Configure and Troubleshoot SSO for Agents and Partition Admin in ECE

Contents

Introduction

This document describes the steps required to configure Single Sign-On (SSO) for Agents and Partition Administrators in an ECE solution.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

Cisco Packaged Contact Center Enterprise (PCCE)

Cisco Unified Contact Center Enterprise (UCCE)

Enterprise Chat and Email (ECE)

Microsoft Active Directory

Components Used

The information in this document is based on these software and hardware versions:

UCCE Version: 12.6(1)

ECE Version: 12.6(1)

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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

Enterprise Chat and Email (ECE) consoles can be accessed outside of Finesse, however, SSO must be enabled to allow agents and supervisors to log in to ECE through Finesse.

Single Sign-On can also be configured for new partition administrators. This ensures that new users who log in to Cisco Administrator desktop are granted access to the Enterprise Chat and Email Administration Console.

Important things to note about Single Sign-On:

- The process of configuring a system for single sign-on must be performed to the Security node at the partition level by a partition user with the necessary actions: View Application Security and Manage Application Security.
- For supervisors and administrators to log into the consoles other than the Agent Console, once SSO is enabled, you must provide a valid External URL of the Application in the partition settings. See General Partition Settings for more information.
- A Java Keystore (JKS) certificate is needed to configure SSO to allow users with administrator or supervisor roles to sign in to partition 1 of ECE outside of Finesse using their SSO login credentials. Consult your IT department to receive the JKS certificate.
- A Secure Sockets Layer (SSL) certificate of Cisco IDS must be imported to all application servers in an installation. To obtain the necessary SSL certificate file, contact your IT department or Cisco IDS support.
- DB server collation for Unified CCE is case-sensitive. The username in the claim returned from the user info endpoint URL and the username in Unified CCE must be same. If they are not the same, single sign-on agents are not recognized as logged in and ECE cannot send agent availability to Unified CCE.
- Configuring SSO for Cisco IDS affects users who have been configured in Unified CCE for Single Sign-On. Ensure that the users you wish to enable for SSO in ECE are configured for SSO in Unified CCE. Consult your Unified CCE administrator for more information.

Note:

- Ensure that the users you wish to enable for SSO in ECE are configured for SSO in Unified CCE.
- This document specifies the steps to configure Relying Part Trust for ECE in a Single AD FS Deployment where Resource Federation Server and Account Federation Server are installed on the same machine.
- For a Split AD FS deployment, navigate to the ECE Install and Configure guide for the respective version.

Configuration Steps

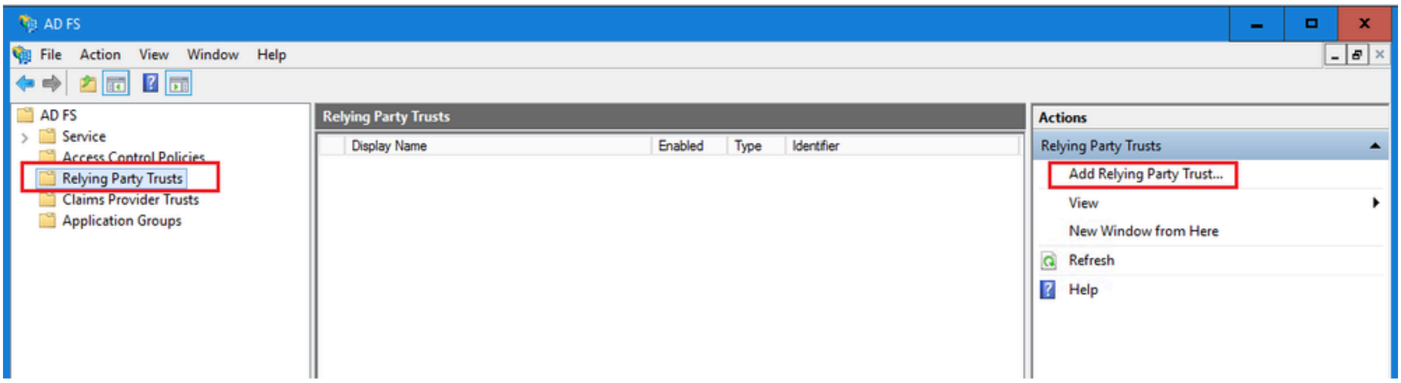
Configuring Relying Party Trust for ECE

Step 1

Open **AD FS** Management console and navigate to AD FS > Trust Relationships > Relying Party Trust.

Step 2

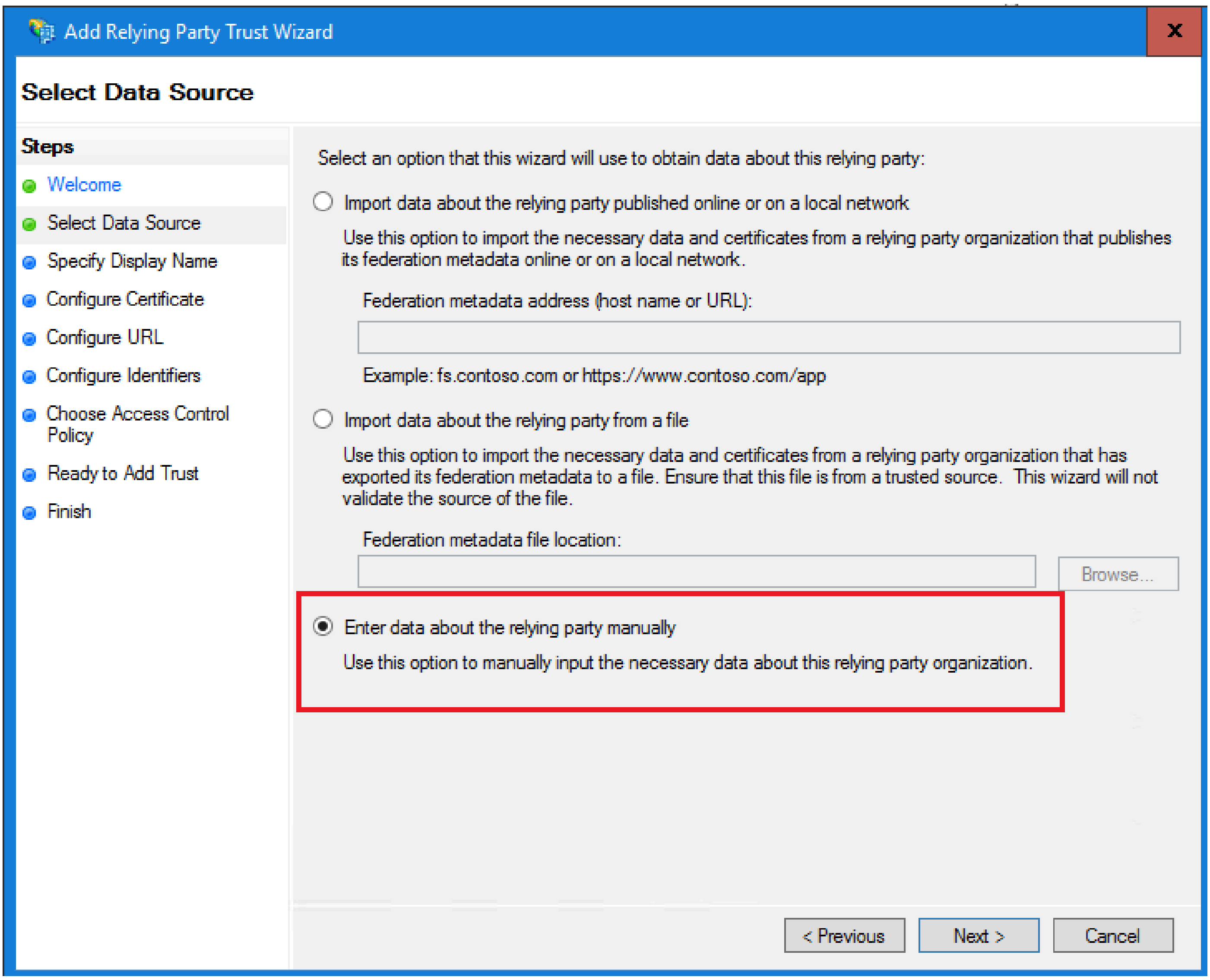
In the Actions section, click on **Add Relying Party Trust...**



Step 3

In the Add Relying Party Trust wizard, click on Start and complete the next steps:

a. In the Select Data Source page, select the **Enter data about the reply party manually** option and click Next.



Select Data Source

Select an option that this wizard will use to obtain data about this relying party:

○ Import data about the relying party published online or on a local network

Use this option to import the necessary data and certificates from a relying party organization that publishes its federation metadata online or on a local network.

Federation metadata address (host name or URL):

Example: fs.contoso.com or https://www.contoso.com/app

○ Import data about the relying party from a file

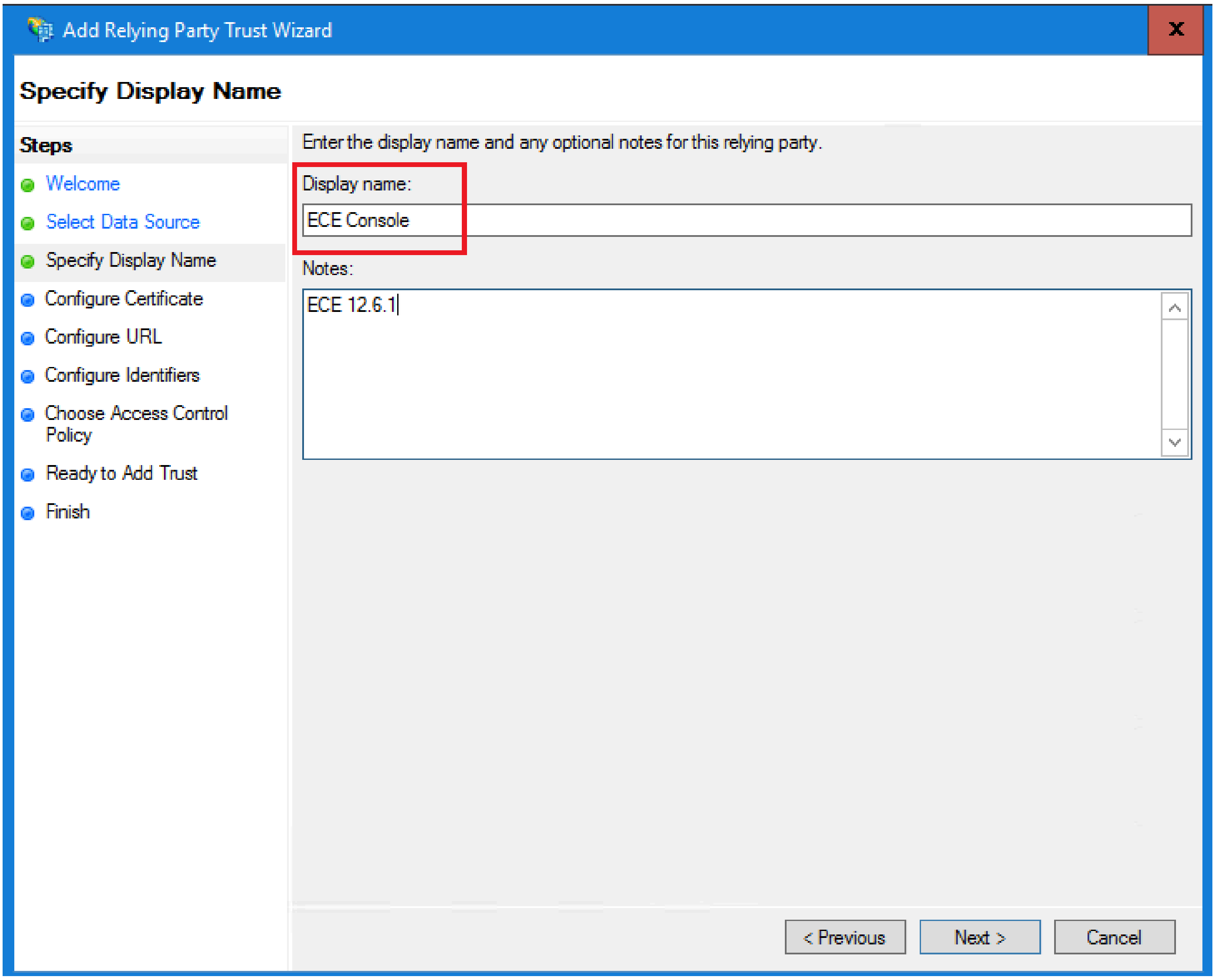
Use this option to import the necessary data and certificates from a relying party organization that has exported its federation metadata to a file. Ensure that this file is from a trusted source. This wizard will not validate the source of the file.

Federation metadata file location:

● Enter data about the relying party manually

Use this option to manually input the necessary data about this relying party organization.

b. In the Specify Display Name page, provide a Display name for the relying party. Click Next



Enter the display name and any optional notes for this relying party.

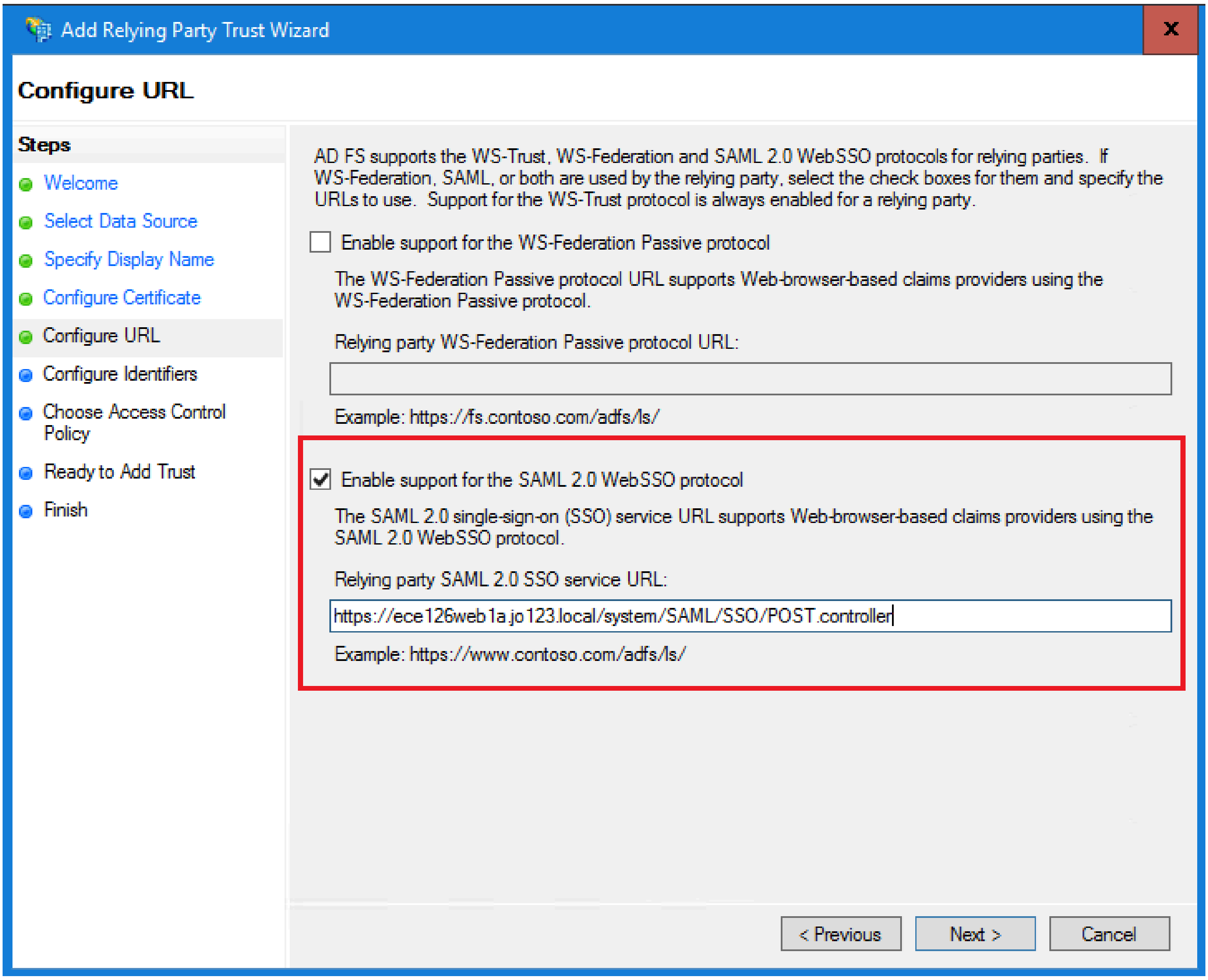
Display name: ECE Console

Notes: ECE 12.6.1

c. In the Configure URL page:

i. Select the **Enable support for the SAML 2.0 Web SSO protocol** option.

ii. In the *Relying Party SAML 2.0 SSO server URL* field provide the URL in the format: ***https://<Web-Server-Or-Load-Balancer-FQDN>/system/SAML/SSO/POST.controller***



Add Relying Party Trust Wizard

Configure URL

Steps
- Welcome
- Select Data Source
- Specify Display Name
- Configure Certificate
- Configure URL
- Configure Identifiers
- Choose Access Control Policy
- Ready to Add Trust
- Finish

AD FS supports the WS-Trust, WS-Federation and SAML 2.0 WebSSO protocols for relying parties. If WS-Federation, SAML, or both are used by the relying party, select the check boxes for them and specify the URLs to use. Support for the WS-Trust protocol is always enabled for a relying party.

□ Enable support for the WS-Federation Passive protocol

The WS-Federation Passive protocol URL supports Web-browser-based claims providers using the WS-Federation Passive protocol.

Relying party WS-Federation Passive protocol URL:

Example: https://fs.contoso.com/adfs/ls/

☑ Enable support for the SAML 2.0 WebSSO protocol

The SAML 2.0 single-sign-on (SSO) service URL supports Web-browser-based claims providers using the SAML 2.0 WebSSO protocol.

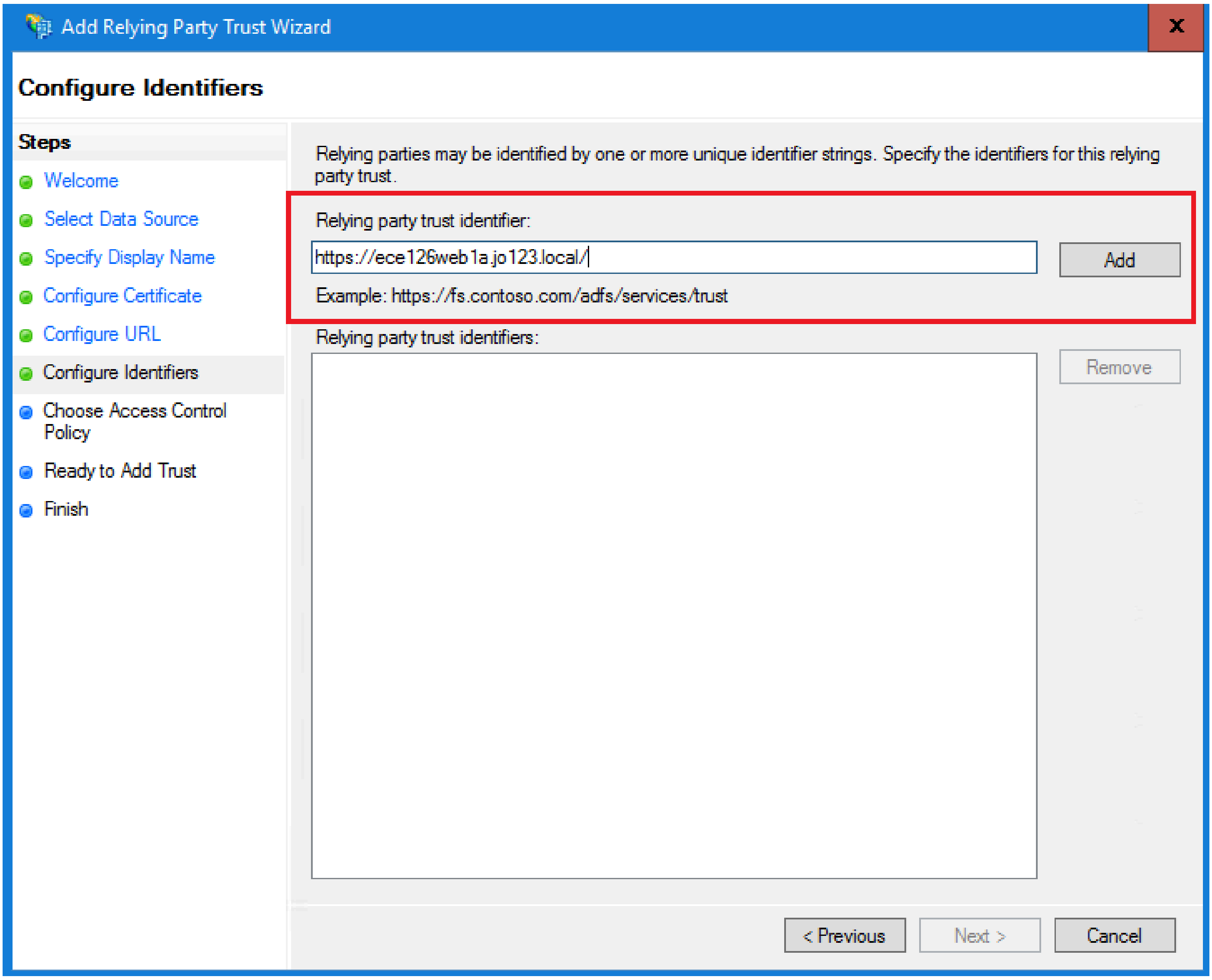
Relying party SAML 2.0 SSO service URL:

https://ece126web1a.jo123.local/system/SAML/SSO/POST.controller

Example: https://www.contoso.com/adfs/ls/

d. In the Configure Identifiers page, provide the **Relying party trust identifier** and click Add.

- Value must be in the format: *https://<Web-Server-Or-Load-Balancer-FQDN>/*



Add Relying Party Trust Wizard

Configure Identifiers

Relying parties may be identified by one or more unique identifier strings. Specify the identifiers for this relying party trust.

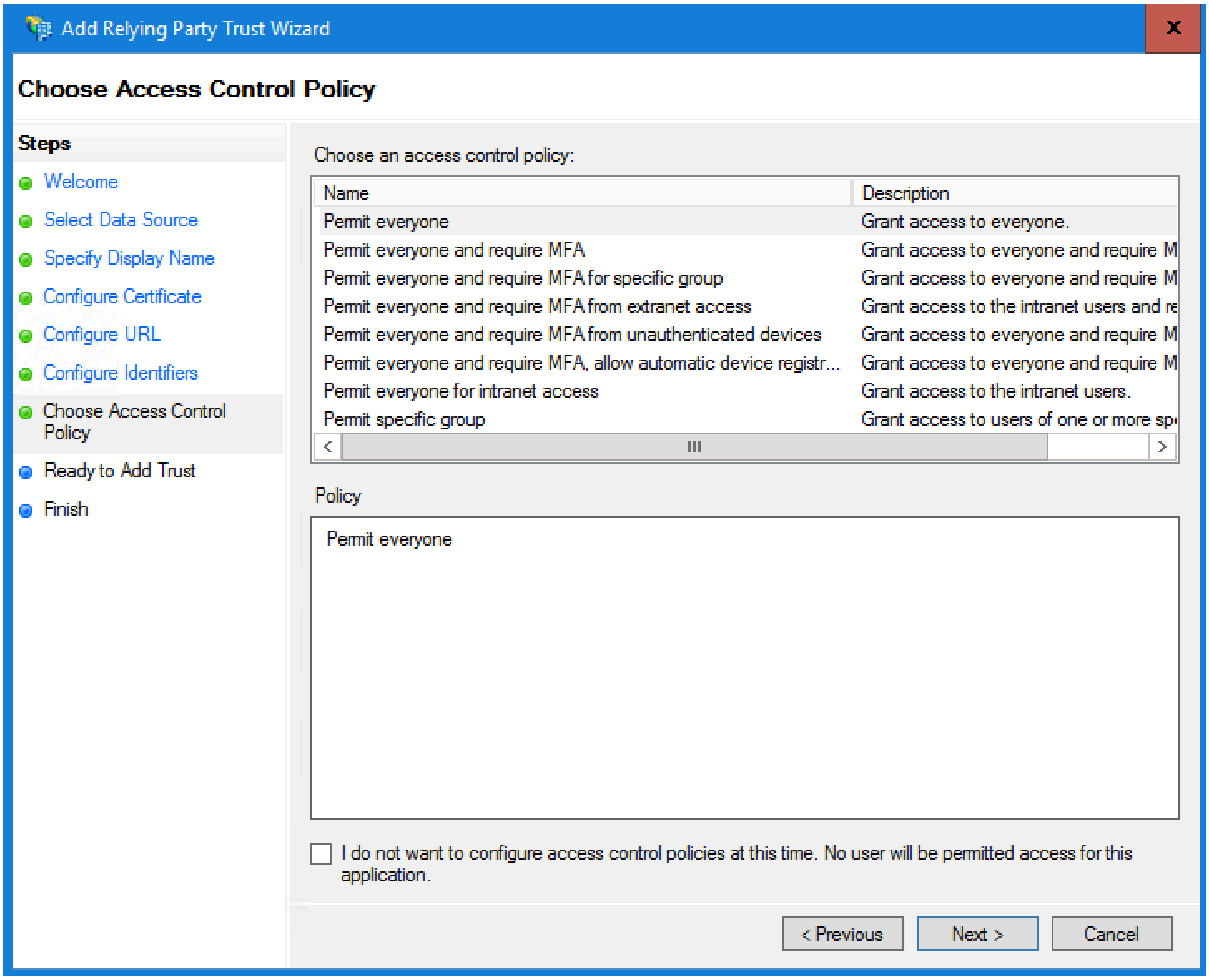
Relying party trust identifier:

https://ece126web1a.jo123.local/

Example: https://fs.contoso.com/adfs/services/trust

Relying party trust identifiers:

e. In the *Choose Access Control Policy* page, click next with the default value 'Permit everyone' policy.



Choose Access Control Policy

Choose an access control policy:

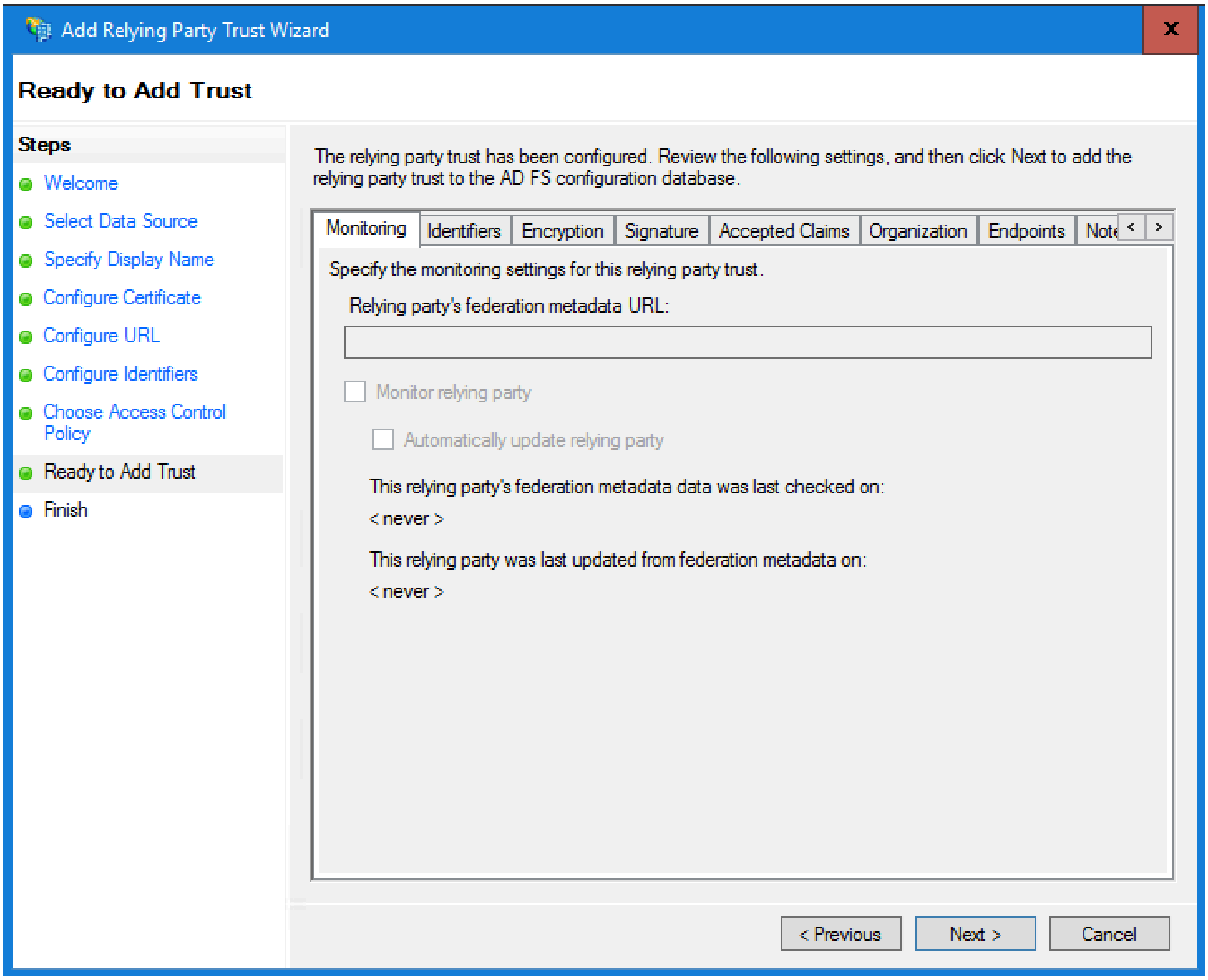
Name	Description
Permit everyone	Grant access to everyone.
Permit everyone and require MFA	Grant access to everyone and require M
Permit everyone and require MFA for specific group	Grant access to everyone and require M
Permit everyone and require MFA from extranet access	Grant access to the intranet users and re
Permit everyone and require MFA from unauthenticated devices	Grant access to everyone and require M
Permit everyone and require MFA, allow automatic device registr...	Grant access to everyone and require M
Permit everyone for intranet access	Grant access to the intranet users.
Permit specific group	Grant access to users of one or more sp

Policy

Permit everyone

□ I do not want to configure access control policies at this time. No user will be permitted access for this application.

f. In the *Ready to Add Trust* page, click Next.



Ready to Add Trust

The relying party trust has been configured. Review the following settings, and then click Next to add the relying party trust to the AD FS configuration database.

Specify the monitoring settings for this relying party trust.

Relying party's federation metadata URL:

□ Monitor relying party

□ Automatically update relying party

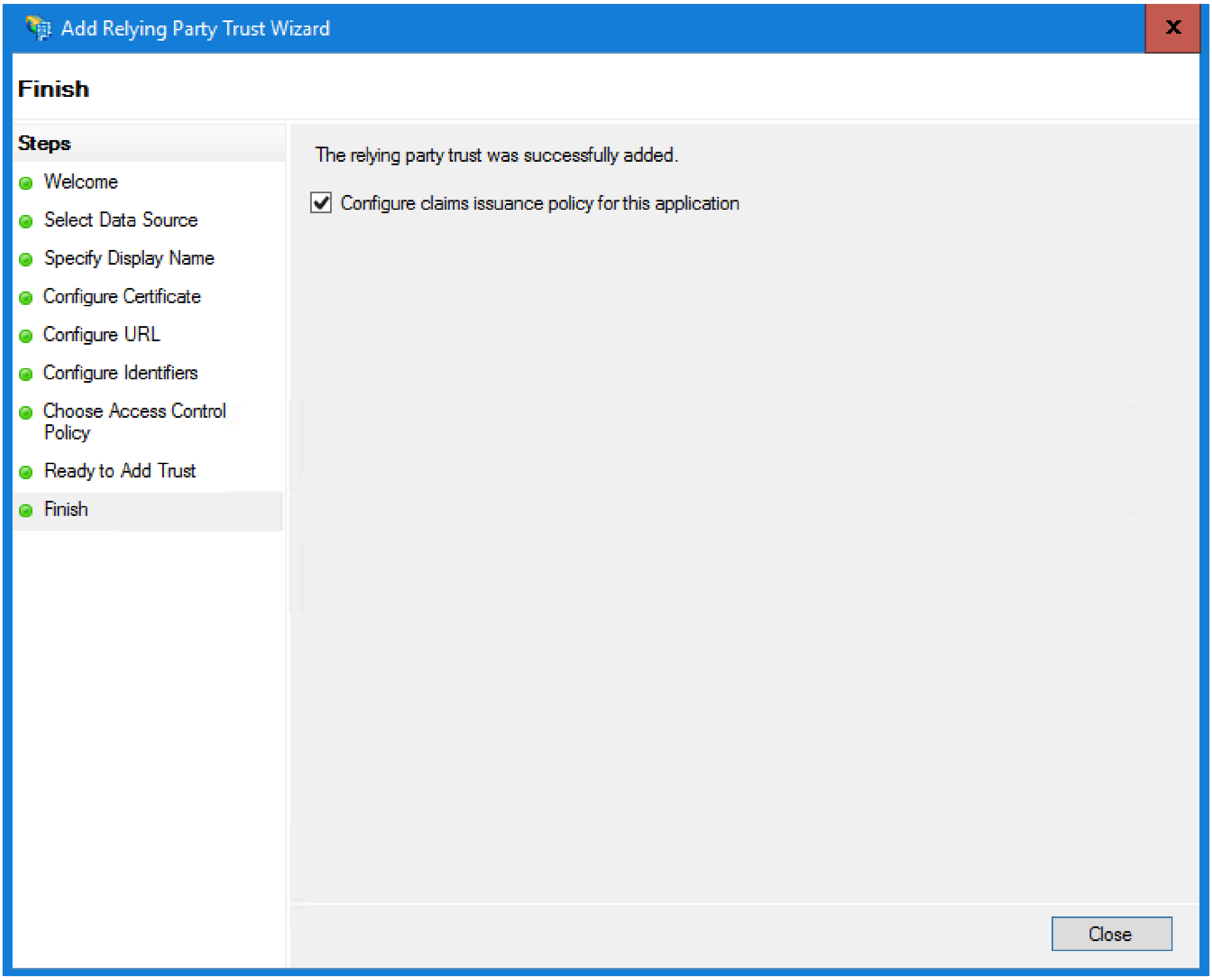
This relying party's federation metadata data was last checked on:

< never >

This relying party was last updated from federation metadata on:

< never >

g. Once the relying party trust is successfully added, click Close.

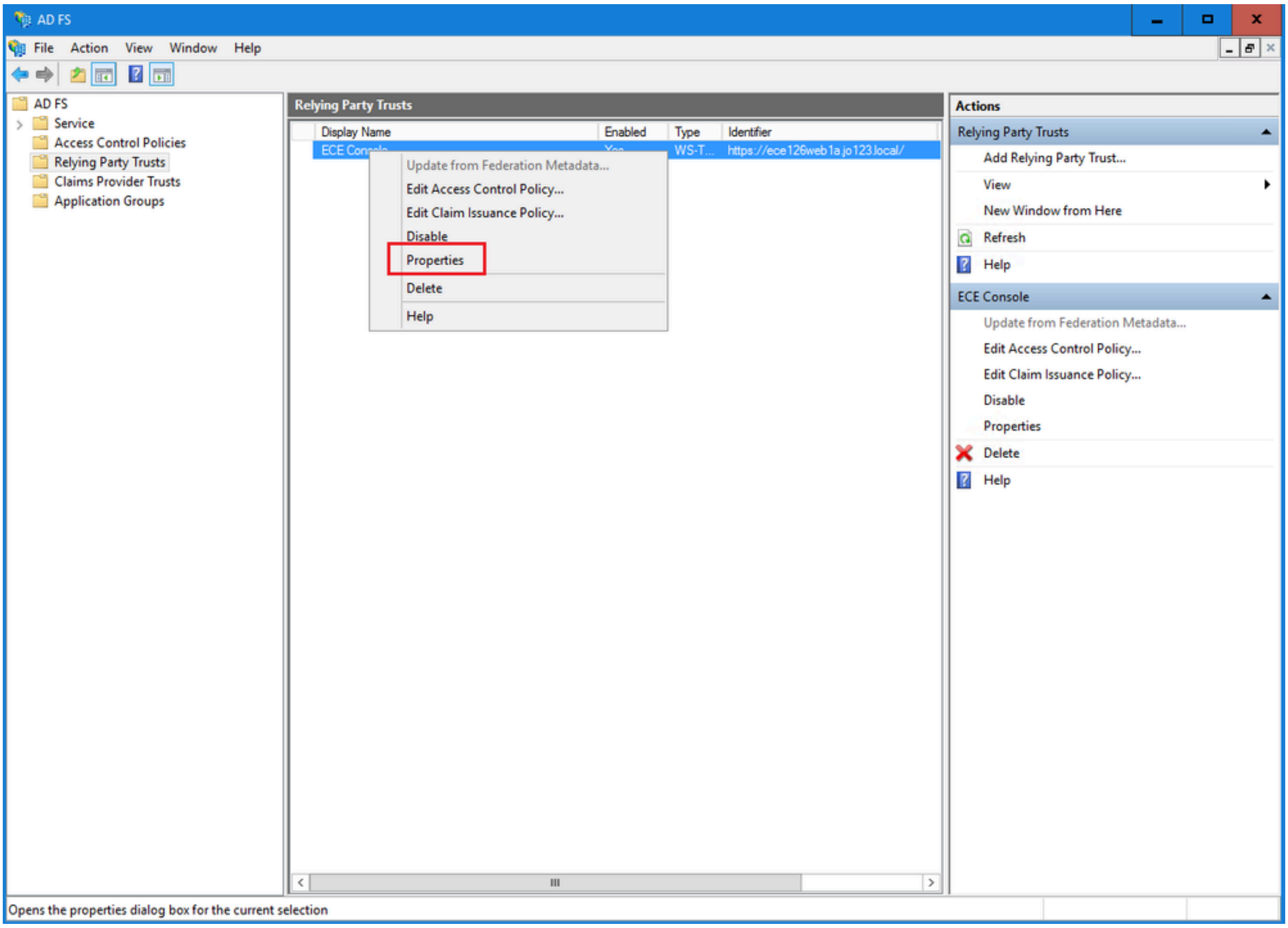


The relying party trust was successfully added.

☑ Configure claims issuance policy for this application

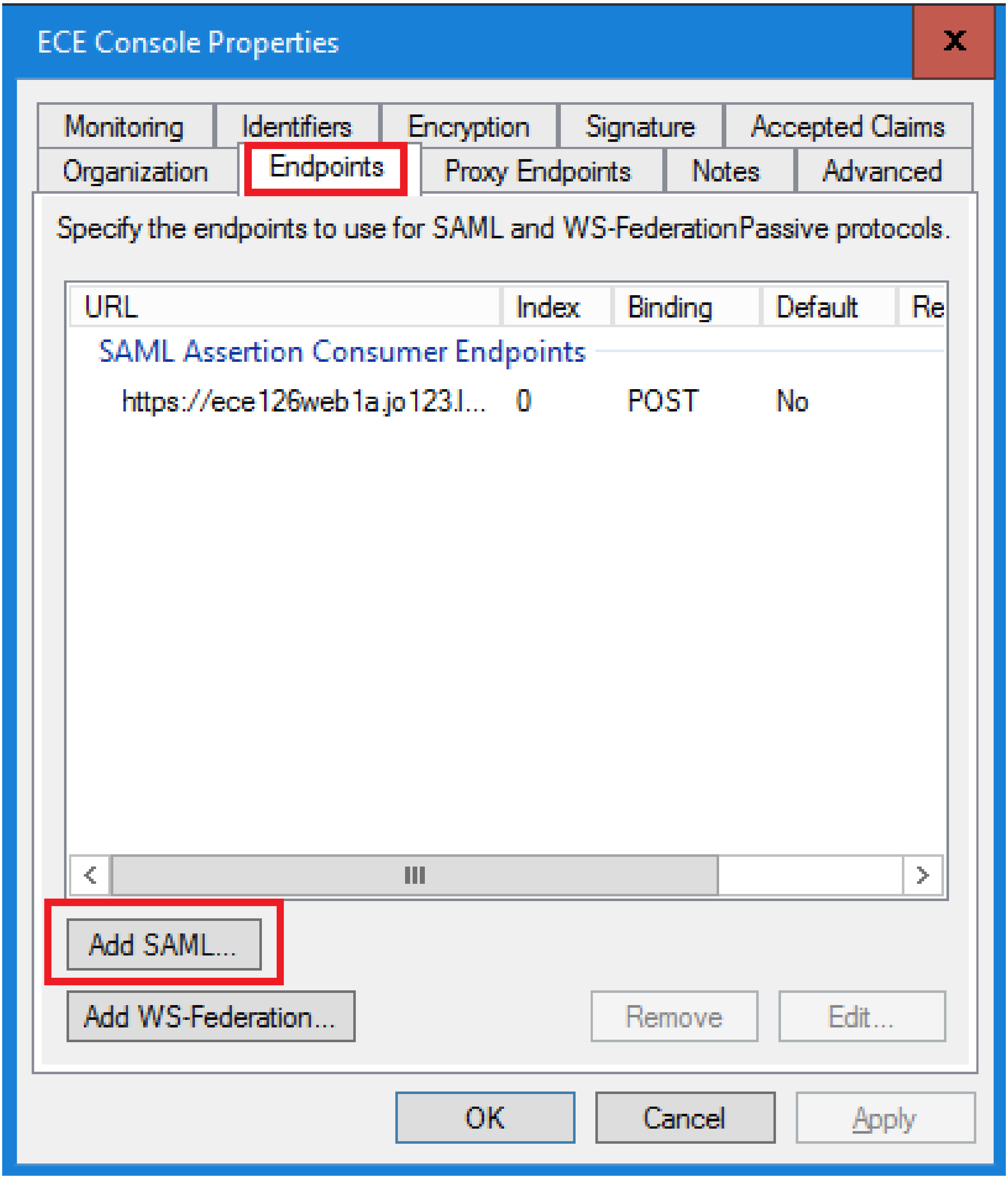
Step 4

In the **Relying Provider Trusts** list, select the Relying Party trust created for ECE and in the actions section click **Properties**.


AD FS
File Action View Window Help
AD FS
Service
Access Control Policies
Relying Party Trusts
Claims Provider Trusts
Application Groups
Relying Party Trusts
Display Name
Enabled
Type
Identifier
ECE Console
Yes
WS-T...
https://ece126web1a.jo123.local/
Update from Federation Metadata...
Edit Access Control Policy...
Edit Claim Issuance Policy...
Disable
Properties
Delete
Help
Actions
Relying Party Trusts
Add Relying Party Trust...
View
New Window from Here
Refresh
Help
ECE Console
Update from Federation Metadata...
Edit Access Control Policy...
Edit Claim Issuance Policy...
Disable
Properties
Delete
Help
Opens the properties dialog box for the current selection

Step 5

In the Properties window, navigate to the **Endpoints** tab and click the **Add SAML..** button



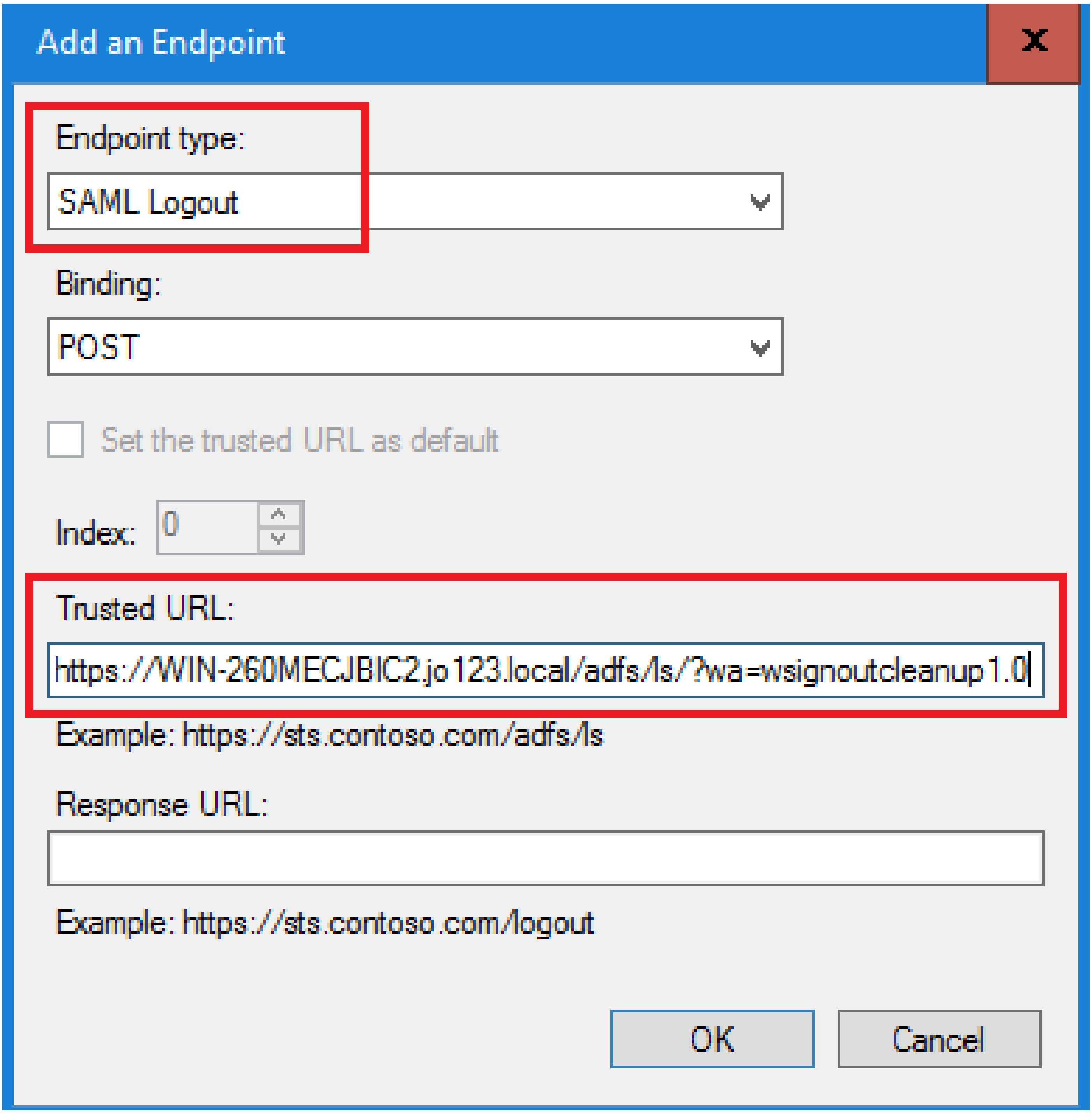
Specify the endpoints to use for SAML and WS-FederationPassive protocols.

URL	Index	Binding	Default	Re
SAML Assertion Consumer Endpoints				
https://ece126web1a.jo123.l...	0	POST	No	

Step 6

In the **Add an Endpoint** window, configure as noted:

1. Select the Endpoint type as *SAML Logout*.
2. Specify the Trusted URL as *https://<ADFS-server-FQDN>/adfs/ls/?wa=wsignoutcleanup1.0*
3. Click OK.



Add an Endpoint

Endpoint type:

SAML Logout

Binding:

POST

□ Set the trusted URL as default

Index: 0

Trusted URL:

https://WIN-260MECJBIC2.jo123.local/adfs/ls/?wa=wsignoutcleanup1.0

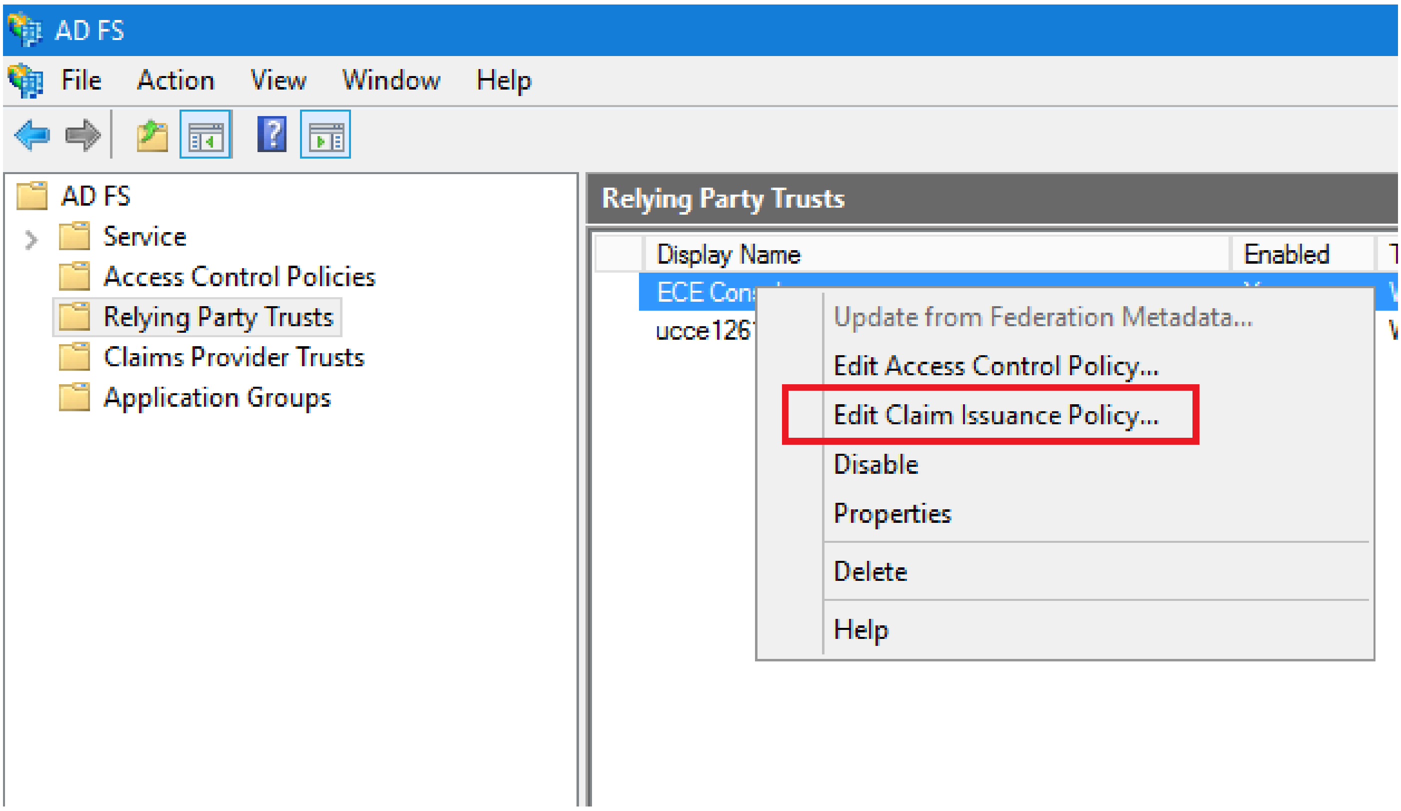
Example: https://sts.contoso.com/adfs/ls

Response URL:

Example: https://sts.contoso.com/logout

Step 7

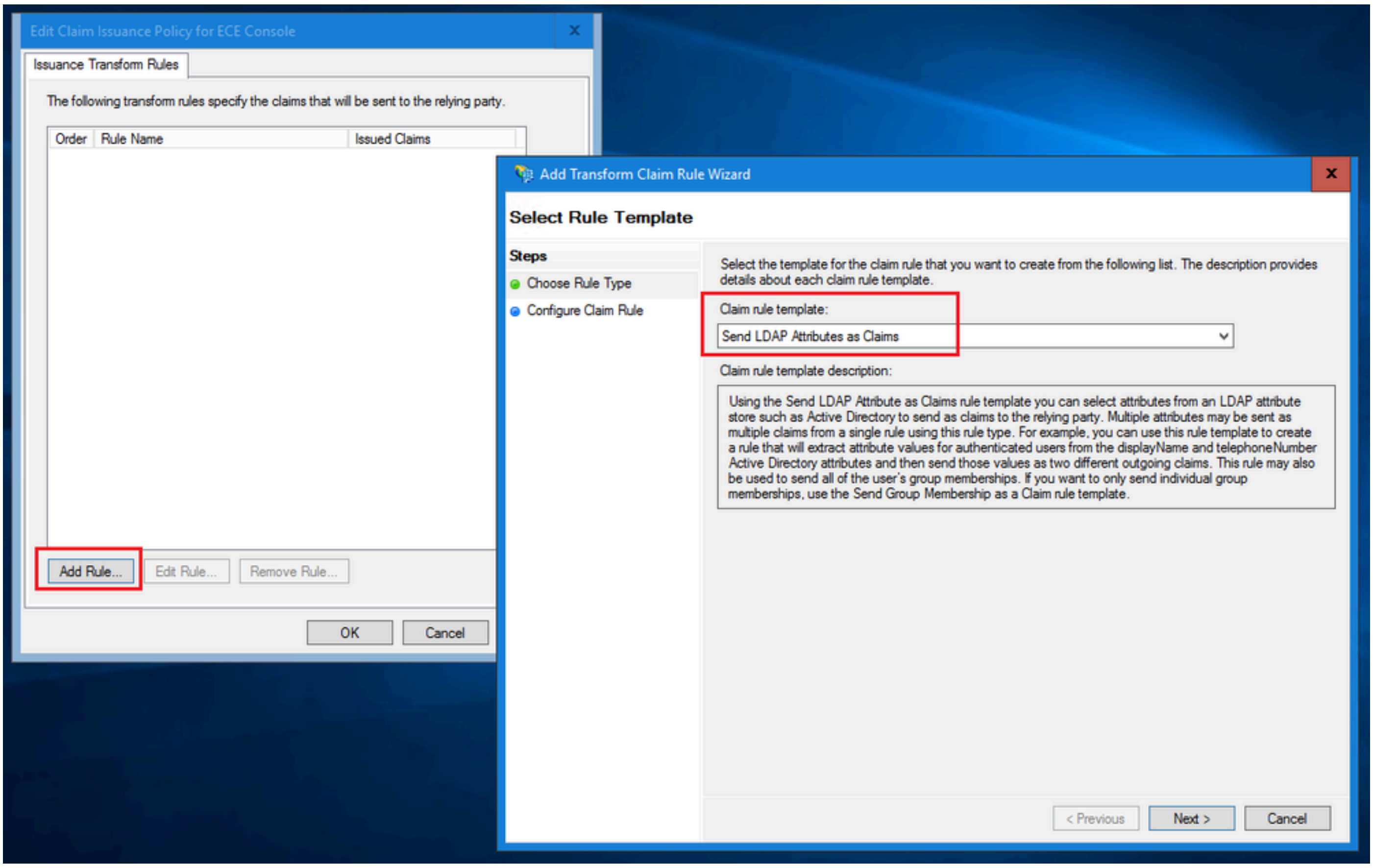
In the Relying Provider Trusts list, select the trust created for ECE, and in the actions section click **Edit Claim Insurance Policy**.



Step 8

In the Edit Claim Insurance Policy window, under the Issuance Transform Rules tab, click the **Add Rule...** button and configure as shown:

a. In the Choose Rule Type page, select **Send LDAP Attributes as Claims** from the drop down and click Next.



The following transform rules specify the claims that will be sent to the relying party.

Order	Rule Name	Issued Claims

Select Rule Template

Select the template for the claim rule that you want to create from the following list. The description provides details about each claim rule template.

Claim rule template: Send LDAP Attributes as Claims

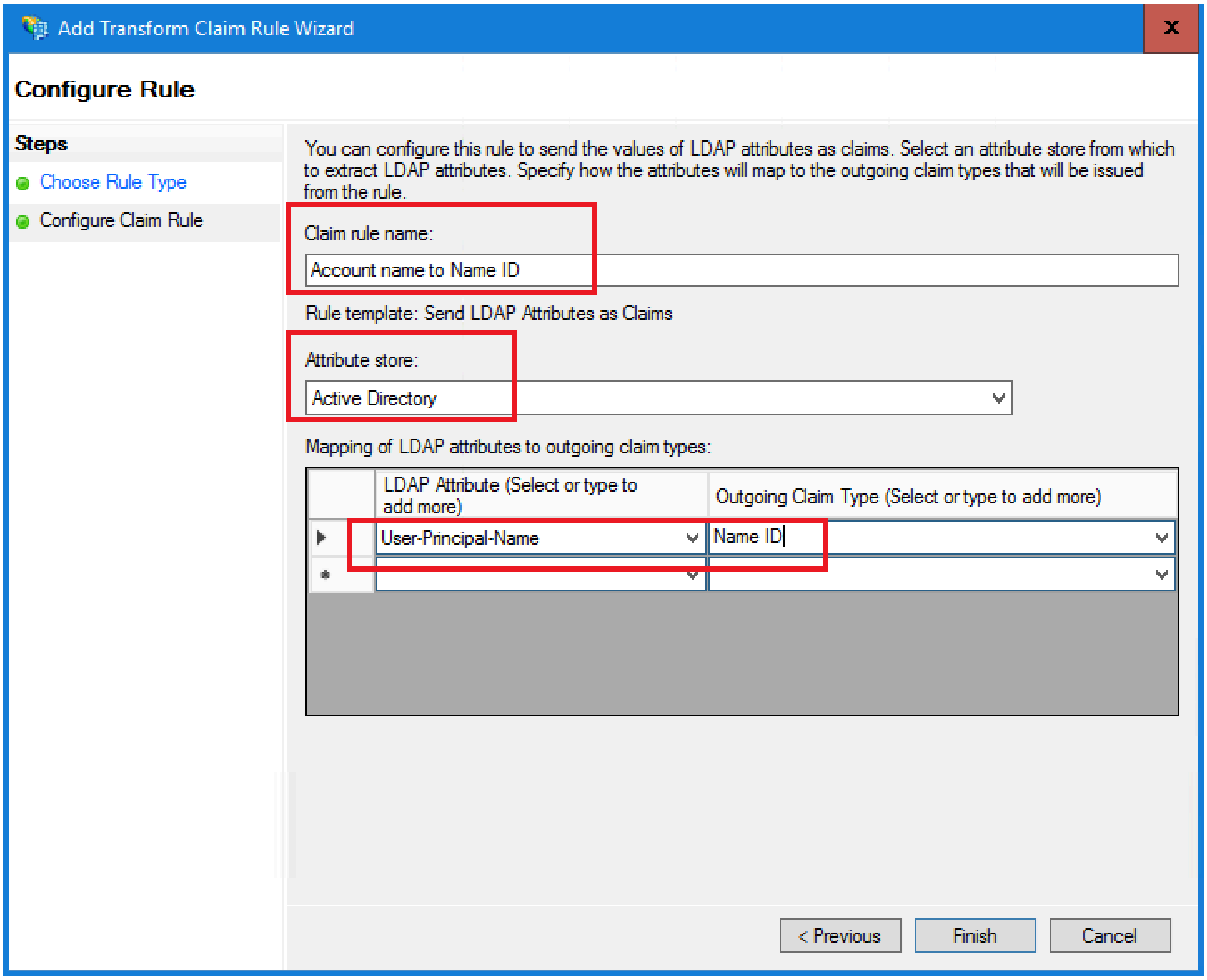
Claim rule template description:

Using the Send LDAP Attribute as Claims rule template you can select attributes from an LDAP attribute store such as Active Directory to send as claims to the relying party. Multiple attributes may be sent as multiple claims from a single rule using this rule type. For example, you can use this rule template to create a rule that will extract attribute values for authenticated users from the displayName and telephoneNumber Active Directory attributes and then send those values as two different outgoing claims. This rule may also be used to send all of the user's group memberships. If you want to only send individual group memberships, use the Send Group Membership as a Claim rule template.

b. In the Configure Claim Rule page:

1. Provide the **Claim rule name** and select the **Attribute store**.
2. Define mapping of LDAP attribute and the outgoing claim type.

- Select **Name ID** as the outgoing claim type name.
- Click Finish to go back to the Edit Claim Insurance Policy window and then click OK.



Configure 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

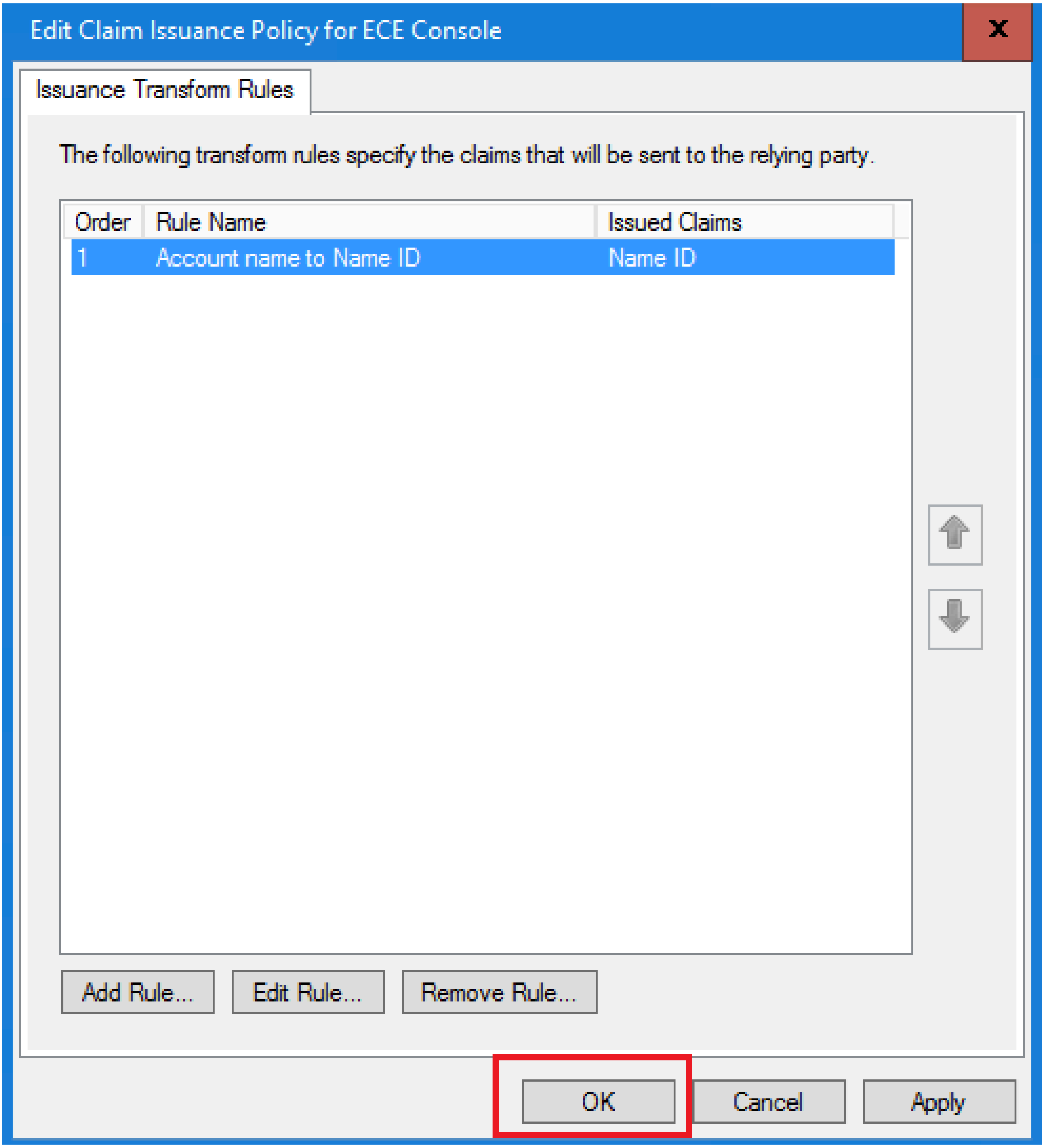
Rule template: Send LDAP Attributes as Claims

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
*		



Edit Claim Issuance Policy for ECE Console

Issuance Transform Rules

The following transform rules specify the claims that will be sent to the relying party.

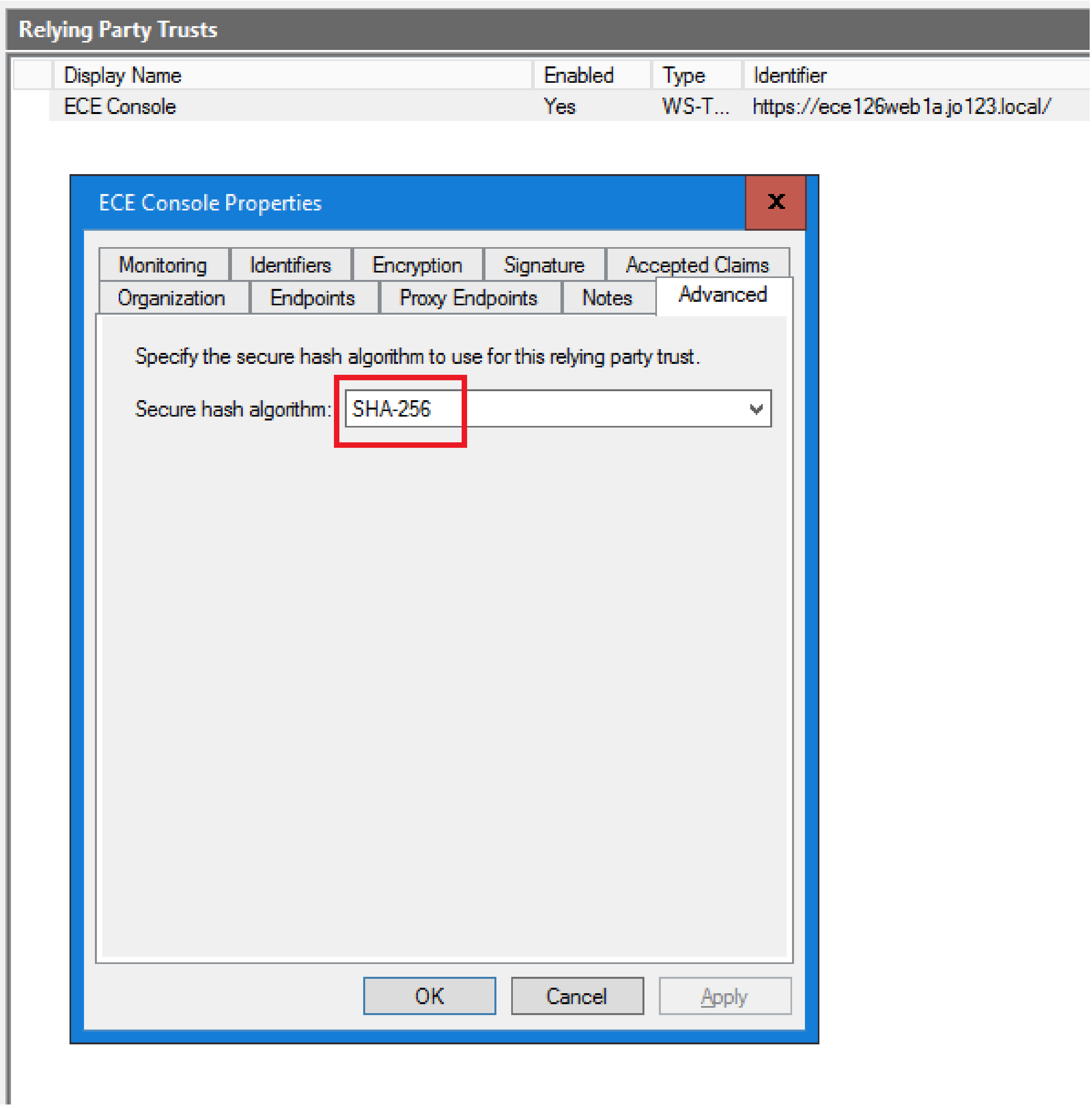
Order	Rule Name	Issued Claims
1	Account name to Name ID	Name ID

Step 9

In the Relying Provider Trusts list, double-click the ECE relying party trust which you created.

In the Properties window that opens, go to the Advanced tab and set the Secure hash algorithm to SHA-1 or SHA-256. Click OK to close the window.

Note: This value must need to match the 'Signing algorithm' value set for the 'Service Provider' under SSO Configurations in ECE



Display Name	Enabled	Type	Identifier
ECE Console	Yes	WS-T...	https://ece126web1a.jo123.local/

Specify the secure hash algorithm to use for this relying party trust.

Secure hash algorithm: SHA-256

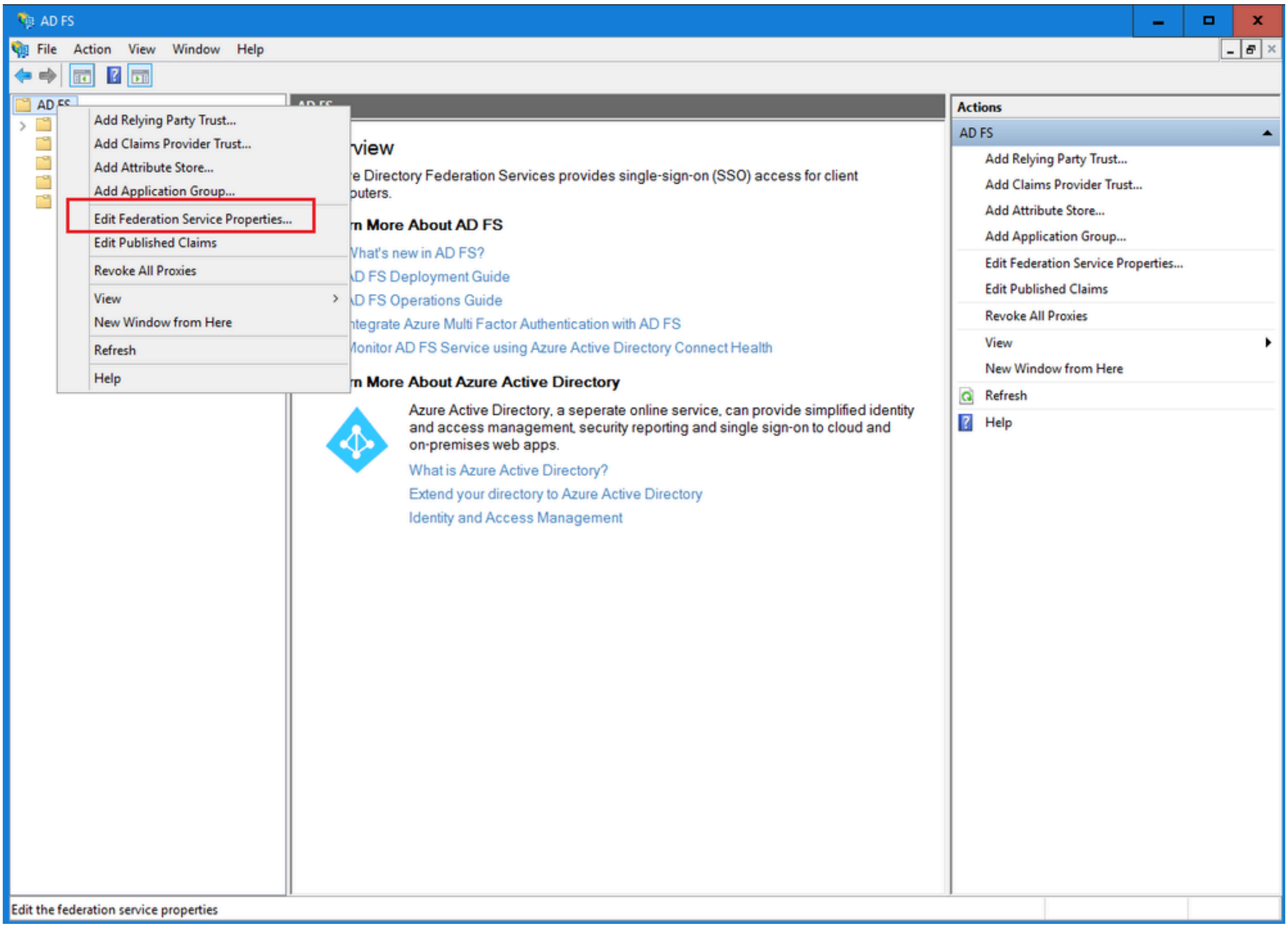
Step 10

Verify and note down the ***Federation Service Identifier*** value.

- In the AD FS Management console, select and right click AD FS > Edit Federation Service Properties > General tab > Federation Service Identifier

Note:

- This value must be added exactly as is when configuring the 'Entity ID' value for Identity Provider under SSO Configurations in ECE.
- Using http:// does NOT mean that ADFS is not secure, this is simply an identifier.



view

e Directory Federation Services provides single-sign-on (SSO) access for client puters.

n More About AD FS

Vhat's new in AD FS?

D FS Deployment Guide

D FS Operations Guide

ntegrate Azure Multi Factor Authentication with AD FS

Monitor AD FS Service using Azure Active Directory Connect Health

n More About Azure Active Directory

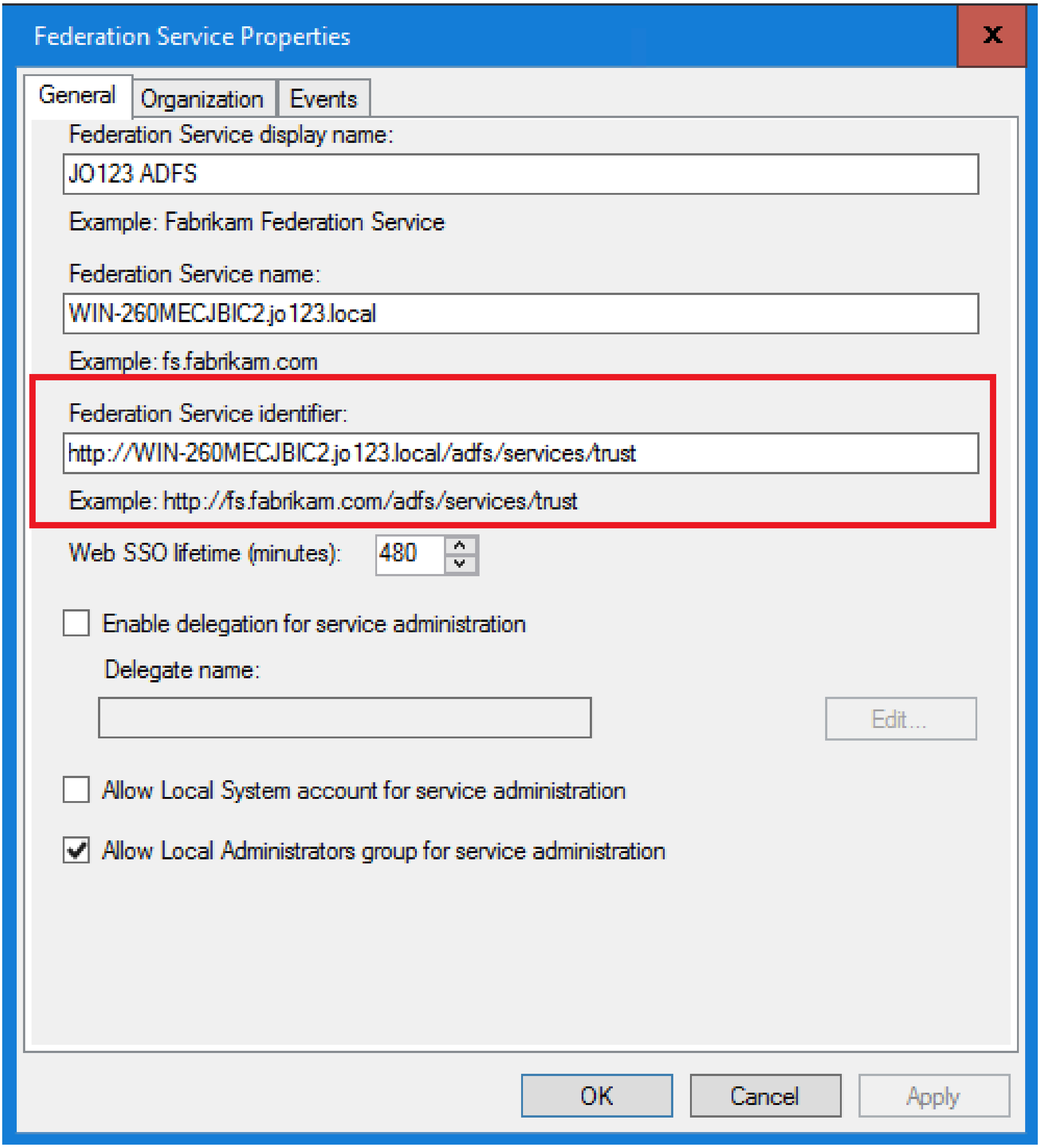
Azure Active Directory, a seperate online service, can provide simplified identity and access management, security reporting and single sign-on to cloud and on-premises web apps.

What is Azure Active Directory?

Extend your directory to Azure Active Directory

Identity and Access Management

Edit the federation service properties



Federation Service Properties

General | Organization | Events

Federation Service display name:

JO123 ADFS

Example: Fabrikam Federation Service

Federation Service name:

WIN-260MECJBIC2.jo123.local

Example: fs.fabrikam.com

Federation Service identifier:

http://WIN-260MECJBIC2.jo123.local/adfs/services/trust

Example: http://fs.fabrikam.com/adfs/services/trust

Web SSO lifetime (minutes): 480

□ Enable delegation for service administration

Delegate name:

□ Allow Local System account for service administration

☑ Allow Local Administrators group for service administration

Configuring an Identity Provider

Step 11

A Java Keystore (JKS) certificate is needed to configure SSO to allow users with administrator or supervisor roles to sign in to partition of ECE outside of Finesse using their SSO login credentials.

If you wish to configure SSO to allow users with administrator or supervisor roles to sign in to the partition of ECE outside of Finesse using their SSO login credentials, the Java Keystore (JKS) certificate must be converted to public key certificate and configured in Relying Party Trust created on the IdP server for ECE.

Consult your IT department to receive the JKS certificate.

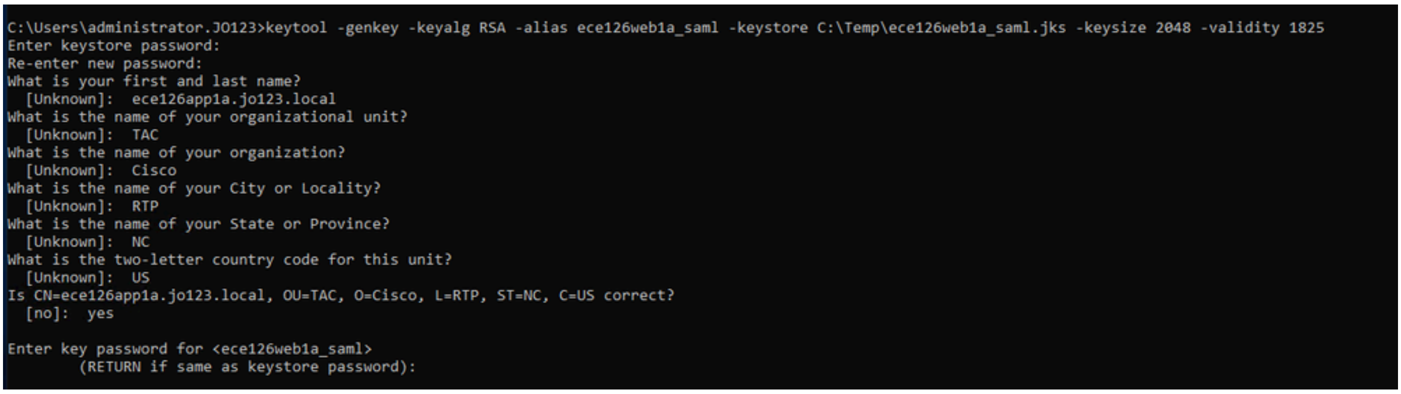
Note: These steps are applicable for systems using ADFS as the identity provider. Other identity providers can have different methods to configure public key certificate.

Here is an example of how a JKS file was generated in the lab:

a. Generate JKS:

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

Note: The keystore password, alias name, and key password entered here are used while configuring 'Service Provider' config under SSO Configurations in 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. Export the certificate:

This keytool command exports the certificate file in the.crt format with file name *ece126web1a_saml.crt* into the *C:\Temp* directory.

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

Step 12

Configuring an Identity Provider

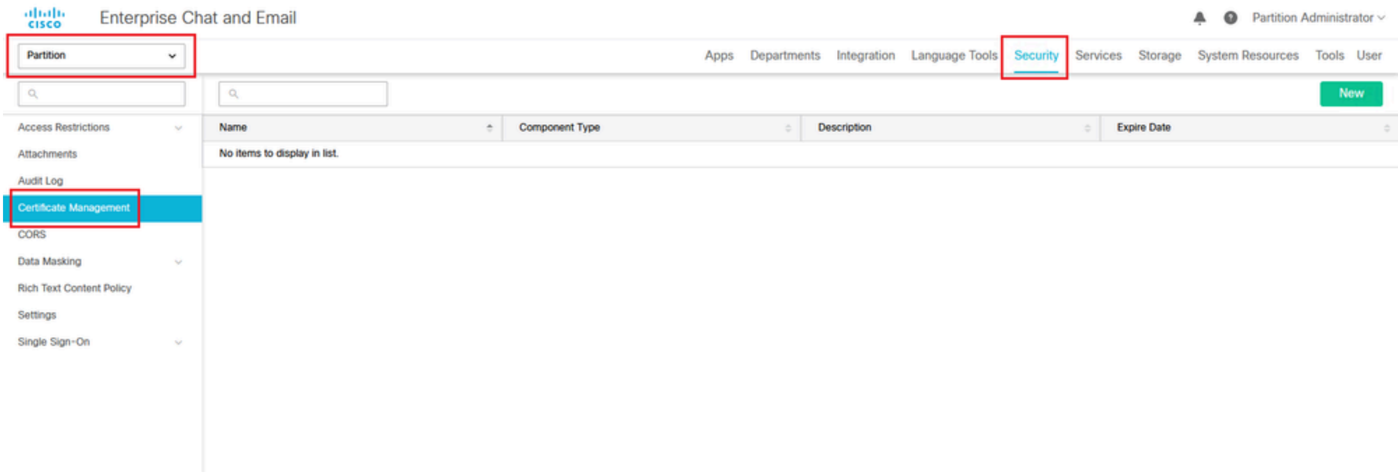
1. On the AD FS Management console, select and right click the Relying Party Trust created for ECE.
2. Open the Properties window for the trust and under the Signature tab, click the Add button.
3. Add the public certificate (.crt file generated in the previous step) and click OK.

Creating and Importing Certificates

Step 13

Before configuring SSO to use Cisco IDS for Single Sign-On for Agents, the Tomcat certificate from the Cisco IdS server must be imported into the application.

a. In the ECE Admin console, under partition-level Menu, click the **Security** option and then select **Certificate Management** from the left side Menu.

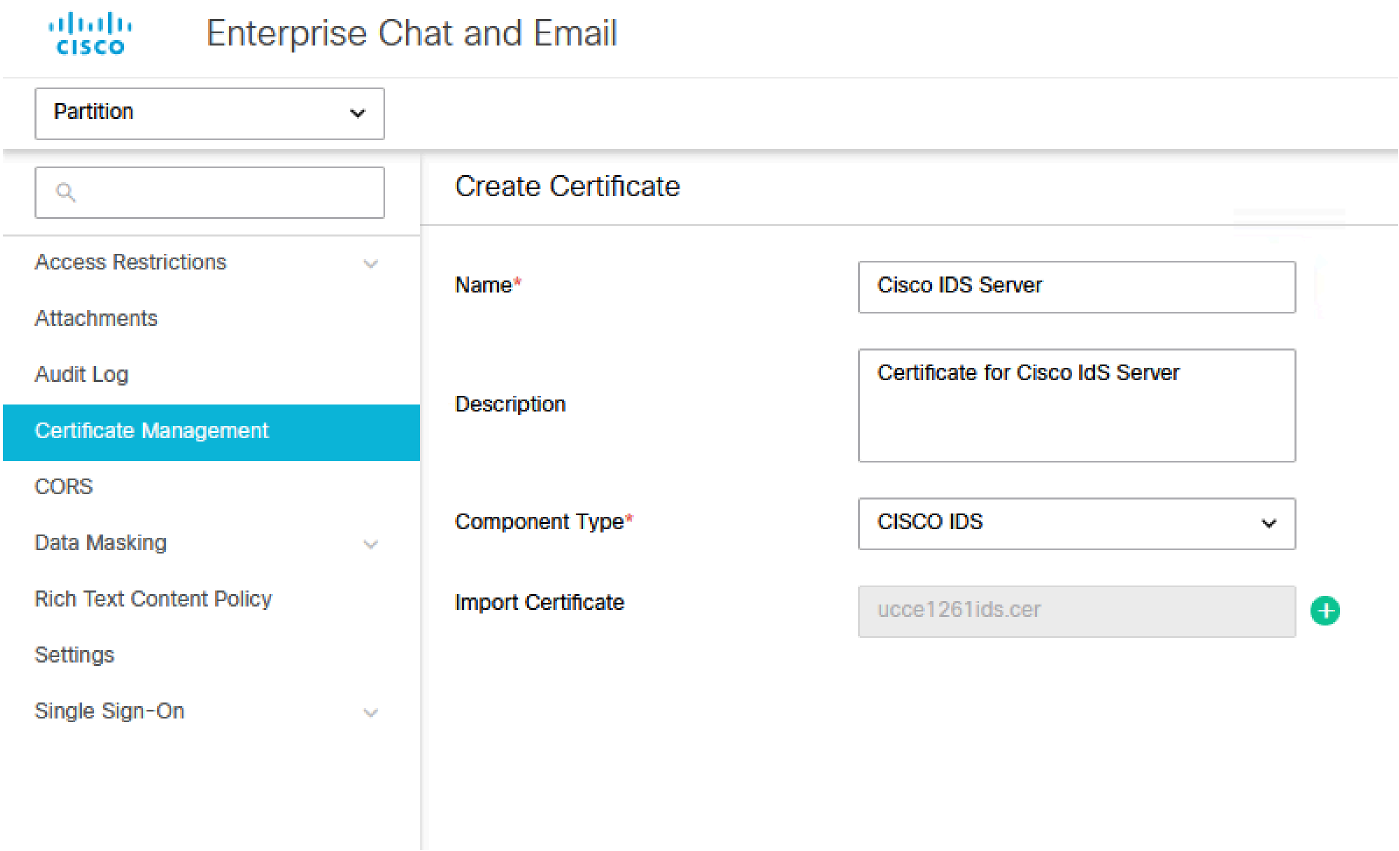


Name	Component Type	Description	Expire Date
No items to display in list.			

b. In the **Certificate Management** space, click the New button and enter the appropriate details:

- Name: Type a name for the certificate.
- Description: Add a description for the certificate.
- Component Type: Select CISCO IDS.
- Import Certificate: To import the certificate, click the Search and Add button and enter the details requested:
- Certificate file: Click the Browse button and select the certificate you wish to import. The certificates can only be imported in the .pem, .der (BINARY), or .cer/cert formats.
- Alias Name: Provide an alias for your certificate.

c. Click Save



Create Certificate

Name*: Cisco IDS Server

Description: Certificate for Cisco IdS Server

Component Type*: CISCO IDS

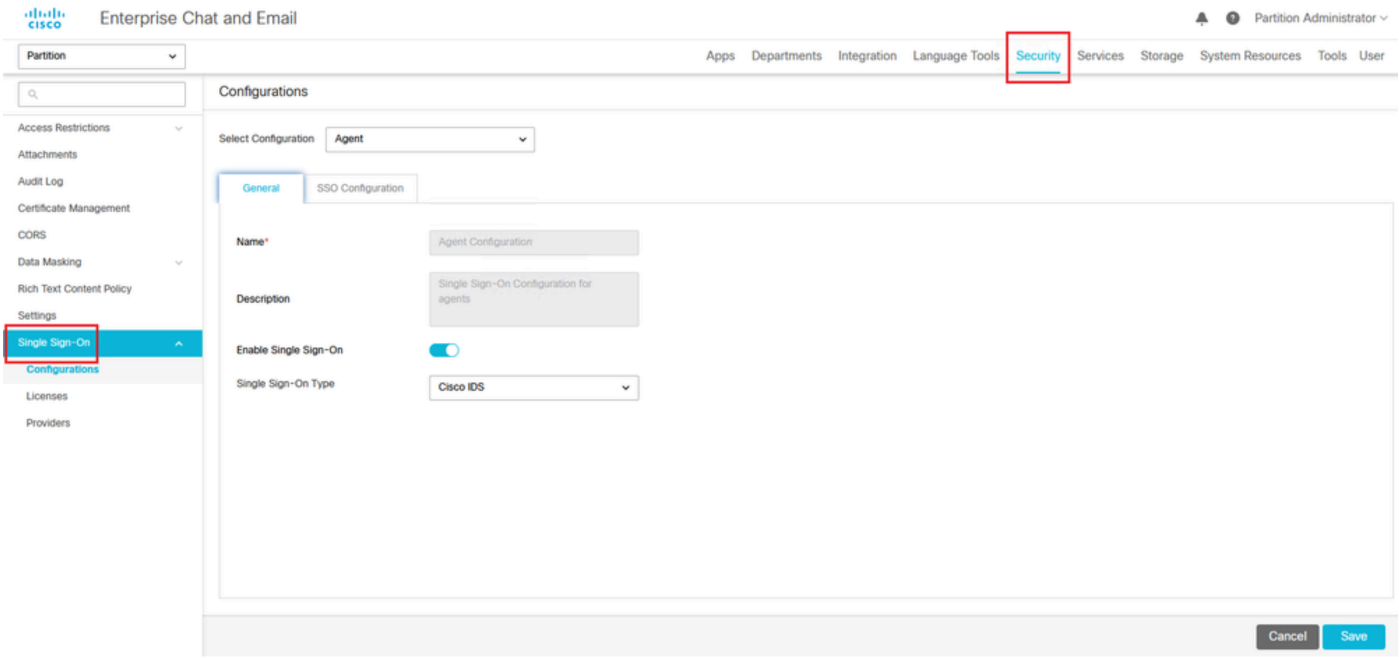
Import Certificate: ucce1261ids.cer

Configuring Agent Single Sign-On

Step 14

1. In the ECE Admin console, under partition-level Menu, click the Security option and then select **Single Sign-On** > **Configurations** from the left side Menu.
2. In the Select Configuration drop down, select **Agent** and set the configuration under the General tab:

- Enable Single Sign-On: Click the Toggle button to enable SSO.
- Single Sign-On Type: Select Cisco IDS.



Configurations

Select Configuration: Agent

Name*: Agent Configuration

Description: Single Sign-On Configuration for agents

Enable Single Sign-On

Single Sign-On Type: Cisco IDS

Step 15

Click the **SSO Configuration** tab and provide the configuration details:

a. OpenID Connect Provider

Primary User Info Endpoint URL

- The User Info Endpoint URL of the primary Cisco IDS server.
- This URL validates the user token/User Info API.
- It is in format: https://cisco-ids-1:8553/ids/v1/oauth/userinfo where cisco-ids-1 indicates the Fully Qualified Domain Name (FQDN) of the Primary Cisco IDS server.

User Identity Claim Name

- The name of the claim returned by the User Info Endpoint URL, which identifies the username in Unified or Packaged CCE.
- The claim name and the username in Unified or Packaged CCE must match.
- This is one of the claims obtained in response to the Bearer token validation.
- If the username of agents in Unified or Packaged CCE matches the User Principal Name, provide “upn” as the value for User Identity Claim name field.
- If username of agents in Unified or Packaged CCE matches with the SAM Account Name, provide “sub” as the value for User Identity Claim name field.

Secondary User Info Endpoint URL

- The secondary user Info Endpoint URL of the Cisco IDS server.
- It is in format: ***https://cisco-ids-2:8553/ids/v1/oauth/userinfo*** where cisco-ids-2 indicates the Fully Qualified Domain Name (FQDN) of the Secondary Cisco IDS server.

User Info Endpoint URL Method

- The HTTP method used by ECE for making Bearer token validation calls to the User Info Endpoint URL.
- Select POST from the list of options presented (POST is selected here to match the IDS server’s method).

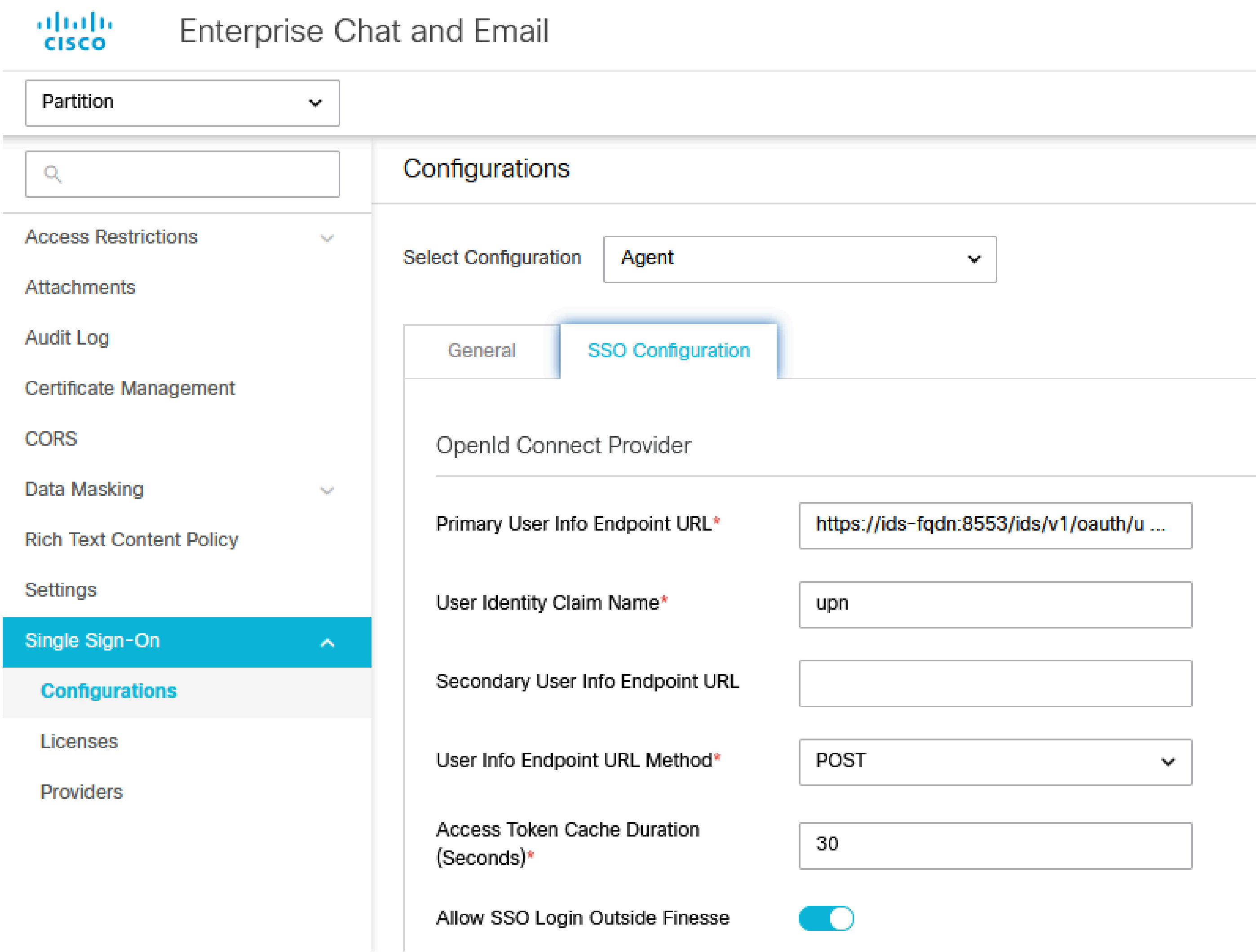
POST: Method used to send data to the Cisco IDS server at the specified endpoint.

Access Token Cache Duration (Seconds)

- The duration, in seconds, for which a Bearer token must be cached in ECE.
- Bearer tokens for which validation calls are successful are only stored in caches. (Minimum value: 1; maximum value 30)

Allow SSO Login Outside Finesse

- Click this Toggle button if you wish to allow users with administrator or supervisor roles to sign into the partition of ECE outside of Finesse using their SSO login credentials.
- If enabled, information under the Identity Provider and Service Provider sections must be provided.
- This requires that your IdP configuration allows for a shared IdP server.



Select Configuration: Agent

Primary User Info Endpoint URL*: https://ids-fqdn:8553/ids/v1/oauth/u ...

User Identity Claim Name*: upn

Secondary User Info Endpoint URL:

User Info Endpoint URL Method*: POST

Access Token Cache Duration (Seconds)*: 30

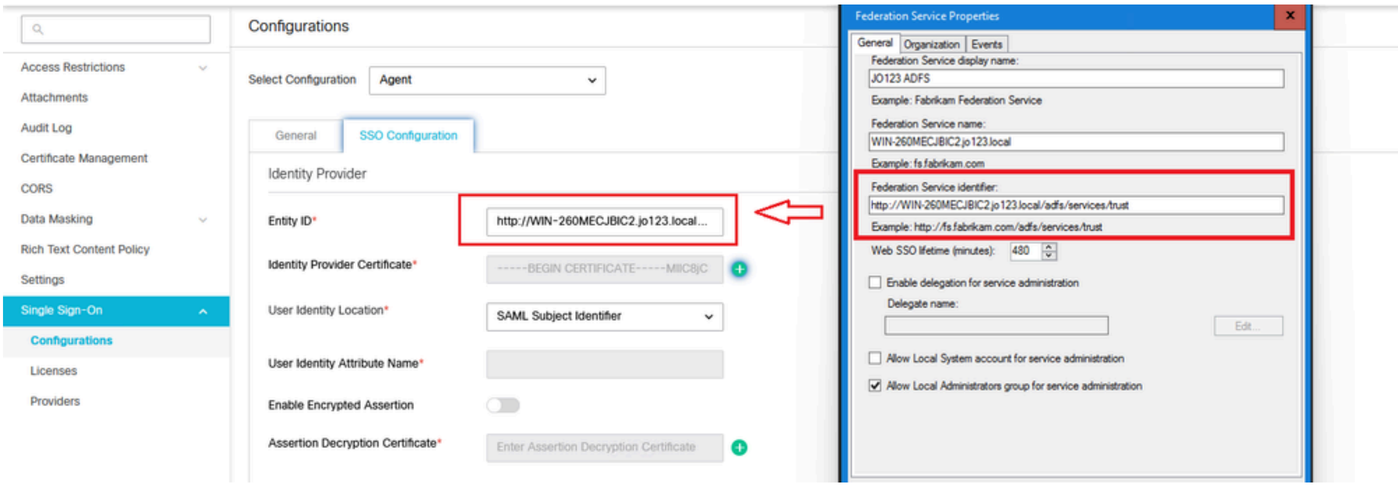
Allow SSO Login Outside Finesse: ●

b. Identity Provider

Entity ID

- Entity ID of the IdP server.

Note: This value must match exactly as the 'Federation Service Identifier' value in the AD FS Management console.



Configurations

Select Configuration: Agent

Identity Provider

Entity ID*: http://WIN-260MECJBIC2.jo123.local...

Identity Provider Certificate*: -----BEGIN CERTIFICATE-----MIIC8jC

User Identity Location*: SAML Subject Identifier

User Identity Attribute Name*:

Enable Encrypted Assertion

Assertion Decryption Certificate*: Enter Assertion Decryption Certificate

Federation Service Properties

Federation Service display name: JO123 ADFS

Example: Fabrikam Federation Service

Federation Service name: WIN-260MECJBIC2.jo123.local

Example: fs.fabrikam.com

Federation Service identifier: http://WIN-260MECJBIC2.jo123.local/adfs/services/trust

Example: http://fs.fabrikam.com/adfs/services/trust

Web SSO lifetime (minutes): 480

□ Enable delegation for service administration

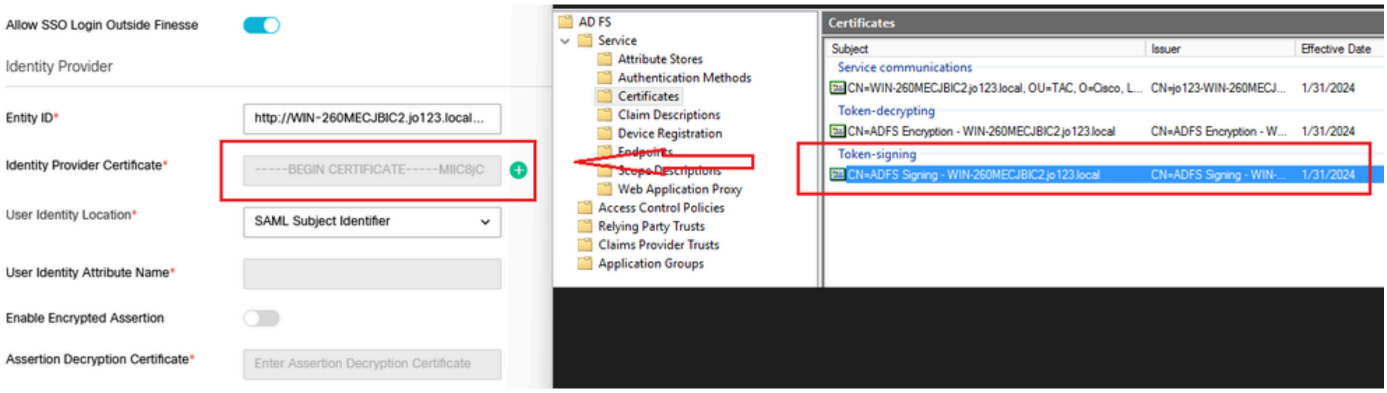
Delegate name:

□ Allow Local System account for service administration

☑ Allow Local Administrators group for service administration

Identity Provider Certificate

- The public key certificate.
- The certificate must start with “-----BEGIN CERTIFICATE-----” and end with “-----END CERTIFICATE-----”
- This is the Token-signing certificate in the *AD FS Management Console > Service > Certificates > Token-signing.*



Allow SSO Login Outside Finesse ☑

Identity Provider

Entity ID*: http://WIN-260MECJBIC2.jo123.local...

Identity Provider Certificate*: -----BEGIN CERTIFICATE-----MIIC8jC

User Identity Location*: SAML Subject Identifier

User Identity Attribute Name*:

Enable Encrypted Assertion ☐

Assertion Decryption Certificate*: Enter Assertion Decryption Certificate

Certificates

Subject	Issuer	Effective Date
Service communications		
CN=WIN-260MECJBIC2.jo123.local, OU=TAC, O=Cisco, L...	CN=jo123-WIN-260MECJ...	1/31/2024
Token-decrypting		
CN=ADFS Encryption - WIN-260MECJBIC2.jo123.local	CN=ADFS Encryption - W...	1/31/2024
Token-signing		
CN=ADFS Signing - WIN-260MECJBIC2.jo123.local	CN=ADFS Signing - WIN-...	1/31/2024

User Identity Location

- Select *SAML Subject Identifier* to set the identity location in the certificate to the default SAML subject identifier, as in the subject in the SAML assertion, for example, the username in the <saml:Subject>.
- Select *SAML Attribute* to assign the identity location to a specific attribute in the certificate, for example, email.address. Provide the attribute in the User Identity Attribute Name field.

User Identity Attribute Name

- Applicable only when User ID Location value is an SAML attribute.
- This can be adjusted within the SAML assertion and used to select a different attribute for the authentication of users, such as an email address.
- It can also be used to create new users with a SAML Attribute.
- For example, if a user is identified through the value provided in the email.address attribute, and the value of email address provided does not match any user in the system, a new user is created with the provided SAML attributes.

Enable Encrypted Assertion (Optional)

- If you wish to enable encrypted assertion with the Identity Provider for console login, click the Toggle button set the value to Enabled.
- If not, set the value to Disabled.

Assertion Decryption Certificate

If Enable encrypted assertion is set to Enabled, click the Search and Add button and confirm your choice to change the certificate.

Provide the details in the Assertion Decryption Certificate window:

- *Java Keystore File: Provide the file path of your Java Keystore File. This file is in the .jks format and contains the decryption key the system needs to access files secured by the Identity Provider.*
- *Alias Name: The unique identifier for the decryption key.*
- *Keystore Password: The password required for accessing the Java Keystore File.*
- *Key Password: The password required for accessing the Alias' decryption key.*

Note: This needs to match the certificate in the 'Encryption' tab of the configured ECE Relying Party Trust on AD FS Management console.

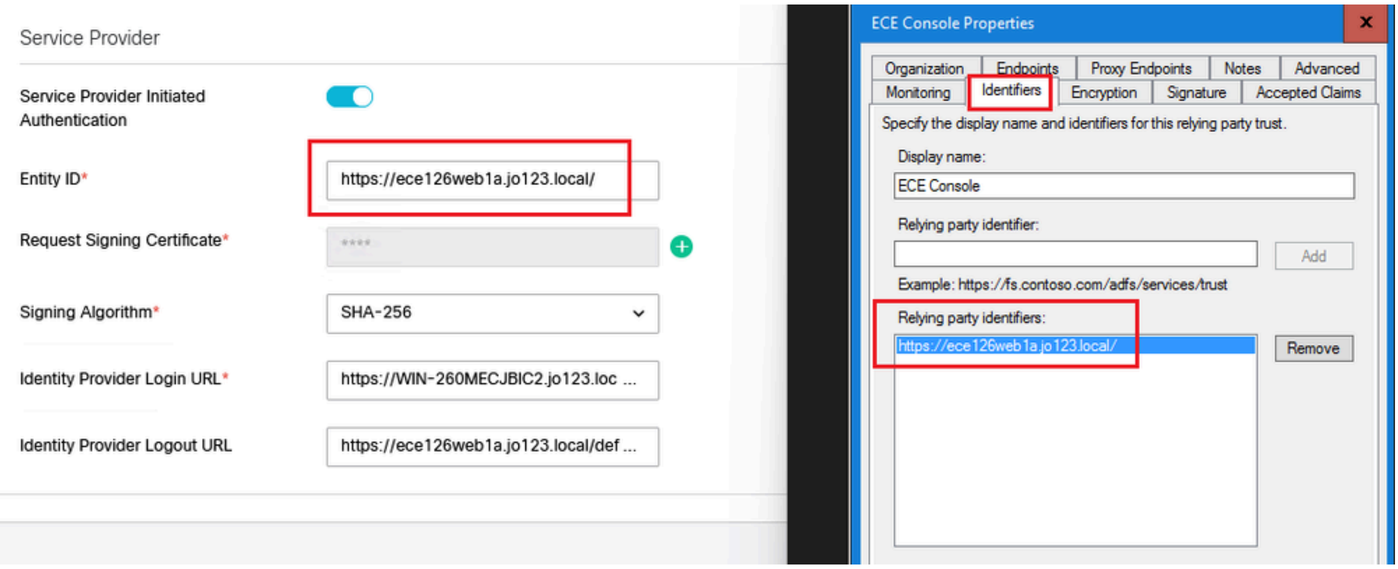
c. Service Provider

Service Provider Initiated Authentication

- Set the toggle button to Enabled.

Entity ID

- Provide the External URL of the ECE application.



Service Provider

Service Provider Initiated Authentication

Entity ID* https://ece126web1a.jo123.local/

Request Signing Certificate* ****

Signing Algorithm* SHA-256

Identity Provider Login URL* https://WIN-260MECJBIC2.jo123.loc ...

Identity Provider Logout URL https://ece126web1a.jo123.local/def ...

ECE Console Properties

Specify the display name and identifiers for this relying party trust.

Display name:

ECE Console

Relying party identifier:

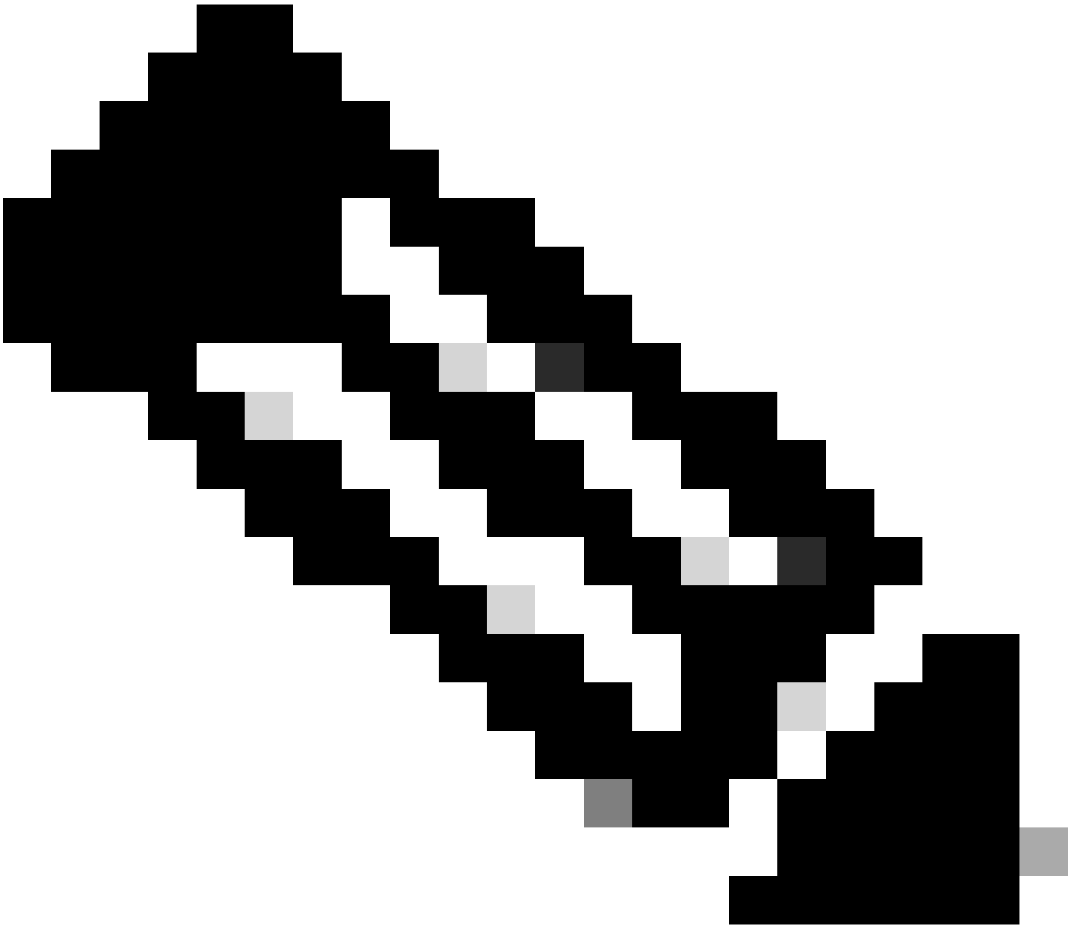
Example: https://fs.contoso.com/adfs/services/trust

Relying party identifiers:

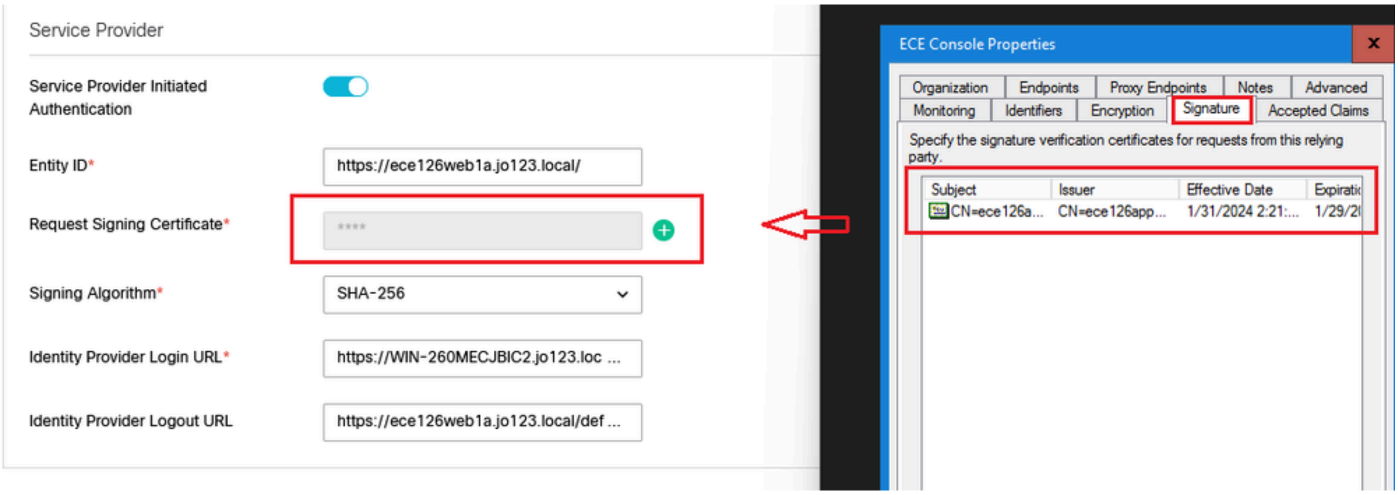
https://ece126web1a.jo123.local/

Request Signing Certificate

- A Java Keystore (JKS) certificate is needed to provide the necessary information.
- Upload the .jks file using the alias name and keystore/key password generated in step 11.



Note: This needs to match the certificate uploaded to the 'Signature' tab of the configured ECE Relying Party Trust on AD FS Management console.



Service Provider

Service Provider Initiated Authentication

Entity ID*: https://ece126web1a.jo123.local/

Request Signing Certificate*: ****

Signing Algorithm*: SHA-256

Identity Provider Login URL*: https://WIN-260MECJBIC2.jo123.loc ...

Identity Provider Logout URL: https://ece126web1a.jo123.local/def ...

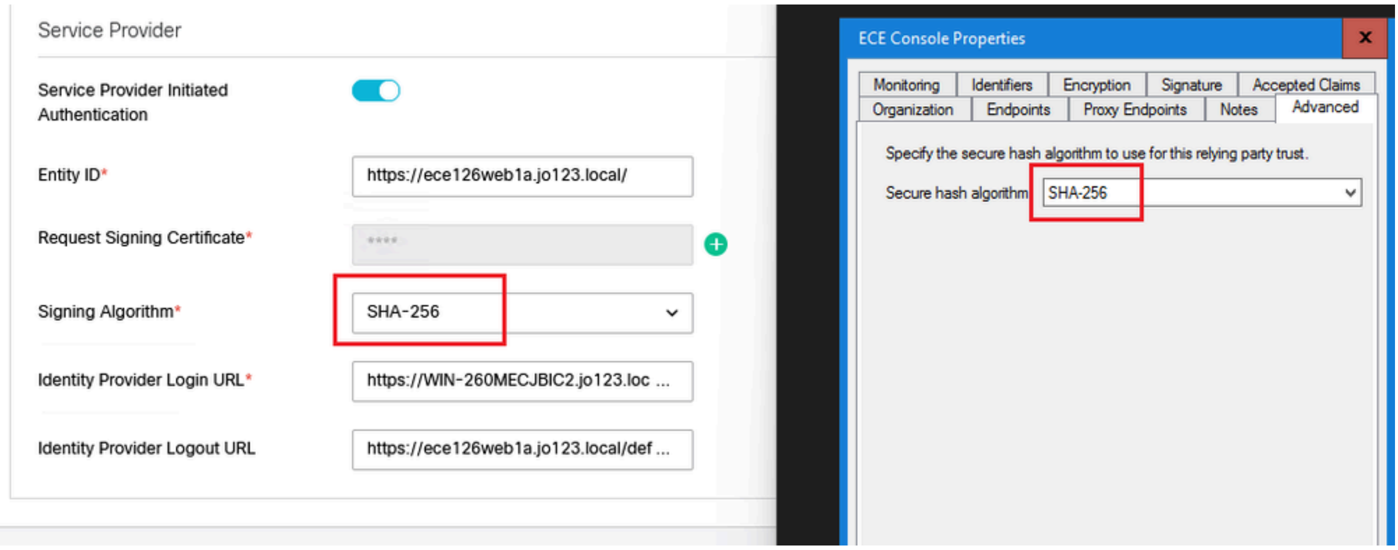
ECE Console Properties

Specify the signature verification certificates for requests from this relying party.

Subject	Issuer	Effective Date	Expiratio
CN=ece126a...	CN=ece126app...	1/31/2024 2:21:...	1/29/2

Signing Algorithm

- Set the signing algorithm for the service provider.
- If using ADFS, this value must match with the algorithm selected in the relying party trust created for ECE under the Advanced tab.



Service Provider

Service Provider Initiated Authentication

Entity ID*: https://ece126web1a.jo123.local/

Request Signing Certificate*: ****

Signing Algorithm*: SHA-256

Identity Provider Login URL*: https://WIN-260MECJBIC2.jo123.loc ...

Identity Provider Logout URL: https://ece126web1a.jo123.local/def ...

ECE Console Properties

Specify the secure hash algorithm to use for this relying party trust.

Secure hash algorithm: SHA-256

Identity Provider Login URL

- The URL for SAML authentication.
- For example, for ADFS, this would be http://<ADFS>/adfs/ls.

Identity Provider Logout URL

- The URL to which users are redirected upon logging out. This is optional and can be any URL.
- For example, agents can be redirected to https://www.cisco.com or any other URL after SSO logout.

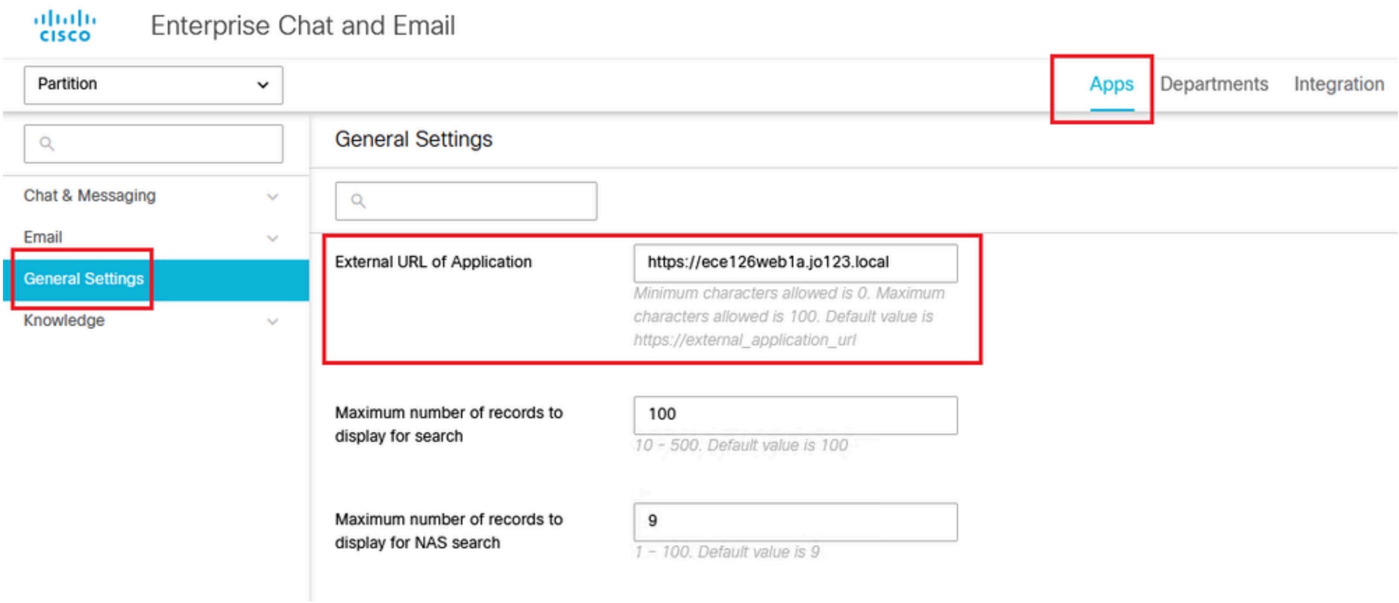
Step 16

Click Save

Set the Web Server/LB URL in the Partition settings

Step 17

Ensure the correct Web Server/LB URL is entered under the Partition settings > select the **Apps** tab and navigate to **General Settings** > **External URL of the Application**



External URL of Application: https://ece126web1a.jo123.local

Minimum characters allowed is 0. Maximum characters allowed is 100. Default value is https://external_application_url

Maximum number of records to display for search: 100

10 - 500. Default value is 100

Maximum number of records to display for NAS search: 9

1 - 100. Default value is 9

Configuring SSO for Partition Administrators

Note:

- This step applies to PCCE only.
- This is for the ECE gadget accessed within CCE Admin WEB interface https:///cceadmin.

Step 18

To configure SSO for Partition Administrator

1. In the ECE Admin console, under partition-level Menu, click the Security option and then select Single Sign-On > Configurations from the left side Menu.
2. In the Select Configuration drop down, select Partition Administrators and enter the configuration details:

LDAP URL

- The URL of the LDAP server.
- This can be Domain Controller URL (for example, ldap://LDAP_server:389) or Global Catalog URL (for example, ldap://LDAP_server:3268) of the LDAP server.
- Partition can be added automatically to the system when ECE is accessed via the CCE Administration Console if ECE is configured with LDAP lookup.

- However, in Active Directory deployments with multiple domains in a single forest or where Alternate UPNs are configured, the Domain Controller URL with the standard LDAP ports of 389 and 636 must not be used.
- The LDAP integration can be configured to use the Global Catalog URL with ports 3268 and 3269.

Note: It is best practice to use Global Catalog URL. If you do not use a GC, an error in the ApplicationServer logs is as follows.

- *Exception in LDAP authentication <@> javax.naming.PartialResultException: Unprocessed Continuation Reference(s); remaining name 'DC=example,DC=com'*

DN attribute

- The attribute of the DN that contains the user login name.
- For example, userPrincipalName.

Base

- The value specified for Base is used by the application as the search base.

- Search base is the starting location for search in LDAP directory tree.
- For example, DC=mycompany, DC=com.

DN for LDAP search

- If your LDAP system does not allow anonymous bind, provide the Distinguished Name (DN) of a user who has search permissions on the LDAP directory tree.
- If the LDAP server allows anonymous bind, leave this field blank.

Password

- If your LDAP system does not allow anonymous bind, provide the password of a user who has search permissions on the LDAP directory tree.
- If the LDAP server allows anonymous bind, leave this field blank.

Step 19

Click Save

This now completes the Single Sign-On configuration for Agents and Partition Administrators in ECE.

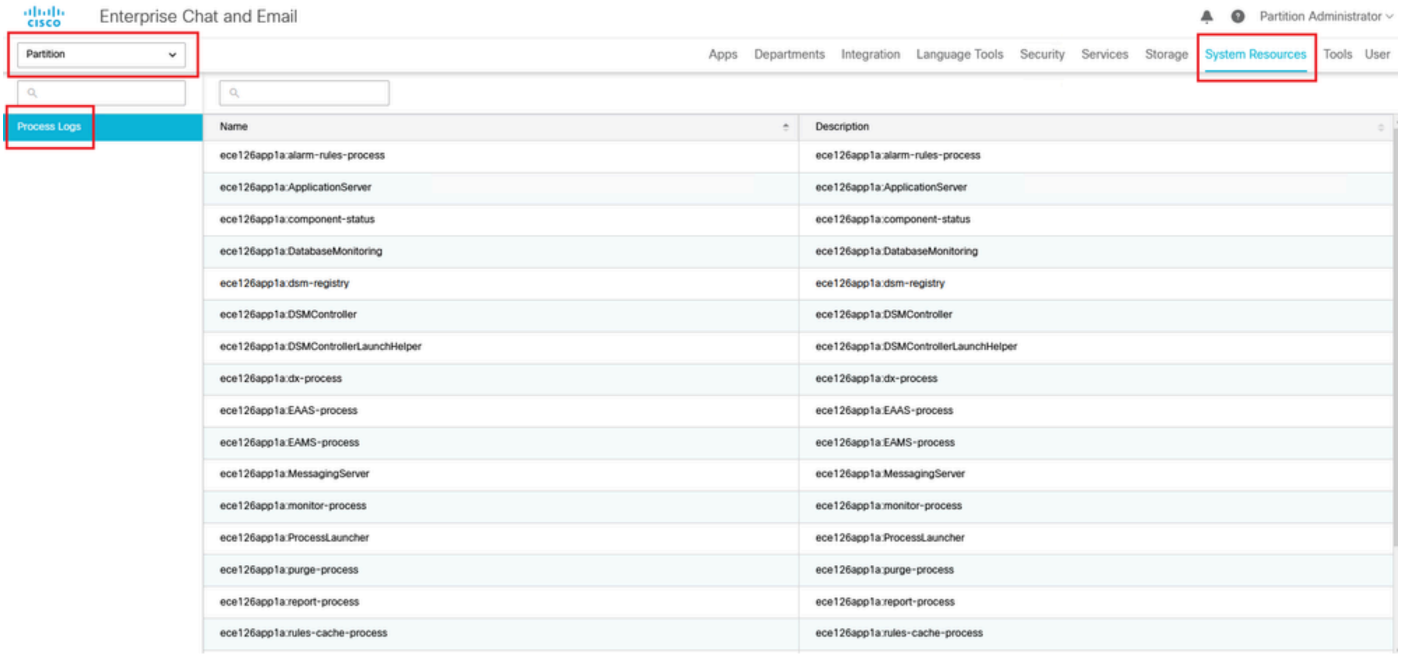
Troubleshooting

Setting Trace level

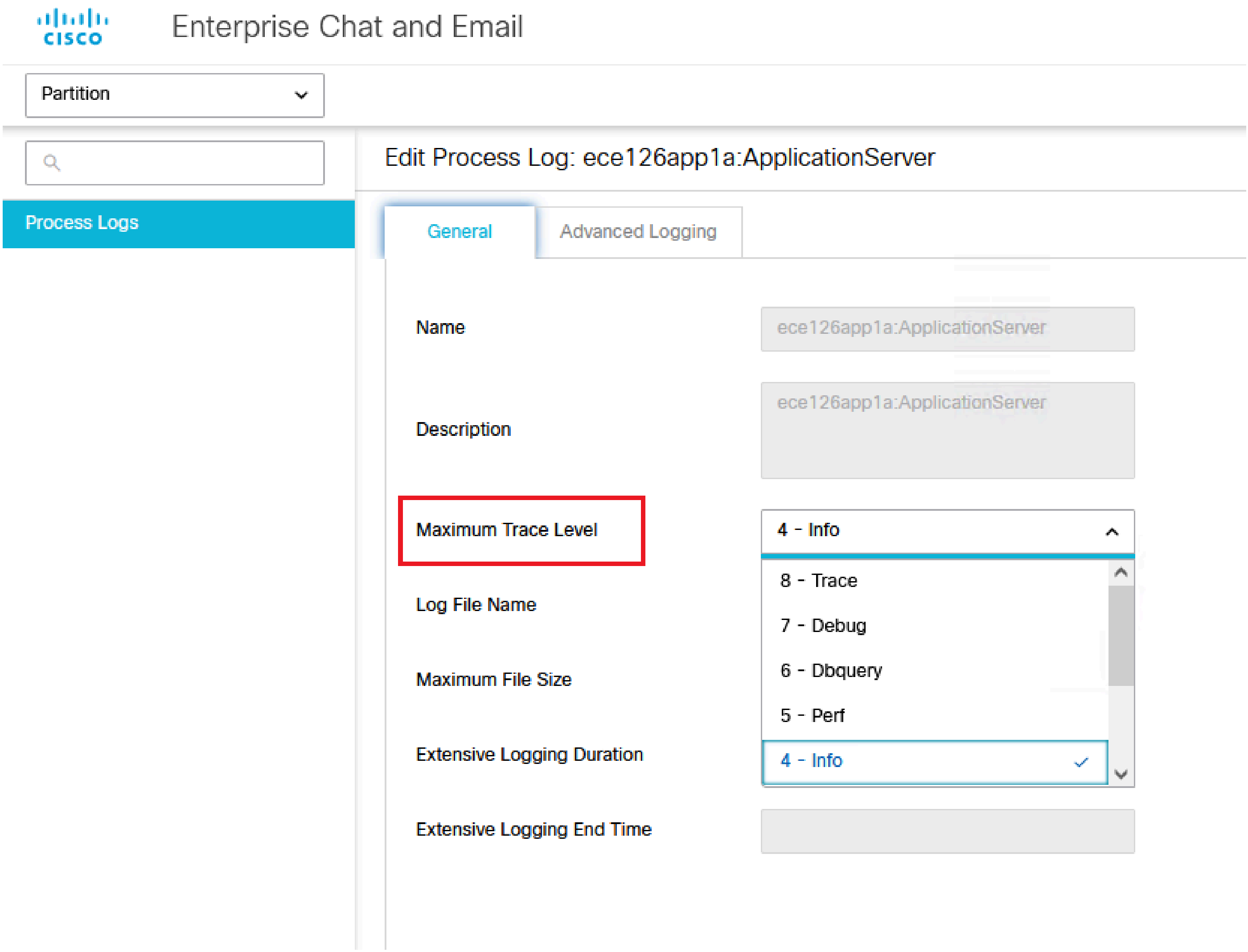
1. In the ECE Admin console, under partition-level Menu, click the **System Resources** option and then select **Process Logs** from the left side Menu.
2. From the list of the processes, select the ***ApplicationServer*** process > set the desired trace level from the '**Maximum Trace Level**' drop down menu.

Note:

- For troubleshooting the SSO login errors during initial setup or re-configuration, set the ApplicationServer process trace to level 7.
- Once the error is reproduced, set the trace level back to the default level 4, to avoid overwriting of the logs.



Name	Description
ece126app1a:alarm-rules-process	ece126app1a:alarm-rules-process
ece126app1a:ApplicationServer	ece126app1a:ApplicationServer
ece126app1a:component-status	ece126app1a:component-status
ece126app1a:DatabaseMonitoring	ece126app1a:DatabaseMonitoring
ece126app1a:dsm-registry	ece126app1a:dsm-registry
ece126app1a:DSMController	ece126app1a:DSMController
ece126app1a:DSMControllerLaunchHelper	ece126app1a:DSMControllerLaunchHelper
ece126app1a:dx-process	ece126app1a:dx-process
ece126app1a:EAAS-process	ece126app1a:EAAS-process
ece126app1a:EAMS-process	ece126app1a:EAMS-process
ece126app1a:MessagingServer	ece126app1a:MessagingServer
ece126app1a:monitor-process	ece126app1a:monitor-process
ece126app1a:ProcessLauncher	ece126app1a:ProcessLauncher
ece126app1a:purge-process	ece126app1a:purge-process
ece126app1a:report-process	ece126app1a:report-process
ece126app1a:rules-cache-process	ece126app1a:rules-cache-process



Edit Process Log: ece126app1a:ApplicationServer

Name: ece126app1a:ApplicationServer

Description: ece126app1a:ApplicationServer

Maximum Trace Level: 4 - Info

Log File Name

Maximum File Size

Extensive Logging Duration

Extensive Logging End Time

Troubleshooting Scenario 1

Error

- Error Code: 500
- Error Description: The application is not able to login the user at this time as Identity Provider login failed.

Log Analysis

- IdP login failed - ***<samlp:Status><samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Responder" /></samlp:Status>***
- Here the status "Responder" indicates that there is some issue on the AD FS side - in this case, primarily with the "Request Signing certificate" uploaded on ECE Admin console (SSO Configuration > Service Provider) and the certificate uploaded to the ECE Relying Party Trust under the 'Signature' tab.
- This is the certificate that is generated using the Java Keystore File.

Application Server logs - Trace level 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
```

Resolution

- Refer the '***Request Signing Certificate***' configuration under the section 'Configuring Agent Single Sign-On - Service Provider'.
- Ensure the Java Keystore .jks file generated in **Step 11** is uploaded to the "Request Signing certificate" field on ECE Admin console under SSO Configuration > Select Configuration 'Agent' > 'SSO Configuration' tab > Service Provider > Request Signing certificate.
- Ensure the .crt file is uploaded under the 'Signature' tab of the ECE Relying Party Trust (**Step 12**).

Troubleshooting Scenario 2

Error

- Error Code: 400
- Error Description: SAML Response token is invalid: signature validation failed.

Log Analysis

- This error indicates that there is a mismatch in the certificate between the 'Token-signing certificate' on ADFS and the 'Identity provider certificate' on the ECE SSO Configuration.

Application Server logs - Trace level 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
```

Resolution

- The error seen in the log snippet, '*Could not parse certificate: java.io.IOException: Incomplete data*', indicates that the '***Identity Provider Certificate***' content is not entered correctly
- To resolve this: On the AS FS Management > AD FS > Service > Certificates > Token-Signing > Export this certificate > open in a text editor > copy all the contents > paste under 'Identity provider certificate' filed in the SSO configuration > Save.
- Refer the 'Identity Provider Certificate' configuration under the section 'Configuring Agent single sign-on - Identity Provider' (**Step 15**).

Troubleshooting Scenario 3

Error

- Error Code: 401-114
- Error Description: User Identity not found in SAML attribute.

Log Analysis

Application Server logs - Trace level 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 <@
```

Resolution

- This error indicates a configuration issue/mismatch in the 'User Identity Location' and the 'User Identity Attribute Name' fields.
- Check and correct the '**User Identity Location**' and the '**User Identity Attribute Name**' in the ECE Admin console, under Single Sign-On > Configurations > in the Select Configuration drop down, select Agent > SSO Configuration tab > Identify Provider (**Step 15**).

Related Information

These are the key documents you must review thoroughly before you start any ECE installation or integration. This is not a comprehensive list of ECE documents.

Note:

- Most ECE documents have two versions. Please ensure that you download and use the versions that are for PCCE. The document title has either for Packaged Contact Center Enterprise or (For PCCE) or (For UCCE and PCCE) after the version number.
- Ensure that you check the start page for Cisco Enterprise Chat and Email documentation for any updates prior to any install, upgrade, or integration.
- https://www.cisco.com/c/en/us/support/customer-collaboration/cisco-enterprise-chat-email/series.html

ECE Version 12.6(1)

- Enterprise Chat and Email Administrator’s Guide