrix Cloud.

#### Nota

Un servidor FAS local puede emitir certificados de usuario para permitir el acceso a Citrix Cloud y a Citrix Virtual Apps and Desktops al mismo tiempo.

## desconectar de Citrix Cloud

Después de eliminar el servidor FAS de la ubicación de recursos de Citrix Cloud, como se describe en este [artículo de Citrix Workspace](#), en **Conectar a Citrix Cloud** seleccione **Deshabilitar**.

# Configuración avanzada

---

Los artículos de esta sección ofrecen orientación avanzada sobre la configuración y la administración de Federated Authentication Service (FAS).

## Información relacionada

- La referencia principal para la instalación y la configuración inicial de FAS es el artículo [Instalar y configurar](#).
- El artículo [Arquitecturas de implementación](#) ofrece resúmenes de las principales arquitecturas de FAS, además de enlaces a otros artículos sobre las arquitecturas más complejas.

## Habilitar el Servicio de autenticación federada para un cliente de inquilino

Este artículo describe los pasos para habilitar el Servicio de autenticación federada (FAS) en entornos de proveedor de servicios gestionados (MSP) multiinquilino. Para obtener más información, consulte [Arquitectura de referencia: Citrix Service Provider DaaS](#).

## Requisitos previos

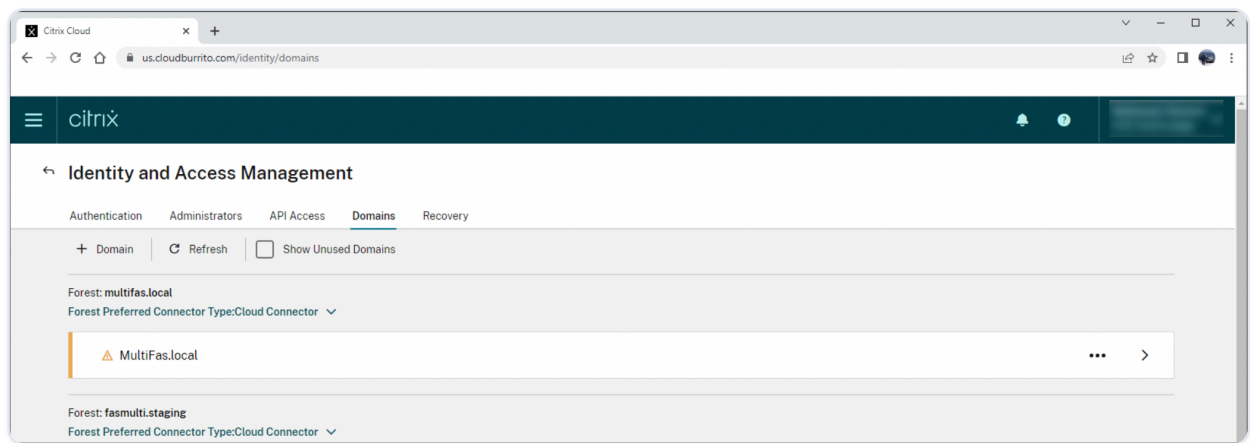
- Tiene acceso de administrador a Dominios y Ubicación de recursos en Citrix Cloud. Para obtener más información, consulte [Modificar permisos de administrador](#).
- Ha configurado una relación de inquilino-MSP. Para obtener más información, consulte [Citrix DaaS para proveedores de servicios de Citrix](#).

## Configurar el cliente MSP

1. Utilice un Cloud Connector para que los dominios de Active Directory estén disponibles para Citrix Cloud.

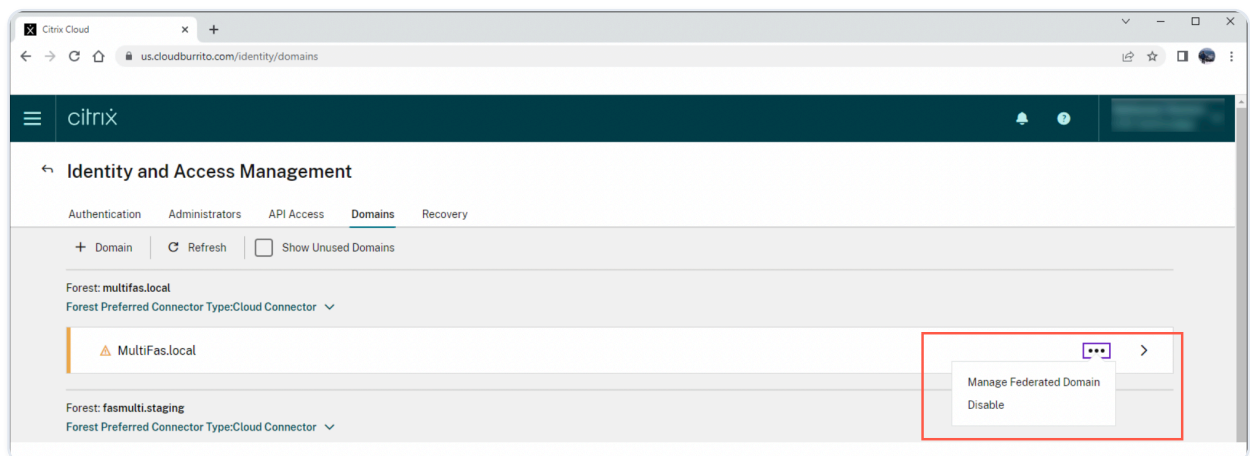
Conecte la infraestructura local a Citrix Cloud [instalando Cloud Connectors](#).

verificar que los dominios asociados con el controlador de dominio local estén disponibles en **Identity and Access Management > Domains**.



## 2. Federar el dominio al inquilino.

Seleccione el dominio y haga clic en el menú desplegable (...) y haga clic en **Manage Federated Domains**.



Busque el inquilino y haga clic en +. Luego haga clic en **Apply**.

Add or remove customers to create a federated domain

1 available customers [Add all](#)

0 federated customers [Remove all](#)

Search... Q

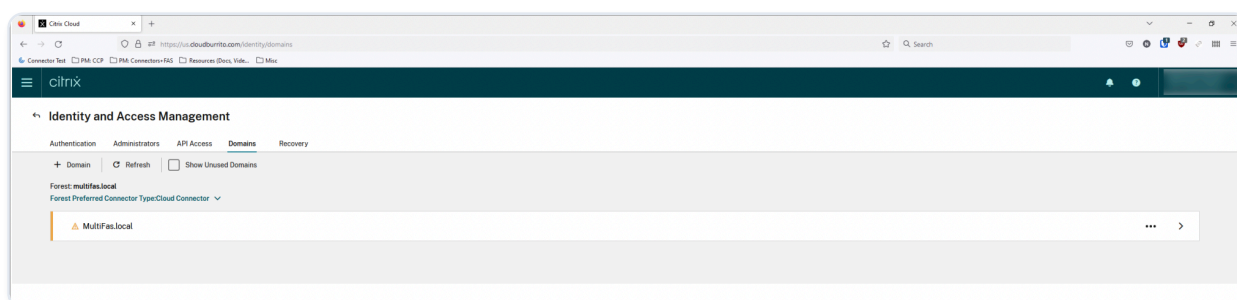
Search... Q

FAS Tenant1 with service profile. +

Cancel Apply

3. verificar que los dominios asociados estén presentes en el inquilino.

Este paso es opcional. Inicie sesión en la consola para los clientes inquilinos y verificar que los dominios aparecen en **Identity and Access Management > Domains**.



Vuelva al cliente MSP.

4. Instale y registre un servidor FAS con Citrix Cloud.

Instale FAS en el bosque de Active Directory (AD) donde se encuentran los recursos de Citrix Virtual Apps and Desktops del inquilino. Conecte FAS a la ubicación de recursos en la nube asociada a ese bosque de AD. Para instalar un servidor FAS, consulte [Instalar y configurar](#).

5. Configurar el cliente inquilino

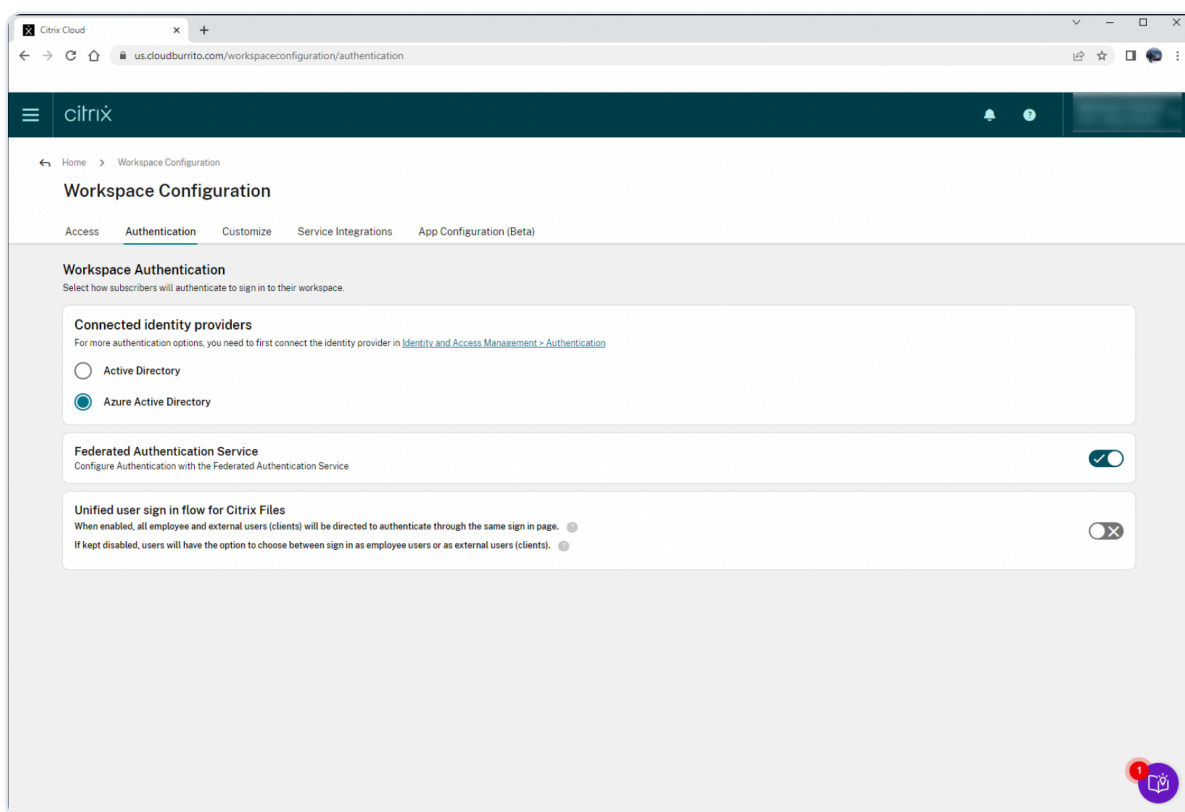
## Habilitar FAS para el cliente inquilino

- Configure su proveedor de identidades (IdP)

Cambie al cliente inquilino. Vaya a **Identity and Access Management > Authentication**. Conéctese a su IdP y asegúrese de que AD esté sincronizado con el IdP.

- Habilitar FAS para un inquilino

Vaya a **Workspace Configuration > Authentication**. Seleccione la autenticación que ha configurado y habilite FAS.



## Problema conocido

Existe un problema conocido al eliminar un dominio MSP antes de eliminar los dominios federados para los inquilinos. Aún puede habilitar FAS para los inquilinos, pero FAS falla ya que el dominio ya no existe para MSP.

## Inicio de sesión único de Azure Active Directory

Citrix Federated Authentication Service (FAS) proporciona inicio de sesión único (SSO) a los Virtual Delivery Agents (VDA) unidos a un dominio. FAS logra el SSO al proporcionar al VDA un certificado de usuario, que el VDA utiliza para autenticar al usuario en Active Directory (AD). Una

vez que inicia sesión en la sesión VDA, puede acceder a los recursos de AD sin volver a autenticarse.

Es común implementar Azure Active Directory (AAD) con sincronización entre su AD y AAD, lo que crea identidades híbridas tanto para usuarios como para equipos. Este artículo describe la configuración adicional necesaria para lograr el SSO en AAD desde su sesión VDA al usar FAS, lo que permite al usuario acceder a aplicaciones protegidas por AAD sin volver a autenticarse.

**NOTA:**

- No necesita ninguna configuración especial para que FAS use SSO para AAD.
- No necesita los certificados de FAS en la sesión.
- Puede usar cualquier versión de FAS.
- Puede usar cualquier versión del VDA que sea compatible con FAS.

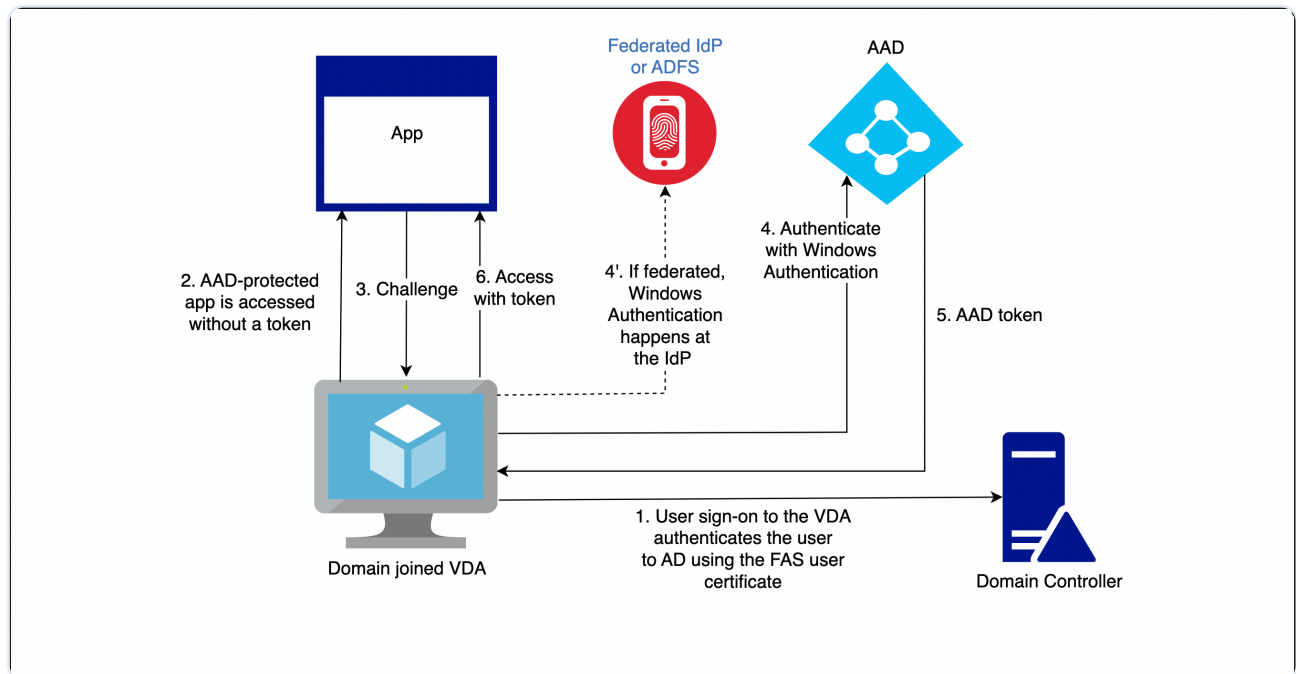
Las técnicas para el SSO de AAD se resumen en la siguiente tabla:

| TIPO DE AUTENTICACIÓN DE AAD                           | EL VDA ESTÁ UNIDO A UN DOMINIO                | EL VDA ESTÁ UNIDO EN MODO HÍBRIDO                                                      |
|--------------------------------------------------------|-----------------------------------------------|----------------------------------------------------------------------------------------|
| Administrado                                           | Usar SSO de AAD sin interrupciones            | Usar autenticación basada en certificados de AAD                                       |
| Federado a Active Directory Federation Services (ADFS) | Habilitar la autenticación de Windows en ADFS | Asegúrese de que el punto de conexión WS-Trust <i>certificatemixed</i> esté habilitado |
| Federado a un proveedor de identidades de terceros     | Usar una solución de terceros                 | Usar una solución de terceros                                                          |

- Un dominio AAD administrado es aquel en el que la autenticación del usuario se realiza en AAD, a veces denominada autenticación AAD nativa.
- Un dominio AAD federado es aquel en el que AAD está configurado para redirigir la autenticación a otro lugar. Por ejemplo, a ADFS o a un proveedor de identidades de terceros.
- Un VDA unido híbrido está unido a AD y unido a AAD.

## VDA unidos a un dominio

Para los VDA unidos a un dominio, logre el SSO en AAD mediante la autenticación de Windows (tradicionalmente denominada autenticación integrada de Windows o Kerberos). La autenticación en AAD se produce cuando el usuario accede a una aplicación protegida por AAD desde la sesión del VDA. El siguiente diagrama muestra el proceso de autenticación a un alto nivel:



Los detalles exactos varían según si el dominio AAD está administrado o federado.

Para obtener información sobre la configuración del dominio AAD administrado, consulte [Inicio de sesión único sin problemas](#).

Para un dominio AAD federado a ADFS, habilite la autenticación de Windows en el servidor ADFS.

Para un dominio AAD federado a un proveedor de identidades de terceros, existe una solución similar. Póngase en contacto con su proveedor de identidades para obtener ayuda.

**NOTA:**

También puede usar las soluciones enumeradas para los VDA unidos a un dominio para los VDA unidos de forma híbrida. Pero no se genera un token de actualización principal (PRT) de AAD al usar FAS.

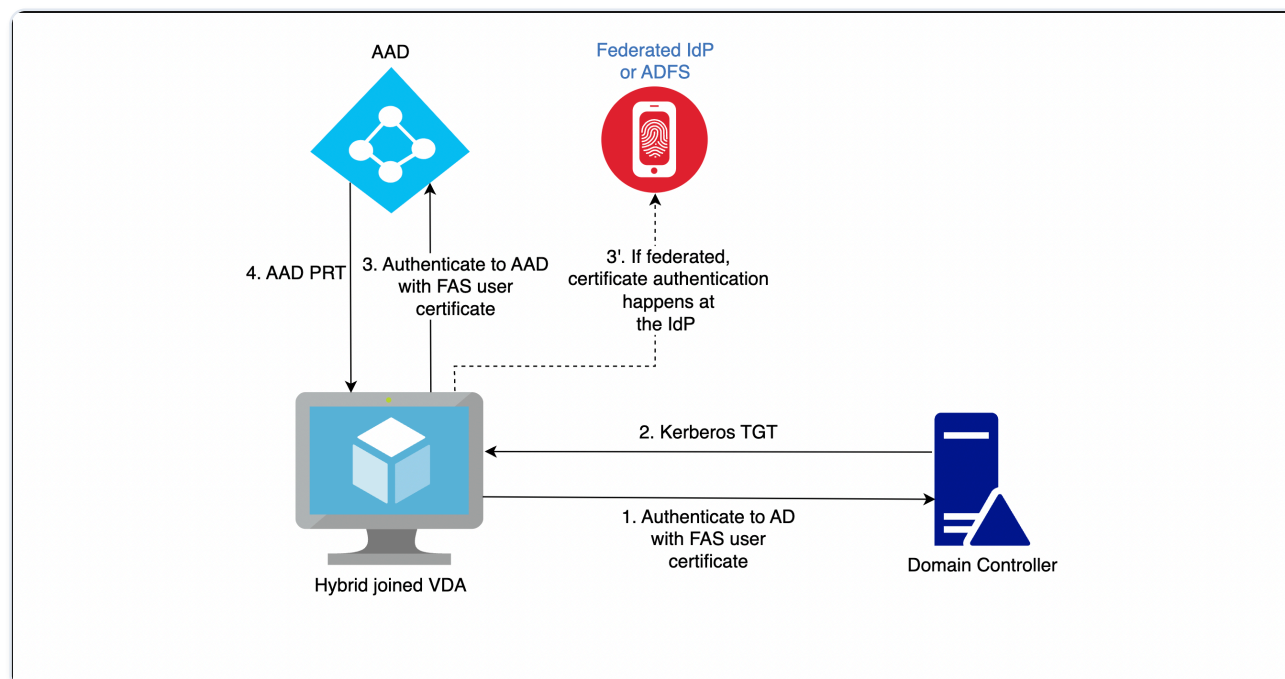
## VDA unidos de forma híbrida

Los VDA unidos de forma híbrida se unen a AD y AAD al mismo tiempo. Cuando el usuario inicia sesión en el VDA, se crean los siguientes artefactos:

- Un Ticket Granting Ticket (TGT) de Kerberos, para autenticarse en los recursos de AD
- Un token de actualización principal (PRT), para autenticarse en los recursos de AAD

El PRT contiene información tanto sobre el usuario como sobre el equipo. Esta información se utiliza en una política de acceso condicional de AAD si es necesario.

Dado que FAS autentica al usuario proporcionando un certificado al VDA, un PRT solo se puede crear si se implementa la autenticación basada en certificados para AAD. El siguiente diagrama muestra el proceso de autenticación a un alto nivel:



Los detalles exactos varían según si el dominio AAD está administrado o federado.

Para un dominio AAD administrado, configure AAD CBA. Para obtener más información, consulte [Información general sobre la autenticación basada en certificados de Azure AD](#). El VDA utiliza AAD CBA para autenticar al usuario en AAD con el certificado FAS del usuario.

#### NOTA:

La documentación de Microsoft describe el inicio de sesión con un certificado de tarjeta inteligente, pero la técnica subyacente se aplica al iniciar sesión con un certificado de usuario de FAS.

Para un dominio AAD federado a ADFS, el VDA utiliza el punto de conexión WS-Trust *certificatemixed* del servidor ADFS para autenticar al usuario en AAD con el certificado FAS del usuario. Este punto de conexión está habilitado de forma predeterminada.

Para un dominio AAD federado a un proveedor de identidades de terceros, puede existir una solución similar. El proveedor de identidades debe implementar un punto de conexión WS-Trust *certificatemixed*. Póngase en contacto con su proveedor de identidades para obtener ayuda.

## Configuración de la autoridad de certificación

Este artículo describe la configuración avanzada de Federated Authentication Service (FAS) para integrarse con servidores de autoridad de certificación (CA). La mayoría de estas configuraciones no son compatibles con la consola de administración de FAS. Las instrucciones utilizan las API de PowerShell proporcionadas por FAS. Debe tener un conocimiento básico de PowerShell antes de ejecutar cualquier instrucción de este artículo.

### Configurar varios servidores CA para su uso en FAS

Puede usar la consola de administración de FAS para configurar FAS con varias CA al crear o editar una regla:

The screenshot shows the 'Edit Rule' window for rule 'hello'. The left sidebar contains a navigation menu with the following items: Template, Certificate authority (selected), In-session use, Access control, Restrictions, and Summary. The main content area has a title bar 'Edit rule "hello"' and a description: 'Choose the certificate authority (CA) where user certificates will be generated. You can choose multiple certificate authorities for load balancing and failover.' There is a 'Refresh' button in the top right. Below the description is a table with two columns: 'Name' and 'Status'. The table contains two rows, both with a checked checkbox in the 'Name' column and 'Template available' in the 'Status' column. The first row's name is 'adfs.net/adfs-AD-CA' and the second is 'adfs.net/adfs-CA2-CA'. At the bottom of the table is a checkbox labeled 'Only show CAs publishing Citrix\_SmartcardLogon (recommended)' which is also checked. At the bottom right of the window are 'Apply' and 'Cancel' buttons.

| Name                                                     | Status             |
|----------------------------------------------------------|--------------------|
| <input checked="" type="checkbox"/> adfs.net/adfs-AD-CA  | Template available |
| <input checked="" type="checkbox"/> adfs.net/adfs-CA2-CA | Template available |

Todas las CA que seleccione deben estar publicando la plantilla de certificado Citrix\_SmartcardLogon (o cualquier otra plantilla que haya elegido en su regla).

Si una de las CA que desea utilizar no está publicando la plantilla deseada, realice el paso [Configurar una autoridad de certificación](#) para esa CA.

**NOTA:**

No es necesario realizar el paso [Autorizar este servicio](#) para cada CA, ya que el certificado de autorización configurado en este paso se puede utilizar en cualquiera de sus CA.

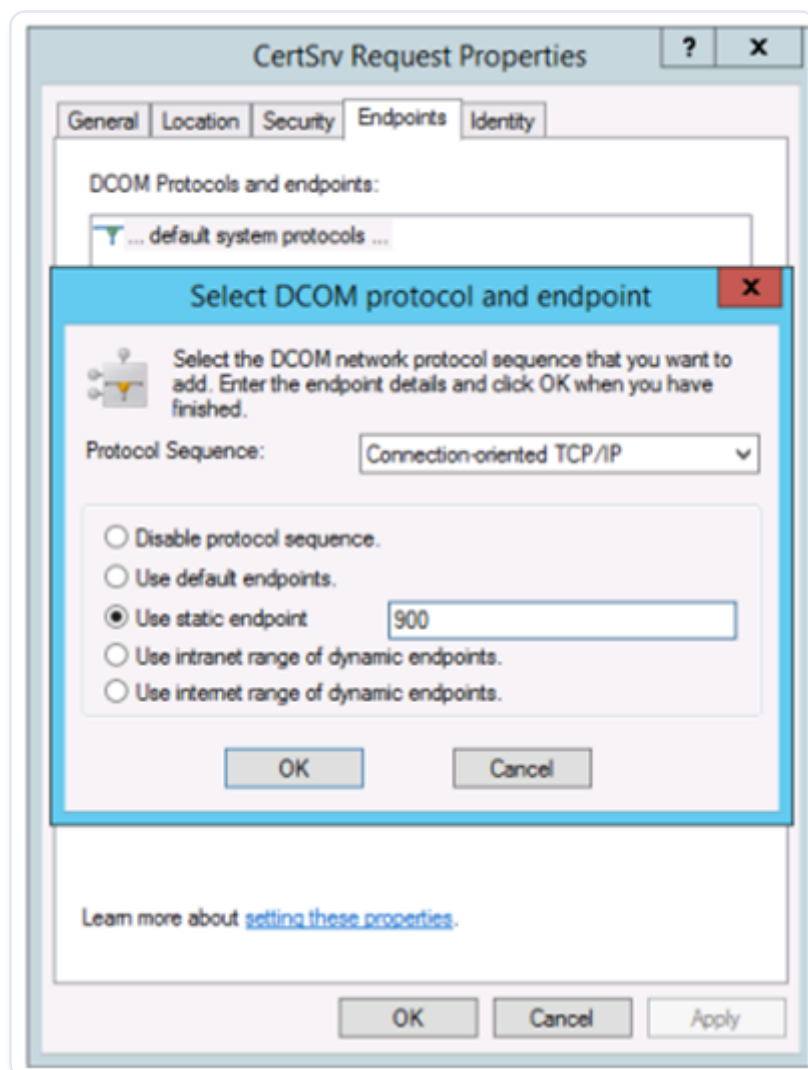
## Cambios de comportamiento esperados

Después de configurar el servidor FAS con varios servidores CA, la generación de certificados de usuario se distribuye entre todos los servidores CA configurados. Además, si uno de los servidores CA configurados falla, el servidor FAS cambiará a otro servidor CA disponible.

## Configurar la autoridad de certificación de Microsoft para el acceso TCP

De forma predeterminada, la CA de Microsoft utiliza DCOM para el acceso. Esto puede generar complejidades al implementar la seguridad del firewall, por lo que Microsoft tiene una disposición para cambiar a un puerto TCP estático. En la CA de Microsoft, use

**Inicio>Ejecutar>dcomcnfg.exe** para abrir el panel de configuración de DCOM, expanda *Equipos>Mi PC>Configuración de DCOM* para mostrar el nodo **Solicitud de CertSrv**, luego edite las propiedades de la aplicación DCOM Solicitud de CertSrv:



Cambie los "Puntos finales" para seleccionar un punto final estático y especifique un número de puerto TCP (900 en el gráfico anterior).

Reinicie la autoridad de certificación de Microsoft y envíe una solicitud de certificado. Si ejecuta `netstat -a -n -b`, debería ver que certsrv ahora está escuchando 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 FAS (ni ninguna otra máquina que utilice la autoridad de certificación), porque DCOM tiene una etapa de negociación que utiliza el puerto RPC. Cuando un cliente necesita usar DCOM, se conecta al servicio DCOM RPC en el servidor de certificados y solicita acceso a un servidor DCOM particular. Esto activa la apertura del puerto 900, y el servidor DCOM indica al servidor FAS cómo conectarse.

## Generar previamente certificados de usuario

El tiempo de inicio de sesión para los usuarios mejorará significativamente cuando los certificados de usuario se generen previamente dentro del servidor FAS. Las siguientes secciones describen cómo se puede hacer, ya sea para servidores FAS únicos o múltiples.

### Obtener una lista de usuarios de Active Directory

Puede mejorar la generación de certificados consultando AD y almacenando 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 -NoTypeInfoation -Encoding utf8
-delimiter "," $filename

} else {

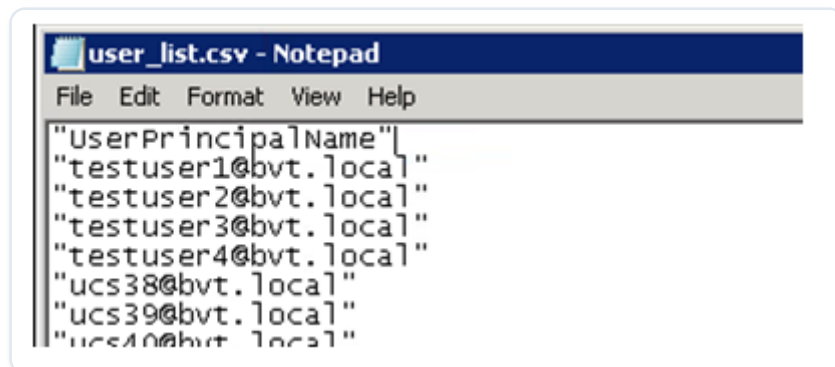
    Get-ADUser -Filter {(UserPrincipalName -ne "null") -and (Enabled -eq
"true")}} -Properties UserPrincipalName | Select UserPrincipalName |
Export-Csv -NoTypeInfoation -Encoding utf8 -delimiter "," $filename

}
```

Get-ADUser es un cmdlet estándar para consultar una lista de usuarios. El ejemplo anterior contiene un argumento de filtro para listar solo los usuarios con un UserPrincipalName y un estado de cuenta 'enabled'.

El argumento `SearchBase` restringe la parte de AD donde buscar usuarios. Puede omitirlo si desea incluir a todos los usuarios de AD. Nota: Esta consulta podría devolver un gran número de usuarios.

El CSV tiene un aspecto similar a este:



## Servidor FAS

El siguiente script de PowerShell toma la lista de usuarios generada previamente y crea una lista de 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  
  
}  
  
}
```

Si tiene más de un servidor FAS, el certificado de un usuario en particular se generará dos veces: una en el servidor principal y otra en el servidor de conmutación por error.

El script anterior está diseñado para una regla llamada 'default'. Si tiene un nombre de regla diferente (por ejemplo, 'hello'), simplemente cambie la variable \$rule en el script.

Citrix FAS Administration Console - connected to localhost

Initial Setup Rules Advanced [Connect to...](#)

A rule defines a smartcard-class certificate that signs users into a Citrix environment.

[+ Create rule](#)

|         |                                                                                                                                                                         |                |
|---------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------|
| Default |   | <b>Summary</b> |
| hello   |   |                |

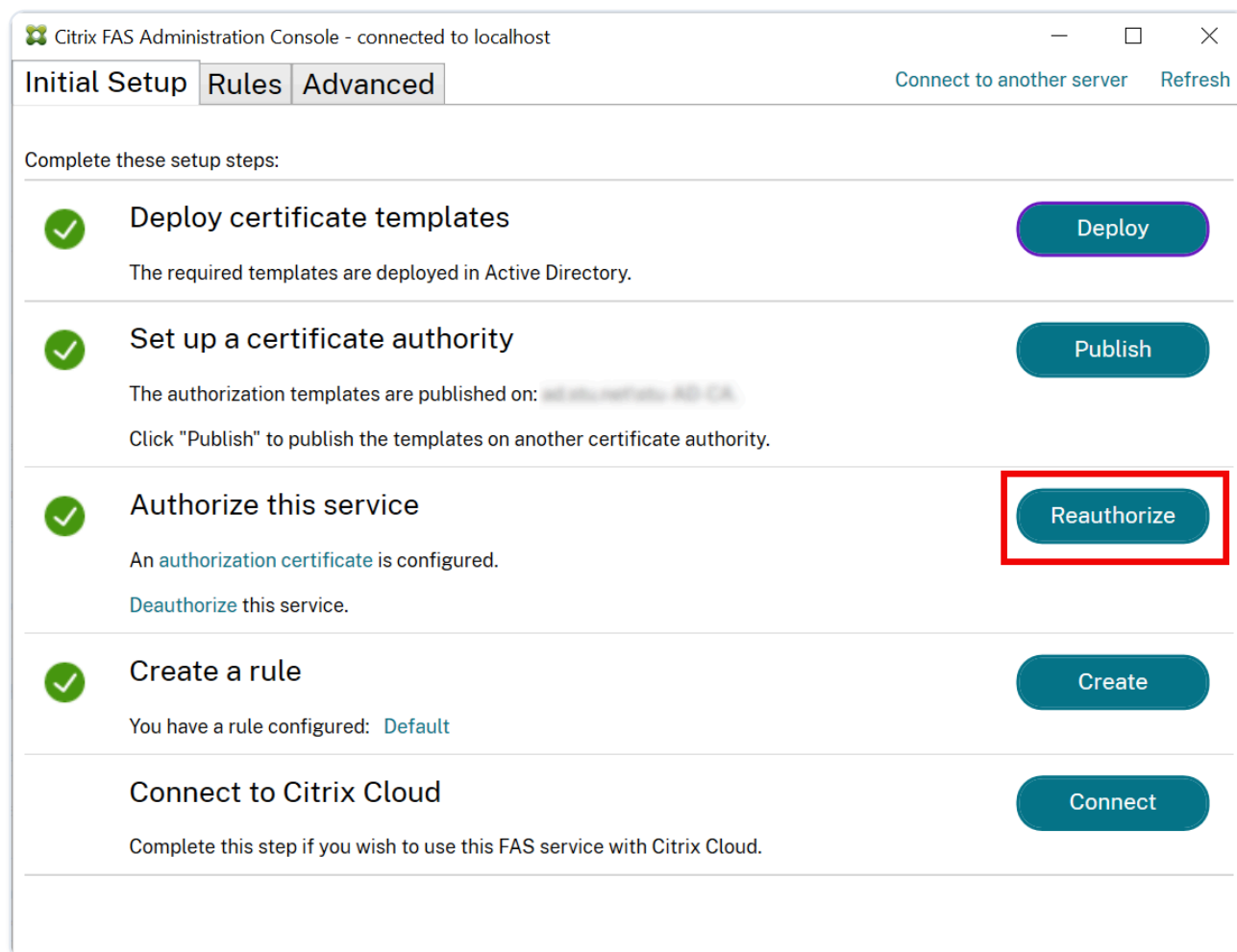
|                   |                       |
|-------------------|-----------------------|
| <b>Rule name:</b> | hello                 |
| <b>Status:</b>    | OK                    |
| <b>Template:</b>  | Citrix_SmartcardLogon |

## Renovar certificados de la autoridad de registro

Si hay más de un servidor FAS en uso, puede renovar un certificado de autorización FAS sin afectar a los usuarios que han iniciado sesión.

### NOTA:

También puede usar la GUI para volver a autorizar FAS:



Complete la siguiente secuencia:

1. Crear un nuevo certificado de autorización: `New-FasAuthorizationCertificate`
2. Anote el GUID del nuevo certificado de autorización, tal como lo devuelve: `Get-FasAuthorizationCertificate`
3. Ponga el servidor FAS en modo de mantenimiento: `Set-FasServer -Address <FAS server> -MaintenanceMode $true`
4. Intercambie el nuevo certificado de autorización: `Set-FasCertificateDefinition -AuthorizationCertificate <GUID>`
5. Saque el servidor FAS del modo de mantenimiento: `Set-FasServer -Address <FAS server> -MaintenanceMode $false`
6. Elimine el certificado de autorización antiguo: `Remove-FasAuthorizationCertificate`

## Información relacionada

- El artículo [Instalar y configurar](#) es la referencia principal para la instalación y configuración de FAS.

- Las implementaciones comunes de Federated Authentication Service se resumen en el artículo [Arquitecturas de implementación](#).
- Otros artículos prácticos se presentan en el artículo [Configuración avanzada](#).

## Protección de claves privadas

### Introducción

Los certificados se almacenan en una base de datos incrustada en el servidor FAS. Las claves privadas asociadas se almacenan mediante la cuenta de servicio de red del servidor FAS y se marcan como no exportables de forma predeterminada.

Existen dos tipos de claves privadas:

- La clave privada asociada al certificado de la entidad de registro, de la plantilla de certificado Citrix\_RegistrationAuthority.
- Las claves privadas asociadas a los certificados de usuario, de la plantilla de certificado Citrix\_SmartcardLogon.

En realidad, hay dos certificados de entidad de registro:

Citrix\_RegistrationAuthority\_ManualAuthorization (válido durante 24 horas de forma predeterminada) y Citrix\_RegistrationAuthority (válido durante dos años de forma predeterminada).

Durante el paso 3 de la ficha **Configuración inicial** de la consola de administración de Federated Authentication Service (FAS), al hacer clic en **Autorizar**, el servidor 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. Este es un certificado temporal, válido durante 24 horas de forma predeterminada. La entidad de certificación no emite este certificado automáticamente; su emisión debe ser autorizada manualmente en la entidad de certificación por un administrador. Una vez que el certificado se emite al servidor FAS, FAS utiliza el certificado Citrix\_RegistrationAuthority\_ManualAuthorization para obtener automáticamente el certificado Citrix\_RegistrationAuthority (válido durante dos años de forma predeterminada). El servidor 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 entidad de registro es especialmente sensible, porque la directiva de certificado de la entidad 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 controle esta clave puede conectarse al entorno como cualquiera de los usuarios del conjunto.

Puede configurar el servidor FAS para proteger las claves privadas de una manera que se ajuste a los requisitos de seguridad de su organización, utilizando una de las siguientes opciones:

- Microsoft Enhanced RSA and AES Cryptographic Provider o Microsoft Software Key Storage Provider para el certificado de la entidad de registro y las claves privadas de los certificados de usuario.
- Microsoft Platform Key Storage Provider con un chip Trusted Platform Module (TPM) para la clave privada del certificado de la entidad de registro, y Microsoft Enhanced RSA and AES Cryptographic Provider o Microsoft Software Key Storage Provider para las claves privadas de los certificados de usuario.
- Un Cryptographic Service o Key Storage Provider de un proveedor de módulos de seguridad de hardware (HSM) con el dispositivo HSM para el certificado de la entidad de registro y las claves privadas de los certificados de usuario.

## Configuración de claves privadas

Configure FAS para usar una de las tres opciones. Use un editor de texto para modificar el archivo Citrix.Authentication.FederatedAuthenticationService.exe.config. La ubicación predeterminada del archivo es la carpeta Program Files\Citrix\Federated Authentication Service en el servidor 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.Suppress" value="" / -->

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

FAS lee el archivo de configuración solo cuando se inicia el servicio. Si se cambia algún valor, FAS debe reiniciarse para que los nuevos parámetros surtan efecto.

Establezca los valores relevantes en el archivo

Citrix.Authentication.FederatedAuthenticationService.exe.config de la siguiente manera:

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

| VALOR                  | COMENTARIO           |
|------------------------|----------------------|
| verdadero              | Usar las API de CAPI |
| falso (predeterminado) | Usar las API de CNG  |

Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.**ProviderName** (nombre del proveedor a utilizar)

| VALOR                                                            | COMENTARIO                                                                                                                                                                                                                                                                                                             |
|------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Proveedor criptográfico mejorado de Microsoft RSA y AES          | Proveedor CAPI predeterminado                                                                                                                                                                                                                                                                                          |
| Proveedor de almacenamiento de claves de software de Microsoft   | Proveedor CNG predeterminado                                                                                                                                                                                                                                                                                           |
| Proveedor de almacenamiento de claves de plataforma de Microsoft | Proveedor TPM predeterminado. Tenga en cuenta que TPM no se recomienda para claves de usuario. Utilice TPM solo para la clave de la autoridad de registro. Si tiene previsto ejecutar su servidor FAS en un entorno virtualizado, consulte con su proveedor de TPM y de hipervisor si la virtualización es compatible. |
| CSP/Proveedor de almacenamiento de claves del proveedor de HSM   | Suministrado por el proveedor de HSM. El valor difiere entre proveedores. Si tiene previsto ejecutar su servidor FAS en un entorno virtualizado, consulte con su proveedor de HSM si la virtualización es compatible.                                                                                                  |

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

| VALOR | COMENTARIO                                                                                                                                                                                                                    |
|-------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 24    | Predeterminado. Se refiere a la propiedad Microsoft KeyContainerPermissionAccessEntry.Provider Type PROV_RSA_AES 24. Siempre debe ser 24, a menos que utilice un HSM con CAPI y el proveedor de HSM especifique lo contrario. |

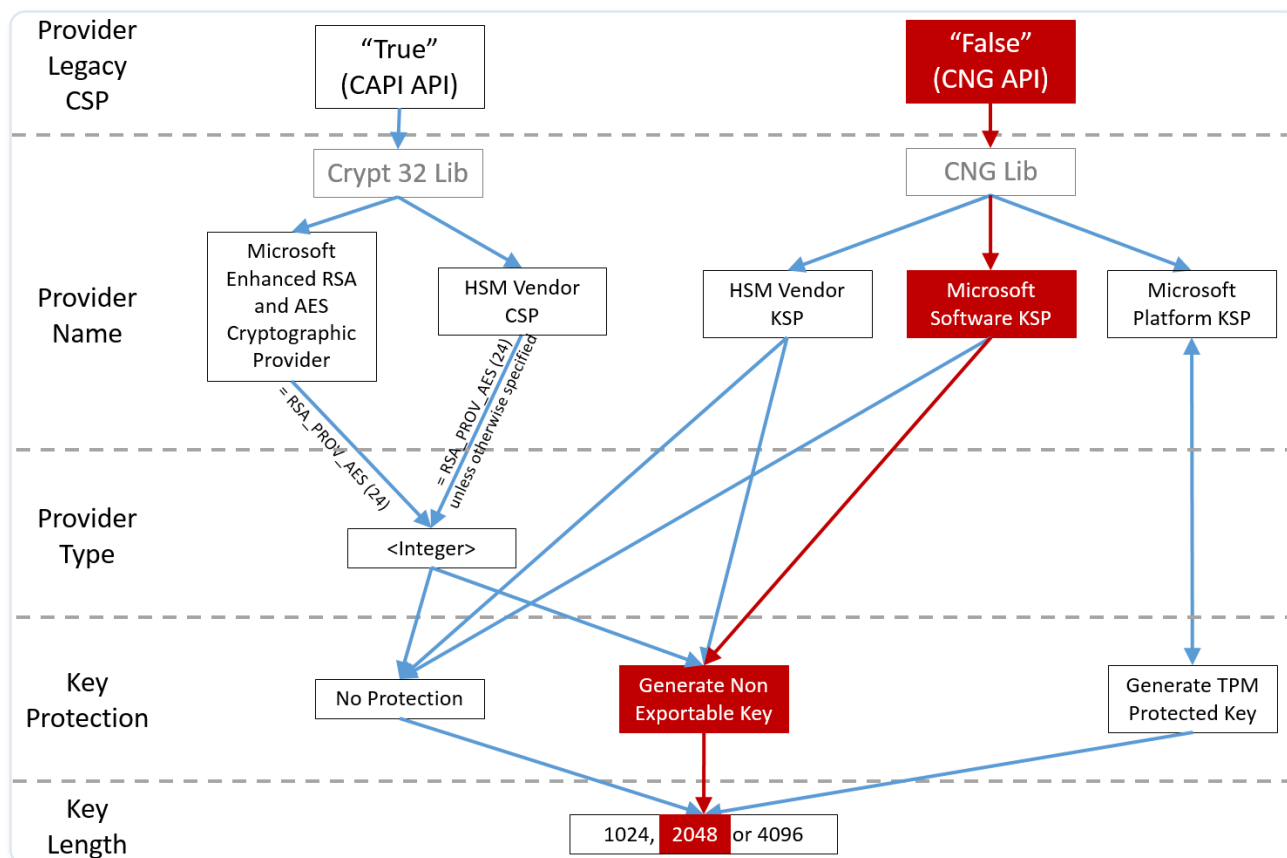
Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.**KeyProtection** (Cuando FAS necesita realizar una operación de clave privada, utiliza el valor especificado aquí) Controla la marca "exportable" de las claves privadas. Permite el uso del almacenamiento de claves TPM, si es compatible con el hardware.

| VALOR                    | COMENTARIO                                                                                                                                                                                   |
|--------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Sin protección           | La clave privada se puede exportar.                                                                                                                                                          |
| GenerateNonExportableKey | Predeterminado. La clave privada no se puede exportar.                                                                                                                                       |
| GenerateTPMProtectedKey  | La clave privada se gestionará mediante el TPM. La clave privada se almacena a través del ProviderName que especificó en ProviderName (por ejemplo, Microsoft Platform Key Storage Provider) |

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

| VALOR | COMENTARIO                                          |
|-------|-----------------------------------------------------|
| 2048  | Predeterminado. También se pueden usar 1024 o 4096. |

La configuración del archivo de configuración se representa gráficamente de la siguiente manera (los valores predeterminados de instalación se muestran en rojo):



## Ejemplos de escenarios de configuración

### Ejemplo 1

Este ejemplo cubre la clave privada del certificado de la autoridad de registro y las claves privadas de los certificados de usuario almacenadas mediante el Microsoft Software Key Storage Provider

Esta es la configuración predeterminada posterior a la instalación. No se requiere ninguna configuración adicional de clave privada.

### Ejemplo 2

Este ejemplo muestra la clave privada del certificado de la autoridad de registro almacenada en el TPM de hardware de la placa base del servidor FAS a través del Proveedor de almacenamiento de claves de plataforma de Microsoft, y las claves privadas de los certificados de usuario almacenadas mediante el Proveedor de almacenamiento de claves de software de Microsoft.

Este escenario asume que el TPM de la placa base de su servidor FAS se ha habilitado en la BIOS según la documentación del fabricante del TPM y luego se ha inicializado en Windows; consulte [<https://docs.microsoft.com/es-es/previous-versions/windows/it-pro/windows-vista/cc749022\(v=ws.10\)>](https://docs.microsoft.com/es-es/previous-versions/windows/it-pro/windows-vista/cc749022(v=ws.10)>).

## Uso de la consola de administración de FAS

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

Al realizar la configuración inicial de FAS, después de implementar las plantillas de certificado y configurar la autoridad de certificación, pero antes de autorizar el servicio (paso 3 de la secuencia de configuración):

**Paso 1:** Edite el archivo de configuración cambiando la siguiente línea de la siguiente manera:

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

El archivo debería aparecer ahora de la siguiente manera:

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

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

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

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

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

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

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

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

Algunos TPM restringen la longitud de la clave. La longitud de clave predeterminada es de 2048 bits. Asegúrese de especificar una longitud de clave compatible con su hardware.

**Paso 2:** Reinicie el servicio Citrix Federated Authentication Service para leer los valores del archivo de configuración.

**Paso 3:** Autorice el servicio.

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

Para confirmar que la clave privada del certificado de la autoridad de registro se está almacenando correctamente en el TPM, utilice los siguientes 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:

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

**Paso 5:** Vuelva a editar el archivo de configuración de la siguiente manera:

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

#### NOTA:

Aunque FAS puede generar certificados de usuario con claves protegidas por TPM, el hardware de TPM puede ser demasiado lento para implementaciones grandes.

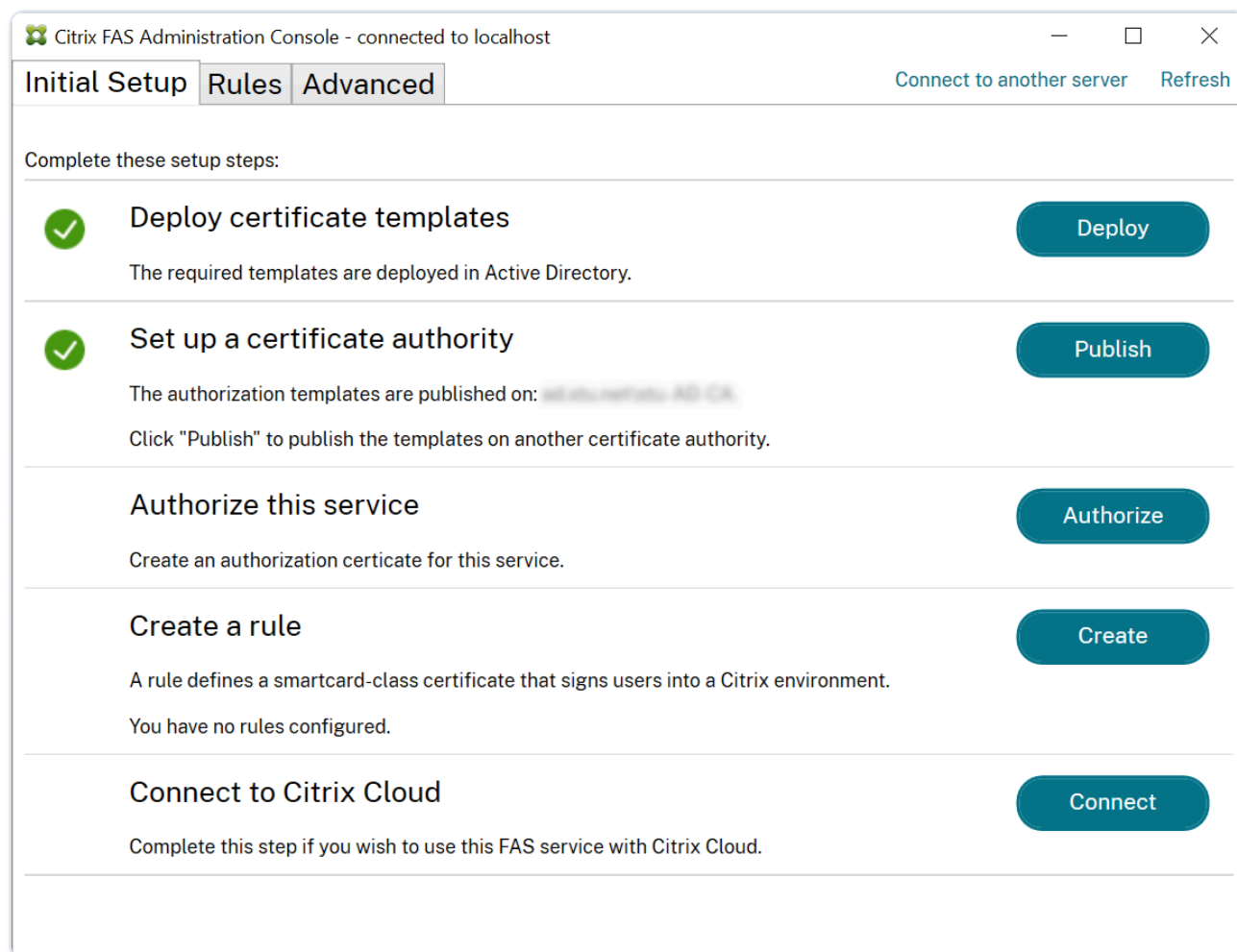
**Paso 6:** Reinicie FAS. Esto obliga al servicio a volver a leer el archivo de configuración y a reflejar los valores modificados. Las operaciones automáticas posteriores de clave privada afectarán a las claves de certificado de usuario; esas operaciones no almacenarán las claves privadas en el TPM, sino que utilizarán el Proveedor de almacenamiento de claves de software de Microsoft.

**Paso 7:** Seleccione la ficha **Reglas** en la consola de administración de FAS y edite la configuración como se describe en [Instalar y configurar](#).

## Uso de PowerShell

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

**Paso 1:** Durante la configuración inicial de FAS mediante la consola de administración, complete solo los dos primeros pasos: "Implementar plantillas de certificado" y "Configurar una autoridad de certificación".



**Paso 2:** En el servidor de la autoridad de certificación, agregue el complemento MMC Plantillas de certificado. Haga clic con el botón secundario en la plantilla

**Citrix\_RegistrationAuthority\_ManualAuthorization** 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:

**Properties of New Template**

|                      |         |                  |              |                       |          |
|----------------------|---------|------------------|--------------|-----------------------|----------|
| Subject Name         |         | Server           |              | Issuance Requirements |          |
| Superseded Templates |         |                  | Extensions   |                       | Security |
| Compatibility        | General | Request Handling | Cryptography | Key Attestation       |          |

Template display name:  
Offline\_RA

Template name:  
Offline\_RA

Validity period: 2 years      Renewal period: 0 days

☐ Publish certificate in Active Directory  
☐ Do not automatically reenroll if a duplicate certificate exists in Active Directory

OK Cancel Apply Help

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

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

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

**Paso 5:** Genere el par de claves RSA dentro del TPM del servidor FAS y cree la solicitud de firma de certificado introduciendo el siguiente cmdlet de PowerShell en el servidor FAS. **Nota:** Algunos TPM restringen la longitud de la clave. La longitud de clave predeterminada es de 2048 bits. Asegúrese de especificar una longitud de clave compatible con su hardware.

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

Por ejemplo:

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

Se muestra lo siguiente:

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

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

**NOTAS:**

- El GUID de Id. (en este ejemplo, "5ac3d8bd-b484-4ebe-abf8-4b2cfd62ca39") es necesario en un paso posterior.
- Considere este cmdlet de PowerShell como una "anulación" única que se utiliza para generar la clave privada del certificado de la entidad de registro.
- Al ejecutar este cmdlet, se comprueban los valores leídos del archivo de configuración cuando se inició FAS para determinar la longitud de clave que se va a utilizar (el valor predeterminado es 2048).
- Dado que -UseTPM se establece en \$true en esta operación manual de clave privada del certificado de la entidad de registro iniciada por PowerShell, el sistema ignora los valores del archivo que no coinciden con la configuración necesaria para usar un TPM.
- La ejecución de este cmdlet no cambia ninguna configuración en el archivo de configuración.
- Durante las operaciones automáticas posteriores de clave privada del certificado de usuario iniciadas por FAS, se utilizan los valores que se leyeron del archivo cuando se inició FAS.
- También es posible establecer el valor de KeyProtection en el archivo de configuración como GenerateTPMProtectedKey cuando el FAS server emite certificados de usuario para generar claves privadas de certificado de usuario protegidas por el TPM.

Para verificar que se utilizó el TPM para generar el par de claves, consulte el registro de aplicaciones en el Visor de eventos de Windows en el FAS server, en el momento en que se genera el par de claves.

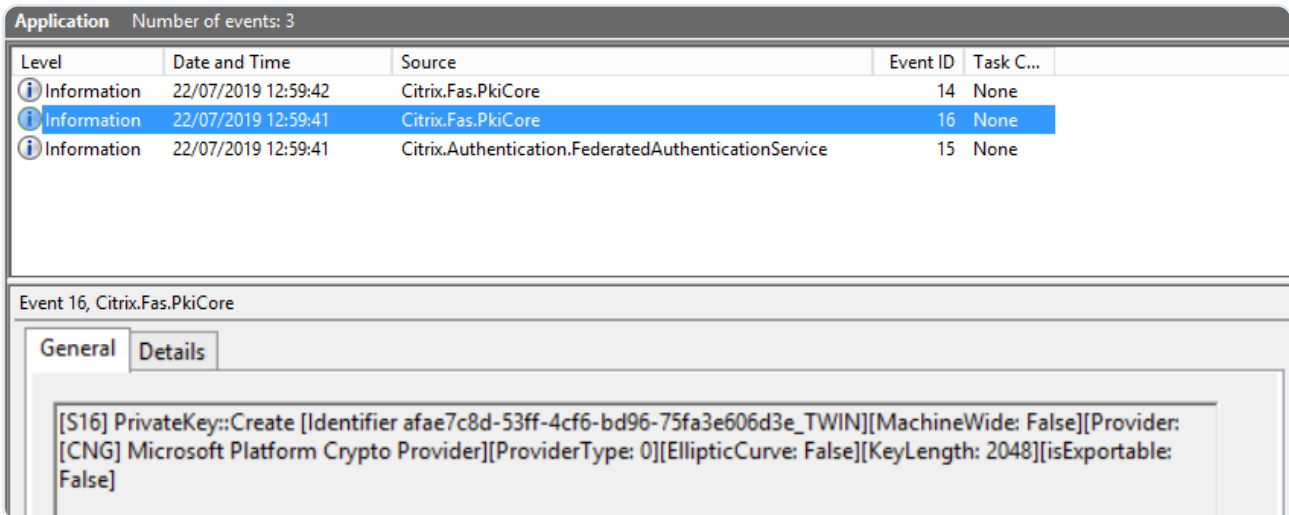
|                                                                                     |             |                     |                                                      |    |      |
|-------------------------------------------------------------------------------------|-------------|---------------------|--------------------------------------------------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

| Event 15, Citrix.Authentication.FederatedAuthenticationService                                                                              |         |
|---------------------------------------------------------------------------------------------------------------------------------------------|---------|
| General                                                                                                                                     | Details |
| [S15] Administrator [CITRIXTEST\Administrator] creating certificate request [TPM: True] [correlation: e61a73d7-bb61-44af-8d21-1159d864d82e] |         |

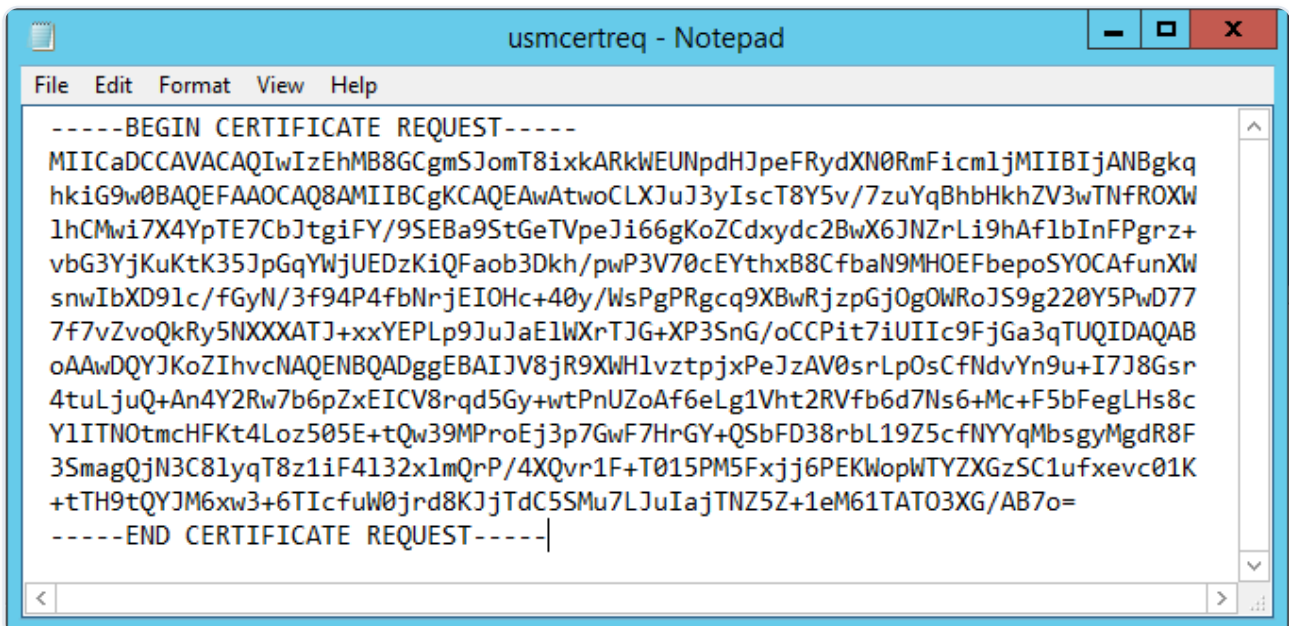
**Nota:** ""

Seguido de:



**Nota:** "Proveedor: Microsoft Platform Crypto Provider"

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



**Paso 7:** Envíe la solicitud de firma de certificado a su autoridad de certificación escribiendo lo siguiente en PowerShell en el FAS server:

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

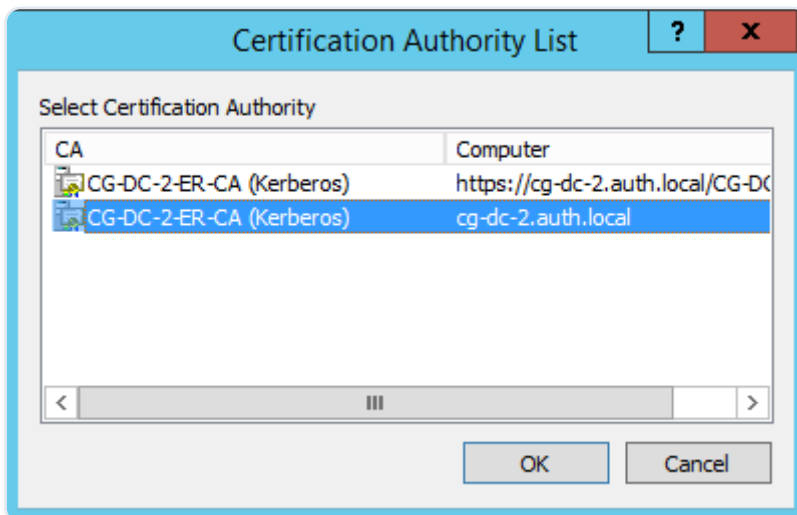
Por ejemplo:

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

Se muestra lo siguiente:

```
PS C:\Users\Administrator.AUTH> certreq -submit -attrib "certificatetemplate:Offline_RA" C:\Users\Administrator.AUTH\Desktop\usmcertreq.txt
Active Directory Enrollment Policy
{4F76160E-DB0C-4D21-A4FD-2E29502177C2}
ldap:
```

En este punto, puede aparecer una ventana de Lista de Autoridades de Certificación. La autoridad de certificación de este ejemplo tiene la inscripción habilitada tanto para http (arriba) como para DCOM (abajo). Seleccione la opción DCOM, si está disponible:

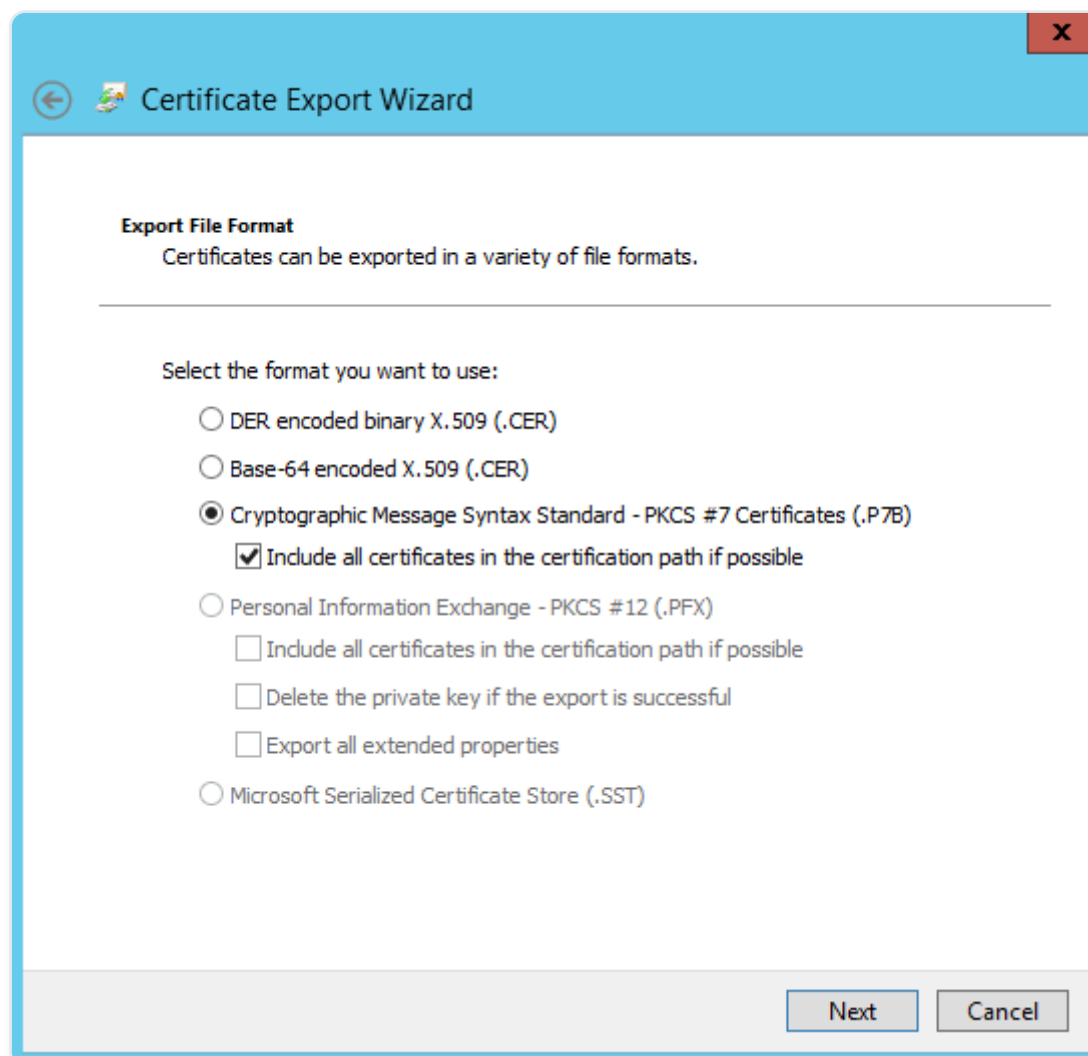


Una vez que se haya especificado la autoridad de certificación, PowerShell muestra el RequestID:

```
PS C:\Users\Administrator.AUTH> certreq -submit -attrib "certificatetemplate:Offline_RA" C:\Users\Administrator.AUTH\Desktop\usmcertreq.txt
Active Directory Enrollment Policy
{4F76160E-DB0C-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 autoridad de certificación, en el complemento MMC de la autoridad de certificación, haga clic en **Solicitudes pendientes**. Anote el ID de solicitud. A continuación, haga clic con el botón derecho 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 pestaña **Detalles**. Haga clic en **Copiar a archivo**. Se inicia el Asistente para exportación de certificados. Haga clic en **Siguiente**. Elija las siguientes opciones para el formato de archivo:



El formato debe ser **"Estándar de sintaxis de mensajes criptográficos – Certificados PKCS #7 (.P7B)"** y **"Incluir todos los certificados en la ruta de certificación si es posible"** debe estar seleccionada.

**Paso 10:** Copie el archivo de certificado exportado en el servidor FAS.

**Paso 11:** Importe el certificado de la autoridad de registro en el servidor FAS introduciendo el siguiente cmdlet de PowerShell en el servidor 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
```

Se muestra lo siguiente:

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

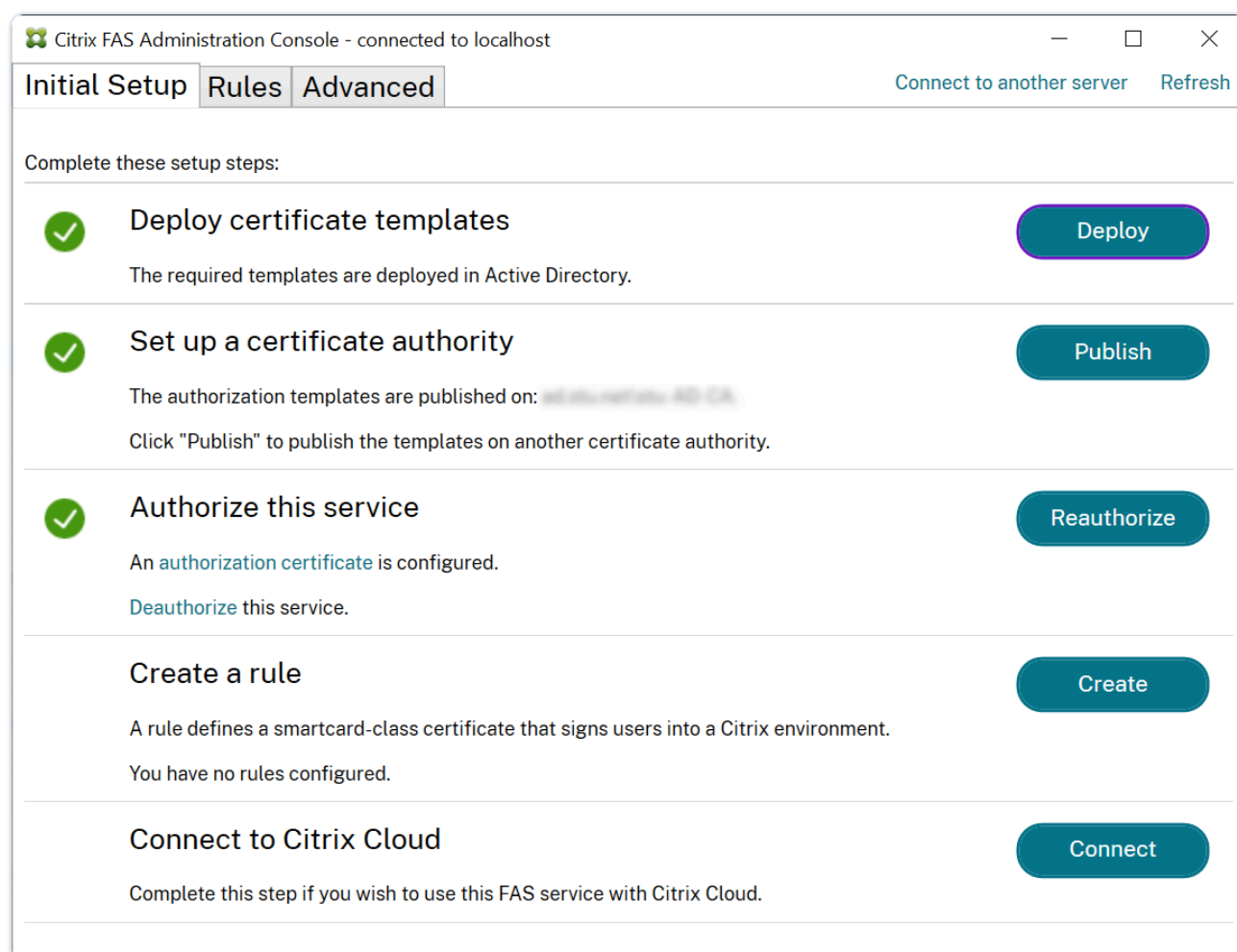
Id                : 74d427ff-c55b-4d6d-87ae-1ff98b0c2705
Address           : [Offline CSR]
TrustArea        : 978816cd-8b2f-4695-8c5d-08bb7df1816b
CertificateRequest :
Status           : Ok
```

Para confirmar que la clave privada del certificado de la autoridad de registro se almacena correctamente en el TPM, utilice los siguientes 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:

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

Get-FasAuthorizationCertificate -FullCertInfo -Address localhost
```

**Paso 12:** Cierre la consola de administración de FAS y, a continuación, reiníciela.



**Nota:** El paso "Autorizar este servicio" tiene una marca de verificación verde.

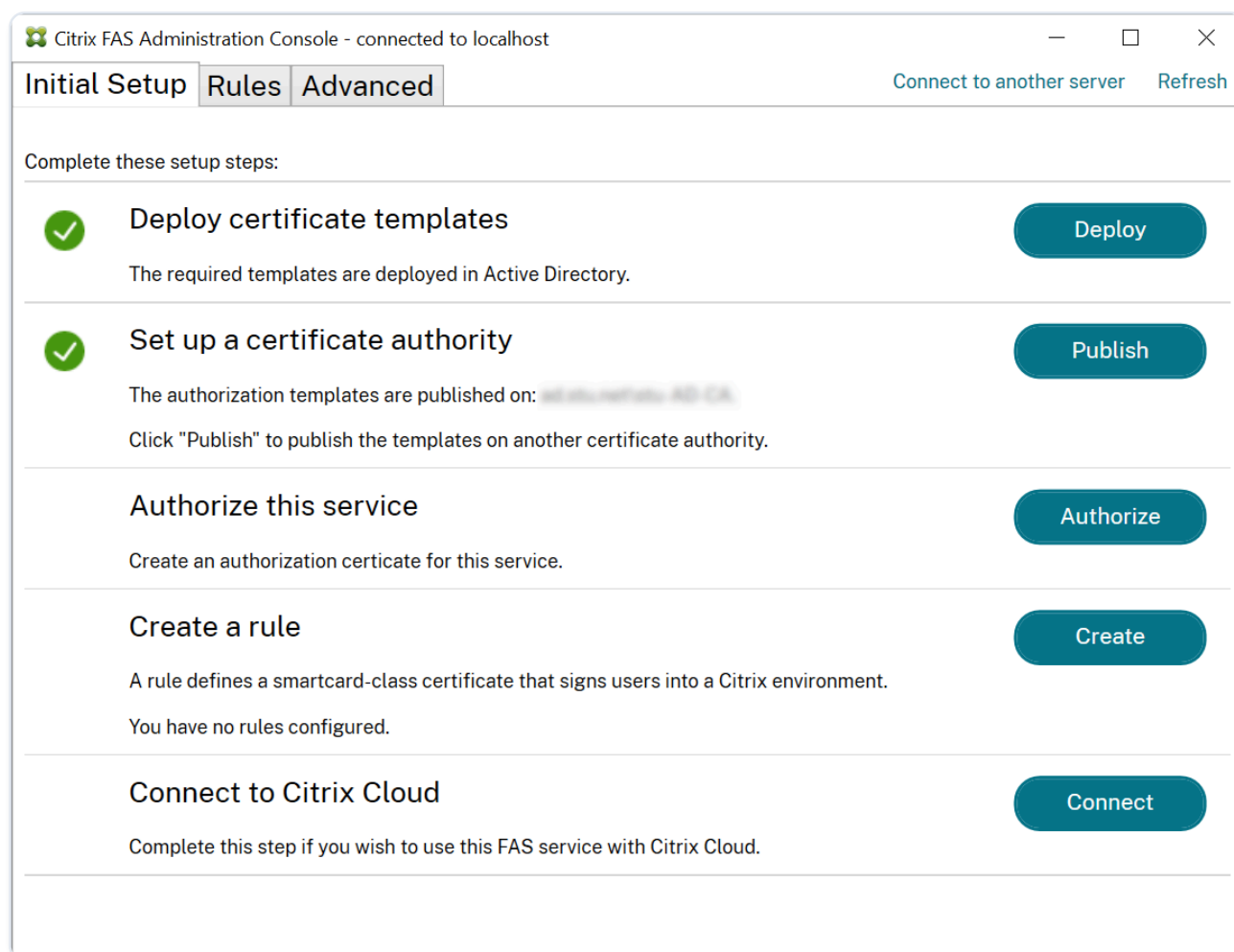
**Paso 13:** Seleccione la ficha **Reglas** en la consola de administración de FAS y edite la configuración descrita en [Instalar y configurar](#).

### Ejemplo 3

Este ejemplo cubre una clave privada de certificado de autoridad de registro y claves privadas de certificados de usuario almacenadas en un HSM. Este ejemplo asume un HSM configurado. Su HSM tendrá un nombre de proveedor, por ejemplo, "Proveedor de almacenamiento de claves del proveedor de HSM".

Si tiene previsto ejecutar su servidor FAS en un entorno virtualizado, consulte con el proveedor de su HSM sobre la compatibilidad con hipervisores.

**Paso 1.** Durante la configuración inicial de FAS mediante la consola de administración, complete solo los dos primeros pasos: "Implementar plantillas de certificado" y "Configurar una autoridad de certificación".



**Paso 2:** Consulte la documentación del proveedor de su HSM para determinar el valor de ProviderName de su HSM. Si su HSM utiliza CAPI, el proveedor podría denominarse en la documentación como Cryptographic Service Provider (CSP). Si su HSM utiliza CNG, el proveedor podría denominarse Key Storage Provider (KSP).

**Paso 3:** Edite el archivo de configuración de la siguiente manera:

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

El archivo debería aparecer ahora de la siguiente manera:

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

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

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

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

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

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

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

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

Este escenario asume que su HSM utiliza CNG, por lo que el valor de ProviderLegacyCsp se establece en false. Si su HSM utiliza CAPI, el valor de ProviderLegacyCsp debe establecerse en true. Consulte la documentación de su proveedor de HSM para determinar si su HSM utiliza CAPI o CNG. Consulte también la documentación de su proveedor de HSM sobre las longitudes de clave admitidas para la generación de claves RSA asimétricas. En este ejemplo, la longitud de clave se establece en el valor predeterminado de 2048 bits. Asegúrese de que la longitud de clave que especifique sea compatible con su hardware.

**Paso 4:** Reinicie el Servicio de autenticación federada de Citrix para leer los valores del archivo de configuración.

**Paso 5:** Genere el par de claves RSA dentro del HSM y cree la solicitud de firma de certificado haciendo clic en **Autorizar** en la pestaña **Configuración inicial** de la consola de administración de FAS.

**Paso 6:** Para verificar que el par de claves se generó en el HSM, compruebe 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: [Proveedor: Proveedor de almacenamiento de claves del proveedor de HSM]

**Paso 7:** En el servidor de la entidad de certificación, en la MMC de la entidad de certificación, 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\UCSHSMS   |                        |

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

**Nota:** El paso "Autorizar este servicio" tiene una marca de verificación verde.

Citrix FAS Administration Console - connected to localhost

Initial Setup Rules Advanced [Connect to another server](#) [Refresh](#)

Complete these setup steps:

- Deploy certificate templates** [Deploy](#)  
 The required templates are deployed in Active Directory.
- Set up a certificate authority** [Publish](#)  
 The authorization templates are published on: [adcs.certsrv.ms](#)  
 Click "Publish" to publish the templates on another certificate authority.
- Authorize this service** [Reauthorize](#)  
 An [authorization certificate](#) is configured.  
[Deauthorize](#) this service.
- Create a rule** [Create](#)  
 A rule defines a smartcard-class certificate that signs users into a Citrix environment.  
 You have no rules configured.
- Connect to Citrix Cloud** [Connect](#)  
 Complete this step if you wish to use this FAS service with Citrix Cloud.

**Paso 8:** Seleccione la pestaña **Reglas** en la consola de administración de FAS y edite la configuración como se describe en [Instalar y configurar](#).

## Almacenamiento de certificados de FAS

FAS no utiliza el almacén de certificados de Microsoft en el servidor FAS para almacenar sus certificados. Utiliza una base de datos incrustada.

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

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

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

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

[illegible]

Para obtener una lista de certificados de usuario, introduzca:

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

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

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

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

**NOTA:**

Cuando se utiliza un HSM para almacenar claves privadas, los contenedores HSM se identifican con un GUID. El GUID de la clave privada en el HSM se puede obtener mediante:

```
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

- [Instalar y configurar](#) es la referencia principal para la instalación y configuración de FAS.
- Las implementaciones comunes de FAS se resumen en el artículo [Descripción general de las arquitecturas de Federated Authentication Services](#).
- Otros artículos prácticos se presentan en el artículo [Configuración avanzada](#).

## Configuración de seguridad y red

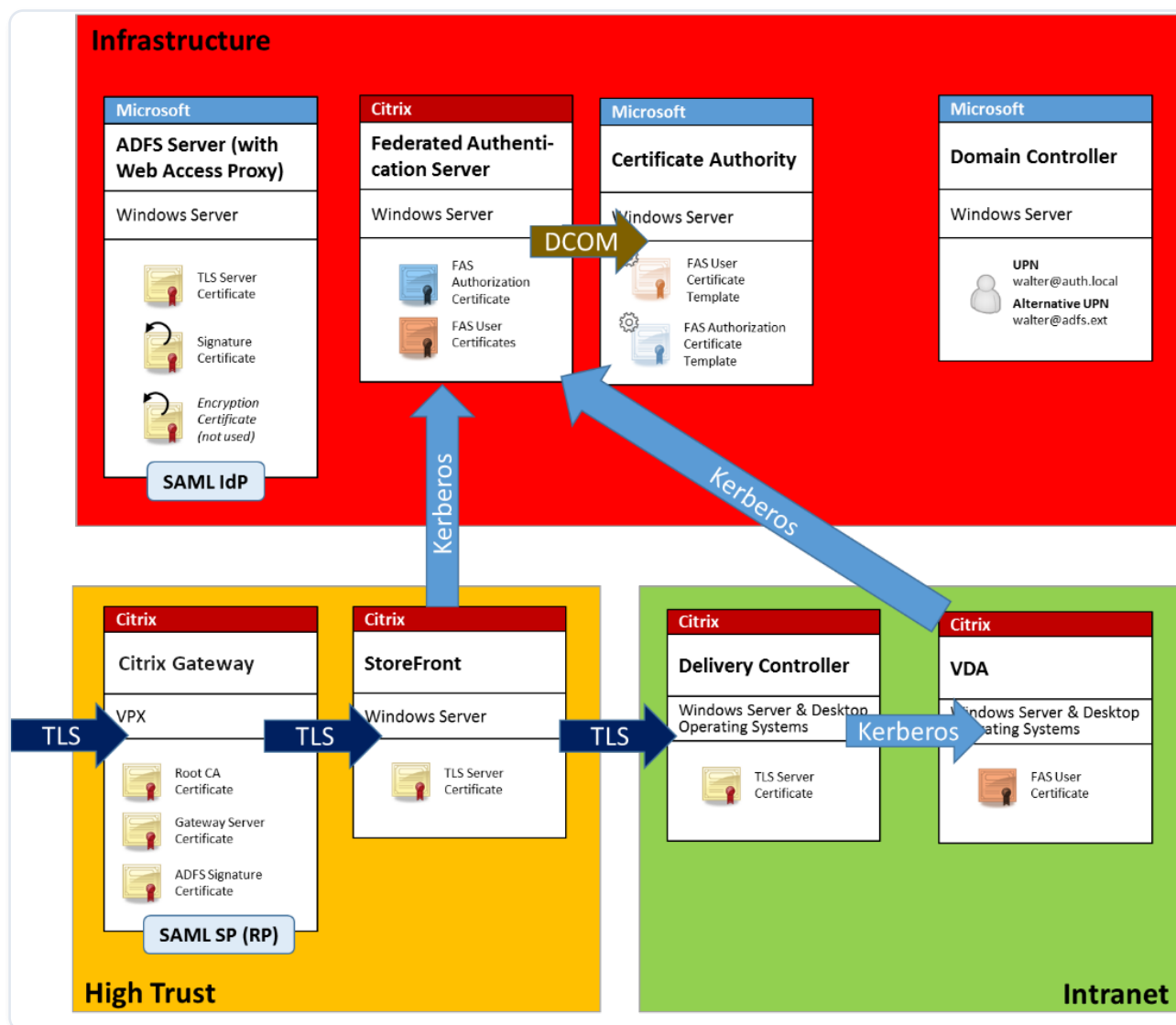
Federated Authentication Service (FAS) está estrechamente integrado con Microsoft Active Directory y la autoridad de certificación de Microsoft. Asegúrese de que el sistema se administre y proteja adecuadamente, desarrollando una política de seguridad como lo haría para un controlador de dominio u otra infraestructura crítica.

Este documento ofrece una descripción general de los problemas de seguridad que deben tenerse en cuenta al implementar FAS. También proporciona una descripción general de las funciones disponibles que podrían ayudar a proteger su infraestructura.

## Arquitectura de red

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

El servidor FAS forma parte de la infraestructura crítica para la seguridad, junto con la autoridad de certificación y el controlador de dominio. En un entorno federado, Citrix Gateway y Citrix StoreFront son componentes que realizan la autenticación de usuarios. Otros componentes de Citrix Virtual Apps and Desktops™ no se ven afectados por la introducción de FAS.



## Firewall y seguridad de red

El protocolo TLS a través del puerto 443 protege la comunicación entre Citrix Gateway, StoreFront y los componentes de Delivery Controller™. El servidor StoreFront solo realiza conexiones salientes, y Citrix Gateway solo acepta conexiones a través de Internet mediante el puerto HTTPS 443.

El servidor StoreFront se comunica con el servidor FAS a través del puerto 80 mediante Kerberos con autenticación mutua. La autenticación utiliza la identidad Kerberos HOST/fqdn del servidor FAS y la identidad de la cuenta de máquina Kerberos del servidor StoreFront. Este método de autenticación genera un «identificador de credenciales» de un solo uso necesario para que Citrix Virtual Delivery Agent (VDA) inicie sesión del usuario.

Cuando una sesión HDX se conecta al VDA, el VDA también se comunica con el servidor FAS a través del puerto 80. La autenticación utiliza la identidad Kerberos HOST/fqdn del servidor FAS y

la identidad de máquina Kerberos del VDA. Además, el VDA debe proporcionar el «identificador de credenciales» para acceder al certificado y a la clave privada.

La autoridad de certificación de Microsoft acepta la comunicación mediante DCOM autenticado por Kerberos, que se puede configurar para usar un puerto TCP fijo. La autoridad de certificación requiere que el servidor FAS suministre un paquete CMC firmado por un certificado de agente de inscripción de confianza.

| SERVIDOR                                | PUERTOS DE FIREWALL                                                                                             |
|-----------------------------------------|-----------------------------------------------------------------------------------------------------------------|
| Federated Authentication Service        | [in] Kerberos over HTTP desde StoreFront™ y VDAs, [out] DCOM a la autoridad de certificación de Microsoft       |
| Citrix Gateway                          | [in] HTTPS desde máquinas cliente, [in/out] HTTPS hacia/desde el servidor StoreFront, [out] HDX a VDA           |
| StoreFront                              | [in] HTTPS desde Citrix Gateway, [out] HTTPS al Delivery Controller, [out] Kerberos HTTP a FAS                  |
| Delivery Controller                     | [in] HTTPS desde el servidor StoreFront, [in/out] Kerberos over HTTP desde VDAs                                 |
| VDA                                     | [in/out] Kerberos over HTTP desde Delivery Controller, [in] HDX desde Citrix Gateway, [out] Kerberos HTTP a FAS |
| Autoridad de certificación de Microsoft | [in] DCOM y firmado desde FAS                                                                                   |

## Conexiones entre Citrix Federated Authentication Service y Citrix Cloud™

La consola y FAS acceden a las siguientes direcciones utilizando la cuenta de usuario y la cuenta de servicio de red, respectivamente.

- Consola de administración de FAS, bajo la cuenta de usuario
  - \*.cloud.com
  - \*.citrixworkspacesapi.net
  - Direcciones requeridas por un proveedor de identidades de terceros, si se utiliza uno en su entorno

- Servicio FAS, bajo la cuenta de servicio de red:
  - \*.citrixworkspacesapi.net
  - \*.citrixnetworkapi.net

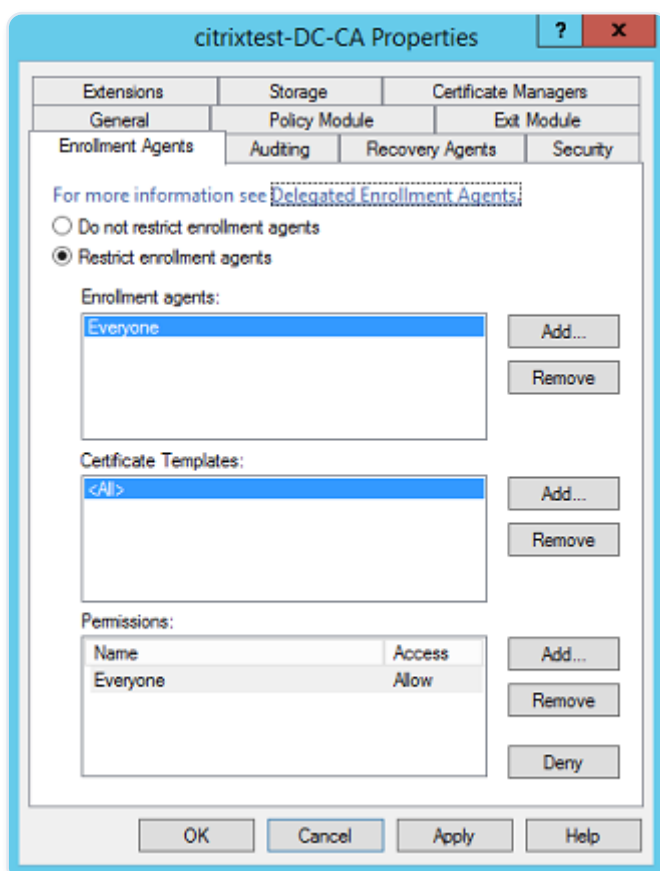
Si su entorno incluye servidores proxy, configure el proxy de usuario con las direcciones de la consola de administración de FAS. Además, asegúrese de que la dirección de la cuenta de servicio de red esté configurada mediante netsh o una herramienta similar.

## Consideraciones de seguridad

FAS tiene un certificado de autoridad de registro que le permite emitir certificados de forma autónoma para los usuarios de su dominio. Ayuda a desarrollar e implementar una política de seguridad para proteger los servidores FAS y restringir sus permisos.

## Agentes de inscripción delegados

FAS emite certificados de usuario actuando como agente de inscripción. La Autoridad de certificación de Microsoft le permite restringir los agentes de inscripción, las plantillas de certificado y los usuarios para los que los agentes de inscripción pueden emitir certificados.



Puede utilizar el diálogo proporcionado para asegurarse de que:

- La lista *Agentes de inscripción* contiene solo servidores FAS.

- La lista *Plantillas de certificado* contiene solo las plantillas FAS.
- La lista *Permisos* contiene los usuarios a los que se les permite usar FAS. Por ejemplo, se recomienda no emitir certificados a los administradores o al grupo de usuarios protegidos.

## Configuración de la lista de control de acceso

Como se describe en la sección [Configurar reglas](#), debe configurar una lista de servidores StoreFront. Estos servidores StoreFront afirman las identidades de los usuarios a FAS cuando se emiten certificados. Del mismo modo, puede restringir a qué usuarios se les emitirán certificados y a qué máquinas VDA pueden autenticarse. Esta función se suma a cualquier característica de seguridad estándar de Active Directory o de la autoridad de certificación que configure.

## Configuración del firewall

Toda la comunicación con los servidores FAS utiliza conexiones de red Kerberos de Windows Communication Foundation (WCF) autenticadas mutuamente a través del puerto 80.

## Supervisión del registro de eventos

FAS y el VDA escriben información en el registro de eventos de Windows. Este registro se puede utilizar para supervisar y auditar información. La sección [Registros de eventos](#) enumera las entradas del registro de eventos que se pueden generar.

## Módulos de seguridad de hardware

Todas las claves privadas, incluidas las claves de certificado de usuario emitidas por FAS, se almacenan como claves privadas no exportables por la cuenta de servicio de red. FAS admite el uso de un módulo de seguridad de hardware criptográfico, si su política de seguridad lo requiere.

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

| PARÁMETRO         | DESCRIPCIÓN                                                                                                                                                                        |
|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ProviderLegacyCsp | Cuando se establece en true, FAS utiliza la API de criptografía de Microsoft (CAPI). De lo contrario, FAS utiliza la API de criptografía de próxima generación de Microsoft (CNG). |

| PARÁMETRO     | DESCRIPCIÓN                                                                                                                                                                                                          |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ProviderName  | Nombre del proveedor CAPI o CNG que se va a utilizar.                                                                                                                                                                |
| ProviderType  | Se refiere a la propiedad Microsoft KeyContainerPermissionAccessEntry.ProviderType PROV_RSA_AES 24. Siempre debe ser 24 a menos que esté utilizando un HSM con CAPI y el proveedor del HSM especifique lo contrario. |
| KeyProtection | Controla el indicador "Exportable" de las claves privadas. También permite el uso del almacenamiento de claves del Módulo de plataforma segura (TPM), si es compatible con el hardware.                              |
| KeyLength     | Longitud de clave para claves privadas RSA. Los valores admitidos son 1024, 2048 y 4096 (predeterminado: 2048).                                                                                                      |

## Responsabilidades de administración

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

| NOMBRE                                       | RESPONSABILIDAD                                            |
|----------------------------------------------|------------------------------------------------------------|
| Administrador de empresa                     | Instalar y proteger plantillas de certificado en el bosque |
| Administrador de dominio                     | Configurar la configuración de directivas de grupo         |
| Administrador de la entidad de certificación | Configurar la autoridad de certificación                   |
| Administrador de FAS                         | Instalar y configurar el servidor FAS                      |
| Administrador de StoreFront/Citrix Gateway   | Configurar la autenticación de usuario                     |
| Administrador de Citrix Virtual Desktops™    | Configurar VDA y Controllers                               |

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

## Configuración de directivas de grupo

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

Citrix recomienda aplicar una única directiva a todas las máquinas del entorno para evitar una configuración incorrecta. Tenga cuidado al modificar la lista de servidores FAS, especialmente al eliminar o reordenar entradas.

El control de esta GPO debe limitarse a los administradores de FAS (y/o administradores de dominio) que instalan y desmantelan los servidores FAS. Tenga cuidado de no reutilizar el nombre FQDN de una máquina poco después de desmantelar un servidor FAS.

## Plantillas de certificado

Si no quiere usar la plantilla de certificado Citrix\_SmartcardLogon que se incluye con FAS, puede modificar una copia de ella. Se admiten las siguientes modificaciones.

### Cambiar el nombre de una plantilla de certificado

Si desea cambiar el nombre de Citrix\_SmartcardLogon para que coincida con el estándar de nomenclatura de plantillas de su organización, debe:

- Crear una copia de la plantilla de certificado y cambiarle el nombre para que coincida con el estándar de nomenclatura de plantillas de su organización.
- Usar los comandos de PowerShell de FAS para administrar FAS, en lugar de la interfaz de usuario administrativa. (La interfaz de usuario administrativa solo está diseñada para usarse con los nombres de plantilla predeterminados de Citrix).
  - Usar el complemento Plantillas de certificado de Microsoft MMC o el comando Publish-FasMsTemplate para publicar la plantilla, y
  - Usar el comando New-FasCertificateDefinition para configurar FAS con el nombre de la plantilla.

## Modificar las propiedades generales

De forma predeterminada, la vida útil de un certificado de usuario es de siete días. Puede modificar el período de validez en la plantilla de certificado.

No modifique el período de renovación. FAS ignora esta configuración en la plantilla de certificado. FAS renueva automáticamente el certificado a la mitad de su período de validez.

## Modificar las propiedades de control de solicitudes

No modifique estas propiedades. FAS ignora esta configuración en la plantilla de certificado. FAS siempre desactiva **Permitir la exportación de la clave privada** y desactiva **Renovar con la misma clave**.

## Modificar las propiedades de criptografía

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

Consulte (</es-es/federated-authentication-service/2308/config-manage/private-key-protection.html>) para ver la protección de clave privada para las configuraciones equivalentes que proporciona FAS.

## Modificar las propiedades de atestación de clave

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

## Modificar las propiedades de las plantillas reemplazadas

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

## Modificar las propiedades de las extensiones

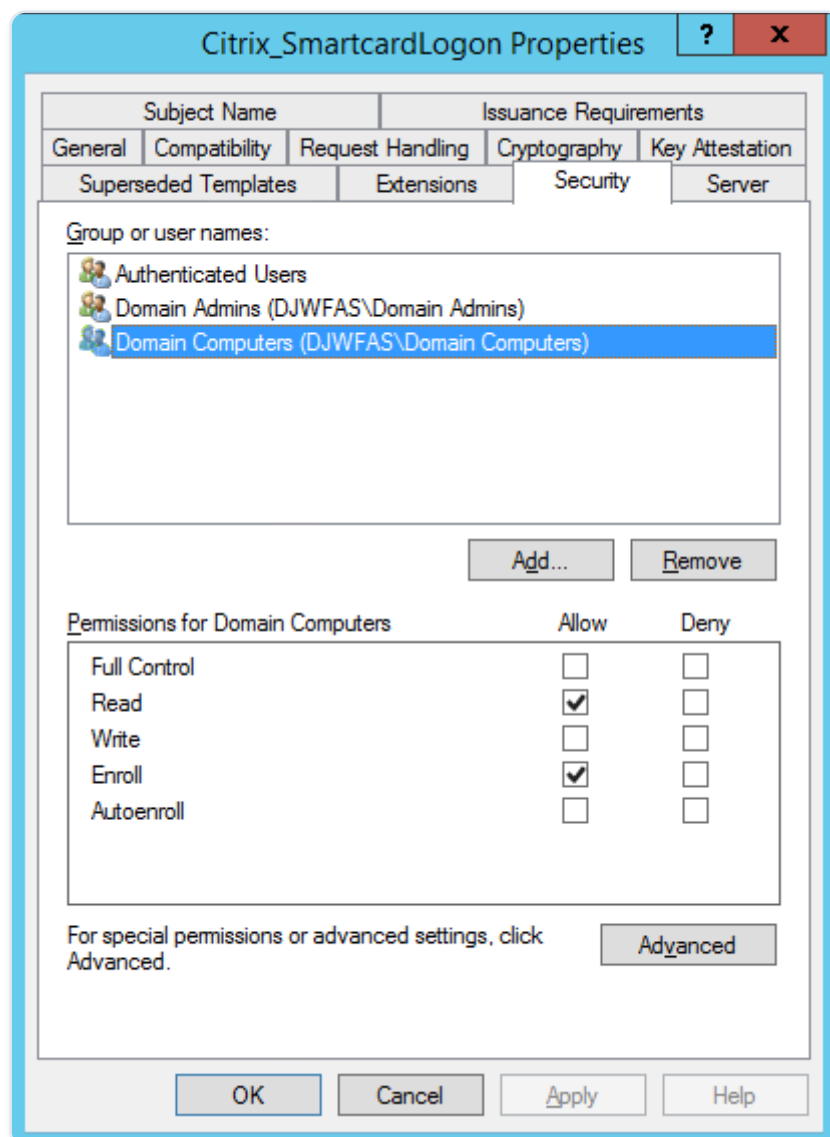
Puede modificar esta configuración para que coincida con la política de su organización.

Nota: Una configuración de extensión inadecuada puede causar problemas de seguridad o dar lugar a certificados inutilizables.

## Modificar las propiedades de seguridad

Citrix recomienda que modifique esta configuración para permitir los permisos de **Lectura e Inscripción** solo para las cuentas de máquina de los servidores FAS. El servicio FAS no requiere ningún otro permiso. Sin embargo, al igual que con otras plantillas de certificados, puede:

- permitir a los administradores leer o escribir la plantilla
- permitir a los usuarios autenticados leer la plantilla



## Modificar las propiedades del nombre del sujeto

Citrix recomienda no modificar estas propiedades.

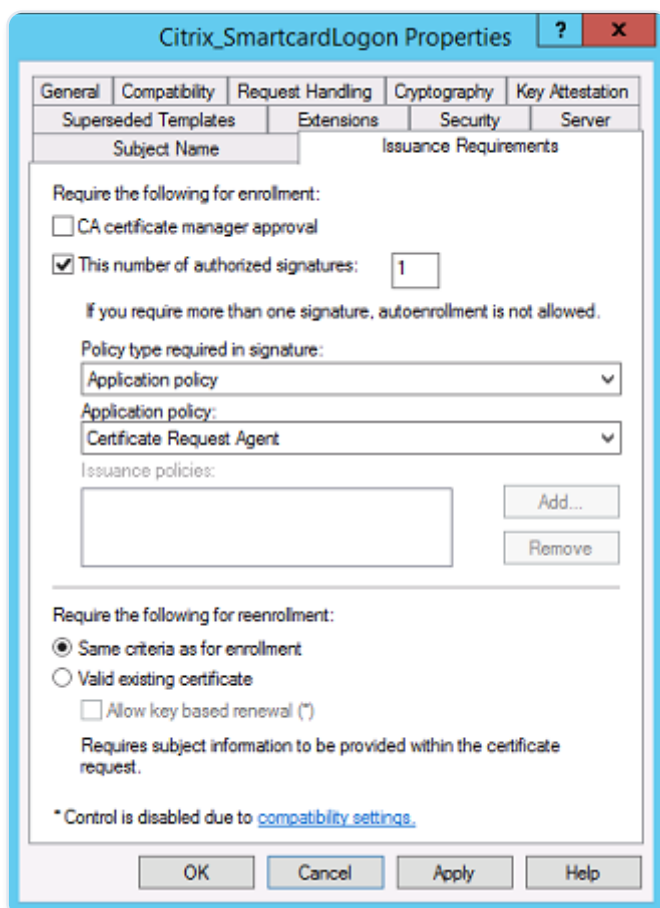
La plantilla tiene seleccionada la opción *Crear a partir de esta información de Active Directory*, lo que hace que la autoridad de certificación incluya el SID del usuario en una extensión de certificado, lo que proporciona una asignación sólida a la cuenta de Active Directory del usuario.

## Modificar las propiedades del servidor

Aunque Citrix no lo recomienda, puede modificar esta configuración para que coincida con la política de su organización, si es necesario.

## Modificar las propiedades de requisitos de emisión

No modifique esta configuración. Esta configuración debe ser la que se muestra:



## Modificar las propiedades de compatibilidad

Puede modificar esta configuración. La configuración debe ser al menos **CA de Windows Server 2003** (versión de esquema 2). Sin embargo, FAS solo admite CA de Windows Server 2008 y posteriores. Además, como se explicó anteriormente, FAS ignora la configuración adicional disponible al seleccionar **CA de Windows Server 2008** (versión de esquema 3) o **CA de Windows Server 2012** (versión de esquema 4).

## Administración de 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 del certificado de emisión que utiliza.

## Publicación de 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 optar por publicar esa plantilla.

Una práctica de seguridad sencilla es publicar solo las plantillas de certificado de la autoridad de registro cuando se instalan los servidores FAS, o insistir en un proceso de emisión completamente sin conexión. En cualquier caso, el administrador de la entidad de certificación debe mantener un

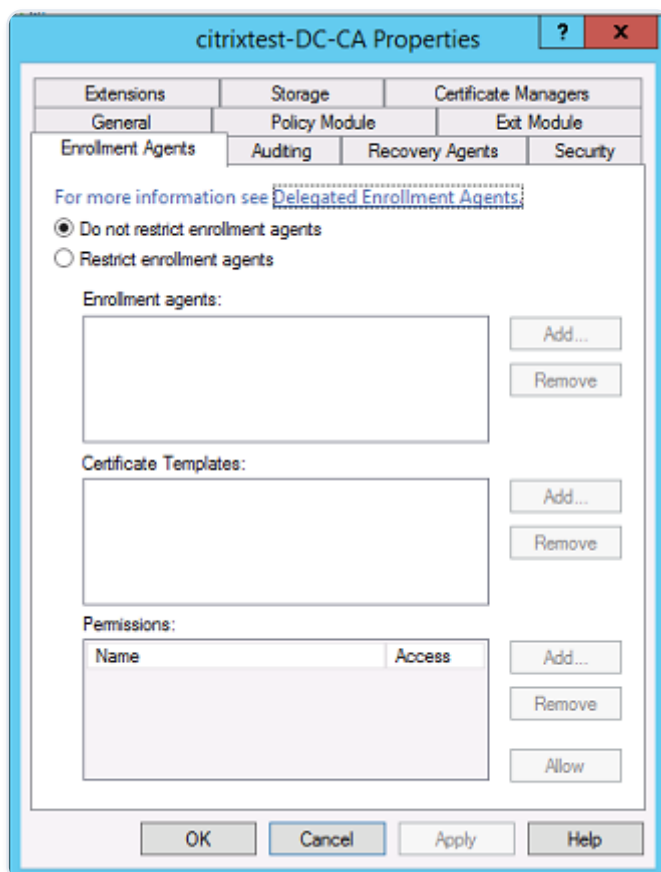
control completo sobre la autorización de las solicitudes de certificado de la autoridad de registro y tener una política para autorizar los servidores FAS.

## Configuración del firewall

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

## Inscripción restringida

De forma predeterminada, cualquier titular de un certificado de autoridad de registro puede emitir certificados a cualquier usuario, utilizando cualquier plantilla de certificado que permita el acceso. Esta emisión de certificados debe restringirse a un grupo de usuarios no privilegiados utilizando la propiedad de la entidad de certificación "Restringir agentes de inscripción".



## Módulos de directivas y auditoría

Para implementaciones avanzadas, se pueden usar módulos de seguridad personalizados para rastrear y vetar la emisión de certificados.

## Administración de FAS

FAS tiene varias funciones de seguridad.

### Restringir StoreFront, usuarios y VDA a través de una ACL

En el centro del modelo de seguridad de FAS está el control de qué cuentas de Kerberos pueden acceder a la funcionalidad:

| VECTOR DE ACCESO    | DESCRIPCIÓN                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|---------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| StoreFront [IdP]    | Se confía en estas cuentas de Kerberos para declarar que un usuario se ha autenticado correctamente. Si una de estas cuentas se ve comprometida, se pueden crear y usar certificados para los usuarios permitidos por la configuración de FAS.                                                                                                                                                                                                                                                             |
| VDA [Relying party] | Estas son las máquinas a las que se les permite acceder a los certificados y claves privadas. También se necesita un identificador de credenciales recuperado por el IdP, por lo que una cuenta de VDA comprometida en este grupo tiene un alcance limitado para atacar el sistema.                                                                                                                                                                                                                        |
| Usuarios            | Esta opción controla qué usuarios pueden ser afirmados por el IdP. Tenga en cuenta que hay una superposición con las opciones de configuración de "Restricted Enrollment Agent" en la autoridad de certificación. En general, es aconsejable incluir solo cuentas no privilegiadas en esta lista. Esto evita que una cuenta de StoreFront comprometida escale privilegios a un nivel administrativo superior. En particular, las cuentas de administrador de dominio no deben ser permitidas por esta ACL. |

### Configurar reglas

Las reglas son útiles si varias implementaciones independientes de Citrix Virtual Apps™ o Citrix Virtual Desktops utilizan la misma infraestructura de servidor FAS. Cada regla tiene un conjunto

independiente de opciones de configuración; en particular, las listas de control de acceso (ACL) de Kerberos se pueden configurar de forma independiente.

## **Configurar la autoridad de certificación y las plantillas**

Se pueden configurar diferentes plantillas de certificado y CA para diferentes derechos de acceso. Las configuraciones avanzadas pueden optar por utilizar certificados menos o más potentes, según el entorno. Por ejemplo, los usuarios identificados como "externos" pueden tener un certificado con menos privilegios que los usuarios "internos".

## **Certificados en sesión y de autenticación**

El administrador de FAS puede controlar si el certificado utilizado para autenticarse está disponible para su uso en la sesión del usuario. Por ejemplo, un usuario puede tener solo certificados de "firma" disponibles en la sesión, mientras que el certificado de "inicio de sesión" más potente se utiliza solo al iniciar sesión.

## **Protección de clave privada y longitud de clave**

El administrador de FAS puede configurar FAS para almacenar claves privadas en un Módulo de seguridad de hardware (HSM) o un Módulo de plataforma de confianza (TPM). Citrix recomienda que al menos la clave privada del certificado de la autoridad de registro esté protegida almacenándola en un TPM. FAS ofrece la opción de guardar la clave privada en un TPM como parte del proceso de solicitud de certificado "sin conexión".

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

## **Registros de eventos**

El servidor FAS proporciona [registros de eventos](#) detallados de configuración y tiempo de ejecución, que se pueden utilizar para auditorías y detección de intrusiones.

## **Acceso administrativo y herramientas de administración**

FAS incluye funciones y herramientas de administración remota (Kerberos con autenticación mutua). Los miembros del "Grupo de administradores locales" tienen control total sobre la configuración de FAS. La configuración de FAS debe mantenerse correctamente.

## Administradores de Citrix Virtual Apps, Citrix Virtual Desktops y VDA

El uso de FAS no cambia el modelo de seguridad de los administradores de Delivery Controller y 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. Se deben mantener las auditorías y los registros de eventos.

## Seguridad general del servidor Windows

Todos los servidores deben estar totalmente parcheados y disponer de software estándar de firewall y antivirus. Los servidores de infraestructura críticos para la seguridad deben mantenerse en una ubicación físicamente segura, prestando atención al cifrado de disco y a las opciones de mantenimiento de máquinas virtuales.

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

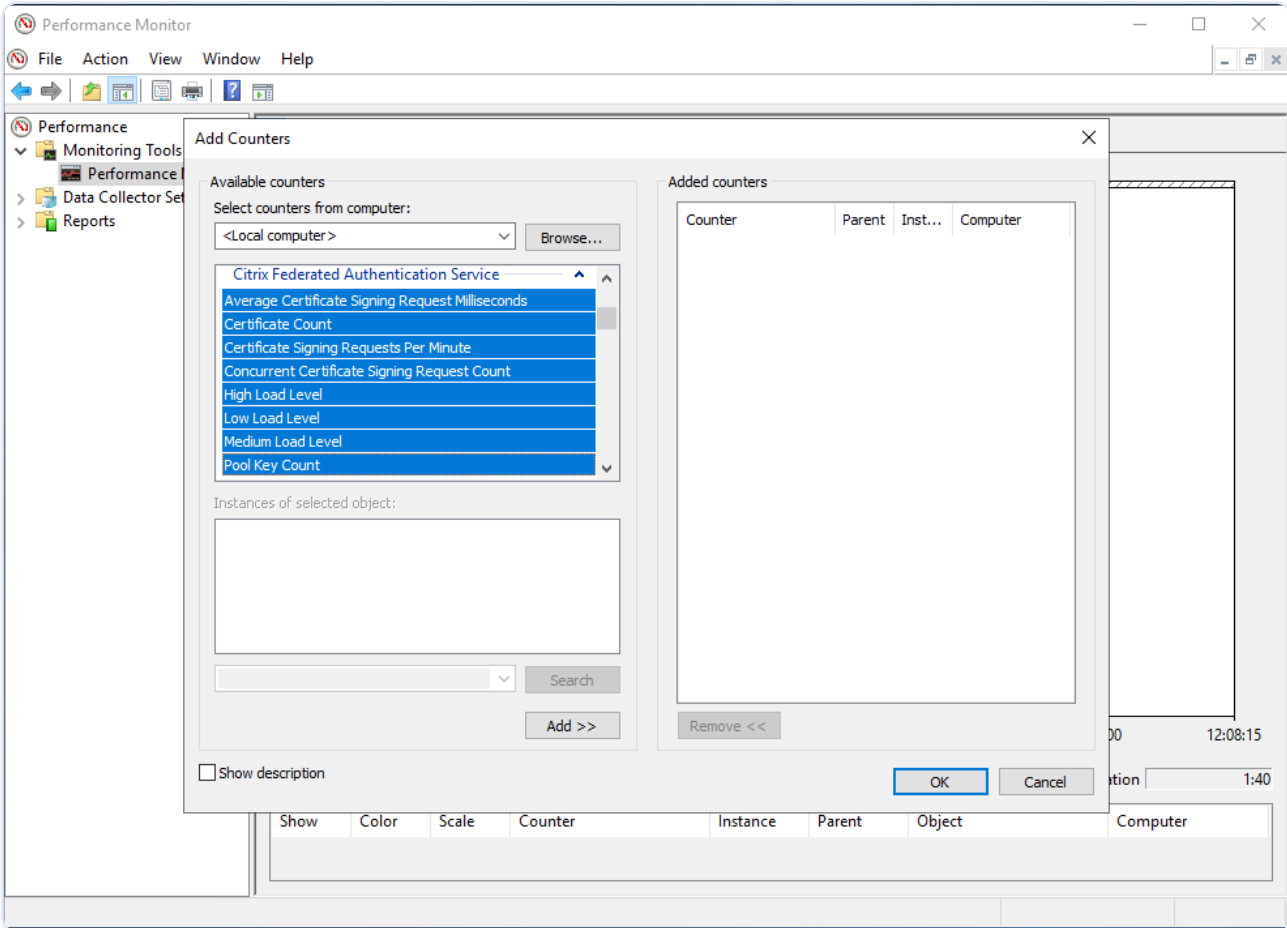
El acceso RDP debe limitarse a los administradores autorizados. Citrix recomienda el inicio de sesión con tarjeta inteligente para las cuentas de usuario, especialmente para las cuentas de autoridad de certificación y de administrador de dominio.

## Información relacionada

- (</es-es/federated-authentication-service/2308/install-configure.html>) es la referencia principal para la instalación y configuración de FAS.
- Las arquitecturas de FAS se presentan en el artículo (</es-es/federated-authentication-service/2308/deployment-architectures.html>).
- Otros artículos prácticos se presentan en el artículo (</es-es/federated-authentication-service/2308/config-manage.html>).

## Contadores de rendimiento

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



La siguiente tabla enumera los contadores disponibles. A menos que se indique lo contrario, cada contador se actualiza cada 10 segundos.

| NOMBRE                                                        | DESCRIPCIÓN                                                                                                                                                          |
|---------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Promedio de milisegundos de solicitud de firma de certificado | La duración promedio (en milisegundos) de las solicitudes de firma de certificado, calculada a partir de los datos del minuto anterior.                              |
| Recuento de certificados                                      | El número de certificados gestionados por el Servicio de autenticación federada.                                                                                     |
| Solicitudes de firma de certificado por minuto                | El número de solicitudes de firma de certificado emitidas por el Servicio de autenticación federada por minuto, calculado a partir de los datos del minuto anterior. |
| Recuento de solicitudes de firma de certificado simultáneas   | El número de solicitudes de firma de certificado simultáneas que está atendiendo el Servicio de autenticación federada.                                              |

| NOMBRE                                  | DESCRIPCIÓN                                                                                                                                                                                                                                                                                                                                          |
|-----------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Recuento de claves de grupo             | El número de pares de claves pregenerados en el grupo de claves que se pueden utilizar para las solicitudes de firma de certificados.                                                                                                                                                                                                                |
| Operaciones de clave privada por minuto | El número de operaciones de clave privada de certificado que el Servicio de autenticación federada realiza por minuto, calculado a partir de los datos del minuto anterior.                                                                                                                                                                          |
| Recuento de sesiones                    | El número de sesiones VDA que el Servicio de autenticación federada está rastreando.                                                                                                                                                                                                                                                                 |
| Nivel de carga bajo/medio/alto          | Estimaciones de la carga que el Servicio de autenticación federada puede aceptar en términos de solicitudes de firma de certificados por minuto. Las estimaciones se actualizan cada minuto, utilizando datos del minuto anterior. Superar el umbral de "carga alta" puede provocar que fallen los inicios de aplicaciones o escritorios publicados. |

## Solucionar problemas de inicio de sesión de Windows

Este artículo describe los registros y mensajes de error que Windows proporciona cuando un usuario inicia sesión utilizando certificados, tarjetas inteligentes o ambos. Estos registros proporcionan información que puede utilizar para solucionar errores de autenticación.

### Certificados e infraestructura de clave pública

Windows Active Directory mantiene varias tiendas de certificados que administran certificados para los usuarios que inician sesión.

- **Almacén de certificados NTAAuth:** Para autenticarse en Windows, la autoridad de certificación que emite inmediatamente los certificados de usuario (es decir, no se admite el encadenamiento) debe colocarse en el almacén NTAAuth. Para ver estos certificados, desde el programa certutil, introduzca: `certutil -viewstore -enterprise NTAAuth`
- **Almacenes de certificados raíz e intermedios:** Por lo general, los sistemas de inicio de sesión con certificados solo pueden proporcionar un único certificado, por lo que si se utiliza una cadena, el almacén de certificados intermedios en todas las máquinas debe incluir estos

certificados. El certificado raíz debe estar en el Almacén de raíces de confianza, y el penúltimo certificado debe estar en el almacén NTAuth.

- **Extensiones de certificado de inicio de sesión y Directiva de grupo:** Windows se puede configurar para aplicar la verificación de EKUs y otras políticas de certificado. Consulte la documentación de Microsoft: [https://docs.microsoft.com/es-es/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/ff404287\(v=ws.10\)>](https://docs.microsoft.com/es-es/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/ff404287(v=ws.10)>).

| POLÍTICA DE REGISTRO                               | DESCRIPCIÓN                                                                                                                                                                                  |
|----------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AllowCertificatesWithNoEKU                         | Cuando está deshabilitado, los certificados deben incluir el uso de clave extendido (EKU) de inicio de sesión con tarjeta inteligente.                                                       |
| AllowSignatureOnlyKeys                             | De forma predeterminada, Windows filtra las claves privadas de los certificados que no permiten el descifrado RSA. Esta opción anula ese filtro.                                             |
| AllowTimeInvalidCertificates                       | De forma predeterminada, Windows filtra los certificados caducados. Esta opción anula ese filtro.                                                                                            |
| EnumerateECCerts                                   | Habilita la autenticación de curva elíptica.                                                                                                                                                 |
| X509HintsNeeded                                    | Si un certificado no contiene un nombre principal de usuario (UPN) único, o es ambiguo, esta opción permite a los usuarios especificar manualmente su cuenta de inicio de sesión de Windows. |
| UseCachedCRLOnlyAnd, IgnoreRevocationUnknownErrors | Deshabilita la comprobación de revocación (establecida en el controlador de dominio).                                                                                                        |

- **Certificados de controlador de dominio:** Para autenticar las conexiones Kerberos, todos los servidores deben tener los certificados de "Controlador de dominio" adecuados. Estos se pueden solicitar utilizando el menú del complemento MMC "Almacén personal de certificados del equipo local".

## Asignación de nombres UPN y certificados

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

## Nombres UPN en Active Directory

De forma predeterminada, cada usuario en Active Directory tiene un UPN implícito basado en el patrón `<samUsername>@<domainNetBios>` y `<samUsername>@<domainFQDN>`. Los dominios y FQDN disponibles se incluyen en la entrada RootDSE del bosque. Un único dominio puede tener varias direcciones FQDN registradas en el RootDSE.

Además, cada usuario en Active Directory tiene un UPN explícito y `altUserPrincipalNames`. Estas son entradas LDAP que especifican el UPN para el usuario.

Al buscar usuarios por UPN, Windows busca primero en el dominio actual (basado en la identidad del proceso que busca el UPN) los UPN explícitos y luego los UPN alternativos. Si no hay coincidencias, busca el UPN implícito, que puede resolverse en diferentes dominios del bosque.

## Servicio de asignación de certificados

Si un certificado no incluye un UPN explícito, Active Directory tiene la opción de almacenar un certificado público exacto para cada uso en un atributo "x509certificate". Para resolver dicho certificado a un usuario, un equipo puede consultar este atributo directamente (por defecto, en un único dominio).

Se proporciona una opción para que el usuario especifique una cuenta de usuario que acelera esta búsqueda y también permite que esta función se utilice en un entorno entre dominios.

Si hay varios dominios en el bosque y el usuario no especifica explícitamente un dominio, el rootDSE de Active Directory especifica la ubicación del Servicio de Asignación de Certificados. Este se encuentra en una máquina de catálogo global y tiene una vista en caché de todos los atributos de certificado x509 en el bosque. Este equipo se puede utilizar para encontrar eficientemente una cuenta de usuario en cualquier dominio, basándose únicamente en el certificado.

## Controlar la selección del controlador de dominio de inicio de sesión

Cuando un entorno contiene varios controladores de dominio, es útil ver y restringir qué controlador de dominio se utiliza para la autenticación, para que los registros puedan habilitarse y recuperarse.

## Controlar la selección del controlador de dominio

Para forzar a Windows a usar un controlador de dominio de Windows específico para el inicio de sesión, puede establecer explícitamente la lista de controladores de dominio que utiliza una máquina Windows configurando el archivo `lmhosts`: `\Windows\System32\drivers\etc\lmhosts`.

Normalmente hay un archivo de ejemplo llamado "lmhosts.sam" en esa ubicación. Simplemente incluya una línea:

```
1.2.3.4 dcnetbiosname #Preferido #Dominio:mydomaini
```

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

Después de un reinicio, la máquina Windows utiliza esa información para iniciar sesión en mydomain. Esta configuración debe revertirse cuando la depuración haya finalizado.

## Identificar el controlador de dominio en uso

Al iniciar sesión, Windows establece una variable de entorno MSDOS con el controlador de dominio que inició la sesión del usuario. Para ver esto, inicie el símbolo del sistema con el comando: **echo %LOGONSERVER%**.

Los registros relacionados con la autenticación se almacenan en el equipo devuelto por este comando.

## Habilitar eventos de auditoría de cuenta

De forma predeterminada, los controladores de dominio de Windows no habilitan los registros completos de auditoría de cuentas. Esto se puede controlar a través de las directivas de auditoría en la configuración de seguridad del editor de directivas de grupo. Para abrir el editor de directivas de grupo, ejecute `gpedit.msc` en el controlador de dominio. Una vez habilitadas las directivas de auditoría, el controlador de dominio produce información adicional de registro de eventos en el registro de seguridad.

Habilitar eventos de auditoría de cuenta(</en-us/federated-authentication-service/2308/media/fas-troubleshoot-logon-auditpolicy.png>)

## Registros de validación de certificados

### Comprobar la validez del certificado

Si un certificado de tarjeta inteligente se exporta como un certificado DER (no se requiere clave privada), puede validarlo con el comando: `certutil -verificar user.cer`

### Habilitar el registro de CAPI

En el controlador de dominio y en la máquina de los usuarios, abra el visor de eventos y habilite el registro para Microsoft/Windows/CAPI2/Operational Logs.

En el controlador de dominio y en la máquina VDA, abra el visor de eventos y vaya a **Registros de aplicaciones y servicios > Microsoft > Windows > CAPI2 > Operational**. Haga clic con el botón derecho en **Operational** y seleccione **Habilitar registro**.

Además, ajuste el registro de CAPI con los valores del registro en:

`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\crypt32`. Los siguientes valores no existen de forma predeterminada, debe crearlos. Elimine los valores si desea volver a la configuración de registro de CAPI2 predeterminada.

| VALOR                       | DESCRIPCIÓN                                            |
|-----------------------------|--------------------------------------------------------|
| DiagLevel (DWORD)           | Nivel de detalle (0 a 5)                               |
| DiagMatchAnyMask (QUADWORD) | Filtro de eventos (use 0xffffffff para todos)          |
| DiagProcessName (MULTI_SZ)  | Filtrar por nombre de proceso (por ejemplo, LSASS.exe) |

## Registros CAPI

| MENSAJE                      | DESCRIPCIÓN                                                                                                                                  |
|------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------|
| Crear cadena                 | LSA llamó a CertGetCertificateChain (incluye el resultado)                                                                                   |
| verificar Revocación         | LSA llamó a CertVerifyRevocation (incluye el resultado)                                                                                      |
| Objetos X509                 | En modo detallado, los certificados y las listas de revocación de certificados (CRL) se vuelcan en<br>AppData\LocalLow\Microsoft\X509Objects |
| verificar Política de cadena | LSA llamó a CertVerifyChainPolicy (incluye parámetros)                                                                                       |

## Mensajes de error

| CÓDIGO DE ERROR          | DESCRIPCIÓN                                                                                      |
|--------------------------|--------------------------------------------------------------------------------------------------|
| Certificado no confiable | No se pudo construir el certificado de la tarjeta inteligente utilizando los certificados de los |

| CÓDIGO DE ERROR                                    | DESCRIPCIÓN                                                                                                                                                                                                                                                                                                                                     |
|----------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                    | almacenes de certificados raíz intermedios y de confianza del equipo.                                                                                                                                                                                                                                                                           |
| Error de comprobación de revocación de certificado | No se pudo descargar la CRL de la tarjeta inteligente desde la dirección especificada por el punto de distribución de CRL del certificado. Si la comprobación de revocación es obligatoria, esto impide que el inicio de sesión se realice correctamente. Consulte la sección <a href="#">Infraestructura de clave pública y certificados</a> . |
| Errores de uso del certificado                     | El certificado no es adecuado para el inicio de sesión. Por ejemplo, podría ser un certificado de servidor o un certificado de firma.                                                                                                                                                                                                           |

## Registros de Kerberos

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

| SUBÁRBOL                                          | 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          |

Los registros de Kerberos se envían al registro de eventos del sistema.

- Los mensajes como "certificado no fiable" deberían ser fáciles de diagnosticar.
- Hay dos códigos de error informativos que se pueden ignorar sin problemas:
  - KDC\_ERR\_PREAUTH\_REQUIRED (utilizado para la compatibilidad con versiones anteriores de controladores de dominio)

- Error desconocido 0x4b

## Registros del controlador de dominio y de la estación de trabajo

Esta sección describe las entradas de registro esperadas en el controlador de dominio y la estación de trabajo cuando el usuario inicia sesión con un certificado.

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

### Registro CAPI2 del controlador de dominio

Durante un inicio de sesión, el controlador de dominio valida el certificado del emisor, lo que produce una secuencia de entradas de registro con el siguiente formato.

| 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 mensaje final del registro de eventos muestra que lsass.exe en el controlador de dominio construye una cadena basada en el certificado proporcionado por el VDA y la verifica para comprobar su validez (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, siendo el evento clave el 4768, donde el certificado se utiliza para emitir el Ticket de concesión de tickets de Kerberos (krbtgt).

Los mensajes anteriores a este muestran la cuenta de máquina del servidor autenticándose en el controlador de dominio. Los mensajes posteriores a este muestran la cuenta de usuario perteneciente al nuevo krbtgt que se utiliza para autenticarse en el controlador de dominio.

| Keywords      | Date and Time       | Source            | Event ID | Task Category                      |
|---------------|---------------------|-------------------|----------|------------------------------------|
| Audit Success | 21/06/2016 15:14:56 | Security-Auditing | 4624     | Logon                              |
| Audit Success | 21/06/2016 15:14:56 | Security-Auditing | 4624     | Logon                              |
| Audit Success | 21/06/2016 15:14:54 | Security-Auditing | 4769     | Kerberos Service Ticket Operations |
| Audit Success | 21/06/2016 15:14:54 | Security-Auditing | 4768     | Kerberos Authentication Service    |
| Audit Success | 21/06/2016 15:14:54 | Security-Auditing | 4769     | Kerberos Service Ticket Operations |
| Audit Success | 21/06/2016 15:14:54 | Security-Auditing | 4634     | Logoff                             |
| Audit Success | 21/06/2016 15:14:54 | Security-Auditing | 4624     | Logon                              |
| Audit Success | 21/06/2016 15:14:54 | Security-Auditing | 4624     | Logon                              |

**Event 4768, Security-Auditing**

General Details

☒ Friendly View
☐ XML View

**+ System**

**- EventData**

**TargetUserName** fred

**TargetDomainName** CITRIXTEST.NET

**TargetSid** S-1-5-21-390731715-1143989709-1377117006-1106

**ServiceName** krbtgt

**ServiceSid** S-1-5-21-390731715-1143989709-1377117006-502

**TicketOptions** 0x40810010

**Status** 0x0

**TicketEncryptionType** 0x12

**PreAuthType** 16

**IpAddress** ::ffff:192.168.0.10

**IpPort** 49348

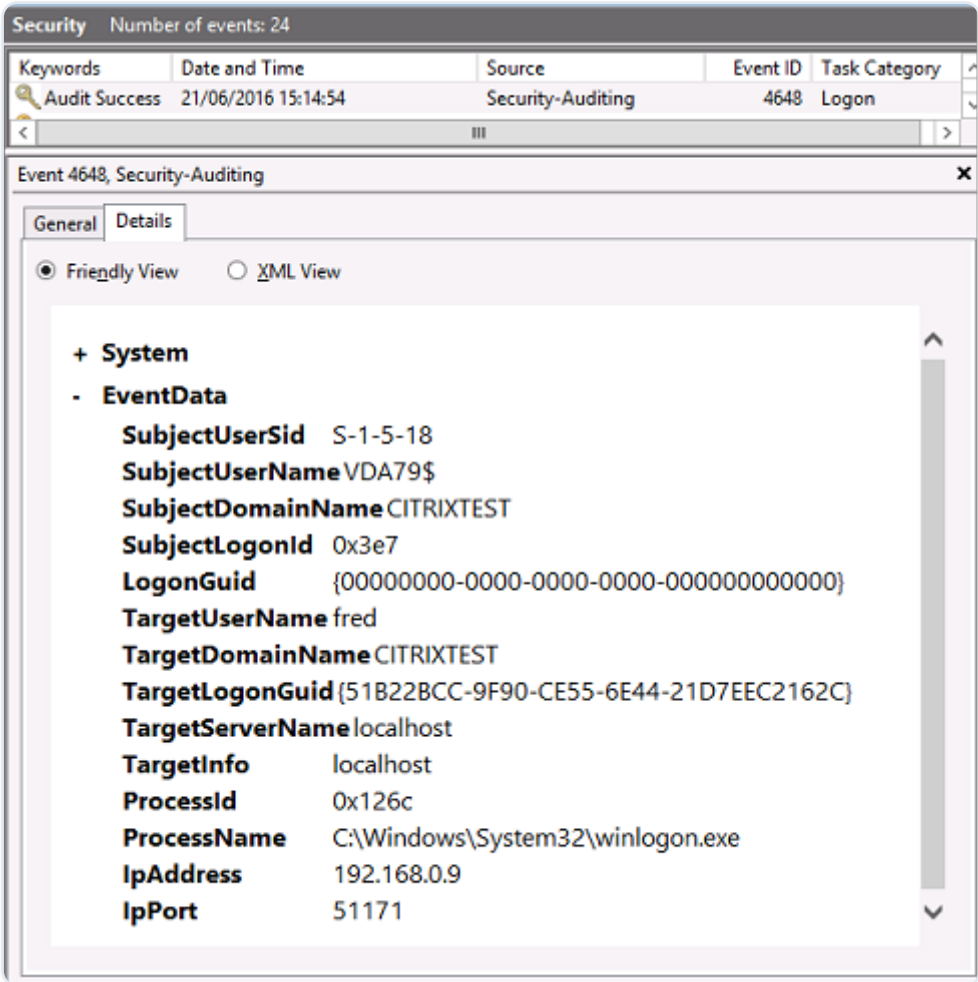
**CertIssuerName** citrixtest-DC-CA

**CertSerialNumber** 5F0001D1FCA2AC30F36879CEEC00000001D1FC

**CertThumbprint** 23BC65AFB7F18787ADAAAD5CEF09CC7505C4176F

## Registro de seguridad del VDA

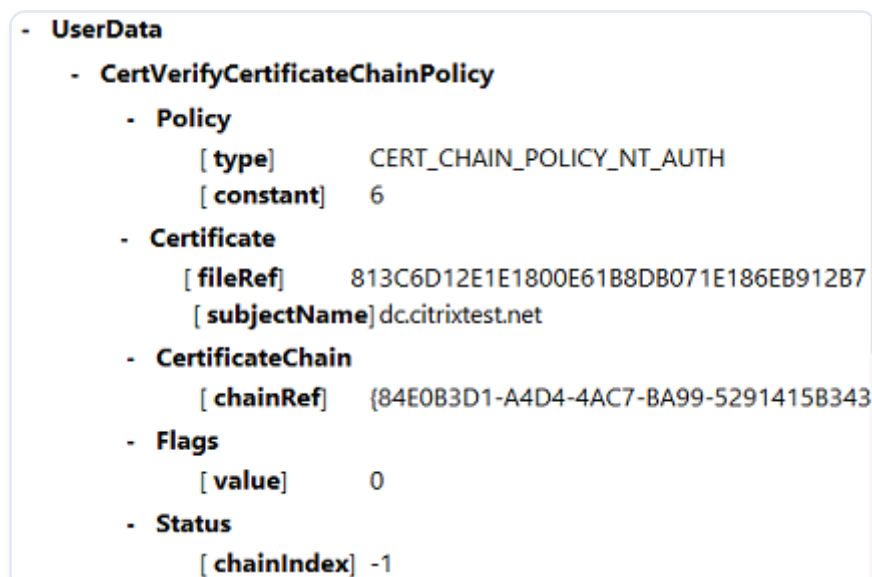
Los registros de auditoría de seguridad de VDA correspondientes al evento de inicio de sesión son la entrada con el ID de evento 4648, originada en winlogon.exe.



### Registro CAPI de VDA

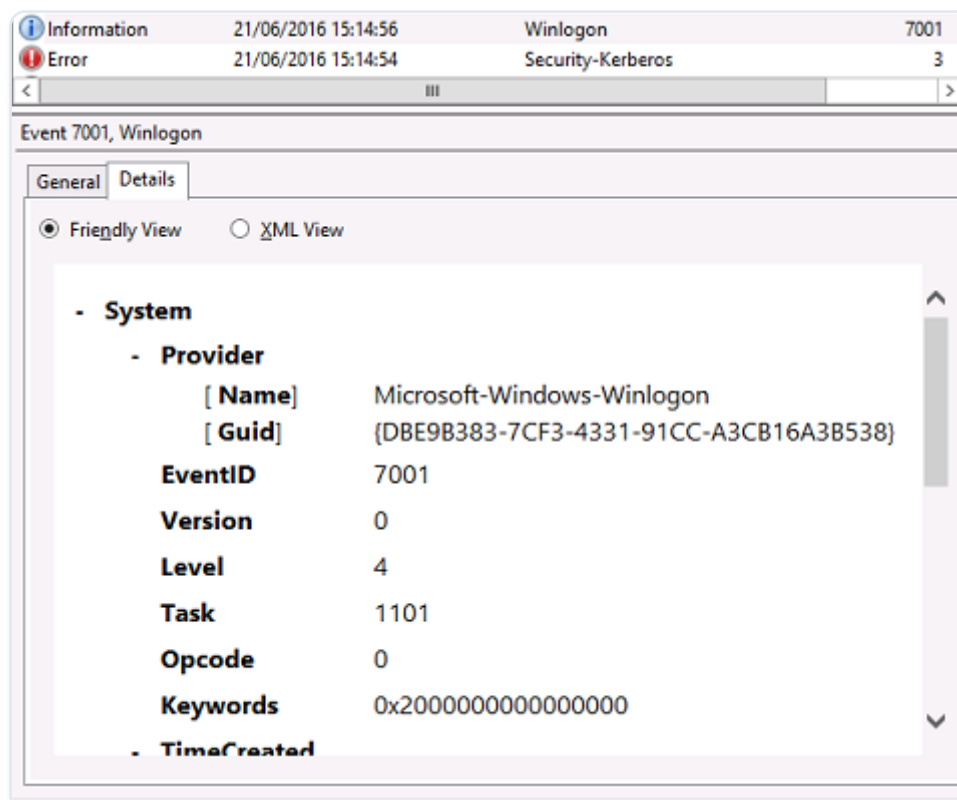
Este registro CAPI de VDA de ejemplo muestra una única secuencia de creación y verificación de cadena desde lsass.exe, validando el certificado del controlador de dominio (dc.citrixtest.net).

|             |                     |       |    |                   |
|-------------|---------------------|-------|----|-------------------|
| Information | 21/06/2016 15:14:54 | CAPI2 | 30 | Verify Chain P... |
| Information | 21/06/2016 15:14:54 | CAPI2 | 11 | Build Chain       |
| Information | 21/06/2016 15:14:54 | CAPI2 | 90 | X509 Objects      |
| Information | 21/06/2016 15:14:54 | CAPI2 | 41 | Verify Revocat... |
| Information | 21/06/2016 15:14:54 | CAPI2 | 40 | Verify Revocat... |
| Information | 21/06/2016 15:14:54 | CAPI2 | 10 | Build Chain       |



## Registro del sistema de VDA

Cuando el registro de Kerberos está habilitado, el Registro del sistema muestra el error KDC\_ERR\_PREAUTH\_REQUIRED (que se puede ignorar) y una entrada de Winlogon que indica que el inicio de sesión de Kerberos fue correcto.



## Supervisión de FAS mediante el registro de eventos de Windows

Todos los eventos de FAS se escriben en el registro de eventos de la aplicación de Windows. Puede utilizar productos como System Center Operations Manager (SCOM) para supervisar el estado de su servicio FAS mediante los procesos y eventos descritos aquí.

## ¿Se está ejecutando el servicio FAS?

Para determinar si el servicio FAS se está ejecutando, supervise el proceso Citrix.Authentication.FederatedAuthenticationService.exe.

En esta sección solo se describen los eventos más importantes para supervisar el servicio FAS. Para obtener la lista completa de códigos de eventos de FAS, consulte [Registros de eventos de FAS](#).

## Eventos de estado de FAS

Los siguientes eventos muestran si su servicio FAS está en buen estado.

El origen del evento es **Citrix.Authentication.FederatedAuthenticationService**.

| EVENTO | TEXTO DEL EVENTO                                                            | EXPLICACIÓN                                                                                                        | NOTAS                                                                                                    |
|--------|-----------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------|
| [S003] | Administrador [{0}] configurando el modo de mantenimiento en [{1}]          | El servicio FAS se puso en modo de mantenimiento o se sacó de él.                                                  | Mientras está en modo de mantenimiento, el servidor FAS no se puede usar para el inicio de sesión único. |
| [S022] | Administrador [{0}] configurando el modo de mantenimiento en Desactivado    | El servicio FAS se sacó del modo de mantenimiento.                                                                 | Disponible a partir de FAS 10.7 / Citrix Virtual Apps and Desktops 2109.                                 |
| [S023] | Administrador [{0}] estableciendo el modo de mantenimiento en Activado      | El servicio FAS se puso en modo de mantenimiento.                                                                  | Disponible a partir de FAS 10.7 / Citrix Virtual Apps and Desktops 2109.                                 |
| [S123] | No se pudo emitir un certificado para [upn: {0} role: {1}] [exception: {2}] | Este evento ocurre después de [S124] si ninguna de las CA con las que FAS está configurado emitió correctamente un | Este evento indica que todas las CA configuradas no funcionan. Si FAS está configurado para usar un HSM, |

| EVENTO | TEXTO DEL EVENTO                                                                                            | EXPLICACIÓN                                                                                                                                                                                                                      | NOTAS                                                                                                                                                                                                                                    |
|--------|-------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|        |                                                                                                             | certificado de usuario. El inicio de sesión único fallará para ese usuario.                                                                                                                                                      | también puede indicar que el HSM no funciona.                                                                                                                                                                                            |
| [S124] | No se pudo emitir un certificado para [upn: {0} role: {1}] en [certificate authority: {2}] [exception: {3}] | Se produjo un error cuando FAS intentó solicitar un certificado de usuario a la CA dada. Si FAS está configurado con más de una CA, FAS intenta la solicitud en otra CA.                                                         | Este evento puede indicar que la CA no funciona o no es contactable. Si FAS está configurado para usar un HSM, también puede indicar que el HSM no funciona. La excepción se puede usar para ayudar a identificar la causa del problema. |
| [S413] | El certificado de autorización caduca pronto ({0} días restantes). Detalles del certificado: {1}            | Este evento se genera periódicamente cuando el certificado de autorización de FAS está cerca de caducar. Por defecto, el evento se genera cada día si el certificado de autorización está dentro de los 30 días de su caducidad. | La configuración predeterminada se puede ajustar usando el cmdlet <b>Set-FasRaCertificateMonitor</b> ; consulte <a href="#">cmdlets de PowerShell</a> .                                                                                  |
| [S414] | El certificado de autorización ha caducado. Detalles del certificado: {0}                                   | Este evento se genera periódicamente cuando el certificado de autorización de FAS ha caducado. De forma                                                                                                                          | Una vez caducado, FAS no puede generar nuevos certificados de usuario y el inicio de sesión único empieza a fallar.                                                                                                                      |

| EVENTO | TEXTO DEL EVENTO | EXPLICACIÓN                                         | NOTAS |
|--------|------------------|-----------------------------------------------------|-------|
|        |                  | predeterminada, el evento se genera todos los días. |       |

## Eventos de FAS conectados a la nube

Si utiliza FAS con Citrix Cloud™, los siguientes eventos muestran si su servicio FAS está en buen estado.

El origen del evento es **Citrix.Fas.Cloud**.

| EVENTO | TEXTO DEL EVENTO                                                                                                                                          | EXPLICACIÓN                                                                                                                                                                                      | NOTAS                                                                                                                                                                                                                                                                                                                          |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [S012] | El servicio FAS está disponible para el inicio de sesión único desde Citrix Cloud                                                                         | Este evento indica que el inicio de sesión único desde Workspace (es decir, Citrix Cloud) debería funcionar.                                                                                     | Antes de emitir este evento, FAS comprueba (1) que está configurado, (2) que no está en modo de mantenimiento y (3) que está conectado a Citrix Cloud.                                                                                                                                                                         |
| [S013] | El servicio FAS no está disponible para el inicio de sesión único desde Citrix Cloud. [{0}] Puede encontrar más detalles en la consola de administración. | Este evento indica que FAS no puede proporcionar inicio de sesión único desde Workspace (es decir, Citrix Cloud). El mensaje incluye el motivo por el que el inicio de sesión único no funciona. | FAS mantiene una conexión persistente con Citrix Cloud. De vez en cuando, esta conexión puede terminar por varias razones (como un fallo de red o una política de duración de la conexión en un servidor proxy). Cuando esto ocurre, el texto del evento contiene "El servicio no está conectado a la nube". <b>Este es un</b> |

| EVENTO | TEXTO DEL EVENTO | EXPLICACIÓN | NOTAS                                                                                                 |
|--------|------------------|-------------|-------------------------------------------------------------------------------------------------------|
|        |                  |             | <b>comportamiento normal, y FAS intenta inmediatamente restablecer una conexión con Citrix Cloud.</b> |

## Eventos de seguridad

Los siguientes eventos indican que una entidad no autorizada intentó usar FAS.

El origen del evento es **Citrix.Authentication.FederatedAuthenticationService**.

| EVENTO | TEXTO DEL EVENTO                                                              | EXPLICACIÓN                                                                                                                                                                                                                                                              |
|--------|-------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [S001] | ACCESO DENEGADO: El usuario [{0}] no es miembro del grupo de administradores  | Se intentó ver o cambiar la configuración de FAS, pero el autor de la llamada no era un administrador de FAS.                                                                                                                                                            |
| [S002] | ACCESO DENEGADO: El usuario [{0}] no es administrador del rol [{1}]           | Se intentó ver o cambiar la configuración de una regla de FAS, pero el autor de la llamada no era un administrador de FAS.                                                                                                                                               |
| [S101] | El servidor [{0}] no está autorizado para afirmar identidades en el rol [{1}] | Se intentó afirmar identidades de usuario, pero el autor de la llamada no tiene permiso para hacerlo. Solo los servidores StoreFront™ que se hayan permitido en la configuración de la regla de FAS (y Workspace, si corresponde) pueden afirmar identidades de usuario. |

| EVENTO | TEXTO DEL EVENTO                                                                                                             | EXPLICACIÓN                                                                                                                          |
|--------|------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------|
| [S104] | El servidor [{0}] no pudo afirmar el UPN [{1}] (UPN no permitido por el rol [{2}])                                           | Se intentó afirmar una identidad de usuario, pero la cuenta del usuario no está permitida según la configuración de la regla de FAS. |
| [S205] | Acceso denegado a la parte de confianza: la cuenta de llamada [{0}] no es una parte de confianza permitida de la regla [{1}] | Un VDA intentó realizar un inicio de sesión único con FAS, pero el VDA no está permitido según la configuración de la regla de FAS.  |

## Registros de eventos de FAS

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

### Eventos de administración

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

| CÓDIGOS DE REGISTRO                                                                                                      |
|--------------------------------------------------------------------------------------------------------------------------|
| [S001] ACCESO DENEGADO: El usuario [{0}] no es miembro del grupo de administradores                                      |
| [S002] ACCESO DENEGADO: El usuario [{0}] no es administrador del rol [{1}]                                               |
| [S003] El administrador [{0}] establece el modo de mantenimiento en [{1}]                                                |
| [S004] El administrador [{0}] solicita un certificado de autorización a la CA [{1}] usando las plantillas [{2}] and {3}] |
| [S005] El administrador [{0}] desautoriza la CA [{1}]                                                                    |
| [S006] El administrador [{0}] crea la definición de certificado [{1}]                                                    |
| [S007] El administrador [{0}] actualiza la definición de certificado [{1}]                                               |
| [S008] El administrador [{0}] elimina la definición de certificado [{1}]                                                 |

| CÓDIGOS DE REGISTRO                                                                                                                       |
|-------------------------------------------------------------------------------------------------------------------------------------------|
| [S009] El administrador [{0}] crea la regla [{1}]                                                                                         |
| [S010] El administrador [{0}] actualiza la regla [{1}]                                                                                    |
| [S011] El administrador [{0}] elimina la regla [{1}]                                                                                      |
| [S012] El administrador [{0}] crea el certificado [upn: {1} sid: {2} rule: {3}]Definición de certificado: {4} Contexto de seguridad: {5}] |
| [S013] El administrador [{0}] elimina los certificados [upn: {1} role: {2} Certificate Definition: {3} Security Context: {4}]             |
| [S015] El administrador [{0}] crea la solicitud de certificado [TPM: {1}]                                                                 |
| [S016] Administrador [{0}] importando certificado de autorización [Reference: {1}]                                                        |
| [S022] Administrador [{0}] estableciendo el modo de mantenimiento en Desactivado                                                          |
| [S023] Administrador [{0}] estableciendo el modo de mantenimiento en Activado                                                             |
| [S024] Administrador [{0}] configurando el monitor de estado del sistema                                                                  |
| [S025] Administrador [{0}] configurando el monitor de estado del sistema                                                                  |
| [S026] Administrador [{0}] configurando el monitor de certificados RA                                                                     |
| [S027] Administrador [{0}] restableciendo el monitor de certificados RA                                                                   |
| [S050] Administrador [{0}] creando configuración en la nube: [{1}]                                                                        |
| [S051] Administrador [{0}] actualizando configuración en la nube: [{1}]                                                                   |
| [S052] Administrador [{0}] eliminando configuración en la nube                                                                            |
| [S060] Administrador [{0}] Solicitando registro en la nube. Instancia: {1}                                                                |
| [S060] Administrador [{0}] Solicitando registro en la nube de confianza directa. Instancia: {1} CloudServiceUrlFormat: {2}                |
| [S061] Administrador [{0}] Completando el registro en la nube. Ubicación del recurso: {1}, Nombre de la regla: {2}                        |

**CÓDIGOS DE REGISTRO**

[S062] Administrador [{0}] Registro en la nube completado. Ubicación del recurso: {1} ({2}),  
Nombre de la regla: {3}, Cliente: {4} ({5})

[S063] Se produjo un error de KRS durante el registro en la nube. La excepción fue {0}

[S064] Se produjo un error desconocido durante el registro en la nube. La excepción fue {0}

**CÓDIGOS DE REGISTRO**

[S401] Realizando la actualización de la configuración - [From version {0} to version {1}]

[S402] ERROR: El servicio Citrix Federated Authentication Service debe ejecutarse como Network Service [currently running as: {0}]

[S404] Borrando forzosamente la base de datos de Citrix Federated Authentication Service

[S405] Se produjo un error al migrar los datos del registro a la base de datos: [{0}]

[S406] La migración de datos del registro a la base de datos se ha completado (nota: los certificados de usuario no se migran)

[S407] Los datos basados en el registro no se migraron a una base de datos porque ya existía una

[S408] No se puede revertir la configuración -- [From version {0} to version {1}]

[S409] La configuración de ThreadPool se realizó correctamente: MinThreads se ajustó de  
[workers: {0} completion: {1}] a: [workers: {2} completion: {3}]

[S410] La configuración de ThreadPool falló: no se pudo ajustar MinThreads de [workers: {0}  
completion: {1}] a: [workers: {2} completion: {3}]; esto puede afectar la escalabilidad del servidor  
FAS

[S411] Error al iniciar el servicio FAS: [{0}]

[S412] Actualización de la configuración completada -- [From version {0} to version {1}]

[S413] El certificado de autorización caducará pronto (quedan {0} días). Detalles del certificado: {1}

[S414] El certificado de autorización ha caducado. Detalles del certificado: {0}

**CÓDIGOS DE REGISTRO**

[S415] Las comprobaciones del certificado de autorización se han completado. Se registraron {0} problemas. La próxima comprobación se realizará en {1}

**Creación de aserciones de identidad**

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

**CÓDIGOS DE REGISTRO**

[S101] El servidor [{0}] no está autorizado para afirmar identidades en el rol [{1}]

[S102] El servidor [{0}] no pudo afirmar el UPN [{1}] (Excepción: {2}{3})

[S103] El servidor [{0}] solicitó el UPN [{1}] SID {2}, pero la búsqueda devolvió el SID {3}

[S104] El servidor [{0}] no pudo afirmar el UPN [{1}] (UPN no permitido por el rol [{2}])

[S105] El servidor [{0}] emitió una aserción de identidad [upn: {1}, rol {2}, Contexto de seguridad: {3}]

[S120] Emisión de certificado a [upn: {0} rol: {1} Contexto de seguridad: [{2}]]

[S121] Certificado emitido a [upn: {0} role: {1}] por [certificate authority: {2}]

[S122] Advertencia: El servidor está sobrecargado [upn: {0} rol: {1}][Solicitudes por minuto {2}].

[S123] No se pudo emitir un certificado para [upn: {0} role: {1}] [exception: {2}]

[S124] No se pudo emitir un certificado para [upn: {0} role: {1}] en [certificate authority: {2}] [exception: {3}]

**Actuando como parte que confía**

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

**CÓDIGOS DE REGISTRO**

[S201] La parte que confía [{0}] no tiene acceso a una contraseña.

| CÓDIGOS DE REGISTRO                                                                                                                                 |
|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| [S202] La parte que confía [{0}] no tiene acceso a un certificado.                                                                                  |
| [S203] La parte que confía [{0}] no tiene acceso al CSP de inicio de sesión                                                                         |
| [S204] Parte que confía [{0}] accediendo al CSP de inicio de sesión para [upn: {1}] en el rol: [{2}] [Operation: {3}] según lo autorizado por [{4}] |
| [S205] Acceso denegado a la parte que confía: la cuenta que realiza la llamada [{0}] no es una parte que confía permitida de la regla [{1}]         |
| [S206] La cuenta que realiza la llamada [{0}] no es una parte que confía                                                                            |
| [S208] La operación de clave privada falló [Operation: {0} upn: {1} role: {2} certificateDefinition {3} Error {4} {5}].                             |

## Servidor de certificados en sesión

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

| CÓDIGOS DE REGISTRO                                                                                                                                                                          |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [S301] Acceso denegado: El usuario [{0}] no tiene acceso a una tarjeta inteligente virtual                                                                                                   |
| [S302] El usuario [{0}] solicitó una tarjeta inteligente virtual desconocida [thumbprint: {1}]                                                                                               |
| [S303] Acceso denegado: El usuario [{0}] no coincide con la tarjeta inteligente virtual [upn: {1}]                                                                                           |
| [S304] El usuario [{0}] ejecuta el programa [{1}] en el equipo [{2}] utilizando la tarjeta inteligente virtual [upn: {3} role: {4} thumbprint: {5}] para la operación de clave privada [{6}] |
| [S305] La operación de clave privada falló [Operation: {0}] [upn: {1} role: {2} containerName {3} Error {4} {5}].                                                                            |

## Complemento de aserción de FAS

Estos eventos son registrados por el complemento de aserción de FAS.

| CÓDIGOS DE REGISTRO                                             |
|-----------------------------------------------------------------|
| [S500] No hay ningún complemento de aserción de FAS configurado |

| CÓDIGOS DE REGISTRO                                                                                                                                          |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [S501] No se pudo cargar el complemento de aserción de FAS configurado [exception:{0}]                                                                       |
| [S502] Complemento de aserción de FAS cargado [pluginId={0}] [assembly={1}] [location={2}]                                                                   |
| [S503] El servidor [{0}] no pudo afirmar el UPN [{1}] (se proporcionó evidencia de inicio de sesión, pero el complemento [{2}] no lo admite)                 |
| [S504] El servidor [{0}] no pudo afirmar el UPN [{1}] (se proporcionó evidencia de inicio de sesión, pero no hay ningún complemento de FAS configurado)      |
| [S505] El servidor [{0}] no pudo afirmar el UPN [{1}] (el complemento [{2}] rechazó la evidencia de inicio de sesión con el estado [{3}] y el mensaje [{4}]) |
| [S506] El complemento [{0}] aceptó la evidencia de inicio de sesión del servidor [{1}] para UPN [{2}] con el mensaje [{3}]                                   |
| [S507] El servidor [{0}] no pudo afirmar el UPN [{1}] (el complemento [{2}] lanzó la excepción [{3}] durante el método [{4}])                                |
| [S507] El servidor [{0}] no pudo afirmar el UPN [{1}] (el complemento [{2}] lanzó la excepción [{3}])                                                        |
| [S508] El servidor [{0}] no pudo afirmar el UPN [{1}] (se proporcionó la disposición de acceso, pero el complemento [{2}] no la admite)                      |
| [S509] El servidor [{0}] no pudo afirmar el UPN [{1}] (se proporcionó la disposición de acceso, pero no hay ningún complemento FAS configurado)              |
| [S510] El servidor [{0}] no pudo afirmar el UPN [{1}] (la disposición de acceso fue considerada no válida por el complemento [{2}])                          |

## FAS habilitado para Workspace

Estos eventos se registran cuando se utiliza FAS con Workspace.

| CÓDIGOS DE REGISTRO                                                                                  |
|------------------------------------------------------------------------------------------------------|
| [S001] Clave de autorización de Citrix Cloud rotada [fas id: {0}] [old key id:{1}] [new key id:{2}]  |
| [S002] El módulo de soporte en la nube se está iniciando. URL del servicio en la nube de FasHub: {0} |
| [S003] FAS registrado en la nube [fas id: {0}] [transaction id: {1}]                                 |

## CÓDIGOS DE REGISTRO

[S004] FAS no pudo registrarse en la nube [fas id: {0}] [transaction id: {1}] [exception: {2}]

[S005] FAS envió su configuración actual a la nube [fas id: {0}] [transaction id: {1}]

[S006] FAS no pudo enviar su configuración actual a la nube [fas id: {0}] [transaction id: {1}] [exception: {2}]

[S007] FAS se ha dado de baja de la nube [fas id: {0}] [transaction id: {1}]

[S009] FAS no pudo darse de baja de la nube [fas id: {0}] [transaction id: {1}] [exception: {2}]

[S010] El servicio FAS está conectado a la URL de mensajería en la nube: {0}

[S011] El servicio FAS no está conectado a la nube

[S012] El servicio FAS está disponible para el inicio de sesión único desde Citrix Cloud

[S013] El servicio FAS no está disponible para el inicio de sesión único desde Citrix Cloud. [{0}] Se pueden encontrar más detalles en la consola de administración

[S014] Una llamada al servicio en la nube <service name> falló [fas id: {0}] [transaction id: {1}] [exception: {2}]

[S015] Se bloqueó un mensaje de Citrix Cloud porque el emisor no tiene permiso [message ID {0}] [transaction ID {1}] [caller {2}]

[S016] Una llamada al servicio en la nube <service name> se realizó correctamente [fas id: {0}] [transaction id: {1}]

[S019] FAS descargó su configuración de la nube [fas id: {0}] [transaction id: {1}]

[S020] FAS no pudo descargar su configuración de la nube [fas id: {0}] [transaction id: {1}] [exception: {2}]

[S021] El módulo de soporte en la nube no pudo iniciarse. Excepción: {0}

[S022] El módulo de soporte en la nube se está deteniendo

[S023] No se pudo rotar la clave de autorización de Citrix Cloud [fas id: {0}] [current key id:{1}] [new key id:{2}] [keys in cloud:{3}]

| CÓDIGOS DE REGISTRO                                                                                                           |
|-------------------------------------------------------------------------------------------------------------------------------|
| [S024] Iniciando la rotación de la clave de autorización de Citrix Cloud [fas id: {0}] [current key id: {1}] [new key id:{2}] |
| [S025] La clave de autorización de este servicio está presente en Citrix Cloud [current key: {0}] [keys in cloud: {1}]        |
| [S026] La clave de autorización de este servicio no está presente en Citrix Cloud [current key: {0}] [keys in cloud: {1}]     |
| [S027] Se actualizó el formato de almacenamiento de la clave de autorización de Citrix Cloud [fas id: {0}]                    |

## Inicio de sesión

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

| CÓDIGOS DE REGISTRO                                                                                                                           |
|-----------------------------------------------------------------------------------------------------------------------------------------------|
| [S101] Error en el inicio de sesión de aserción de identidad. Servicio de autenticación federada no reconocido [id: {0}]                      |
| [S102] Error en el inicio de sesión de aserción de identidad. No se pudo buscar el SID para {0} [Exception: {1}{2}]                           |
| [S103] Error en el inicio de sesión de aserción de identidad. El usuario {0} tiene el SID {1}, se esperaba el SID {2}                         |
| [S104] Error en el inicio de sesión de aserción de identidad. No se pudo conectar al Servicio de autenticación federada: {0} [Error: {1} {2}] |
| [S105] Inicio de sesión de aserción de identidad. Iniciando sesión [Username: {0} Domain: {1}]                                                |
| [S106] Inicio de sesión de aserción de identidad.\n\nServicio de autenticación federada: {0}\n\nIniciando sesión [Certificate: {1}]           |
| [S107] Error en el inicio de sesión de aserción de identidad. [Exception: {0}{1}]                                                             |
| [S108] Subsistema de aserción de identidad. ACCESO_DENEGADO [Caller: {0}]                                                                     |

## Certificados en sesión

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

| CÓDIGOS DE REGISTRO                                                                                                            |
|--------------------------------------------------------------------------------------------------------------------------------|
| [S201] Acceso a tarjeta inteligente virtual autorizado por [{0}] para [PID: {1} Program Name: {2} Certificate thumbprint: {3}] |
| [S203] Subsistema de tarjeta inteligente virtual. Acceso denegado [caller: {0}, session {1}]                                   |
| [S204] Subsistema de tarjeta inteligente virtual. Compatibilidad con tarjeta inteligente inhabilitada                          |

## Solicitud de certificado y generación de par de claves

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

| CÓDIGOS DE REGISTRO                                                                                                                             |
|-------------------------------------------------------------------------------------------------------------------------------------------------|
| [S001] TrustArea::TrustArea: Certificado instalado [TrustArea: {0} Certificate {1} TrustAreaJoinParameters {2}]                                 |
| [S014] Pkcs10Request::Create: Solicitud PKCS10 creada [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 REGISTRO                                                                                                               |
|-----------------------------------------------------------------------------------------------------------------------------------|
| [S104] MicrosoftCertificateAuthority::GetCredentials: Autorizado para usar {0}                                                    |
| [S105] MicrosoftCertificateAuthority::SubmitCertificateRequest Error al enviar la respuesta [{0}]                                 |
| [S106] MicrosoftCertificateAuthority::SubmitCertificateRequest Certificado emitido [{0}]                                          |
| [S112] MicrosoftCertificateAuthority::SubmitCertificateRequest - Esperando aprobación [CR_DISP_UNDER_SUBMISSION] [Reference: {0}] |

## Mensajes de error para el usuario final

Esta sección enumera los mensajes de error comunes que se muestran a 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 tiene un certificado y una clave privada válidos, pero el controlador de dominio de Kerberos ha rechazado la conexión. Consulte la sección <b>Registros de Kerberos</b> de este artículo.                                                                                                                                                                                                                  |
| El sistema no pudo iniciar su sesión. Sus credenciales no pudieron verificarse. / La solicitud no es compatible                           | No se puede contactar con el controlador de dominio, o el controlador de dominio no se ha configurado con un certificado para admitir la autenticación con tarjeta inteligente. Inscriba el controlador de dominio para un certificado de "Autenticación Kerberos", "Autenticación de controlador de dominio" o "Controlador de dominio". Vale la pena intentarlo, incluso cuando el certificado existente parece ser válido. |
| Es posible que el sistema no inicie su sesión. El certificado de tarjeta inteligente utilizado para la autenticación no era de confianza. | Los certificados intermedios y raíz no están instalados en el equipo local. Consulte <a href="#">Certificados e infraestructura de clave pública</a> .                                                                                                                                                                                                                                                                        |
| Solicitud incorrecta                                                                                                                      | Esto suele indicar que las extensiones del certificado no están configuradas correctamente, o que la clave RSA es demasiado corta (<2048 bits).                                                                                                                                                                                                                                                                               |

## Información relacionada

- [Configurar un dominio para el inicio de sesión con tarjeta inteligente](#)
- [Directivas de inicio de sesión con tarjeta inteligente](#)
- [Habilitar el registro de CAPI](#)
- [Habilitar el registro de Kerberos](#)
- [Directrices para habilitar el inicio de sesión con tarjeta inteligente con autoridades de certificación de terceros](#)

## Cmdlets de PowerShell

Puede usar la consola de administración del Servicio de autenticación federada (FAS) para implementaciones sencillas; sin embargo, la interfaz de PowerShell ofrece opciones más avanzadas. Si tiene previsto usar opciones que no están disponibles en la consola, Citrix recomienda usar solo PowerShell para la configuración.

El siguiente comando agrega los cmdlets de PowerShell de FAS:

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

En una ventana de PowerShell, puede usar `Get-Help \<nombre del cmdlet>` para mostrar la ayuda del cmdlet.

Para obtener más información sobre los cmdlets del SDK de PowerShell de FAS, consulte

`<https://developer-docs.citrix.com/projects/federated-authentication-service-powershell-cmdlets/en/latest/>`.

# Arquitecturas de implementación

---

## Introducción

Federated Authentication Service (FAS) es un componente de Citrix® que se integra con la entidad de certificación de Active Directory, lo que permite autenticar a los usuarios sin problemas en un entorno de Citrix. Este documento describe varias arquitecturas de autenticación que pueden ser adecuadas para su implementación.

Cuando está habilitado, FAS delega las decisiones de autenticación de usuario a los servidores StoreFront de confianza. StoreFront tiene un conjunto completo de opciones de autenticación integradas basadas en tecnologías web modernas, y es fácilmente extensible mediante el SDK de StoreFront o complementos de IIS de terceros. El objetivo de diseño básico es que cualquier tecnología de autenticación que pueda autenticar a un usuario en un sitio web ahora se puede usar para iniciar sesión en una implementación de Citrix Virtual Apps o Citrix Virtual Desktops™.

Este documento describe ejemplos de arquitecturas de implementación de nivel superior, en orden creciente de complejidad.

- [Implementación interna](#)
- [Implementación de Citrix Gateway](#)
- [ADFS SAML](#)
- [Asignación de cuentas B2B](#)
- [Unión a Azure AD de Windows 10](#)

Se proporcionan enlaces a artículos relacionados con FAS. Para todas las arquitecturas, el artículo [Instalar y configurar](#) es la referencia principal para configurar FAS.

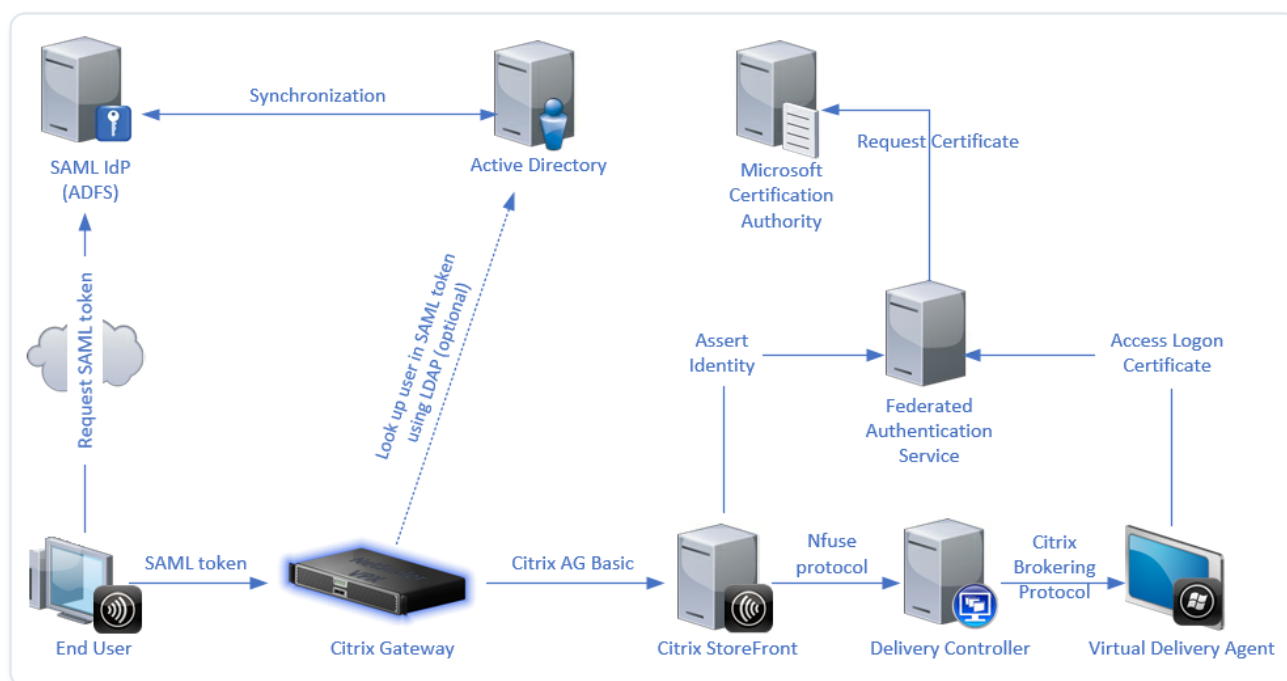
## Descripción general de la arquitectura

FAS está autorizado para emitir certificados de clase de tarjeta inteligente automáticamente en nombre de los usuarios de Active Directory que son autenticados por StoreFront. Esto utiliza API similares a las herramientas que permiten a los administradores aprovisionar tarjetas inteligentes físicas. Cuando un usuario es intermediado a un Virtual Delivery Agent (VDA) de Citrix Virtual

Apps™ o Citrix Virtual Desktops, el certificado se adjunta a la máquina y el dominio de Windows ve el inicio de sesión como una autenticación estándar de tarjeta inteligente.

Los servidores StoreFront™ de confianza se ponen en contacto con FAS cuando los usuarios solicitan acceso al entorno de Citrix. FAS concede un ticket que permite que una única sesión de Citrix Virtual Apps o Citrix Virtual Desktops se autentique con un certificado para esa sesión. Cuando un VDA necesita autenticar a un usuario, se conecta a FAS y canjea el ticket. Solo FAS tiene acceso a la clave privada del certificado de usuario; el VDA debe enviar a FAS cada operación de firma y descifrado que necesite realizar con el certificado.

El siguiente diagrama muestra la integración de FAS con una entidad de certificación de Microsoft y la prestación de servicios de soporte a StoreFront y a los Virtual Delivery Agents (VDA) de Citrix Virtual Apps and Desktops™.



## Implementación interna

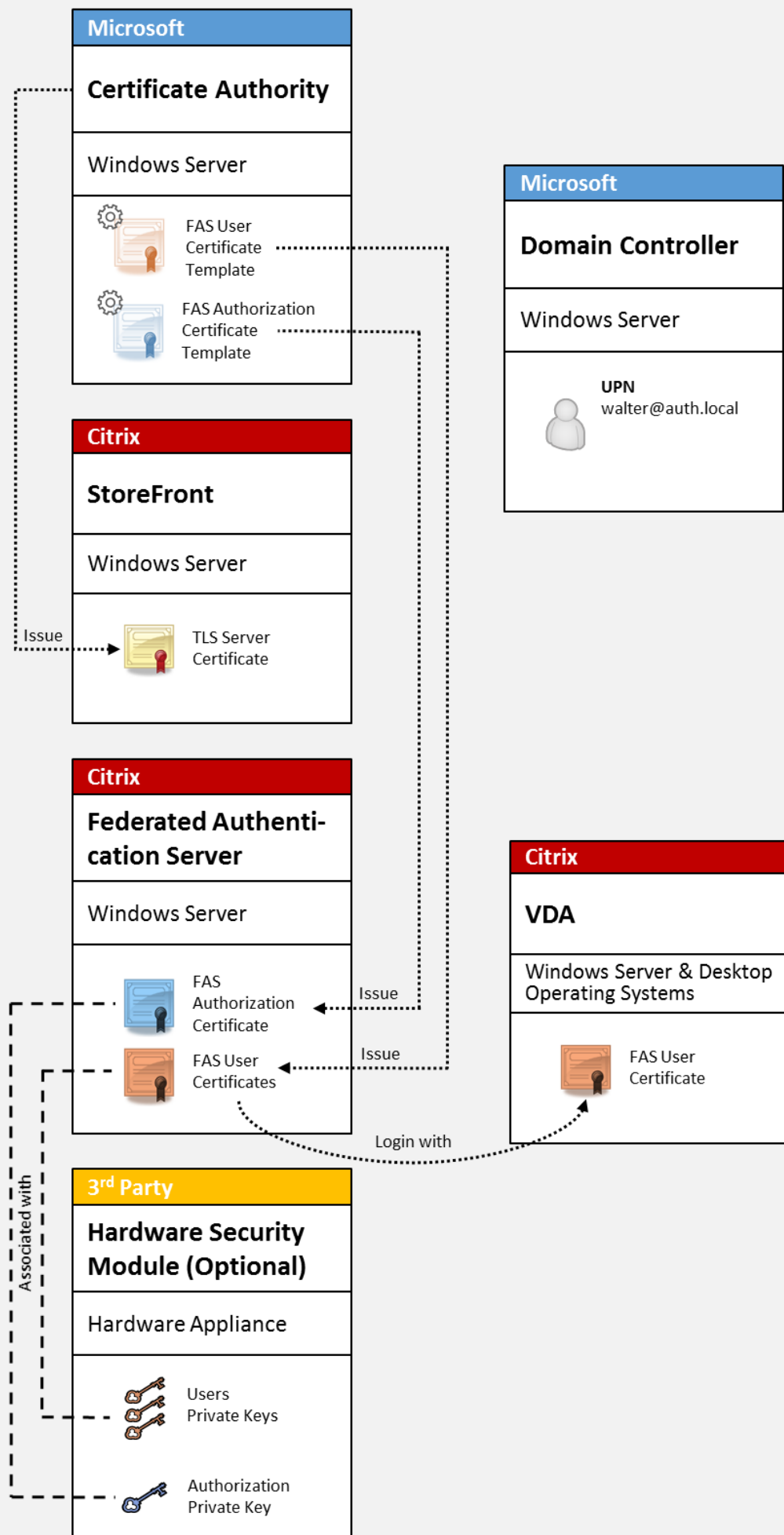
FAS permite a los usuarios autenticarse de forma segura en StoreFront utilizando una variedad de opciones de autenticación (incluido el inicio de sesión único de Kerberos) y conectarse a una sesión de Citrix HDX™ completamente autenticada.

Esto permite la autenticación de Windows sin solicitudes para introducir credenciales de usuario o PIN de tarjeta inteligente, y sin utilizar funciones de "administración de contraseñas guardadas" como el Servicio de inicio de sesión único. Esto se puede utilizar para reemplazar las funciones de inicio de sesión de delegación restringida de Kerberos disponibles 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 o no en los dispositivos de punto final con una tarjeta inteligente. Esto permite una migración fluida a modelos de autenticación de dos factores, incluso desde dispositivos como teléfonos inteligentes y tabletas que no tienen un lector de tarjetas inteligentes.

Esta implementación añade un nuevo servidor que ejecuta FAS, el cual está autorizado para emitir certificados de clase de tarjeta inteligente en nombre de los usuarios. Estos certificados se utilizan luego para iniciar sesión en las sesiones de usuario en un entorno Citrix HDX como si se hubiera utilizado un inicio de sesión con tarjeta inteligente.

## AUTH.LOCAL domain



El entorno de Citrix Virtual Apps o Citrix Virtual Desktops debe configurarse de manera similar al inicio de sesión con tarjeta inteligente, lo cual se documenta en [CTX206156](#).

En una implementación existente, esto generalmente implica solo asegurarse de que una autoridad de certificación de Microsoft unida a un dominio esté disponible y de que a los controladores de dominio se les hayan asignado certificados de controlador de dominio. (Consulte la sección "Emisión de certificados de controlador de dominio" en CTX206156).

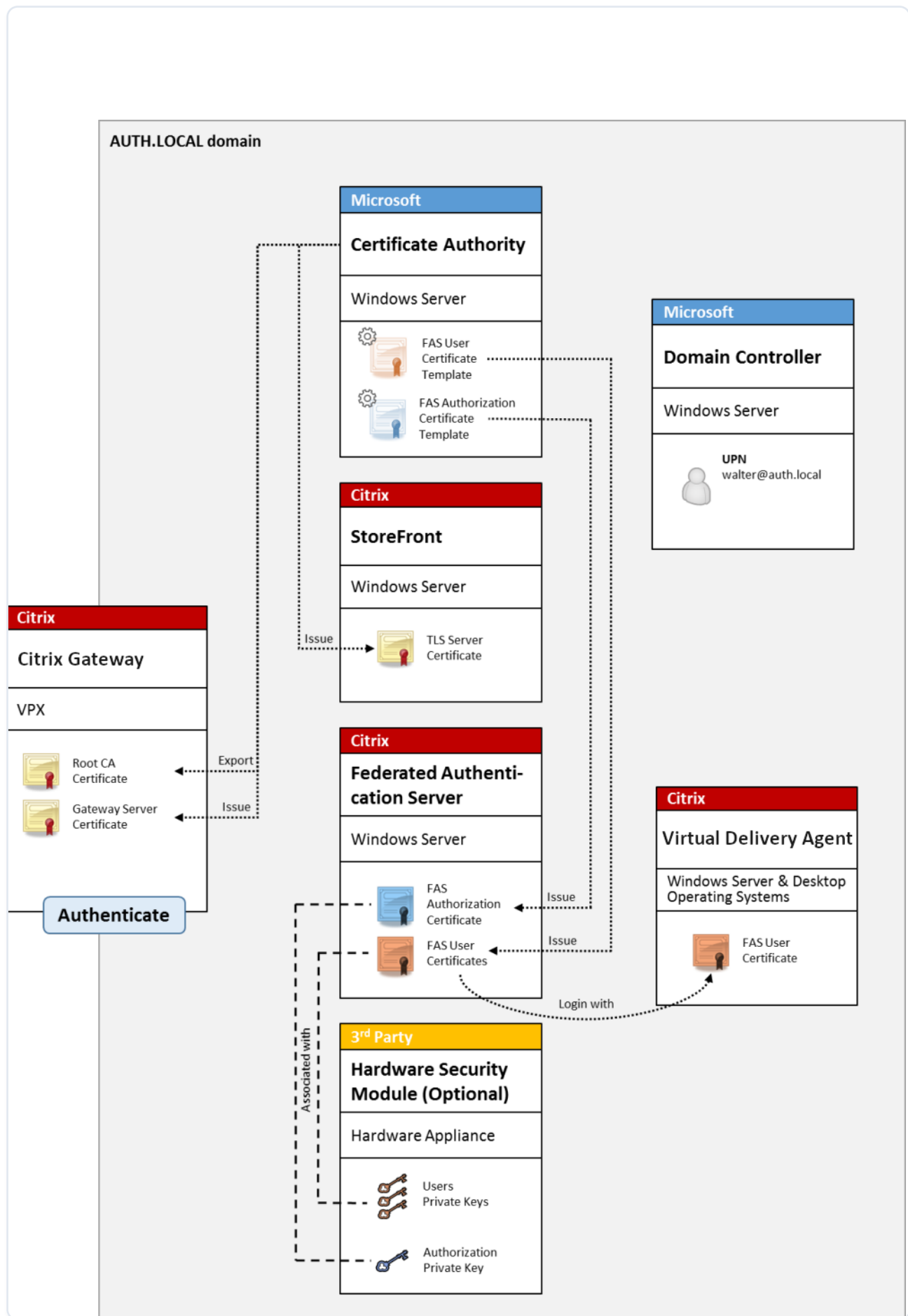
Información relacionada:

- Las claves se pueden almacenar en un Módulo de seguridad de hardware (HSM) o en un Módulo de plataforma segura (TPM) integrado. Para obtener más información, consulte el artículo [Protección de clave privada](#).
- El artículo [Instalar y configurar](#) describe cómo instalar y configurar FAS.

## Implementación de Citrix Gateway

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

Esta implementación se puede utilizar para evitar múltiples solicitudes de PIN que ocurren al autenticarse primero en Citrix Gateway y luego iniciar sesión en una sesión de usuario. También permite el uso de tecnologías avanzadas de autenticación de Citrix Gateway sin requerir adicionalmente contraseñas de AD o tarjetas inteligentes.



El entorno de Citrix Virtual Apps o Citrix Virtual Desktops debe configurarse de forma similar al inicio de sesión con tarjeta inteligente, lo cual está documentado en [CTX206156](#).

En una implementación existente, esto normalmente solo implica asegurarse de que haya una autoridad de certificación de Microsoft unida a un dominio disponible y de que a los controladores de dominio se les hayan asignado certificados de controlador de dominio. (Consulte la sección "Emisión de certificados de controlador de dominio" en CTX206156).

Al configurar Citrix Gateway como sistema de autenticación principal, asegúrese de que todas las conexiones entre Citrix Gateway y StoreFront estén protegidas con TLS. En particular, asegúrese de que la URL de devolución de llamada (Callback Url) esté configurada correctamente para que apunte al servidor de Citrix Gateway, ya que esto se puede usar para autenticar el servidor de Citrix Gateway en esta implementación.

**Add NetScaler Gateway Appliance**

**StoreFront**

- ✓ General Settings
- ✓ Secure Ticket Authority
- Authentication Settings**
- Summary

**Authentication Settings**

These settings specify how the remote user provides authentication credentials

Version: 10.0 (Build 69.4) or later

VServer IP address: v10.0: SNIP or MIP, v10.1+: VIP

Logon type: Domain

Smart card fallback: None

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

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

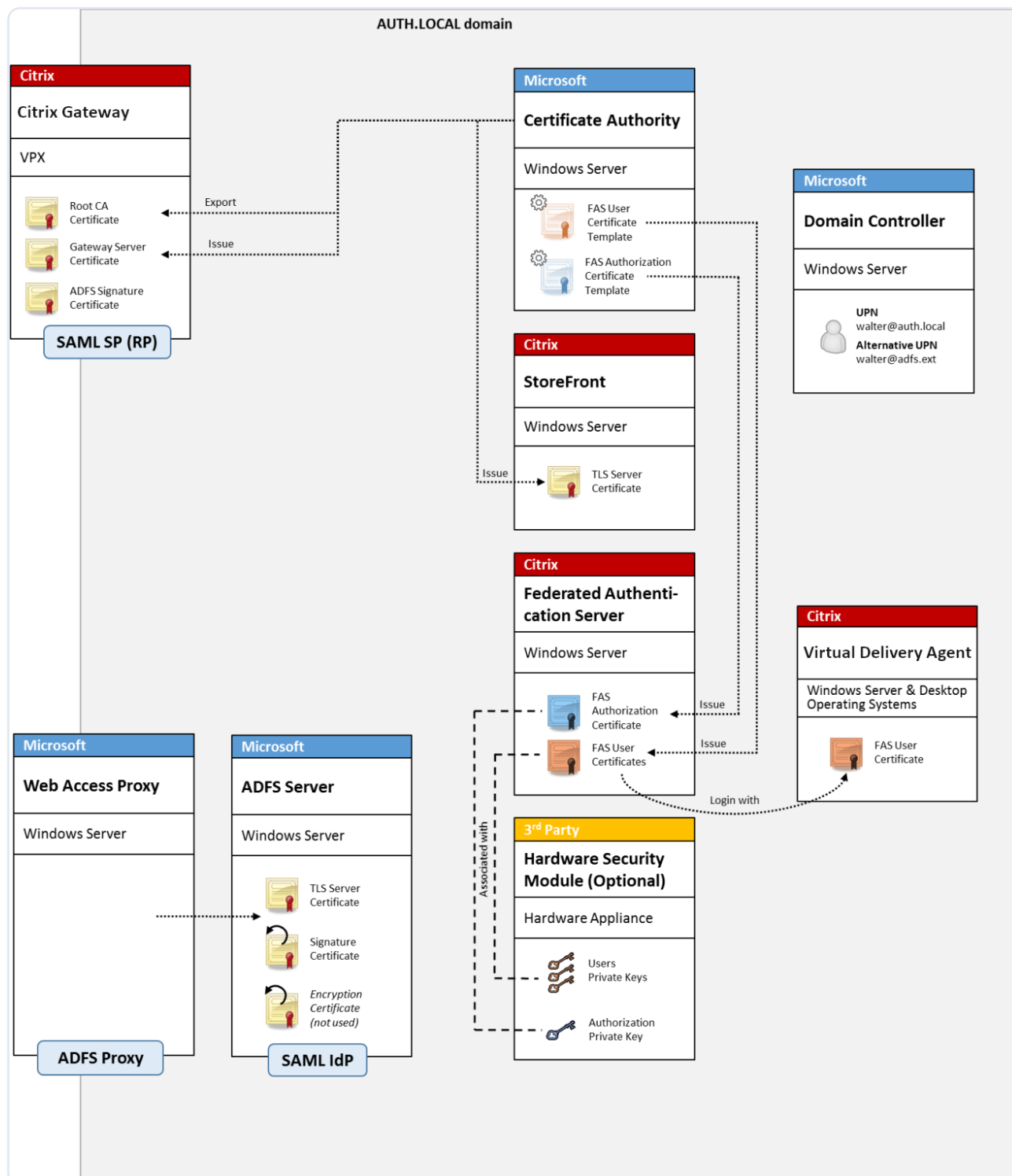
Back Create Cancel

Información relacionada:

- Para configurar Citrix Gateway, consulte "[How to Configure NetScaler Gateway 10.5 to use with StoreFront 3.6 and Citrix Virtual Desktops 7.6.](#)"
- [Install and configure](#) describe cómo instalar y configurar FAS.

## Implementación de ADFS SAML

Una tecnología clave de autenticación de Citrix Gateway permite la integración con Microsoft ADFS, que puede actuar como 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. Esto significa que el servidor FAS permite que la autenticación de un usuario se delegue al servidor Microsoft ADFS (u otro IdP compatible con SAML).



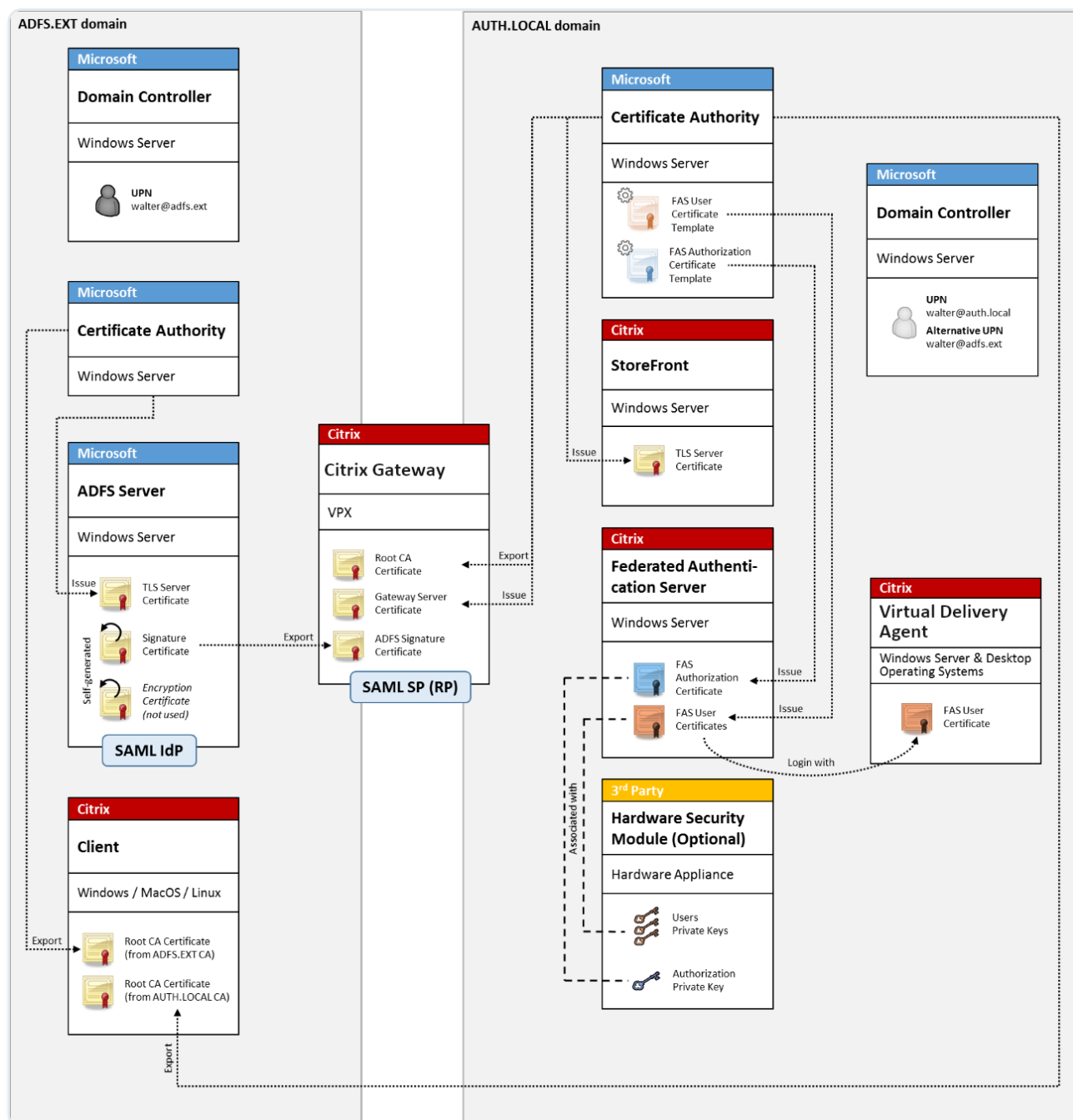
ADFS se utiliza comúnmente para autenticar de forma segura a los usuarios en los recursos corporativos de forma remota a través de Internet; por ejemplo, a menudo se utiliza para la integración con Office 365.

Información relacionada:

- El artículo [ADFS deployment](#) contiene detalles.
- El artículo [Install and configure](#) describe cómo instalar y configurar FAS.
- La sección [Citrix Gateway deployment](#) de este artículo contiene consideraciones de configuración.

## Asignación de cuentas B2B

Si dos empresas desean utilizar los sistemas informáticos de la otra, una opción común es configurar un servidor de Active Directory Federation Service (ADFS) con una relación de confianza. Esto permite a los usuarios de una empresa autenticarse sin problemas en el entorno de Active Directory (AD) de la otra empresa. Al iniciar sesión, cada usuario utiliza sus propias credenciales de inicio de sesión de la empresa; ADFS asigna automáticamente esto a una "cuenta en la sombra" en el entorno de AD de la empresa asociada.



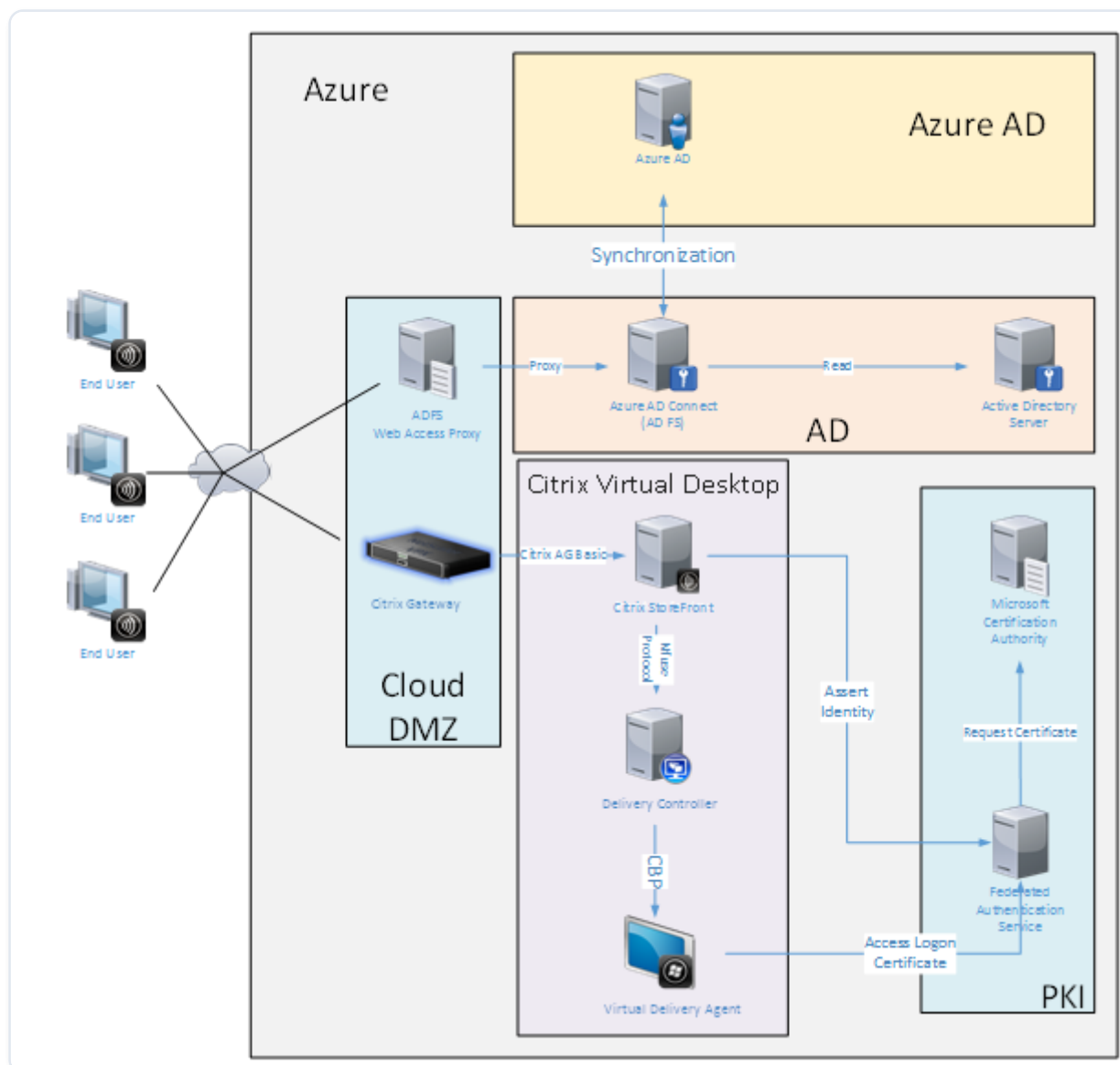
Información relacionada:

- El artículo [Instalar y configurar](#) describe cómo instalar y configurar FAS.

## Unión a Azure AD en Windows 10

Windows 10 introdujo el concepto de "Unión a Azure AD", que es conceptualmente similar a la unión a un dominio de Windows tradicional, pero está dirigido a escenarios "a través de Internet". Esto funciona bien con ordenadores portátiles y tabletas. Al igual que con la unión a un dominio de Windows tradicional, Azure AD tiene la funcionalidad de permitir modelos de inicio de sesión único

para sitios web y recursos de la empresa. Todos estos son "compatibles con Internet", por lo que funcionarán desde cualquier ubicación conectada a Internet, no solo desde la LAN de la oficina.



Esta implementación es un ejemplo en el que, en la práctica, no existe el concepto de "usuarios finales en la oficina". Los ordenadores portátiles se inscriben y se autentican completamente a través de Internet utilizando las funciones modernas de Azure AD.

Tenga en cuenta que la infraestructura de esta implementación puede ejecutarse en cualquier lugar donde haya una dirección IP disponible: en las instalaciones, en un proveedor de alojamiento, en Azure o en 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.

Información relacionada:

- El artículo [Instalar y configurar](#) describe cómo instalar y configurar FAS.

- El artículo [Integración de Azure AD](#) contiene detalles.

## Implementación de ADFS

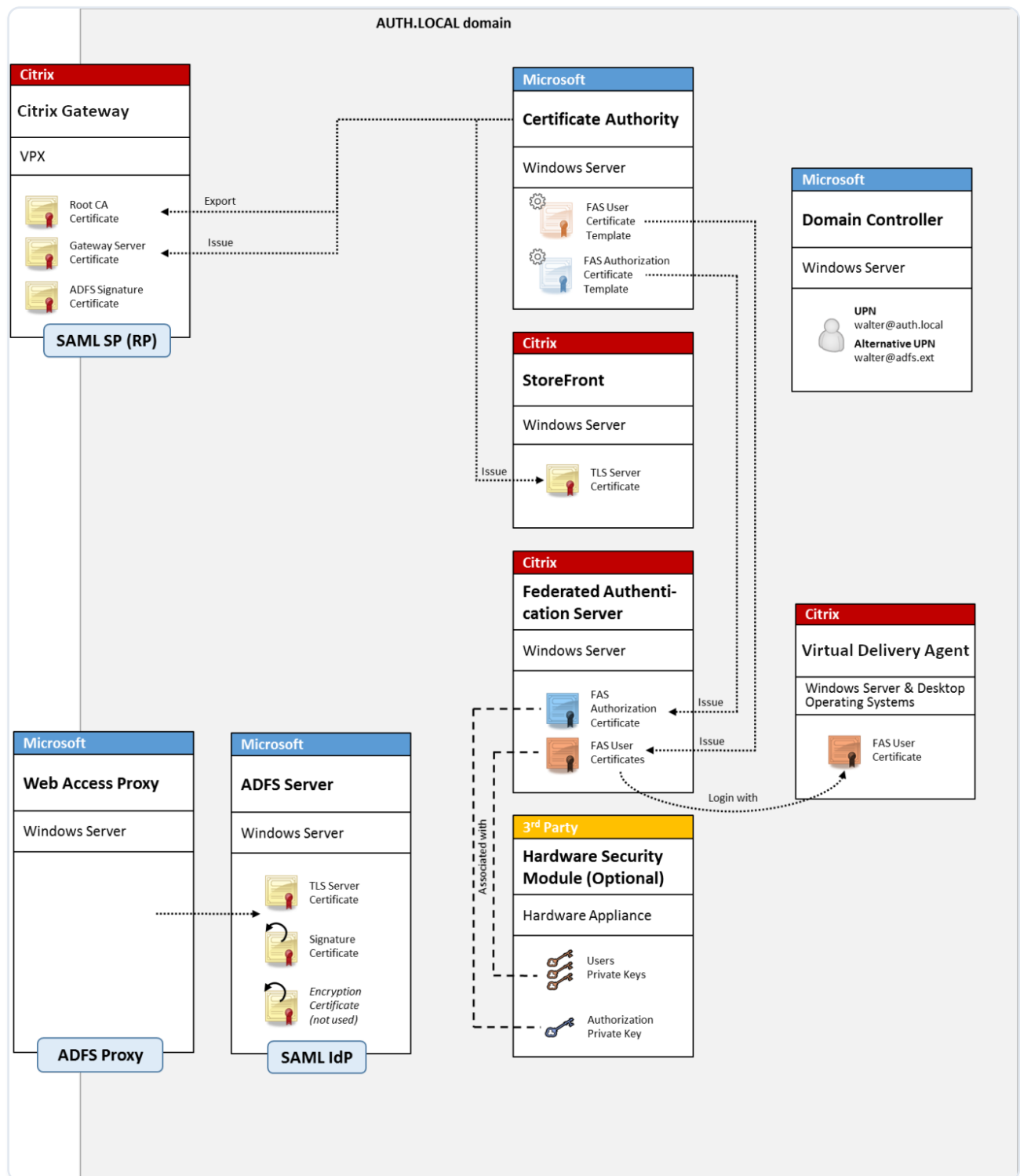
### Introducción

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

Muchas organizaciones utilizan ADFS para gestionar el acceso seguro de los usuarios a sitios web que requieren un único punto de autenticación. Por ejemplo, una empresa puede tener contenido adicional y descargas disponibles para los empleados; esas ubicaciones deben protegerse con credenciales de inicio de sesión estándar de Windows.

El Servicio de autenticación federada (FAS) también permite integrar Citrix Gateway y Citrix StoreFront™ con el sistema de inicio de sesión de ADFS, lo que reduce la posible confusión para los empleados.

Esta implementación integra Citrix Gateway como parte de confianza de Microsoft ADFS.



**NOTA:**

No hay diferencias si el recurso de back-end es Windows VDA o Linux VDA.

## Información general de SAML

Security Assertion Markup Language (SAML) es un sistema de inicio de sesión de navegador web simple de "redirección a una página de inicio de sesión". La configuración incluye los siguientes elementos:

### URL de redirección

Cuando Citrix Gateway detecta que un usuario necesita autenticarse, indica al navegador web del usuario que realice una solicitud HTTP POST a una página web de inicio de sesión SAML en el servidor ADFS. Normalmente, se trata de una dirección `https://` con el formato: `https://adfs.mycompany.com/adfs/ls`.

Esta solicitud POST de página web incluye otra información, incluida la "dirección de retorno" a la que ADFS devolverá al usuario cuando se complete el inicio de sesión.

### Identificador

El EntityId es un identificador único que Citrix Gateway incluye en sus datos POST a ADFS. Esto informa a ADFS qué servicio está intentando iniciar sesión el usuario y aplica diferentes políticas de autenticación según corresponda. Si se emite, el XML de autenticación SAML solo será adecuado para iniciar sesión en el servicio identificado por el EntityId.

Normalmente, el EntityID es la URL de la página de inicio de sesión del servidor Citrix Gateway, pero generalmente puede ser cualquier cosa, siempre que Citrix Gateway y ADFS estén de acuerdo en ello: `https://ns.mycompany.com/application/logonpage`.

### Dirección de retorno

Si la autenticación es exitosa, ADFS indica al navegador web del usuario que envíe un XML de autenticación SAML de vuelta a una de las URL de respuesta (Reply URLs) configuradas para el 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 dirección URL de respuesta configurada, Citrix Gateway puede elegir una en su POST original a ADFS.

### Certificado de firma

ADFS firma criptográficamente los blobs XML de autenticación SAML utilizando su clave privada. Para validar esta firma, Citrix Gateway debe configurarse para verificar estas firmas utilizando la clave pública incluida en un archivo de certificado. El archivo de certificado suele ser un archivo de texto obtenido del servidor ADFS.

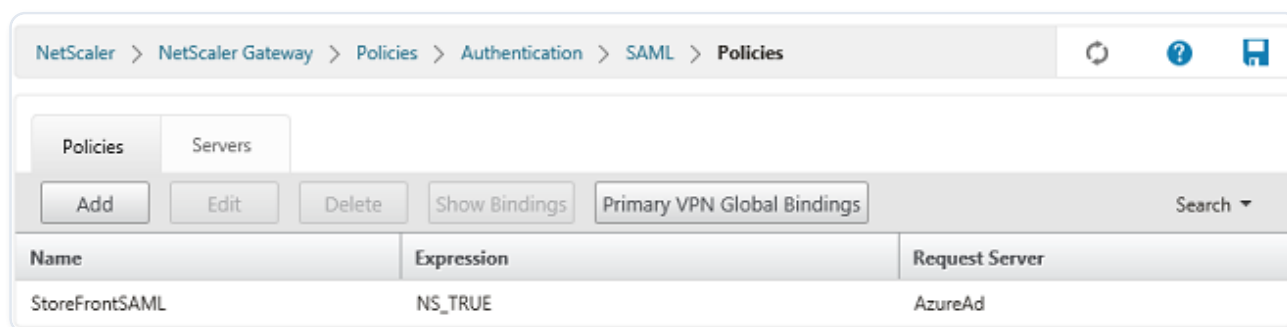
## URL de cierre de sesión único

ADFS y Citrix Gateway admiten un sistema de "cierre de sesión central". Esta es una URL que Citrix Gateway consulta ocasionalmente para verificar que el blob XML de autenticación SAML todavía representa una sesión actualmente iniciada.

Esta es una característica opcional que no necesita ser configurada. Suele ser una dirección `https://` con el formato `https://adfs.mycompany.com/adfs/logout`. (Tenga en cuenta que puede ser la misma que la URL de inicio de sesión único).

## Configuración

La sección [Implementación de Citrix Gateway](#) describe cómo configurar Citrix Gateway para manejar las opciones de autenticación LDAP estándar. Una vez completado con éxito, puede crear una nueva política de autenticación en Citrix Gateway que permita la autenticación SAML. Esto puede reemplazar la política LDAP predeterminada utilizada por el asistente de Citrix Gateway.



## Rellenar la política SAML

Configure el nuevo servidor IdP SAML utilizando la información obtenida previamente de la consola de administración de ADFS. Cuando se aplica esta política, Citrix Gateway redirige al usuario a ADFS para iniciar sesión y, a cambio, acepta un token de autenticación SAML firmado por ADFS.

Create Authentication SAML Server

Create Authentication SAML Server

Name\*

AzureAd

Authentication Type

SAML

IDP Certificate Name\*

AzureADSAML

+

Redirect URL\*

29f-4c20-9826-14d5e484c62e/saml2

Single Logout URL

29f-4c20-9826-14d5e484c62e/saml2

User Field

userprincipalname

Signing Certificate Name

Issuer Name

https://ns.citrixsaml demo.net/Citrix/

Reject Unsigned Assertion\*

ON

SAML Binding\*

POST

Default Authentication Group

Skew Time(mins)

5

5

Two Factor

☐ ON
☒ OFF

Assertion Consumer Service Index

255

Attribute Consuming Service Index

255

Requested Authentication Context\*

Exact

Authentication Class Types

InternetProtocol  
InternetProtocolPassword

Signature Algorithm\*

☐ RSA-SHA1
☒ RSA-SHA256

Digest Method\*

☐ SHA1
☒ SHA256

☐ Send Thumbprint
☒ Enforce Username

Attribute 1

Attribute 3

Attribute 5

Attribute 7

## Información relacionada

- [Instalar y configurar](#) es la referencia principal para la instalación y configuración de FAS.
- Las implementaciones comunes de FAS se resumen en el artículo [Arquitecturas de implementación](#).
- Los artículos "Cómo hacer" se presentan en el artículo [Configuración avanzada](#).

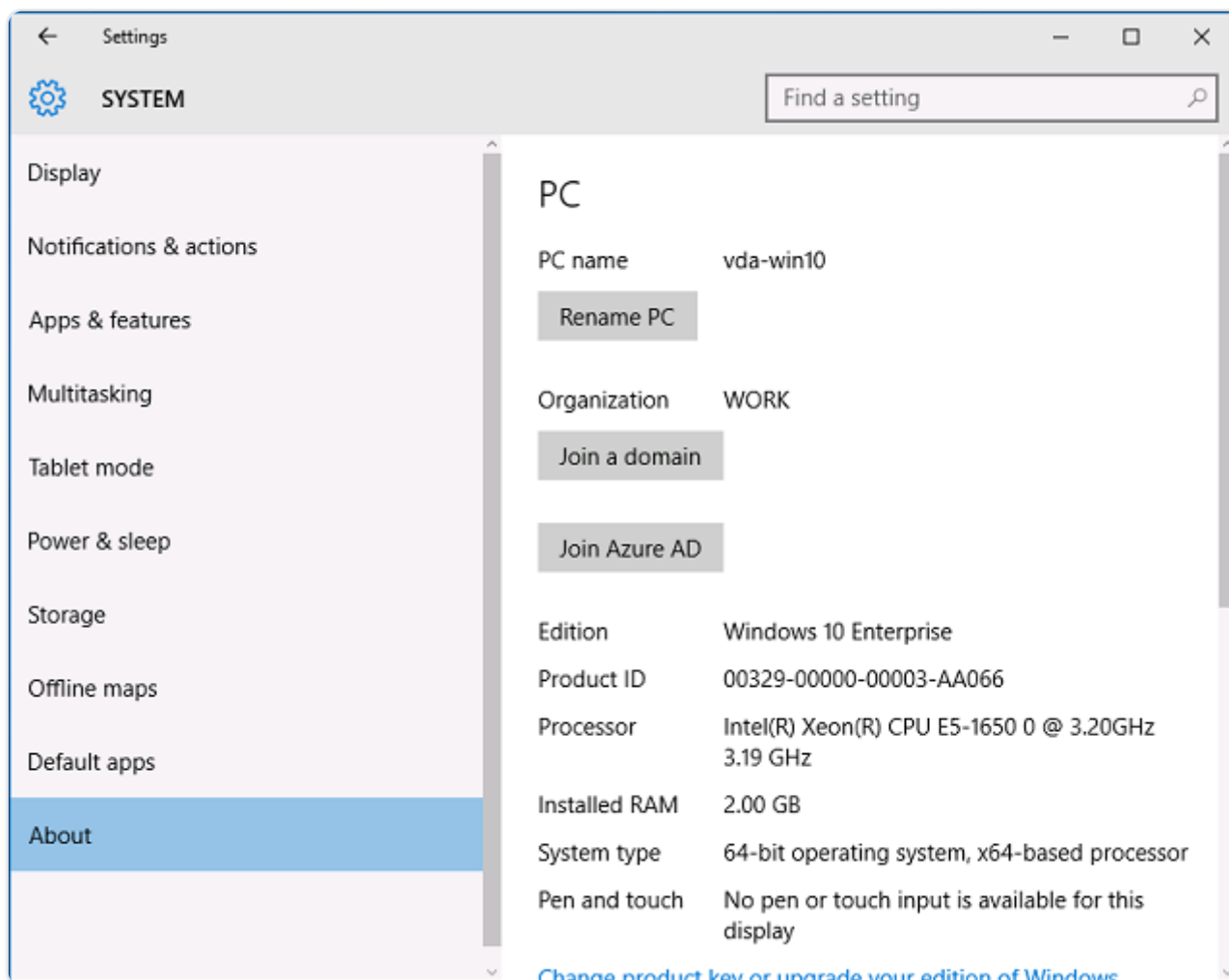
## Integración de Azure AD

### Introducción

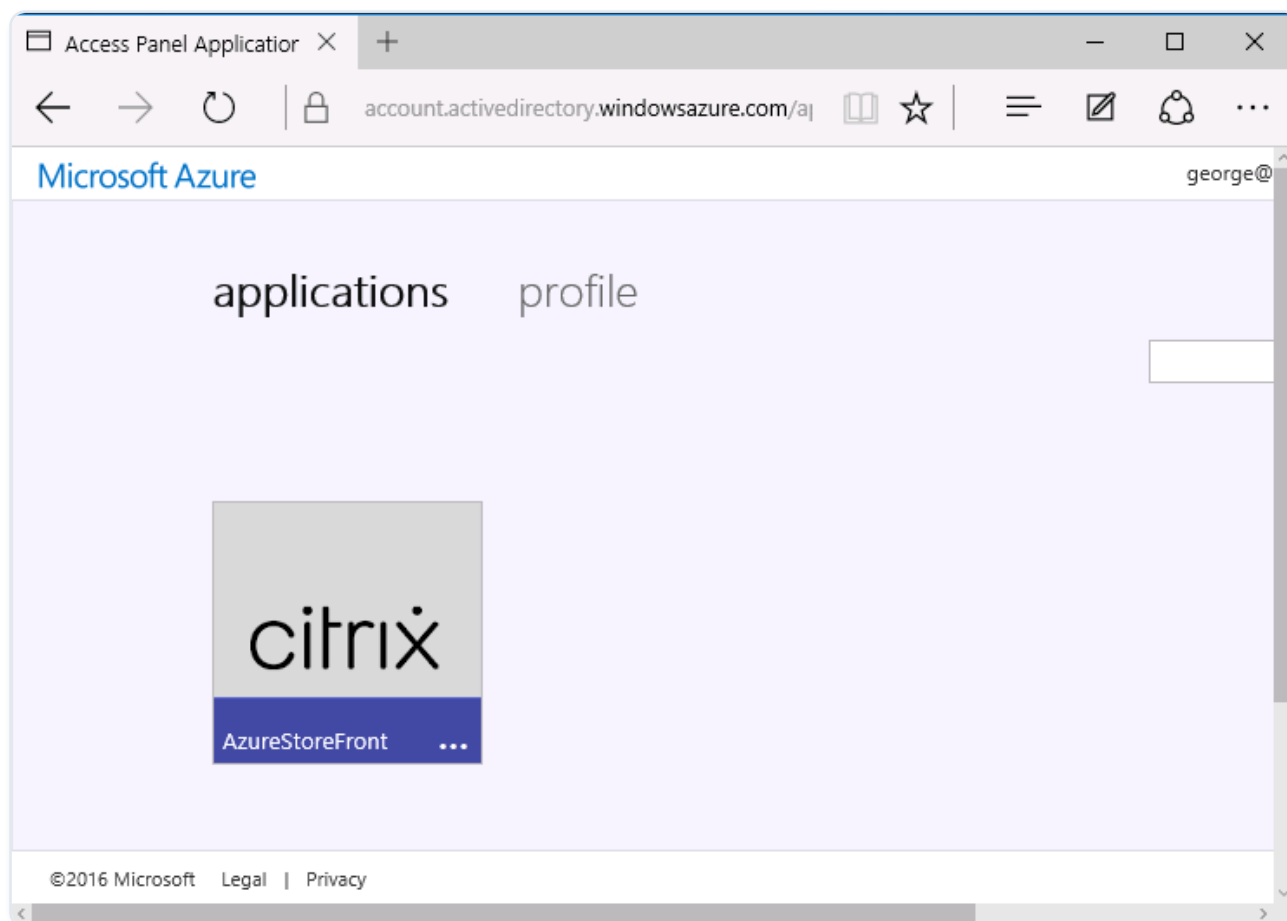
Este documento describe cómo integrar un entorno Citrix con la función de Azure AD de Windows 10. Windows 10 introdujo Azure AD, que es un nuevo modelo de unión a dominio donde los

portátiles itinerantes pueden unirse a un dominio corporativo a través de Internet con fines de administración e inicio de sesión único.

La implementación de ejemplo de este documento describe un sistema en el que TI proporciona a los nuevos usuarios una dirección de correo electrónico corporativa y un código de inscripción para sus portátiles personales con Windows 10. Los usuarios acceden a este código a través de la opción **Sistema > Acerca de > Unirse a Azure AD** en el panel de **Configuración**.



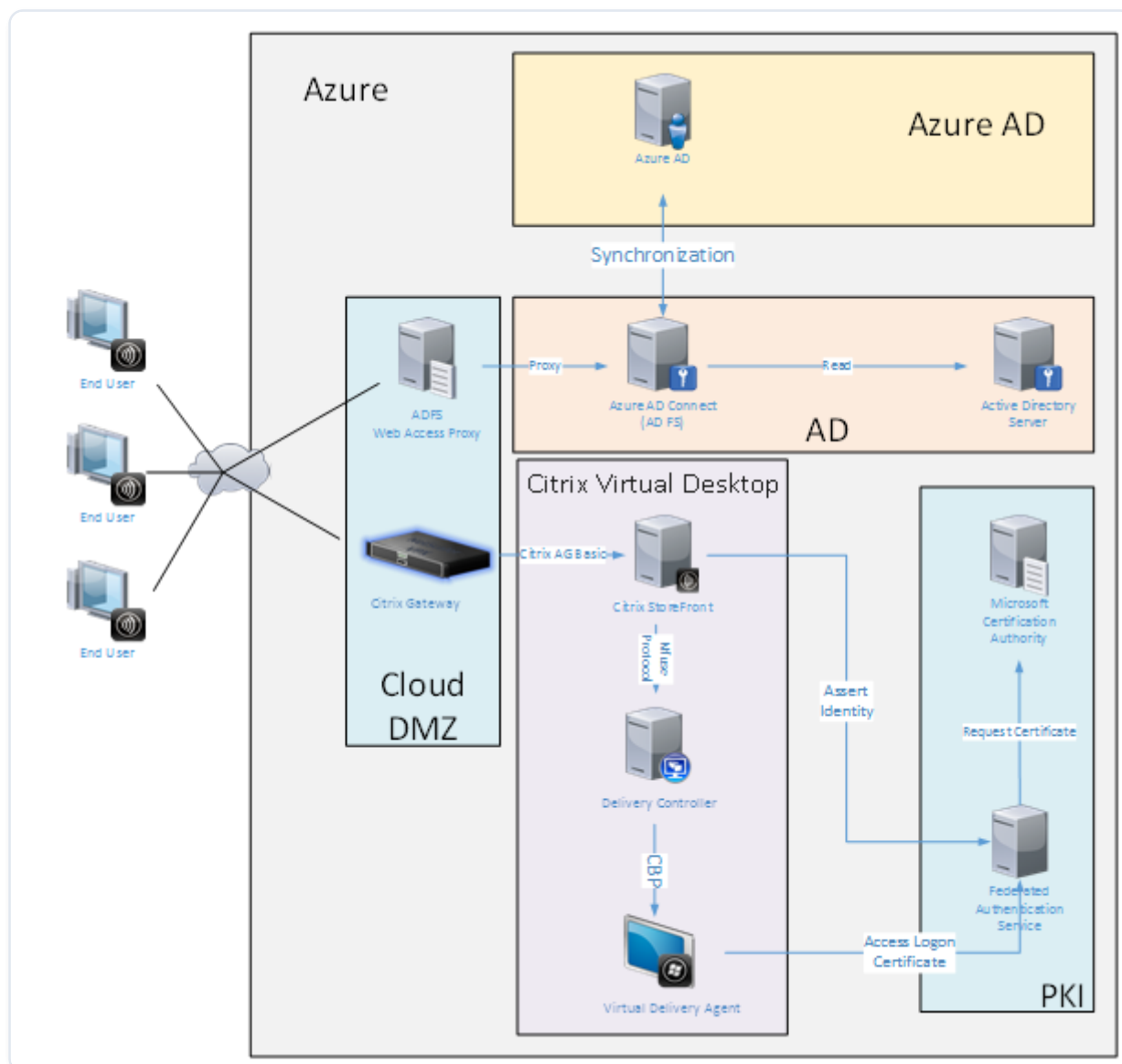
Una vez inscrito el portátil, el navegador web Microsoft Edge inicia sesión automáticamente en los sitios web de la empresa y en las aplicaciones publicadas de Citrix a través de la página web de aplicaciones SaaS de Azure, junto con otras aplicaciones de Azure como Office 365.



## Arquitectura

Esta arquitectura replica una red corporativa tradicional completamente dentro de Azure, integrándose con tecnologías de nube modernas como Azure AD y Office 365. Todos los usuarios finales se consideran trabajadores remotos, sin el concepto de estar en una intranet de oficina.

El modelo se puede aplicar a empresas con sistemas locales existentes, ya que la sincronización de Azure AD Connect puede establecer un puente con Azure a través de Internet.



Las conexiones seguras y el inicio de sesión único, que tradicionalmente habrían sido LAN con firewall y autenticación Kerberos/NTLM, se reemplazan en esta arquitectura por conexiones TLS a Azure y SAML. Los nuevos servicios se crean como aplicaciones de Azure unidas a Azure AD. Las aplicaciones existentes que requieren Active Directory (como una base de datos de SQL Server) se pueden ejecutar utilizando una VM de servidor de Active Directory estándar en la parte IAAS del servicio en la nube de Azure.

Cuando un usuario inicia una aplicación tradicional, se accede a ella mediante las aplicaciones publicadas de Citrix Virtual Apps and Desktops™. Los diferentes tipos de aplicaciones se recopilan a través de la página **Aplicaciones de Azure** del usuario, utilizando las funciones de inicio de sesión único de Microsoft Edge. Microsoft también proporciona aplicaciones para Android e iOS 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 controle la zona de delegación para el sufijo del nombre de dominio. Para ello, el administrador puede utilizar la función de zona DNS de Azure.

Este ejemplo utiliza el nombre de zona DNS *citrixsamldemo.net*.

The screenshot shows the Azure DNS console interface. At the top, there's a header with the DNS icon and a title bar. Below the header, there are four icons: Settings, Record set, Delete, and Refresh. The main content area is titled 'Essentials' and displays the following information:

- Resource group:** citrixsamldemo
- Subscription name:** Visual Studio Professional with MSDN
- Subscription ID:** df22436f-d4f9-46ae-be7b-6479cdaeefca
- Name server 1:** ns1-01.azure-dns.com.
- Name server 2:** ns2-01.azure-dns.net.
- Name server 3:** ns3-01.azure-dns.org.
- Name server 4:** ns4-01.azure-dns.info.

Below this information, there's a search bar labeled 'Search record sets'. Underneath the search bar is a table with the following columns: NAME, TYPE, TTL, and VALUE.

| NAME | TYPE  | TTL    | VALUE                                                                                                                                             |
|------|-------|--------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| @    | NS    | 172800 | ns1-01.azure-dns.com.<br>ns2-01.azure-dns.net.<br>ns3-01.azure-dns.org.<br>ns4-01.azure-dns.info. ...                                             |
| @    | SOA   | 3600   | Email: azuredns-hostmaster.microsoft....<br>Host: ns1-01.azure-dns.com.<br>Refresh: 3600<br>Retry: 300<br>Expire: 2419200<br>Minimum TTL: 300 ... |
| fs   | CNAME | 3600   | adfs-citrixsamldemo.westeurope.cloud... ...                                                                                                       |

La consola muestra los nombres de los servidores de nombres DNS de Azure. Estos deben referenciarse en las entradas NS del registrador DNS para la zona (por ejemplo,

`citrixsamldemo.net. NS n1-01.azure-dns.com` )

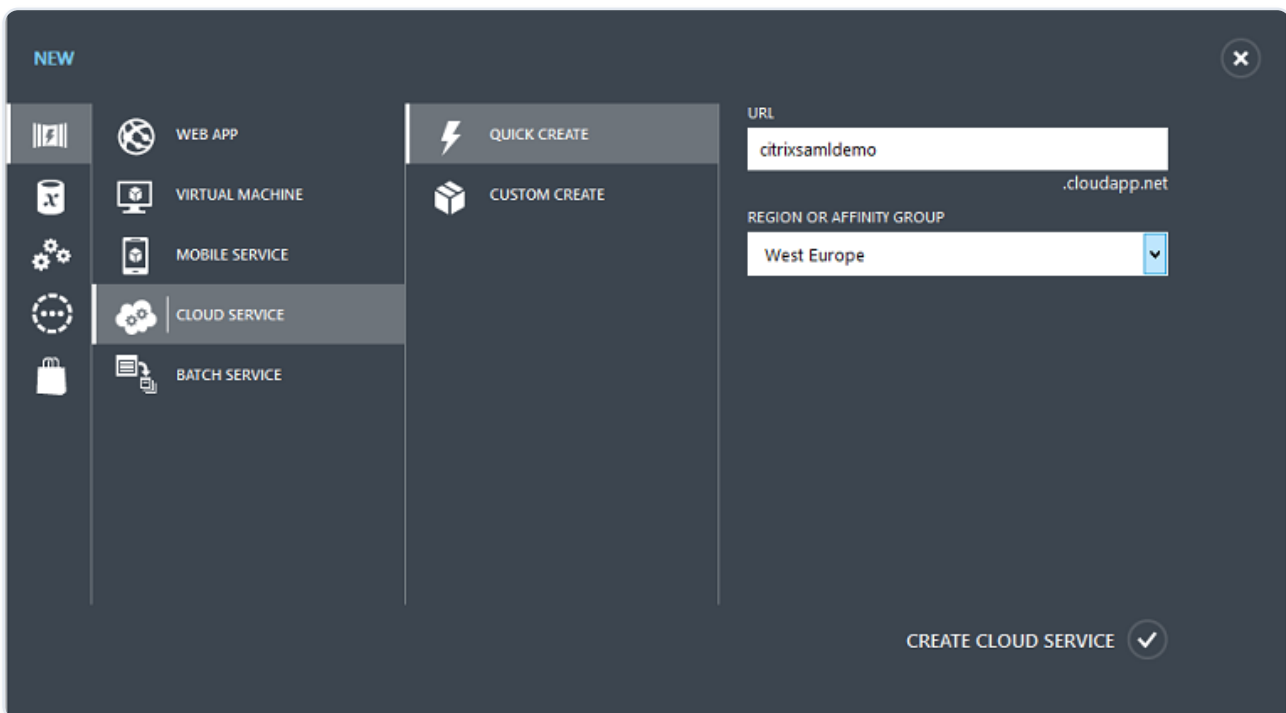
Al agregar referencias a máquinas virtuales que se ejecutan en Azure, lo más fácil es usar un puntero CNAME al registro DNS administrado por Azure para la máquina virtual. Si la dirección IP de la máquina virtual cambia, no necesitará actualizar manualmente el archivo de zona DNS.

Los sufijos de dirección DNS internos y externos coincidirán para esta implementación. El dominio es citrixsamldemo.net y utiliza un 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 en la nube

Este ejemplo configura un entorno Citrix, incluido un entorno AD con un servidor ADFS ejecutándose en Azure. Se crea un servicio en la nube, denominado "citrixsamldemo".



## Crear máquinas virtuales Windows

Cree cinco máquinas virtuales Windows que se ejecuten en el servicio en la nube:

- Controlador de dominio (domaincontrol)
- Servidor ADFS de Azure Connect (adfs)
- Proxy de acceso web de ADFS (Web Application Proxy, no unido a un dominio)
- Citrix Virtual Apps and Desktops Controlador de entrega
- Agente de entrega virtual (VDA) de Citrix Virtual Apps and Desktops

Microsoft Azure

Create virtual machine > Basics

Create virtual machine

Basics

1 Basics  
Configure basic settings

2 Size  
Choose virtual machine size

3 Settings  
Configure optional features

4 Summary  
Windows Server 2012 R2 Datacenter

\* Name

\* User name

\* Password

Subscription  
Visual Studio Professional with MSDN

\* Resource group  
citrixsamldemo

Location  
West Europe

OK

## Controlador de dominio

- Agregue los roles de **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 del dominio, agregue el rol de **Servicios de certificación de Active Directory**.
- Cree una cuenta de usuario normal para realizar pruebas (por ejemplo, [George@citrixsamldemo.net](mailto:George@citrixsamldemo.net)).
- Dado que este servidor ejecutará DNS interno, todos los servidores deben consultar este servidor para la resolución de DNS. Esto se puede hacer a través de la página de **configuración de DNS de Azure**. (Para obtener más información, consulte el Apéndice de este documento).

## Controlador ADFS y servidor proxy de aplicación web

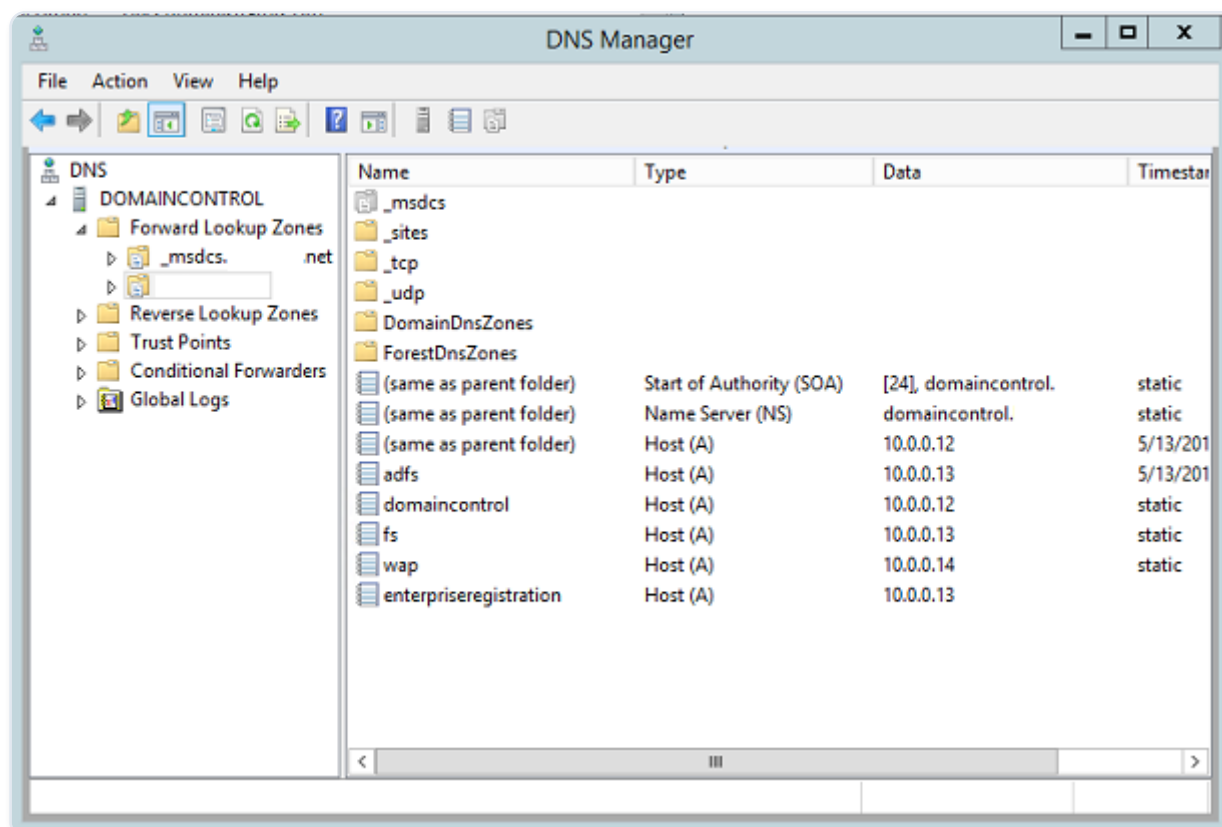
- Una el servidor ADFS al dominio citrixsamldemo. El servidor proxy de aplicación web debe permanecer en un grupo de trabajo aislado, por lo que debe registrar manualmente una dirección DNS con el DNS de AD.
- Ejecute el cmdlet **Enable-PSRemoting -Force** en estos servidores para permitir el acceso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

## Controlador de entrega y VDA de Citrix Virtual Desktops™

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

## Configurar un DNS interno

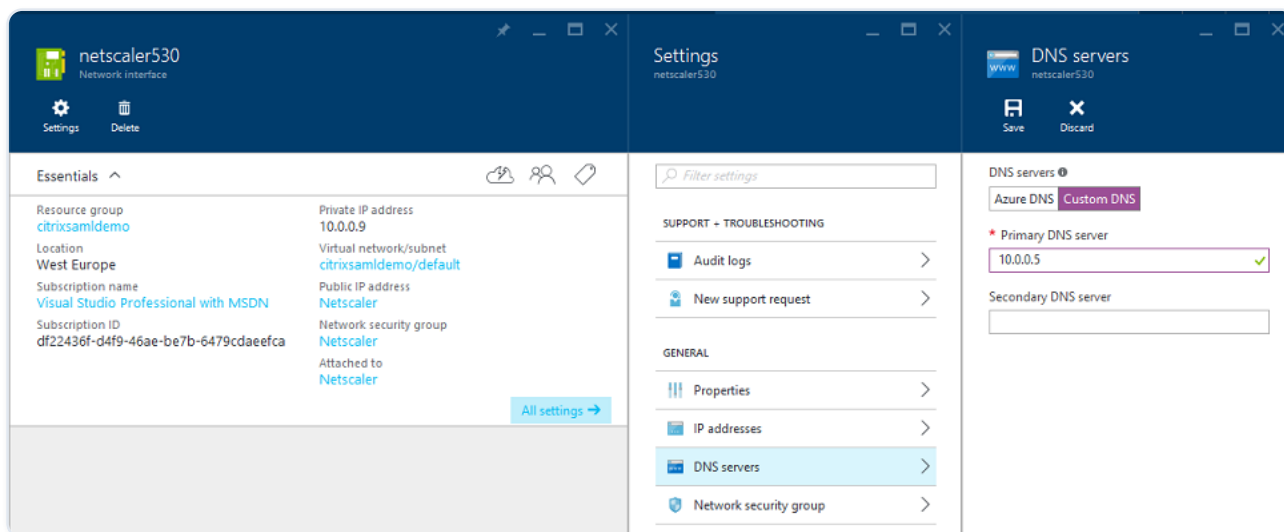
Una vez instalado el controlador de dominio, configure el servidor DNS para que gestione la vista interna de citrixsamldemo.net y actúe como reenviador a un servidor DNS externo (por ejemplo: 8.8.8.8).



Agregue un registro estático para:

- wap.citrixsamldemo.net
- fs.citrixsamldemo.net
- enterpriseregistration.citrixsaml.net

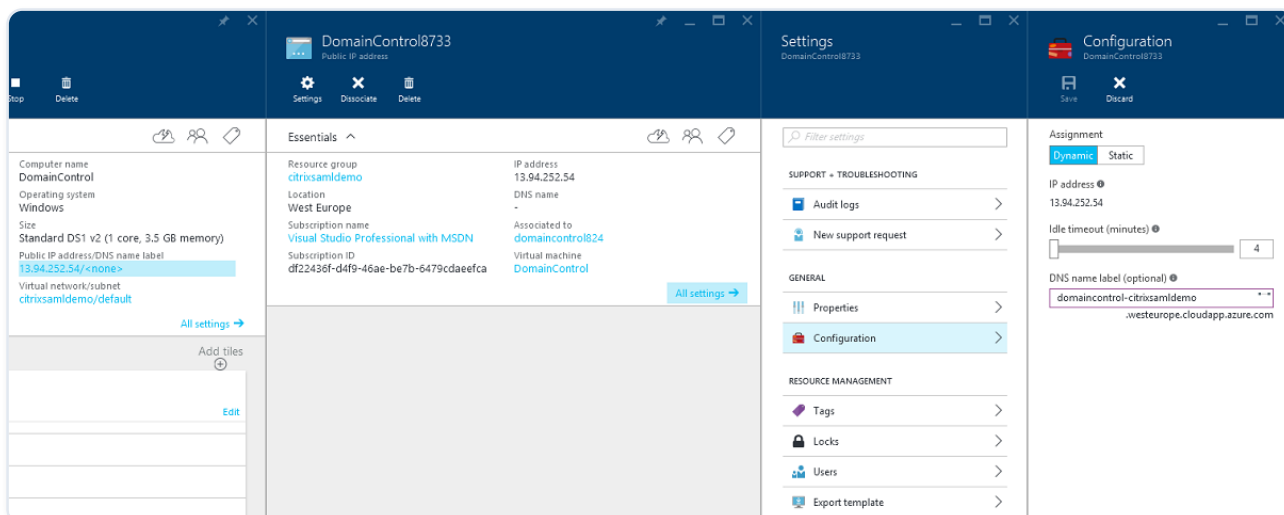
Todas las máquinas virtuales que se ejecutan en Azure deben configurarse para usar solo este servidor DNS. Puede hacerlo a través de la GUI de la interfaz de red.



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

## Configurar una dirección DNS externa

Cuando una máquina virtual está en ejecución, Azure mantiene su propio servidor de zona DNS que apunta a la dirección IP pública actual asignada a la máquina virtual. Esta es una característica útil para habilitar porque Azure asigna direcciones IP cuando se inicia cada máquina virtual, de forma predeterminada.

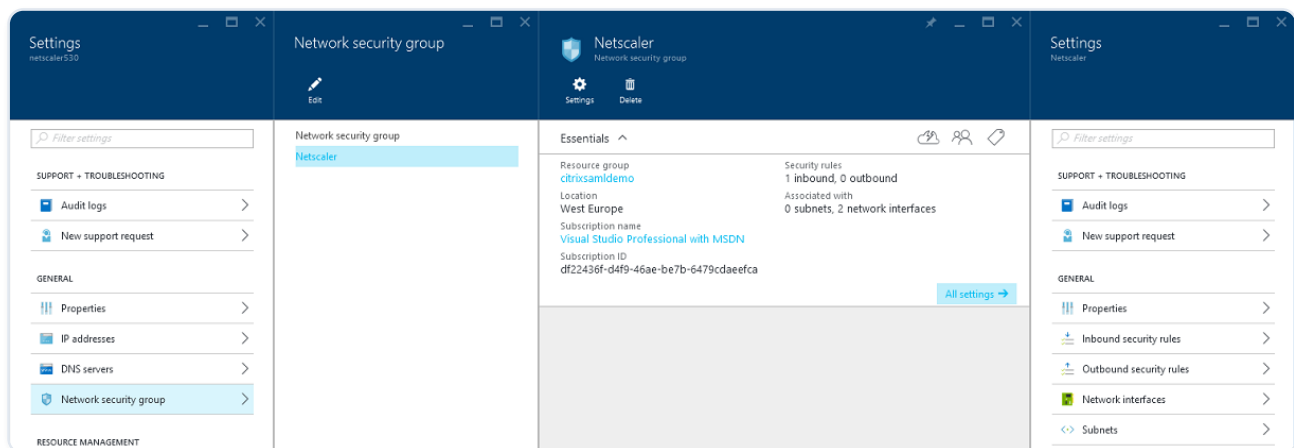


Este ejemplo asigna una dirección DNS de domaincontrol-citrixsamldemo.westeurope.cloudapp.azure.com al controlador de dominio.

Tenga en cuenta que, una vez completada la configuración remota, solo las máquinas virtuales de Web Application Proxy y Citrix Gateway deben tener direcciones IP públicas habilitadas. (Durante la configuración, la dirección IP pública se utiliza para el acceso RDP al entorno).

## Configurar grupos de seguridad

La nube de Azure administra las reglas de firewall para el acceso TCP/UDP a las máquinas virtuales desde Internet mediante grupos de seguridad. De forma predeterminada, todas las máquinas virtuales permiten el acceso RDP. Los servidores Citrix Gateway y Web Application Proxy también deben permitir TLS en el puerto 443.

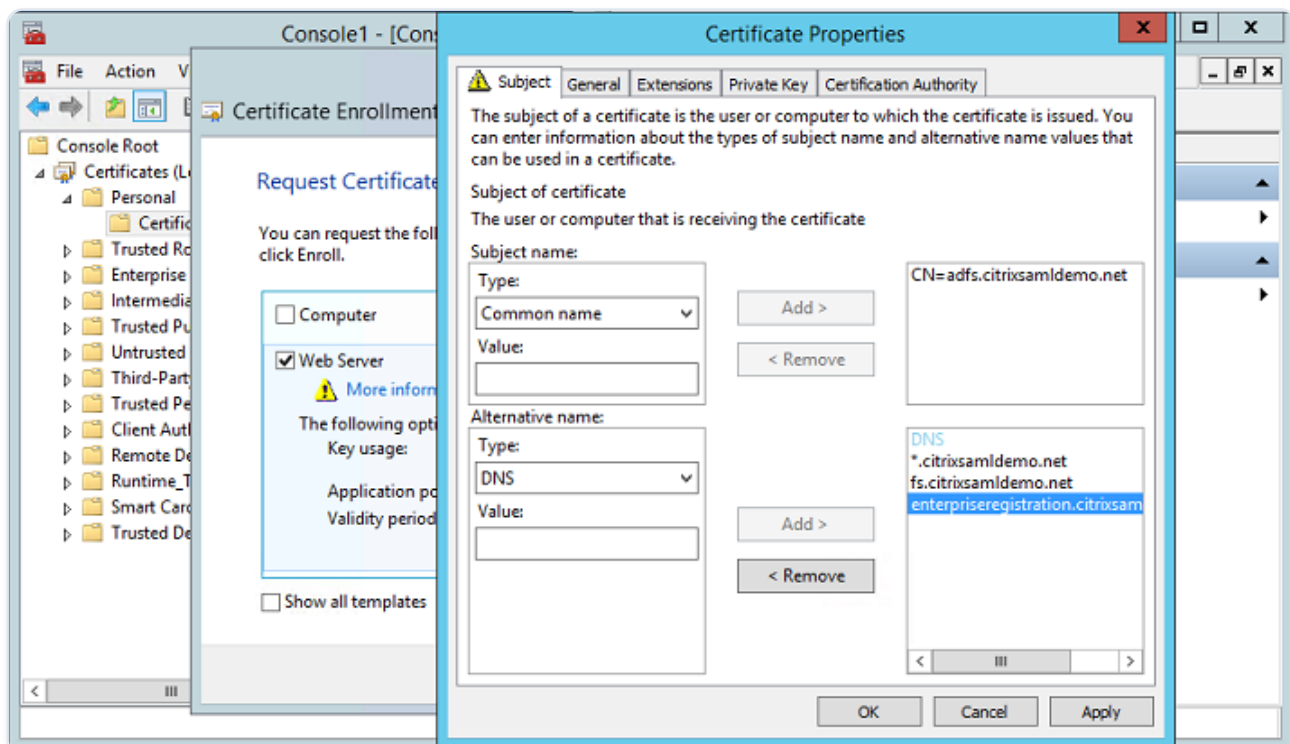


## Crear un certificado ADFS

Habilite la plantilla de certificado **Servidor web** en la autoridad de certificación de Microsoft. Esto permite la creación de un certificado con direcciones DNS personalizadas que se puede exportar (incluida la clave privada) a un archivo pfx. Debe instalar este certificado tanto en los servidores ADFS como en los de Web Application Proxy, por lo que el archivo PFX es la opción preferida.

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

- Nombre común:
  - adfs.citrixsamldemo.net
- Nombre alternativo del asunto:
  - \*.citrixsamldemo.net
  - fs.citrixsamldemo. red
  - enterpriseregistration.citrixsamldemo.net



Exporte el certificado a un archivo pfx, incluida una clave privada protegida con 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 nuevo directorio

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

**ADD DIRECTORY**

**DIRECTORY** ⓘ

Create new directory ▼

**NAME** ⓘ

CitrixSAMLdemo

**DOMAIN NAME** ⓘ

citrixsaml demo ✓ .onmicrosoft.com

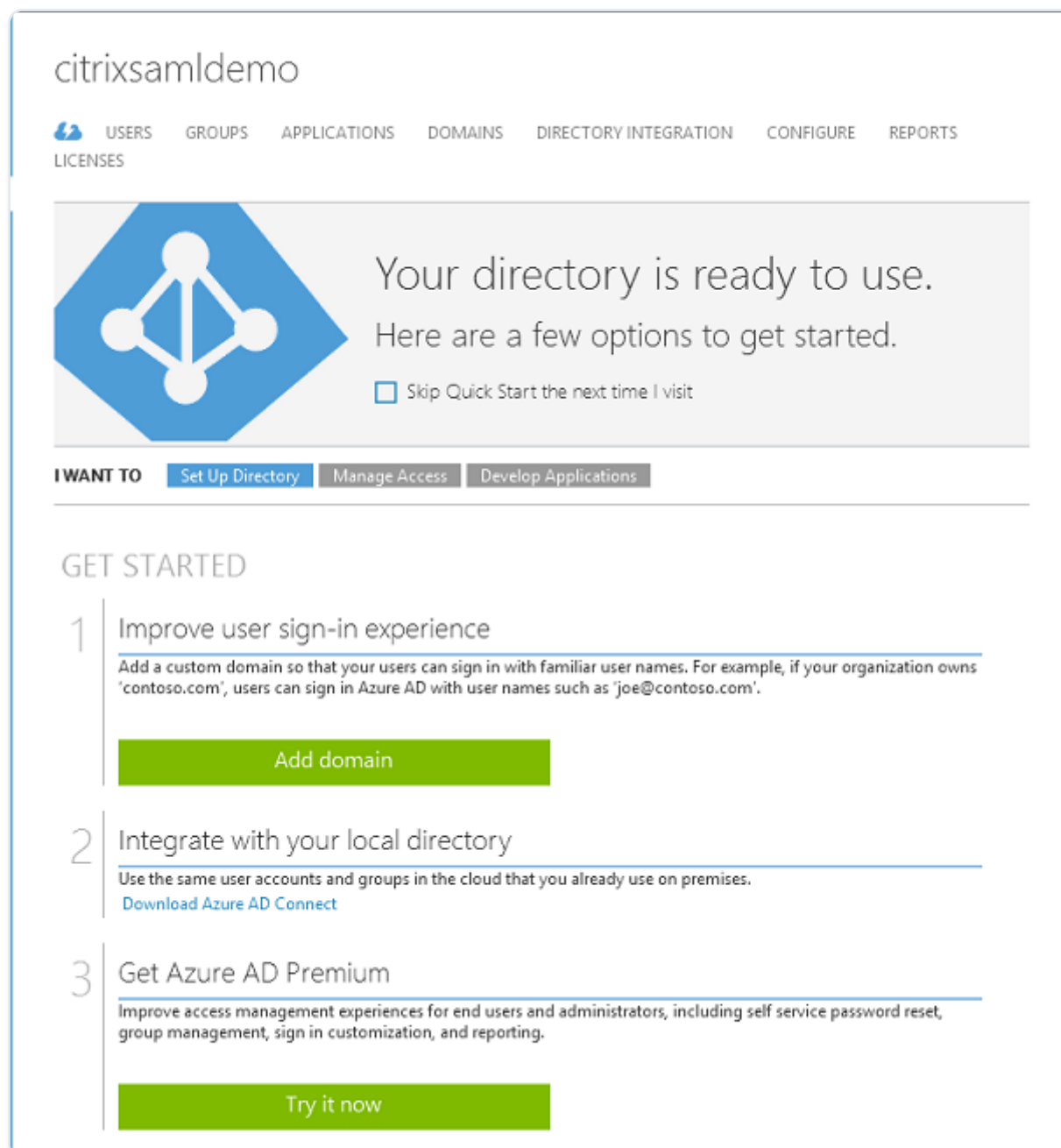
**COUNTRY OR REGION** ⓘ

United Kingdom ▼

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

✓

Cuando se complete, aparecerá una página de resumen.



**citrixsamdemo**

USERS GROUPS APPLICATIONS DOMAINS DIRECTORY INTEGRATION CONFIGURE REPORTS  
LICENSES

 Your directory is ready to use.  
Here are a few options to get started.

☐ Skip Quick Start the next time I visit

**I WANT TO** [Set Up Directory](#) [Manage Access](#) [Develop Applications](#)

**GET STARTED**

- 1 Improve user sign-in experience**  
Add a custom domain so that your users can sign in with familiar user names. For example, if your organization owns 'contoso.com', users can sign in Azure AD with user names such as 'joe@contoso.com'.  
[Add domain](#)
- 2 Integrate with your local directory**  
Use the same user accounts and groups in the cloud that you already use on premises.  
[Download Azure AD Connect](#)
- 3 Get Azure AD Premium**  
Improve access management experiences for end users and administrators, including self service password reset, group management, sign in customization, and reporting.  
[Try it now](#)

## Crear un usuario administrador global (AzureAdmin)

Cree un administrador global en Azure (en este ejemplo,

[AzureAdmin@citrixsamdemo.onmicrosoft.com](mailto:AzureAdmin@citrixsamdemo.onmicrosoft.com)) e inicie sesión con la nueva cuenta para configurar una contraseña.

ADD USER

user profile

FIRST NAME: Azure

LAST NAME: Admin

DISPLAY NAME: Azure Admin

ROLE: Global Admin

ALTERNATE EMAIL ADDRESS: [Red exclamation mark]

MULTI-FACTOR AUTHENTICATION: ☐ Enable Multi-Factor Authentication

1 3

## Registrar su dominio con Azure AD

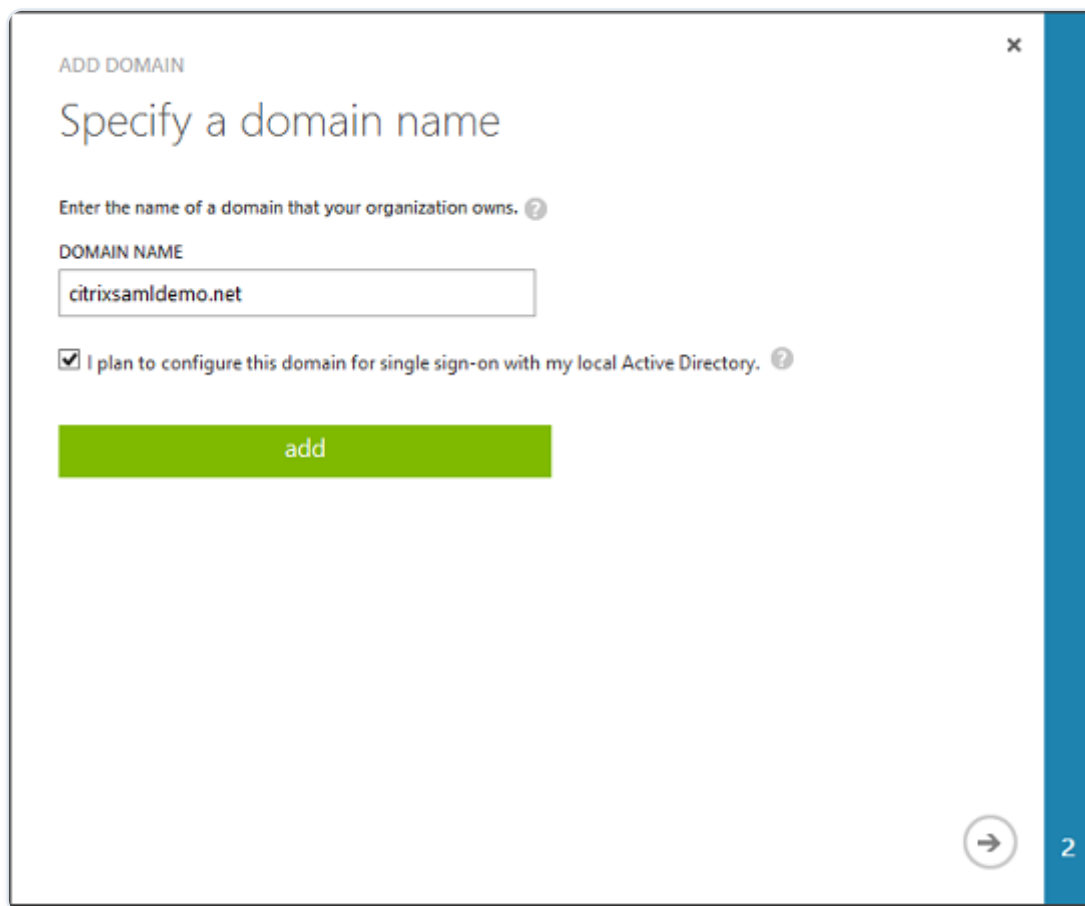
Por defecto, los usuarios se identifican con una dirección de correo electrónico con el formato:

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

Aunque esto funciona sin configuración adicional, es mejor una dirección de correo electrónico con formato estándar, preferiblemente una que coincida con 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. El ejemplo utiliza `citrixsamldemo.net`.

Si está configurando ADFS para el inicio de sesión único, active la casilla de verificación.



ADD DOMAIN

Specify a domain name

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

DOMAIN NAME

citrixsaml-demo.net

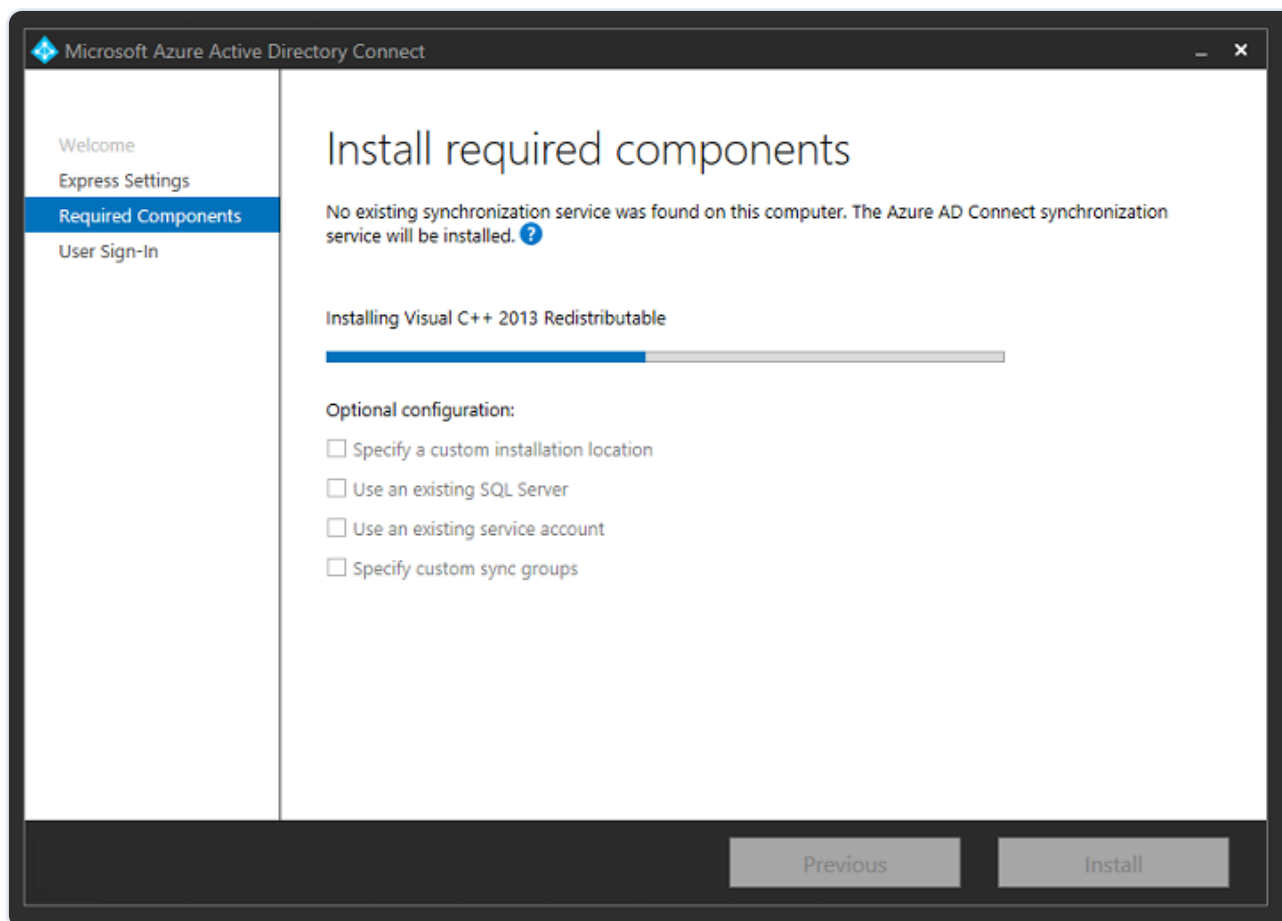
☒ I plan to configure this domain for single sign-on with my local Active Directory. ?

add

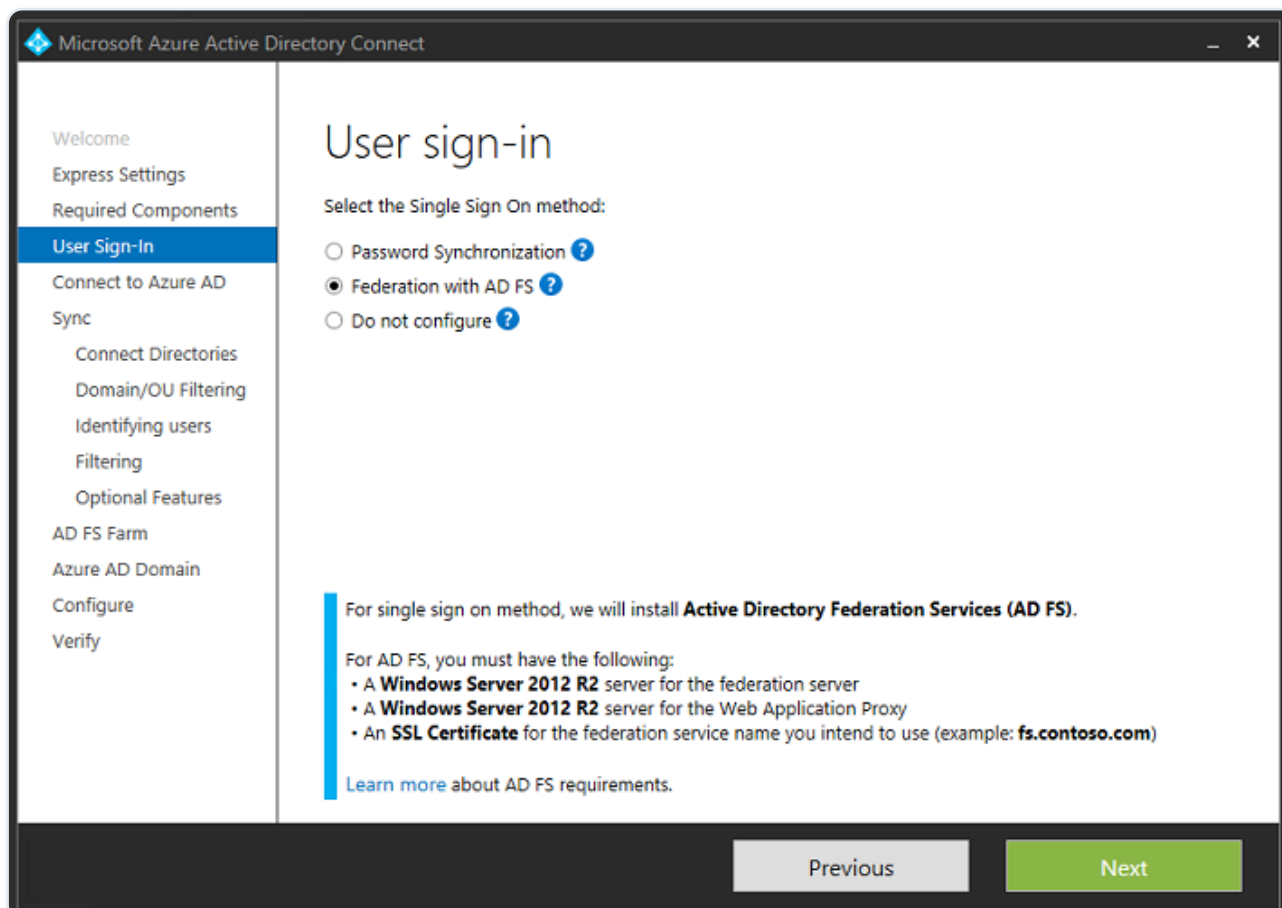
2

## Instalar Azure AD Connect

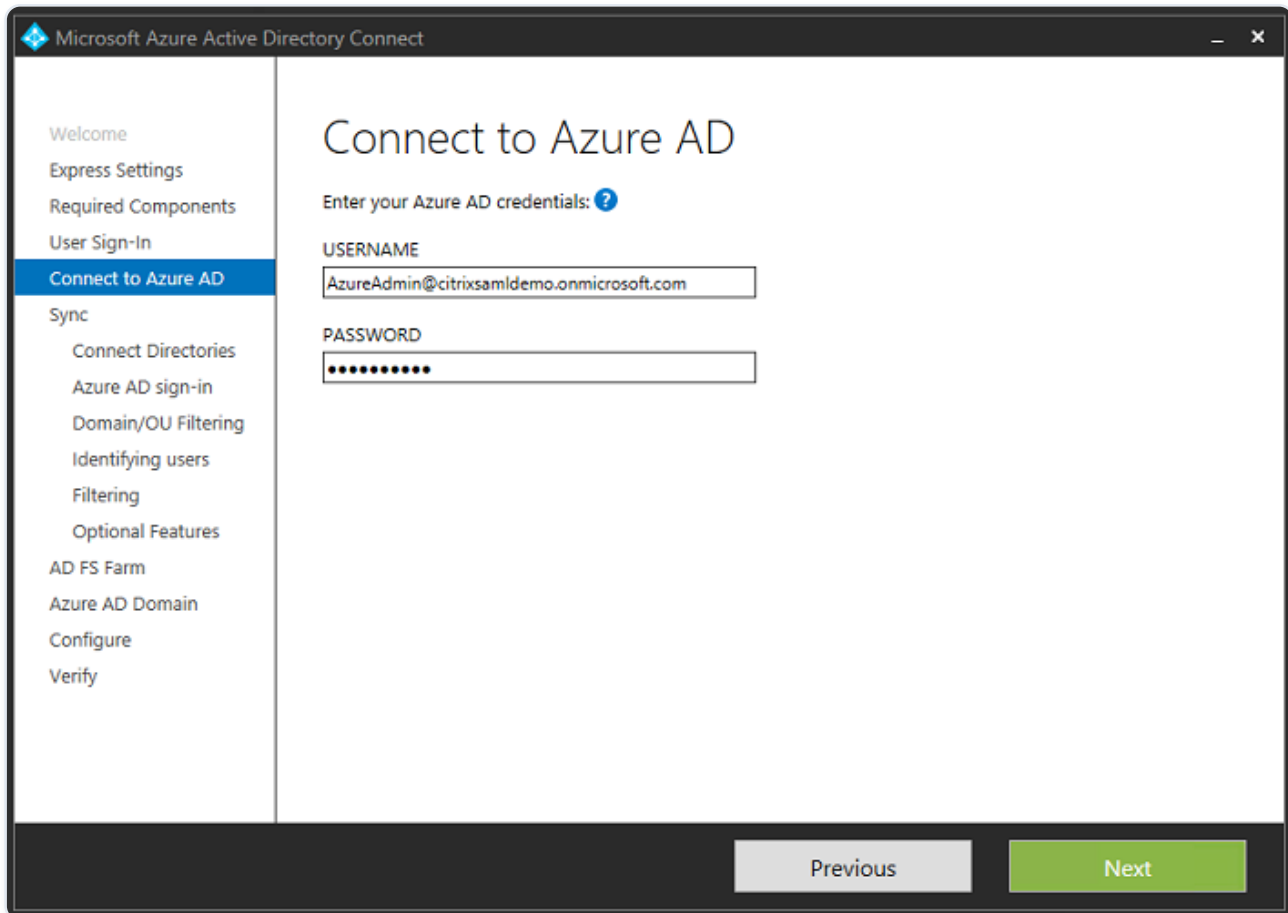
El paso 2 de la GUI de configuración de Azure AD redirige a la página de descarga de Microsoft para Azure AD Connect. Instálelo en la VM de ADFS. Utilice la **instalación personalizada**, en lugar de la **configuración rápida**, para que las opciones de ADFS estén disponibles.



Seleccione la opción de inicio de sesión único **Federación con AD FS**.



Conéctese a Azure con la cuenta de administrador que creó anteriormente.



The screenshot shows the 'Microsoft Azure Active Directory Connect' window. The left sidebar contains a list of steps: Welcome, Express Settings, Required Components, User Sign-In, **Connect to Azure AD** (highlighted), Sync, Connect Directories, Azure AD sign-in, Domain/OU Filtering, Identifying users, Filtering, Optional Features, AD FS Farm, Azure AD Domain, Configure, and Verify. The main area is titled 'Connect to Azure AD' and prompts the user to 'Enter your Azure AD credentials:'. It includes two input fields: 'USERNAME' with the value 'AzureAdmin@citrixsaml-demo.onmicrosoft.com' and 'PASSWORD' with masked characters. At the bottom right, there are 'Previous' and 'Next' buttons.

Seleccione el bosque de AD interno.

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

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

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

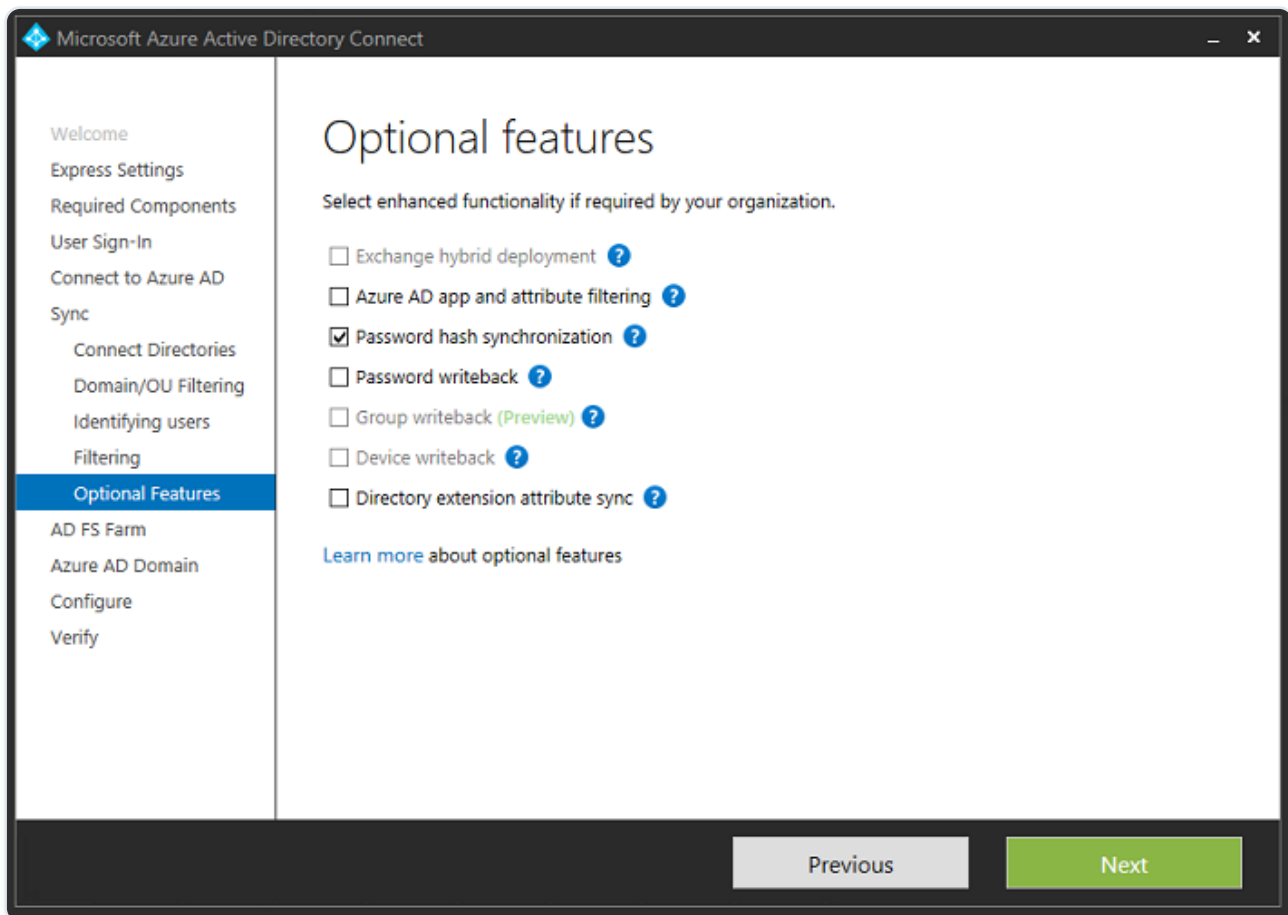
Si la estructura del directorio es sencilla, puede confiar en que los nombres de usuario son lo suficientemente únicos como para identificar a un usuario que inicia sesión.

The screenshot shows the 'Uniquely identifying your users' configuration window in Microsoft Azure Active Directory Connect. The window has a dark title bar and a sidebar on the left with navigation links: Welcome, Express Settings, Required Components, User Sign-In, Connect to Azure AD, Sync, Connect Directories, Domain/OU Filtering, Identifying users (highlighted), Filtering, Optional Features, AD FS Farm, Azure AD Domain, Configure, and Verify. The main content area is titled 'Uniquely identifying your users' and contains two sections. The first section, 'Select how users should be identified in your on-premises directories.', has a radio button selected for 'Users are represented only once across all directories.' and another radio button for 'User identities exist across multiple directories. Match using:', which is expanded to show options: 'Mail attribute' (selected), 'ObjectSID and msExchMasterAccountSID/msRTCSIP-OriginatorSID attributes', 'SAMAccountName and MailNickName attributes', and 'A specific attribute'. Below these is a 'CUSTOM ATTRIBUTE' dropdown menu. The second section, 'Select how users should be identified with Azure AD.', has a 'SOURCE ANCHOR' dropdown menu set to 'objectGUID' and a 'USER PRINCIPAL NAME' dropdown menu set to 'userPrincipalName'. At the bottom of the window are 'Previous' and 'Next' buttons.

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

The screenshot shows the 'Filter users and devices' window in the Microsoft Azure Active Directory Connect application. The window has a dark title bar with the Microsoft logo and the text 'Microsoft Azure Active Directory Connect'. On the left is a navigation pane with a list of steps: 'Welcome', 'Express Settings', 'Required Components', 'User Sign-In', 'Connect to Azure AD', 'Sync', 'Filtering' (highlighted in blue), 'Optional Features', 'AD FS Farm', 'Azure AD Domain', 'Configure', and 'Verify'. The main area is titled 'Filter users and devices' and contains the instruction: 'For a pilot deployment, specify a group containing your users and devices that will be synchronized.' Below this are two radio buttons: 'Synchronize all users and devices' (selected) and 'Synchronize selected' (with a question mark icon). Under 'Synchronize selected', there are two columns: 'FOREST' and 'GROUP'. The 'FOREST' column contains the text 'citrixsamldemo.cloudapp.net'. The 'GROUP' column has a text input field with the placeholder text 'Enter a name or DN of a group' and a 'Resolve' button to its right. At the bottom of the window are two buttons: 'Previous' (disabled) and 'Next' (active).

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



Seleccione el archivo PFX del certificado que se utilizará en AD FS, especificando fs.citrixsamldemo.net como nombre DNS.

Microsoft Azure Active Directory Connect

## AD FS Farm

Configure a new Windows Server 2012 R2 AD FS farm

Use an existing Windows Server 2012 R2 AD FS farm

Specify the SSL certificate used to secure the communication between clients and AD FS.

☒ Provide a PFX Certificate File

☐ Use a Certificate installed on the Federation Machines

CERTIFICATE FILE ?

C:\Users\Fred.CITRIXSAMLDEMO\Desktop\adfs.pfx Browse

SUBJECT NAME

\*.citrixsaml demo.net

SUBJECT NAME PREFIX

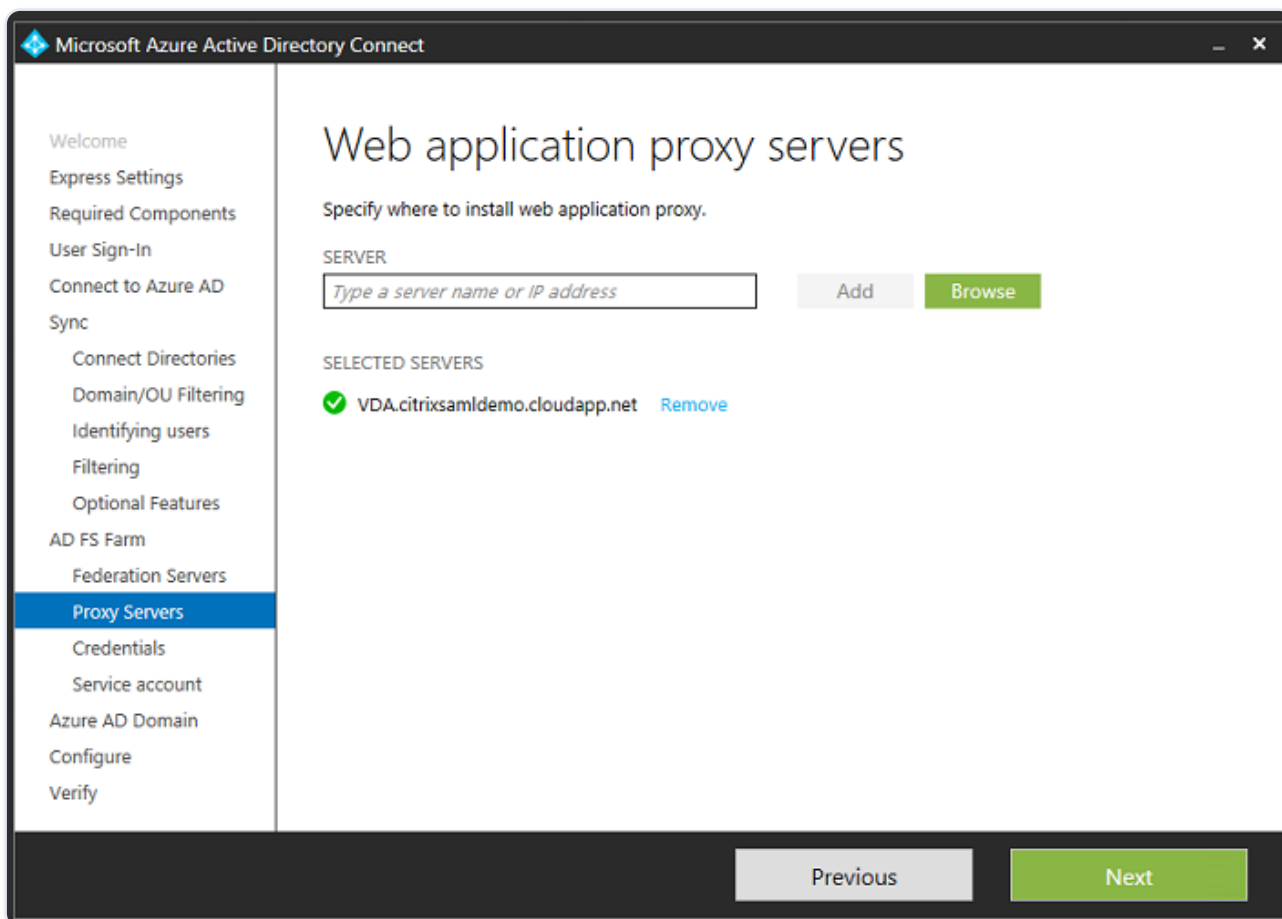
fs ✓

FEDERATION SERVICE NAME

https://fs.citrixsaml demo.net

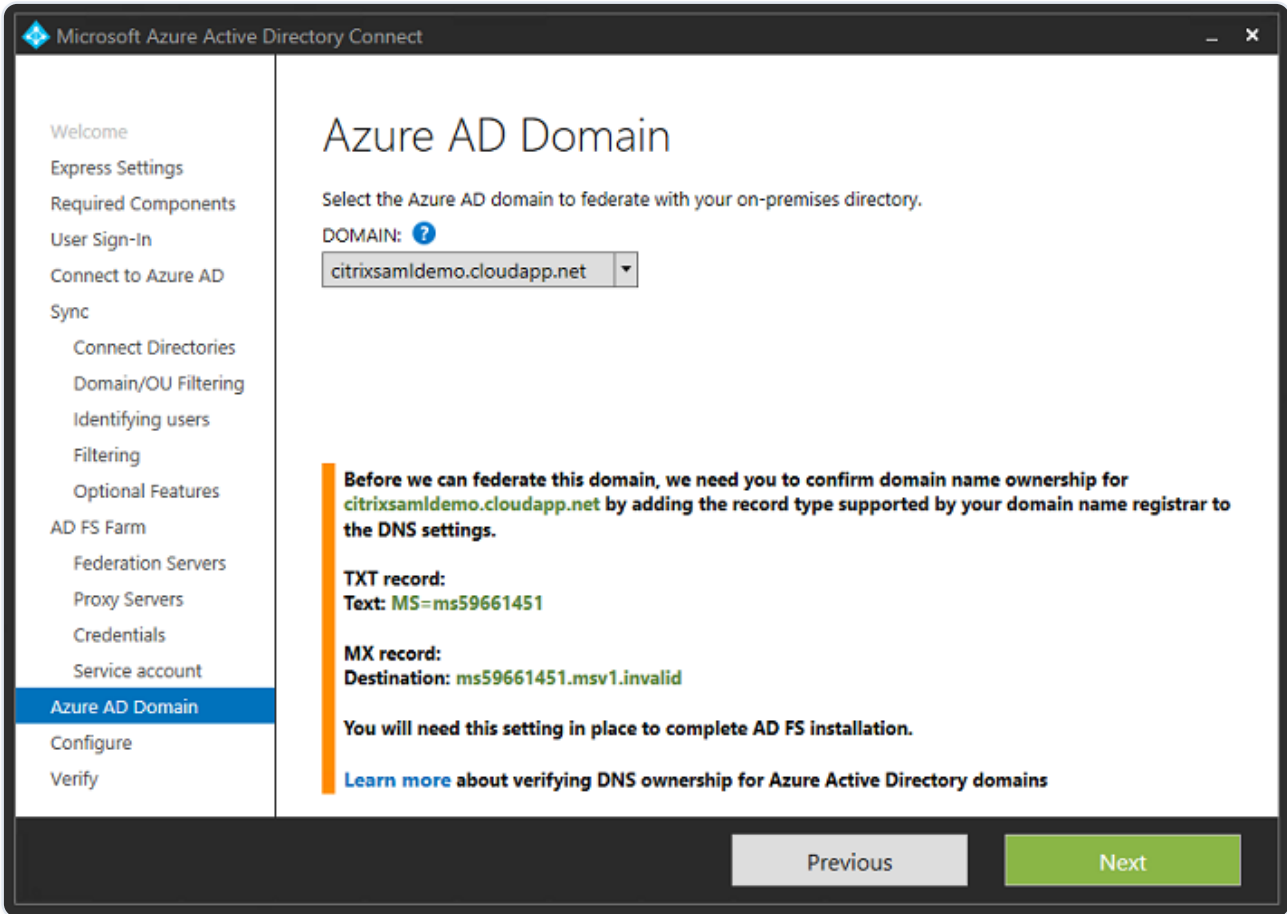
Previous Next

Cuando se le solicite que seleccione un servidor proxy, introduzca la dirección del servidor wap.citrixsaml demo.net. Es posible que deba ejecutar el cmdlet **Enable-PSRemoting -Force** como administrador en el servidor proxy de aplicación web para que Azure AD Connect pueda configurarlo.

**NOTA:**

Si este paso falla debido a problemas de confianza de PowerShell remoto, intente unir el servidor proxy de aplicación web al dominio.

Para los pasos restantes del asistente, utilice las contraseñas de administrador estándar y cree una cuenta de servicio para ADFS. Azure AD Connect le pedirá entonces que valide la propiedad de la zona DNS.



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

| Search record sets |       |        |                                                                                                                                                  |
|--------------------|-------|--------|--------------------------------------------------------------------------------------------------------------------------------------------------|
| NAME               | TYPE  | TTL    | VALUE                                                                                                                                            |
| @                  | NS    | 172800 | ns1-01.azure-dns.com.<br>ns2-01.azure-dns.net.<br>ns3-01.azure-dns.org.<br>ns4-01.azure-dns.info. ...                                            |
| @                  | SOA   | 3600   | Email: azuredns-hostmaster.microsoft...<br>Host: ns1-01.azure-dns.com.<br>Refresh: 3600<br>Retry: 300<br>Expire: 2419200<br>Minimum TTL: 300 ... |
| @                  | TXT   | 3600   | ms70102213 ...                                                                                                                                   |
| fs                 | CNAME | 3600   | adfs-citrixsamldemo.westeurope.cloud... ...                                                                                                      |

Haga clic en **verificar** en la Consola de administración de Azure.

CitrixSamIDemo



USERS

GROUPS

APPLICATIONS

DOMAINS

DIRECTORY INTEGRATION

CONFIGURE

REPORTS

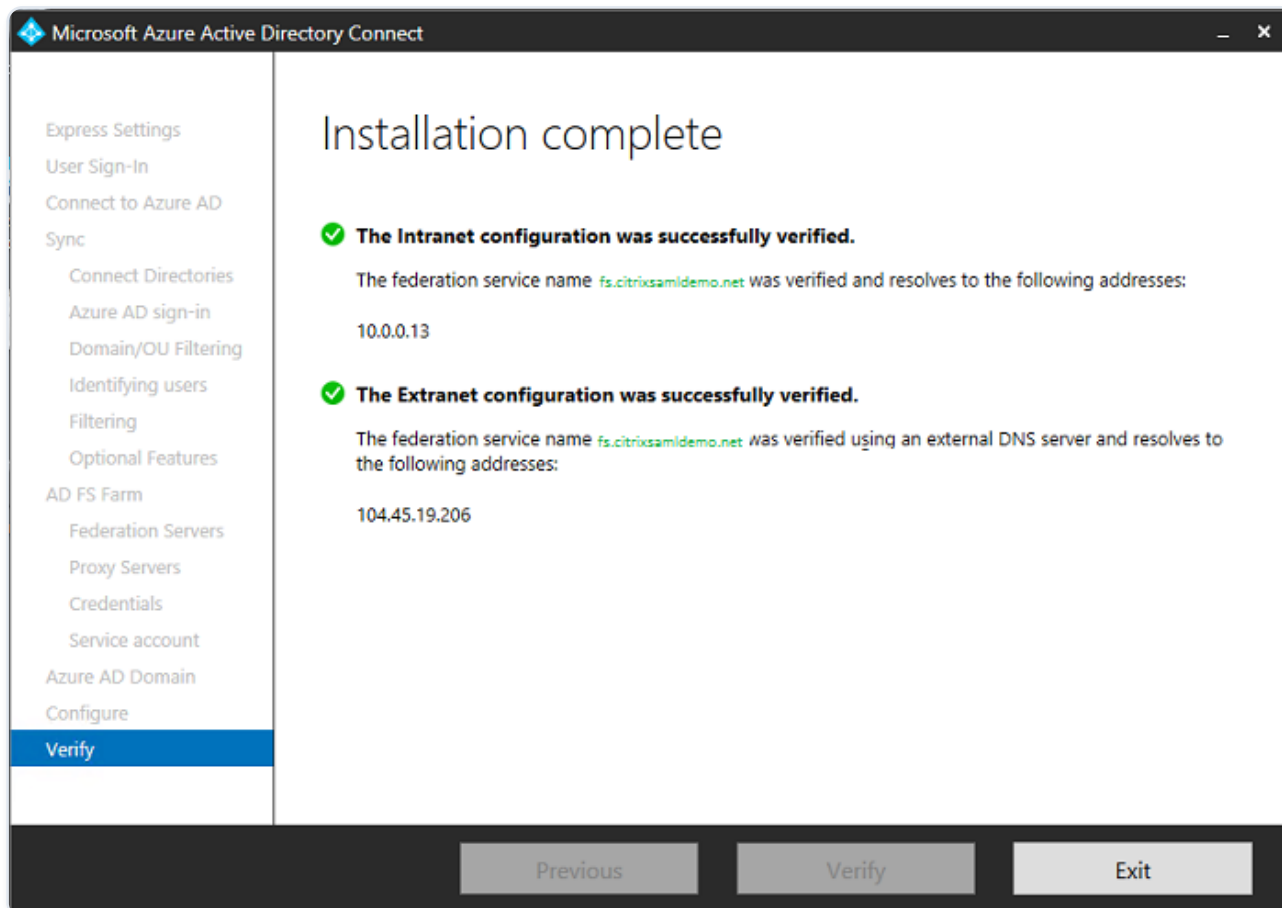
LICENSES

| DOMAIN NAME                    | TYPE   | STATUS                                                                                         | SINGLE SIGN-ON | PRIMARY DOMAIN |  |
|--------------------------------|--------|------------------------------------------------------------------------------------------------|----------------|----------------|---------------------------------------------------------------------------------------|
| citrixsamldemo.onmicrosoft.com | Basic  |  Active     | Not Available  | Yes            |                                                                                       |
| citrixsamldemo.net             | Custom |  Unverified | Not Configured | No             |                                                                                       |

**NOTA:**

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

Cuando se complete, se contactará con la dirección externa fs.citrixsamldemo.net a través del puerto 443.



## Habilitar la unión a Azure AD

Cuando un usuario introduce una dirección de correo electrónico para que Windows 10 pueda realizar la unión a Azure AD, el sufijo DNS se utiliza para construir un registro DNS CNAME que debe apuntar a ADFS: `enterpriseregistration.\<upnsuffix>`.

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

enterpriseregistration.citrixsaml demo.net

Type

CNAME

\* TTL

1

TTL unit

Minutes

Alias

fs.citrixsaml demo.net

Si no está utilizando una autoridad de certificación pública, asegúrese de que el certificado raíz de ADFS esté instalado en el equipo con Windows 10 para que Windows confíe en el servidor ADFS. Realice una unión a un dominio de Azure AD utilizando la cuenta de usuario estándar generada anteriormente.

Let's get you signed in

Work or school account

George@citrixsaml demo.net

Password

[I forgot my password](#)

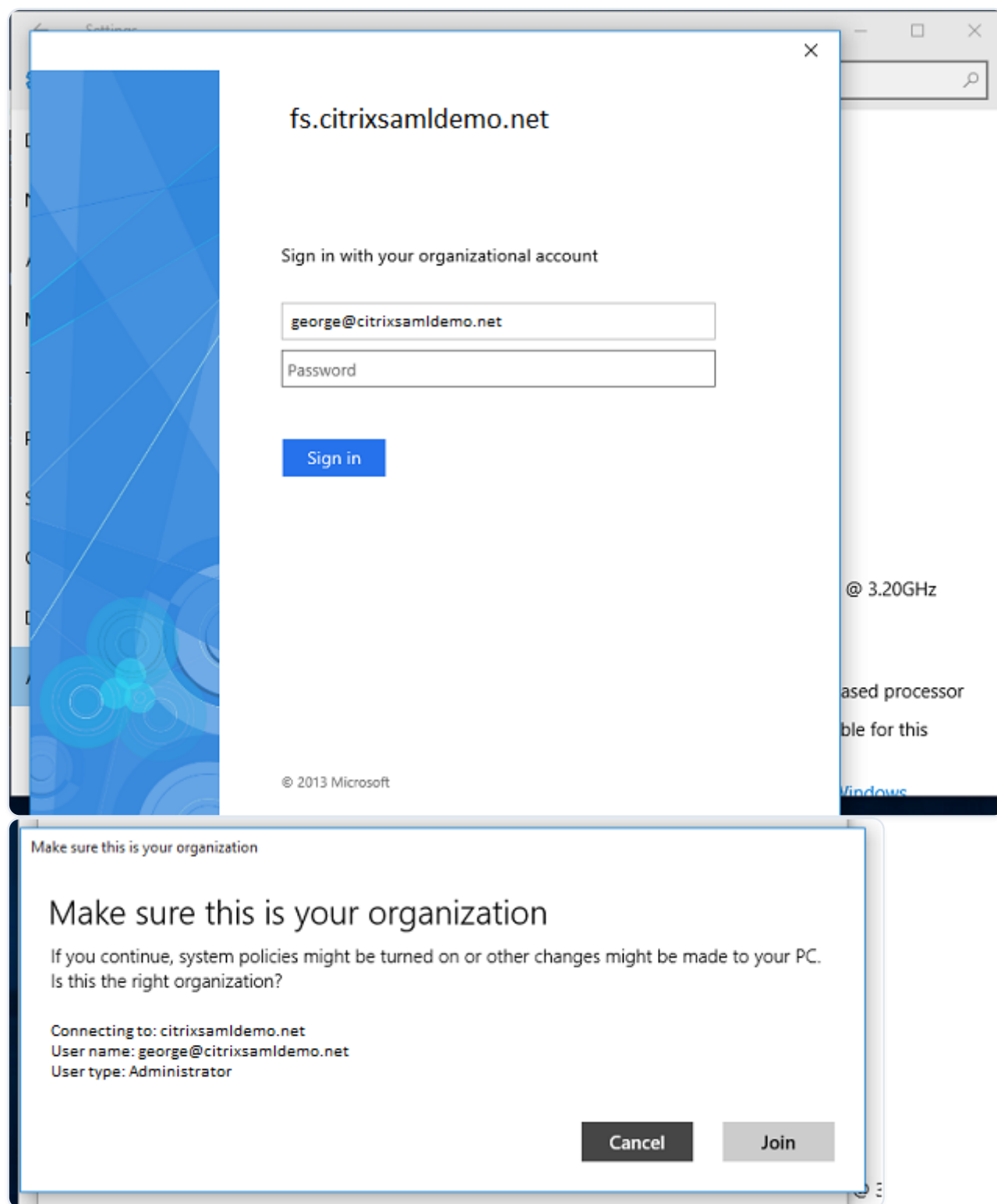
Which account should I use?

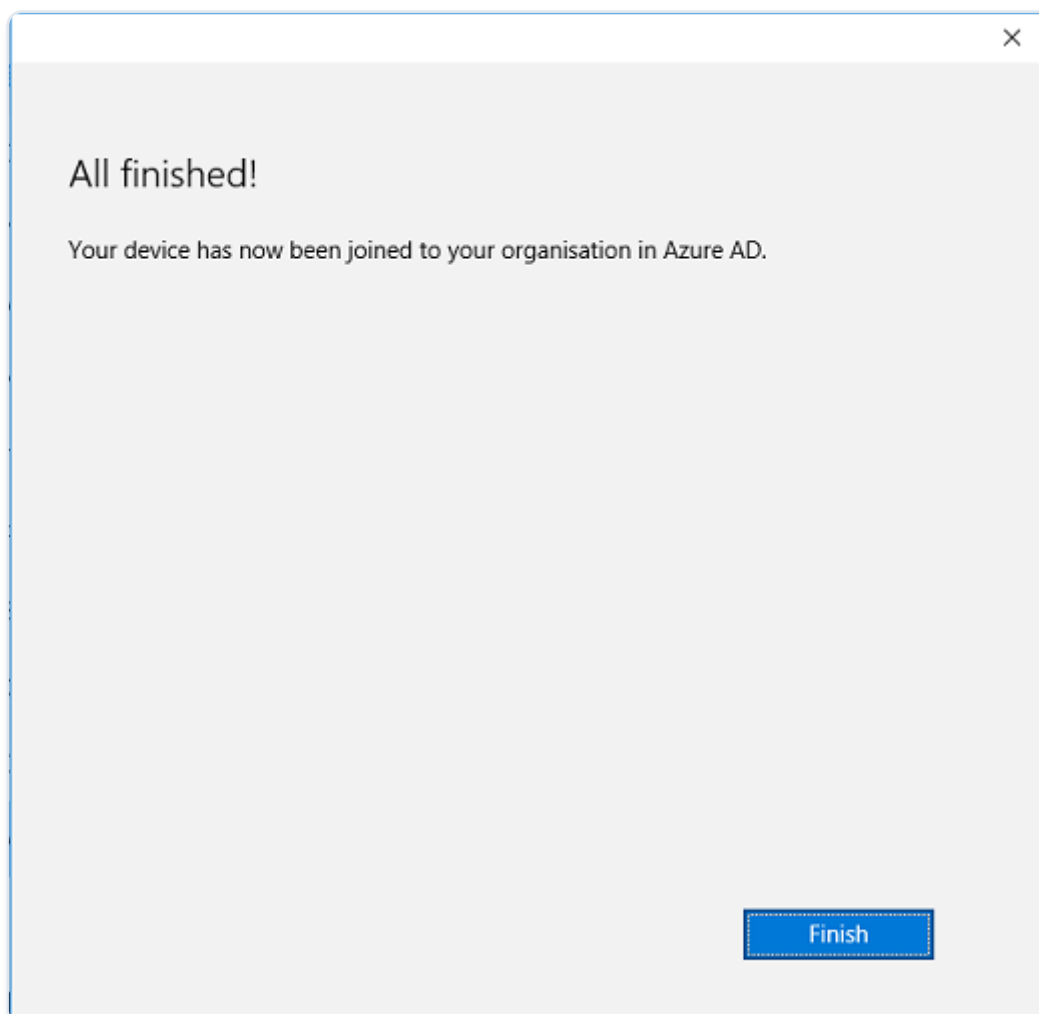
Sign in with the username and password you use with Office 365 (or other business services from Microsoft).

[Privacy statement](#)

Sign in Back

Tenga en cuenta que el UPN debe coincidir con el UPN reconocido por el controlador de dominio de ADFS.



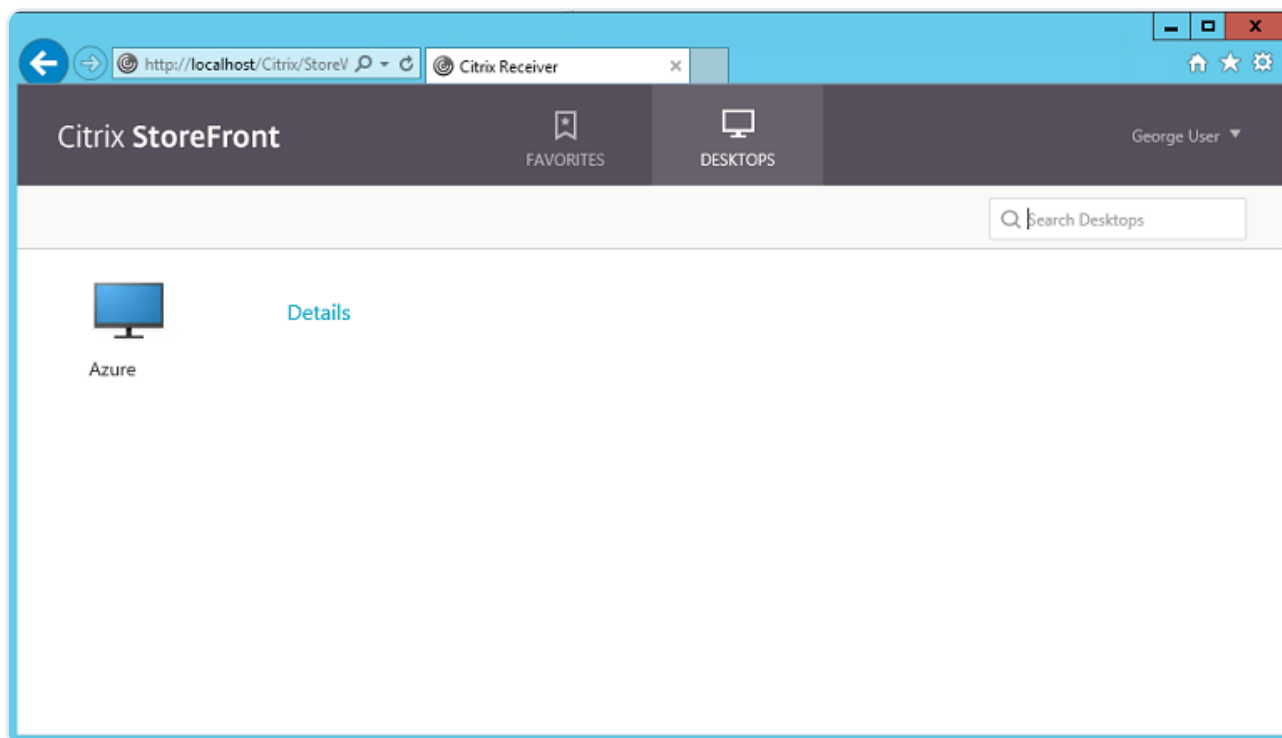


verificar que la unión a Azure AD se realizó correctamente reiniciando la máquina e iniciando sesión con la dirección de correo electrónico del usuario. Una vez iniciada la sesión, inicie Microsoft Edge y conéctese a `<http://myapps.microsoft.com>`. El sitio web debería utilizar el inicio de sesión único automáticamente.

## Instalar Citrix Virtual Apps o Citrix Virtual Desktops

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

En este ejemplo, StoreFront está instalado en el mismo servidor que el Delivery Controller. El VDA se instala como un trabajador RDS de Windows 2012 R2 independiente, sin integrarse con Machine Creation Services (aunque esto se puede configurar opcionalmente). Compruebe que el usuario [George@citrixsamldemo.net](mailto:George@citrixsamldemo.net) puede autenticarse con una contraseña antes de continuar.



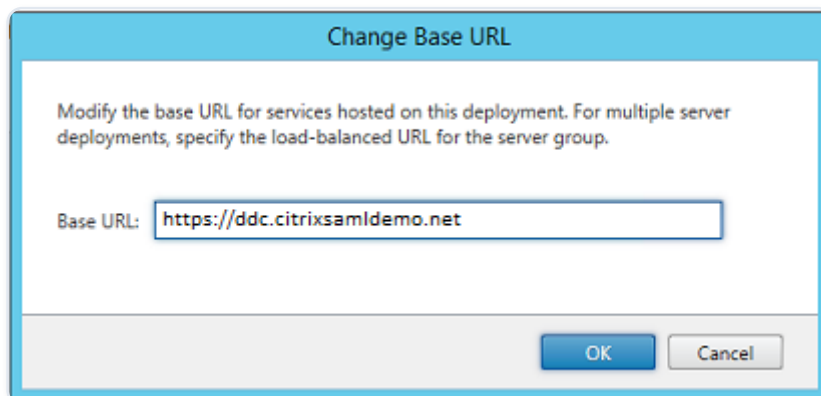
Ejecute el cmdlet de PowerShell **Set-BrokerSite -TrustRequestsSentToTheXmlServicePort \$true** en el Controller para permitir que StoreFront™ se autentique sin las credenciales de los usuarios.

## Instalar el Servicio de autenticación federada

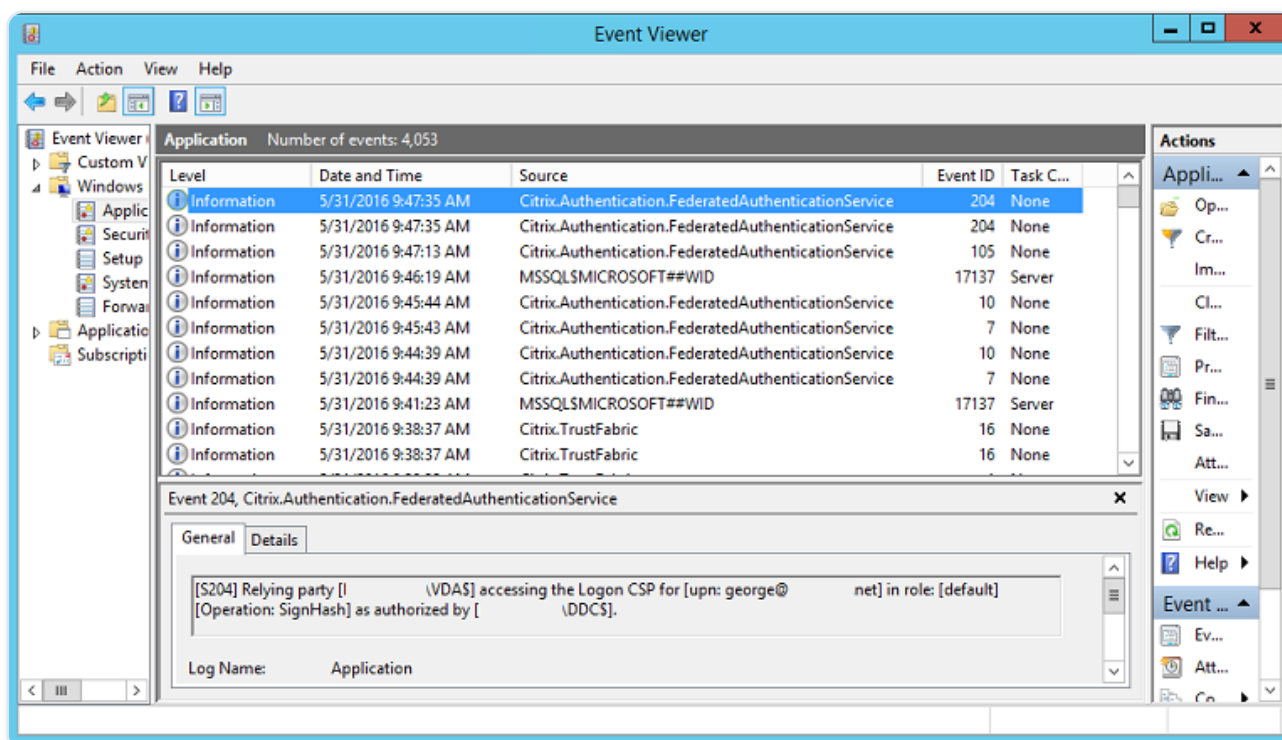
Instale FAS en el servidor ADFS y configure una regla para que el Delivery Controller actúe como un StoreFront de confianza (ya que, en este ejemplo, StoreFront está instalado en la misma VM que el Delivery Controller). Consulte [Instalar y configurar](#).

## 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 base de StoreFront a https:.

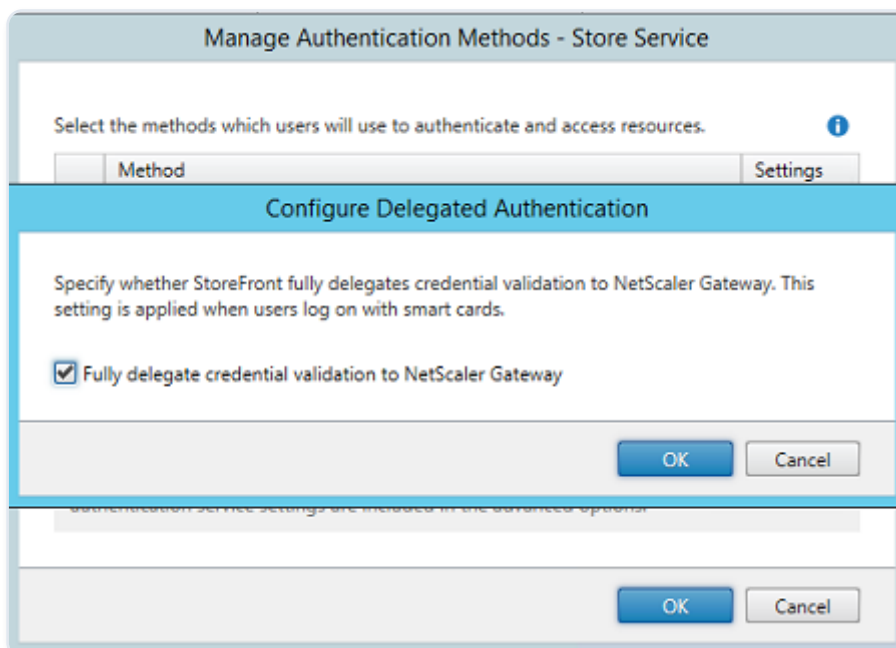


Configure StoreFront para usar el servidor FAS (utilice el script de PowerShell en [Instalar y configurar](#)), y pruebe internamente en Azure, asegurándose de que el inicio de sesión utiliza FAS comprobando el visor de eventos en el servidor FAS.

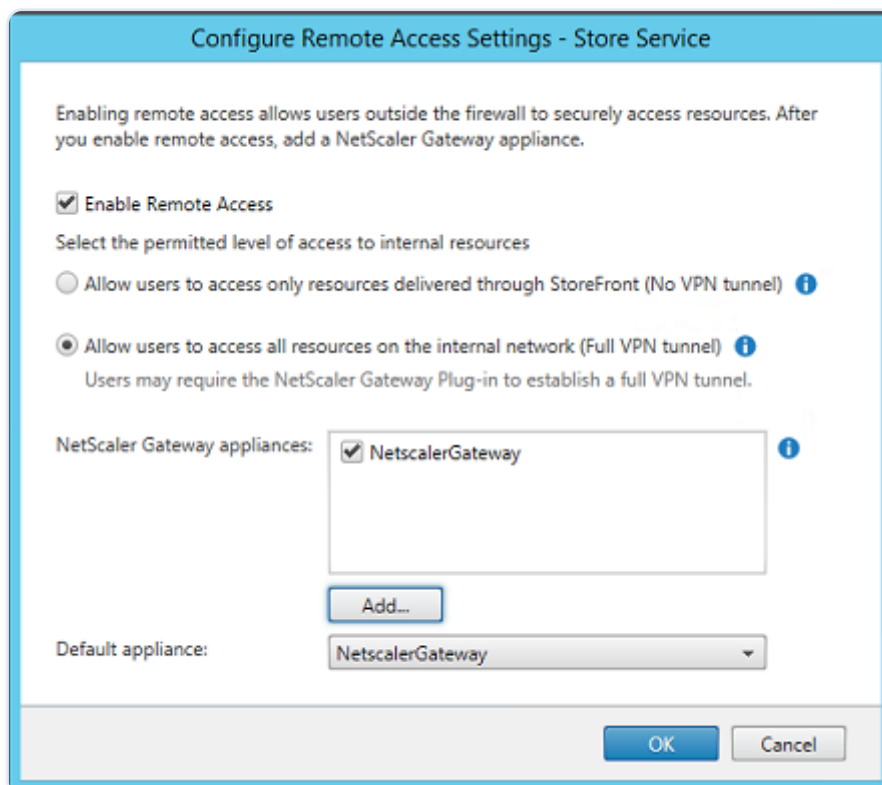


## Configurar StoreFront para usar Citrix Gateway

Mediante la GUI de **Administrar métodos de autenticación** en la consola de administración de StoreFront, configure StoreFront para usar Citrix Gateway para realizar la autenticación.

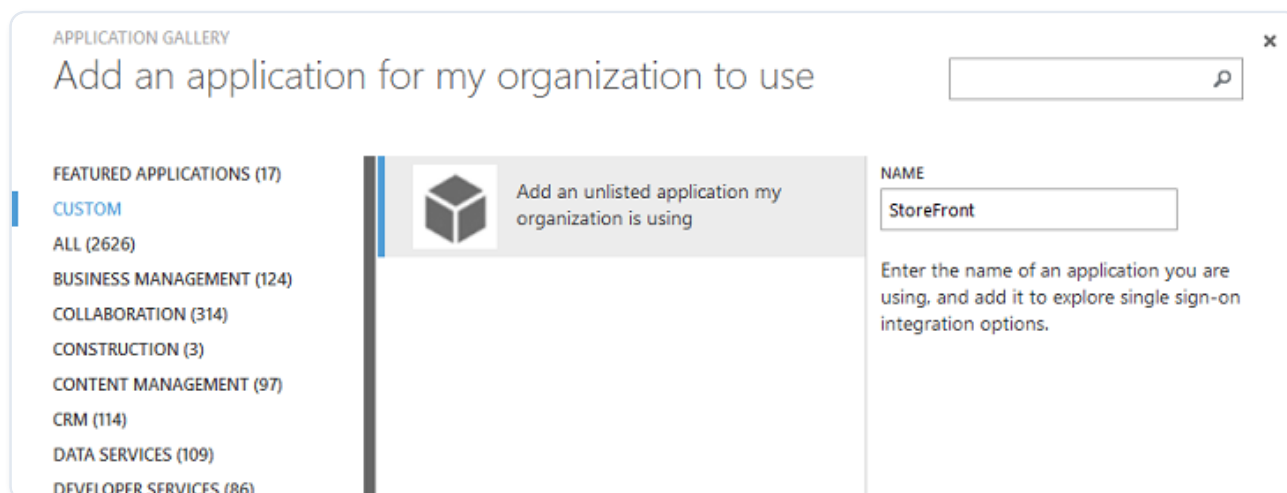


Para integrar las opciones de autenticación de Citrix Gateway, configure una Secure Ticket Authority (STA) y configure la dirección de Citrix Gateway.



## Configurar una nueva aplicación de Azure AD para el inicio de sesión único en StoreFront

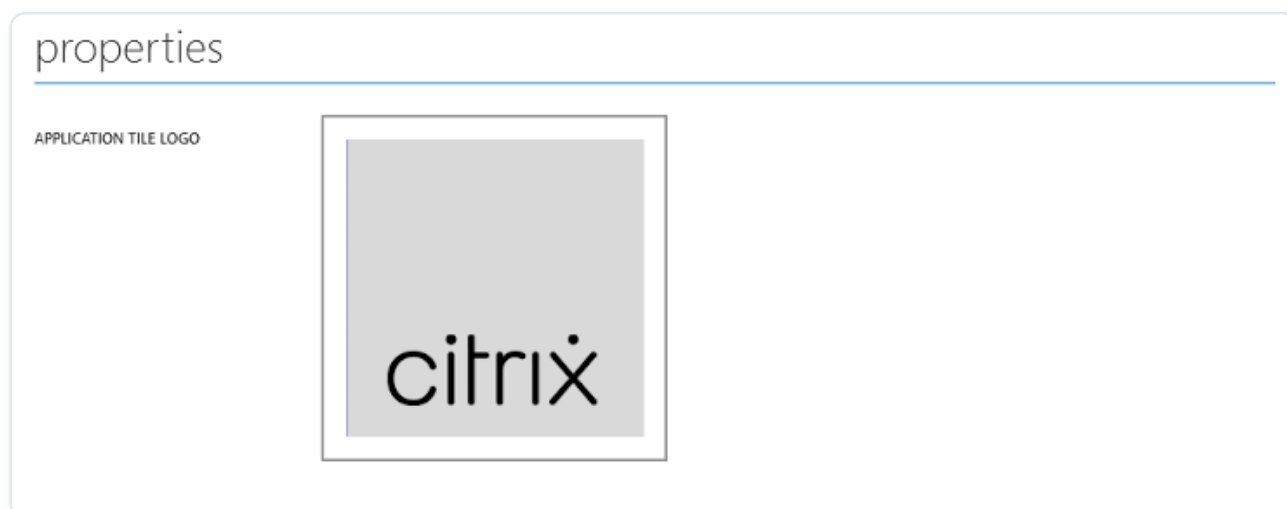
Esta sección utiliza las funciones de inicio de sesión único de Azure AD SAML 2.0, que actualmente requieren una suscripción a Azure Active Directory Premium. En la herramienta de administración de Azure AD, seleccione **Nueva aplicación** y elija **Agregar una aplicación de la Galería**.



Seleccione **PERSONALIZADO > Agregar una aplicación no listada que mi organización está usando** para crear una nueva aplicación personalizada para sus usuarios.

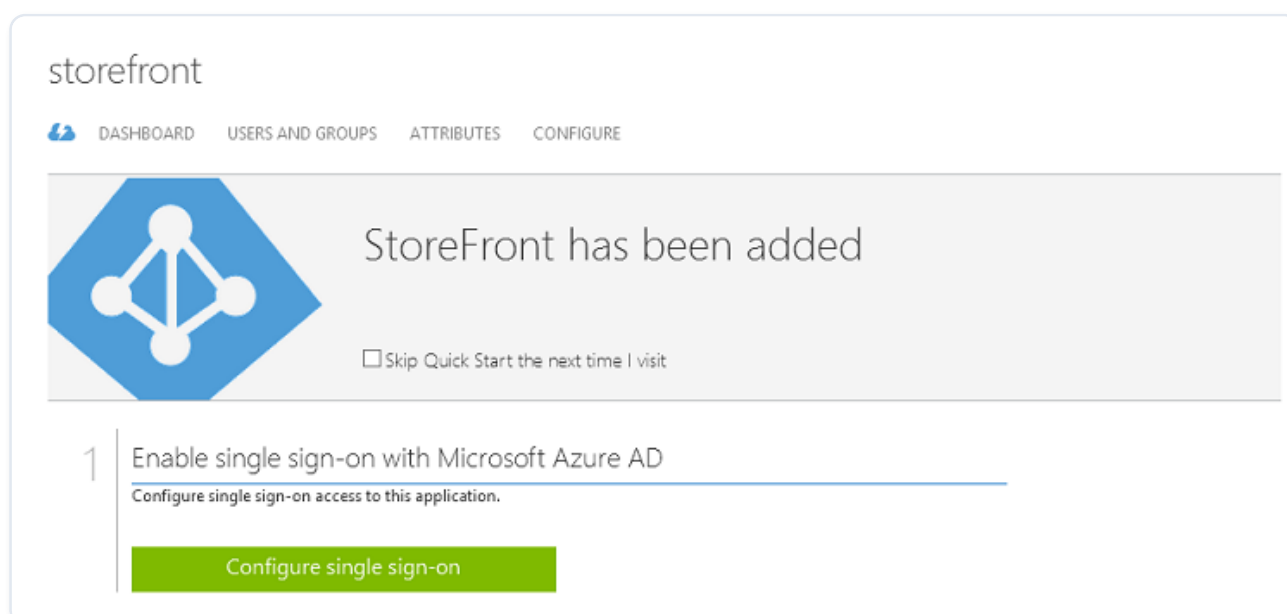
## Configurar un icono

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



## Configurar la autenticación SAML

Vuelva a la página de información general del panel de la aplicación y seleccione **Configurar inicio de sesión único**.



Esta implementación utilizará la autenticación SAML 2.0, que corresponde a **Inicio de sesión único de Microsoft Azure AD**.

CONFIGURE SINGLE SIGN-ON

## How would you like users to sign on to StoreFront?

- ☒ **Microsoft Azure AD Single Sign-On**  
Establish federation between Microsoft Azure AD and StoreFront  
[Learn more](#)
- ☐ **Password Single Sign-On**  
Microsoft Azure AD stores account credentials for users to sign on to StoreFront  
[Learn more](#)
- ☐ **Existing Single Sign-On**  
Configures Microsoft Azure AD to support single sign-on to StoreFront using Active Directory Federation Services or another third-party single sign-on provider.  
[Learn more](#)

El **Identificador** puede ser una cadena arbitraria (debe coincidir con la configuración proporcionada a Citrix Gateway); en este ejemplo, la **URL de respuesta** es `/cgi/samlauth` en el servidor de Citrix Gateway.

CONFIGURE SINGLE SIGN-ON

## Configure App Settings

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

IDENTIFIER ?  
 ✓

REPLY URL ?  
 ✓

☐ Show advanced settings (optional).

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

La siguiente página contiene información que se utiliza para configurar Citrix Gateway como parte de confianza para Azure AD.

CONFIGURE SINGLE SIGN-ON

## Configure single sign-on at AzureStoreFront

To accept the SAML token issued by Azure Active Directory, your application will need the information below. Refer to your application's SAML documentation or source code for details.

- The following certificate will be used for federated single sign-on:  
Thumbprint: 8D1E02EBF7C111EDDBBD325F5260538A9626A73B  
Expiry: 05/31/2018 11:06:20 UTC  
  
[Download Certificate \(Base 64 - most common\)](#)
[Download Certificate \(Raw\)](#)
[Download Metadata \(XML\)](#)
- Configure the certificate and values in AzureStoreFront  

ISSUER URL

SINGLE SIGN-ON SERVICE URL

SINGLE SIGN-OUT SERVICE URL

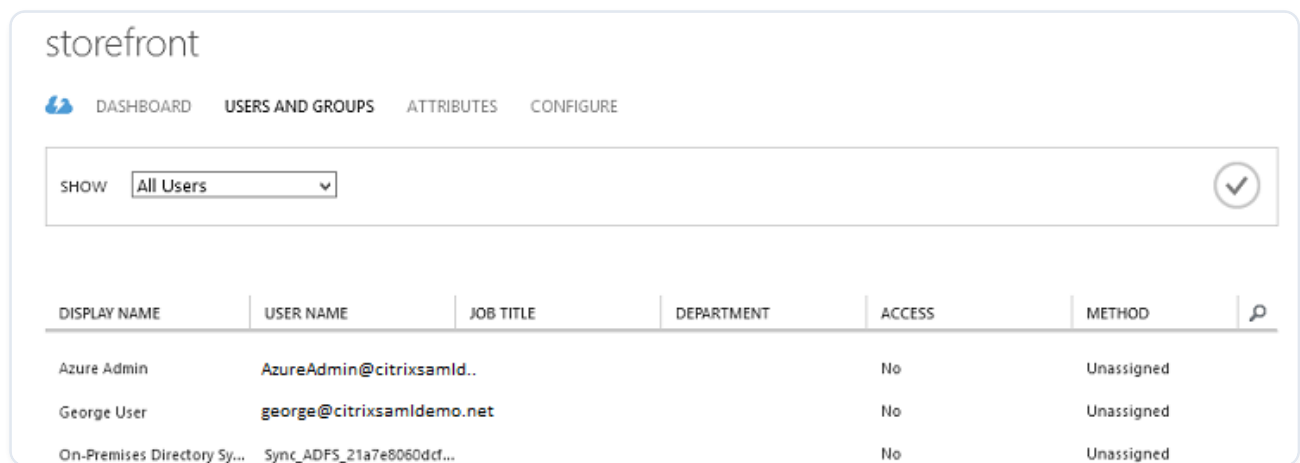
☐ Confirm that you have configured single sign-on as described above. Checking this will enable the current certificate to start working for this application.

← →

Descargue el certificado de firma de confianza base 64 y copie las URL de inicio y cierre de sesión. Las pegará más tarde en las pantallas de configuración de Citrix Gateway.

## Asignar la aplicación a los usuarios

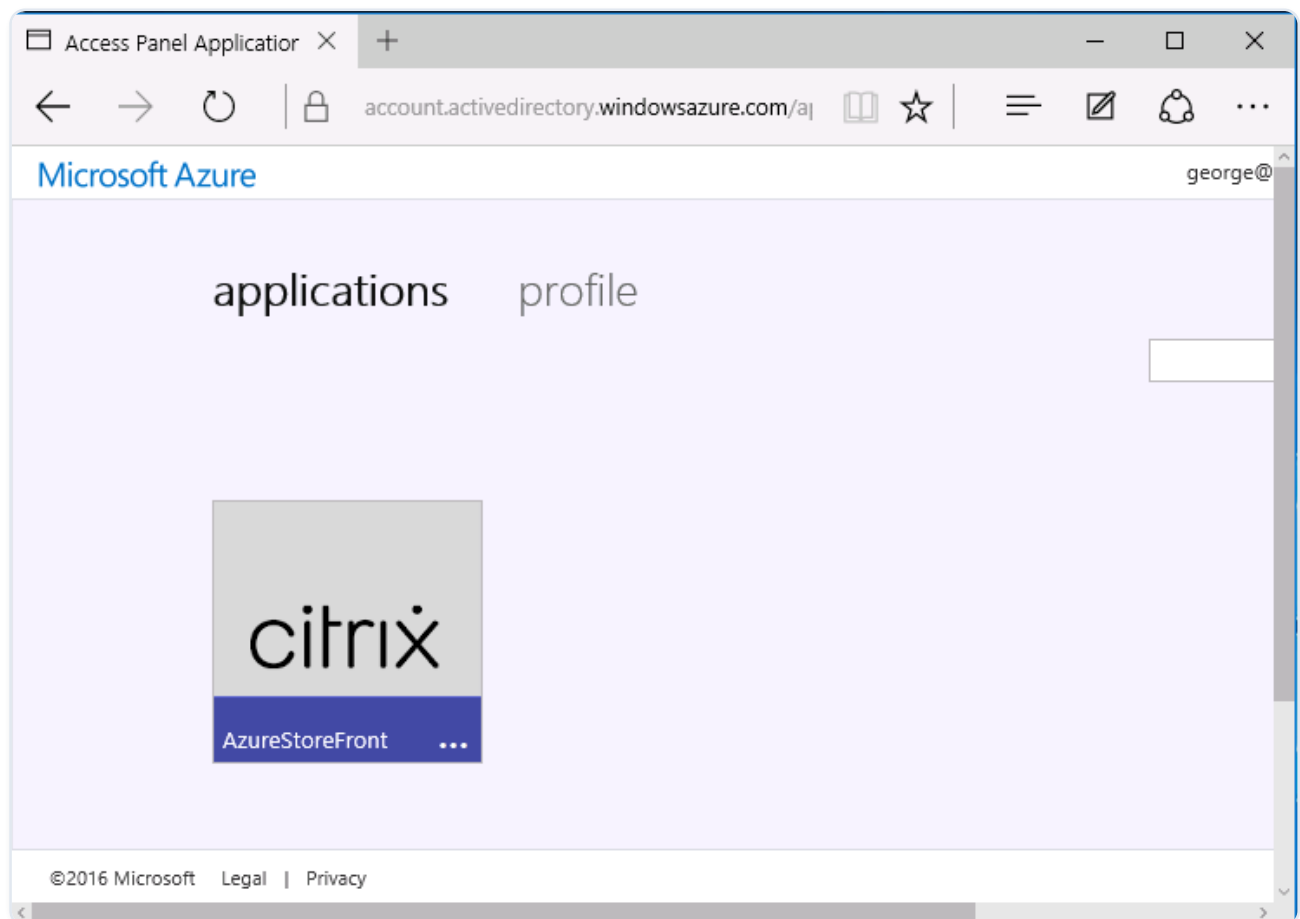
El paso final es habilitar la aplicación para que aparezca en la página de control "myapps.microsoft.com" de los usuarios. Esto se hace en la página USUARIOS Y GRUPOS. Asigne acceso a las cuentas de usuario de dominio sincronizadas por Azure AD Connect. También se pueden usar otras cuentas, pero deben asignarse explícitamente porque no se ajustan al patrón \&lt;user>@\&lt;domain>.



| DISPLAY NAME                | USER NAME                 | JOB TITLE | DEPARTMENT | ACCESS | METHOD     |
|-----------------------------|---------------------------|-----------|------------|--------|------------|
| Azure Admin                 | AzureAdmin@citrixsamld..  |           |            | No     | Unassigned |
| George User                 | george@citrixsamldemo.net |           |            | No     | Unassigned |
| On-Premises Directory Sy... | Sync_ADFS_21a7e8060dcf... |           |            | No     | Unassigned |

## Página de MyApps

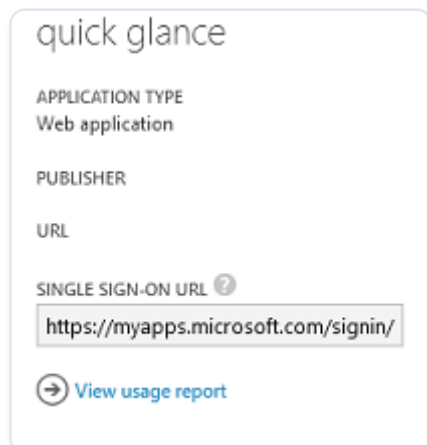
Cuando la aplicación se ha configurado, aparece en las listas de aplicaciones de Azure de los usuarios cuando visitan `<https://myapps.microsoft.com>`.



Cuando está unido a Azure AD, Windows 10 admite el inicio de sesión único en las aplicaciones de Azure para el usuario que inicia sesión. Al hacer clic en el icono, el navegador se dirige a la página web SAML `cgi/samlauth` que se configuró anteriormente.

## URL de inicio de sesión único

Vuelva a la aplicación en el panel de Azure AD. Ahora hay una URL de inicio de sesión único disponible para la aplicación. Esta URL se utiliza para proporcionar enlaces de navegador web o para crear accesos directos en el menú Inicio que lleven a los usuarios directamente a StoreFront.



Pegue esta URL en un navegador web para asegurarse de que Azure AD le redirige a la página web cgi/samlauth de Citrix Gateway configurada anteriormente. Esto solo funciona para los usuarios a los que se les ha asignado y solo proporcionará inicio de sesión único para las sesiones de inicio de sesión de Windows 10 unidas a Azure AD. (A otros usuarios se les solicitarán las credenciales de Azure AD).

## Instalar y configurar Citrix Gateway

Para acceder de forma remota a la implementación, este ejemplo utiliza una VM separada que ejecuta NetScaler (ahora Citrix Gateway). Esto se puede adquirir en Azure Store. Este ejemplo utiliza la versión "Bring your own License" de NetScaler 11.0.

Inicie sesión en la VM de NetScaler®, apuntando un navegador web a la dirección IP interna, utilizando las credenciales especificadas cuando el usuario se autenticó. Tenga en cuenta que debe cambiar la contraseña del usuario nsroot en una VM de Azure AD.

Agregue licencias, seleccionando **reiniciar** después de agregar cada archivo de licencia, y apunte el resolutor DNS al controlador de dominio de Microsoft.

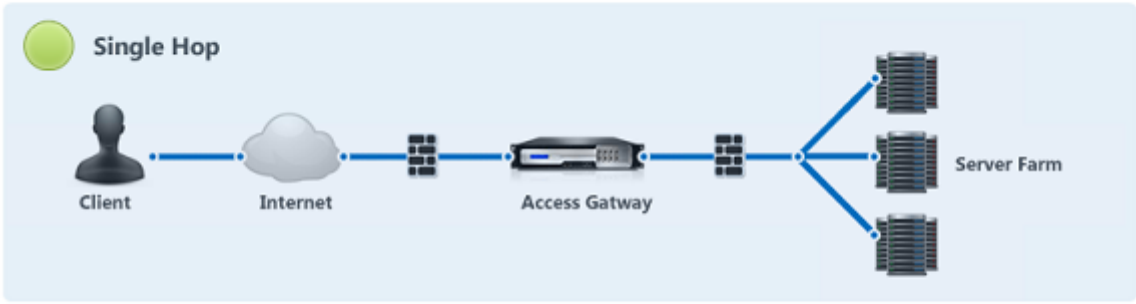
## Ejecute el asistente de configuración de Citrix Virtual Apps and Desktops

Este ejemplo comienza configurando una integración sencilla de StoreFront sin SAML. Una vez que esa implementación funciona, añade una política de inicio de sesión SAML.

**XenApp/XenDesktop Setup Wizard**

What is your deployment

**Single Hop**



The diagram illustrates the 'Single Hop' deployment architecture. It shows a 'Client' (represented by a person icon) connecting to the 'Internet' (cloud icon). From the Internet, the connection goes through a series of network components (routers and switches) to an 'Access Gateway' (server rack icon). Finally, the connection is routed through another set of network components to a 'Server Farm' (multiple server rack icons).

What is your Citrix Integration Point?

StoreFront

Continue Cancel

Seleccione la configuración estándar de Citrix Gateway StoreFront. Para su uso en Microsoft Azure, este ejemplo configura el puerto 4433, en lugar del puerto 443. Alternativamente, puede reenviar o reasignar el puerto del sitio web administrativo de Citrix Gateway.

**NetScaler Gateway Settings**

NetScaler Gateway IP Address\*

10 . 0 . 0 . 18

Port\*

4433

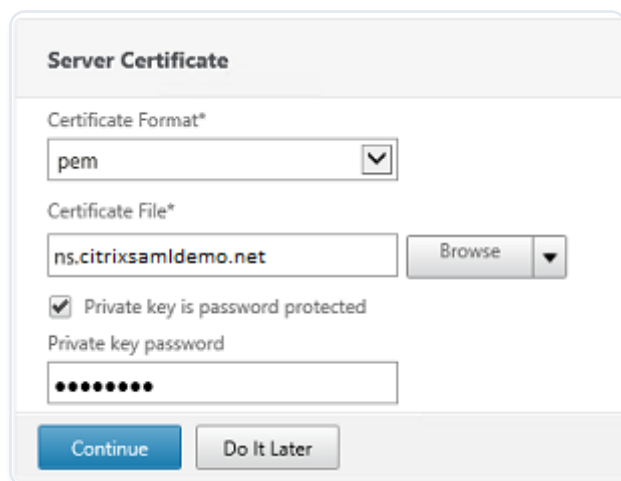
Virtual Server Name\*

ns.citrixsaml demo.net

☐ Redirect requests from port 80 to secure port

Continue Cancel

Para simplificar, el ejemplo carga un certificado de servidor y una clave privada existentes almacenados en un archivo.



**Server Certificate**

Certificate Format\*  
pem

Certificate File\*  
ns.citrixsamldemo.net Browse

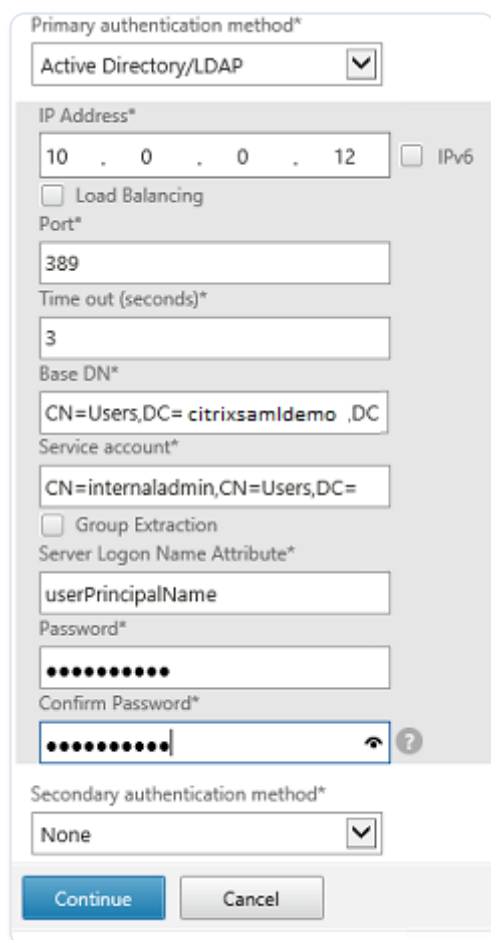
☒ Private key is password protected

Private key password  
.....

Continue Do It Later

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

El controlador de dominio se utilizará para la resolución de cuentas, así que añada su dirección IP al método de autenticación principal. Tenga en cuenta los formatos esperados en cada campo del cuadro de diálogo.



Primary authentication method\*  
Active Directory/LDAP

IP Address\*  
10 . 0 . 0 . 12 IPv6

☐ Load Balancing

Port\*  
389

Time out (seconds)\*  
3

Base DN\*  
CN=Users,DC= citrixsamldemo ,DC

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

☐ Group Extraction

Server Logon Name Attribute\*  
userPrincipalName

Password\*  
.....

Confirm Password\*  
.....

Secondary authentication method\*  
None

Continue Cancel

## Configurar la dirección de StoreFront

En este ejemplo, StoreFront se ha configurado utilizando HTTPS, así que seleccione las opciones de protocolo SSL.

**StoreFront**

StoreFront FQDN\*

ddc.citrixsamldemo.net

Site Path\*

/Citrix/StoreWeb

Single Sign-on Domain\*

citrixsamldemo

Store Name\*

/Citrix/StoreWeb

Secure Ticket Authority Server\*

http://ddc.citrixsamldemo.net/sta

StoreFront Server\*

10 . 0 . 0 . 15

Protocol\*

SSL

Port\*

443

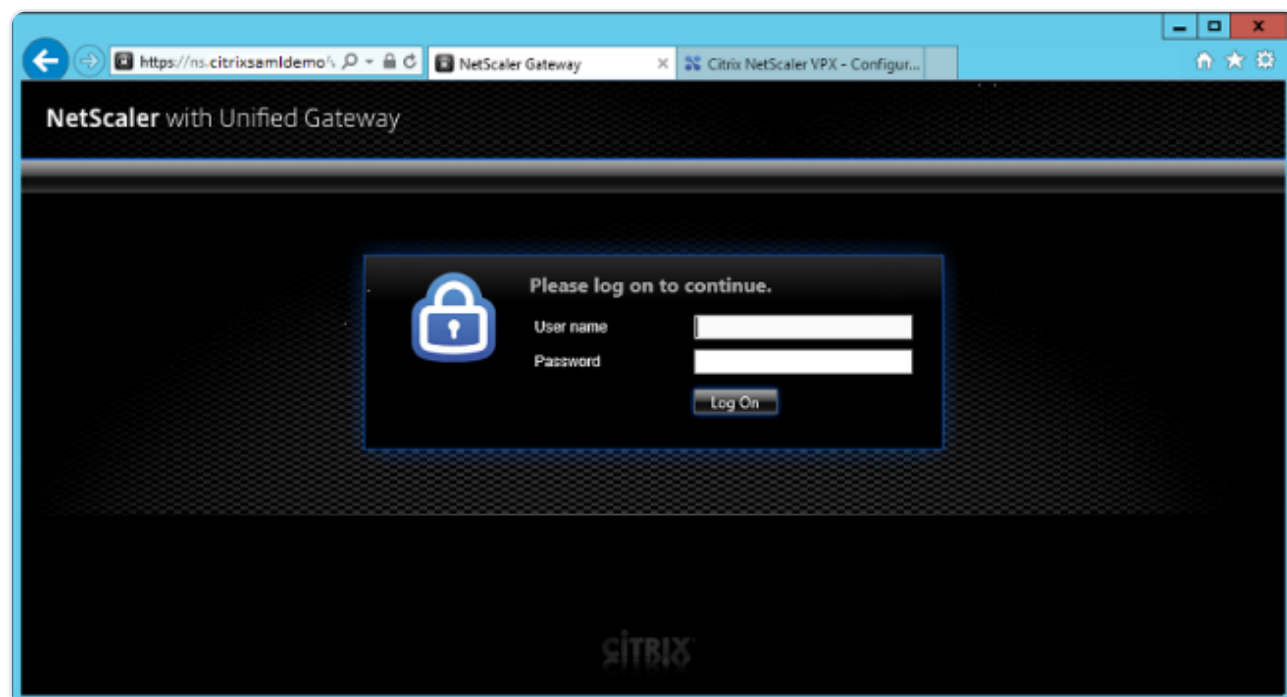
☐ Load Balancing

Continue

Cancel

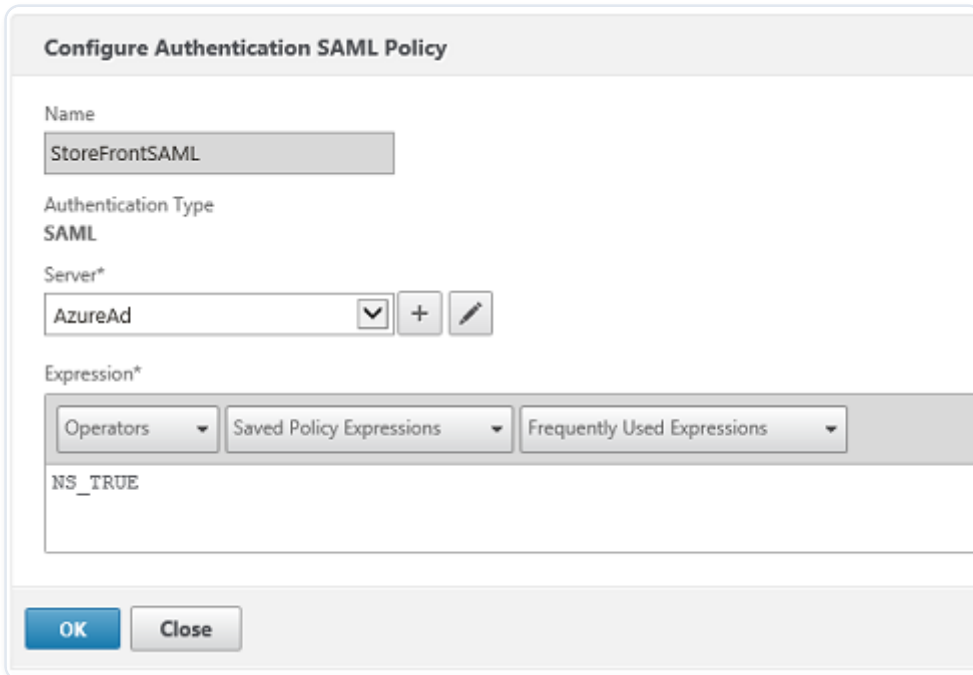
## verificar la implementación de Citrix Gateway

Conéctese a Citrix Gateway y compruebe que la autenticación y el inicio son correctos 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 SAML, con una expresión de **NS\_TRUE**.



**Configure Authentication SAML Policy**

Name  
StoreFrontSAML

Authentication Type  
SAML

Server\*  
AzureAd

Expression\*  
Operators Saved Policy Expressions Frequently Used Expressions  
NS\_TRUE

OK Close

Configure el nuevo servidor IdP de SAML, utilizando la información obtenida de Azure AD anteriormente.

### Create Authentication SAML Server

### Create Authentication SAML Server

Name\*

Authentication Type

SAML

IDP Certificate Name\*

Redirect URL\*

Single Logout URL

User Field

Signing Certificate Name

Issuer Name

Reject Unsigned Assertion\*

SAML Binding\*

Default Authentication Group

Skew Time(mins)

5

Two Factor

☐ ON ☒ OFF

Assertion Consumer Service Index

Attribute Consuming Service Index

Requested Authentication Context\*

Authentication Class Types



Signature Algorithm\*

☐ RSA-SHA1 ☒ RSA-SHA256

Digest Method\*

☐ SHA1 ☒ SHA256

☐ Send Thumbprint

☒ Enforce Username

Attribute 1

Attribute 3

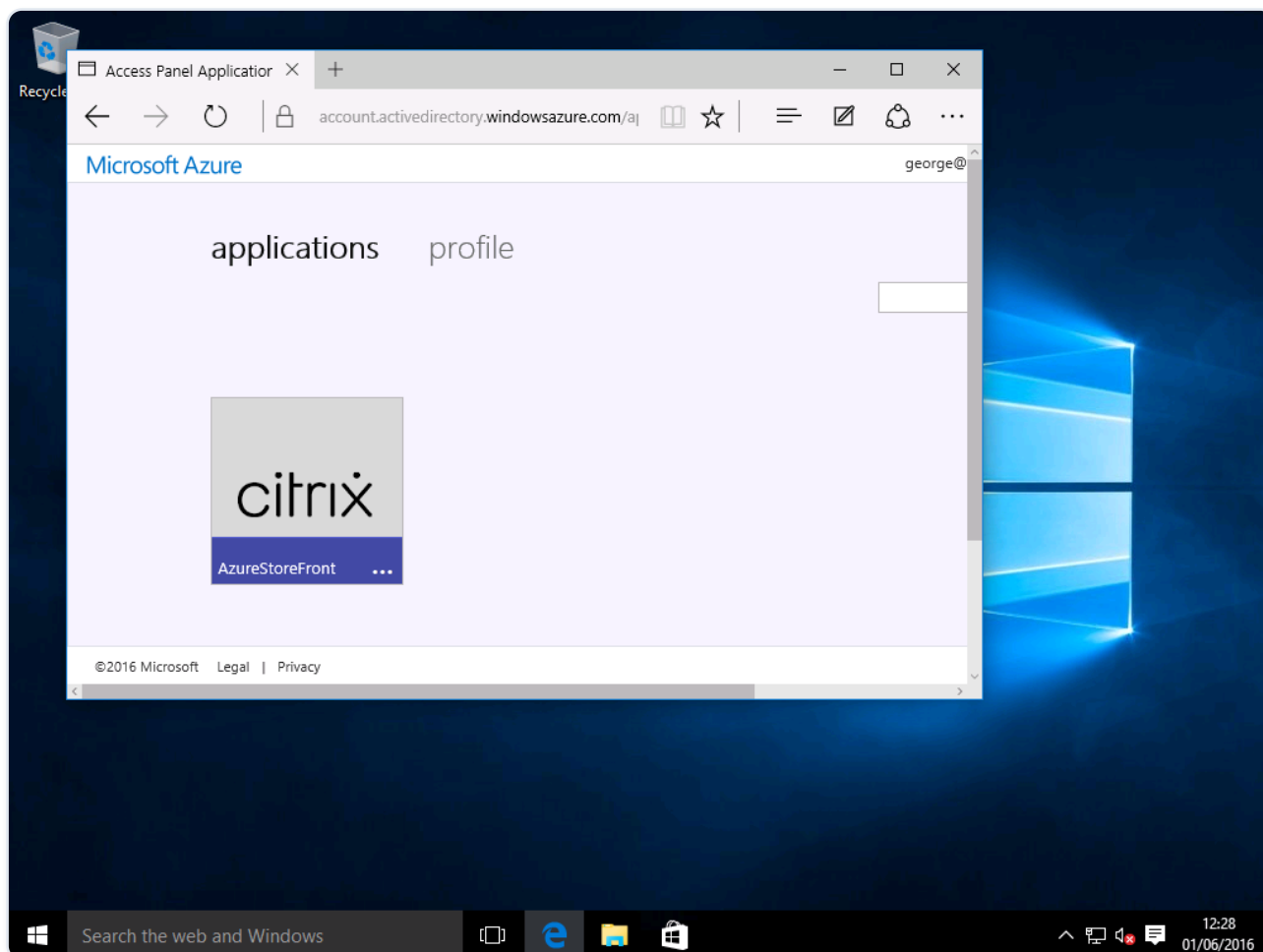
Attribute 5

Attribute 7

## verificar el sistema de extremo a extremo

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

El navegador web debería mostrar las aplicaciones de Azure AD para el usuario.



verificar que al hacer clic en el icono se le redirige a un servidor StoreFront autenticado.

Del mismo modo, verificar que las conexiones directas mediante la URL de inicio de sesión único y una conexión directa al sitio de Citrix Gateway le redirigen a Microsoft Azure y de vuelta.

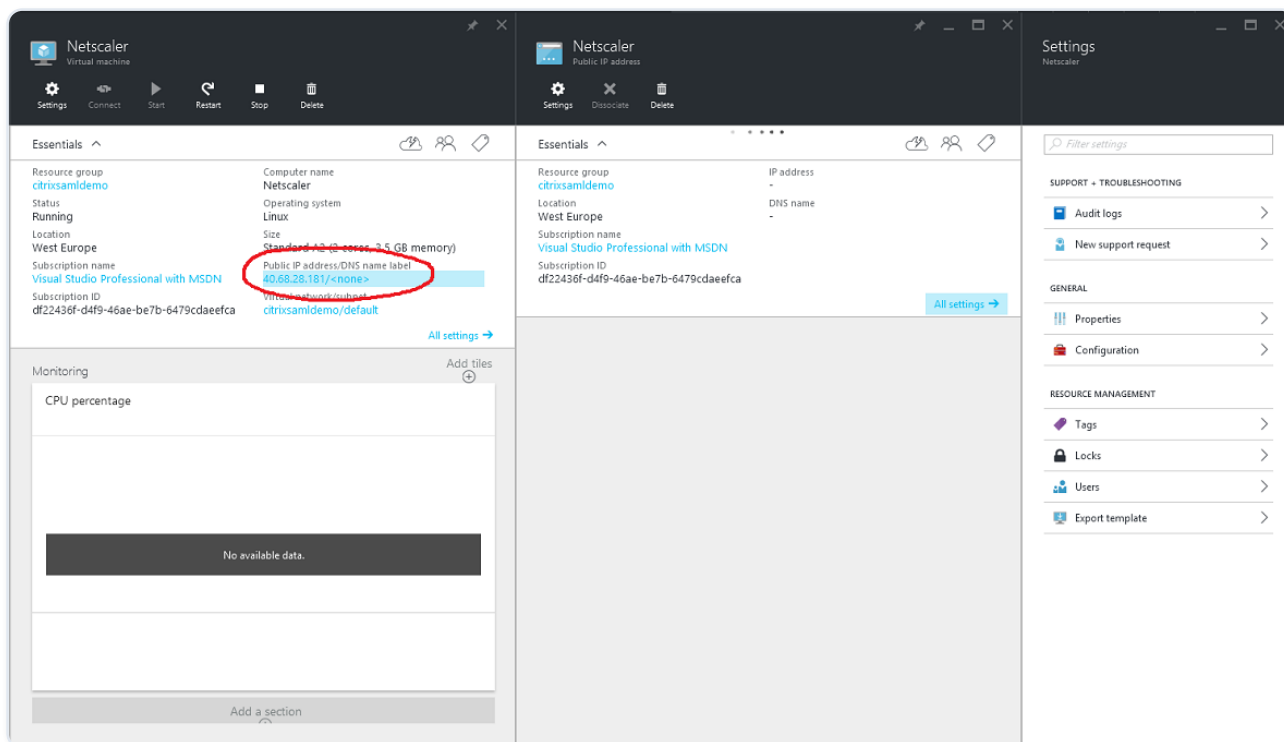
Finalmente, verificar que las máquinas no unidas a Azure AD también funcionan con las mismas URL (aunque habrá un inicio de sesión explícito único en Azure AD para la primera conexión).

## Apéndice

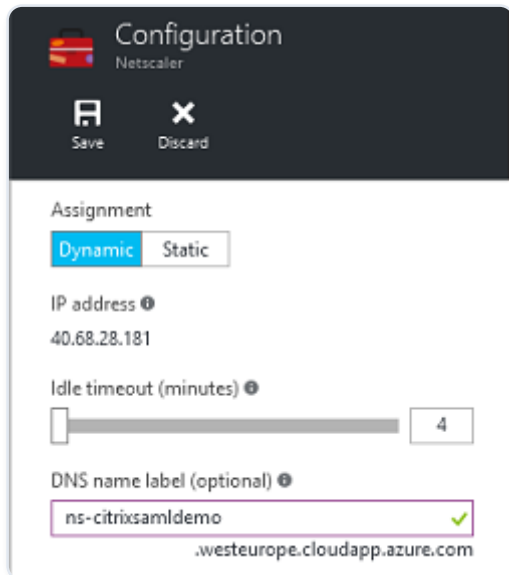
Debe configurar las siguientes opciones estándar al configurar una máquina virtual en Azure.

### Proporcione una dirección IP pública y una dirección DNS

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



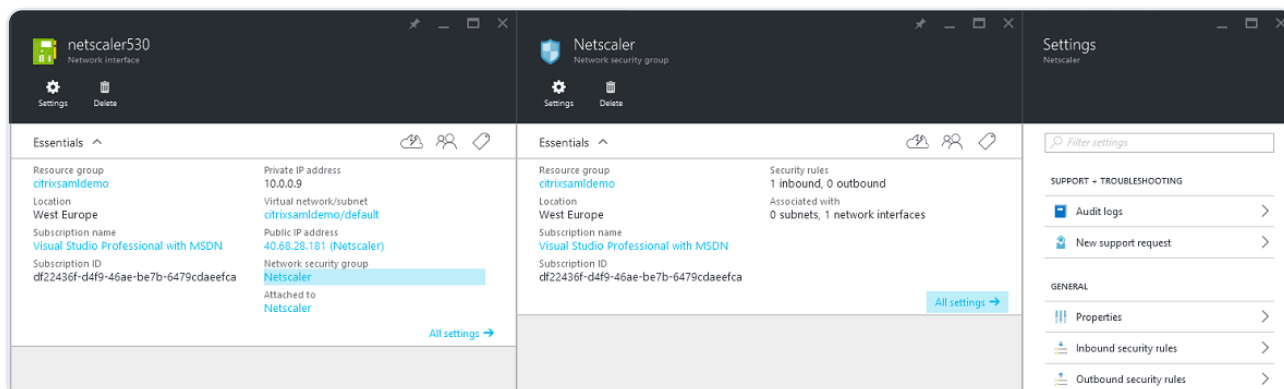
Seleccione **Configuración** de la **etiqueta de dirección IP pública/nombre DNS**. Elija una dirección DNS pública para la VM. Esto se puede usar para referencias CNAME en otros archivos de zona DNS, lo que garantiza que todos los registros DNS sigan apuntando correctamente a la VM, incluso si la dirección IP se reasigna.



## Configurar reglas de firewall (grupo de seguridad)

Cada VM en la nube tiene un conjunto de reglas de firewall aplicadas automáticamente, conocido como grupo de seguridad. El grupo de seguridad controla el tráfico reenviado de la dirección IP pública a la privada. Por defecto, Azure permite que RDP se reenvíe a todas las VM. Los servidores Citrix Gateway y ADFS también deben reenviar tráfico TLS (443).

Abra **Interfaces de red** para una VM y, a continuación, haga clic en la etiqueta **Grupo de seguridad de red**. Configure las **Reglas de seguridad de entrada** para permitir el tráfico de red adecuado.



## Información relacionada

- [Instalar y configurar](#) es la referencia principal para la instalación y configuración de FAS.
- Las implementaciones comunes de FAS se resumen en el artículo [Arquitecturas de implementación](#).
- Los artículos de tipo "Cómo hacer" se presentan en el artículo [Configuración avanzada](#).

# Historial de la documentación de Federated Authentication Service 2308

---

La siguiente tabla describe cambios importantes en la documentación de Federated Authentication Service 2308. Para recibir notificaciones sobre estas actualizaciones, suscríbete al feed RSS.

| FECHA       | CAMBIO                                                       | DESCRIPCIÓN                                                                                                                      |
|-------------|--------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|
| 14 Sep 2023 | Lanzamiento inicial de Federated Authentication Service 2308 | Lanzamiento inicial de Federated Authentication Service 2308. Para obtener más información, consulta <a href="#">Novedades</a> . |