ECEでのエージェントとパーティション管理者のSSOの設定およびトラブルシューティング

内容

はじめに

このドキュメントでは、ECEソリューションでエージェントおよびパーティション管理者のシングルサインオン(SSO)を設定するために必要な手順について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

Cisco Packaged Contact Center Enterprise(PCCE)

Cisco Unified Contact Center Enterprise（UCCE）

エンタープライズチャットおよび電子メール(ECE)

Microsoft Active Directory

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

UCCEバージョン：12.6(1)

ECEバージョン：12.6(1)

Windows Server 2016上のMicrosoft Active Directoryフェデレーションサービス(ADFS)

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

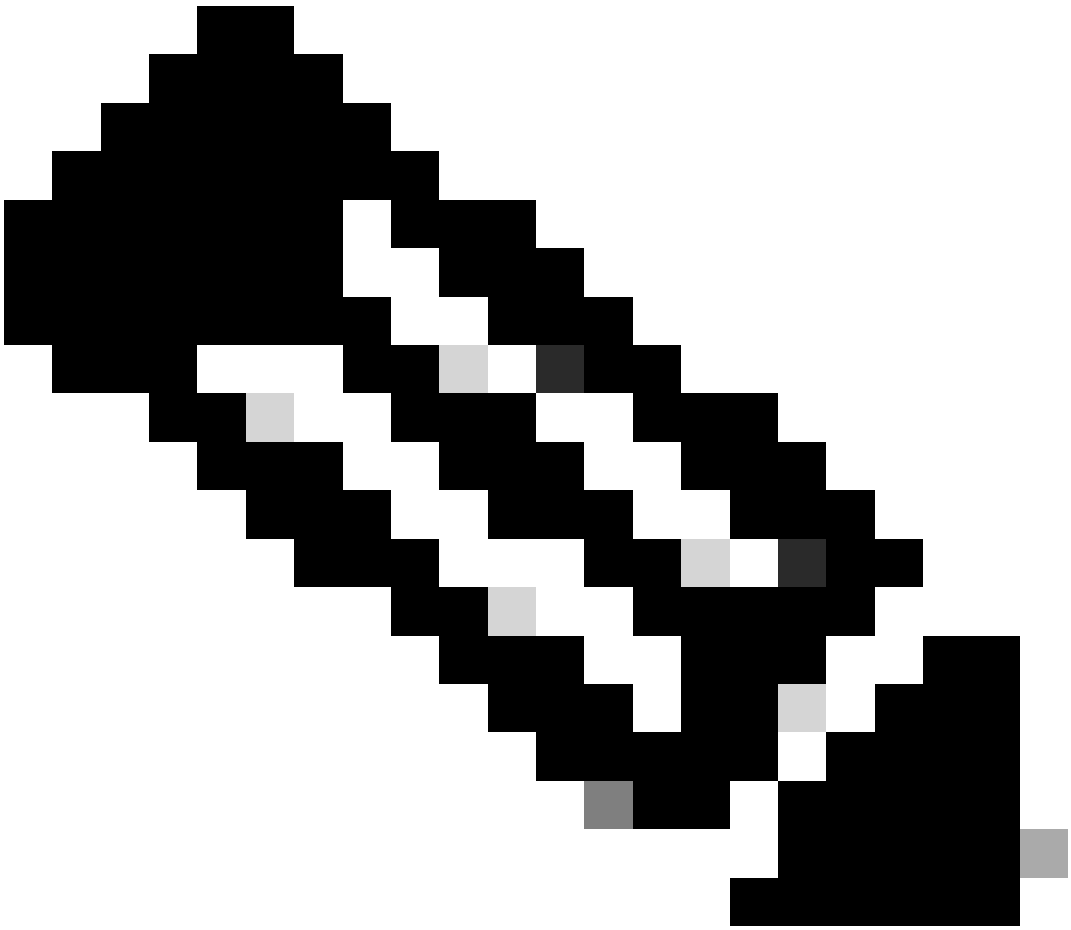
Enterprise Chat and Email(ECE)コンソールはFinesseの外部からアクセスできますが、エージェントとスーパーバイザがFinesseを介してECEにログインできるようにするには、SSOを有効にする必要があります。

新しいパーティション管理者用にシングルサインオンを設定することもできます。これにより、Cisco Administratorデスクトップにログインした新規ユーザに、Enterprise ChatおよびEmail Administration Consoleへのアクセス権が付与されます。

シングルサインオンに関する重要な注意事項：

- シングルサインオン用のシステムを構成するプロセスは、パーティションユーザーが必要なアクション（アプリケーションセキュリティの表示とアプリケーションセキュリティの管理）を使用して、パーティションレベルでセキュリティノードに対して実行する必要があります。
- スーパーバイザおよび管理者がエージェントコンソール以外のコンソールにログインするには、SSOを有効にした後、パーティション設定でアプリケーションの有効な外部URLを指定する必要があります。詳細については、「一般的なパーティション設定」を参照してください。
- 管理者ロールまたはスーパーバイザロールを持つユーザがSSOログインクレデンシャルを使用してFinesse外部のECEのパーティション1にサインインできるようにSSOを設定するには、Java Keystore(JKS)証明書が必要です。JKS証明書を受け取るには、IT部門に問い合

わせてください。
- Cisco IDSのSecure Sockets Layer(SSL)証明書は、インストールのすべてのアプリケーションサーバにインポートする必要があります。必要なSSL証明書ファイルを取得するには、IT部門またはCisco IDSサポートに問い合わせてください。
- Unified CCEのDBサーバの照合順序では、大文字と小文字が区別されます。ユーザ情報エンドポイントURLから返される要求のユーザ名と、Unified CCEのユーザ名は同じでなければなりません。これらが同じでない場合、シングルサインオンエージェントはログインしていると認識されず、ECEはエージェントのアベイラビリティをUnified CCEに送信できません。
- Cisco IDSのSSOの設定は、シングルサインオン用にUnified CCEで設定されているユーザに影響します。ECEでSSOを有効にするユーザが、Unified CCEでSSO用に設定されていることを確認します。詳細については、Unified CCE管理者に問い合わせてください。



注：

- ECEでSSOを有効にするユーザが、Unified CCEでSSO用に設定されていることを確認します。
- このドキュメントでは、リソースフェデレーションサーバーとアカウントフェデレ

ーションサーバーが同じコンピューターにインストールされている単一AD FS展開で、ECEの証明書利用者信頼を構成する手順について説明します。
- スプリットAD FS導入の場合は、各バージョンのECEインストールおよび構成ガイドに移動します。

設定手順

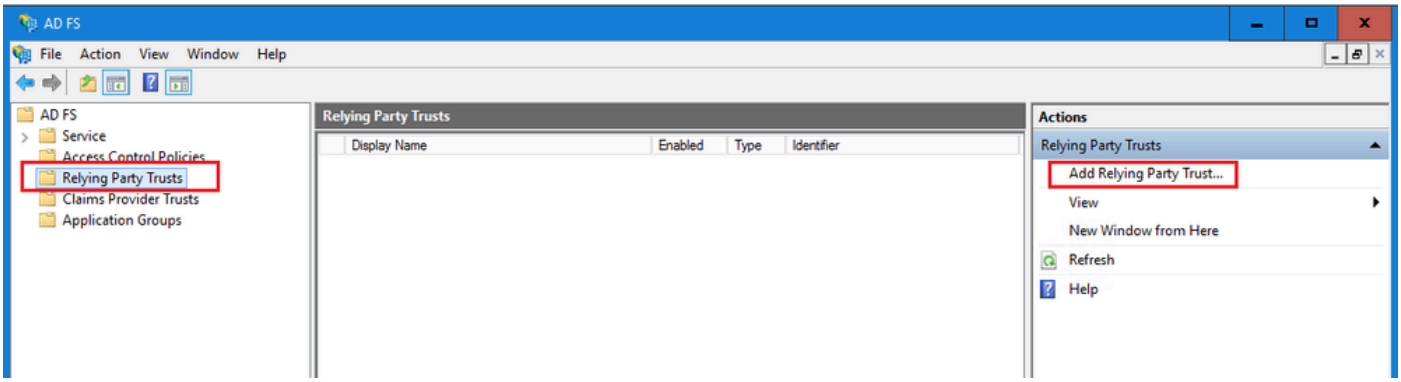
ECEの証明書利用者信頼の設定

手順 1

AD FS管理コンソールを開き、AD FS > Trust Relationships > Relying Party Trustに移動します。

手順 2

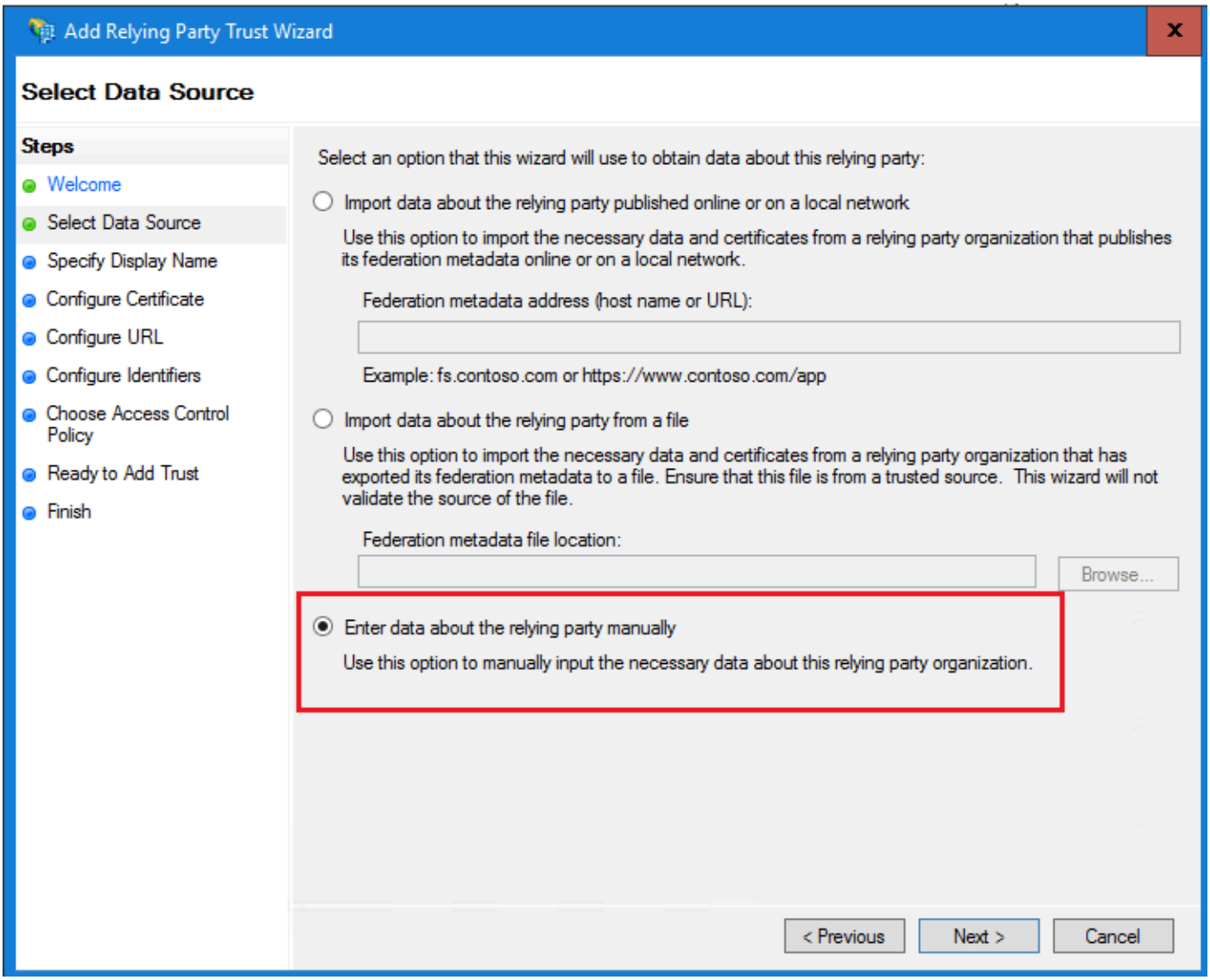
Actionsセクションで、Add Relying Party Trust...をクリックします。



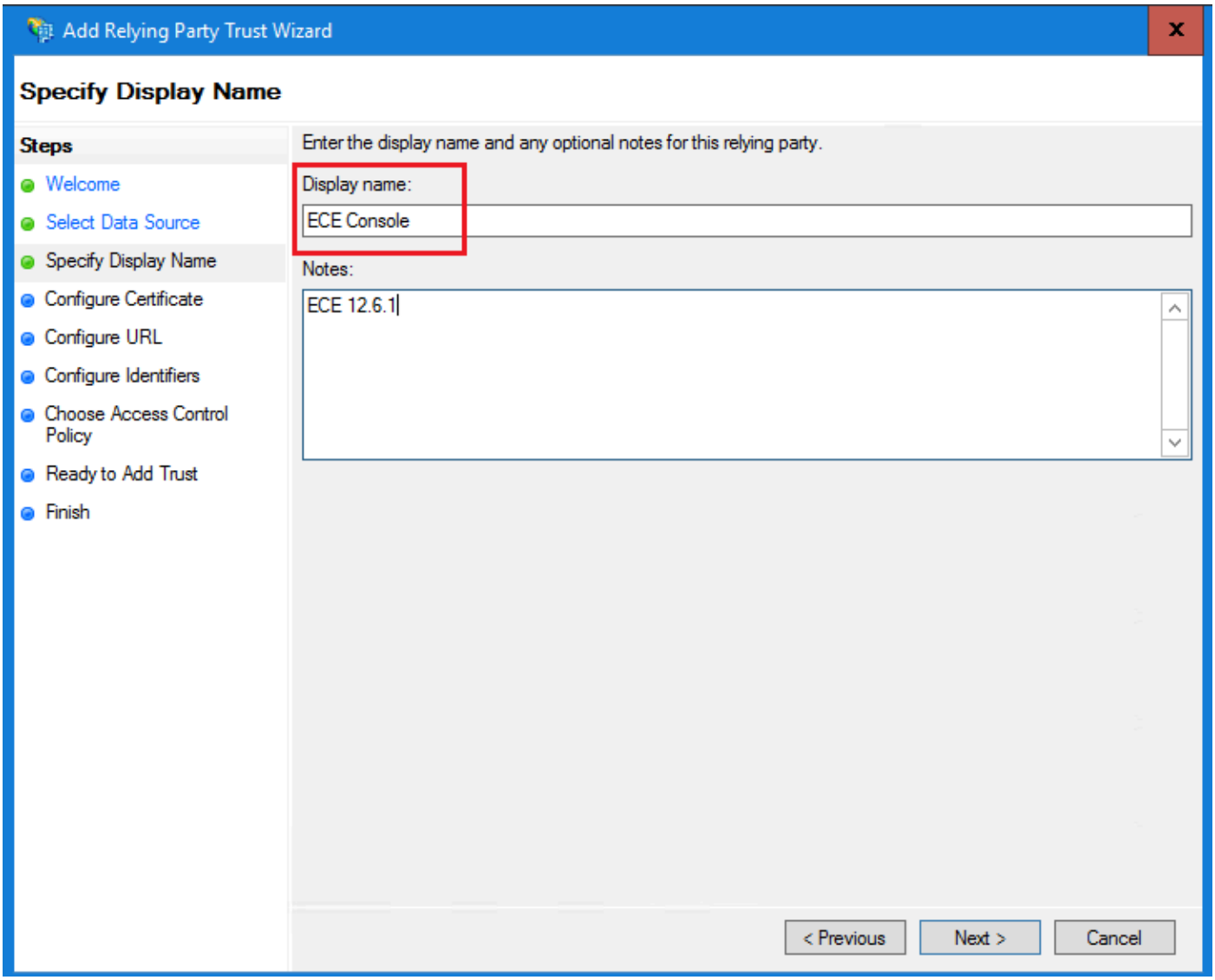
手順 3

証明書利用者信頼の追加ウィザードで、[開始]をクリックし、次の手順を実行します。

a. Select Data SourceページでEnter data about the reply party manuallyオプションを選択し、Nextをクリックします。



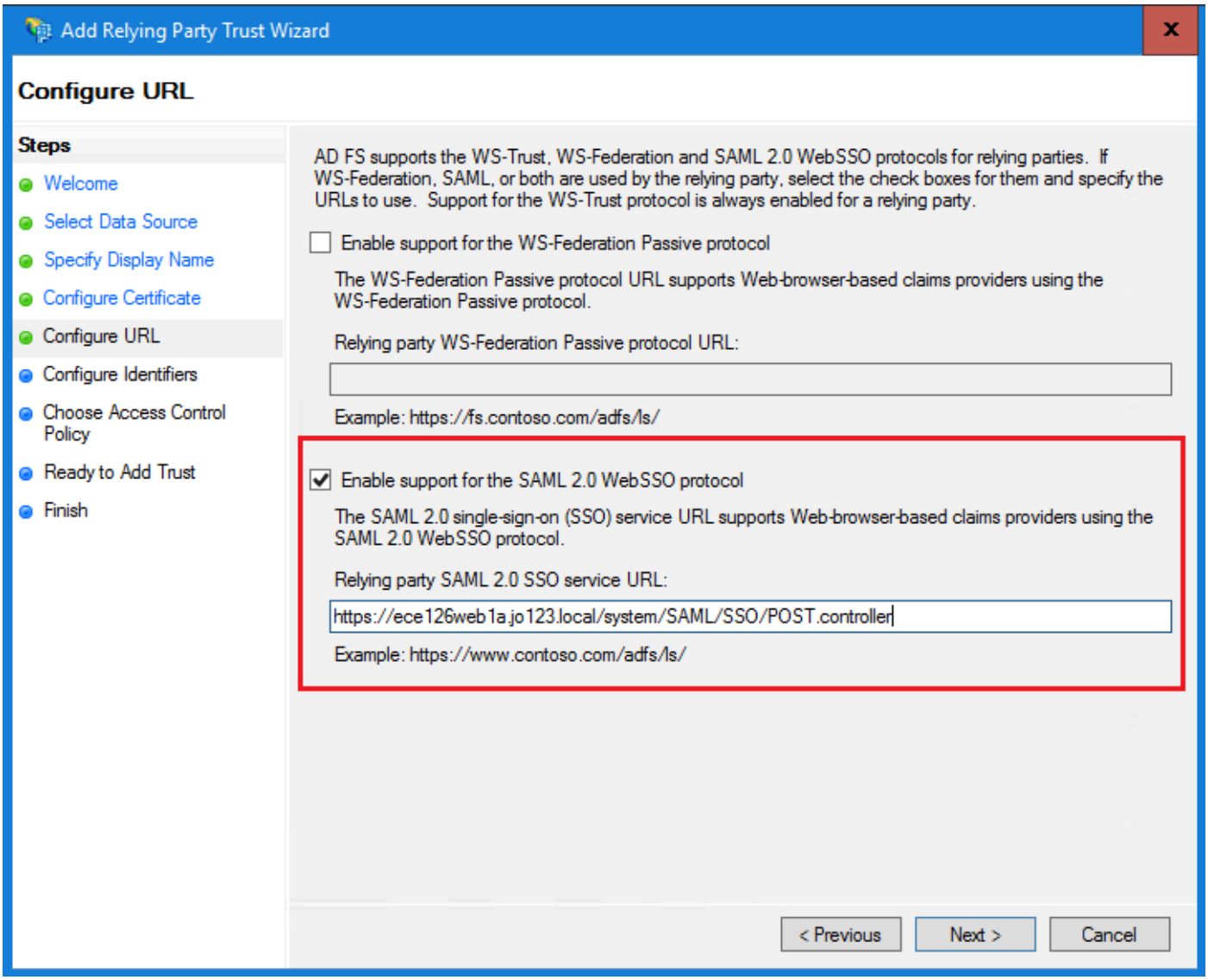
b. 「表示名の指定」ページで、証明書利用者の表示名を指定します。[Next] をクリックします。



c. 「URLの構成」ページで、次の操作を行います。

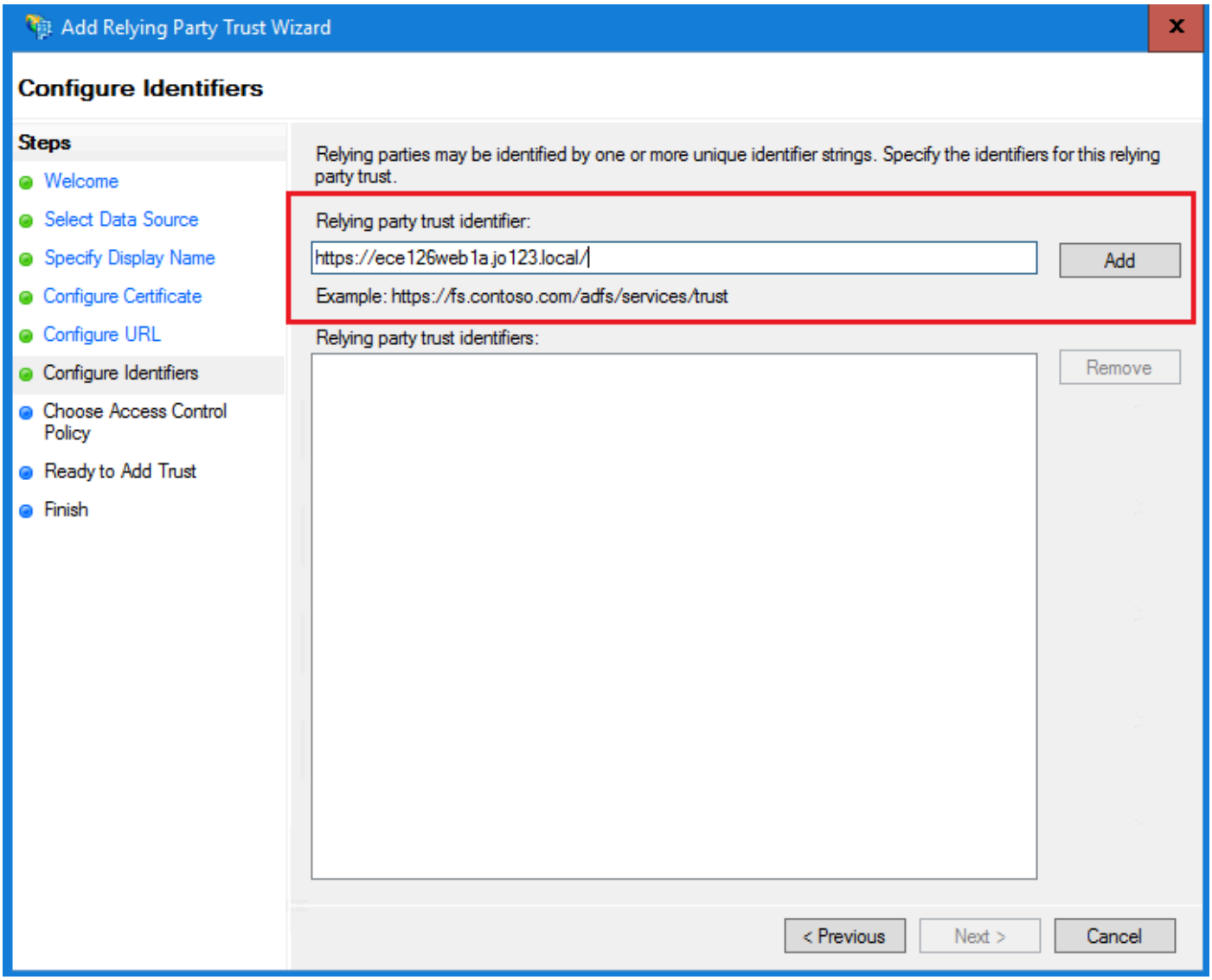
i. Enable support for the SAML 2.0 Web SSO protocolオプションを選択します。

ii. 証明書利用者SAML 2.0 SSOサーバのURLフィールドに、https://<Web-Server-Or-Load-Balancer-FQDN>/system/SAML/SSO/POST.controller形式のURLを入力します。

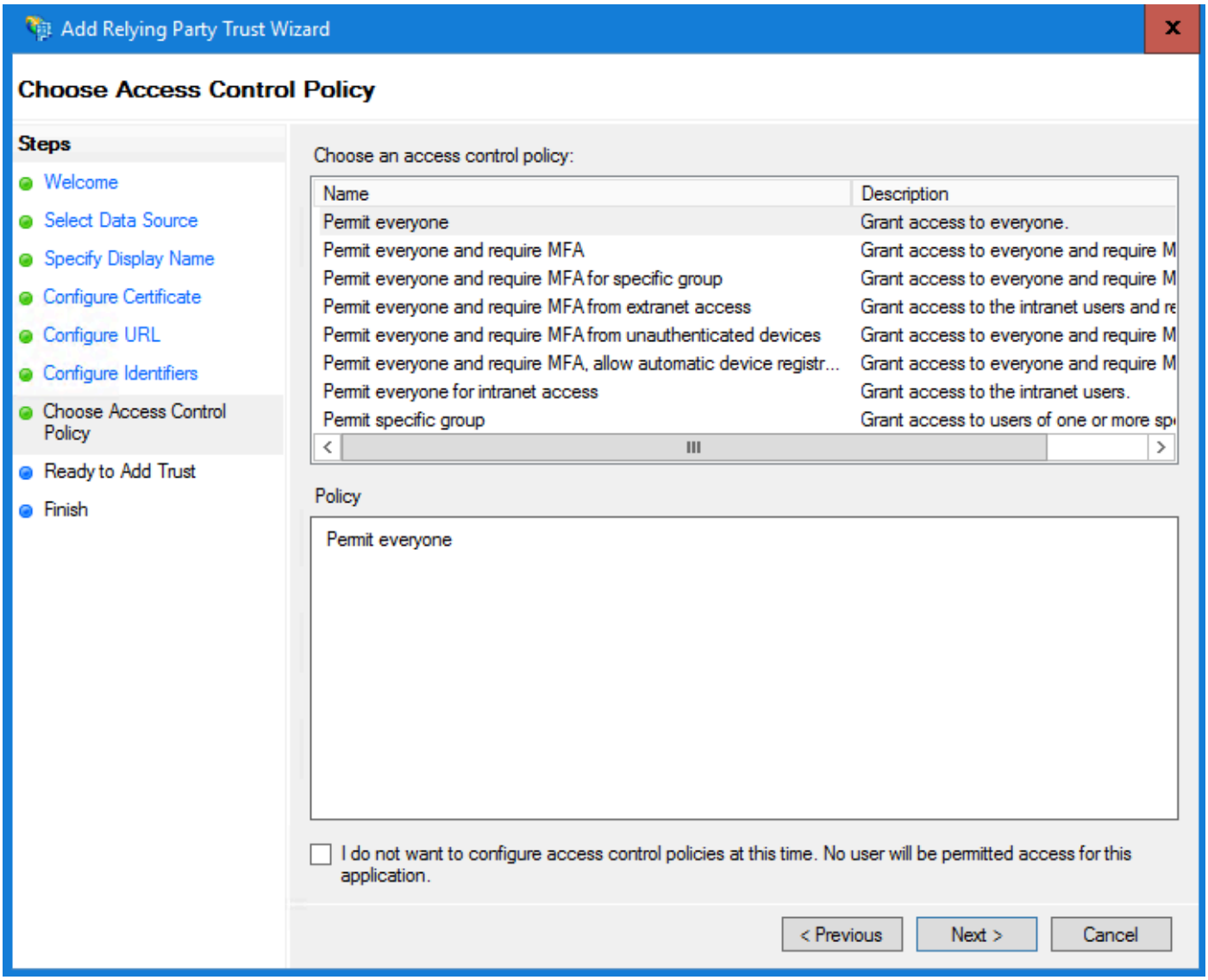


d. Configure Identifiersページで、証明書利用者信頼識別子を指定し、Addをクリックします。

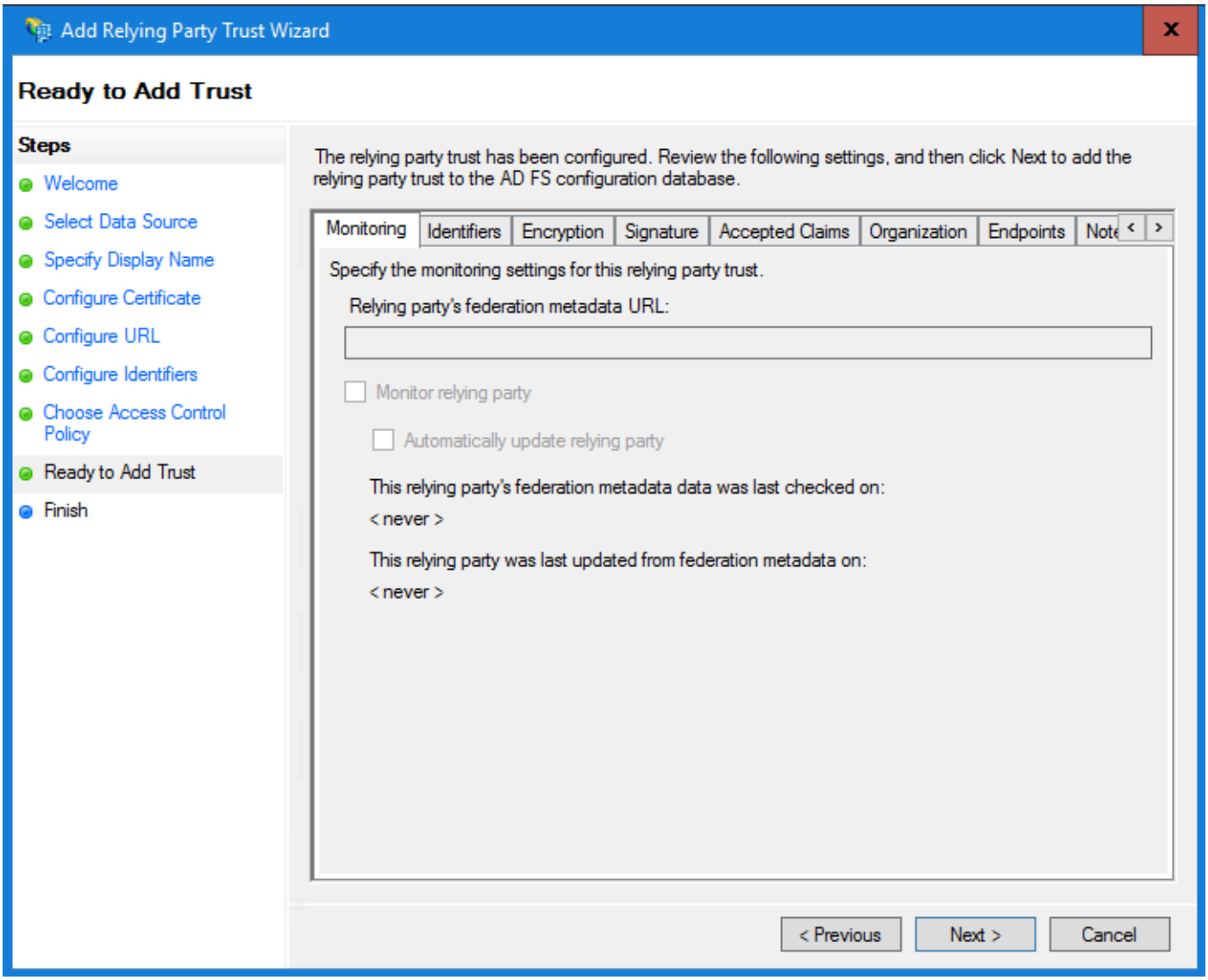
- 値はhttps://<Web-Server-Or-Load-Balancer-FQDN>/形式である必要があります。



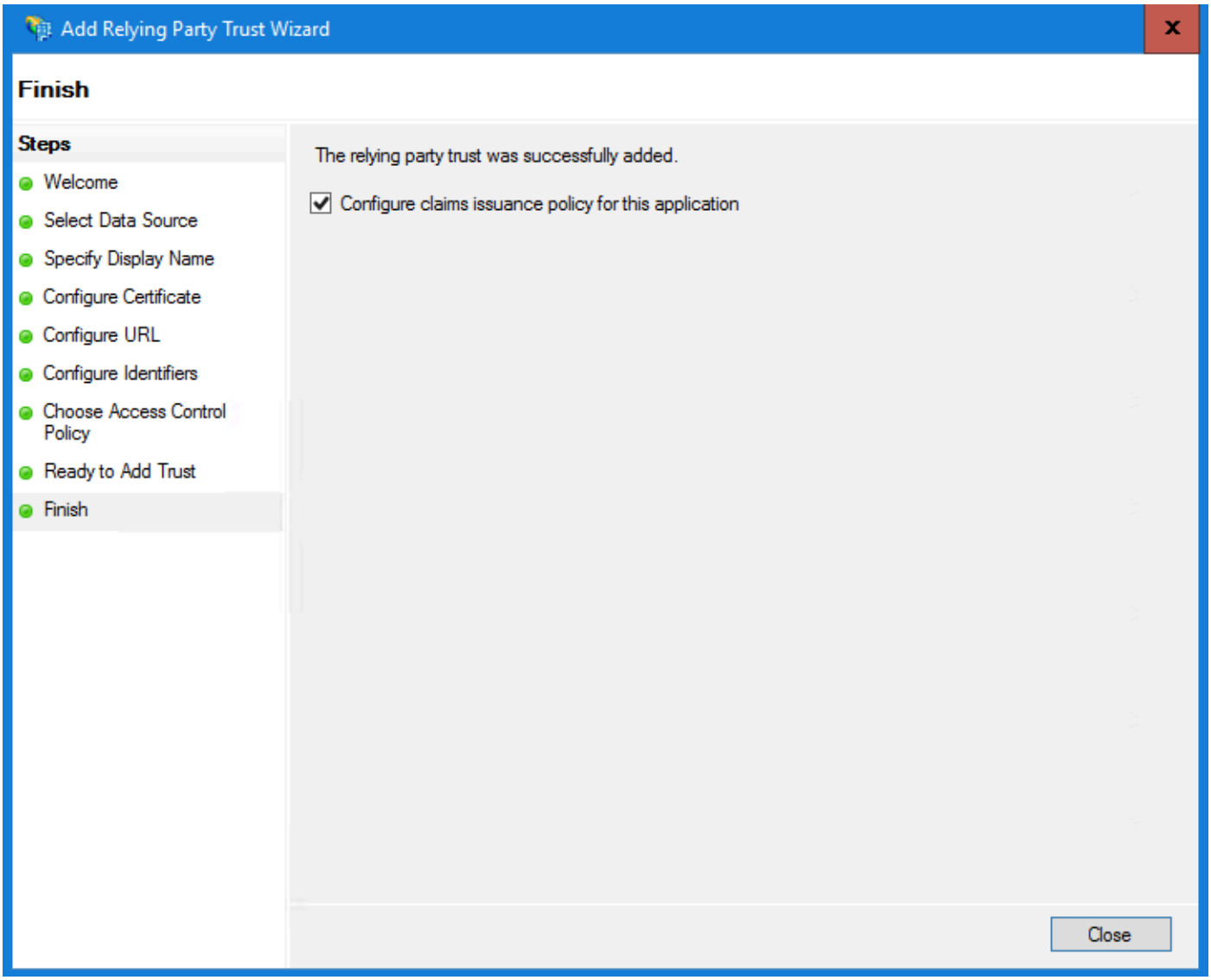
e.Choose Access Control Policyページで、デフォルト値の「Permit everyone」ポリシーでNextをクリックします。



f. 「信頼を追加する準備ができました」ページで、「次へ」をクリックします。

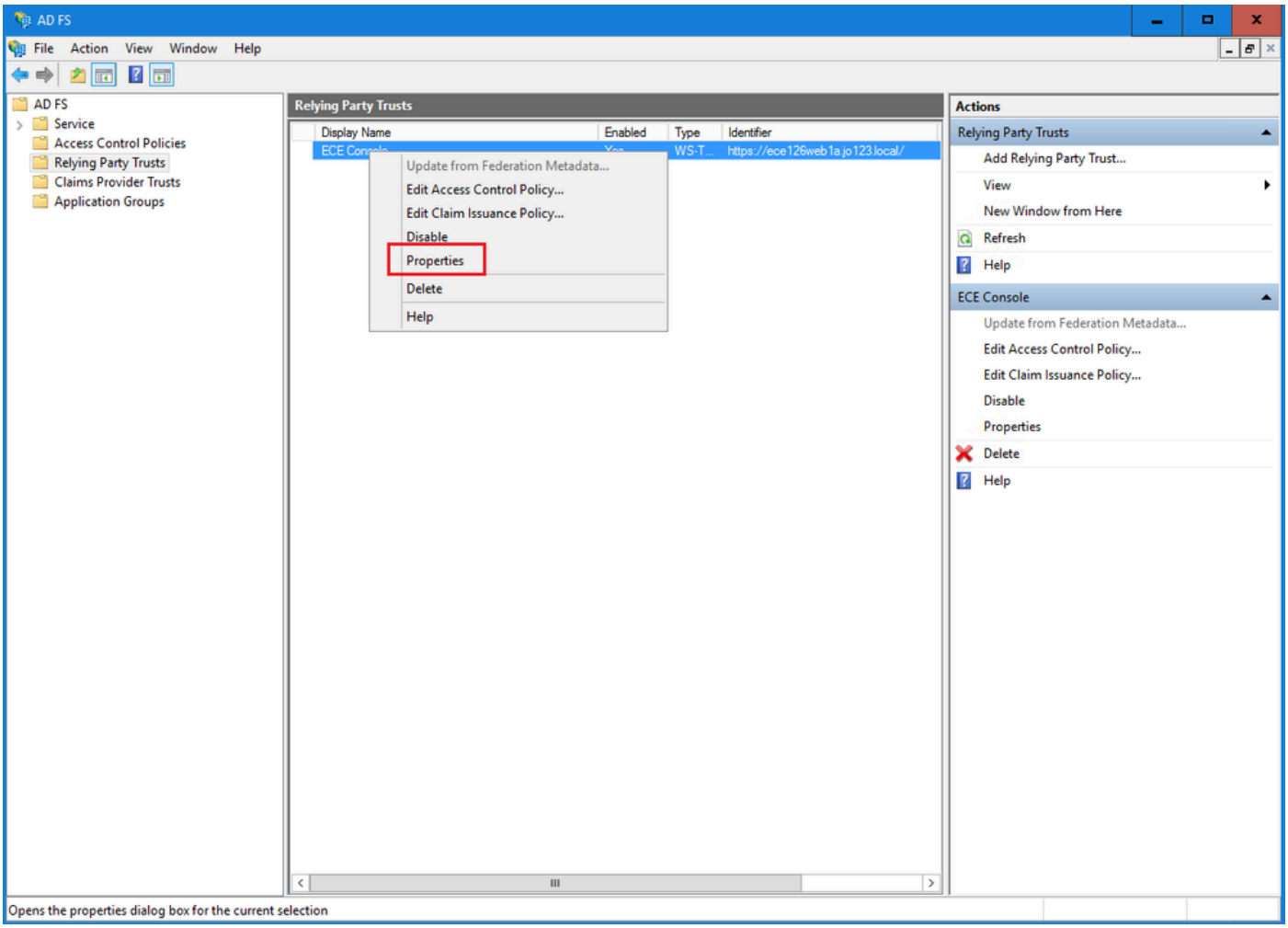


g.証明書利用者信頼が正常に追加されたら、[閉じる]をクリックします。



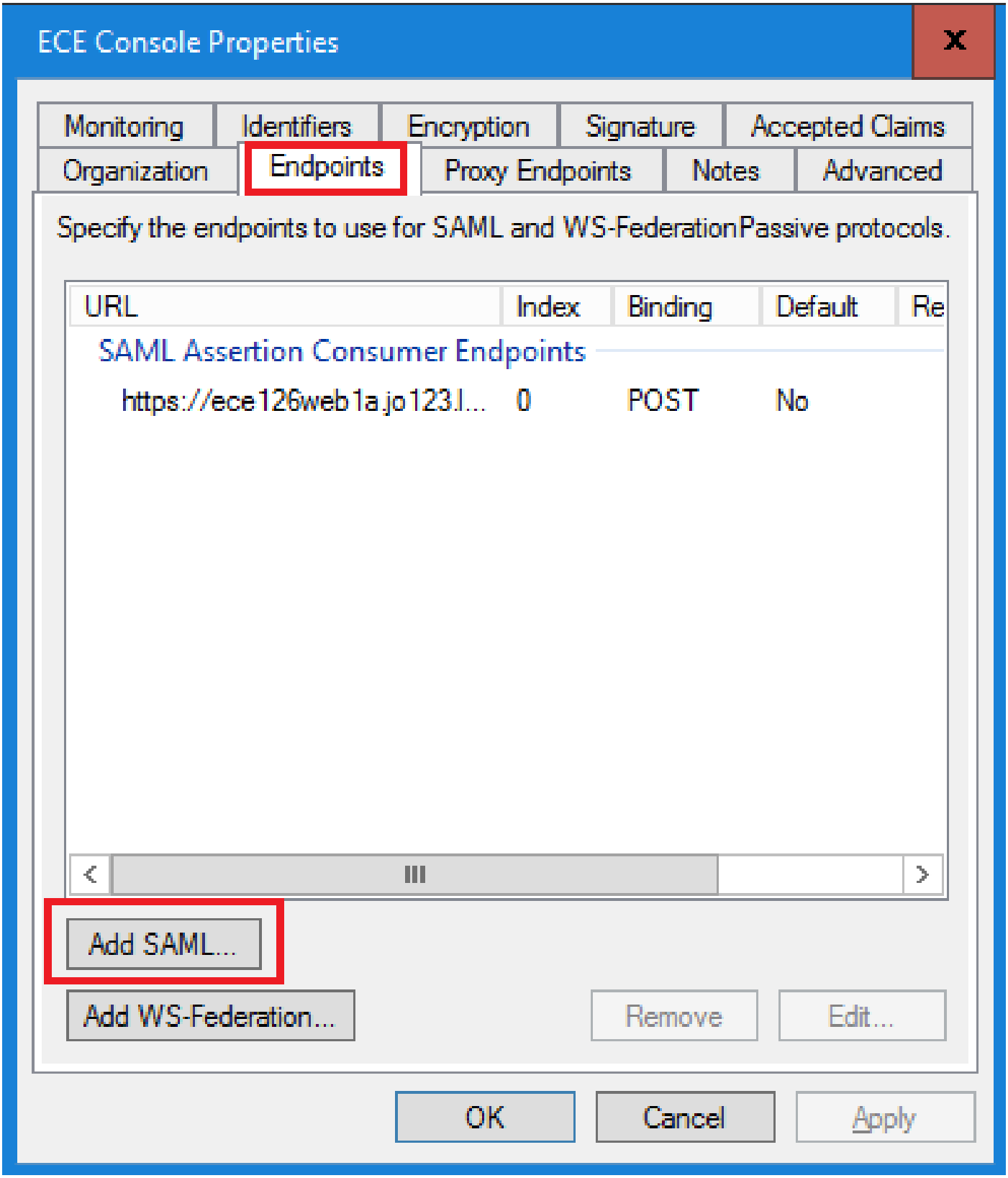
手順 4

信頼プロバイダーの信頼の一覧で、ECE用に作成された証明書利用者信頼を選択し、操作セクションでプロパティをクリックします。



手順 5

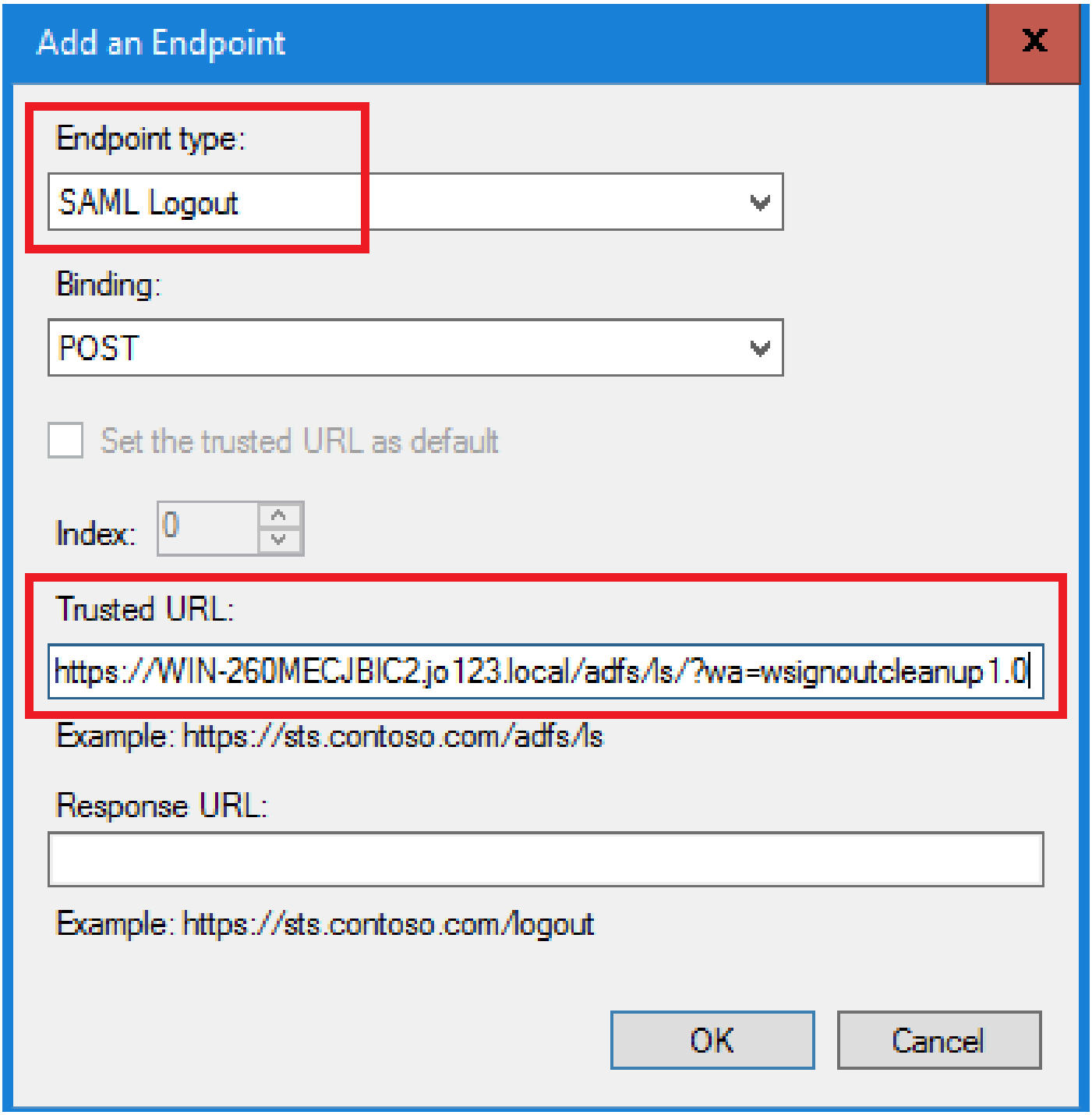
Propertiesウィンドウで、Endpointsタブに移動し、Add SAML..ボタンをクリックします



手順 6

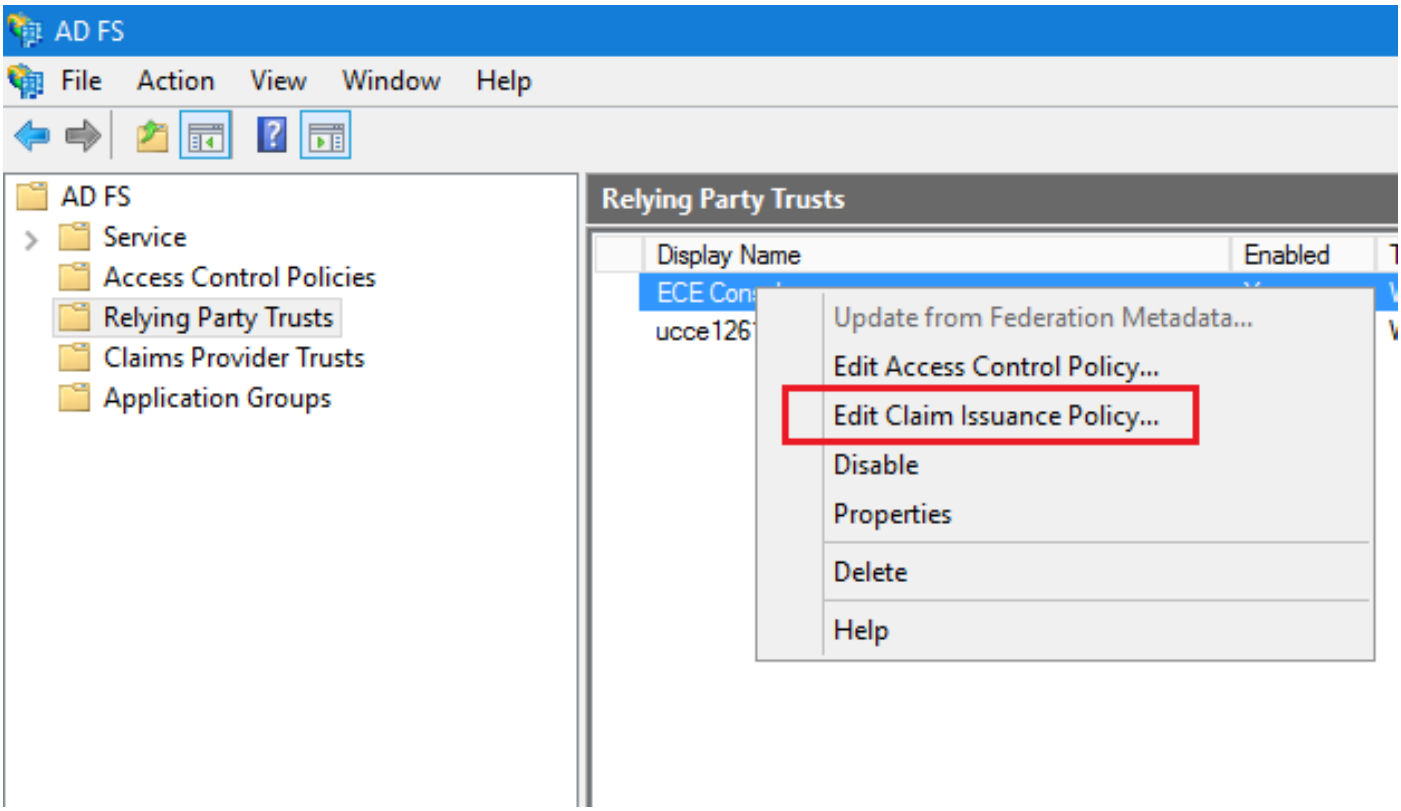
Add an Endpointウィンドウで、次のように設定します。

1. エンドポイントタイプとしてSAML Logoutを選択します。
2. 信頼できるURLをhttps://<ADFS-server-FQDN>/adfs/ls/?wa=wsignoutcleanup1.0として指定します。
3. [OK] をクリックします。



ステップ7

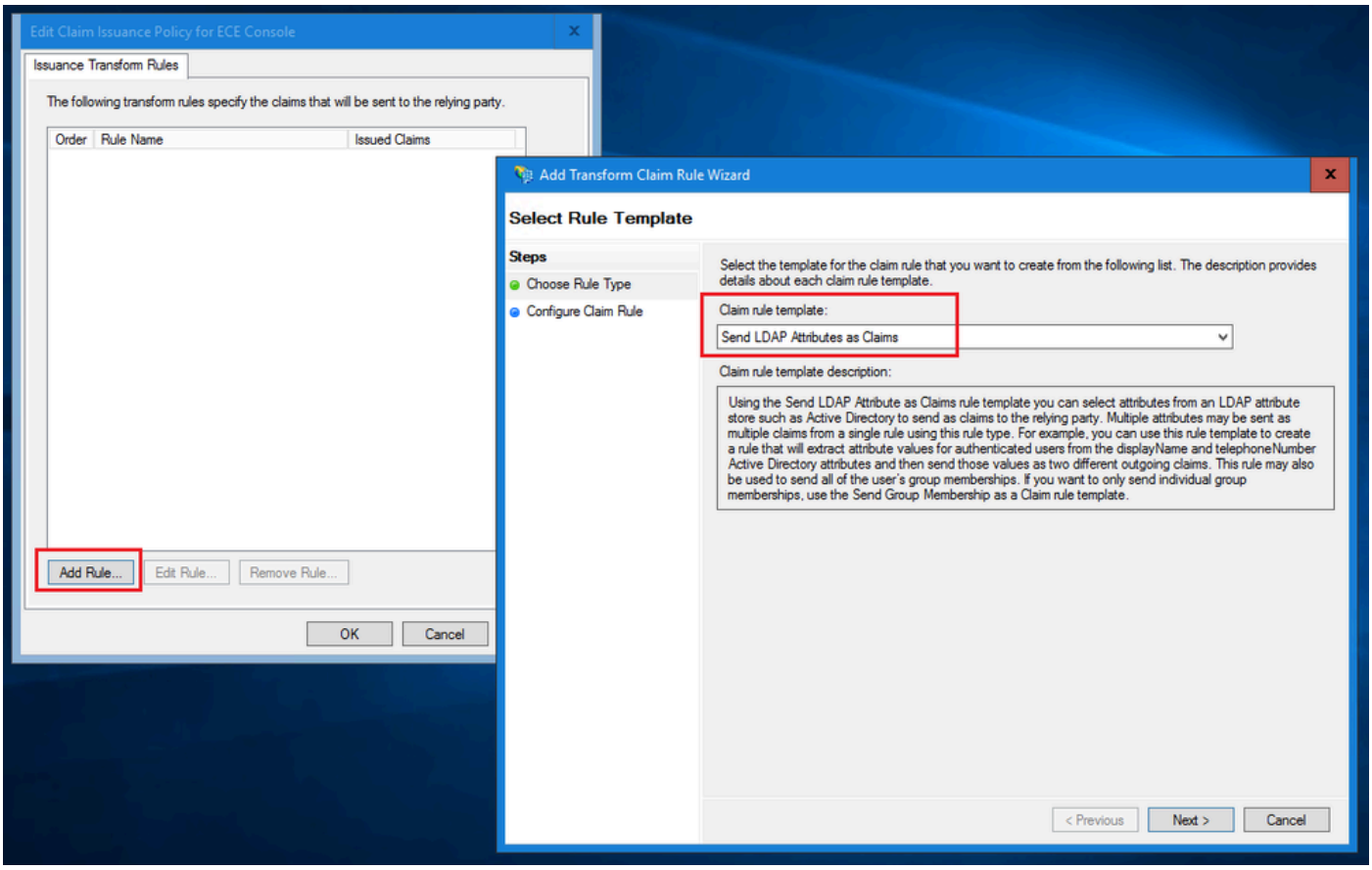
[信頼プロバイダーの信頼]の一覧で、ECE用に作成された信頼を選択し、[操作]セクションで[要求保険契約の編集]をクリックします。



手順 8

Edit Claim Insurance PolicyウィンドウのIssuance Transform Rulesタブで、Add Rule...ボタンをクリックし、次のように設定します。

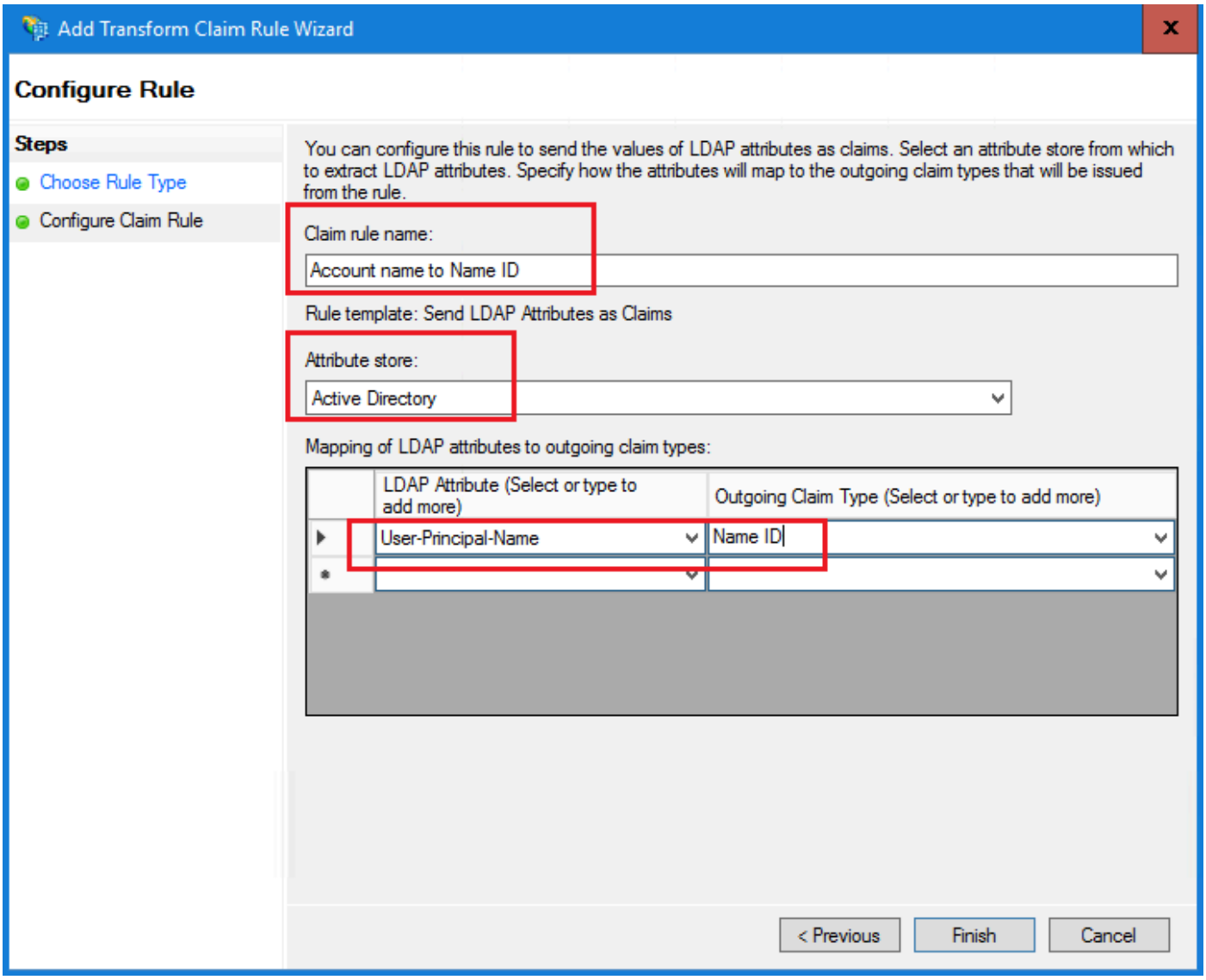
a. Choose Rule Typeページで、ドロップダウンからSend LDAP Attributes as Claimsを選択し、Nextをクリックします。

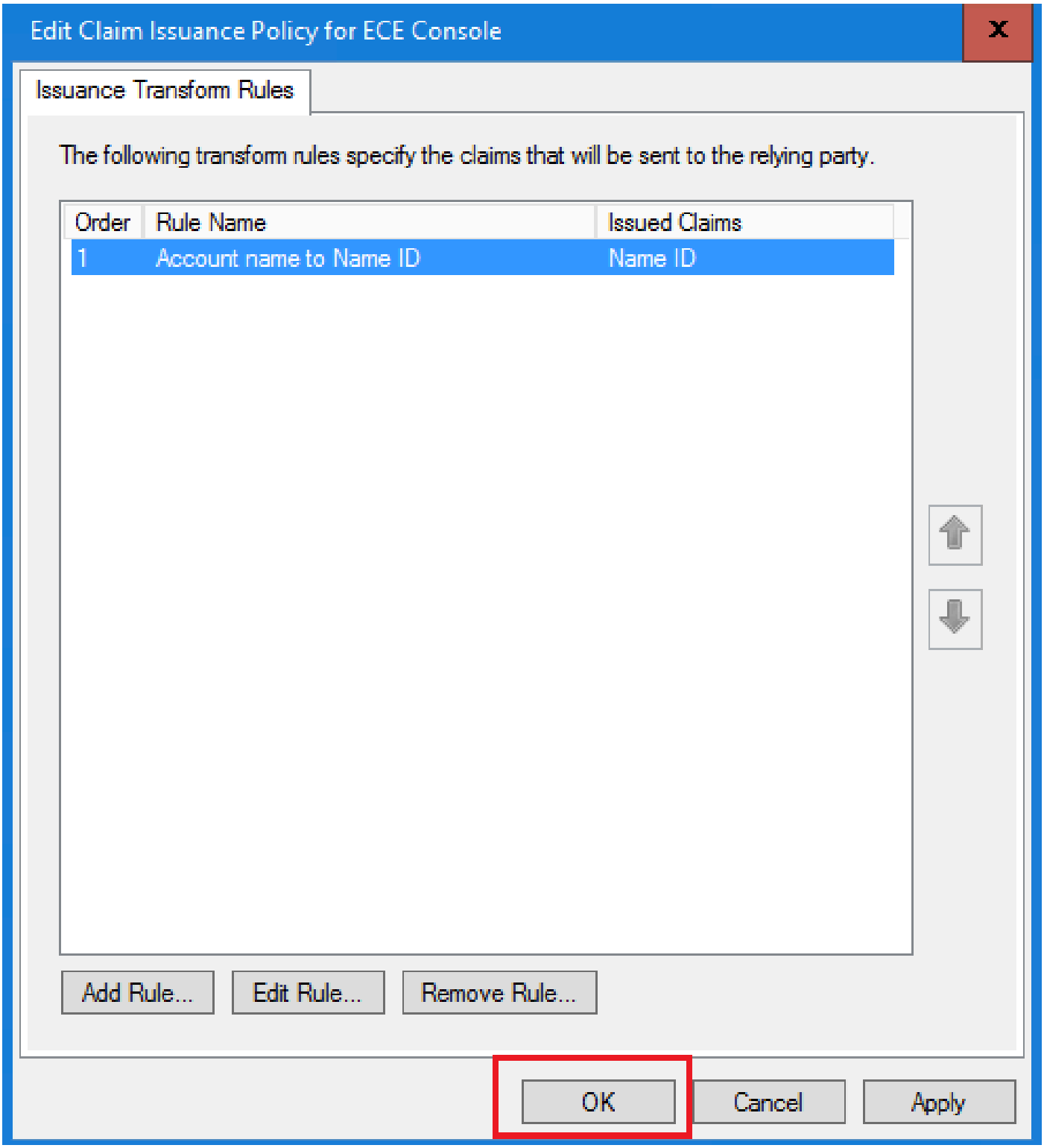


b. [クレームルールの構成]ページで、次の操作を行います。

1. クレームルール名を入力し、属性ストアを選択します。
2. LDAP属性と出力方向の要求の種類のマッピングを定義します。

- 出力方向の要求の種類の名前として、名前IDを選択します。
- Finishをクリックしてedit Claim Insurance Policyウィンドウに戻り、OKをクリックします。

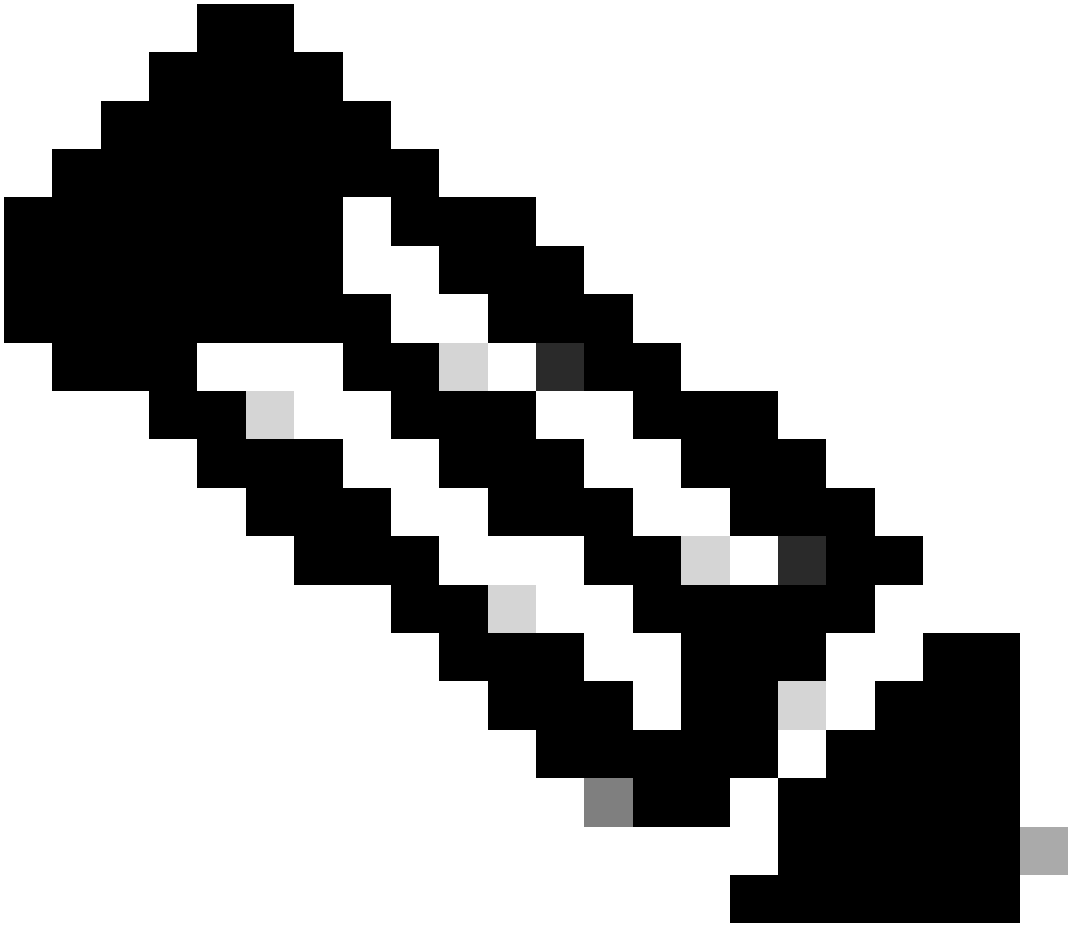

Add Transform Claim Rule Wizard
Configure Rule
Steps
Choose Rule Type
Configure Claim Rule
You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that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



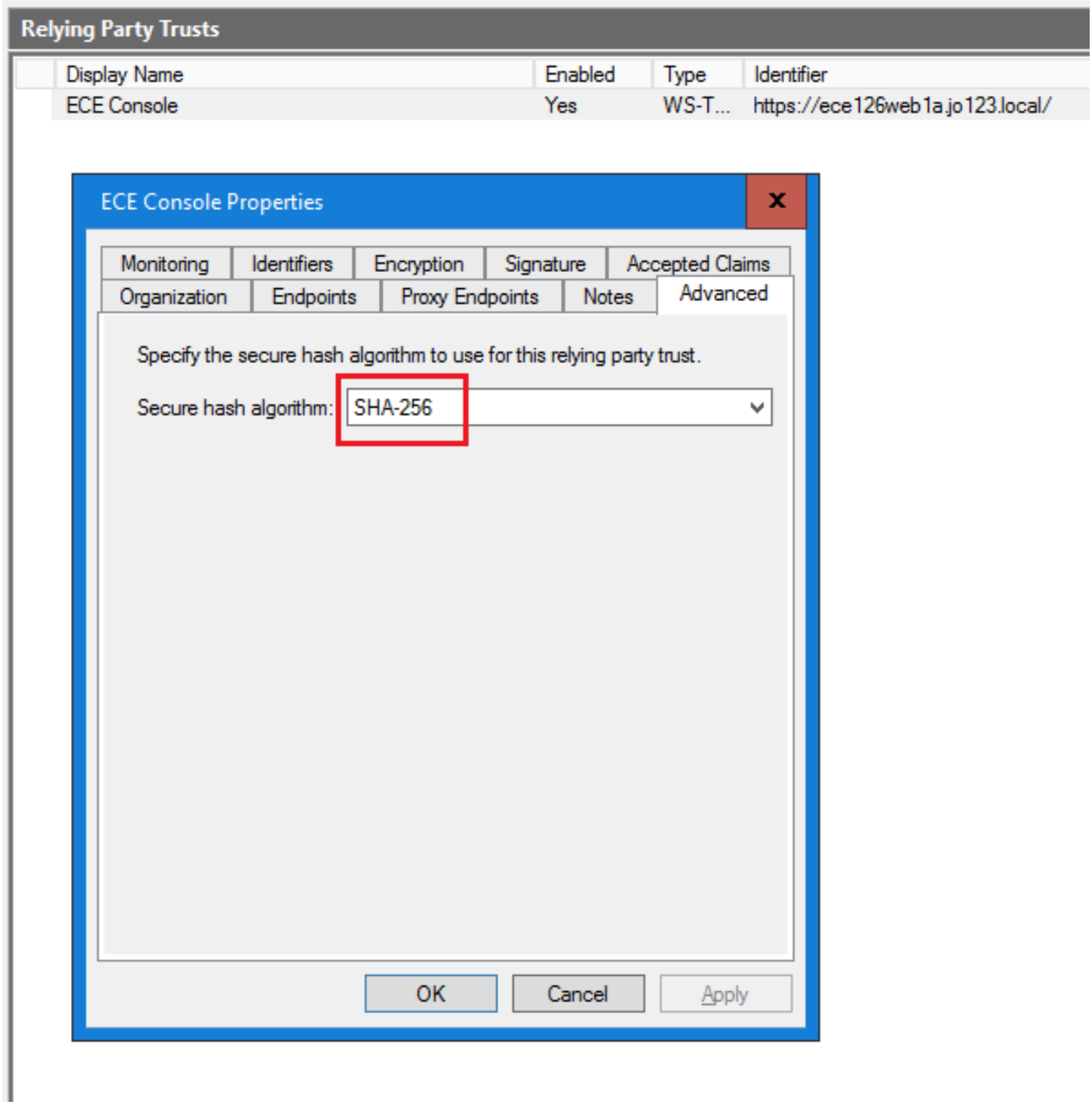
手順 9

[信頼プロバイダーの信頼]の一覧で、作成したECE証明書利用者信頼をダブルクリックします。

開いたPropertiesウィンドウで、Advancedタブに移動し、Secure hash algorithmをSHA-1またはSHA-256に設定します。OK をクリックして、ウィンドウを閉じます。



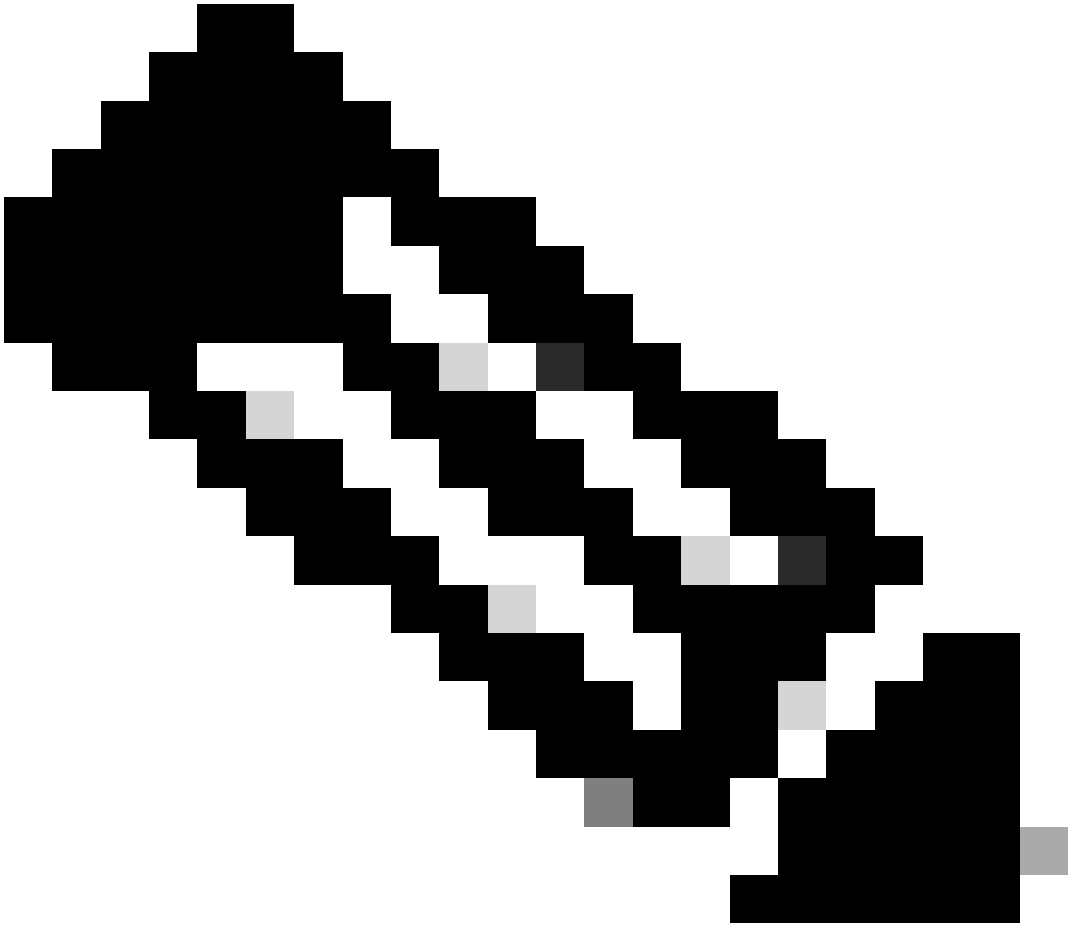
注：この値は、ECEのSSO設定で「サービスプロバイダー」に設定されている「署名アルゴリズム」の値と一致している必要があります



手順 10

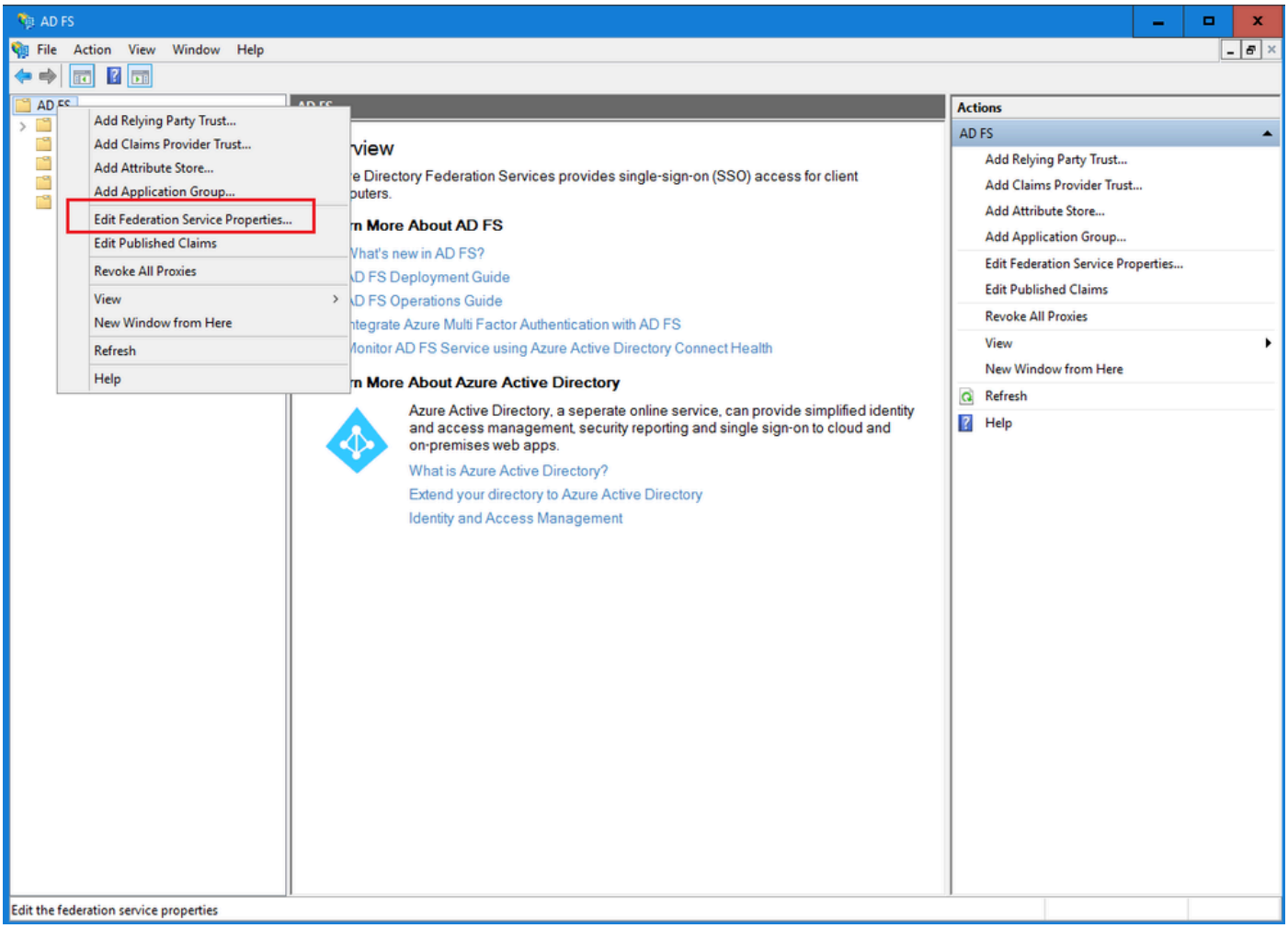
Federation Service Identifierの値を確認し、メモしてください。

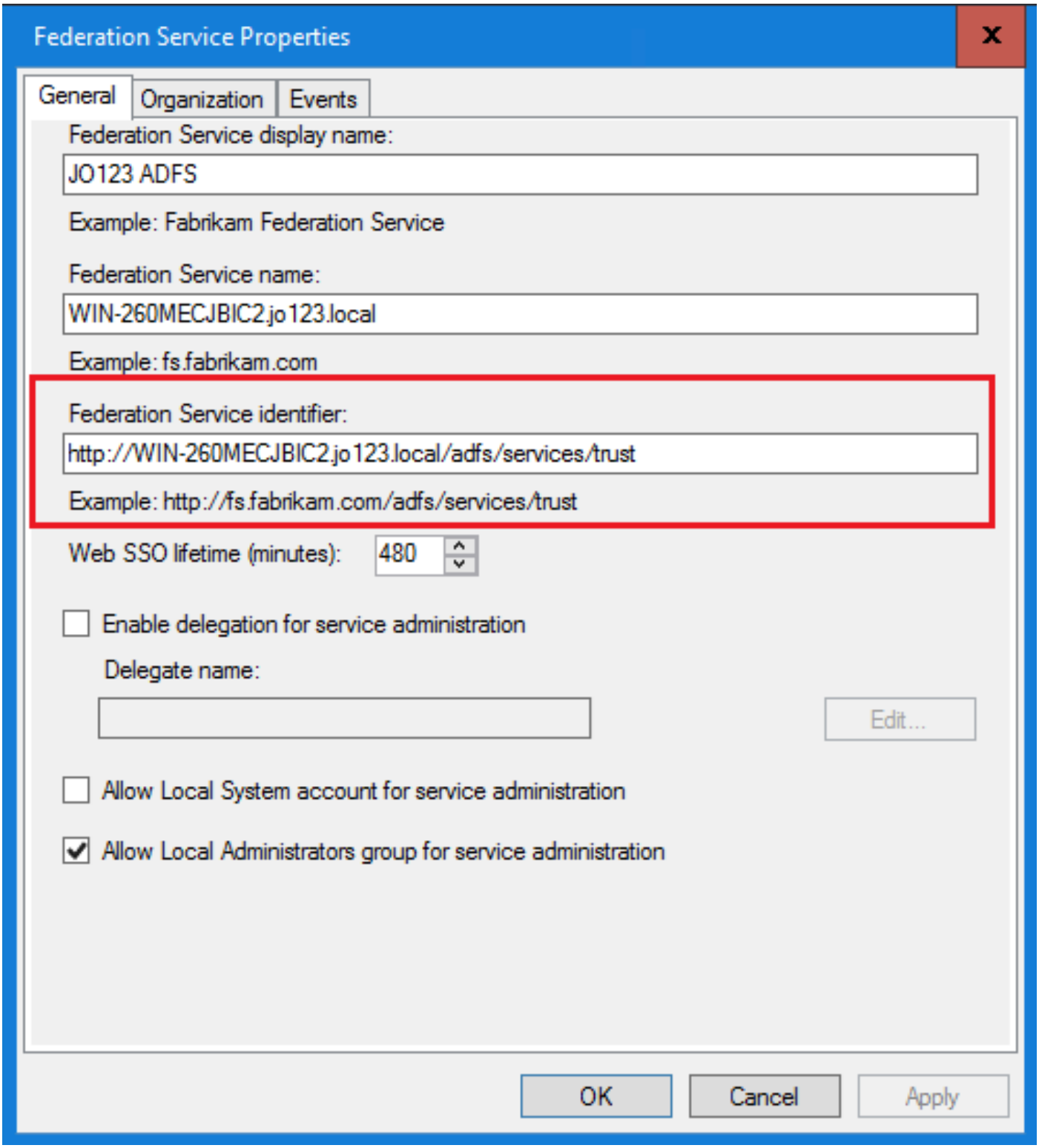
- AD FS管理コンソールで、AD FS >フェデレーションサービスのプロパティの編集>全般タブ>フェデレーションサービス識別子を選択し、右クリックします



注：

- この値は、ECEのSSO設定でアイデンティティプロバイダーの「エンティティID」値を設定するときと同じように追加する必要があります。
- http://を使用することは、ADFSが安全ではないことを意味するわけではありません。これは単なる識別子です。


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



IDプロバイダーの設定

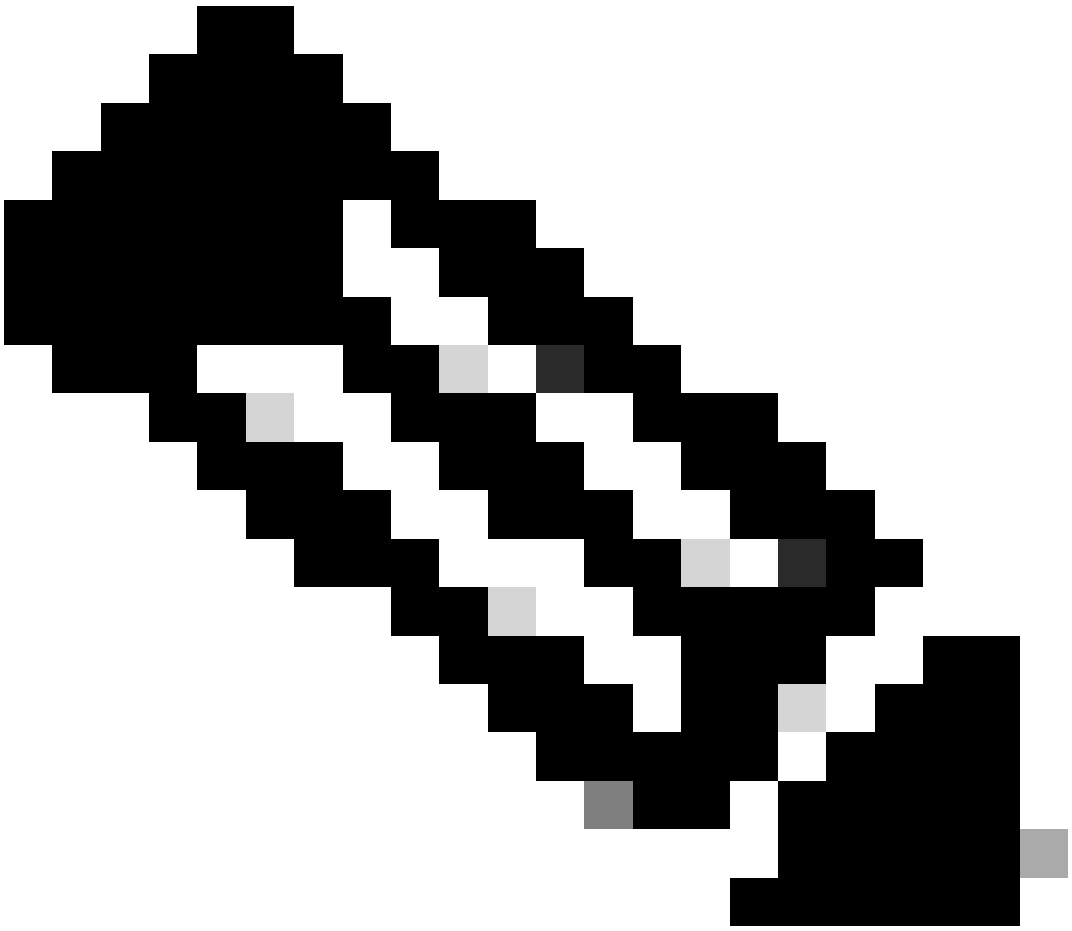
手順 11

管理者ロールまたはスーパーバイザロールを持つユーザがSSOログインクレデンシャルを使用してFinesseの外部のECEのパーティションにサインインできるようにSSOを設定するには、Java Keystore(JKS)証明書が必要です。

管理者またはスーパーバイザの役割を持つユーザがSSOログインクレデンシャルを使用して

Finesseの外部のECEのパーティションにサインインできるようにSSOを設定する場合は、Javaキーストア(JKS)証明書を公開キー証明書に変換し、ECEのIdPサーバで作成された証明書利用者信頼で設定する必要があります。

JKS証明書を受け取るには、IT部門に問い合わせてください。

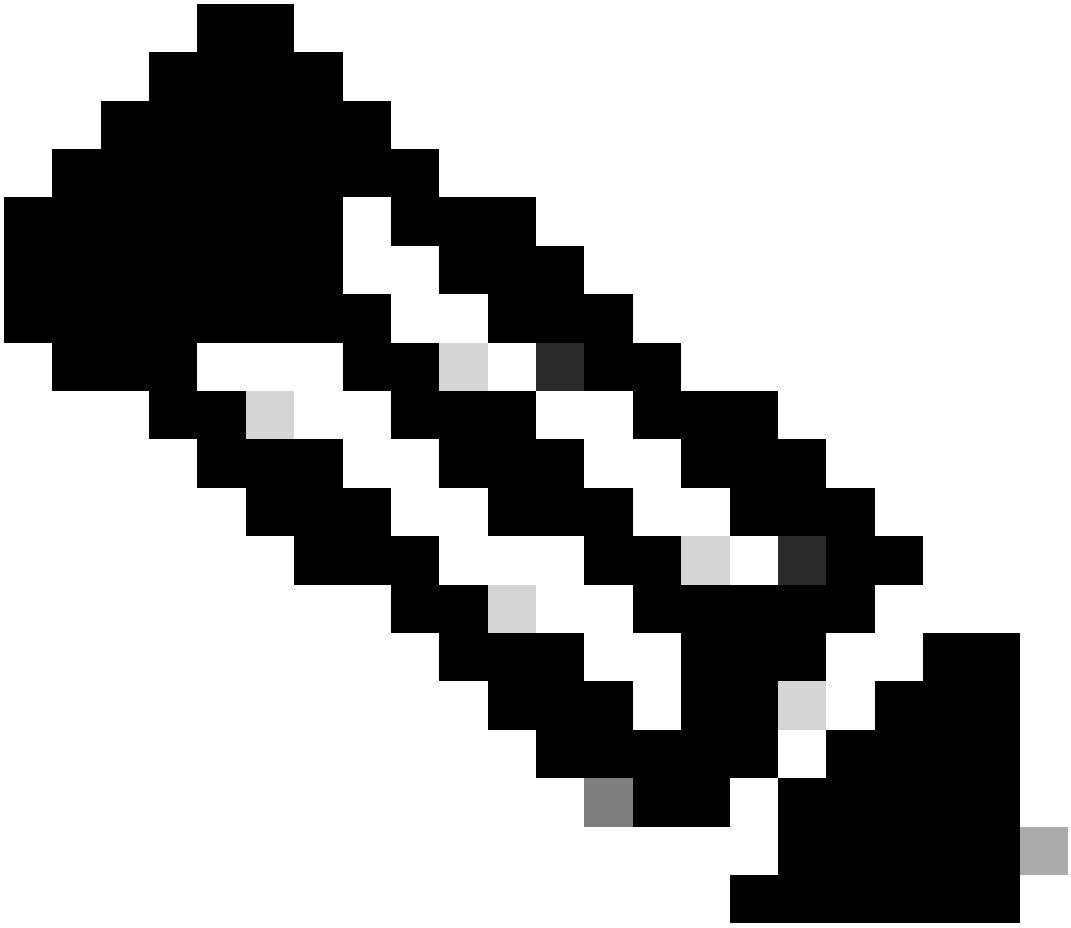


注：これらの手順は、IDプロバイダーとしてADFSを使用するシステムに適用されます。他のIDプロバイダーは、公開キー証明書を設定する方法が異なる場合があります。

ラボでJKSファイルが生成された例を次に示します。

a. JKSを生成します。

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



注：ここで入力したキーストアパスワード、エイリアス名、およびキーパスワードは、ECEのSSO設定で「サービスプロバイダー」設定を設定する際に使用されます。

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

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

b.証明書をエクスポートします。

このkeytoolコマンドは、ece126web1a_saml.crtというファイル名を持つ.crt形式の証明書ファイルをC:\Tempディレクトリにエクスポートします。

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

手順 12

IDプロバイダーの設定

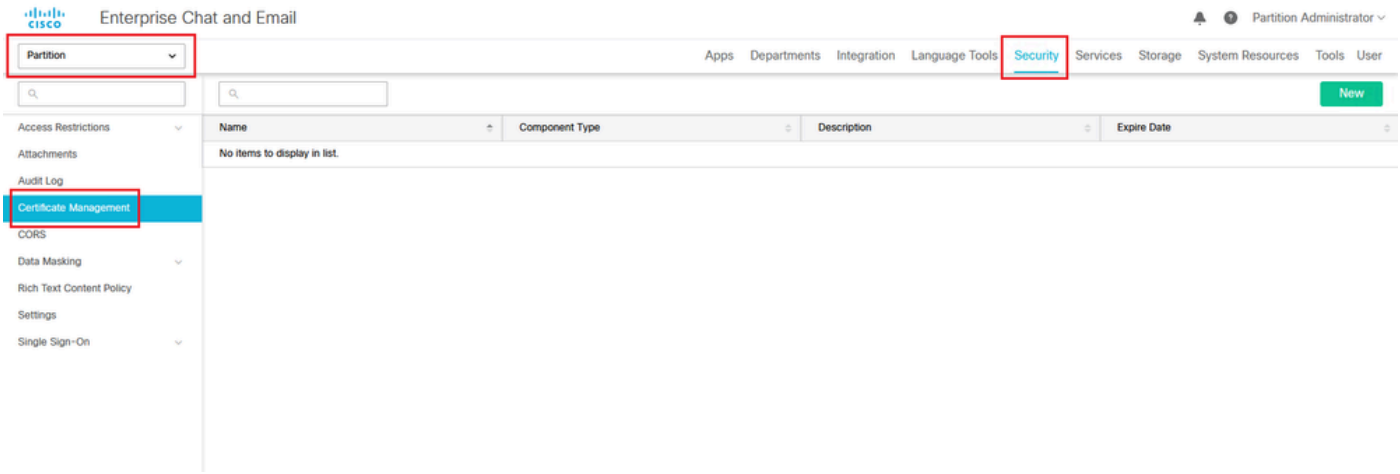
1. AD FS管理コンソールで、ECE用に作成された証明書利用者信頼を選択し、右クリックします。
2. 信頼の[プロパティ]ウィンドウを開き、[署名]タブで[追加]ボタンをクリックします。
3. 公開証明書（前の手順で生成した.crtファイル）を追加し、OKをクリックします。

証明書の作成とインポート

手順 13

エージェントのシングルサインオンにCisco IDSを使用するようにSSOを設定する前に、Cisco IdSサーバからのTomcat証明書をアプリケーションにインポートする必要があります。

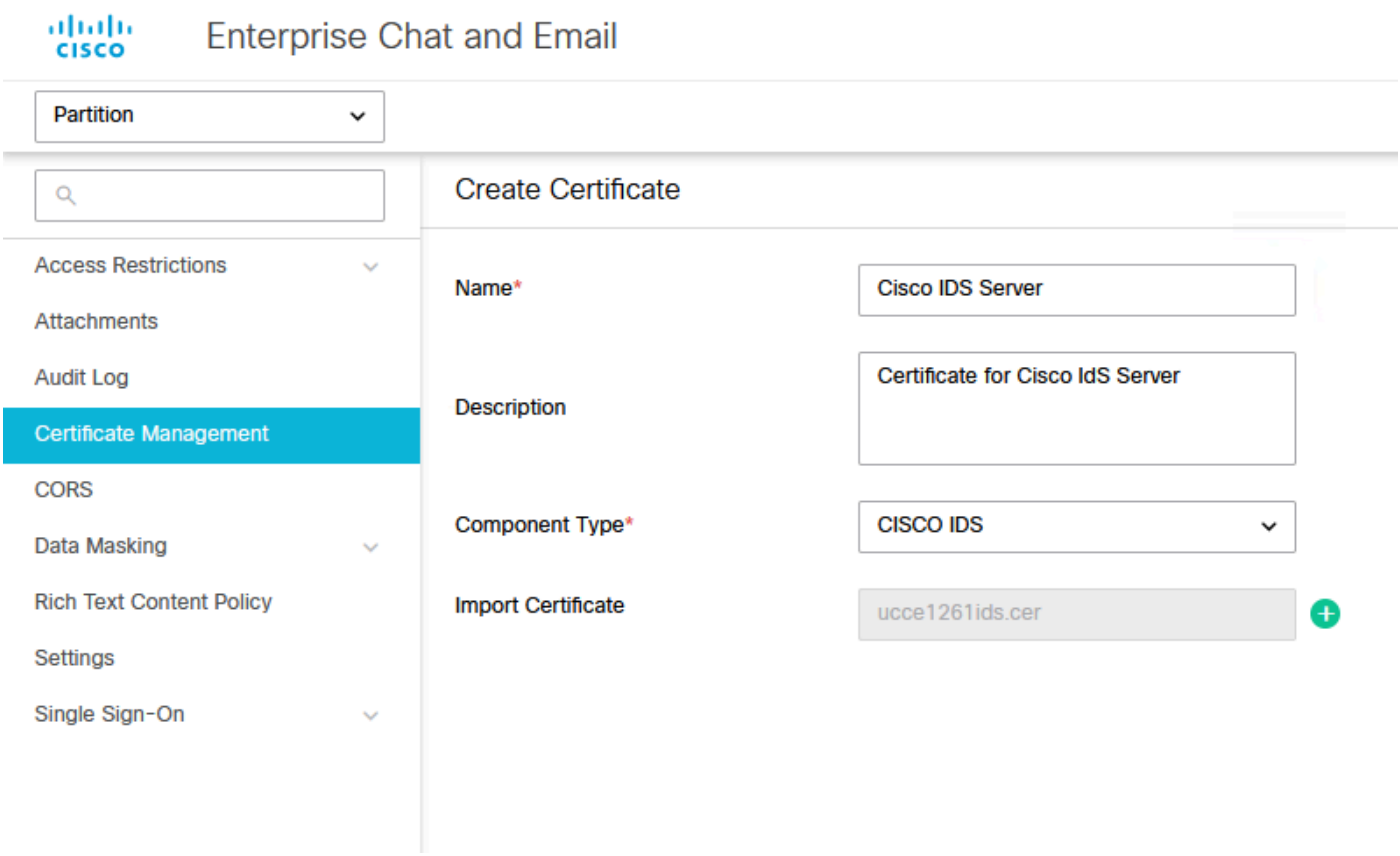
a. ECE管理コンソールのパーティションレベルメニューで、Securityオプションをクリックし、左側のメニューからCertificate Managementを選択します。



b. Certificate Managementスペースで、Newボタンをクリックし、該当する詳細情報を入力します。

- 名前：証明書の名前を入力します。
- 説明：証明書の説明を追加します。
- Component Type:CISCO IDSを選択します。
- 証明書のインポート：証明書をインポートするには、[検索と追加]ボタンをクリックし、要求された詳細を入力します。
- 証明書ファイル： [参照]ボタンをクリックし、インポートする証明書を選択します。証明書は、.pem、.der(BINARY)、または.cer/cert形式でのみインポートできます。
- エイリアス名：証明書のエイリアスを指定します。

c.「保存」をクリックします。

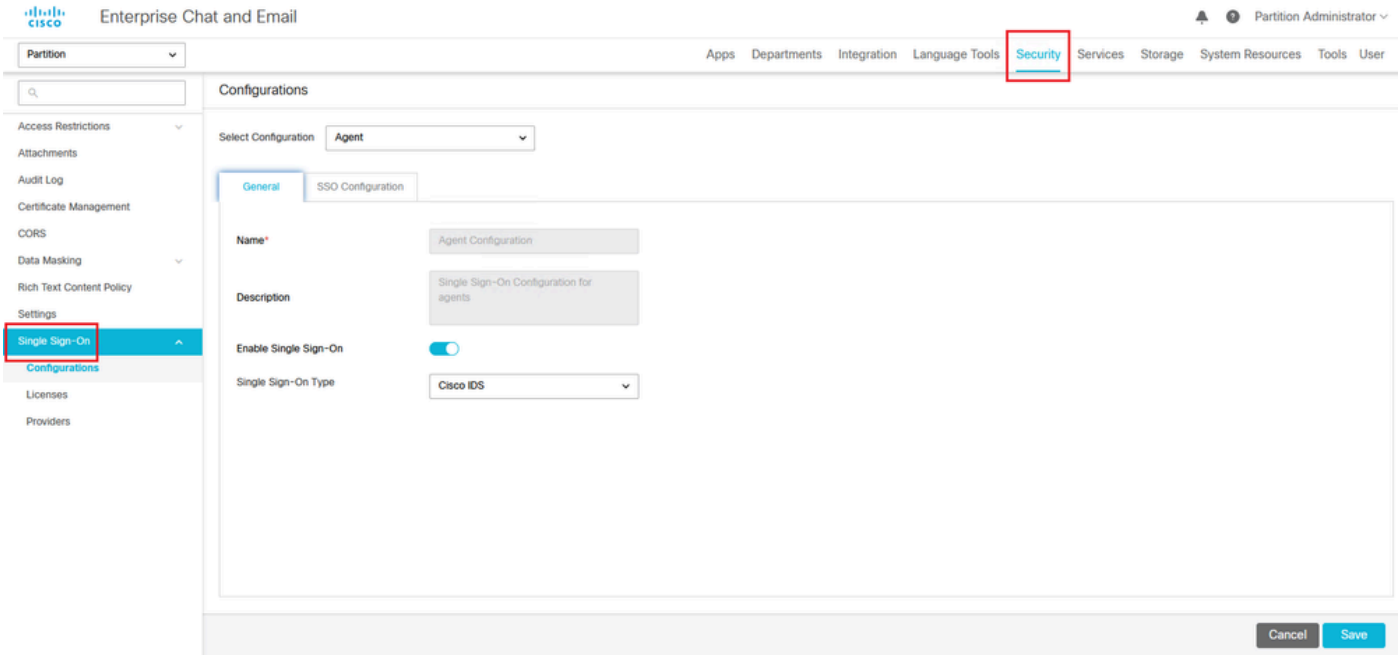


エージェントシングルサインオンの設定

手順 14

1. ECE管理コンソールのパーティションレベルメニューで、Securityオプションをクリックし、左側のメニューからSingle Sign-On > Configurationsを選択します。
2. Select Configurationドロップダウンで、Agentを選択し、Generalタブで設定を行います。

- シングルサインオンの有効化：SSOを有効にするには、トグルボタンをクリックします。
- Single Sign-On Type（シングルサインオンタイプ）:Cisco IDSを選択します。



手順 15

SSO Configurationタブをクリックして、設定の詳細を指定します。

a. OpenID Connectプロバイダー

プライマリユーザー情報エンドポイントURL

- プライマリCisco IDSサーバのユーザ情報エンドポイントURL。
- このURLは、ユーザートークン/ユーザ情報APIを検証します。
- 形式はhttps://cisco-ids-1:8553/ids/v1/oauth/userinfoです。ここで、cisco-ids-1は、プライマリCisco IDSサーバの完全修飾ドメイン名(FQDN)を示します。

ユーザーID要求の名前

- ユーザ情報エンドポイントURLによって返される要求の名前。Unified CCEまたはPackaged CCE内のユーザ名を識別します。
- Unified CCEまたはPackaged CCEのクレーム名とユーザ名は一致している必要があります。
- これは、ベアラートークン検証に応じて取得されるクレームの1つです。
- Unified CCEまたはPackaged CCEのエージェントのユーザ名がユーザプリンシパル名(UPN)と一致する場合は、ユーザID請求名(UDN)フィールドの値として「upn」を指定します。
- Unified CCEまたはPackaged CCEのエージェントのユーザ名がSAMアカウント名と一致する場合は、ユーザID請求名フィールドの値として「sub」を指定します。

セカンダリユーザー情報エンドポイントURL

- Cisco IDSサーバのセカンダリユーザ情報エンドポイントURL。
- 形式はhttps://cisco-ids-2:8553/ids/v1/oauth/userinfoです。ここで、cisco-ids-2は、セカンダリCisco IDSサーバの完全修飾ドメイン名(FQDN)を示します。

ユーザー情報エンドポイントURLメソッド

- ユーザ情報エンドポイントURLへのベアラートークン検証コールを行うためにECEが使用するHTTPメソッド。
- 表示されたオプションのリストからPOSTを選択します（POSTはIDSサーバの方式に合わせてここで選択します）。

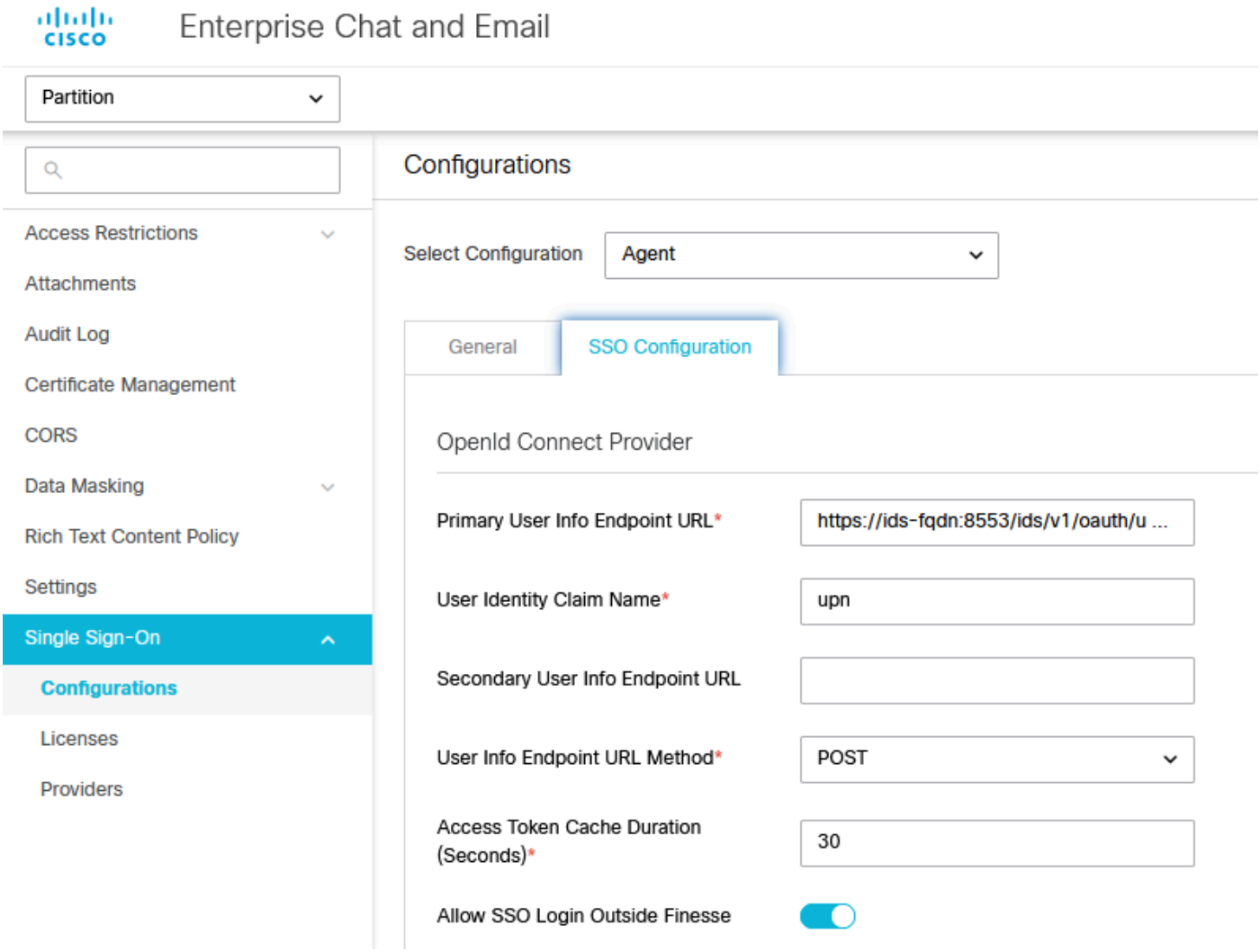
POST：指定されたエンドポイントでCisco IDSサーバにデータを送信するために使用される方式。

アクセストークンのキャッシュ期間（秒）

- ベアラートークンをECEにキャッシュする必要がある期間（秒単位）。
- 検証コールが成功したベアラトークンは、キャッシュにのみ保存されます。（最小値：1、最大値：30）

Finesse外部のSSOログインの許可

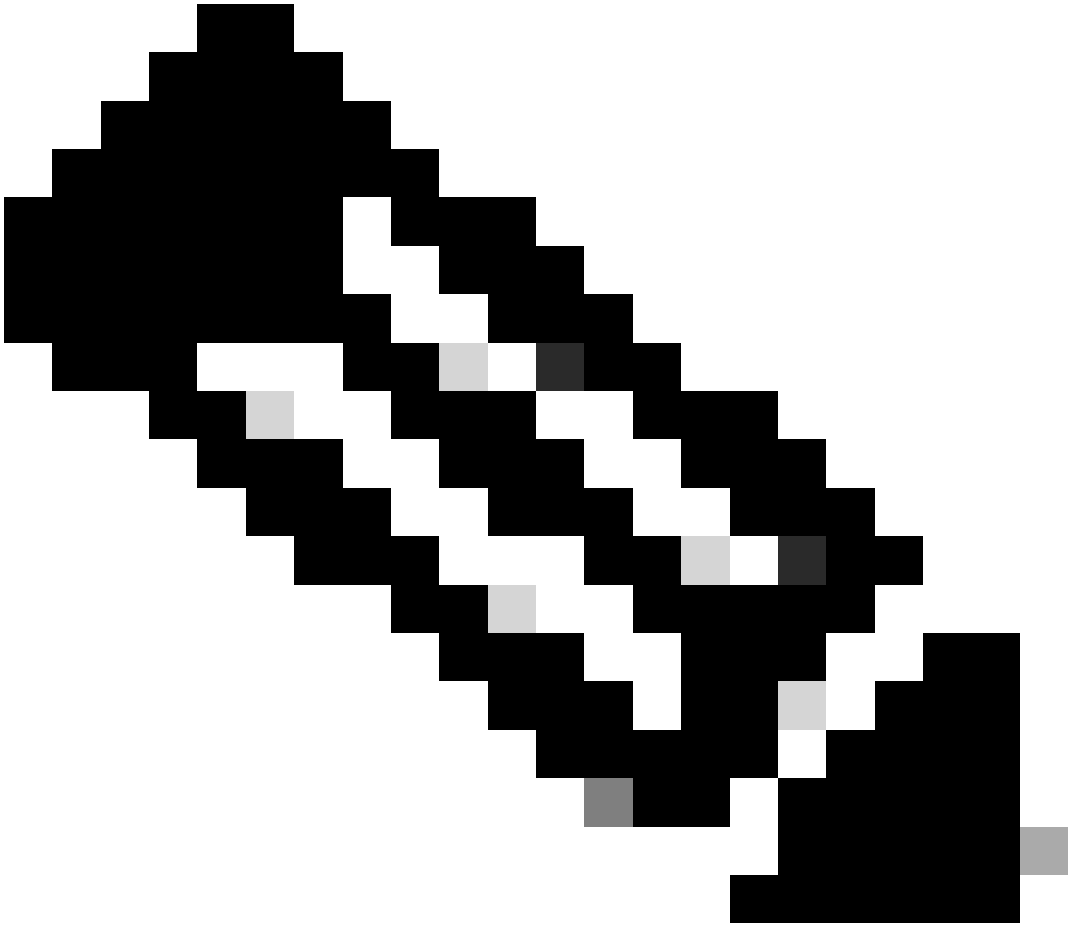
- 管理者ロールまたはスーパーバイザロールを持つユーザが、SSOログインクレデンシャルを使用してFinesseの外部のECEのパーティションにサインインできるようにする場合は、このトグルボタンをクリックします。
- 有効にした場合は、[IDプロバイダー]セクションおよび[サービスプロバイダー]セクションに情報を指定する必要があります。
- そのためには、IdP設定で共有IdPサーバが許可されている必要があります。



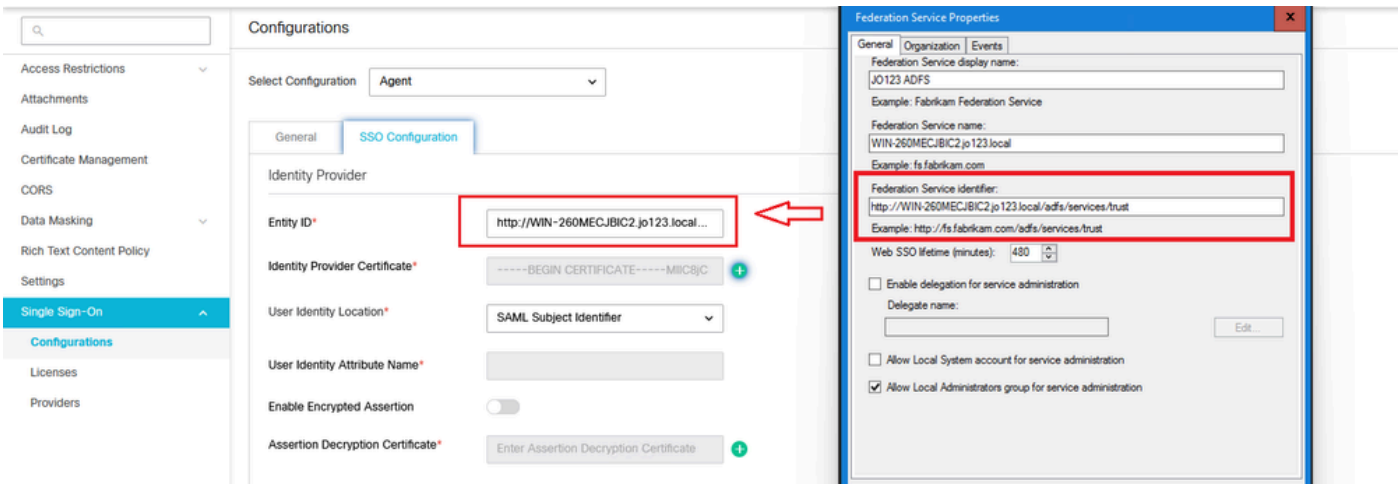
b.アイデンティティプロバイダー

エンティティID

- IdPサーバーのエンティティID。

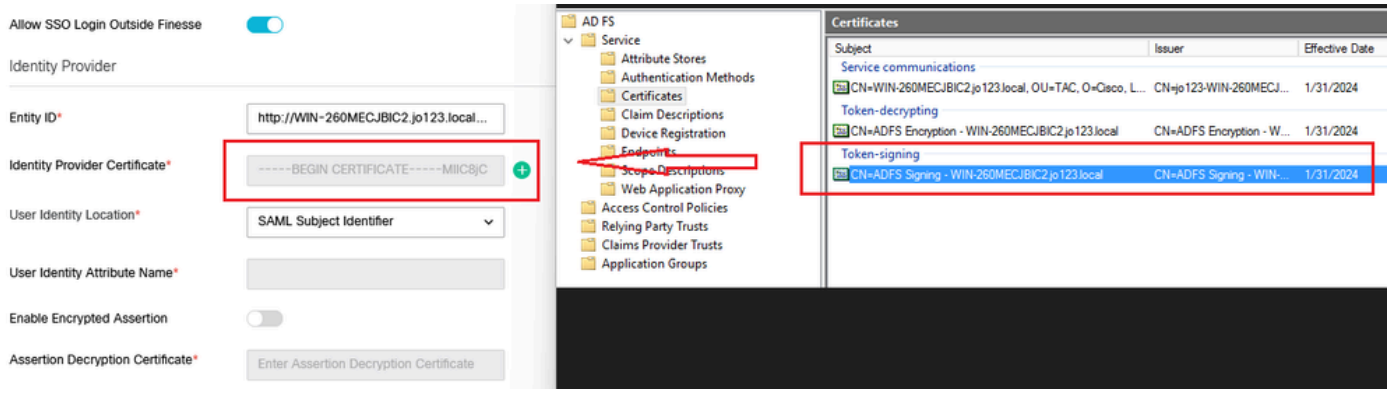


注：この値は、AD FS管理コンソールの[フェデレーションサービス識別子]の値と完全に一致している必要があります。



IDプロバイダー証明書

- 公開鍵証明書。
- 証明書は「-----BEGIN CERTIFICATE-----」で始まり、「-----END CERTIFICATE-----」で終わる必要があります。
- これは、AD FS管理コンソール>サービス>証明書>トークン署名のトークン署名証明書です。



ユーザIDの場所

- SAML Subject Identifierを選択して、証明書内のIDの場所をデフォルトのSAMLサブジェクト識別子（SAMLアサーションのサブジェクトの場合は、<saml:Subject>のユーザ名など）に設定します。
- 証明書の特定の属性（email.addressなど）にIDの場所を割り当てるには、SAML Attributeを選択します。User Identity Attribute Nameフィールドに属性を指定します。

ユーザID属性名

- ユーザIDロケーション値がSAML属性の場合にのみ適用されます。
- これはSAMLアサーション内で調整でき、電子メールアドレスなどのユーザ認証用に別の属性を選択するために使用できます。
- また、SAML属性を持つ新しいユーザを作成するために使用することもできます。
- たとえば、email.address属性で指定された値によってユーザが識別され、指定された電子メールアドレスの値がシステム内のどのユーザとも一致しない場合、指定されたSAML属性で新しいユーザが作成されます。

暗号化されたアサーションを有効にする（オプション）

- コンソールログイン用にアイデンティティプロバイダーで暗号化されたアサーションを有効にするには、トグルボタンをクリックして値を有効に設定します。
- そうでない場合は、値をDisabledに設定します。

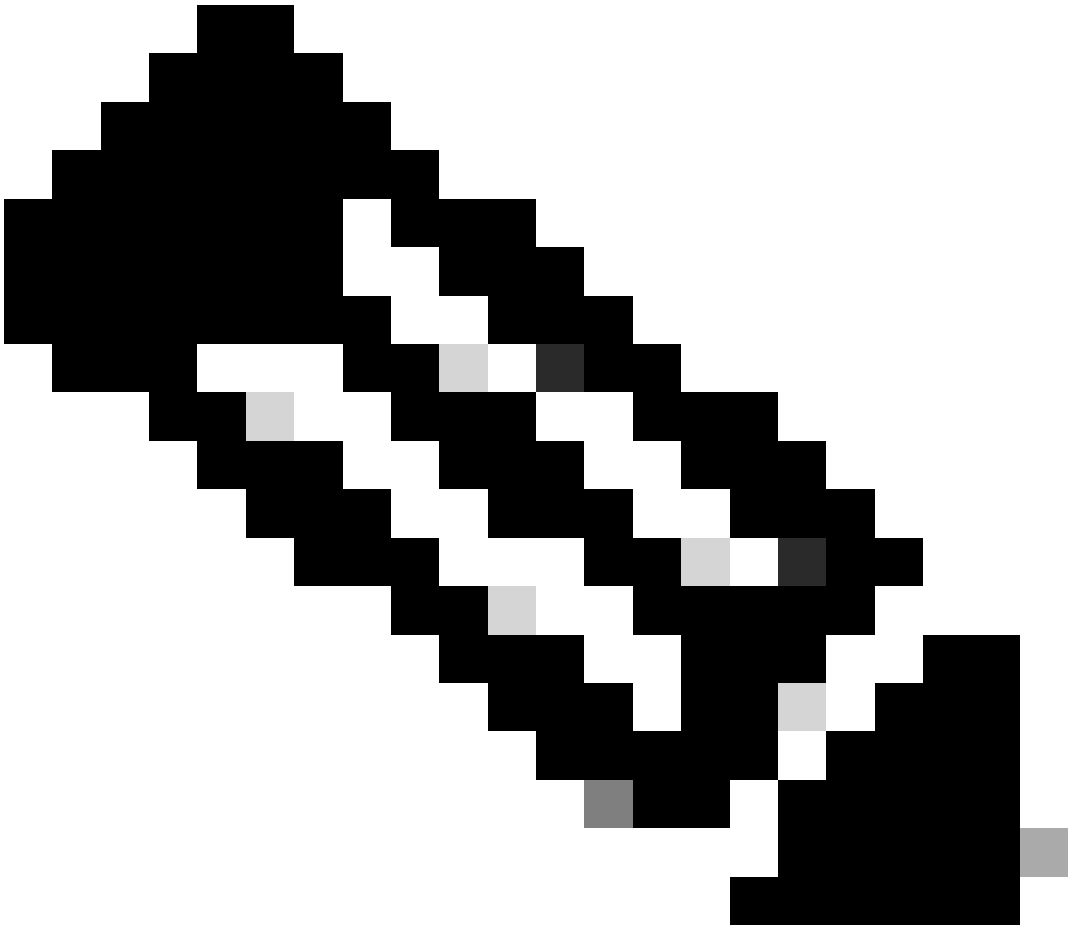
アサーション復号化証明書

Enable encrypted assertionがEnabledに設定されている場合は、Search and Addボタンをクリックし、選択を確認して証明書を変更します。

Assertion Decryption Certificateウィンドウで詳細を指定します。

- Javaキーストアファイル： Javaキーストアファイルのファイルパスを指定します。このファイルは.jks形式で、アイデンティティプロバイダーによって保護されているファイルにシ

ステムがアクセスするために必要な復号化キーが含まれています。
- Alias Name：復号キーの一意の識別子。
- Keystore Password:Javaキーストアファイルにアクセスするために必要なパスワード。
- Key Password：エイリアスの復号化キーにアクセスするために必要なパスワード。



注：これは、AD FS管理コンソールで構成されたECE証明書利用者信頼の[暗号化]タブの証明書と一致する必要があります。

---

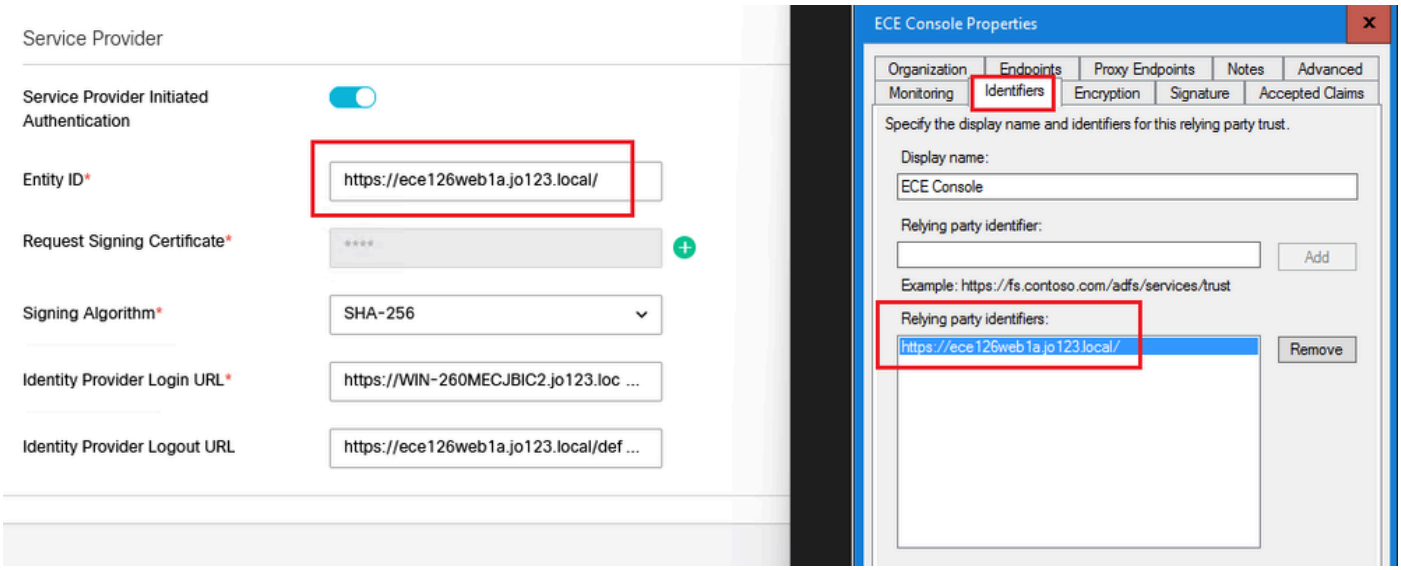
c.サービスプロバイダー

サービスプロバイダー開始認証

- トグルボタンを有効に設定します。

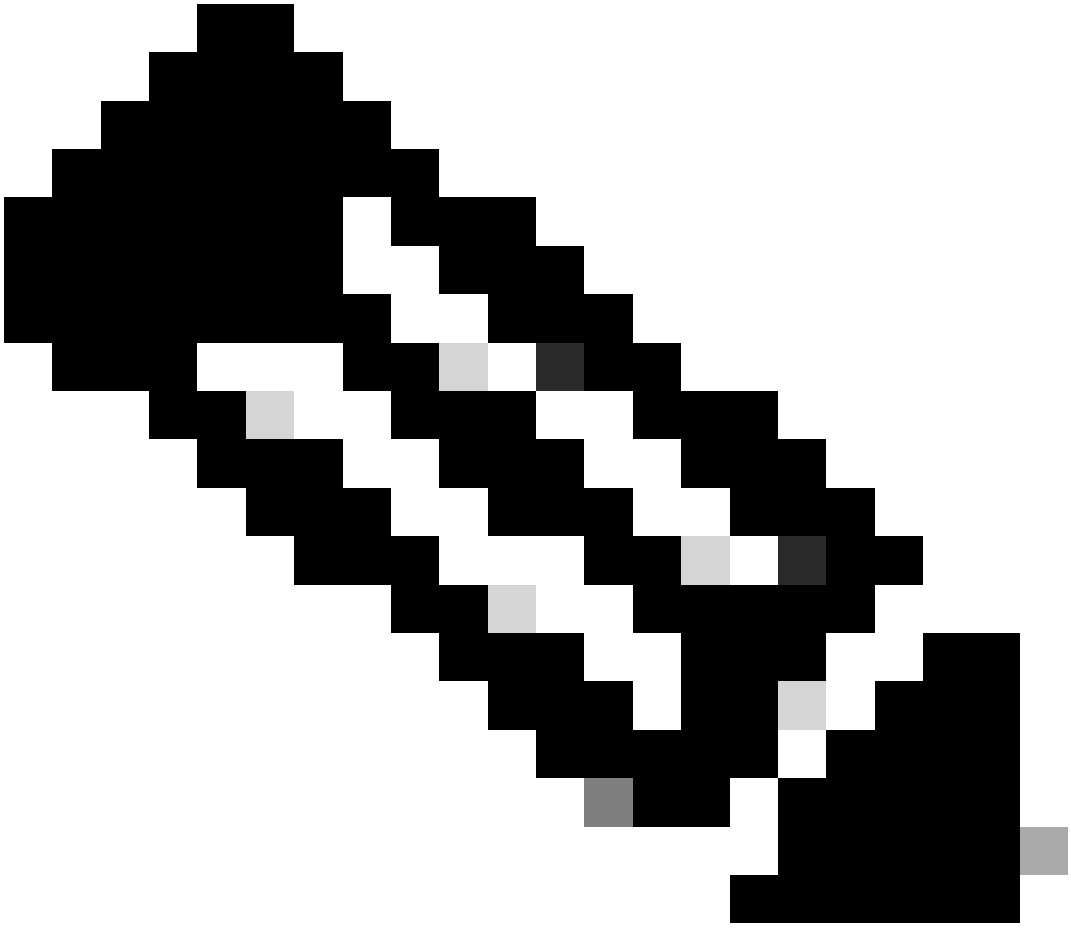
エンティティID

- ECEアプリケーションの外部URLを指定します。

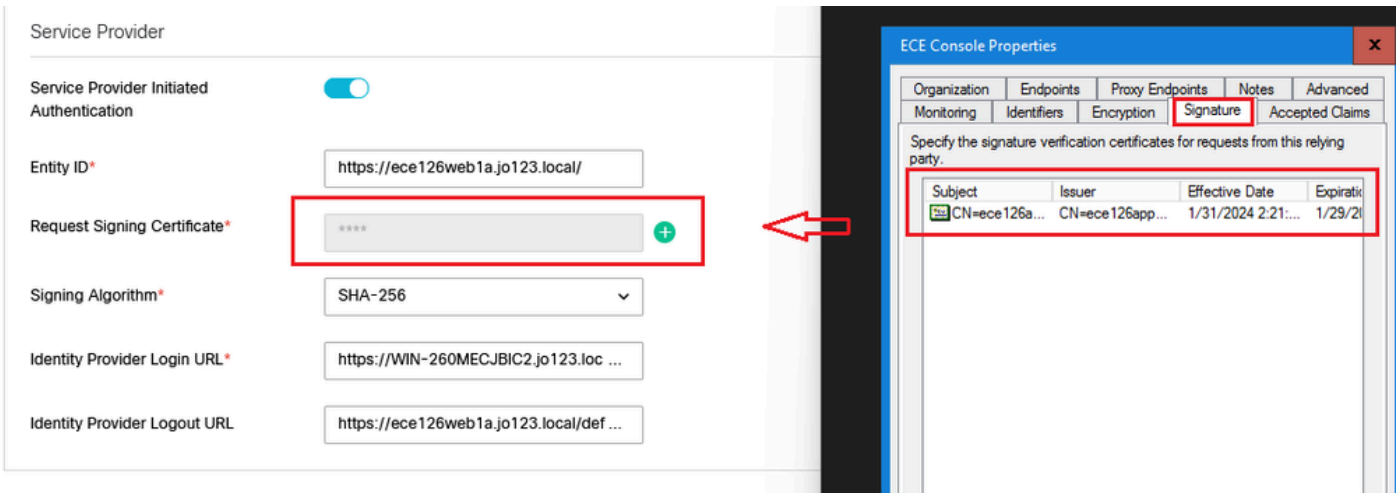


署名証明書の要求

- 必要な情報を提供するには、Javaキーストア(JKS)証明書が必要です。
- ステップ11で生成したエイリアス名とキーストア/キーパスワードを使用して、.jksファイルをアップロードします。

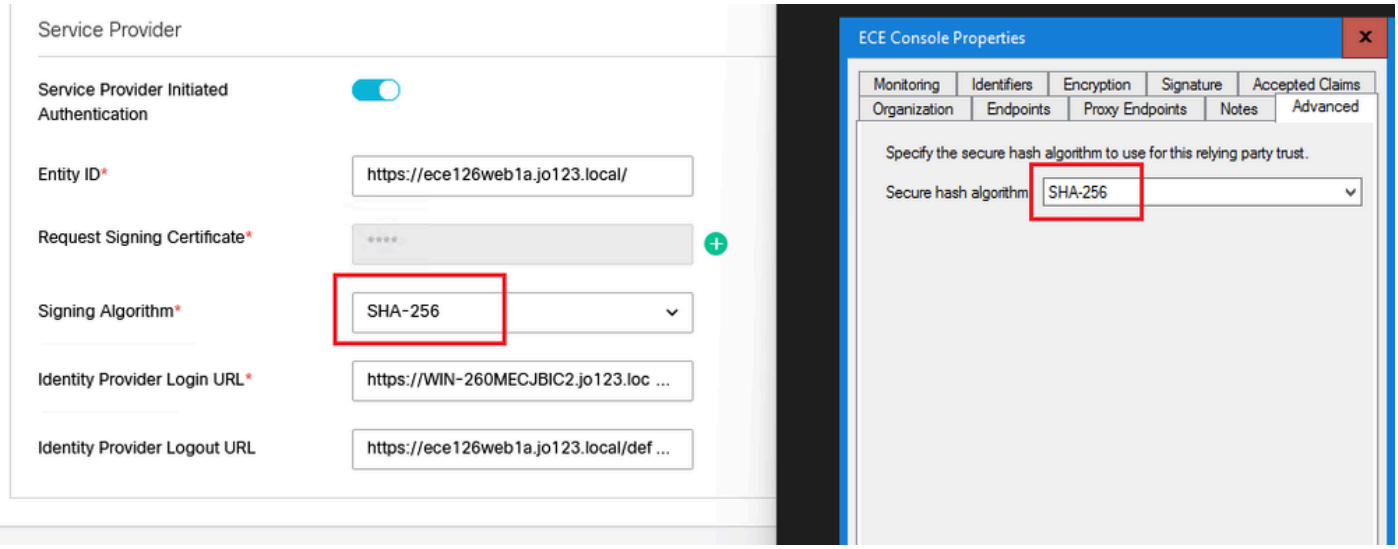


注：これは、AD FS管理コンソールで構成されたECE証明書利用者信頼の[署名]タブにアップロードされた証明書と一致する必要があります。



署名アルゴリズム

- サービスプロバイダーの署名アルゴリズムを設定します。
- ADFSを使用する場合、この値は、ECE用にAdvancedタブで作成された証明書利用者信頼で選択したアルゴリズムと一致する必要があります。



IDプロバイダーのログインURL

- SAML認証用のURL。
- たとえば、ADFSの場合、これはhttp://<ADFS>/adfs/lsです。

IDプロバイダーのログアウトURL

- ログアウト時にユーザーがリダイレクトされるURL。これはオプションで、任意のURLを指定できます。
- たとえば、SSOログアウト後に、エージェントをhttps://www.cisco.comまたはその他の任意のURLにリダイレクトできます。

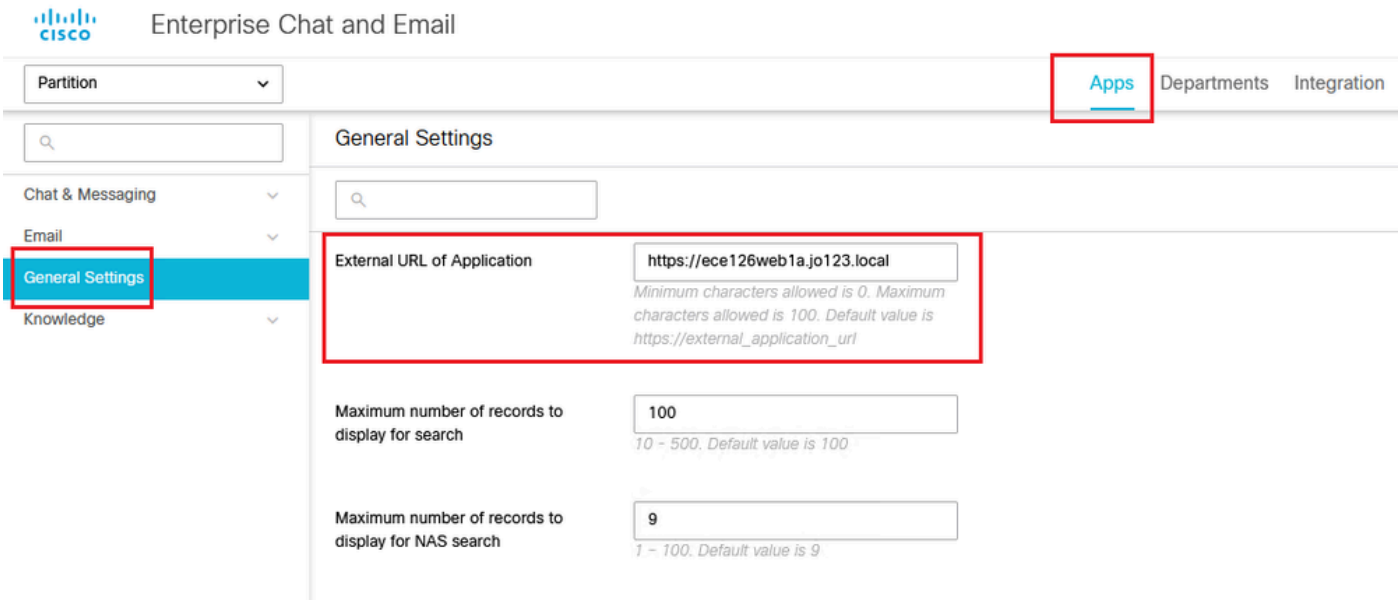
手順 16

[Save] をクリックします。

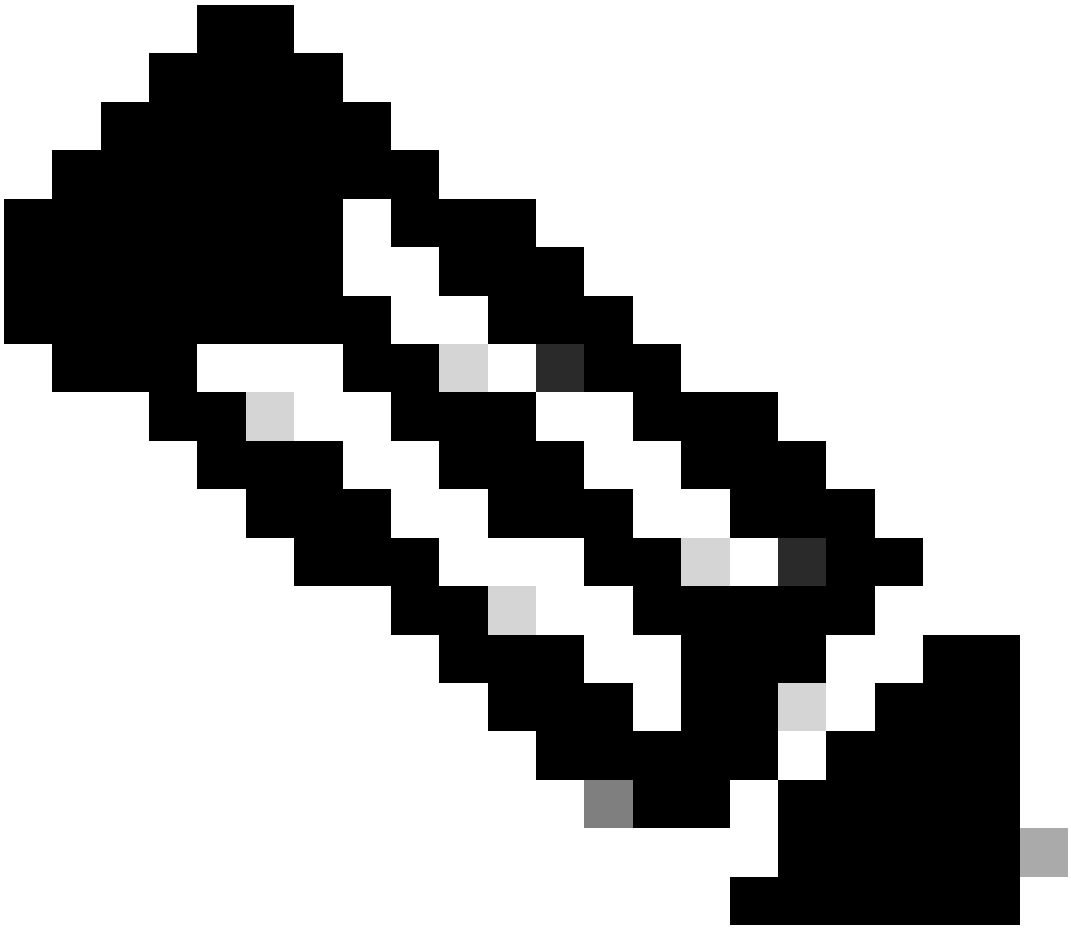
パーティション設定でWeb Server/LB URLを設定します

手順 17

Partition settingsの下で正しいWeb Server/LB URLが入力されていることを確認し、Appsタブを選択して、General Settings > External URL of the Applicationに移動します。



パーティション管理者用のSSOの構成



注：

- この手順はPCCEにのみ適用されます。
- これは、CCE管理WEBインターフェイスhttps:///cceadmin内でアクセスされるECEガジェット用です。

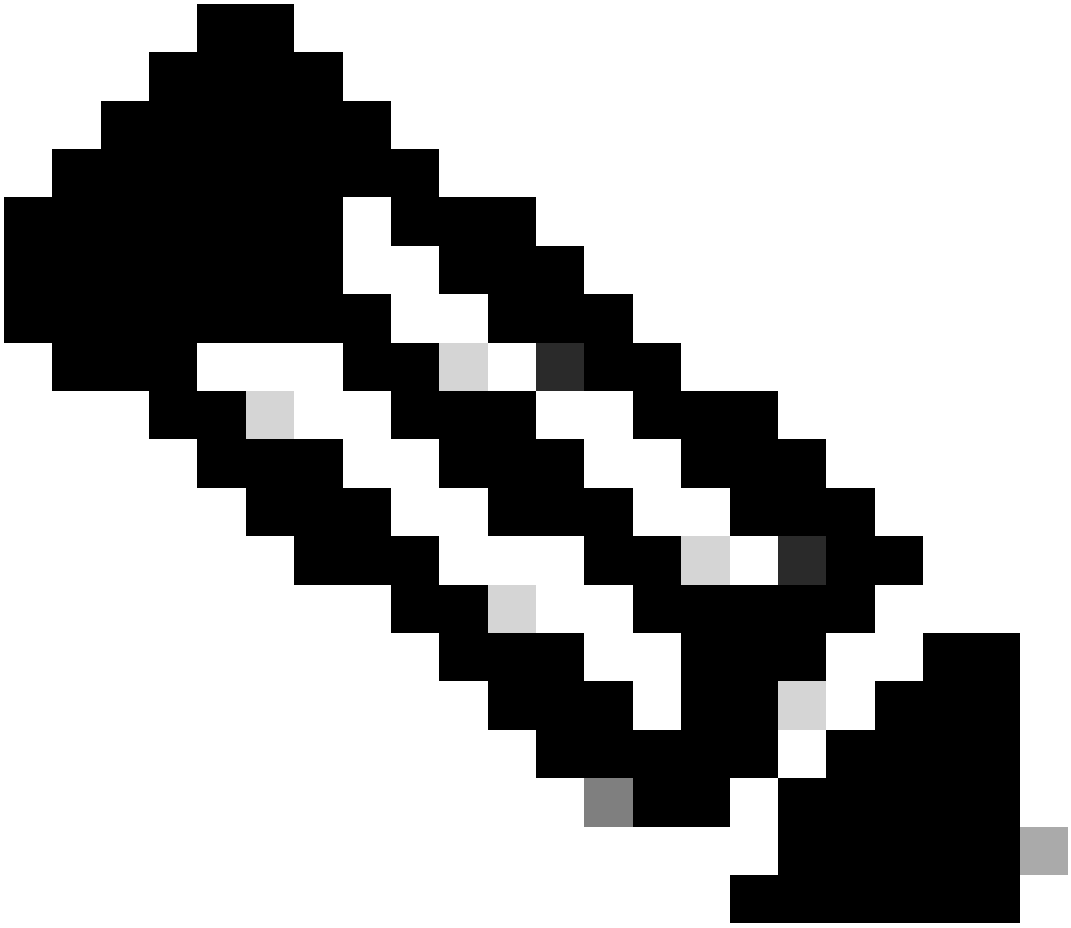
手順 18

Partition AdministratorのSSOを構成するには

1. ECE管理コンソールのパーティションレベルメニューで、Securityオプションをクリックし、左側のメニューからSingle Sign-On > Configurationsを選択します。
2. Select Configurationドロップダウンで、Partition Administratorsを選択し、設定の詳細を入力します。

LDAPのURL

- LDAPサーバのURL。
- これは、LDAPサーバのドメインコントローラURL(ldap://LDAP_server:389など)またはグローバルカタログURL(ldap://LDAP_server:3268など)です。
- ECEがLDAPルックアップを使用して設定されている場合、ECEがCCE管理コンソールを介してアクセスされると、パーティションをシステムに自動的に追加できます。
- ただし、1つのフォレスト内に複数のドメインがあるActive Directoryの展開や、代替UPNが構成されている場合は、標準LDAPポートが389および636のドメインコントローラURLを使用しないでください。
- LDAP統合は、グローバルカタログURLをポート3268および3269で使用するように設定できます。



注：グローバルカタログURLを使用することをお勧めします。 GCを使用しない場合、ApplicationServerログには次のようなエラーが記録されます。

- LDAP認証の例外<@>
  javax.naming.PartialResultException：未処理の継続参照。残りの名前 'DC=example,DC=com'

DN属性

- ユーザログイン名を含むDNの属性。
- たとえば、userPrincipalNameです。

ベース

- Baseに指定した値は、アプリケーションによって検索ベースとして使用されます。
- 検索ベースは、LDAPディレクトリツリーでの検索の開始位置です。
- たとえば、DC=mycompany、DC=comなどです。

LDAP検索用のDN

- LDAPシステムで匿名バインドが許可されていない場合は、LDAPディレクトリツリーで検索権限を持つユーザーの識別名(DN)を指定します。
- LDAPサーバで匿名バインドが許可されている場合は、このフィールドを空白のままにします。

Password

- LDAPシステムで匿名バインドが許可されていない場合は、LDAPディレクトリツリーで検索権限を持つユーザのパスワードを指定します。
- LDAPサーバで匿名バインドが許可されている場合は、このフィールドを空白のままにします。

手順 19

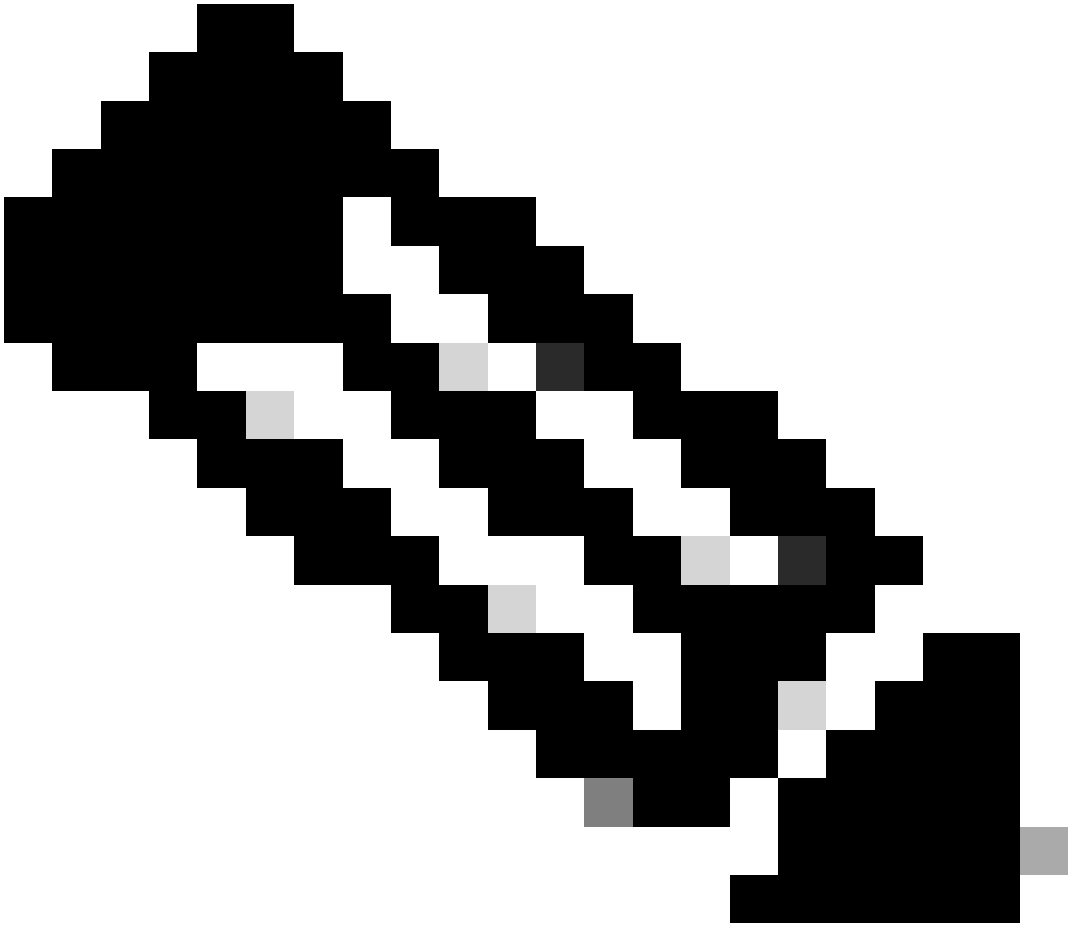
[Save] をクリックします。

これで、ECEのエージェントとパーティション管理者のシングルサインオン設定が完了しました。

トラブルシューティング

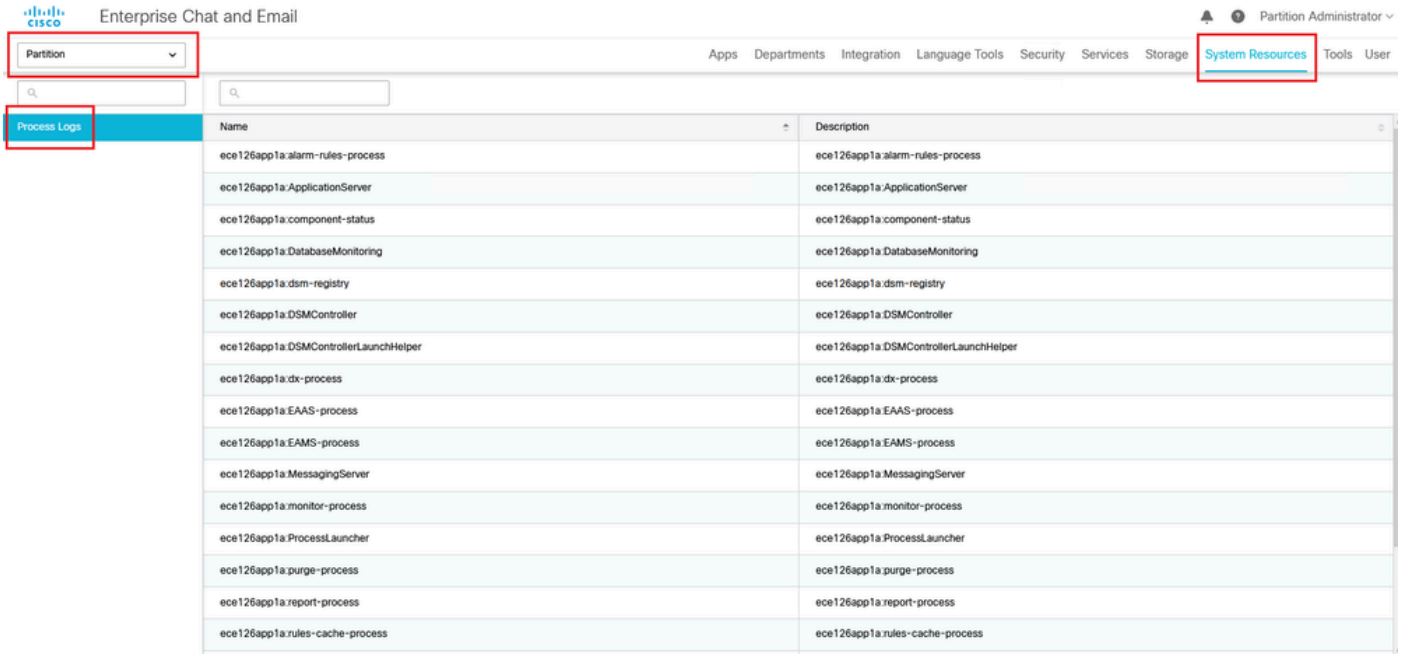
トレースレベルの設定

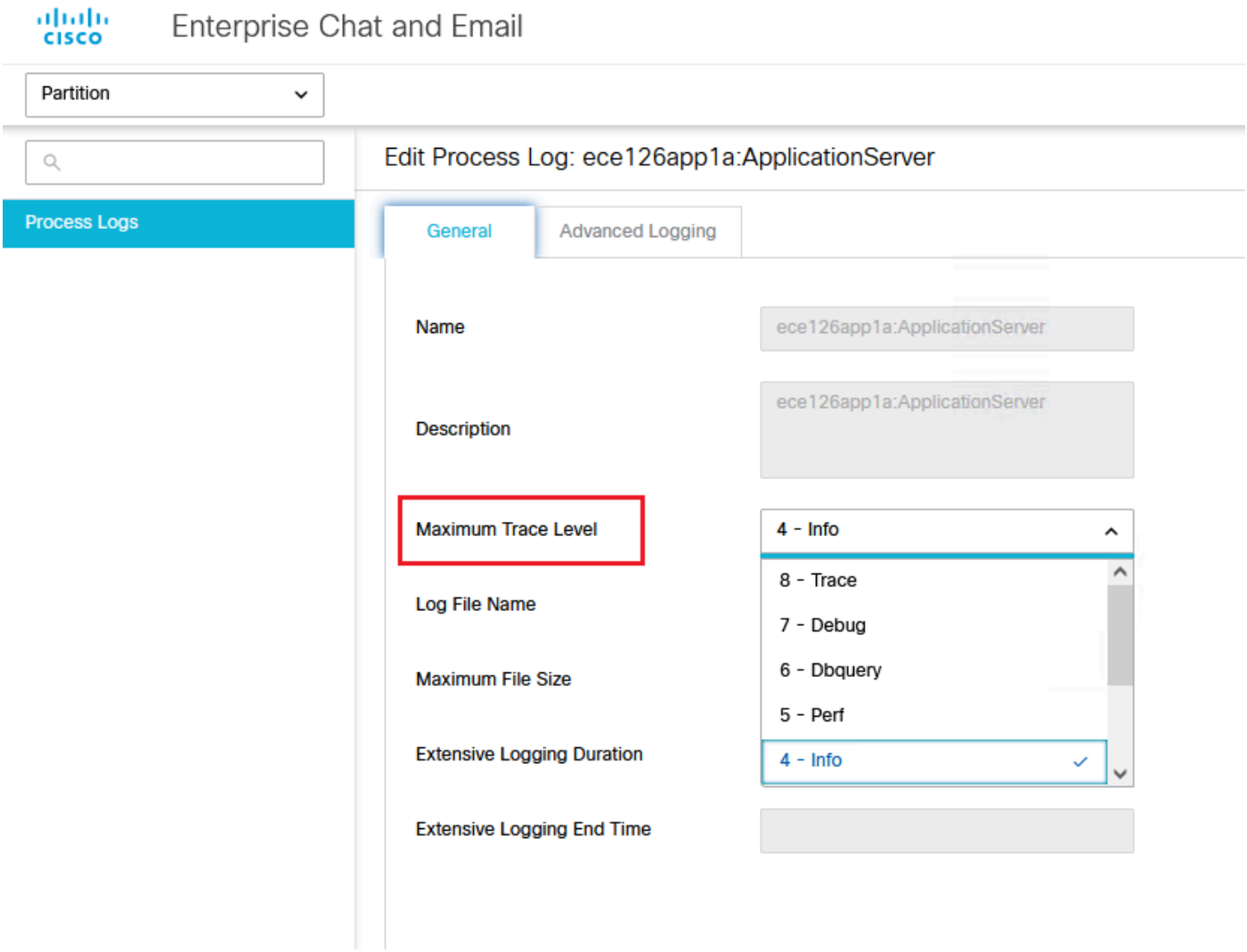
1. ECE管理コンソールのパーティションレベルメニューで、System Resourcesオプションをクリックし、左側のメニューからProcess Logsを選択します。
2. プロセスのリストからApplicationServerプロセスを選択し、「Maximum Trace Level」ドロップダウンメニューから目的のトレースレベルを設定します。



注：

- 初期セットアップまたは再設定中のSSOログインエラーのトラブルシューティングを行うには、ApplicationServerプロセストレースをレベル7に設定します。
- エラーが再現されたら、ログが上書きされないように、トレースレベルをデフォルトレベル4に戻します。





トラブルシューティングシナリオ1

エラー

- エラーコード： 500
- エラーの説明：アイデンティティプロバイダーのログインに失敗したため、アプリケーションは現時点でユーザーにログインできません。

ログ分析

- IdPログインに失敗しました – <samlp:Status><samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Responder" /></samlp:Status>
- ここで、「Responder」というステータスは、AD FS側で何らかの問題があることを示します。この場合、主にECE管理コンソール（SSO設定>サービスプロバイダー）にアップロードされた「Request Signing Certificate」と、「Signature」タブでECE証明書利用者信頼にアップロードされた証明書が原因です。
- これは、Javaキーストアファイルを使用して生成される証明書です。

アプリケーションサーバログ：トレースレベル7:

<#root>

unmarshallAndValidateResponse:

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

L10N_USER_STATUS_CODE_ERROR:

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

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

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

解決方法

- 「エージェントシングルサインオンの設定 – サービスプロバイダー」セクションの「証明書の署名の要求」設定を参照してください。
- ステップ11で生成したJava Keystore .jksファイルが、ECE管理コンソールのSSO

Configuration > Select Configuration 'Agent' > 'SSO Configuration' tab > Service Provider > Request Signing certificateの下の"Request Signing Certificate"フィールドにアップロードされていることを確認します。
- ECE証明書利用者信頼(ステップ12)の「Signature」タブで、.crtファイルがアップロードされていることを確認します。

トラブルシューティングシナリオ2

エラー

- エラーコード： 400
- エラーの説明： SAML応答トークンが無効です：署名の検証に失敗しました。

ログ分析

- このエラーは、ADFSの「トークン署名証明書」とECE SSO設定の「アイデンティティプロバイダー証明書」の証明書が一致していないことを示します。

アプリケーションサーバログ：トレースレベル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
```

解決方法

- ログスニペットに「Could not parse certificate: java.io.IOException: Incomplete data」というエラーが表示される場合は、「Identity Provider Certificate」の内容が正しく入力されていないことを示しています
- これを解決するには、AS FS Management > AD FS > Service > Certificates > Token-Signing >この証明書のエクスポート>テキストエディタで開く>すべての内容をコピー> SSO設定でファイルの「IDプロバイダー証明書」の下に貼り付ける> Saveを実行します。
- 「エージェントシングルサインオンの設定 – アイデンティティプロバイダー」セクション(ステップ15)で「アイデンティティプロバイダー証明書」の設定を参照してください。

トラブルシューティングシナリオ3

エラー

- エラーコード：401-114
- エラーの説明： SAML属性にユーザーIDが見つかりません。

ログ分析

アプリケーションサーバログ：トレースレベル7:

<#root>

getSSODataFromSAMLToken:

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

L10N_USER_IDENTIFIER_NOT_FOUND_IN_ATTRIBUTE:

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

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

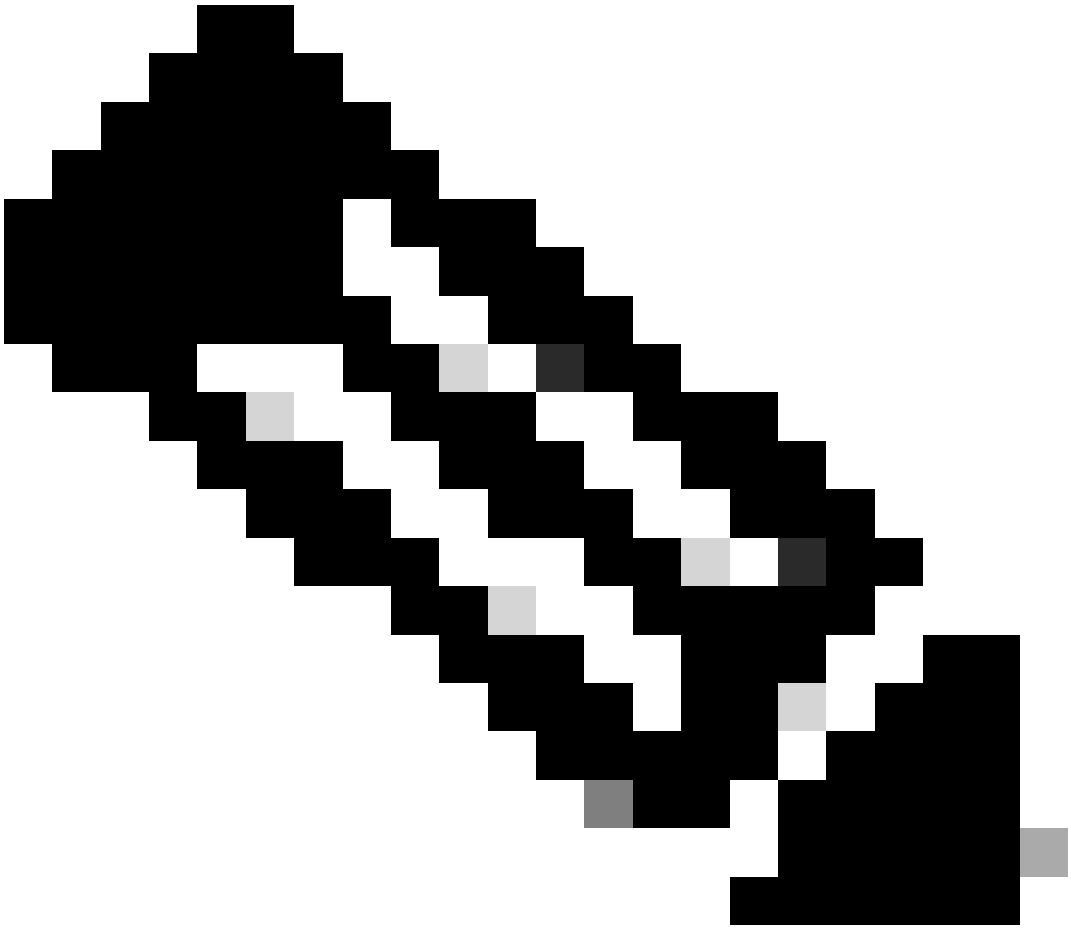
```
2024-02-01 01:44:32.083 GMT+0000 <@> DEBUG <@> [1220:qtp815320891-1220] <@> ProcessId:7716 <@> PID:1 <@
2024-02-01 01:44:32.083 GMT+0000 <@> TRACE <@> [1220:qtp815320891-1220] <@> ProcessId:7716 <@> PID:1 <@
```

解決方法

- このエラーは、「User Identity Location」フィールドと「User Identity Attribute Name」フィールドの設定の問題または不一致を示します。
- ECE管理コンソールの[Single Sign-On] > [Configurations]の下の[Select Configuration]ドロップダウンで、[Agent] > [SSO Configuration]タブ> [Identify Provider]を選択し、[User Identity Location]と[User Identity Attribute Name]を確認して修正します(ステップ15)。

関連情報

これらは、ECEのインストールまたは統合を開始する前に十分に確認する必要がある重要なドキュメントです。これはECEドキュメントの包括的なリストではありません。



注：

- ほとんどのECEドキュメントには2つのバージョンがあります。PCCE用のバージョンをダウンロードして使用してください。ドキュメントタイトルは、バージョン番号の後にPackaged Contact Center Enterpriseまたは（PCCEの場合）または（UCCEおよびPCCEの場合）のどちらかになります。
- インストール、アップグレード、または統合の前に、必ずCisco Enterprise Chatおよび電子メールのドキュメントのスタートページでアップデートを確認してください。
- https://www.cisco.com/c/en/us/support/customer-collaboration/cisco-enterprise-chat-email/series.html

ECEバージョン12.6(1)

- エンタープライズチャットおよび電子メール管理者ガイド

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。