

SSO voor agents en Partitie Admin in ECE configureren en problemen oplossen

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Configuratiestappen](#)

[Relying Party Trust configureren voor ECE](#)

[Een identiteitsprovider configureren](#)

[Certificaten aanmaken en importeren](#)

[Enkelvoudige aanmelding van Agent configureren](#)

[De URL van de webserver/LB in de instellingen van de partitie instellen](#)

[SSO configureren voor partitiebeheerders](#)

[Probleemoplossing](#)

[Overtrek-niveau instellen](#)

[Problemen oplossen in scenario 1](#)

[Fout](#)

[Analyse van logboeken](#)

[Resolutie](#)

[Problemen oplossen in scenario 2](#)

[Fout](#)

[Analyse van logboeken](#)

[Resolutie](#)

[Scenario 3 voor probleemoplossing](#)

[Fout](#)

[Analyse van logboeken](#)

[Resolutie](#)

[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft de stappen die nodig zijn om Single Sign-On (SSO) voor Agents en Partition Administrators te configureren in een ECE-oplossing.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

Cisco Packaging Contact Center Enterprise (PCCE)

Cisco Unified Contact Center Enterprise (UCS)

Enterprise Chat en e-mail (ECE)

Microsoft Active Directory

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

UCS versie: 12.6(1)

ECE-versie: 12.6(1)

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

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

De Enterprise Chat en Email (ECE) consoles kunnen buiten Finesse worden geopend, maar SSO moet worden ingeschakeld om agenten en toezichthouders in staat te stellen via Finesse in te loggen bij ECE.

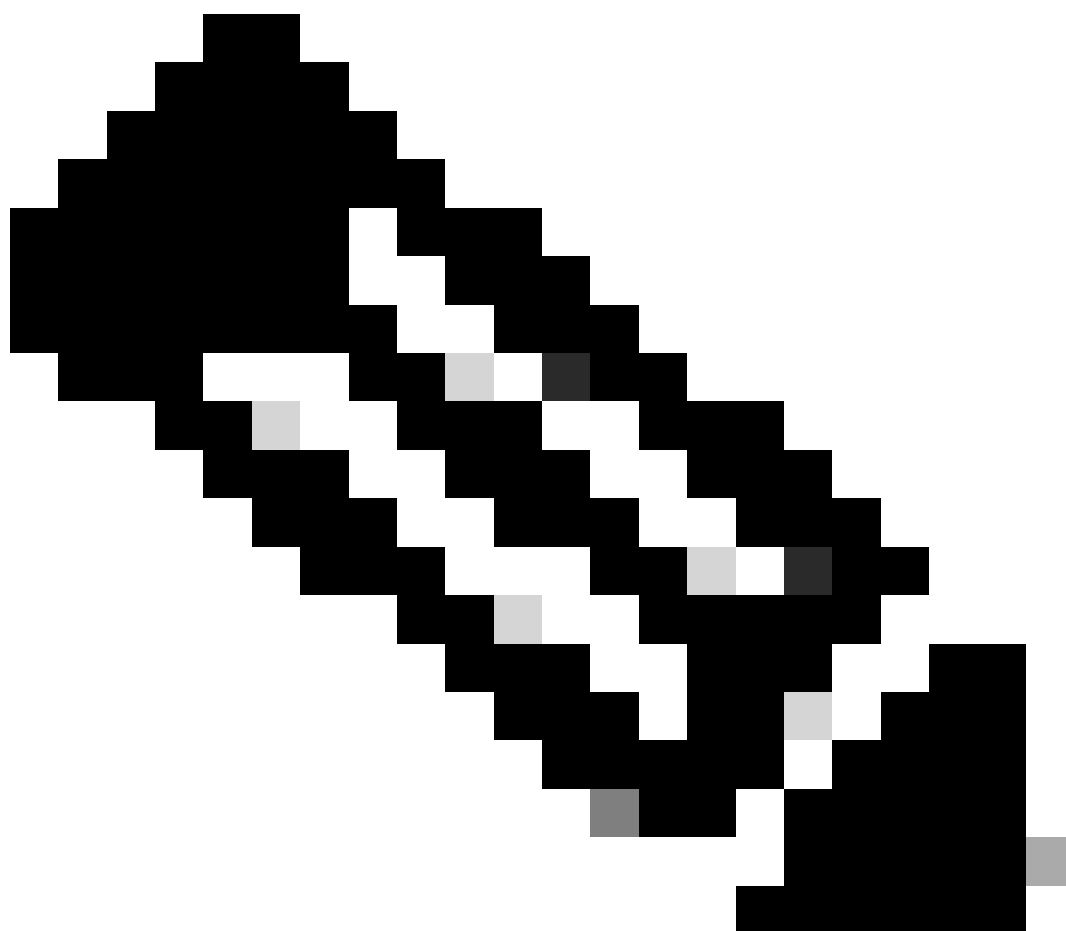
Single Sign-On kan ook worden geconfigureerd voor nieuwe partitiebeheerders. Dit waarborgt dat nieuwe gebruikers die inloggen op de Cisco Administrator-desktop toegang krijgen tot de Enterprise Chat- en e-mailbeheerconsole.

Belangrijke opmerkingen over Single Sign-On:

- Het proces van het configureren van een systeem voor eenmalige aanmelding moet worden uitgevoerd naar het Security knooppunt op partitieniveau door een partitiegebruiker met de nodige acties: Application Security weergeven en Application Security beheren.
- Voor supervisors en beheerders om in de consoles buiten de Agent-console in te loggen, moet u, zodra SSO is ingeschakeld, een geldige externe URL van de toepassing in de partitie-instellingen opgeven. Zie Algemene partitie-instellingen voor meer informatie.
- Een Java Keystore (JKS) certificaat is nodig om SSO te configureren zodat gebruikers met beheerder- of supervisor-rollen kunnen inloggen op partitie 1 van ECE buiten Finesse met behulp van hun SSO-inloggegevens. Vraag je IT afdeling om het JKS certificaat te ontvangen.
- Er moet een SSL-certificaat (Secure Sockets Layer) van Cisco IDS worden geïmporteerd

naar alle toepassingservers in een installatie. Neem contact op met uw IT-afdeling of Cisco IDS-ondersteuning om het benodigde SSL-certificaatbestand te verkrijgen.

- DB-servercollatie voor Unified CCE is hoofdlettergevoelig. De gebruikersnaam in de claim die wordt geretourneerd van de gebruikersinfo-endpoint URL en de gebruikersnaam in Unified CCE moeten hetzelfde zijn. Als zij niet hetzelfde zijn, worden de enige sign-on agenten niet herkend zoals het programma geopend en ECE kan agent geen beschikbaarheid naar Unified CCE verzenden.
 - Als u SSO voor Cisco IDS configureert, heeft dit gevolgen voor gebruikers die zijn geconfigureerd in Unified CCE voor eenmalige aanmelding. Zorg ervoor dat de gebruikers die u voor SSO in ECE wilt inschakelen, voor SSO in Unified CCE zijn geconfigureerd. Raadpleeg uw Unified CCE-beheerder voor meer informatie.
-



Opmerking:

- Zorg ervoor dat de gebruikers die u voor SSO in ECE wilt inschakelen, voor SSO in Unified CCE zijn geconfigureerd.
 - Dit document beschrijft de stappen om Relying Part Trust voor ECE in een Single AD FS-implementatie te configureren waar Resource Federation Server en Account
-

- Federation Server op dezelfde machine zijn geïnstalleerd.
- Voor een Split AD FS-implementatie, navigeer naar de ECE Installatie en Configureren handleiding voor de betreffende versie.

Configuratiestappen

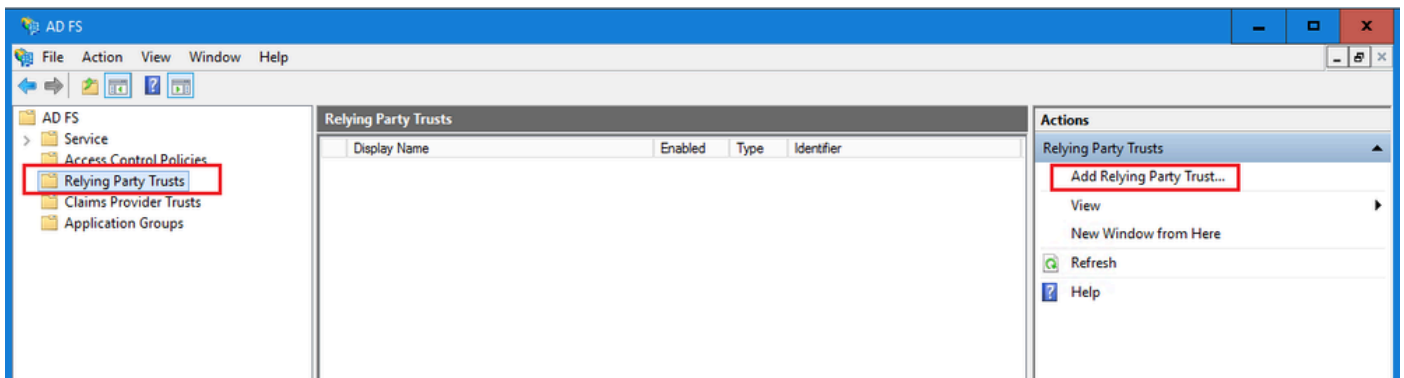
Relying Party Trust configureren voor ECE

Stap 1

Open AD FS Management console en navigeer naar AD FS > Trust Relations > Relying Party Trust.

Stap 2

Klik in het gedeelte Acties op Vertrouwen op Relying Party toevoegen...



Stap 3

In de Add Relying Party Trust wizard klikt u op Start en voltooit u de volgende stappen:

- a. Selecteer op de pagina Gegevensbron selecteren de optie Gegevens over de antwoordpartij handmatig invoeren en klik op Volgende.

Add Relying Party Trust Wizard

Select Data Source

Steps

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

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.

< Previous Next > Cancel

b. Typ in de pagina Display naam opgeven een weergavenaam voor de vertrouwende partij. Klik op Volgende

The screenshot shows the 'Add Relying Party Trust Wizard' window, specifically the 'Specify Display Name' step. The window title is 'Add Relying Party Trust Wizard'. The main heading is 'Specify Display Name'. Below the heading, there is a 'Steps' list on the left and a main configuration area on the right. The 'Steps' list includes: Welcome, Select Data Source, Specify Display Name (current step), Configure Certificate, Configure URL, Configure Identifiers, Choose Access Control Policy, Ready to Add Trust, and Finish. The main configuration area contains the instruction 'Enter the display name and any optional notes for this relying party.' There is a 'Display name:' label followed by a text box containing 'ECE Console'. Below this is a 'Notes:' label followed by a text area containing 'ECE 12.6.1'. At the bottom right, there are three buttons: '< Previous', 'Next >', and 'Cancel'.

c. Op de pagina URL configureren:

i. Selecteer de optie Ondersteuning voor SAML 2.0 Web SSO-protocol inschakelen.

ii. Geef in het URL-veld van de Relying Party SAML 2.0 SSO-server de URL in de indeling:
`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.

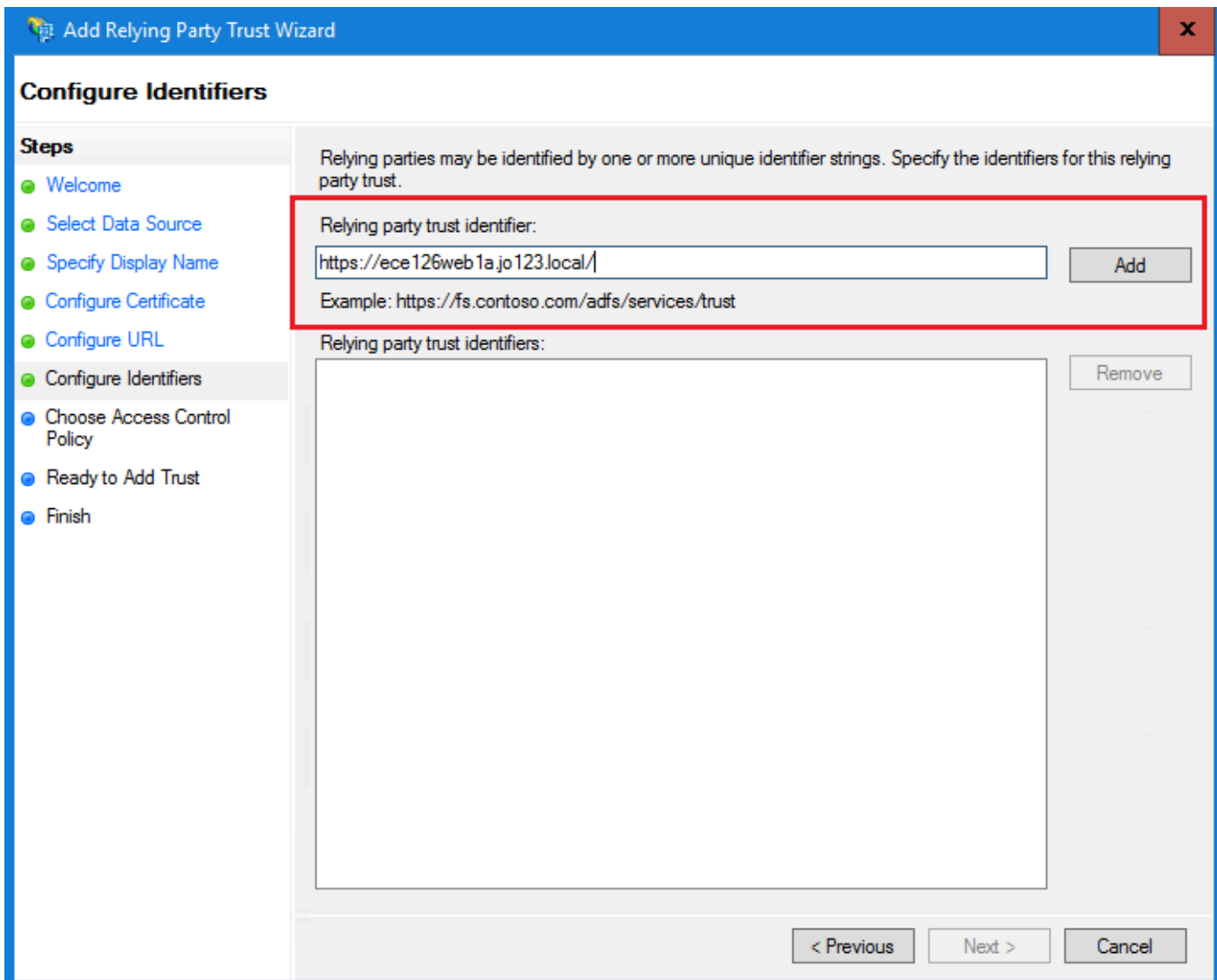
Relying party SAML 2.0 SSO service URL:

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

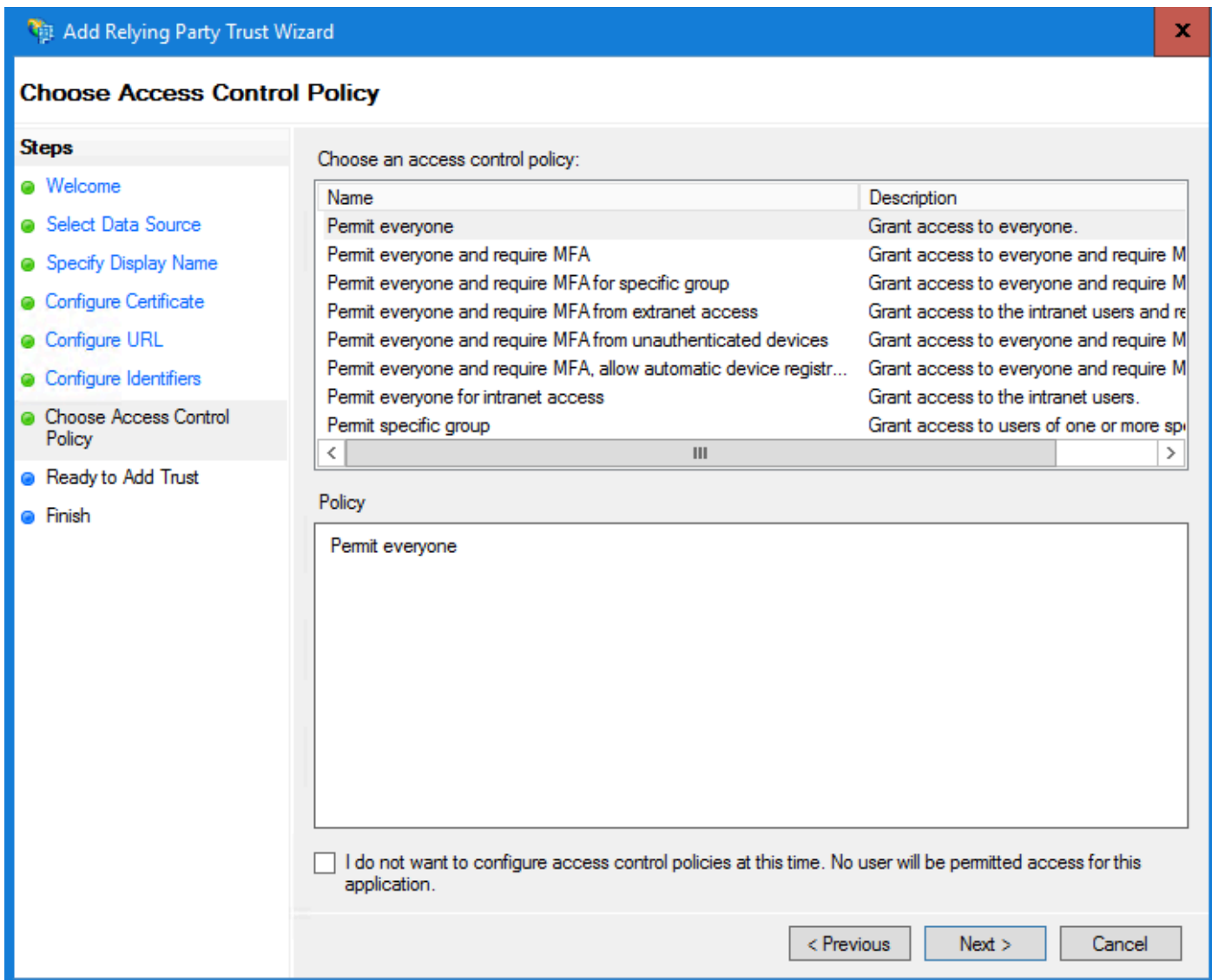
< Previous Next > Cancel

d. Typ op de pagina Identifiers configureren de identificatiecode van het vertrouwen van de Relying Party (Relying party trust) en klik op Add.

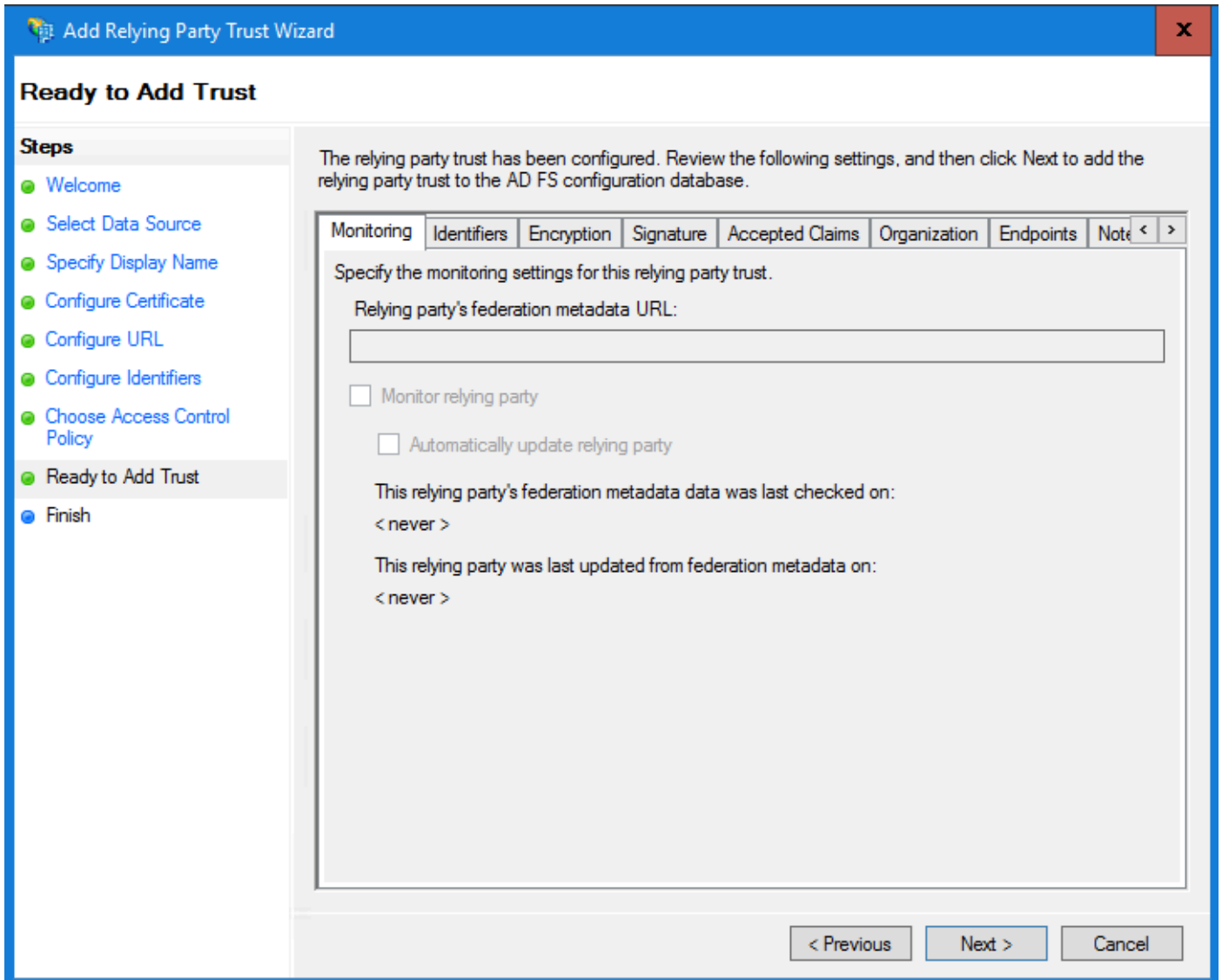
- Waarde moet in de indeling zijn: <https://<Web-server-or-Load-Balancer-FQDN>/>



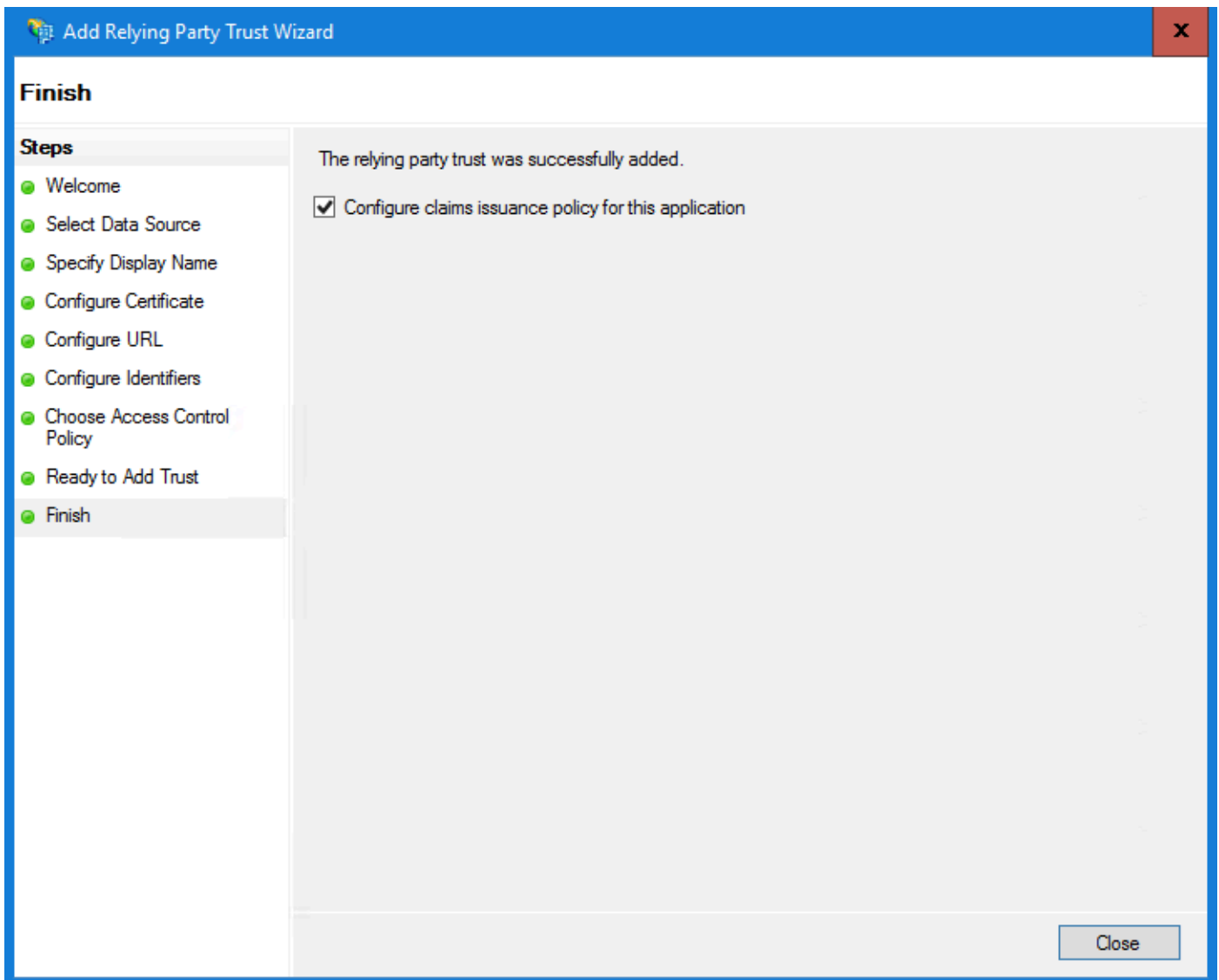
e. Klik op de pagina Toegangsbeheer kiezen op Volgende met de standaardwaarde 'Laat iedereen toe'.



f. Klik in de pagina Klaar om vertrouwen toe te voegen op Volgende.

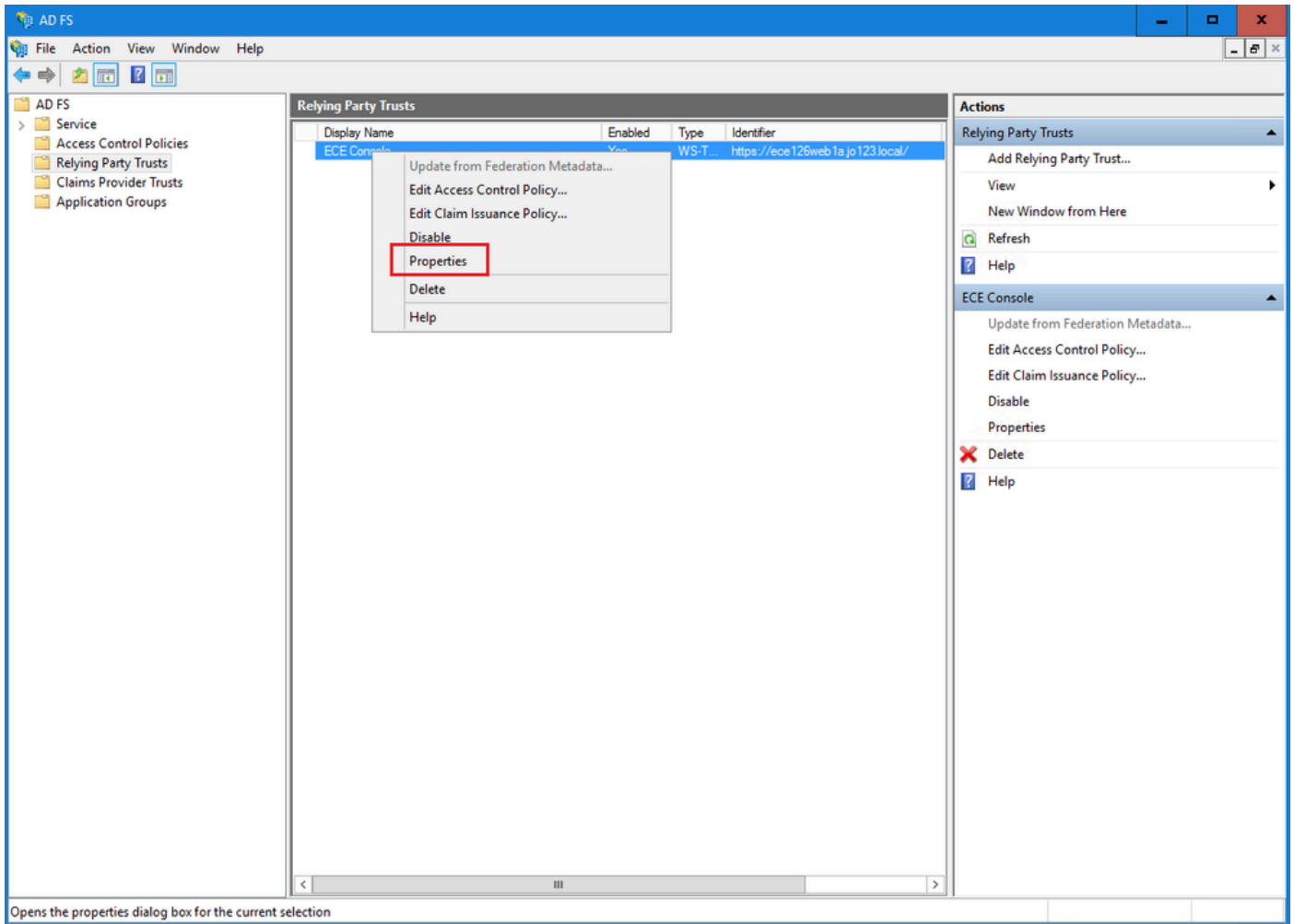


g. Klik op Sluiten zodra het vertrouwen van de vertrouwende partij is toegevoegd.



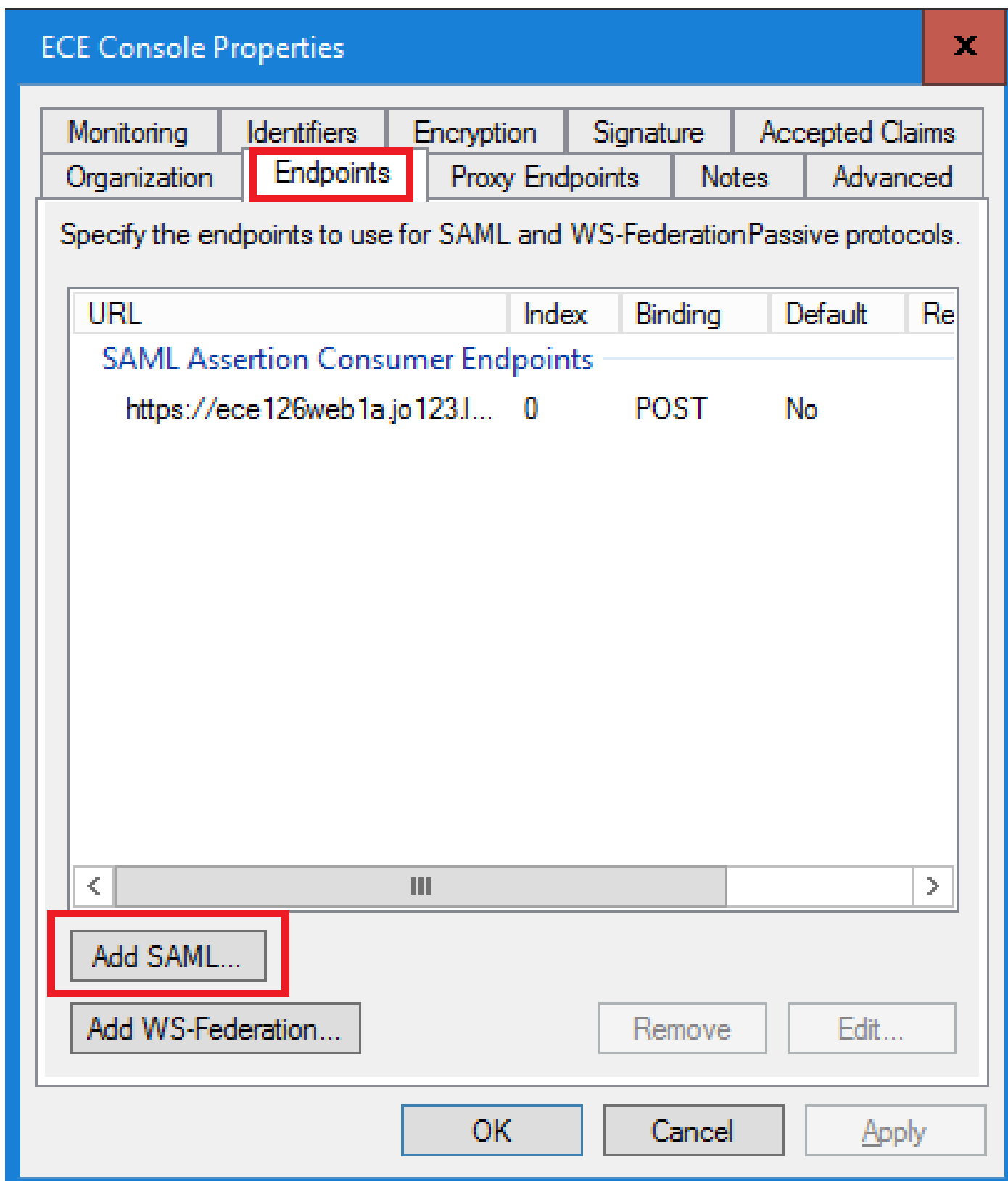
Stap 4

In de lijst Relying Provider Trusts selecteert u het Relying Party-vertrouwen dat voor ECE is gecreëerd en klikt u in het gedeelte acties op Eigenschappen.



Stap 5

Navigeer in het venster Eigenschappen naar het tabblad Endpoints en klik op de knop SAML toevoegen



Stap 6

Voer in het venster Add an Endpoint de volgende handelingen uit:

1. Selecteer het type eindpunt als uitlogging van SAML.
2. Specificeer de vertrouwde URL als `https://<ADFS-server-FQDN>/adfs/ls/?wa=wsignoutcleanup1.0`
3. Klik op OK.

Add an Endpoint X

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`

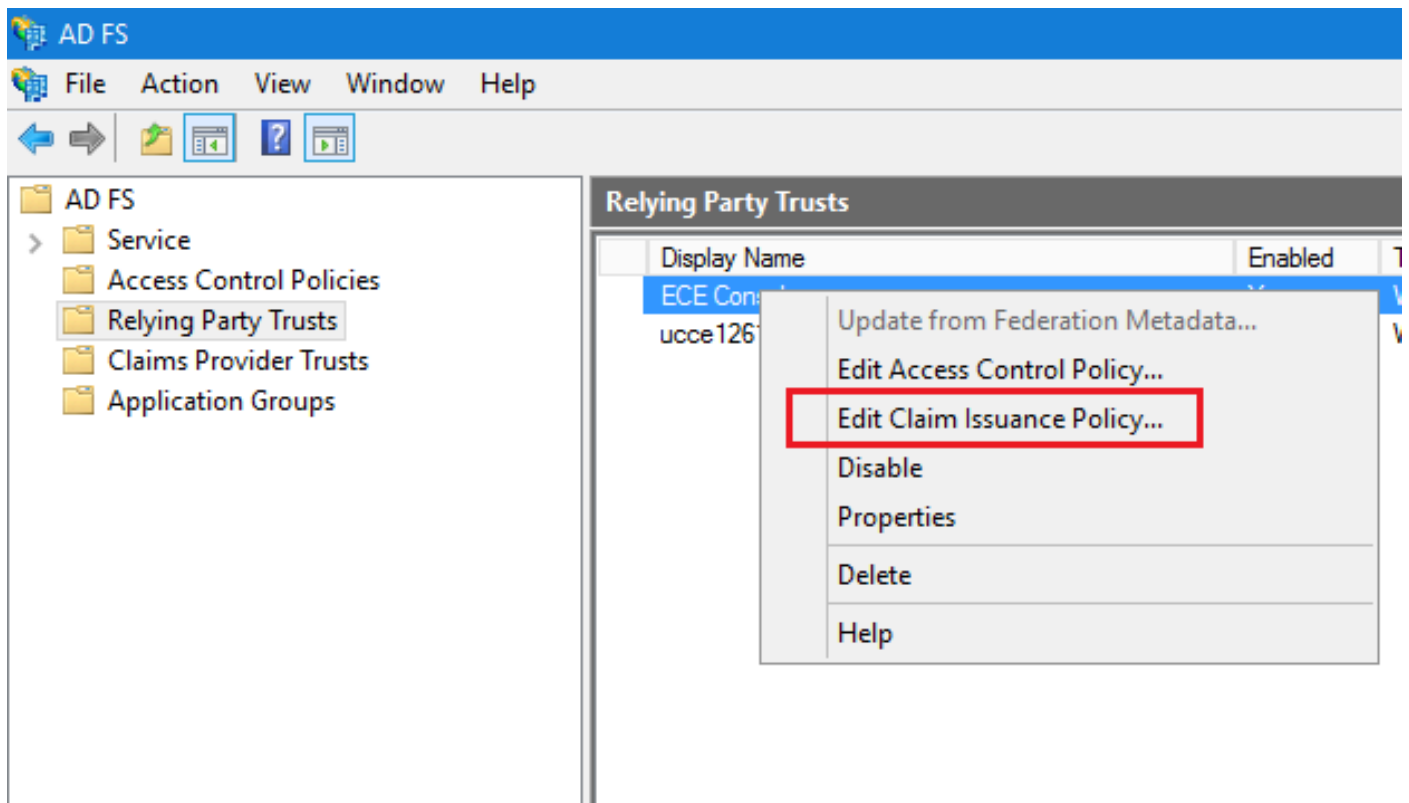
Response URL:

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

OK Cancel

Stap 7

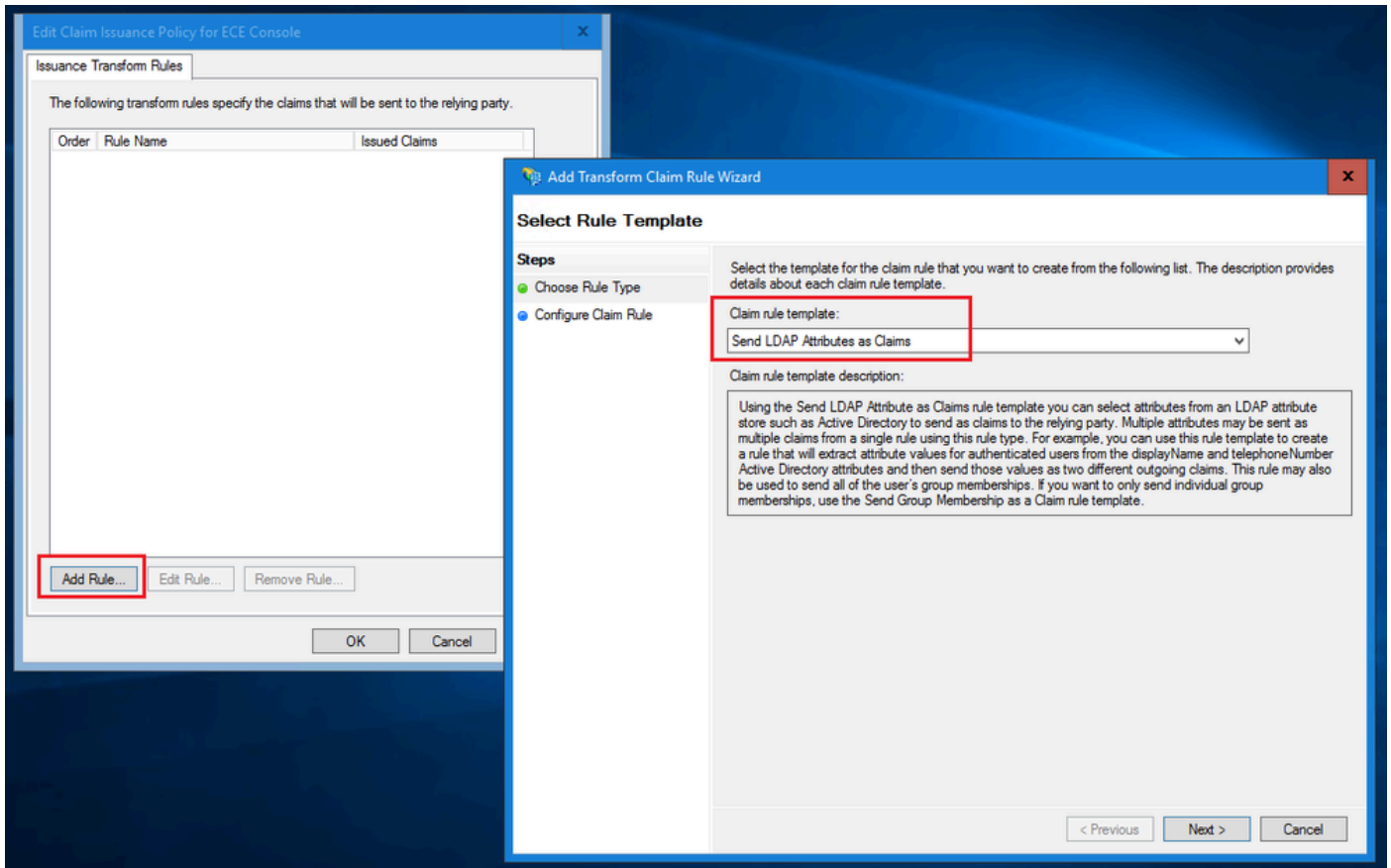
In de lijst Relying Provider Trusts selecteert u het vertrouwen dat voor ECE is gecreëerd en klikt u in het gedeelte acties op Claim Insurance Policy bewerken.



Stap 8

Klik in het venster Verzekeringsbeleid voor claim bewerken onder het tabblad Uitgiftetransformatieregels op de knop Regel toevoegen... en configureer zoals aangegeven:

- a. Selecteer op de pagina Type regel kiezen de optie LDAP-kenmerken als claims verzenden uit de vervolgkeuzelijst en klik op Volgende.



b. Op de pagina Claimregel instellen:

1. Geef de naam van de claimregel op en selecteer de naam van het kenmerk.
 2. Definieer de toewijzing van het LDAP-kenmerk en het type uitgaande claim.
- Selecteer Naam-ID als de naam van het uitgaande claimtype.
 - Klik op Voltoeien om terug te gaan naar het venster Aansprakelijkheidsverzekering bewerken en klik vervolgens op OK.

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

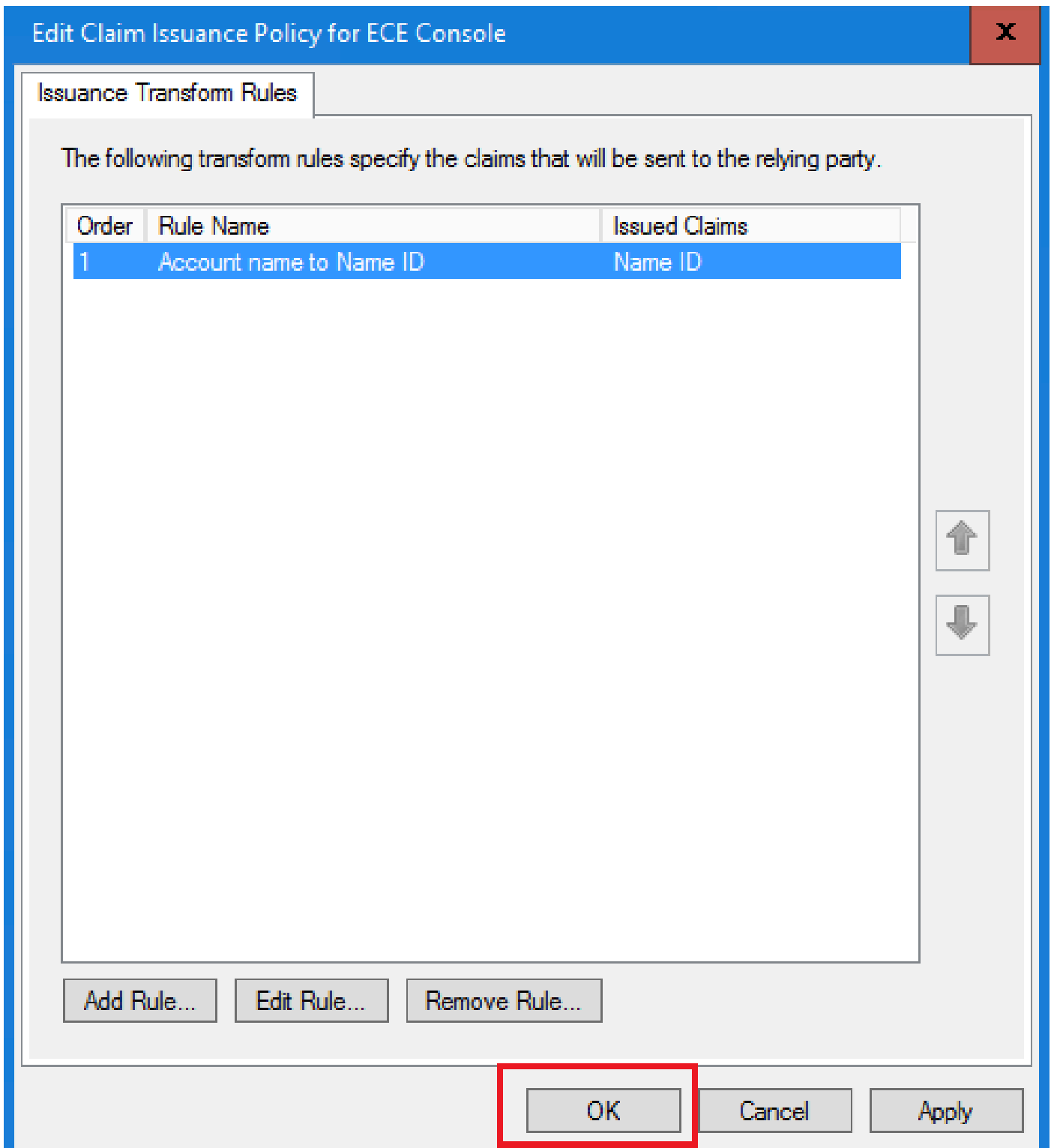
Mapping of LDAP attributes to outgoing claim types:

	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



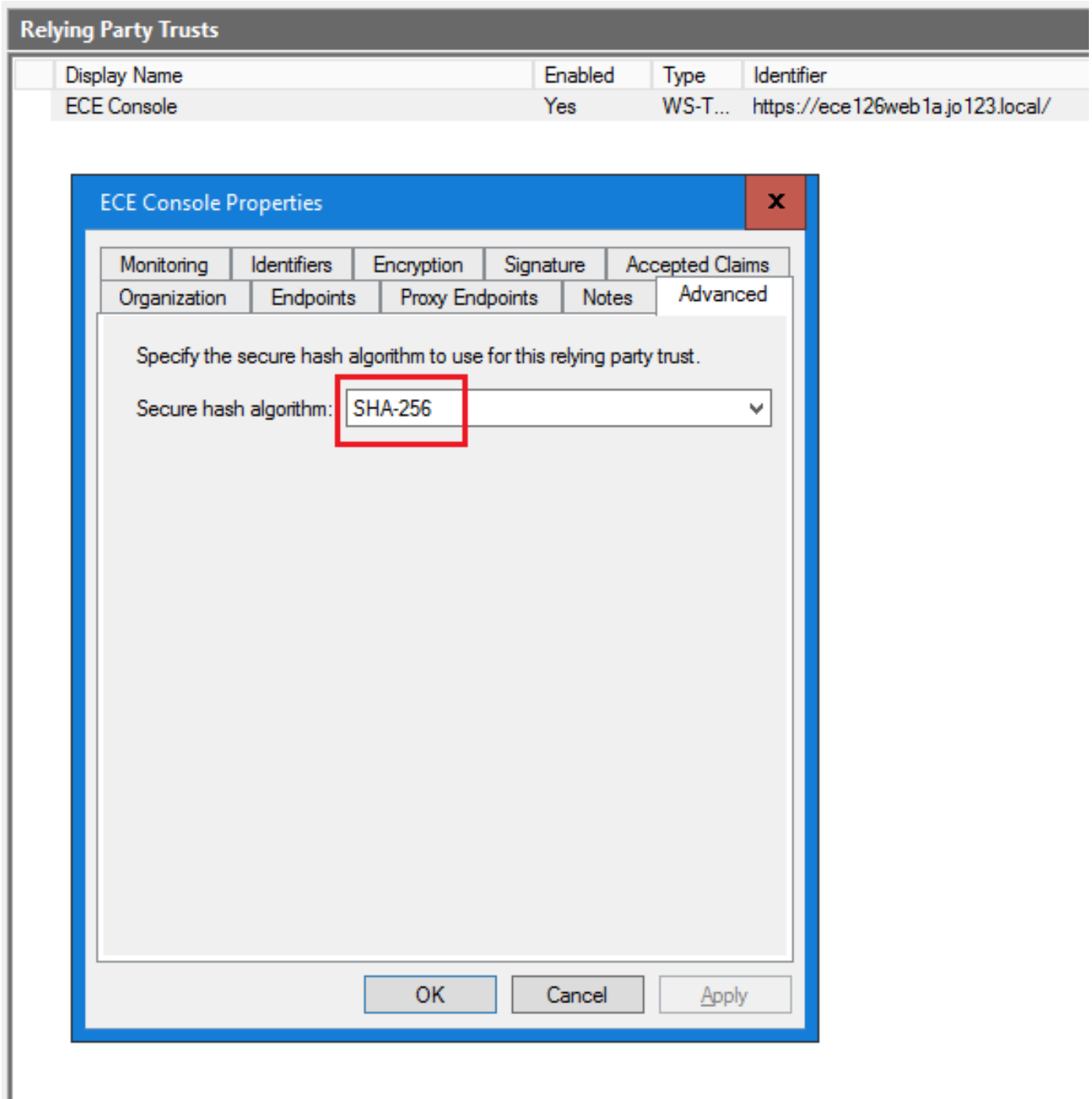
Stap 9

Dubbelklik in de lijst Relying Provider Trusts op het ECE Relying Party-vertrouwen dat u hebt gemaakt.

In het venster Properties dat nu wordt geopend, gaat u naar het tabblad Advanced en stelt u het Secure-hashalgoritme in op SHA-1 of SHA-256. Klik op OK om het venster te sluiten.



Opmerking: deze waarde moet overeenkomen met de waarde voor 'Ondertekeningsalgoritme' voor de 'Serviceprovider' onder SSO-configuraties in ECE



Stap 10

Controleer en noteer de waarde voor Federation Service Identifier.

- Selecteer in de AD FS Management-console AD FS en klik met de rechtermuisknop op AD FS > Federation Service Properties > General tab > Federation Service Identifier



Opmerking:

- Deze waarde moet exact worden toegevoegd zoals het geval is bij het configureren van de 'Entity ID'-waarde voor Identity Provider onder SSO-configuraties in ECE.
- Gebruik van `http://` betekent NIET dat ADFS niet veilig is, dit is gewoon een identifier.



The screenshot shows the AD FS console interface. The top menu bar includes 'File', 'Action', 'View', 'Window', and 'Help'. The left-hand navigation pane shows a tree view with 'AD FS' selected. A context menu is open over the 'AD FS' node, with the option 'Edit Federation Service Properties...' highlighted by a red rectangular box. Other menu items include 'Add Relying Party Trust...', 'Add Claims Provider Trust...', 'Add Attribute Store...', 'Add Application Group...', 'Edit Published Claims', 'Revoke All Proxies', 'View', 'New Window from Here', 'Refresh', and 'Help'. The main content area displays a 'view' of the AD FS configuration page, featuring a blue diamond icon and text about Azure Active Directory. The right-hand pane, titled 'Actions', lists the same menu options as the context menu. At the bottom of the console, a status bar displays the text '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:
 Edit...

Allow Local System account for service administration

Allow Local Administrators group for service administration

OK Cancel Apply

Een identiteitsprovider configureren

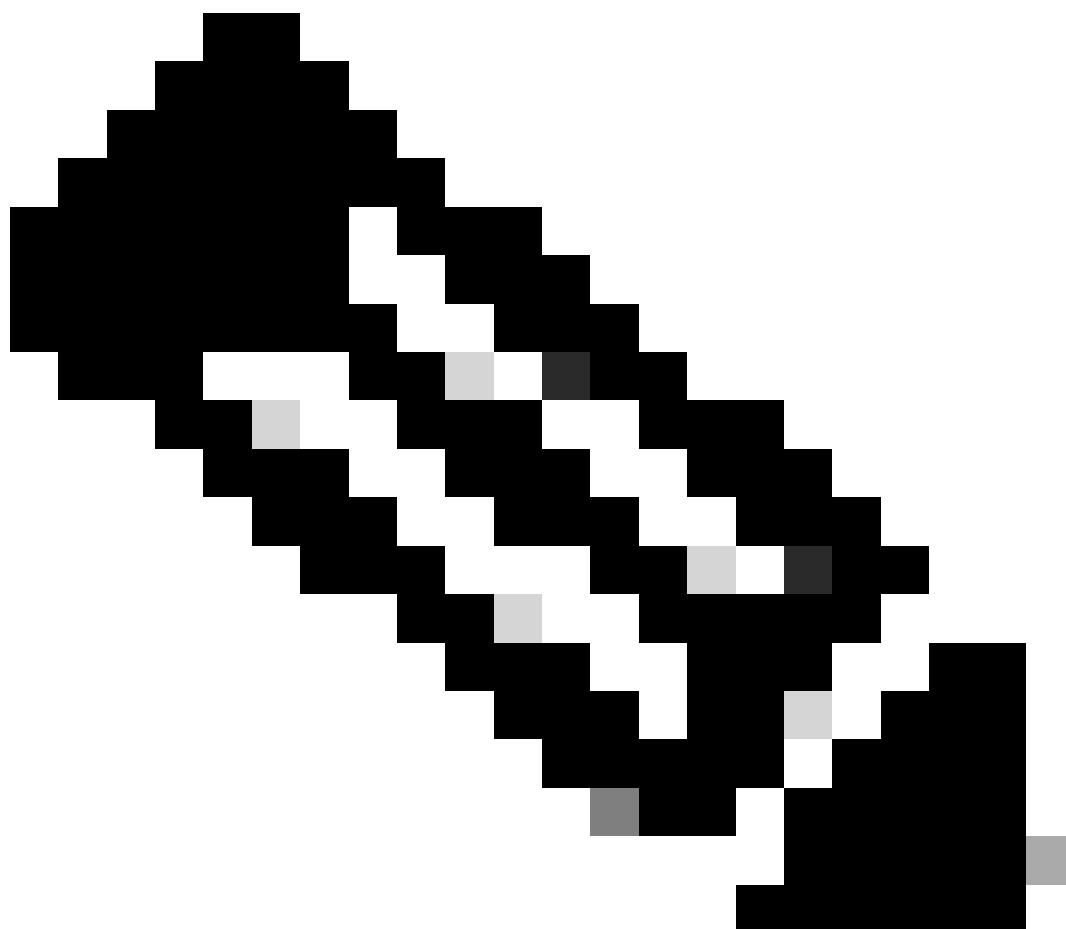
Stap 11

Een Java Keystore (JKS) certificaat is nodig om SSO te configureren zodat gebruikers met beheerder- of supervisor-rollen kunnen inloggen op de partitie van ECE buiten Finesse met behulp van hun SSO-inloggegevens.

Als u SSO wilt configureren om gebruikers met beheerder- of supervisor-rollen in staat te stellen

om in te loggen op de partitie van ECE buiten Finesse met behulp van hun SSO-inloggegevens, moet het Java Keystore (JKS)-certificaat worden geconverteerd naar het openbare sleutelcertificaat en worden geconfigureerd in Relying Party Trust op de IdP-server voor ECE.

Vraag je IT afdeling om het JKS certificaat te ontvangen.

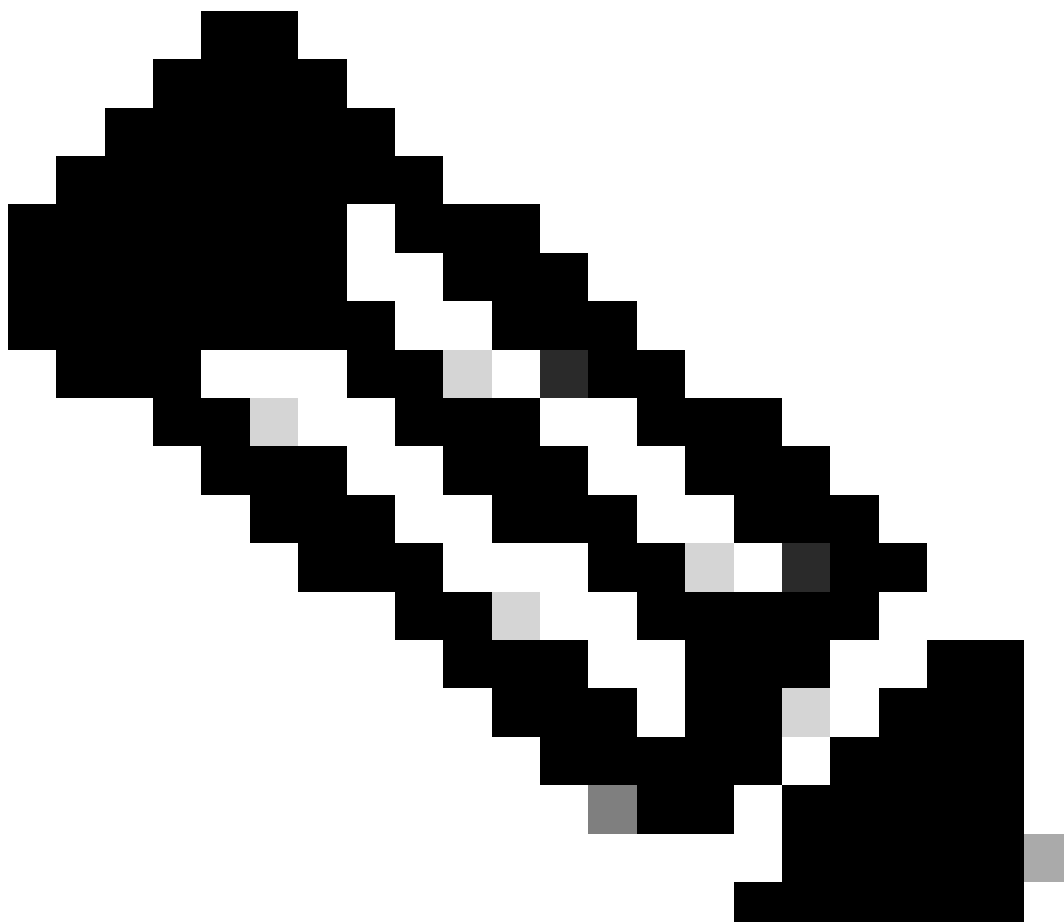


Opmerking: deze stappen zijn van toepassing op systemen die ADFS gebruiken als aanbieder van identiteiten. Andere identiteitsaanbieders kunnen verschillende methoden hebben om public key certificate te configureren.

Hier is een voorbeeld van hoe een JKS-bestand is gegenereerd in het lab:

a. JKS genereren:

```
keytool -genkey -keyalg RSA -alias ece126web1a_saml -keystore C:\Temp\ece126web1a_saml.jks -keysize 2048
```



Opmerking: het wachtwoord, de naam van de alias en het sleutelwachtwoord die hier zijn ingevoerd, worden gebruikt bij het configureren van een 'serviceprovider'-configuratie onder SSO-configuraties in ECE.

```
C:\Users\administrator.J0123>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. Het certificaat uitvoeren:

Deze keytool opdracht exporteert het certificaat bestand in het.crt formaat met bestandsnaam

ece126web1a_saml.crt naar de C:\Temp directory.

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

Stap 12

Een identiteitsprovider configureren

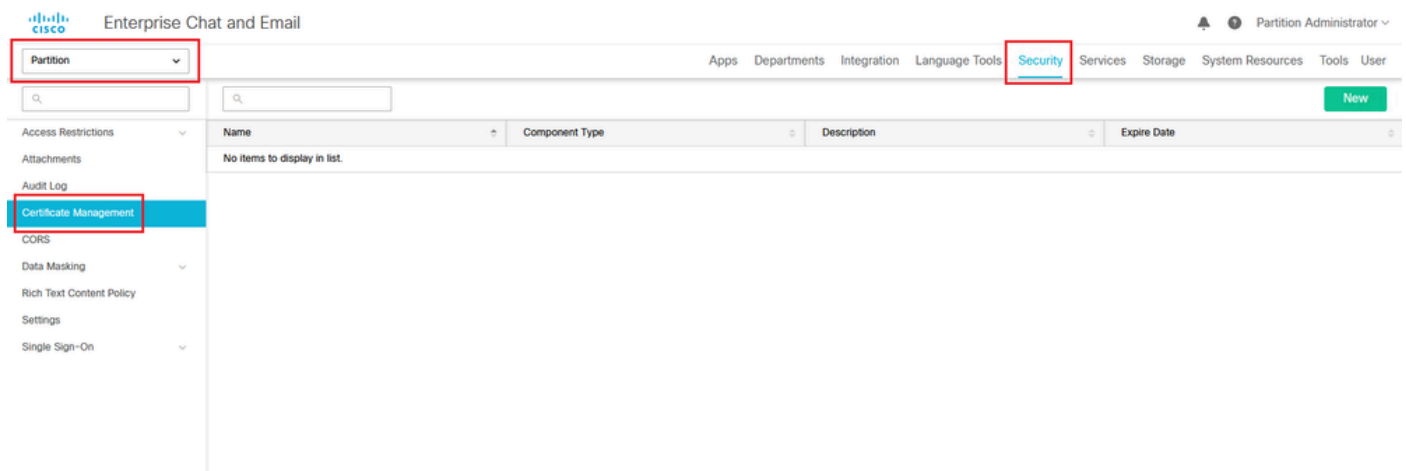
1. Selecteer en klik met de rechtermuisknop op de AD FS-beheerconsole van de Relying Party Trust die voor ECE is gemaakt.
2. Open het venster Eigenschappen voor het vertrouwen en klik onder het tabblad Handtekening op de knop Toevoegen.
3. Voeg het openbare certificaat toe (.crt-bestand dat in de vorige stap is gegenereerd) en klik op OK.

Certificaten aanmaken en importeren

Stap 13

Alvorens SSO te configureren om Cisco IDS voor Single Sign-On voor agents te gebruiken, moet het Tomcat-certificaat van de Cisco IDS-server in de toepassing worden geïmporteerd.

a. Klik in de ECE Admin-console, onder het menu op partitieniveau, op de Security-optie en selecteer vervolgens Certificate Management in het linkermenu.



b. Klik in de ruimte Certificaatbeheer op de knop Nieuw en voer de gewenste gegevens in:

- **Naam:** Typ een naam voor het certificaat.
- **Beschrijving:** Een beschrijving van het certificaat toevoegen.
- **Component Type:** selecteer Cisco IDS.
- **Importeer Certificaat:** om het certificaat te importeren, klikt u op de knop Zoeken en toevoegen en voert u de gevraagde gegevens in:
- **Certificaatbestand:** Klik op de knop Bladeren en selecteer het certificaat dat u wilt importeren. De certificaten kunnen alleen worden geïmporteerd in de bestandsindelingen

.pem, .der (BINARY) en .cer/cert.

- Alias Naam: Geef een alias voor uw certificaat.

c. Klik op Opslaan

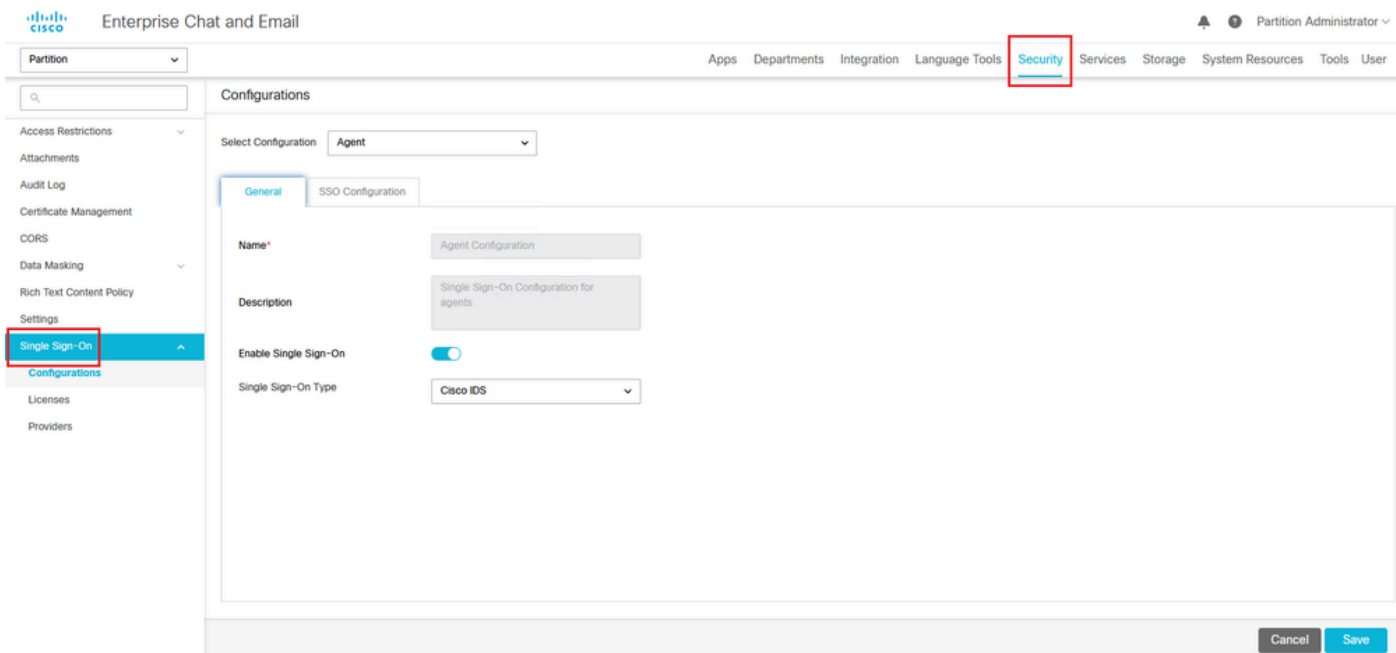
The screenshot shows the Cisco Enterprise Chat and Email Admin Console. At the top left is the Cisco logo and the title 'Enterprise Chat and Email'. Below this is a 'Partition' dropdown menu. A search bar is visible on the left. A navigation menu on the left includes: Access Restrictions, Attachments, Audit Log, Certificate Management (highlighted in blue), CORS, Data Masking, Rich Text Content Policy, Settings, and Single Sign-On. The main content area is titled 'Create Certificate' and contains the following fields:

- Name***: Cisco IDS Server
- Description**: Certificate for Cisco IdS Server
- Component Type***: CISCO IDS (dropdown menu)
- Import Certificate**: ucce1261ids.cer (with a green plus icon to the right)

Enkelvoudige aanmelding van Agent configureren

Stap 14

1. Klik in de ECE Admin-console onder het menu op partitieniveau op de optie Beveiliging en selecteer vervolgens Single Sign-On > Configuraties in het menu aan de linkerkant.
2. Selecteer in de vervolgkeuzelijst Select Configuration de optie Agent en stel de configuratie in onder het tabblad General:
 - Eenmalige aanmelding inschakelen: klik op de knop In-/uitschakelen om SSO in te schakelen.
 - Type eenmalige aanmelding: selecteer Cisco IDS.



Stap 15

Klik op het tabblad SSO Configuration en geef de configuratiedetails op:

a. OpenID Connect-provider

URL voor primaire gebruikersinfo

- De URL van het eindpunt van gebruikersinformatie van de primaire Cisco IDS-server.
- Deze URL valideert het gebruikerstoken/API met gebruikersinformatie.
- Het is in formaat: <https://cisco-ids-1:8553/ids/v1/oauth/userinfo> waar cisco-ids-1 op de Fully Qualified Domain Name (FQDN) van de primaire Cisco IDS-server wijst.

Gebruikersidentificatieclaim Naam

- De naam van de claim die wordt geretourneerd door de URL van het gebruikersinfo-endpoint, die de gebruikersnaam in Unified of Packaged CCE identificeert.
- De claimnaam en de gebruikersnaam in Unified of Packaged CCE moeten overeenkomen.
- Dit is een van de beweringen die zijn verkregen in antwoord op de validering van de Bearer-token.
- Als de gebruikersnaam van agenten in Unified of Packaged CCE overeenkomt met de naam van het hoofd van de gebruiker, verstrek "upn" als de waarde voor het veld voor de naam van de gebruikersidentiteit.
- Als de gebruikersnaam van agenten in Unified of Packaged CCE overeenkomt met de naam van de SAM-account, geef "sub" op als de waarde voor het veld voor de gebruikersnaam.

URL voor secundaire gebruikersinformatie

- De secundaire URL van het gebruikersinfo-endpoint van de Cisco IDS-server.
- Het is in formaat: <https://cisco-ids-2:8553/ids/v1/oauth/userinfo> waar cisco-ids-2 op de Volledig Gekwalificeerde Naam van het Domein (FQDN) van de Secundaire server van Cisco IDS wijst.

URL-methode voor gebruikersinfo

- De HTTP-methode die door ECE wordt gebruikt voor het maken van bevestigingsoproepen voor tokens aan toonder naar de URL van het gebruikersinfo-endpoint.
- Selecteer POST uit de lijst van voorgestelde opties (de POST wordt hier geselecteerd om de methode van de IDS-server aan te passen).

POST: Methode die wordt gebruikt om gegevens naar de Cisco IDS-server op het opgegeven eindpunt te verzenden.

Duur van access Token Cache (seconden)

- De duur in seconden waarvoor een Bearer-token in ECE moet worden opgeslagen.
- Tokens aan toonder waarvoor validatieoproepen succesvol zijn, worden alleen in caches opgeslagen. (Minimumwaarde: 1; maximumwaarde 30)

Aanmelden bij SSB buiten Finesse toestaan

- Klik op deze knop in-/uitschakelen als u gebruikers met een beheerder- of supervisor-rol wilt toestaan om in de verdeling van ECE buiten Finesse te tekenen met behulp van hun SSO-inloggegevens.
- Indien ingeschakeld, moet informatie onder de secties Identity Provider en Service Provider worden verstrekt.
- Dit vereist dat uw IDp configuratie toestaat voor een gedeelde IDp server.



Partition

Configurations

Select Configuration

General **SSO Configuration**

OpenId Connect Provider

Primary User Info Endpoint URL*	<input type="text" value="https://ids-fqdn:8553/ids/v1/oauth/u ..."/>
User Identity Claim Name*	<input type="text" value="upn"/>
Secondary User Info Endpoint URL	<input type="text" value=""/>
User Info Endpoint URL Method*	<input type="text" value="POST"/>
Access Token Cache Duration (Seconds)*	<input type="text" value="30"/>
Allow SSO Login Outside Finesse	<input checked="" type="checkbox"/>

b. Identiteitsleverancier

Entiteits-ID

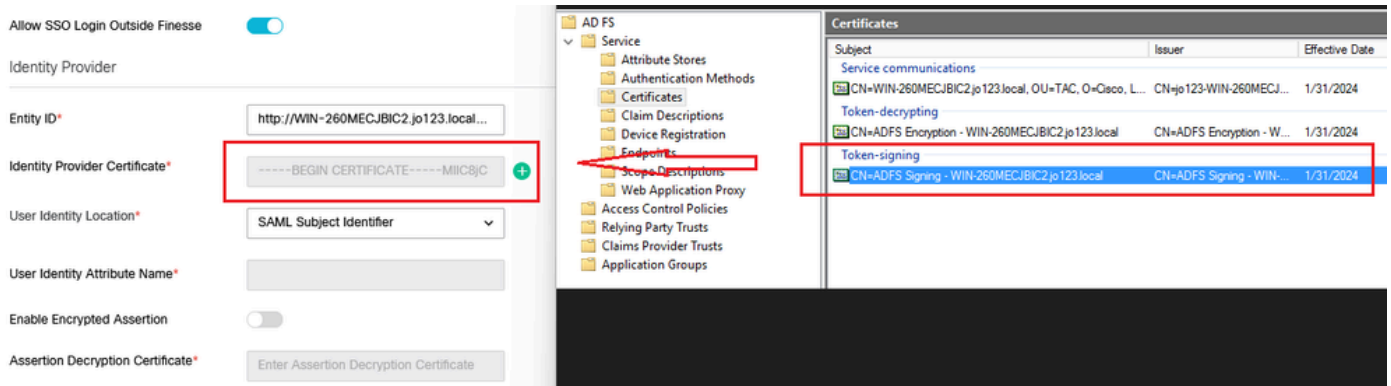
- ID-entiteit van de IDp-server.

Opmerking: deze waarde moet exact overeenkomen met de 'Federation Service Identifier'-waarde in de AD FS-beheerconsole.

The screenshot displays the AD FS Management console interface. On the left, a navigation pane shows 'Single Sign-On' selected, with 'Configurations' expanded. The main area shows the 'Configurations' page for the 'Agent' configuration, with the 'SSO Configuration' tab active. Under the 'Identity Provider' section, the 'Entity ID*' field is highlighted with a red box and contains the value 'http://WIN-260MECJBIC2.jo123.local...'. A red arrow points from this field to the 'Federation Service Properties' dialog box on the right. The dialog box has the 'General' tab selected, and the 'Federation Service Identifier' field is also highlighted with a red box, containing the value 'http://WIN-260MECJBIC2.jo123.local/adfs/services/trust'. Other fields in the dialog include 'Federation Service display name' (JO123 ADFS), 'Federation Service name' (WIN-260MECJBIC2.jo123.local), and 'Web SSO lifetime (minutes)' (480). There are also checkboxes for 'Enable delegation for service administration', 'Allow Local System account for service administration', and 'Allow Local Administrators group for service administration' (checked).

Certificaat van identiteitsverstrekker

- Het publieke sleutelcertificaat.
- Het certificaat moet beginnen met "-----BEGIN CERTIFICAAT-----" en eindigen met "-----END CERTIFICAAT-----"
- Dit is het Token-ondertekeningscertificaat in de AD FS-beheerconsole > Service > Certificaten > Token-ondertekening.



Gebruikersidentificatielocatie

- Selecteer SAML Onderwerp Identifier om de identiteitslocatie in het certificaat in te stellen op de standaard SAML onderwerp identifier, zoals in het onderwerp in de SAML-bewering, bijvoorbeeld de gebruikersnaam in de <saml:Onderwerp>.
- Selecteer SAML Attribute om de identiteitslocatie toe te wijzen aan een specifiek kenmerk in het certificaat, bijvoorbeeld e-mailadres. Vermeld de eigenschap in het veld Naam gebruikersidentiteitskenmerk.

Naam van gebruikersidentificatie-kenmerk

- Alleen van toepassing als de waarde voor de locatie van de gebruikers-id een SAML-kenmerk is.
- Dit kan worden aangepast binnen de SAML-assertie en worden gebruikt om een ander kenmerk te selecteren voor de verificatie van gebruikers, zoals een e-mailadres.
- Het kan ook worden gebruikt om nieuwe gebruikers te maken met een SAML Attribute.
- Bijvoorbeeld, als een gebruiker wordt geïdentificeerd door de waarde die in het email.address attribuut wordt verstrekt, en de waarde van e-mailadres dat wordt verstrekt geen gebruiker in het systeem aanpast, wordt een nieuwe gebruiker gemaakt met de verstrekte SAML attributen.

Encrypted Assertion inschakelen (optioneel)

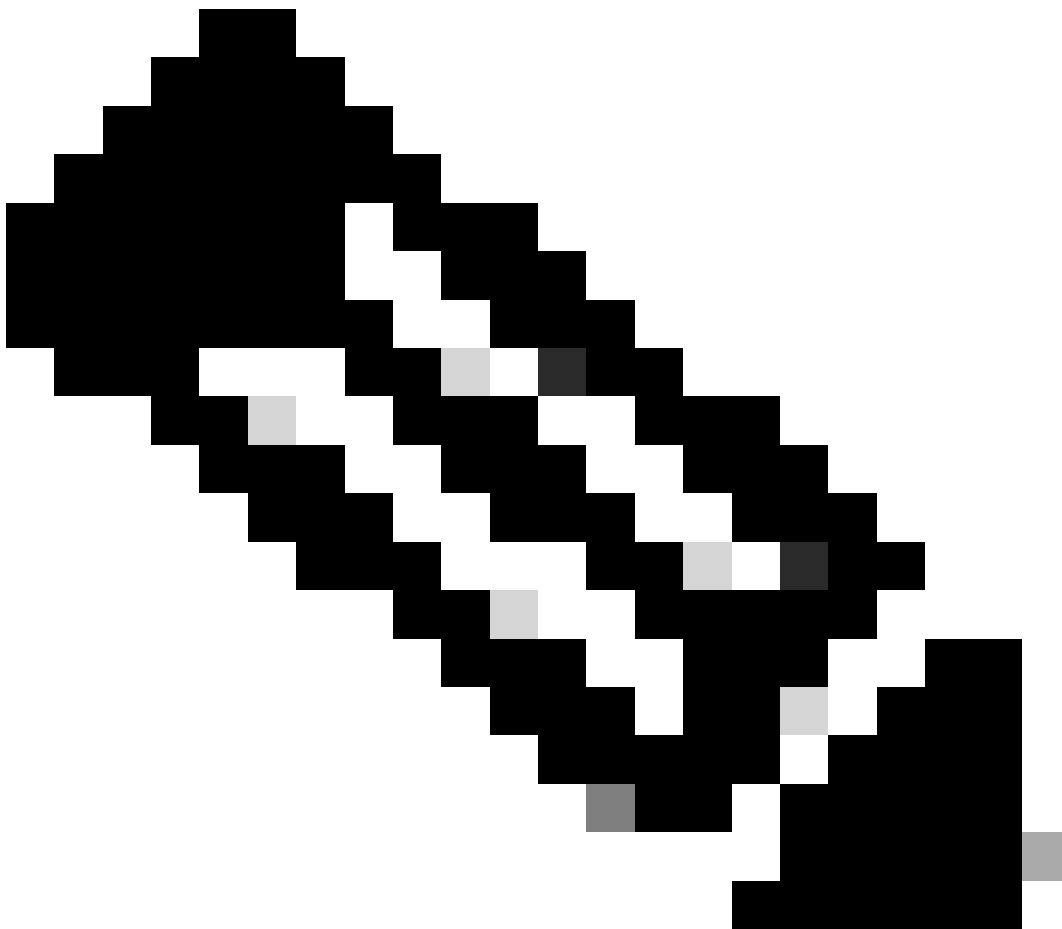
- Als u versleutelde bevestiging met de Identity Provider voor consolelogin wilt inschakelen, klikt u op de knop In-/uitschakelen om de waarde in te stellen op Ingeschakeld.
- Als dit niet het geval is, stelt u de waarde in op Uitgeschakeld.

Certificaat voor assertiedecryptie

Als de optie Versleutelde bewering inschakelen is ingesteld op Ingeschakeld, klikt u op de knop Zoeken en toevoegen en bevestigt u uw keuze om het certificaat te wijzigen.

Geef de informatie in het venster Assertion Decryption Certificate op:

- Java Keystore File: Geef het bestandspad van uw Java Keystore File op. Dit bestand heeft de .jks-indeling en bevat de decryptie-sleutel die het systeem nodig heeft om toegang te krijgen tot bestanden die zijn beveiligd door de Identity Provider.
 - Aliasnaam: de unieke identicator voor de decryptiesleutel.
 - Keystore Wachtwoord: Het wachtwoord dat nodig is voor het openen van het Java Keystore Bestand.
 - Sleutelwachtwoord: het wachtwoord dat nodig is om de decryptiesleutel van de alias te kunnen gebruiken.
-



Opmerking: Dit moet overeenkomen met het certificaat op het tabblad 'Encryptie' van de geconfigureerde ECE Relying Party Trust op AD FS-beheerconsole.

c. Serviceprovider

Door serviceproviders geïnitieerde verificatie

- Stel de knevelknop in op Ingeschakeld.

Entiteits-ID

- Vermeld de externe URL van de ECE-applicatie.

The image shows two screenshots related to configuring a Service Provider for ECE Console.

The left screenshot shows the 'Service Provider' configuration page. The 'Service Provider Initiated Authentication' toggle is turned on. The 'Entity ID*' field is highlighted with a red box and contains the URL 'https://ece126web1a.jo123.local/'. Other fields include 'Request Signing Certificate*' (masked with asterisks), 'Signing Algorithm*' (set to SHA-256), 'Identity Provider Login URL*' (https://WIN-260MECJBIC2.jo123.loc...), and 'Identity Provider Logout URL' (https://ece126web1a.jo123.local/def...).

The right screenshot shows the 'ECE Console Properties' dialog box. The 'Identifiers' tab is selected and highlighted with a red box. The 'Display name' is 'ECE Console'. The 'Relying party identifier' field is empty. Below it, the 'Relying party identifiers' list contains one entry: 'https://ece126web1a.jo123.local/', which is also highlighted with a red box. There are 'Add' and 'Remove' buttons next to the list.

Ondertekeningscertificaat aanvragen

- Een Java Keystore (JKS) certificaat is nodig om de benodigde informatie te verstrekken.
- Upload het .jks-bestand met behulp van de aliasnaam en het keystore/key wachtwoord dat is gegenereerd in stap 11.




Opmerking: Dit moet overeenkomen met het geüploade certificaat op het tabblad 'Handtekening' van de geconfigureerde ECE Relying Party Trust op AD FS Management console.

Service Provider

Service Provider Initiated Authentication

Entity ID*

Request Signing Certificate* 

Signing Algorithm*


Identity Provider Login URL*


Identity Provider Logout URL

ECE Console Properties

Organization Endpoints Proxy Endpoints Notes Advanced
Monitoring Identifiers Encryption **Signature** Accepted Claims

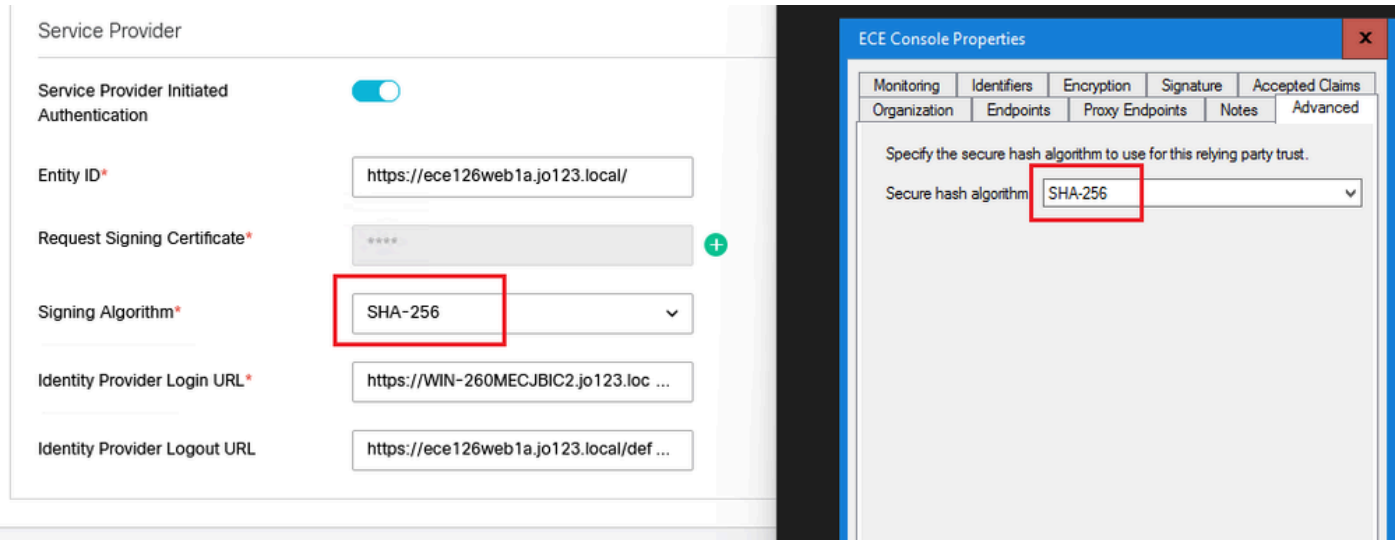
Specify the signature verification certificates for requests from this relying party.

Subject	Issuer	Effective Date	Expiration
 CN=ece126a...	CN=ece126app...	1/31/2024 2:21:...	1/29/20...



Algoritme ondertekenen

- Stel het ondertekeningsalgoritme in voor de serviceprovider.
- Als u ADFS gebruikt, moet deze waarde overeenkomen met het algoritme dat is geselecteerd in het vertrouwen van de vertrouwende partij dat voor ECE is gemaakt onder het tabblad Advanced.



Aanmelden bij identiteitsprovider-URL

- De URL voor SAML-verificatie.
- Voor ADFS is dit bijvoorbeeld <http://<ADFS>/adfs/ls>.

URL voor aanmelding bij identiteitsprovider

- De URL waarnaar gebruikers worden omgeleid bij uitloggen. Dit is optioneel en kan elke URL zijn.
- Bijvoorbeeld, kunnen de agenten aan <https://www.cisco.com> of een andere URL na SSO logout worden opnieuw gericht.

Stap 16

Klik op Opslaan

De URL van de webserver/LB in de instellingen van de partitie instellen

Stap 17

Zorg ervoor dat de juiste URL voor de webserver/LB is ingevoerd onder de instellingen voor partitie > selecteer het tabblad Apps en navigeer naar Algemene instellingen > Externe URL van de toepassing



Partition

General Settings

Chat & Messaging

Email

General Settings

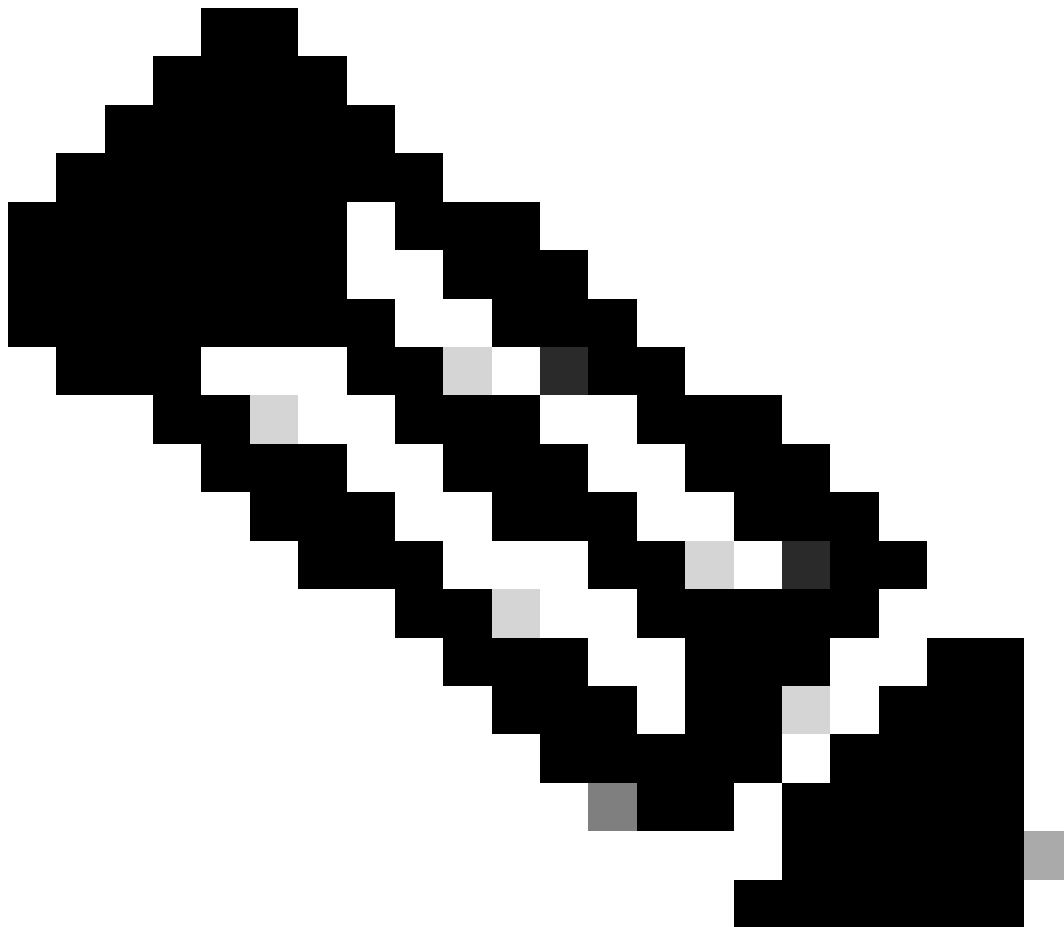
Knowledge

External URL of Application
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
10 - 500. Default value is 100

Maximum number of records to display for NAS search
1 - 100. Default value is 9

SSO configureren voor partitiebeheerders



Opmerking:

- Deze stap is alleen van toepassing op de PCE.
- Dit is voor het ECE-gadget dat wordt gebruikt in de CCE Admin WEB-interface <https://cceadmin>.

Stap 18

Zo configureert u SSO voor Partitiebeheerder

1. Klik in de ECE Admin-console onder het menu op partitieniveau op de optie Beveiliging en selecteer vervolgens Single Sign-On > Configuraties in het menu aan de linkerkant.
2. Selecteer in de vervolgkeuzelijst Select Configuration de optie Partition Administrator's en voer de configuratiegegevens in:

LDAP URL

- De URL van de LDAP-server.
- Dit kan Domain Controller URL (bijvoorbeeld ldap://LDAP_server:389) of Global Catalog URL (bijvoorbeeld ldap://LDAP_server:3268) van de LDAP-server zijn.
- Partitie kan automatisch aan het systeem worden toegevoegd wanneer ECE via de CCE-beheerconsole wordt benaderd als ECE is geconfigureerd met LDAP lookup.
- In Active Directory-implementaties met meerdere domeinen in één bos of waar alternatieve UPN's zijn geconfigureerd, mag de Domain Controller-URL met de standaard LDAP-poorten van 389 en 636 niet worden gebruikt.
- De LDAP integratie kan worden geconfigureerd om de Global Catalog URL met poorten 3268 en 3269 te gebruiken.



Opmerking: het is best practice om de URL van de wereldwijde catalogus te gebruiken. Als u geen GC gebruikt, is een fout in de ApplicationServer-logbestanden als volgt.

- Uitzondering bij LDAP-verificatie <@>
javax.naming.PartialResultException: Unprocessed Continuation Reference(s);
resterende naam 'DC=example, DC=com'

DN-kenmerk

- Het attribuut van de DN dat de gebruikerslogin naam bevat.
- Bijvoorbeeld, userPrincipalName.

Basis

- De waarde die is opgegeven voor Base wordt door de applicatie gebruikt als de zoekbasis.
- Zoekbasis is de startlocatie voor zoeken in de LDAP directory tree.
- Bijvoorbeeld DC=mycompany, DC=com.

DN voor LDAP-zoekopdracht

- Als uw LDAP systeem niet anonieme bind toestaat, geef dan de Distinguished Name (DN) van een gebruiker die zoekrechten heeft in de LDAP directory tree.
- Als de LDAP-server anoniem bindt, laat u dit veld leeg.

Wachtwoord

- Als uw LDAP systeem niet anonieme bind toestaat, geef dan het wachtwoord van een gebruiker die zoekrechten heeft in de LDAP directory tree.
- Als de LDAP-server anoniem bindt, laat u dit veld leeg.

Stap 19

Klik op Opslaan

Dit voltooit nu de Single Sign-On configuratie voor Agenten en Partition Administrators in ECE.

Probleemoplossing

Overtrek-niveau instellen

1. Klik in de ECE Admin-console onder het menu op partitieniveau op de optie Systeembronnen en selecteer vervolgens Logbestanden verwerken in het menu links.
2. Selecteer in de lijst met processen het ApplicationServer-proces > het gewenste overtrek-niveau instellen in het keuzemenu 'Maximale overtrek'.



Opmerking:

- Voor het oplossen van problemen met de SSO-inlogfouten tijdens de eerste configuratie of herconfiguratie, stelt u het proces van ApplicationServer op niveau 7 in.
 - Nadat de fout is gereproduceerd, stelt u het niveau terug in op standaardniveau 4 om overschrijven van de logbestanden te voorkomen.
-

Enterprise Chat and Email

Partition Administrator

Partition

Apps Departments Integration Language Tools Security Services Storage System Resources Tools User

Process 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

Enterprise Chat and Email

Partition

Edit Process Log: ece126app1a:ApplicationServer

Process Logs

General Advanced Logging

Name ece126app1a:ApplicationServer

Description ece126app1a:ApplicationServer

Maximum Trace Level 4 - Info

Log File Name

Maximum File Size

Extensive Logging Duration 4 - Info

Extensive Logging End Time

Problemen oplossen in scenario 1

Fout

- Foutcode: 500
- Fout Beschrijving: De toepassing kan de gebruiker op dit moment niet inloggen omdat de aanmelding bij Identity Provider is mislukt.

Analyse van logboeken

- Aanmelding IDp mislukt - `<samlp:Status><samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Responder" /></samlp:Status>`
- Hier geeft de status "Responder" aan dat er een probleem is aan de kant van de AD FS - in dit geval voornamelijk met het "Vraag Ondertekeningscertificaat" geüpload op de ECE Admin-console (SSO Configuration > Service Provider) en het certificaat geüpload naar de ECE Relying Party Trust onder het tabblad 'Handtekening'.
- Dit is het certificaat dat wordt gegenereerd met behulp van het Java Keystore File.

Toepassingsserverlogbestanden - Trackniveau 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_Handler.java:100)
at com.egain.platform.module.security.sso.handler.SAML2_0_Handler.validateReqWithAttributes(SAML2_0_Handler.java:100)
at com.egain.platform.module.security.sso.handler.SAML2_0_Handler.validateReqWithAttributes(SAML2_0_Handler.java:100)
at com.egain.platform.module.security.sso.handler.OpenIDConnect_Handler.validateReqWithAttributes(OpenIDConnect_Handler.java:100)
at com.egain.platform.module.security.sso.admin.SSOAdministrator.validateRequestWithAttributes(SSOAdministrator.java:100)
at com.egain.platform.module.security.sso.controller.SSOControllerServlet.doPost(SSOControllerServlet.java:100)
.
.
.
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 Provider is not available.
```

```
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:
```

Resolutie

- Raadpleeg de configuratie 'Aanvraagondertekeningscertificaat' onder de sectie 'Agent Single Sign-On configureren - Serviceprovider'.
- Zorg ervoor dat het in Stap 11 gegenereerde Java Keystore .jks-bestand is geüpload naar

het veld "Certificaat aanvragen" op de ECE Admin-console onder SSO Configuration > Select Configuration 'Agent' > 'SSO Configuration' tabblad > Service Provider > Certificaat aanvragen.

- Zorg ervoor dat het .crt bestand is geüpload onder het tabblad 'Handtekening' van de ECE Relying Party Trust (Stap 12).

Problemen oplossen in scenario 2

Fout

- Foutcode: 400
- Error Description: SAML Response token is ongeldig: handtekening validatie is mislukt.

Analyse van logboeken

- Deze fout geeft aan dat het certificaat een verschil bevat tussen het 'Token-signed certificate' op ADFS en het 'Identity provider certificate' in de ECE SSO Configuration.

Toepassingsserverlogbestanden - Trackniveau 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:
```

Resolutie

- De fout in het logfragment "Kan certificaat niet parsen: java.io.IOException: Onvolledige gegevens" geeft aan dat de inhoud van het identiteitsbewijs niet correct is ingevoerd
- Om dit op te lossen: op het AS FS Management > AD FS > Service > Certificaten > Token-Signing > Exporteren dit certificaat > openen in een teksteditor > kopiëren alle inhoud > plakken onder 'Identity provider certificate' in de SSO-configuratie > Opslaan.
- Raadpleeg de configuratie 'Identity Provider Certificate' in de sectie 'Configuration Agent single sign-on - Identity Provider' (Stap 15).

Scenario 3 voor probleemoplossing

Fout

- Foutcode: 401-114
- Fout Beschrijving: Gebruiker Identity niet gevonden in SAML attribuut.

Analyse van logboeken

Toepassingsserverlogbestanden - Trackniveau 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_Handler.java:100)  
    at com.egain.platform.module.security.sso.handler.SAML2_0_Handler.unmarshallAndValidateResponse(SAML2_0_Handler.java:110)  
    at com.egain.platform.module.security.sso.handler.SAML2_0_Handler.validateReqWithAttributes(SAML2_0_Handler.java:120)  
    at com.egain.platform.module.security.sso.handler.SAML2_0_Handler.validateReqWithAttributes(SAML2_0_Handler.java:130)  
    at com.egain.platform.module.security.sso.handler.OpenIDConnect_Handler.validateReqWithAttributes(OpenIDConnect_Handler.java:140)  
    at com.egain.platform.module.security.sso.admin.SSOAdministrator.validateRequestWithAttributes(SSOAdministrator.java:150)  
    at com.egain.platform.module.security.sso.controller.SSOControllerServlet.doPost(SSOControllerServlet.java:160)  
    at javax.servlet.http.HttpServlet.service(HttpServlet.java:706)  
    at javax.servlet.http.HttpServlet.service(HttpServlet.java:854)  
    at java.lang.Thread.run(Thread.java:830) [?:?]
```

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

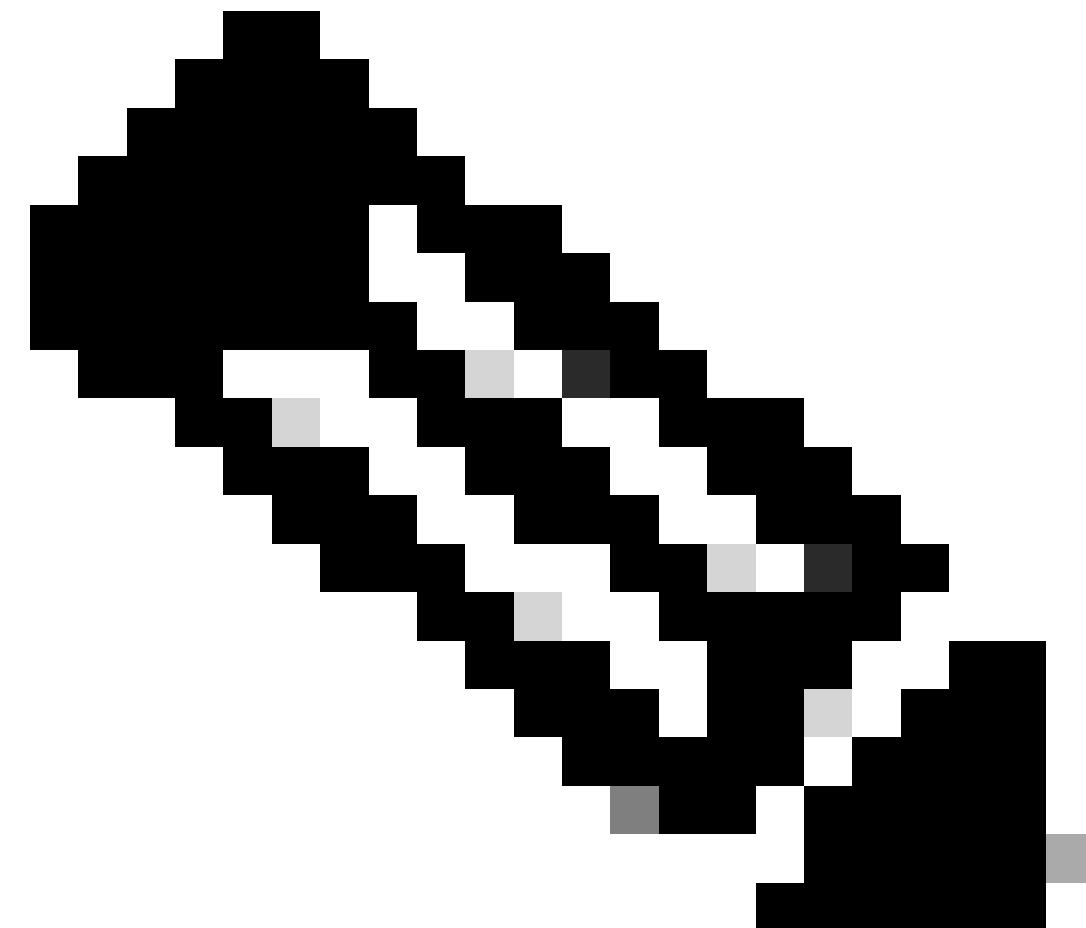
```
2024-02-01 01:44:32.083 GMT+0000 <@> DEBUG <@> [1220:qtp815320891-1220] <@> ProcessId:7716 <@> PID:1 <@>
```

Resolutie

- Deze fout geeft een configuratieprobleem/mismatch aan in de velden 'Gebruikersidentiteitslocatie' en 'Gebruikersidentiteitsnaam'.
- Controleer en corrigeer de 'User Identity Location' en de 'User Identity Attribute Name' in de ECE Admin-console, onder Single Sign-On > Configuraties > in de vervolgkeuzelijst Select Configuration, selecteer Agent > SSO Configuration tabblad > Identify Provider (Stap 15).

Gerelateerde informatie

Dit zijn de belangrijkste documenten die u grondig moet herzien voordat u een ECE-installatie of integratie start. Dit is geen volledige lijst van ECE-documenten.



Opmerking:

-
- De meeste ECE-documenten hebben twee versies. Zorg ervoor dat u de versies downloadt en gebruikt die voor PCCE zijn. De documenttitel heeft of voor Packaged Contact Center Enterprise of (voor PCCE) of (voor UCCE en PCCE) na het versienummer.
 - Zorg ervoor dat u de startpagina controleert op Cisco Enterprise Chat en E-mail documentatie voor alle updates voorafgaand aan de installatie, upgrade of integratie.
 - <https://www.cisco.com/c/en/us/support/customer-collaboration/cisco-enterprise-chat-email/series.html>
-

ECE versie 12.6(1)

- [Beheerdershandleiding voor Enterprise Chat en E-mail](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.