



Servicio de autenticación federada

Contents

Servicio de autenticación federada 2511	10
Versiones anteriores	10
Referencias	11
Federated Authentication Service 2511	12
La lista de direcciones de FAS ya no es necesaria en el VDA	12
Compatibilidad con la recopilación central de Always-On Tracing	12
Problemas resueltos	12
Problemas conocidos	13
Avisos de terceros	13
Requisitos del sistema	14
Instalar y configurar	16
Secuencia de instalación y configuración	16
Instalar el Servicio de autenticación federada	16
Actualización de FAS	17
Habilitar el complemento FAS en los almacenes de StoreFront	17
Configurar el Delivery Controller™	18
Configurar la Directiva de grupo	18
Comportamiento en la sesión	22
Ámbito de la solicitud	22
Tiempo de espera del consentimiento	23
desconectar al bloquear	23
Uso de la consola de administración de Federated Authentication Service	23
Implementar plantillas de certificado	24
Configurar los servicios de certificados de Active Directory	26
Autorizar Federated Authentication Service	27
Configurar reglas	29

Conectarse a Citrix Cloud	34
desconectar de Citrix Cloud	39
Configuración avanzada	40
Información relacionada	40
Emisión de tickets FAS V2 y la lista de direcciones del registro	40
Compatibilidad	40
Versión de ticket FAS que entiende el VDA	41
Configurar tíquets FAS V2 con StoreFront	42
Configurar tíquets FAS V2 con Citrix Cloud Workspace	42
Otros cambios de PowerShell	43
Mostrar el FQDN y el puerto del servidor FAS	43
Parámetro de dirección de los cmdlets	43
Habilitar el Servicio de autenticación federada para un cliente de inquilino	43
Requisitos previos	43
Configurar el cliente MSP	44
Problema conocido	46
Inicio de sesión único de Azure Active Directory	47
VDA unidos a un dominio	48
VDA unidos de forma híbrida	49
Configuración de la autoridad de certificación	51
Configurar varios servidores de CA para su uso en FAS	51
Cambios de comportamiento esperados	52
Configurar la autoridad de certificación de Microsoft para el acceso TCP	53
Pre-generar certificados de usuario	54
Obtener una lista de usuarios de Active Directory	54
Servidor FAS	55
Renovar el certificado de autorización de FAS	57
Uso de la consola de administración de FAS	57

Uso de PowerShell	58
Desautorizar FAS y eliminar certificados FAS	58
Usar la consola de administración de FAS	58
Usar PowerShell	60
Autorización sin conexión	61
Información relacionada	66
Protección de clave privada	67
Introducción	67
Información sobre certificados y plantillas de FAS	68
Certificado de autorización de FAS	68
Certificados de usuario de FAS	69
Opciones de almacenamiento de claves privadas	70
Comandos de PowerShell para la configuración de claves	71
Ejemplos de escenarios de configuración	76
Ejemplo 1: Almacenar todas las claves en Microsoft Software Key Storage Provider	76
Ejemplo 2: Almacenar la clave del certificado de autorización en un TPM	77
Ejemplo 3: Almacenar todas las claves en un HSM	77
Ejemplo 4: Usar claves de curva elíptica	77
Probar la configuración de la clave privada	78
Inspeccionar certificados FAS	79
Inspección del certificado de autorización	79
Inspección de certificados de usuario	80
Actualización desde versiones de FAS anteriores a Citrix Virtual Apps and Desktops 2411	81
Remotización criptográfica	84
Inhabilitar la comunicación remota de KSP	85
Modo de mantenimiento	85
Uso de la consola de administración	86
Uso de PowerShell	86

Información relacionada	86
Configuración de seguridad y red	86
Arquitectura de red y seguridad	87
Comunicación entre StoreFront y FAS	88
Comunicación entre VDA y FAS	88
Comunicación entre FAS y la autoridad de certificación de Microsoft	88
Conexiones entre Citrix Federated Authentication Service y Citrix Cloud™	89
Más información	89
Consideraciones de seguridad	90
Agentes de inscripción delegados	90
Configuración de la lista de control de acceso	91
Configuración del firewall	91
Cambiar el puerto del servidor FAS	91
Supervisión del registro de eventos	92
Módulos de seguridad de hardware	92
Responsabilidades de administración	92
Configuración de directivas de grupo	93
Plantillas de certificado	94
Cambiar el nombre de una plantilla de certificado	94
Modificar las propiedades generales	94
Modificar las propiedades de gestión de solicitudes	94
Modificar las propiedades de criptografía	94
Modificar las propiedades de atestación de clave	95
Modificar las propiedades de plantillas reemplazadas	95
Modificar las propiedades de extensiones	95
Modificar las propiedades de seguridad	95
Modificar las propiedades del nombre del sujeto	96
Modificar las propiedades del servidor	96

Modificar las propiedades de los requisitos de emisión	97
Modificar las propiedades de compatibilidad	97
Administración de la autoridad de certificación	97
Publicación de plantillas	97
Configuración del firewall	98
Inscripción restringida	98
Módulos de directivas y auditoría	98
Administración de FAS	98
Restringir StoreFront, usuarios y VDA mediante una ACL	98
Configurar reglas	99
Configurar la autoridad de certificación y las plantillas	99
Certificados en sesión y de autenticación	99
Protección de clave privada y longitud de clave	100
Registros de eventos	100
Acceso administrativo y herramientas de administración	100
Administradores de Citrix Virtual Apps, Citrix Virtual Desktops y VDA	100
Seguridad general del servidor Windows	100
Compatibilidad con el Estándar Federal de Procesamiento de Información (FIPS)	101
Información relacionada	101
Contadores de rendimiento	101
Solucionar problemas de inicio de sesión de Windows	103
Certificados e infraestructura de clave pública	103
Asignación de nombres UPN y certificados	104
Nombres UPN en Active Directory	105
Servicio de asignación de certificados	105
Controlar la selección del controlador de dominio de inicio de sesión	105
Controlar la selección del controlador de dominio	106
Identificar el controlador de dominio en uso	106

Habilitar eventos de auditoría de cuenta	106
Registros de validación de certificados	107
Comprobar la validez del certificado	107
Habilitar el registro de CAPI	107
Registros CAPI	108
Mensajes de error	108
Registros de Kerberos	109
Registros del controlador de dominio y de la estación de trabajo	109
Registro CAPI2 del controlador de dominio	110
Registro de seguridad del controlador de dominio	111
Registro de seguridad del VDA	112
Registro CAPI de VDA	113
Registro del sistema de VDA	114
Supervisión de FAS mediante el registro de eventos de Windows	114
¿Se está ejecutando el servicio FAS?	115
Eventos de estado de FAS	115
Eventos de FAS conectados a la nube	117
Eventos de seguridad	118
Registros de eventos de FAS	119
Eventos de administración	119
Creación de aserciones de identidad	122
Actuando como parte de confianza	123
Servidor de certificados en sesión	123
Complemento de aserción de FAS	124
FAS habilitado para Workspace	125
Inicio de sesión	126
Certificados en sesión	127
Solicitud de certificado y generación de par de claves	127

Mensajes de error del usuario final	128
Rastreo siempre activo de FAS	129
Recopilación de rastreo siempre activo	130
Deshabilitar el rastreo siempre activo	130
Envío de rastreo siempre activo a un servidor de registro central	130
Información relacionada	130
Cmdlets de PowerShell	130
Opciones del instalador de FAS	131
Opciones de línea de comandos para instalar FAS	131
Instalar FAS en Windows Server Core	132
Administración de FAS en Windows Server Core	133
Arquitecturas de implementación	134
Introducción	134
Descripción general de la arquitectura	134
Implementación interna	135
Implementación de Citrix Gateway	138
Implementación de ADFS SAML	141
Asignación de cuentas B2B	142
Unión a Azure AD en Windows 10	143
Implementación de ADFS	145
Introducción	145
Información general de SAML	147
URL de redirección	147
Identificador	147
Dirección de retorno	147
Certificado de firma	147
URL de cierre de sesión único	148
Configuración	148

Rellenar la política SAML	148
Información relacionada	149

Servicio de autenticación federada 2511

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, permitiéndoles 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.

Servicio de autenticación federada 2511 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 2507 LTSR](#)
- [Servicio de autenticación federada 2503](#)
- [Servicio de autenticación federada 2411](#)
- [Servicio de autenticación federada 2407](#)
- [Servicio de autenticación federada 2402 LTSR](#)
- [Servicio de autenticación federada 2311](#)
- [Servicio de autenticación federada 2308](#)
- [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](#)
- [XenApp y XenDesktop 7.15 Versión de servicio a largo plazo](#)

La estrategia de 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 Active Directory Certificate Services](#)
- [Configuración de Windows para el inicio de sesión con certificado](#)

Federated Authentication Service 2511

Esta versión de Federated Authentication Service (FAS) incluye las siguientes funciones nuevas. Para obtener información sobre las correcciones de errores, consulte [Problemas resueltos](#).

La lista de direcciones de FAS ya no es necesaria en el VDA

La versión 2511 de Citrix Virtual Apps and Desktops admite un nuevo formato de ticket de FAS, conocido como **FAS V2 ticketing**.

Cuando los servidores FAS y los VDA de su implementación ejecutan Citrix Virtual Apps and Desktops 2511 o una versión posterior, ya no es necesaria la lista de direcciones de FAS en el registro del VDA.

Para obtener más información, consulte [Tickets FAS V2 y la lista de direcciones del registro](#).

Compatibilidad con la recopilación central de Always-On Tracing

Con el rastreo siempre activo (always-on tracing), FAS registra su actividad en el sistema de archivos. Esta función ayuda a solucionar problemas y, potencialmente, elimina la necesidad de reproducir un incidente que haya ocurrido.

Esta versión permite que el rastreo siempre activo se envíe automáticamente a un servidor central de su implementación.

Para obtener más información, consulte [Rastreo siempre activo de FAS](#).

Problemas resueltos

- La itinerancia de sesiones de Citrix Virtual Apps and Desktops con FAS desconectar-on-lock habilitado funciona de forma fiable. La solución está en el complemento FAS VDA. .

Problemas conocidos

Las siguientes acciones eliminan las directivas de grupo de FAS basadas en el registro en el VDA, lo que provoca errores de inicio de sesión único:

- Actualizar el VDA de Citrix Virtual Apps and Desktops 2411 a cualquier versión futura
- Actualizar el VDA de Citrix Virtual Apps and Desktops 2503 a cualquier versión futura
- Desinstalar Citrix Virtual Apps and Desktops 2411 del VDA
- Desinstalar Citrix Virtual Apps and Desktops 2503 del VDA

Ejecute el siguiente comando en el VDA para restaurar las directivas de grupo de FAS:

```
gpupdate /force
```

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 2025, ediciones Standard y Datacenter
 - Windows Server 2022, ediciones Standard y Datacenter
 - Windows Server 2019, 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 de 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 [cmdlets de PowerShell](#) de FAS requieren Windows PowerShell de 64 bits instalado en el servidor FAS.
- Se requiere una entidad de certificación (CA) de Microsoft Enterprise o cualquier otra CA validada para emitir certificados de usuario. Los siguientes proveedores de PKI que no son de Microsoft han validado sus soluciones para su uso con FAS. Para obtener soporte con estas validaciones, póngase en contacto con el proveedor:
 - Keyfactor Command
 - Sectigo Certificate Manager
 - Venafi Zero-Touch PKI
 - HDI PKIaaS (Venafi)
 - Entrust WNES
 - AppViewX
 - Evertrust Horizon CLM
 - Opentrust PKI
 - IDnomic PKI-3
 - DigiCert Autoenrollment Server

- Para obtener soporte y orientación para usar FAS con una CA que no sea de Microsoft, puede ponerse en contacto con el proveedor de PKI correspondiente.
- Para las entidades de certificación que no sean de Microsoft, asegúrese de lo siguiente:
 - La entidad de certificación (CA) está registrada en Active Directory como un servicio de inscripción.
 - El certificado de CA se encuentra en el almacén NTAuth del controlador de dominio. Para obtener más información, consulte [Cómo importar certificados de entidad de certificación \(CA\) de terceros en el almacén NTAuth de la empresa](#).
- Para obtener más información, consulte la [Guía de implementación: Citrix Federated Authentication Service y Sectigo MS Agent](#).

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.

Al planificar la implementación de este servicio, revise la sección [Consideraciones de seguridad](#).

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 entidades de certificación
 - c. Autorizar a FAS a usar sus entidades 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 entidad de certificación. FAS se puede instalar desde cualquiera de las siguientes opciones:

- el instalador de Citrix Virtual Apps and Desktops™, desde el botón **Federated Authentication Service** en la pantalla de inicio de ejecución automática al insertar la ISO
- `XenDesktopFasSetup.exe` ubicado en la ISO de Citrix Virtual Apps and Desktops en `x64\XenDesktop Setup\XenDesktopFasSetup.exe`
- `FasSetup_XXXX.exe`, el archivo de instalación independiente de FAS, disponible en el archivo de instalación independiente de FAS (disponible en [Citrix Downloads](#))

Cualquiera de estos instala 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 o CitrixFederatedAuthenticationService.adml)
- Archivos de plantilla de certificado
- [Contadores de rendimiento y registros de eventos](#)
- Servicio de telemetría de Citrix, que proporciona soporte para el rastreo siempre activo de FAS
- [Citrix Scout](#), una aplicación que se puede utilizar para recopilar diagnósticos como el rastreo siempre activo

Para obtener más información sobre los instaladores, consulte [Opciones de línea de comandos para instalar FAS](#).

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 es accesible por un servidor StoreFront™ habilitado para Federation Authentication Service, 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 FAS en los almacenes de StoreFront

NOTA:

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

Para obtener más detalles sobre cómo habilitar el complemento FAS en los almacenes de StoreFront, consulte <https://docs.citrix.com/es-es/storefront/current-release/configure-authentication-and-delegation/fas>.

Configurar el Delivery Controller™

NOTA:

No necesita este paso si utiliza 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 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

NOTA:

Si todos sus servidores FAS y VDA son de la versión 2511 o posterior, la lista FQDN de la Directiva de grupo en el VDA ya no es necesaria. Consulte [Emisión de tickets de FAS V2 y la lista de direcciones del registro](#)

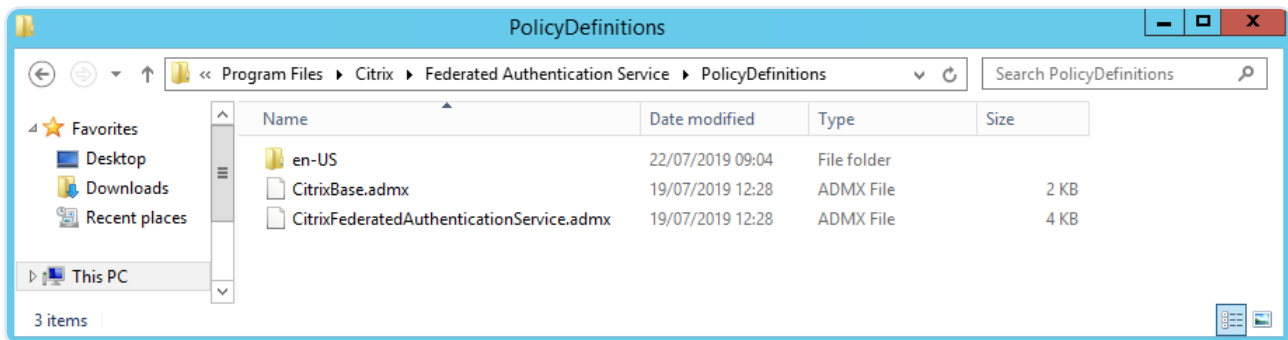
Después de instalar FAS, utilice las plantillas de Directiva de grupo proporcionadas en la instalación para especificar los nombres de dominio completos (FQDN) de los servidores en la Directiva de grupo.

IMPORTANTE:

Asegúrese de que los servidores 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 StoreFront, los VDA y la máquina que ejecuta la consola de administración de FAS vean la misma lista de FQDN. Consulte el paso 6.

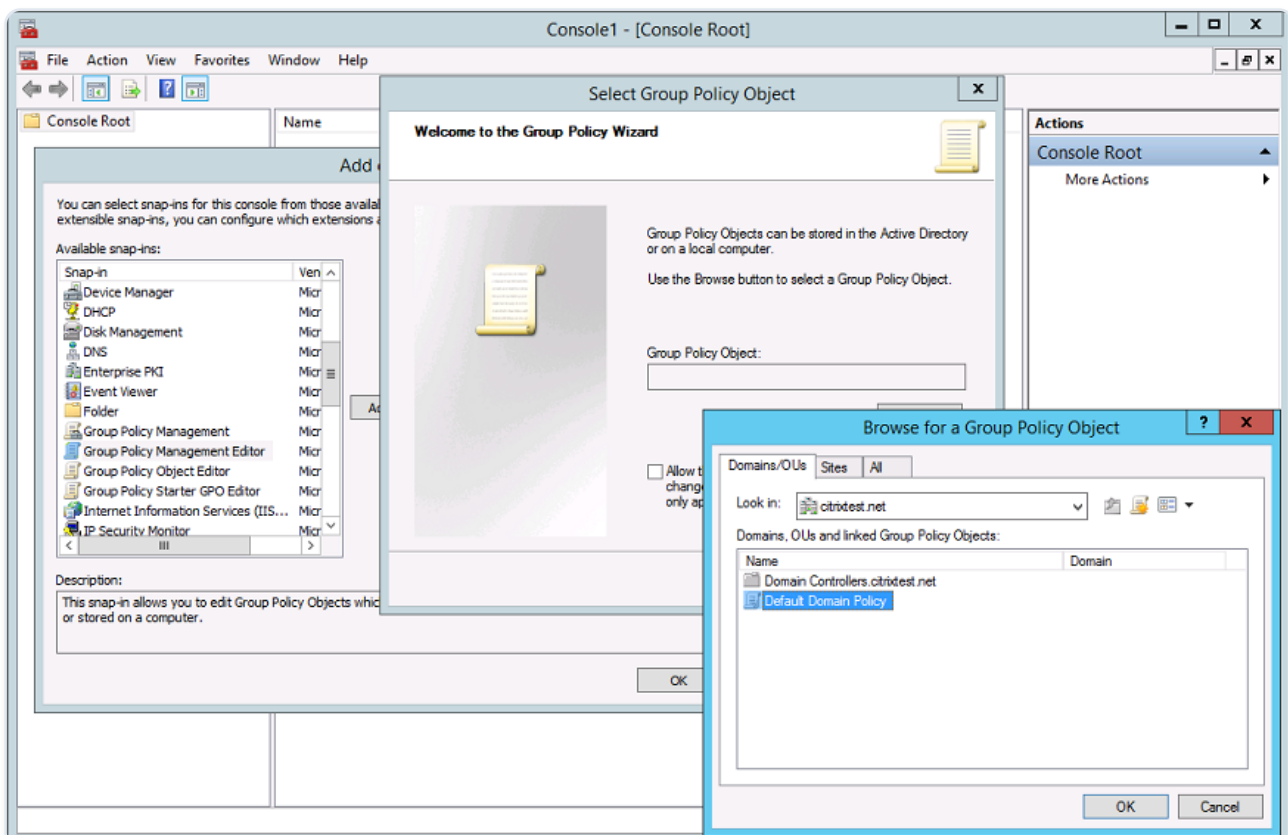
Paso 1. En el servidor donde instaló FAS, localice los archivos C:\Program Files\Citrix\Federated Authentication Service\PolicyDefinitions\CitrixFederatedAuthenticationService.admx y CitrixBase.admx, y la carpeta en-US.



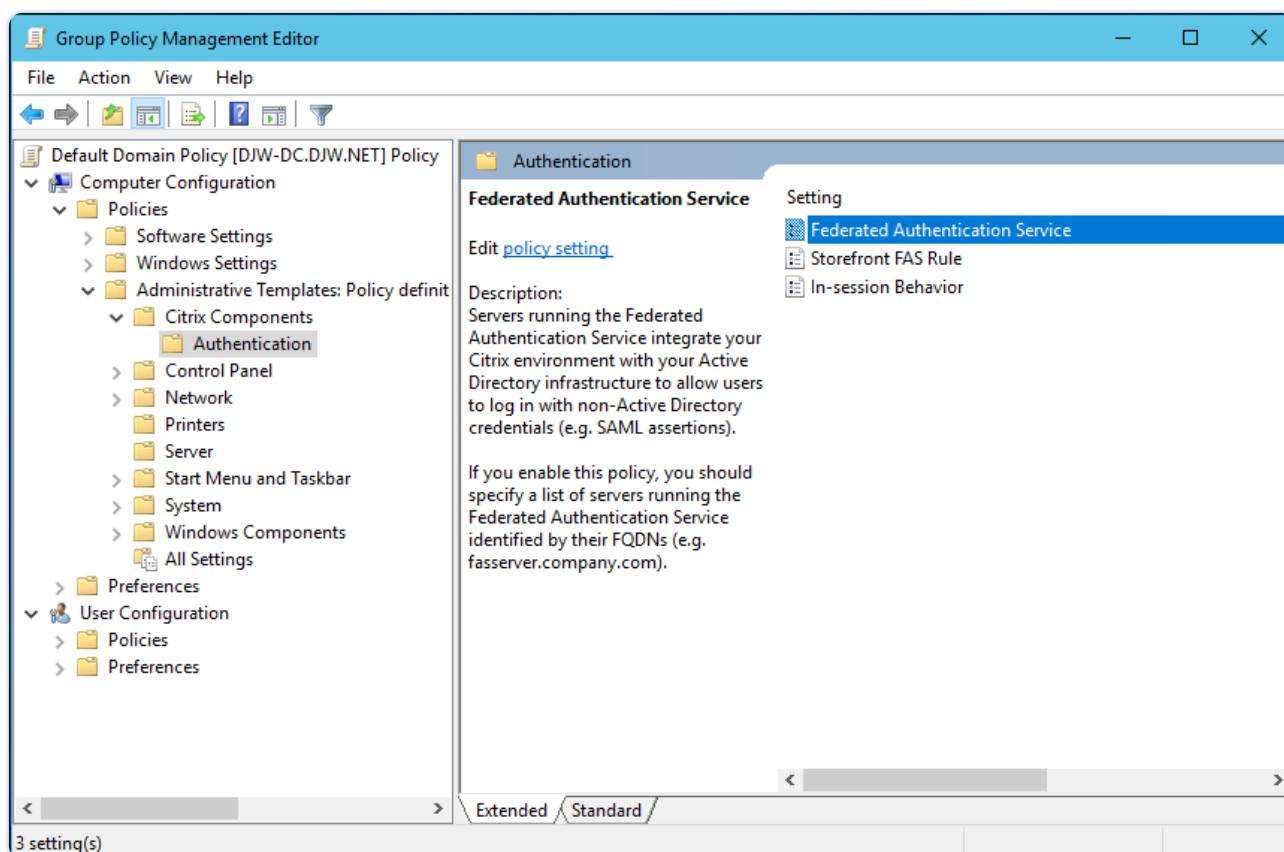
Paso 2. Copie estos archivos en sus controladores de dominio y colóquelos en las subcarpetas C:\Windows\PolicyDefinitions y en-US.

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**. También 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 (VDA, servidores StoreFront, herramientas de administración).

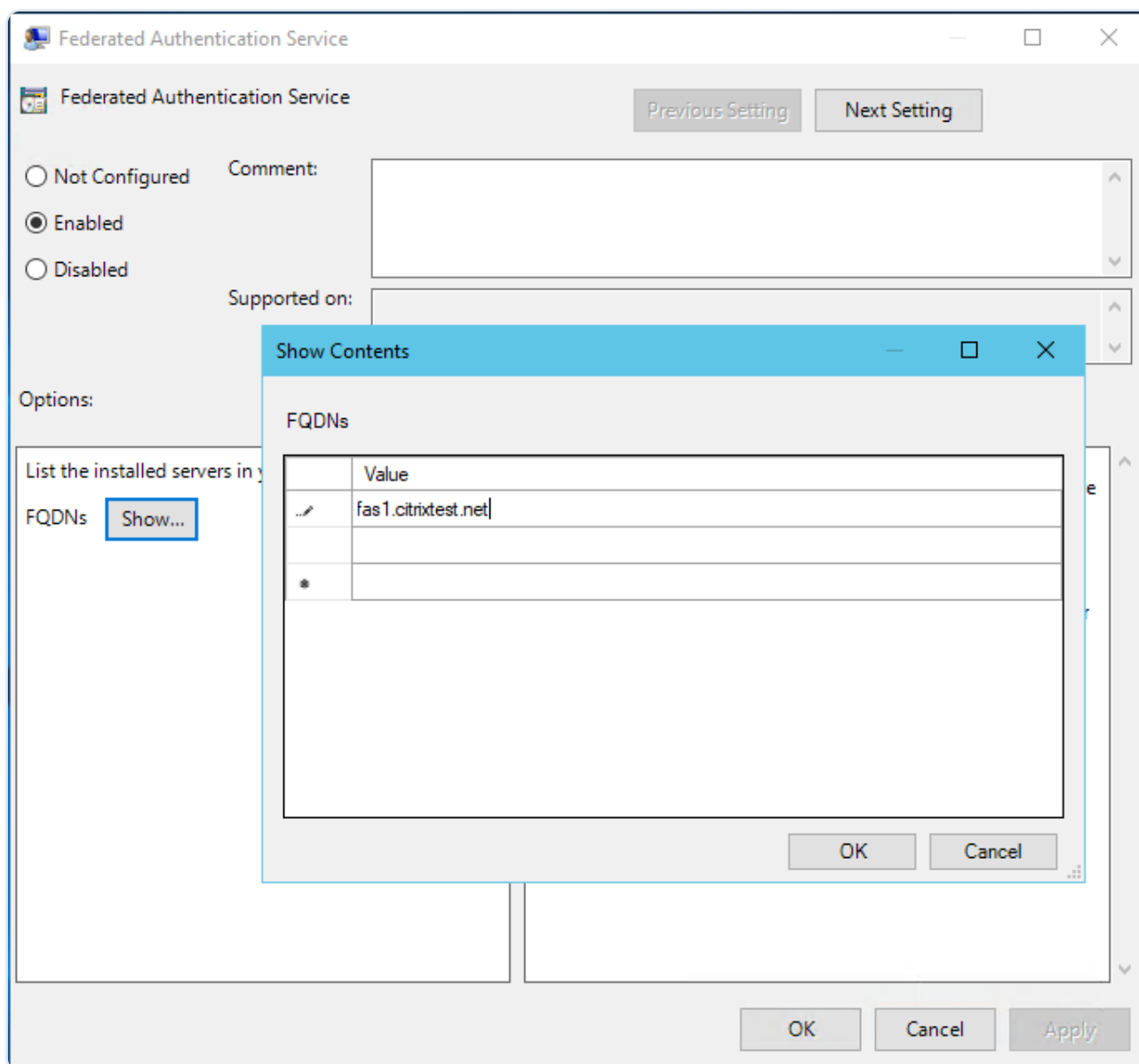


Paso 4. Vaya a la directiva *Federated Authentication Service* en Configuración del equipo/ Directivas/Plantillas administrativas/Componentes de Citrix/Autenticación.

**NOTA:**

La configuración de la directiva 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 Federated Authentication Service aparece en la carpeta **Plantillas administrativas > Componentes de Citrix > Autenticación**.

Paso 5. Abra la directiva 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 como lo ven los VDA, 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 Directiva 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](#).

In-session Behavior

Previous Setting Next Setting

☐ Not Configured Comment:
☒ Enabled
☐ Disabled

Supported on:

Options:

Prompt Scope: **Per-process**

Consent timeout (seconds):

☒ Disconnect on lock

Help:

Enabling this policy activates an agent process (Citrix.Authentication.VirtualSmartcard.exe) which runs inside the user's VDA session. This agent process provides support for the following functionality:

- In-session Certificates
- Disconnect-on-lock

In-session Certificates:

Certificates and private keys securely managed by the Federated Authentication Service can be made available to programs running in a user's VDA session.

Note that an in-session certificate is only available if this policy is enabled AND if the FAS rule used to create the certificate has in-session use allowed.

Most deployments do NOT need to use in-session certificates, because FAS performs a full Active Directory login to the VDA,

OK Cancel Apply

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 el proceso de agente de FAS se ejecute.

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 del consentimiento

Si esta directiva está habilitada, **Tiempo de espera de consentimiento** controla cuánto tiempo (en segundos) dura el consentimiento. Por ejemplo, con 300 segundos, los usuarios ven un mensaje cada cinco minutos. Un valor de cero solicita a los usuarios para 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 extraer 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 en el 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](#).

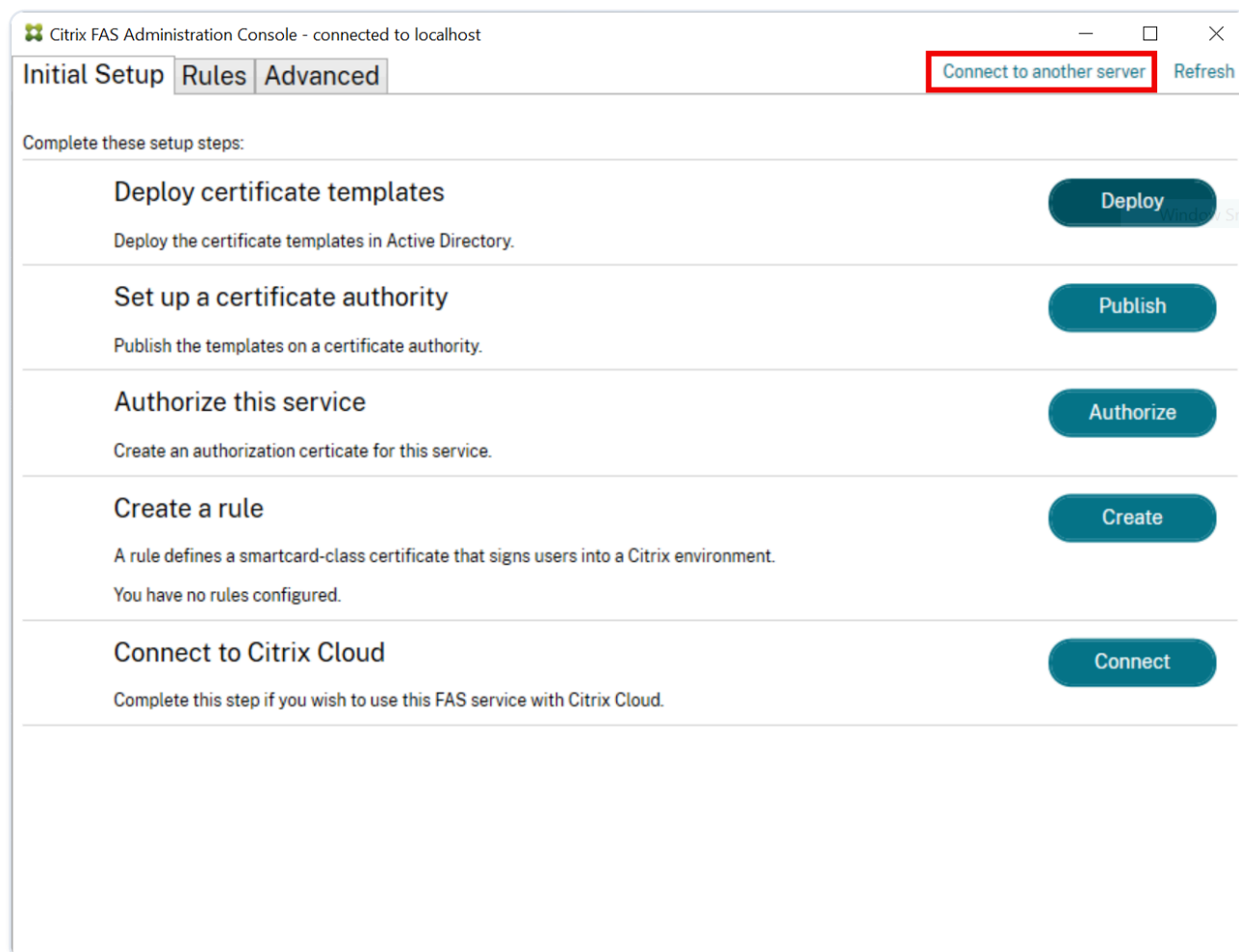
La consola de administración de FAS se instala como parte de FAS. Se coloca un icono (Citrix Federated Authentication Service) en el menú Inicio.

La primera vez que utilice la consola de administración, le guiará a través de los siguientes procesos para:

- Implementar plantillas de certificado.
- Configurar la entidad de certificación.
- Autorizar a FAS para usar 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 utilizando **Conectarse a otro servidor** en la parte superior derecha de la consola.



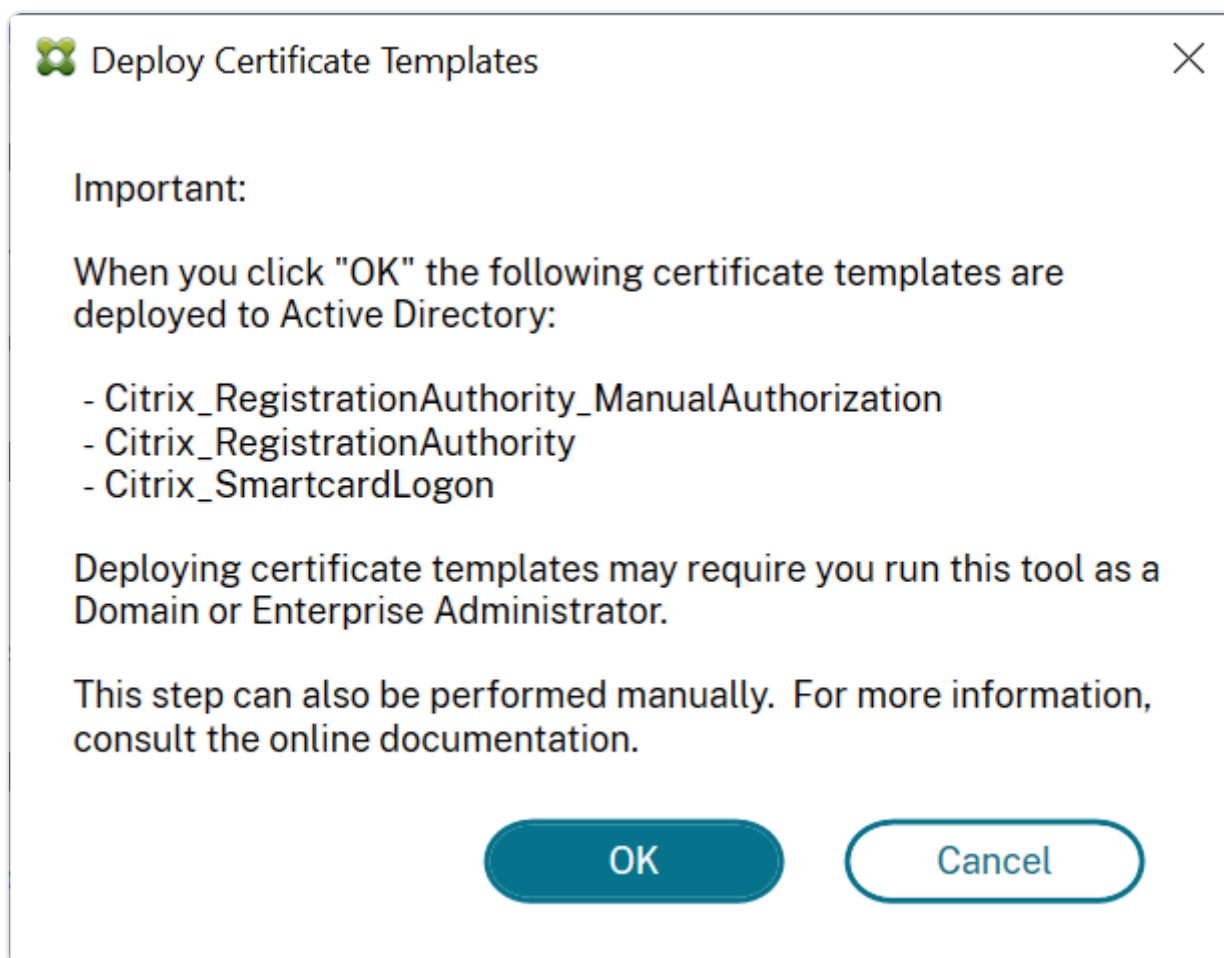
Implementar plantillas de certificado

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

- Citrix_RegistrationAuthority_ManualAuthorization
- Citrix_RegistrationAuthority

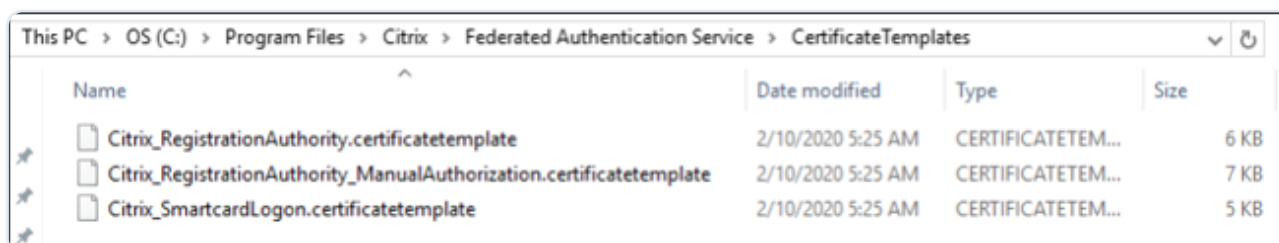
- Citrix_SmartcardLogon

Estas plantillas deben registrarse en Active Directory. Haga clic en el botón **Implementar** y, a continuación, 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, entréguelos a su administrador de Active Directory.

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

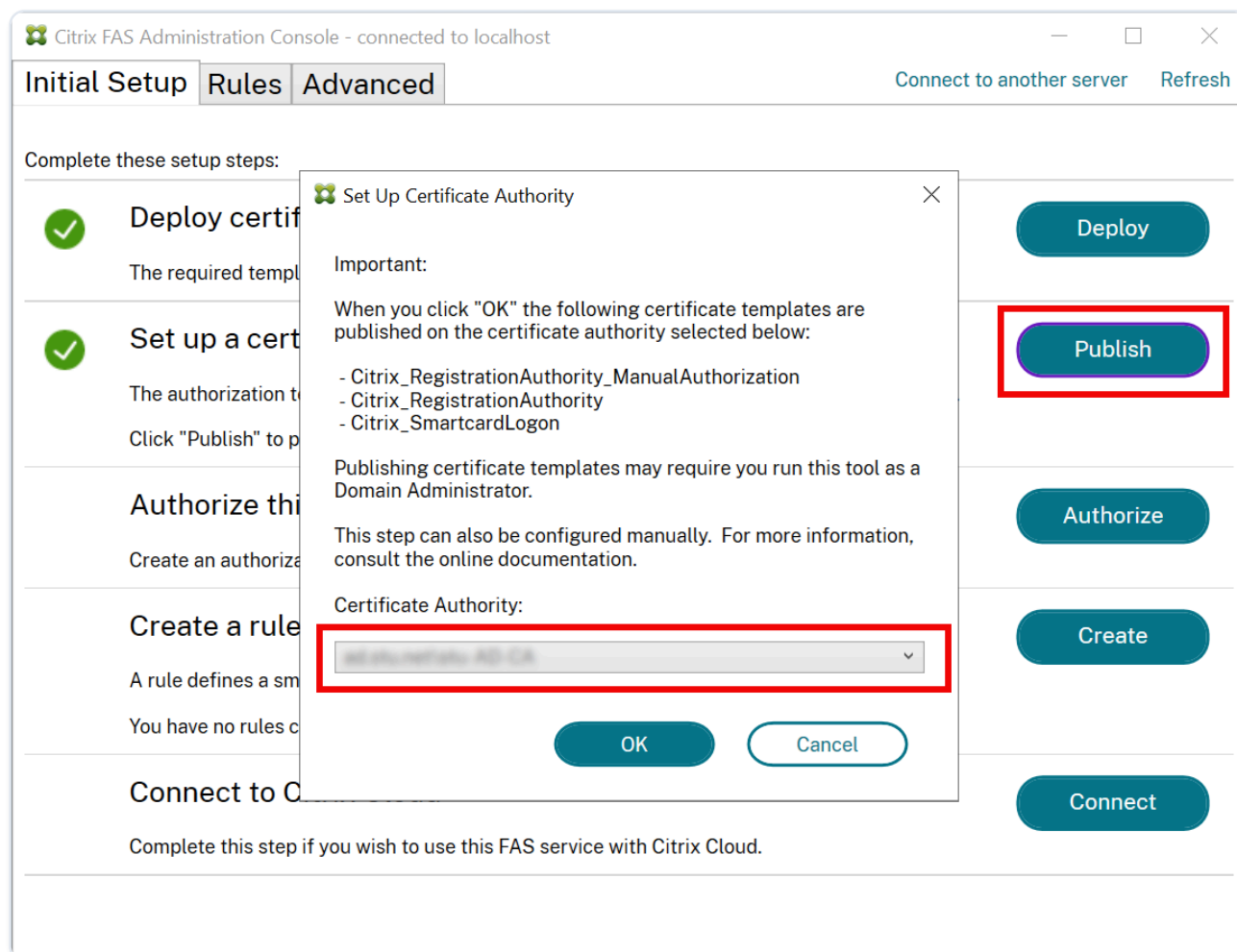
```
$template =  
[System.IO.File]::ReadAllBytes("$Pwd\Citrix_SmartcardLogon.certificatetemp  
late")  
  
$CertEnrol = New-Object -ComObject  
X509Enrollment.CX509EnrollmentPolicyWebService  
  
$CertEnrol.InitializeImport($template)  
  
$comtemplate = $CertEnrol.GetTemplates().ItemByIndex(0)  
  
$writabletemplate = New-Object -ComObject  
X509Enrollment.CX509CertificateTemplateADWritable  
  
$writabletemplate.Initialize($comtemplate)  
  
$writabletemplate.Commit(1, $NULL)
```

Configurar los servicios de certificados de Active Directory

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

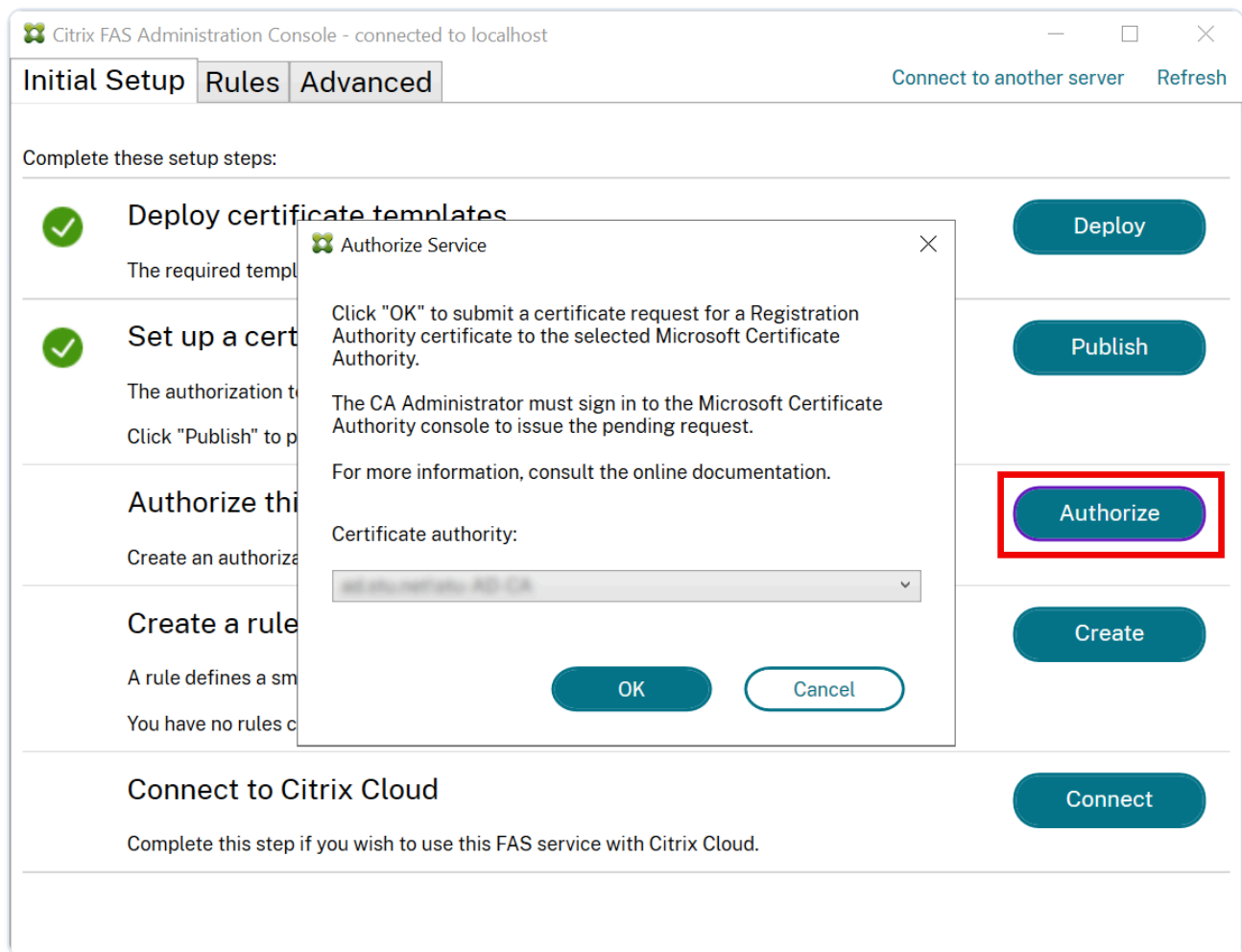
Un usuario con permisos para administrar la autoridad de certificación debe publicar las plantillas en al menos un servidor. Utilice **Configurar autoridad de certificación** para publicarlas.

(Las plantillas de certificado también se pueden publicar mediante la consola de la Autoridad de certificación de Microsoft.)



Autorizar Federated Authentication Service

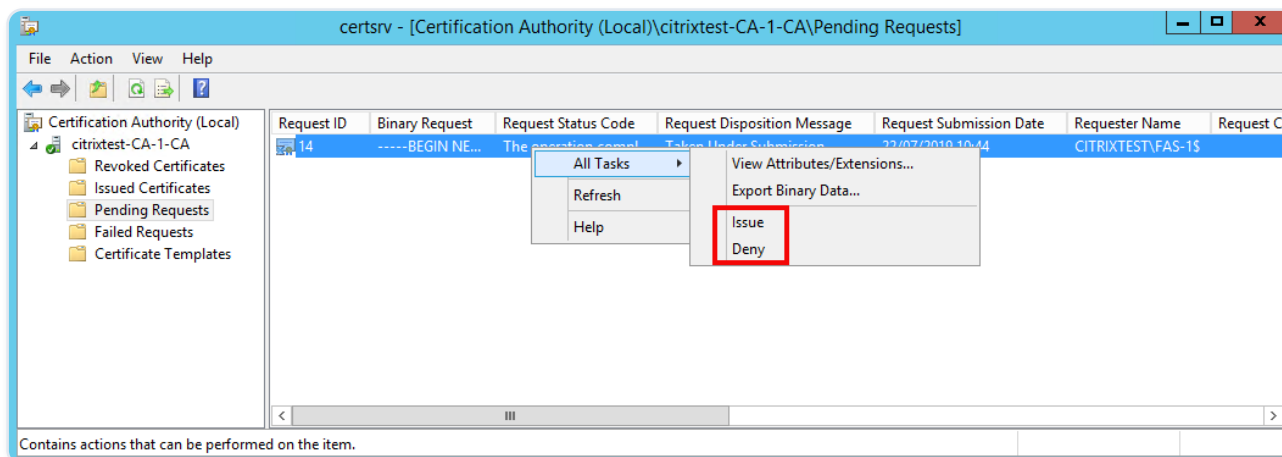
Este paso inicia la autorización de FAS. La consola de administración utiliza la plantilla Citrix_RegistrationAuthority_ManualAuthorization para generar una solicitud de certificado y, a continuación, la envía a una de las autoridades de certificación que publican esa plantilla.



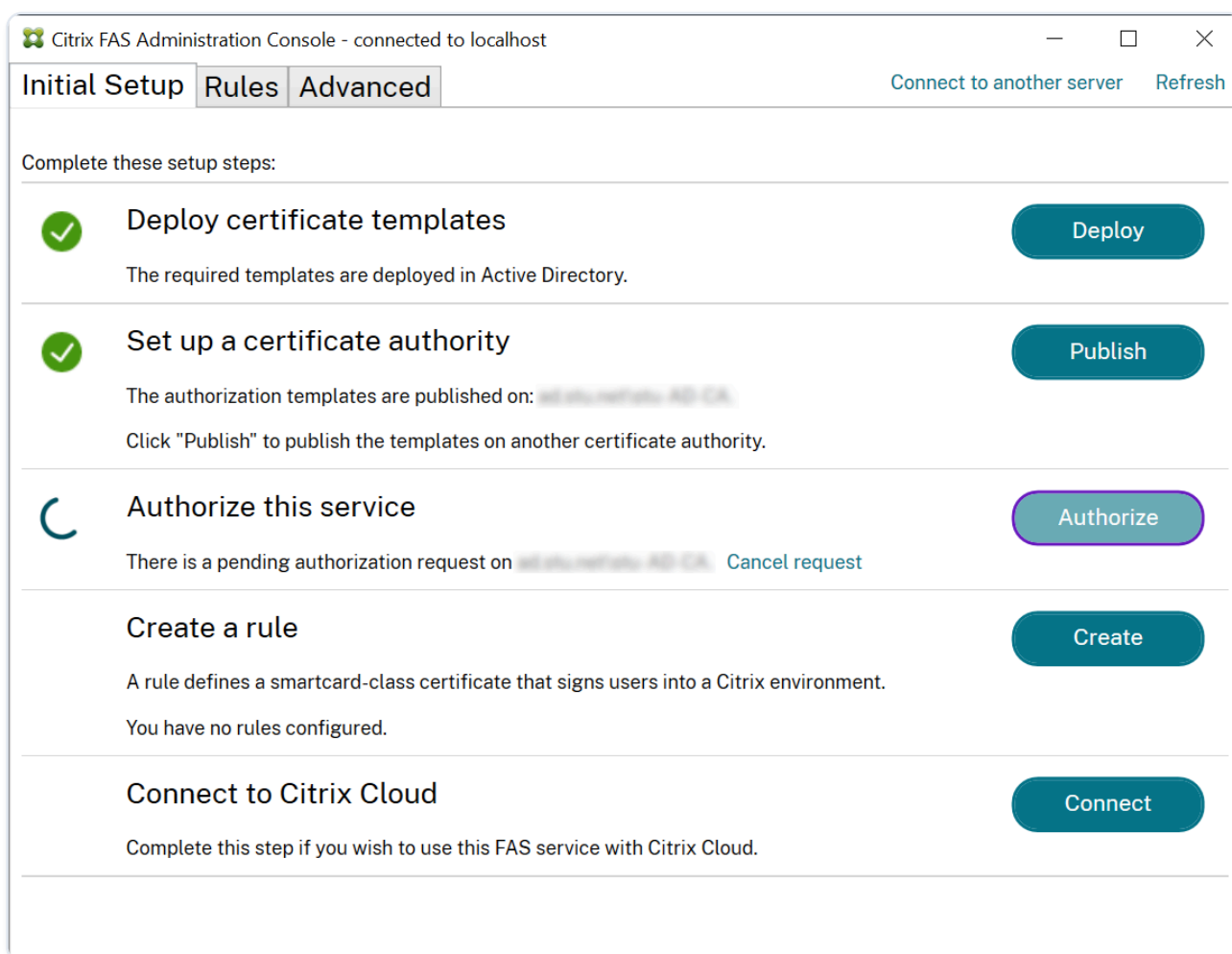
Una vez enviada la solicitud, aparece en la lista **Solicitudes pendientes** de la consola de la Autoridad de certificación de Microsoft como una solicitud pendiente de la cuenta de máquina de FAS. El administrador de la autoridad de certificación debe emitir o denegar la solicitud antes de que la configuración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

La consola de administración de FAS muestra un 'indicador de progreso' hasta que el administrador elige **Emitir** o **Denegar**.

En la consola de la Autoridad de certificación de Microsoft, haga clic con el botón derecho 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 las indicaciones de 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 a las que se permite 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 que las utilicen diferentes servidores StoreFront o Workspace. Configure los servidores StoreFront para que soliciten la regla personalizada por su 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
	Rule name: Default
	Status: OK
	Template: Citrix_SmartcardLogon
	Certificate authorities: ad-00000000-AD-CA
	Certificate available in-session: No
	Access control: Configured
	Restrictions: Not configured
	Cloud rule: 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 la misma (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 la entidad 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 usa 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 desde la sesión 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 del inicio de sesión para su uso por parte de las aplicaciones. Por ejemplo, si necesita autenticación TLS en servidores web dentro de la sesión 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:

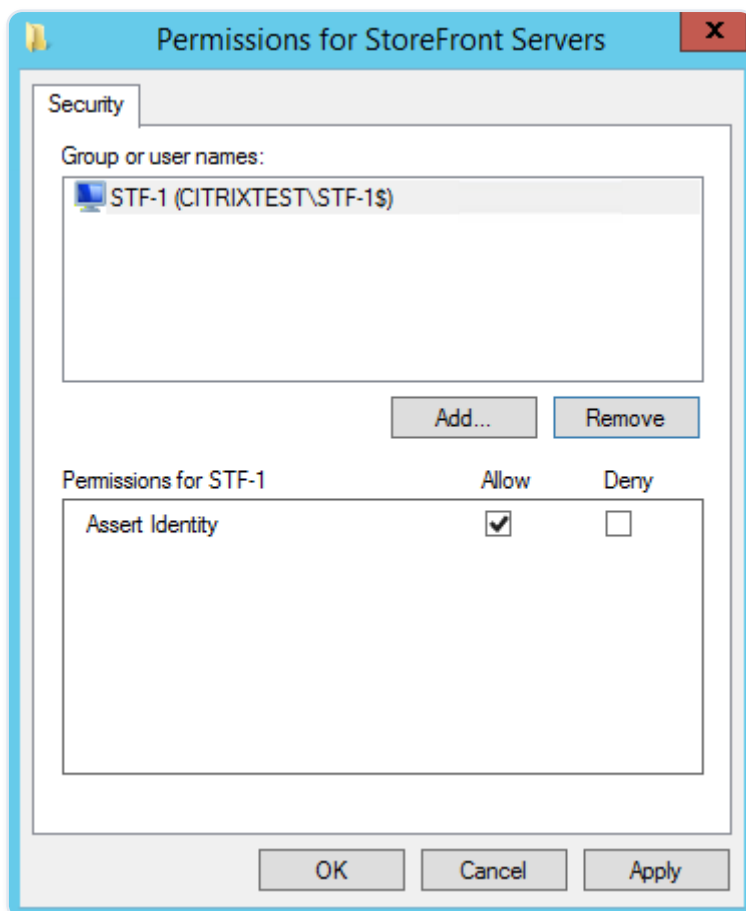
La configuración de **Control de acceso** es crítica para la seguridad y debe administrarse con cuidado.

Nota:

Si utiliza el servidor FAS solo con Citrix Cloud, no necesita configurar el Control de acceso. Cuando Citrix Cloud utiliza una regla, se omiten 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 una implementación de StoreFront local utiliza la regla.

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

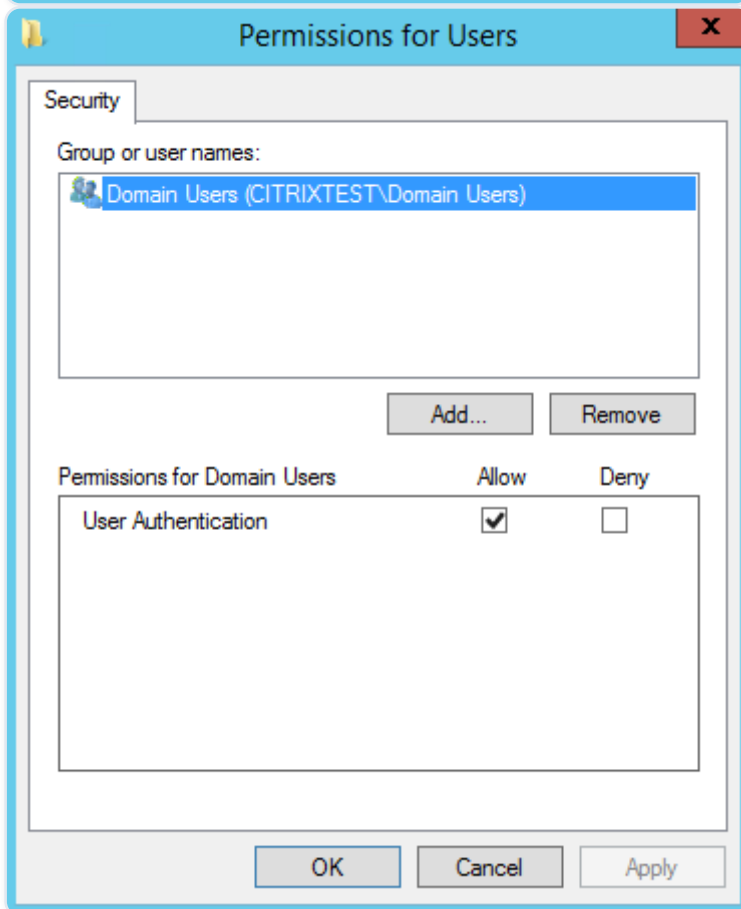
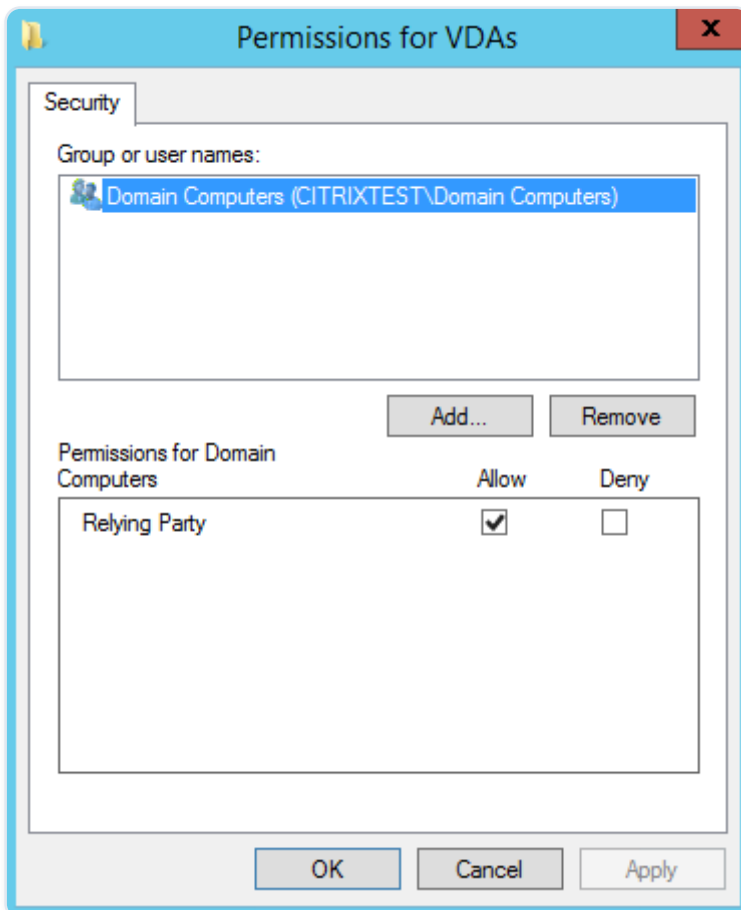


Restricciones: La lista de máquinas VDA que pueden iniciar sesión de usuarios mediante FAS y la lista de usuarios a los que se pueden emitir certificados a través de FAS.

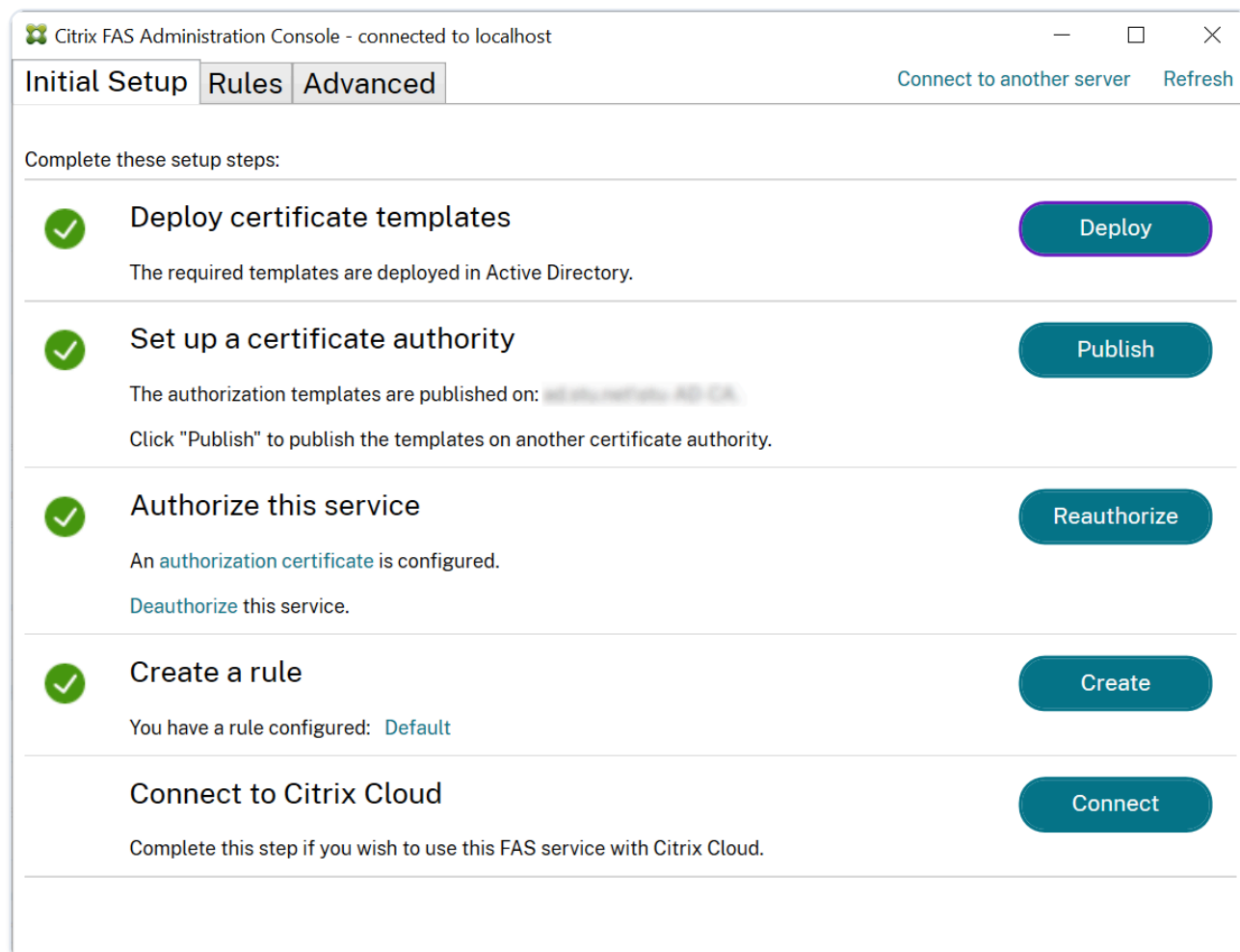
- **Administrar permisos de VDA** le permite especificar qué VDA pueden usar FAS para iniciar sesión del usuario. La lista de VDA predeterminada es Equipos del dominio.
- **Administrar permisos de usuario** le permite especificar qué usuarios pueden usar FAS para iniciar sesión en un VDA. La lista de usuarios predeterminada es Usuarios del dominio.

NOTA:

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



Regla de la nube: Indica si la regla se aplica cuando se reciben aserciones de identidad de Citrix Workspace. Al conectarse a Citrix Cloud, 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](#)

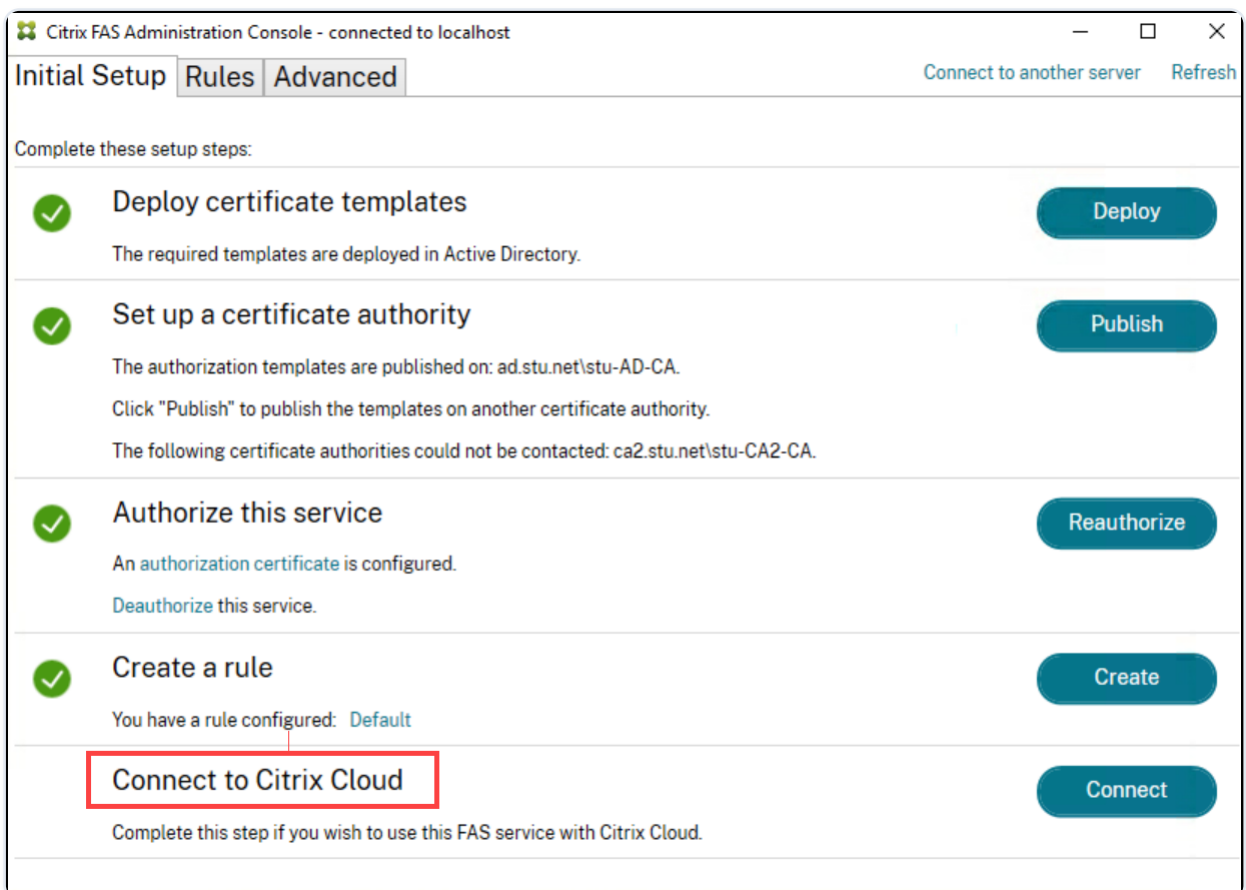
Complete these setup steps:

-  **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.

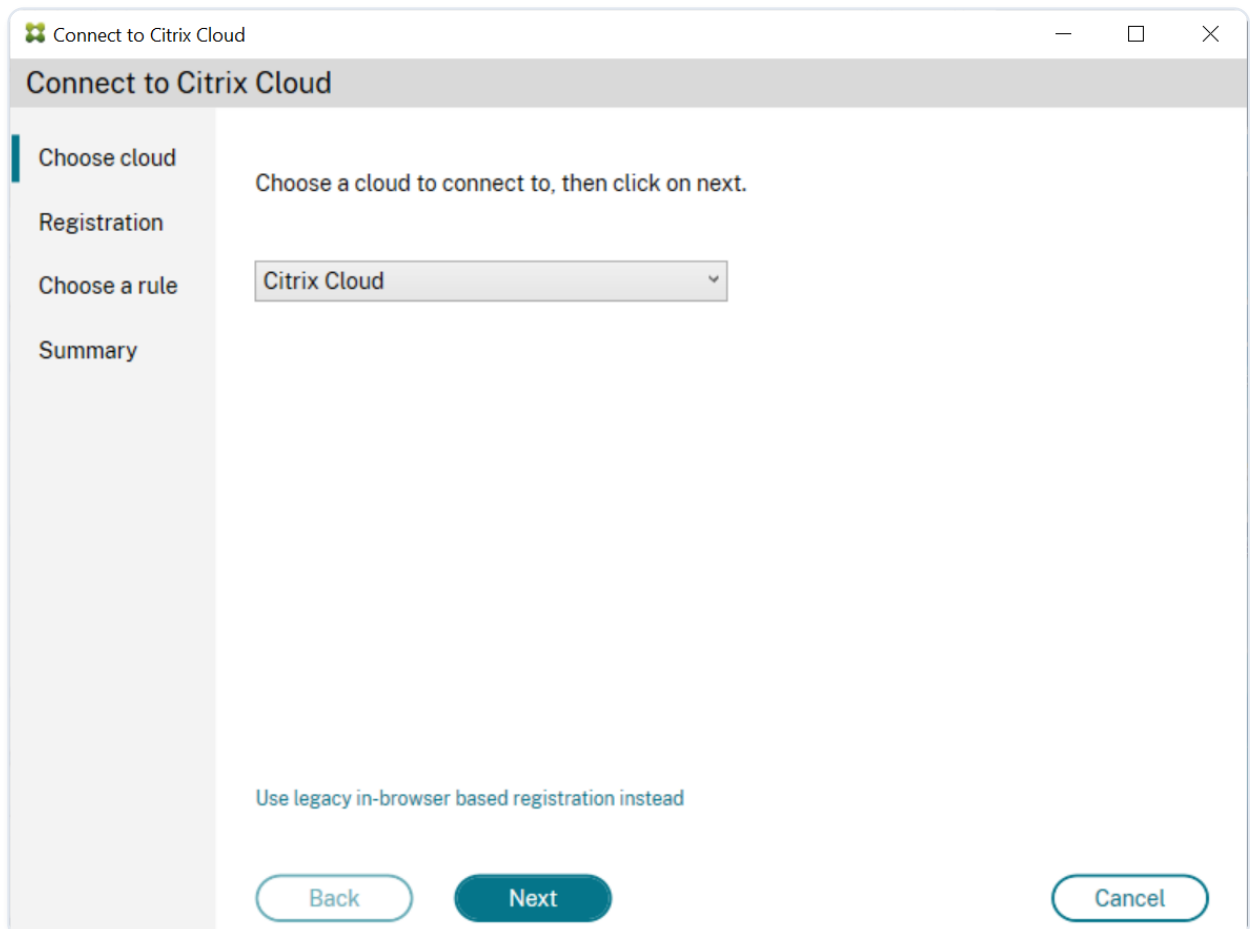
Conectarse a Citrix Cloud

Puede conectar el servidor FAS a Citrix Cloud con Citrix Workspace. Consulte este [artículo de Citrix Workspace](#).

1. En la ficha Initial Setup, en **Connect to Citrix Cloud**, haga clic en **Connect**.



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



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

Connect to Citrix Cloud

Choose cloud

Registration

Choose a rule

Summary

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:

<https://citrix.cloudconnect.com/identity/api/v1/registration> Copy

Confirmation Code:

DDQESDAE Copy

Waiting for confirmation...

Back Next Cancel

4. Una vez validado el código de registro, seleccione la **Resource location** requerida 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, with a "Copy" button to its right.
- Confirmation Code:** A text field containing the code "78552997", with a "Copy" button to its right.
- Resource location:** A dropdown menu with the text "My Resource Location" and a downward arrow.
- Navigation buttons:** "Back", "Next", and "Cancel" buttons at the bottom of the window.

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

The screenshot shows the 'Connect to Citrix Cloud' wizard window. 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 the 'Use an existing rule:' option, there is a sub-option 'Default' which is selected with a radio button. At the bottom, there is a text 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 **Summary**, haga clic en **Finish** 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 displays a summary of the configuration with the following fields: 'Customer:' (blurred), 'Resource location:' (blurred), '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 quitar el servidor FAS de la ubicación de recursos de Citrix Cloud, tal como se describe en este (</es-es/citrix-workspace/workspace-federated-authentication.html>) , en **Conectar a Citrix Cloud** seleccione **Inhabilitar**.

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 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.

Emisión de tickets FAS V2 y la lista de direcciones del registro

Antes de FAS 2511, FAS creaba tickets en formato **V1** (versión 1), que comienzan con un byte de índice. El VDA necesita determinar qué servidor FAS emitió el ticket. Para ello, utiliza el byte de índice para buscar la dirección FAS en la lista de direcciones FAS de su registro.

La GPO generalmente configura la lista de direcciones FAS en el VDA. En los VDA de Windows, la ubicación del registro de la lista de direcciones es

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\Authentication\UserCredentialService\Addresses
```

La lista de direcciones en el VDA debe coincidir exactamente con la lista de direcciones en StoreFront; de lo contrario, el inicio de sesión único fallará. Este requisito era una fuente importante de errores de configuración para los clientes, especialmente aquellos con implementaciones complejas.

FAS 2511 introduce los tickets en formato **V2** (versión 2). La dirección (es decir, FQDN y puerto) del servidor FAS se escribe en el propio ticket, por lo que el VDA no necesita consultar la lista de direcciones del registro.

Compatibilidad

A partir de la versión 2511, FAS genera tickets V2 de forma predeterminada. Los tickets V2 son compatibles con todas las versiones de VDA de Windows y Linux.

Los VDA anteriores a la versión 2511 siguen consultando la lista de direcciones del registro, utilizando el byte de índice como se describe en la sección anterior.

Solo los VDA de Windows y Linux de la versión 2511 y posteriores pueden analizar tickets V2 y, por lo tanto, no necesitan la lista de direcciones del registro.

Los tickets V2 son compatibles con cualquier versión de StoreFront, y no es necesaria una actualización de StoreFront.

Si experimenta problemas con los tickets V2, puede configurar FAS para generar tickets V1 utilizando este comando de PowerShell:

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

Para volver a la generación de tickets V2, utilice este comando de PowerShell:

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

Versión de ticket FAS que entiende el VDA

Solo VDA 2511 y versiones posteriores pueden analizar tickets V2. Las versiones anteriores tratan el ticket V2 como si fuera un ticket V1.

Para confirmar si un VDA entiende la versión del ticket V2, inspeccione el registro de eventos en el servidor FAS.

Si FAS y su VDA son 2511 o posterior, debe ver una entrada de registro de eventos similar a la siguiente durante el inicio del VDA. El evento se encuentra en el **Registro de Windows > Registro de aplicaciones** de su servidor FAS:

```
Level: Information
```

```
Source: Citrix.Authentication.FederatedAuthenticationService
```

```
EventId: 204
```

```
Text: [S204] Relying party [VDA machine name] accessing the Logon Provider
for [User UPN] in role: [FAS Role] [Operation: XXXX] as authorized by
[StoreFront machine name]. Caller ticket version: 2. [correlation: XXXX]
```

En este evento, la versión del tíquet del llamante es **2**. Esto indica que el VDA no necesita configurarse con una lista de direcciones FAS del registro.

Por el contrario, si su VDA no admite tíquets V2, la entrada del registro de eventos tendrá la versión del tíquet del llamante **1**:

```
Level: Information
```

```
Source: Citrix.Authentication.FederatedAuthenticationService
```

```
EventId: 204
```

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

Configurar tíquets FAS V2 con StoreFront

Se puede usar cualquier versión de StoreFront, ya que el tíquet FAS es opaco para StoreFront y no se requiere ninguna configuración especial.

La configuración de las direcciones del servidor FAS en StoreFront sigue utilizando la lista de direcciones del registro, proporcionada mediante una GPO.

Configurar tíquets FAS V2 con Citrix Cloud Workspace

Cuando FAS está conectado a Citrix Cloud, FAS requiere que su dirección esté presente en su propia lista de direcciones del registro. Este comportamiento es para admitir tíquets V1. Si no se encuentra, la consola de administración de FAS muestra una advertencia y FAS no proporciona un inicio de sesión único para los inicios de Citrix Cloud Workspace.

Sin embargo, si toda su implementación utiliza tíquets V2 (es decir, su servidor FAS y sus VDA son 2511 o posterior), entonces no es necesaria la lista de direcciones del registro en el servidor FAS.

Puede usar el siguiente PowerShell para evitar que un FAS conectado a la nube requiera la lista de direcciones del registro:

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

Otros cambios de PowerShell

Además de los comandos mencionados anteriormente, se han realizado los siguientes cambios en PowerShell de FAS 2511.

Mostrar el FQDN y el puerto del servidor FAS

El siguiente comando de PowerShell ahora devuelve el FQDN y el puerto de escucha del servidor FAS. Esta es la información de dirección de FAS codificada en los tiquets V2.

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

Parámetro de dirección de los cmdlets

Antes de 2511, cualquier parámetro Address de un comando de PowerShell de FAS (que no fuera "localhost") se comprobaba con la lista de direcciones del registro del servidor FAS. Para cambiar este comportamiento, era necesario usar el siguiente comando:

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

A partir de 2511, los comandos de PowerShell de FAS no comprueban el parámetro Address con la lista de direcciones. Para revertir al comportamiento anterior, ejecute el siguiente comando de PowerShell:

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

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 administrados (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](#).

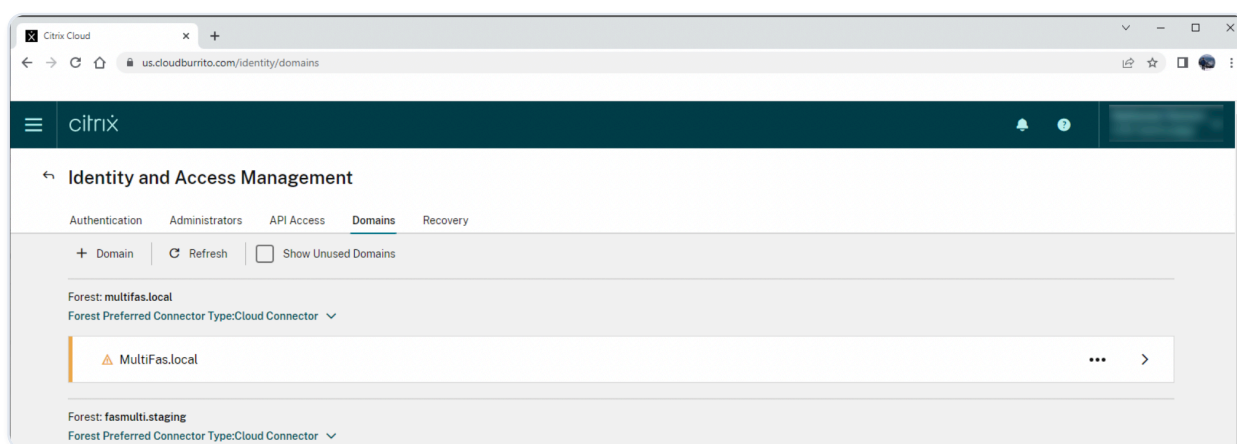
- Ha configurado una relación de inquilino-MSP. Para obtener más información, consulte [Citrix DaaS para proveedores de servicios de Citrix](#).

Configurar el cliente MSP

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

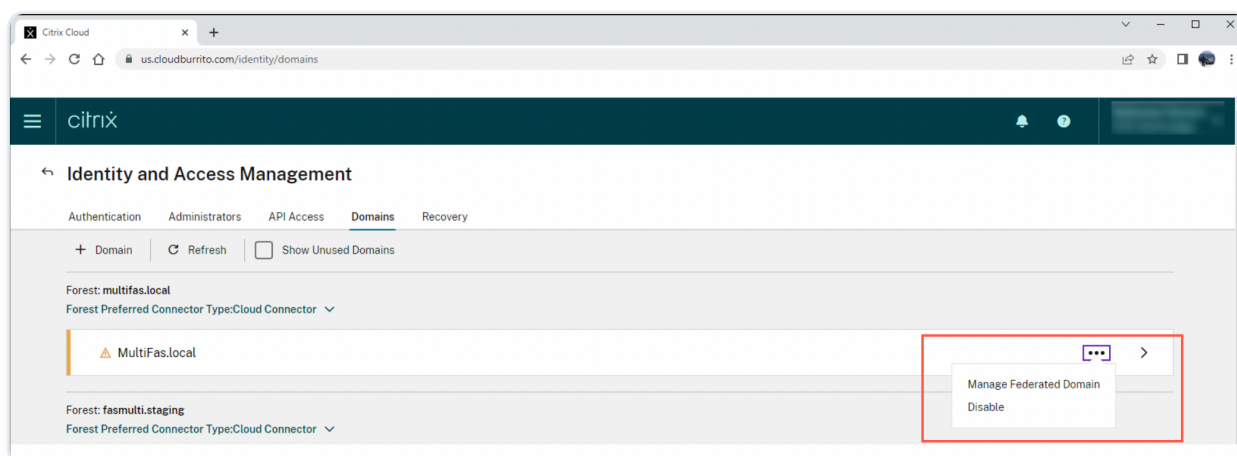
Conecte la infraestructura local a Citrix Cloud [instalando Cloud Connectors](#).

verificar que los dominios asociados con el controlador de dominio local estén disponibles en **Administración de identidades y accesos > Dominios**.

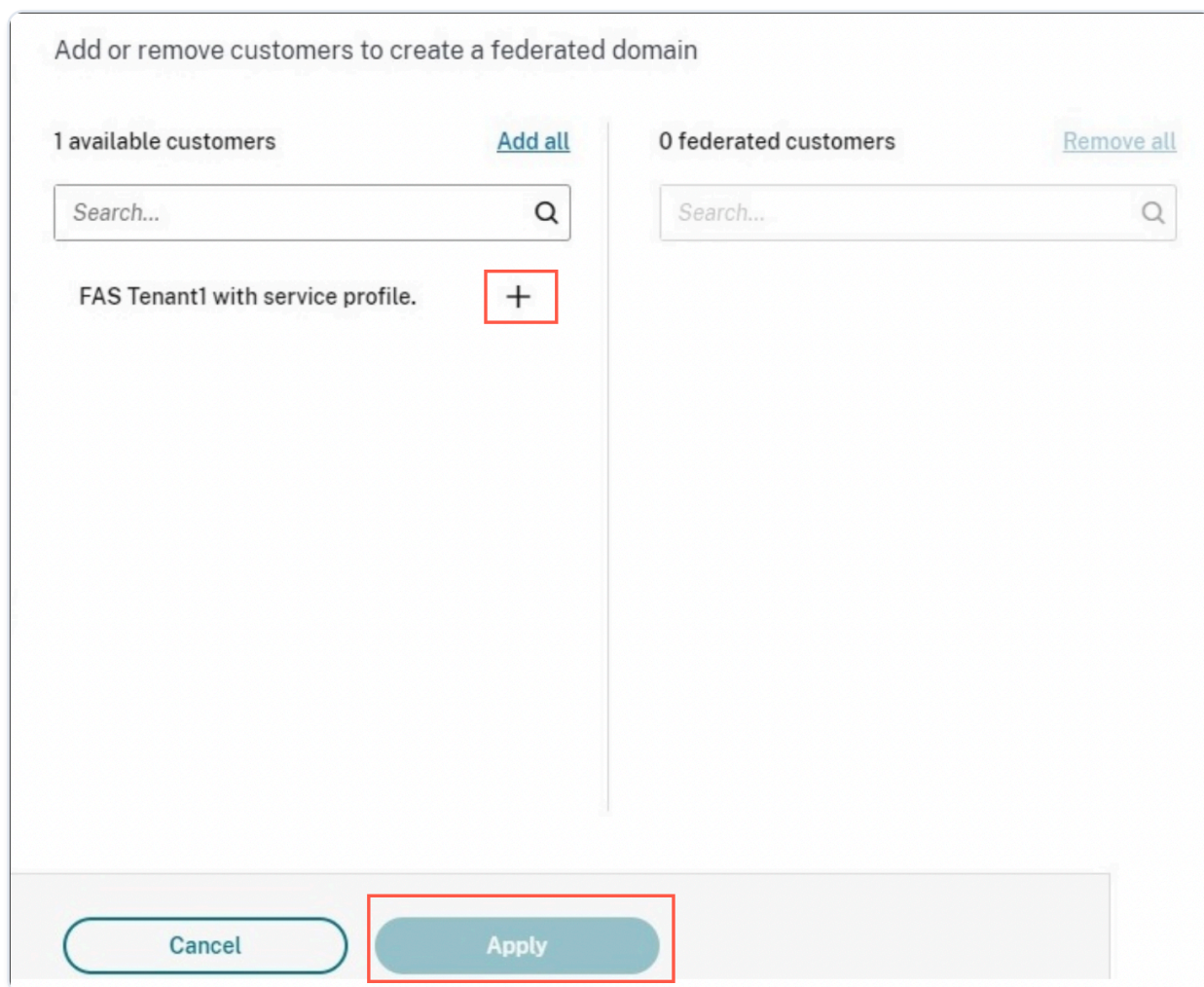


2. Federar el dominio al inquilino.

Seleccione el dominio y haga clic en el menú desplegable (...) y, a continuación, haga clic en **Administrar dominios federados**.

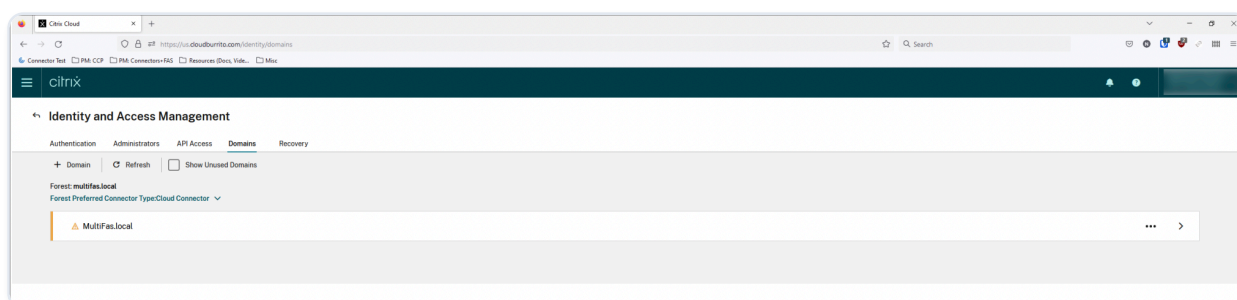


Busque el inquilino y haga clic en **+**. A continuación, haga clic en **Aplicar**.



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

Este paso es opcional. Inicie sesión en la consola para los clientes inquilinos y verificar que los dominios aparecen en **Administración de identidades y accesos > Dominios**.



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

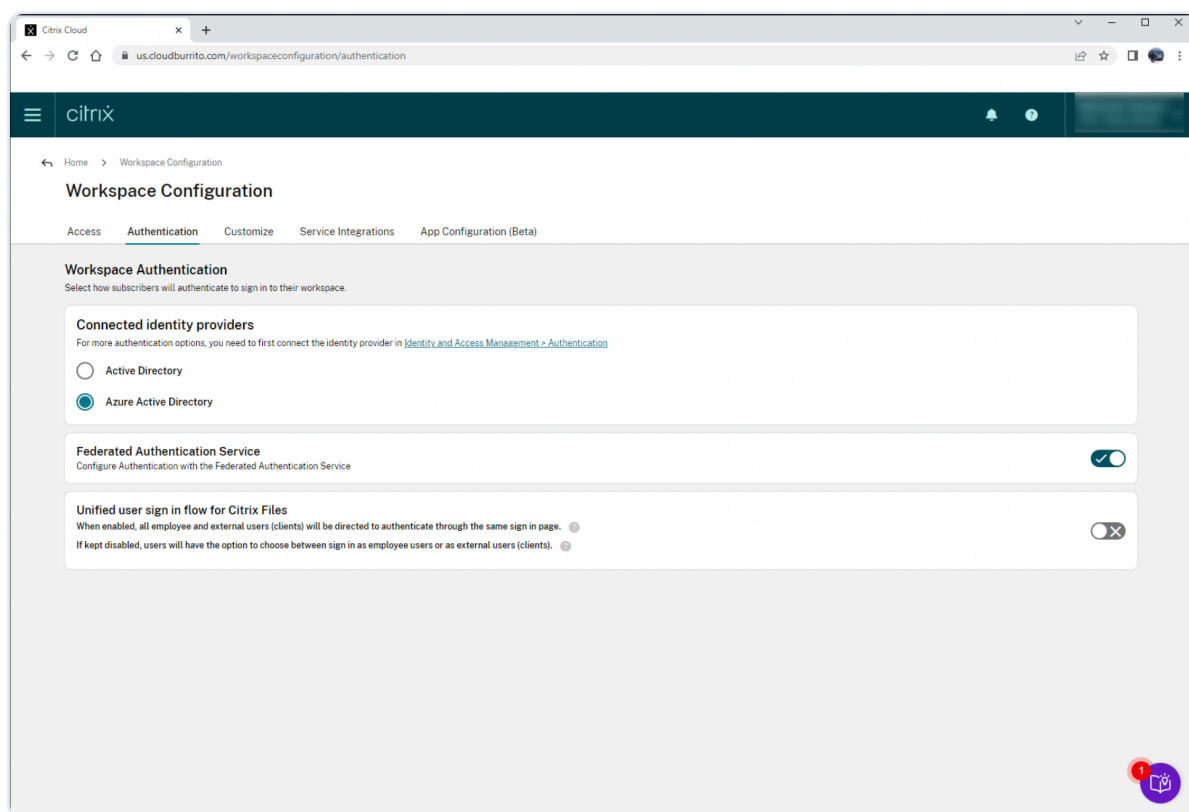
Habilitar FAS para el cliente inquilino

- Configure su proveedor de identidades (IdP)

Cambie al cliente inquilino. Vaya a **Administración de identidades y accesos > Autenticación**. Conéctese a su IdP y asegúrese de que AD esté sincronizado con el IdP.

- Habilitar FAS para un inquilino

Vaya a **Configuración de Workspace > Autenticación**. Seleccione la autenticación que haya 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

NOTA:

Desde julio de 2023, Microsoft ha cambiado el nombre de Azure Active Directory (Azure AD) a Microsoft Entra ID. En este documento, cualquier referencia a Azure Active Directory, Azure AD o AAD ahora se refiere a Microsoft Entra ID.

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 inicie sesión en la sesión de VDA, podrá acceder a los recursos de AD sin volver a autenticarse.

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

NOTA:

- No necesita ninguna configuración especial para que FAS use el SSO para Microsoft Entra ID.
- No necesita los certificados en sesión de FAS.
- Puede usar cualquier versión de FAS.
- Puede usar cualquier versión del VDA que admita FAS.

Las técnicas para el SSO de Microsoft Entra ID se resumen en la siguiente tabla:

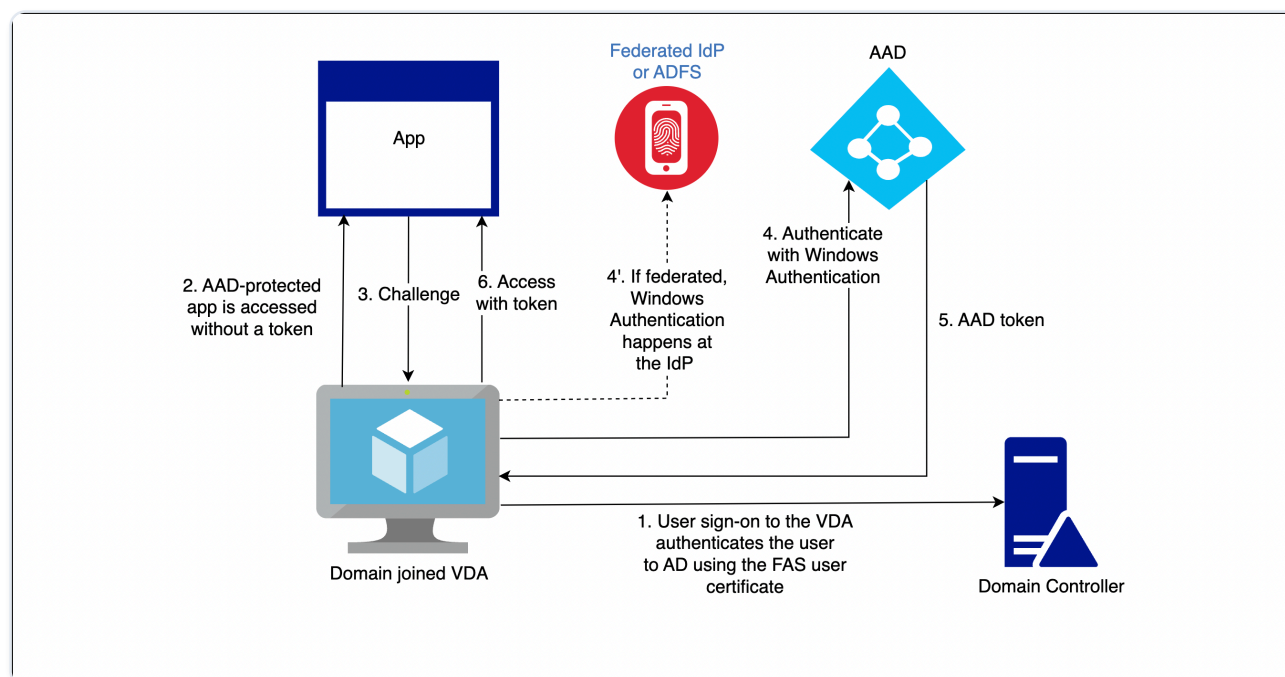
TIPO DE AUTENTICACIÓN DE ME-ID	EL VDA ESTÁ UNIDO A UN DOMINIO	EL VDA ESTÁ UNIDO DE FORMA HÍBRIDA
Administrado	Usar SSO transparente de ME-ID	Usar autenticación basada en certificados de ME-ID

TIPO DE AUTENTICACIÓN DE ME-ID	EL VDA ESTÁ UNIDO A UN DOMINIO	EL VDA ESTÁ UNIDO DE FORMA HÍBRIDA
Federado con Active Directory Federation Services (ADFS)	Habilitar la autenticación de Windows en ADFS	Asegurarse de que el punto de conexión WS-Trust <i>certificatemixed</i> esté habilitado
Federado con un proveedor de identidades de terceros	Usar una solución de terceros	Usar una solución de terceros

- Un dominio de Microsoft Entra ID administrado es aquel en el que la autenticación del usuario se produce en Microsoft Entra ID, a veces denominada autenticación nativa de Microsoft Entra ID.
- Un dominio de Microsoft Entra ID federado es aquel en el que Microsoft Entra ID 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 Microsoft Entra ID.

VDA unidos a un dominio

Para los VDA unidos a un dominio, logre el SSO en Microsoft Entra ID mediante la autenticación de Windows (tradicionalmente denominada autenticación integrada de Windows o Kerberos). La autenticación en Microsoft Entra ID se produce cuando el usuario accede a una aplicación protegida por Microsoft Entra ID 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 de Microsoft Entra ID está administrado o federado.

Para obtener información sobre la configuración del dominio de Microsoft Entra ID administrado, consulte [Inicio de sesión único sin interrupciones](#).

Para un dominio de Microsoft Entra ID federado con ADFS, habilite la autenticación de Windows en el servidor ADFS.

Para un dominio de Microsoft Entra ID federado con 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 Microsoft Entra ID al usar FAS.

VDA unidos de forma híbrida

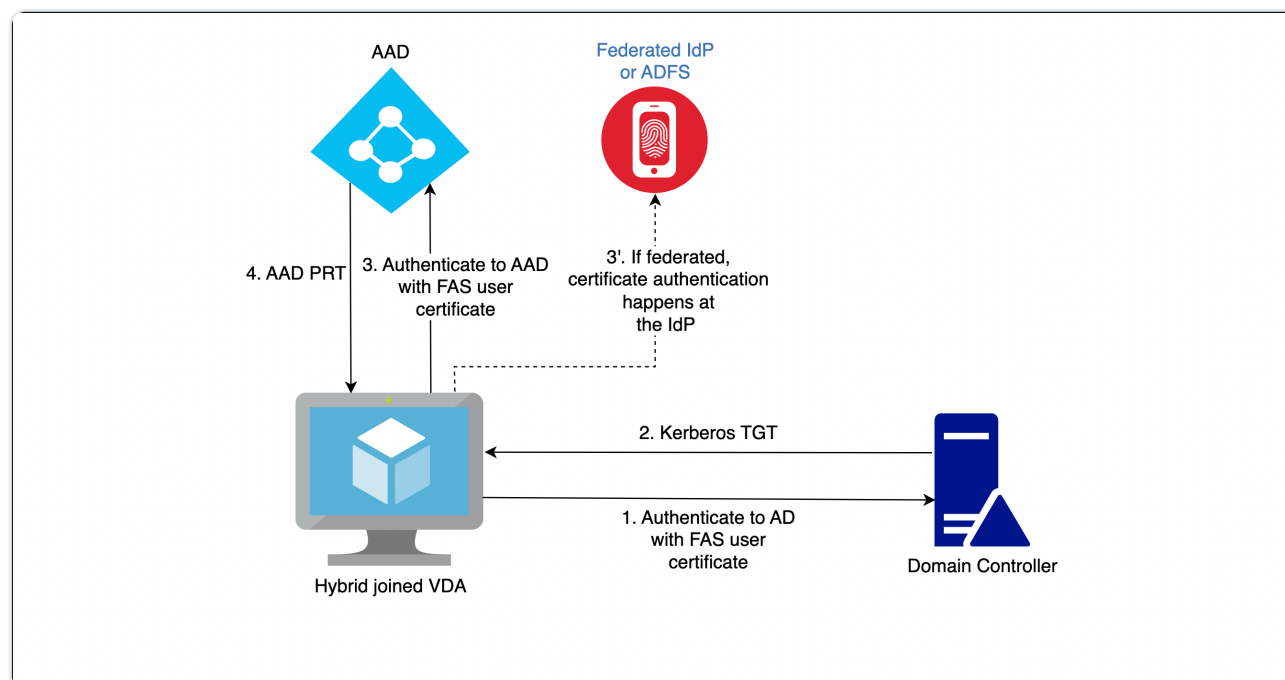
Los VDA unidos de forma híbrida se unen a AD y a Microsoft Entra ID al mismo tiempo. Cuando el usuario inicia sesión en el VDA, se crean los siguientes artefactos:

- 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 Microsoft Entra ID

El PRT contiene información tanto sobre el usuario como sobre el equipo. Esta información se utiliza en una directiva de acceso condicional de Microsoft Entra ID 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 Microsoft Entra ID. El siguiente diagrama muestra el proceso de autenticación a un alto nivel:



Los detalles exactos varían según si el dominio de Microsoft Entra ID está administrado o federado.

Para un dominio de Microsoft Entra ID administrado, configure Microsoft Entra ID CBA. Para obtener más información, consulte [Información general sobre la autenticación basada en certificados de Azure AD](#). El VDA utiliza Microsoft Entra ID CBA para autenticar al usuario en Microsoft Entra ID 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 de Microsoft Entra ID federado con ADFS, el VDA utiliza el punto de conexión WS-Trust *certificatemixed* del servidor ADFS para autenticar al usuario en Microsoft Entra ID con el certificado FAS del usuario. Este punto de conexión está habilitado de forma predeterminada.

Para un dominio de Microsoft Entra ID federado con 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 conocimientos básicos de PowerShell antes de ejecutar cualquier instrucción de este artículo.

Configurar varios servidores de CA para su uso en FAS

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

Edit rule "hello"

Choose the certificate authority (CA) where user certificates will be generated. You can choose multiple certificate authorities for load balancing and failover. [Refresh](#)

Name	Status
☒ ad-itu.net-AD-CA	Template available
☒ ad-itu.net-CA2-CA	Template available

☒ Only show CAs publishing Citrix_SmartcardLogon (recommended).

[Apply](#) [Cancel](#)

Todas las CA que seleccione deben publicar la plantilla de certificado Citrix_SmartcardLogon (o la plantilla que haya elegido en su regla).

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

NOTA:

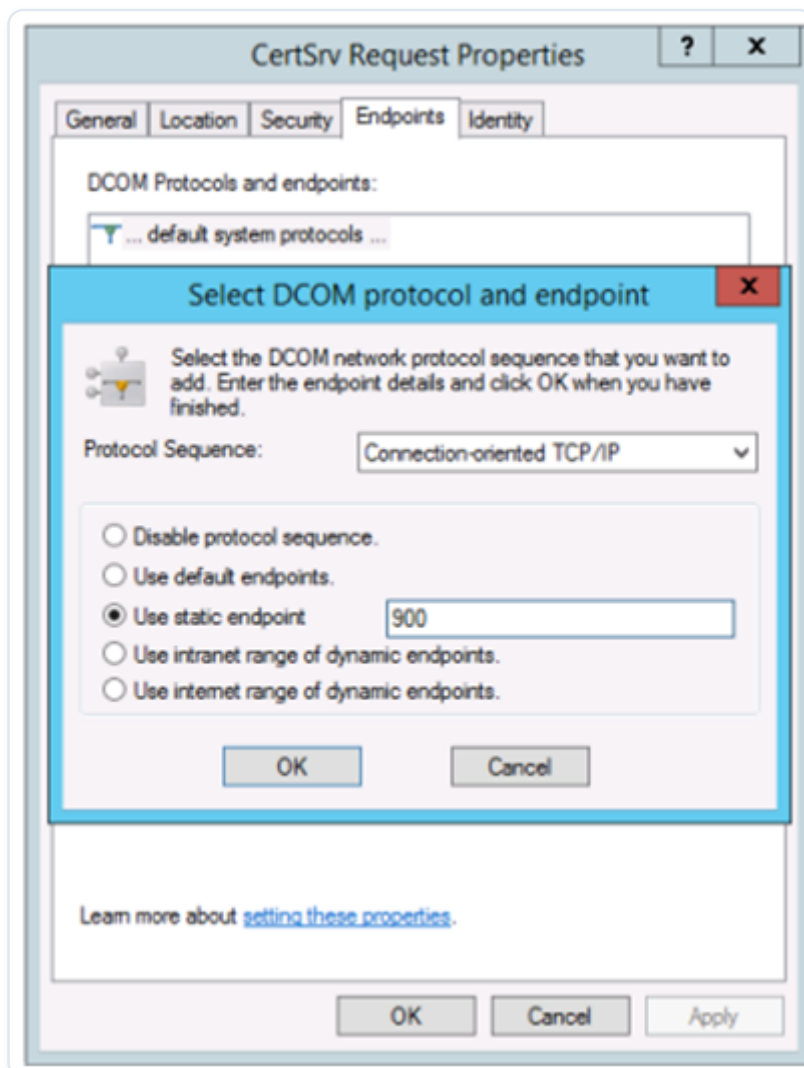
No es necesario realizar el paso [Autorizar este servicio](#) para cada CA, ya que el certificado de autorización configurado en este paso se puede usar en cualquiera de sus CA.

Cambios de comportamiento esperados

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

Configurar la autoridad de certificación de Microsoft para el acceso TCP

FAS accede a la CA de Microsoft mediante DCOM. DCOM utiliza el puerto 135 para detectar el puerto en el que el servicio está escuchando. De forma predeterminada, el puerto de escucha se asigna dinámicamente. Esto puede generar complejidades al implementar la seguridad del firewall. Por lo tanto, Microsoft tiene una disposición para configurar un puerto estático. Para configurar un puerto estático en la CA de Microsoft, seleccione **Inicio > Ejecutar > dcomcnfg.exe** para abrir el panel de **configuración de DCOM**. Expanda **Equipos > Mi PC > Configuración DCOM** para mostrar el nodo Solicitud de CertSrv. A continuación, edite las propiedades de la aplicación DCOM Solicitud de CertSrv:



Cambie los **Extremos** para seleccionar un extremo estático y especifique un número de puerto TCP (900 en el gráfico anterior).

En este ejemplo, el firewall debe permitir el puerto 135 y el puerto 900.

Reinicie la autoridad de certificación de Microsoft para aplicar el cambio.

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 135. Cuando un cliente necesita usar DCOM, se conecta al servicio DCOM RPC en el servidor y solicita acceso a un servidor DCOM particular. Esto hace que se abra el puerto 900 (en este ejemplo), y el servidor DCOM indica al cliente que se conecte a ese puerto.

Pre-generar certificados de usuario

El tiempo de inicio de sesión para los usuarios mejorará significativamente cuando los certificados de usuario se pre-generen 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 el 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
```

```
}
```

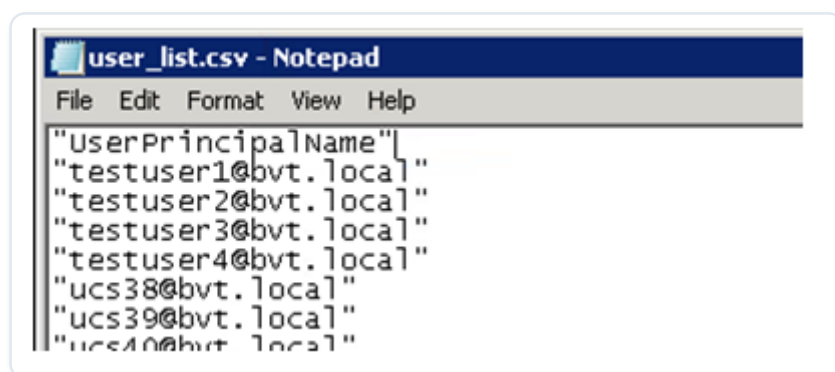
`Get-ADUser` es un cmdlet estándar para consultar una lista de usuarios. El ejemplo anterior contiene un argumento de filtro para listar solo los usuarios con un `UserPrincipalName` y un estado de cuenta 'habilitado'.

El argumento `SearchBase` restringe la parte del AD donde buscar usuarios. Puede omitirlo si desea incluir a todos los usuarios del 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 genera 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'), 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](#)

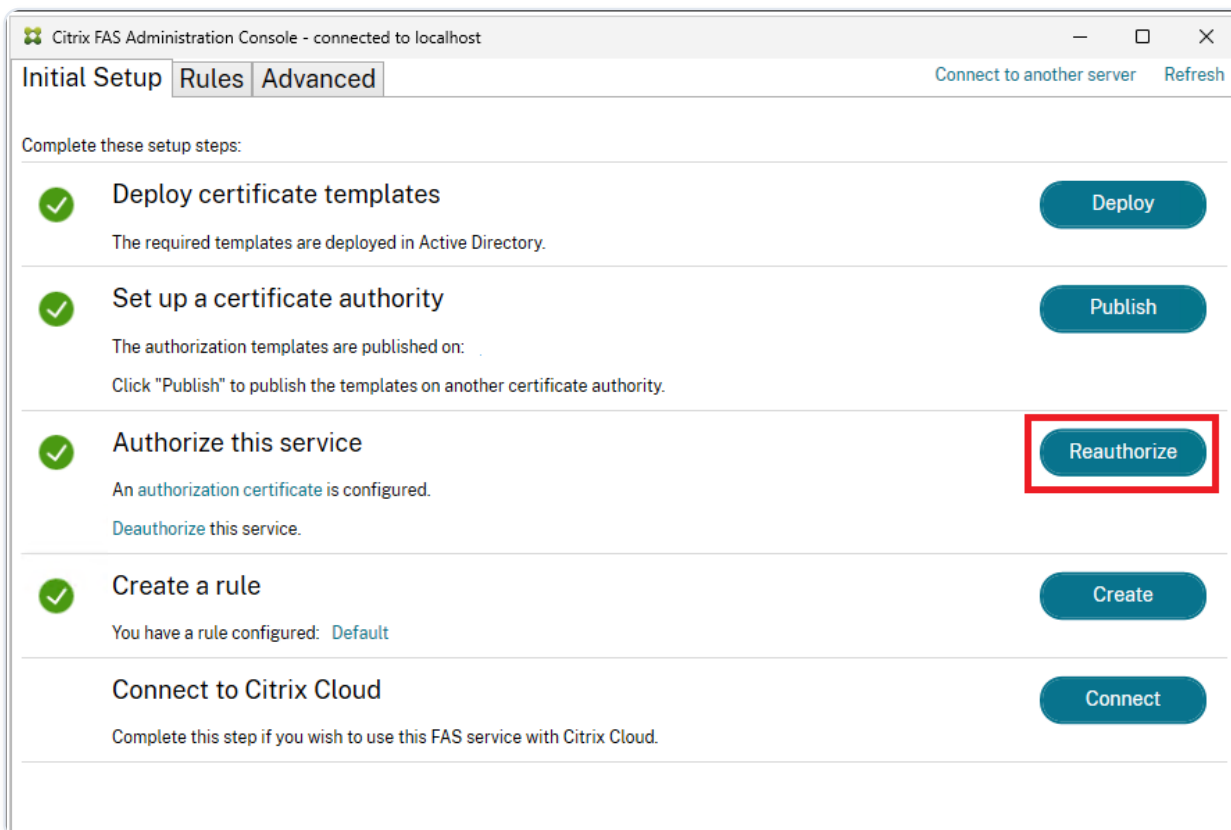
Rule Name	Summary
Default	
hello	Rule name: hello Status: OK Template: Citrix_SmartcardLogon

Renovar el certificado de autorización de FAS

Puede renovar un certificado de autorización de FAS sin interrumpir a los usuarios de FAS.

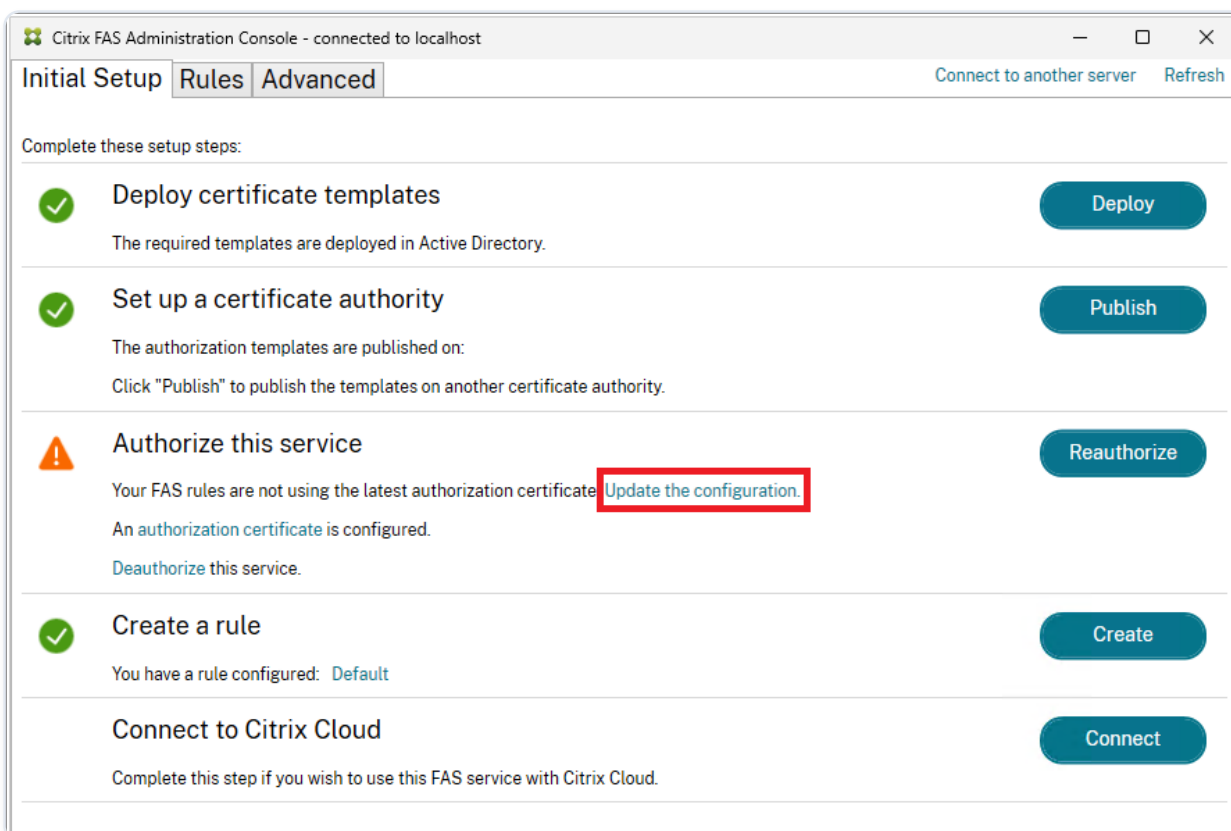
Uso de la consola de administración de FAS

- Haga clic en **Volver a autorizar** para generar una nueva solicitud de certificado de autorización de FAS:



Debe aprobar manualmente la solicitud en la CA. Para obtener más información, consulte [Autorizar Federated Authentication Service](#).

- Una vez que se ha generado un nuevo certificado de autorización, FAS indica que aún no está asociado con sus reglas. Haga clic en **Actualizar la configuración** para asociar el nuevo certificado de autorización con sus reglas.



Uso de PowerShell

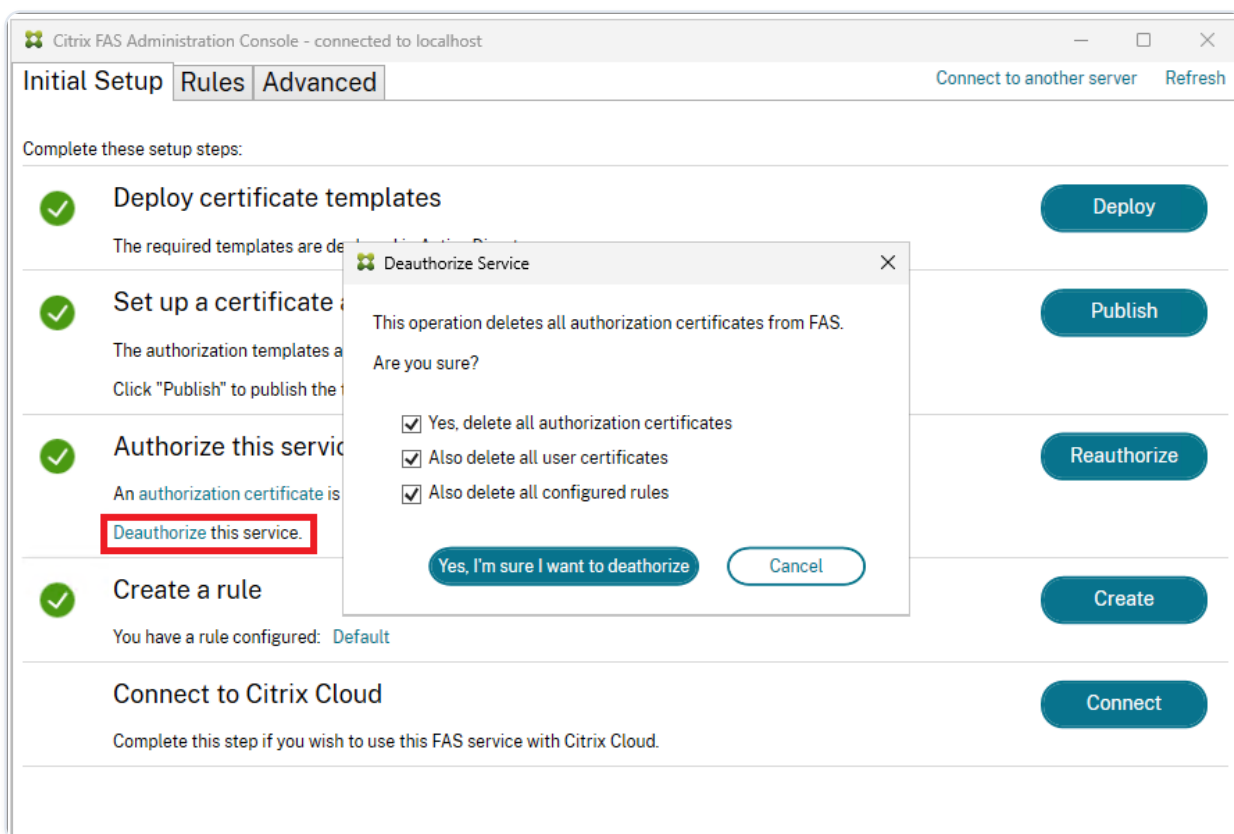
Complete la siguiente secuencia:

1. Crear un certificado de autorización: `New-FasAuthorizationCertificate`
2. Anote el GUID del nuevo certificado de autorización, tal como lo devuelve: `Get-FasAuthorizationCertificate`
3. Intercambiar el nuevo certificado de autorización: `Set-FasCertificateDefinition - AuthorizationCertificate <GUID>`
4. Eliminar el certificado de autorización antiguo: `Remove-FasAuthorizationCertificate`. Asegúrese de usar `DeleteUserCerts $false option`, para que la actividad del usuario no se vea interrumpida.

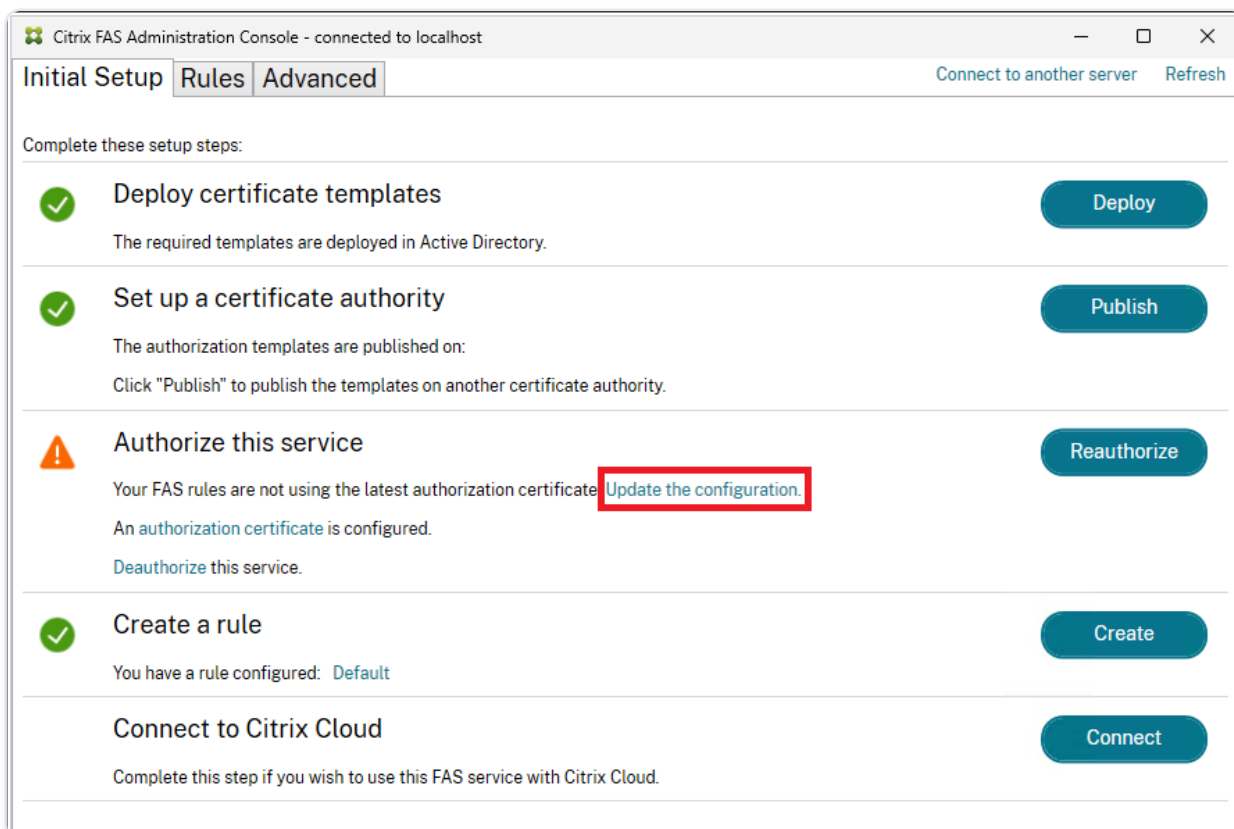
Desautorizar FAS y eliminar certificados FAS

Usar la consola de administración de FAS

- Haga clic en el enlace **Desautorizar** y elimine los certificados de autorización. Puede eliminar todos los certificados de usuario y todas las reglas (aunque no es necesario para borrar los certificados).



- Si no elimina las reglas, al autorizar FAS más tarde, recibirá una advertencia:



La advertencia indica que el certificado de autorización aún no está asociado a sus reglas. Haga clic en **Actualizar la configuración** para asociar el nuevo certificado de autorización a sus reglas.

Usar PowerShell

Utilice el siguiente comando de PowerShell para eliminar el certificado de autorización y los certificados de usuario:

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

NOTA:

`Get-FasAuthorizationCertificate` devuelve una lista de certificados de autorización y solicitudes de certificados de autorización pendientes, para que inspeccione el valor de `$AuthCert` antes de continuar con `Remove-FasAuthorizationCertificate`.

Puede eliminar el certificado de autorización, pero conservar los certificados de usuario, estableciendo el parámetro `DeleteUserCerts` en false:

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

Los certificados de usuario restantes aún pueden ser utilizados por FAS para el inicio de sesión de VDA y los certificados de sesión, lo que es útil al renovar la autorización de FAS. Para obtener más información, consulte [Renovar el certificado de autorización de FAS](#).

- Puede eliminar los certificados de usuario de la siguiente manera:

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

Este comando elimina todos los certificados de usuario del servidor FAS. El comando tiene opciones para filtrar el conjunto de certificados eliminados.

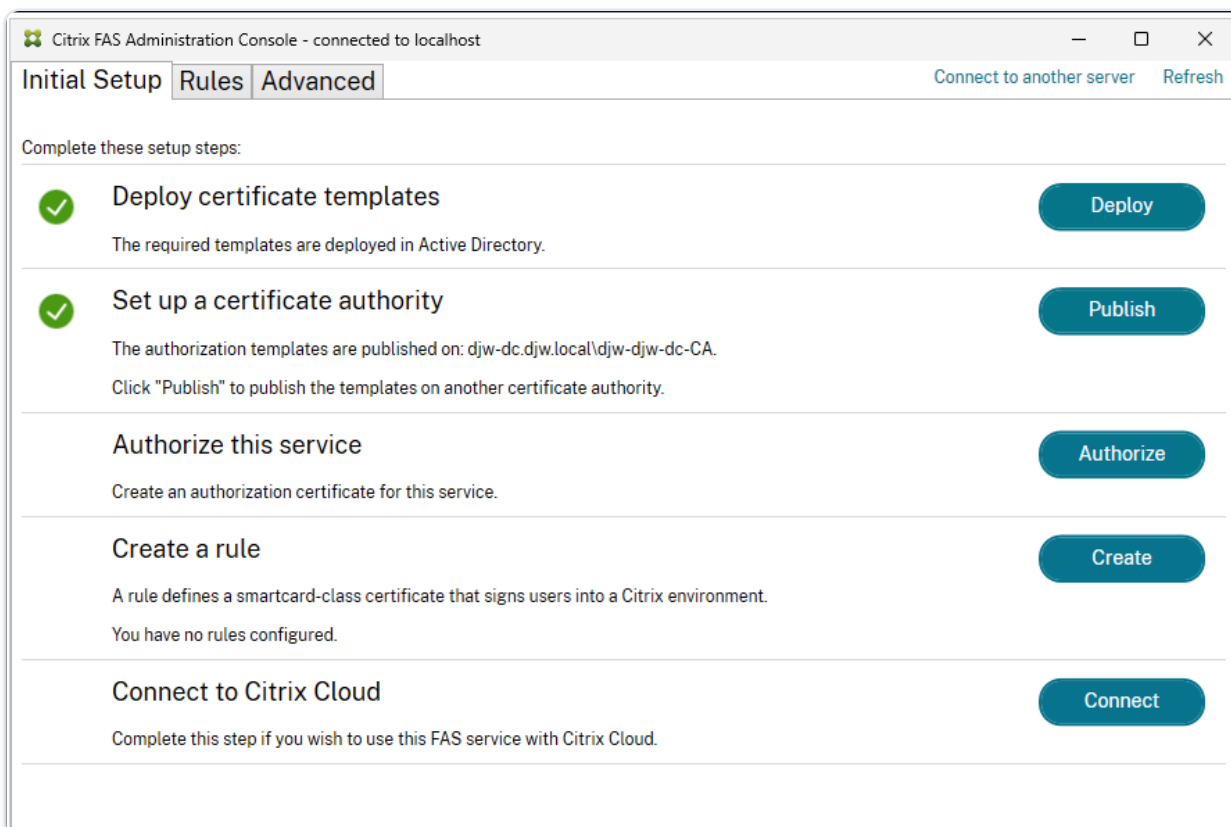
NOTA:

Cuando FAS elimina un certificado de autorización o de usuario de su almacenamiento interno, también elimina el par de claves asociado.

Autorización sin conexión

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

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**.



2. Cargue los siguientes cmdlets de PowerShell en el servidor FAS:

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

3. Genere el par de claves y cree la solicitud de firma de certificado introduciendo el siguiente cmdlet de PowerShell en el servidor FAS:

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

Esto da como resultado:

```
PS C:\> $AuthCertRequest = New-FasAuthorizationCertificateRequest -Address localhost
PS C:\> $AuthCertRequest

Id                : a0da658f-a7e4-49b7-a0c3-6381c26a83a5
Address           : [Offline CSR]
TrustArea         :
CertificateRequest : -----BEGIN CERTIFICATE REQUEST-----
                  [Redacted Content]
                  -----END CERTIFICATE REQUEST-----
Status            : WaitingForApproval
```

NOTA:

Las propiedades del par de claves generado vienen determinadas por la configuración de la clave de autorización de FAS. Para obtener más información, consulte [Protección de clave privada](#).

4. Copie la solicitud de certificado en el disco:

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

5. Presente el archivo de solicitud de certificado (en este ejemplo, authcert.csr) a su autoridad de certificación, apruebe la solicitud y obtenga una respuesta de certificado.

Los cinco pasos siguientes son específicos para usar una autoridad de certificación de Microsoft Enterprise; para otras CA, póngase en contacto con su proveedor de CA para obtener ayuda.

- En el servidor de la autoridad de certificación, agregue el complemento MMC Plantillas de certificado. Haga clic con el botón derecho 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 dos 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

- En el servidor de la entidad de certificación, agregue el complemento MMC de la entidad de certificación. Haga clic con el botón secundario en **Plantillas de certificado**. Seleccione **Nuevo** y, a continuación, haga clic en **Plantilla de certificado para emitir**. Elija la plantilla que creó.
- Envíe la solicitud de firma de certificado a su entidad de certificación escribiendo lo siguiente en un símbolo del sistema de PowerShell en el servidor FAS:

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

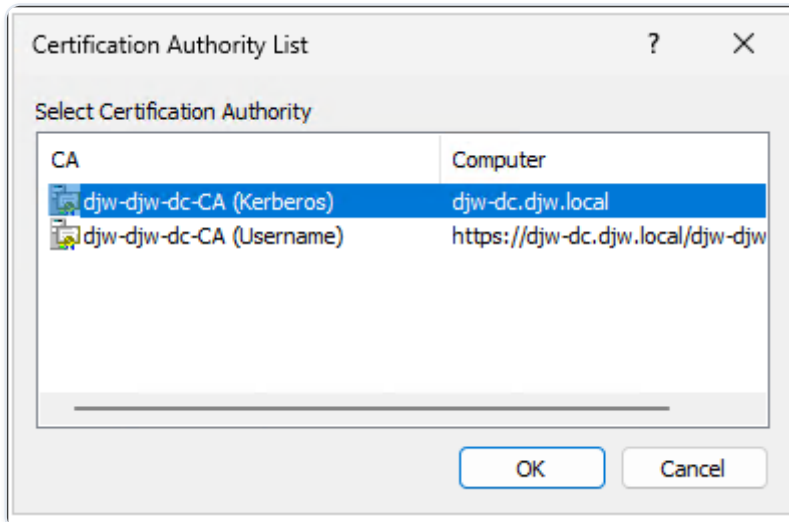
Por ejemplo:

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

La ejecución del comando anterior da como resultado:

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

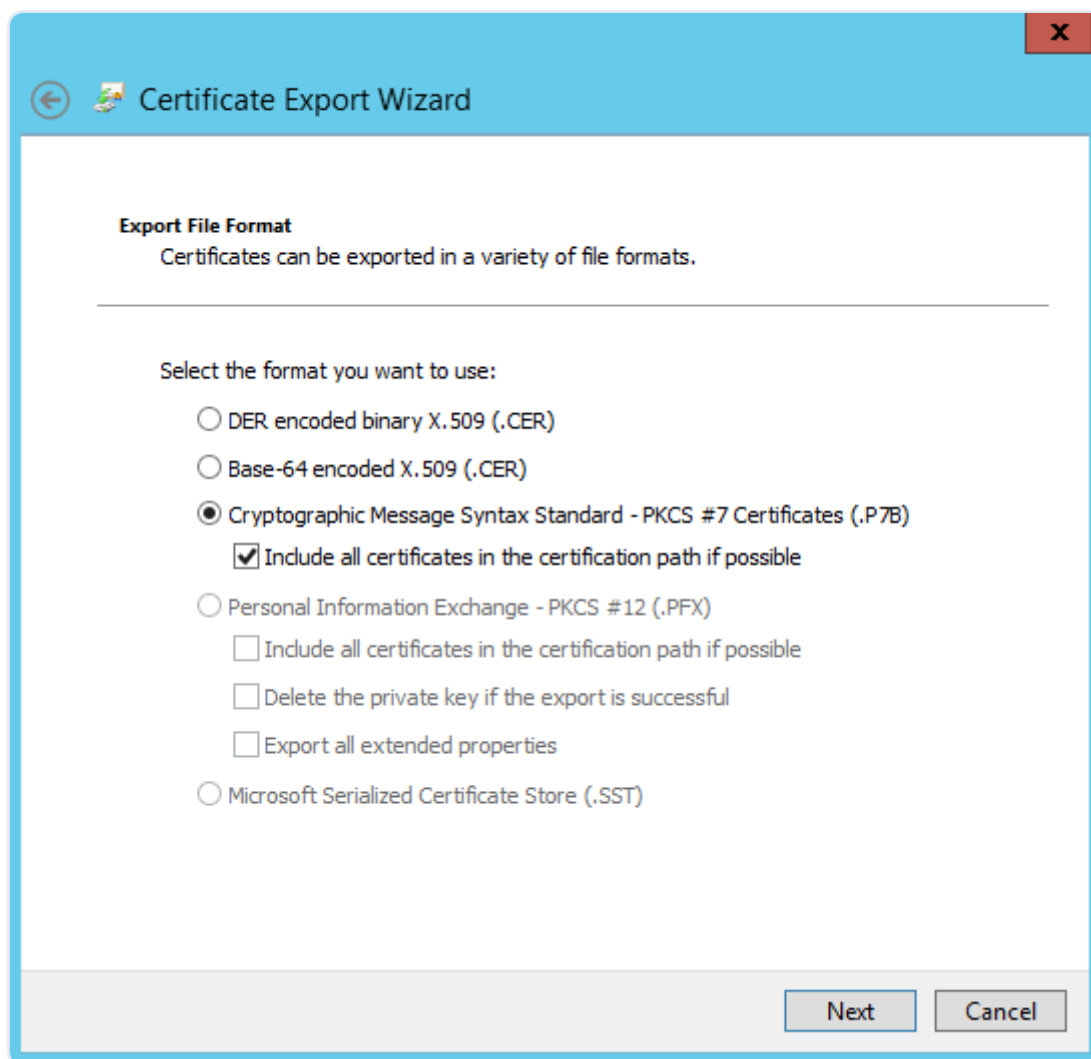
En este punto, puede aparecer una ventana de **Lista de entidades de certificación**. La entidad de certificación de este ejemplo tiene habilitada la inscripción DCOM (arriba) y HTTP (abajo). Seleccione **DCOM**, si está disponible, y luego haga clic en **Aceptar**:



Una vez especificada la entidad de certificación, el comando se completa y muestra el RequestID:

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

- En el servidor de la entidad de certificación, en el complemento MMC de la entidad de certificación, haga clic en **Solicitudes pendientes**. Busque el Request ID. Luego, haga clic con el botón secundario en la solicitud y elija **Emitir**.
- Seleccione el nodo **Certificados emitidos**. Busque el certificado que se emitió (el Request ID debe coincidir). Haga doble clic para abrir el certificado. Seleccione la ficha **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 **Cryptographic Message Syntax Standard – PKCS #7 Certificates (.P7B)** y debe estar seleccionada la opción **Incluir todos los certificados en la ruta de certificación si es posible**.

6. Copie el archivo de certificado exportado en el servidor FAS.
7. 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 localhost -Id  
$AuthCertRequest.Id -Pkcs7CertificateFile <Certificate file from step  
6>
```

Por ejemplo:

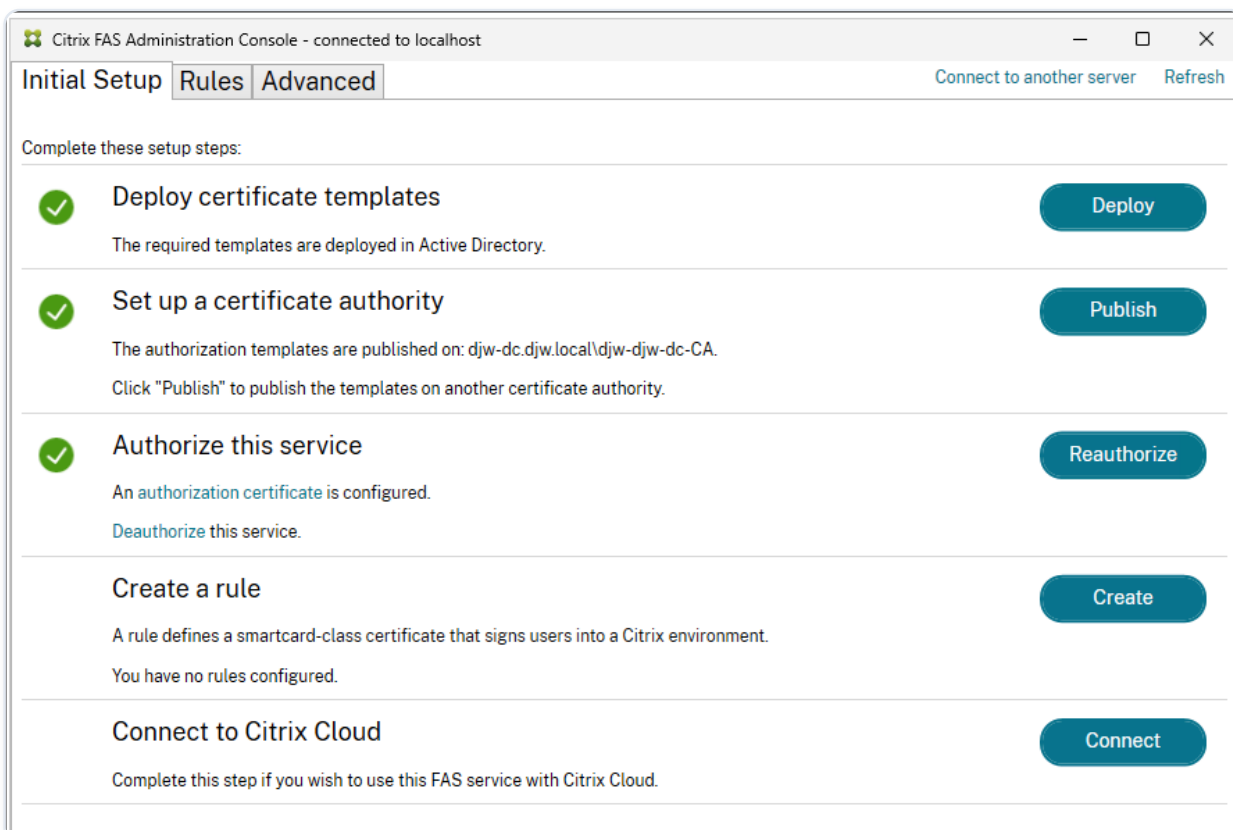
```
Import-FasAuthorizationCertificateResponse -Address localhost -Id  
$AuthCertRequest.Id -Pkcs7CertificateFile C:\temp\response.p7b
```

La ejecución de este comando da como resultado:

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

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

8. Compruebe la consola de administración de FAS. Debe mostrar que FAS ya está autorizado.



NOTA:

El paso **Autorizar este servicio** tiene una marca de verificación verde al lado.

9. Continúe la configuración creando una regla. Para obtener más detalles, consulte [Configurar reglas](#).

Información relacionada

- El artículo [Instalar y configurar](#) es la referencia principal para la instalación y configuración de FAS.
- Las implementaciones comunes del Servicio de autenticación federada se resumen en el artículo [Arquitecturas de implementación](#).

- Otros artículos **prácticos** se presentan en el artículo [Configuración avanzada](#).

Protección de clave privada

Introducción

Los certificados de FAS se almacenan en una base de datos incrustada en el servidor FAS. Las claves privadas asociadas a los certificados de FAS se almacenan en la cuenta de Servicio de red del servidor FAS. De forma predeterminada, las claves no son exportables, son RSA de 2048 bits y se crean y almacenan en el Proveedor de almacenamiento de claves de software de Microsoft.

Mediante los comandos de PowerShell de FAS [cmdlets de PowerShell](#), es posible cambiar las propiedades y la ubicación de almacenamiento de las claves privadas.

NOTA:

La configuración y los certificados de FAS se almacenan localmente en el servidor FAS. Los datos no se comparten entre los servidores FAS.

En las versiones de FAS anteriores a Citrix Virtual Apps and Desktops 2411, las propiedades de la clave privada se configuraban editando el archivo XML en `%programfiles%\Citrix\Federated Authentication`

`Service\Citrix.Authentication.FederatedAuthenticationService.exe.config`. Esto ha sido reemplazado por comandos de PowerShell, que ofrecen más flexibilidad y se pueden aplicar sin reiniciar el servidor FAS. Además, a diferencia de la configuración del archivo XML, la configuración realizada con PowerShell se mantiene cuando se actualiza el servidor FAS. Por lo tanto, la configuración mediante el archivo XML para los siguientes ajustes ya no es compatible:

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

Consulte la sección [Actualización desde versiones de FAS anteriores a Citrix Virtual Apps and Desktops™ 2411](#).

Información sobre certificados y plantillas de FAS

FAS posee dos tipos de certificados: el certificado de autorización, del que normalmente hay una instancia, y los certificados de usuario.

NOTA:

El certificado de autorización de FAS también se conoce a veces como certificado de **Autoridad de registro o Agente de solicitud (RA)**.

FAS utiliza plantillas de certificado al solicitar certificados, como se describe en la siguiente sección. Aunque FAS especifica el nombre de una plantilla en las solicitudes de certificado, no lee el contenido de la plantilla. Por lo tanto, cambiar la configuración de la plantilla no influye en las solicitudes de certificado realizadas por FAS. Cambiar ciertas propiedades de la plantilla afecta al certificado generado por la CA. Por ejemplo, puede cambiar el período de validez mediante la plantilla.

Certificado de autorización de FAS

Este certificado se crea al configurar FAS. Puede usar el botón **Autorizar** o **Volver a autorizar** de la consola de administración de FAS para solicitar un nuevo certificado de autorización.

También es posible usar comandos de PowerShell, que ofrecen más flexibilidad:

- `New-FasAuthorizationCertificate`: Este comando se comporta de forma similar a la consola de administración de FAS, excepto que es posible especificar las plantillas de certificado que se usarán en el proceso de autorización.
- `New-FasAuthorizationCertificateRequest`: Este comando crea una solicitud *sin conexión* para un certificado de autorización; [Autorización sin conexión](#).

El certificado de autorización también se conoce a veces como certificado RA, porque FAS actúa como una autoridad de registro, es decir, solicita certificados en nombre de un usuario. El certificado tiene el uso de clave mejorado **Agente de solicitud de certificado**, que permite usarlo como credencial de autorización al solicitar certificados de usuario de FAS.

De forma predeterminada, el proceso de autorización utiliza las siguientes plantillas:

- `Citrix_RegistrationAuthority_ManualAuthorization`: El certificado creado con esta plantilla es temporal y de corta duración, y se utiliza para *arrancar* el proceso de autorización;
- `Citrix_RegistrationAuthority`: El certificado creado con esta plantilla tiene una validez prolongada y lo almacena el servidor FAS.

La autorización de FAS da como resultado los siguientes pasos:

1. FAS crea un par de claves y envía una **Solicitud de firma de certificado** (CSR) a la CA, especificando la clave pública del par de claves y la plantilla `Citrix_RegistrationAuthority_ManualAuthorization`.
2. Los requisitos de emisión de la plantilla especifican que la CSR debe ser aprobada manualmente por el administrador de la CA.
3. Una vez que el administrador de la CA ha aprobado la CSR, la CA crea un certificado que FAS recupera. Este certificado tiene una validez corta de un día y solo se utiliza para el siguiente paso. Una vez utilizado, FAS destruye el certificado y su par de claves.
4. FAS crea otro par de claves y envía una segunda CSR a la CA, especificando la clave pública de este par de claves y la plantilla `Citrix_RegistrationAuthority`. La solicitud es autorizada y firmada con el certificado del paso anterior.
5. La CA emite automáticamente el certificado, FAS lo recupera y FAS ahora está **Autorizado**. De forma predeterminada, este certificado de autorización tiene una validez de dos años.

La configuración utilizada para crear los pares de claves mencionados anteriormente se puede ver con este comando de PowerShell:

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

Certificados de usuario de FAS

FAS crea certificados de usuario para iniciar sesión de los usuarios en los VDA.

Cuando FAS crea un certificado de usuario, se producen los siguientes pasos:

- FAS crea un par de claves y envía una CSR a la CA, especificando la clave pública del par de claves, la identidad del usuario y, de forma predeterminada, la plantilla `Citrix_SmartcardLogon` (la plantilla utilizada es configurable).
- La CSR se firma con el certificado de autorización de FAS.
- La plantilla `Citrix_SmartcardLogon` tiene el requisito de emisión `Application Policy: Certificate Request Agent`. Como este atributo está presente en el certificado de autorización de FAS, la CA emite automáticamente el certificado de usuario.
- FAS recupera el certificado y lo almacena en una base de datos incrustada en el servidor FAS.
- De forma predeterminada, el certificado tiene una validez de una semana.

Más tarde, el certificado de usuario se pone a disposición del VDA para iniciar sesión del usuario.

La configuración utilizada para crear el par de claves mencionado anteriormente se puede ver con el siguiente comando de PowerShell:

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

Opciones de almacenamiento de claves privadas

FAS se puede configurar para crear y almacenar pares de claves en tres categorías de almacenamiento:

- **Software:** Normalmente, mediante el **Proveedor de almacenamiento de claves de software de Microsoft**, que solo está protegido por software; los datos se almacenan en el disco.
- **Módulo de plataforma segura (TPM):** El TPM puede ser hardware físico en el equipo o un TPM virtual proporcionado por un hipervisor.
- **Módulo de seguridad de hardware (HSM):** Es un periférico de hardware o un dispositivo de red diseñado para almacenar de forma segura claves criptográficas.

NOTA:

Hay que tener en cuenta una contrapartida. El almacenamiento de hardware puede ser más seguro, pero a menudo es menos eficiente, especialmente al crear y almacenar un gran número de pares de claves de certificados de usuario.

La clave privada asociada al certificado de autorización de FAS es especialmente sensible, ya que la directiva del certificado permite a quien posea la clave privada autorizar solicitudes de certificado para cualquier usuario. Como consecuencia, quien controle esta clave puede conectarse al entorno como cualquier usuario.

NOTA:

Las CA de Microsoft se pueden configurar para restringir el poder del certificado de autorización de FAS, incluido el conjunto de usuarios para los que se pueden emitir certificados. Consulte [Agentes de inscripción delegados](#).

Por esta razón, FAS le permite configurar las propiedades de la clave privada para los certificados de autorización y de usuario de forma independiente.

Algunas configuraciones típicas son las siguientes:

CLAVE DE CERTIFICADO DE AUTORIZACIÓN	CLAVES DE CERTIFICADO DE USUARIO	COMENTARIO
Software	Software	Configuración predeterminada
TPM	Software	El certificado de autorización tiene protección de hardware
HSM	HSM	Todos los certificados tienen protección de hardware

NOTA:

No se recomienda un TPM de hardware para las claves de usuario. Utilice TPM solo para la clave del certificado de autorización. Si tiene previsto ejecutar su servidor FAS en un entorno virtualizado, consulte con su proveedor de hipervisor si se admite la virtualización de TPM.

Comandos de PowerShell para la configuración de claves

Los comandos relacionados con la configuración de claves privadas son los siguientes:

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

Para obtener más información, consulte [cmdlets de PowerShell](#).

La configuración de clave para los certificados de autorización y de usuario es independiente, especificada por el argumento `CertificateType`. Por ejemplo, para obtener la configuración de clave privada utilizada al solicitar un certificado de autorización (certificado RA):

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

Para obtener la configuración de clave privada utilizada al solicitar un certificado de usuario:

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

Puede usar **Set-FasKeyConfig** y **Get-FasKeyConfig** para establecer e inspeccionar las siguientes propiedades de clave privada:

PROPIEDAD	PREDETERMINADO	COMENTARIO
Longitud	2048	Longitud de clave en bits. Tenga en cuenta que, en la GUI de la plantilla de Microsoft, la pestaña Cryptograhpy especifica el tamaño de clave <i>mínimo</i>. La CA rechaza la CSR si la longitud de clave configurada en FAS es inferior al tamaño de clave mínimo especificado en la plantilla. Para claves RSA, las longitudes pueden ser 1024 bits, 2048 bits o 4096 bits. Para claves ECC, las longitudes pueden ser 256 bits, 384 bits o 521 bits.
Exportable	falso	Si la clave privada se puede exportar desde su proveedor.
Prefijo	ninguno	Especifica un prefijo para añadir al identificador de las claves privadas generadas por FAS. Los identificadores generados se componen del prefijo y un GUID. Por

PROPIEDAD	PREDETERMINADO	COMENTARIO	
		ejemplo, MyPrefix70277985 -6908-4C6F-BE59- B08691456804 .	
EllipticCurve	falso	Si es true, se genera un par de claves ECC; de lo contrario, se genera un par de claves RSA.	
Proveedor de almacenamiento de claves (KSP)	verdadero	Si es verdadero, FAS utiliza la API moderna de Windows CNG, y se debe especificar un KSP en la propiedad Provider . Si es falso, FAS utiliza la API CAPI heredada, y se debe especificar un Proveedor de servicios criptográficos (CSP) en la propiedad Provider. Citrix recomienda usar un KSP.	
Provider	Microsoft Software Key Storage Provider	El nombre del proveedor donde se crean y almacenan los pares de claves. Puede cambiar esta propiedad para especificar un TPM o HSM. El KSP (o CSP) de un HSM lo proporciona el	

PROPIEDAD	PREDETERMINADO	COMENTARIO
		proveedor del HSM. Ellos proporcionan instrucciones sobre cómo instalar su software y el nombre del proveedor.
CSPTType	24	Solo relevante si la propiedad KSP está establecida en false. Se refiere a Microsoft KeyContainerPermissionAccessEntry.ProviderType Property PROV_RSA_AES 24 . Siempre debe ser 24 a menos que esté utilizando un HSM con un CSP, y el proveedor del HSM especifique lo contrario.

Además, **Set-FasKeyConfig** se puede usar con los siguientes modificadores, proporcionados para mayor comodidad:

INDICADOR	DESCRIPCIÓN
-UseDefaultSoftwareProvider	Establece la propiedad Provider en Microsoft Software Key Storage Provider y el campo KSP en true .
-UseDefaultTpmProvider	Establece la propiedad Provider en Microsoft Platform Crypto Provider y el campo KSP en true .

Microsoft Software Key Storage Provider es el proveedor que se usa normalmente para crear y almacenar claves en el disco.

Microsoft Platform Crypto Provider es el proveedor que se usa normalmente para crear y almacenar claves en un TPM.

Get-FasKeyConfig también proporciona campos que ayudan a confirmar qué proveedor y algoritmo se están utilizando:

CAMPO	SIGNIFICADO
IsDefaultSoftwareProvider	Si es true, indica que el proveedor está establecido en Microsoft Software Key Storage Provider y el campo KSP está establecido en true .
IsDefaultTpmProvider	Si es verdadero, indica que el proveedor está configurado como Microsoft Platform Crypto Provider y el campo KSP está configurado como true .
Algoritmo	RSA indica que se crearán claves RSA (la propiedad EllipticCurve es false). ECC indica que se crearán claves ECC (la propiedad EllipticCurve es true).

Puede restaurar la configuración predeterminada usando `Reset-FasKeyConfig`.

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

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

NOTA:

Los cambios realizados en la configuración de la clave privada (usando `Set-FasKeyConfig` o `Reset-FasKeyConfig`) se aplican inmediatamente a los certificados recién creados. Sin embargo, los certificados de autorización y de usuario existentes con una configuración diferente no se ven afectados.

Puede eliminar los certificados existentes desautorizando el servicio FAS desde la consola de administración o usando comandos de PowerShell en [Desautorizar FAS y eliminar certificados FAS](#).

Cualquier clave pregenerada en el grupo de claves que no se ajuste a la configuración actual de la clave de usuario se descarta.

Ejemplos de escenarios de configuración

En cada ejemplo, configure la clave usando PowerShell antes de autorizar el servicio FAS, ya que los certificados existentes no se ven afectados por ningún cambio de configuración.

Si ya tiene certificados de autorización o de usuario con una configuración de clave incorrecta, puede eliminarlos consultando [Inspeccionar certificados FAS](#) y [Desautorizar FAS y eliminar certificados FAS](#).

Si su servidor FAS está en una implementación *activa*, considere ponerlo en modo de mantenimiento mientras realiza cambios de configuración [Modo de mantenimiento](#).

Ejemplo 1: Almacenar todas las claves en Microsoft Software Key Storage Provider

Como esto es así por defecto, no se requiere ninguna configuración adicional.

Si ha cambiado la configuración de su clave anteriormente, puede volver a usar el **Proveedor de almacenamiento de claves de software de Microsoft** con los siguientes comandos:

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

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

Puede usar `Reset-FasKeyConfig` para volver al **Proveedor de almacenamiento de claves de software de Microsoft** y, además, restaurar todas las demás configuraciones de clave a los valores predeterminados.

Ejemplo 2: Almacenar la clave del certificado de autorización en un TPM

Este ejemplo ilustra el almacenamiento de la clave del certificado de autorización de FAS en un TPM (real o virtual), mientras que las claves de los certificados de usuario se almacenan en el **Proveedor de almacenamiento de claves de software de Microsoft**.

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

Utilice los siguientes comandos de PowerShell:

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

Ejemplo 3: Almacenar todas las claves en un HSM

Este ejemplo ilustra el uso de un HSM para almacenar las claves privadas de los certificados de autorización y de usuario. Este ejemplo asume un HSM configurado. Su HSM tendrá un nombre de proveedor. Por ejemplo, **Proveedor de almacenamiento de claves del proveedor de HSM**.

Utilice los siguientes comandos de PowerShell (sustituya el texto de ejemplo por el nombre real del proveedor de su HSM):

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

Ejemplo 4: Usar claves de curva elíptica

De forma predeterminada, FAS genera claves RSA. En este ejemplo, las claves de curva elíptica (ECC) se configuran tanto para el certificado de autorización como para los certificados de usuario.

El ejemplo utiliza diferentes longitudes de clave. El certificado de autorización se configura con una clave de 384 bits y los certificados de usuario se configuran con una clave de 256 bits.

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

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

En este punto, las solicitudes de certificados de autorización y de usuario pueden ser rechazadas por la CA porque el tamaño mínimo de clave en las plantillas de certificados de FAS está establecido en 1024 bits de forma predeterminada.

Por lo tanto, para este ejemplo, es necesario cambiar el tamaño mínimo de clave en las plantillas de la siguiente manera:

- **Citrix_RegistrationAuthority_ManualAuthorization and Citrix_RegistrationAuthority** : Cambie el tamaño mínimo de clave a 384 (o inferior)
- **Citrix_SmartcardLogon** : Cambie el tamaño mínimo de clave a 256 (o inferior)

Para editar las plantillas, ejecute **mmc.exe** y agregue el complemento **Plantillas de certificado**. Localice la plantilla y abra sus propiedades. La configuración del tamaño mínimo de clave se encuentra en la ficha **Criptografía** de las propiedades de la plantilla.

NOTA:

Los certificados de usuario con claves ECC solo se admiten en VDA de Windows que ejecuten Citrix Virtual Apps and Desktops 2411 o posterior. Las claves ECC no se admiten en VDA de Linux.

Probar la configuración de la clave privada

Aunque el comando **Set-FasKeyConfig** realiza algunas validaciones, aún es posible establecer una configuración de clave no válida. Por ejemplo, puede cometer un error en el nombre del proveedor de su HSM, o la longitud de clave que especifique puede no ser compatible con su hardware.

El comando **Test-FasKeyConfig** puede ayudar. Intenta crear un par de claves utilizando la configuración de clave actual e informa de **éxito** o **error**. Si se produce un error, se proporciona una indicación del motivo del error. Si tiene éxito, el par de claves se destruye inmediatamente.

Los siguientes comandos de PowerShell prueban la autorización y la configuración de la clave de usuario, respectivamente:

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

Una vez que haya autorizado su servidor FAS y creado una regla, puede crear adicionalmente una CSR de prueba para un certificado de usuario de la siguiente manera:

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

Sustituya [<mailto:user@example.com/>](mailto:user@example.com) por un UPN real de su implementación de Active Directory. La regla de FAS normalmente se denomina **default**. Pero, si prefiere probar otra regla que haya configurado, especifique ese nombre en su lugar.

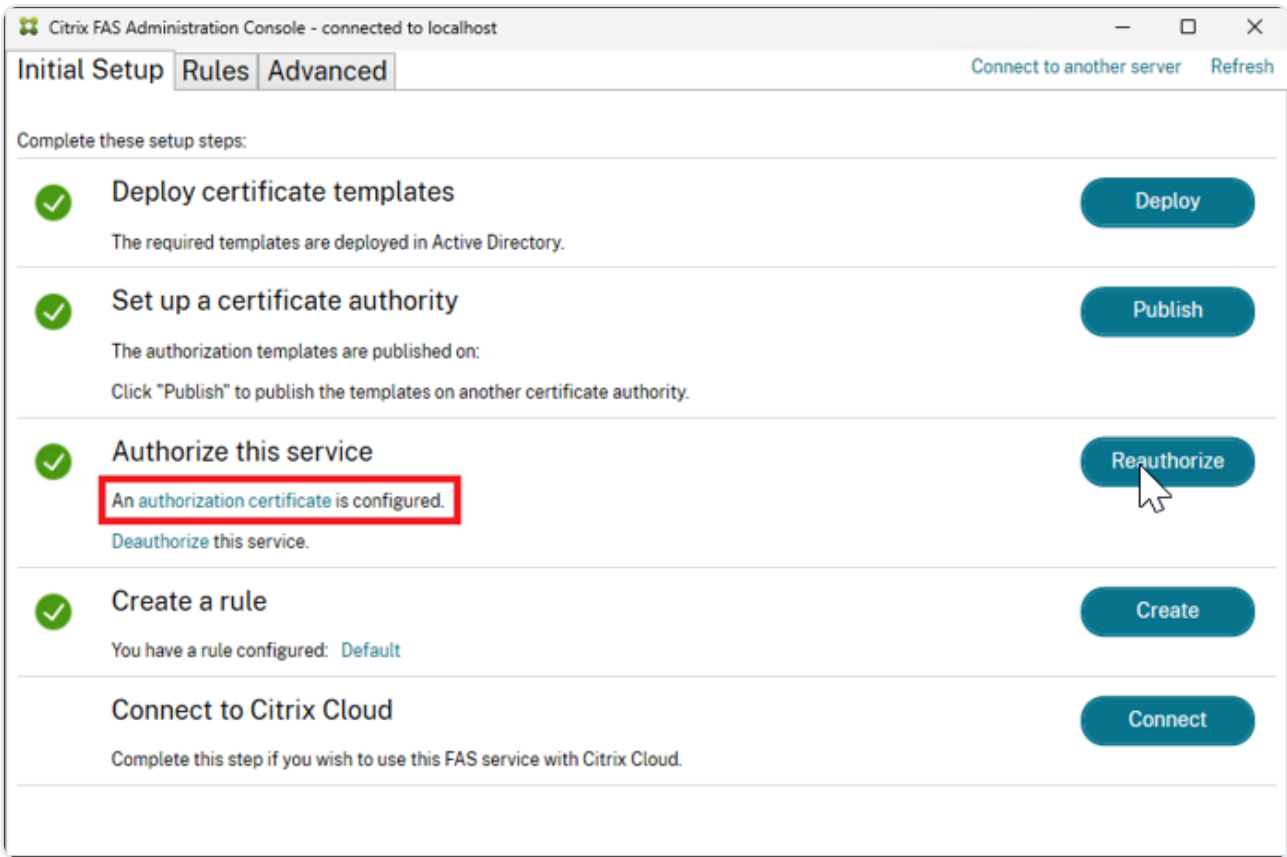
Si la CSR tiene éxito, FAS descarta el certificado resultante.

Inspeccionar certificados FAS

Puede usar PowerShell para inspeccionar las propiedades de un certificado y determinar dónde se almacena la clave privada asociada.

Inspección del certificado de autorización

Puede ver el certificado de autorización haciendo clic en el enlace **certificado de autorización** en la consola de administración de FAS:



Sin embargo, para obtener información más detallada, utilice PowerShell:

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

Se devuelven varios campos, incluido **PrivateKeyProvider**, que contiene una indicación del proveedor donde se creó y almacenó el certificado.

PRIVATEKEYPROVIDER	DÓNDE SE ALMACENA LA CLAVE
Proveedor de almacenamiento de claves de software de Microsoft	La clave se almacena en el disco, protegida por el proveedor de software de Microsoft.
Proveedor de criptografía de plataforma de Microsoft	La clave se almacena en un TPM (real o virtual).
Proveedor de almacenamiento de claves de proveedor de HSM (solo ejemplo)	La clave se almacena en un HSM (en este ejemplo, el proveedor del fabricante se denomina HSM Vendor Key Storage Provider)

Inspección de certificados de usuario

Puede obtener una lista de todos los certificados de usuario almacenados en caché en el servidor FAS de la siguiente manera:

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

El parámetro *KeyInfo* hace que la salida contenga más información sobre la clave privada asociada al certificado. En particular, el campo **PrivateKeyProvider** indica dónde se almacena el par de claves asociado al certificado (consulte la sección anterior para interpretar este valor).

Puede filtrar el conjunto de certificados devueltos utilizando varios parámetros opcionales, como `-UserPrincipalName`.

El campo de certificado de la salida del comando es un certificado de usuario codificado en PEM. Copie el texto en un archivo `.crt` para mostrar el certificado utilizando la GUI de certificados de Windows de la siguiente manera:

COMANDO	DESCRIPCIÓN
<pre>\$CertInfos = Get-FasUserCertificate -Address localhost</pre>	Puede haber varios certificados de usuario en esta lista
<pre>\$CertInfo = \$CertInfos[0]</pre>	En este ejemplo, seleccionamos el primer certificado de usuario
<pre>\$CertInfo.Certificate > c: \temp\user.crt</pre>	Envíe los datos PEM a un archivo <code>.crt</code>
<pre>c:\temp\user.crt</pre>	Abra el archivo <code>.crt</code> en la GUI de Windows

Actualización desde versiones de FAS anteriores a Citrix Virtual Apps and Desktops 2411

En las versiones de FAS anteriores a Citrix Virtual Apps and Desktops 2411, las propiedades de la clave privada se configuraban editando el archivo XML en

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

Esto ha sido sustituido por los comandos de PowerShell descritos en este documento, que ofrecen más flexibilidad y se pueden aplicar sin reiniciar el servidor FAS.

Además, a diferencia de la configuración del archivo XML, la configuración realizada con PowerShell se mantiene cuando se actualiza el servidor FAS.

La configuración del archivo XML relevante para la configuración de la clave privada se enumera a continuación, con sus parámetros de PowerShell correspondientes (tal como se utilizan en `Get-FasKeyConfig` y `Set-FasKeyConfig`):

CONFIGURACIÓN DEL ARCHIVO XML	VALOR PREDETERMINADO EN EL ARCHIVO XML	EQUIVALENTE DE POWERSHELL	COMENTARIO
<code>Citrix.Trust</code> <code>Fabric.Client</code> <code>SDK.TrustArea</code> <code>JoinParameters.KeyLength</code>	2048	<code>-Length</code>	-
<code>Citrix.Trust</code> <code>Fabric.Client</code> <code>SDK.TrustArea</code> <code>JoinParameters.KeyProtection</code>	<code>GenerateNonExportableKey</code>	<code>-Exportable</code> <code>-UseDefaultTpmProvider</code>	• <code>NoProtection</code> se logra configurando <code>-Exportable</code> en <code>\$true</code> <code>-GenerateNonExportableKey</code> se logra configurando <code>-Exportable</code> en <code>\$false</code> <code>-GenerateTPMProtectedKey</code> se logra especificando el

CONFIGURACIÓN DEL ARCHIVO XML	VALOR PREDETERMINADO EN EL ARCHIVO XML	EQUIVALENTE DE POWERSHELL	COMENTARIO
			modificador -UseDefaultTpmProvider
Citrix.TrustFabric.ClientSDK.TrustAreas.JoinParameters.ProviderLegacyCsp	falso	-Ksp	- ProviderLegacyCsp false se logra configurando -Ksp en \$true -ProviderLegacyCsp se logra estableciendo -Ksp en \$false
Citrix.TrustFabric.ClientSDK.TrustAreas.JoinParameters.ProviderName	-	-Provider	-
Citrix.TrustFabric.ClientSDK.TrustAreas.JoinParameters.ProviderType	-	-CspType	-

Los valores predeterminados de la configuración XML y los valores predeterminados de PowerShell son funcionalmente equivalentes. Es decir, de forma predeterminada, las propiedades

de los pares de claves generados por FAS en esta versión y en las versiones anteriores a Citrix Virtual Apps and Desktops 2411 son las mismas.

Por lo tanto, si no ha cambiado ninguna de las configuraciones anteriores en el archivo de configuración XML, no es necesario que realice ninguna acción al actualizar FAS.

Sin embargo, si ha cambiado alguna de las configuraciones anteriores, actualice FAS de la siguiente manera:

- Ponga FAS en modo de mantenimiento; [Modo de mantenimiento](#).
- Actualice FAS **in situ** simplemente ejecutando el instalador de FAS; una vez actualizado, todas las configuraciones anteriores no estarán presentes en el archivo XML y no se podrán configurar en el archivo XML.
- Utilice el comando de PowerShell `Set-FasKeyConfig`, como se describe en [Comandos de PowerShell para la configuración de claves](#), para establecer la configuración de la clave privada de FAS según sea necesario; tenga en cuenta la configuración que necesita para sus certificados de autorización y de usuario.
- Pruebe su configuración, como se describe en [Prueba de la configuración de la clave privada](#)
- Saque el servidor FAS del modo de mantenimiento

La próxima vez que actualice, se conservará la configuración de la clave privada de FAS y no será necesario realizar ninguna acción especial.

Remotización criptográfica

Las claves privadas asociadas a los certificados de usuario de FAS nunca se transfieren al VDA. En su lugar, cuando el VDA necesita utilizar el certificado FAS de un usuario, ya sea para iniciar sesión en el VDA o para su uso en la sesión, la solicitud criptográfica se envía de forma remota al servidor FAS. Esto mejora la seguridad, ya que las claves privadas nunca abandonan el almacenamiento de claves de FAS (ya sea almacenamiento de software, TPM o HSM).

En los VDA de Windows, esto se logra mediante el uso de un par de proveedores en el VDA. El código de la aplicación o del sistema operativo que realiza la solicitud criptográfica no sabe que la operación se está enviando de forma remota al servidor FAS.

Antes de Citrix Virtual Apps and Desktops 2411, los proveedores eran **Proveedores de servicios criptográficos** (CSP), donde el acceso del código de las aplicaciones y del sistema operativo se realizaba a través de la API CAPI de Windows más antigua. Los proveedores eran:

- `CitrixLogonCsp.dll`: para el inicio de sesión único en el VDA

- `CitrixVirtualSmartcardCsp.dll` : para certificados en la sesión

A partir de Citrix Virtual Apps and Desktops 2411, se suministran proveedores de almacenamiento de claves (KSP) adicionales en el VDA. Las aplicaciones y el código del sistema operativo acceden a estos con la API CNG de Windows más reciente. Los nuevos proveedores son:

- `CitrixLogonKsp.dll` : para el inicio de sesión único en el VDA
- `CitrixVirtualSmartcardKsp.dll` : para certificados en la sesión

KSP es una forma más actualizada de exponer las operaciones criptográficas a las aplicaciones de Windows, lo que proporciona más capacidades. Por ejemplo:

- Se admiten certificados con claves ECC
- Se admite el relleno de esquema de firma probabilística (PSS)

Se utiliza la comunicación remota de KSP (es decir, la comunicación remota a través de los nuevos KSP) si tanto FAS como el VDA ejecutan Citrix Virtual Apps and Desktops 2411 o posterior. De lo contrario, el sistema recurre al uso de los CSP más antiguos para la comunicación remota.

Inhabilitar la comunicación remota de KSP

En caso de problemas de compatibilidad, es posible inhabilitar la comunicación remota de KSP para que siempre se pueda utilizar la comunicación remota de CSP más antigua.

Utilice el siguiente PowerShell:

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

Modo de mantenimiento

Al realizar cambios en la configuración de un servidor FAS *activo*, considere la posibilidad de ponerlo en modo de mantenimiento.

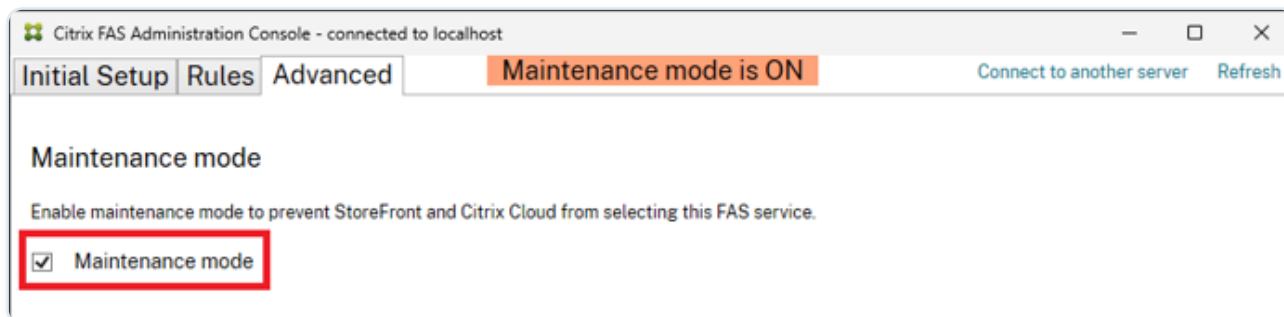
Cuando FAS está en modo de mantenimiento, se cumple lo siguiente:

- Cuando **Workspace** o **StoreFront™** llaman a FAS como parte de la secuencia de inicio de la aplicación o el escritorio publicados, FAS indica que está en modo de mantenimiento; el interlocutor debe reaccionar a esto eligiendo un servidor FAS diferente.
- Como precaución adicional, FAS no permite la creación automática de certificados de usuario cuando está en modo de mantenimiento. Así se evita la creación involuntaria de certificados de usuario con configuraciones no deseadas.

- Sin embargo, las actividades que implican certificados de usuario existentes, como el inicio de sesión de VDA o el uso en sesión, siguen estando permitidas.

Aunque no se permite la creación automática de certificados de usuario, los administradores pueden seguir creando certificados de usuario mediante comandos de PowerShell como `New-FasUserCertificate` o `Test-FasCertificateSigningRequest`.

Uso de la consola de administración



Uso de PowerShell

Ponga un servidor FAS en modo de mantenimiento de la siguiente manera:

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

Saque un servidor FAS del modo de mantenimiento (y vuelva a la operación normal) de la siguiente manera:

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

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

El Servicio de autenticación federada (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 visión 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 y seguridad

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.

Diagrama que muestra servidores y protocolos(/en-us/federated-authentication-service/2511/media/fas-security-network.png)

SERVIDOR	CONEXIONES
Servicio de autenticación federada	[in] HTTP con seguridad Kerberos desde StoreFront™ y VDA, [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 a Delivery Controller™, [out] HTTP con seguridad Kerberos a FAS
Controlador de entrega	[in] HTTPS desde el servidor StoreFront, [in/out] HTTP con seguridad Kerberos desde los VDA
VDA	[in/out] HTTP con seguridad Kerberos desde el Controlador de entrega, [in] HDX desde Citrix Gateway, [out] HTTP con seguridad Kerberos a FAS
Autoridad de certificación de Microsoft	[in] DCOM desde FAS

Comunicación entre StoreFront y FAS

- Al iniciar un VDA, el servidor StoreFront se pone en contacto con el servidor FAS para obtener un tíquet de un solo uso que necesita el agente de entrega virtual de Citrix (VDA) para iniciar sesión el usuario.
- StoreFront se conecta a FAS mediante SOAP a través de HTTP. De forma predeterminada, utiliza el puerto 80.
- Se autentica mediante Kerberos mutuo con la identidad Kerberos HOST/fqdn del servidor FAS y la identidad de cuenta de máquina Kerberos del servidor StoreFront.
- Los datos se cifran mediante [seguridad a nivel de mensaje](#). No se requiere ninguna configuración adicional para habilitar el cifrado.

Comunicación entre VDA y FAS

Cuando una sesión HDX™ se conecta al VDA, el VDA se pone en contacto con el servidor FAS para solicitar un certificado.

- El VDA se conecta al servidor FAS mediante SOAP a través de HTTP. De forma predeterminada, utiliza el puerto 80.
- Se autentica mediante Kerberos mutuo con la identidad Kerberos HOST/fqdn del servidor FAS y la identidad de máquina Kerberos del VDA. Además, el VDA debe proporcionar el "identificador de credencial" para acceder al certificado y la clave privada.
- Los datos se cifran mediante [seguridad a nivel de mensaje](#). No se requiere ninguna configuración adicional para habilitar el cifrado.

Comunicación entre FAS y la autoridad de certificación de Microsoft

Cuando un usuario inicia un VDA, si el servidor FAS aún no tiene un certificado para el usuario, se comunica con la autoridad de certificación para solicitar un certificado. La autoridad de certificación requiere que el servidor FAS proporcione un paquete CMC firmado por un certificado de agente de inscripción de confianza.

- El servidor FAS se comunica con la autoridad de certificación de Microsoft mediante DCOM. Para obtener información sobre los puertos necesarios, consulte la [documentación de Microsoft](#).
- Se autentica mediante Kerberos.

Conexiones entre Citrix Federated Authentication Service y Citrix Cloud™

Si va a conectar FAS a Citrix Cloud, los servidores FAS deben poder acceder a las siguientes direcciones a través del puerto HTTPS 443.

Citrix Cloud:

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

Citrix Cloud Japan:

- Consola de administración de FAS, en la cuenta del usuario
 - *.citrixcloud.jp
 - *.citrixworkspacesapi.jp
 - Direcciones requeridas por un proveedor de identidades de terceros, si se utiliza uno en su entorno
- Servicio FAS, en la cuenta de servicio de red:
 - *.citrixworkspacesapi.jp
 - *.citrixnetworkapi.jp

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.

Más información

Para obtener información sobre cómo proteger la comunicación entre otros componentes de Citrix, consulte los siguientes artículos:

- [Citrix Virtual Apps and Desktops - Consideraciones de seguridad y prácticas recomendadas.](#)

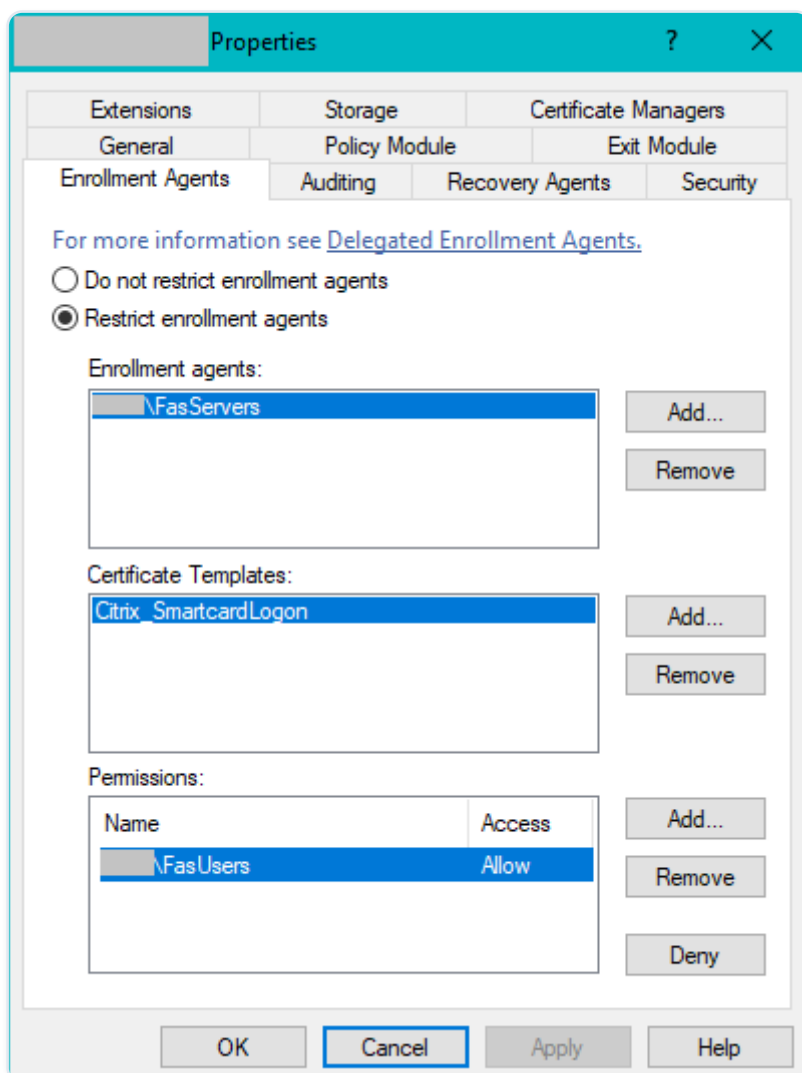
- Proteja su implementación de StoreFront.

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 entidad de certificación de Microsoft permite restringir los agentes de inscripción, las plantillas de certificado y los usuarios para los que los agentes de inscripción pueden emitir certificados.



Puede usar el cuadro de diálogo proporcionado para asegurarse de que:

- La lista *Agentes de inscripción* contiene solo servidores FAS (suponiendo que no se requieran otros agentes de inscripción en su implementación de Active Directory).

- La lista *Plantillas de certificado* contiene solo las plantillas FAS utilizadas para emitir certificados de usuario. De forma predeterminada, esta es la plantilla `Citrix_SmartcardLogon`.
- La lista *Permisos* contiene los usuarios a los que se les permite usar FAS. Por ejemplo, se recomienda no emitir certificados a administradores o al grupo Usuarios protegidos.

NOTA:

Cualquier cambio en la pertenencia a grupos de Active Directory de una cuenta de equipo no surte efecto hasta que se reinicia el equipo.

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 usuario a FAS cuando se emiten certificados. Del mismo modo, puede restringir a qué usuarios se les emiten certificados y a qué máquinas VDA pueden autenticarse. Esta función se suma a cualquier característica de seguridad estándar de Active Directory o de la entidad de certificación que configure.

Configuración del firewall

El servidor FAS debe aceptar conexiones entrantes de StoreFront y VDA, utilizando el puerto 80 a menos que [se configure de otra manera](#). Para obtener más información sobre la comunicación de red, consulte [Arquitectura de red y seguridad](#).

El instalador de FAS puede configurar opcionalmente el firewall de Windows. Para obtener más información, consulte [Opciones del instalador de FAS](#).

Cambiar el puerto del servidor FAS

El servidor FAS usa el puerto 80 de forma predeterminada. Puede personalizar el puerto:

NOTA:

Puede cambiar el puerto del servidor FAS al puerto 443, pero esto no cambia el protocolo utilizado por FAS. FAS no utiliza HTTPS aunque esté configurado en el puerto 443.

1. Ejecute la siguiente línea de comandos en su servidor FAS:

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

Sustituya `[port]` por el número de puerto que desee utilizar.

El conmutador `/CONFIGUREFIREWALL` hace que se actualice el firewall de Windows para permitir las conexiones entrantes en el puerto especificado.

2. Reinicie el servicio FAS.
3. En el objeto de directiva de grupo de FAS, actualice la lista de servidores FAS para incluir el puerto (por ejemplo, `fas.example.com:[port]`).
4. Propague el cambio al servidor FAS, StoreFront y el VDA (por ejemplo, usando `gpupdate /force`)

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 mediante los comandos de **PowerShell**. Se pueden usar diferentes configuraciones para las claves privadas de los certificados de autorización de FAS y las claves de los certificados de usuario. Para obtener más detalles, consulte [Protección de clave privada](#)

Responsabilidades de administración

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

NOMBRE	RESPONSABILIDAD
Administrador de empresa	Instalar y proteger plantillas de certificados en el bosque

NOMBRE	RESPONSABILIDAD
Administrador de dominio	Configurar la configuración de directivas de grupo
Administrador de la entidad de certificación	Configurar la entidad 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 VDAs 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

NOTA:

Si todos sus servidores FAS y VDA son de la versión 2511 o posterior, la lista FQDN de la directiva de grupo en el VDA ya no es necesaria. Consulte [Emisión de tickets de FAS V2 y la lista de direcciones del registro](#).

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 verificar 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. Además, si el servidor FAS está conectado a Citrix Cloud, la directiva de grupo también debe aplicarse al propio servidor 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.

La configuración de la directiva de grupo de FAS aparece en el registro en

`HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\Authentication` . La lista de FQDN de FAS de la directiva de grupo aparece en la subclave

`HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\Authentication\UserCredentialService\Addresses`

Plantillas de certificado

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

Cambiar el nombre de una plantilla de certificado

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

- Cree una copia de la plantilla de certificado y cámbiele el nombre para que coincida con el estándar de nomenclatura de plantillas de su organización.
- Utilice 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).
 - Utilice el complemento Plantillas de certificado de Microsoft MMC o el comando Publish-FasMsTemplate para publicar su plantilla, y
 - Utilice el comando New-FasCertificateDefinition para configurar FAS con el nombre de su 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 gestión de solicitudes

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

Consulte [Protección de clave privada](#) para ver la configuración que proporciona FAS.

Modificar las propiedades de criptografía

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

Consulte [Protección de clave privada](#) para ver la configuración equivalente 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 plantillas reemplazadas

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

Modificar las propiedades de 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

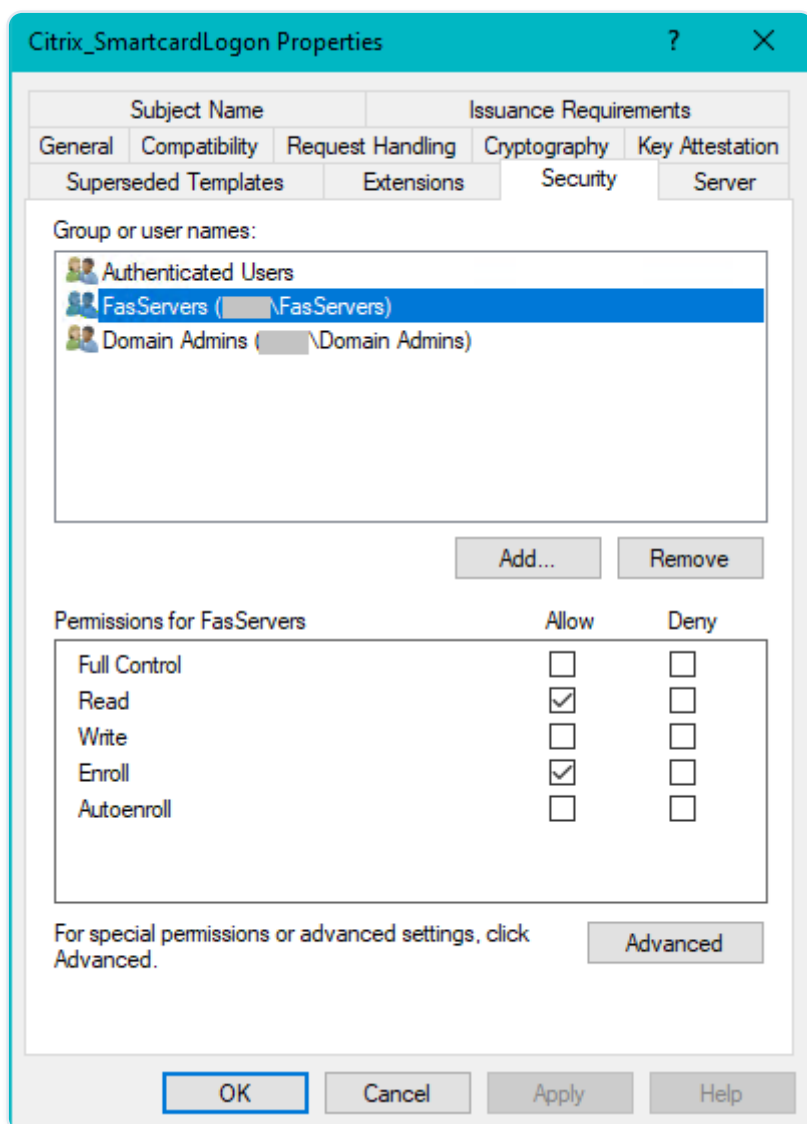
Citrix recomienda que modifique esta configuración para permitir los permisos de **Lectura e Inscripción** solo para las cuentas de máquina de los servidores FAS. El servicio FAS no requiere ningún otro permiso.

Además:

- permita que los **usuarios autenticados lean** la plantilla. Esto es necesario, ya que las propias entidades de certificación deben poder leer la plantilla.
- permita que los administradores de su entidad de certificación **lean y escriban** la plantilla.

La recomendación se aplica a las tres plantillas FAS:

- Citrix_SmartcardLogon
- Citrix_RegistrationAuthority
- Citrix_RegistrationAuthority_ManualAuthorization

**NOTA:**

Cualquier cambio en la pertenencia a grupos de Active Directory de una cuenta de equipo no surte efecto hasta que se reinicia el equipo.

Modificar las propiedades del nombre del sujeto

Citrix recomienda no modificar estas propiedades.

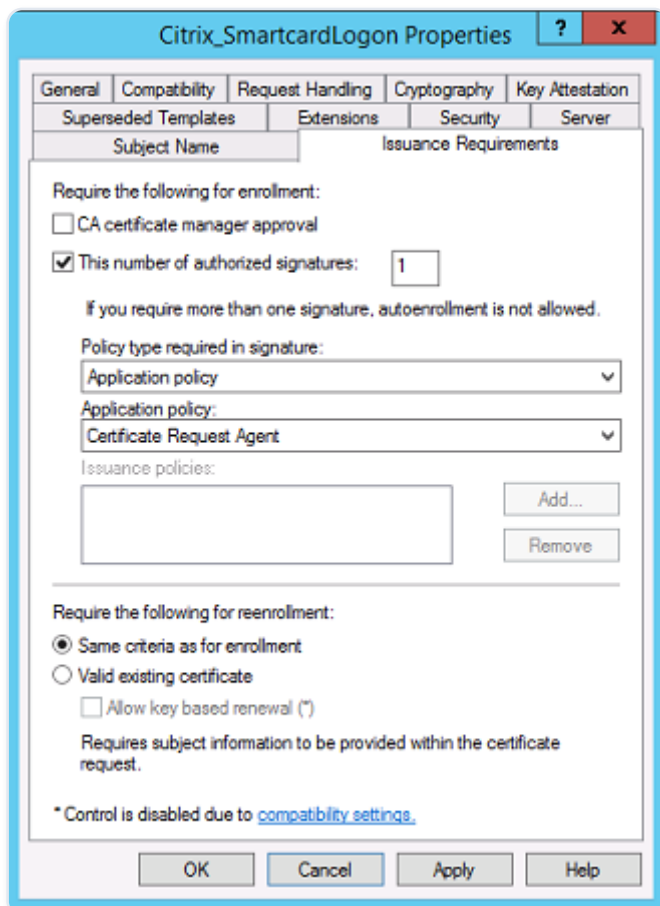
La plantilla tiene seleccionada la opción *Crear a partir de esta información de Active Directory*, lo que hace que la autoridad de certificación incluya el SID del usuario en una extensión de certificado, lo que proporciona una asignación sólida a la cuenta de Active Directory del usuario.

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 los requisitos de emisión

No modifique esta configuración. Esta configuración debe ser como 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 autoridad de certificación

El administrador de la autoridad de certificación es responsable de la configuración del servidor de la autoridad de certificación y de la clave privada del certificado de emisión que utiliza.

Publicación de plantillas

Para que una autoridad de certificación emita certificados basados en una plantilla proporcionada por el administrador de la empresa, el administrador de la autoridad 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 autoridad de certificación debe mantener un control total 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 autoridad de certificación tiene el control de la configuración del firewall de red de la autoridad de certificación, lo que permite controlar las conexiones entrantes. El administrador de la autoridad de certificación puede configurar reglas de firewall y DCOM TCP 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. Citrix recomienda que la emisión de certificados se restrinja a un grupo de usuarios sin privilegios mediante la propiedad de autoridad de certificación **Restringir agentes de inscripción**. Consulte [Agentes de inscripción delegados](#).

Módulos de directivas y auditoría

Para implementaciones avanzadas, se pueden utilizar 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 mediante una ACL

En el centro del modelo de seguridad de FAS se encuentra 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 utilizar certificados para los usuarios permitidos por la configuración de FAS.

VECTOR DE ACCESO	DESCRIPCIÓN
VDA [Relying party]	Estas son las máquinas a las que se permite acceder a los certificados y las claves privadas. También se necesita un identificador de credencial recuperado por el IdP, por lo que una cuenta 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 "Agente de inscripción restringido" 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 eleve los 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 usar 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 autorización de FAS esté protegida almacenándola en un TPM.

De manera similar, 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 al menos 2048 bits de longitud si se utiliza RSA.

NOTA:

Aunque FAS puede generar y almacenar claves de certificado de usuario en un TPM o HSM, el hardware puede ser demasiado lento o tener limitaciones de tamaño para implementaciones grandes.

Para obtener más detalles, consulte [Protección de clave privada](#).

Registros de eventos

El servidor FAS proporciona [registros de eventos](#) detallados de configuración y tiempo de ejecución, que se pueden usar 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 los registros de auditoría y eventos.

Seguridad general del servidor Windows

Todos los servidores deben estar completamente actualizados y disponer de un firewall estándar y software 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 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.

Compatibilidad con el Estándar Federal de Procesamiento de Información (FIPS)

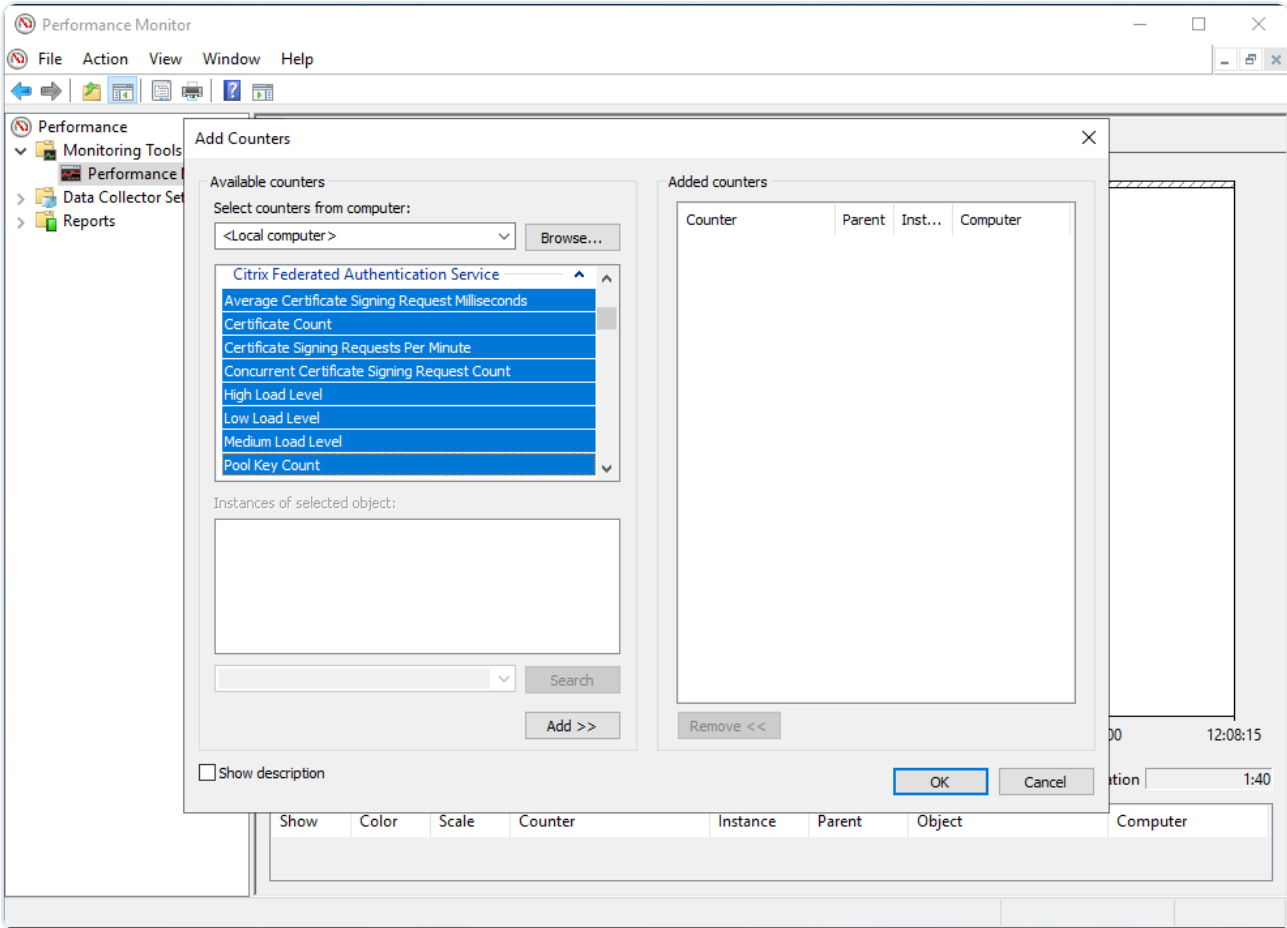
FAS utiliza los [algoritmos criptográficos validados por FIPS](#) en equipos Windows habilitados para FIPS. Si configura FAS para usar un TPM o HSM para el almacenamiento de claves, consulte a su proveedor de hardware para obtener información sobre el cumplimiento de FIPS.

Información relacionada

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

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 utilizando 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 utilizando 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 usar para solicitudes de firma de certificados.
Operaciones de clave privada por minuto	El número de operaciones de clave privada de certificado que realiza el Servicio de autenticación federada por minuto, calculado a partir de los datos del minuto anterior.
Recuento de sesiones	El número de sesiones VDA que rastrea el Servicio de autenticación federada.
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 o tarjetas inteligentes, o ambos. Estos registros proporcionan información que puede utilizar para solucionar problemas de autenticación.

Certificados e infraestructura de clave pública

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

- **Almacén de certificados NTAUTH:** 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 NTAUTH. Para ver estos certificados, desde el programa certutil, introduzca: `certutil -viewstore -enterprise NTAUTH`
- **Almacenes de certificados raíz e intermedios:** Normalmente, los sistemas de inicio de sesión con certificado 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 directivas 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)>).

DIRECTIVA 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 si 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 (establecido 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 de 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 de 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 (basándose en la identidad del proceso que busca el UPN) los UPN explícitos y, a continuación, 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 (de forma predeterminada, en un único dominio).

Se ofrece una opción para que el usuario especifique una cuenta de usuario que acelera esta búsqueda y también permite que esta característica 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, de modo que se puedan habilitar y recuperar los registros.

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 usa 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 nombredcnetbios #PRE #DOM:mydomai
```

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.

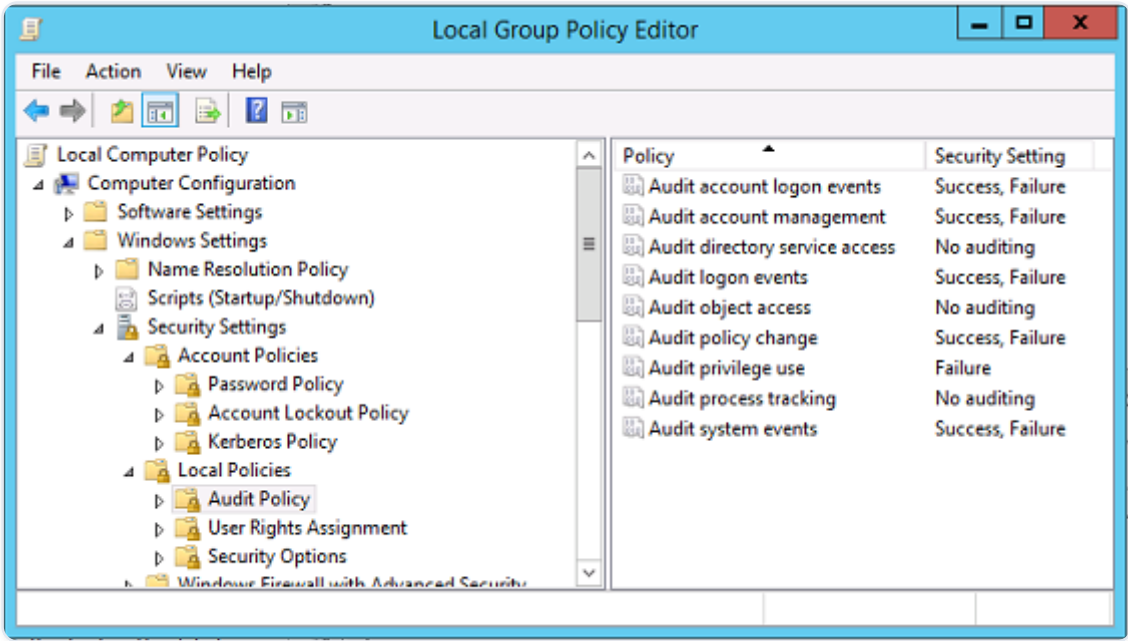
Identificar el controlador de dominio en uso

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 cuenta. Esto se puede controlar a través de las políticas 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 políticas de auditoría, el controlador de dominio produce información adicional de registro de eventos en el registro de seguridad.



Registros de validación de certificados

Comprobar la validez del certificado

Si un certificado de tarjeta inteligente se exporta como 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/Registros operativos.

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

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

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

VALOR	DESCRIPCIÓN
DiagLevel (DWORD)	Nivel de verbosidad (0 a 5)
DiagMatchAnyMask (QUADWORD)	Filtro de eventos (use 0xffffffff para todos)

VALOR	DESCRIPCIÓN
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 AppData\LocalLow\Microsoft\X509Objects
verificar política de cadena	LSA llamó a CertVerifyChainPolicy (incluye parámetros)

Mensajes de error

CÓDIGO DE ERROR	DESCRIPCIÓN
Certificado no de confianza	No se pudo generar el certificado de la tarjeta inteligente utilizando los certificados de los almacenes de certificados intermedios y de raíz 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 /es-es/federated-authentication-service/2511/config-manage/troubleshoot-logon.html#certificates-and-public-key-

CÓDIGO DE ERROR	DESCRIPCIÓN
	infrastructure) [Certificados e infraestructura de clave pública].
Errores de uso de 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

El registro de Kerberos se envía al registro de eventos del sistema.

- Los mensajes como **certificado no fiable** deben ser fáciles de diagnosticar.
- Dos códigos de error son informativos y 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 en 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 (krbtgt) de Kerberos.

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 utilizándose 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

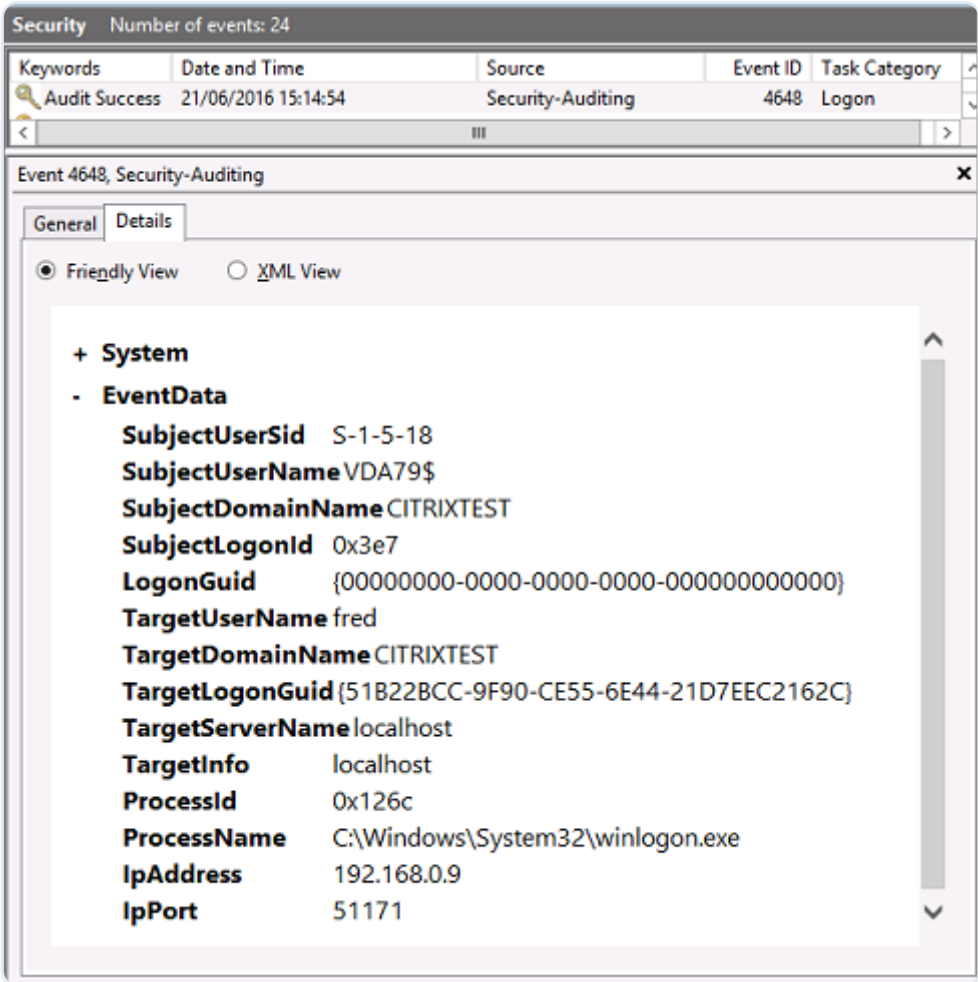
CertIssuerName citrixtest-DC-CA

CertSerialNumber 5F0001D1FCA2AC30F36879CEEC00000001D1FC

CertThumbprint 23BC65AFB7F18787ADAAAD5CEF09CC7505C4176F

Registro de seguridad del VDA

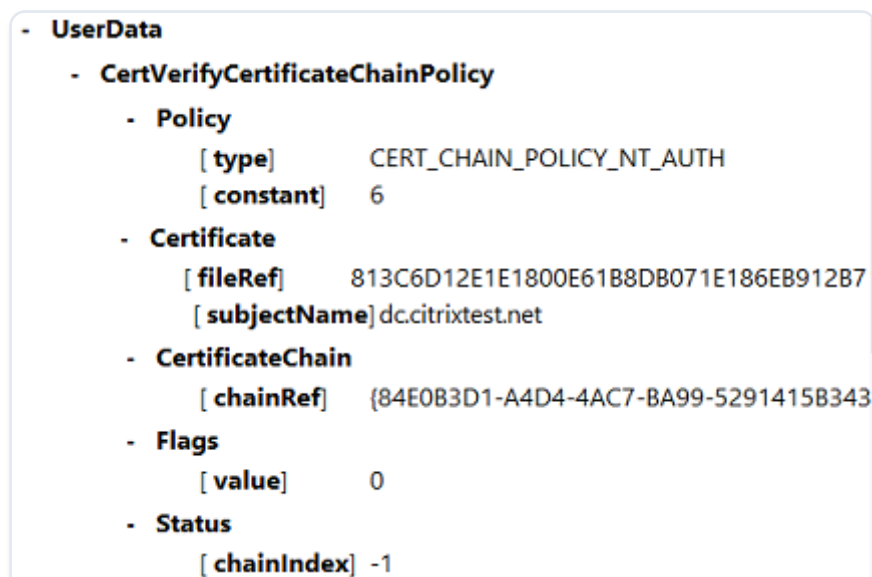
Los registros de auditoría de seguridad de VDA correspondientes al evento de inicio de sesión son la entrada con el ID de evento 4648, originada en winlogon.exe.



Registro CAPI de VDA

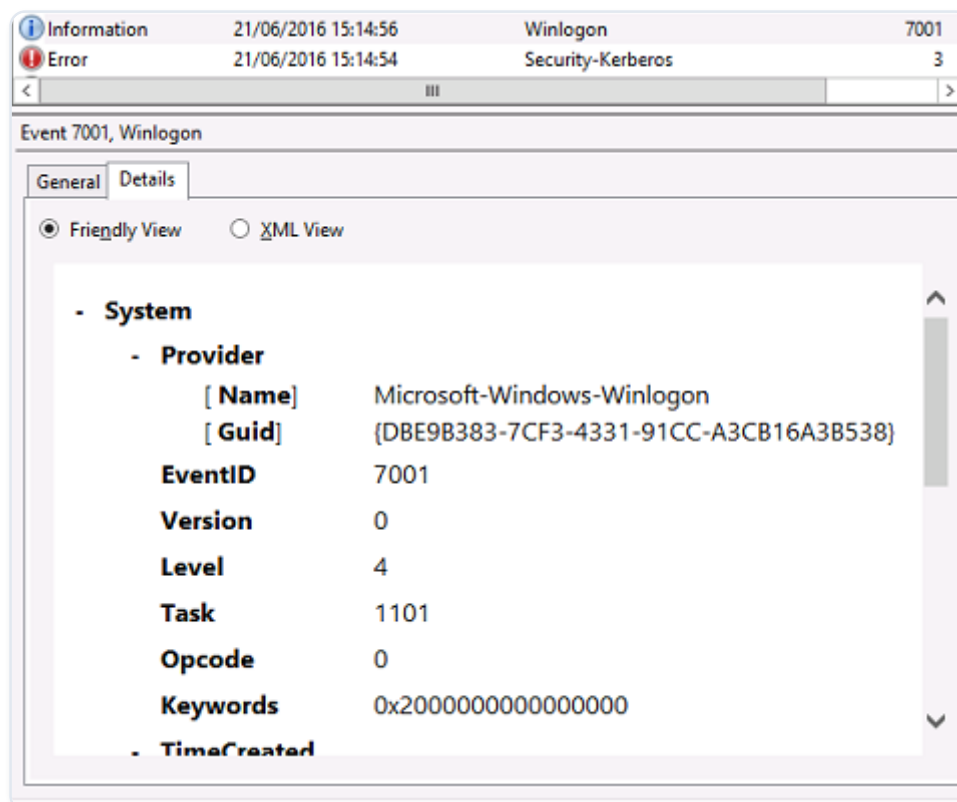
Este ejemplo de registro CAPI de VDA muestra una única secuencia de creación y verificación de cadena desde lsass.exe, validando el certificado del controlador de dominio (dc.citrixtest.net).

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 del inicio de sesión de Windows que indica que el inicio de sesión de Kerberos se realizó correctamente.



Supervisión de FAS mediante el registro de eventos de Windows

Todos los eventos de FAS se escriben en el **registro de eventos de aplicación** de Windows. Puede utilizar productos como System Center Operations Manager (SCOM) para supervisar el estado de su servicio FAS utilizando 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 se describen solo 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 o se quitó del modo de mantenimiento.	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 quitó del modo de mantenimiento.	Disponible a partir de FAS 10.7 / Citrix Virtual Apps and Desktops 2109.
[S023]	Administrador [{0}] configurando 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 en ninguna CA 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 indicada. 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 caducará pronto (quedan {0} días). Detalles del certificado: {1}	Este evento se genera periódicamente cuando el certificado de autorización de FAS está cerca de caducar. De forma predeterminada, el evento se genera todos los días si el certificado de autorización caduca en un plazo de 30 días.	La configuración predeterminada se puede ajustar mediante el cmdlet Set-FasRaCertificateMonitor ; consulte cmdlets de PowerShell .
[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.	Una vez caducado, FAS no puede generar nuevos certificados de usuario y el inicio de

EVENTO	TEXTO DEL EVENTO	EXPLICACIÓN	NOTAS
		De forma predeterminada, el evento se genera todos los días.	sesión único empieza a fallar.

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 un 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 "Service is not connected to the

EVENTO	TEXTO DEL EVENTO	EXPLICACIÓN	NOTAS
			cloud". Este es un comportamiento normal, y FAS intenta inmediatamente restablecer una conexión con Citrix Cloud.

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 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™, a los que se les ha 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 la regla [{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 que confía: la cuenta de llamada [{0}] no es una parte que confía 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 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}] utilizando las plantillas [{2}] and {3}]
[S005] El administrador [{0}] elimina la autorización FAS [RA cert id: {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
[S028] Administrador [{0}] estableciendo la configuración de clave para el certificado [{1}] en [{2}]
[S029] Administrador [{0}] restableciendo la configuración de clave para el certificado [{1}] a los valores predeterminados [{2}]
[S030] Administrador [{0}] estableciendo las propiedades del servicio en [{1}]
[S031] Administrador [{0}] desautorizando CA [RA cert id: {1}]
[S050] Administrador [{0}] creando configuración de la nube: [{1}]
[S051] Administrador [{0}] actualizando configuración de la nube: [{1}]
[S052] Administrador [{0}] eliminando configuración de la nube

CÓDIGOS DE REGISTRO

[S060] Administrador [{0}] Solicitando registro en la nube. Instancia: {1}

[S060] Administrador [{0}] Solicitando el registro de confianza directa en la nube. Instancia: {1}
CloudServiceUrlFormat: {2}

[S061] Administrador [{0}] Completando el registro en la nube. Ubicación del recurso: {1}, Nombre de la regla: {2}

[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}

[S065] Administrador [{0}] Solicitando el registro de confianza directa en la nube. Instancia: {1}
CloudServiceUrlFormat: {2}

CÓDIGOS DE REGISTRO

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

[S402] ERROR: El Servicio de autenticación federada de Citrix debe ejecutarse como Servicio de red [currently running as: {0}]

[S404] Borrando forzosamente la base de datos del Servicio de autenticación federada de Citrix

[S405] Se produjo un error al migrar 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 degradar la configuración -- [From version {0} to version {1}]

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

CÓDIGOS DE REGISTRO
[S410] Error en la configuración de ThreadPool: 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 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}
[S415] Comprobaciones del certificado de autorización completadas. 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}] (el UPN no está permitido por la regla [{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} role: {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} role: {1}][Solicitudes por minuto {2}].
[S123] No se pudo emitir un certificado en ninguna CA para [upn: {0} role: {1}] [exception: {2}]

CÓDIGOS DE REGISTRO
[S124] No se pudo emitir un certificado para [upn: {0} role: {1}] en [certificate authority: {2}] [exception: {3}]
[S125] La llamada agotó el tiempo de espera después de {0} segundos esperando que se completara la solicitud de certificado pendiente [upn: {1} role: {2} Contexto de seguridad: [{3}]]
[S126] El servidor [{0}] intentó afirmar una identidad utilizando una regla no definida [{1}]
[S127] FAS no pudo solicitar un certificado para [upn: {0} role: {1} definition: {2}] porque el servidor está en modo de mantenimiento; use el cmdlet de PowerShell Set-FasServer para cambiar el comportamiento mientras está en modo de mantenimiento

Actuando como parte de confianza

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 de confianza [{0}] no tiene acceso a una contraseña.
[S202] La parte de confianza [{0}] no tiene acceso a un certificado.
[S203] La parte de confianza [{0}] no tiene acceso al proveedor de inicio de sesión
[S204] Parte de confianza [{0}] accediendo al Proveedor de inicio de sesión para [upn: {1}] en el rol: [{2}] [Operation: {3}] según lo autorizado por [{4}]
[S205] Acceso denegado a la parte de confianza: la cuenta de llamada [{0}] no es una parte de confianza permitida de la regla [{1}]
[S206] La cuenta de llamada [{0}] no es una parte de confianza
[S208] La operación de clave privada falló [Operation: {0} upn: {1} role: {2} certificateDefinition {3} Error {4} {5}].
[S209] Certificado en caché no encontrado. [Caller: {0}] [upn: {1}] [role: {2}] [cert definition: {3}] [Operation: {4}]

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}] ejecutando 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
[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 la 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 el 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}])

CÓDIGOS DE REGISTRO
[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 de 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}]
[S004] FAS no se pudo registrar 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 dio 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}] Puede encontrar más detalles en la consola de administración.

CÓDIGOS DE REGISTRO

[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 autor de la llamada 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 se pudo iniciar. 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}]

[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}]

[S028] FAS envió su telemetría actual a la nube [fas id: {0}] [transaction id: {1}]

[S029] FAS no pudo enviar su telemetría actual a la nube [fas id: {0}] [transaction id: {1}]
[exception: {2}]

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. Índice de GPO del Servicio de autenticación federada no reconocido [index: {0}] [registry name: {1}]
[S102] Error en el inicio de sesión de aserción de identidad. Error en la búsqueda de SID para {0} [Exception: {1}{2}]
[S103] Error en el inicio de sesión de aserción de identidad. El usuario {0} tiene el SID {1}, pero el SID esperado es {2}
[S104] Error en el inicio de sesión de aserción de identidad. La llamada a {0} devolvió [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. ACCESS_DENIED [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. Soporte de tarjeta inteligente deshabilitado

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

CÓDIGOS DE REGISTRO
[S104] FAS recibió un certificado de autorización de la CA {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 del 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 Registros de Kerberos 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

MENSAJE DE ERROR MOSTRADO	DESCRIPCIÓN Y REFERENCIA
	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.
El sistema no pudo iniciar 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 Certificados e infraestructura de clave pública .
Solicitud incorrecta	Esto suele indicar que las extensiones del certificado no están configuradas correctamente, o que la clave RSA es demasiado corta (<2048 bits).

Rastreo siempre activo de FAS

Con el rastreo siempre activo, FAS registra su actividad en el sistema de archivos. Esto puede ayudar con la resolución de problemas, eliminando potencialmente la necesidad de reproducir un incidente que haya ocurrido.

El rastreo siempre activo se habilita al instalar o actualizar FAS mediante cualquiera de estos métodos:

- El instalador de Citrix Virtual Apps and Desktops™: desde el botón **Federated Authentication Service** en la pantalla de inicio automático al insertar la ISO
- `XenDesktopFasSetup.exe` : Ubicado en la ISO de Citrix Virtual Apps and Desktops en `x64\XenDesktop_Setup\XenDesktopFasSetup.exe`
- `FasSetup_xxxx.exe` : el archivo de instalación independiente de FAS, disponible en [Citrix Downloads](#).

NOTA:

El rastreo siempre activo no está disponible si instala o actualiza mediante el archivo **MSI del instalador de FAS**, `FederatedAuthenticationService_x64.msi`.

Recopilación de rastreo siempre activo

Utilice [Citrix Scout](#) para recopilar el rastreo siempre activo y otros datos de diagnóstico de su servidor FAS. **Citrix Scout** se instala al instalar FAS mediante cualquiera de los métodos anteriores.

Deshabilitar el rastreo siempre activo

Si por alguna razón desea deshabilitar el rastreo siempre activo, detenga y deshabilite el **Citrix Telemetry Service** en su servidor FAS.

Envío de rastreo siempre activo a un servidor de registro central

Para obtener más información y pasos de configuración, consulte el [artículo de AOT](#).

Información relacionada

- [Configuración de 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 de Federated Authentication Service (FAS) para implementaciones sencillas; sin embargo, la interfaz de PowerShell ofrece opciones más avanzadas. Si planea 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 <cmdlet name>` 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/>.

Opciones del instalador de FAS

Opciones de línea de comandos para instalar FAS

Las siguientes opciones son válidas con ambos:

1. Archivo `XenDesktopFasSetup.exe` ubicado en la ISO de Citrix Virtual Apps and Desktops en `x64\XenDesktop Setup\XenDesktopFasSetup.exe`
2. `FasSetup_xxxx.exe`, donde `xxxx` es la versión disponible en [Citrix Downloads](#)

- `/configure_firewall`

Abre todos los puertos del firewall de Windows utilizados por los componentes que se están instalando, si el servicio de Firewall de Windows está en ejecución, incluso si el firewall no está habilitado. Si utiliza un firewall de terceros o ningún firewall, debe abrir los puertos manualmente. FAS requiere el puerto TCP 80 de entrada.

- `/help` or `/h` or `/?` ?

Muestra la ayuda del comando.

- `/noreboot`

Evita un reinicio después de la instalación.

- `/quiet` o `/passive`

No aparece ninguna interfaz de usuario durante la instalación. La única evidencia del proceso de instalación y configuración se encuentra en el Administrador de tareas de Windows. Si se omite esta opción, se inicia la interfaz gráfica.

- `/remove`

Elimina FAS.

- `/installdir`

Especifica la carpeta de instalación.

Para obtener información sobre cómo Citrix informa del resultado de las instalaciones de componentes, consulte [Códigos de retorno de instalación de Citrix](#).

Instalar FAS en Windows Server Core

El ISO de Citrix Virtual Apps and Desktops o el archivo ejecutable del instalador independiente de FAS (`FasSetup_xxxx.exe`) son las formas preferidas de instalar FAS. Sin embargo, según las funciones del sistema operativo que estén habilitadas, es posible que no pueda utilizarlos para instalar en Windows Server Core.

En su lugar, utilice los siguientes archivos MSI del ISO de Citrix Virtual Apps and Desktops™:

ARCHIVO MSI	UBICACIÓN EN EL ISO	COMENTARIO
<code>FederatedAuthenticationService_x64.msi</code>	<code>x64\Federated Authentication Service</code>	Obligatorio
<code>TelemetryServiceInstaller_x64.msi</code>	<code>x64\Virtual Desktop Components</code>	Recomendado, proporciona compatibilidad con Always-on Tracing

Como requisito previo, debe instalarse `.net4.8`.

Para instalar o actualizar, use los siguientes comandos:

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

msiexec /i TelemetryServiceInstaller_x64.msi [/quiet]

net start "Citrix Telemetry Service"
```

Las opciones son:

- `/quiet` : No muestra ninguna interfaz de usuario
- `CONFIGUREFIREWALL`: Especifica **YES** para configurar el firewall y permitir las conexiones entrantes en el puerto 80. El valor predeterminado si se omite esta opción es **NO**

Para quitar FAS, use los siguientes comandos:

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

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

Administración de FAS en Windows Server Core

Puede configurar y administrar FAS localmente o desde otro equipo que tenga FAS instalado, utilizando cualquiera de las siguientes opciones:

- Los [cmdlets de PowerShell de FAS](#)
- La [GUI de la consola de administración de FAS](#)

Cuando utilice los cmdlets de PowerShell, establezca el parámetro `-Address` en el FQDN del servidor FAS de destino. Alternativamente, puede establecer la variable `$CitrixFasAddress` en el FQDN. Puede especificar **localhost** si desea administrar el FAS local.

Cuando utilice la consola de administración de FAS, haga clic en el enlace **Connect to another server** en la esquina superior derecha.

Arquitecturas de implementación

Introducción

El Servicio de autenticación federada (FAS) es un componente de Citrix® que se integra con su entidad de certificación de Active Directory, lo que permite a los usuarios autenticarse sin problemas en un entorno 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 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 pueda usar para iniciar sesión en una implementación de Citrix Virtual Apps o Citrix Virtual Desktops™.

Este documento describe ejemplos de arquitecturas de implementación de alto nivel, 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.

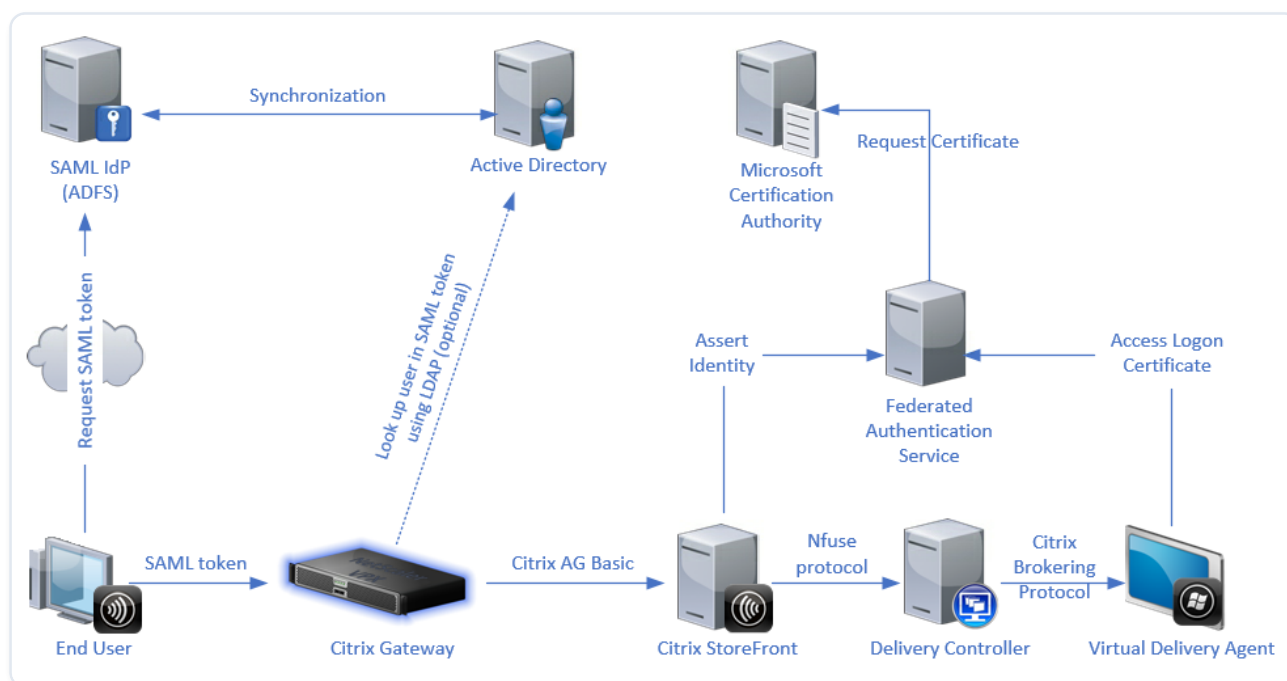
Descripción general de la arquitectura

FAS está autorizado a emitir automáticamente certificados de clase de tarjeta inteligente 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 de tarjeta inteligente estándar.

Los servidores StoreFront™ de confianza se ponen en contacto con FAS cuando los usuarios solicitan acceso al entorno 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 cada operación de firma y descifrado que necesite realizar con el certificado a FAS.

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



Implementación interna

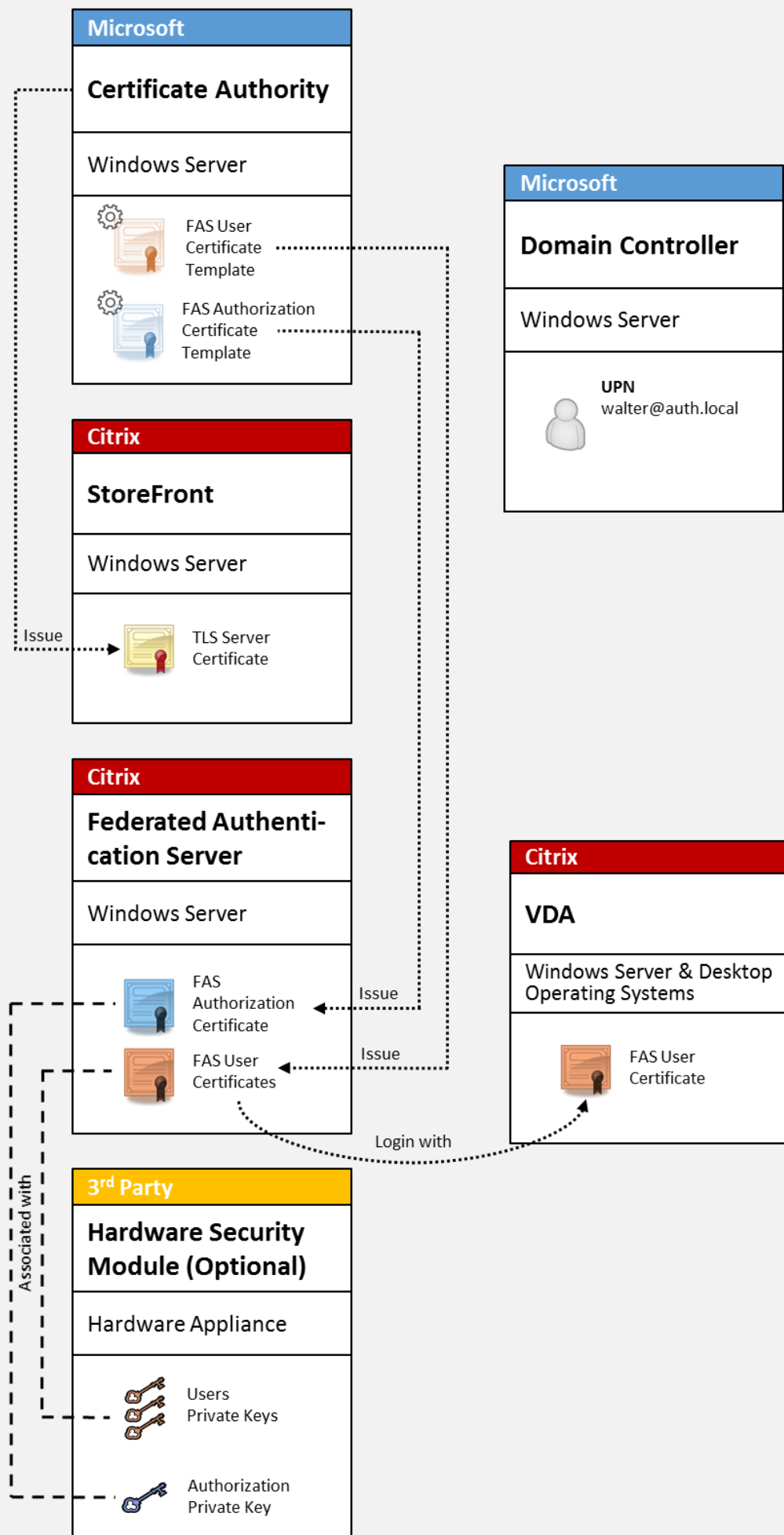
FAS permite a los usuarios autenticarse de forma segura en StoreFront utilizando una variedad de opciones de autenticación (incluido el inicio de sesión único de Kerberos) y conectarse a una sesión de Citrix HDX™ completamente autenticada.

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 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 está documentado 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.)

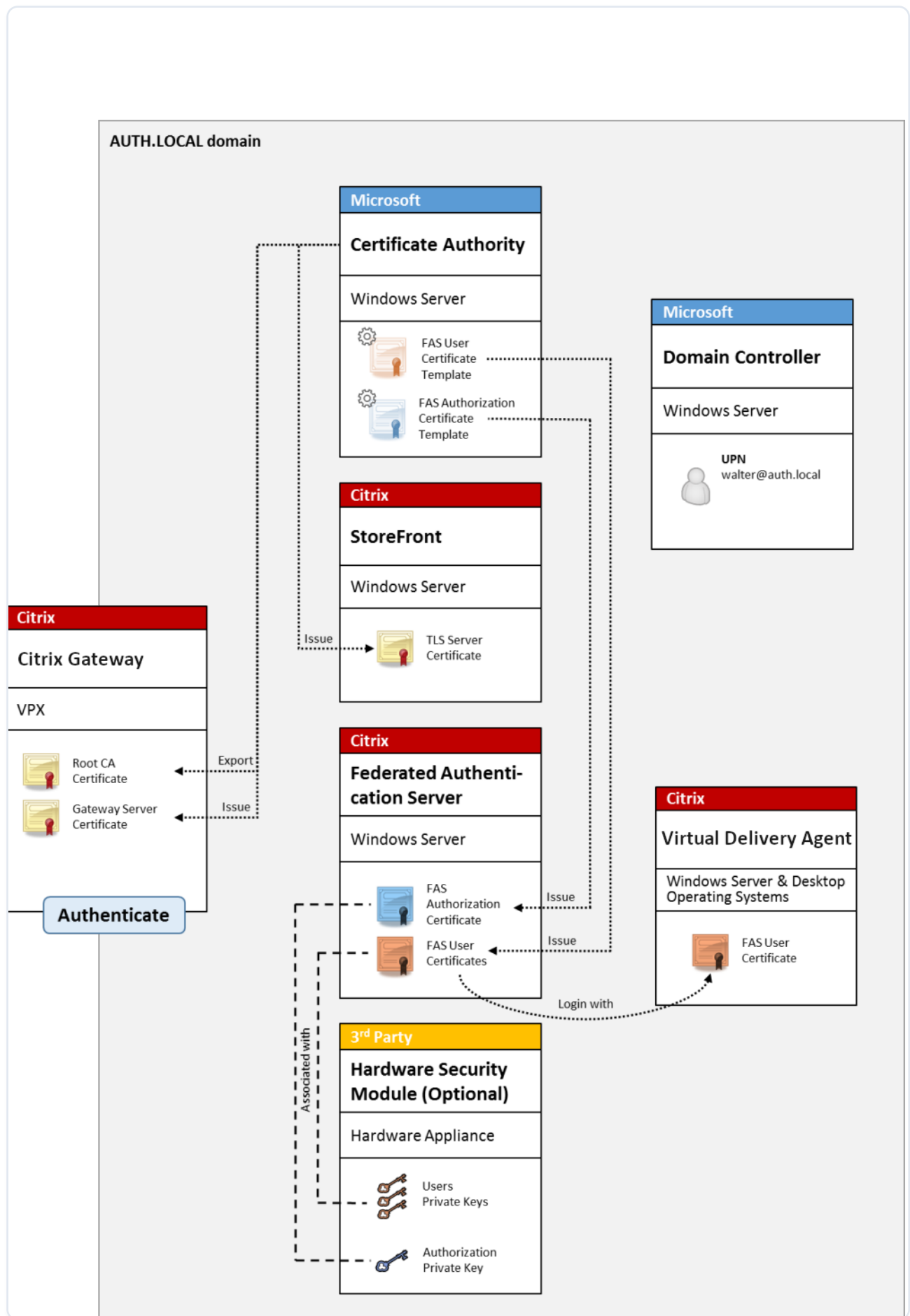
Información relacionada:

- 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 detalles, 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, trasladando el punto principal de autenticación al propio Citrix Gateway. Citrix Gateway incluye opciones sofisticadas 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 que se documenta en [CTX206156](#).

En una implementación existente, esto normalmente solo implica asegurarse de que haya una autoridad de certificación de Microsoft unida al 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 apuntar 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.

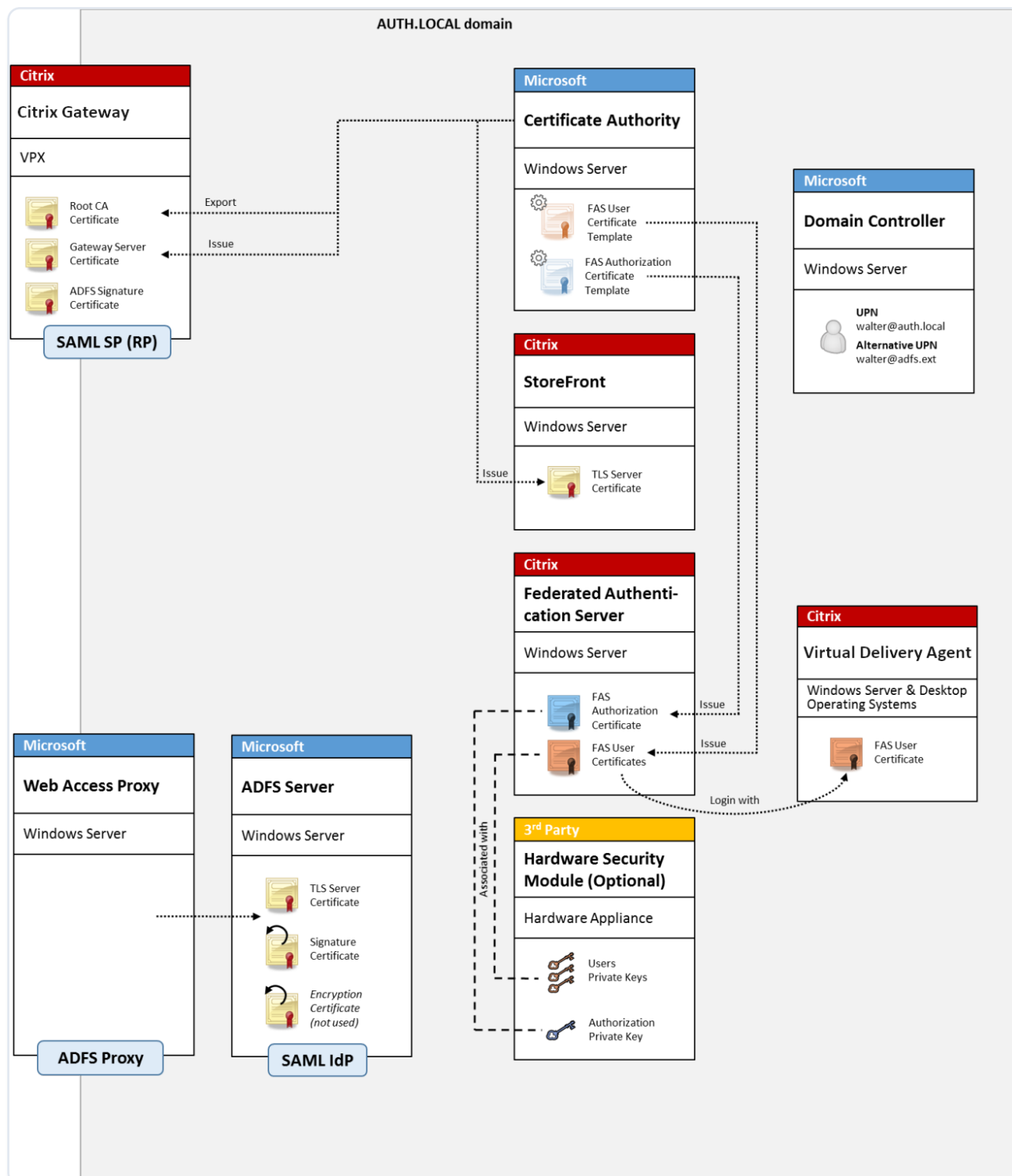
Back Create Cancel

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).



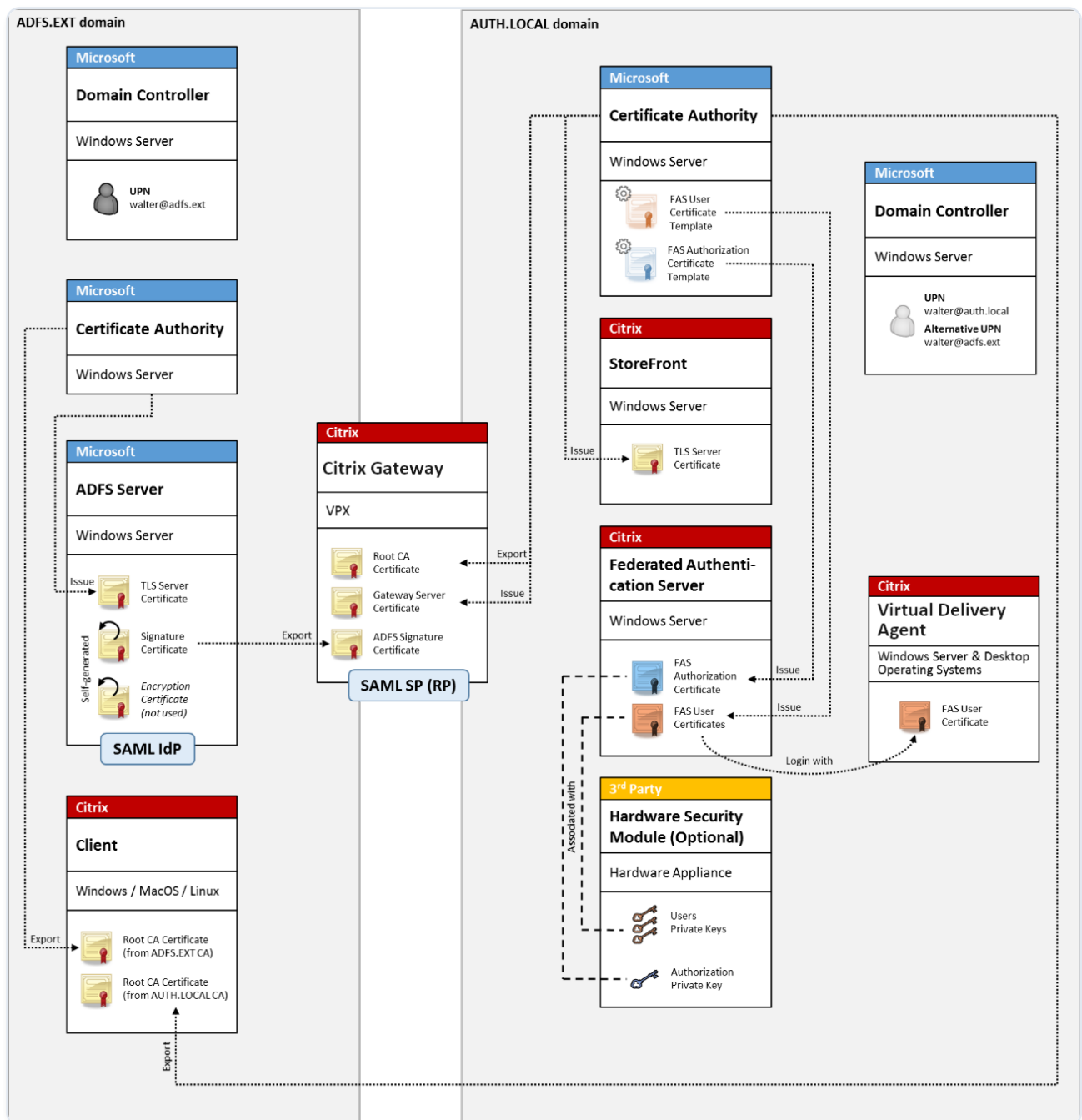
ADFS se utiliza comúnmente para autenticar de forma segura a los usuarios en los recursos corporativos de forma remota a través de Internet; por ejemplo, a menudo se utiliza para la integración con Office 365.

Información relacionada:

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



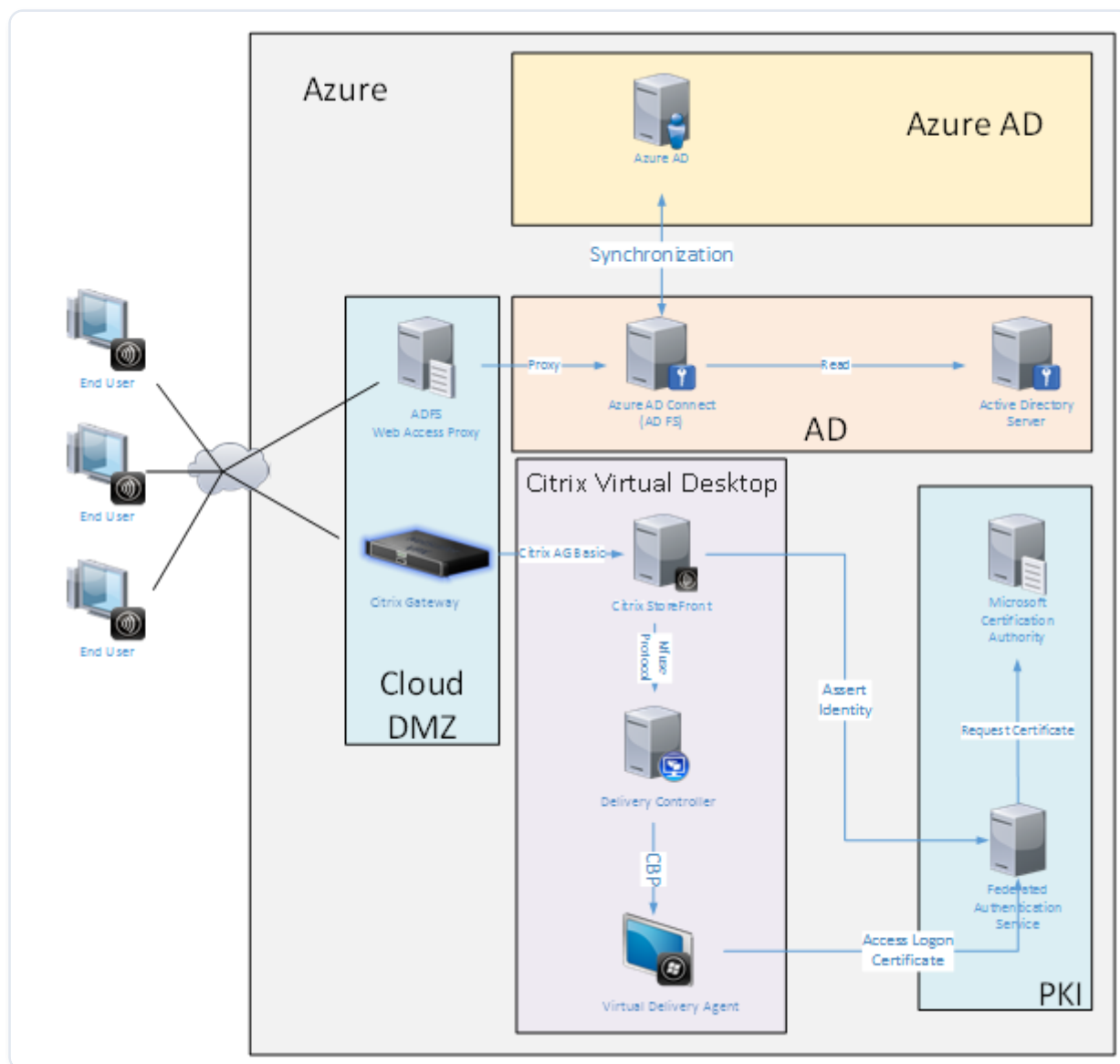
Información relacionada:

- 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 ellos 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 autentican completamente a través de Internet utilizando las características 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.

Implementación de ADFS

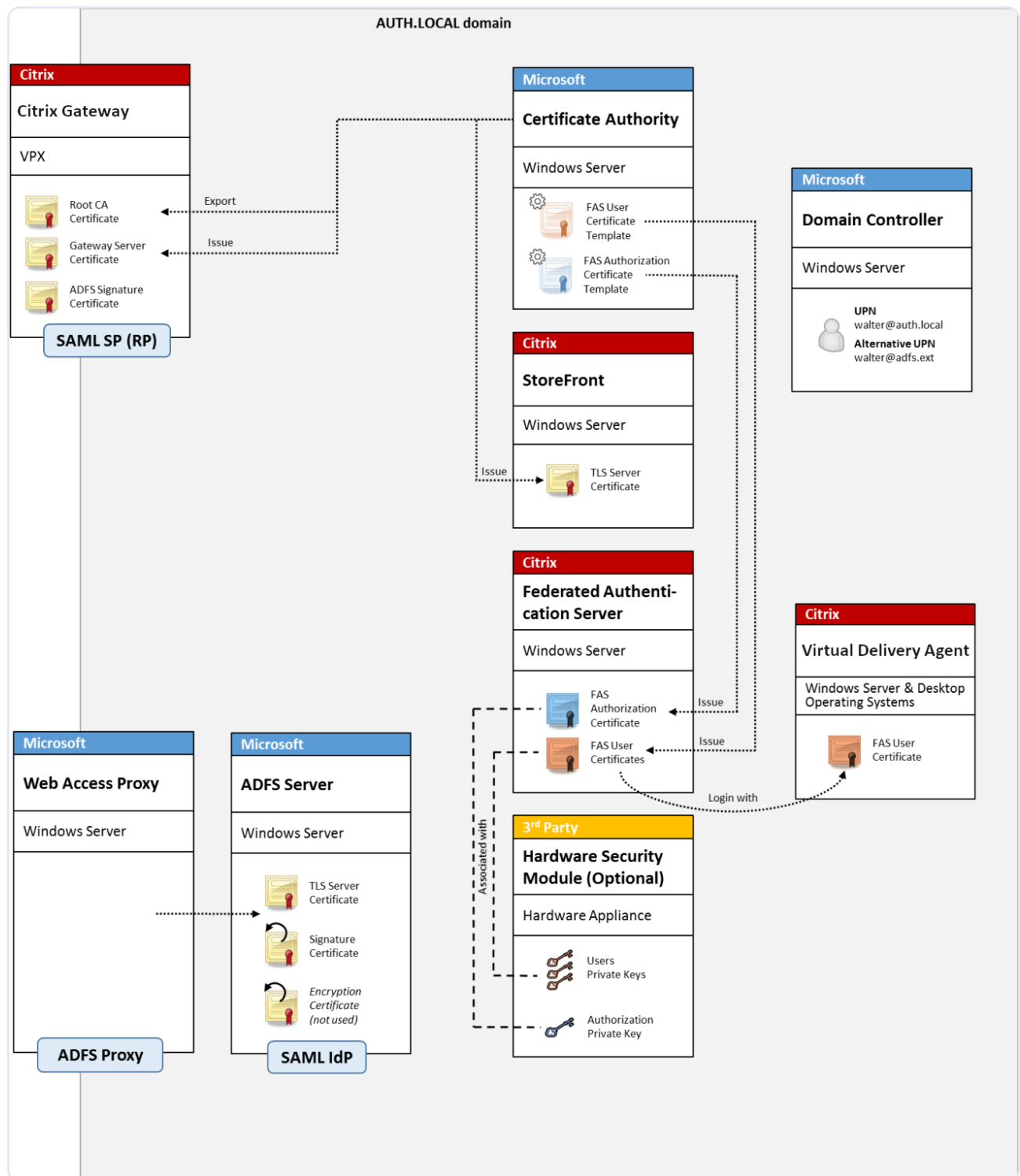
Introducción

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

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

Federated Authentication Service (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 en 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 a qué servicio intenta iniciar sesión el usuario y permite aplicar 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 de 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 correcta, ADFS indica al navegador web del usuario que envíe un XML de autenticación SAML a una de las URL de respuesta configuradas para el EntityId. Normalmente, esta es una dirección `https://` en el servidor original de Citrix Gateway 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.

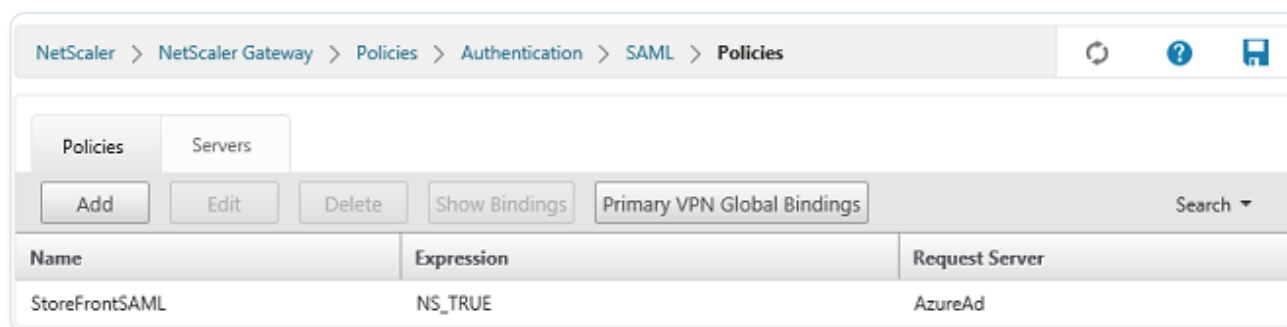
URL de cierre de sesión único

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

Esta es una característica opcional que no necesita configurarse. Normalmente es 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 gestionar 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 el inicio de 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

Attri

Attribute 3

Attri

Attribute 5

Attri

Attribute 7

Attri

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](#).