SAML SSO Requirements for Identity Providers

Requirements for Identity Providers

This section provides an outline of the requirements that Identity Providers must meet in order to deploy SAML SSO services for Cisco Collaboration applications.

Identity Providers must adhere to the following guidelines:

- Support is for SAML 2.0 only.
- Supports Service-Provider initiated SSO only.
- Set the NameID Format attribute to *urn:oasis:names:tc:SAML:2.0:nameid-format:transient*
- Configure a claim on the IdP to include the *uid* attribute name with a value that is mapped to LDAP attributes (for example SAMAccountName).
- Cisco Unified Communications Manager uses ACS url index in the Authentication Request. The IdP must be able the index to the ACS url in the Service Provider metadata. This is compliant with SAML standards.
- It's not supported to have multiple certificates in the Signing and Encryption portion of the SAML Assertion. See CSCvq78479.

When configuring SAML SSO, make sure to deploy the following in your Cisco Collaboration Deployment:

- Network Time Protocol—Deploy NTP in your environment so that the times in your Cisco Collaboration Deployment and your Identity Provider are synced. Make sure that the time difference between the IdP and the Cisco Collaboration deployment does not exceed 3 seconds.
- DNS—Your Cisco Collaboration applications and your Identity Provider must be able to resolve each other’s addresses.
- LDAP—You must have an LDAP Directory sync configured in your Cisco Collaboration deployment. However, we recommend that you disable LDAP authentication.

- Certificates—You must exchange metadata files between your Cisco Collaboration deployment and the Identity Provider. The metadata contains the certificates that are required to create a trust relationship between your Collaboration deployment and the Identity Provider. You can use either a tomcat certificate or a system-generated self-signed certificate to establish trust.

SAML Agreement Types

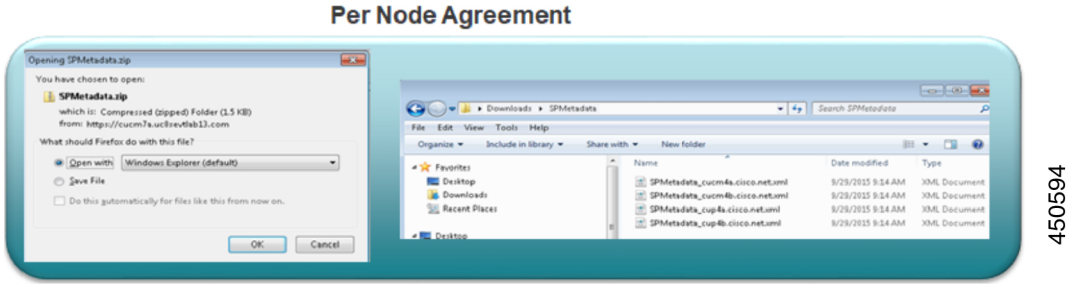
Cisco Unified Communications Manager supports two types of SAML metadata agreements:

- Cluster Wide—With this deployment, a single metadata agreement must be configured, which covers the entire cluster.
- Per Node—With this deployment, you must configure multiple metadata agreements, with a separate agreement for each cluster node. Each cluster node has a separate metadata exchange with the Identity Provider.

Figure 1: Two types of SAML metadata agreements in Cisco Unified Communications Manger

The following image illustrates the contents of a metadata zip file that was generated on Cisco Unified Communications Manager using a per node agreement. In this example, the IM and Presence Service is deployed using a Standard Deployment (non-centralized) so the zip file contains separate metadata xml files for each Unified Communications Manager and IM and Presence Service cluster node.

Figure 2: UC Metadata File Downloaded from Cisco Unified Communications Manger

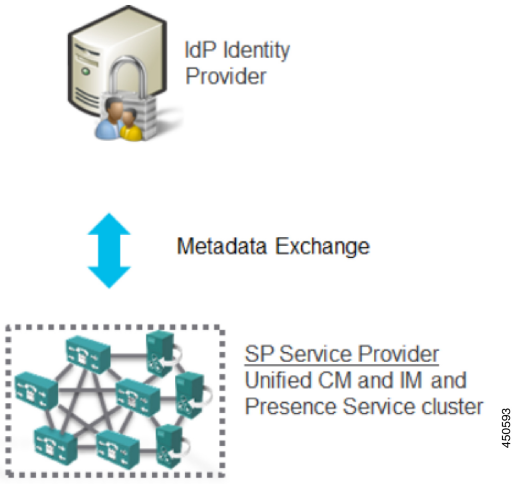


Note If you have a Centralized Deployment for the IM and Presence Service, your IM and Presence deployment is in a separate cluster from your telephony cluster. With Cluster Wide agreements, you must generate metadata separately for your telephony cluster, and for your IM and Presence cluster.

Metadata Exchange

As a part of the process for setting up SAML SSO, you must exchange metadata files between your UC deployment and the Identity Provider.

Figure 3: SAML Metadata Exchange



Following is an example of a UC metadata file that was generated from the Service Provider (Cisco Unified Communications Manager).

Metadata File from Service Provider (Cisco Unified Communications Manager)

```
<?xml version="1.0" encoding="UTF-8"?>
<!--With Single Cluster agreement the entityID is always the publisher FQDN-->
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
ID="cucm0a.identitylab20.ciscolabs.com" entity ID="cucm0a.identitylab20.ciscolabs.com">
     <!--We don't require AuthN or signed Assertions but comply to what the IdP requests-->

     <md:SPSSODescriptor AuthnRequestsSigned="false" WantAssertionsSigned="false"
protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
       <md:KeyDescriptor use="signing">
   <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
     <ds:X509Data>
       <ds:X509Certificate>MIIDzzCCA........</ds:X509Certificate>
     </ds:X509Data>
   </ds:KeyInfo>
  </md:KeyDescriptor>
   <!--Certificate for Signing and/or Encryption-->
  <md:KeyDescriptor use="encryption">
    <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
      <ds:X509Data>
        <ds:X509Certificate>MIIDzzCCA........</ds:X509Certificate>
      </ds:X509Data>
    </ds:KeyInfo>
  </md:KeyDescriptor>
   <!--We only support name-id format transient-->
  <md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:transient</md:NameIDFormat>
         <!--ACS URL for the Client to POST the answer from the IdP, two per node in the
cluster-->
```

```
   <md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://cucm0a.identitylab20.ciscolabs.com:8443/ssosp/saml/SSO/alias/cucm0a.identitylab20.ciscolabs.com"
 index="0"/>
               <md:AssertionConsumerService
Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
Location="https://cucm0a.identitylab20.ciscolabs.com:8443/ssosp/saml/SSO/alias/cucm0a.identitylab20.ciscolabs.com"
 index="1"/>
     </md:SPSSODescriptor>
</md:EntityDescriptor>
```

Following is an example of a metadata file that was generated from an Identity Provide (Active Directory Federation Service)

Metadata File from Identity Provider (Active Directory Federation Service)

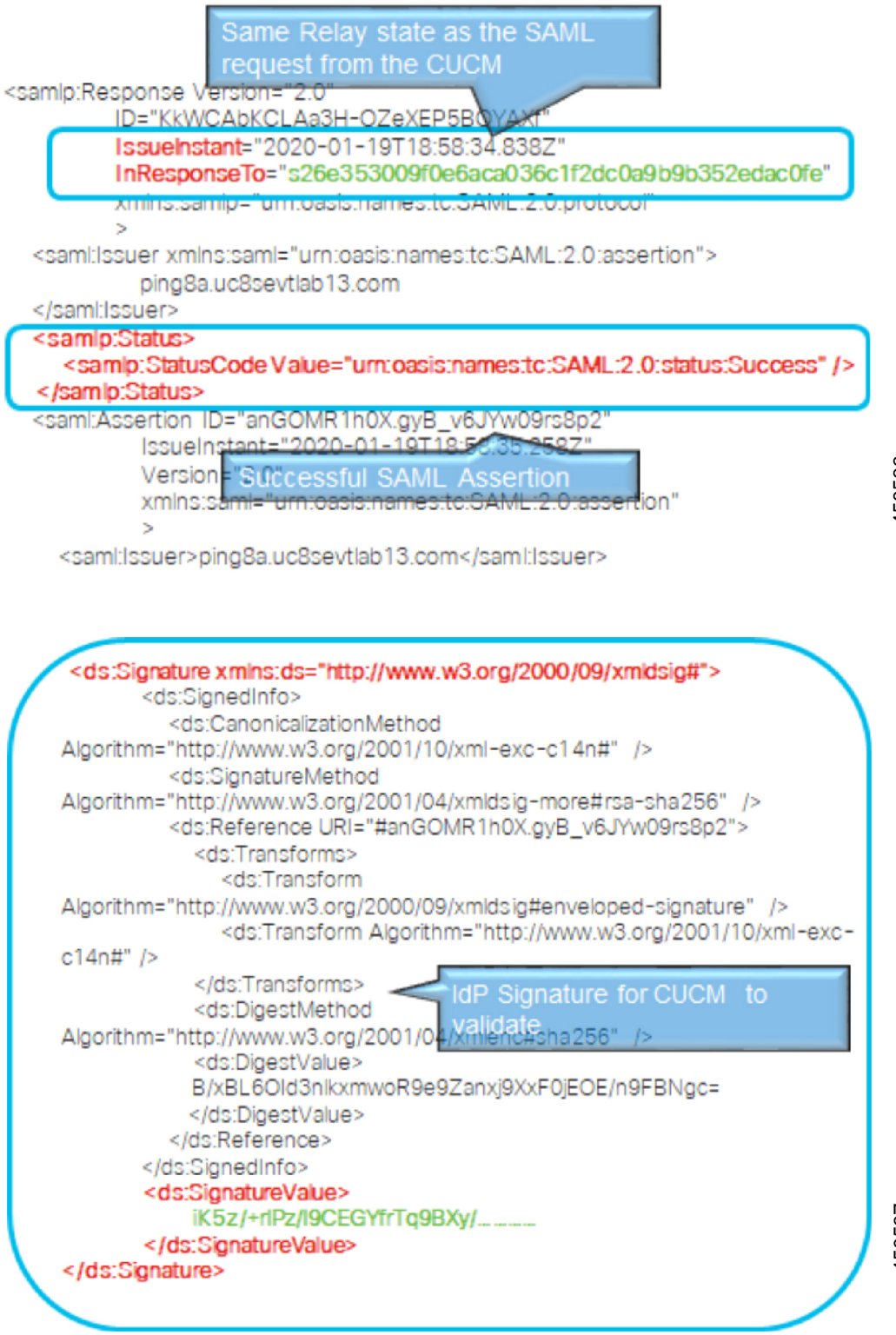
```
<?xml version="1.0"?
<!--entityID=IdP Entity ID-->
<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata"
ID="_b12fe1b5-6866-40cc-94be-9d9d8cb71916"
   entityID="http://WIN-2019SSO.cisco-dod.com/adfs/services/trust">
 <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
   <ds:SignedInfo>
     <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
       <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
    <ds:Reference URI="#_b12fe1b5-6866-40cc-94be-9d9d8cb71916">
                 <ds:Transforms>
                   <ds:Transform
Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
                   <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                 </ds:Transforms>
      <!--Sign the metadata provided to the SP for extra security-->
      <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
      <ds:DigestValue>VAcIv2uw6zG8YVVWP0IDYMZ/e7CN9o4oR8XBGiysujY=</ds:DigestValue>
    </ds:Reference>
   </ds:SignedInfo>
   <ds:SignatureValue>44RAgZ17YfwLdcRodZPcZ5PH05sLVbkDx4uAYq+EC4K+ZhiTs8aUZQ/.........
   </ds:SignatureValue>
   <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
  <X509Data>
   <IDPSSODescriptor
protocolSupportEnumeration="http://docs.oasis-open.org/ws-sx/ws-trust/200512
http://schemas.xmlsoap.org/ws/2005/02/trust
http://docs.oasis-open.org/wsfed/federation/200706"
ServiceDisplayName="administrator.cisco-dod.com">
 <KeyDescriptor use="encryption">
   <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
     <X509Data>
  <X509Certificate>MIIGHzCCBQegAwIBAgITHAAADUerWbVHyqoM.........
  </X509Certificate>
     </X509Data>
   </KeyInfo>
 </KeyDescriptor>
 <KeyDescriptor use="signing">
   <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
     <X509Data>
         <!--Cert for signing and/or encrypting the SAML Assertion-->
  <X509Certificate>MIIC7jCCAdagAwIBAgIQJH7di/.........</ds:X509Certificate>
    </KeyInfo>
 </KeyDescriptor>
   <!--Single Sign On Service details for HTTP-Redirect and HTTP-POST-->
   <SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
Location="https://win-2019sso.cisco-dod.com/adfs/ls/"/
   <SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
```

```
Location="https://win-2019sso.cisco-dod.com/adfs/ls/"/>
   <!--NameID format offer for this agreement-->
   <NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</NameIDFormat>
   <NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:persistent</NameIDFormat>
   <NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:transient</NameIDFormat>
   <AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://win-2019sso.cisco-dod.com/adfs/ls/" index="0" isDefault="true"/>
   <AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Artifact"
Location="https://win-2019sso.cisco-dod.com/adfs/ls/" index="1"/>
   <AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
Location="https://win-2019sso.cisco-dod.com/adfs/ls/" index="2"/>
   </IDPSSODescriptor>
</EntityDescriptor>
```

SAML Assertions

Following is an example of the SAML Assertion that is sent from the Identity Provider to Cisco Unified Communications Manager:

Figure 4: SAML Assertion Example



SAML OAuth Authentication Flow

Following is an example of the authentication flow for an OAuth authentication request with the Identity Provider.

Figure 5: OAuth Authentication Flow