Cisco Collaboration Identity Foundation SSO Lab - Microsoft™ AD FS 2.0 v1

Last Updated: 09-JUL-2015

About This Solution

Single Sign-On (SSO) technology is critical to any organization looking to increase security through its IT infrastructure. SSO allows employees to access most or all of their internal company resources using one standard login. This corporate login can be used for any internal company web page with its authentication challenge pointing back to a centralized web server. There are many solutions in the market today, with Microsoft Active Directory Federation Services (AD FS), PingFederate by Ping, and ForgeRock OpenAM being the most popular. Implementing SSO in your organization gives you the following benefits:

- Reduces phishing success and time spent re-entering passwords for the same identity
- Supports conventional authentication such as Windows credentials (i.e., username/password)
- Reduces IT costs due to lower number of Technology Help Desk calls about passwords
- Provides security on all levels of entry/exit/access to systems without the inconvenience of re-prompting users
- Enables centralized reporting for compliance adherence.

In this lab, you will learn the essentials of Microsoft AD FS 2.0 and how you can enable SSO in an enterprise environment. For more information on AD FS, please see the Microsoft TechNet Product Overview page.

About This Lab

This **Identity Foundation Training** lab includes:

- SAML Technology overview
- Setting up and configuring Microsoft AD FS 2.0 for SSO
    - Username and password authentication
- Configuring Cisco Unified CM, IM & Presence, and Unity Connection for SSO
- Kerberos based authentication with Microsoft AD FS
- Certificates based authentication with AD FS

Lab Requirements

The table below outlines the requirements for this preconfigured demonstration.

Table 1. Demonstration Requirements

Required	Optional
• Laptop • Cisco AnyConnect	• None

Lab Configuration

This demonstration contains preconfigured users and components to illustrate the scripted scenarios and features of this solution. All information needed to access the demonstration components, is located in the **Topology** and **Servers** menus of your active demonstration.

- **Topology Menu**. Click on any server in the topology and a popup window will appear with available server options.
- **Servers Menu**. Click on ⊞ or ▶ next to any server name to display the available server options and credentials.

Table 2. Demonstration User Information

User Name	User ID	Password
Anita Perez	aperez	C1sco12345

Lab Topology

This demonstration includes several server virtual machines. Most of the servers are fully configurable using the administrative level account. Administrative account details are included in the script steps where relevant and in the server details table.

Figure 1. Lab Topology Overview

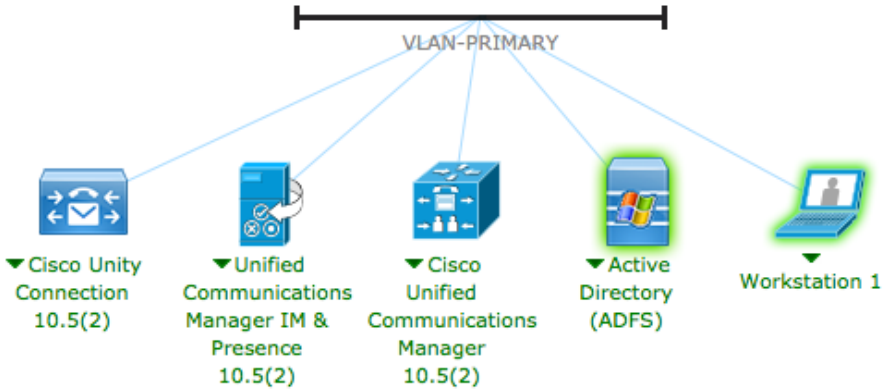


Table 3. Server Information

Name	Description	Host Name (FQDN)	IP Address	Username	Password
Unified CM	Cisco Unified Communications Manager v10.5(2)	cucm1.dcloud.cisco.com	198.18.133.3	administrator	dCloud123!
IM & P	Cisco IM & Presence Server v10.5(2)	cup1.dcloud.cisco.com	198.18.133.4	administrator	dCloud123!
Unity Connection	Cisco Unity Connection Server v10.5(2)	cuc1.dcloud.cisco.com	198.18.133.5	administrator	dCloud123!
Active Directory	Microsoft Active Directory Server 2008, ADFS v2	ad1.dcloud.cisco.com	198.18.133.1	administrator	C1sco12345
Workstation 1	Windows 7	wkst1.dcloud.cisco.com	198.18.133.36	aperez	C1sco12345

Lab Preparation

BEFORE DEMONSTRATING

We strongly recommend that you go through this process at least once, before presenting in front of a live audience. This will allow you to become familiar with the structure of the document and the demonstration.

PREPARATION IS KEY TO A SUCCESSFUL CUSTOMER PRESENTATION.

Follow the steps below to schedule your demonstration and configure your demonstration environment.

1. Browse to dcloud.cisco.com, choose the location closest to you, and then login with your **Cisco.com credentials**.
2. Schedule a demonstration. [Show Me How]
3. Test your bandwidth from the demonstration location before performing any demonstration scenario. [Show Me How]
4. Verify your demonstration is **Active** under **My Demonstrations** on the **My Dashboard** page in the Cisco dCloud UI.
   - It may take up to **45 minutes for your demonstration to become active**.
5. If you are not connected to the lab from behind a router, on your laptop, use **Cisco AnyConnect** paired with the session credentials from the UI to connect to the lab. [Show Me How]
6. From your laptop, access the demonstration workstation named **wkst1** located at **198.18.133.36** and login using the following credentials: Username: **dcloud\aperez**, Password: **C1sco12345**.
   - **Recommended method**: Use **Cisco AnyConnect** [Show Me How] and the **local RDP client on your laptop**. [Show Me How]
7. From your laptop, access the demonstration workstation named **ad1** located at **198.18.133.1** and login using the following credentials: Username: **dcloud\administrator**, Password: **C1sco12345**.
   - **Recommended method**: Use **Cisco AnyConnect** [Show Me How] and the **local RDP client on your laptop**. [Show Me How]

NOTE: If you run into any problems with the lab, we recommend you look in Appendix B – Troubleshooting. This appendix gives solutions to common error messages you will find in this lab.

Scenario 1: Understanding SAML

This section was extracted from the UC10.5 SRND to give you a brief explanation on SAML so that you understand what you are doing in the configuration.

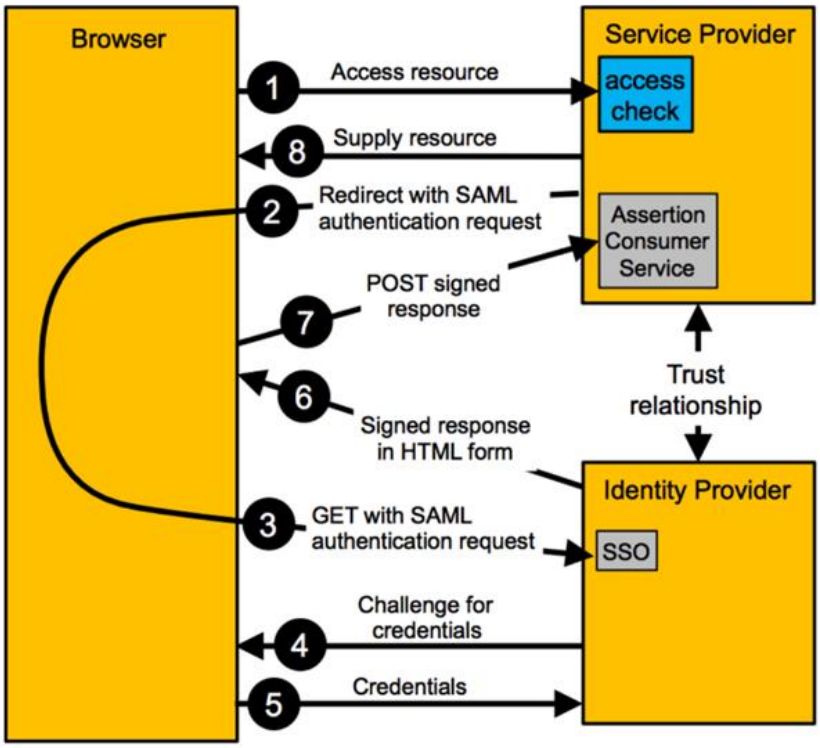
It is very important that you read this section. Before starting configuring SSO features.

The more typical web SSO flow used with Cisco Collaboration Services is Service Provider (SP) initiated web SSO. In that case, the user directly (without visiting an Identity Provider (IdP) first) tries to access a protected resource on an SP. The SP then sends the user to the IDP to get authenticated and then finally the user presents the authentication assertion received from the IDP to the SP to get access.

The SAML web browser SSO profile provides a variety of options depending on whether the authentication is IdP or SP initiated and on how the messages are exchanged between IdP and SP. As mentioned above Cisco Collaboration services only use SP initiated SSO where the SP when a user tries to access a protected resource first send the user to an IdP to authenticate. The IdP then builds an authentication assertion and sends the user back to the SP with that assertion.

The binding used for the messages exchange between IdP and SP for Cisco Collaboration services is the Redirect/POST binding. Here an HTTP 302 redirect is used to send the SAML authentication request message from the SP to the IDP and the authentication response from IdP to SP is sent using an HTTP POST message.

Figure 2. SP-Initiated SSO (Redirect/POST binding)



General steps of a SAML based authentication flow

1. The user tries to access a service or resource by pointing the browser to the URL hosted on the application server. The browser at this moment does not have an active session with the service.

2. The SP realizes that the request originates from a client without an active session. Based on the SSO configuration the SP now generates a SAML authentication request to be sent to the appropriate the IdP defined as part of SSO configuration. The SAML request contains information about the SP generating the request. This is required so that the IdP can identify the SPs sending SAML requests.
3. The SP does not communicate directly with the IdP to authenticate the user. Instead, the SP redirects the browser to the IdP. The URL used for this redirect is taken from the IdP metadata exchanged earlier. The SAML request to be sent to the IDP is included in the redirect as a URL query parameter using Base64 encoding.

This redirecting HTTP 302 may look like the following example:

- HTTP/1.1 302 Found
- Location: https://pingsso.home.org:9031/idp/SSO.saml2?SAMLRequest=nZLNbtswEITveQqCd1m0pKoWYRlwYxQ1kDZK5OaQG02tYwISqXLJtH37kkra%2FBjwodflcPab3V2iGPqRr7076lv44QEdIb%2BGXiOfXmrqreZGoEKuxQDIneTt%2BusVz2aMj9Y4I01PL7abmmJWVCxnku07sYCqFAu2KGWVdaycV1AWRbnPPjJZlDkld2BRGV3TYEPJFtHDVqMT2oUSm%2BcJq5Ks2LGK5x84K%2B8p2QQ0pYWbfh2dG5Gn6aj0A6KZHc0AM2MfeACYp6ob07a9nsUEGSWfjZUwJazpQfQIsWEjENUj%2FKs0z1E%2BKd0F0%2FO5908i5F92uyZprtsdJWtEsJHu0mj0A9gW7KOS8P326oVXejkk4F94F0WRpyEBjmmkjdip6JXAEyldXSyjhE%2FDsq%2BWdJ5V%2FOWiq%2FeWy%2FSV4bP9yL8Fi%2B2mMb2Sv%2F%2FnFuK8B%2BHOq2NFdclhknJnhUYF2lHSNrH%2FjQ9DOCiwNT2ZA1n3vfl5aUG4sD5nPdDVU5K37CFQenrdqz8%3D&RelayState=s249030c0bda8e96a8086c92d0619e6446b270c463

The encoded SAML authentication request shown above can be decoded as:

```
<samlp:AuthnRequest xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"

       ID="s249030c0bda8e96a8086c92d0619e6446b270c463"

       Version="2.0"

       IssueInstant="2013-09-19T09:35:06Z"

       Destination="https://pingsso.home.org:9031/idp/SSO.saml2"

       ForceAuthn="false"

       IsPassive="false"

       ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"

AssertionConsumerServiceURL="https://cucm-eu.home.org:8443/ssosp/saml/SSO/alias/cucm-
eu.home.org">

  <saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">cucm-eu.home.org</saml:Issuer>

  <samlp:NameIDPolicy xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"

Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient"

       SPNameQualifier="cucm-eu.home.org"

       AllowCreate="true"

       />

</samlp:AuthnRequest>
```

4. The browser receives the redirect, follows the URL and issues the corresponding GET to the IdP. The SAML request is maintained. The browser at this stage does not have an active session with the IdP

5. After receiving the new request from a browser with no active session, the IdP authenticates the user based on the pre-configured authentication mechanisms. Possible authentication mechanisms include user/password, PKI/CAC or Kerberos. For user/password authentication, the IdP might push a form to the user to enter the credentials (e.g. 200 OK with IdP login form). For the actual authentication, the IdP might depend on backend systems like for example an LDAP server for user/password authentication.
   One key point here is that the exchange of credentials for the purpose of authentication takes place between the IdP and the browser. The SP is not involved and does not see the credentials.

6. The browser provides further information required for the authentication process. For the user/password case, this would be a POST with the information. For other authentication mechanisms, other details would need to be sent to the IdP by the browser.

7. The IdP now checks and validates the provided credentials. The check could involve interactions with respective backend systems (LDAP bind for user/password based authentication against LDAP, communication with Kerberos server to validate ticket etc.).

8. Finally, the IdP generates a SAML response for the SP. This response contains the SAML assertion documenting the result of the authentication process. The SAML assertion in addition to the basic ***"Yes/No"*** information also contains validity information and information about attributes describing the authenticated entity. At least the user id of the authenticated entity has to be included in the well-known attribute "**uid**" so that the SP can extract this information from the assertion to relate the authenticated entity to users existing in the local database.
   The SAML assertion is signed by the IdP according to the SSO key information published in the IdP metadata. This makes sure that the SP can verify the authenticity of the SAML assertion.
   The IdP returns the SAML assertion to the browser in a hidden form in a 200 OK message. The hidden form instructs the browser to POST the SAML assertion to the Assertion Consumer Service (ACS) of the SP.
   The IdP also sets a ***session cookie*** on the browser which is cached by the browser. If the browser needs to get subsequent SAML assertions, it will send the session cookie together with the SAML requests. The IdP will then realize that it already has a valid session with the browser and assert the authentication of the previously authenticated user without prompting for credentials again. This enables SSO against multiple SPs. Session expiry times for these session cookies are configured on the IdP.

9. The browser follows the hidden POST received in the 200 OK and POSTs the SAML assertion to the Assertion Consumer Service on the SP.

10. The SP extracts the SAML assertion from the POST and validates the signature of the assertion. This guarantees the authenticity of the SAML assertion and the IdP. The user identifier received in the SAML assertion in attribute "**uid**" is then used to decide whether the user is authorized to access the requested service. This is based on local access control configuration on the SP.

11. The SP grants access to the requested resource and sends back the content in a 200 OK to the browser. The SP also sets a session cookie in the browser so that for subsequent access requests from the same browser to the same SP the SP does not need to initiate an exchange with the IdP anymore. The IdP will only be involved for requests from the same browser after the SP session cookie will have been expired.

This concludes this lab activity.

Scenario 2: Setting up Microsoft™ AD FS 2.0

This section will describe the steps to configure SSO using Microsoft™ Active Directory Federation Services® as Identity Provider (IdP).

NOTE: Due to time management, some parts of this lab are already pre-configured such as **Installing Microsoft™ AD FS2.0** and **Basic AD FS 2.0 setup wizard (both explained in Appendix C).**
By default, AD FS2.0 has Username/Password Authentication enabled, so no extra steps are needed to prepare AD FS2.0 to enable this Authentication method. For other authentication methods, AD FS2.0 needs customization to be part of the lab steps.

Username/Password based Authentication with AD FS 2.0

RDP to AD 1 (198.18.133.1) and login with **dcloud\administrator** / **C1sco12345**

Setting up Unified CM Voice & Video for SSO

NOTE: The LDAP configuration for Unified CM has already done due to interest of time. If you would like to see the steps for this, you can see them in Appendix A.

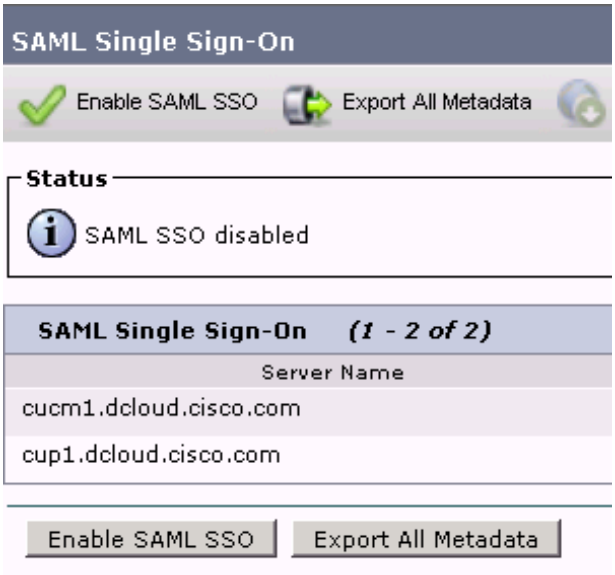
Setting up AD FS 2.0 for Unified CM Voice & Video

NOTE: You already configured the Username/Password authentication mechanism in ADFS2 , now you need to configure the SSO connection on Unified CM.

First task is to to get the Unified CM metadata for the SAML Assertion with the IdP.

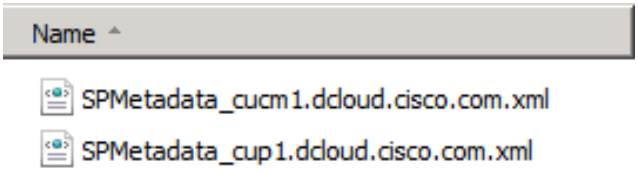
1. Within the AD1 RDP session, open Internet Explorer and navigate to **Collaboration Server Links** > **Cisco Unified Communications Manager**. Then click on the **Cisco Unified Commucations Manager** link.
2. Login with **administrator** / **dCloud123!**
3. Navigate to to **System** > **SAML Single Sign-On**.
4. Click on **Export All Metadata**.

Figure 3. Export All Metadata



5. After a few seconds click the **Save** button on the bottom of the page to save to the AD1 Desktop.
6. Minimize Internet Explorer, right click the **SPMetadata.zip** file, choose **Extract All** and then click **Extract**.
7. Check that you have the following two files in the new **SPMetadata** folder on your Desktop:

Figure 4. Directory Contents



8. If you look inside the xml files you will see what will be sent to the IdP and requested in the contract agreement. This starts the SAML negotiation between the Service Provider (SP) and the IdP. Each file contains one agreement for each SP (since Unified CM exports automaticaly Unified CM and IM&P Metadata you have two files). What is specified in each file, sets the “ground rule” for the autorization process. See the following figure for more information.

Figure 5. XML File Contents

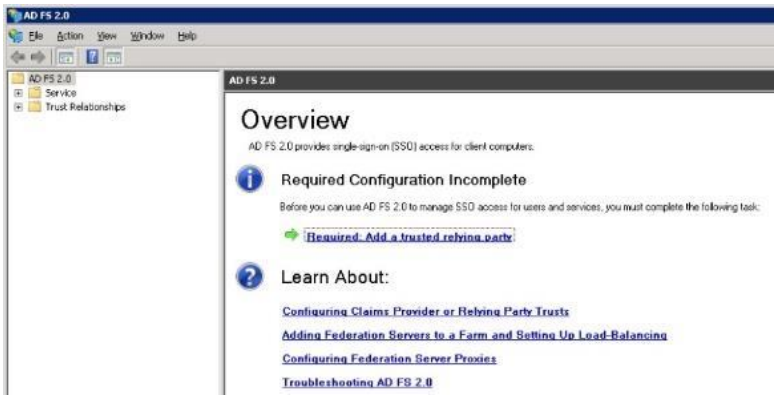

```
<?xml version="1.0" encoding="UTF-8"?>
- <md:EntityDescriptor entityID="cucm1.dcloud.cisco.com" ID="cucm1.dcloud.cisco.com" xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata">
  - <md:SPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol" WantAssertionsSigned="false" AuthnRequestsSigned="false">
    - <md:KeyDescriptor use="signing">
      - <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        - <ds:X509Data>
            <ds:X509Certificate>MIIF1TCCBL2gAwIBAgIKHrvFUgAAAAAAFDANBgkqhkiG9w0BAQUFADBcMRMwEQYKCZImiZPyLGQB GRYDY29tMRUwEwYKCZImiZPyLGQBGRYFY2lzY28xFjAUBgoJkiaJk/IsZAEZFgZkY2xvdWQxFjAU
            BgNVBAMTDWRjbG91ZC1BRDEtQ0EwHhcNMTUwNDI3MTQwNTU2WhcNMTcwNDI2MTQwNTU2WjB/MQsw CQYDVQQGEwJVUzEOMAwGA1UECBMFVGV4YXMxEzARBgNVBAcTClJpY2hhcmRzb24xFjAUBgNVBAoT
            DUNpc2NvIFN5c3RlbXMxDzANBgNVBAsTBmRDbG91ZDEiMCAGA1UEAxMZY3VjbTEuZGNsb3VkLmNp c2NvLmNvbS1tczCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAK1z5z1cQtwzg149nc6z
            Pf2W/B7rD/oEGZPLI0p8Bo66cUqVIGI+Fwb1L52sikX4Bl5fQizvGK/vrqjWj0Jv54mVt/2m7E20 ty3WHTsR+F48OHXEIwZGQFycfRDSt6Z3KrgRnC0Wp2gmouQ9OH5DSz9lBDuzyTp84u50l1TJiLC
            nu1ch5gcnDcfXq/u92k7uqFceOaP+2WthgDL3s7+Dgf/Q0De1bM5Lcoe6VmScMtGoVRiYaQTeN8f vQ87pDHMbC8AKhPhprtCmzWgYZIuvC3yaMzUswfAjNwYNAQD+MKJ5r0LU0BV06X3KM6/nPYVuat
            xAlUWb2FgVizJU5fLgcCAwEAAaOCAnQwggJwMBMGA1UdJQQMMAoGCCsGAQUFBwMBMA4GA1UdDwEB /wQEAwIFoDBKBgNVHREEQzBBghZjdWNtMS5kY2xvdWQuY2lzY28uY29tghBkY2xvdWQuY2lzY28u
            Y29tghVjdXAxLmRjbG91ZC5jaXNjby5jb20wHQYDVR0OBBYEFDdADw7DBcgPtC1KPtBFdAw40L8b MB8GA1UdIwQYMBaAFBEmr1qmbMgWk1CkzOyBy/qv0pb4MIHPBgNVHR8EgccwgcQwgcGggb6ggbuG
            gbhsZGFwOi8vLONOPWRjbG91ZC1BRDEtQ0EsQ049YWQxLENOPUNEUCxDTj1QdWJsaWMlMjBLZXkl MjBTZXJ2aWNlcyxDTj1TZXJ2aWNlcyxDTj1Db25maWd1cmF0aW9uLERDPWRjbG91ZCxEQz1jaXNj
            byxEQz1jb20/Y2VydGlmaWNhdGVSZXZvY2F0aW9uTGlzdD9iYXNlP29iamVjdENsYXNzPWNSTERp c3RyaWJ1dGlvblBvaW50MIHHBggrBgEFBQcBAQSBujCBtzCBtAYIKwYBBQUHMAKGgadsZGFwOi8v
            L0NOPWRjbG91ZC1BRDEtQ0EsQ049QUlBLENOPVB1YmxpYyUyMEtleSUyMFNlcnZpY2VzLENOPVNl cnZpY2VzLENOPUNvbmZpZ3VyYXRpb24sREM9ZGNsb3VkLERDPWNpc2NvLERDPWNvbT9jQUNlcnRp
            ZmljYXRlP2Jhc2U/b2JqZWN0Q2xhc3M9Y2VydGlmaWNhdGlvbkF1dGhvcml0eTAhBgkrBgEEAYI3 FAIEFB4SAFcAZQBiAFMAZQByAHYAZQByMA0GCSqGSIb3DQEBBQUAA4IBAQBt1KHBfpaqQ1C3w+Wv
            GzHQrS6wZIWTNc5vybf9GeCGLjYj45DxGLLyQBbGB3umHaAPdPDf8p/pwT3eP9xAruJcc2CoArma JCgo35ti/gCxzIVoSCESBT/1X9Ku6uzdIf7FCg+aPFeRhjpcgOCJUXv8DWAysGdNoSrzo1WJjDvz
            HI5IKfidRFoxJBdZ6KuXZTkDjsGBQJYGK/7CMDC8ioc0Gv9z1iZ7p/OnLaAit2y3ctdkT55wzLZ9 v3GBV8RMHpxgDH3kAZ1M6cZXg32OAu2rKW41UORiogxuaQBeyqdgbGxOd83sop6fmg1U11C7IVZR
            aKTM3RZc02sdydRlHnJX</ds:X509Certificate>
        </ds:X509Data>
      </ds:KeyInfo>
    </md:KeyDescriptor>
  - <md:KeyDescriptor use="encryption">
    - <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
      - <ds:X509Data>
          <ds:X509Certificate>MIIF1TCCBL2gAwIBAgIKHrvFUgAAAAAAFDANBgkqhkiG9w0BAQUFADBcMRMwEQYKCZImiZPyLGQB GRYDY29tMRUwEwYKCZImiZPyLGQBGRYFY2lzY28xFjAUBgoJkiaJk/IsZAEZFgZkY2xvdWQxFjAU
            BgNVBAMTDWRjbG91ZC1BRDEtQ0EwHhcNMTUwNDI3MTQwNTU2WhcNMTcwNDI2MTQwNTU2WjB/MQsw CQYDVQQGEwJVUzEOMAwGA1UECBMFVGV4YXMxEzARBgNVBAcTClJpY2hhcmRzb24xFjAUBgNVBAoT
            DUNpc2NvIFN5c3RlbXMxDzANBgNVBAsTBmRDbG91ZDEiMCAGA1UEAxMZY3VjbTEuZGNsb3VkLmNp c2NvLmNvbS1tczCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAK1z5z1cQtwzg149nc6z
            Pf2W/B7rD/oEGZPLI0p8Bo66cUqVIGI+Fwb1L52sikX4Bl5fQizvGK/vrqjWj0Jv54mVt/2m7E20 ty3WHTsR+F48OHXEIwZGQFycfRDSt6Z3KrgRnC0Wp2gmouQ9OH5DSz9lBDuzyTp84u50l1TJiLC
            nu1ch5gcnDcfXq/u92k7uqFceOaP+2WthgDL3s7+Dgf/Q0De1bM5Lcoe6VmScMtGoVRiYaQTeN8f vQ87pDHMbC8AKhPhprtCmzWgYZIuvC3yaMzUswfAjNwYNAQD+MKJ5r0LU0BV06X3KM6/nPYVuat
            xAlUWb2FgVizJU5fLgcCAwEAAaOCAnQwggJwMBMGA1UdJQQMMAoGCCsGAQUFBwMBMA4GA1UdDwEB /wQEAwIFoDBKBgNVHREEQzBBghZjdWNtMS5kY2xvdWQuY2lzY28uY29tghBkY2xvdWQuY2lzY28u
            Y29tghVjdXAxLmRjbG91ZC5jaXNjby5jb20wHQYDVR0OBBYEFDdADw7DBcgPtC1KPtBFdAw40L8b MB8GA1UdIwQYMBaAFBEmr1qmbMgWk1CkzOyBy/qv0pb4MIHPBgNVHR8EgccwgcQwgcGggb6ggbuG
            gbhsZGFwOi8vLONOPWRjbG91ZC1BRDEtQ0EsQ049QUlBLENOPVB1YmxpYyUyMEtleSUyMFNlcnZpY2VzLENOPVNl cnZpY2VzLENOPUNvbmZpZ3VyYXRpb24sREM9ZGNsb3VkLERDPWNpc2NvLERDPWNvbT9jQUNlcnRp
            ZmljYXRlP2Jhc2U/b2JqZWN0Q2xhc3M9Y2VydGlmaWNhdGlvbkF1dGhvcml0eTAhBgkrBgEEAYI3 FAIEFB4SAFcAZQBiAFMAZQByAHYAZQByMA0GCSqGSIb3DQEBBQUAA4IBAQBt1KHBfpaqQ1C3w+Wv
            GzHQrS6wZIWTNc5vybf9GeCGLjYj45DxGLLyQBbGB3umHaAPdPDf8p/pwT3eP9xAruJcc2CoArma JCgo35ti/gCxzIVoSCESBT/1X9Ku6uzdIf7FCg+aPFeRhjpcgOCJUXv8DWAysGdNoSrzo1WJjDvz
            HI5IKfidRFoxJBdZ6KuXZTkDjsGBQJYGK/7CMDC8ioc0Gv9z1iZ7p/OnLaAit2y3ctdkT55wzLZ9 v3GBV8RMHpxgDH3kAZ1M6cZXg32OAu2rKW41UORiogxuaQBeyqdgbGxOd83sop6fmg1U11C7IVZR
            aKTM3RZc02sdydRlHnJX</ds:X509Certificate>
        </ds:X509Data>
      </ds:KeyInfo>
    </md:KeyDescriptor>
    <md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:transient</md:NameIDFormat>
    <md:AssertionConsumerService index="0" Location="https://cucm1.dcloud.cisco.com:8443/ssosp/saml/SSO/alias/cucm1.dcloud.cisco.com" Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"/>
  </md:SPSSODescriptor>
</md:EntityDescriptor>
```


9. For further details on the SAML stardard please refer to the OASIS Standard - https://www.oasis-open.org/committees/security

10. Open the Active Directory Federation Services 2.0 Management Console using the icon [ ]in the taskbar.

11. Click **Required: Add a trusted relying party**. This is the Microsoft wording for Service Provider.

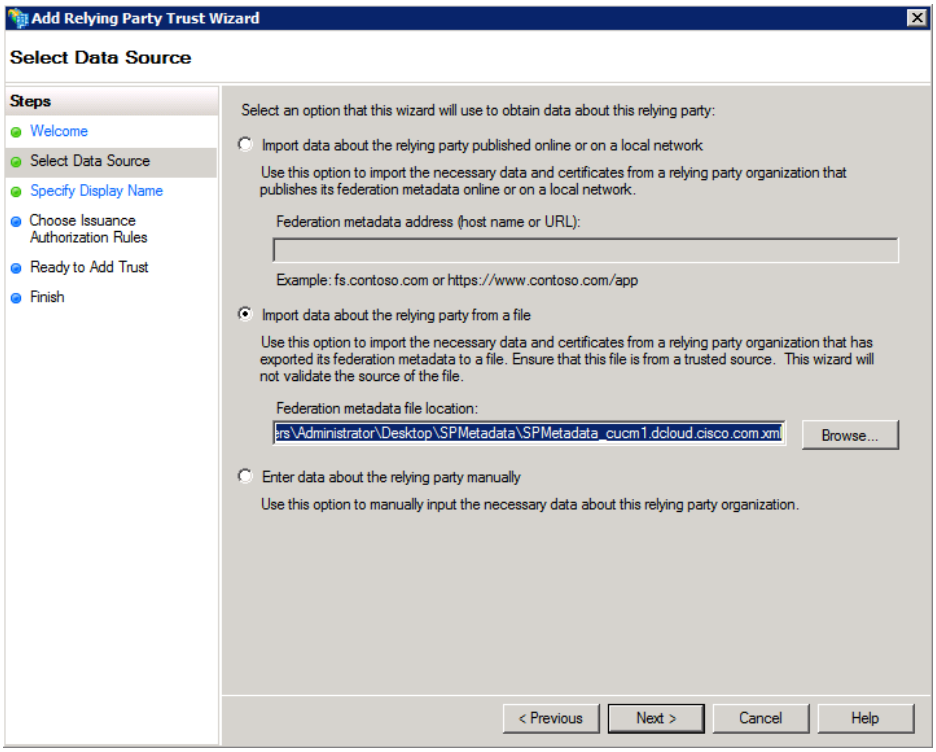
Figure 6. Add a Trusted Relying Party



12. This starts a setup wizard. Click **Start** to begin.

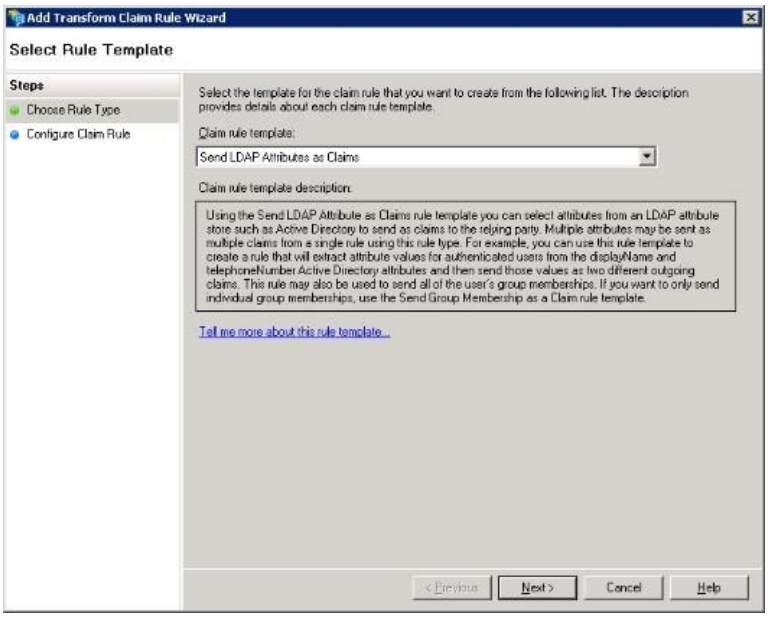
13. Check **Import data about the relying party from a file**, click **Browse** and import the **SPMetadata_cucm1.dcloud.cisco.com.xml** metadata XML file in the **Desktop\SPMetadata** folder, and then click **Next**.

Figure 7. Import XML File



14. Enter **cucm1** as the display name and click **Next**.
15. Confirm the radio button next to **Permit all user to access this relying party** is selected and click **Next**.
16. Click **Next** again.
17. Confirm that **Open the Edit Claim Rules dialog…** is checked and click **Close**.
18. Click **Add Rule**.
19. Keep **Send LDAP Attributes as Claims** selected from the **Claim rule template** drop down menu and click **Next**.

Figure 8. Rule Type



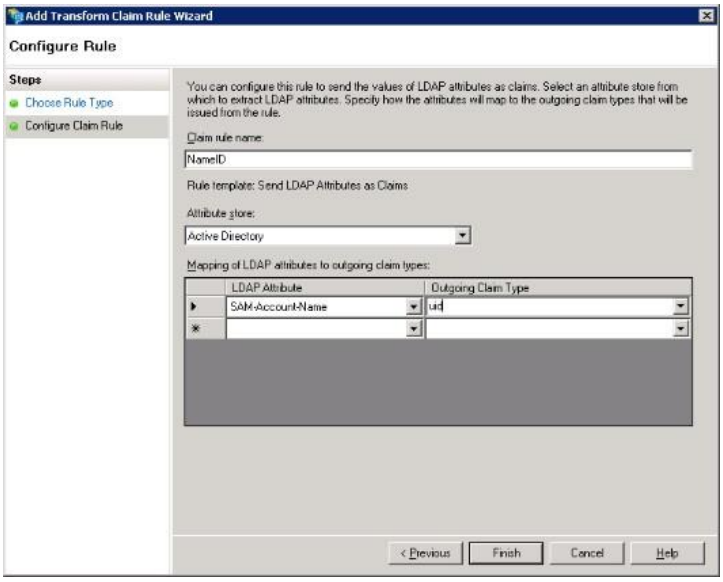
20. Enter the following information for the Claim Rule.

NOTE: the UID must be lower case and will NOT be in the drop down menu.

Table 4. Rule Configuration

Setting	Input
Claim rule name	**NameID**
Attribute Store	**Active Directory**
LDAP Attribute	**SAM-Account-Name**
Outgoing Claim Type	**uid**

Figure 9. Rule Configuration

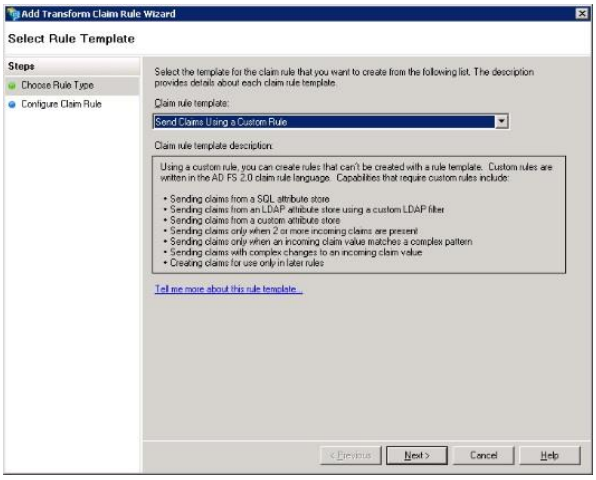


21. Click **Finish** to continue.

22. Click **Add Rule** again to add another rule.

23. Select **Send Claims Using a Custom Rule** from the drop down menu and click **Next**.

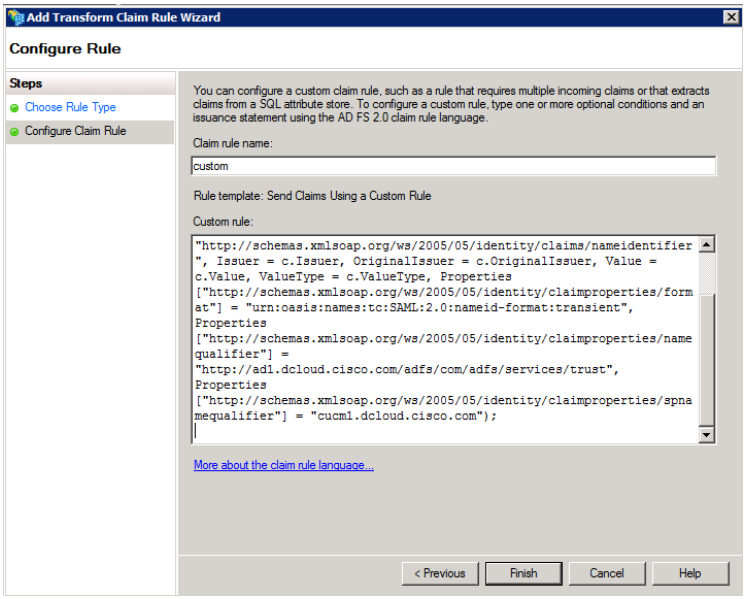
Figure 10. Custom Rule



24. Enter **custom** for the rule name and copy/paste the following text in the rule window.

```
c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"]
 => issue(Type = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier",
Issuer = c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType =
c.ValueType,
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"] =
"urn:oasis:names:tc:SAML:2.0:nameid-format:transient",
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/namequalifier"] =
"http://ad1.dcloud.cisco.com/adfs/com/adfs/services/trust",
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spnamequalifier"]
= "cucm1.dcloud.cisco.com");
```

Figure 11. Custom Rule



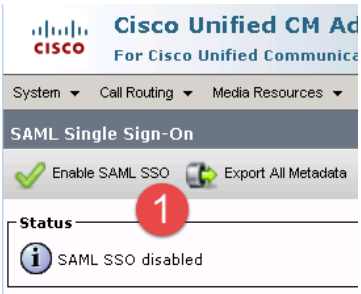
25. Click **Finish** to continue. You should now have two rules defined on ADFS.
26. Click **Apply** and **OK** to close the rules window. You have now successfully added Unified CM as a trusted relying party (SP) to ADFS2.0.

Setup Cisco Unified CM Voice & Video SSO

You need to provide Cisco UCM with information about our IdP. This information is exchanged using XML metadata. The XML file required has already been downloaded for you and placed on the AD1 Desktop.

1. Go back to the Unified CM Administrator tab and click the **Enable SAML SSO** icon.

Figure 12. Enable SAML SSO

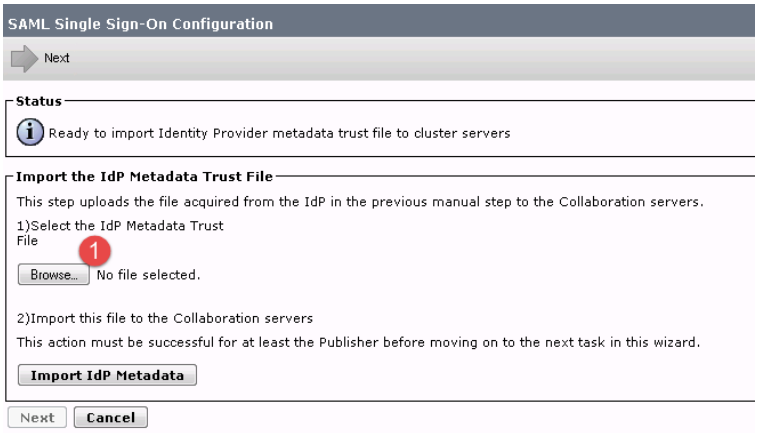


2. On the Security Popup, click **Continue**.
3. Click **Next** because the IdP Metadata Trust File was downloaded for you on the desktop.

NOTE: If you needed to download this file yourself, you would use the following URL: https://ad1.dcloud.cisco.com/FederationMetadata/2007-06/FederationMetadata.xml

4. Click on **Browse…** and choose the IdP Metadata File on the Desktop called **FederationMetadata.xml**.

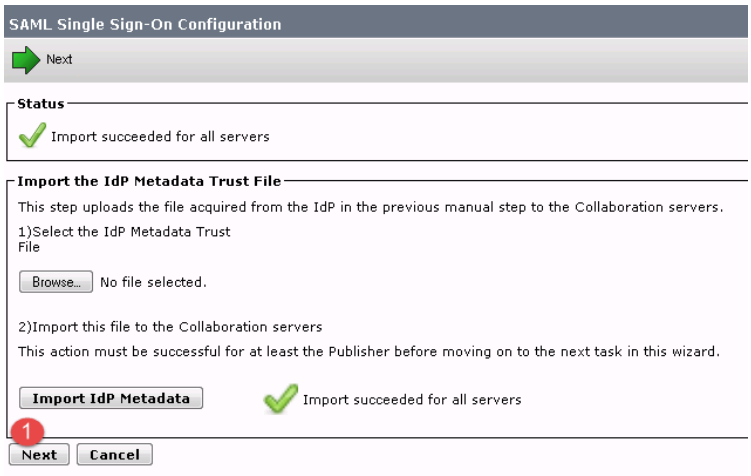
Figure 13. Import IdP Metadata File



5. Click **Import IdP Metadata**.

6. Verify that the Metadata is imported successfully and click **Next**.

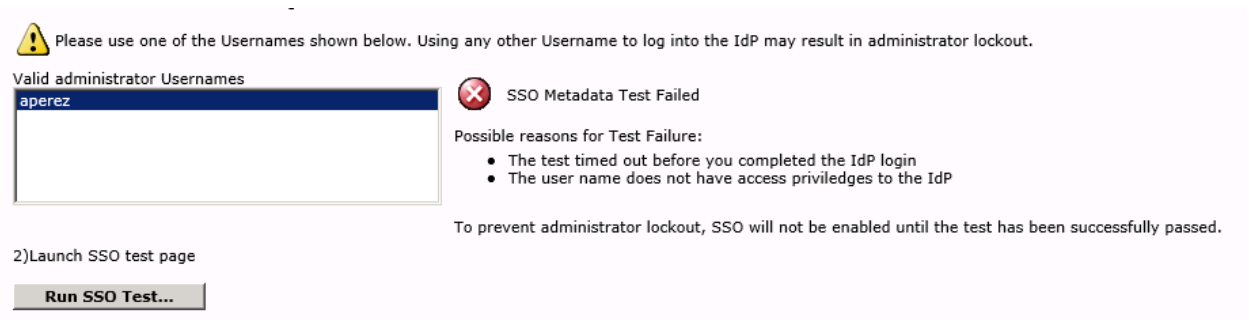
Figure 14. Import Successful



7. You already download the Unified CM cluster Trust Metadata Files in previous steps, so click **Next**.

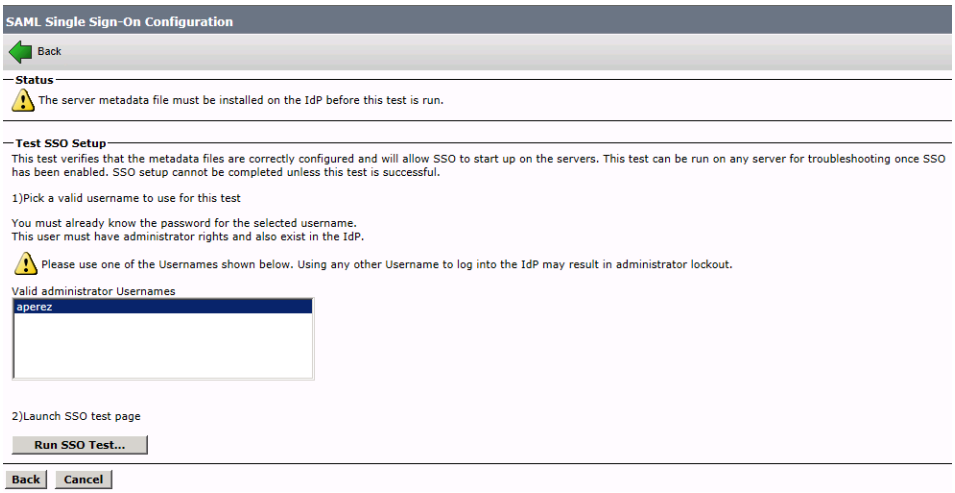
NOTE: There is a 60-second timer running to complete the next few steps. If you do not enter the username and password in Step 10 below in time then you will get an error on the SSO Test as shown below:

Figure 15. SSO Test Timeout



8. The next process will verify the SAML Assertion with ADFS2.0. Click the user **aperez**, and then click **Run SSO Test…**

Figure 16. Run SSO Test



9. In the new window that pops up click **Continue to this website**.
10. Enter Username **aperez** and Password **C1sco12345** and click **OK**.
11. Check if the output message is **SSO Test Succeeded!** If so, then click **Close**.

NOTE: In rare instances, the first time you enable SSO on Unified CM it will not work on the Administration page initially but it will work on the Self Care Portal. The quick fix for this is to disable and then re-enable SSO. The next few steps will first test SSO with the Self Care Portal and then proceed to disable SSO so you can complete the steps above again to re-enable SSO.

1. Click the **home** button to go back to the dCloud links page.
2. Navigate to **Collaboration Server Links** > **Cisco Unified Communications Manager**.
3. Click the **Cisco Unified Communications Self Care Portal** link.
4. This time you should receive an SSO login, which proves that SSO is enabled. There is no need to login at this time. First, you will disable SSO.
5. Navigate back to the Unified CM administration page at **Firefox Home Page** > **Collaboration Server Links** > **Cisco Unified Communications Manager** and click **Cisco Unified Communications Manage**r.
6. Login with username **administrator** and password **dCloud123!**.
7. Navigate to **System** > **SAML Single Sign-On**.
8. Click **Disable SAML SSO** and then **Continue**.
9. Close the browser and then reopen it.
10. Navigate back to the Unified CM administration page at **Collaboration Server Links** > **Cisco Unified Communications Manager**.

11. If you still see the **Recovery URL to bypass Single Sign On (SSO)** link then SSO is still disabled. Keep refreshing your page until that link disappears.

12. Once the link disappears, click the **Cisco Unified Communications Manager** link and login with username **administrator** and password **dCloud123!**.

13. Navigate to **System** > **SAML Single Sign-On**.

14. Follow this link to run through the steps in this section again and re-enable SSO. You should then have a successful SSO test and continue with the rest of this lab.

12. Click **Finish**.

NOTE: Clicking **Finish** will complete enabling SSO on all the servers in this cluster. There will be a short delay while the applications are being updated.

13. You have now successfully completed the basic configuration tasks to enable SSO on UCM using ADFS2.0. Close the web browser so it clears all of the session cookies.

NOTE: It is VERY important to close and reopen Internet Explorer. You are asked to do this several times in this lab. Please be sure to perform this step, as it will clear the cookies from the browser and make it request new login information from the server.

14. Minimize the Remote desktop Connection.

Verify operation on Unified CM SSO functionality

You will now test SSO with an established Username and Password using Workstation 1.

1. RDP to Workstation 1 (198.18.133.36) and login with **dcloud\aperez** / **C1sco12345** , open Internet Explorer and navigate to **Collaboration Server Links** > **Cisco Unified Communications Manager**
2. You will notice there is new option under **Installed Applications** called **Recovery URL to bypass Single Sign-on (SSO)**. If the link is not there, refresh your page until the link appears.
3. Click on this link to open the SSO recovery page.

The recovery option provides a backdoor into Unified CM, which allows you to login locally to Unified CM in the event of an outage at the Identity Provider so you can still administer the box if the SSO provider is down.

NOTE: If you get a 404 error this means the Tomcat service is still restarting. Refresh your browser until you get a login screen.

Figure 17. SSO Recovery Link

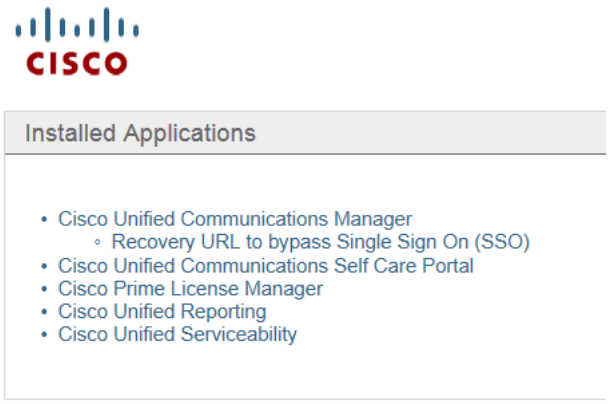
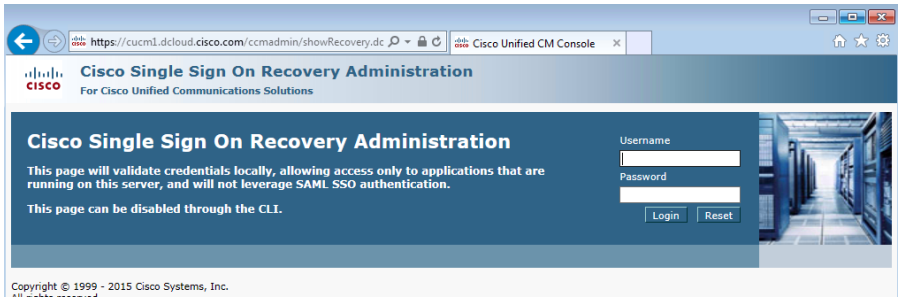
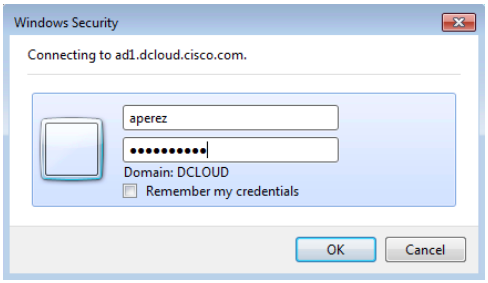


Figure 18. SSO Recovery Login Page



4. Click the back button [] to go back to the main Unified Communications Manager Administration landing page again.
5. Click on the **Cisco Unified Communications Manager** link and notice that you are now presented with an authentication prompt and not the usual Admin login page.

Figure 19. Login Prompt



6. Login as **aperez** with password **C1sco12345** and click **OK** to continue. If your credentials are correct, you will be logged into the Administration page.

Before enabling SSO, the Unified CM admin page prompted you with a HTML form for username and password. After enabling SSO, Unified CM does not handle the Authentication part; this means that the IdP is prompting you with a basic username and password pop-up.

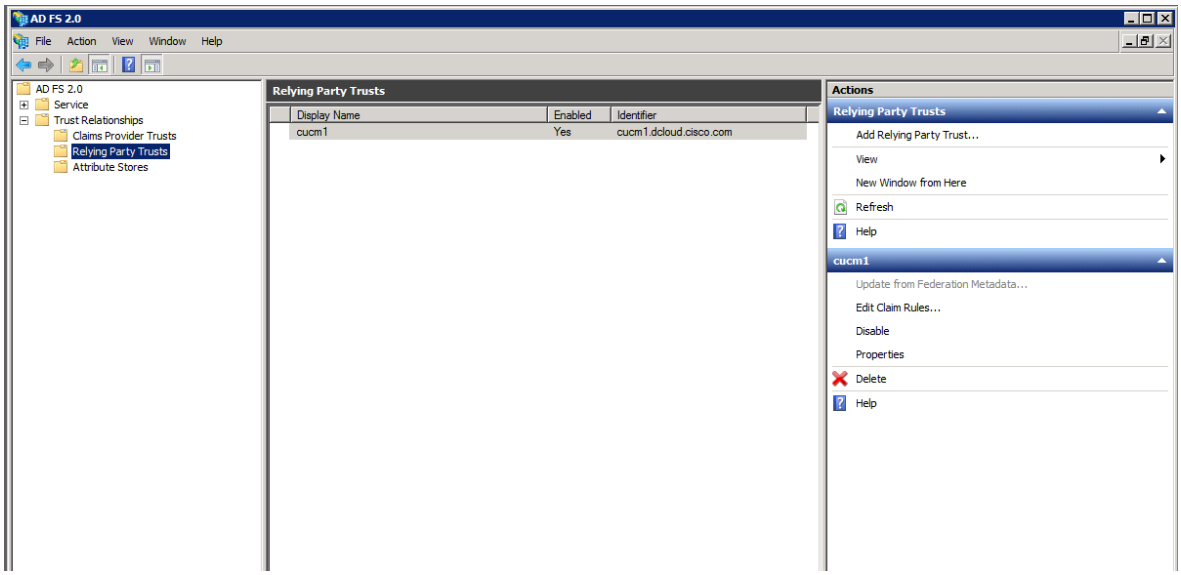
Congratulations! You just SSO enabled your first collaboration product!

Setting up ADFS2 for Unified CM IM&P

Earlier in the lab, you downloaded the Trust Metadata File set. The .zip file contains the metadata for both Cisco Unified Communications Manager Voice & Video and Cisco Unified Communications Manager IM & Presence. Now you will use this file to set up the IM and Presence for the Active Directory server.

1. Go back to the RDP connection to the AD1 server and open the window to the Active Directory Federation Services 2.0 Management Console you opened earlier.
2. Click **Add Relying Party Trust…** at the top right of the window.

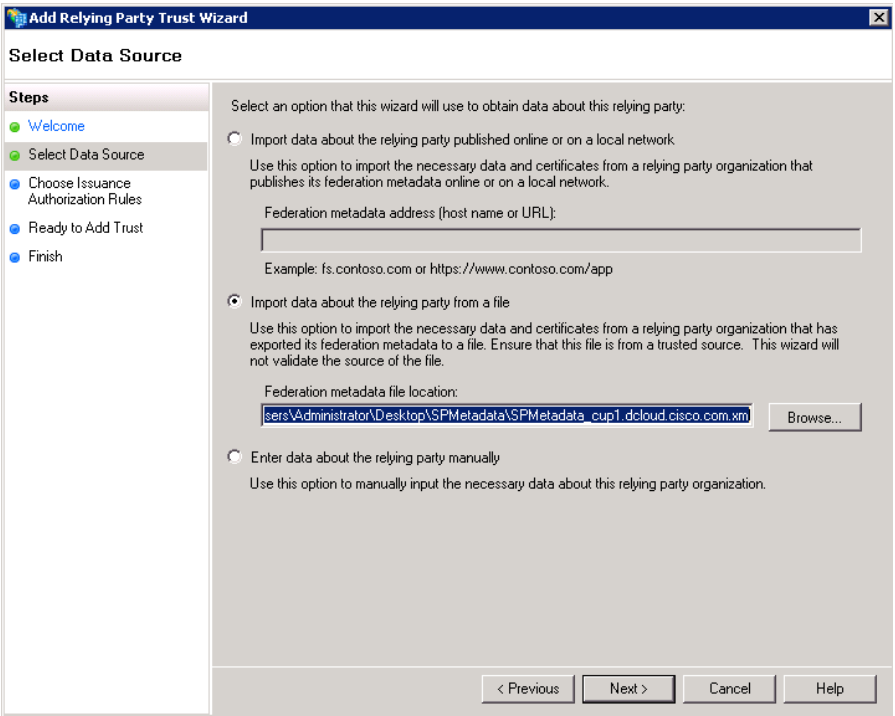
Figure 20. Add Relying Party Trust



3. This opens a setup wizard. Click **Start** to continue.
4. Click the radio button next to **Import data about the relying party from a file**.

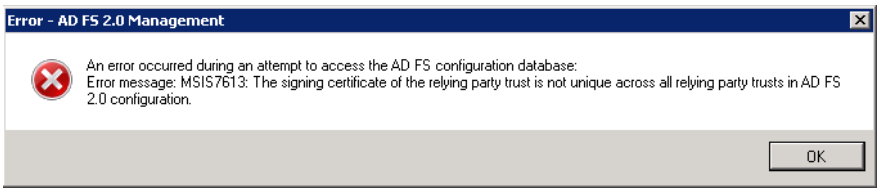
5. Click **Browse** and choose the **SPMetadata_cup1.dcloud.cisco.com.xml** metadata XML file in the **Desktop\SPMetadata** folder you saved and click **Next**.

Figure 21. Choosing the XML File



6. Enter **cup1** as the display name and click **Next**.
7. Click the radio button next to **Permit all user to access this relying party** and click **Next**.
8. Click **Next** at the next screen.
9. Click **OK** at the following error message.

Figure 22. Error Message

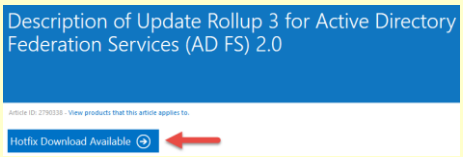


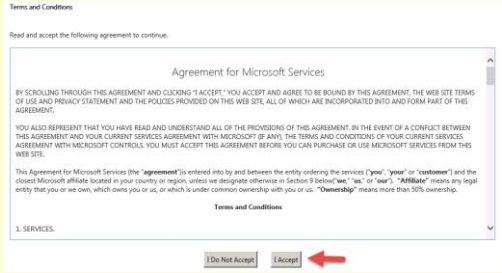
10. You will need to **Cancel** the Add Relying Party Trust Wizard and close AD FS2.0 Management console.

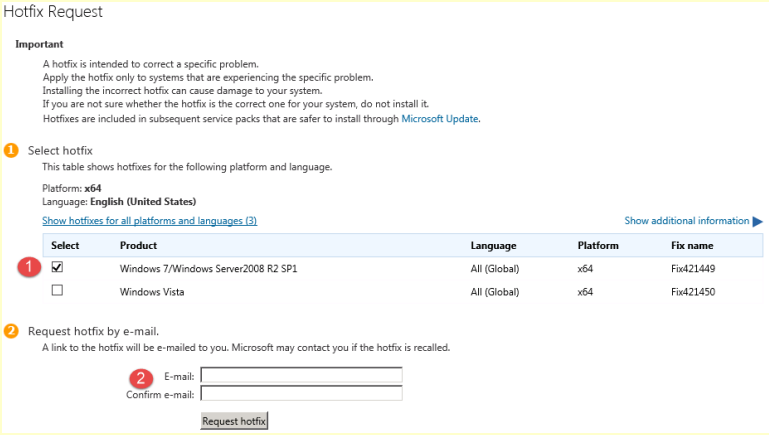
To solve the above error you will have to deploy Microsoft Rollup Update 3 package. The file has been downloaded for you. It will be on the ad1.dcloud.cisco.com server.

NOTE: Due to multi-SAN (Subject Alternate Name) Certificates used in the UCM cluster, AD FS2.0 needs to be patched with Rollup Update 3 package.

If it were not already done, you would download this package from Microsoft at http://support.microsoft.com/kb/2790338

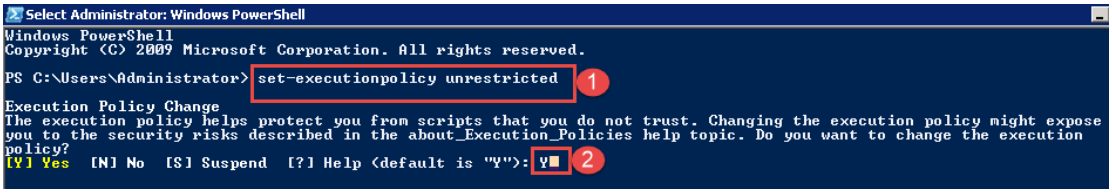






11. In this step, you will need to install the Microsoft Rollup Update 3 for AD FS2.0 and reboot the ad1.dclouc.cisco.com server. On the Active Directory server, execute the file **Windows6.1-KB2790338-v2-x64.msu** file on the AD1 **Desktop**.
12. Click **Yes** to install Hotfix KB2790338.
13. Click **Restart Now** on the ad1.dcloud.cisco.com server, DO NOT shutdown the server or you will not be able to get back to it. The server Restart will take 1 or 2 minutes.
14. After a few minutes, create another RDP connection to AD1 (198.18.133.1) and login with **administrator** / **C1sco12345**.
15. You need to execute a PowerShell® Script, from the Taskbar click the PowerShell icon [].
16. At the PowerShell prompt type: **set-executionpolicy unrestricted**.
17. Accept the execution by typing **Y**.

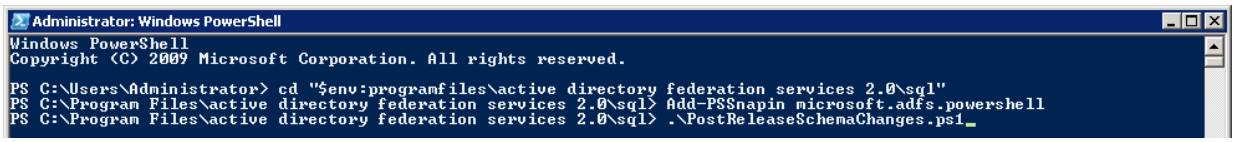
Figure 23. PowerShell Prompt



18. At the PowerShell prompt type the three command lines below. You can copy all at one time and paste them in together.

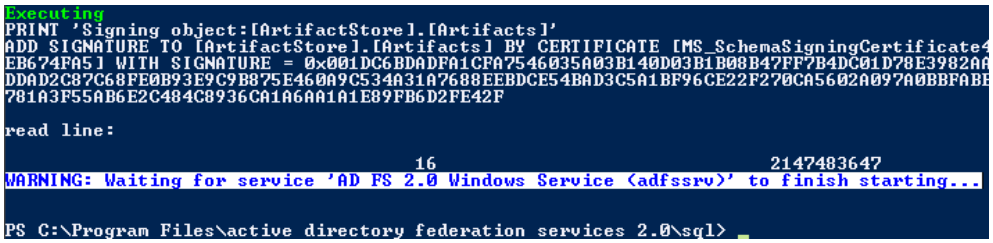
```
cd "$env:programfiles\active directory federation services 2.0\sql"

Add-PSSnapin microsoft.adfs.powershell

.\PostReleaseSchemaChanges.ps1
```

Figure 24. PowerShell Commands



19. You should see the following output:

Figure 25. PowerShell Output

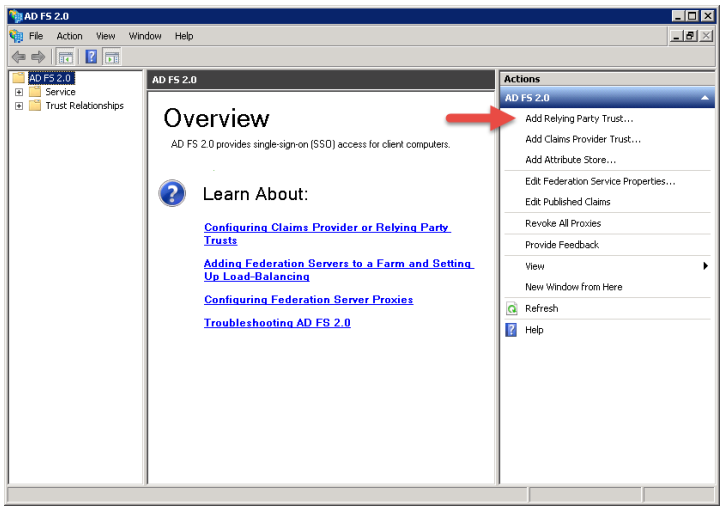


20. After applying this script the AD FS 2.0 service will be restarted so please be patient before opening AD FS 2.0 Management console again. You can now close PowerShell.

21. Open the Active Directory Federation Services 2.0 Management Console again by using the icon in the taskbar [ ].

22. Click **Add Relying Party Trust…**

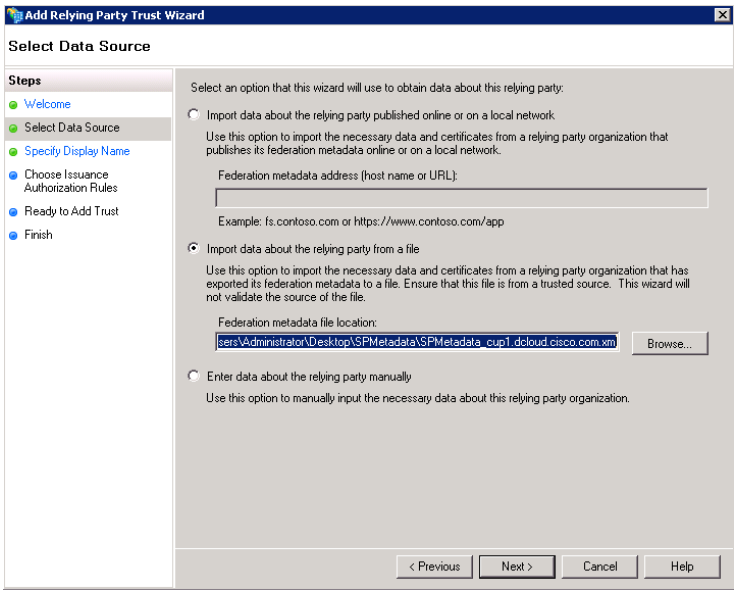
Figure 26. Add Relying Party Trust



23. This opens a setup wizard. Click **Start** to continue.

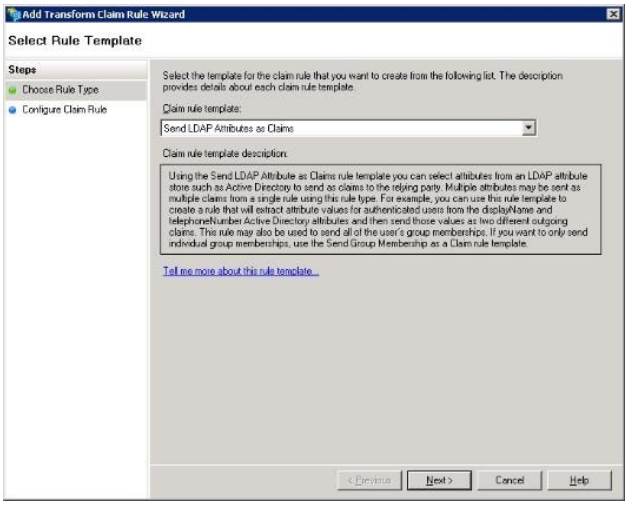
24. Click the radio button next to **Import data about the relying party from a file**.
25. Click **Browse** and choose the **SPMetadata_cup1.dcloud.cisco.com.xml** metadata XML file in the **Desktop\SPMetadata** folder you saved and click **Next**.

Figure 27. Choosing the XML File



26. Enter **cup1** as the display name and click **Next**.
27. Click the radio button next to **Permit all user to access this relying party** and click **Next**.
28. Click **Next** at the next screen.
29. Click **Close** to finish the wizard.
30. Click **Add Rule**.
31. Keep **Send LDAP Attributes as Claims** selected and click **Next**.

Figure 28. LDAP Attributes Menu



NOTE: The UID must be in lower case and will NOT be in the drop down menu.

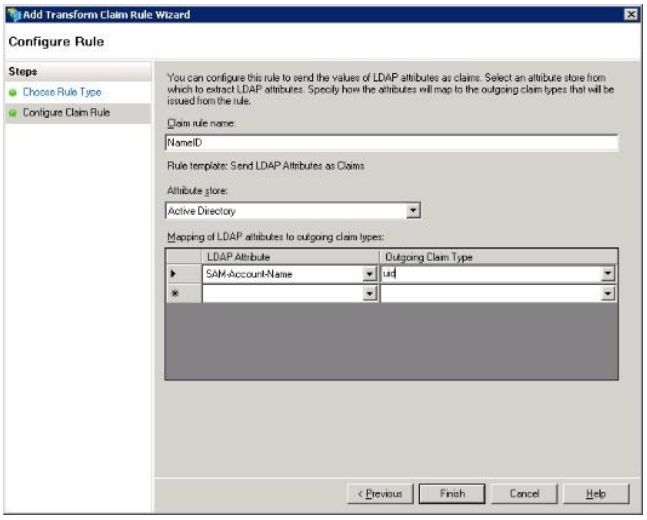
32. Configure the following parameters:

Table 5. LDAP Parameters

Setting	Input
Claim rule name	**NameID**
Attribute Store	**Active Directory**
LDAP Attribute	**SAM-Account-Name**
Outgoing Claim Type	**uid**

33. Click **Finish** to continue.

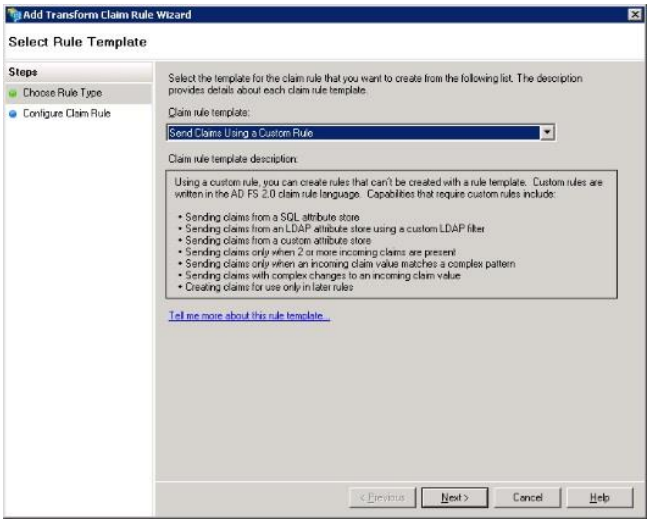
Figure 29. Claim Rule



34. Click **Add Rule** again to add another rule.

35. Choose **Send Claims Using a Custom Rule** and click **Next**.

Figure 30. LDAP Attributes Menu

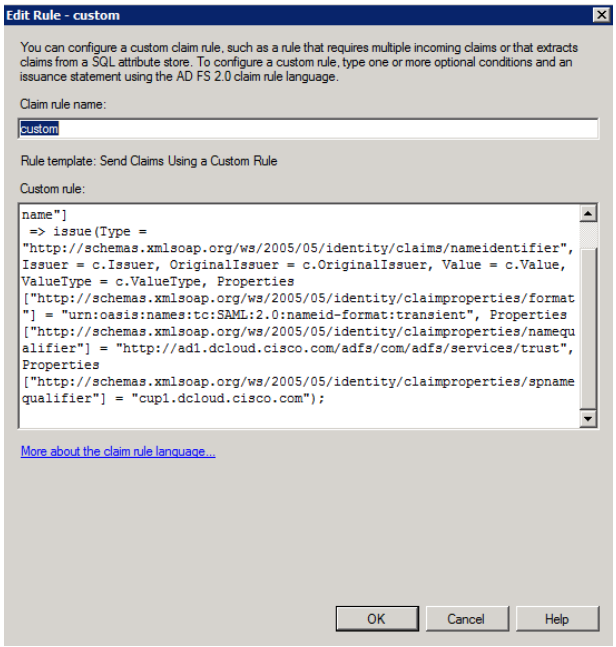


36. Create a custom rule called **custom**. Copy the following text in the rule window and paste into the **Custom** rule field:

```
c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"]
 => issue(Type = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier", Issuer
= c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType = c.ValueType,
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"] =
"urn:oasis:names:tc:SAML:2.0:nameid-format:transient",
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/namequalifier"] =
"http://ad1.dcloud.cisco.com/adfs/com/adfs/services/trust",
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spnamequalifier"] =
"cup1.dcloud.cisco.com");
```

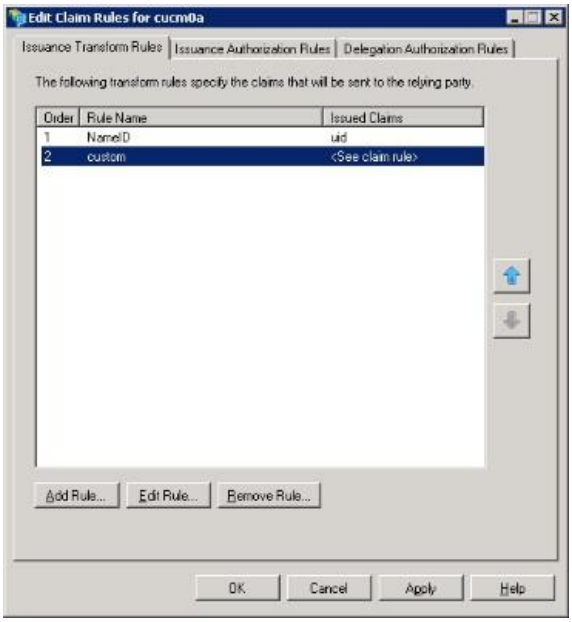
37. Click **Finish** to continue.

Figure 31. Custom Claim Rule



38. You should now have two rules defined on ADFS. Click **Apply** and **OK** to close the rules window.

Figure 32. Rules Window



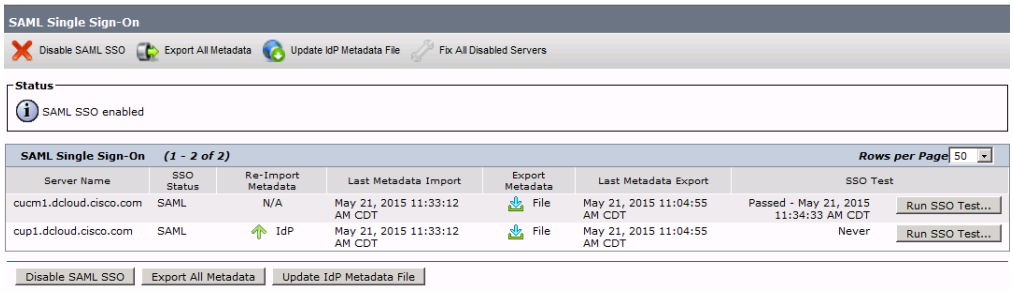
You have now successfully added Cisco Unified Communications Manager IM&P as a trusted relying party to AD FS2.0.

Setup Cisco Unified Communications Manager IM&P SSO

You need to provide Cisco Unified Communications Manager IM&P with information about our IdP. This information is exchanged using XML metadata.

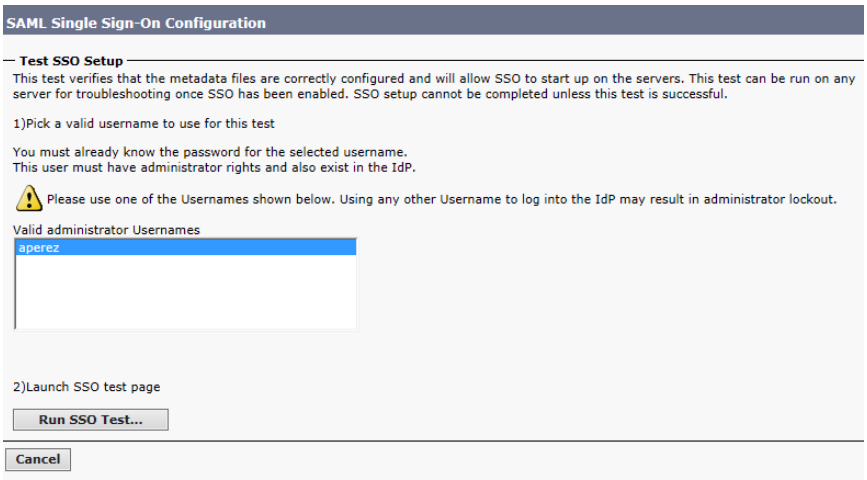
1. You already downloaded the IdP Metadata Trust file on previous steps so you can use the same Metadata file on other Relaying Parties. This file was saved into the user Downloads folder.
2. Back on Workstation 1 open **Internet Explorer** and on the Unified CM Administration page navigate to the **System** > **SAML Single Sign-On**.
3. Click on **Run SSO Test…** for the bottom entry.

Figure 33. Run SSO Test



4. Click on the user **aperez** and click on **Run SSO Test…** again.

Figure 34. Run SSO Test



5. Click on **Continue to this website (not recommended)**.

6. If you see the output message, **SSO Test Succeeded!** you can click **Close**.

Figure 35. SSO Test Succeeded

7. Click **Close**.

You have now successfully completed the basic configuration tasks to enable SSO on Unified CM IM&P using ADFS2.0.

Setup Unity Connection SSO

Due to interest of time, the LDAP Synchronization has already been created for you. The process is documented in Appendix A for your reference.

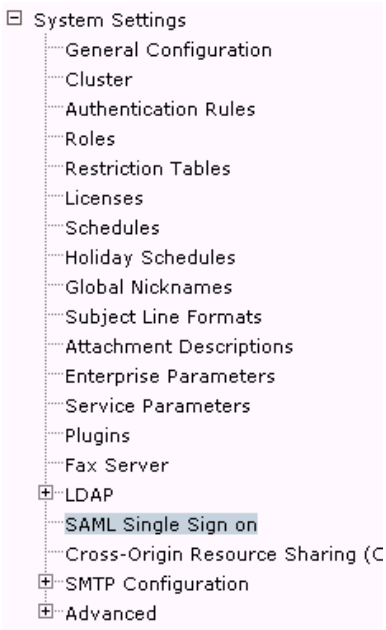
LDAP Synchronization is Mandatory in order to enable SSO.

1. Open the RDP connection to AD1 again, open Internet Explorer and navigate to **Collaboration Server Links** > **Cisco Unity Connection**.

2. Click on the **Cisco Unity Connection** link.

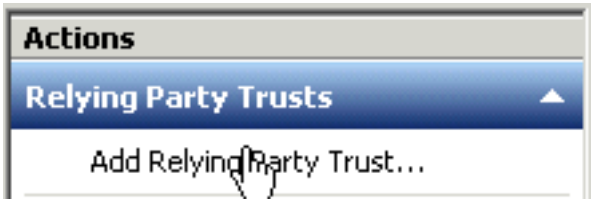
3. Login with username **administrator** and password **dCloud123!**.
4. Scroll down to **Systems Settings** and click **SAML Single Sign On**.

Figure 36. SAML Single Sign-On



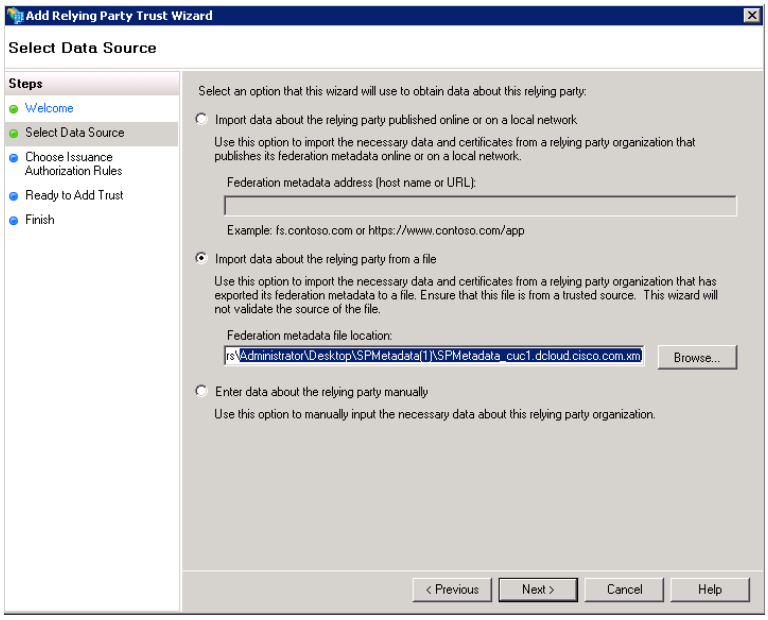
5. Click on **Export All Metadata**.
6. Click the **Save** button at the bottom of the page to save the zip file to the Desktop, minimize Internet Explorer, then right click on the file **SPMetadata(1)** zip file and choose **Extract All**. Remember there is already a zip file on the desktop with the same name. Make sure to extract the one with the (1) at the end.
7. After successful extraction, you will now also have a **SPMetadata_cuc1cdcloud.cisco.com.xml** file in the **SPMetadata(1)** folder.
8. Go back to the **AD FS 2.0 Management console** and click **Relying Party Trusts** > **Add Relying Party Trust**.

Figure 37. Add Relying Trust



9. Click **Start** to begin the setup wizard.
10. Click the **Import data about the relying party from a file** radio button and click **Browse**.
11. Choose the **SPMetadata_cuc1.dcloud.cisco.com.xml** metadata XML file in the **Desktop\SPMetadata(1)** folder you saved and click **Next**.

Figure 38. XML Metadata File



12. Enter **cuc1** as the display name and click **Next**.
13. Keep the radio button next to **Permit all user to access this relying party** selected and click **Next**.
14. Click **Next** to continue.
15. Click **Close**.
16. Click **Add Rule**.
17. Keep **Send LDAP Attributes as Claims** select in the drop down menu and click **Next**.
18. Configure the following parameters and click **Finish**.

Table 6. LDAP Parameters

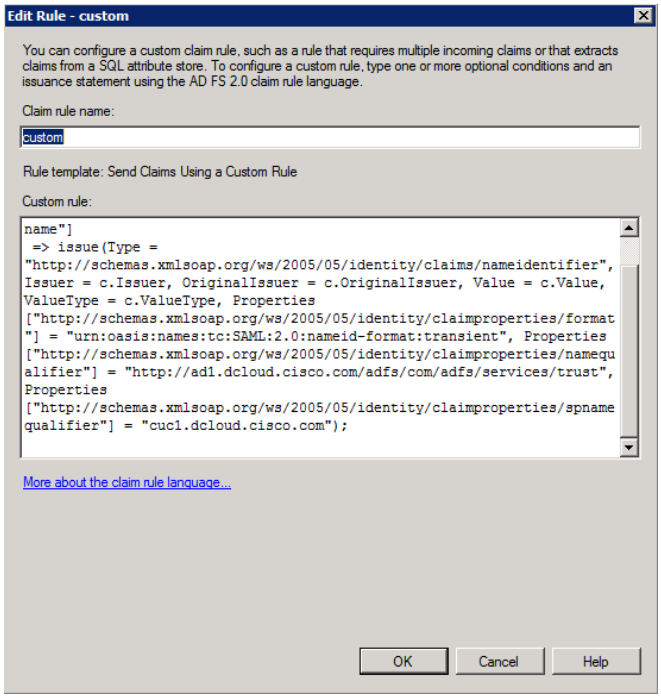
Setting	Input
Claim Rule Name	**NameID**
Attribute Store	**Active Directory**
LDAP Attribute	**SAM-Account-Name**
Outgoing Claim Type	**uid**

19. Click **Add Rule** again to add another rule.
20. From the drop down menu choose **Send Claims Using a Custom Rule** and click **Next**.
21. Created a custom rule called **custom**. Copy and paste the followed text in the rule window:

```
c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"]
 => issue(Type = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier",
Issuer = c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType =
c.ValueType,
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"] =
"urn:oasis:names:tc:SAML:2.0:nameid-format:transient",
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/namequalifier"] =
"http://ad1.dcloud.cisco.com/adfs/com/adfs/services/trust",
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spnamequalifier"]
= "cuc1.dcloud.cisco.com");
```

22. Click **Finish** to continue.

Figure 39. Custom Rule

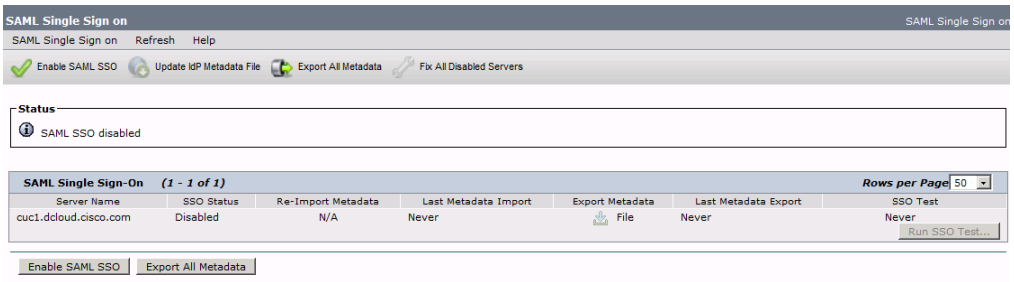


23. You should now have two rules defined on ADFS. Click **Apply** and **OK** to close the rules window. You have now successfully added Unity Connection as a trusted relying party to ADFS.

24. Go back to the browser tab with the Unity Connection Administration page.

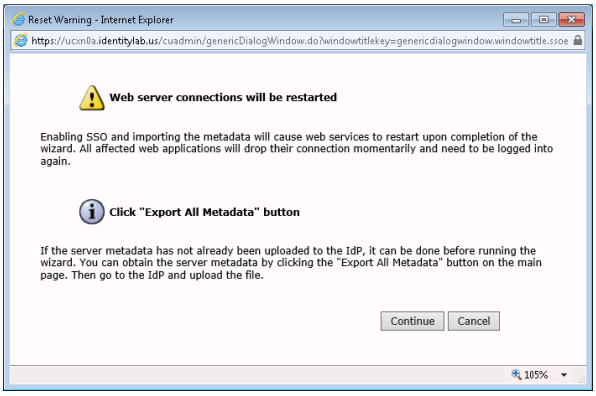
25. Click **Enable SAML SSO**.

Figure 40. Enable SAML SSO



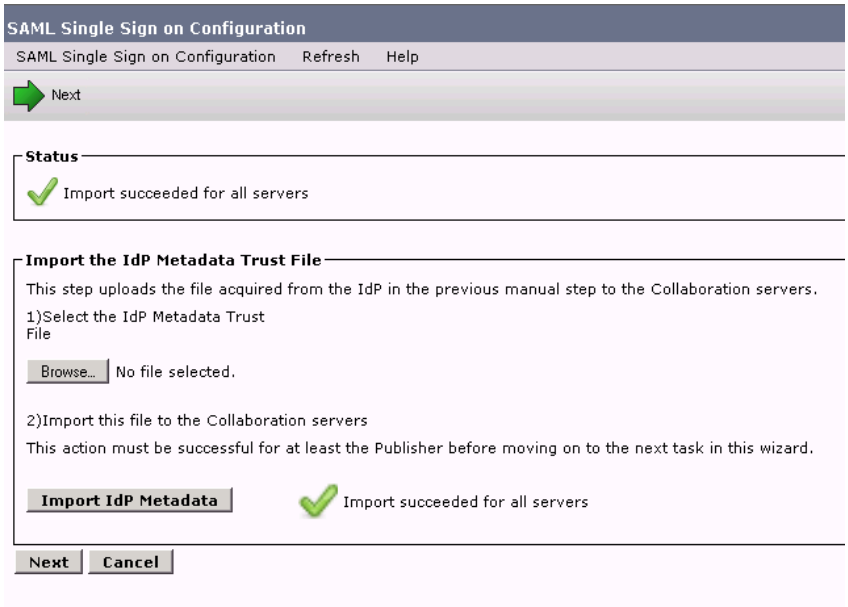
26. Click **Continue**.

Figure 41. Export All Metadata



27. Click **Next**.
28. The IdP Metadata Trust file has already downloaded for you. It is on the Desktop.
29. Click **Browse** and navigate to the Desktop and choose the **FederationMetadata.xml** file.
30. Click **Import IdP Metadata**. See the figure below for more information:

Figure 42. Import IdP Metadata



31. Click **Next**.
32. Click **Next** again since you already downloaded the trust file in the previous step.
33. Click **aperez** and click **Run SSO Test**. As you did before, click **Continue to this website..**

Figure 43. Run Test

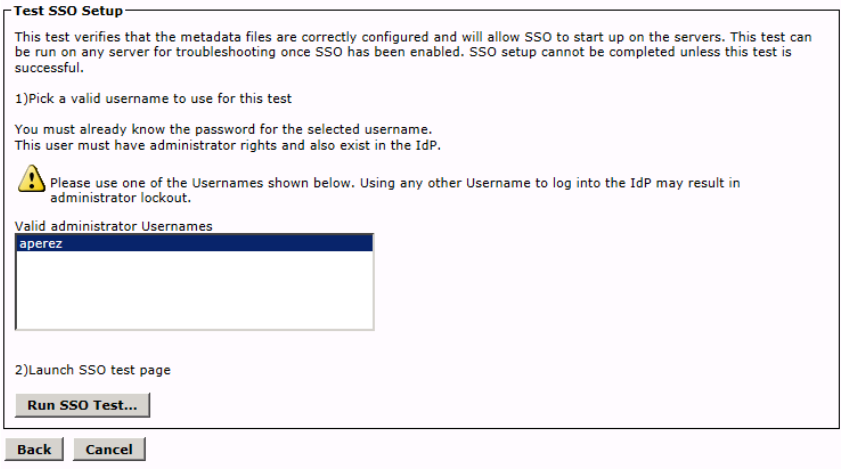
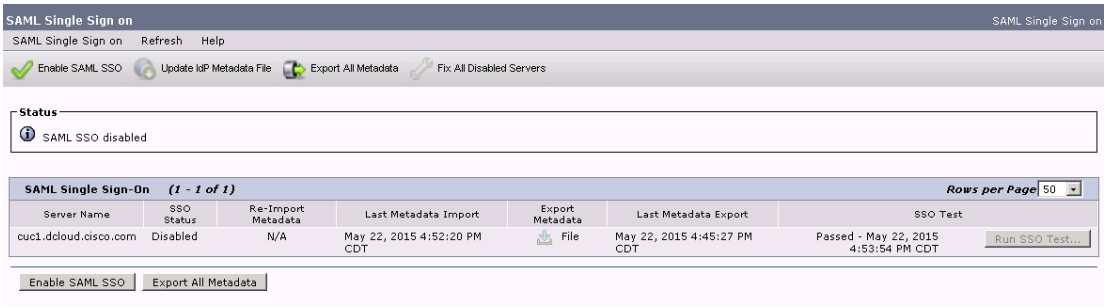


Figure 44. SSO Successful

34. After a successful test, click **Finish**.
35. Click **SAML Single Sign On** from the left hand window again.
36. You should see the following notice showing the date and time of the successful configuration. Enabling SSO on Unity Connection will restart Cisco Tomcat service; this might take up to 3 minutes.

Figure 45. SAML SSO Enabled



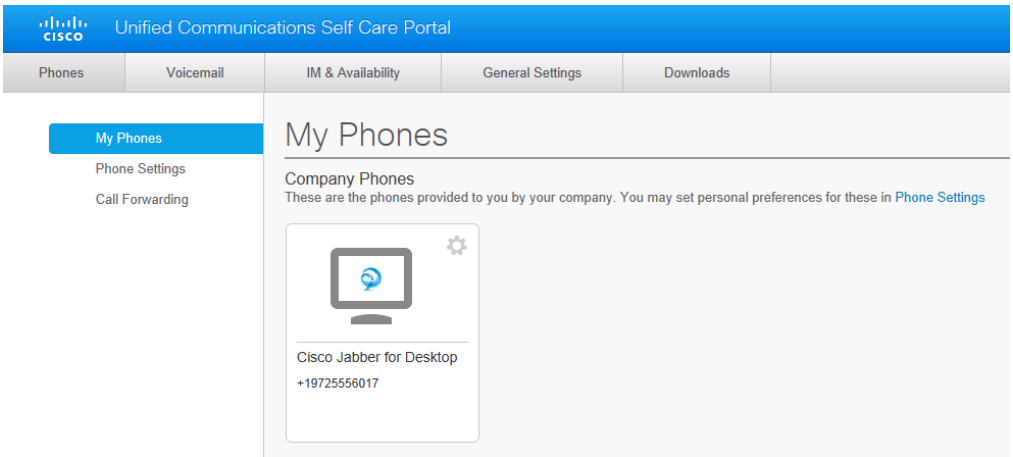
This concludes this lab activity.

Verify operation of Username/Password based Authentication

1. Open back up the RDP connection to Workstation 1.
2. Close the browser and reopen, then navigate to **Collaboration Server Links > Cisco Unified Communications Manager**.
3. Click on **Cisco Unified Communications Self Care Portal**.

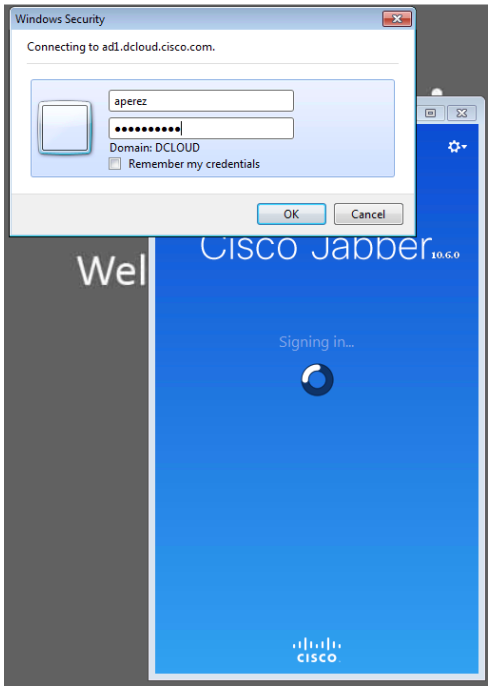
4. Login as Username **aperez** with Password **C1sco12345**.
5. You should see the **Self Care portal**.

Figure 46. Self Care Portal



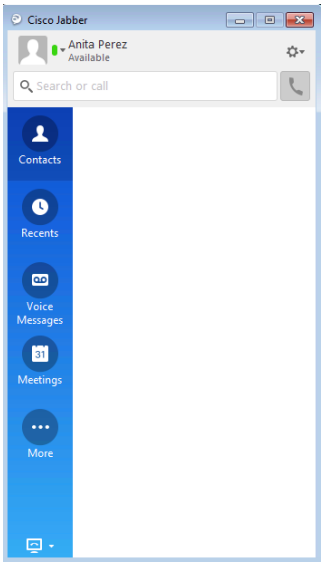
6. Minimize the web browser and execute the **CiscoJabberSetup.msi**. file on the Workstation 1 Desktop.
7. Follow the Jabber installation wizard by clicking **Accept and Install**.
8. Leave the box checked for **Launch Cisco Jabber** and click **Finish**.
9. Login to Jabber as Username **aperez** with Password **C1sco12345**.
10. Notice that you are seeing a login prompt and not the standard Jabber login window.

Figure 47. Jabber Login Prompt



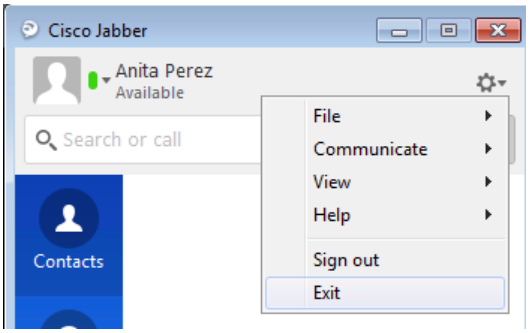
11. After login, Jabber will be fully authenticated.

Figure 48. Full Authentication



12. Exit from Jabber. Be sure to click **Settings** > **Exit**, because clicking the **X** will just minimize Jabber instead of closing it.

Figure 49. Exit Jabber



This concludes this lab activity.

Kerberos based Authentication with AD FS 2.0

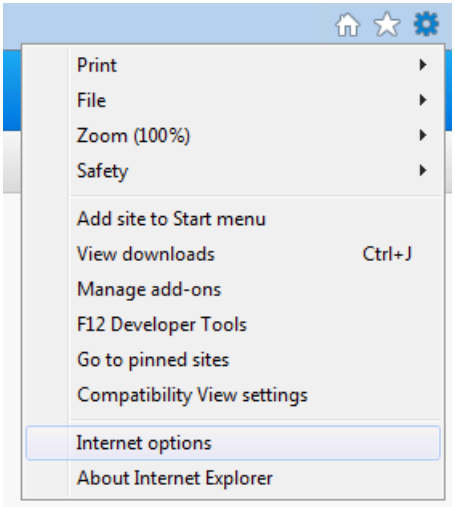
In this section, you are going to utilize the fact that the user is logged in to Active Directory. You will get rid of the username/password prompt at the SSO server and instead let the web browser use the Kerberos authentication of the Windows Domain.

NOTE: By default, AD FS 2.0 has Kerberos enabled, so you do not have to configure anything at server side.

Configuring MS Internet Explorer for Kerberos-based authentication

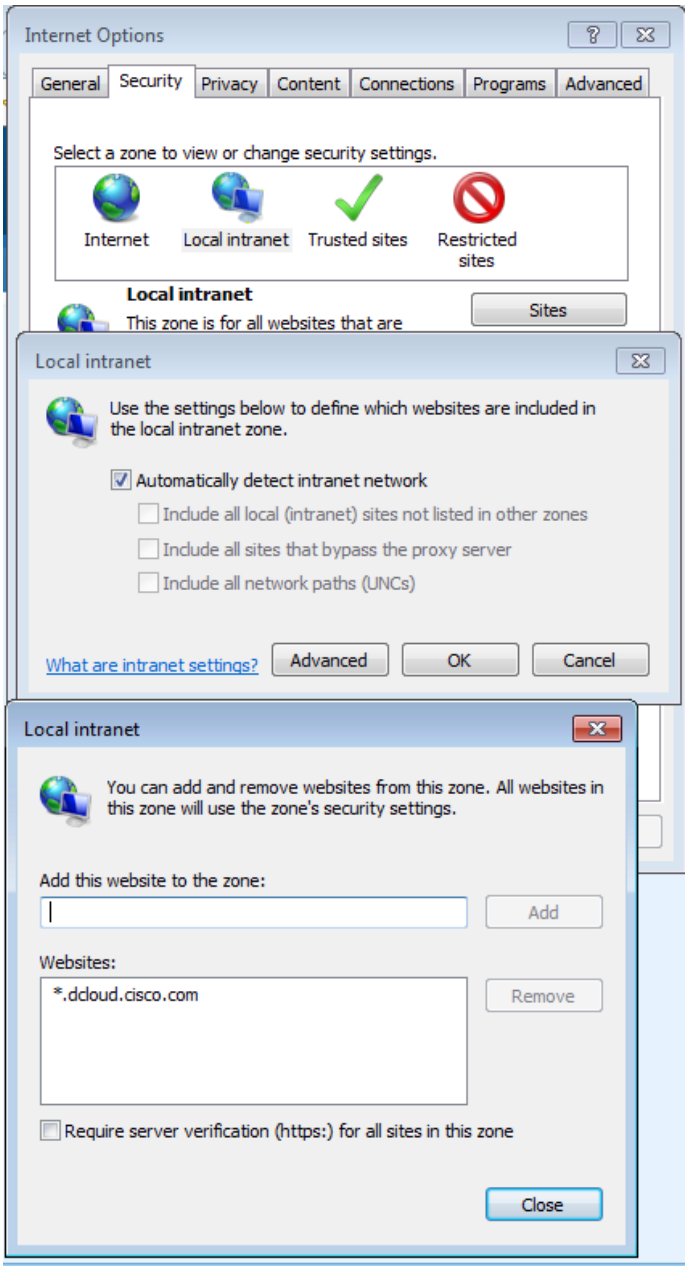
1. Open Internet Explorer on Workstation 1 and open **Internet Options**.

Figure 50. Internet Options



2. Navigate to **Security**, click **Local Intranet** and click **Sites...** Click **Advanced** and in the dialog box enter ***.dcloud.cisco.com** in the **Add this website to the zone** and click **Add**.

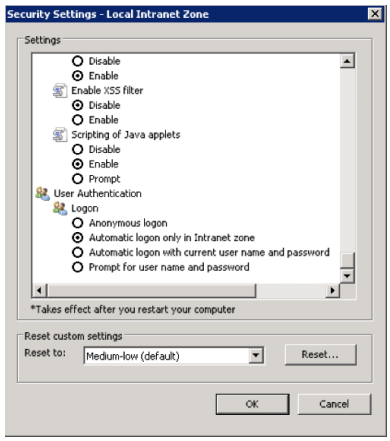
Figure 51. Adding Exceptions



3. Close the dialogs and get back to the **Internet options...** section. Click **Custom level...** in the **Security** tab.

4. Scroll down and verify that **User Authentication > Logon** (at the bottom) is set to **Automatic logon only in Intranet zone**.

Figure 52. Security Settings



Verify operation of Kerberos based Authentication

1. Close the browser and reopen. Navigate to **Collaboration Server Links** > **Cisco Unified Communications Manager**
2. Click on **Cisco Unified Communications Self Care Portal**.
3. You should see the Self Care portal and the user will not be prompted for any authentication.
4. Double-click the Cisco Jabber shortcut on the workstation desktop. You can see that Jabber will not prompt for any authentication. At this point, Jabber will be fully authenticated.
5. Exit Jabber.

This concludes this lab activity.

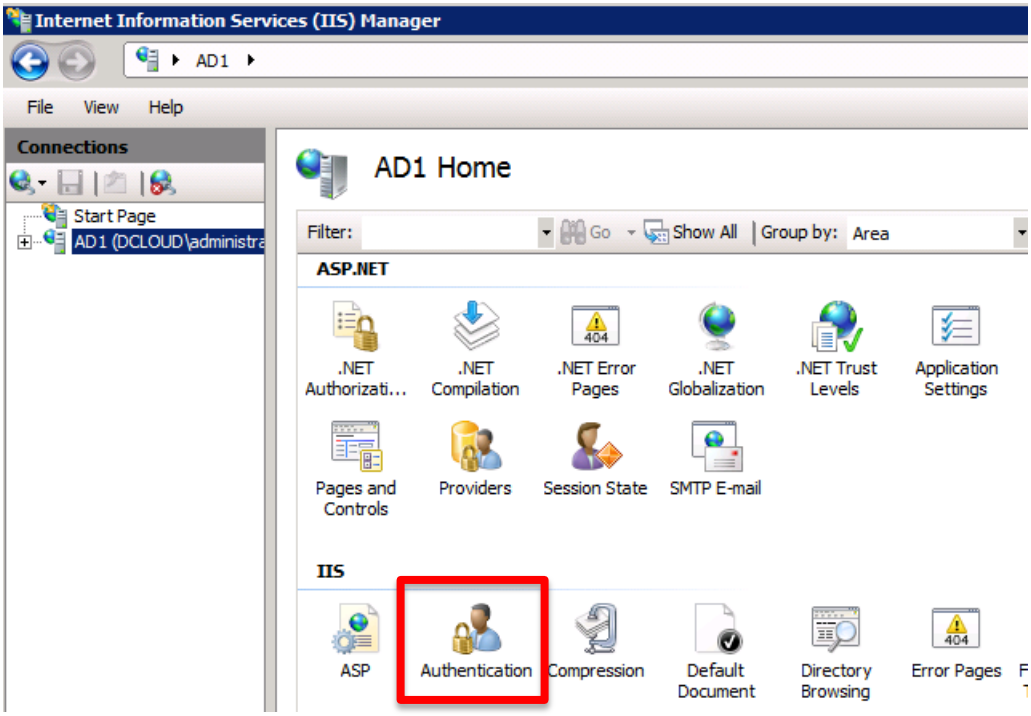
Certificates based Authentication with ADFS2.0

In this section, you are going to use certificates to authenticate the user to the ADFS. In order to do so, the user will have to apply for the certificate and install it to his/her machine. Because ADFS is integrated with Active Directory, the certificate will be automatically stored in Active Directory and will associate the certificate to the user account. This will ensure that once the user authenticates using the certificate, ADFS will know who he/she is. In other words, the Active Directory provides mapping between the certificate and the username (sAMAccountName in our lab).

NOTE: In order to enable AD FS 2.0 Certificate Authentication it is necessary to add a Service Role to Internet Information Server (Web Server). In the interest of time, this was pre-configured for you in the lab. For reference, we have included the instructions in Appendix C.

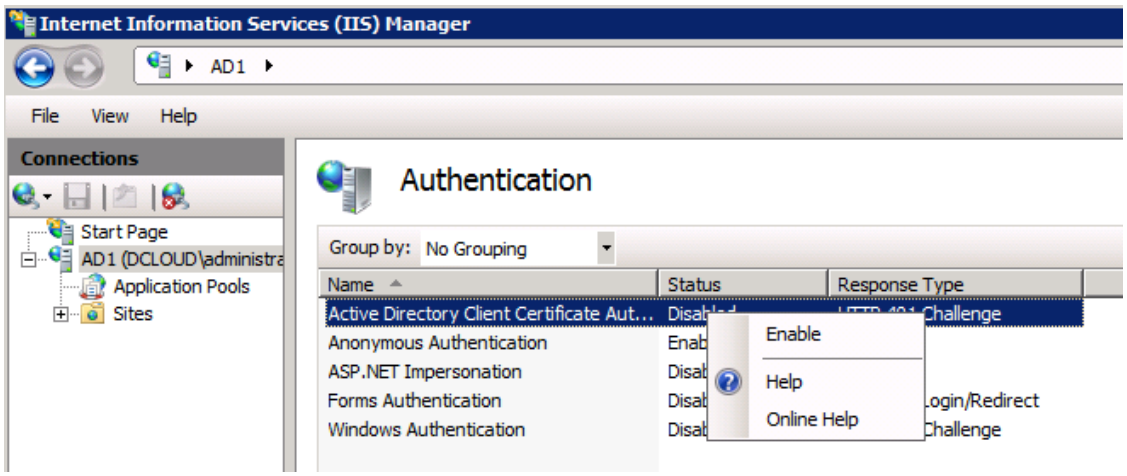
1. Open the RDP connection to AD1 and then launch **Internet Information Services (IIS) Manager** by using the icon [] in the Taskbar.
2. Navigate to **AD1**, and open the **Authentication** module.

Figure 53. Authentication Module



3. Enable the **Active Directory Client Certificate Authentication** by right clicking on it and choosing **Enable** from the menu.

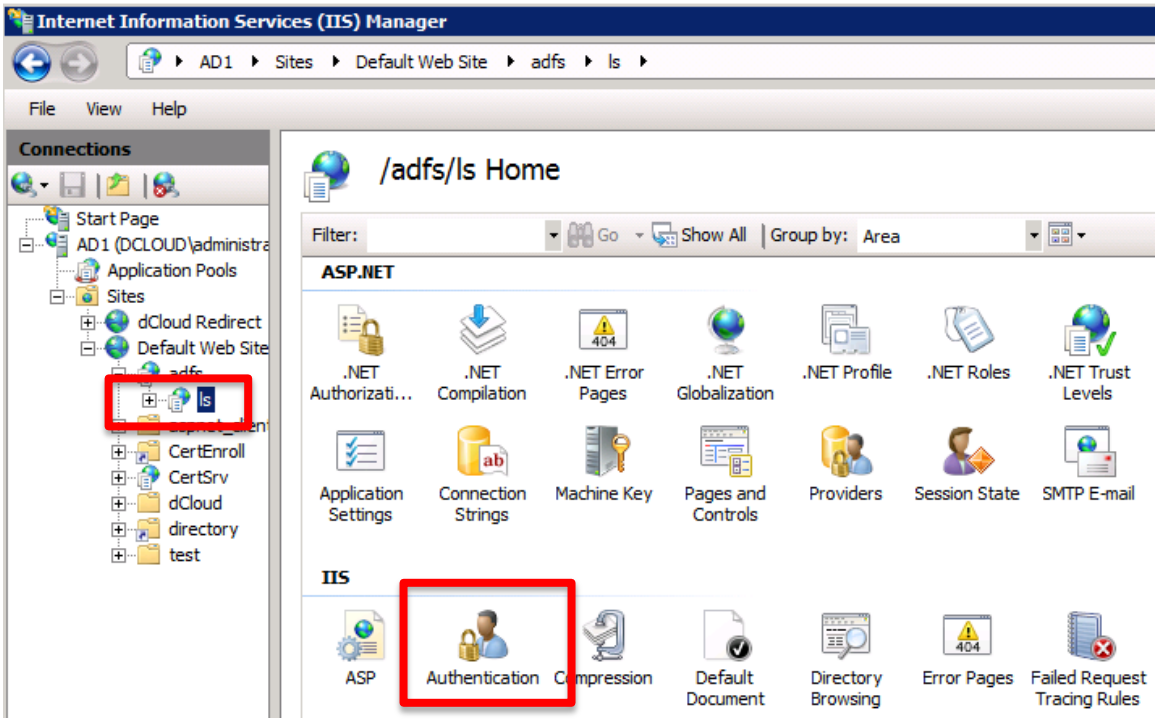
Figure 54. AD Client Certificate Authentication



4. Note that this has to be done at the server level. If you check the Authentication in the **Default Web Site** or its sub-folders, you will not see the **Active Directory Client Certificate Authentication**.

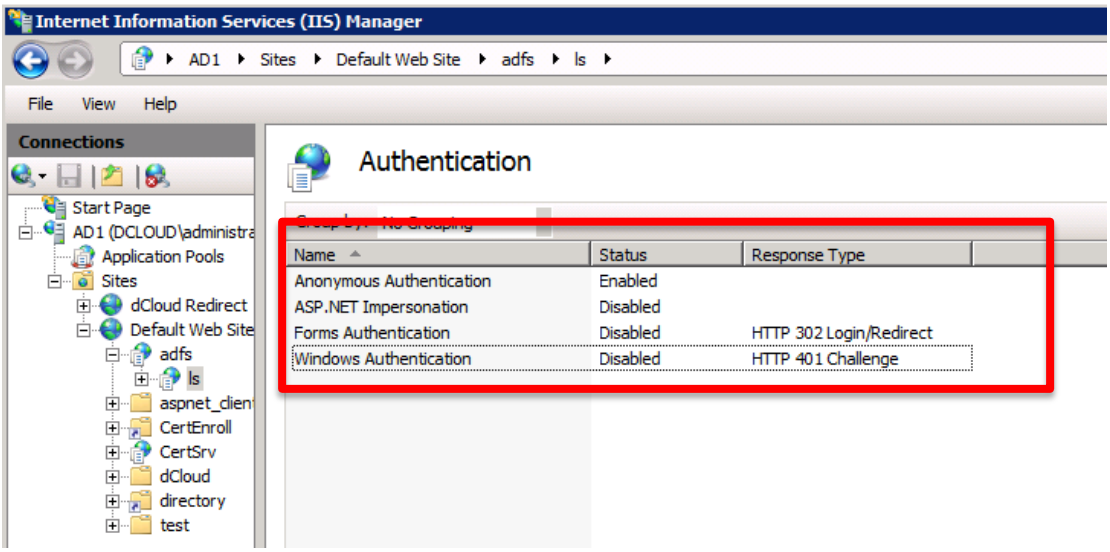
5. In IIS Manager, navigate to **AD1/Sites/Default Web Site/adfs/ls** and open the **Authentication** module.

Figure 55. Authentication Module



6. Set the **Windows Authentication** to **Disabled** and **Forms Authentication** to **Disabled**. Also, make sure the **Anonymous Authentication** is **Enabled**.

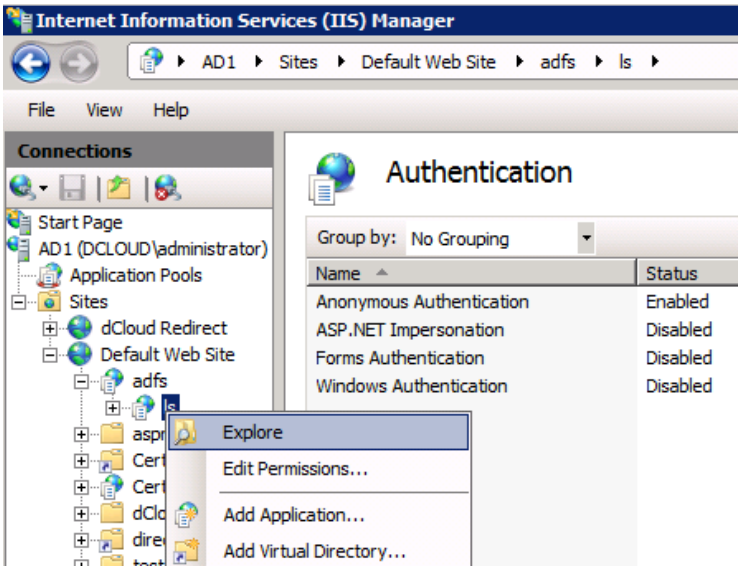
Figure 56. Services Configuration



NOTE: Although it seems that now you have replaced the Kerberos/NTLM (Windows Authentication) for Digital Certificates authentication you still need to do a final piece of configuration inside the ADFS.

7. Right-click the **ls** in IIS Manager and choose **Explore**.

Figure 57. IIS Manager



8. On the AD1 Desktop copy the file (Ctrl + C) **web-certs.config**, click back on the explorer window and paste into the folder **C:\inetpub\adfs\ls**.
9. Rename the **web.config** file to **web-krb.config** and then rename **web-certs.config** to **web.config**.
10. The **web-certs.config** file includes a change that needs to be done in order that certificate-based authentication would take precedence over Kerberos authentication. The difference between the configuration files is shown below. This reflects the order of authentication that ADFS will use for authenticate the user.

The **web-krb.config** file includes this piece of configuration:

```
<localAuthenticationTypes>
  <add name="Integrated" page="auth/integrated/" />
  <add name="Forms" page="FormsSignIn.aspx" />
  <add name="Basic" page="auth/basic/" />
  <add name="TlsClient" page="auth/sslclient/" />
</localAuthenticationTypes>
```

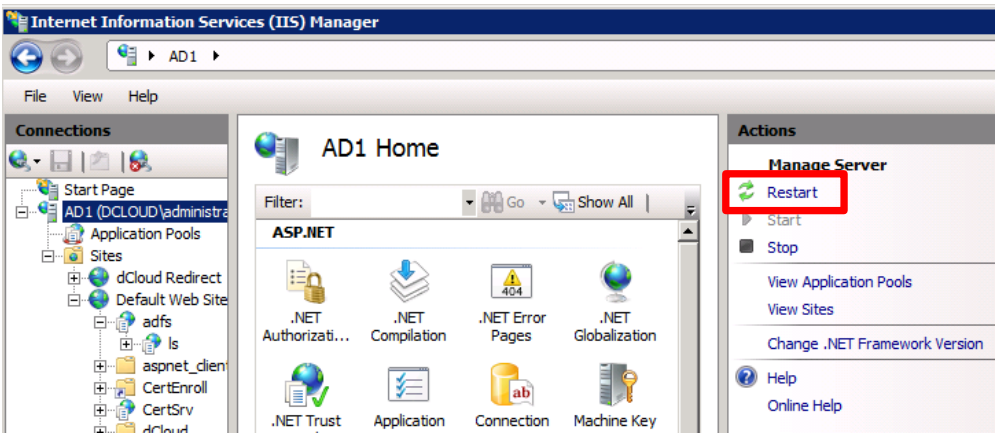
The **web-certs.config** file has the certificate-based authentication at the first place:

```
<localAuthenticationTypes>
  <add name="TlsClient" page="auth/sslclient/" />
  <add name="Integrated" page="auth/integrated/" />
  <add name="Forms" page="FormsSignIn.aspx" />
  <add name="Basic" page="auth/basic/" />
</localAuthenticationTypes>
```

NOTE: The ADFS is now configured for certificate-based authentication. Now still you need to create a user certificate and make sure your web browser will be able to use it.

11. You need to restart IIS so those modifications take effect. Go Back to IIS Manager, choose AD1 and then click **Restart**.

Figure 58. Restart IIS Server

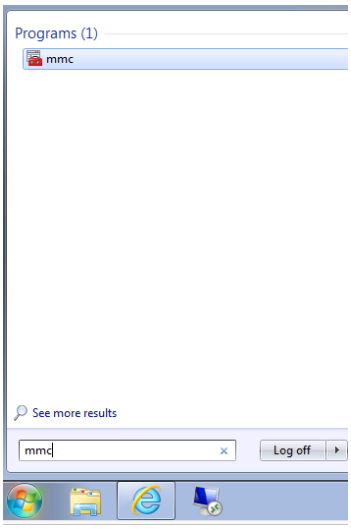


Create a user certificate to use for certificate-based authentication

To be able to authenticate successfully based on certificates the users trying to authenticate obviously require a user certificate. Perform these steps on Workstation 1.

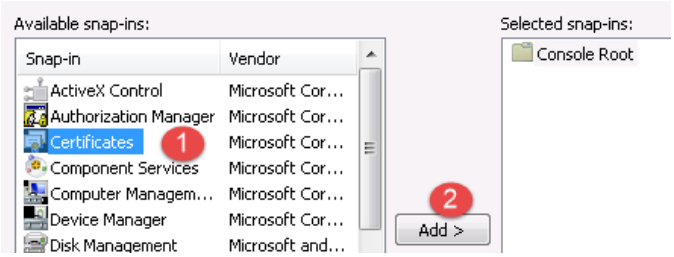
1. On **Workstation 1**, open the **Microsoft Management Console** by entering **mmc** under **Start/Search programs and files** and clicking the program.

Figure 59. MMC



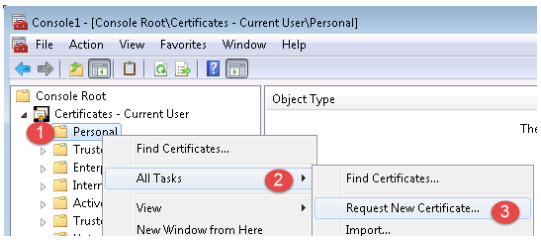
2. On the **File** menu, click **Add/Remove Snap-in**.
3. Click **Certificates** and click **Add**.

Figure 60. Add Certificates



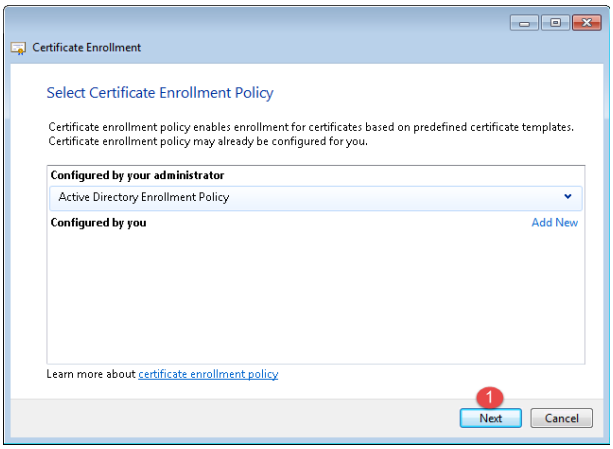
4. Leave the default as **My user account** and click **Finish**.
5. Click **OK**.
6. Expand **Certificates – Current User** and right-click on **Personal** and choose **All Tasks** > **Request New Certificate**. This starts a setup wizard.

Figure 61. Request New Certificate



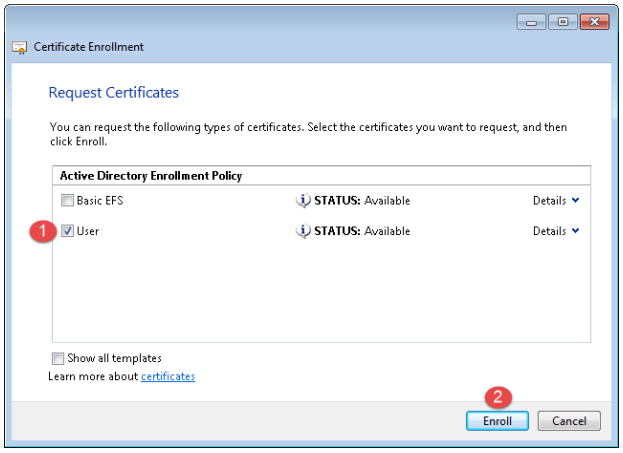
7. Click **Next** to begin.
8. Leave the defaults on the first screen and click **Next**.

Figure 62. Certificate Enrollment Policy



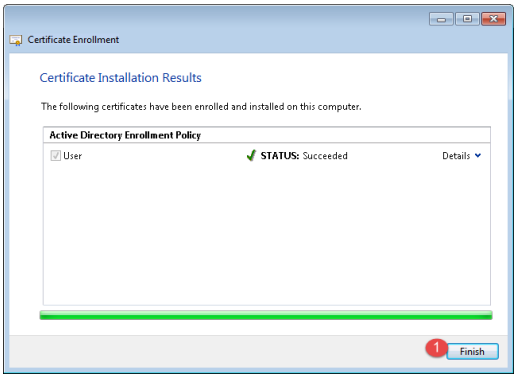
9. Click the box next to the standard **User** certificate template and click **Enroll**. The enrolment process starts, and certificate is issued.

Figure 63. User Enrollment



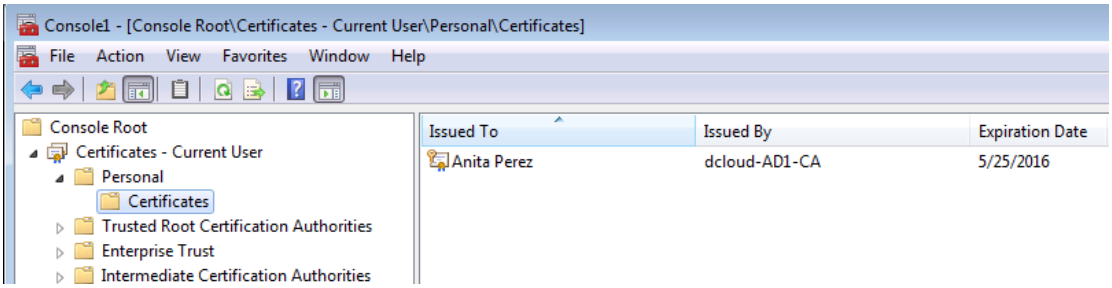
10. When you see a successful status, you can click **Finish**.

Figure 64. Successful Enrollment



11. The issued certificate shows up in the **Certificates** folder.

Figure 65. Certificates Folder



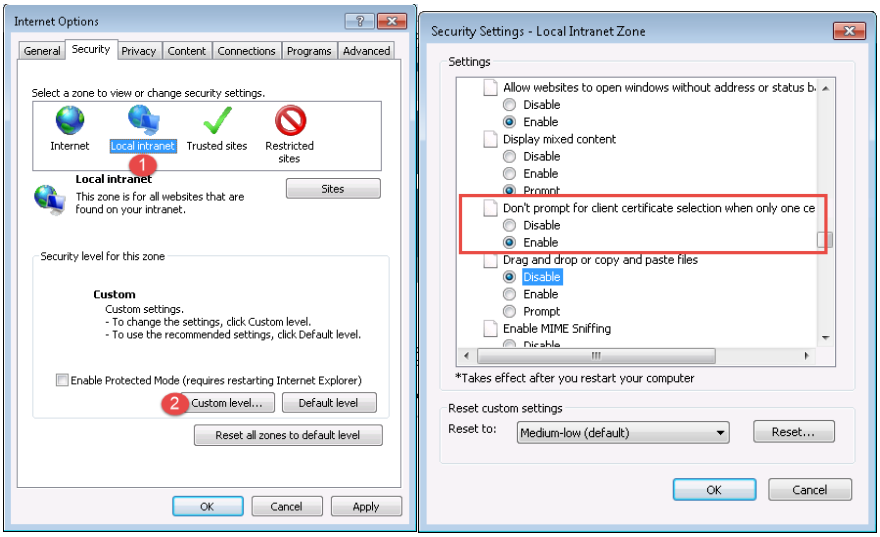
Configure MS Internet Explorer to use the user certificate for authentication

Internet Explorer is using the certificate storage in Windows so once you finish the certificate enrolment IE can start using it.

If you want to verify that the certificate-based authentication is active, perform the following instructions:

1. Open the **Internet options** dialog and choose the **Security** tab.
2. Click **Local intranet** and click **Custom level**.
3. Scroll down to the **Miscellaneous** section and make sure that **Don't prompt for client certificate selection when only one certificate exists** is set to **Disable**.
4. Click **OK**, **Yes**, and then **OK** again to continue.

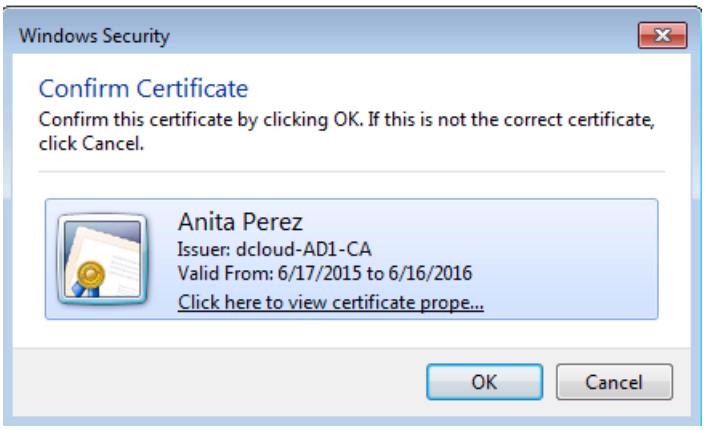
Figure 66. Internet Options



Verify operation of Certificate based authentication

1. Close Internet Explorer and reopen it. Navigate to the Cisco Unified Communications Manager Self Care Portal.
2. You should see a Confirm Certificate window pop up. Click OK and then notice you will not have to login as before.

Figure 67. Confirm Certificate



3. Open Cisco Jabber from the desktop shortcut.

4. You can see that Jabber will not ask for a username or password.
5. At this point, Jabber will be fully authenticated.
6. You can **Exit** from Jabber.

Congratulations! You have completed all lab activities.

Appendix A: SSO and LDAP Functions on Cisco UC Systems

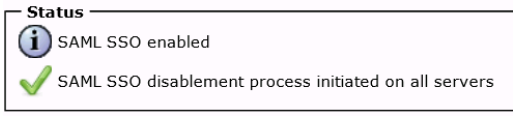
NOTE: These steps are for reference ONLY for when you run this in a production environment. You do not need to complete these in the lab.

Disable SSO on Cisco Unified CM

1. Open a browser and open the UCM Management Console at https://cucm1.dcloud.cisco.com.
2. Click on **Recovery URL to bypass Single Sign On (SSO)**.
3. Login as Username: **admin** and Password: **C1sco12345**.
4. Go to **System** menu > **SAML Single Sign-On**.
5. Click on **Disable SAML SSO**.
6. Click on **Continue**.
7. After clicking Continue, Cisco Tomcat will restart, please allow a couple of minutes to this task.

NOTE: Disabling SSO on Cisco UCM it will disable for all nodes in that cluster (including IM&P nodes).

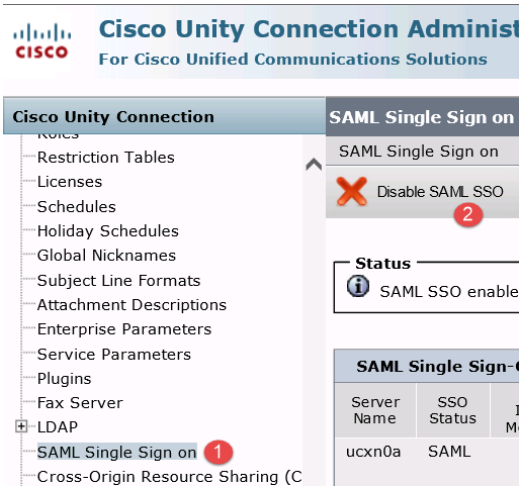
Figure 68. SAML SSO Disablement



Disable SSO on Unity Connection

1. Open a browser and open the Unity Connection Management Console at https://cuc1.dcloud.cisco.com.
2. Click on **Recovery URL to bypass Single Sign On (SSO)**.
3. Authenticate with User Name: **administrator** and Password: **C1sco12345**.
4. On the right navigation pane, click **SAML Single Sign-On**.
5. Click on **Disable SAML SSO** once the page loads.

Figure 69. Disable SAML SSO



6. Click **Continue**.

7. After clicking Continue, Cisco Tomcat will restart, please allow a couple of minutes to this task.

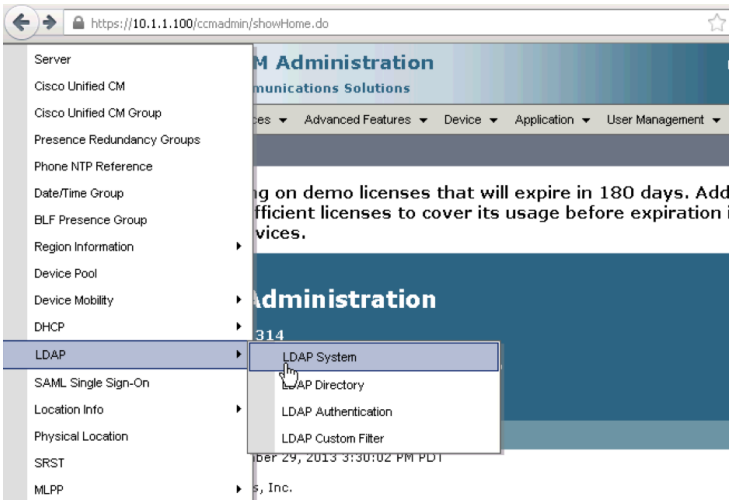
Setting up Unified CM to Synchronize with LDAP

1. Open Firefox and navigate to Collaboration Server Links > Cisco Unified Communications Manager and click the **Cisco Unified Communication Manager** link.

2. Login as **administrator** with password **C1sco12345**.

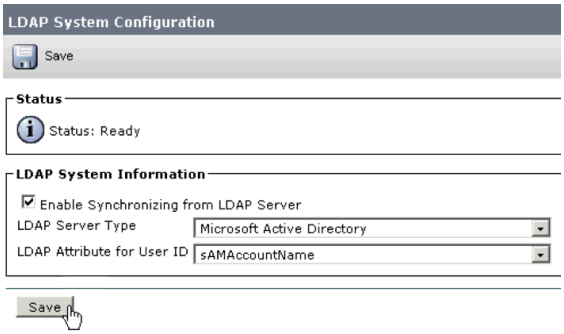
3. Click **System** > **LDAP** > **LDAP system**.

Figure 70. LDAP Menu



4. Check the box next to **Enable Synchronizing from LDAP Server** and click **Save**.

Figure 71. Enble Sync from LDAP Server



5. Click **System** > **LDAP** > **LDAP directory**.

6. Click **Add New**.

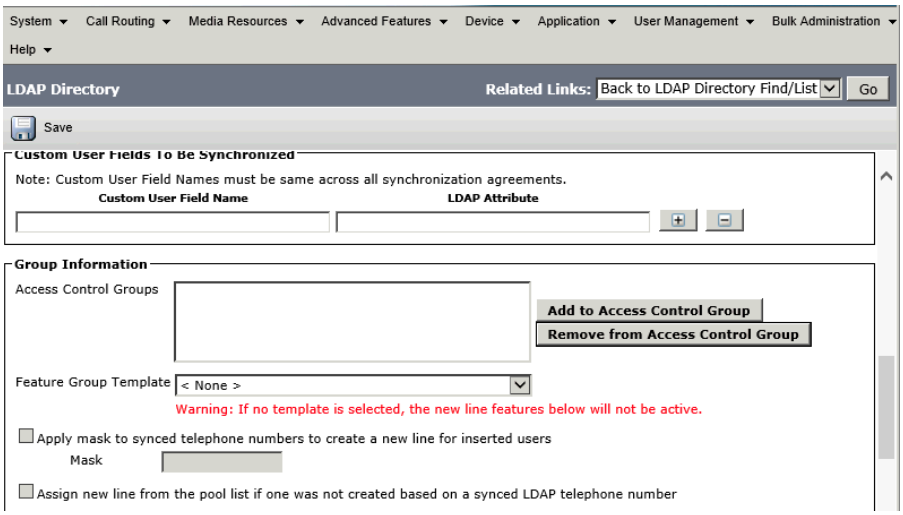
7. Enter the following LDAP information:

Table 7. LDAP Configuration

Setting	Input
LDAP Configuration Name	**ad1**
LDAP Manager Distinguished Name	**cn=administrator,cn=users,dc=dcloud,dc=cisco,dc=com**
LDAP Password	**C1sco12345**
Confirm Password	**C1sco12345**
LDAP User Search Base	**ou=id users, dc=dcloud, dc=cisco, dc=com**

8. Under **Group Information** click **Add to Access Control Group** and then click **Find**.

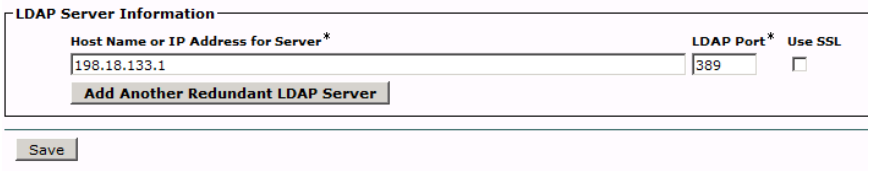
Figure 72. Add to Access Control Group



9. Check the boxes next to **Standard CCM End Users** and **Standard CTI Enabled** and then click **Add Selected**.

10. Scroll down to **LDAP Server Information** and add the IP address of AD as **198.18.133.1** and LDAP port as **389** and then click **Save**.

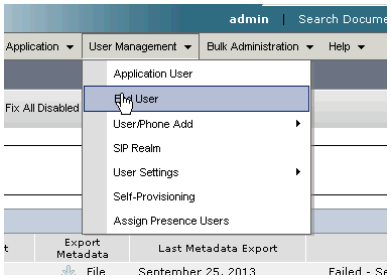
Figure 73. LDAP Server Information



11. Click **Perform Full Sync Now** and then **OK**.

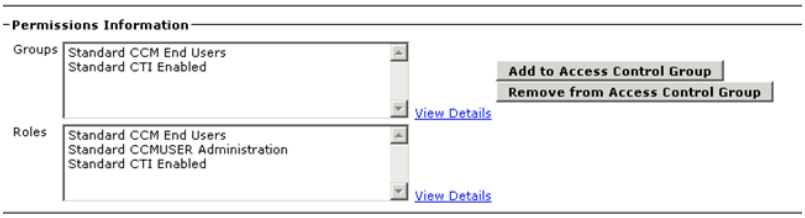
12. Navigate to **User Management** > **End User**, click **Find** and then click the **amckenzie** link to open his profile.

Figure 74. End user profile



13. Scroll down to the **Permissions Information** section and click **Add to Access Control Group**.

Figure 75. Permissions Information



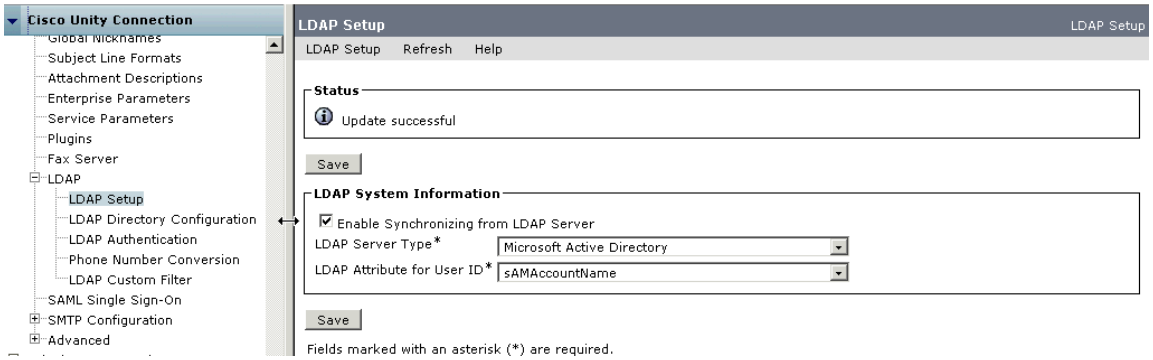
14. Check the box next to **Standard CCM Super Users** and click **Add Selected**. Click **Save**.

Performing LDAP Sync on Cisco Unity Connection

1. Scroll down to **LDAP** and click **LDAP Setup**.

2. Check **Enable Synchronizing from LDAP Server** and click **Save**.

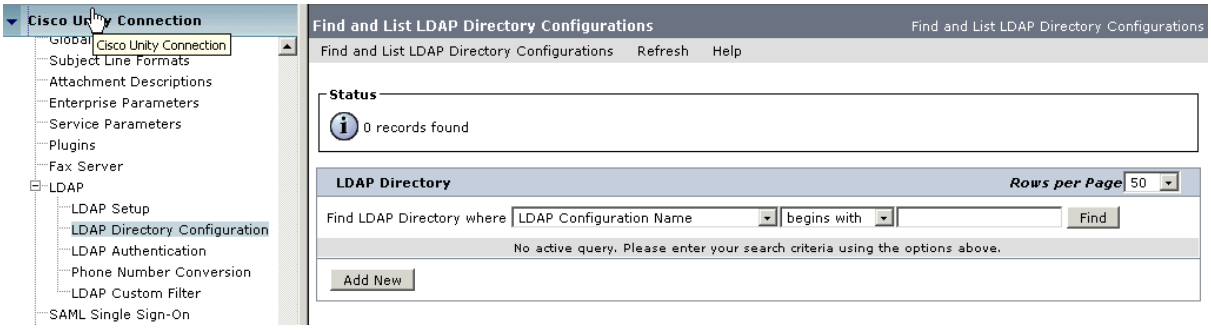
Figure 76. LDAP Setup



3. Click **LDAP** > **LDAP Directory Configuration**.

4. Click **Add New**.

Figure 77. Directory Configuration



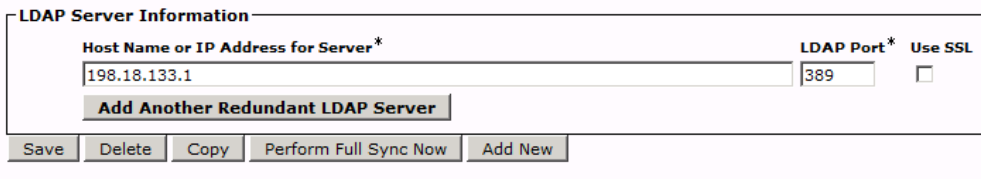
5. Populate the following LDAP information.

Table 8. LDAP Configuration

Setting	Input
LDAP Configuration Name	**ad1**
LDAP Manager Distinguished Name	**cn=administrator,cn=Users,dc=dcloud,dc=cisco,dc=com**
LDAP Password	**C1sco12345**
Confirm Password	**C1sco12345**
LDAP User Search Base	**ou=id users, dc=dcloud, dc=cisco, dc=com**

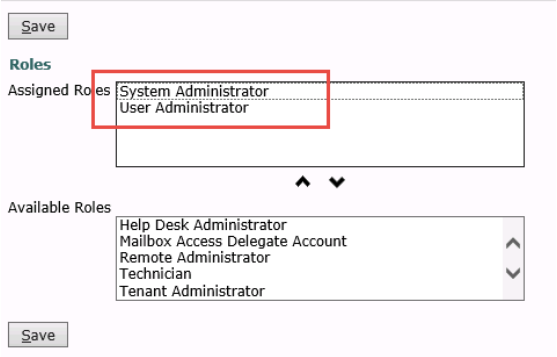
6. Scroll down to **LDAP Server Information** add the IP address of the Active Directory server (198.18.133.1).

Figure 78. AD Server Address



7. Click **Save** and then click **Perform Full Sync Now**. Click **OK**
8. Navigate to **Users** > **Import Users**. Under **Find** choose **LDAP Directory** in the drop down menu for **Find End Users In**. Click the **Find** button.
9. Under **Import With** choose **voicemailusertemplate** for **Based on Template**.
10. Click **Import All and then OK**.
11. Wait for the users to synchronize and then go to **Users** > **Users menu**.
12. Click on **Find**.
13. Click the **aperez** link.
14. Navigate to **Edit** > **Roles**.
15. Using the up arrow [^] assign the roles **System Administrator** and **User Administrator** and click **Save**.

Figure 79. Assign Roles



Appendix B: Troubleshooting

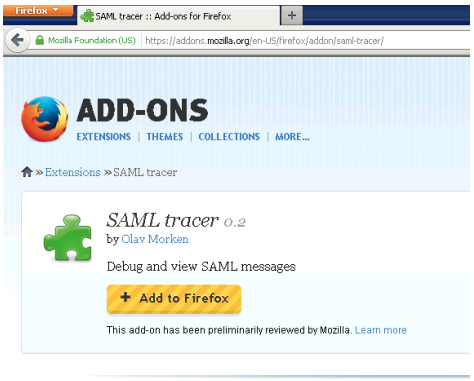
Troubleshooting SAML Messages

As with most labs, you might need to verify that WebEx Meeting and the IdP (PingFederate in this case) are exchanging the right information.

One tool that can be used is called SAML Tracer, a free add-on to Firefox.

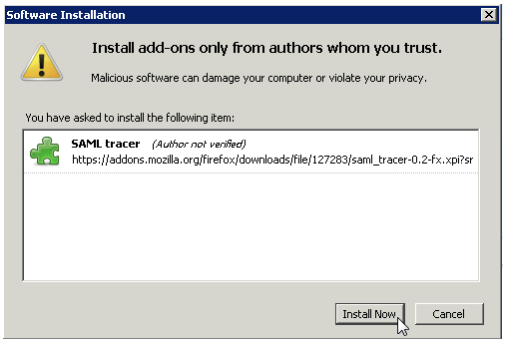
1. Download this application from https://addons.mozilla.org/en-US/firefox/addon/saml-tracer/.
2. Click on **Add to FireFox**.

Figure 80. SAML Tracer FF Add-on



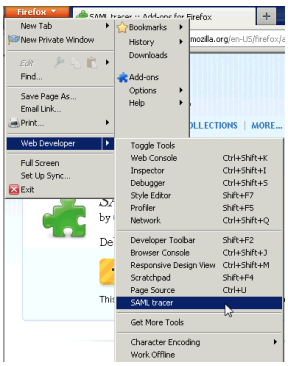
3. Click on **Install Now** and then **Restart Now**.

Figure 81. Software Wizard



4. You can start SAML tracer by going to **Firefox** > **Web Developer** > **SAML Tracer**.

Figure 82. SAML Tracer

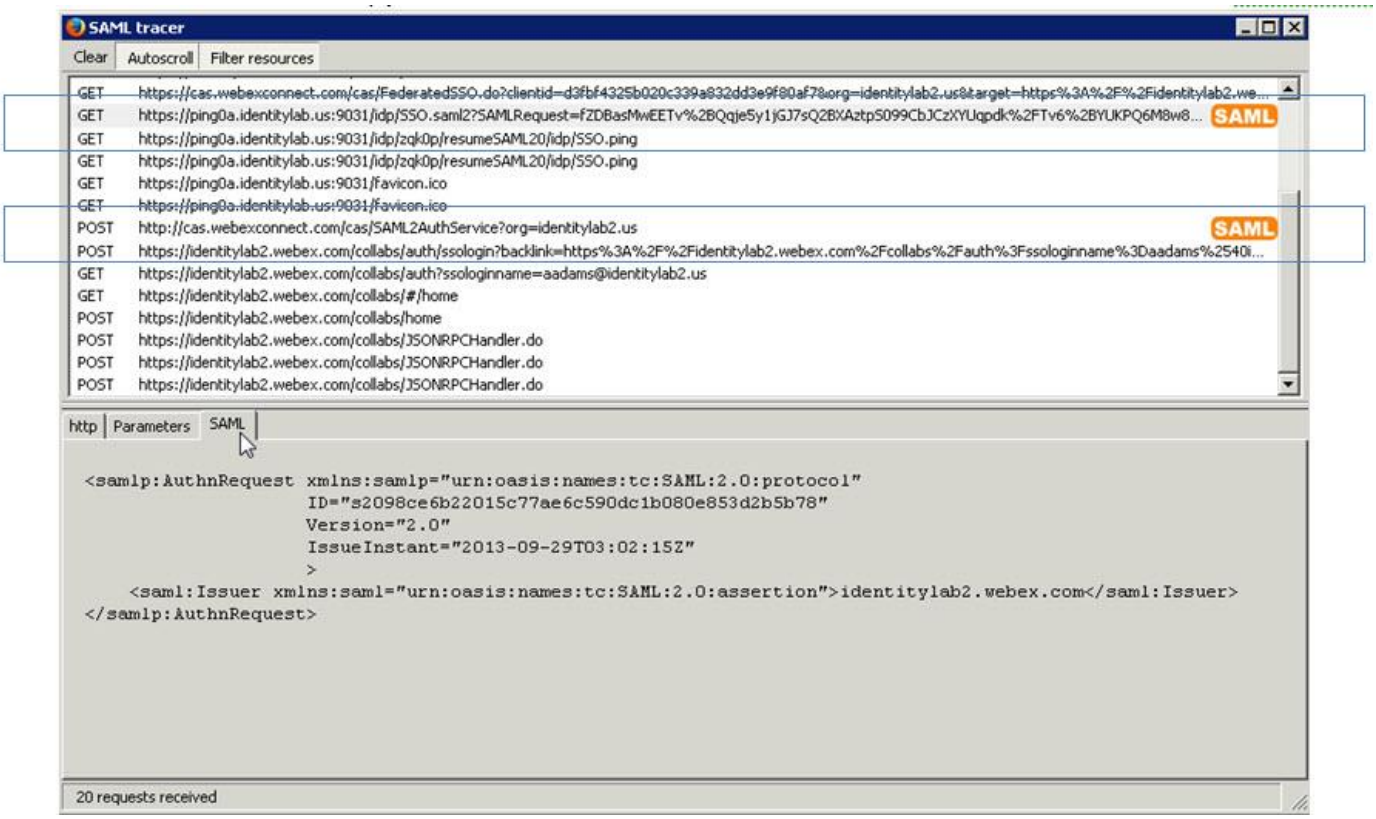


5. Keep this running in the background and then point your browser to a web enabled SSO service, for example Cisco UCM Self-Care portal.

6. Login using the account aperez@dcloud.cisco.com.

7. Check on SAML Tracer, you should see two SAML entries listed. These are GET and POST entries.

Figure 83. SAML Tracer Entries



8. In the verbose section, you should see the SAML exchange, such as the following:

```
<samlp:AuthnRequest xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"

                    ID="s2098ce6b22015c77ae6c590dc1b080e853d2b5b78"
```

```
                    Version="2.0"
                    IssueInstant="2013-09-29T03:02:15Z"
                    >
    <saml:Issuer
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">dcloud.cisco.webex.com</saml:Issuer>
</samlp:AuthnRequest>
```

9. You can see the assertion and the IDP SP web site (dcloud.cisco.webex.com).
10. If you click on the second SAML statement and select SAML in the verbose, you should see the following:

```
<samlp:Response Version="2.0"
                ID="aVETGdhw0f6PYKMyw0TOO4i0cLq"
                IssueInstant="2013-09-29T03:02:14.608Z"
                InResponseTo="s2098ce6b22015c77ae6c590dc1b080e853d2b5b78"
                xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
                >
    <saml:Issuer
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">ping1.dcloud.cisco.com</saml:Issuer>
    <samlp:Status>
        <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success" />
```

11. You should see that the exchange was successful. You will also see the exchange of the SAML attributes such as First Name, Last Name, email and UID. An example of e-mail is given below:

```
<saml:Attribute Name="email"
                            NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
                            >
                <saml:AttributeValue xsi:type="xs:string"
                                     xmlns:xs="http://www.w3.org/2001/XMLSchema"
                                     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
                                     >bbanks@dcloud.cisco.com</saml:AttributeValue>
            </saml:Attribute>
```

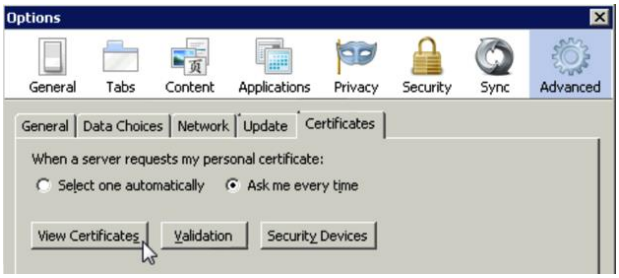
With SAML Tracer, you should be able to see if the SAML messages in line with your configuration in this case. If you do not see these, then you can go back to your IdP and WebEx configuration to see why this exchange is not taking place.

Configure Firefox to use the user certificate for authentication

Now this user certificate needs to be imported into Firefox so that Firefox can use this certificate for certificate-based authentication.

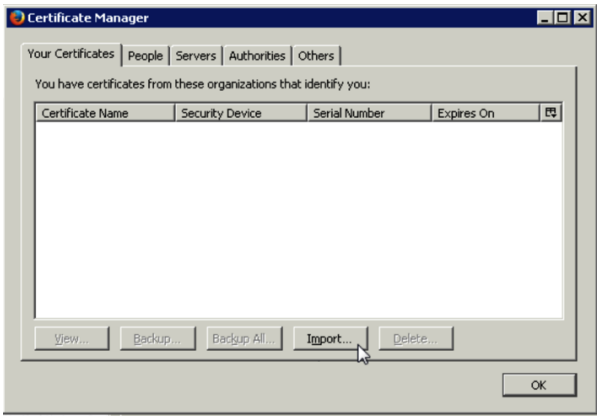
1. In the advanced Firefox options, click **View certificates** to open the **Firefox Certificate Manager**.

Figure 84. Certificate Manager



2. Click **Import**.

Figure 85. Import Certificate

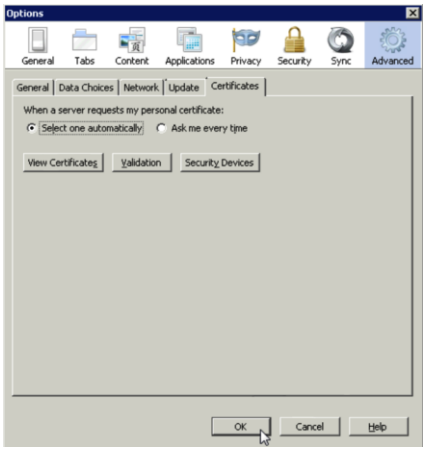


3. Click the certificate file on your Desktop (**aperez**) and enter the password for that user (**C1sco12345**).
4. The imported certificate now shows up in the **Your Certificates** tab. Click **Ok** to close the Certificate Manager.

Figure 86. Certificate Manager

5. Enable **Select one automatically** and click **Ok** to close the options dialog.

Figure 87. Certificates Tab



Appendix C: IdP Installations

NOTE: This chapter is for your reference only, everything has been already done for you, just read it and use it in future deployments, nothing need to be done in the Identity LAB, we already put this work in the master images.

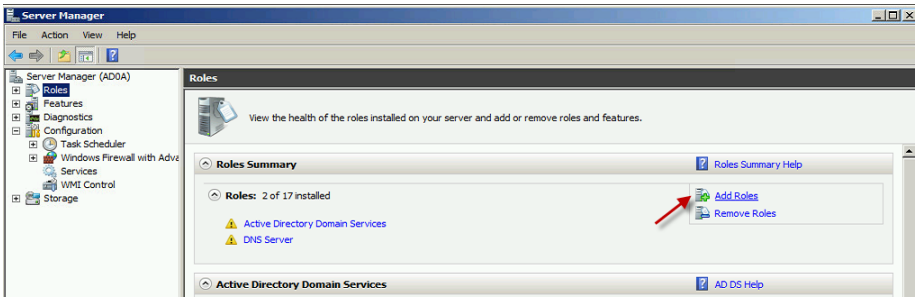
How to install Microsoft AD FS2.0

After having installed a Windows 2008 R2 Server with DNS role, you need to promote the server to Domain Controller (Deploy Active Directory).

The next task will be installing Microsoft Certificate Services.

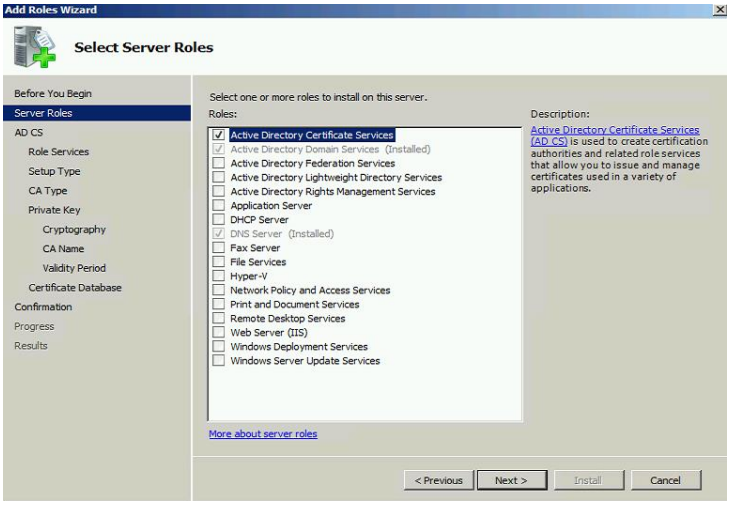
1. Go to **Server Manager** and in **Roles** click **Add Roles**.

Figure 88. Server Manager



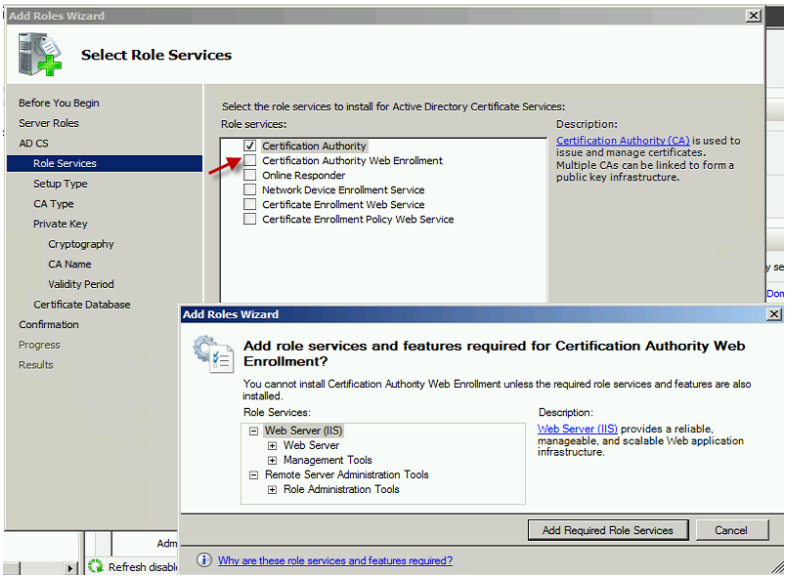
2. Click the box for the **Active Directory Certificate Services Role**. Click **Next**.

Figure 89. AD Certificate Services Role



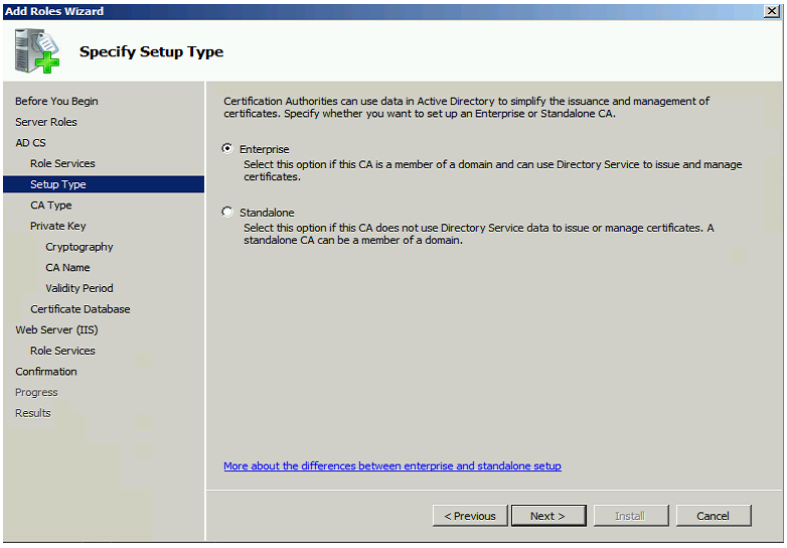
3. You have the option to deploy additional services. Deploy the services **Certificate Authority** and **Certificate Authority Web Enrollment**, at that time another Wizard will start to add extra Roles for IIS.

Figure 90. Additional Services



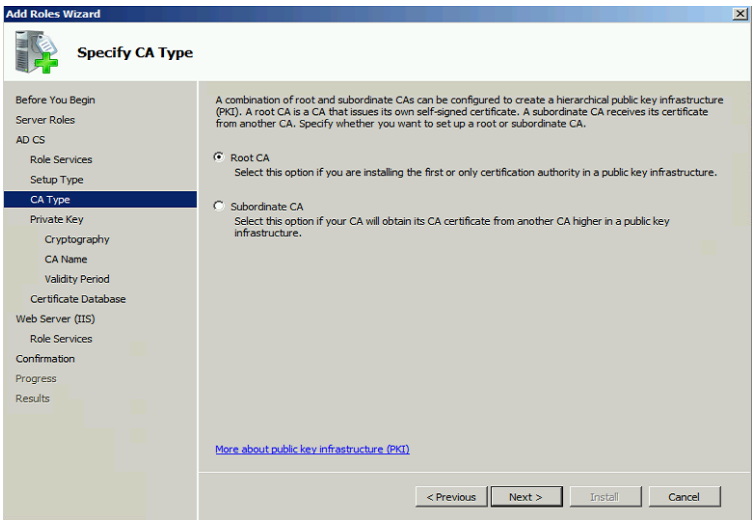
4. For the setup type, you choose **Enterprise**, it should be what you see in most of our customer, but it makes no difference for our specific deployment, could even be Standalone CA. Click **Next**.

Figure 91. Setup Type



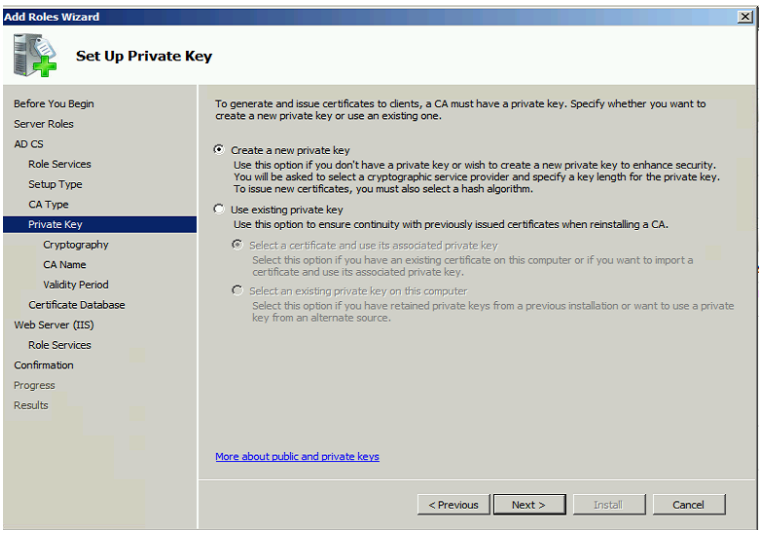
5. For the CA Type you choose **Root CA**, since you do not have other CA already running in our organization.

Figure 92. CA Type



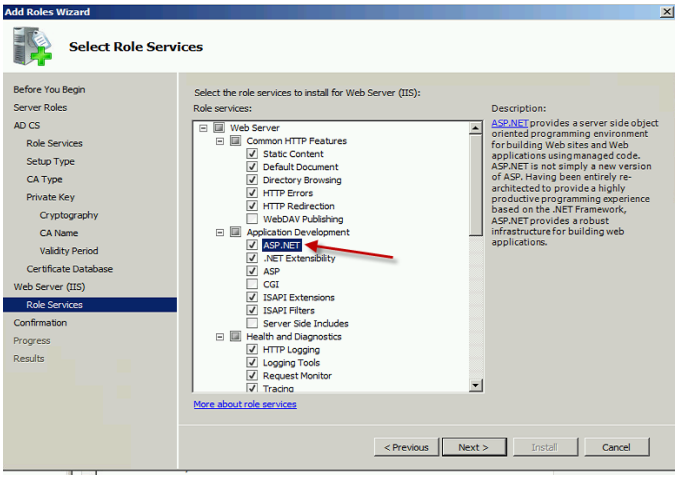
6. The next step will be to create the private key for your CA. Choose this option and click **Next**.

Figure 93. Private Key



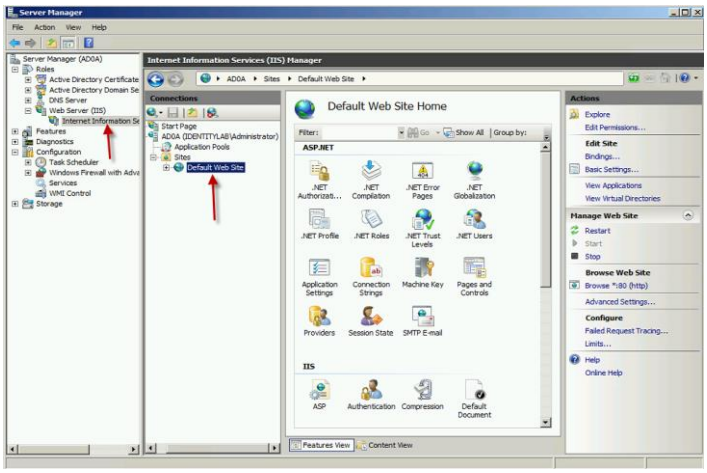
7. After configuring the CA, you need to configure the Sole Services for IIS, since it is necessary for the Web Enrolment of the CA. For our ADFS deployment you will need an extra Role in IIS, click on **ASP.NET** under **Application Development**.

Figure 94. Add Role



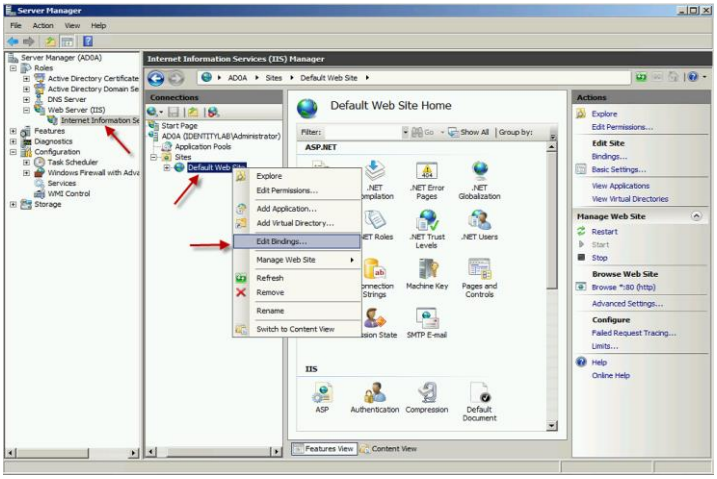
8. In the Server Manager click on **Web Server** > **IIS**, and then right click on **Default Web Site**. You need to change the Binding to allow HTTPS along with HTTP.

Figure 95. Server Manager



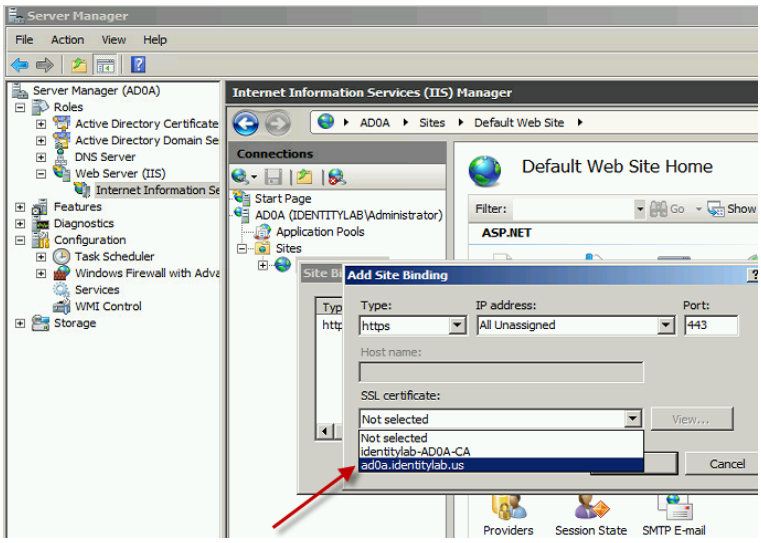
9. After you right-click, you need to choose **Edit Bindings**.

Figure 96. Edit Bindings



10. Add a new **Site Bindings** and choose **https** as the type. Choose for SSL certificate the server certificate that should have the same FQDN as your Ad1 server (ad1.cloud.cisco.com).

Figure 97. Adding HTTPS to Bindings

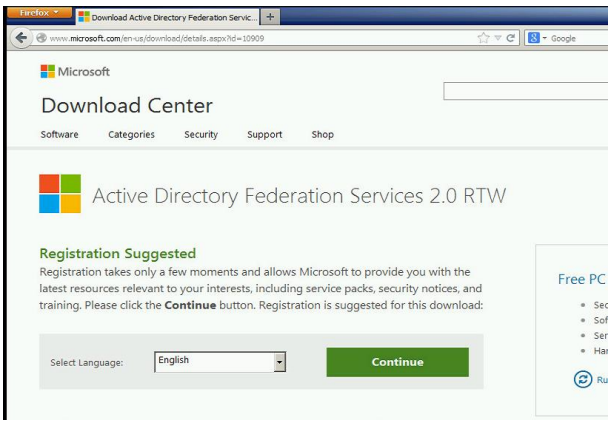


Everything is done from platform perspective now you need to install ADFS2. In the roles that you have in the server manager you will see ADFS but that version is version 1 that does not provide SAML.

Therefore, you need to go on the web to get ADFS2.

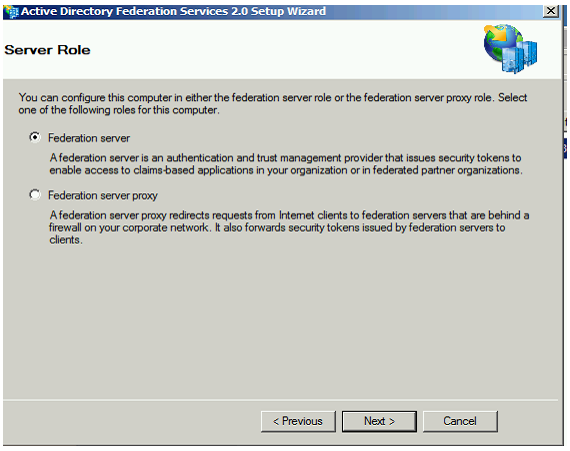
11. Go to the link http://www.microsoft.com/en-us/download/details.aspx?id=10909 Set the language and click the **Continue** button.

Figure 98. Download Center



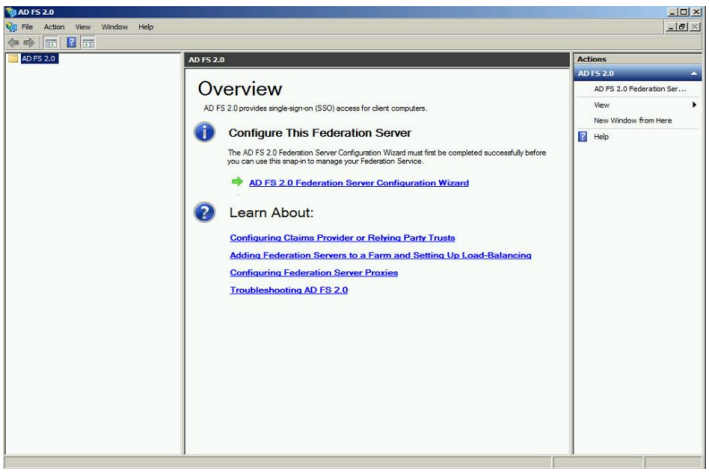
12. Choose the correct version for your OS. In our case, it is the first check box for **Windows 2008 R2**. Click **Download**.
13. Double-click on the **AdfsSetup.exe** file that you downloaded.
14. For the Server Role choose the **Federation Server**, since you are installing the IdP to be inside the customer network in the private LAN. Click **Next**.

Figure 99. Server Role



15. The product is installed and you can open it from the taskbar or start menu.

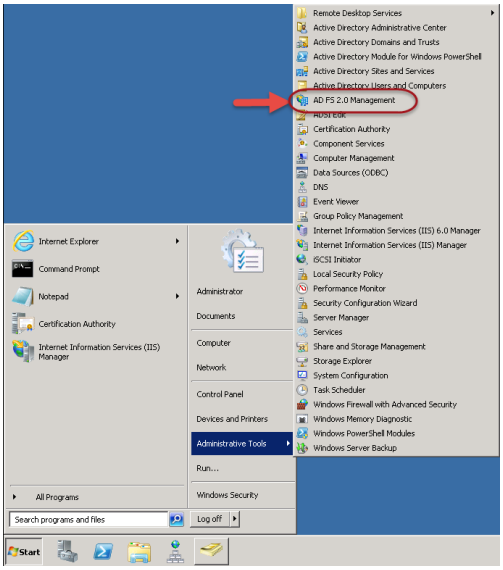
Figure 100. AD FS 2.0



ADFS 2.0 initial configuration

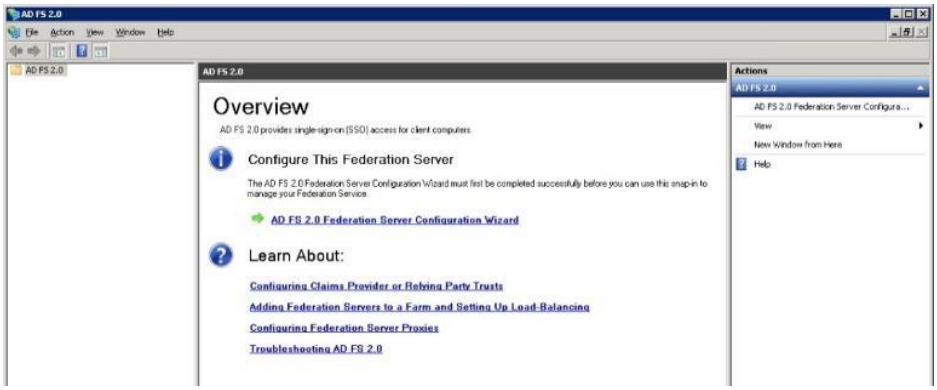
1. Launch the ADFS Management console. You may need to perform a search from the start menu if not listed. **Start** > **Administrative Tools** > **AD FS 2.0 Management** is the typical path.

Figure 101. AD FS 2.0 Management



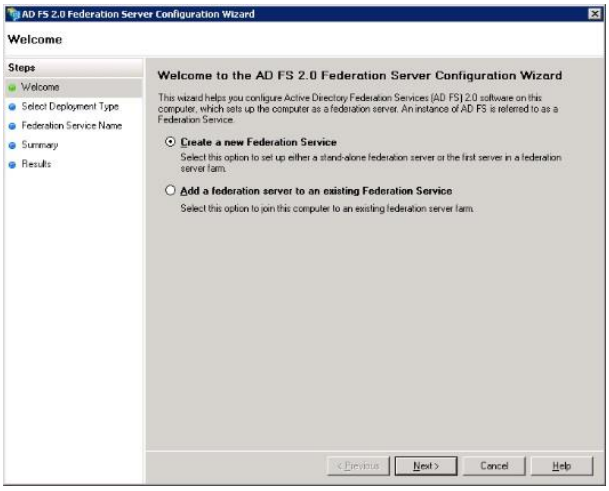
2. Click the **AD FS 2.0 Federation Server Configuration Wizard** option to start your ADFS server configuration.

Figure 102. AD FS 2.0 Configuration Wizard



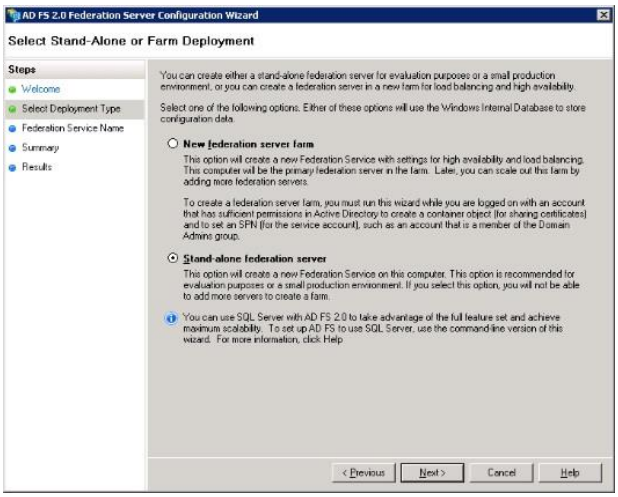
3. Choose **Create a new Federation Service** and click **Next**.

Figure 103. Create a New Federation Service



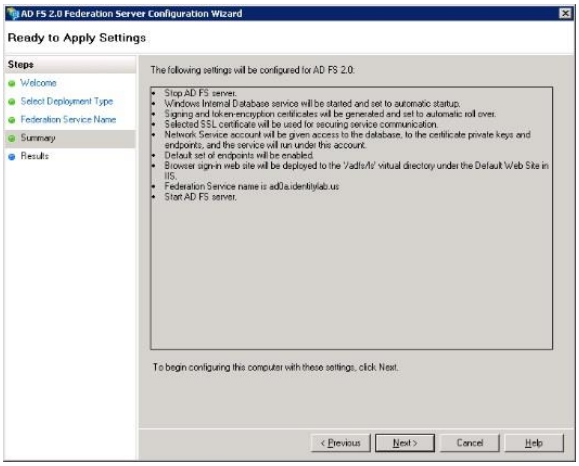
4. Choose **Stand-alone Federation Server** and click **Next**.

Figure 104. Stand-alone Federation Server



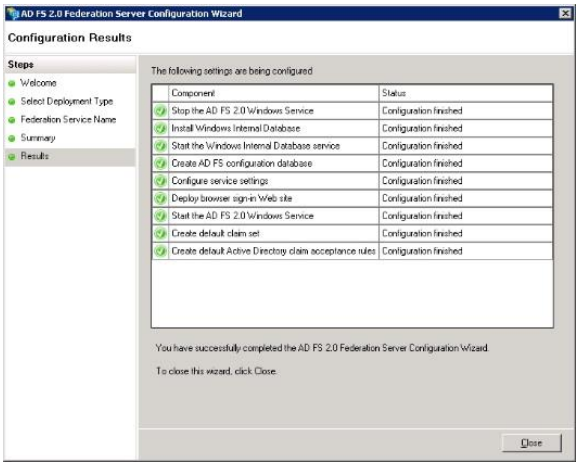
6. Under SSL certificate, choose the **ad1.dcloud.cisco.com** certificate from the list. The Federation Service name will auto-populate. Click **Next**.

Figure 105. SSL Certificate



7. Review the settings and click **Next** to apply the settings.

Figure 106. Settings Summary



8. Confirm all the components have completed **successfully** and click **Close** to end the wizard and return to the main management console. This may take a few minutes.

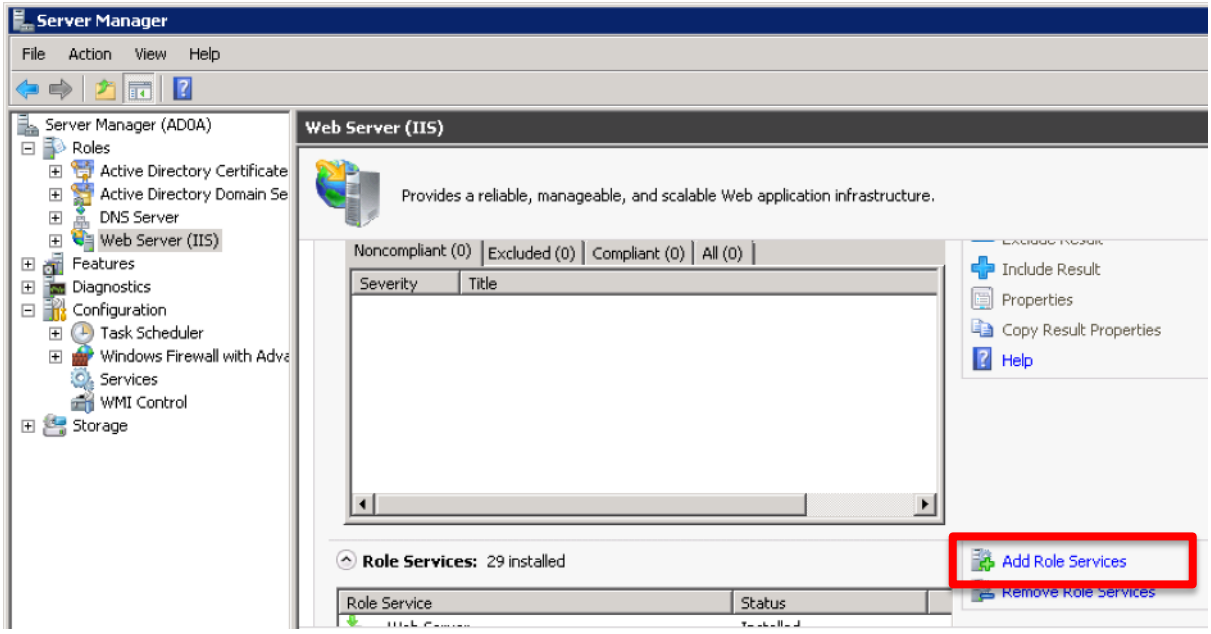
9. ADFS is now effectively enabled and configured as an Identity Provider (IdP). Next, you need to add Cisco UCM as a trusted Relying partner. Before you can to this, you need to do some configuration over in Cisco UCM Administration.

Setting up Certificates Services on the Active Directory Server

1. Re-open the Remote Desktop Connection to **ad1.dcloud.cisco.com**.

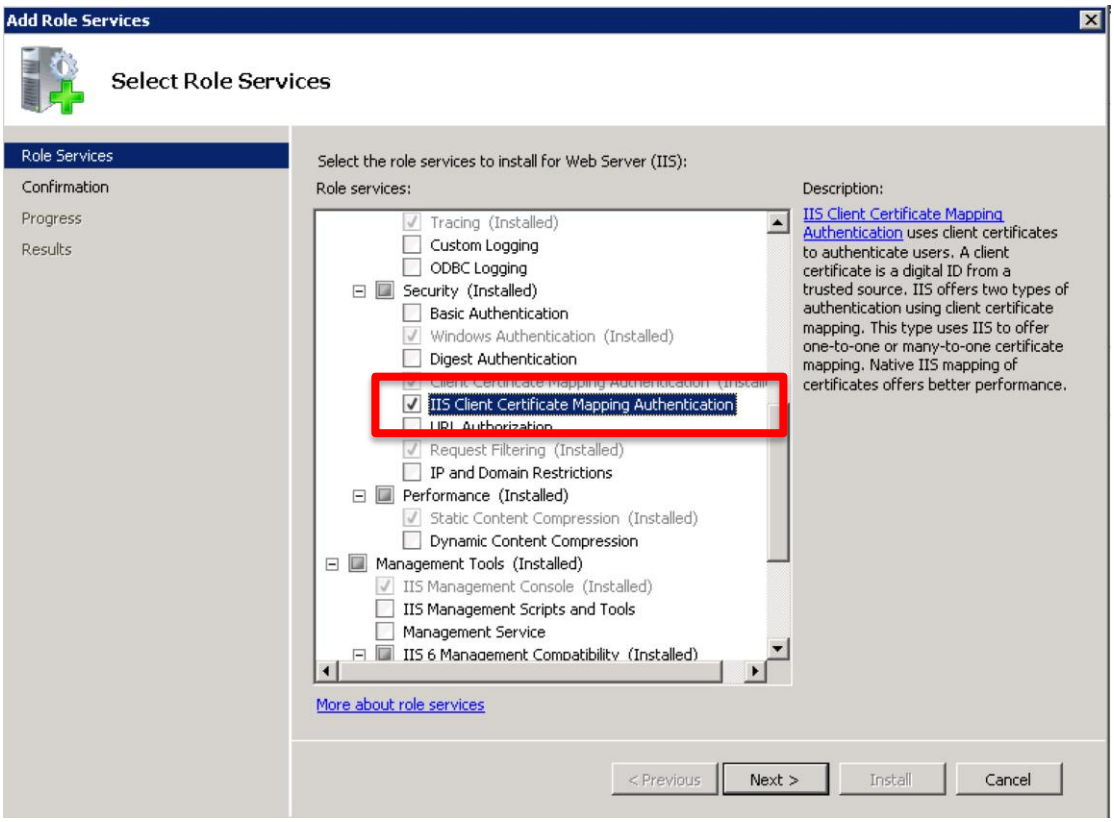
2. Open **Server Manager** and expand **Roles** > **Web Server(IIS)**. Click **Add Role Services**.

Figure 107. Server Manager



3. Click **Security** > **IIS Client Certificate Mapping Authentication**, press **Next** and let it install.

Figure 108. Certificate Mapping Authentication



Appendix D: Use CA signed certificates on Cisco UC

The lab environment has a number of other webservers (Communications Manager, Unity Connection) that all use self-signed certificates. You might want to also configure these servers to also use CA signed certificates.

Use the following Hints as your guide:

- On VOS platforms certificate management is done in the **Cisco Unified Operating System Administration** GUI
- The CA certificate needs to be uploaded to **tomcat-trust**
- The web server CSR has to be created as a **tomcat certificate**
- The CSR response has to be uploaded as a **tomcat certificate**
- You need to restart Tomcat so that Tomcat picks up the new certificate. This can only be done on the CLI by issuing the command **utils service restart Cisco Tomcat**

THIS IS OPTIONAL and not required for certificate based SAML SSO to work. However, it is recommended as best practice.