

Configurazione e risoluzione dei problemi di SSO per gli agenti e l'amministratore delle partizioni in ECE

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Procedura di configurazione](#)

[Configurazione dell'attendibilità componente per ECE](#)

[Configurazione di un provider di identità](#)

[Creazione e importazione di certificati](#)

[Configurazione di Single Sign-On dell'agente](#)

[Impostare l'URL del server Web o del bilanciamento del carico nelle impostazioni della partizione](#)

[Configurazione di SSO per gli amministratori della partizione](#)

[Risoluzione dei problemi](#)

[Impostazione del livello di traccia](#)

[Risoluzione dei problemi dello scenario 1](#)

[Errore](#)

[Analisi log](#)

[Risoluzione](#)

[Scenario di risoluzione dei problemi 2](#)

[Errore](#)

[Analisi log](#)

[Risoluzione](#)

[Scenario di risoluzione dei problemi 3](#)

[Errore](#)

[Analisi log](#)

[Risoluzione](#)

[Informazioni correlate](#)

Introduzione

In questo documento vengono descritti i passaggi necessari per configurare Single Sign-On (SSO) per gli agenti e gli amministratori delle partizioni in una soluzione ECE.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

Cisco Packaged Contact Center Enterprise (PCCE)

Cisco Unified Contact Center Enterprise (UCCE)

Enterprise Chat and Email (ECE)

Microsoft Active Directory

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

Versione UCCE: 12.6(1)

Versione ECE: 12.6(1)

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

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

È possibile accedere alle console Enterprise Chat and Email (ECE) all'esterno di Finesse; tuttavia, l'SSO deve essere abilitato per consentire ad agenti e supervisor di accedere a ECE tramite Finesse.

È inoltre possibile configurare Single Sign-On per i nuovi amministratori delle partizioni. In questo modo, ai nuovi utenti che accedono al desktop di Cisco Administrator viene concesso l'accesso a Enterprise Chat and Email Administration Console.

Aspetti importanti da notare relativi a Single Sign-On:

- Il processo di configurazione di un sistema per Single Sign-On deve essere eseguito sul nodo Protezione a livello di partizione da un utente della partizione con le azioni necessarie: Visualizza protezione applicazione e Gestisci protezione applicazione.
- Per consentire a supervisor e amministratori di accedere a console diverse da quella dell'agente, una volta abilitato l'SSO, è necessario fornire un URL esterno valido dell'applicazione nelle impostazioni della partizione. Per ulteriori informazioni, vedere Impostazioni generali delle partizioni.
- È necessario un certificato Java Keystore (JKS) per configurare SSO per consentire agli

utenti con ruoli di amministratore o supervisore di accedere alla partizione 1 di ECE all'esterno di Finesse utilizzando le credenziali di accesso SSO. Consultare il reparto IT per ricevere il certificato JKS.

- È necessario importare un certificato SSL (Secure Sockets Layer) di Cisco IDS in tutti i server applicazioni di un'installazione. Per ottenere il file del certificato SSL necessario, contattare il reparto IT o il supporto Cisco IDS.
 - Le regole di confronto del server di database per Unified CCE distinguono tra maiuscole e minuscole. Il nome utente nell'attestazione restituito dall'URL dell'endpoint delle informazioni utente e il nome utente in Unified CCE devono essere uguali. In caso contrario, gli agenti Single Sign-On non vengono riconosciuti come connessi e ECE non può inviare la disponibilità dell'agente a Unified CCE.
 - La configurazione di SSO per Cisco IDS influisce sugli utenti configurati in Unified CCE per Single Sign-On. Verificare che gli utenti che si desidera abilitare per l'SSO in ECE siano configurati per l'SSO in Unified CCE. Per ulteriori informazioni, rivolgersi all'amministratore di Unified CCE.
-

Nota:

- Verificare che gli utenti che si desidera abilitare per l'SSO in ECE siano configurati per l'SSO in Unified CCE.
- In questo documento viene descritto come configurare l'attendibilità della relying part per ECE in una singola distribuzione di AD FS in cui nello stesso computer sono installati Server federativo di risorse e Server federativo di account.
- Per una distribuzione di ADFS divisa, passare alla guida all'installazione e alla configurazione ECE per la versione corrispondente.

Procedura di configurazione

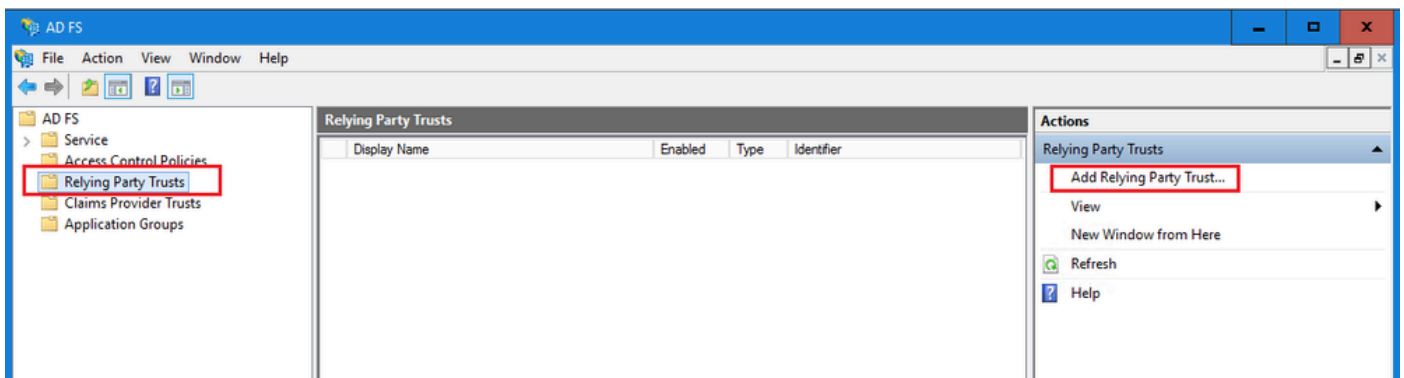
Configurazione dell'attendibilità componente per ECE

Passaggio 1

Aprire la console di gestione di AD FS e selezionare AD FS > Relazioni di trust > Attendibilità componente.

Passaggio 2

Nella sezione Azioni fare clic su Aggiungi attendibilità componente...



Passaggio 3

Nella procedura guidata Aggiungi attendibilità componente fare clic su Start e completare i passaggi seguenti:

- a. Nella pagina Seleziona origine dati, selezionare l'opzione Immettere manualmente i dati sulla parte di risposta e fare clic su Avanti.

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.

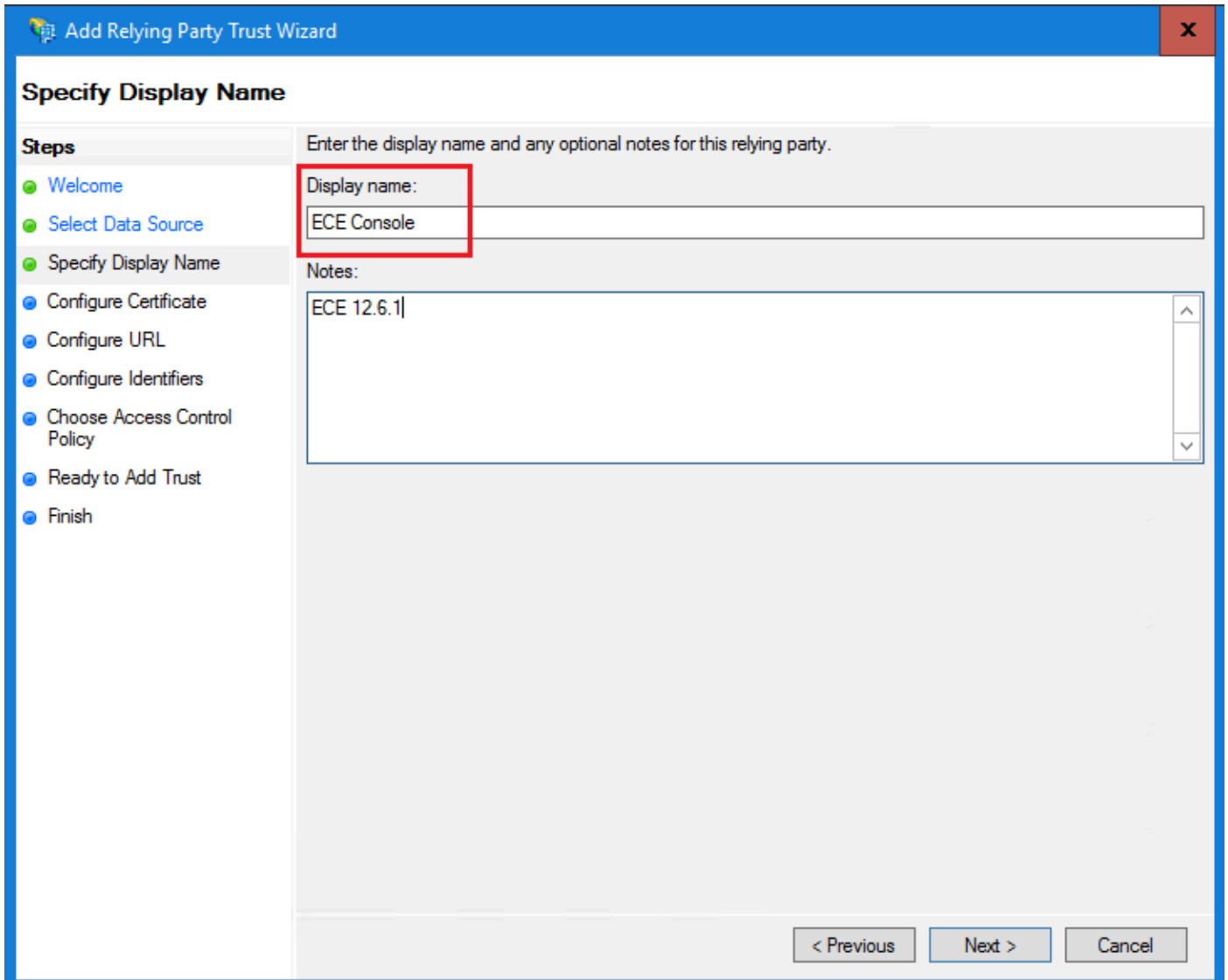
Federation metadata file location:

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. Nella pagina Specificare il nome visualizzato, fornire un nome visualizzato per il componente. Fare clic su Avanti.



c. Nella pagina Configura URL:

i. Selezionare l'opzione Abilita supporto per il protocollo SAML 2.0 Web SSO.

ii. Nel campo URL server SAML 2.0 SSO componente specificare l'URL nel formato: `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.

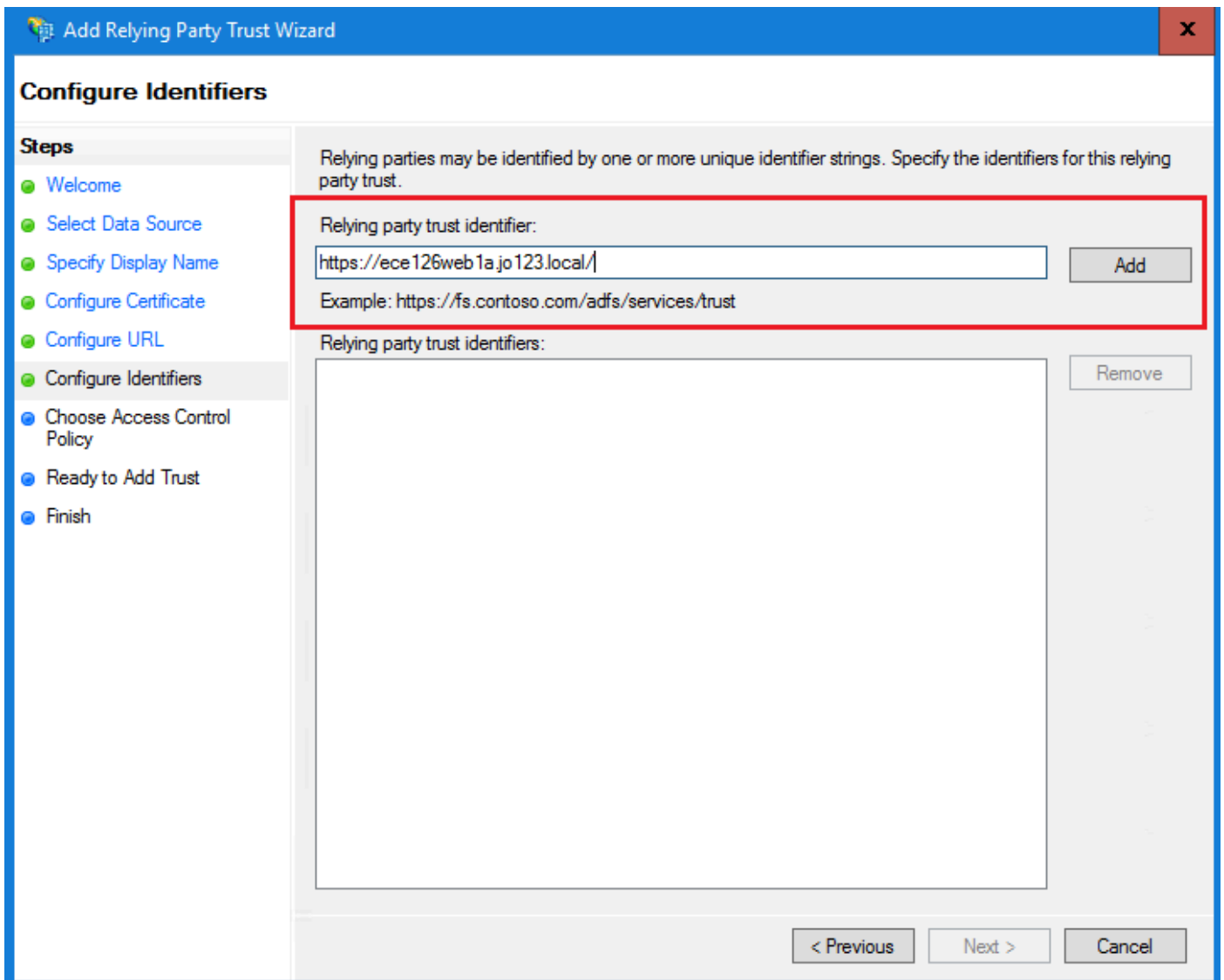
Relying party SAML 2.0 SSO service URL:

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

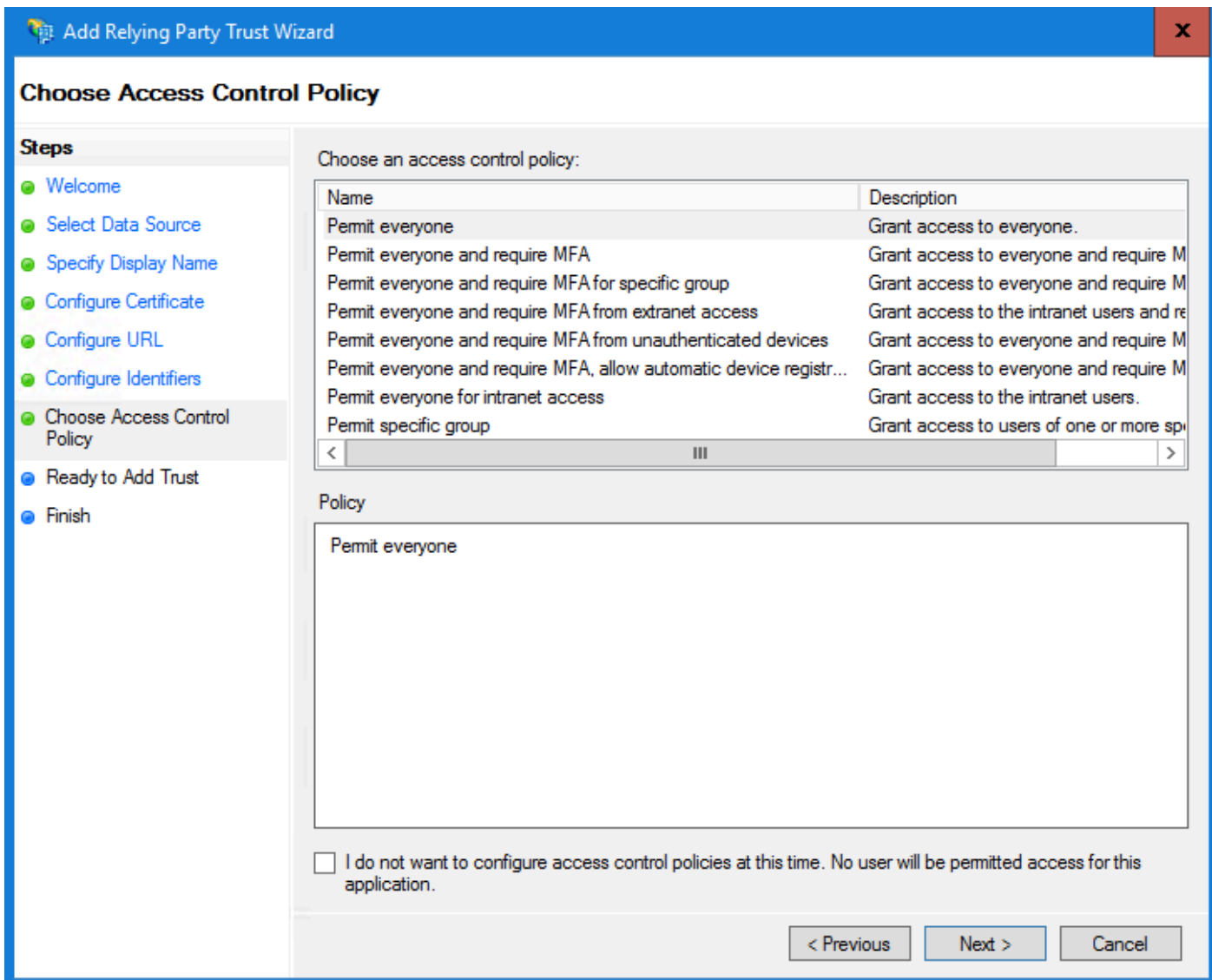
< Previous Next > Cancel

d. Nella pagina Configura identificatori, fornire l'identificatore di attendibilità del componente e fare clic su Aggiungi.

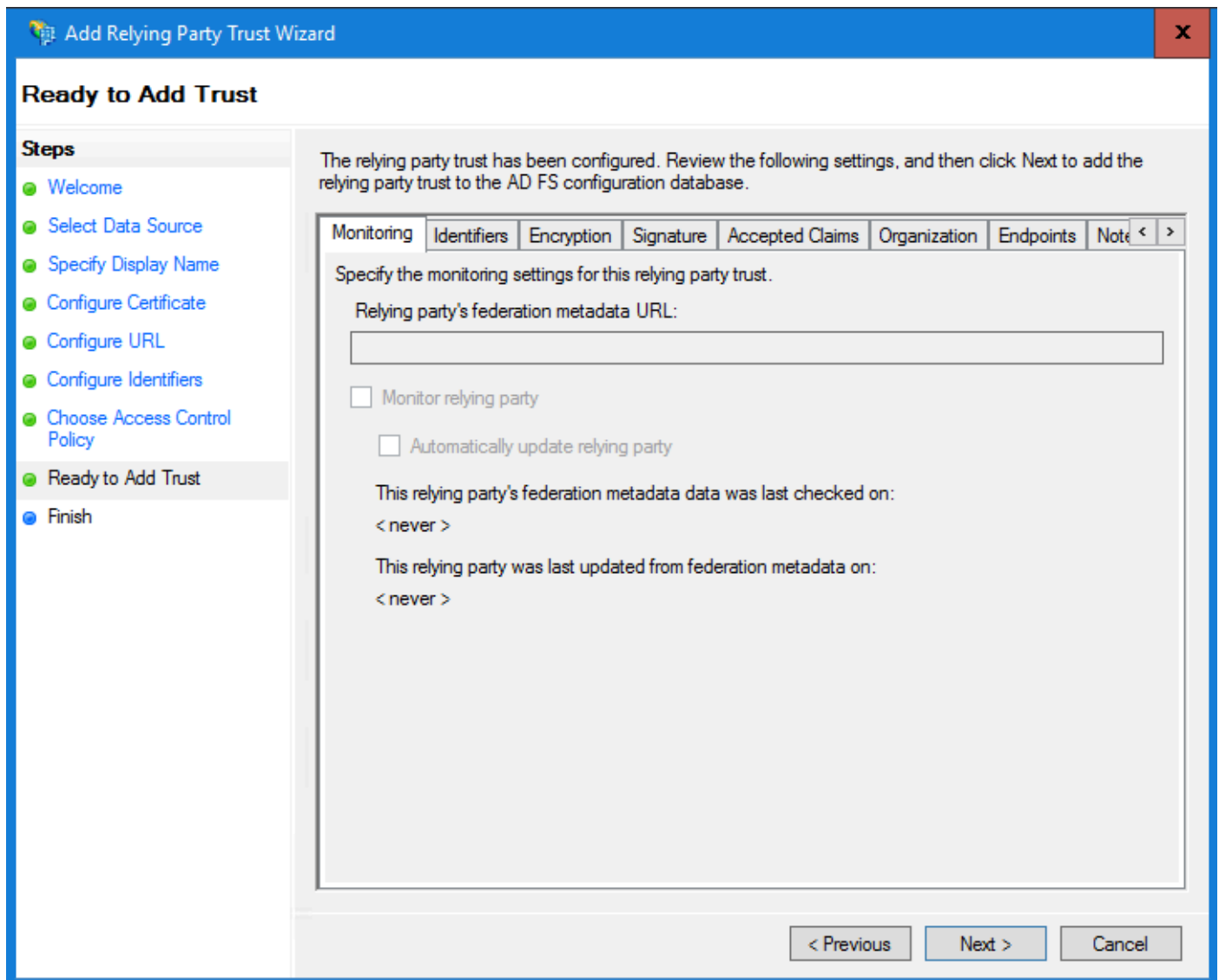
- Il formato del valore deve essere: <https://<FQDN-Server-Web-Or-Load-Balancer>/>



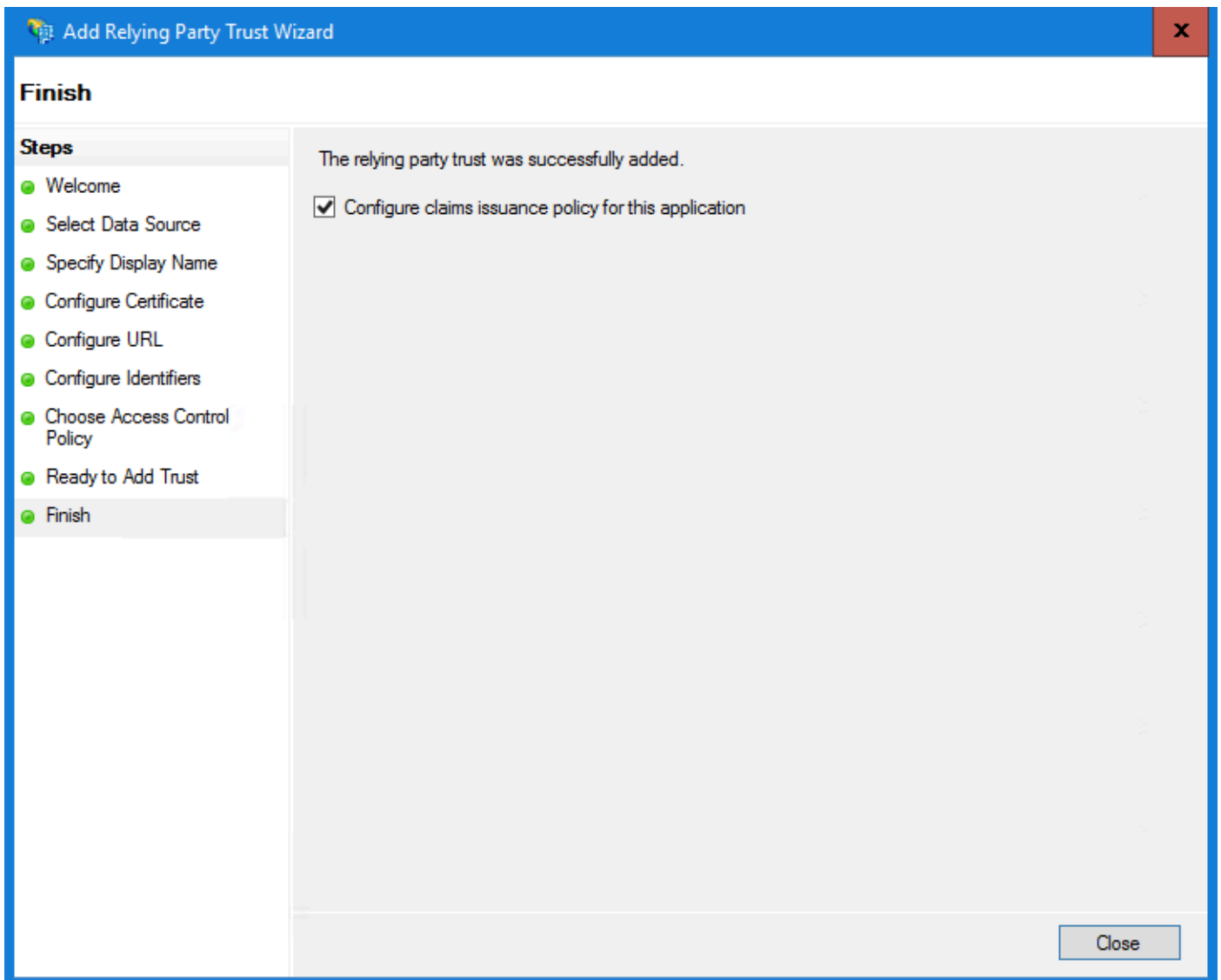
e. Nella pagina Scegli i criteri di controllo di accesso, fare clic su avanti con il criterio predefinito 'Autorizza tutti'.



f. Nella pagina Pronto per aggiungere trust, fare clic su Avanti.

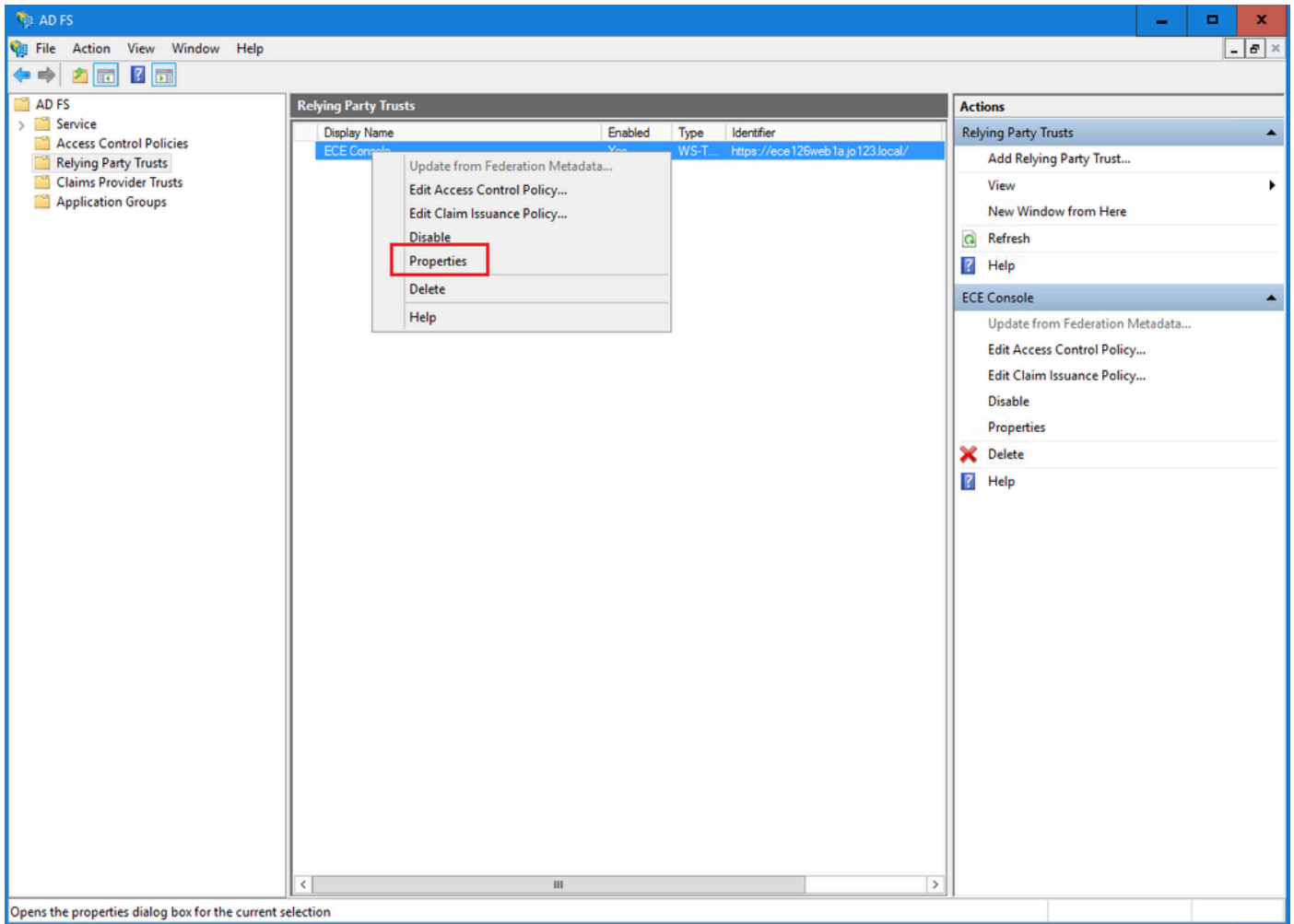


g. Dopo aver aggiunto l'attendibilità del componente, fare clic su Chiudi.



Passaggio 4

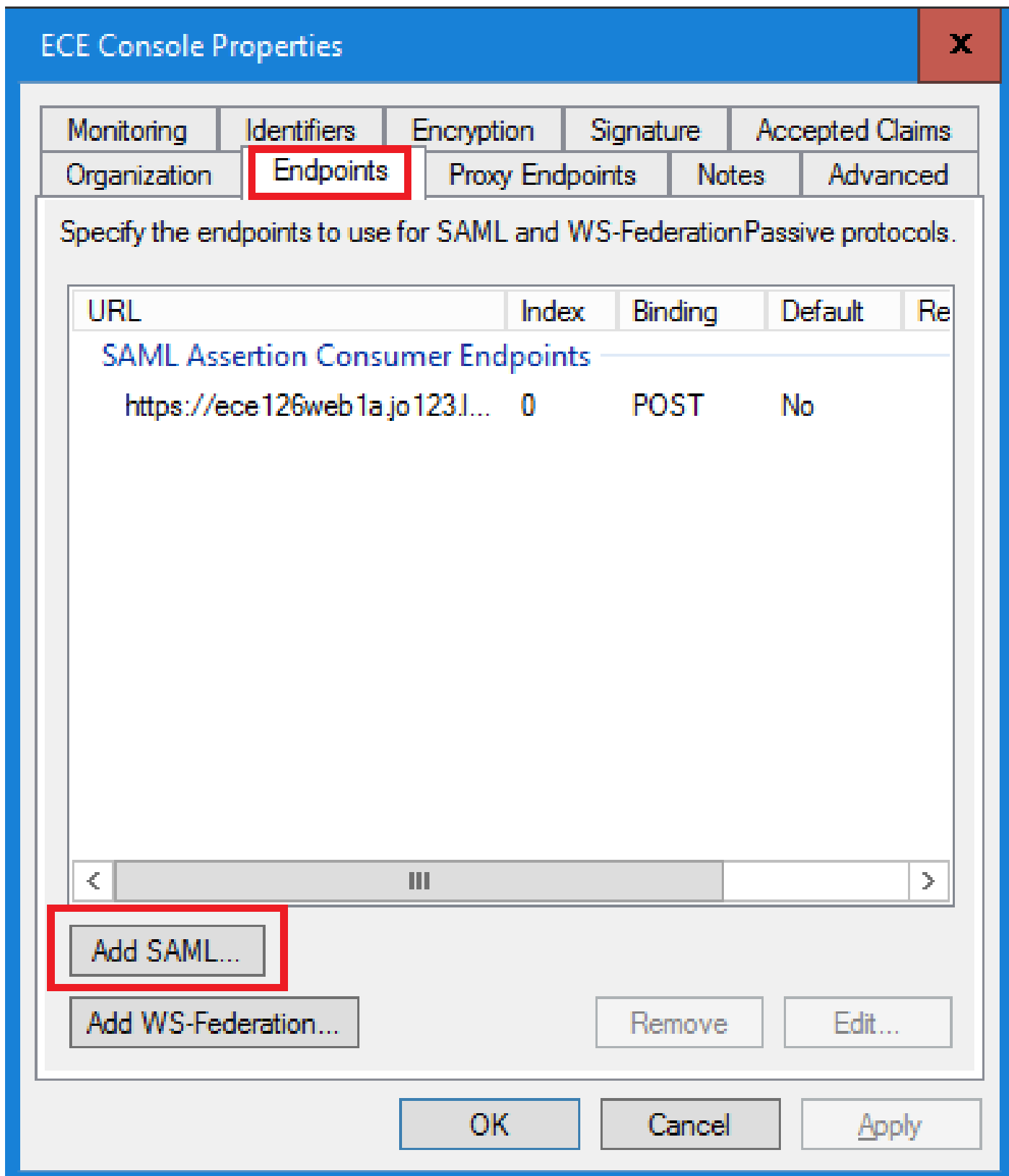
Nell'elenco Attendibilità provider di servizi di base selezionare l'attendibilità del componente creata per ECE e nella sezione Azioni fare clic su Proprietà.



Opens the properties dialog box for the current selection

Passaggio 5

Nella finestra Proprietà, passare alla scheda Endpoints e fare clic sul pulsante Add SAML...



Passaggio 6

Nella finestra Add an Endpoint, configurare come indicato:

1. Selezionare il tipo di endpoint come Disconnessione SAML.
2. Specificare l'URL attendibile come `https://<ADFS-server-FQDN>/adfs/ls/?wa=wsignoutcleanup1.0`
3. Fare clic su 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`

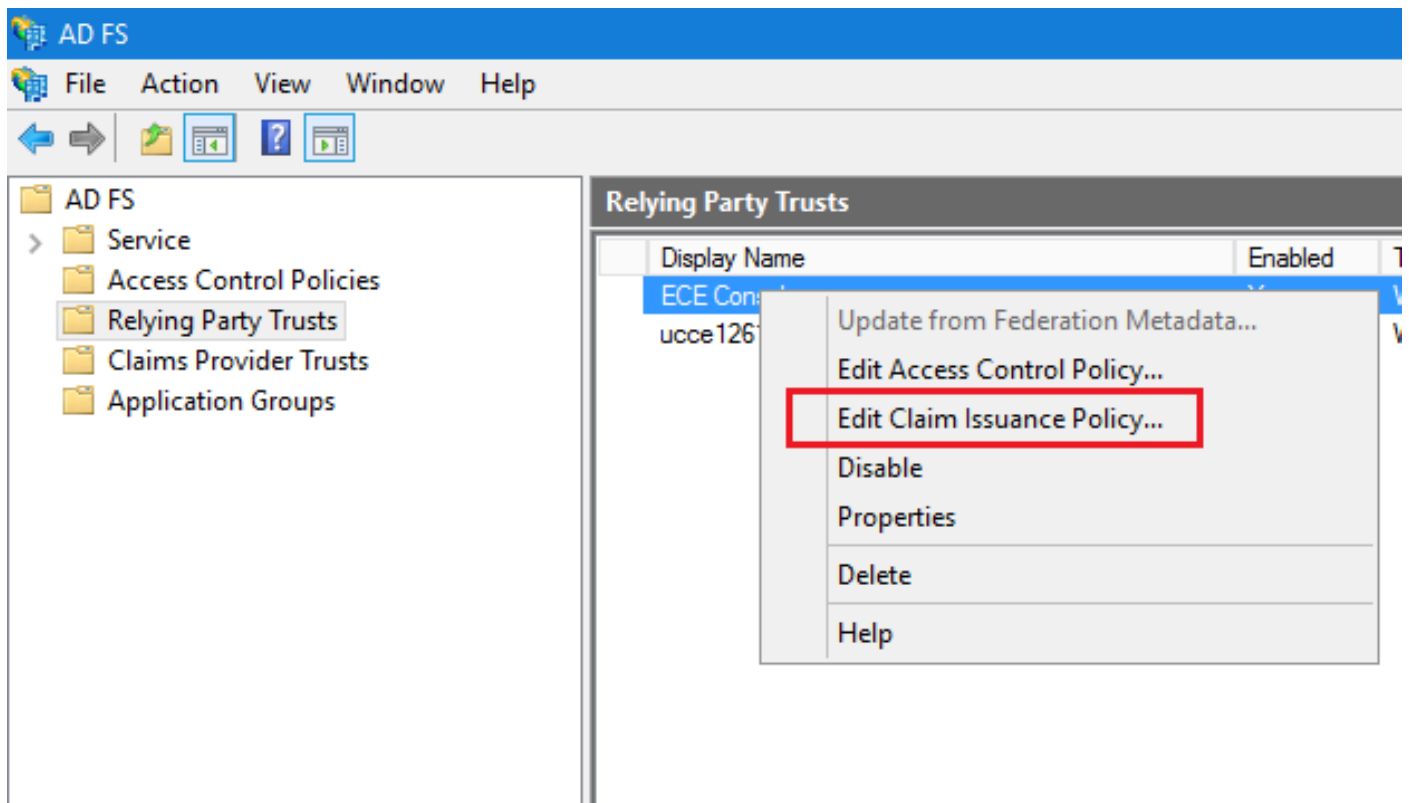
Response URL:

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

OK Cancel

Passaggio 7

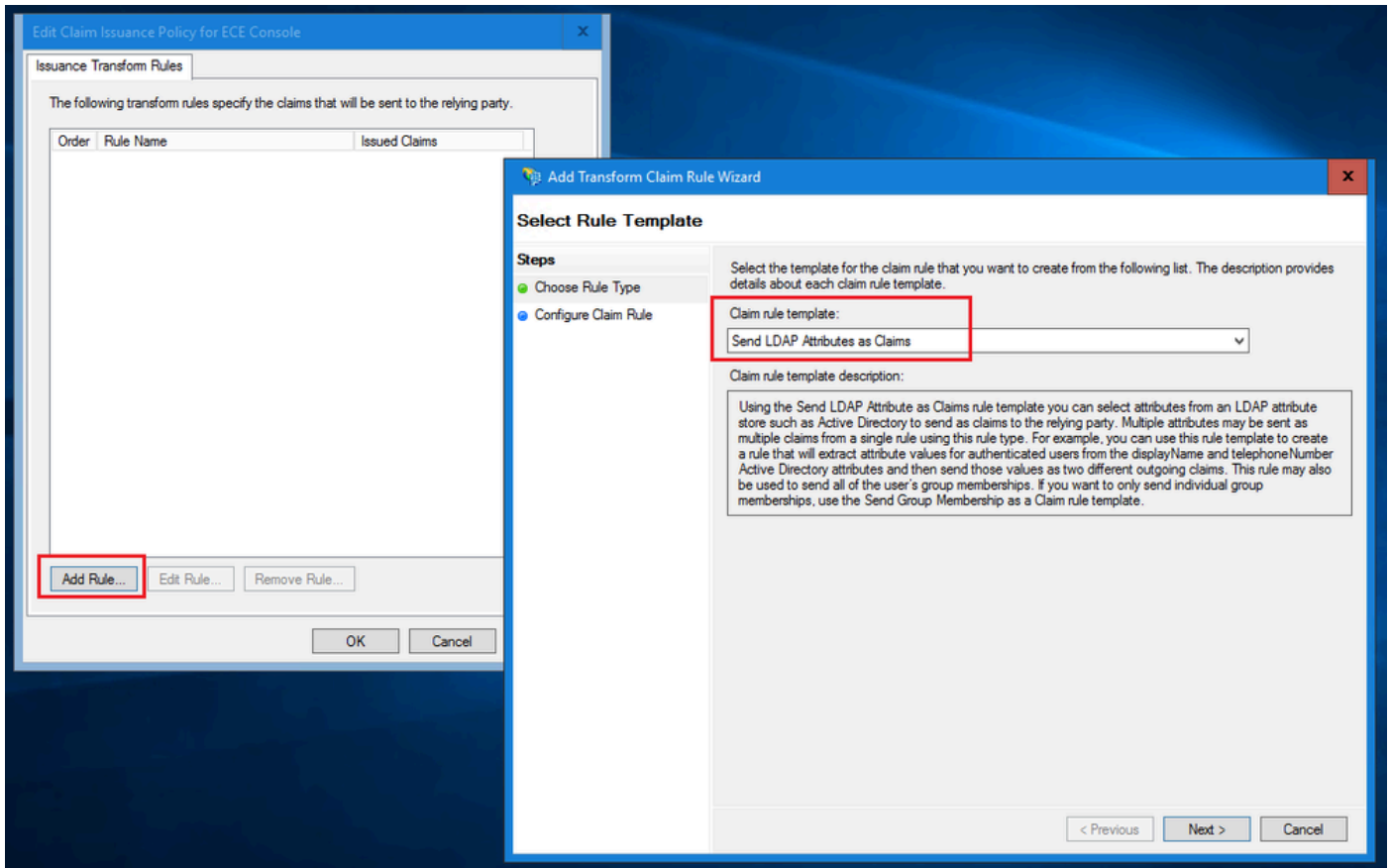
Nell'elenco Trust provider di servizi di base selezionare il trust creato per ECE e nella sezione Azioni fare clic su Modifica polizza di assicurazione attestazione.



Passaggio 8

Nella finestra Modifica polizza assicurativa risarcimento, nella scheda Regole di trasformazione rilascio, fare clic sul pulsante Aggiungi regola... e configurare come mostrato di seguito:

- a. Nella pagina Scegli tipo di regola, selezionare Invia attributi LDAP come attestazioni dall'elenco a discesa e fare clic su Avanti.



b. Nella pagina Configura regola attestazione:

1. Specificare il nome della regola attestazione e selezionare l'archivio attributi.
 2. Definire il mapping dell'attributo LDAP e il tipo di attestazione in uscita.
- Selezionare ID nome come nome del tipo di attestazione in uscita.
 - Fare clic su Fine per tornare alla finestra Modifica polizza assicurativa risarcimento e quindi fare clic su 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

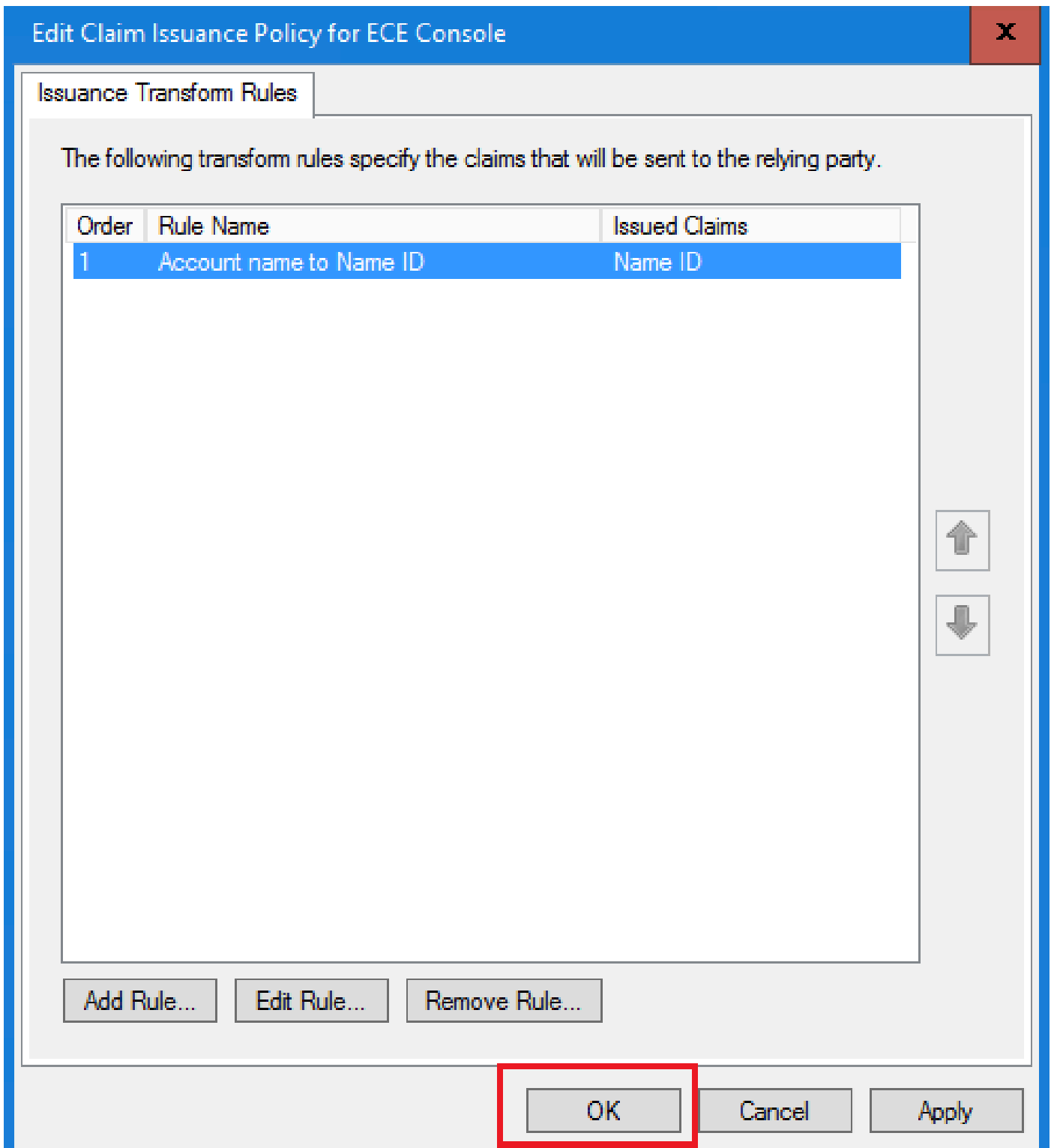
Mapping of LDAP attributes to outgoing claim types:

	LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
▶	User-Principal-Name	Name ID
*		

< Previous

Finish

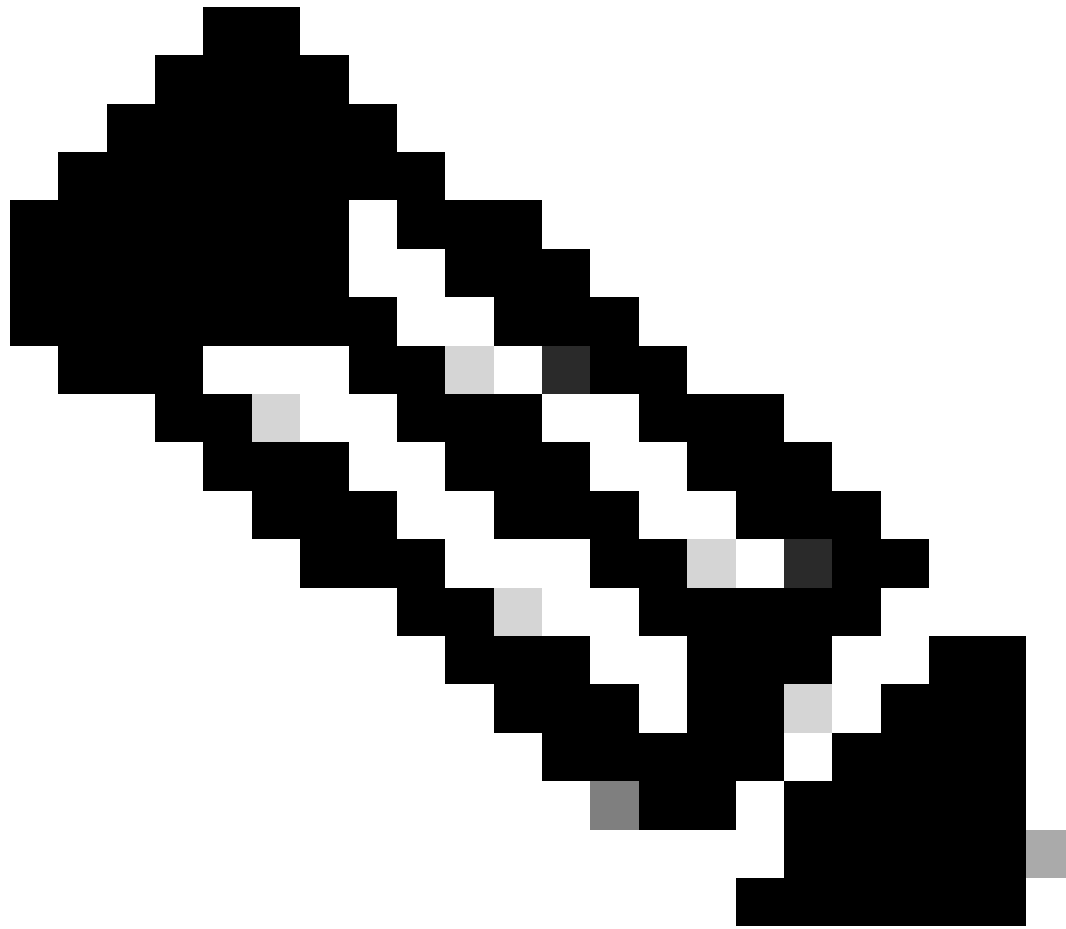
Cancel



Passaggio 9

Nell'elenco Attendibilità provider di servizi fare doppio clic sull'attendibilità del componente ECE creata.

Nella finestra Proprietà visualizzata passare alla scheda Avanzate e impostare l'algoritmo hash di protezione su SHA-1 o SHA-256. Fare clic su OK per chiudere la finestra.



Nota: questo valore deve corrispondere al valore 'Signing algorithm' impostato per 'Service Provider' nelle configurazioni SSO in ECE

Relying Party Trusts

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

ECE Console Properties

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

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

Secure hash algorithm:

OK Cancel Apply

Passaggio 10

Verificare e annotare il valore dell'identificatore del servizio federativo.

- Nella console Gestione ADFS selezionare e fare clic con il pulsante destro del mouse su ADFS > Modifica proprietà servizio federativo > scheda Generale > Identificatore servizio federativo



Nota:

- Questo valore deve essere aggiunto esattamente come lo è quando si configura il valore 'Entity ID' per Identity Provider in Configurazioni SSO in ECE.
 - L'utilizzo di http:// NON significa che ADFS non sia sicuro, ma semplicemente un identificatore.
-

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 options in the menu 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 information about AD FS, including a 'view' section and links for 'More About AD FS' and 'More About Azure Active Directory'. The 'Actions' pane on the right side of the console lists the same set of actions as the context menu. At the bottom of the console, a status bar displays the text 'Edit the federation service properties'.

Federation Service Properties X

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

Configurazione di un provider di identità

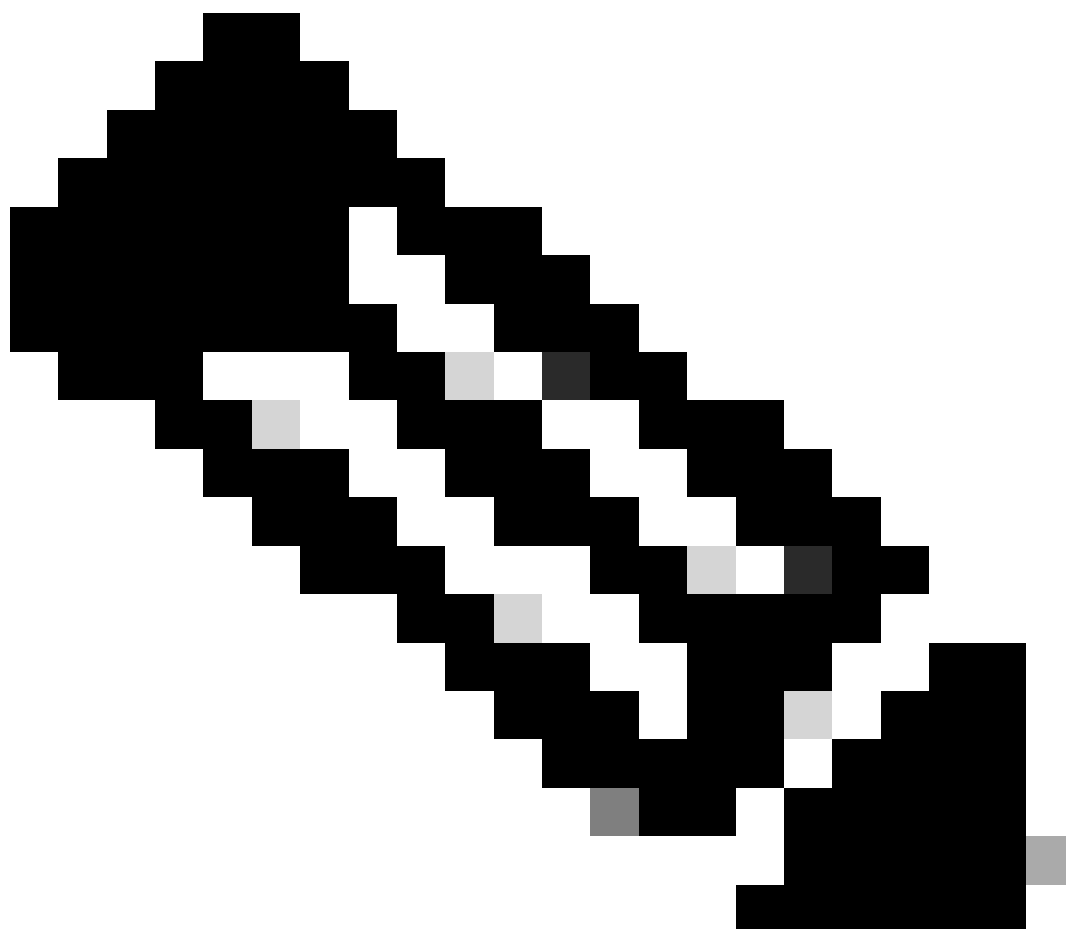
Passaggio 11

È necessario un certificato Java Keystore (JKS) per configurare SSO per consentire agli utenti con ruoli di amministratore o supervisore di accedere alla partizione ECE al di fuori di Finesse utilizzando le credenziali di accesso SSO.

Se si desidera configurare SSO per consentire agli utenti con ruoli di amministratore o supervisore

di accedere alla partizione ECE all'esterno di Finesse utilizzando le credenziali di accesso SSO, il certificato Java Keystore (JKS) deve essere convertito in certificato a chiave pubblica e configurato in Attendibilità componente creata sul server IdP per ECE.

Consultare il reparto IT per ricevere il certificato JKS.

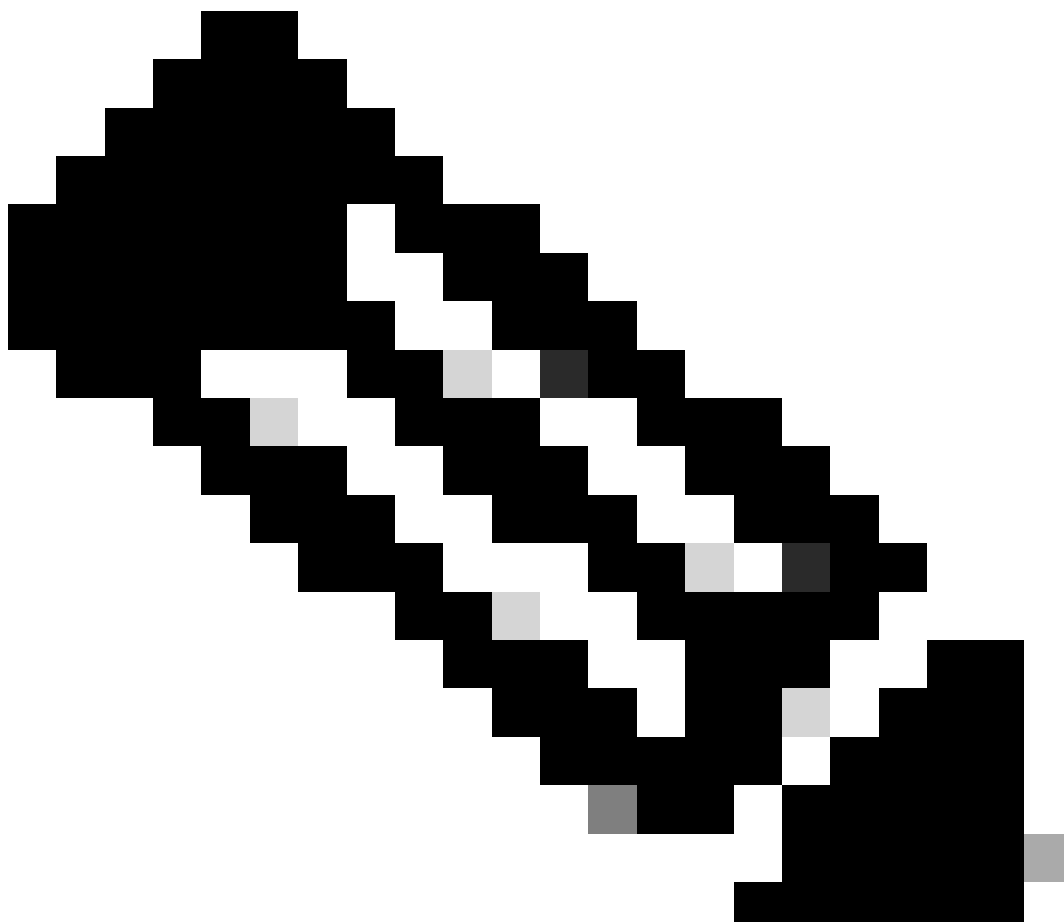


Nota: questi passaggi sono applicabili ai sistemi che utilizzano ADFS come provider di identità. Altri provider di identità possono disporre di metodi diversi per configurare il certificato a chiave pubblica.

Di seguito è riportato un esempio di come è stato generato un file JKS nel laboratorio:

a. Generare JKS:

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



Nota: la password del keystore, il nome alias e la password della chiave immessi qui vengono utilizzati durante la configurazione della configurazione 'Service Provider' in Configurazioni SSO 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. Esportare il certificato:

Questo comando keytool esporta il file di certificato nel formato .crt con nome file

ece126web1a_saml.crt nella directory C:\Temp.

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

Passaggio 12

Configurazione di un provider di identità

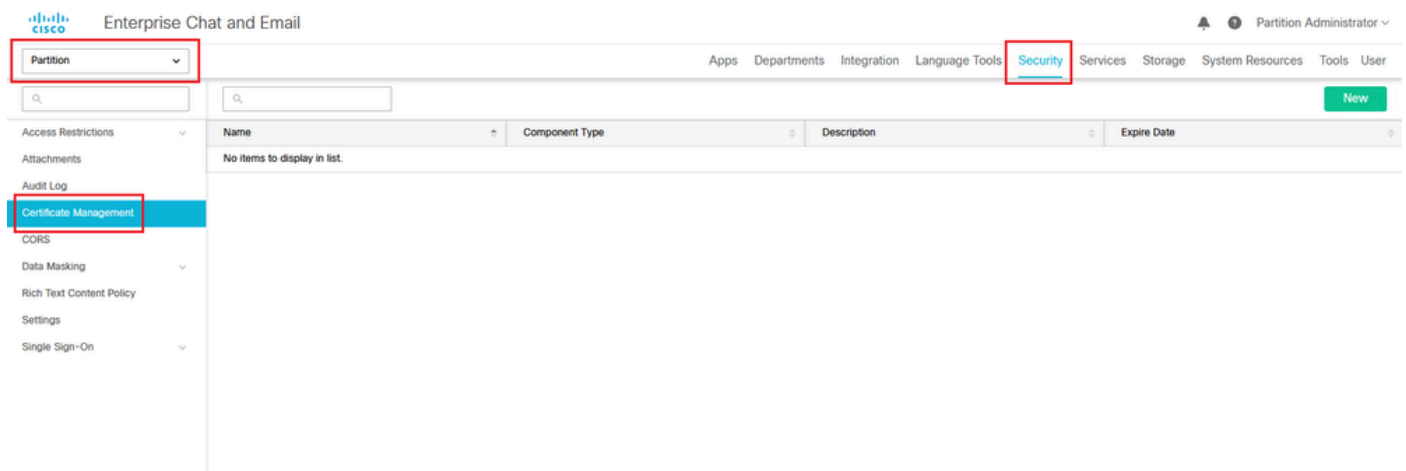
1. Nella console Gestione AD FS selezionare e fare clic con il pulsante destro del mouse sull'attendibilità componente creata per ECE.
2. Aprire la finestra Proprietà relativa al trust e nella scheda Firma fare clic sul pulsante Aggiungi.
3. Aggiungere il certificato pubblico (file crt generato nel passaggio precedente) e fare clic su OK.

Creazione e importazione di certificati

Passaggio 13

Prima di configurare l'SSO per l'utilizzo di Cisco IDS per Single Sign-On per gli agenti, è necessario importare nell'applicazione il certificato Tomcat dal server Cisco IdS.

a. Nella console di amministrazione ECE, in Menu a livello di partizione, fare clic sull'opzione Sicurezza e selezionare Gestione certificati dal menu a sinistra.



b. Nello spazio Gestione certificati, fare clic sul pulsante Nuovo e immettere i dettagli appropriati:

- Nome: digitare un nome per il certificato.
- Descrizione: aggiungere una descrizione per il certificato.
- Tipo di componente: selezionare CISCO IDS.
- Importa certificato: per importare il certificato, fare clic sul pulsante Cerca e aggiungi e immettere i dettagli richiesti:
- File certificato: fare clic sul pulsante Sfoglia e selezionare il certificato che si desidera importare. I certificati possono essere importati solo nei formati .pem, .der (BINARY) o

.cer/cert.

- Nome alias: specificare un alias per il certificato.

c. Fare clic su Salva

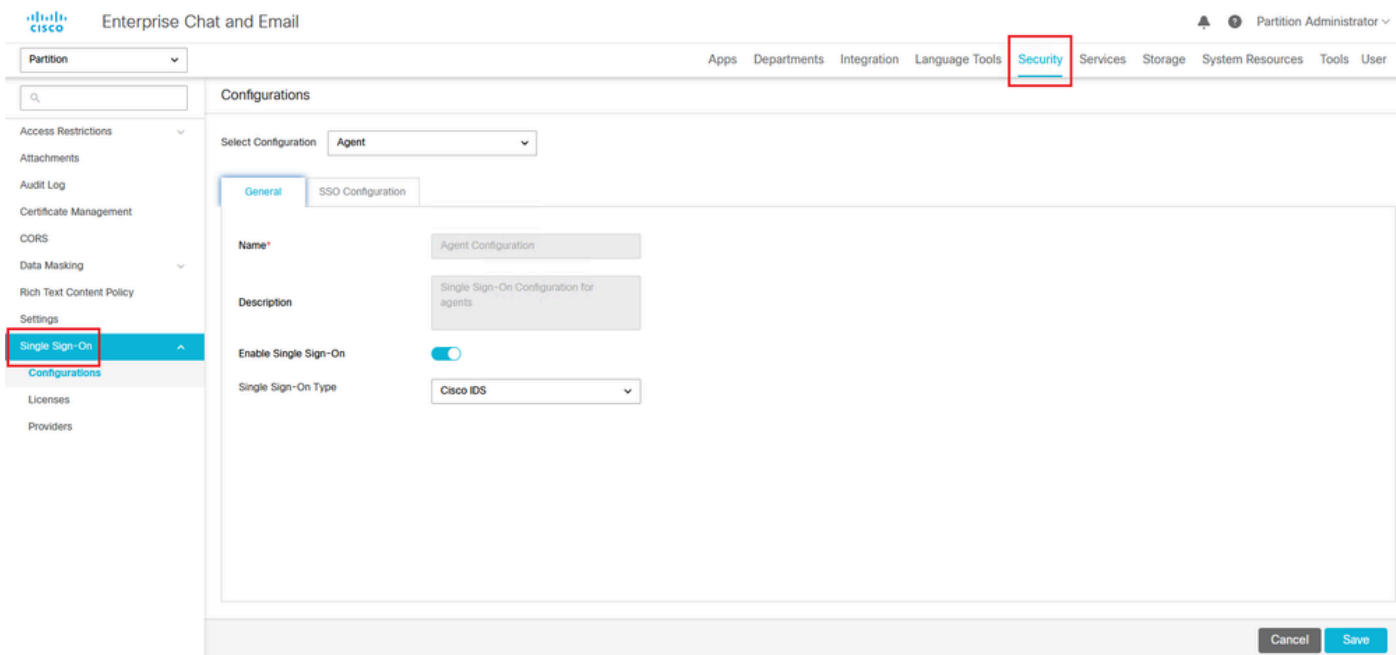
The screenshot shows the Cisco Enterprise Chat and Email administration interface. At the top left is the Cisco logo and the title 'Enterprise Chat and Email'. Below this is a 'Partition' dropdown menu. A search bar is located on the left side of the main content area. A navigation sidebar on the left contains the following items: '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)

Configurazione di Single Sign-On dell'agente

Passaggio 14

1. Nella console di amministrazione ECE, in Menu a livello di partizione, fare clic sull'opzione Protezione, quindi selezionare Single Sign-On > Configurazioni dal menu a sinistra.
2. Nell'elenco a discesa Seleziona configurazione, selezionare Agent e impostare la configurazione nella scheda Generale:
 - Abilita Single Sign-On: fare clic sul pulsante Attiva/disattiva per abilitare l'SSO.
 - Tipo Single Sign-On: selezionare Cisco IDS.



Passaggio 15

Fare clic sulla scheda Configurazione SSO e fornire i dettagli di configurazione:

a. Provider di connessione OpenID

URL endpoint informazioni utente primario

- URL dell'endpoint di informazioni utente del server Cisco IDS primario.
- Questo URL convalida l'API token utente/informazioni utente.
- Il formato è: <https://cisco-ids-1:8553/ids/v1/oauth/userinfo> dove cisco-ids-1 indica il nome di dominio completo (FQDN) del server Cisco IDS primario.

Nome attestazione d'identità utente

- Nome dell'attestazione restituita dall'URL dell'endpoint di informazioni utente, che identifica il nome utente in Unified o Packaged CCE.
- Il nome dell'attestazione e il nome utente in Unified o Packaged CCE devono corrispondere.
- Questa è una delle attestazioni ottenute in risposta alla convalida del token Bearer.
- Se il nome utente degli agenti in Unified o Packaged CCE corrisponde al nome dell'entità utente, specificare "upn" come valore per il campo Nome attestazione identità utente.
- Se il nome utente degli agenti in Unified o Packaged CCE corrisponde al nome account SAM, fornire "sub" come valore per il campo Nome attestazione identità utente.

URL endpoint informazioni utente secondario

- URL dell'endpoint di informazioni utente secondario del server Cisco IDS.
- Il formato è il seguente: <https://cisco-ids-2:8553/ids/v1/oauth/userinfo> dove cisco-ids-2 indica il nome di dominio completo (FQDN) del server Cisco IDS secondario.

Metodo URL endpoint informazioni utente

- Metodo HTTP utilizzato da ECE per eseguire chiamate di convalida del token Bearer all'URL dell'endpoint di informazioni utente.
- Selezionare POST dall'elenco di opzioni presentato (POST è selezionato qui per corrispondere al metodo del server IDS).

POST: metodo utilizzato per inviare dati al server Cisco IDS all'endpoint specificato.

Durata cache token di accesso (secondi)

- Durata, in secondi, della memorizzazione nella cache in ECE di un token Bearer.
- I token di connessione per i quali le chiamate di convalida hanno esito positivo vengono archiviati solo nelle cache. (Valore minimo: 1; valore massimo: 30)

Consenti accesso SSO all'esterno di Finesse

- Fare clic su questo pulsante Attiva/disattiva se si desidera consentire agli utenti con ruoli di amministratore o supervisore di accedere alla partizione ECE all'esterno di Finesse utilizzando le credenziali di accesso SSO.
- Se questa opzione è abilitata, è necessario fornire le informazioni nelle sezioni Identity Provider e Service Provider.
- È quindi necessario che la configurazione IdP consenta un server IdP condiviso.



Partition ▼

- Access Restrictions ▼
- Attachments
- Audit Log
- Certificate Management
- CORS
- Data Masking ▼
- Rich Text Content Policy
- Settings
- Single Sign-On ^
- Configurations
- Licenses
- Providers

Configurations

Select Configuration Agent ▼

General

SSO Configuration

OpenId Connect Provider

Primary User Info Endpoint URL *

User Identity Claim Name *

Secondary User Info Endpoint URL

User Info Endpoint URL Method * POST ▼

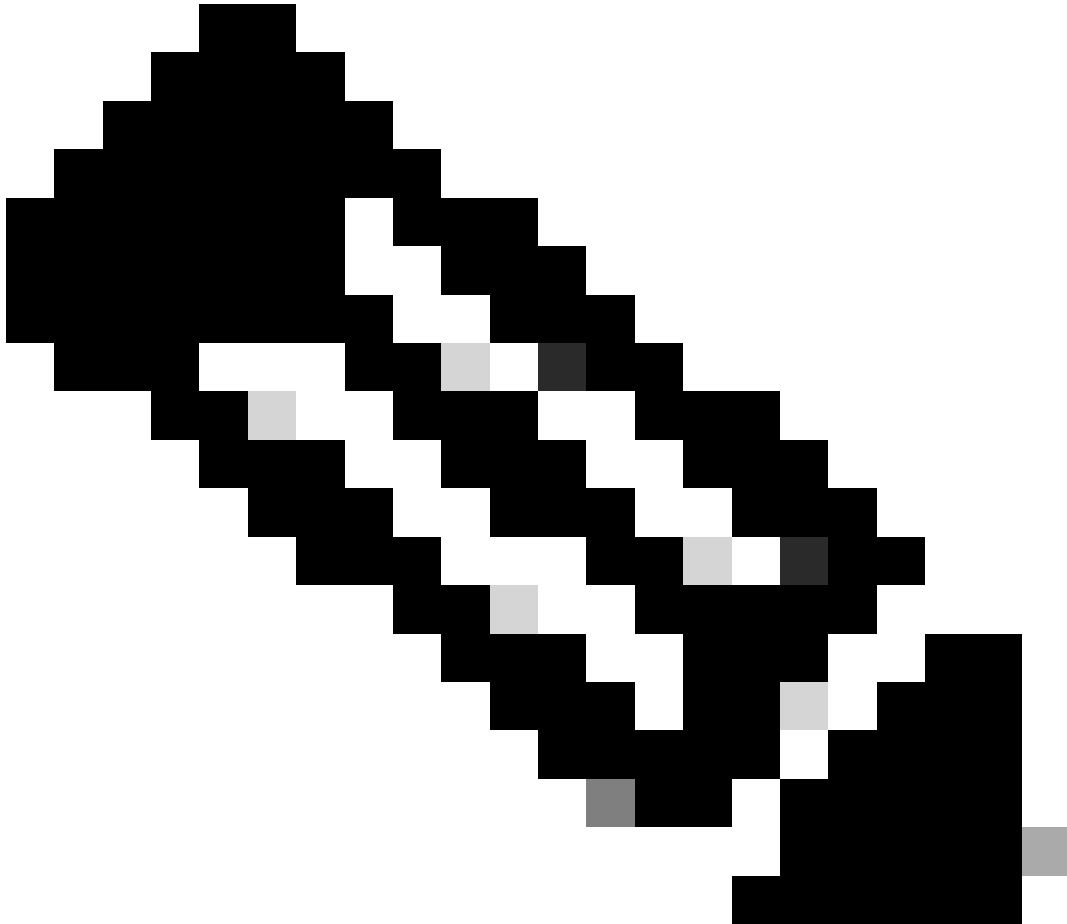
Access Token Cache Duration (Seconds) *

Allow SSO Login Outside Finesse

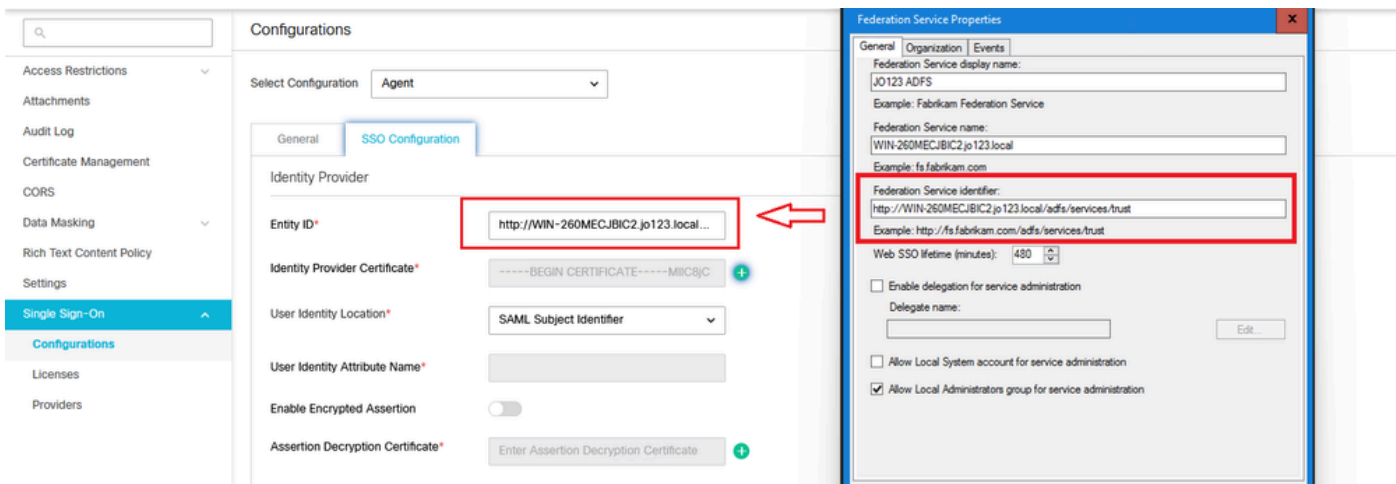
b. Provider di identità

ID entità

- ID entità del server IdP.
-

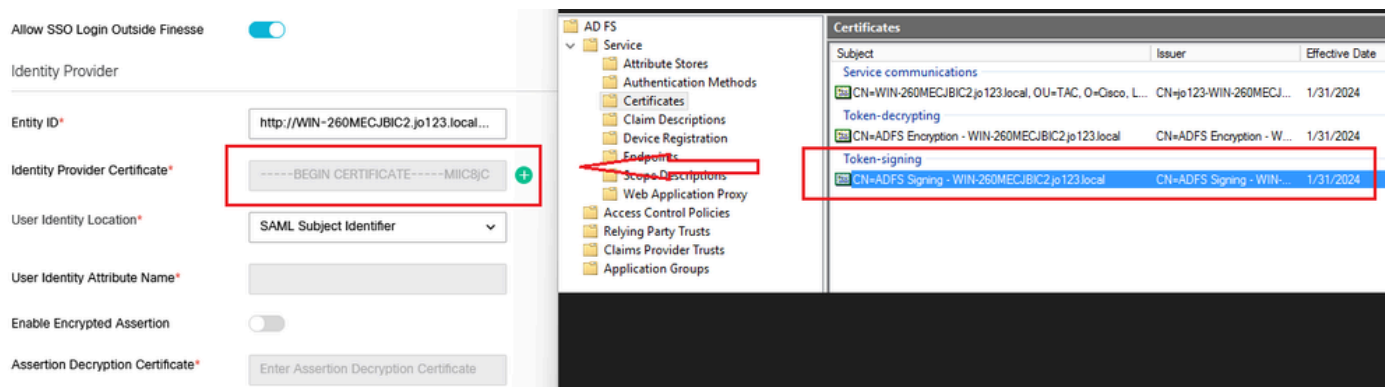


Nota: questo valore deve corrispondere esattamente al valore 'Identificatore servizio federativo' nella console Gestione AD FS.



Certificato provider di identità

- Il certificato della chiave pubblica.
- Il certificato deve iniziare con "—BEGIN CERTIFICATE—" e terminare con "—END CERTIFICATE—"
- Certificato per la firma di token in Console di gestione AD FS > Servizio > Certificati > Firma di token.



Percorso identità utente

- Selezionare SAML Subject Identifier per impostare la posizione dell'identità nel certificato sull'identificativo soggetto SAML predefinito, come nel soggetto nell'asserzione SAML, ad esempio il nome utente in <saml:Subject>.
- Selezionare Attributo SAML per assegnare la posizione dell'identità a un attributo specifico nel certificato, ad esempio email.address. Specificare l'attributo nel campo Nome attributo identità utente.

Nome attributo identità utente

- Applicabile solo quando il valore Posizione ID utente è un attributo SAML.
- Questa impostazione può essere modificata all'interno dell'asserzione SAML e utilizzata per selezionare un attributo diverso per l'autenticazione degli utenti, ad esempio un indirizzo di posta elettronica.
- Può inoltre essere utilizzato per creare nuovi utenti con un attributo SAML.
- Ad esempio, se un utente viene identificato tramite il valore fornito nell'attributo

email.address e il valore dell'indirizzo di posta elettronica fornito non corrisponde ad alcun utente del sistema, viene creato un nuovo utente con gli attributi SAML forniti.

Abilita asserzione crittografata (facoltativo)

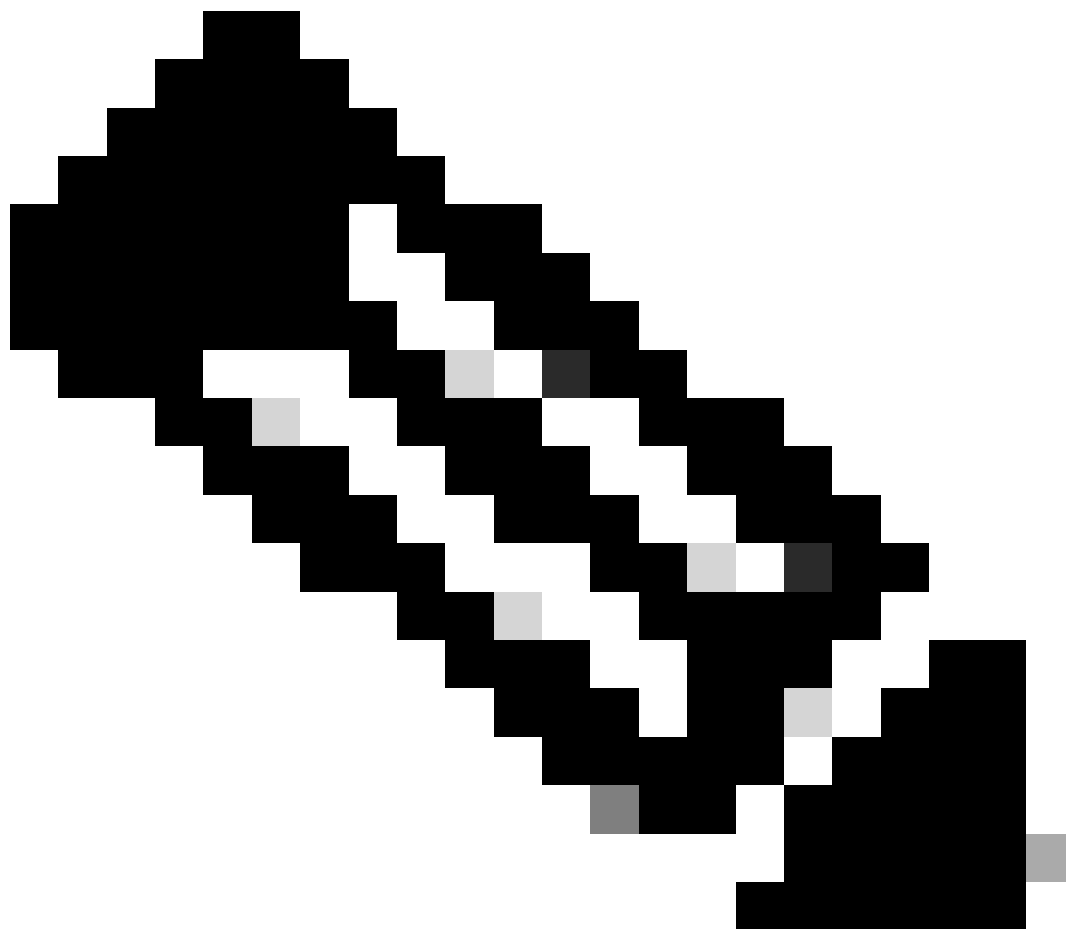
- Se si desidera abilitare l'asserzione crittografata con il provider di identità per l'accesso alla console, fare clic sul pulsante Attiva/disattiva e impostare il valore su Abilitato.
- In caso contrario, impostare il valore su Disabled.

Certificato decrittografia asserzione

Se l'opzione Abilita asserzione crittografata è impostata su Abilitato, fare clic sul pulsante Cerca e aggiungi e confermare la modifica del certificato.

Specificare i dettagli nella finestra Certificato decrittografia asserzione:

- File keystore Java: fornire il percorso del file keystore Java. Il file è in formato .jks e contiene la chiave di decrittografia necessaria al sistema per accedere ai file protetti dal provider di identità.
- Nome alias: l'identificatore univoco della chiave di decrittografia.
- Password keystore: la password necessaria per accedere al file keystore Java.
- Password chiave: la password necessaria per accedere alla chiave di decrittografia dell'alias.



Nota: è necessario che corrisponda al certificato nella scheda 'Crittografia' dell'attendibilità componente ECE configurata nella console di gestione AD FS.

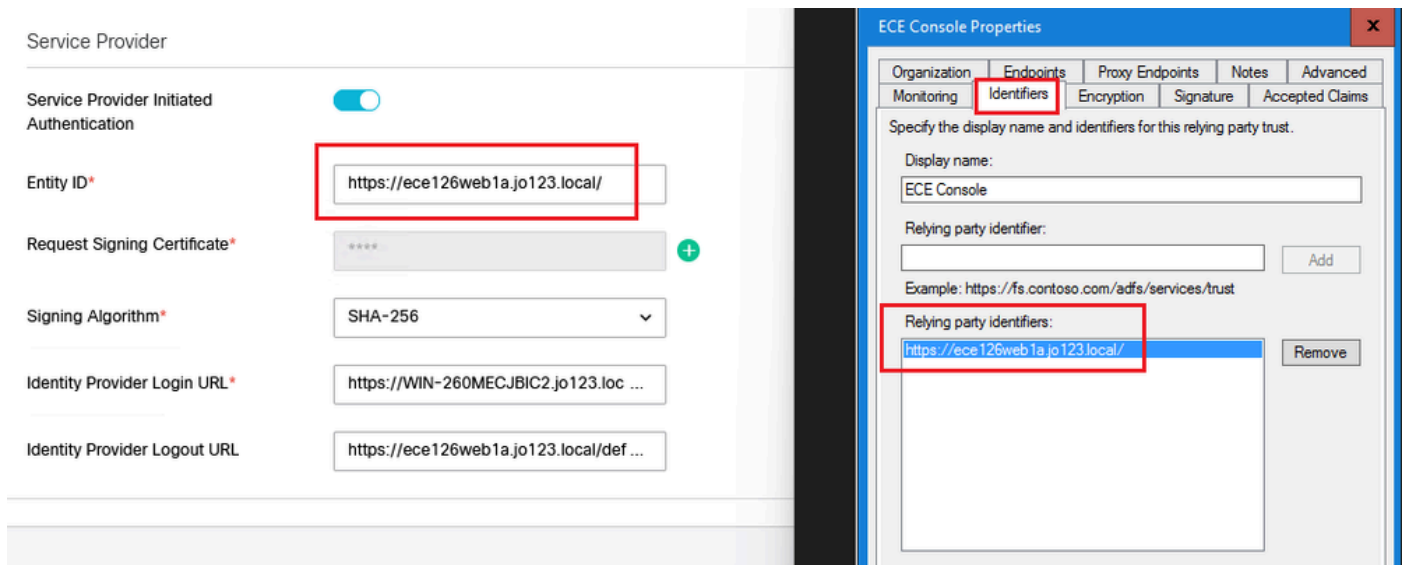
c. Fornitore di servizi

Autenticazione avviata dal provider di servizi

- Impostare l'interruttore su Enabled.

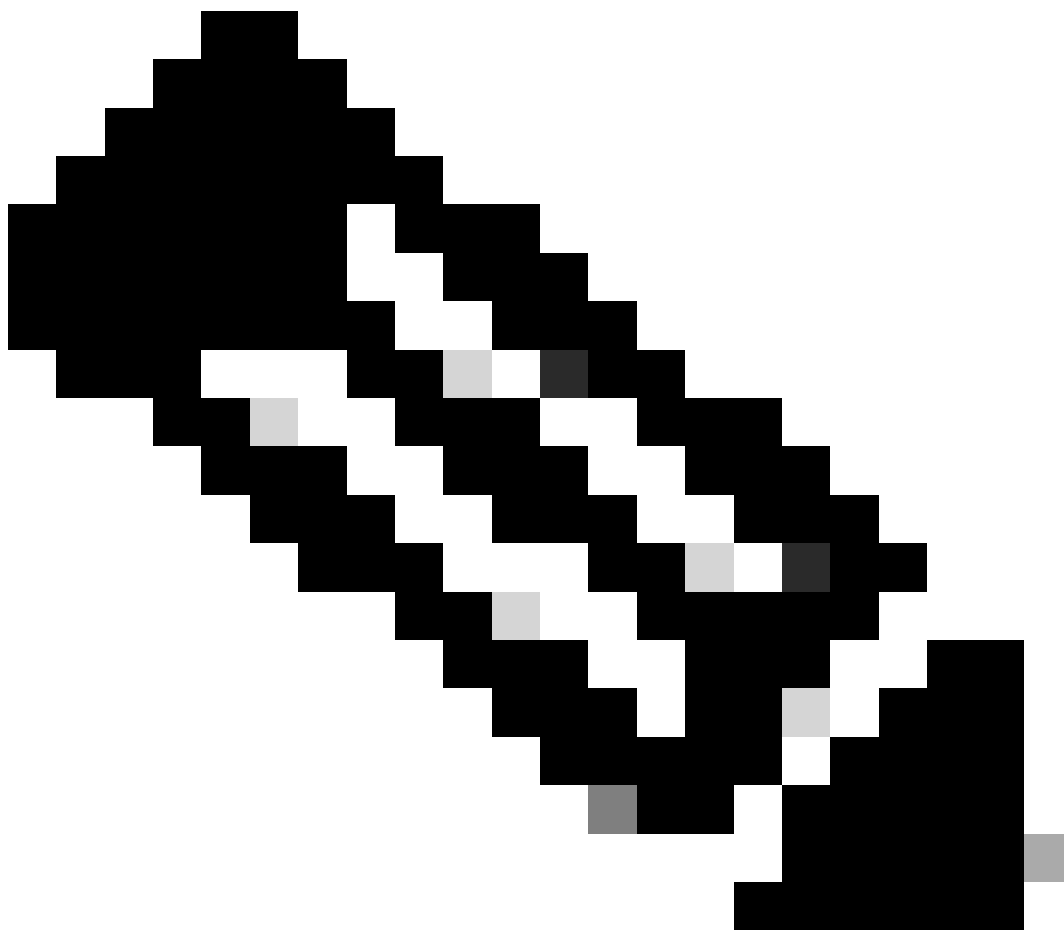
ID entità

- Fornire l'URL esterno dell'applicazione ECE.



Richiedi certificato di firma

- È necessario un certificato Java Keystore (JKS) per fornire le informazioni necessarie.
- Caricare il file .jks utilizzando il nome alias e la password keystore/key generati nel passaggio 11.




Nota: è necessario che corrisponda al certificato caricato nella scheda 'Firma' dell'attendibilità componente ECE configurata nella console di gestione AD FS.

Service Provider

Service Provider Initiated Authentication

Entity ID*

Request Signing Certificate* 

Signing Algorithm*


Identity Provider Login URL*

Identity Provider Logout URL

ECE Console Properties

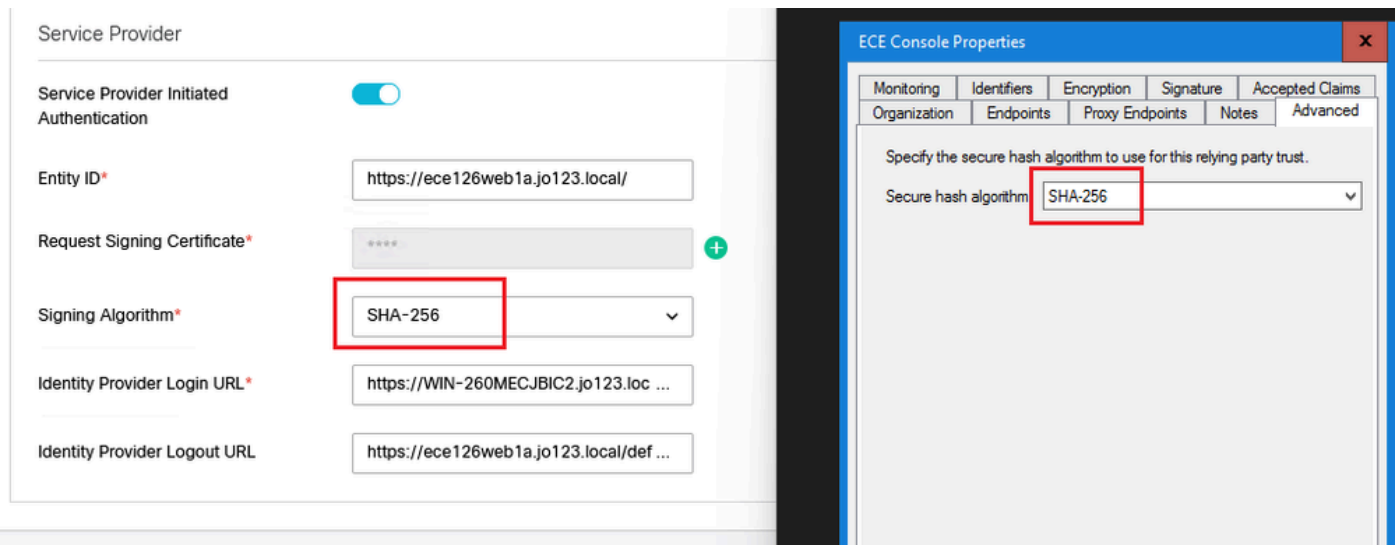
Organization Endpoints Proxy Endpoints Notes Advanced
Monitoring Identifiers Encryption **Signature** Accepted Claims

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:...	1/29/21...

Algoritmo di firma

- Impostare l'algoritmo di firma per il provider di servizi.
- Se si utilizza ADFS, questo valore deve corrispondere all'algoritmo selezionato nell'attendibilità del componente creato per ECE nella scheda Avanzate.



URL di accesso al provider di identità

- URL per l'autenticazione SAML.
- Per ADFS, ad esempio, questo valore è <http://<ADFS>/adfs/ls>.

URL di disconnessione del provider di identità

- URL a cui gli utenti vengono reindirizzati dopo la disconnessione. Questo valore è facoltativo e può essere qualsiasi URL.
- Ad esempio, gli agenti possono essere reindirizzati a <https://www.cisco.com> o a qualsiasi altro URL dopo la disconnessione da SSO.

Passaggio 16

Fare clic su Salva.

Impostare l'URL del server Web o del bilanciamento del carico nelle impostazioni della partizione

Passaggio 17

Assicurarsi che sia stato immesso l'URL corretto del server Web/bilanciamento carico in Impostazioni partizione > selezionare la scheda Apps e passare a Impostazioni generali > URL esterno dell'applicazione



Partition

General Settings

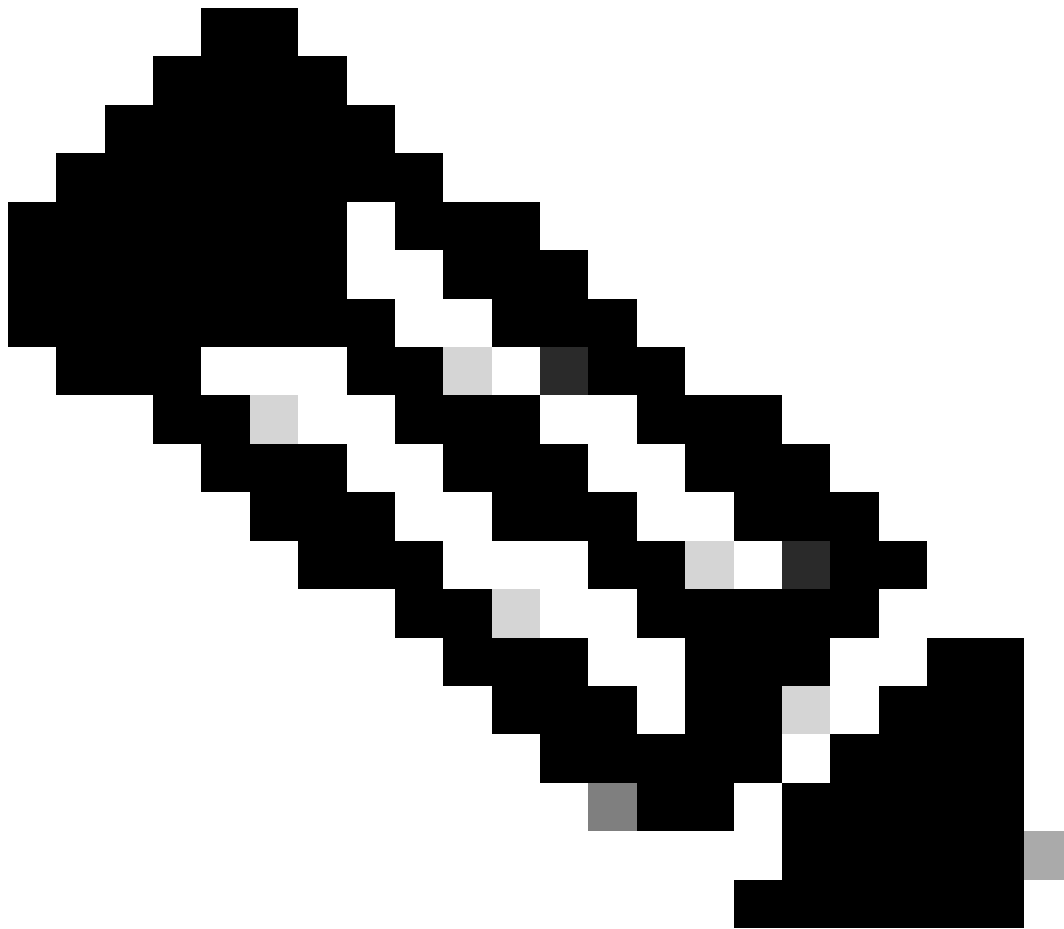
- Chat & Messaging
- Email
- General Settings**
- Knowledge

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

Configurazione di SSO per gli amministratori della partizione



Nota:

- Questo passaggio è valido solo per PCCE.
- Questo è per il gadget ECE a cui si accede tramite l'interfaccia WEB CCE Admin <https://cceadmin>.

Passaggio 18

Per configurare SSO per l'amministratore delle partizioni

1. Nella console di amministrazione ECE, in Menu a livello di partizione, fare clic sull'opzione Security, quindi selezionare Single Sign-On > Configurations dal menu a sinistra.
2. Nell'elenco a discesa Seleziona configurazione, selezionare Amministratori partizioni e immettere i dettagli di configurazione:

URL LDAP

- URL del server LDAP.
- Può trattarsi dell'URL del controller di dominio (ad esempio, ldap://LDAP_server:389) o dell'URL del catalogo globale (ad esempio, ldap://LDAP_server:3268) del server LDAP.
- La partizione può essere aggiunta automaticamente al sistema quando si accede a ECE tramite la console di amministrazione CCE, se ECE è configurato con la ricerca LDAP.
- Tuttavia, nelle distribuzioni di Active Directory con più domini in una singola foresta o in cui sono configurati UPN alternativi, non utilizzare l'URL del controller di dominio con le porte LDAP standard 389 e 636.
- L'integrazione LDAP può essere configurata per utilizzare l'URL del catalogo globale con le porte 3268 e 3269.



Nota: è buona norma utilizzare URL del catalogo globale. Se non si utilizza un catalogo globale, di seguito viene riportato un errore nei registri di ApplicationServer.

- Eccezione nell'autenticazione LDAP <@>
javax.naming.PartialResultException: riferimenti di continuazione non elaborati;
nome rimanente 'DC=example,DC=com'

Attributo DN

- Attributo del DN che contiene il nome di accesso dell'utente.
- Ad esempio, userPrincipalName.

Base

- Il valore specificato per Base viene utilizzato dall'applicazione come base di ricerca.
- Base di ricerca è la posizione iniziale per la ricerca nella struttura di directory LDAP.
- Ad esempio, DC=società, DC=com.

DN per ricerca LDAP

- Se il sistema LDAP non consente l'associazione anonima, fornire il nome distinto (DN) di un utente che dispone di autorizzazioni di ricerca nella struttura di directory LDAP.
- Se il server LDAP consente l'associazione anonima, lasciare vuoto questo campo.

Password

- Se il sistema LDAP non consente l'associazione anonima, fornire la password di un utente che dispone delle autorizzazioni di ricerca nella struttura di directory LDAP.
- Se il server LDAP consente l'associazione anonima, lasciare vuoto questo campo.

Passaggio 19

Fare clic su Salva.

In questo modo viene completata la configurazione Single Sign-On per gli agenti e gli amministratori delle partizioni in ECE.

Risoluzione dei problemi

Impostazione del livello di traccia

1. Nella console di amministrazione ECE, in Menu a livello di partizione, fare clic sull'opzione Risorse di sistema e quindi selezionare Process Logs dal menu a sinistra.
2. Dall'elenco dei processi, selezionare il processo ApplicationServer > impostare il livello di traccia desiderato dal menu a discesa 'Livello di traccia massimo'.



Nota:

- Per la risoluzione degli errori di accesso SSO durante la configurazione iniziale o la riconfigurazione, impostare la traccia del processo di ApplicationServer sul livello 7.
 - Una volta riprodotto l'errore, ripristinare il livello di traccia predefinito 4 per evitare la sovrascrittura dei log.
-

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

Extensive Logging End Time

8 - Trace

7 - Debug

6 - Dbquery

5 - Perf

4 - Info ✓

Risoluzione dei problemi dello scenario 1

Errore

- Codice errore: 500
- Descrizione dell'errore: l'applicazione non è in grado di accedere all'utente in questo momento perché l'accesso al provider di identità non è riuscito.

Analisi log

- Accesso a IdP non riuscito - `<samlp:Status><samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Responder" /></samlp:Status>`
- In questo caso, lo stato "Risponditore" indica la presenza di un problema sul lato AD FS, in questo caso principalmente con il "Certificato di firma della richiesta" caricato sulla console di amministrazione ECE (Configurazione SSO > Provider di servizi) e il certificato caricato nell'attendibilità del componente ECE nella scheda 'Firma'.
- Si tratta del certificato generato utilizzando il file keystore Java.

Registri di Application Server - Livello di traccia 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:
```

Risoluzione

- Fare riferimento alla configurazione 'Request Signing Certificate' nella sezione 'Configuring Agent Single Sign-On - Service Provider'.
- Accertarsi che il file Java Keystore .jks generato nel passo 11 sia caricato nel campo

"Request Signing Certificate" (Certificato di firma richiesta) della console di amministrazione ECE in Configurazione SSO > Selezionare la configurazione 'Agent' > scheda 'Configurazione SSO' > Provider di servizi > Certificato di firma richiesta.

- Verificare che il file .crt venga caricato nella scheda 'Firma' dell'attendibilità componente ECE (passaggio 12).

Scenario di risoluzione dei problemi 2

Errore

- Codice errore: 400
- Descrizione errore: token di risposta SAML non valido. Convalida della firma non riuscita.

Analisi log

- Questo errore indica una mancata corrispondenza nel certificato tra il 'certificato per la firma di token' in ADFS e il 'certificato del provider di identità' nella configurazione SSO ECE.

Registri di Application Server - Livello di traccia 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:
```

Risoluzione

- L'errore rilevato nel frammento di registro 'Impossibile analizzare il certificato: java.io.IOException: Incomplete data' indica che il contenuto 'Identity Provider Certificate' non è stato immesso correttamente
- Per risolvere il problema: In Gestione AS FS > AD FS > Servizio > Certificati > Firma token > Esporta il certificato > Apri in un editor di testo > Copia tutto il contenuto > Incolla in 'Certificato provider di identità' archiviato nella configurazione SSO > Salva.
- Fare riferimento alla configurazione 'Certificato provider di identità' nella sezione 'Configurazione del servizio Single Sign-on dell'agente - Provider di identità' (passaggio 15).

Scenario di risoluzione dei problemi 3

Errore

- Codice di errore: 401-114
- Descrizione errore: impossibile trovare l'identità utente nell'attributo SAML.

Analisi log

Registri di Application Server - Livello di traccia 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: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:830) [?:?]
```

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

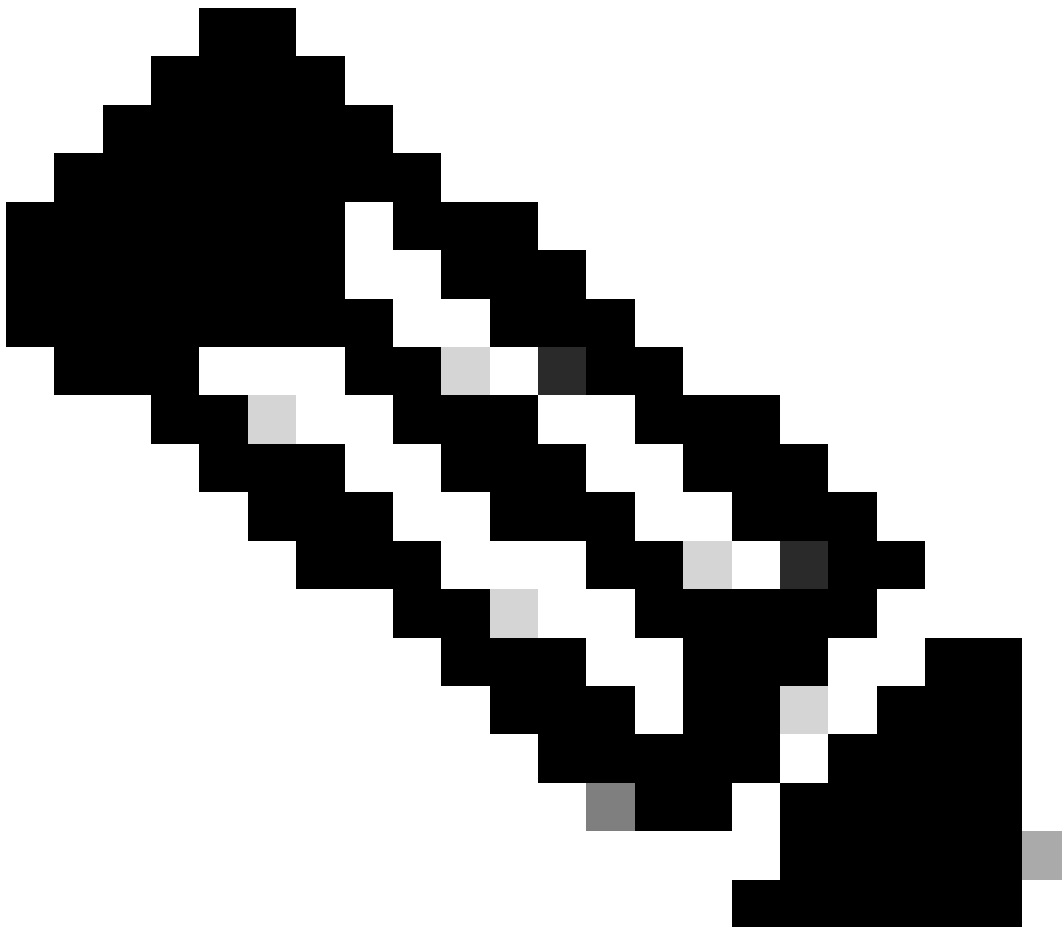
2024-02-01 01:44:32.083 GMT+0000 <@> DEBUG <@> [1220:qtp815320891-1220] <@> ProcessId:7716 <@> PID:1 <@>
2024-02-01 01:44:32.083 GMT+0000 <@> TRACE <@> [1220:qtp815320891-1220] <@> ProcessId:7716 <@> PID:1 <@>

Risoluzione

- Questo errore indica un problema o una mancata corrispondenza nella configurazione nei campi 'Posizione identità utente' e 'Nome attributo identità utente'.
- Controllare e correggere i parametri 'Posizione identità utente' e 'Nome attributo identità utente' nella console di amministrazione ECE, in Single Sign-On > Configurazioni > nell'elenco a discesa Seleziona configurazione, selezionare Agente > scheda Configurazione SSO > Identifica provider (passo 15).

Informazioni correlate

Questi sono i documenti chiave che è necessario esaminare attentamente prima di iniziare qualsiasi installazione o integrazione ECE. Non si tratta di un elenco esaustivo di documenti ECE.



Nota:

- La maggior parte dei documenti ECE ha due versioni. Accertarsi di scaricare e utilizzare le versioni disponibili per PCCE. Il titolo del documento è per Packaged Contact Center Enterprise o (Per PCCE) o (Per UCCE e PCCE) dopo il numero di versione.
 - Prima di procedere all'installazione, all'aggiornamento o all'integrazione, verificare se nella pagina iniziale della documentazione di Cisco Enterprise Chat and Email sono disponibili aggiornamenti.
 - <https://www.cisco.com/c/en/us/support/customer-collaboration/cisco-enterprise-chat-email/series.html>
-

ECE versione 12.6(1)

- [Guida per l'amministratore di Enterprise Chat and Email](#)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).