Configuración y solución de problemas de SSO para agentes y administradores de particiones en ECE

Contenido

Introducción

Este documento describe los pasos necesarios para configurar el inicio de sesión único (SSO) para agentes y administradores de particiones en una solución ECE.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

Cisco Packaged Contact Center Enterprise (PCCE)

Cisco Unified Contact Center Enterprise (UCCE)

Chat empresarial y correo electrónico (ECE)

Microsoft Active Directory

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

Versión de UCCE: 12.6(1)

Versión ECE: 12.6(1)

Microsoft Active Directory Federation Service (ADFS) en Windows Server 2016

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Se puede acceder a las consolas de chat y correo electrónico empresariales (ECE) fuera de Finesse; sin embargo, se debe habilitar SSO para que los agentes y supervisores puedan iniciar sesión en ECE a través de Finesse.

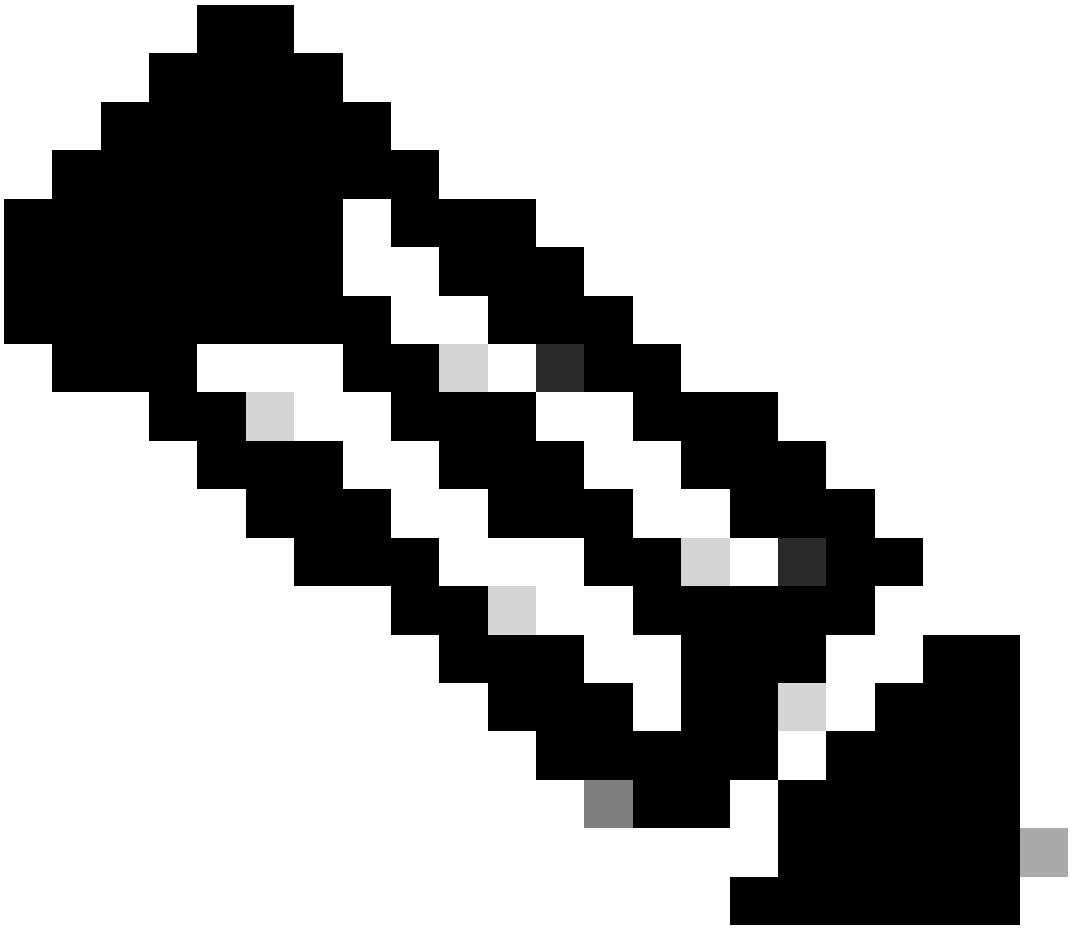
El inicio de sesión único también se puede configurar para los nuevos administradores de particiones. Esto garantiza que los nuevos usuarios que inician sesión en Cisco Administrator Desktop tengan acceso a Enterprise Chat and Email Administration Console.

Aspectos importantes que debe tener en cuenta sobre el inicio de sesión único:

- El proceso de configuración de un sistema para el inicio de sesión único debe realizarlo un usuario de la partición con las acciones necesarias en el nodo Seguridad de la aplicación y Administrar seguridad de la aplicación.
- Para que los supervisores y administradores inicien sesión en las consolas que no sean la consola de agente, una vez que se haya habilitado SSO, debe proporcionar una URL externa válida de la aplicación en la configuración de la partición. Consulte Configuración general de la partición para obtener más información.
- Se necesita un certificado de almacén de claves Java (JKS) para configurar SSO de modo

que los usuarios con funciones de administrador o supervisor puedan iniciar sesión en la partición 1 de ECE fuera de Finesse con sus credenciales de inicio de sesión de SSO. Póngase en contacto con el departamento de TI para recibir el certificado JKS.

- Se debe importar un certificado de Secure Sockets Layer (SSL) de Cisco IDS a todos los servidores de aplicaciones de una instalación. Para obtener el archivo de certificado SSL necesario, póngase en contacto con el departamento de TI o con el servicio de asistencia de Cisco IDS.
- La intercalación del servidor de base de datos para Unified CCE distingue entre mayúsculas y minúsculas. El nombre de usuario de la notificación devuelto por la dirección URL del extremo de información de usuario y el nombre de usuario de Unified CCE deben ser iguales. Si no son iguales, los agentes de inicio de sesión único no se reconocen como conectados y ECE no puede enviar la disponibilidad del agente a Unified CCE.
- La configuración de SSO para Cisco IDS afecta a los usuarios que se han configurado en Unified CCE para el inicio de sesión único. Asegúrese de que los usuarios que desea activar para SSO en ECE están configurados para SSO en Unified CCE. Póngase en contacto con el administrador de Unified CCE para obtener más información.



Nota:

- Asegúrese de que los usuarios que desea activar para SSO en ECE están configurados para SSO en Unified CCE.
- Este documento especifica los pasos para configurar la confianza de piezas de confianza para ECE en una implementación de AD FS única donde el servidor de federación de recursos y el servidor de federación de cuentas están instalados en el mismo equipo.
- Para una implementación de AD FS dividida, diríjase a la guía de instalación y configuración de ECE para la versión correspondiente.

Configuration Steps

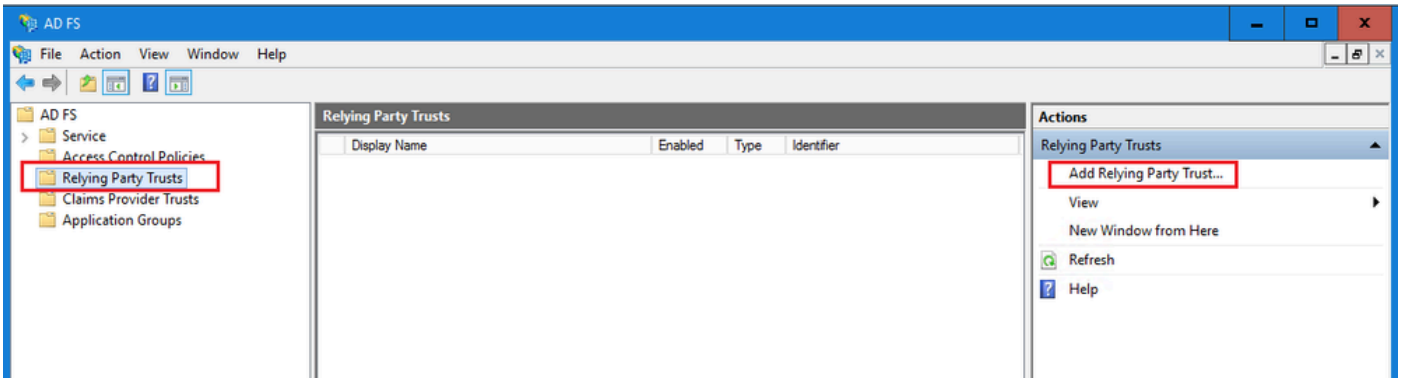
Configuración de Confianza de la Parte Confiadora para ECE

Paso 1

Abra la consola de administración de AD FS y vaya a AD FS > Relaciones de confianza > Confianza de la persona de confianza.

Paso 2

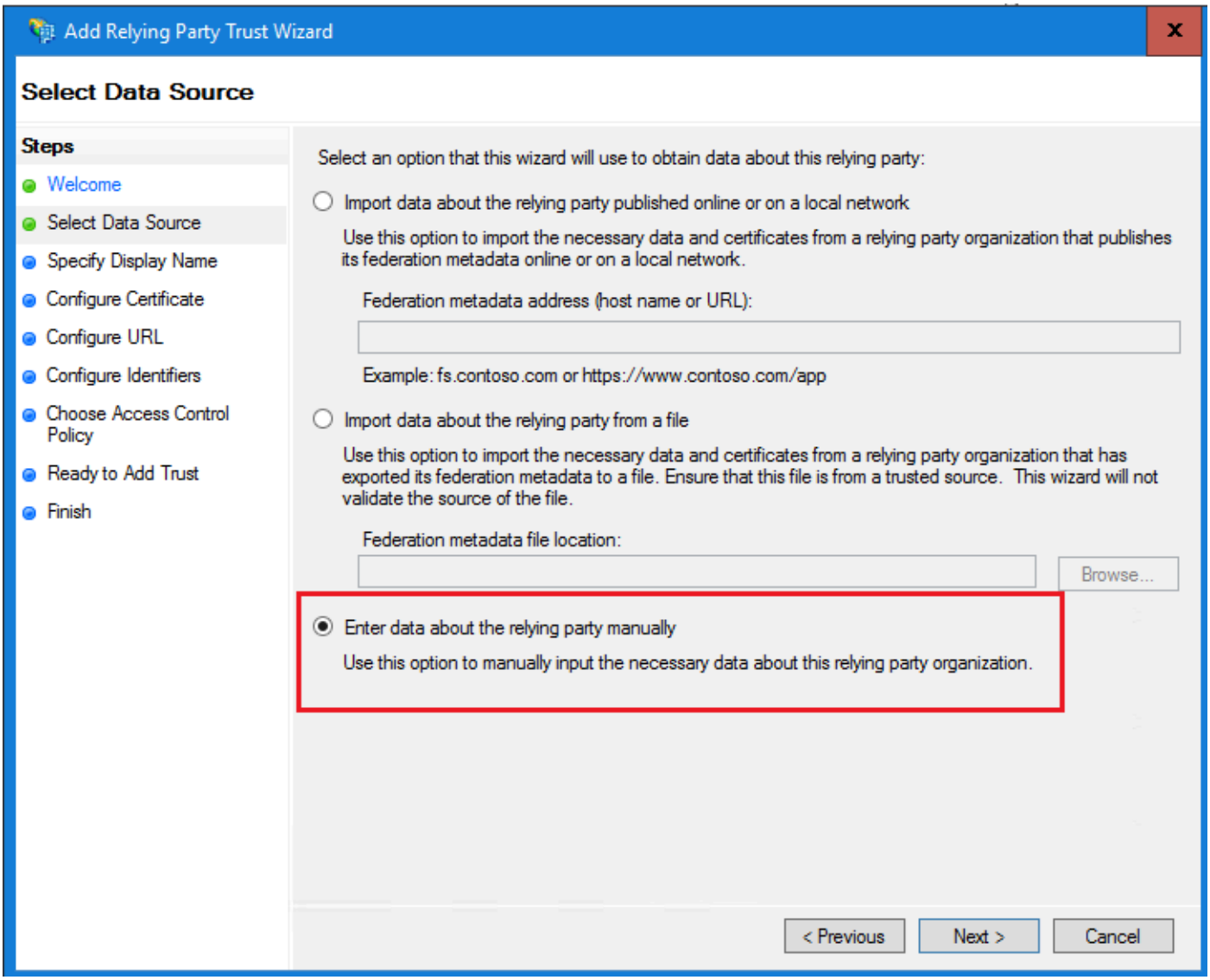
En la sección Acciones, haga clic en Agregar confianza de usuario de confianza...



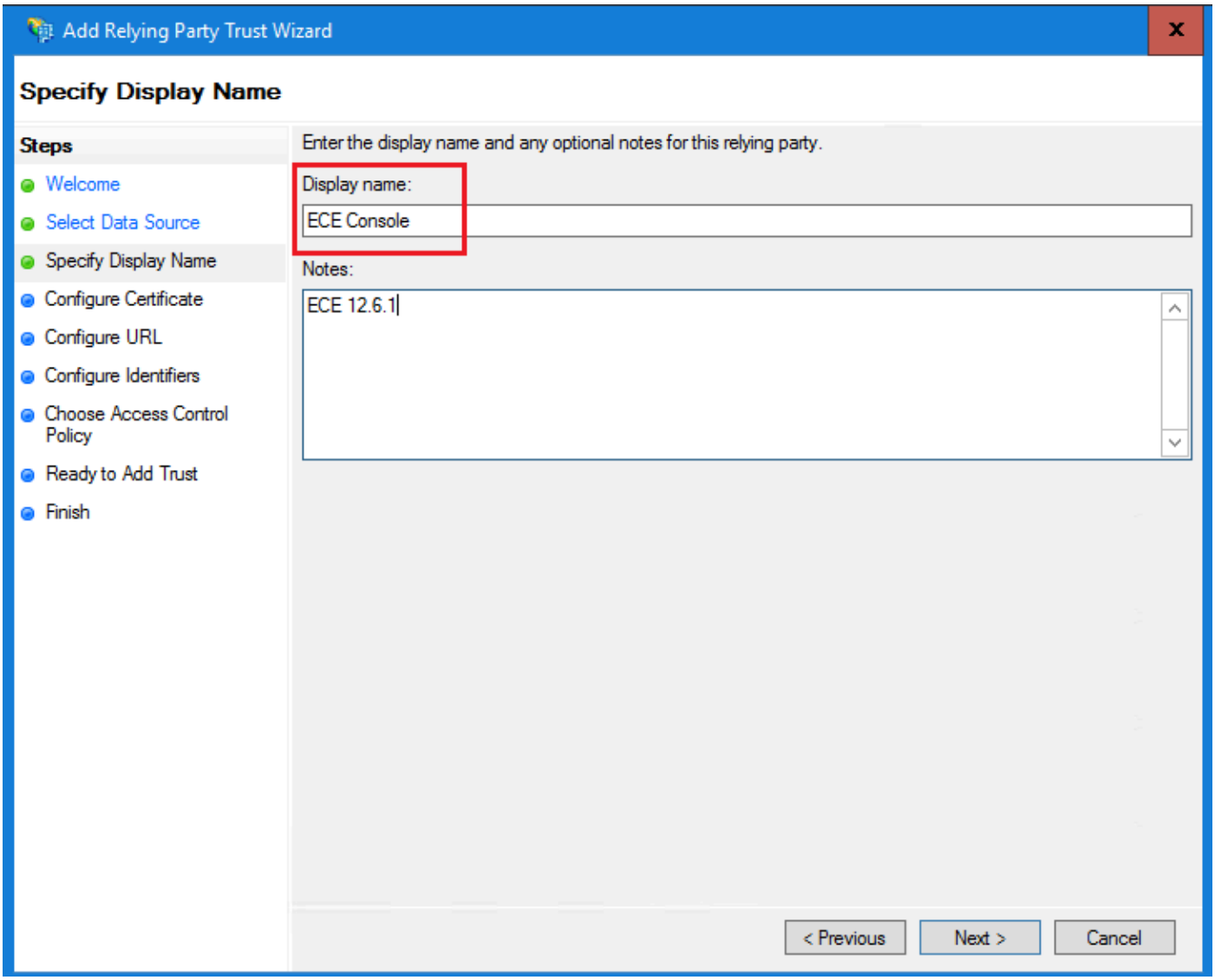
Paso 3

En el asistente para agregar confianza de usuario de confianza, haga clic en Inicio y realice los pasos siguientes:

a. En la página Seleccionar origen de datos, seleccione la opción Introducir datos sobre la parte de respuesta manualmente y haga clic en Siguiente.



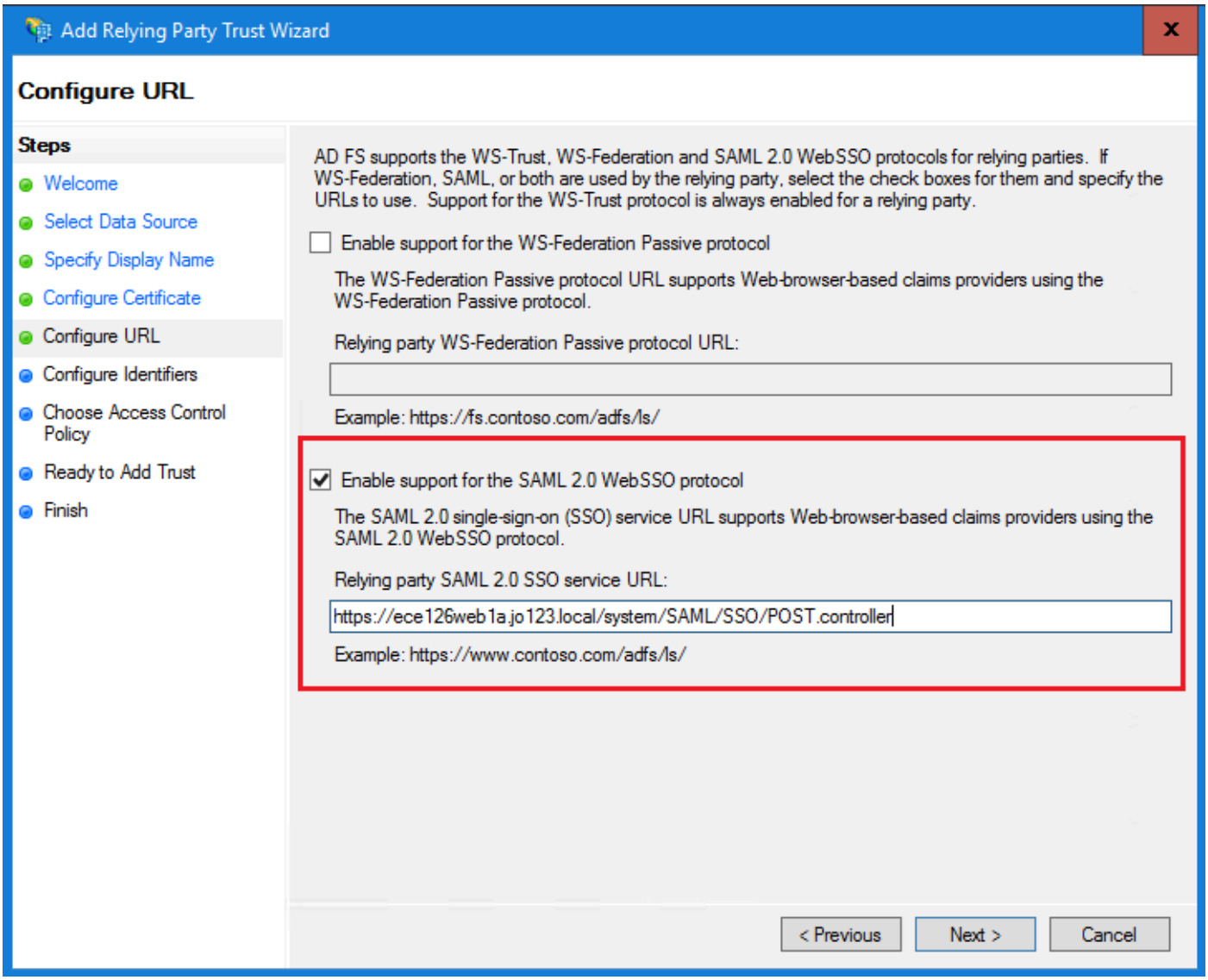
b. En la página Especificar Nombre para Mostrar, proporcione un nombre para mostrar para el usuario de confianza. Haga clic en Next (Siguiente)



c. En la página Configurar URL:

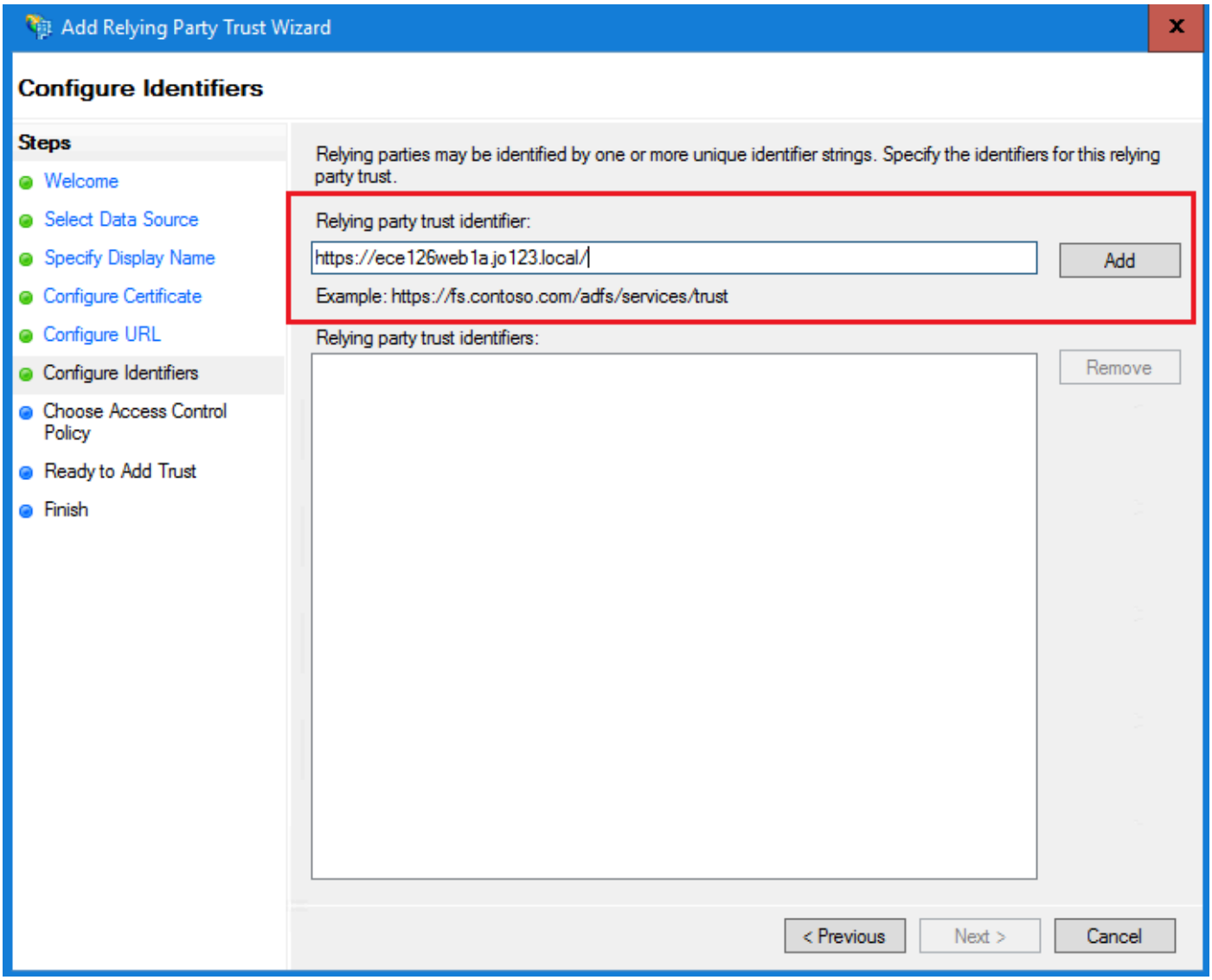
i. Seleccione la opción Habilitar soporte para el protocolo SSO Web SAML 2.0.

ii. En el campo URL del servidor SSO SAML 2.0 del usuario de confianza, proporcione la URL con el formato: https://<FQDN de servidor web o equilibrador de carga>/system/SAML/SSO/POST.controller

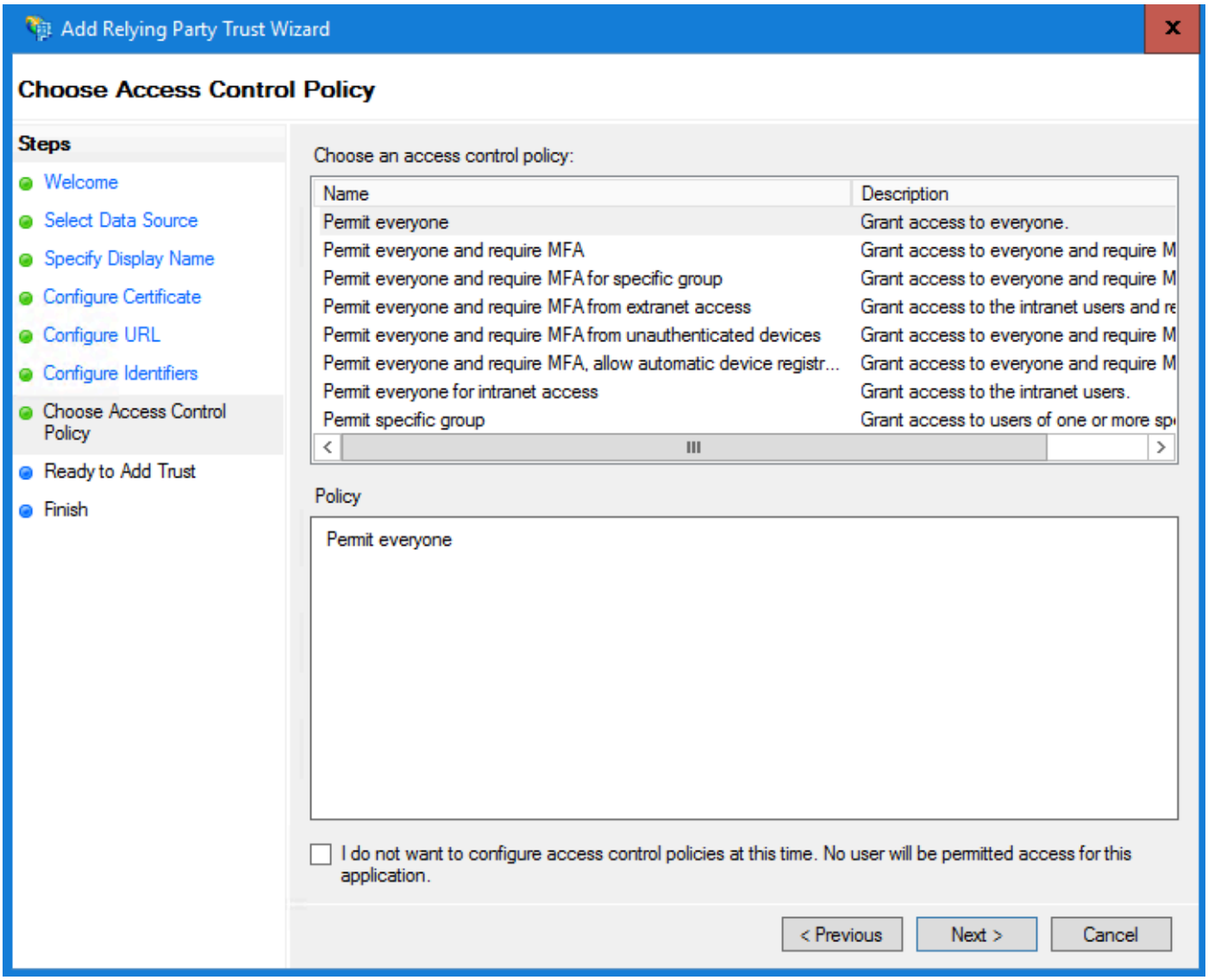


d. En la página Configurar identificadores, proporcione el identificador de confianza de usuario de confianza y haga clic en Agregar.

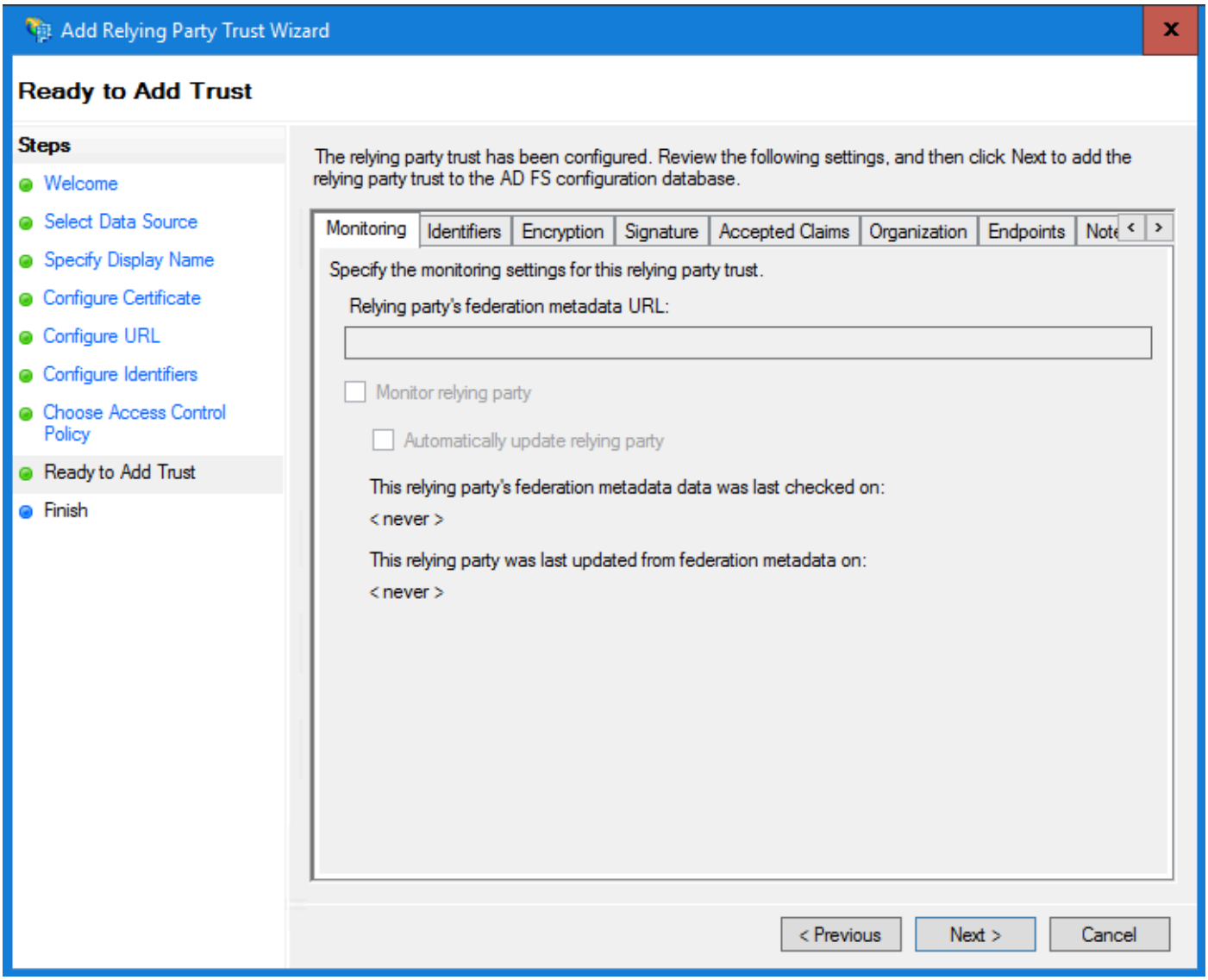
- El valor debe tener el formato: https://<FQDN de servidor web o equilibrador de carga>/



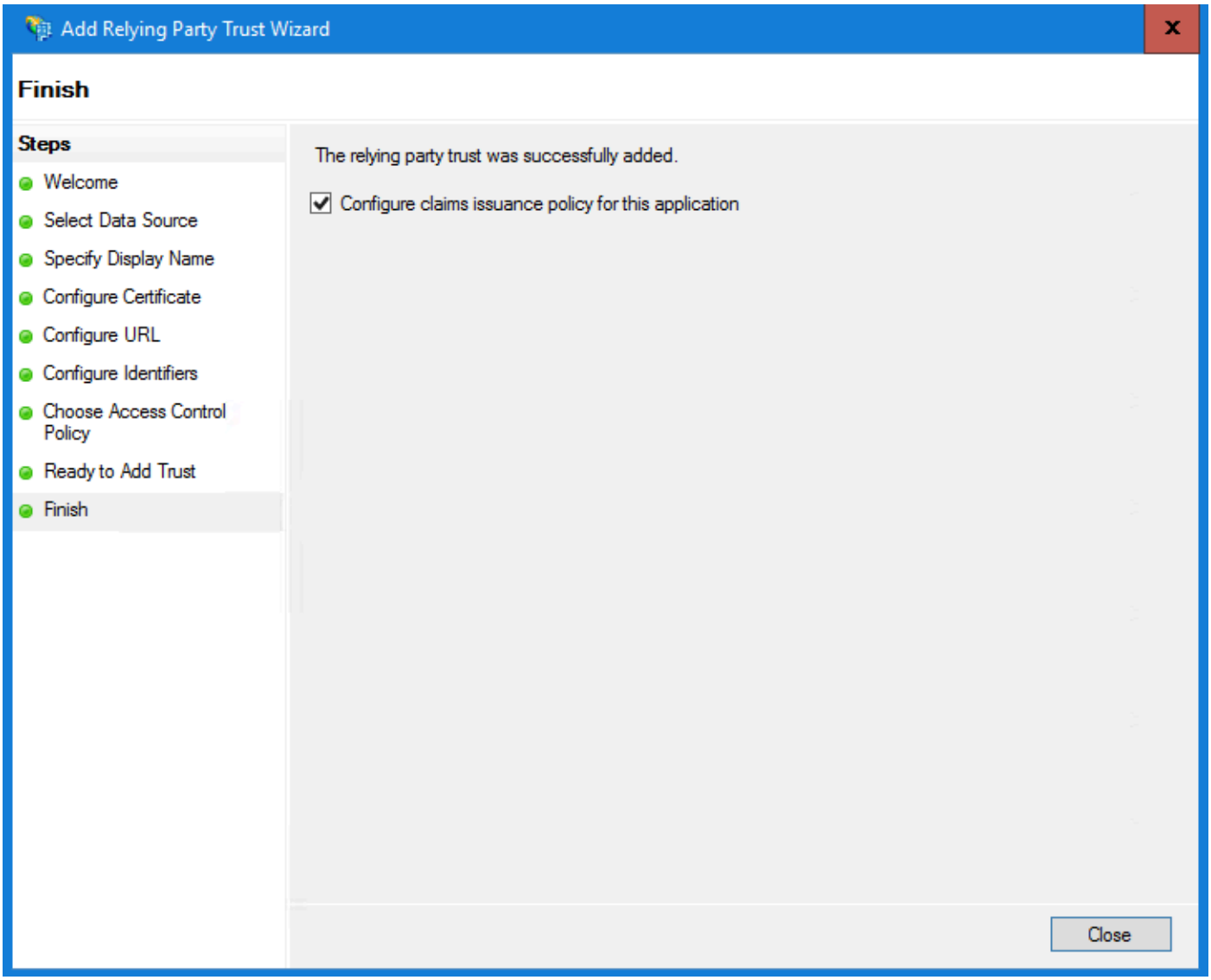
e. En la página Choose Access Control Policy, haga clic en next con el valor predeterminado de la política 'Permit everyone'.



f. En la página Preparado para agregar confianza, haga clic en Siguiente.

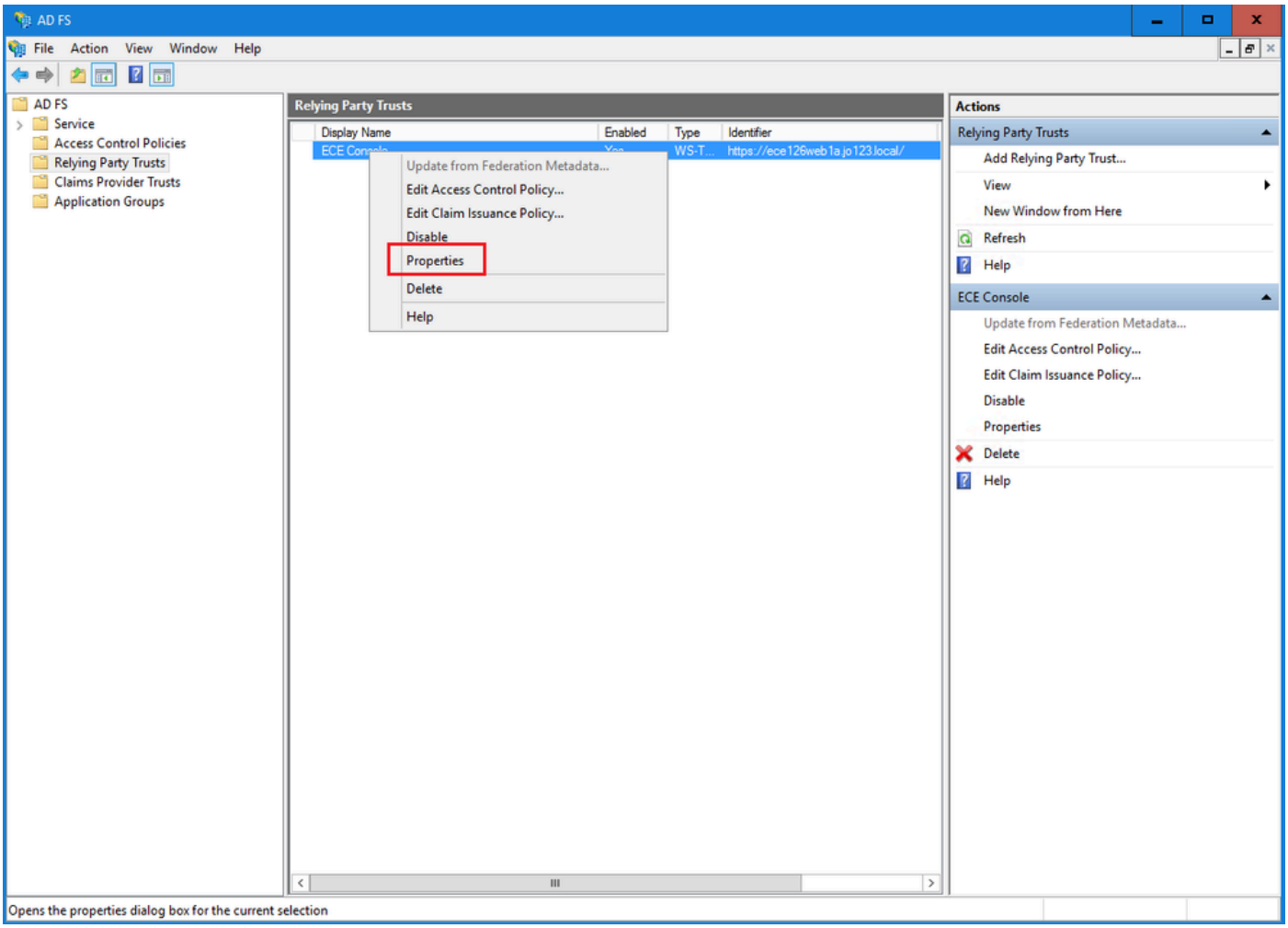


g. Una vez agregada correctamente la confianza de usuario de confianza, haga clic en Cerrar.



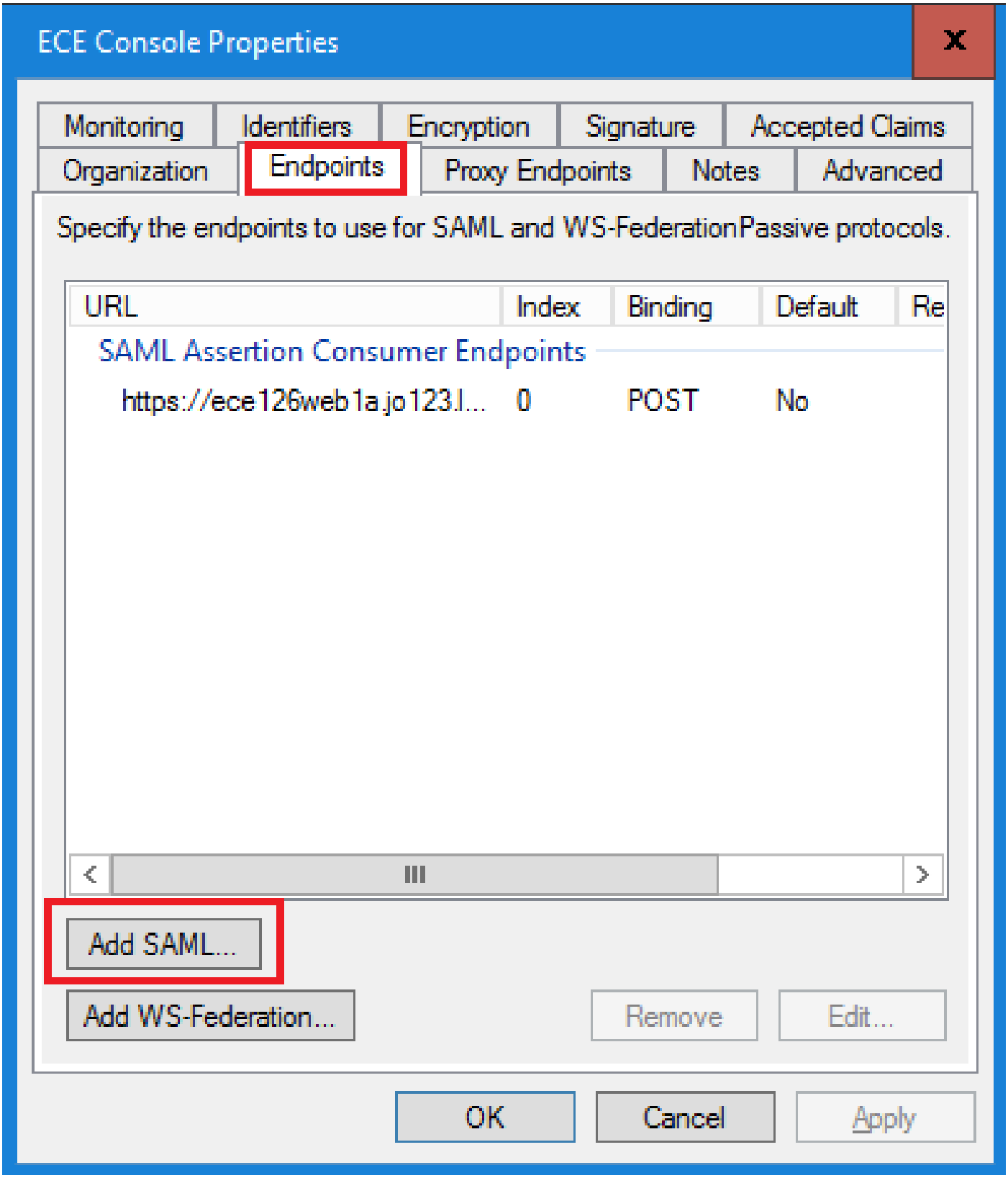
Paso 4

En la lista Confianzas de proveedores de confianza, seleccione la confianza de usuario de confianza creada para ECE y, en la sección de acciones, haga clic en Propiedades.



Paso 5

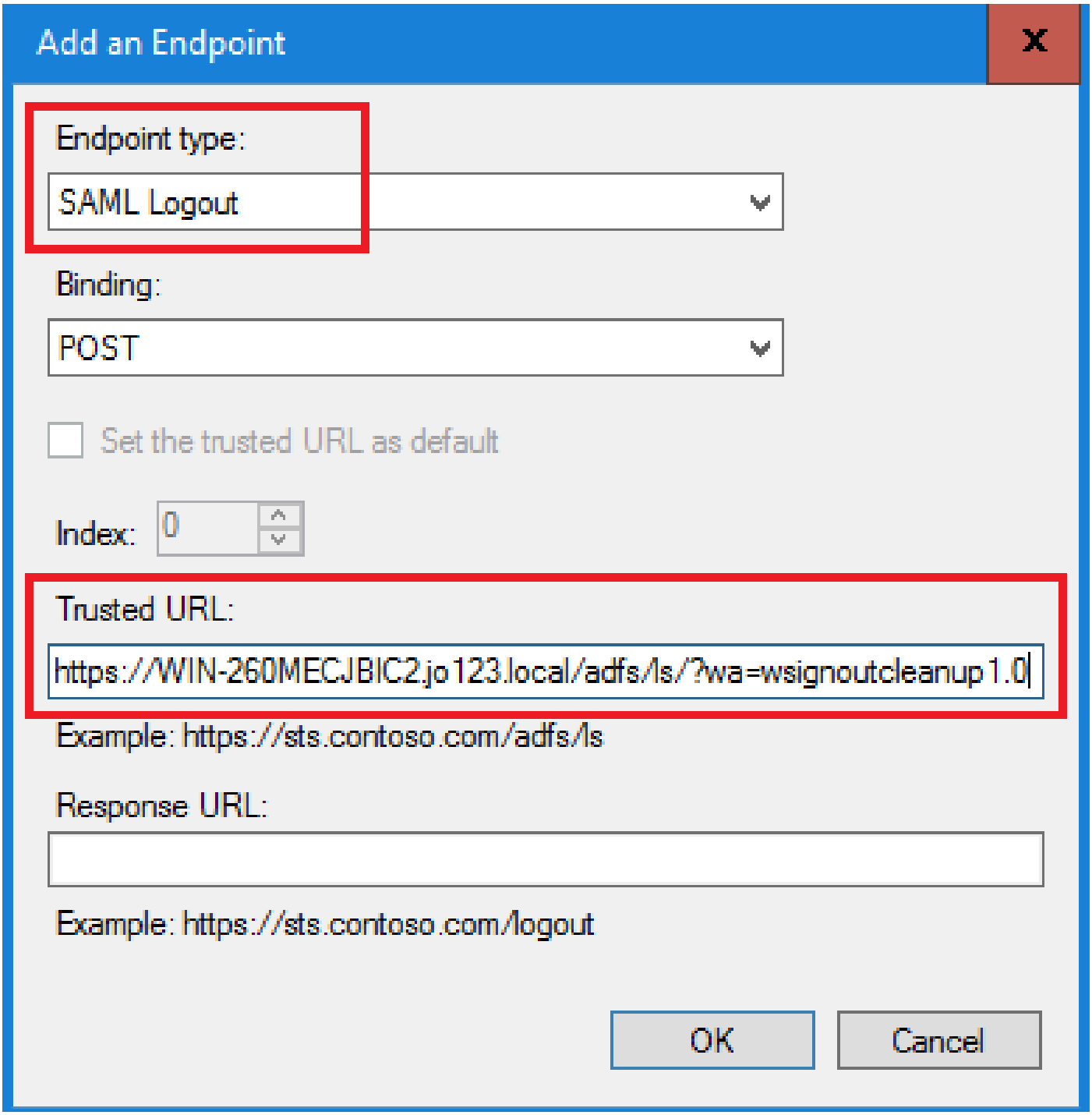
En la ventana Propiedades, desplácese a la pestaña Terminales y haga clic en el botón Agregar SAML..



Paso 6

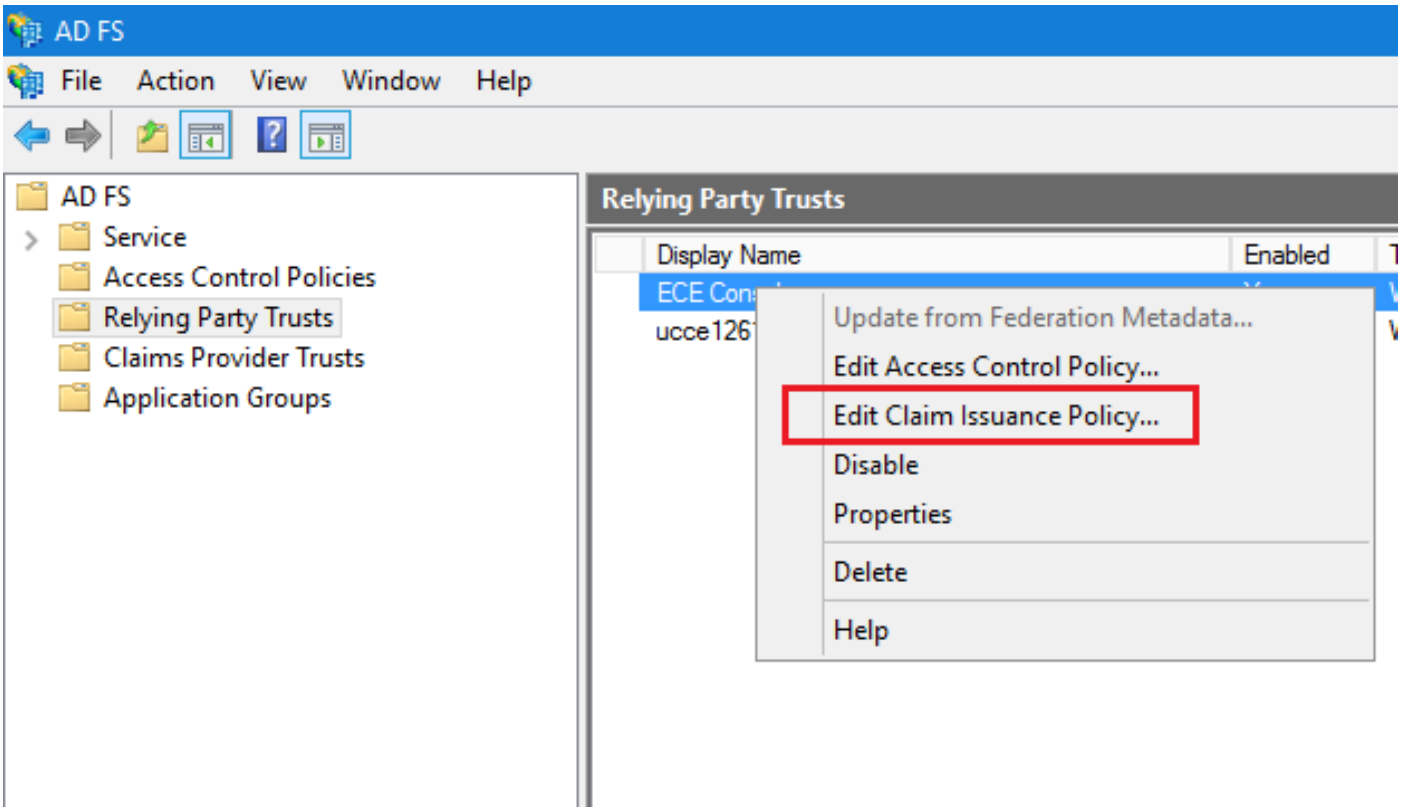
En la ventana Add an Endpoint, configure como se indica:

1. Seleccione el tipo de terminal como cierre de sesión de SAML.
2. Especifique la URL de confianza como https://<ADFS-server-FQDN>/adfs/ls/?wa=wsignoutcleanup1.0
3. Click OK.



Paso 7

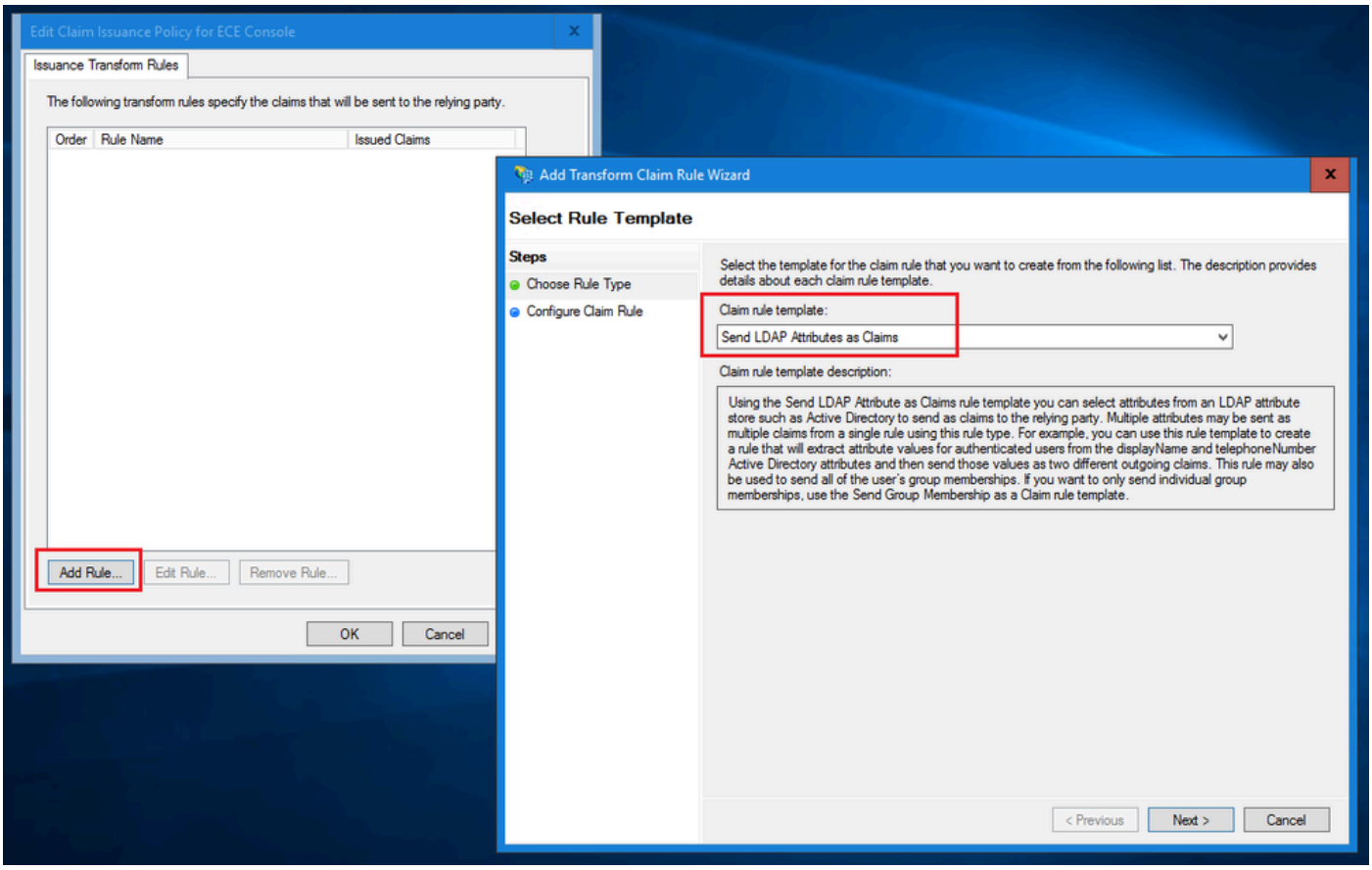
En la lista Confianza de proveedores, seleccione la confianza creada para ECE y, en la sección de acciones, haga clic en Editar póliza de seguro de reclamación.



Paso 8

En la ventana Editar póliza de seguro de reclamación, en la pestaña Reglas de transformación de emisión, haga clic en el botón Agregar regla... y configure como se muestra:

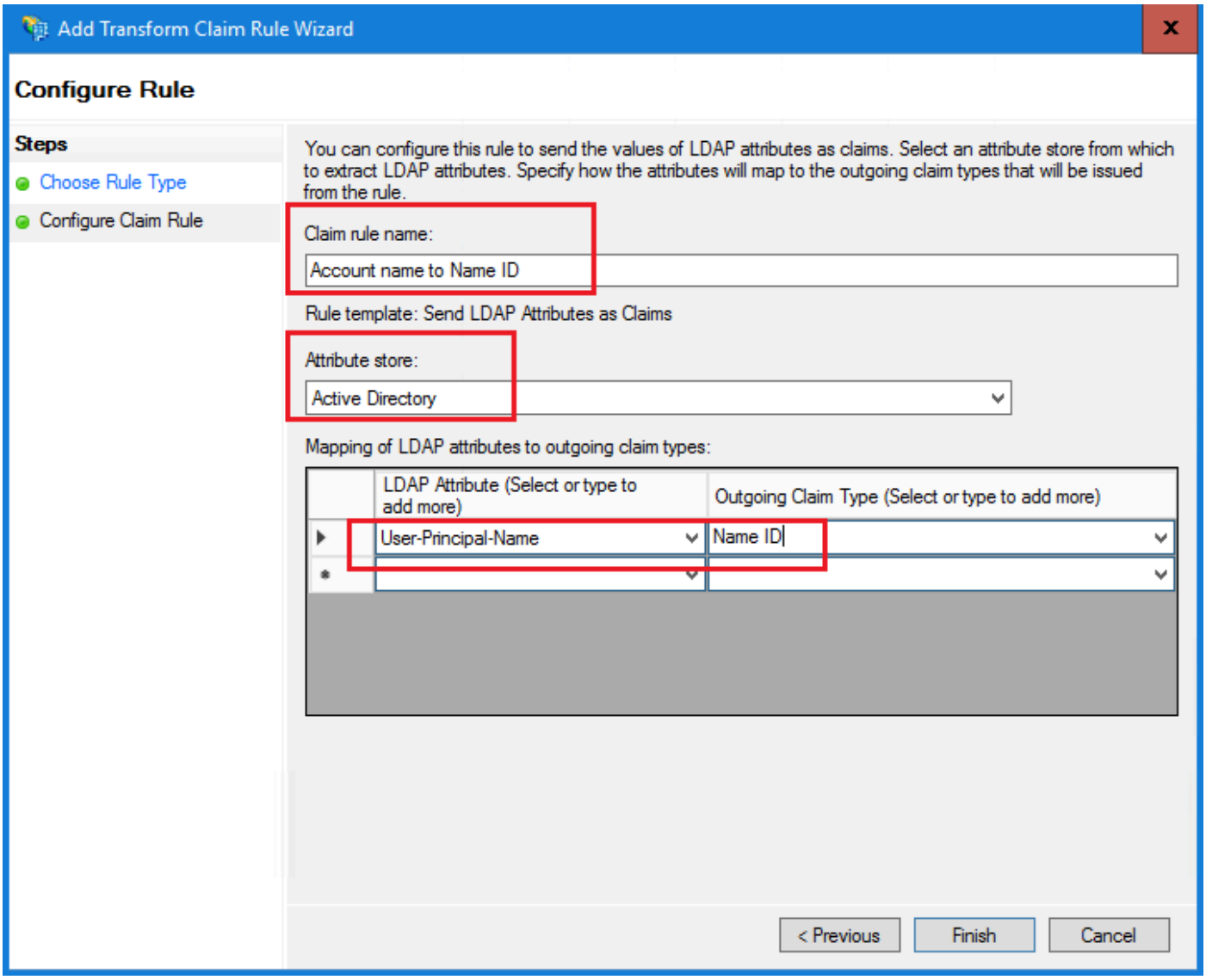
a. En la página Choose Rule Type (Elegir tipo de regla), seleccione Send LDAP Attributes as Claims (Enviar atributos LDAP como notificaciones) en el menú desplegable y haga clic en Next (Siguiente).

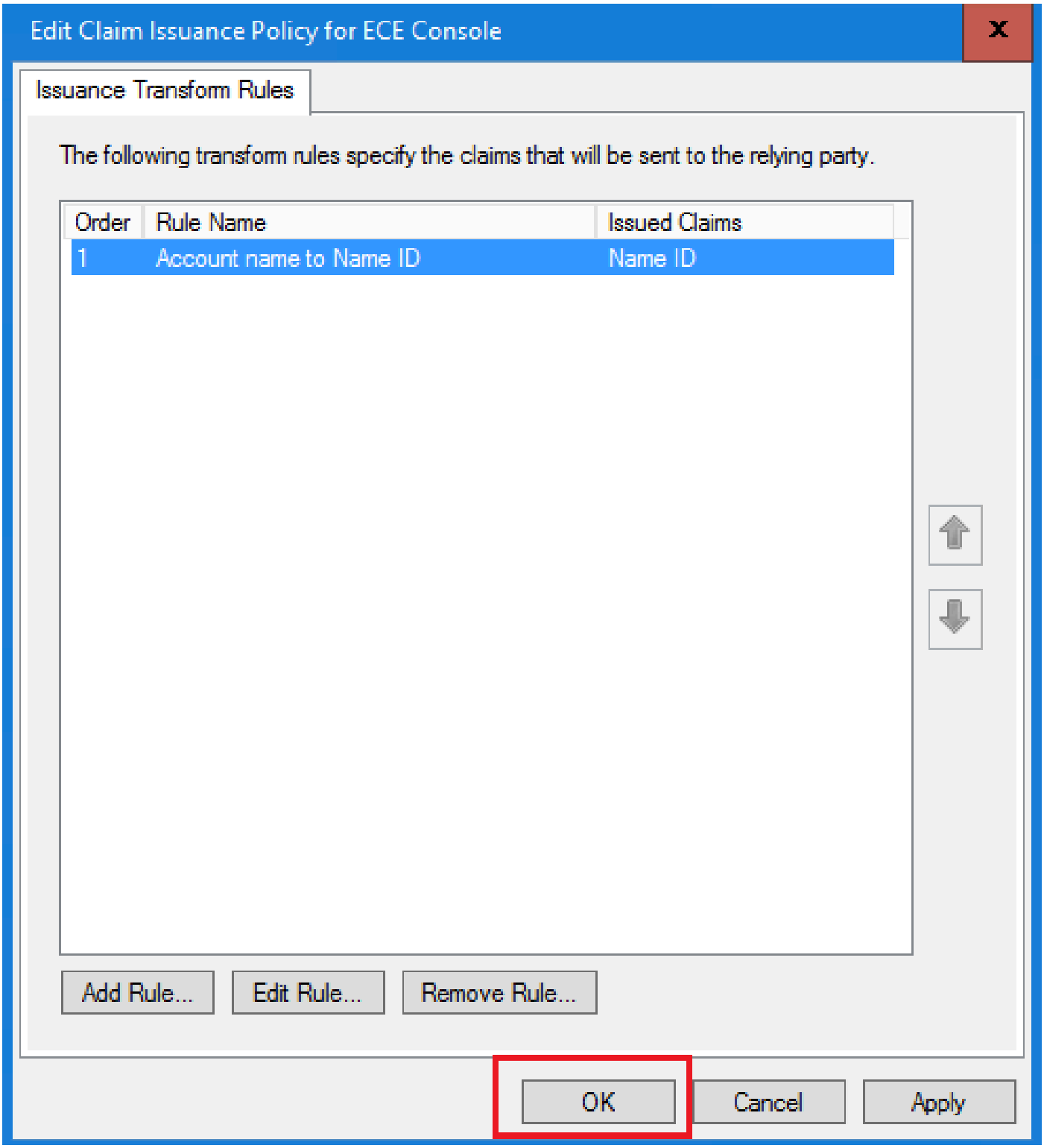


b. En la página Configurar regla de reclamación:

1. Proporcione el nombre de la regla de reclamación y seleccione el almacén de atributos.
2. Defina la asignación del atributo LDAP y el tipo de notificación saliente.

- Seleccione Name ID como el nombre del tipo de notificación saliente.
- Haga clic en Finalizar para volver a la ventana Editar póliza de seguro de reclamación y, a continuación, haga clic en Aceptar.

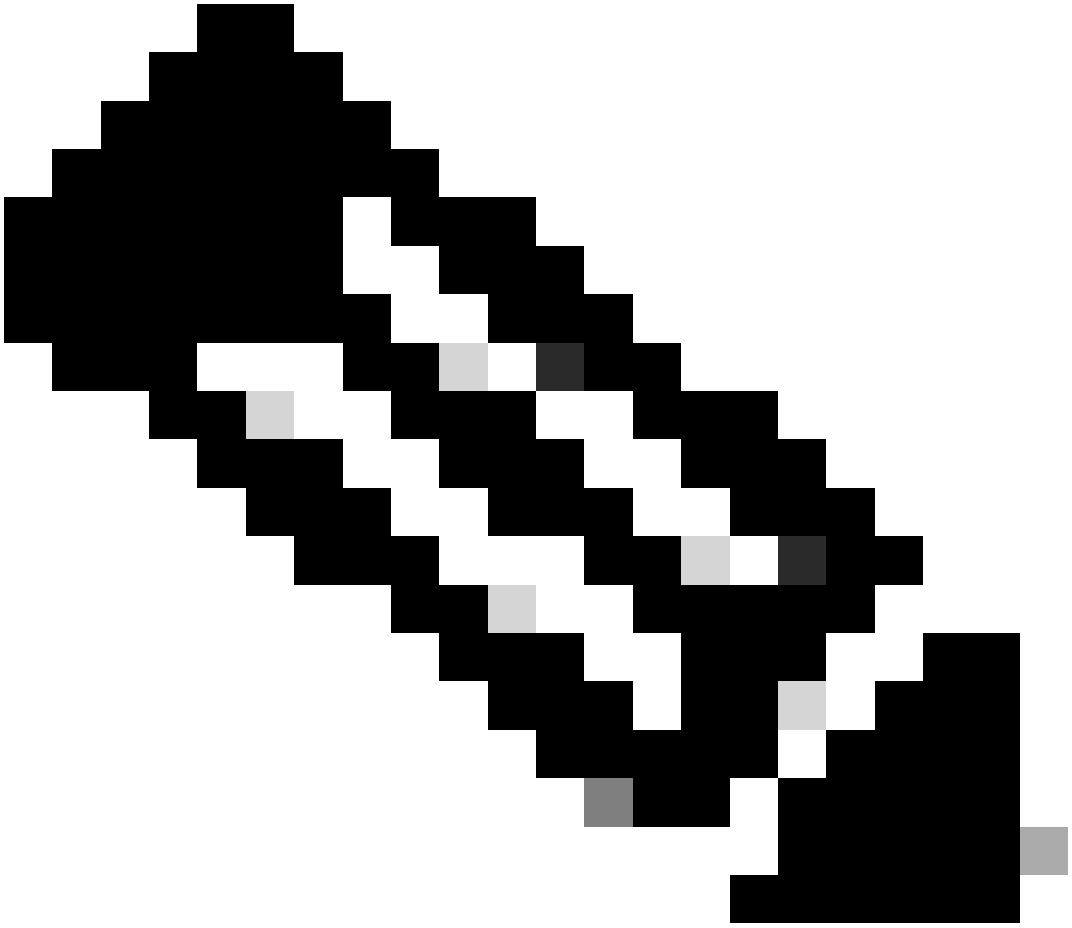

Add Transform Claim Rule Wizard
Configure Rule
Steps
Choose Rule Type
Configure Claim Rule
You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.
Claim rule name:
Account name to Name ID
Rule template: Send LDAP Attributes as Claims
Attribute store:
Active Directory
Mapping of LDAP attributes to outgoing claim types:
LDAP Attribute (Select or type to add more)
Outgoing Claim Type (Select or type to add more)
User-Principal-Name
Name ID
< Previous
Finish
Cancel



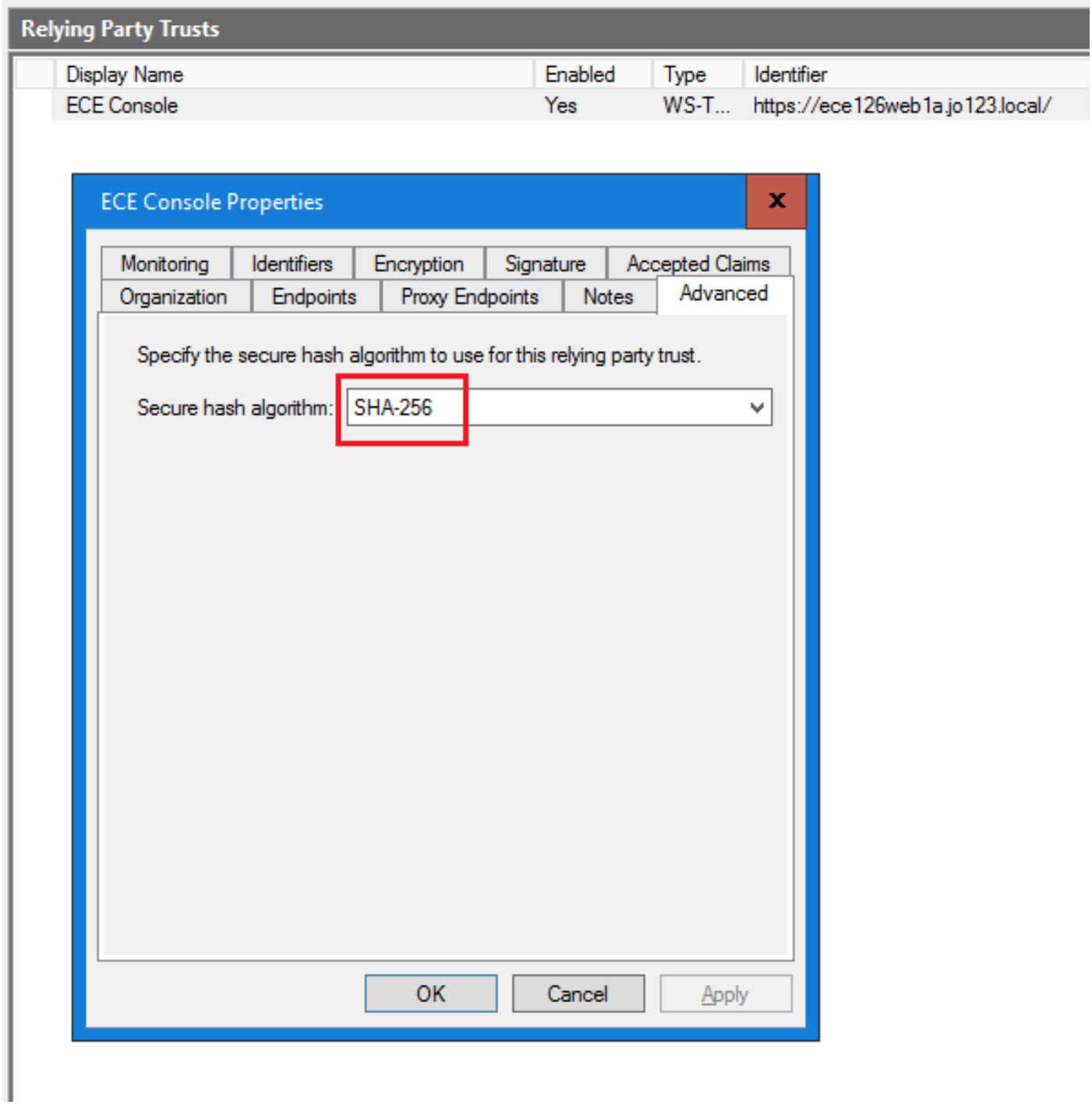
Paso 9

En la lista Confianzas de proveedores de confianza, haga doble clic en la confianza de usuario de confianza de ECE que ha creado.

En la ventana Propiedades que se abre, vaya a la ficha Avanzadas y establezca el algoritmo hash seguro en SHA-1 o SHA-256. Haga clic en Accept (Aceptar) para cerrar la ventana.



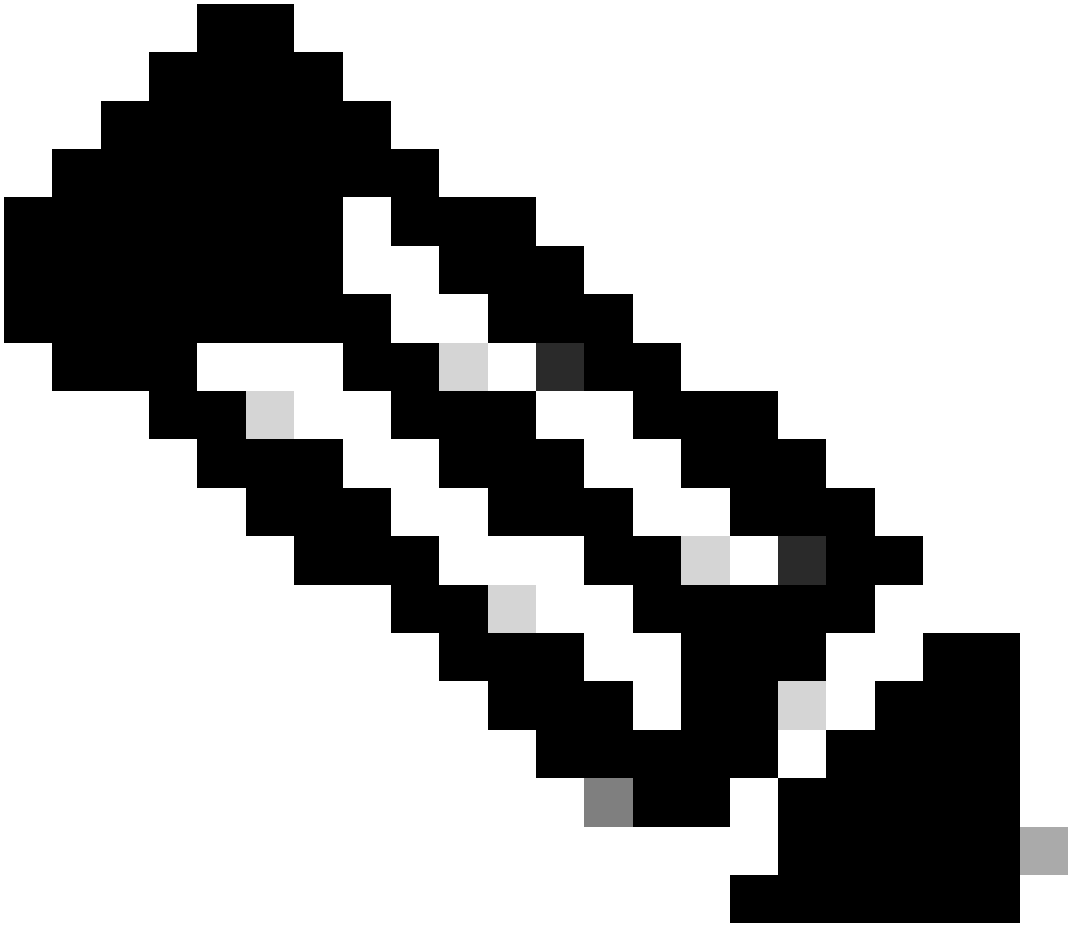
Nota: este valor debe coincidir con el valor del 'algoritmo de firma' establecido para el 'proveedor de servicios' en Configuraciones de SSO en ECE



Paso 10

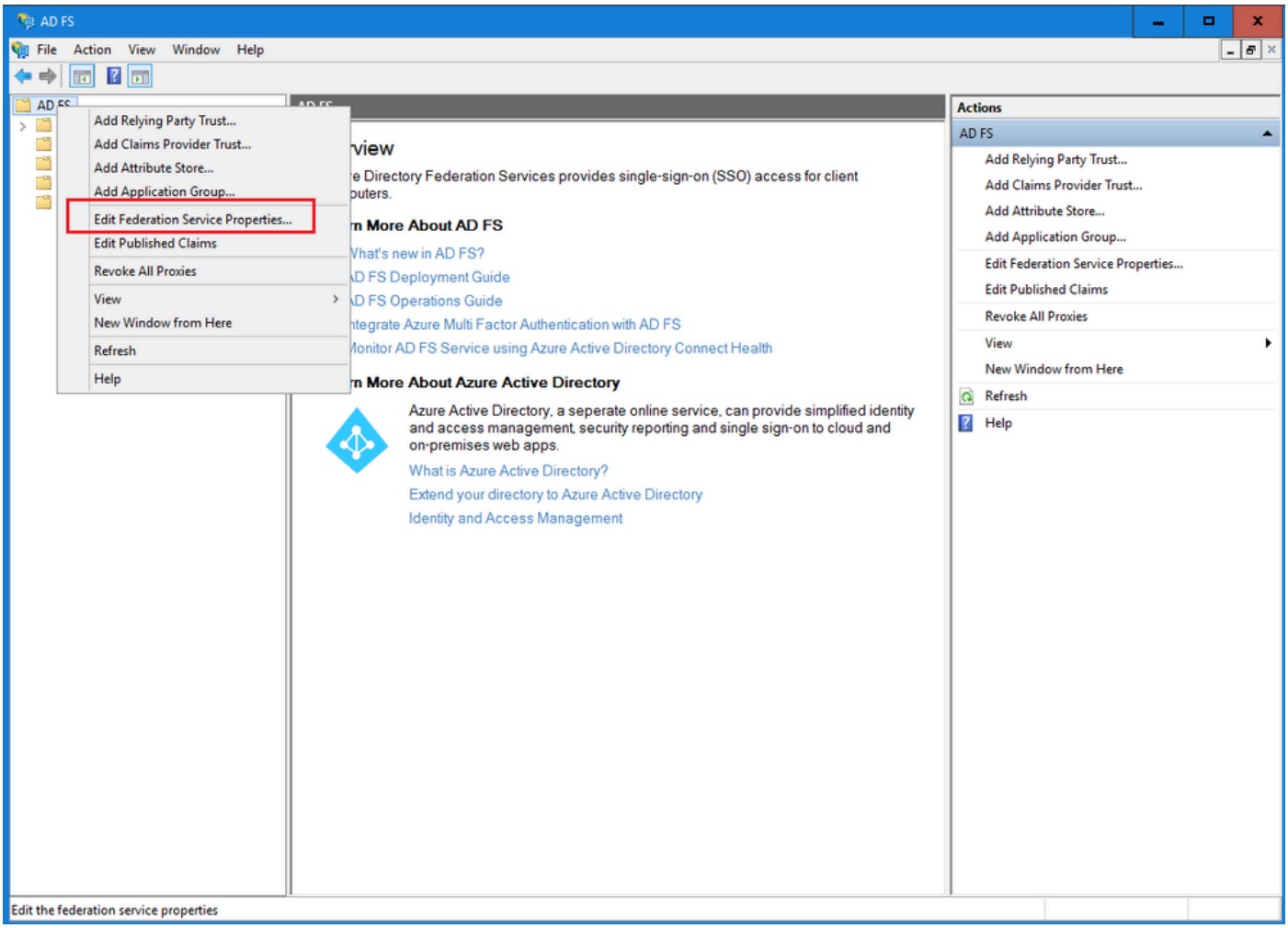
Verifique y anote el valor del Identificador del Servicio de federación.

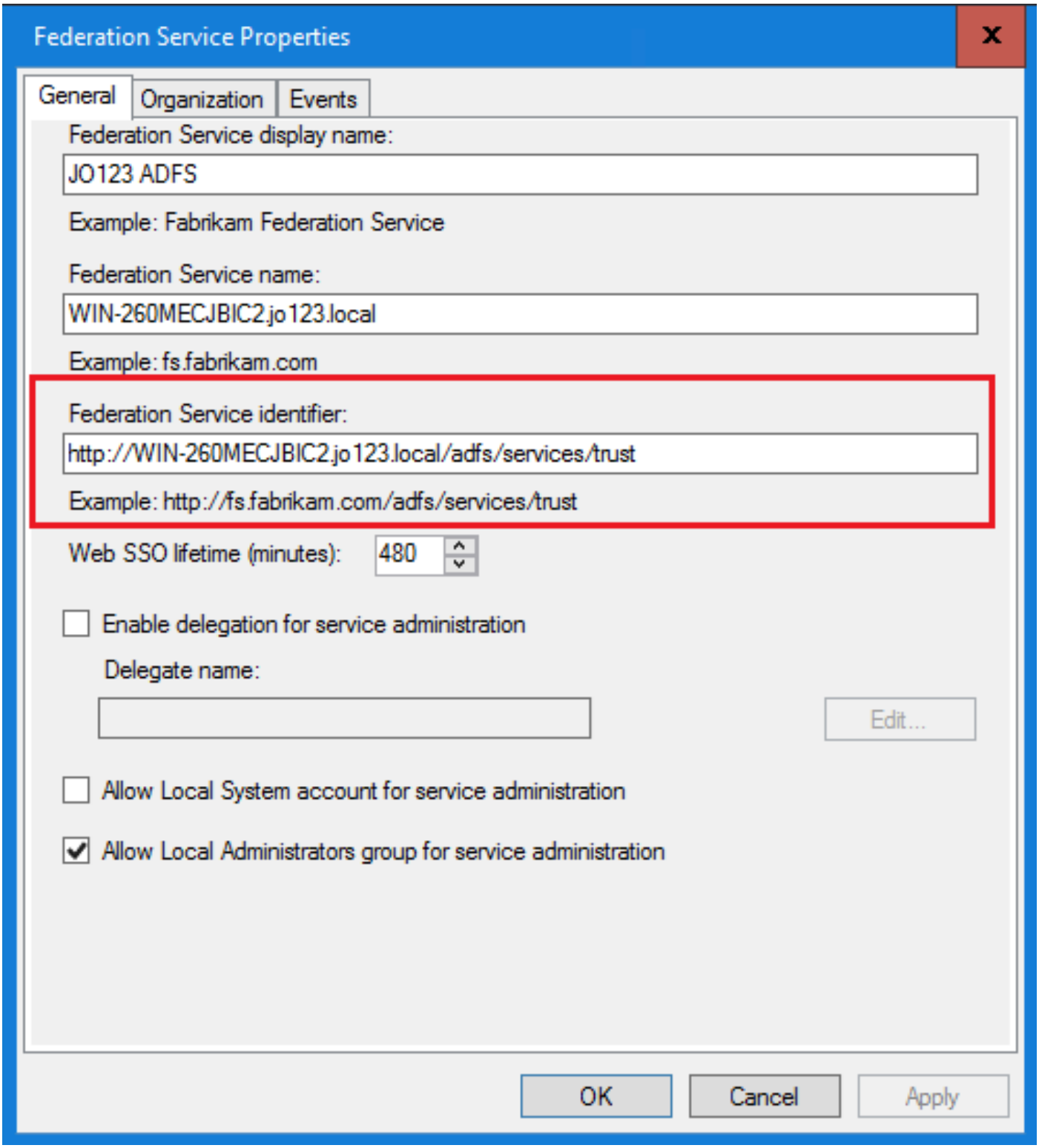
- En la consola de administración de AD FS, seleccione AD FS > Editar propiedades del servicio de federación > ficha General > Identificador del servicio de federación y haga clic con el botón secundario del mouse en él



Nota:

- Este valor debe agregarse exactamente tal como se indica al configurar el valor "Id. de entidad" para el proveedor de identidad en Configuraciones de SSO en ECE.
- El uso de http:// NO significa que ADFS no sea seguro, sino simplemente un identificador.


AD FS
File Action View Window Help
Add Relying Party Trust...
Add Claims Provider Trust...
Add Attribute Store...
Add Application Group...
Edit Federation Service Properties...
Edit Published Claims
Revoke All Proxies
View
New Window from Here
Refresh
Help
view
e Directory Federation Services provides single-sign-on (SSO) access for client
puters.
rn More About AD FS
What's new in AD FS?
D FS Deployment Guide
D FS Operations Guide
tegrate Azure Multi Factor Authentication with AD FS
Monitor AD FS Service using Azure Active Directory Connect Health
rn More About Azure Active Directory
Azure Active Directory, a seperate online service, can provide simplified identity
and access management, security reporting and single sign-on to cloud and
on-premises web apps.
What is Azure Active Directory?
Extend your directory to Azure Active Directory
Identity and Access Management
Actions
AD FS
Add Relying Party Trust...
Add Claims Provider Trust...
Add Attribute Store...
Add Application Group...
Edit Federation Service Properties...
Edit Published Claims
Revoke All Proxies
View
New Window from Here
Refresh
Help
Edit the federation service properties



Configuración de un proveedor de identidad

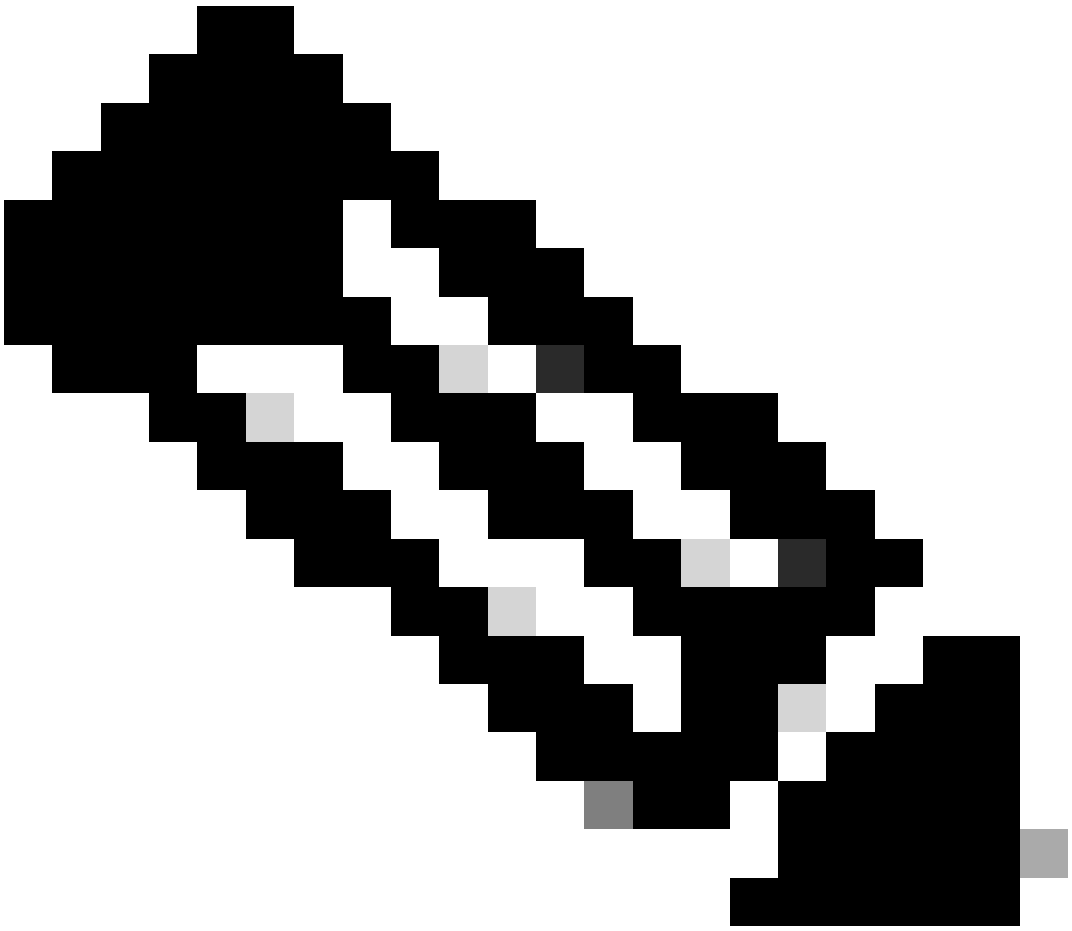
Paso 11

Se necesita un certificado de almacén de claves Java (JKS) para configurar SSO de modo que los usuarios con funciones de administrador o supervisor puedan iniciar sesión en la partición de ECE fuera de Finesse con sus credenciales de inicio de sesión de SSO.

Si desea configurar SSO para permitir que los usuarios con roles de administrador o supervisor

inicien sesión en la partición de ECE fuera de Finesse con sus credenciales de inicio de sesión de SSO, el certificado de almacén de claves Java (JKS) debe convertirse en certificado de clave pública y configurarse en Confianza de usuario de confianza creada en el servidor IdP para ECE.

Póngase en contacto con el departamento de TI para recibir el certificado JKS.

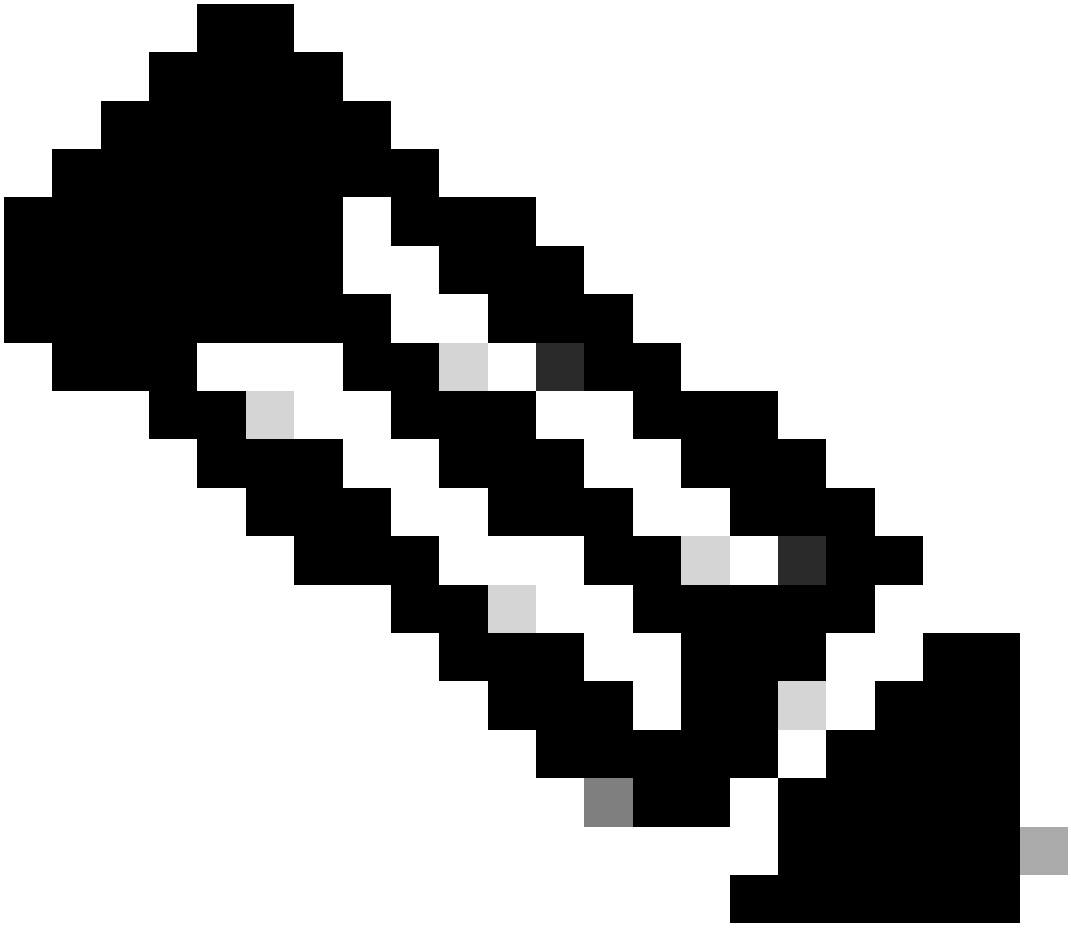


> Nota: estos pasos se aplican a los sistemas que utilizan ADFS como proveedor de identidad. Otros proveedores de identidad pueden tener diferentes métodos para configurar el certificado de clave pública.

A continuación se muestra un ejemplo de cómo se generó un archivo JKS en el laboratorio:

a. Generar JKS:

```
keytool -genkey -keyalg RSA -alias ece126web1a_saml -keystore C:\Temp\ece126web1a_saml.jks -keysize 204
```



Nota: La contraseña del almacén de claves, el nombre de alias y la contraseña de clave introducidos aquí se utilizan al configurar la configuración del proveedor de servicios en Configuraciones de SSO en ECE.

```
C:\Users\administrator.JO123>keytool -genkey -keyalg RSA -alias ece126web1a_saml -keystore C:\Temp\ece126web1a_saml.jks -keysize 2048 -validity 1825
Enter keystore password:
Re-enter new password:
What is your first and last name?
  [Unknown]:  ece126app1a.jo123.local
What is the name of your organizational unit?
  [Unknown]:  TAC
What is the name of your organization?
  [Unknown]:  Cisco
What is the name of your City or Locality?
  [Unknown]:  RTP
What is the name of your State or Province?
  [Unknown]:  NC
What is the two-letter country code for this unit?
  [Unknown]:  US
Is CN=ece126app1a.jo123.local, OU=TAC, O=Cisco, L=RTP, ST=NC, C=US correct?
  [no]:  yes

Enter key password for <ece126web1a_saml>
        (RETURN if same as keystore password):
```

b. Exportar el certificado:

Este comando keytool exporta el archivo de certificado en formato .crt con el nombre de archivo

ece126web1a_saml.crt al directorio C:\Temp.

```
keytool -exportcert -alias ece126web1a_saml -keystore C:\Temp\ece126web1a_saml.jks -rfc -file C:\Temp\e
```

Paso 12

Configuración de un proveedor de identidad

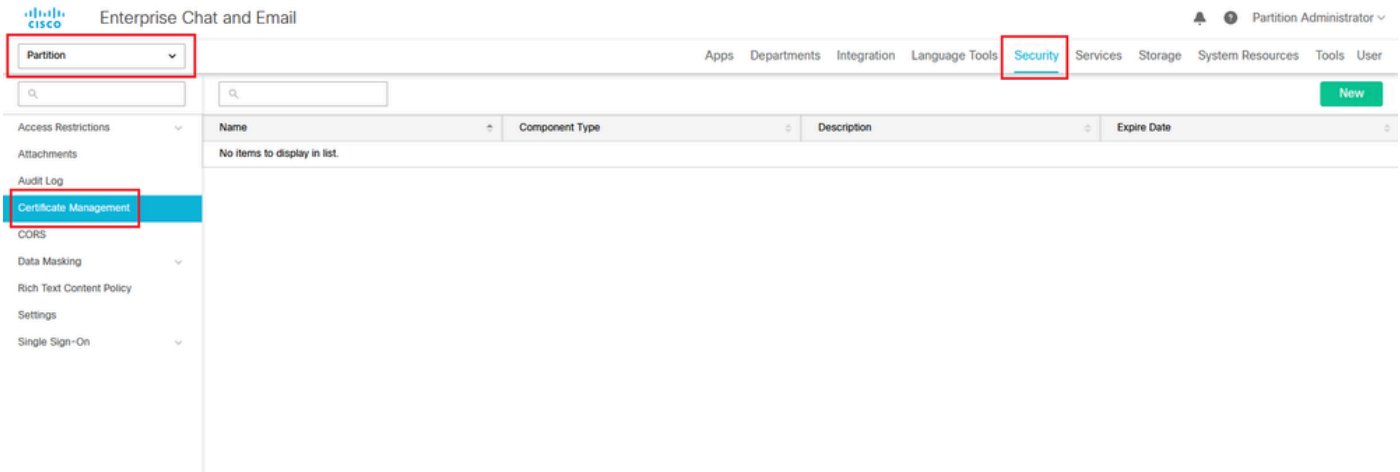
1. En la consola de administración de AD FS, seleccione y haga clic con el botón secundario del mouse (ratón) en la confianza de usuario de confianza creada para ECE.
2. Abra la ventana Propiedades de la confianza y, en la ficha Firma, haga clic en el botón Agregar.
3. Agregue el certificado público (archivo .crt generado en el paso anterior) y haga clic en Aceptar.

Creación e importación de certificados

Paso 13

Antes de configurar SSO para utilizar Cisco IDS para el inicio de sesión único para agentes, el certificado Tomcat del servidor de Cisco IdS debe importarse a la aplicación.

a. En la consola de administración de ECE, en Menú de nivel de partición, haga clic en la opción Seguridad y luego seleccione Administración de certificados en el menú del lado izquierdo.

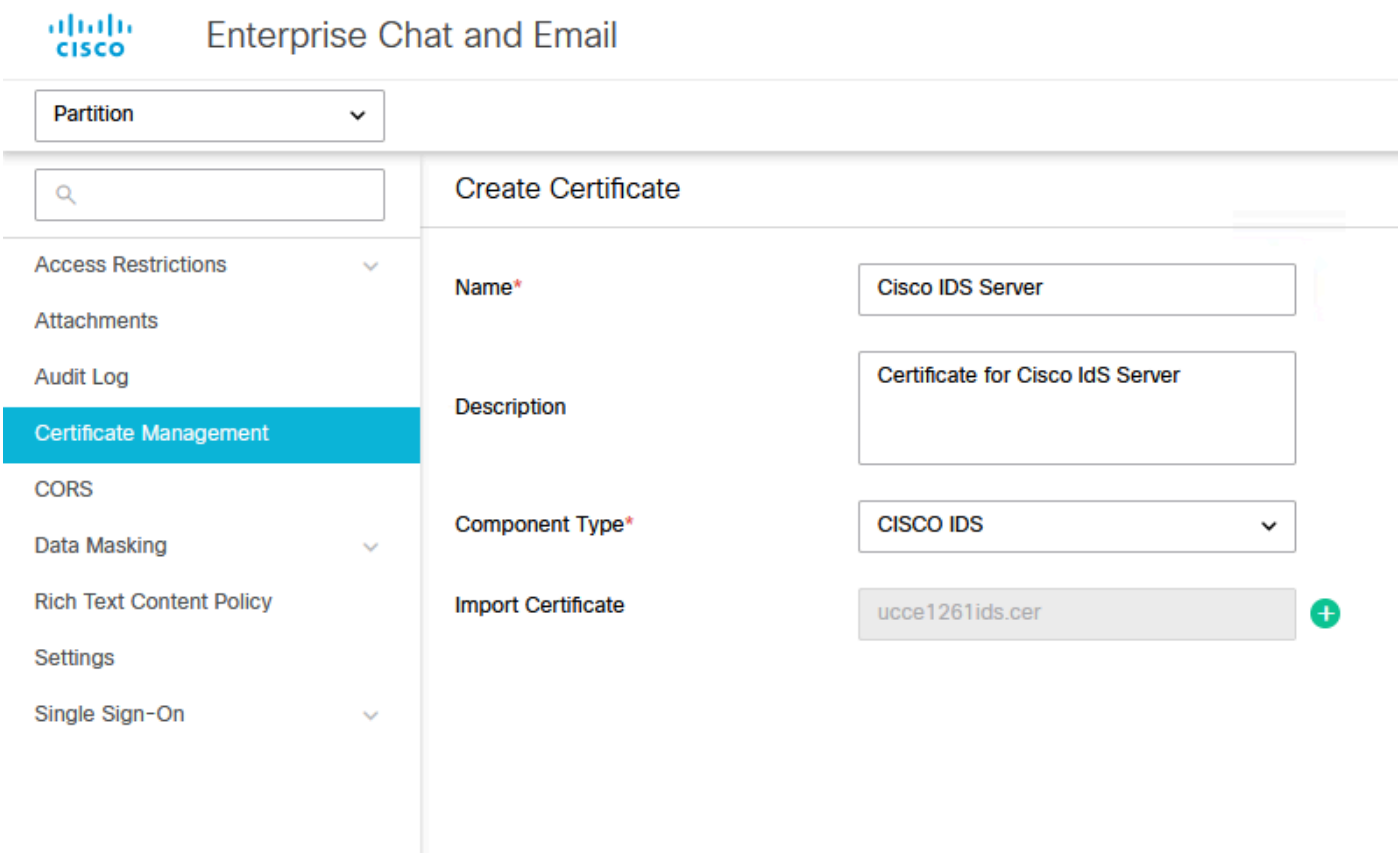


b. En el espacio Administración de certificados, haga clic en el botón Nuevo e introduzca los detalles adecuados:

- Nombre: escriba un nombre para el certificado.
- Descripción: agregue una descripción para el certificado.
- Tipo de componente: Seleccione CISCO IDS.
- Importar certificado: para importar el certificado, haga clic en el botón Buscar y agregar e introduzca los detalles solicitados:
- Archivo de certificado: Haga clic en el botón Browse (Examinar) y seleccione el certificado

que desea importar. Los certificados sólo se pueden importar en los formatos .pem, .der (BINARY) o .cer/cert.
- Nombre de alias: introduzca un alias para el certificado.

c. Haga clic en Guardar

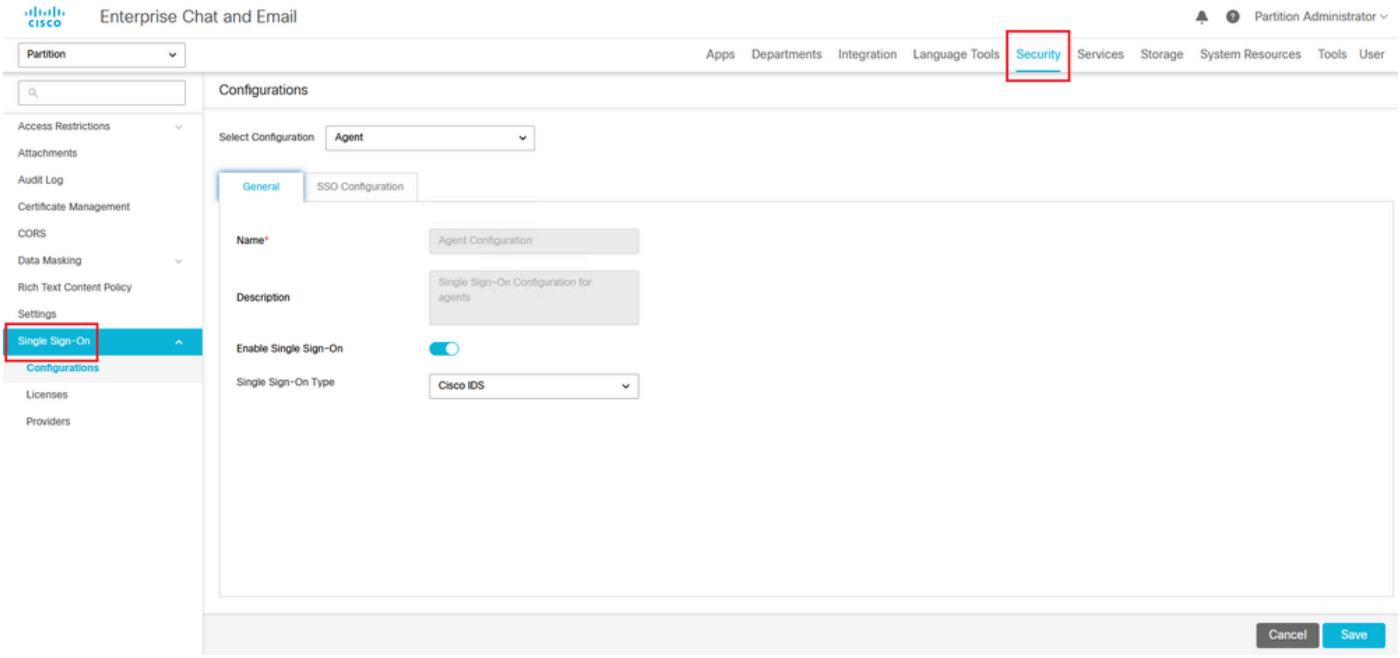


Configuración de Inicio de sesión único del agente

Paso 14

1. En la consola de administración de ECE, en el menú de nivel de partición, haga clic en la opción Security y, a continuación, seleccione Single Sign-On > Configurations en el menú de la izquierda.
2. En el menú desplegable Seleccionar configuración, seleccione Agente y establezca la configuración en la ficha General:

- Activar inicio de sesión único: haga clic en el botón Alternar para activar el inicio de sesión único.
- Tipo de inicio de sesión único: Seleccione Cisco IDS.



Paso 15

Haga clic en la pestaña SSO Configuration y proporcione los detalles de la configuración:

a. Proveedor de OpenID Connect

URL de terminal de información de usuario principal

- La URL de terminal de información del usuario del servidor IDS de Cisco principal.
- Esta URL valida el token de usuario/API de información de usuario.
- Está en el formato: https://cisco-ids-1:8553/ids/v1/oauth/userinfo, donde cisco-ids-1 indica el nombre de dominio completamente calificado (FQDN) del servidor principal de Cisco IDS.

Nombre de reclamación de identidad de usuario

- Nombre de la notificación devuelta por la dirección URL del terminal de información del usuario, que identifica el nombre de usuario en Unified o Packaged CCE.
- El nombre de la reclamación y el nombre de usuario de Unified o Packaged CCE deben coincidir.
- Esta es una de las notificaciones obtenidas en respuesta a la validación del token portador.
- Si el nombre de usuario de los agentes de Unified o Packaged CCE coincide con el nombre principal de usuario, proporcione "upn" como valor del campo Nombre de reclamación de identidad de usuario.
- Si el nombre de usuario de los agentes de Unified o Packaged CCE coincide con el nombre de cuenta SAM, proporcione "sub" como valor del campo Nombre de reclamación de identidad de usuario.

URL de terminal de información de usuario secundario

- La URL del terminal de información del usuario secundario del servidor IDS de Cisco.
- Está en el formato: https://cisco-ids-2:8553/ids/v1/oauth/userinfo, donde cisco-ids-2 indica el nombre de dominio completamente calificado (FQDN) del servidor secundario de Cisco IDS.

Método URL de terminal de información de usuario

- El método HTTP utilizado por ECE para realizar llamadas de validación de token portador a la URL de terminal de información de usuario.
- Seleccione POST en la lista de opciones presentadas (POST se selecciona aquí para coincidir con el método del servidor IDS).

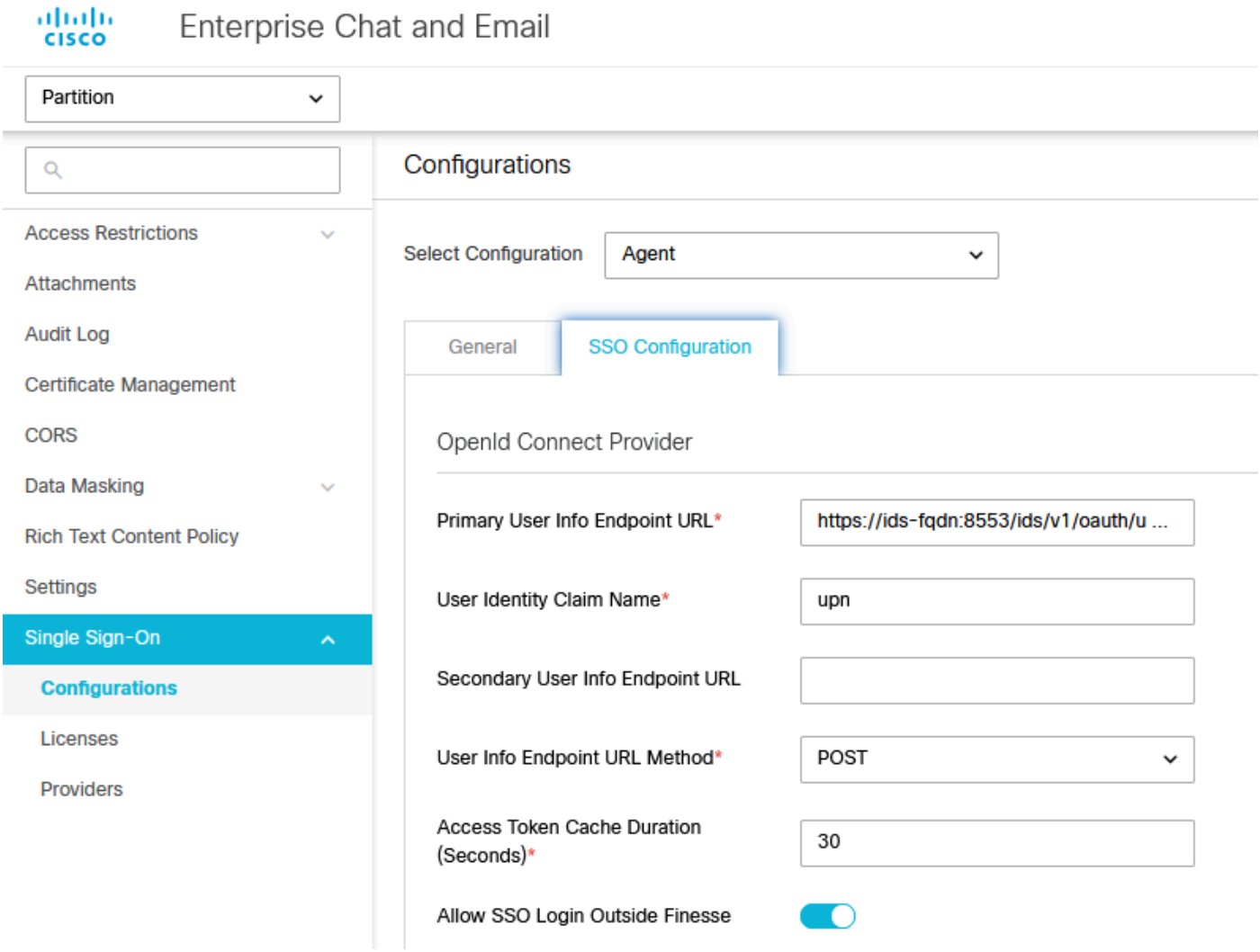
POST: método utilizado para enviar datos al servidor IDS de Cisco en el extremo especificado.

Duración de caché de token de acceso (segundos)

- La duración, en segundos, durante la cual un token portador debe almacenarse en caché en ECE.
- Los tokens portadores para los que las llamadas de validación son correctas sólo se almacenan en cachés. (Valor mínimo: 1; valor máximo: 30)

Permitir inicio de sesión SSO fuera de Finesse

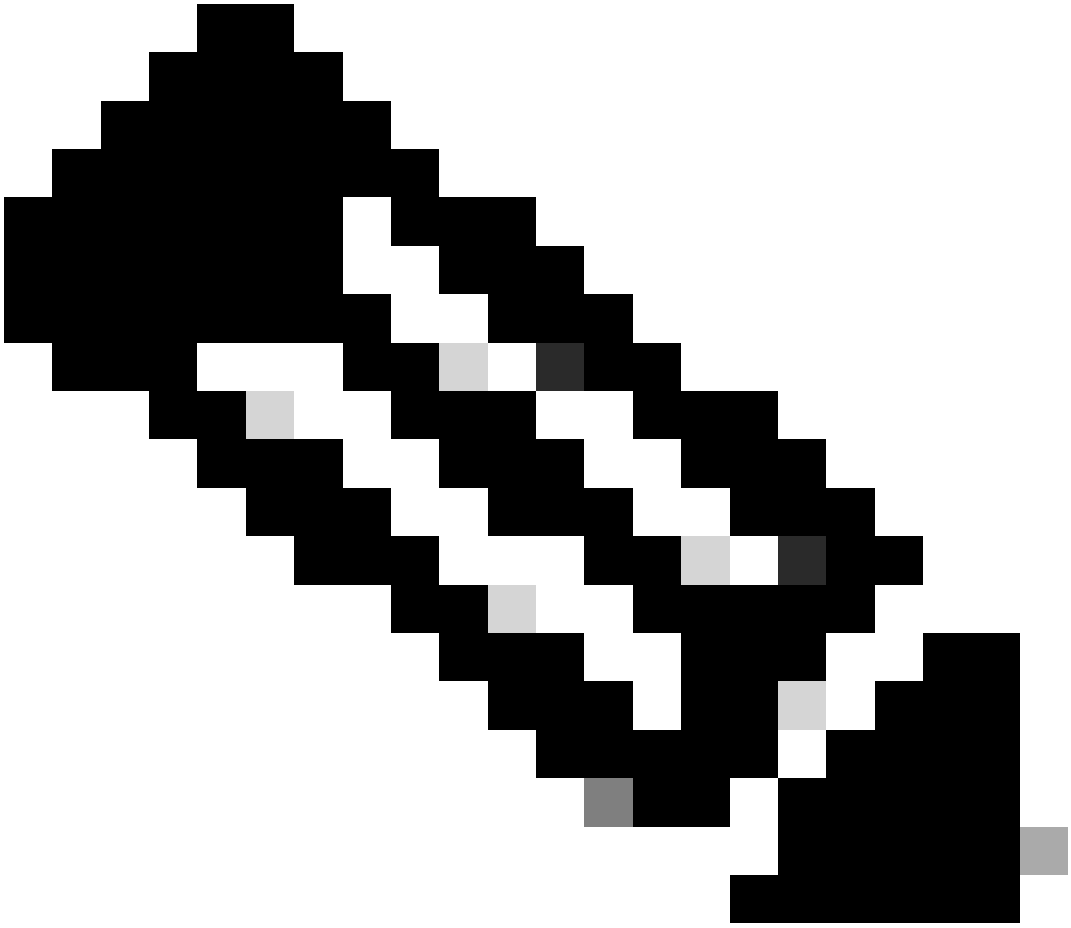
- Haga clic en este botón Alternar si desea permitir que los usuarios con funciones de administrador o supervisor inicien sesión en la partición de ECE fuera de Finesse con sus credenciales de inicio de sesión de SSO.
- Si se activa, se debe proporcionar información en las secciones Proveedor de identidad y Proveedor de servicios.
- Esto requiere que su configuración de IdP permita un servidor de IdP compartido.



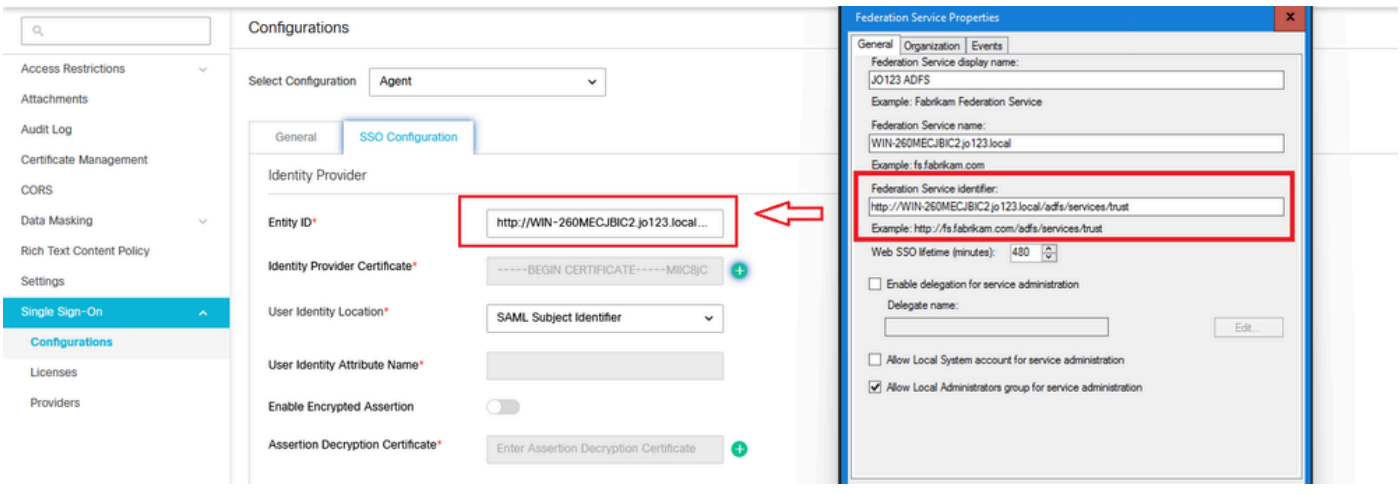
b. Proveedor de identidad

ID de entidad

- Id. de entidad del servidor IdP.

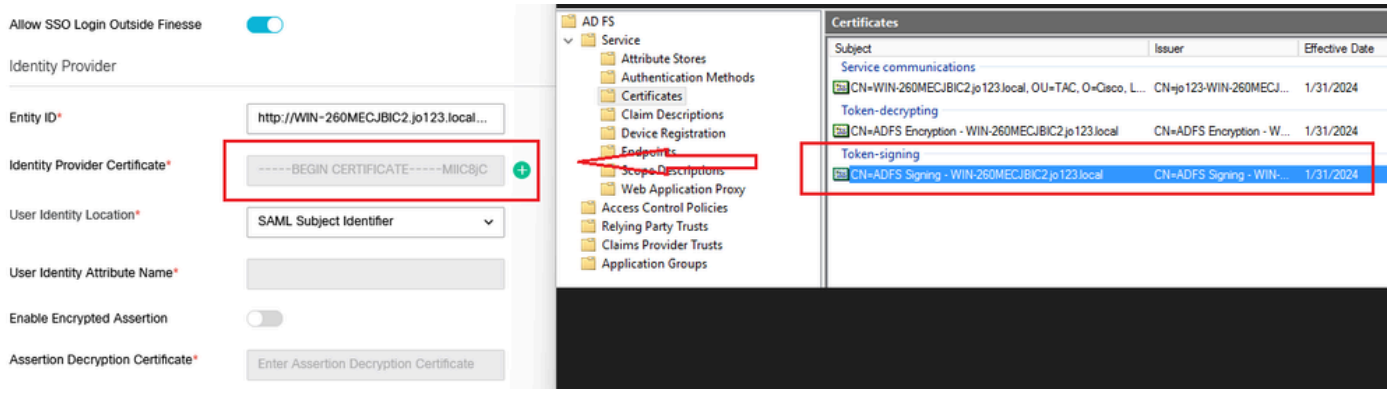


Nota: este valor debe coincidir exactamente con el valor 'Identificador de servicio de federación' de la consola de administración de AD FS.



Certificado del proveedor de identidad

- El certificado de clave pública.
- El certificado debe comenzar con "-----BEGIN CERTIFICATE-----" y terminar con "-----END CERTIFICATE-----"
- Este es el certificado de firma de token en la Consola de administración de AD FS > Servicio > Certificados > Firma de token.



Ubicación de identidad de usuario

- Seleccione SAML Subject Identifier para establecer la ubicación de identidad en el certificado con el identificador de asunto SAML predeterminado, como en el asunto de la afirmación SAML, por ejemplo, el nombre de usuario en <saml:Subject>.
- Seleccione Atributo SAML para asignar la ubicación de identidad a un atributo específico del certificado, por ejemplo, email.address. Proporcione el atributo en el campo Nombre de atributo de identidad de usuario.

Nombre de atributo de identidad de usuario

- Sólo se aplica cuando el valor de Ubicación de ID de usuario es un atributo SAML.
- Esto se puede ajustar dentro de la afirmación SAML y se puede utilizar para seleccionar un atributo diferente para la autenticación de usuarios, como una dirección de correo electrónico.
- También se puede utilizar para crear nuevos usuarios con un atributo SAML.
- Por ejemplo, si se identifica a un usuario mediante el valor proporcionado en el atributo email.address y el valor de la dirección de correo electrónico proporcionada no coincide con ningún usuario del sistema, se crea un nuevo usuario con los atributos SAML proporcionados.

Habilitar aserción cifrada (opcional)

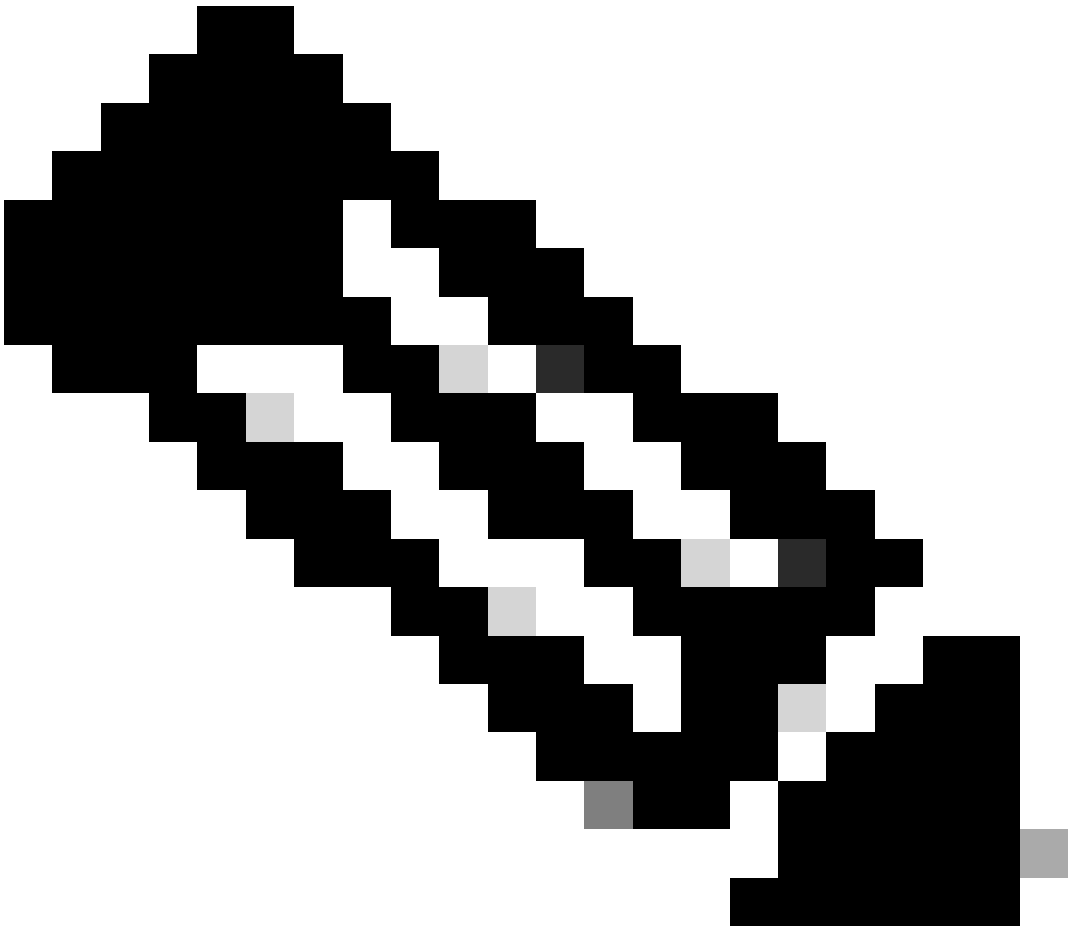
- Si desea activar la aserción cifrada con el proveedor de identidad para el inicio de sesión en la consola, haga clic en el botón Toggle (Alternar) para establecer el valor en Enabled (Activado).
- Si no es así, establezca el valor en Disabled (Desactivado).

Certificado de descifrado de aserción

Si Habilitar aserción cifrada está establecido en Habilitado, haga clic en el botón Buscar y agregar y confirme su elección para cambiar el certificado.

Proporcione los detalles en la ventana Certificado de descifrado de aserción:

- Archivo de Almacén de Claves Java: Introduzca la ruta del archivo del almacén de claves Java. Este archivo tiene el formato .jks y contiene la clave de descifrado que el sistema necesita para acceder a los archivos protegidos por el proveedor de identidad.
- Nombre de Alias: Identificador exclusivo de la clave de descifrado.
- Contraseña del Almacén de Claves: Contraseña necesaria para acceder al archivo de almacén de claves Java.
- Key Password (Contraseña de clave): Contraseña necesaria para acceder a la clave de descifrado del alias.



> Nota: debe coincidir con el certificado de la ficha 'Cifrado' de la confianza de usuario de confianza de ECE configurada en la consola de administración de AD FS.

---

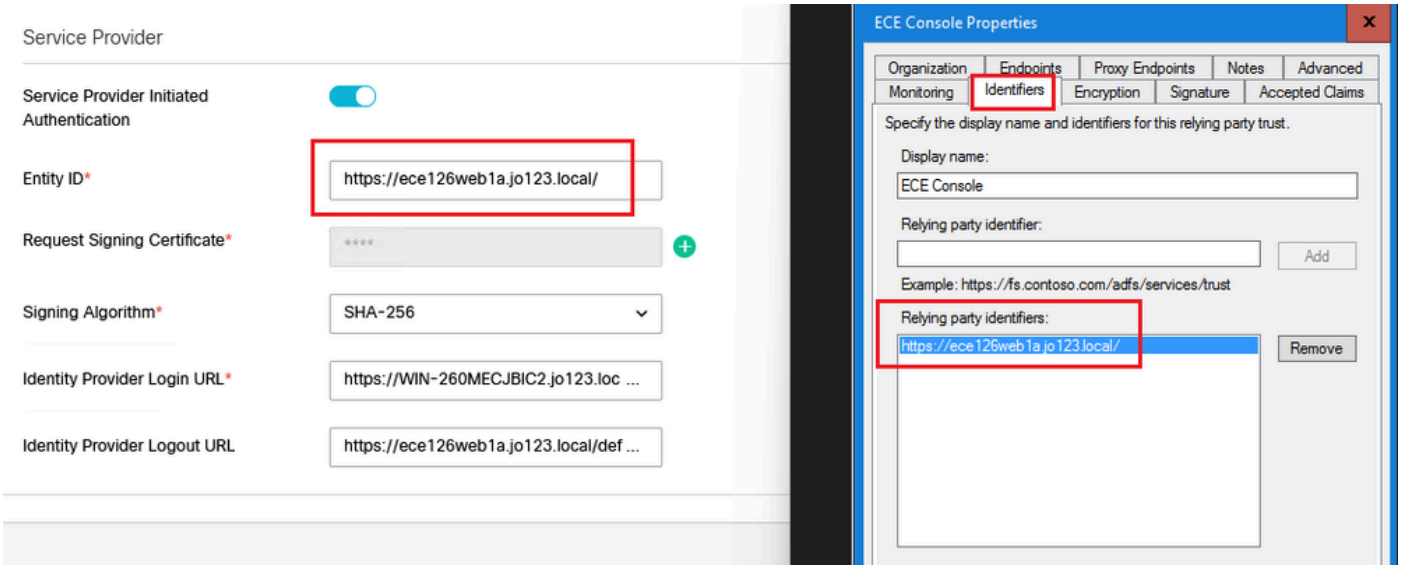
c. Proveedor de servicios

Autenticación iniciada por el proveedor de servicios

- Establezca el botón de alternancia en Activado.

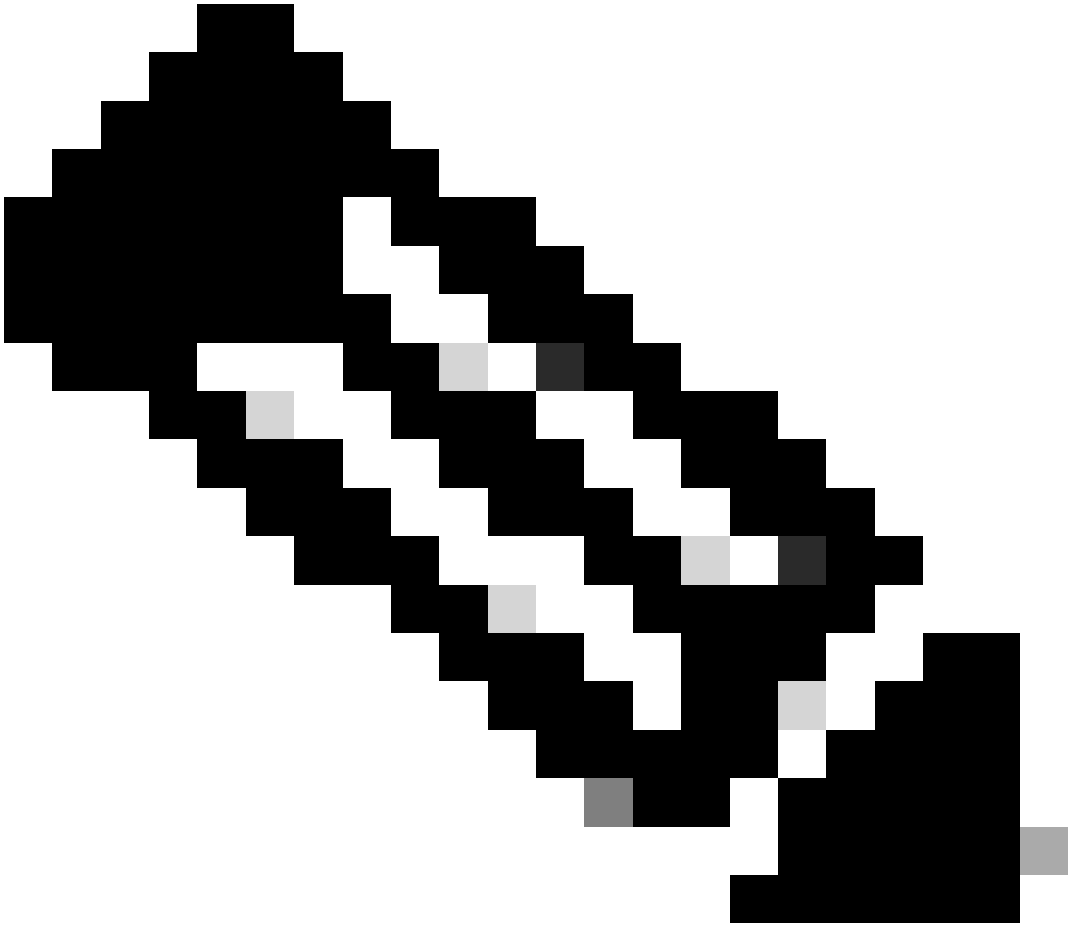
ID de entidad

- Proporcione la URL externa de la aplicación ECE.

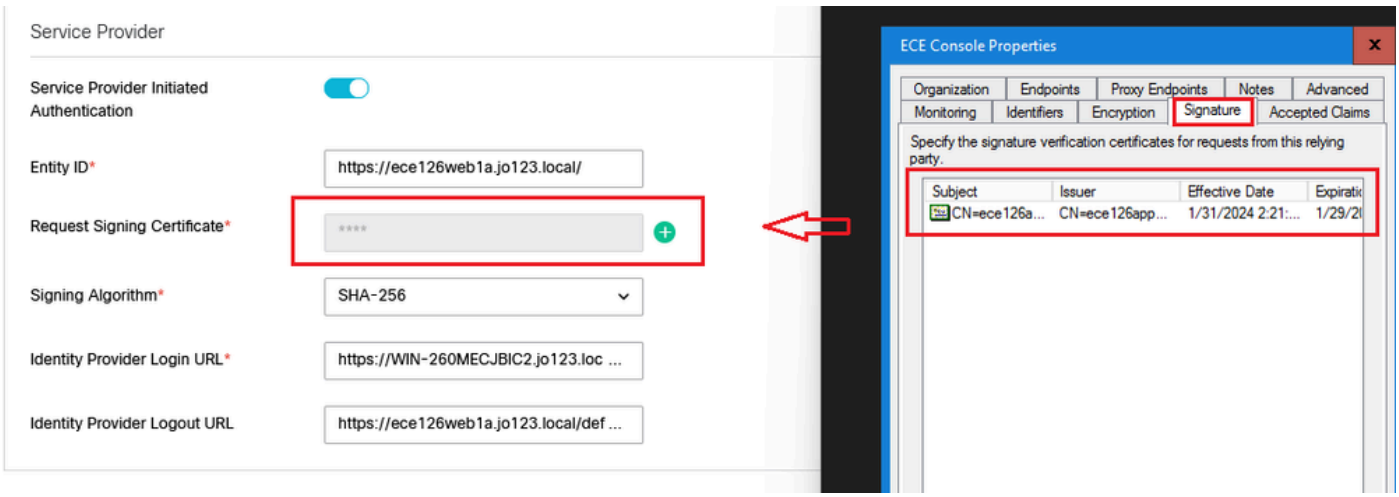


Solicitar certificado de firma

- Se necesita un certificado de almacén de claves Java (JKS) para proporcionar la información necesaria.
- Cargue el archivo .jks con el nombre de alias y la contraseña del almacén de claves/clave generados en el paso 11.

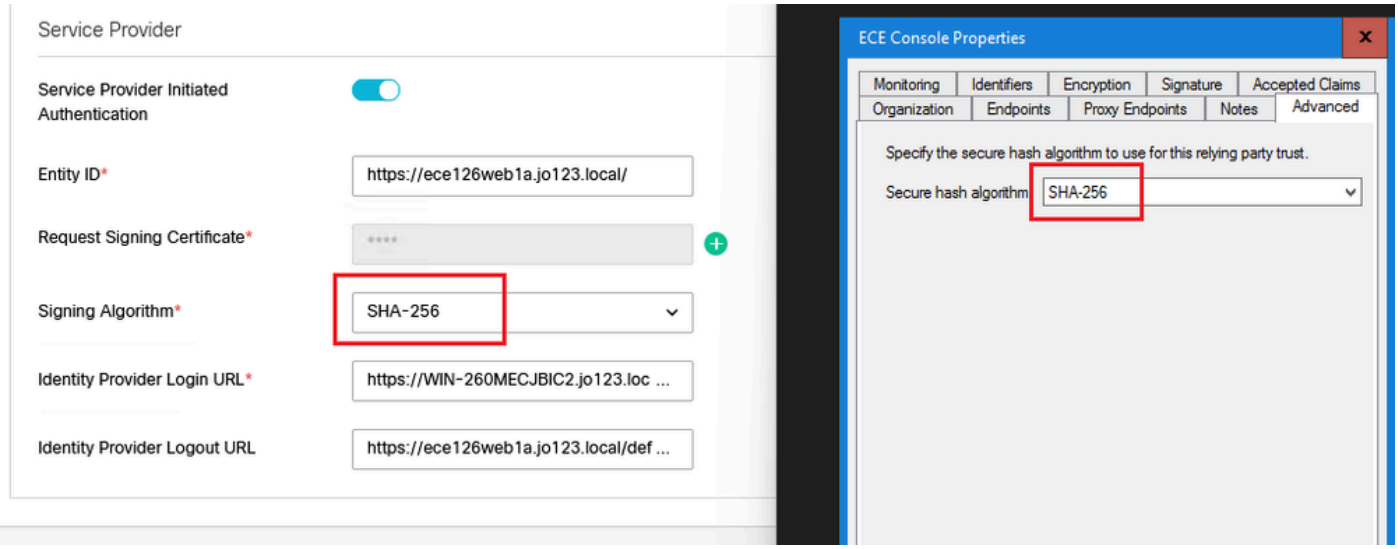


Nota: debe coincidir con el certificado cargado en la ficha "Firma" de la confianza de usuario de confianza de ECE configurada en la consola de administración de AD FS.



Algoritmo de firma

- Establezca el algoritmo de firma para el proveedor de servicios.
- Si utiliza ADFS, este valor debe coincidir con el algoritmo seleccionado en la confianza de usuario de confianza creada para ECE en la ficha Avanzadas.



URL de inicio de sesión del proveedor de identidad

- La URL para la autenticación SAML.
- Por ejemplo, para ADFS, sería http://<ADFS>/adfs/ls.

URL de cierre de sesión del proveedor de identidad

- Dirección URL a la que se redirige a los usuarios al cerrar sesión. Esta opción es opcional y puede ser cualquier URL.
- Por ejemplo, los agentes se pueden redirigir a https://www.cisco.com o a cualquier otra URL después de cerrar la sesión de SSO.

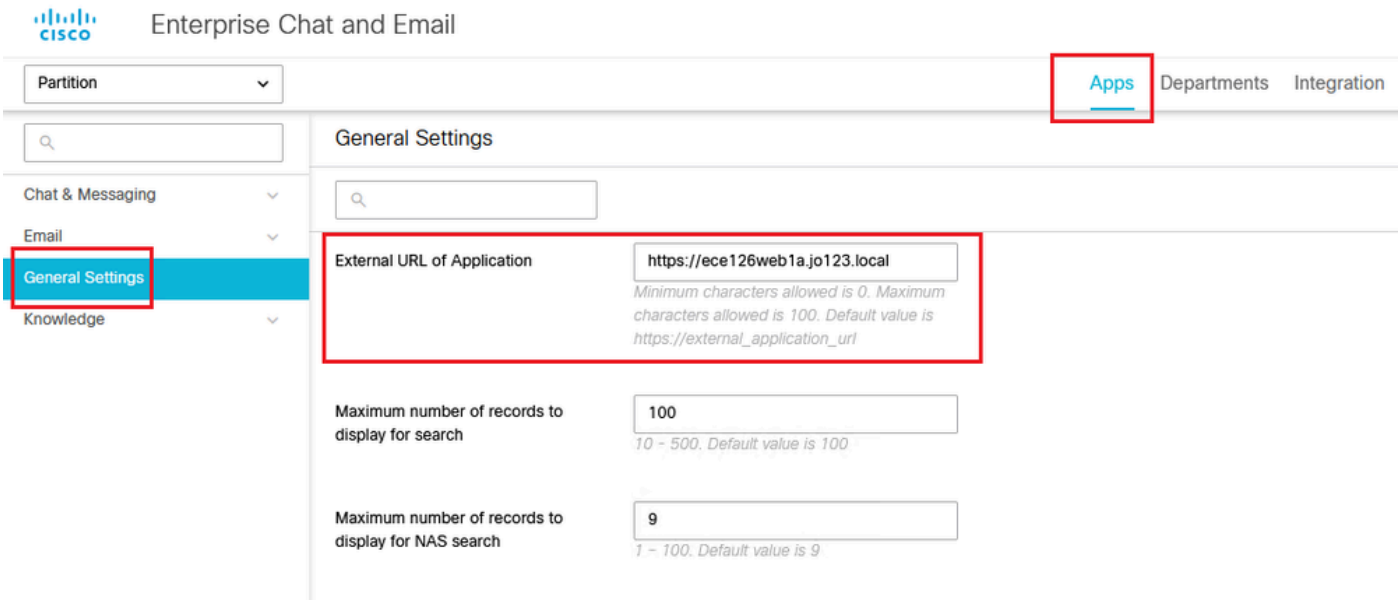
Paso 16

Haga clic en Save (Guardar).

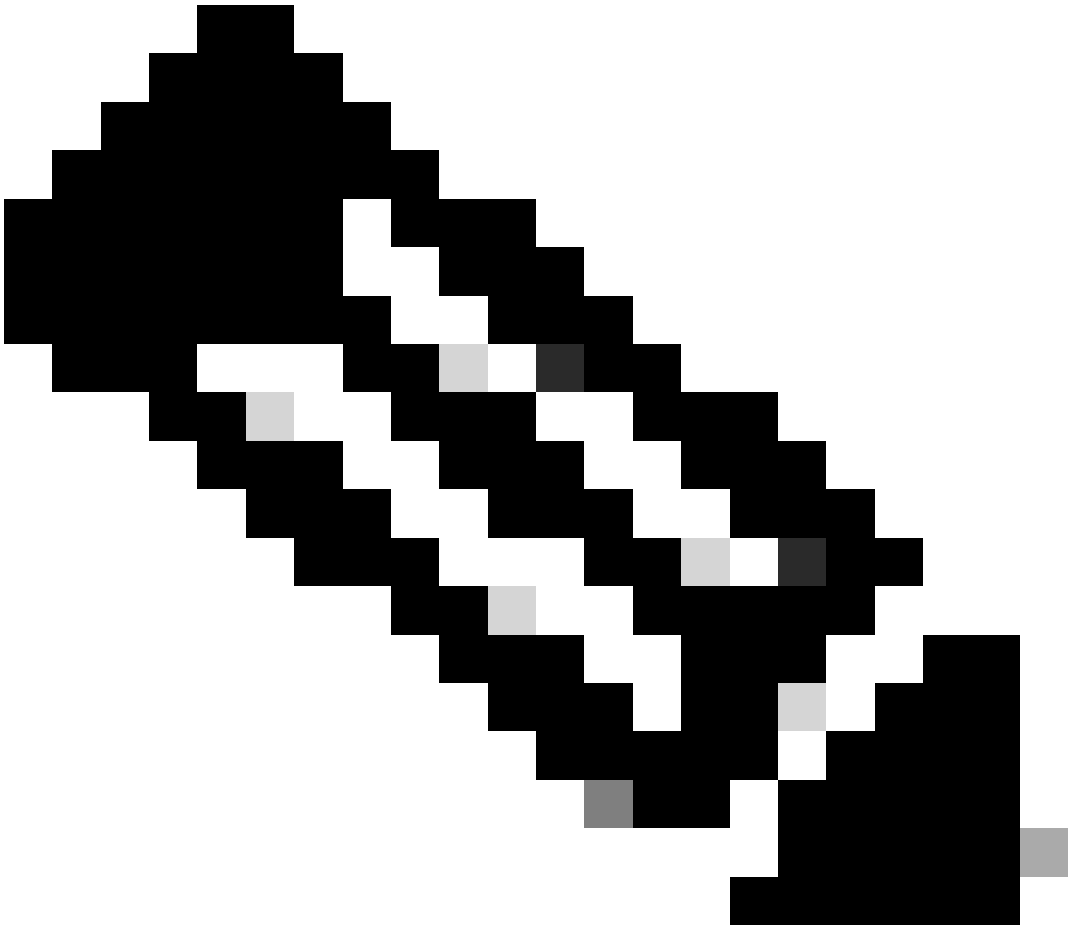
Establezca la URL del servidor Web/LB en la configuración de la partición

Paso 17

Asegúrese de ingresar la URL correcta del servidor Web/LB en la configuración de la partición > seleccione la pestaña Aplicaciones y navegue hasta Configuración general > URL externo de la aplicación



Configuración de SSO para Administradores de Partición



Nota:

- Este paso se aplica sólo a PCCE.
- Se trata del gadget ECE al que se accede desde la interfaz WEB de administración de CCE https:///cceadmin.

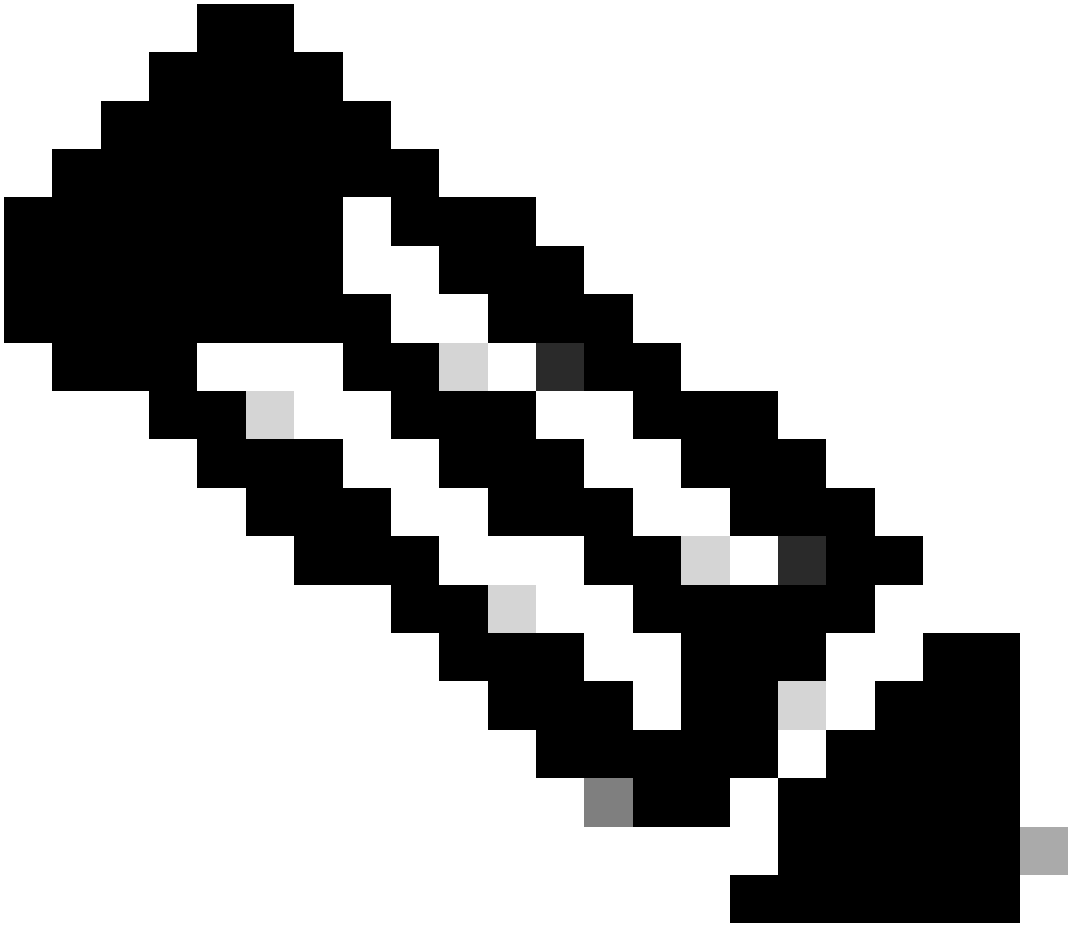
Paso 18

Para configurar SSO para el administrador de particiones

1. En la consola de administración de ECE, en el menú de nivel de partición, haga clic en la opción Seguridad y, a continuación, seleccione Inicio de sesión único > Configuraciones en el menú de la izquierda.
2. En el menú desplegable Seleccionar configuración, seleccione Administradores de partición e introduzca los detalles de configuración:

URL LDAP

- La URL del servidor LDAP.
- Puede ser la URL del controlador de dominio (por ejemplo, ldap://LDAP_server:389) o la URL del catálogo global (por ejemplo, ldap://LDAP_server:3268) del servidor LDAP.
- La partición se puede agregar automáticamente al sistema cuando se accede a ECE a través de la consola de administración de CCE si ECE está configurado con búsqueda LDAP.
- Sin embargo, en las implementaciones de Active Directory con varios dominios en un único bosque o donde se configuran UPN alternativos, no se debe utilizar la URL del controlador de dominio con los puertos LDAP estándar 389 y 636.
- La integración LDAP se puede configurar para utilizar la URL del catálogo global con los puertos 3268 y 3269.



Nota: se recomienda utilizar la URL de catálogo global. Si no utiliza un GC, un error en los registros de ApplicationServer es el siguiente.

- Excepción en la autenticación LDAP <@> javax.aming.PartialResultException: referencias de continuación sin procesar; nombre restante 'DC=ejemplo,DC=com'

---

atributo DN

- Atributo del DN que contiene el nombre de inicio de sesión del usuario.
- Por ejemplo, userPrincipalName.

Base

- La aplicación utiliza el valor especificado para Base como base de búsqueda.
- La base de búsqueda es la ubicación inicial para la búsqueda en el árbol de directorios LDAP.
- Por ejemplo, DC=miempresa, DC=com.

DN para búsqueda LDAP

- Si el sistema LDAP no permite el enlace anónimo, proporcione el nombre distinguido (DN) de un usuario que tenga permisos de búsqueda en el árbol de directorios LDAP.
- Si el servidor LDAP permite el enlace anónimo, deje este campo en blanco.

Contraseña

- Si su sistema LDAP no permite el enlace anónimo, proporcione la contraseña de un usuario que tenga permisos de búsqueda en el árbol de directorios LDAP.
- Si el servidor LDAP permite el enlace anónimo, deje este campo en blanco.

Paso 19

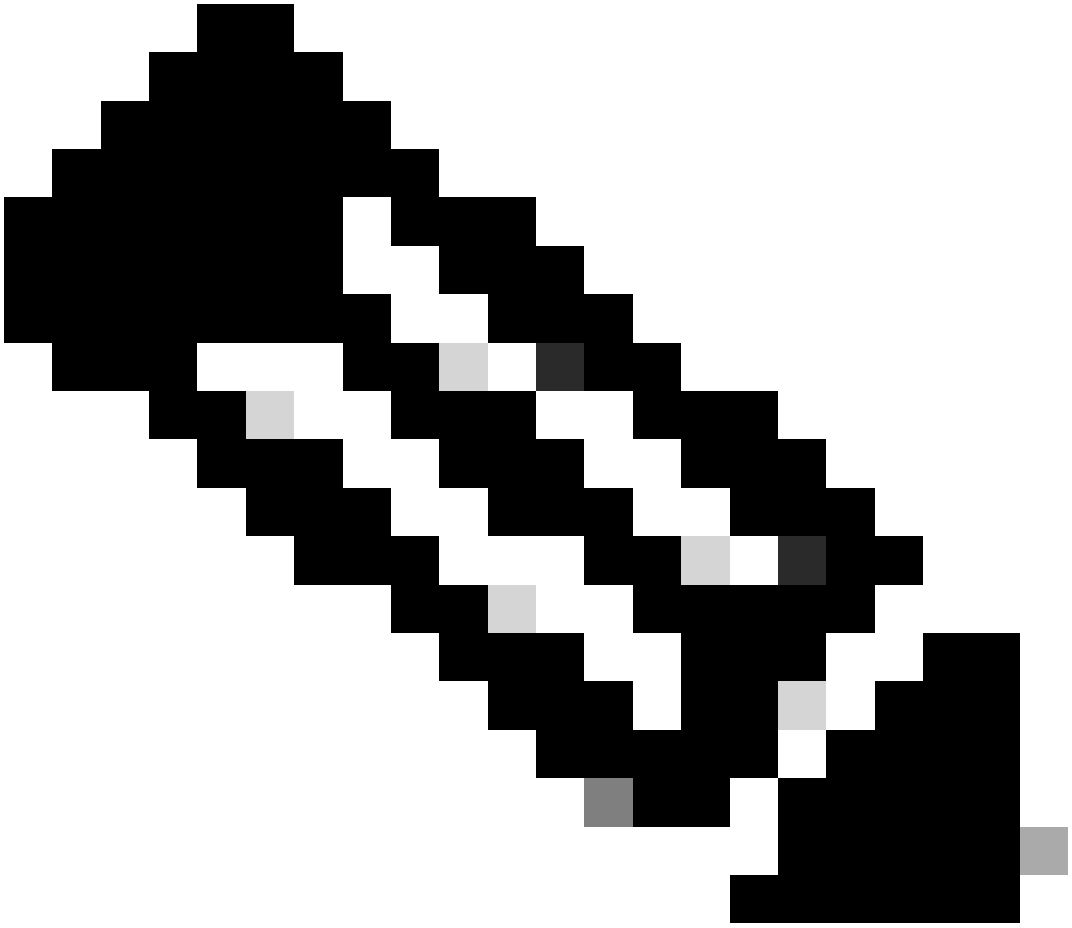
Haga clic en Save (Guardar).

Con esto finaliza la configuración de inicio de sesión único para agentes y administradores de particiones en ECE.

Resolución de problemas

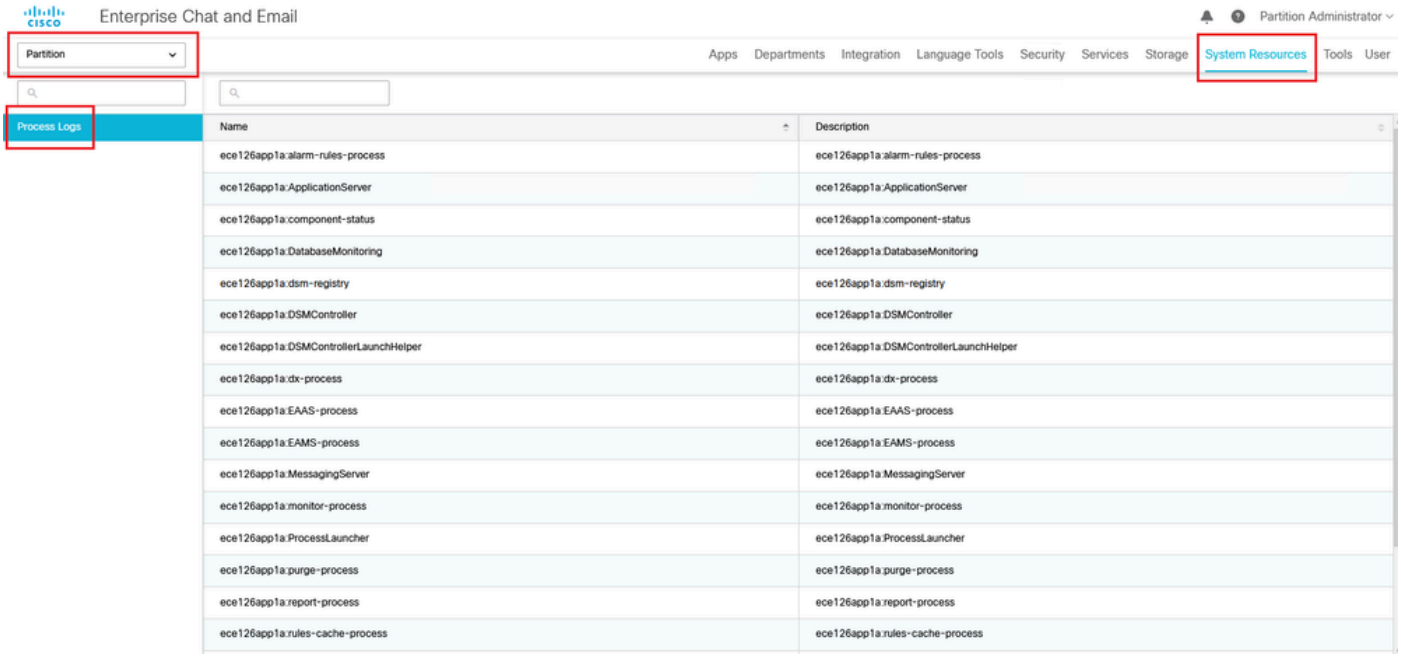
Configuración del nivel de seguimiento

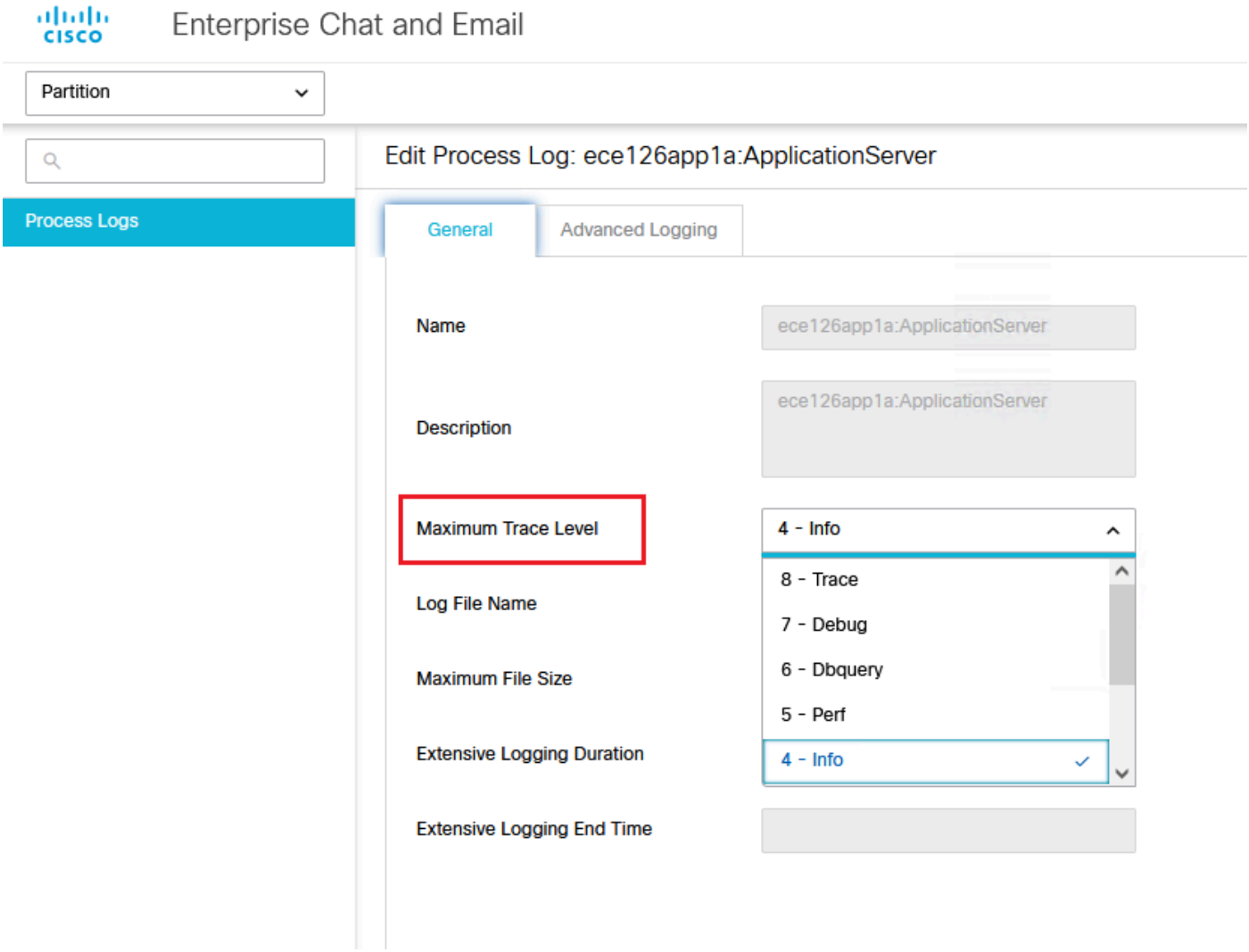
1. En la consola de administración de ECE, en el menú de nivel de partición, haga clic en la opción Recursos del sistema y, a continuación, seleccione Registros de proceso en el menú de la izquierda.
2. En la lista de procesos, seleccione el proceso ApplicationServer > establezca el nivel de seguimiento deseado en el menú desplegable 'Maximum Trace Level'.



Nota:

- Para solucionar los errores de inicio de sesión de SSO durante la instalación inicial o la reconfiguración, establezca el seguimiento de procesos de ApplicationServer en el nivel 7.
- Una vez que se reproduzca el error, vuelva a establecer el nivel de seguimiento en el nivel 4 predeterminado para evitar que se sobrescriban los registros.





Situación de solución de problemas 1

Error

- Código de error: 500
- Descripción del error: la aplicación no puede iniciar sesión en el usuario en este momento porque se ha producido un error en el inicio de sesión del proveedor de identidad.

Análisis de registro

- Error de inicio de sesión IdP - <samlp:Status><samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Responder" /></samlp:Status>
- En este caso, el estado "Respondedor" indica que hay algún problema en el lado de AD FS, en este caso, principalmente con el "Solicitar certificado de firma" cargado en la consola de administración de ECE (Configuración de SSO > Proveedor de servicios) y el certificado cargado en el Fideicomiso de confianza de ECE en la pestaña "Firma".
- Este es el certificado que se genera con el archivo de almacén de claves Java.

Registros del servidor de aplicaciones - Nivel de seguimiento 7:

<#root>

unmarshallAndValidateResponse:

```
2022-09-21 18:18:15.002 GMT+0000 <@> ERROR <@> [392364:qtp1158258131-392364] <@> ProcessId:3272 <@> PID
2022-09-21 18:18:15.002 GMT+0000 <@> INFO <@> [392364:qtp1158258131-392364] <@> ProcessId:3272 <@> PID:
```

L10N_USER_STATUS_CODE_ERROR:

```
2022-09-21 18:18:15.002 GMT+0000 <@> ERROR <@> [392364:qtp1158258131-392364] <@> ProcessId:3272 <@> PID
at com.egain.platform.module.security.sso.handler.SAML2_0_Handler.unmarshallAndValidateResponse(SAML2_0
at com.egain.platform.module.security.sso.handler.SAML2_0_Handler.validateReqWithAttributes(SAML2_0_Han
at com.egain.platform.module.security.sso.handler.SAML2_0_Handler.validateReqWithAttributes(SAML2_0_Han
at com.egain.platform.module.security.sso.handler.OpenIDConnect_Handler.validateReqWithAttributes(OpenI
at com.egain.platform.module.security.sso.admin.SSOAdministrator.validateRequestWithAttributes(SSOAdmin
at com.egain.platform.module.security.sso.controller.SSOControllerServlet.doPost(SSOControllerServlet.j
.
.
.
.
at java.lang.Thread.run(Thread.java:834) ~[?:?]
```

```
errorCode=500&errorString=The application is not able to login the user at this time as Identity Provide
```

```
2022-09-21 18:18:15.003 GMT+0000 <@> DEBUG <@> [392364:qtp1158258131-392364] <@> ProcessId:3272 <@> PID
2022-09-21 18:18:15.003 GMT+0000 <@> DEBUG <@> [392364:qtp1158258131-392364] <@> ProcessId:3272 <@> PID
```

Resolución

- Consulte la configuración de "Solicitar certificado de firma" en la sección "Configuración del inicio de sesión único del agente: proveedor de servicios".
- Asegúrese de que el archivo .jks del almacén de claves Java generado en el paso 11 se

carga en el campo "Solicitar certificado de firma" en la consola de administración de ECE en Configuración de SSO > Seleccionar configuración 'Agente' > ficha 'Configuración de SSO' > Proveedor de servicios > Solicitar certificado de firma.
- Asegúrese de que el archivo .crt se carga en la pestaña "Firma" de la ECE Relying Party Trust (Paso 12).

Situación de solución de problemas 2

Error

- Código de error: 400
- Descripción del error: el token de respuesta de SAML no es válido: no se pudo validar la firma.

Análisis de registro

- Este error indica que hay una discordancia en el certificado entre el 'Certificado de firma de token' en ADFS y el 'Certificado del proveedor de identidad' en la configuración de SSO de ECE.

Registros del servidor de aplicaciones - Nivel de seguimiento 7:

<#root>

Entering 'validateSSOCertificate' and validating the saml response against certificate:

2022-10-07 15:27:34.523 GMT+0000 <@> DEBUG <@> [537838:qtp1158258131-537838] <@> ProcessId:3272 <@> PID
2022-10-07 15:27:34.520 GMT+0000 <@> DEBUG <@> [537838:qtp1158258131-537838] <@> ProcessId:3272 <@> PID
2022-10-07 15:27:34.521 GMT+0000 <@> DEBUG <@> [537838:qtp1158258131-537838] <@> ProcessId:3272 <@> PID
2022-10-07 15:27:34.521 GMT+0000 <@> DEBUG <@> [537838:qtp1158258131-537838] <@> ProcessId:3272 <@> PID
2022-10-07 15:27:34.521 GMT+0000 <@> DEBUG <@> [537838:qtp1158258131-537838] <@> ProcessId:3272 <@> PID
2022-10-07 15:27:34.523 GMT+0000 <@> DEBUG <@> [537838:qtp1158258131-537838] <@> ProcessId:3272 <@> PID
.....
-----END CERTIFICATE----- <@>
2022-10-07 15:27:34.523 GMT+0000 <@> INFO <@> [537838:qtp1158258131-537838] <@> ProcessId:3272 <@> PID:

Error: Could not parse certificate: java.io.IOException: Incomplete data:

2022-10-07 15:27:34.523 GMT+0000 <@> ERROR <@> [537838:qtp1158258131-537838] <@> ProcessId:3272 <@> PID
2022-10-07 15:27:34.524 GMT+0000 <@> DEBUG <@> [537838:qtp1158258131-537838] <@> ProcessId:3272 <@> PID
2022-10-07 15:27:34.525 GMT+0000 <@> DEBUG <@> [537838:qtp1158258131-537838] <@> ProcessId:3272 <@> PID
2022-10-07 15:27:34.525 GMT+0000 <@> DEBUG <@> [537838:qtp1158258131-537838] <@> ProcessId:3272 <@> PID

Signature validation failed:

2022-10-07 15:27:34.525 GMT+0000 <@> ERROR <@> [537838:qtp1158258131-537838] <@> ProcessId:3272 <@> PID
2022-10-07 15:27:34.525 GMT+0000 <@> INFO <@> [537838:qtp1158258131-537838] <@> ProcessId:3272 <@> PID:
2022-10-07 15:27:34.525 GMT+0000 <@> ERROR <@> [537838:qtp1158258131-537838] <@> ProcessId:3272 <@> PID
2022-10-07 15:27:34.525 GMT+0000 <@> DEBUG <@> [537838:qtp1158258131-537838] <@> ProcessId:3272 <@> PID

Resolución

- El error que aparece en el fragmento de registro, 'No se pudo analizar el certificado: java.io.IOException: Incomplete data', indica que el contenido de 'Certificado del proveedor de identidad' no se ha introducido correctamente
- Para resolver esto: en la Administración de AS FS > AD FS > Servicio > Certificados > Firma de token > Exportar este certificado > abra en un editor de texto > copie todo el contenido > pegue en el campo 'Certificado del proveedor de identidad' en la configuración de SSO > Guardar.
- Consulte la configuración del 'Certificado del proveedor de identidad' en la sección 'Configuración del inicio de sesión único del agente - Proveedor de identidad' (Paso 15).

Situación de solución de problemas 3

Error

- Código de error: 401-114
- Descripción del error: identidad de usuario no encontrada en el atributo SAML.

Análisis de registro

Registros del servidor de aplicaciones - Nivel de seguimiento 7:

<#root>

getSSODataFromSAMLToken:

2024-02-01 01:44:32.081 GMT+0000 <@> ERROR <@> [1220:qtp815320891-1220] <@> ProcessId:7716 <@> PID:1 <@
2024-02-01 01:44:32.081 GMT+0000 <@> TRACE <@> [1220:qtp815320891-1220] <@> ProcessId:7716 <@> PID:1 <@

L10N_USER_IDENTIFIER_NOT_FOUND_IN_ATTRIBUTE:

2024-02-01 01:44:32.081 GMT+0000 <@> ERROR <@> [1220:qtp815320891-1220] <@> ProcessId:7716 <@> PID:1 <@
com.egain.platform.module.security.sso.exception.SSOLoginException: null
at com.egain.platform.module.security.sso.handler.SAML2_0_Handler.getSSODataFromSAMLToken(SAML2_0_Hand
*at com.egain.platform.module.security.sso.handler.SAML2_0_Handler.unmarshallAndValidateResponse(SAML2_*
at com.egain.platform.module.security.sso.handler.SAML2_0_Handler.validateReqWithAttributes(SAML2_0_Ha
at com.egain.platform.module.security.sso.handler.SAML2_0_Handler.validateReqWithAttributes(SAML2_0_Ha
at com.egain.platform.module.security.sso.handler.OpenIDConnect_Handler.validateReqWithAttributes(Open
at com.egain.platform.module.security.sso.admin.SSOAdministrator.validateRequestWithAttributes(SSOAdmi
at com.egain.platform.module.security.sso.controller.SSOControllerServlet.doPost(SSOControllerServlet.
.
.
.
at java.lang.Thread.run(Thread.java:830) [?:?]

errorCode=401-114&errorString=User Identity not found in SAML attribute: 'upn':

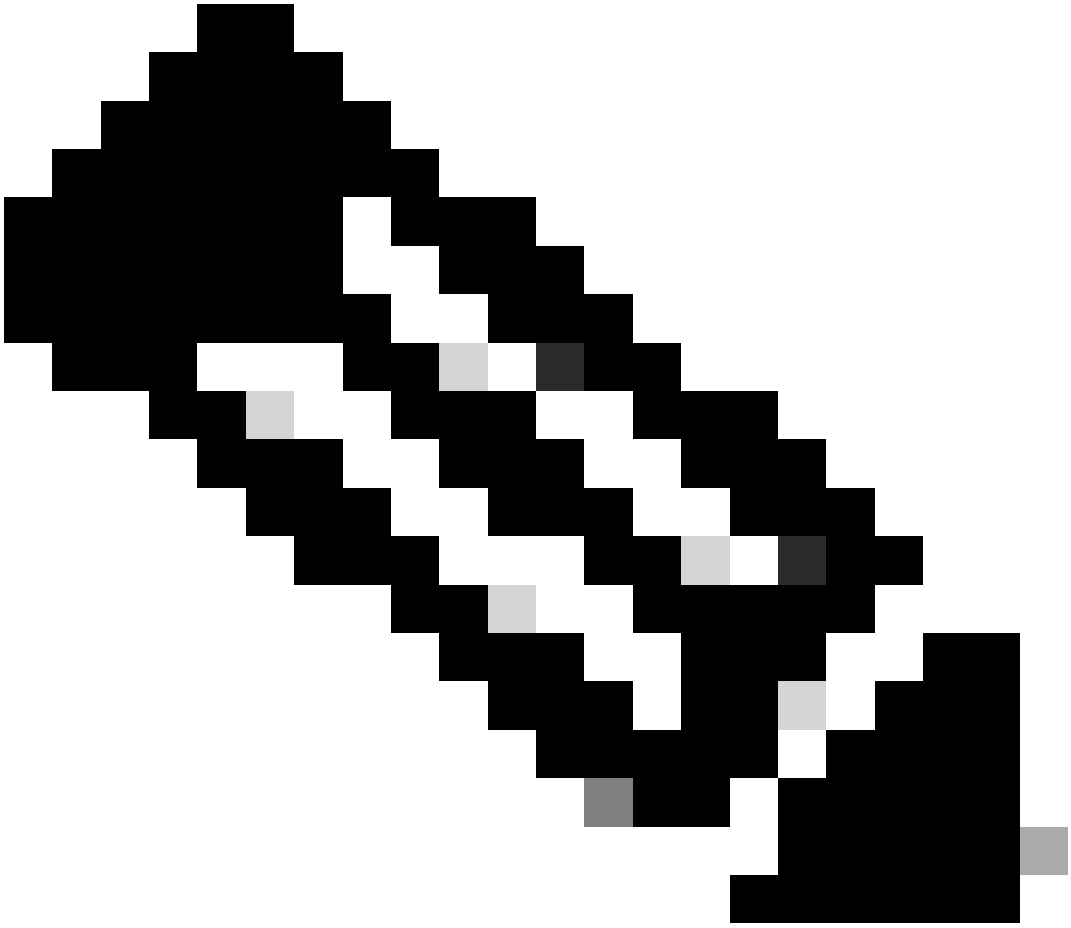
```
2024-02-01 01:44:32.083 GMT+0000 <@> DEBUG <@> [1220:qtp815320891-1220] <@> ProcessId:7716 <@> PID:1 <@
2024-02-01 01:44:32.083 GMT+0000 <@> TRACE <@> [1220:qtp815320891-1220] <@> ProcessId:7716 <@> PID:1 <@
```

Resolución

- Este error indica un problema de configuración o una falta de coincidencia en los campos 'Ubicación de identidad de usuario' y 'Nombre de atributo de identidad de usuario'.
- Verifique y corrija la 'Ubicación de identidad del usuario' y el 'Nombre de atributo de identidad del usuario' en la consola de administración de ECE, en Inicio de sesión único > Configuraciones > en el menú desplegable Seleccionar configuración, seleccione Agente > ficha Configuración de SSO > Identificar proveedor (Paso 15).

Información Relacionada

Estos son los documentos clave que debe revisar a fondo antes de iniciar cualquier instalación o integración de ECE. No se trata de una lista completa de documentos de la CEPE.



Nota:

- La mayoría de los documentos ECE tienen dos versiones. Asegúrese de descargar y utilizar las versiones correspondientes a PCCE. El título del documento es para Packaged Contact Center Enterprise o (para PCCE) o (para UCCE y PCCE) después del número de versión.
- Asegúrese de consultar la página de inicio de la documentación de Cisco Enterprise Chat y Email para ver si hay alguna actualización antes de realizar cualquier instalación, actualización o integración.
- https://www.cisco.com/c/en/us/support/customer-collaboration/cisco-enterprise-chat-email/series.html

---

ECE Versión 12.6(1)

- Guía del administrador de correo electrónico y chat empresarial

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).