Unity Connection Version 10.5 SAML SSO Configuration Example

Contents

Introduction

This document describes how to configure and verify Security Assertion Markup Language (SAML) Single Sign-on (SSO) for Cisco Unity Connection (UCXN).

Prerequisites

Requirements

Network Time Protocol (NTP) Setup

For SAML SSO to work, you must install the correct NTP setup and make sure that the time difference between the Identity Provider (IdP) and the Unified Communications applications does not exceed three seconds. For information about synchronizing clocks, see the NTP Settings section in Cisco Unified Communications Operating System Administration Guide.

Domain Name Server (DNS) Setup

Unified Communications applications can use DNS in order to resolve Fully Qualified Domain Names (FQDNs) to IP addresses. The Service Providers and the IdP must be resolvable by the browser.

Active Directory Federation Service (AD FS) Version 2.0 must be installed and configured in order to handle SAML requests.

Components Used

The information in this document is based on these software and hardware versions:

- AD FS Version 2.0 as IdP
- UCXN as Service Provider
- Microsoft Internet Explorer Version 10

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Background Information

SAML is an XML-based, open-standard data format for data exchange. It is an authentication protocol used by Service Providers in order to authenticate a user. The security authentication information is passed between an IdP and the Service Provider.

SAML is an open standard that enables clients to authenticate against any SAML-enabled collaboration (or Unified Communication) service regardless of the client platform.

All Cisco Unified Communication web interfaces, such as Cisco Unified Communications Manager (CUCM) or UCXN, use SAML Version 2.0 protocol in the SAML SSO feature. In order to authenticate the Lightweight Directory Access Protocol (LDAP) user, UCXN delegates an authentication request to the IdP. This authentication request generated by the UCXN is an SAML Request. The IdP authenticates and returns an SAML Assertion. The SAML Assertion shows either Yes (authenticated) or No (authentication failed).

SAML SSO allows a LDAP user to log into client applications with a username and password that authenticates on the IdP. A user sign-in to any of the supported web applications on Unified Communication products, after you enable the SAML SSO feature, also gains access to these web applications on UCXN (apart from CUCM and CUCM IM and Presence):

Unity Connection users	Web applications
LDAP users with administrator rights	• UCXN Administration • Cisco UCXN Serviceability • Cisco Unified Serviceability • Cisco Personal Communications Assistant • Web Inbox • Mini Web Inbox (desktop version)
LDAP users without administrator rights	• Cisco Personal Communications Assistant • Web Inbox • Mini Web Inbox (desktop version) • Cisco Jabber Clients

Configure

Network Diagram

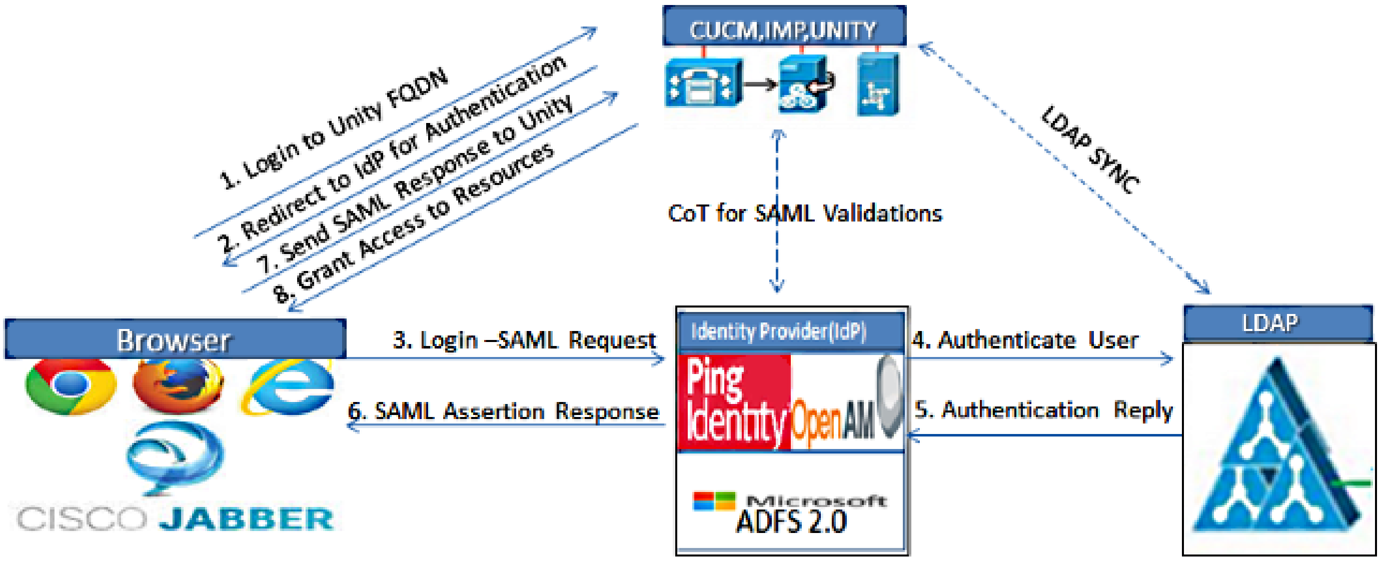
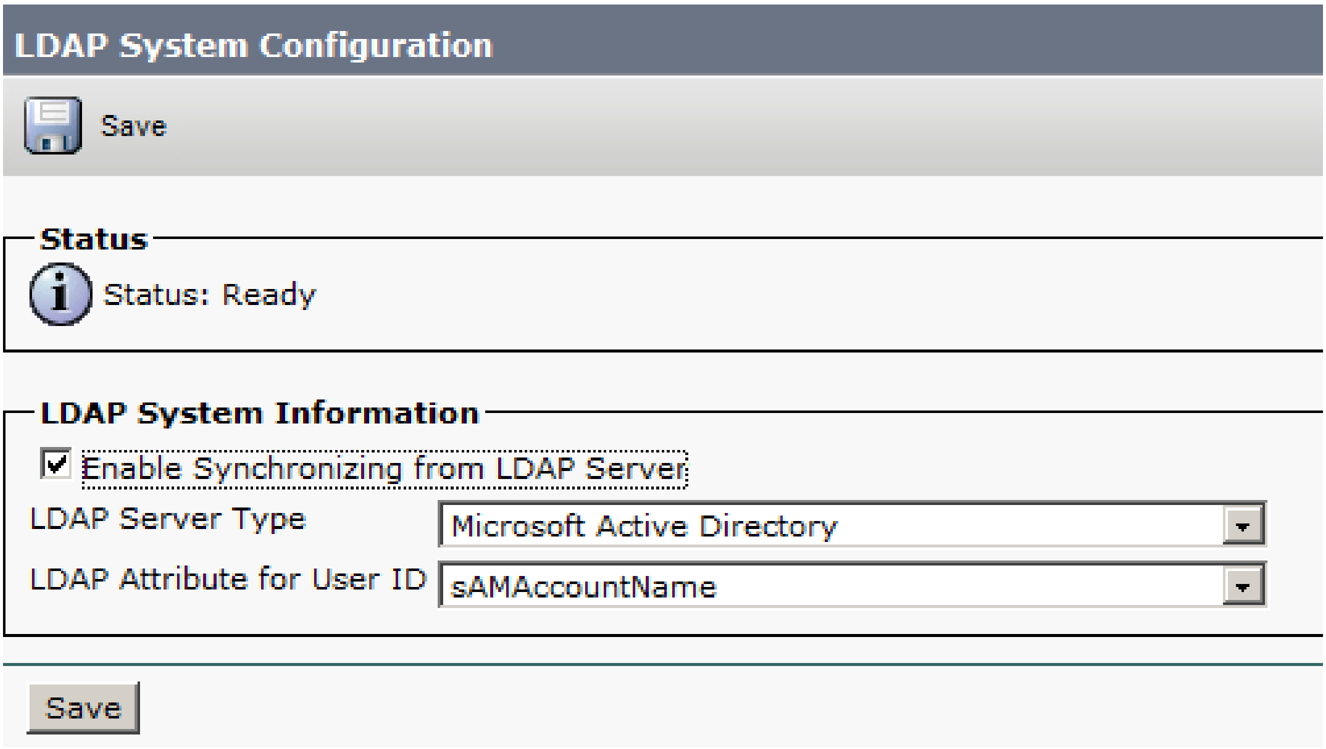


Figure :SAML Single sign SSO Call Flow for Collaboration Servers

Directory Setup

1. Sign into the UCXN Administration Page and select **LDAP** and click **LDAP Setup**.

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



LDAP System Configuration

Status

Status: Ready

LDAP System Information

☑ Enable Synchronizing from LDAP Server

LDAP Server Type: Microsoft Active Directory

LDAP Attribute for User ID: sAMAccountName

3. Click **LDAP**.

4. Click **LDAP Directory Configuration**.

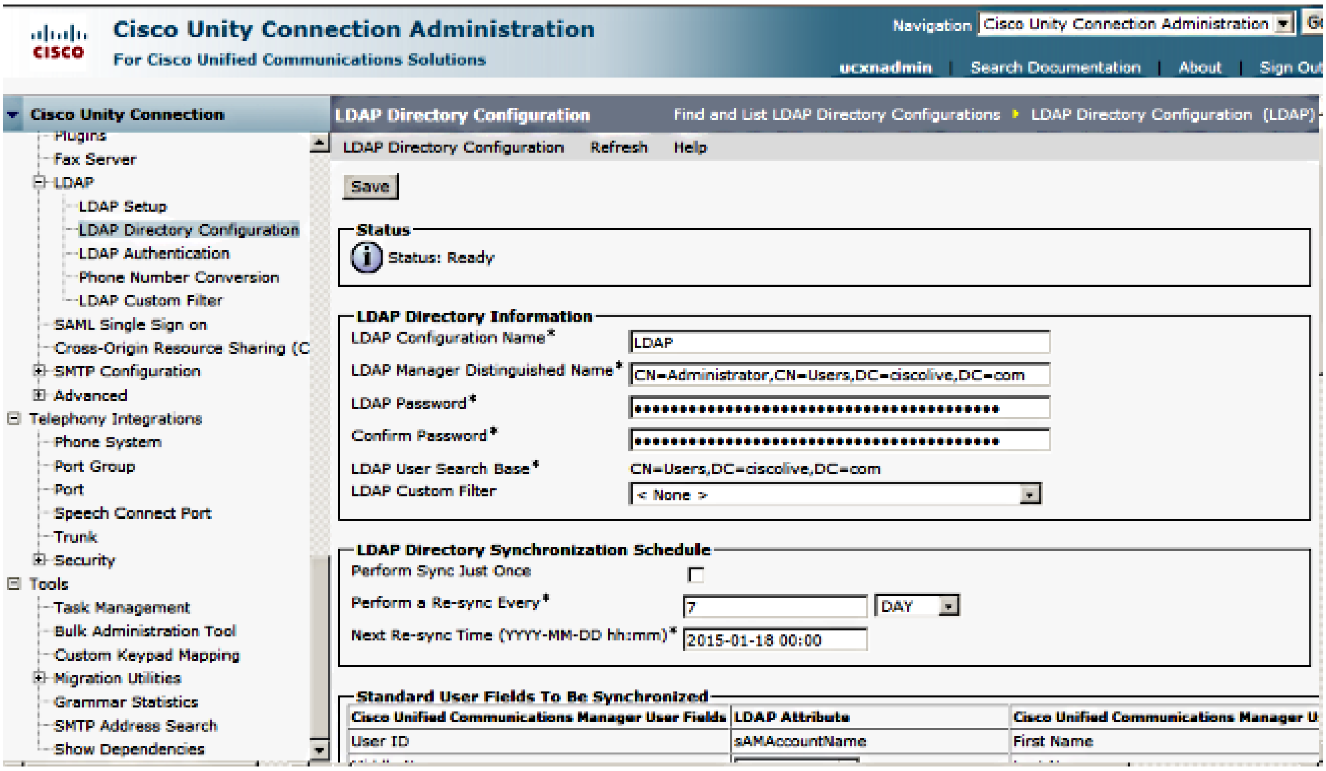
5. Click **Add New**.

6. Configure these items:

   LDAP directory account settingsUser attributes to be synchronizedSynchronization scheduleLDAP server Hostname or IP address and port number

7. Check **Use SSL** if you want to use Secure Socket Layer (SSL) in order to communicate with the LDAP directory.

   Tip: If you configure LDAP over SSL, upload the LDAP directory certificate onto CUCM. Refer to the LDAP directory content in the Cisco Unified Communications Manager SRND for information about the account synchronization mechanism for specific LDAP products and general best practices for LDAP synchronization.



Status

Status: Ready

LDAP Directory Information

LDAP Configuration Name*	LDAP
LDAP Manager Distinguished Name*	CN=Administrator,CN=Users,DC=ciscolive,DC=com
LDAP Password*	••
Confirm Password*	••
LDAP User Search Base*	CN=Users,DC=ciscolive,DC=com
LDAP Custom Filter	< None >

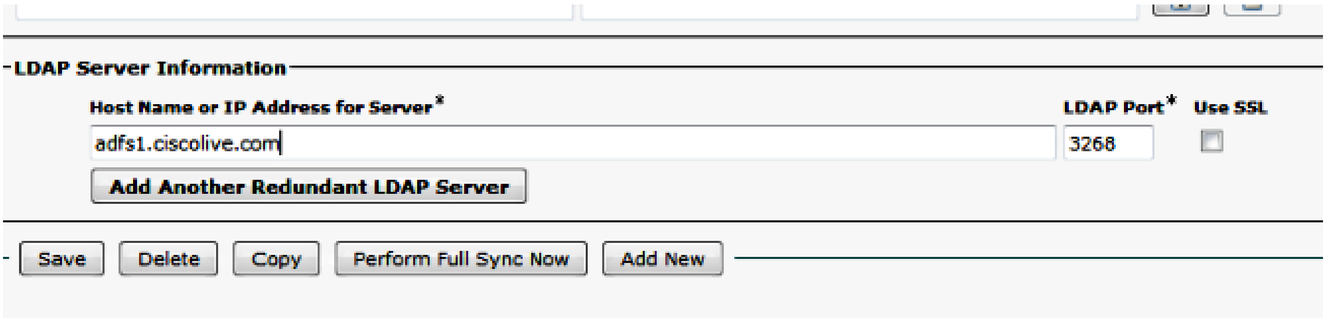
LDAP Directory Synchronization Schedule

Perform Sync Just Once	□
Perform a Re-sync Every*	7 DAY
Next Re-sync Time (YYYY-MM-DD hh:mm)*	2015-01-18 00:00

Standard User Fields To Be Synchronized

Cisco Unified Communications Manager User Fields	LDAP Attribute	Cisco Unified Communications Manager U
User ID	sAMAccountName	First Name

8. Click **Perform Full Sync Now**.



LDAP Server Information

Host Name or IP Address for Server*	LDAP Port*	Use SSL
adfs1.ciscolive.com	3268	□

Note: Make sure **Cisco DirSync** service is enabled in the Serviceability web page before you click Save.

9. Expand **Users** and select **Import Users**.

10. In the **Find Unified Communications Manager End Users** list, select **LDAP Directory**.

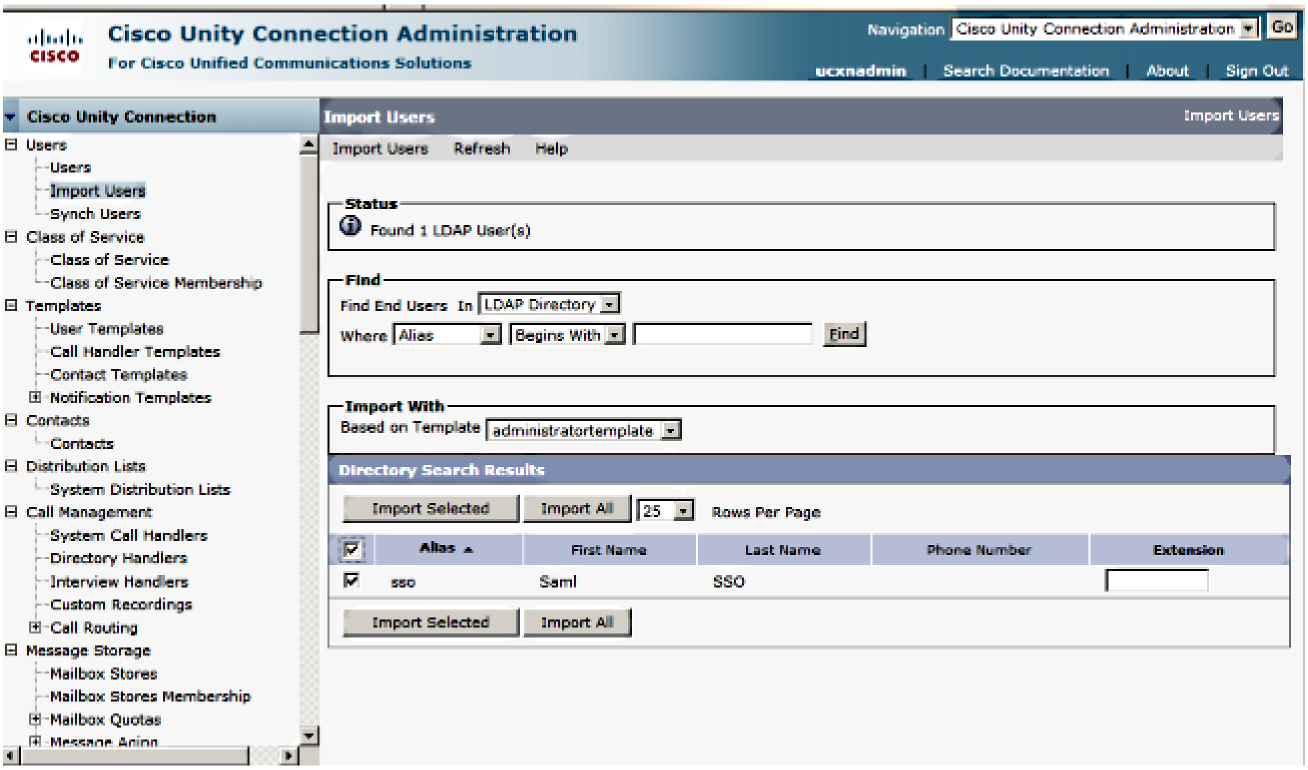
11. If you want to import only a subset of the users in the LDAP directory with which you have integrated UCXN, enter the applicable specifications in the search fields.

12. Select **Find**.

13. In the Based on Template list, select the **Administrator template** that you want UCXN to use when it creates the selected users.

    Caution: If you specify an administrator template, the users will not have mailboxes.

14. Check the check boxes for the LDAP users for whom you want to create UCXN users and click **Import Selected**.



Import Users

Status

Found 1 LDAP User(s)

Find

Find End Users In: LDAP Directory

Where: Alias, Begins With

Import With

Based on Template: administratortemplate

Directory Search Results

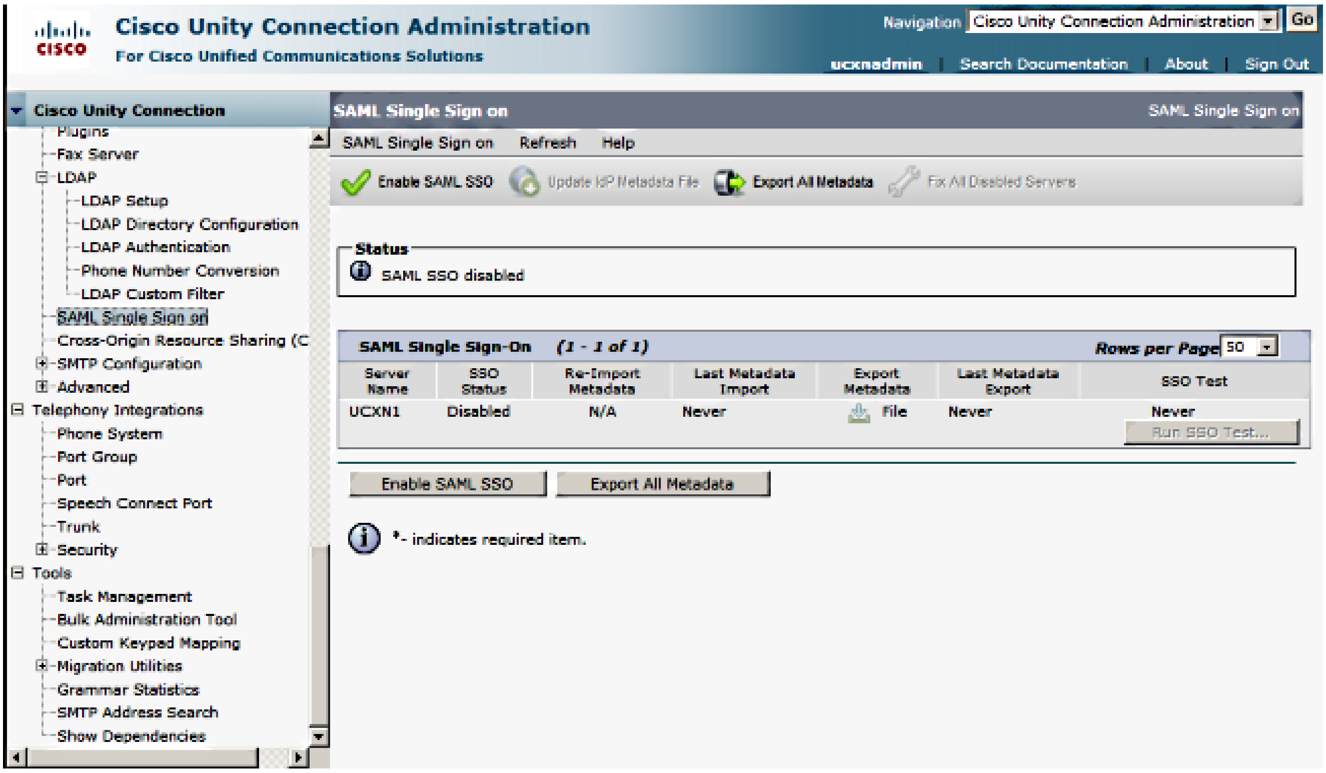
25 Rows Per Page

☑	Alias ▲	First Name	Last Name	Phone Number	Extension
☑	sso	Saml	SSO		

Enable SAML SSO

1. Log into the UCXN Administration user interface.

2. Choose **System** > **SAML Single Sign-on** and the SAML SSO Configuration window opens.



Status

SAML SSO disabled

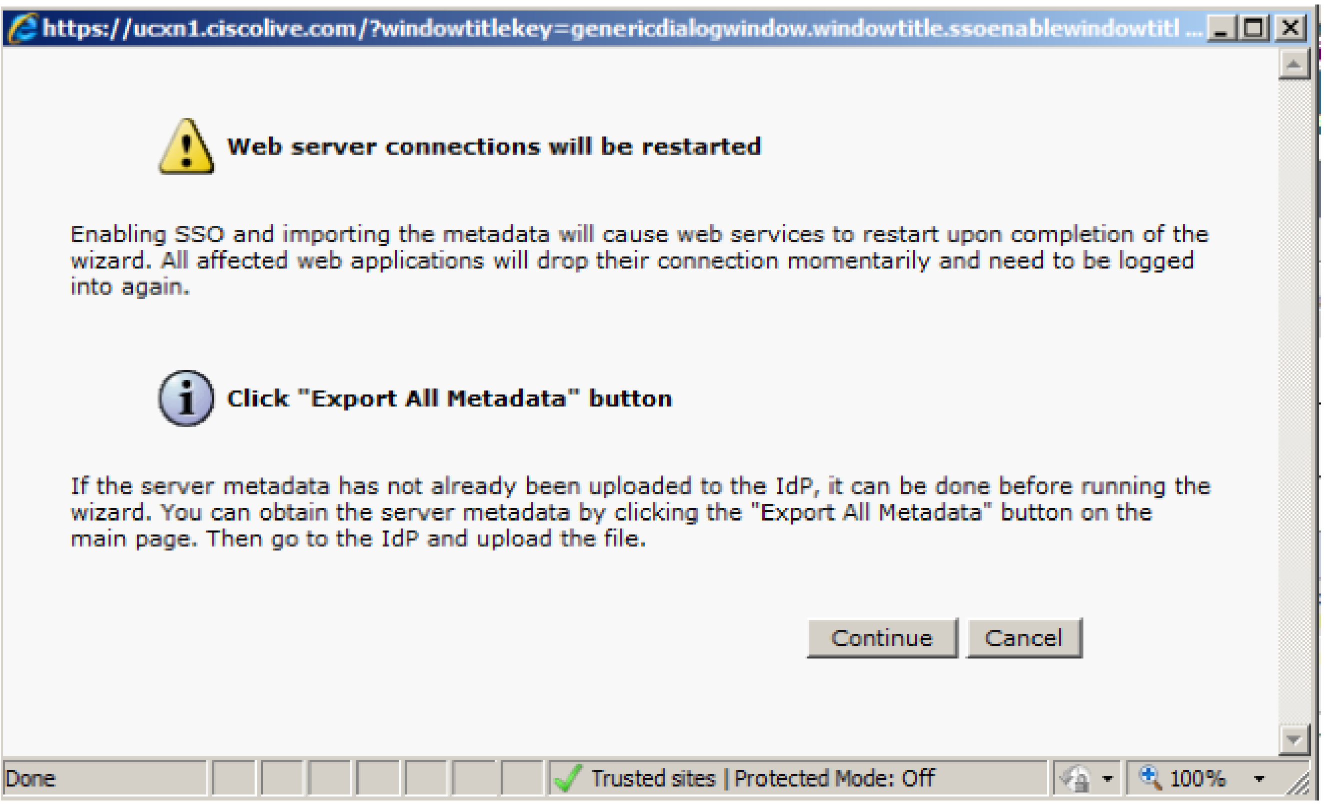
SAML Single Sign-On (1 - 1 of 1) Rows per Page 50

Server Name	SSO Status	Re-Import Metadata	Last Metadata Import	Export Metadata	Last Metadata Export	SSO Test
UCXN1	Disabled	N/A	Never	File	Never	Never Run SSO Test...

*- indicates required item.

3. In order to enable SAML SSO on the cluster, click **Enable SAML SSO**.

4. In the Reset Warning window, click **Continue.**


https://ucxn1.ciscolive.com/?windowtitlekey=genericdialogwindow.windowtitle.ssoenablewindowtitl ...

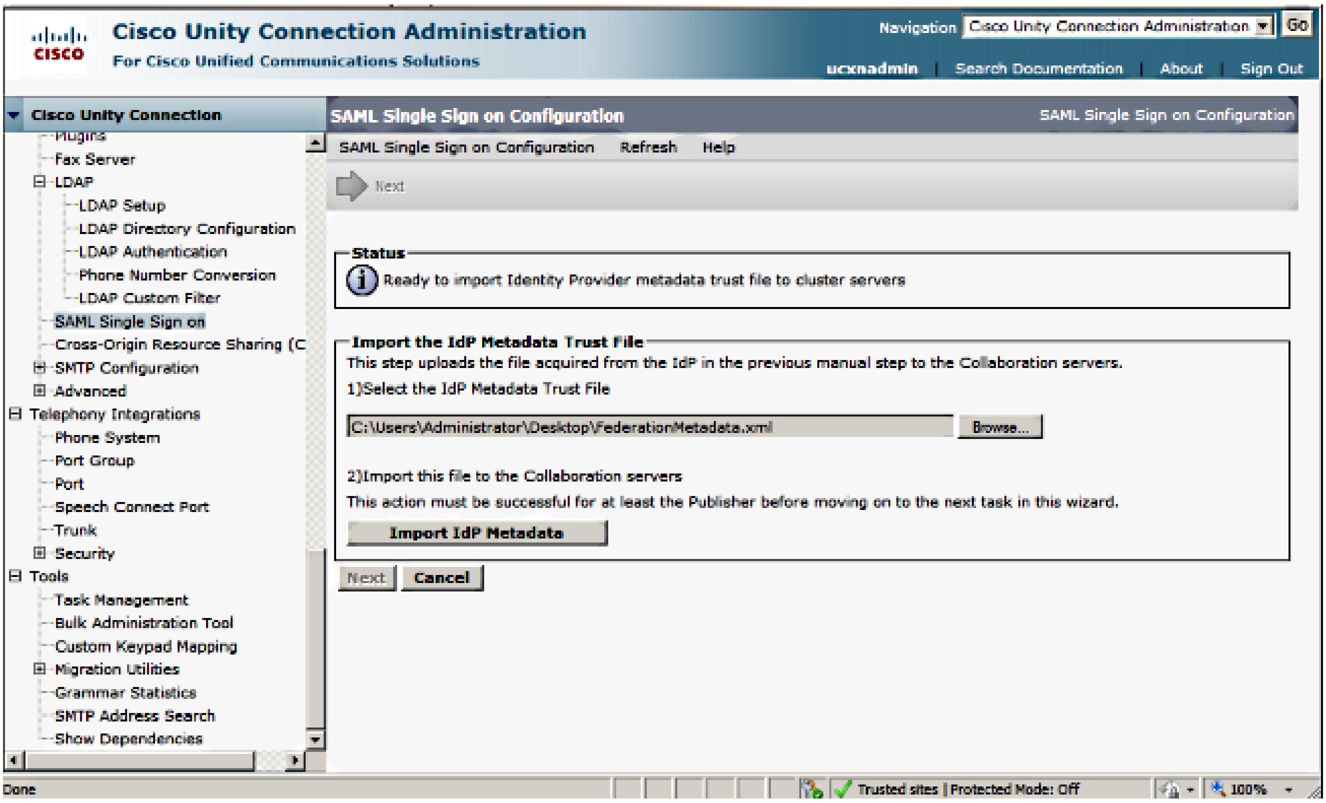
Web server connections will be restarted

Enabling SSO and importing the metadata will cause web services to restart upon completion of the wizard. All affected web applications will drop their connection momentarily and need to be logged into again.

Click "Export All Metadata" button

If the server metadata has not already been uploaded to the IdP, it can be done before running the wizard. You can obtain the server metadata by clicking the "Export All Metadata" button on the main page. Then go to the IdP and upload the file.

5. On the SSO screen, click **Browse** in order to import the **FederationMetadata.xml** metadata XML file with the **Download Idp Metadata** step.



Status

Ready to import Identity Provider metadata trust file to cluster servers

Import the IdP Metadata Trust File

This step uploads the file acquired from the IdP in the previous manual step to the Collaboration servers.

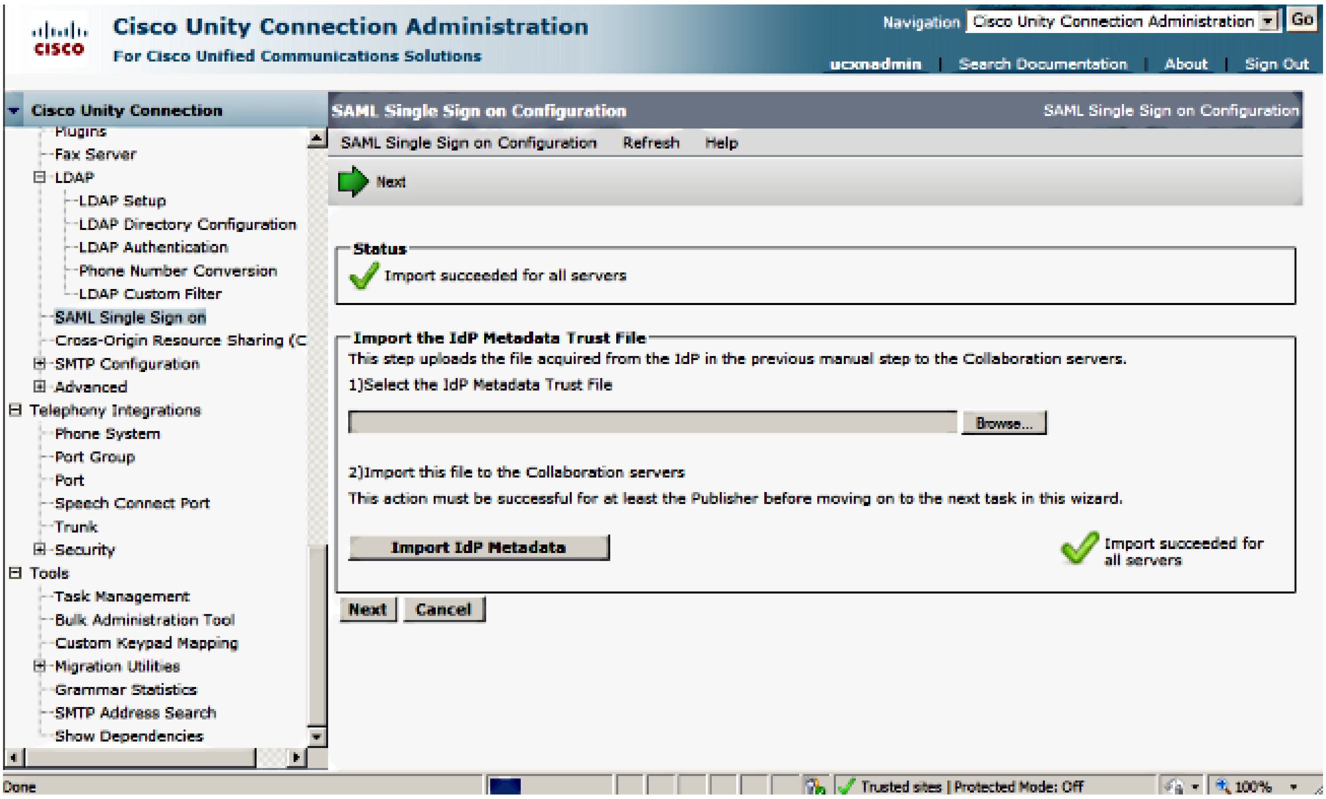
1)Select the IdP Metadata Trust File

C:\Users\Administrator\Desktop\FederationMetadata.xml Browse...

2)Import this file to the Collaboration servers

This action must be successful for at least the Publisher before moving on to the next task in this wizard.

6. Once the metadata file is uploaded, click **Import IdP Metadata** in order to import the IdP information to UCXN. Confirm that the import was successful and click **Next** to continue.



Status

✓ Import succeeded for all servers

Import the IdP Metadata Trust File

This step uploads the file acquired from the IdP in the previous manual step to the Collaboration servers.

1)Select the IdP Metadata Trust File

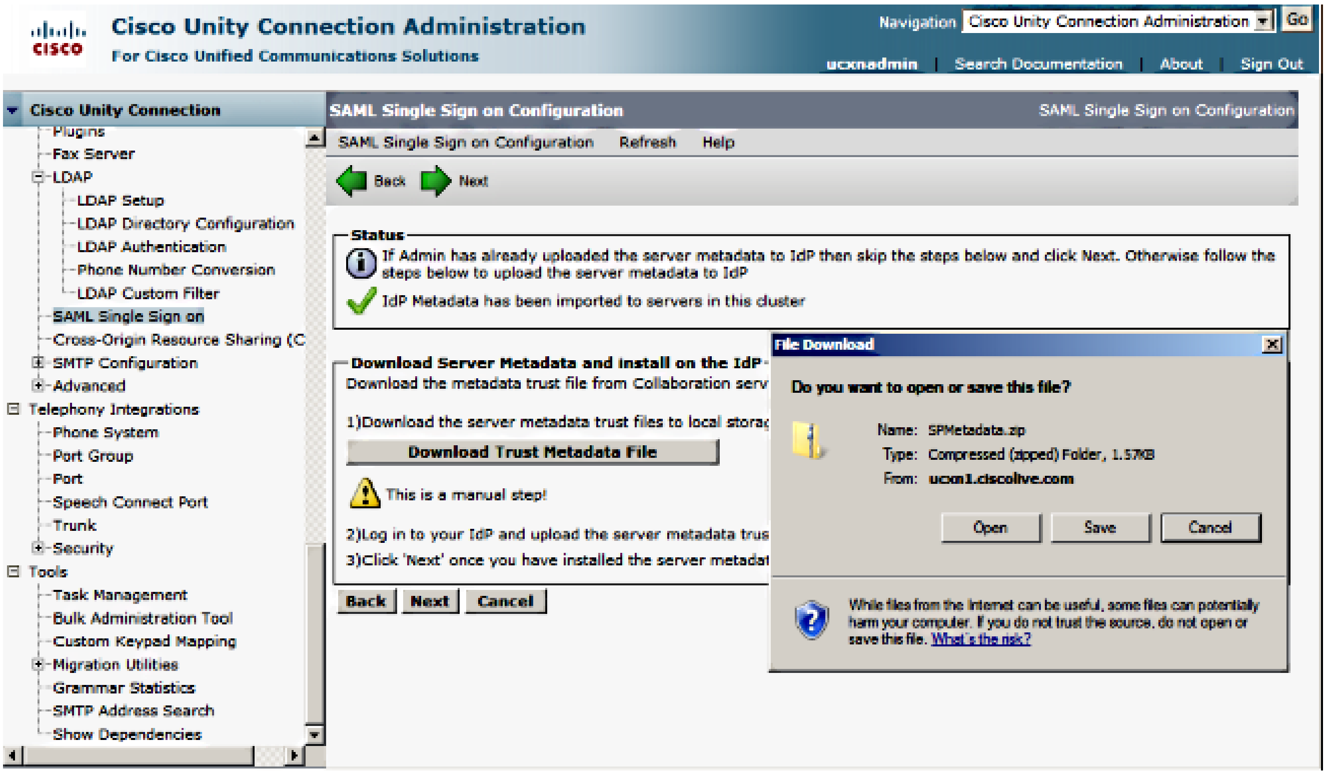
Browse...

2)Import this file to the Collaboration servers

This action must be successful for at least the Publisher before moving on to the next task in this wizard.

✓ Import succeeded for all servers

7. Click **Download Trust Metadata Fileset** (do this only if you have not configured ADFS already with UCXN Metadata) in order to save the UCXN metadata to a local folder and go to Add UCXN as Relaying Party Trust. Once the AD FS configuration is completed, proceed to Step 8.



Status

If Admin has already uploaded the server metadata to IdP then skip the steps below and click Next. Otherwise follow the steps below to upload the server metadata to IdP

IdP Metadata has been imported to servers in this cluster

Download Server Metadata and install on the IdP

Download the metadata trust file from Collaboration serv

1)Download the server metadata trust files to local storag

This is a manual step!

2)Log in to your IdP and upload the server metadata trus

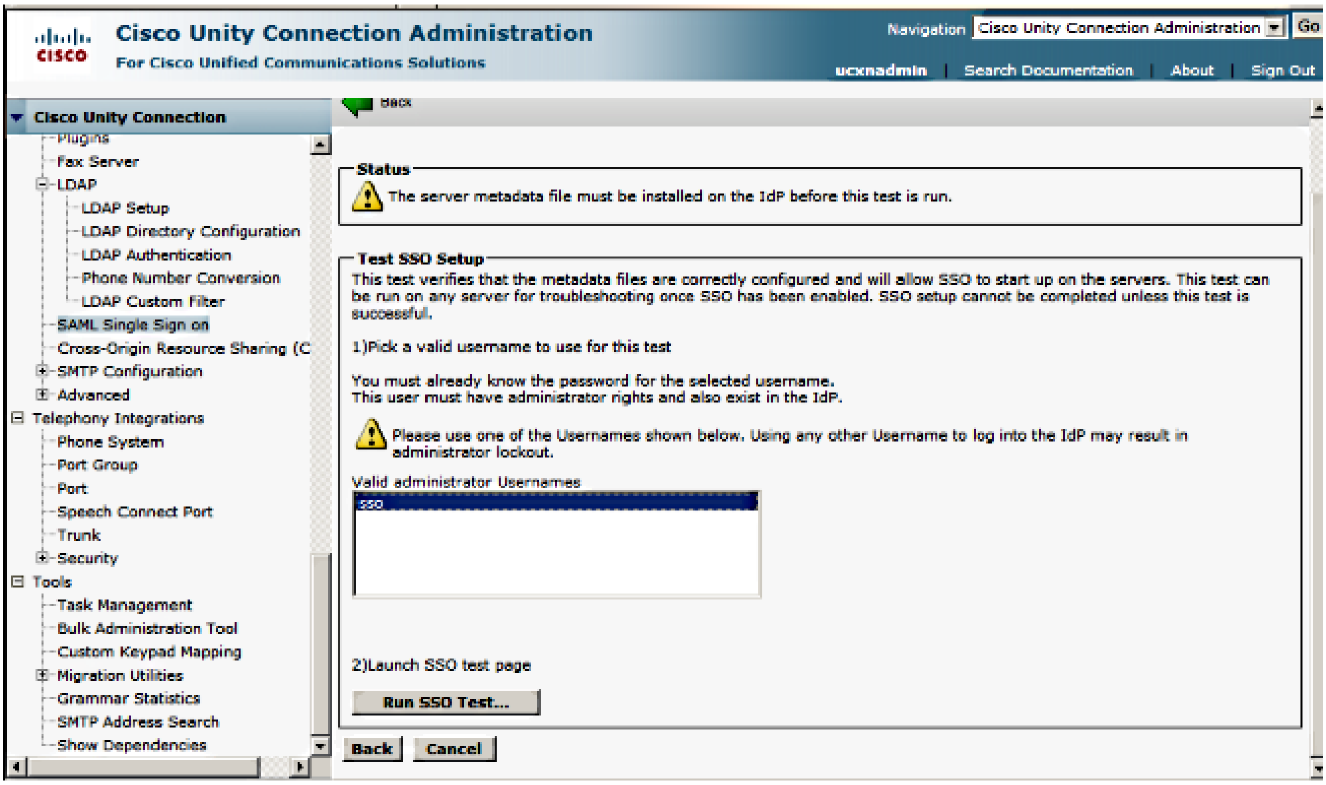
3)Click 'Next' once you have installed the server metadat

Do you want to open or save this file?

Name: SPMetadata.zip
Type: Compressed (zipped) Folder, 1.57KB
From: ucxn1.ciscolive.com

While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not open or save this file. What's the risk?

8. Select **SSO** as the administrative user and click **Run SSO Test**.



Status

The server metadata file must be installed on the IdP before this test is run.

Test SSO Setup

This test verifies that the metadata files are correctly configured and will allow SSO to start up on the servers. This test can be run on any server for troubleshooting once SSO has been enabled. SSO setup cannot be completed unless this test is successful.

1)Pick a valid username to use for this test

You must already know the password for the selected username.
This user must have administrator rights and also exist in the IdP.

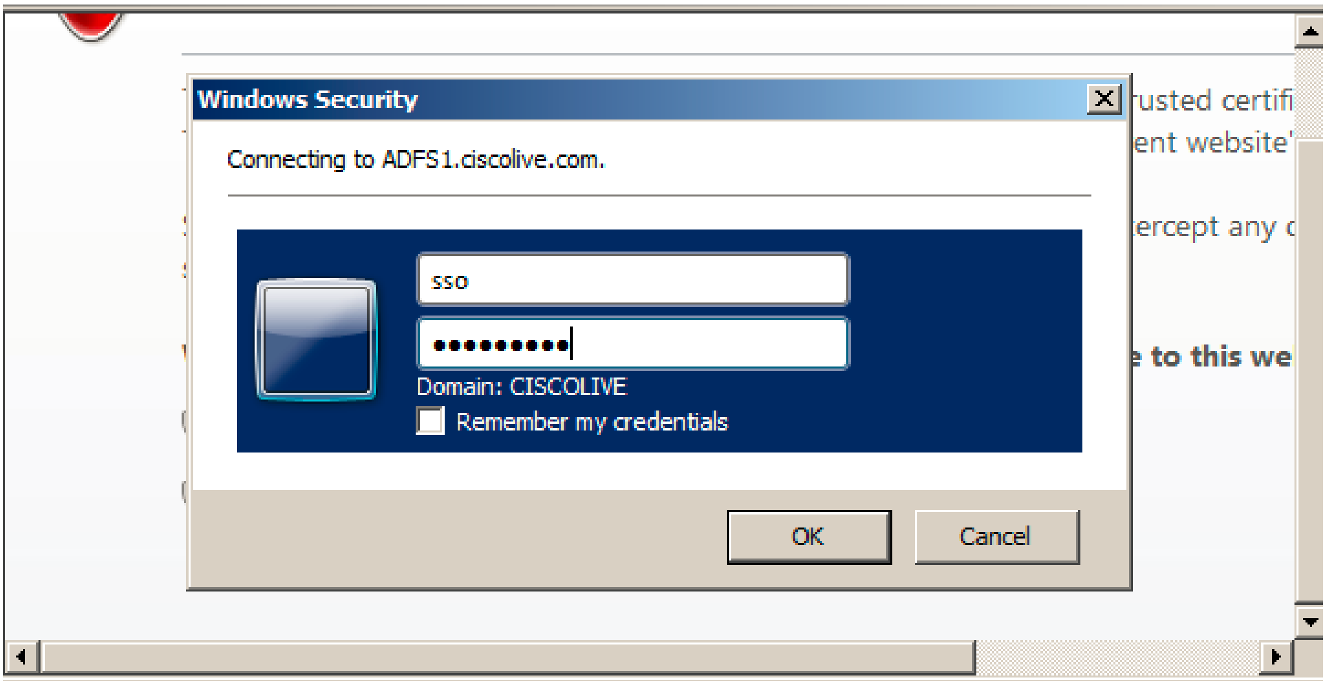
Please use one of the Usernames shown below. Using any other Username to log into the IdP may result in administrator lockout.

Valid administrator Usernames

SSO

2)Launch SSO test page

9. Ignore Certificate Warnings and proceed further. When you are prompted for credentials, enter user SSO's username and password and click **OK**.



Windows Security

Connecting to ADFS1.ciscolive.com.

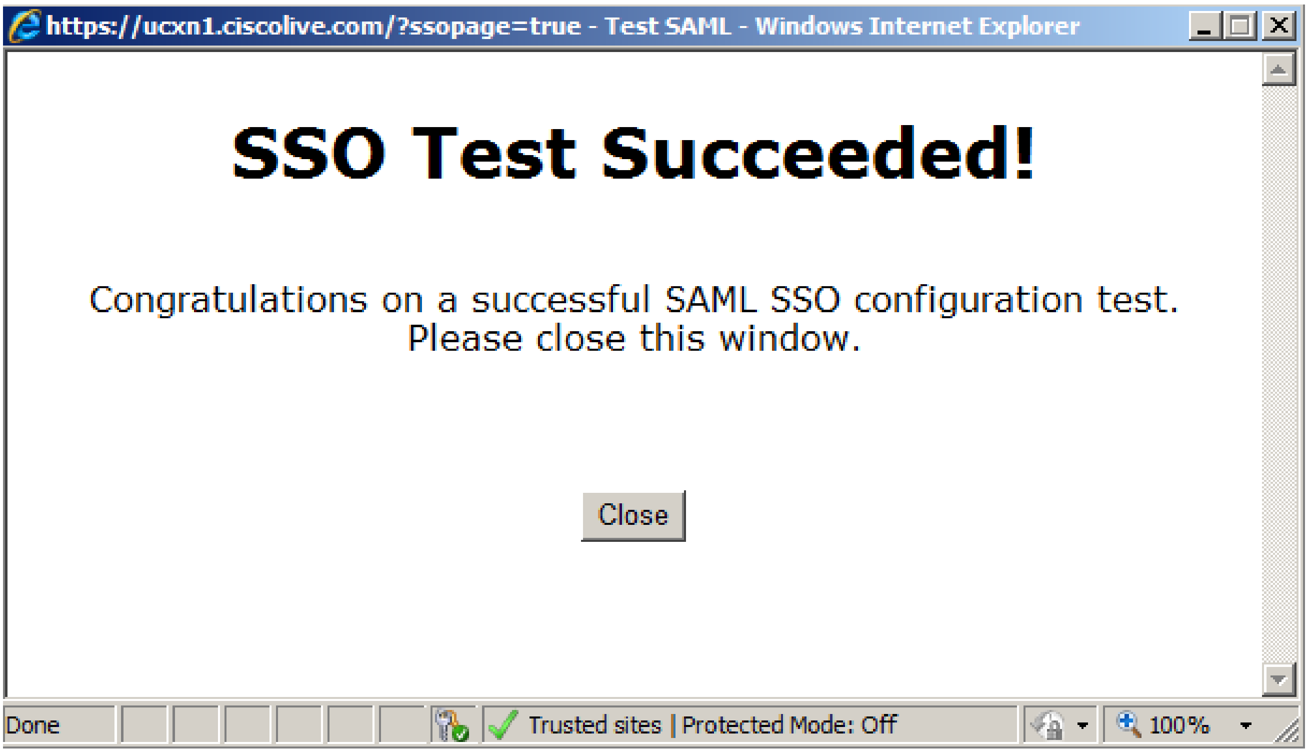
sso

Domain: CISCOLIVE

☐ Remember my credentials

Note: This configuration example is based on UCXN and AD FS self-signed certificates. In case you use Certificate Authority (CA) certificates, appropriate certificates must be installed on both AD FS and UCXN. Refer to Certificate Management and Validation for more information.

10. After all steps are complete, you receive the "SSO Test Succeeded!" message. Click **Close** and **Finish** in order to continue.



https://ucxn1.ciscolive.com/?ssopage=true - Test SAML - Windows Internet Explorer

SSO Test Succeeded!

Congratulations on a successful SAML SSO configuration test.
Please close this window.

You have now successfully completed the configuration tasks to enable SSO on UCXN with AD FS.

Mandatory Note: Run the SSO Test for UCXN Subscriber if it is a cluster in order to enable

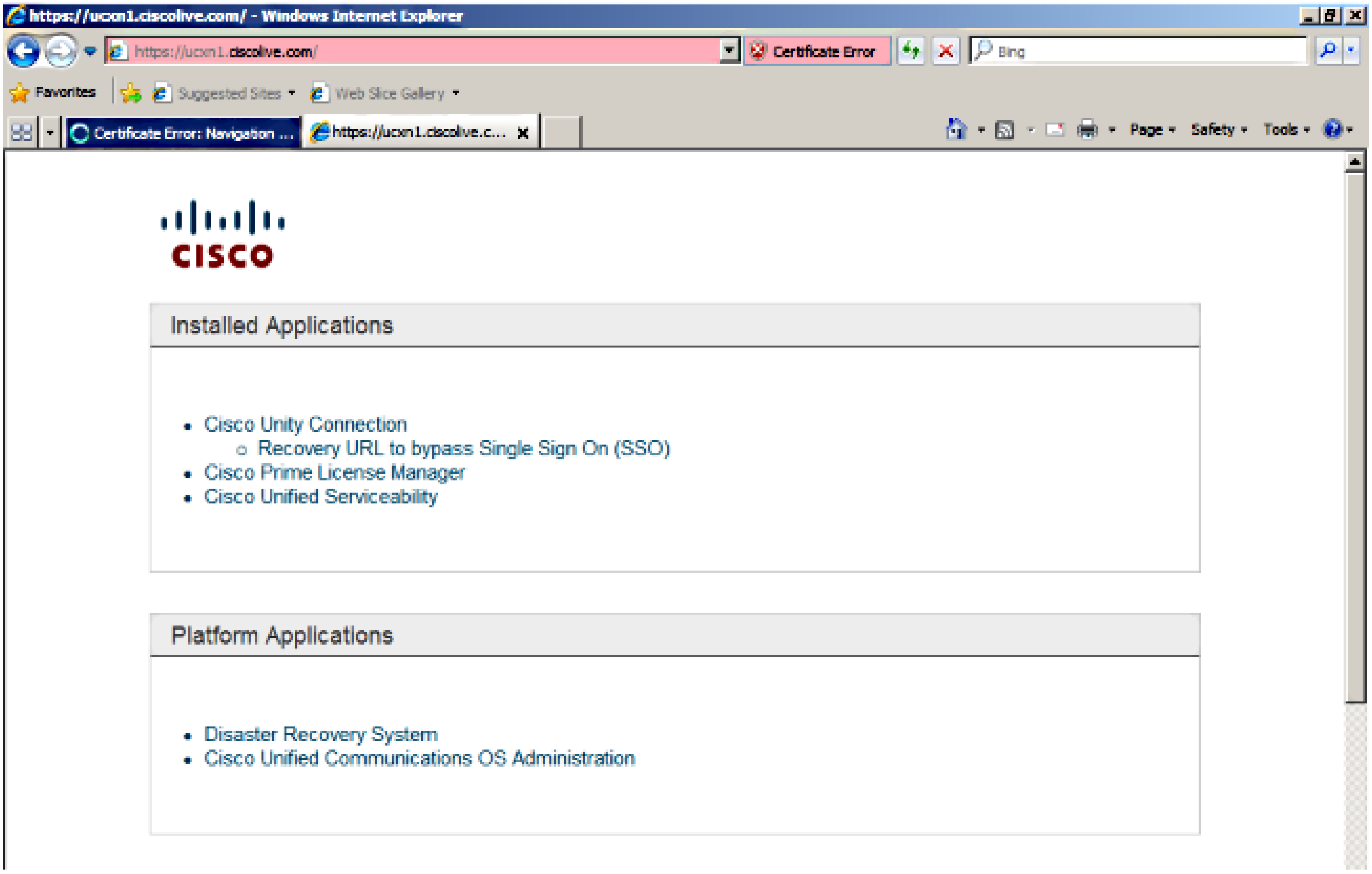
SAML SSO. AD FS must be configured for all of the nodes of UCXN in a cluster.

Tip: If you configure all nodes' metadata XML files on IdP and you start to enable the SSO operation on one node, then SAML SSO will be enabled on all of the nodes in the cluster automatically.

You can also configure CUCM and CUCM IM and Presence for SAML SSO if you want to use SAML SSO for Cisco Jabber Clients and give a true SSO experience to end users.

Verify

Open a web browser and enter the FQDN of UCXN and you see a new option under Installed Applications called **Recovery URL to bypass Single Sign-on (SSO)**. Once you click the **Cisco Unity Connection** link, you are prompted for credentials by the AD FS. After you enter user SSO's credentials, you will be successfully logged into Unity Administration page, Unified Serviceability page.


https://ucxn1.ciscolive.com/ - Windows Internet Explorer
https://ucxn1.ciscolive.com/
Certificate Error
Bing
Favorites
Suggested Sites
Web Slice Gallery
Certificate Error: Navigation ...
https://ucxn1.ciscolive.c...
Page
Safety
Tools
cisco

Installed Applications

- Cisco Unity Connection
  - Recovery URL to bypass Single Sign On (SSO)
- Cisco Prime License Manager
- Cisco Unified Serviceability

Platform Applications

- Disaster Recovery System
- Cisco Unified Communications OS Administration

Note: SAML SSO does not enable access to these pages:
- Prime Licensing Manager
- OS Administration
- Disaster Recovery system

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.

Refer to Troubleshooting SAML SSO for Collaboration Products 10.x for more information.