Configuration and Administration of Cisco Unified Presence Release 8.6
June 16, 2014
Preface 1-1
   About this Guide 1-1
   Audience 1-1
   Organization 1-1
   Related Documents 1-2
   Conventions 1-2
   Obtain Documentation and Submit a Service Request 1-3
   Cisco Product Security Overview 1-3

Deployment Planning

Cisco Unified Presence Features and Functions 1-1
   Cisco Unified Presence Components 1-1
      Main Components 1-1
      SIP Interface 1-2
      AXL/ SOAP Interface 1-3
      LDAP Interface 1-3
      XMPP Interface 1-3
   Deployment Models 1-4
      Single-node Deployments and Multi-node High Availability Deployments 1-4
      Multi-node Scalability Feature 1-4
         Multi-node Scalability Enhancements 1-4
         Scalability Examples 1-5
      Clustering over WAN 1-6
      IM-only Deployment 1-6
   User Assignment 1-6
      User Assignment Mode Recommendations 1-6
      Manual User Assignment Recommendations 1-7
      User Redistribution 1-8
   End User Management 1-8
   Availability and Instant Messaging 1-9
      Chat 1-9
         IM Forking 1-9
         Offline IM 1-9
         Broadcast IM 1-9
         Chat Rooms on Cisco Unified Presence 1-10
      Chat Room Limits 1-10
      File Transfer 1-10
Important Notes about Cisco Unified Presence and Chat 1-11
IM Compliance 1-11
Cisco Unified Communications Manager Integration 1-11
LDAP Integrations 1-11
Third-party Integrations 1-12
Third-party Client Integrations 1-13
  Supported Third-party XMPP Clients 1-13
  License Requirements for Third-party Clients 1-14
  XMPP Client Integration on Cisco Unified Communications Manager 1-14
  LDAP Integration for XMPP Contact Search 1-14
  Domain Name for XMPP Clients 1-14
  DNS Configuration for XMPP Clients 1-15
Security 1-15

CHAPTER 2
Multi-node Scalability and WAN Deployments 2-1
  Multi-node Scalability Feature 2-1
  Scalability Enhancements 2-1
  Scalability Options for Deployment 2-1
  Cluster-wide DNS SRV 2-2
  Local Failover 2-3
  Subcluster Failure Detection 2-3
  Method Event Routing 2-3
  External Database Recommendations 2-4
  Clustering over WAN for Intracluster and Intercluster Deployments 2-4
    Intracluster Deployments over WAN 2-4
      Multi-node Configuration for Deployment over WAN 2-5
    Intercluster Deployments 2-5
        Intercluster Deployments over WAN 2-5
        Intercluster Peer Relationships 2-5
        Intercluster Router-to-Router Connections 2-6
        Node Name Value for Intercluster 2-6
        Domain Value for Intercluster Deployments 2-7
        Secure Intercluster Router-to-Router Connections 2-7

CHAPTER 3
Cisco Unified Presence Planning Requirements 3-1
  Multi-node Hardware Recommendations 3-1
  Intercluster Hardware Recommendations 3-2
  Supported Cisco End Points 3-2
Contents

CHAPTER 4
License Requirements 4-1
Cisco Unified Personal Communicator License Requirements 4-1
User License Requirements 4-1
Adjunct Licensing 4-2

PART 2
System Configuration

CHAPTER 5
Cisco Unified Presence Configuration for an IM-only Deployment 5-1
IM-only Configuration Steps 5-1

CHAPTER 6
Cisco Unified Communications Manager Configuration for Integration with Cisco Unified Presence 6-1
CTI Interface 6-1
User and Device Configuration on Cisco Unified Communications Manager 6-2
Configuring the Inter-Presence Group Subscription Parameter 6-3
SIP Trunk Configuration on Cisco Unified Communications Manager 6-4
Configure the SIP Trunk Security Profile for Cisco Unified Presence 6-4
Configuring the SIP Trunk for Cisco Unified Presence 6-5
Configure Phone Presence for Cisco Unified Communications Manager Outside of Cluster 6-6
Configuring a TLS Peer Subject 6-6
Configuring a TLS Context 6-7
Verify Required Services are Running on Cisco Unified Communications Manager 6-7

CHAPTER 7
Cisco Unified Presence Network Setup 7-1
Configuration Changes and Service Restart Notifications 7-1
Service Restart Notifications 7-1
Cisco UP XCP Router Restart 7-2
Restart the Cisco UP XCP Router Service 7-2
Turn on the Cisco UP XCP Text Conference Service 7-2
DNS Domain Configuration 7-3
Cisco Unified Presence Release 8.6(4) and Earlier 7-3
Cisco Unified Presence Release 8.6(5) and Later 7-3
Cisco Unified Presence Clusters Deployed in Different DNS Domain or Subdomains 7-4
Cisco Unified Presence Nodes within a Cluster Deployed within Different DNS Domains or Subdomains 7-4
Cisco Unified Presence Nodes within a Cluster Deployed in a DNS Domain that is Different to the Associated Cisco Unified Communications Manager Cluster 7-5
Specify the DNS Domain Associated with Cisco Unified Communications Manager Cluster 7-7
Domain Value Configuration 7-7
Replacing the Default Presence Domain after Installation 7-7
Cisco Unified Presence Release 8.6(4) and Earlier 7-8
Cisco Unified Presence Release 8.6(5) and Later 7-8
Changing the Presence Domain Value 7-9
Cisco Unified Presence Release 8.6(4) and Earlier 7-9
Cisco Unified Presence Release 8.6(5) and Later 7-10
Routing Information Configuration on Cisco Unified Presence 7-11
Routing Communication Recommendations 7-11
Configure MDNS Routing and Cluster ID 7-11
Configure Routing Communication 7-12
Configure Cluster ID 7-13
Configure the Throttling Rate for Availability State Change Messages 7-13
Configure the Proxy Server Settings 7-14
SIP Digest Authentication 7-14
Turn on Cisco Unified Presence Services 7-15
Turn on the Sync Agent 7-15
Turn on Cisco Unified Presence Services 7-16

CHAPTER 8
IP Phone Presence Setup 8-1
Static Route Configuration on Cisco Unified Presence 8-1
Route Embed Templates 8-1
Configure Route Embed Templates on Cisco Unified Presence 8-2
Configure Static Routes on Cisco Unified Presence 8-3
Presence Gateway Configuration on Cisco Unified Presence 8-5
Presence Gateway Configuration Option 8-5
Configure the Presence Gateway 8-6
Configure the SIP Publish Trunk on Cisco Unified Presence 8-6

CHAPTER 9
LDAP Directory Integration 9-1
LDAP Directory Integration with Cisco Unified Communications Manager 9-2
Secure Connection Between Cisco Unified Communications Manager and the LDAP Directory 9-3
Configuring the LDAP Synchronization for User Provisioning 9-3
Secure Connection between Cisco Unified Communications Manager and the LDAP Directory 9-3
Configure the LDAP Synchronization for User Provisioning 9-3
Upload LDAP Authentication Server Certificates 9-4
Configure LDAP Authentication 9-5
Configure a Secure Connection between Cisco Unified Presence and the LDAP Directory 9-6

LDAP Directory Integration with Cisco Unified Personal Communicator 9-6
Rules for a Displayed Contact Name 9-7
(Cisco Unified Personal Communicator Release 8.0) Fetch Contact Pictures from a Web Server 9-7
Configure the LDAP Attribute Map for Cisco Unified Personal Communicator 9-8
Configure LDAP Server Names and Addresses for Cisco Unified Personal Communicator 9-9
Create LDAP Profiles and Add Cisco Unified Personal Communicator Users to the Profile 9-10

LDAP Directory Integration for Contact Searches on XMPP Clients 9-12
LDAP Account Lock Issue 9-13
Configure LDAP Server Names and Addresses for XMPP Clients 9-13
Configure the LDAP Search Settings for XMPP Clients 9-14
Turn on the Cisco UP XCP Directory Service 9-16

CHAPTER 10
Third-party XMPP Client Application Configuration on Cisco Unified Presence 10-1
Verify Domain Name for XMPP Clients 10-1
Configure a Secure Connection between Cisco Unified Presence and XMPP Clients 10-1
Turn on Cisco Unified Presence Services to Support XMPP Clients 10-2

CHAPTER 11
Security Configuration on Cisco Unified Presence 11-1
Create Login Banner 11-1
Cisco Unified Presence Certificate Types 11-2
Certificate Exchange Configuration between Cisco Unified Presence and Cisco Unified Communications Manager 11-3
Prerequisites for Configuring Security 11-3
Import the Cisco Unified Communications Manager Certificate to Cisco Unified Presence 11-4
Restart the SIP Proxy Service 11-4
Download the Certificate from Cisco Unified Presence 11-4
Upload the Cisco Unified Presence Certificate to Cisco Unified Communications Manager 11-5
Restart the Cisco Unified Communications Manager Service 11-5
SIP Security Settings Configuration on Cisco Unified Presence 11-6
Configuring a TLS Peer Subject 11-6
Configuring a TLS Context 11-7
Configuring the SIP Proxy-to-Proxy Intracluster Protocol Type 11-7
XMPP Security Settings configuration on Cisco Unified Presence 11-8
XMPP Security Modes 11-8
Configuration and Administration of Cisco Unified Presence Release 8.6

PART 2  System Configuration

CHAPTER 11  XMPP Certificate Settings

Configure the XMPP Certificate Settings 11-9
FIPS 140-2 Mode Configuration 11-10
Node Reboot in FIPS 140-2 Mode 11-10
Forced Manual Sync of Certificates 11-10

CHAPTER 12  FIPS 140-2 Mode Configuration

Intercluster Peer Configuration 12-1
Prerequisites for Intercluster Deployment 12-1
Intercluster Peer Configuration 12-2
Configure an Intercluster Peer 12-2
Turn on the Intercluster Sync Agent 12-3
Verify the Intercluster Peer Status 12-4
Update Intercluster Sync Agent Tomcat Trust Certificates 12-4

CHAPTER 13  Node Reboot in FIPS 140-2 Mode

Forced Manual Sync of Certificates 11-10

CHAPTER 14  Forced Manual Sync of Certificates

CHAPTER 12  Intercluster Peer Configuration

Prerequisites for Intercluster Deployment 12-1
Intercluster Peer Configuration 12-2
Configure an Intercluster Peer 12-2
Turn on the Intercluster Sync Agent 12-3
Verify the Intercluster Peer Status 12-4
Update Intercluster Sync Agent Tomcat Trust Certificates 12-4

PART 3  Feature Configuration

CHAPTER 13  Configure the XMPP Certificate Settings

Availability and Instant Messaging Configuration 13-1
Availability Setup 13-1
Turn On or Off Availability Sharing 13-1
Configure Ad-hoc Presence Subscription Settings 13-2
Configure Maximum Contact List Size Per User 13-3
Configure Maximum Number of Watchers Per User 13-4
IM Setup 13-4
Turn On or Off Instant Messaging for a Cisco Unified Presence Cluster 13-4
Turn On or Off Offline Instant Messaging 13-5
Allow Clients to Log Instant Message History 13-6
Configure Do Not Disturb Settings 13-6

CHAPTER 14  Configure the XMPP Certificate Settings

Cisco IP PhoneMessenger Service Configuration 14-1
Prerequisites for Integrating Cisco IP PhoneMessenger 14-1
Cisco IP PhoneMessenger Configuration on Cisco Unified Communications Manager 14-1
Configure Cisco IP PhoneMessenger as an Application User 14-2
Configure a Phone Service for the Cisco IP PhoneMessenger 14-2
Subscribe Phones to the Cisco IP PhoneMessenger Service 14-3
Cisco IP PhoneMessenger Configuration on Cisco Unified Presence 14-3
Configure the Cisco IP PhoneMessenger Settings 14-4
Use Cisco IP PhoneMessenger Across Clusters 14-4
Configure Meeting Notification Settings 14-5
Meeting Notification Feature Information 14-5
Configuring Cisco IP Phone Messenger Response Messages 14-6
Send a Broadcast Message 14-7
Sign Out a Cisco IP Phone Messenger User 14-7

CHAPTER 15
End User Setup and Handling 15-1
End User Setup and Handling on Cisco Unified Presence 15-1
Configure User Assignment in System Topology 15-1
Authorization Policy Configuration 15-2
Automatic Authorization 15-2
User Policy and Automatic Authorization 15-3
Configure the Authorization Policy 15-4
Bulk Rename of Contact IDs 15-5
Bulk Export of User Contact Lists 15-6
Bulk Import of User Contact Lists 15-8
Check Maximum Contact List Size 15-9
Upload the Input File using BAT 15-10
Create a New Bulk Administration Job 15-10
Check Results of Bulk Administration Job 15-10

CHAPTER 16
Single Sign-On Configuration 16-1
Introduction 16-1
Task Flow for Single Sign-On Configuration 16-1
System Requirements 16-2
Before You Begin 16-4
Single Sign-On Configuration 16-4
Provision Active Directory for Single Sign-On 16-4
Client Browser Configuration for Single Sign-On 16-5
Configure Internet Explorer for Single Sign-On 16-5
Configure Firefox for Single Sign-On 16-7
Windows Registry Configuration for Real-Time Monitoring Tool 16-7
Install Java 16-8
Import Cisco Unified Presence Certificates into OpenAM 16-11
Install Tomcat 16-13
Deploy OpenAM War on Apache Tomcat 16-17
Set up OpenAM using the GUI Configurator 16-17
Set up Policies on OpenAM Server 16-19
Configure Single Sign-On Module Instance 16-21
Configure J2EE Agent Profile on OpenAM 16-22
Set the OpenAM Session Timeout 16-24
Import the OpenAM Certificate into Cisco Unified Presence 16-25
Activate Single Sign-On 16-26
  Configure Access Permissions Before Enabling Single Sign-On 16-27
  Enable Single Sign-On 16-28
Disable Single Sign-On 16-29
  Configure Access Permissions Before Disabling Single Sign-On 16-29
  Disable Single Sign-On 16-30
Uninstall OpenAM 16-31
Set the Debug Level 16-32

PART 4
Administration

CHAPTER 17
Multi-node Deployment Administration 17-1
  Multi-node Deployment Models 17-1
    Balanced User Assignment Redundant High Availability Deployment 17-1
    Active/Standby User Assignment Redundant High Availability Deployment 17-2
    High Availability for Cisco Unified Personal Communicator 7.x and 8.x Clients 17-3
    Cisco Unified Personal Communicator Sign-in and Redirect 17-4
  Cluster Topology Management 17-5
    Subcluster, Node and User Management Recommendations 17-5
      Node Creation and Movement Recommendations 17-5
      Node Name Recommendations 17-6
    Add a New Node 17-7
    Expand the Cluster 17-8
    Create Subclusters in System Topology 17-9
    Create, Assign and Move Nodes in System Topology 17-10
  High Availability Deployments 17-12
    Requirements for High Availability 17-12
    High Availability in a Subcluster 17-12
    Impact of Failover to Cisco Unified Presence Clients and Services 17-13
    Automatic Failover Detection 17-13
    Automatic Fallback 17-15
    Cisco UP Server Recovery Manager (SRM) 17-15
    Manual Failover and Fallback 17-16
    Important Note about High Availability and Intercluster Deployments 17-16
  High Availability Configuration 17-16
    Turn On or Off High Availability for a Subcluster 17-17
    Configure the Advanced Service Parameters for the Server Recovery Manager 17-18
CHAPTER 18  Chat Setup and Management 18-1

Chat Deployments 18-1
Scenario 1 18-1
Scenario 2 18-2
Scenario 3 18-2
Scenario 4 18-3
Scenario 5 18-4

Chat Settings Administration 18-4
Change IM Gateway Settings 18-5
Enable File Transfer 18-5
Limit the Number of Sign-in Sessions 18-6
Enable Persistent Chat 18-6

Chat Node Alias Management 18-8
Chat Node Aliases 18-8
Key Considerations 18-9
Turn On System-generated Chat Node Aliases 18-9
Manage Chat Node Aliases Manually 18-10
Turn On the Cisco UP XCP Text Conference Service 18-12

CHAPTER 19  User Migration between Cisco Unified Presence Clusters 19-1

Unassign Users from the Current Cluster 19-2
Export User Contact Lists 19-3
Unlicense Users  19-4
Move Users to the New Cluster  19-4
    LDAP Sync Enabled on Cisco Unified Communications Manager  19-4
    Move Users to the New Organizational Unit  19-4
    Synchronize the Users to the New Home Cluster  19-5
    LDAP Sync not Enabled on Cisco Unified Communications Manager  19-5
License the Users on the New Cluster  19-5
Import Contact Lists on the New Home Cluster  19-6

CHAPTER 20
Multilingual Support Configuration  20-1
    Install the Locale Installer on Cisco Unified Communications Manager  20-1
    Install the Locale Installer on Cisco Unified Presence  20-3
    Localized Applications  20-5

PART 5
Troubleshooting
CHAPTER 21
Troubleshooting High Availability  21-1
    Node States, Causes and Recommended Actions  21-1

CHAPTER 22
Troubleshooting a Cisco Unified Presence Multi-node Deployment  22-1
    Monitor a Multi-node System  22-1
    Resolve a Hardware Problem  22-2
    Cisco UP Replication Watcher Service  22-3

CHAPTER 23
Troubleshooting Single Sign-On  23-1
    "Invalid Profile Credentials" Message  23-1
    "Module Name Is Invalid" Message  23-2
    "Invalid OpenAM Access Manager (OpenAM) Server URL" Message  23-2
    Web Browser Indicates a 401 Error  23-2
    Web Browser Indicates a 403 Error or Displays a Blank Screen  23-2
    "User Is Not Authorized to Perform This Function" Error  23-3
    Web Browser Indicates an HTTP 404 Error  23-3
    Web Browser Indicates an HTTP 500 Error or Displays a Blank Screen  23-3
    "Authentication Failed" Message  23-4
    Web Browser Displays an OpenAM Login Screen  23-4
    Web Browser Displays Cisco Unified Presence Login Screen  23-4
    Internet Explorer Prompts for Username and Password  23-5
Preface

About this Guide

This document provides administrators with the information required to deploy Cisco Unified Presence.

Audience

This document intended for administrators who are responsible for setting up and maintain Cisco Unified Presence.

Organization

This document contains the following parts:

- **Deployment Planning** - describes Cisco Unified Presence features and functions, multi-node scalability and WAN deployments, and planning and license requirements.

- **System Configuration** - describes how to configure Cisco Unified Presence post installation and includes information about integrating with Cisco Unified Communications Manager, network setup, IP Phone presence setup, LDAP directory integration, security configuration and intercluster peer configuration.

- **Feature Configuration** - describes how to configure Cisco Unified Presence features and includes information about availability and instant messaging configuration, Cisco IP PhoneMessenger service configuration, end user setup and handling, and single sign-on configuration.
• **Administration** - describes how to administer your Cisco Unified Presence deployment and includes information about multi-node deployment administration, chat setup and management, user migration between clusters, and multilingual support configuration.

• **Troubleshooting** - contains information about troubleshooting your Cisco Unified Presence deployment.

• **Appendix** - contains information about high availability client login profiles, XMPP standards compliance and a glossary of terms.

## Related Documents

**Cisco Unified Presence Solution Reference Network Design (SRND) Document:**

**Cisco Unified Presence Compatibility Matrices and Port List:**

**Cisco Unified Presence Release Notes:**

**Cisco Unified Communications Manager information:**

**Cisco Unified Personal Communicator Documentation:**

## Conventions

This document uses the following conventions.

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>boldface</strong> font</td>
<td>Commands and keywords are in <strong>boldface</strong>.</td>
</tr>
<tr>
<td><strong>italic</strong> font</td>
<td>Arguments for which you supply values are in <strong>italics</strong>.</td>
</tr>
<tr>
<td>[ ]</td>
<td>Elements in square brackets are optional.</td>
</tr>
<tr>
<td>{ x</td>
<td>y</td>
</tr>
<tr>
<td>[ x</td>
<td>y</td>
</tr>
<tr>
<td>string</td>
<td>A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.</td>
</tr>
<tr>
<td>Convention</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>screen font</strong></td>
<td>Terminal sessions and information the system displays are in <strong>screen font</strong>.</td>
</tr>
<tr>
<td><strong>boldface screen font</strong></td>
<td>Information you must enter is in <strong>boldface screen font</strong>.</td>
</tr>
<tr>
<td><strong>italic screen font</strong></td>
<td>Arguments for which you supply values are in <strong>italic screen font</strong>.</td>
</tr>
<tr>
<td>^</td>
<td>The symbol ^ represents the key labeled Control—for example, the key combination ^D in a screen display means hold down the Control key while you press the D key.</td>
</tr>
<tr>
<td>&lt;&gt;</td>
<td>Nonprinting characters, such as passwords, are in angle brackets.</td>
</tr>
</tbody>
</table>

**Note**
Means reader take note. Notes contain helpful suggestions or references to material not covered in the publication.

**Caution**
Means reader be careful. In this situation, you might do something that could result in equipment damage or loss of data.

**Timesaver**
Means the described action saves time. You can save time by performing the action described in the paragraph.

**Tip**
Means the information contains useful tips.

**Obtain Documentation and Submit a Service Request**

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly What's New in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation, at:


Subscribe to the What's New in Cisco Product Documentation as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.

**Cisco Product Security Overview**

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors
and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

Further information regarding U.S. export regulations may be found at http://www.access.gpo.gov/bis/ear/ear_data.html.
PART 1

Deployment Planning

- Cisco Unified Presence Features and Functions
- Multi-node Scalability and WAN Deployments
- Cisco Unified Presence Planning Requirements
- License Requirements
Cisco Unified Presence Features and Functions

June 16, 2014

- Cisco Unified Presence Components, page 1-1
- Deployment Models, page 1-4
- User Assignment, page 1-6
- End User Management, page 1-8
- Availability and Instant Messaging, page 1-9
- IM Compliance, page 1-11
- LDAP Integrations, page 1-11
- Third-party Integrations, page 1-12
- Third-party Client Integrations, page 1-13
- Security, page 1-15

Cisco Unified Presence Components

Main Components

Figure 1-1 provides an overview of a Cisco Unified Presence deployment, including the main components and interfaces between Cisco Unified Communications Manager and Cisco Unified Presence.
Cisco Unified Presence Components

Figure 1-1  Cisco Unified Presence Basic Deployment

A Session Initiation Protocol (SIP) connection handles the availability information exchange between Cisco Unified Communications Manager and Cisco Unified Presence. To enable the SIP connection on Cisco Unified Communications Manager, you must configure a SIP trunk pointing to the Cisco Unified Presence server.

On Cisco Unified Presence, configuring Cisco Unified Communications Manager as a Presence Gateway will allow Cisco Unified Presence to send SIP subscribe messages to Cisco Unified Communications Manager over the SIP trunk.

Note  Cisco Unified Presence does not support clients (Cisco clients or third party) connecting to Cisco Unified Presence using SIP/SIMPLE interface over TLS. Only a SIP connection over TCP is supported.

Related Topics
- SIP Trunk Configuration on Cisco Unified Communications Manager, page 6-4
AXL/SOAP Interface

The AXL/SOAP interface handles the database synchronization from Cisco Unified Communications Manager and populates the Cisco Unified Presence database. To activate the database synchronization, you must start the Sync Agent service on Cisco Unified Presence.

By default the Sync Agent load balances all users equally across all nodes within the Cisco Unified Presence cluster. You also have the option to manually assign users to a particular node in the Cisco Unified Presence cluster.

For guidelines on the recommended synchronization intervals when executing a database synchronization with Cisco Unified Communications Manager, see the Cisco Unified Presence SRND document.

Related Topics
- Cisco Unified Presence SRND:
- Turn on the Sync Agent, page 7-15

LDAP Interface

Cisco Unified Communications Manager obtains all user information via manual configuration or synchronization directly over LDAP. Cisco Unified Presence then synchronizes all this user information from Cisco Unified Communications Manager (using the AXL/SOAP interface).

Cisco Unified Presence provides LDAP authentication for users of the Cisco Unified Personal Communicator client and Cisco Unified Presence user interface. If a Cisco Unified Personal Communicator user logs into Cisco Unified Presence, and LDAP authentication is enabled on Cisco Unified Communications Manager, Cisco Unified Presence goes directly to the LDAP directory for Cisco Unified Personal Communicator user authentication. Once Cisco Unified Personal Communicator is authenticated, Cisco Unified Presence forwards this information to Cisco Unified Personal Communicator to continue the user login.

Cisco Unified Personal Communicator and third party XMPP clients use the LDAP directory to allow users to search and add contacts.

Related Topic
LDAP Directory Integration, page 9-1

XMPP Interface

An XMPP connection handles the exchange of availability information and instant messaging operations for XMPP-based clients. Cisco Unified Presence supports temporary (ad-hoc) and persistent chat rooms for XMPP-based clients. An IM Gateway supports the IM interoperability between SIP-based and XMPP-based clients in a Cisco Unified Presence deployment.

Related Topics
- Third-party XMPP Client Application Configuration on Cisco Unified Presence, page 10-1
Deployment Models

Single-node Deployments and Multi-node High Availability Deployments

Cisco Unified Presence Release 8.6 supports single-node and multi-node High Availability deployments. In a single-node deployment within a subcluster, there is no High Availability failover protection for users assigned to the node. The multi-node feature introduces the concept of a subcluster. A subcluster is a single Cisco Unified Presence server, or a pair of Cisco Unified Presence servers, where each node has an independent database and set of users operating with a shared availability database that is able to support common users.

In a dual-node deployment within a subcluster, if you turn on High Availability in the subcluster, users have failover protection; each node acts as a backup for the other node allowing clients to fail over in case of outages of components or nodes. When you turn on High Availability in a subcluster, all users in the subcluster have redundancy and full failover capabilities.

Cisco recommends that you configure your Cisco Unified Presence deployments as High Availability deployments. Although mixed mode deployments are permitted, for example High Availability subclusters and non-High Availability subclusters in a single deployment, Cisco does not recommend this configuration.

You must manually turn on High Availability in a subcluster. You can achieve a High Availability deployment by configuring the Balanced Mode (Redundant High Availability) or the Active/Standby Redundant High Availability deployment models, and turning on High Availability in your deployment.

Related Topics

- High Availability Deployments, page 17-12
- Create Subclusters in System Topology, page 17-9

Multi-node Scalability Feature

Multi-node Scalability Enhancements

The Cisco Unified Presence multi-node scalability feature supports the following:

- Maximum of six nodes per cluster
- In an IM-only deployment, 25,000 users per node
- 45,000 users per cluster with maximum of 15,000 users per node in a full Unified Communication mode deployment
- Administrable customer-defined limit on the maximum contacts per user (default unlimited)
- Cisco Unified Presence continues to support intercluster deployments with the multi-node feature
- With High Availability enabled, subclusters include active nodes and standby nodes, whereby the standard node takes over when the active node goes down.
Scalaiblity Examples

Single Cisco Unified Communications Manager without Cisco Unified Presence

Scaleability:
- 4,000 users that can scale to 13,000 users
- Single Cisco Unified Communications Manager cluster
- High availability not needed

Hardware:
- Cisco MCS 7845 servers

Deployment:
- Three single-server subclusters using User Assignment Mode = balanced

Two Cisco Unified Communications Manager clusters without Cisco Unified Presence

Scaleability:
- 11,000 users that can scale to 24,000 users
- Two Cisco Unified Communications Manager clusters
- High availability is not needed

Hardware:
- Cisco MCS 7845 servers

Deployment:
- Two Cisco Unified Presence clusters (one per Cisco Unified Communications Manager cluster), each with three subclusters with one server using User Assignment Mode = balanced

Single Cisco Unified Communications Manager with Cisco Unified Presence

Scaleability:
- 500 users that can scale to 2500 users
- Single Cisco Unified Communications Manager cluster
- High availability is required

Hardware:
- Cisco MCS 7835 servers

Deployment:
- One 2-server subcluster using User Assignment Mode = balanced

Multiple Cisco Unified Communications Manager clusters with Cisco Unified Presence

Scaleability:
- 5,000 users that can scale to 40,000 users
- Multiple Cisco Unified Communications Manager clusters
- High Availability is required
Hardware

- Cisco MCS 7845 servers

Deployment:

- Multiple Cisco Unified Presence clusters must be set up with intercluster peers between each cluster. Start with a single two-server subcluster, with up to 5000 users for each cluster prior to adding additional subclusters within existing Cisco Unified Presence clusters. With a large number of users within a single Cisco Unified Presence cluster, the User Assignment Mode service parameter to use is dictated by the system administrator. If the desire is to monitor a single server per subcluster, Active/Standby mode might be preferred; if equal user distribution is desired, then Active/Active mode might be preferred.

Clustering over WAN

Cisco Unified Presence Release 8.5(x) or later releases support Clustering over WAN deployments. Any earlier Cisco Unified Presence 8.0(x) releases do not support Clustering over WAN.

Related Topic
Clustering over WAN for Intracluster and Intercluster Deployments, page 2-4

IM-only Deployment

Cisco Unified Presence supports an IM-only deployment. This type of deployment supports up to 25,000 users per node and up to 75,000 users in a Cisco Unified Presence cluster.

Related Topic
Cisco Unified Presence Configuration for an IM-only Deployment, page 5-1

User Assignment

To allow users receive the availability and Instant Messaging (IM) services on Cisco Unified Presence, you must assign users to nodes, and subclusters, in your Cisco Unified Presence deployment. You can manually or automatically assign users in a Cisco Unified Presence deployment. You manage user assignment using the User Assignment Mode parameter on the Sync Agent on Cisco Unified Presence.

If you choose automatic user assignment, the Sync Agent assigns the users to all nodes in all subclusters in an attempt to balance the user assignment evenly across all nodes. You can also configure the Sync Agent to assign the total number of users to only the first (active) node of a subcluster.

If you choose manual user assignment, you must manually assign your users to nodes, and subclusters, using the System Topology interface in Cisco Unified Presence Administration.

User Assignment Mode Recommendations

You can manually or automatically assign users in a Cisco Unified Presence deployment. Use the User Assignment Mode parameter on the Sync Agent to manage user assignment on Cisco Unified Presence:
If set to **Balanced**, Cisco Unified Presence divides all users equally across all nodes in all subclusters. Use this user assignment mode for the Balanced Mode Non-Redundant High Availability and the Balanced Mode Redundant High Availability deployment options.

If set to **Active/Standby**, Cisco Unified Presence assigns all users only to the first node of a subcluster. If there is only a single node in the subcluster, Cisco Unified Presence uses this node for assignment regardless of the location of the node within the subcluster.

If set to **None**, you must manually assign your users to nodes in system topology management GUI.

- **Note**
  - If all the hardware in your cluster is of the same generation and has the same capacity, set the User Assignment Mode to **Balanced**.
  - If you have hardware of mixed generations and capacities in a node, set the User Assignment Mode to **None**. Manually assign your users making sure that each server is not loaded beyond capacity.

**Related Topics**

*User Redistribution, page 1-8*

**Manual User Assignment Recommendations**

If you choose to manually assign users in system topology management GUI, note the following:

- You can manually unassign, assign or reassign users. You can assign users to a single node, and you can also distribute groups of users across the node, or nodes, in a cluster, or a given subcluster.

- If you assign a user to one of the nodes in a subcluster, the other node in the subcluster can become the backup (redundant) node for the user if you turn on High Availability for the subcluster. If you do not configure a backup node in the subcluster, and you do not turn on High Availability for the subcluster, the user does not have High Availability failover protection.

- Users who are assigned may be reassigned, that is, moved to another subcluster, or to a specific node. You can move users individually or in bulk.

- Users can remain unassigned. Unassigned users do not receive availability information.

- **Note**
  - Cisco recommends that you only reassign a user (assign a user that was previously unassigned) if the Cisco UP Presence Engine is running on all nodes in your cluster, otherwise Cisco Unified Presence will not reestablish the availability subscriptions to and from this user.

When you are assigning users, note the following:

- You can only assign users if they are licensed.

- Unassigning or reassigning users results in termination of active sessions. In such instances, clients must reconnect to the new location.

- You can export users in bulk using the Bulk Administration Tool (BAT). You can also use BAT to perform bulk user reassignment from one node to another.

Generally, Cisco recommends that you take the Cisco UP Presence Engine and Cisco UP SIP Proxy services offline when performing bulk operations. Note that taking these services offline will adversely impact performance.
User Redistribution

Note

- If you turn on High Availability in a subcluster, be aware that Cisco Unified Presence does not redistribute users to nodes that are in a failover states; the valid node states that support user redistribution are Normal and Running in Backup Mode.
- If you rebalance your users, you must reconfigure the upper and lower client re-login limit values based on the HA login profile tables, see High Availability Client Login Profiles, page I-1.

After adding or removing nodes, you can redistribute users using the Rebalance Users parameter in system topology management GUI. This parameter redistributes users based on the configured User Assignment mode. These are examples of how you can use the Rebalance Users parameter with the User Assignment mode to manage user assignment:

- Scenario A: The customer has a subcluster with two nodes, and each node contains 5000 users. The User Assignment mode is set to Balanced. The customer then adds a second subcluster with two nodes, and sets the Rebalance Users parameter. Cisco Unified Presence distributes the users evenly to the four nodes so that each node now has 2500 users.
- Scenario B: The customer has a subcluster with two nodes, and each node contains 2500 users. The User Assignment mode is set to Balanced. The customer wants to add a second subcluster with two nodes, but also wants to change the User Assignment mode to Active/Standby. The customer changes the mode to Active/Standby, whereby all 5000 users are redistributed to the first node in the subcluster. The customer then adds a second subcluster with two nodes, and sets the Rebalance Users parameter. Cisco Unified Presence evenly distributes the users across both first nodes in each subcluster. Each first node now has 2500 users.

Cisco strongly recommends that you perform any node movements that involve unassigning or moving a large numbers of users at off peak times. Such large operations can adversely impact performance.

Related Topics

- Node Creation and Movement Recommendations, page 17-5
- Configure User Assignment in System Topology, page 15-1

End User Management

You can use the Cisco Unified Presence GUI to perform the following end user management tasks:

- Authorize presence subscription requests.
- Export contact lists.
- Import contact lists on the home cluster.
For instructions to migrate Cisco Unified Presence users, see topics related to user migration between clusters, user management, and administration.

## Availability and Instant Messaging

### Chat

Point-to-point Instant Messaging (IM) supports real-time conversations between two users at a time. Cisco Unified Presence exchanges messages directly between users, from the sender to the recipient. Users must be online in their IM clients to exchange point-to-point IMs.

From Cisco Unified Presence Release 8.5(x) and later, you can disable both the chat and availability functionality on Cisco Unified Presence.

#### Related Topics
- Turn On or Off Instant Messaging for a Cisco Unified Presence Cluster, page 13-4
- Turn On or Off Availability Sharing, page 13-1

### IM Forking

When a user sends an IM to a contact who is signed in to multiple IM clients, Cisco Unified Presence delivers the IM to each client. This functionality is called IM forking. Cisco Unified Presence continues to fork IMs to each client, until the contact replies. Once the contact replies, Cisco Unified Presence only delivers IMs to the client on which the contact replied.

*Note*

IM forking is not supported when using Cisco IP Phone Messenger (IPPM) with Cisco Unified Personal Communicator Release 7.0.

#### Related Topic

Turn On or Off Offline Instant Messaging, page 13-5

### Offline IM

Offline IM is the ability to send IMs to a contact when they are offline. When a user sends an IM to an offline contact, Cisco Unified Presence stores the IM and delivers the IM when the offline contact signs in to an IM client. From Cisco Unified Presence Release 8.5(x) and later, you can disable offline instant messaging on Cisco Unified Presence.

### Broadcast IM

Broadcast IM is the ability to send an IM to multiple contacts at the same time, for example, a user wants to send a notification to a large group of contacts. Note that not all IM clients support this feature.
Chat Rooms on Cisco Unified Presence

Cisco Unified Presence supports IM exchange in both temporary (ad-hoc) chat rooms and persistent (persistent) chat rooms. By default, the Text Conference (TC) component on Cisco Unified Presence is set up and configured to handle IM exchange in temporary (ad-hoc) chat rooms. There are additional requirements you must configure to support persistent chat rooms, described further in this module.

Temporary chat rooms are IM sessions that remain in existence only as long as one person is still connected to the chat room, and are deleted from the system when the last user leaves the room. Records of the IM conversation are not maintained permanently.

Persistent chat rooms are persistent IM sessions that remain in existence even when all users have left the room and do not terminate like temporary IM sessions. The intent is that users will return to persistent chat rooms over time to collaborate and share knowledge of a specific topic, search through archives of what was said on that topic (if this feature is enabled on Cisco Unified Presence), and then participate in the discussion of that topic in real-time.

The TC component on Cisco Unified Presence enables users to:

- create new rooms, and manage members and configurations of the rooms they create.
- invite other users to rooms.
- determine the availability status of the members displayed within the room. The availability status displayed in a room confirms the attendance of the member in a room but may not reflect their overall availability status.

The Persistent Chat feature on Cisco Unified Presence allows users to:

- search for and join existing chat rooms.
- store a transcript of the chat and make the message history available for searching.

Chat Room Limits

<table>
<thead>
<tr>
<th>Number Of...</th>
<th>Maximum</th>
</tr>
</thead>
<tbody>
<tr>
<td>Persistent chat rooms per node</td>
<td>1500 rooms</td>
</tr>
<tr>
<td>Total rooms per node (temporary and persistent)</td>
<td>16500 rooms</td>
</tr>
<tr>
<td>Occupants per room</td>
<td>1000 occupants</td>
</tr>
<tr>
<td>Messages that appear in chat history.</td>
<td>100 messages</td>
</tr>
</tbody>
</table>

*Note* The default value is 15 messages.

File Transfer

Cisco Unified Presence Release 8.6(x) supports point to point file transfer between XMPP clients compliant with XEP 096 (http://xmpp.org/extensions/xep-0096.html).

For more information, see *Enable File Transfer*, page 18-5.
Important Notes about Cisco Unified Presence and Chat

For SIP to SIP IM, the following services must be running on Cisco Unified Presence:

- Cisco UP SIP Proxy
- Cisco UP Presence Engine
- Cisco UP XCP Router

For SIP to XMPP IM, the following services must be running on Cisco Unified Presence:

- Cisco UP SIP Proxy
- Cisco UP Presence Engine
- Cisco UP XCP Router
- Cisco UP XCP Text Conference Manager

IM Compliance

Instant Message (IM) compliance is a server-side login solution. For information about configuring IM compliance on Cisco Unified Presence, refer to the following documents:

- Instant Messaging Compliance Guide for Cisco Unified Presence:
- Database Setup Guide for Cisco Unified Presence

Cisco Unified Communications Manager Integration

LDAP Integrations

You can configure a corporate LDAP directory in this integration to satisfy a number of different requirements:

- User provisioning: You can provision users automatically from the LDAP directory into the Cisco Unified Communications Manager database. Cisco Unified Communications Manager synchronizes with the LDAP directory content so you avoid having to add, remove, or modify user information manually each time a change occurs in the LDAP directory.

- User authentication: You can authenticate users using the LDAP directory credentials. Cisco Unified Presence synchronizes all the user information from Cisco Unified Communications Manager to provide authentication for users of the Cisco Unified Personal Communicator client and Cisco Unified Presence user interface.
- **User lookup**: You can enable LDAP directory lookups to allow Cisco Unified Personal Communicator client users, or third-party XMPP clients, to search for and add contacts from the LDAP directory.


As the scope of the LDAP integration is dependent on customer requirements and it can vary between companies, there are a number of potential LDAP integration scenarios:

1. You integrate Cisco Unified Communications Manager and Cisco Unified Personal Communicator with an LDAP directory. Cisco strongly recommends this configuration.

2. You integrate Cisco Unified Communications Manager with an LDAP directory, but you do not integrate Cisco Unified Personal Communicator. Cisco does not recommend this configuration because it will impact Cisco Unified Personal Communicator functionality and you will experience performance issues.

3. You integrate Cisco Unified Personal Communicator with an LDAP directory, but you do not integrate Cisco Unified Communications Manager. Cisco does not recommend this configuration because you will have to manually configure all your users on Cisco Unified Communications Manager at initial installation, and each time a change is made on the LDAP directory.

  **Note** When Cisco Unified Communications Manager is not integrated with LDAP, you must verify that the username is *exactly* the same in Active Directory and Cisco Unified Communications Manager before deploying Cisco Unified Presence. If the letter case does not match, the availability status will not work properly in Cisco Unified Personal Communicator Release 7.x. Correct the username in Cisco Unified Communications Manager to match Active Directory.

**Related Topics**

- LDAP Directory Integration with Cisco Unified Personal Communicator, page 9-6

---

**Third-party Integrations**

This guide only details how to configure a basic Cisco Unified Presence deployment. For third-party integrations, see the documents below.
### Third Party Integration

<table>
<thead>
<tr>
<th>Third Party Integration</th>
<th>This Guide Describes...</th>
</tr>
</thead>
</table>
| Integrating Cisco Unified Presence with Microsoft Exchange | • Integrating with Microsoft Exchange 2003, 2007 and 2010  
• Configuring Microsoft Active Directory for this integration |
| Integrating Cisco Unified Presence with Microsoft OCS/LCS for MOC Call Control | • Configuring Cisco Unified Presence as a CSTA gateway for remote call control from the Microsoft Office Communicator client  
• Configuring Microsoft Active Directory for this integration  
• Load-balancing MOC requests in a dual node Cisco Unified Presence deployment over TCP  
• Load-balancing MOC requests in a dual node Cisco Unified Presence deployment over TLS |
| Integrating Cisco Unified Presence for Interdomain Federation | • Configuring Cisco Unified Presence for interdomain federation over the SIP protocol with Microsoft OCS and AOL, and over the XMPP protocol with IBM Sametime, GoogleTalk, WebEx Connect, and another Cisco Unified Presence Release 8.x enterprise. |

### Related Topic
Cisco Unified Presence third-party integration documentation:

### Third-party Client Integrations

### Supported Third-party XMPP Clients
Cisco Unified Presence supports standards-based XMPP to enable third-party XMPP client applications to integrate with Cisco Unified Presence for availability and instant messaging (IM) services. Third-party XMPP clients must comply with the XMPP standard as outlined in the Cisco Software Development Kit (SDK).

This module describes the configuration requirements for integrating XMPP clients with Cisco Unified Presence. If you are integrating XMPP-based API (web) client applications with Cisco Unified Presence, also see developer documentation for Cisco Unified Presence APIs on the Cisco Developer Portal.

### Related Topic
Cisco Developer portal:
http://developer.cisco.com/
License Requirements for Third-party Clients

For each user of an XMPP client application, you require a Cisco Unified Presence user feature license. The Cisco Unified Presence user feature license consumes one Cisco Unified Communications Manager Device License Unit (DLU). On Cisco Unified Communications Manager, you will need to upload the user DLU, and assign Cisco Unified Presence capabilities to the user.

Related Topics

XMPP Client Integration on Cisco Unified Communications Manager

Before you integrate an XMPP client, perform the following tasks on Cisco Unified Communications Manager:

- Configure the licensing requirements. Upload the user DLU, and then assign Cisco Unified Presence capabilities for the user.
- Configure the users and devices. Associate a device with each user, and associate each user with a line appearance.

Related Topics
- Installation Guide for Cisco Unified Presence Release 8.6
- User and Device Configuration on Cisco Unified Communications Manager, page 6-2.

LDAP Integration for XMPP Contact Search

To allow users of the XMPP client applications to search and add contacts from an LDAP directory, configure the LDAP settings for XMPP clients on Cisco Unified Presence.

Related Topic
Configure the LDAP Search Settings for XMPP Clients, page 9-14

Domain Name for XMPP Clients

The domain name on the XMPP client, specifically the XMPP connection attempt domain name, must match the domain on Cisco Unified Presence. To verify the domain value on Cisco Unified Presence, choose Cisco Unified Presence Administration > System > Cluster Topology, click Settings in the right pane, and verify the Domain Name value.
DNS Configuration for XMPP Clients

You must enable DNS SRV in your deployment when you integrate XMPP clients with Cisco Unified Presence. The XMPP client performs a DNS SRV query to find an XMPP server (Cisco Unified Presence) to communicate with, and then performs a record lookup of the XMPP server to get the IP address.

Security

You can configure a secure connection between Cisco Unified Presence and Cisco Unified Communications Manager, XMPP clients, and SIP clients by exchanging certificates. Certificates can be self-signed or generated by a Certificate Authority (CA).

Related Topic
Security Configuration on Cisco Unified Presence
Multi-node Scalability and WAN Deployments

Multi-node Scalability Feature

Scalability Enhancements

The Cisco Unified Presence multi-node scalability feature supports the following:

- Maximum of six nodes per cluster
- In an IM-only deployment, 25,000 users per node
- 45,000 users per cluster with maximum of 15,000 users per node in a full Unified Communication mode deployment
- Administrable customer-defined limit on the maximum contacts per user (default unlimited).
- Cisco Unified Presence continues to support intercluster deployments with the multi-node feature.
- With High Availability enabled, subclusters include active nodes and standby nodes, whereby the standard node takes over when the active node goes down.

Scalability Options for Deployment

Cisco Unified Presence clusters can support up to six nodes. If you originally installed less than six nodes, then you can install additional nodes at any time. If you want to scale your Cisco Unified Presence deployment to support more users, you must consider the multi-node deployment model you have configured. Table 2-1 describes the scalability options for each multi-node deployment model.
Cluster-wide DNS SRV

For DNS configuration, you can define a cluster-wide Cisco Unified Presence address. The SIP Publish Trunk on Cisco Unified Communications Manager uses this address to load-balance SIP PUBLISH messages from Cisco Unified Communications Manager to all nodes in the Cisco Unified Presence cluster. Notably this configuration ensures that the initial SIP PUBLISH messages are load-balanced...
Configuration and Administration of Cisco Unified Presence Release 8.6

Chapter 2 Multi-node Scalability and WAN Deployments

Local Failover

You can also deploy Cisco Unified Presence over WAN where one subcluster is located in one geographic site, and a second subcluster is located in another geographic site. The subcluster can contain a single node, or a dual node for High Availability between the local nodes. This model provides no failover between geographic sites.

Subcluster Failure Detection

Cisco Unified Presence supports a failure detection mechanism for a subcluster. Each node in the subcluster monitors the status, or heartbeat, of the peer node. You can configure the heartbeat connection and heartbeat intervals on Cisco Unified Presence by choosing Cisco Unified Presence Administration > System > Service Parameters > Cisco UP Config Agent (service). In the section General Cisco UP Config Agent Parameters (Clusterwide), configure the following parameters:

- **Heart Beat Interval**: This parameter specifies how often in seconds the Cisco UP Config Agent sends a heartbeat message to the peer Cisco UP Config Agent in the same subcluster. The heartbeat is used to determine network availability. The default value is 60 seconds.
- **Connect Timeout**: This parameter specifies how long in seconds the Cisco UP Config Agent waits to receive a response from a connection request to the peer Cisco UP Config Agent. The default value is 30 seconds.

**Note**
Cisco recommends that you configure these parameters with the default values.

Method Event Routing

External Database Recommendations

If you configure external database server(s) in your Clustering over WAN deployment, Cisco recommends that you co-locate the external database server(s) with the Cisco Unified Presence servers that will use the external database server(s).

Related Topic

Database Setup Guide for Cisco Unified Presence


Clustering over WAN for Intracluster and Intercluster Deployments

Cisco Unified Presence supports clustering over WAN for intracluster and intercluster deployments.

Intracluster Deployments over WAN

Cisco Unified Presence supports intracluster deployments over WAN, using the bandwidth recommendations provided in this module. Cisco Unified Presence supports a single subcluster geographically split over WAN, where one node in the subcluster is in one geographic site and the second node in the subcluster is in another geographic location.

This model can provide geographical redundancy and remote failover, for example failover to a backup Cisco Unified Presence node on a remote site. With this model, the Cisco Unified Presence server does not need to be co-located with the Cisco Unified Communications Manager publisher server. The Cisco Unified Personal Communicator client can be either local or remote to the Cisco Unified Presence server.

This model also supports High Availability for the Cisco Unified Personal Communicator Release 7.x and Cisco Unified Personal Communicator Releases 8.5 and 8.6.

Cisco Unified Presence also supports multiple subclusters in a Clustering over WAN deployment. For information about scale for a Clustering over WAN deployment, see the Cisco Unified Presence SRND.

Related Topic

Cisco Unified Presence Solution Reference Network Design (SRND):

http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/srnd/7x/uc7_0.html
Multi-node Configuration for Deployment over WAN

When you configure the Cisco Unified Presence multi-node feature for an intracluster deployment over WAN, configure the Cisco Unified Presence subcluster, nodes and user assignment as described in the multi-node section, but note the following recommendations:

- For optimum performance, Cisco recommends that you assign the majority of your users to the home Cisco Unified Presence node. This deployment model decreases the volume of messages sent to the remote Cisco Unified Presence server over WAN, however the failover time to the secondary node depends on the number of users failing over.

- If you wish to configure a High Availability deployment model over WAN, you can configure a subcluster-wide DNS SRV address. In this case Cisco Unified Presence sends the initial PUBLISH request message to the node specified by DNS SRV and the response message indicates the host node for the user. Cisco Unified Presence then sends all subsequent PUBLISH messages for that user to the host node. Before configuring this High Availability deployment model, you must consider if you have sufficient bandwidth for the potential volume of messages that may be sent over the WAN.

Related Topics
- Intracluster Deployments over WAN, page 2-4
- Multi-node Deployment Administration, page 17-1

Intercluster Deployments

Intercluster Deployments over WAN

Cisco Unified Presence supports intercluster deployments over WAN, using the bandwidth recommendations provided in this module. This bandwidth is during database sync.

Related Topics
- WAN Bandwidth Requirements, page 3-3
- Intercluster Peer Configuration, page 12-1

Intercluster Peer Relationships

You can configure peer relationships that interconnect standalone Cisco Unified Presence clusters, known as intercluster peers. This intercluster peer functionality allows users in one Cisco Unified Presence cluster to communicate and subscribe to the availability information of users in a remote Cisco Unified Presence cluster within the same domain. Keep in mind that if you delete an intercluster peer from one cluster, then you must also delete the corresponding peer in the remote cluster.

Cisco Unified Presence uses the AXL/SOAP interface to retrieve user information for the home cluster association. Cisco Unified Presence uses this user information to detect if a user is a local user (user on the home cluster), or a user on a remote Cisco Unified Presence cluster within the same domain.

Cisco Unified Presence uses the XMPP interface for the subscription and notification traffic. If Cisco Unified Presence detects a user to be on a remote cluster within the same domain, Cisco Unified Presence reroutes the messages to the remote cluster.
Note
If you configure an intercluster deployment between a Cisco Unified Presence Release 8.0(x) cluster and a cluster running a previous version of Cisco Unified Presence, Cisco Unified Presence uses the existing SIP interface for the subscription and notification traffic.

Caution
Cisco highly recommends that you set up intercluster peers in a staggered manner, as the initial sync uses substantial bandwidth and CPU. Setting up multiple peers at the same time could result in excessive sync times.

Related Topic
How to Perform Intercluster Upgrades. For more information, see the Upgrade Guide for Cisco Unified Presence Release 8.6.

Intercluster Router-to-Router Connections

By default, Cisco Unified Presence assigns all nodes in a cluster as intercluster router-to-router connectors. When Cisco Unified Presence establishes an intercluster peer connection between the clusters over the AXL interface, it synchronizes the information from all intercluster router-to-router connector nodes in the home and remote clusters. Each intercluster router-to-router connector in one cluster then either initiates or accepts an intercluster connection with router-to-router connectors in the other cluster.

Note
Router-to-router connections are dynamically established when a new node is added to the deployment. As a result, you do not need to restart the Cisco UP XCP Router on any node in your deployment when you add a new node.

Related Topic
You can configure a secure XMPP connection between all router-to-router connectors in your Cisco Unified Presence deployment, incorporating both intracluster and intercluster router to router connections. Choose Cisco Unified Presence Administration > System > Security > Settings, and check Enable XMPP Router-to-Router Secure Mode., page 2-7

Node Name Value for Intercluster

Cisco Unified Presence Release 8.6(4) and Earlier

Note
This topic is only applicable if you are not using DNS in your network.

If you configure an intercluster deployment, and you do not use DNS in your network, you must configure the node name value as the IP address of the node.

During installation Cisco Unified Presence only permits you to specify the hostname as the node name value. Therefore, once you complete the installation, you must change the node name value to the IP address of the node.

Perform this configuration on all nodes in both the local and remote clusters.
Cisco Unified Presence Release 8.6(5) and Later

The node name defined for any Cisco Unified Presence node must be resolvable by every other Cisco Unified Presence node on every cluster. Therefore, each Cisco Unified Presence node name must be the FQDN of the node. If DNS is not deployed in your network, each node name must be an IP address.

**Note**
Specifying the hostname as the node name is only supported if all nodes across all clusters share the same DNS domain.

**Note**
When using the Cisco Jabber client, certificate warning messages can be encountered if the IP address is configured as the IM and Presence Service node name. To prevent Cisco Jabber from generating certificate warning messages, the FQDN should be used as the node name.

**Related Topics**
- Cluster Topology Management, page 17-5
- Domain Value for Intercluster Deployments, page 2-7

### Domain Value for Intercluster Deployments

**Note**
This topic is only applicable if you are not using DNS in your network.

If you configure an intercluster deployment, note the following regarding the presence domain value:

- The presence domain value on the local cluster must match the presence domain value on the remote cluster to ensure that intercluster functionality will work correctly.
- If you do not use DNS in your network, Cisco Unified Presence automatically defaults to the Presence domain value DOMAIN.NOT.SET. On both the local and remote cluster, you must replace this default value with a common valid presence domain value, otherwise intercluster functionality will not work correctly.

To configure the Domain value, follow the procedures described in Domain Value Configuration, page 7-7.

**Related Topic**
Node Name Value for Intercluster, page 2-6

### Secure Intercluster Router-to-Router Connections

You can configure a secure XMPP connection between all router-to-router connectors in your Cisco Unified Presence deployment, incorporating both intracluster and intercluster router to router connections. Choose Cisco Unified Presence Administration > System > Security > Settings, and check Enable XMPP Router-to-Router Secure Mode.

When you turn on the secure mode for XMPP router-to-router connections, Cisco Unified Presence enforces a secure SSL connection using XMPP trust certificates. For intercluster deployments, Cisco Unified Presence enforces a secure SSL connection between each router-to-router connector node in the local cluster, and each router connector node in the remote cluster.
Clustering over WAN for Intracluster and Intercluster Deployments
Cisco Unified Presence Planning Requirements

June 16, 2014

- Multi-node Hardware Recommendations, page 3-1
- Intercluster Hardware Recommendations, page 3-2
- Supported Cisco End Points, page 3-2
- Supported LDAP Servers, page 3-2
- WAN Bandwidth Requirements, page 3-3
- Multi-node Performance Recommendations, page 3-4

Multi-node Hardware Recommendations

When configuring the multi-node feature, consider the following:

- Cisco recommends turning on High Availability in your deployment.
- Minimize your hardware, for example, instead of using six MCS 7825 servers that support a total of six thousand users, choose two MCS 7835 servers that can support a total of five thousand users.
- Use the same generation of server hardware.
- Use similar hardware for all nodes in your deployment. If you must mix generations of similar hardware, put the same generations of older hardware together in a subcluster and put fewer users on this subcluster than on the more powerful subclusters. Note that we do not recommend this deployment practice.

**Warning**

For multi-node deployments using mixed hardware (for example, UCS, MCS, or VMware), it is highly recommended that the subscriber and publisher nodes in the same subcluster have similar database size. If a significant difference in database size exists between the two nodes, you will receive an error during installation of the subscriber node.

- Use the following disk drives for the multi-node feature:
  - MCS 7816: minimum one 160GB drive (a 250GB drive can also be used)
  - MCS 7825: minimum two 160GB drives (two 250GB drives can also be used, upgrade required from smaller 80GB drives)
  - MCS 7835: minimum two 146GB drives (upgrade required from smaller 72GB drives)
  - MCS 7845: minimum four 72GB drives (upgrade recommended to four 146GB drives)
Intercluster Hardware Recommendations

When planning an intercluster deployment, it is recommended that similar hardware is used on all Cisco Unified Presence clusters in the Enterprise to allow for syncing of all user data between clusters. For example, if an MCS 7845 is deployed in Cluster A with 15,000 users, then an MCS 7845 should be deployed in Cluster B, even if only needed for 500 users.

Supported Cisco End Points

The multi-node scalability feature supports the following Cisco end points:

- Cisco Unified Communications Manager (desk phone)
- Cisco Unified Personal Communicator Release 8.x (XMPP client)
- Cisco Unified Personal Communicator Release 7.x (SIP client)
- Third-Party XMPP clients
- Cisco Jabber
- Microsoft Office Communicator (Microsoft soft client)
- Lotus Sametime (Lotus soft client)
- Third-Party Interface clients
- Lync 2010 Client (Microsoft Office Communicator client)

Supported LDAP Servers

Cisco Unified Presence integrates with these LDAP directory servers:

- Netscape Directory Server
• Sun ONE Directory Server 5.2
• OpenLDAP

For more information on the LDAP directory server support specifically for Cisco Unified Communications Manager and Cisco Unified Personal Communicator, see the specific product documentation below.

**Related Topics**

- *Release Notes for Cisco Unified Personal Communicator:*
- *Cisco Unified Communications Manager System Guide:*

## WAN Bandwidth Requirements

At a minimum, you must dedicate five megabits per second of bandwidth for each Cisco Unified Presence subcluster, with no more than an eighty millisecond round-trip latency. These bandwidth recommendations apply to both intracluster and intercluster WAN deployments. Any bandwidth less than this recommendation can adversely impact performance.

**Note**

Each Cisco Unified Presence subcluster that you add to your Clustering over WAN deployment requires an additional (dedicated) five megabits per second bandwidth.

## WAN Bandwidth Considerations

When you calculate the bandwidth requirements for your Clustering over WAN deployment, consider the following:

- In your bandwidth considerations, you must include the normal bandwidth consumption of a Cisco Unified Communications Manager cluster. If you configure multiple nodes, Cisco Unified Communications Manager uses a round-robin mechanism to load balance SIP/SIMPLE messages, which consumes more bandwidth. To improve performance and decrease traffic, you could provision a single dedicated Cisco Unified Communications Manager node for all SIP/SIMPLE messages sent between Cisco Unified Presence and Cisco Unified Communications Manager.
- In your bandwidth considerations, we also recommend that you consider the number of contacts in the contact list for a Cisco Unified Personal Communicator user, and the size of user profiles on Cisco Unified Presence. See the Cisco Unified Presence SRND for recommendations regarding the size of a contact list when you deploy Cisco Unified Presence over WAN. Note also that the default contact list size on Cisco Unified Presence is 200, so you need to factor this in to your bandwidth considerations for systems with large numbers of users.

**Related Topic**

Cisco Unified Presence Solution Reference Network Design (SRND):
http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/srnd/7x/uc7_0.html
Multi-node Performance Recommendations

You can achieve optimum performance with the multi-node feature when:

- The resources on all Cisco Unified Presence servers are equivalent in terms of memory, disk size, and age. Mixing hardware classes results in servers that are under-powered, therefore resulting in poor performance.
- You deploy hardware that complies with the hardware recommendations.
- You configure a Balanced Mode deployment model. In this case, the total number of users is equally divided across all nodes in all subclusters. Cisco Unified Presence defaults to Balanced Mode user assignment to achieve optimum performance.

Related Topics

- Clustering over WAN for Intracluster and Intercluster Deployments, page 2-4
- Balanced User Assignment Redundant High Availability Deployment, page 17-1
License Requirements

June 16, 2014

Cisco Unified Personal Communicator License Requirements, page 4-1

Cisco Unified Personal Communicator License Requirements

- User License Requirements, page 4-1
- Adjunct Licensing, page 4-2

User License Requirements

Cisco Unified Communications Manager tracks the number of Cisco Unified Personal Communicator devices that are connected to it and compares it with the number of device licenses that have been purchased.

Table 4-1 describes the user license requirements for Cisco Unified Personal Communicator.
Chapter 4      License Requirements

Adjunct Licensing

From Cisco Unified Communications Manager Release 6.0(1), you can associate a secondary device with a primary device and consume only one device license per device. This is also known as adjunct licensing. On Cisco Unified Communications Manager, you can configure adjunct licensing manually on the Phone Configuration window, using the AXL interface, or using the Bulk Administration Tool (BAT). For releases prior to Cisco Unified Communications Manager Release 6.0(1), three device licenses are consumed.

Adjunct licensing has these restrictions:

- You can associate up to two secondary softphone devices to a primary phone.
- You cannot delete the primary phone unless you remove the associated secondary softphone devices.
- The primary phone must be the device that consumes the most licenses. You cannot make the softphone device the primary phone and associate a Cisco Unified IP Phone as the secondary device.
- Secondary softphone devices are limited to Cisco IP Communicator, Cisco Unified Personal Communicator, and Cisco Unified Mobile Communicator.

What To Do Next

Obtain a license file. For more information, see the Installation Guide for Cisco Unified Presence Release 8.6.

Table 4-1  Cisco Unified Personal Communicator user licensing requirements

<table>
<thead>
<tr>
<th>Configuration</th>
<th>License Requirement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Unified Personal Communicator basic functionality</td>
<td>Cisco Unified Personal Communicator software license</td>
<td>You will require one Cisco Unified Personal Communicator software license per user. The Cisco Unified Personal Communicator software license comes with one Cisco Unified Communications Manager Device License Unit (DLU). You need to assign Cisco Unified Personal Communicator capabilities for a user. This will consume one DLU. On Cisco Unified Communications Manager, you will need to upload the software license for a user, and then assign Cisco Unified Personal Communicator capabilities for a user.</td>
</tr>
<tr>
<td>Cisco Unified Personal Communicator user feature license</td>
<td>You will require one Cisco Unified Personal Communicator user feature license per user. This license is also known as a Cisco Unified Communications Manager phone device license. You upload this license on Cisco Unified Communications Manager.</td>
<td></td>
</tr>
<tr>
<td>Softphone mode (optional)</td>
<td>Cisco Unified Personal Communicator user feature license registered as Cisco Unified Communications Manager softphone</td>
<td>In addition to the normal licensing requirements listed above, you require three Cisco Unified Communications Manager user feature licenses to register as a Cisco Unified Communications Manager softphone (three device licenses are consumed).</td>
</tr>
</tbody>
</table>
PART 2

System Configuration

- Cisco Unified Presence Configuration for an IM-only Deployment
- Cisco Unified Communications Manager Configuration for Integration with Cisco Unified Presence
- Cisco Unified Presence Network Setup
- IP Phone Presence Setup
- LDAP Directory Integration
- Third-party XMPP Client Application Configuration on Cisco Unified Presence
- Security Configuration on Cisco Unified Presence
- Intercluster Peer Configuration
IM-only Configuration Steps

An IM-only deployment supports up to 25,000 users per node and up to 75,000 users in a Cisco Unified Presence cluster. An overview of the configuration steps required to set up an IM-only Cisco Unified Presence deployment is provided in the following table.

<table>
<thead>
<tr>
<th>Configuration Procedure</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create your users on Cisco Unified Communications Manager.</td>
<td>See the Cisco Unified Communications Manager documentation at this URL: <code>http://www.cisco.com/en/US/products/sw/voicesw/ps556/tsd_products_support_series_home.html</code></td>
</tr>
<tr>
<td>On Cisco Unified Presence, perform these configuration procedures to integrate Cisco Unified Personal Communicator:</td>
<td>See the <code>Cisco Unified Personal Communicator Administration Guide for Cisco Unified Presence Release 8.6</code> for more information.</td>
</tr>
<tr>
<td>• Configure the Proxy Listener and TFTP Server Addresses</td>
<td></td>
</tr>
<tr>
<td>• Configure the Cisco Unified Personal Communicator Service Parameter</td>
<td></td>
</tr>
<tr>
<td>Integrate the LDAP server for Cisco Unified Personal Communicator</td>
<td>Follow the configuration procedures described in the chapter LDAP Directory Integration with Cisco Unified Personal Communicator, page 9-6.</td>
</tr>
</tbody>
</table>
CTI Interface

The CTI (Computer Telephony Integration) interface handles all the CTI communication for users on the Cisco Unified Presence server to control phones on Cisco Unified Communications Manager. The CTI functionality allows users of the Cisco Unified Personal Communicator client to run the application in desk phone control mode.

The CTI functionality is also used for the Cisco Unified Presence remote call control feature on the Microsoft Office Communicator client. For information about configuring the remote call control feature, see the Integration Note for Configuring Cisco Unified Presence with Microsoft OCS for MOC Call Control.

To configure CTI functionality for Cisco Unified Presence users on Cisco Unified Communications Manager, users must be associated with a CTI-enabled group, and the primary extension assigned to that user must be enabled for CTI.

To configure Cisco Unified Personal Communicator desk phone control, you must configure a CTI server and profile on Cisco Unified Presence, and assign any users that wish to use the application in desk phone mode to that profile. However, note that all CTI communication occurs directly between Cisco Unified Communications Manager and Cisco Unified Personal Communicator, and not through the Cisco Unified Presence server.

Related Topics

- User and Device Configuration on Cisco Unified Communications Manager, page 6-2
User and Device Configuration on Cisco Unified Communications Manager

Before you configure Cisco Unified Communications Manager for integration with Cisco Unified Presence, make sure that the following user configuration is completed on Cisco Unified Communications Manager. Device configuration is optional.

If you deploy Cisco Unified Personal Communicator, see the chapter on configuring Cisco Unified Communications Manager for Cisco Unified Personal Communicator deployment in the Cisco Unified Personal Communicator Administration Guide.

### Task Notes

**Modify the User Credential Policy**

- If you are not using LDAP,
  - This procedure is only applicable if you are integrating with Cisco Unified Communications Manager version 6.0 or a later release.
  - Cisco recommends that you set an expiration date on the credential policy for users. The only type of user that does not require a credential policy expiration date is an Application user.

**Note**

- If you are using an LDAP server to authenticate your users on Cisco Unified Communications Manager, Cisco Unified Communications Manager does not use the credential policy.

**Menu path**

Cisco Unified Communications Manager Administration > User Management > Credential Policy Default

---

**(Optional) Configure the phone devices, and associate a Directory Number (DN) with each device**

- Check **Allow Control of Device from CTI** to allow the phone to interoperate with the Cisco Unified Personal Communicator client.

**Note**

- For details about configuring a Client Services Framework (CSF), see...(refer to applicable CUCM document).

**Menu path**

Cisco Unified Communications Manager Administration > Device > Phone

---

**Configure the users, and associate a device with each user**

- If you are planning to deploy Cisco Unified Personal Communicator, make sure that the user ID value is unique for each user. The user ID is converted into the softphone device name, and if two users have the same softphone device name Cisco Unified Personal Communicator will not be able to derive the softphone device name, and as a result, will not function properly.

**Menu path**

Cisco Unified Communications Manager Administration > User Management > End User.

---

- Section “How to Configure CTI Gateway Settings for Desk Phone Control on Cisco Unified Presence” in the *Cisco Unified Personal Communicator Administration Guide for Cisco Unified Presence Release 8.6*.
- **Integration Note for Configuring Cisco Unified Presence with Microsoft OCS for MOC Call Control:**
  
Configuring the Inter-Presence Group Subscription Parameter

You enable the Inter-Presence Group Subscription parameter to allow users in one presence group to subscribe to the availability information for users in a different presence group.

**Restriction**

You can only enable the Inter-Presence Group Subscription parameter when the subscription permission for the default Standard Presence Group, or any new Presence Groups, is set to **Use System Default**. To configure Presence Groups, choose **Cisco Unified Communications Manager Administration > System > Presence Groups.**

**Procedure**

1. Choose **Cisco Unified Communications Manager Administration > System > Service Parameters.**
2. Choose Cisco Unified Communications Manager server from the Server menu.
3. Choose **Cisco CallManager** from the Service menu.
4. Click **Allow Subscription** for Default Inter-Presence Group Subscription in the Clusterwide Parameters (System - Presence) section.
5. Click **Save.**

**Related Topic**

Configure Routing Communication, page 7-12
SIP Trunk Configuration on Cisco Unified Communications Manager

Note

The port number that you configure for the SIP Trunk differs depending on the version of Cisco Unified Presence that you are deploying:

- For Cisco Unified Presence version 6.x, configure the port number 5070 for the SIP Trunk.
- For Cisco Unified Presence version 7.0(x) or higher, configure the port number 5060 for the SIP Trunk.

- Configure the SIP Trunk Security Profile for Cisco Unified Presence, page 6-4
- Configuring the SIP Trunk for Cisco Unified Presence, page 6-5

Configure the SIP Trunk Security Profile for Cisco Unified Presence

Procedure

Step 1  Choose Cisco Unified Communications Manager Administration > System > Security > SIP Trunk Security Profile.
Step 2  Click Find.
Step 3  Choose Non Secure SIP Trunk Profile.
Step 4  Click Copy and enter “CUP Trunk” in the Name field.
Step 5  Verify that the setting for Device Security Mode is Non Secure.
Step 6  Verify that the setting for Incoming Transport Type is TCP+UDP.
Step 7  Verify that the setting for Outgoing Transport Type is TCP.
Step 8  Check to enable these items:
  - Accept Presence Subscription
  - Accept Out-of-Dialog REFER
  - Accept Unsolicited Notification
  - Accept Replaces Header
Step 9  Click Save.

What To Do Next
Configuring the SIP Trunk for Cisco Unified Presence, page 6-5
Configuring the SIP Trunk for Cisco Unified Presence

You only configure one SIP trunk between a Cisco Unified Communications Manager cluster and a Cisco Unified Presence cluster. After you configure the SIP trunk, you must assign that SIP trunk as the CUP PUBLISH trunk on Cisco Unified Communications Manager by choosing Cisco Unified Communications Manager Administration > System > Service Parameters.

In the Destination Address field, enter a value using one of the following formats:

- Dotted IP Address
- Fully Qualified Domain Name (FQDN)
- DNS SRV

If High Availability is configured for the Cisco Unified Presence cluster, multiple entries should be entered in the Dotted IP Address or FQDN to identify the various nodes in the cluster. DNS SRV cannot be used for a Cisco Unified Presence cluster if High Availability is configured.

Before You Begin

- Configure the SIP Trunk security profile on Cisco Unified Communications Manager.
- Read the Presence Gateway configuration options topic.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Choose Cisco Unified Communications Manager Administration &gt; Device &gt; Trunk.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Click Add New.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Choose SIP Trunk from the Trunk Type menu.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Choose SIP from the Device Protocol menu.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Choose None for the Trunk Service Type.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Click Next.</td>
</tr>
<tr>
<td>Step 7</td>
<td>Enter CUPS-SIP-Trunk for the Device Name.</td>
</tr>
<tr>
<td>Step 8</td>
<td>Choose a device pool from the Device Pool menu.</td>
</tr>
<tr>
<td>Step 9</td>
<td>In the SIP Information section at the bottom of the window, configure the following values:</td>
</tr>
</tbody>
</table>

  a. In the Destination Address field, enter the dotted IP address, or the FQDN (Fully Qualified Domain Name), which can be resolved by DNS and must match the SRV Cluster Name configured on the Cisco Unified Presence server. For more information, see Configure a Cluster-wide Cisco Unified Presence Address, page 17-24.

  b. Check the Destination Address is an SRV checkbox if you are configuring a multi-node deployment. In this scenario, Cisco Unified Communications Manager performs a DNS SRV record query to resolve the name, for example _sip._tcp.hostname.tld. If you are configuring a single-node deployment, leave this checkbox unchecked and Cisco Unified Communications Manager will perform a DNS A record query to resolve the name, for example hostname.tld.

Note

In both scenarios, the Cisco Unified Communications Manager SIP trunk Destination Address must resolve by DNS and match the SRV Cluster Name configured on the Cisco Unified Presence server. For more information, see Configure a Cluster-wide Cisco Unified Presence Address, page 17-24.
c. Enter **5060** for the Destination Port.
d. Choose **Non Secure SIP Trunk Profile** from the SIP Trunk Security Profile menu.
e. Choose **Standard SIP Profile** from the SIP Profile menu.

**Note**
If you modify the DNS entry of the Publish SIP Trunk SRV record by changing the port number or IP address, you must restart all devices that previously published to that address and ensure each device points to the correct Cisco Unified Presence contact.

---

**Step 10**
Click **Save**.

---

**Related Topics**
- Configure the SIP Trunk Security Profile for Cisco Unified Presence, page 6-4
- Configure the SIP Publish Trunk on Cisco Unified Presence, page 8-6
- Presence Gateway Configuration Option, page 8-5

**What To Do Next**
Cisco IP PhoneMessenger Configuration on Cisco Unified Communications Manager, page 14-1
or
Configure Cisco Unified Personal Communicator on Cisco Unified Communications Manager *(Cisco Unified Personal Communicator Administration Guide for Cisco Unified Presence Release 8.6)*

---

**Configure Phone Presence for Cisco Unified Communications Manager Outside of Cluster**

You can allow phone presence from a Cisco Unified Communications Manager that is outside the Cisco Unified Presence cluster. By default, requests from a Cisco Unified Communications Manager outside of the cluster is not accepted by Cisco Unified Presence. You can also configure a SIP trunk on Cisco Unified Communications Manager.

**Configuring a TLS Peer Subject**

When you import a Cisco Unified Presence certificate, Cisco Unified Presence automatically attempts to add the TLS peer subject to the TLS peer subject list, and to the TLS context list. Verify the TLS peer subject and TLS context configuration is set up to your requirements.

**Before You Begin**
You must configure the TLS Peer Subject before you configure the TLS Context.

**Procedure**

**Step 1**
Choose **Cisco Unified Presence Administration > System > Security > TLS Peer Subjects**.

**Step 2**
Click **Add New**.

**Step 3**
Perform one of the following actions for the Peer Subject Name:
Verify Required Services are Running on Cisco Unified Communications Manager

- Enter the subject CN of the certificate that the server presents.
- Open the certificate, look for the CN and paste it here.

Step 4 Enter the name of the server in the Description field.
Step 5 Click Save.

What To Do Next
Configuring a TLS Context, page 6-7

Configuring a TLS Context

When you import a Cisco Unified Presence certificate, Cisco Unified Presence automatically attempts to add the TLS peer subject to the TLS peer subject list, and to the TLS context list. Verify the TLS peer subject and TLS context configuration is set up to your requirements.

Before You Begin
Configure a TLS peer subject on Cisco Unified Presence.

Procedure

Step 1 Choose Cisco Unified Presence Administration > System > Security > TLS Context Configuration.
Step 2 Click Find.
Step 3 Choose Default_Cisco_UPS_SIP_Proxy_Peer_Auth_TLS_Context.
Step 4 From the list of available TLS peer subjects, choose the TLS peer subject that you configured.
Step 5 Move this TLS peer subject to Selected TLS Peer Subjects.
Step 6 Click Save.
Step 7 Choose Cisco Unified Presence Serviceability > Tools > Service Activation.
Step 8 Restart the Cisco Unified Presence SIP Proxy service for changes to the TLS context to take effect.

Related Topics
- Configuring a TLS Peer Subject, page 6-6
- Restart the SIP Proxy Service, page 11-4

Verify Required Services are Running on Cisco Unified Communications Manager

Procedure

Step 1 On Cisco Unified Communications Manager, choose Cisco Unified Serviceability> Tools > Control Center - Feature Services.
Step 2  Choose a Cisco Unified Communications Manager server from the Server menu.

Step 3  Make sure that the following services are running:
   - Cisco CallManager
   - Cisco TFTP (if you are deploying Cisco Unified Personal Communicator softphone)
   - Cisco CTIManager (if you are deploying Cisco Unified Personal Communicator in desk phone control mode)
   - Cisco AXL Web Service (for data synchronization between Cisco Unified Presence and Cisco Unified Communications Manager)

Step 4  If you need to turn on a specific service, choose Cisco Unified Serviceability > Tools > Service Activation.
Cisco Unified Presence Network Setup

June 16, 2014

- Configuration Changes and Service Restart Notifications, page 7-1
- DNS Domain Configuration, page 7-3
- Domain Value Configuration, page 7-7
- Routing Information Configuration on Cisco Unified Presence, page 7-11
- Configure the Proxy Server Settings, page 7-14
- SIP Digest Authentication, page 7-14
- Turn on Cisco Unified Presence Services, page 7-15

Configuration Changes and Service Restart Notifications

Service Restart Notifications

If you make a configuration change in Cisco Unified Presence Administration that impacts a Cisco Unified Presence XCP service, you will need to restart XCP services for your changes to take effect. Cisco Unified Presence notifies you of exactly which node the configuration change impacts and of any service that you must restart. An Active Notifications popup window displays on each page of Cisco Unified Presence Administration to serve as a visual reminder that you must restart services. Use your mouse to hover over the dialog bubble icon to see the list of active notifications (if any) and associated severity levels. From the list of active notifications you can go directly to Cisco Unified Serviceability, where you can restart the required service.

The topics in this module indicate if you need to perform a service restart, however it is good practice to monitor the service restart popup window for these notifications, particularly if you make any configuration changes after you deploy Cisco Unified Presence in the network.

See the Online Help topic on Service Restart Notifications for information about the types of service notifications, and the service notification security levels.

Related Topic
Cisco UP XCP Router Restart, page 7-2
Cisco UP XCP Router Restart

The Cisco UP XCP Router must be running for all availability and messaging services to function properly on Cisco Unified Presence. This applies to both SIP-based and XMPP-based client messaging. If you restart the Cisco UP XCP Router, Cisco Unified Presence automatically restarts all active XCP services.

The topics in this module indicate if you need to restart the Cisco UP XCP Router following a configuration change. Note that you must restart the Cisco UP XCP Router, not turn off and turn on the Cisco UP XCP Router. If you turn off the Cisco UP XCP Router, rather than restart this service, Cisco Unified Presence stops all other XCP services. Subsequently when you then turn on the XCP router, Cisco Unified Presence will not automatically turn on the other XCP services; you need to manually turn on the other XCP services.

Related Topic
DNs Domain Configuration, page 7-3

Restart the Cisco UP XCP Router Service

Procedure

Step 1 On Cisco Unified Presence, choose Cisco Unified Serviceability > Tools > Control Center - Network Services.
Step 2 Choose the server from the Server list box and click Go.
Step 3 Click the radio button next to the Cisco UP XCP Router service in the Cisco Unified Presence Services section.
Step 4 Click Restart.
Step 5 Click OK when a message indicates that restarting may take a while.

Related Topics
- Service Restart Notifications, page 7-1
- Cisco UP XCP Router Restart, page 7-2

Turn on the Cisco UP XCP Text Conference Service

This procedure applies if you configure the persistent chat room settings, or manually add one or more aliases to a chat node. You must also turn on this service if you want to enable temporary (ad-hoc) chat on a node.

Before You Begin
If persistent chat is enabled, an external database must be associated with the Text Conference Manager service, and the database must be active and reachable or the Text Conference Manager will not start. If the connection with the external database fails after the Text Conference Manager service has started, the Text Conference Manager service will remain active and functional, however, messages will no longer be persisted to database and new persistent rooms cannot be created until the connection recovers.
Chapter 7  Cisco Unified Presence Network Setup

DNS Domain Configuration

Cisco Unified Presence Release 8.6(4) and Earlier

For Cisco Unified Presence Release 8.6(4) and earlier the enterprise-wide presence domain and the DNS domain of any server must match.

Cisco Unified Presence Release 8.6(5) and Later

From Cisco Unified Presence Release 8.6(5), there is no requirement that the enterprise-wide presence domain aligns with the network-level DNS domain of any server.

Cisco Unified Presence deployments can potentially have nodes deployed across multiple network-level DNS domains. What can be supported is dependant on the Cisco Unified Presence node name configuration of each server in the deployment.

If any Cisco Unified Presence node name is set to its hostname, then all Cisco Unified Presence nodes must share the same DNS domain. However, Cisco Unified Presence nodes within a cluster may be deployed in a DNS domain that differs from the associated Cisco Unified Communications Manager cluster.

If all Cisco Unified Presence nodes within the deployment have a node name set to that node's Fully Qualified Domain Name (FQDN) or IP Address, the following deployment options are supported:

- Cisco Unified Presence clusters deployed in different DNS domains or subdomains
- Cisco Unified Presence nodes within a cluster deployed within different DNS domains or subdomains
- Cisco Unified Presence nodes within a cluster deployed in a DNS domain that is different to the associated Cisco Unified Communications Manager cluster

Procedure

Step 1  Choose Cisco Unified Serviceability > Tools > Service Activation.
Step 2  Choose the chat node from the Server menu.
Step 3  Choose the Cisco UP XCP Text Conference Manager service to turn it on.
Step 4  Click Save.

Related Topics
- Enable Persistent Chat, page 18-6
- Manage Chat Node Aliases Manually, page 18-10
- DNS Domain Configuration, page 7-3
Cisco Unified Presence Clusters Deployed in Different DNS Domain or Subdomains

Cisco Unified Presence supports having the nodes associated with one Cisco Unified Presence cluster in a different DNS domain or subdomain to the nodes that form a peer Cisco Unified Presence cluster. The diagram below highlights a sample deployment scenario supported by Cisco Unified Presence.

Figure 7-1  Cisco Unified Presence Clusters Deployed in Different DNS Domain or Subdomains

Cisco Unified Presence Nodes within a Cluster Deployed within Different DNS Domains or Subdomains

Cisco Unified Presence supports having the nodes within any Cisco Unified Presence cluster deployed across multiple DNS domains or subdomains. The following diagram highlights a sample deployment scenario supported by Cisco Unified Presence.

Note

Although the sample deployment in Figure 7-2 shows the Cisco Unified Presence node name set to the FQDN on all nodes, this deployment is also supported if the node name is set to hostname of IP address.
Cisco Unified Presence Nodes within a Cluster Deployed within Different DNS Domains or Subdomains

Note

High availability is also fully supported in scenarios where the two nodes within a High Availability subcluster are in different DNS domains or subdomains.

Cisco Unified Presence Nodes within a Cluster Deployed in a DNS Domain that is Different to the Associated Cisco Unified Communications Manager Cluster

Cisco Unified Presence supports having the Cisco Unified Presence nodes in a different DNS domain to their associated Cisco Unified Communications Manager cluster. The diagram below highlights a sample deployment scenario supported by Cisco Unified Presence.
Note

To support Availability Integration with Cisco Unified Communications Manager, the CUCM Domain SIP Proxy service parameter must match the DNS domain of the Cisco Unified Communications Manager cluster.

By default, the CUCM Domain SIP Proxy service parameter is set to the DNS domain of the Cisco Unified Presence publisher node. Therefore, if the DNS domain of the Cisco Unified Presence publisher node differs from the DNS domain of the Cisco Unified Communications Manager cluster, you must update this service parameter using the Cisco Unified Presence Administration GUI on the Cisco Unified Presence publisher node.

Related Topics

- Specify the DNS Domain Associated with Cisco Unified Communications Manager Cluster, page 7-7
- Domain Value Configuration, page 7-7
- Node Name Recommendations, page 17-6
- Changing the IP Address, Hostname and Domain Name for Cisco Unified Presence on cisco.com
Specify the DNS Domain Associated with Cisco Unified Communications Manager Cluster

**Note**
- This procedure applies only to Cisco Unified Presence Release 8.6(5) and later.
- This procedure is required only if the DNS domain of the Cisco Unified Presence publisher node differs from that of the Cisco Unified Communications Manager servers.

Cisco Unified Presence maintains Access Control List (ACL) entries for all Cisco Unified Communications Manager servers within the cluster. This enables seamless sharing of Availability between the servers. These ACL entries are FQDN based and are generated by appending the Cisco Unified Communications Manager hostname to the DNS domain of the Cisco Unified Presence publisher node.

If the DNS domain of the Cisco Unified Presence publisher node differs from that of the Cisco Unified Communications Manager servers, then invalid ACL entries will be added. To avoid this, you must perform the following procedure from the Cisco Unified Presence Administration GUI of the Cisco Unified Presence publisher node.

**Procedure**

**Step 1** Choose **Cisco Unified Presence Administration > System > Service Parameters**.

**Step 2** From the **Server** drop-down list, choose the Cisco Unified Presence server.

**Step 3** From the **Service** drop-down list, choose **Cisco UP SIP Proxy**.

**Step 4** Edit the **CUCM Domain** field in the General Proxy Parameters (Clusterwide) section to match the DNS domain of the Cisco Unified Communications Manager servers.

By default, this parameter is set to the DNS domain of the Cisco Unified Presence publisher node.

**Step 5** Click **Save**.

---

**Domain Value Configuration**

- Replacing the Default Presence Domain after Installation, page 7-7
- Changing the Presence Domain Value, page 7-9

**Replacing the Default Presence Domain after Installation**

Cisco Unified Presence automatically defaults the presence domain for the cluster to the DNS domain specified during Cisco Unified Presence installation. If you are not using DNS in your network and you did not set a DNS domain at install, the presence domain is set to “DOMAIN.NOT.SET” by default. You must replace this default value with the enterprise-wide presence domain.
Domain Value Configuration

Note
The presence domain must be identical across all clusters in the enterprise. If not, then intercluster communication will not be possible.

Cisco Unified Presence Release 8.6(4) and Earlier

For Cisco Unified Presence Release 8.6(4) and earlier, the presence domain and the DNS domain must match. Perform the following procedure to configure a new presence domain value for the cluster. If you use DNS, this procedure also sets the DNS domain to the same value.

Procedure

Step 1
Stop the Cisco UP SIP Proxy, Cisco UP Presence Engine and Cisco UP XCP Router services on all Cisco Unified Presence nodes in your cluster.

Step 2
Perform the following steps to configure the new domain value:


b. In the right pane, choose Settings.

c. In the Domain Name field, enter the new presence domain and click Save.

d. Choose Cisco Unified Presence Administration > System > Service Parameters, and choose the Cisco UP SIP Proxy service.

e. Configure the Federation Routing Cisco Unified Presence FQDN with the new domain.

f. You will be prompted to confirm these configuration changes. Click OK for both prompts, and then click Save.

Step 3
(DNS deployments only, for non-DNS deployments proceed to Step 4) Use this CLI command to set the new domain:

set network domain <new_domain>

This CLI command invokes a reboot of the server.

Step 4
(DNS and non-DNS deployments) On all nodes in the cluster, manually start the Cisco UP SIP Proxy, Cisco UP Presence Engine and Cisco UP XCP Router services after the reboot is complete (if required). If you are not using DNS, you have completed the replacement of the default domain value.

Step 5
(DNS deployments only) Manually regenerate all certificates on the local Cisco Unified Presence server.

Note
When you regenerate the Tomcat certificate, you must restart Tomcat. You can restart Tomcat after you regenerate all of the certificates on the local server. Use this CLI command to restart Tomcat: utils service restart Cisco Tomcat

Cisco Unified Presence Release 8.6(5) and Later

For Cisco Unified Presence Release 8.6(5) onwards, there is no requirement for the presence domain and the DNS domain to match. Perform the following procedure to configure a new presence domain for the cluster.
Chapter 7 Cisco Unified Presence Network Setup

Domain Value Configuration

Note

The following procedure only changes the presence domain of the cluster. It does not change the DNS domain associated with any Cisco Unified Presence node within that cluster. For instructions on how to change the DNS domain of a Cisco Unified Presence node, see Changing the IP Address, Hostname and Domain Name for Cisco Unified Presence.

Procedure

Step 1
Stop the Cisco UP SIP Proxy, Cisco UP Presence Engine and Cisco UP XCP Router services on all Cisco Unified Presence nodes in your cluster.

Step 2
Choose Cisco Unified Presence Administration > System > Cluster Topology.

Step 3
From the left pane, choose Settings.

Step 4
In the IM and Presence Domain field, enter the new presence domain and click Save.

Step 5
On all nodes in the cluster, manually start the Cisco UP SIP Proxy, Cisco UP Presence Engine and Cisco UP XCP Router services after the reboot is complete (if required).

Changing the Presence Domain Value

Follow this procedure if you want to change the presence domain value within a cluster.

The following procedures are applicable if you have a DNS or non-DNS deployment.

Cisco Unified Presence Release 8.6(4) and Earlier

Note

Cisco highly recommends that you use a DNS deployment. In order to be considered valid, the domain value must match the DNS domain name.

Procedure

Step 1
Stop the Cisco UP SIP Proxy, Presence Engine and XCP Router services on Cisco Unified Presence on all nodes in your cluster.

Step 2
On the publisher node, perform the following steps to configure the new domain value:


b. In the right pane, choose Settings.

c. Configure the Domain Name value with the new domain.

d. Choose Cisco Unified Presence Administration > System > Service Parameters, and choose the Cisco UP SIP Proxy service.

e. Configure the Federation Routing Cisco Unified Presence FQDN with the new domain.

f. You will be prompted to confirm these configuration changes. Click OK for both prompts, and then click Save.
Domain Value Configuration

Chapter 7  Cisco Unified Presence Network Setup

Step 3 (DNS deployments only, for non-DNS deployments proceed to Step 4) On all nodes in the cluster, use this CLI command to set the new domain:

```bash
set network domain <new_domain>
```

This CLI command invokes a reboot of the servers

Step 4 (DNS and non-DNS deployments) On all nodes in the cluster, manually start the Cisco UP SIP Proxy, Cisco UP Presence Engine and Cisco UP XCP Router services after the reboot is complete (if required). If you are not using DNS, you have completed the replacement of the default domain value.

Step 5 (DNS deployments only) Manually regenerate all certificates on each node in the cluster.

Note When you regenerate the Tomcat certificate, you must restart Tomcat. You can restart Tomcat after you regenerate all of the certificates on the local server. Use this CLI command to restart Tomcat:

```bash
utils service restart Cisco Tomcat
```

Step 6 (DNS deployments only) Update the DNS configuration for the new domain. Update any host records and any DNS SRV records that you require for the new domain

Step 7 (DNS deployments only) Configure any XMPP clients with the new domain.

Cisco Unified Presence Release 8.6(5) and Later

For Cisco Unified Presence Release 8.6(5) onwards, there is no requirement for the presence domain and the DNS domain to match.

Note The following procedure only changes the presence domain of the cluster. It does not change the DNS domain associated with any Cisco Unified Presence node within that cluster. For instructions on how to change the DNS domain of a Cisco Unified Presence node, see Changing the IP Address, Hostname and Domain Name for Cisco Unified Presence.

Procedure

Step 1 Stop the Cisco UP SIP Proxy, Cisco UP Presence Engine and Cisco UP XCP Router services on all Cisco Unified Presence nodes in your cluster.

Step 2 On the publisher node, choose Cisco Unified Presence Administration > System > Cluster Topology.

Step 3 From the left pane, choose Settings.

Step 4 In the IM and Presence Domain field, enter the new presence domain and click Save.

Step 5 On all nodes in the cluster, manually start the Cisco UP SIP Proxy, Cisco UP Presence Engine and Cisco UP XCP Router services after the reboot is complete (if required).
Routing Information Configuration on Cisco Unified Presence

Routing Communication Recommendations

MDNS is the default mechanism for establishing the XCP route fabric on Cisco Unified Presence; the network automatically establishes router-to-router connections between all Cisco Unified Presence nodes in a cluster. A requirement for MDNS routing is that all nodes in the cluster are in the same multicast domain. Cisco recommends MDNS routing because it can seamlessly support new XCP routers joining the XCP route fabric.

If you choose MDNS as the routing communication, you must have multicast DNS enabled in your network. In some networks multicast is enabled by default, or enabled in a certain area of the network, for example, in an area that contains the nodes that form the cluster. In these networks, you do not need to perform any additional configuration in your network to use MDNS routing. When multicast DNS is disabled in the network, MDNS packets cannot reach the other nodes in a cluster. If multicast DNS is disabled in your network, you must perform a configuration change to your network equipment to use MDNS routing.

Alternatively, you can choose router-to-router communication for your deployment. In this case, Cisco Unified Presence dynamically configures all router-to-router connections between nodes in a cluster. Choose this routing configuration type if all the nodes in your cluster are not in the same multicast domain. Note that when you choose router-to-router communication:

- Your deployment will incur the additional performance overhead while Cisco Unified Presence establishes the XCP route fabric.
- You do not need to restart the Cisco UP XCP Router on any node in your deployment when you add a new node.
- If you delete or remove a node, you must restart the Cisco UP XCP Router on all nodes in your deployment.

Related Topic
Configure Routing Communication, page 7-12

Configure MDNS Routing and Cluster ID

At installation, the system assigns a unique cluster ID to the Cisco Unified Presence publisher node. The systems distributes the cluster ID so that all nodes in your cluster share the same cluster ID value. The nodes in the cluster use the cluster ID to identify other nodes in the multicast domain using MDNS. A requirement for MDNS routing is that the cluster ID value is unique to prevent nodes in one standalone Cisco Unified Presence cluster from establishing router-to-router connections with nodes in another standalone cluster. Standalone clusters should only communicate over intercluster peer connections.

Choose Cisco Unified Presence Administration > Presence > Settings to view or configure the cluster ID value for a cluster. If you change the cluster ID value, make sure that the value remains unique to your Cisco Unified Presence deployment.

Note
If you deploy the Chat feature, Cisco Unified Presence uses the cluster ID value to define chat server aliases. There are certain configuration scenarios that may require you to change the cluster ID value. See the Group Chat module for details.
Configure Routing Communication

To allow the nodes in a cluster to route messages to each other, you must configure the routing communication type. This setting determines the mechanism for establishing router connections between nodes in a cluster. Configure the routing communication type on the publisher node, and Cisco Unified Presence applies this routing configuration to all nodes in the cluster.

For single node Cisco Unified Presence deployments, Cisco recommends that you leave the routing communication type at the default setting.

Caution

You must configure the routing communication type before you complete your cluster configuration and start to accept user traffic into your Cisco Unified Presence deployment.

Before You Begin

- If you want to use MDNS routing, confirm that MDNS is enabled in your network.
- If you want to use router-to-router communication, and DNS is not available in your network, for each node you must configure the IP address as the node name in the cluster topology. To edit the node name, choose Cisco Unified Presence Administration > System > Cluster Topology, and click the edit link on a node. Perform this configuration after you install Cisco Unified Presence, and before you restart the Cisco UP XCP Router on all nodes.

Note

When using the Cisco Jabber client, certificate warning messages can be encountered if the IP address is configured as the IM and Presence Service node name. To prevent Cisco Jabber from generating certificate warning messages, the FQDN should be used as the node name.

Procedure

Step 1 Choose Cisco Unified Presence Administration > System > Cluster Topology.

Step 2 In the right pane, choose Settings.

Step 3 Choose one of these Routing Communication Types from the menu:

- Multicast DNS (MDNS) - Choose Multicast DNS communication if the nodes in your cluster are in the same multicast domain. Multicast DNS communication is enabled by default on Cisco Unified Presence.

- Router to Router - Choose Router-to-Router communication if the nodes in your cluster are not in the same multicast domain.

Step 4 Click Save.

Step 5 Restart the Cisco UP XCP Router service on all nodes in your deployment.
Configure Cluster ID

At installation, the system assigns a default unique cluster ID to the Cisco Unified Presence publisher node. If you configure multiple nodes in the cluster, the systems distributes the cluster ID so that each node in your cluster shares the same cluster ID value.

Cisco recommends that you leave the cluster ID value at the default setting. If you do change the cluster ID value, note the following:

- If you choose MDNS routing, all nodes must have the same cluster ID to allow them to identify other nodes in the multicast domain.
- If you are deploying the Group Chat feature, Cisco Unified Presence uses the cluster ID value for chat server alias mappings, and there are certain configuration scenarios that may require you to change the cluster ID value. See the Group Chat module for details.

If you change the default Cluster ID value, you only need to make this change on the publisher node, and the system replicates the new Cluster ID value to the other nodes in the cluster.

Procedure

Step 1 Choose Cisco Unified Presence Administration > System > Cluster Topology.
Step 2 In the right pane, choose Settings.
Step 3 View or edit the Cluster ID value.

Note By default, Cisco Unified Presence assigns the cluster ID value “StandaloneCluster” to a cluster. If you are changing this default value, note that the underscore character (_) is not permitted in the Cluster ID value.

Step 4 Click Save.

Configure the Throttling Rate for Availability State Change Messages

To prevent an overload of the on Cisco Unified Presence, you can configure the rate of availability changes sent to the Cisco UP XCP Router in messages per second. When you configure this value, Cisco Unified Presence throttles the rate of availability changes back to meet the configured value.
Configure the Proxy Server Settings

Procedure

Step 1 Choose Cisco Unified Presence Administration > Presence > Routing > Settings.
Step 2 Choose On for the Method/Event Routing Status.
Step 3 Choose Default SIP Proxy TCP Listener for the Preferred Proxy Server.
Step 4 Choose Save.

What To Do Next

- Cisco IP Phone Messenger Configuration on Cisco Unified Presence, page 14-3, or

SIP Digest Authentication

Digest Authentication is enabled by default on Cisco Unified Presence SIP interfaces. Therefore any user that is using Cisco Unified Personal Communicator 7, must have digest credentials configured on CUCM.

Cisco Unified Personal Communicator will then retrieve these credentials through the Cisco Unified Presence SOAP APIs prior to connecting over the SIP interface.

To configure Digest Authentication credentials for a user:

Step 1 From the CUCM Administration GUI, navigate to the User Management > End User.
Step 2 Choose the user from the find list.
Step 3 Enter the credentials in the Digest Credentials text box.
Step 4 Confirm by re-entering the Confirm Digest Credentials text box.
Turn on Cisco Unified Presence Services

**Turn on the Sync Agent**

Cisco recommends that you turn on the Sync Agent on all Cisco Unified Presence nodes in the cluster.

**Before You Begin**
- Configure the topology for your deployment before starting the Sync Agent.
- If you deploy the Cisco Unified Personal Communicator client with Cisco Unified Presence, and you configure system-wide default application profiles (LDAP, CTI Gateway, Voicemail, Conferencing profiles) for your users, configure and enable the default profiles before you activate the Sync Agent.

**Procedure**

**Step 1** Choose Cisco Unified Presence Administration > System > Service Parameters.

**Step 2** Choose the Cisco Unified Presence server from the Server menu.

**Step 3** Choose Cisco UP Sync Agent server from the Service menu.

---

**Note**

The CUCM Bulk Administration tool (From the CUCM Administration GUI, navigate to Bulk Administration > Users > Update Users) allows for digest credentials to be updated in bulk for a set of users.

An alternative to configuring digest credentials is to add specific Access Control List (ACL) entries for each Client Machine on which Cisco Unified Personal Communicator is running.

Having an ACL entry for the client machine ensures that digest authentication is bypassed.

ACL entries are added on the Cisco Unified Presence Admin GUI by:

**Step 1** Navigate to System > Security > Incoming ACL.
**Step 2** Click Add New.
**Step 3** Enter the IP address in Address Pattern.
**Step 4** Optionally enter in a Description value.
**Step 5** Click Save.

**Note**

Bypassing Digest Authentication is not the Cisco recommended approach as the configuration is static and does not allow for deployments where IP addresses are not statically provisioned to machines.
Step 4  Choose a value for the User Assignment Mode as follows:

- If set to **Balanced**, the Sync Agent synchronizes user information to Cisco Unified Presence, and then assigns the users to each node in an attempt to balance the user assignment evenly across all nodes.

- If set to **Active/Standby**, the Sync Agent synchronizes user information to Cisco Unified Presence, and assigns the total number of users to the first node of a subcluster only. If there is only a single node in the subcluster, the Sync Agent uses this node for assignment regardless of the location of the node within the subcluster.

- If set to **None**, the Sync Agent synchronizes user information to Cisco Unified Presence but does not assign any users. You must manually assign your users to nodes using the system topology interface.

Step 5  Click **Save**.

### Related Topics

- [Configure Routing Communication, page 7-12](#)
- Chapter “Configuring Basic Features for Cisco Unified Personal Communicator” in the *Cisco Unified Personal Communicator Administration Guide for Cisco Unified Presence Release 8.6*
- [Turn on Cisco Unified Presence Services, page 7-16](#)

## Turn on Cisco Unified Presence Services

The procedure below lists out the services that you need to turn on when you deploy a basic Cisco Unified Presence configuration. You need to turn on these services on each node in your Cisco Unified Presence cluster.

There are other optional Cisco Unified Presence services that you may need to turn on depending on the additional features that you deploy on Cisco Unified Presence. See the Cisco Unified Presence documentation relating to those specific features for further details.

The Cisco UP XCP Router service must be running for a basic Cisco Unified Presence deployment. Cisco Unified Presence turns on the Cisco UP XCP Router by default. Verify that this network service is on by choosing **Cisco Unified Presence Serviceability > Control Center - Network Services**.

### Procedure

**Step 1**  Choose **Cisco Unified Presence Serviceability > Tools > Service Activation**.

**Step 2**  Choose the Cisco Unified Presence server from the Server menu.

**Step 3**  For a basic Cisco Unified Presence deployment, turn on the following services:

- Cisco UP SIP Proxy
- Cisco UP Presence Engine
- Cisco UP Sync Agent
- Cisco UP XCP Connection Manager
- Cisco UP XCP Authentication Service
Step 4  Click Save.

Related Topics

- Serviceability Configuration and Maintenance Guide for Cisco Unified Presence
- Turn on the Sync Agent, page 7-15
Turn on Cisco Unified Presence Services
IP Phone Presence Setup

Static Route Configuration on Cisco Unified Presence

If you configure a static route for SIP proxy server traffic, consider the following:

- A dynamic route represents a path through the network that is automatically calculated according to routing protocols and routing update messages.
- A static route represents a fixed path that you explicitly configure through the network.
- Static routes take precedence over dynamic routes.

This section contains the following subsections:

- Route Embed Templates, page 8-1
- Configure Route Embed Templates on Cisco Unified Presence, page 8-2
- Configure Static Routes on Cisco Unified Presence, page 8-3

Route Embed Templates

You must define a route embed template for any static route pattern that contains embedded wildcards. The route embed template contains information about the leading digits, the digit length, and location of the embedded wildcards. Before you define a route embed template, consider the sample templates we provide below.

When you define a route embed template, the characters that follow the '.' must match actual telephony digits in the static route. In the sample route embed templates below, we represent these characters with 'x'.

**Sample Route Embed Template A**

Route embed template: **74..78xxxxx***

With this template, Cisco Unified Presence will enable this set of static routes with embedded wildcards:
Chapter 8      IP Phone Presence Setup

**Sample Route Embed Template B**

*Route embed template: 471....xx*  

With this template, Cisco Unified Presence will enable this set of static routes with embedded wildcards:

<table>
<thead>
<tr>
<th>Destination Pattern</th>
<th>Next Hop Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>471….34*</td>
<td>20.20.21.22</td>
</tr>
<tr>
<td>471…55*</td>
<td>21.21.55.79</td>
</tr>
</tbody>
</table>

With this template, Cisco Unified Presence will NOT enable these static route entries:
- 47...344* (The initial string is not ‘471’ as the template defines)
- 471…4* (The string length does not match template)
- 471.450* (The number of wildcards does not match template)

**Configure Route Embed Templates on Cisco Unified Presence**

You can define up to five route embed templates. However, there is no limit to the number of static routes that you can define for any route embed template.

A static route that contains an embedded wildcard must match at least one of the route embed templates.

**Procedure**

**Step 1** Choose **Cisco Unified Presence Administration > System > Service Parameters**.

**Step 2** Choose a Cisco Unified Presence server.

**Step 3** Choose the Cisco UP SIP Proxy service.

**Step 4** Define a route embed templates in the RouteEmbedTemplate field in the Routing Parameters (Clusterwide) section. You can define up to five route embed templates.
Step 5  Click Save.

What To Do Next
Configure Static Routes on Cisco Unified Presence, page 8-3

Configure Static Routes on Cisco Unified Presence

Procedure

Step 1  Choose Cisco Unified Presence Administration > Routing > Static Routes.
Step 2  Click Add New.
Step 3  Configure these static route settings:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination Pattern</td>
<td>This field specifies the pattern of the incoming number, up to a maximum of 255 characters. The SIP proxy allows only 100 static routes to have an identical route pattern. If you exceed this limit, Cisco Unified Presence logs an error.</td>
</tr>
</tbody>
</table>

Wildcard Usage
You can use “.” as a wildcard for a single character and “*” as a wildcard for multiple characters.

Cisco Unified Presence supports embedded ‘.’ wildcard characters in static routes. However, you must define route embed templates for static routes that contain embedded wildcards. Any static route that contains an embedded wildcard must match at least one route embed template. See the route embed template topic (referenced in the Related Topics section below) for information about defining route embed templates.

For phones:
- A dot can exist at the end of the pattern, or embedded in a pattern. If you embed the dot in a pattern, you must create a route embed template to match the pattern.
- An asterisk can only exist at the end of the pattern.

For IP addresses and host names:
- You can use an asterisk as part of the a host name.
- The dot acts as a literal value in a host name.

An escaped asterisk sequence, \\*, matches a literal * and can exist anywhere.

Description  Specifies the description of a particular static route, up to a maximum of 255 characters.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Next Hop</td>
<td>Specifies the domain name or IP address of the destination (next hop) and can be either a Fully Qualified Domain Name (FQDN) or dotted IP address.</td>
</tr>
<tr>
<td></td>
<td>Cisco Unified Presence supports DNS SRV-based call routing. To specify DNS SRV as the next hop for a static route, set this parameter to the DNS SRV name.</td>
</tr>
<tr>
<td>Next Hop Port</td>
<td>Specifies the port number of the destination (next hop). The default port is 5060.</td>
</tr>
<tr>
<td></td>
<td>Cisco Unified Presence supports DNS SRV-based call routing. To specify DNS SRV as the next hop for a static route, set the next hop port parameter to 0.</td>
</tr>
<tr>
<td>Route Type</td>
<td>Specifies the route type: User or Domain. The default value is user.  For example, in the SIP URI &quot;sip:<a href="mailto:19194762030@myhost.com">19194762030@myhost.com</a>&quot; request, the user part is '19194762030', and the host part is 'myhost.com'. If you choose User as the route type, Cisco Unified Presence uses the user-part value '19194762030' for routing SIP traffic. If you choose the Domain as the route type, Cisco Unified Presence uses 'myhost.com' for routing SIP traffic.</td>
</tr>
<tr>
<td>Protocol Type</td>
<td>Specifies the protocol type for this route, TCP, UDP, or TLS. The default value is TCP.</td>
</tr>
<tr>
<td>Priority</td>
<td>Specifies the route priority level. Lower values indicate higher priority. The default value is 1.</td>
</tr>
<tr>
<td></td>
<td>Value range: 1-65535</td>
</tr>
<tr>
<td>Weight</td>
<td>Specifies the route weight. Use this parameter only if two or more routes have the same priority. Higher values indicate which route has the higher priority.</td>
</tr>
<tr>
<td></td>
<td>Value range: 1-65535</td>
</tr>
</tbody>
</table>
| Example:             | Consider these three routes with associated priorities and weights:  
|                      | - 1, 20  
|                      | - 1, 10  
|                      | - 2, 50  
|                     | In this example, the static routes are listed in the correct order. The priority route is based on the lowest value priority, that is 1. Given that two routes share the same priority, the weight parameter with the highest value decides the priority route. In this example, Cisco Unified Presence directs SIP traffic to both routes configured with a priority value of 1, and distributes the traffic according to weight; The route with a weight of 20 receives twice as much traffic as the route with a weight of 10. Note that in this example, Cisco Unified Presence will only attempt to use the route with priority 2, if it has tried both priority 1 routes and both failed. |
| Allow Less-Specific Route | Specifies that the route can be less specific. The default setting is On.                                                                 |

Field Description
Presence Gateway Configuration on Cisco Unified Presence

You must configure Cisco Unified Communications Manager as a Presence Gateway on Cisco Unified Presence to enable the SIP connection that handles the availability information exchange between Cisco Unified Communications Manager and Cisco Unified Presence.

When configuring the Presence Gateway, specify the FQDN (Fully Qualified Domain Name) or the IP address of the associated Cisco Unified Communications Manager server. Depending on your network this value can be one of the following:

- the FQDN address of the Cisco Unified Communications Manager publisher
- a DNS SRV FQDN that resolves to the Cisco Unified Communications Manager subscriber nodes
- the IP address of the Cisco Unified Communications Manager publisher

If DNS SRV is an option in your network, configure the following:
1. Configure the Presence Gateway on the Cisco Unified Presence server with a DNS SRV FQDN of the Cisco Unified Communications Manager subscriber nodes (equally weighted). This will enable Cisco Unified Presence to share availability messages equally among all the servers used for availability information exchange.
2. On Cisco Unified Communications Manager, configure the SIP trunk for the Cisco Unified Presence server with a DNS SRV FQDN of the Cisco Unified Presence publisher and subscriber.

If DNS SRV is not an option in your network, and you are using the IP address of the associated Cisco Unified Communications Manager server, you cannot share availability messaging traffic equally across multiple subscriber nodes because the IP address points to a single subscriber node.

Related Topic
SIP Trunk Configuration on Cisco Unified Communications Manager, page 6-4
Configure the Presence Gateway

Before You Begin
- Read the Presence Gateway configuration options topic.
- Depending on your configuration requirements, obtain the FQDN, DNS SRV FQDN, or the IP address of the associated Cisco Unified Communications Manager server.

Procedure

Step 1  Choose Cisco Unified Presence Administration > Presence > Gateways.
Step 2  Click Add New.
Step 3  Choose CUCM for the Presence Gateway Type.
Step 4  Enter a description of the presence gateway in the Description field.
Step 5  Specify the FQDN, DNS SRV FQDN, or the IP address of the associated Cisco Unified Communications Manager server in the Presence Gateway field.
Step 6  Click Save.

Related Topic
Presence Gateway Configuration Option, page 8-5

What To Do Next
Authorization Policy Configuration, page 15-2

Configure the SIP Publish Trunk on Cisco Unified Presence

When you turn on this setting, Cisco Unified Communications Manager publishes phone availability for all line appearances that are associated with Cisco Unified Presence licensed users.

This procedure is the same operation as assigning a SIP trunk as the CUP PUBLISH trunk in Cisco Unified Communications Manager service parameters.

Procedure

Step 1  Choose Cisco Unified Presence Administration > Presence > Settings.
Step 2  Choose a SIP Trunk from the CUCM SIP Publish Trunk drop-down list.
Step 3  Click Save.
CHAPTER 9

LDAP Directory Integration

June 16, 2014

- LDAP Directory Integration with Cisco Unified Communications Manager, page 9-2
- LDAP Directory Integration with Cisco Unified Personal Communicator, page 9-6
- LDAP Directory Integration for Contact Searches on XMPP Clients, page 9-12
LDAP Directory Integration with Cisco Unified Communications Manager

- Secure Connection Between Cisco Unified Communications Manager and the LDAP Directory, page 9-3
- Configuring the LDAP Synchronization for User Provisioning, page 9-3
- Upload LDAP Authentication Server Certificates, page 9-4
- Configure LDAP Authentication, page 9-5
- Configure a Secure Connection between Cisco Unified Presence and the LDAP Directory, page 9-6
Secure Connection between Cisco Unified Communications Manager and the LDAP Directory

You can secure the connection between the Cisco Unified Communications Manager server and the LDAP directory server by enabling a Secure Socket Layer (SSL) connection for the LDAP server on Cisco Unified Communications Manager, and uploading the SSL certificate to Cisco Unified Communications Manager. You must upload the LDAP SSL certificate as a directory-trust certificate on Cisco Unified Communications Manager Release 7.x and earlier, and as a tomcat-trust certificate on Cisco Unified Communications Manager Release 8.x and later.

After you upload the LDAP SSL certificate, you need to restart the following services on Cisco Unified Communications Manager:

- Directory service
- Tomcat service

Related Topics

- Configure a Secure Connection between Cisco Unified Presence and the LDAP Directory, page 9-6
- Cisco Unified Operating System Maintenance Guide for Cisco Unified Presence

Configure the LDAP Synchronization for User Provisioning

LDAP synchronization uses the Cisco Directory Synchronization (DirSync) tool on Cisco Unified Communications Manager to synchronize information (either manually or periodically) from a corporate LDAP directory. When you enable the DirSync service, Cisco Unified Communications Manager automatically provisions users from the corporate directory. Cisco Unified Communications Manager still uses its local database, but disables its facility to allow you to create user accounts. You use the LDAP directory interface to create and manage user accounts.

Before You Begin

- Make sure that you install the LDAP server before you attempt the LDAP-specific configuration on Cisco Unified Communications Manager.
- Activate the Cisco DirSync service on Cisco Unified Communications Manager.

Restrictions

LDAP synchronization does not apply to application users on Cisco Unified Communications Manager. You must manually provision application users in the Cisco Unified CM Administration interface.

Related Topics

- Release Notes for Cisco Unified Personal Communicator:
- Cisco Unified Communications Manager System Guide:
Procedure

Step 1  Choose Cisco Unified Communications Manager Administration > System > LDAP > LDAP System.

Step 2  Click Add New.

Step 3  Configure the LDAP server type and attribute.

Step 4  Click Enable Synchronizing from LDAP Server.

Step 5  Choose Cisco Unified Communications Manager Administration > System > LDAP > LDAP Directory

Step 6  Configure the following items:
- LDAP directory account settings
- User attributes to be synchronized
- Synchronization schedule
- LDAP server hostname or IP address, and port number

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

Note  If you configure LDAP over SSL, upload the LDAP directory certificate onto Cisco Unified Communications Manager.

Related Topics
- Configure a Secure Connection between Cisco Unified Presence and the LDAP Directory, page 9-6
- Cisco Unified Communication SRND:
  http://www.cisco.com/go/designzone
- Cisco Unified Communications Manager Administration Guide:

What To Do Next
Upload LDAP Authentication Server Certificates, page 9-4

Upload LDAP Authentication Server Certificates

When Cisco Unified Communications Manager LDAP authentication is configured for secure mode (port 636 or 3269), LDAP authentication server certificates, such as Certificate Authority (CA) root and all other Intermediate certificates, must be individually uploaded as “tomcat-trust” to the Cisco Unified Presence server.

Procedure

Step 1  Choose Cisco Unified OS Administration > Security > Certificate Management.

Step 2  Click Upload Certificate.
Step 3  Choose **tomcat-trust** from the **Certificate Name** menu.

Step 4  Browse and choose the LDAP server root certificate from your local computer.

Step 5  Click **Upload File**.

Step 6  Repeat the above steps for all other intermediate certificates.

---

**Related Topic**

Configure a Secure Connection between Cisco Unified Presence and the LDAP Directory, page 9-6

**What To Do Next**

Configure LDAP Authentication, page 9-5

---

## Configure LDAP Authentication

The LDAP authentication feature enables Cisco Unified Communications Manager to authenticate user passwords against the corporate LDAP directory.

**Before You Begin**

Enable LDAP synchronization on Cisco Unified Communications Manager.

**Restrictions**

LDAP authentication does not apply to the passwords of application users; Cisco Unified Communications Manager authenticates application users in its internal database.

**Procedure**

Step 1  Choose **Cisco Unified Communications Manager Administration** > **System** > **LDAP** > **LDAP Authentication**.

Step 2  Enable LDAP authentication for users.

Step 3  Configure the LDAP authentication settings.

Step 4  Configure the LDAP server hostname or IP address, and port number

---

**Note**

To use Secure Socket Layer (SSL) to communicate with the LDAP directory, check **Use SSL**. If you configure LDAP over SSL, upload the LDAP directory certificate to Cisco Unified Communications Manager.

---

**Related Topics**

- Configuring the LDAP Synchronization for User Provisioning, page 9-3
- Configure a Secure Connection between Cisco Unified Presence and the LDAP Directory, page 9-6

**What To Do Next**

Configure a Secure Connection between Cisco Unified Presence and the LDAP Directory, page 9-6
Configure a Secure Connection between Cisco Unified Presence and the LDAP Directory

This topic is only applicable if you configure a secure connection between Cisco Unified Communications Manager and the LDAP directory.

Note
Perform this procedure on all Cisco Unified Presence nodes in the cluster.

Before You Begin
Enable SSL for LDAP on Cisco Unified Communications Manager, and upload the LDAP directory certificate to Cisco Unified Communications Manager.

Procedure

Step 1  Choose Cisco Unified OS Administration > Security > Certificate Management.
Step 2  Click Upload Certificate.
Step 3  Choose tomcat-trust from the Certificate Name menu.
Step 4  Browse and choose the LDAP server certificate from your local computer.
Step 5  Click Upload File.
Step 6  Restart the Tomcat service from the CLI using this command:
        utils service restart Cisco Tomcat

Related Topic
Configure a Secure Connection between Cisco Unified Presence and the LDAP Directory, page 9-6

What To Do Next
LDAP Directory Integration with Cisco Unified Personal Communicator, page 9-6

LDAP Directory Integration with Cisco Unified Personal Communicator

These topics describe how to configure the LDAP settings on Cisco Unified Presence to allow Cisco Unified Personal Communicator users to search and add contacts from the LDAP directory.

Before you perform this configuration, fully integrate the Cisco Unified Personal Communicator client with Cisco Unified Communications Manager and Cisco Unified Presence.

- Rules for a Displayed Contact Name, page 9-7
- (Cisco Unified Personal Communicator Release 8.0) Fetch Contact Pictures from a Web Server, page 9-7
- Configure the LDAP Attribute Map for Cisco Unified Personal Communicator, page 9-8
Rules for a Displayed Contact Name

When you configure the user fields in the LDAP attribute map, note the following rules that determine how Cisco Unified Personal Communicator displays contact names:

- If the user edits a contact name in Cisco Unified Personal Communicator, display this name. This is the Nickname LDAP attribute in Cisco Unified Presence.
- If you configure an LDAP user field for Display Name, display this name.
- If you configure an LDAP user field for Nickname, display this name with the last name.
- Otherwise, display the configured LDAP user fields for the first and last names in the Contact pane. If there is a first name but no last name, display the first name. If there is a last name but no first name, display the last name.
- If you do not configure LDAP user fields for the FirstName and LastName, display the LDAP UserID or the Cisco Unified Presence user ID in the Contact pane.
- If a user adds a non-LDAP contact, the contact details in Cisco Unified Personal Communicator allow the user to edit the Display As name, the first name, and the last name.

Related Topics

- (Cisco Unified Personal Communicator Release 8.0) Fetch Contact Pictures from a Web Server, page 9-7
- Configure the LDAP Attribute Map for Cisco Unified Personal Communicator, page 9-8

(Cisco Unified Personal Communicator Release 8.0) Fetch Contact Pictures from a Web Server

You can configure a parameterized URL string in the Photo field in the LDAP attribute map so that Cisco Unified Personal Communicator can fetch pictures from a web server instead of from the LDAP server. The URL string must contain an LDAP attribute with a query value containing a piece of data that uniquely identifies the photo of the user. Cisco recommends that you use the User ID attribute. However, you can use any LDAP attribute whose query value contains a piece of data that uniquely identifies the photo of the user.

Cisco recommends that you use %%<userID>%% as the substitution string, for example:

- http://mycompany.cisco.com/photo/std/%%uid%%.jpg
- http://mycompany.cisco.com/photo/std/%%sAMAccountName%%.jpg

You must include the double percent symbols in this string, and they must enclose the name of the LDAP attribute to substitute. Cisco Unified Personal Communicator removes the percent symbols and replaces the parameter inside with the results of an LDAP query for the user whose photo it resolves.

For example, if a query result contains the attribute “uid” with a value of “johndoe,” then a template such as http://mycompany.com/photos/%%uid%%.jpg creates the URL http://mycompany.com/photos/johndoe.jpg. Cisco Unified Personal Communicator attempts to fetch the photo.
This substitution technique works only if Cisco Unified Personal Communicator can use the results of the query and can insert it into the template you specify above to construct a working URL that fetches a JPG photo. If the web server that hosts the photos in a company requires a POST (for example, the name of the user is not in the URL) or uses some other cookie name for the photo instead of the username, this technique does not work.

Note

- The URL length is limited to 50 characters.
- Cisco Unified Personal Communicator does not support authentication for this query; the photo must be retrievable from the web server without credentials.

Related Topics

- Rules for a Displayed Contact Name, page 9-7
- Configure the LDAP Attribute Map for Cisco Unified Personal Communicator, page 9-8

Configure the LDAP Attribute Map for Cisco Unified Personal Communicator

Note

The information about fetching a photo from Active Directory in this topic relates only to Cisco Unified Personal Communicator Release 7.1.

You must configure the LDAP attribute map on Cisco Unified Presence where you enter LDAP attributes for your environment and map them to the given Cisco Unified Personal Communicator attributes.

If you want to use LDAP to store your employee profile photos, you must either use a third-party extension to upload the photo files to the LDAP server, or extend the LDAP directory server schema by other means to create an attribute that the LDAP server can associate with an image. For Cisco Unified Personal Communicator to display the profile photo, in the LDAP attribute map, you must map the Cisco Unified Personal Communicator "Photo" value to the appropriate LDAP attribute. By default, Cisco Unified Personal Communicator uses the jpegPhoto LDAP attribute to display the user photo, which is present in the Windows 2003 and 2007 Active Directory schema. Note that Windows 2000 Active Directory uses the thumbnailPhoto attribute.

Before You Begin

- Make sure that you install and set up the LDAP server before you configure the LDAP attribute map on Cisco Unified Presence.
- By default, Cisco Unified Personal Communicator uses the jpegPhoto LDAP attribute, which is present in the Windows 2003 Active Directory schema. By contrast, the Windows 2000 Active Directory uses the thumbnailPhoto attribute.

Restrictions

- The UPC UserID setting in the LDAP attribute map must match the Cisco Unified Communications Manager user ID. This mapping allows a user to add a contact from LDAP to the Contact list in Cisco Unified Personal Communicator. This field associates the LDAP user with the associated user on Cisco Unified Communications Manager and Cisco Unified Presence.
- You can map an LDAP field to only one Cisco Unified Personal Communicator field.
Procedure

Step 1 Choose Cisco Unified Presence Administration > Application > Cisco Jabber > Settings

Step 2 Choose a supported LDAP server from Directory Server Type. The LDAP server populates the LDAP attribute map with Cisco Unified Personal Communicator user fields and LDAP user fields.

Step 3 If necessary, make modifications to the LDAP field to match your specific LDAP directory. The values are common to all LDAP server hosts. Note the following LDAP directory product mappings:

<table>
<thead>
<tr>
<th>Product</th>
<th>LastName Mapping</th>
<th>UserID Mapping</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Active Directory</td>
<td>SN</td>
<td>sAMAccountName</td>
</tr>
<tr>
<td>iPlanet, Sun ONE or OpenLDAP</td>
<td>SN</td>
<td>uid</td>
</tr>
</tbody>
</table>

Step 4 Click Save.

Related Topics

- Rules for a Displayed Contact Name, page 9-7
- (Cisco Unified Personal Communicator Release 8.0) Fetch Contact Pictures from a Web Server, page 9-7

What To Do Next
Configure LDAP Server Names and Addresses for Cisco Unified Personal Communicator, page 9-9

Configure LDAP Server Names and Addresses for Cisco Unified Personal Communicator

Before You Begin
- Configure the LDAP attribute map.
- Obtain the hostnames or IP addresses of the LDAP directories.

Procedure

Step 1 Choose Cisco Unified Presence Administration > Application > Cisco Jabber > LDAP Server.

Step 2 Click Add New.

Step 3 Enter the LDAP server name.

Step 4 Enter an IP address or an FQDN (Fully Qualified Domain Name) of the LDAP server.

Step 5 Specify the port number used by the LDAP server. The defaults are:
- TCP - 389
- TLS - 636
Check the LDAP directory documentation or the LDAP directory configuration for this information.

**Note**  If you integrate with Microsoft Active Directory and if the server is Global Catalog, configure **3268** as the port number.

**Step 6**  Choose **TCP** or **TLS** for the protocol type.

**Note**  If you integrate with Microsoft Active Directory and if the server is Global Catalog, choose **TCP** as the protocol type.

**Step 7**  Click **Save**.

**Troubleshooting Tips**

- The `jpegPhoto` attribute is not available in Microsoft Active Directory Global Catalog server, and it is not indexed (http://msdn2.microsoft.com/en-us/library/ms676813.aspx). If your LDAP configuration uses Global Catalog port 3268, Cisco Unified Personal Communicator cannot retrieve the `jpegPhoto`. Instead, change the LDAP directory configuration to TCP and port 389. Cisco Unified Personal Communicator retrieves the photo when you sign in again.

- If you configure an application dial rule, create proper directory lookup dialing rules in Cisco Unified Communications Manager to make sure that a picture displays both when you place a call to a contact and in the contact details. When you add a contact in Cisco Unified Personal Communicator, the directory lookup returns a 10-digit number (for example, 1234567890). If the user places the call by dialing only four digits (for example, 7890), the picture does not display because 7890 is not a match for 1234567890. Create the following rules to fix this problem:
  
  - Outbound rule to remove the area code. The picture displays in the contact details.
  - Inbound rule for directory lookup to prefix the area code (translate the 4-digit extension number into the 10-digit DID number stored in AD). The picture displays when you place a call.

**Related Topic**

Configure the LDAP Attribute Map for Cisco Unified Personal Communicator, page 9-8

**What To Do Next**

Create LDAP Profiles and Add Cisco Unified Personal Communicator Users to the Profile, page 9-10

**Create LDAP Profiles and Add Cisco Unified Personal Communicator Users to the Profile**

Cisco Unified Personal Communicator connects to an LDAP server on a per-search basis. If the connection to the primary server fails, Cisco Unified Personal Communicator attempts the first backup LDAP server, and if it is not available, it then attempts to connect to the second backup server. Cisco Unified Personal Communicator also periodically attempts to return to the primary LDAP server. If an LDAP query is in process when the system fails over, the next available server completes this LDAP query.
You can see LDAP server information in the server health window in Cisco Unified Personal Communicator (Help > Show Server Health on Windows and Help > Show System Diagnostics on Mac OS). If Cisco Unified Personal Communicator cannot connect to any of the LDAP servers, it reports the failure in the System Diagnostics window.

**Before You Begin**

- Specify the LDAP server names and addresses.
- You must create the LDAP profile before you can add Cisco Unified Personal Communicator licensed users to the profile.

**Procedure**

1. Choose Cisco Unified Presence Administration > Application > Cisco Jabber > LDAP Profile.
2. Click Add New.
3. Enter information into the fields.

**Table 9-1**

<table>
<thead>
<tr>
<th>Field</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter the profile name limited to 128 characters.</td>
</tr>
<tr>
<td>Description</td>
<td>(Optional) Enter a description limited to 128 characters.</td>
</tr>
<tr>
<td>Bind Distinguished Name</td>
<td>(Optional) Enter the administrator-level account information limited to 128 characters. This is the distinguished name with which you bind for authenticated bind. The syntax for this field depends on the type of LDAP server that you deploy. For details, see the LDAP server documentation.</td>
</tr>
<tr>
<td>Anonymous Bind</td>
<td>(Optional) Uncheck this option to use the user credentials to sign in to this LDAP server. For non-anonymous bind operations, Cisco Unified Personal Communicator receives one set of credentials. If configured, these credentials must be valid on the backup LDAP servers. <strong>Note</strong> If you check Anonymous Bind, users can sign in anonymously to the LDAP server with read-only access. Anonymous access might be possible on your directory server, but we do not recommend it. Instead, create a user with read-only privileges on the same directory where the users to be searched are located. Specify the directory number and password in Cisco Unified Presence for Cisco Unified Personal Communicator to use.</td>
</tr>
<tr>
<td>Password</td>
<td>(Optional) Enter the LDAP bind password limited to 128 characters. This is the password for the administrator-level account that you provided in the Bind Distinguished Name string to allow users to access this LDAP server.</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>Reenter the same password as the password you entered in the Password field. (Optional) After configuring Cisco Unified Presence for authenticated bind with the LDAP server, configure the LDAP server for anonymous permissions and anonymous login so that all directory information (name, number, mail, fax, home number, and so forth) is passed to the Cisco Unified Personal Communicator client.</td>
</tr>
</tbody>
</table>
Table 9-1

<table>
<thead>
<tr>
<th>Field</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search Context</td>
<td>(Optional) Enter the location where you configured all the LDAP users. This location is a container or directory. The name is limited to 256 characters. Only use a single OU/LDAP search context.</td>
</tr>
<tr>
<td>Note</td>
<td>If you integrate with Microsoft Active Directory:</td>
</tr>
<tr>
<td></td>
<td>• Set O and OU (OU must contain users; for example, ou=users,dc=cisco,dc=com).</td>
</tr>
<tr>
<td></td>
<td>• The search base should include all users of Cisco Unified Personal Communicator.</td>
</tr>
<tr>
<td>Recursive Search</td>
<td>(Optional) Check to perform a recursive search of the directory starting at the search base.</td>
</tr>
<tr>
<td>Primary LDAP Server and Backup LDAP Server</td>
<td>Choose the primary LDAP server and optional backup servers.</td>
</tr>
<tr>
<td>Make this the Default LDAP Profile for the System</td>
<td>(Optional) Check to add any new users to the system into this default profile. If you turn on this setting, Cisco Unified Presence adds any users that it synchronizes from Cisco Unified Communications Manager to this default profile. Cisco Unified Presence only adds users to this default profile after you choose the default profile (and you turn on the Sync Agent). Cisco Unified Presence does not change any existing profile configuration. Therefore, Cisco recommends that you choose and configure the default profile before you turn on the Sync Agent.</td>
</tr>
<tr>
<td>Add Users to Profile</td>
<td>Click the button to open the Find and List Users window. Click <strong>Find</strong> to populate the search results fields. Alternatively, search for a specific users and click <strong>Find</strong>. To add users to this profile, choose the users, and click <strong>Add Selected</strong>.</td>
</tr>
</tbody>
</table>

Step 4 Click **Save**.

Related Topic
Section “How to Update User Configuration After Deploying Cisco Unified Personal Communicator” in the Cisco Unified Personal Communicator Administration Guide for Cisco Unified Presence Release 8.6

LDAP Directory Integration for Contact Searches on XMPP Clients

These topics describe how to configure the LDAP settings on Cisco Unified Presence to allow users of third-party XMPP client to search and add contacts from the LDAP directory.
The JDS component on Cisco Unified Presence handles the third-party XMPP client communication with the LDAP directory. Third-party XMPP clients send queries to the JDS component on Cisco Unified Presence. The JDS component sends the LDAP queries to the provisioned LDAP servers, and then sends the results back to the XMPP client.

Before you perform the configuration described here, perform the configuration to integrate the XMPP client with Cisco Unified Communications Manager and Cisco Unified Presence. See chapter Third-party XMPP Client Application Configuration on Cisco Unified Presence, page 10-1.

### LDAP Account Lock Issue

If you enter the wrong password for the LDAP server that you configure for third-party XMPP clients, and you restart the XCP services on Cisco Unified Presence, the JDS component will perform multiple attempts to sign in to the LDAP server with the wrong password. If the LDAP server is configured to lock out an account after a number of failed attempts, then the LDAP server may lock the JDS component out at some point. If the JDS component uses the same credentials as other applications that connect to LDAP (applications that are not necessarily on Cisco Unified Presence), these applications will also be locked out of LDAP.

To fix this issue, configure a separate user, with the same role and privileges as the existing LDAP user, and allow only JDS to sign in as this second user. If you enter the wrong password for the LDAP server, only the JDS component is locked out from the LDAP server.

### Configure LDAP Server Names and Addresses for XMPP Clients

If you choose to enable SSL, configure a secure connection between the LDAP server and Cisco Unified Presence. Upload the root CA certificate to Cisco Unified Presence as an xmpp-trust-certificate, following the certificate upload procedure described in this module. The subject CN in the certificate must match the FQDN of the LDAP server.

---

**Note**

If you import a certificate chain (more than one certificate from the root node to the trusted node), import all certificates in the chain except the leaf node. For example, if the CA signs the certificate for the LDAP server, you just import the CA certificate, not the certificate for the LDAP server.

---

**Before You Begin**

Obtain the hostnames or IP addresses of the LDAP directories.

**Procedure**

1. **Step 1** Choose Cisco Unified Presence Administration > Application > Third-Party Clients > Third-Party LDAP Servers.
2. **Step 2** Click Add New.
3. **Step 3** Enter an ID for the LDAP server.
4. **Step 4** Enter the hostname of the LDAP server.
5. **Step 5** Specify the port number on the LDAP server that is listening to the TCP or SSL connection. The default port is 389. If you enable SSL, specify port 636.
Step 6 Specify the username and the password for the LDAP server. These values must match the credentials you configure on the LDAP server.

See the LDAP directory documentation or the LDAP directory configuration for this information.

Step 7 Check Enable SSL if you want to use Secure Socket Layer (SSL) to communicate with the LDAP server.

Note If you enable SSL, the XMPP contact searches may be slower because of the negotiation procedures at SSL connection setup, and data encryption and decryption after Cisco Unified Presence establishes the SSL connection. As a result, if your users perform XMPP contact searches extensively in your deployment, this could impact the overall system performance.

Step 8 Click Save.

Step 9 Start the Cisco UP XCP Router service on all nodes in the cluster (if this service is not already running).

Step 10 If you make an update to the LDAP server configuration for third-party XMPP clients, restart the Cisco UP XCP Directory Service. Choose Cisco Unified Serviceability > Tools > Control Center - Feature Services to restart this service.

Related Topics
- LDAP Account Lock Issue, page 9-13
- Secure Connection Between Cisco Unified Communications Manager and the LDAP Directory, page 9-3
- Configure a Secure Connection between Cisco Unified Presence and the LDAP Directory, page 9-6

What To Do Next
Configure the LDAP Search Settings for XMPP Clients, page 9-14

Configure the LDAP Search Settings for XMPP Clients

You must specify the LDAP search settings that will allow Cisco Unified Presence to successfully perform contact search for third-party XMPP clients.

Third-party XMPP clients connect to an LDAP server on a per-search basis. If the connection to the primary server fails, the XMPP client tries the first backup LDAP server, and if it is not available, it then tries the second backup server and so on. If an LDAP query is in process when the system fails over, the next available server completes this LDAP query.

Optionally you can turn on the retrieval of vCards from the LDAP server. If you turn on vCard retrieval:
- The corporate LDAP directory stores the vCards.
- When XMPP clients search for their own vCard, or the vCard for a contact, the vCards are retrieved from LDAP via the JDS service.
- Clients cannot set or modify their own vCard as they are not authorized to edit the corporate LDAP directory.

If you turn off the retrieval of vCards from LDAP server:
- Cisco Unified Presence stores the vCards in the local database.
- When XMPP clients search for their own vCard, or the vCard for a contact, the vCards are retrieved from the local Cisco Unified Presence database.
Clients can set or modify their own vCard.

**Before You Begin**
Specify the LDAP server names and addresses for XMPP clients.

**Procedure**

**Step 1** Choose **Cisco Unified Presence Administration > Application > Third-Party Clients > Third-Party LDAP Settings**.

**Step 2** Enter information into the fields.

**Step 3** Check **Build vCards from LDAP** if you want to enable users to request vCards for their contacts and retrieve the vCard information from the LDAP server. Leave the check box unchecked if you want clients to be able to automatically request vCards for users as users join the contact list. In this case, clients retrieve the vCard information from the local Cisco Unified Presence database.

**Step 4** Enter the LDAP field required to construct the vCard FN field. Clients use the value in the vCard FN field to display the contact’s name in the contact list when a user requests a contact’s vCard.

**Step 5** In the Searchable LDAP Attributes table, map the client user fields to the appropriate LDAP user fields. If you use Microsoft LDAP Attributes, Cisco Unified Presence populates the default attribute values in the table.

**Step 6** Click **Save**.

**Step 7** Start the Cisco UP XCP Router service (if this service is not already running).

**Step 8** Restart the Cisco XCP Directory service.

**Table 9-2**

<table>
<thead>
<tr>
<th>Field</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDAP Server Type</td>
<td>Choose an LDAP server type from this list:</td>
</tr>
<tr>
<td></td>
<td>• Microsoft Active Directory</td>
</tr>
<tr>
<td></td>
<td>• Generic Directory Server - Choose this menu item if you are using any other supported LDAP server type (iPlanet, Sun ONE or OpenLDAP).</td>
</tr>
<tr>
<td>User Object Class</td>
<td>Enter the User Object Class value appropriate to your LDAP server type. This value must match the User Object Class value configured on your LDAP server. If you use Microsoft Active Directory, the default value is ‘user’.</td>
</tr>
<tr>
<td>Base Context</td>
<td>Enter the Base Context appropriate to your LDAP server. This value must match a previously configured domain, and/or an organizational structure on your LDAP server.</td>
</tr>
<tr>
<td>User Attribute</td>
<td>Enter the User Attribute value appropriate to your LDAP server type. This value must match the User Attribute value configured on your LDAP server. If you use Microsoft Active Directory, the default value is sAMAccountName.</td>
</tr>
<tr>
<td>LDAP Server 1</td>
<td>Choose a primary LDAP server.</td>
</tr>
<tr>
<td>LDAP Server 2</td>
<td>(Optional) Choose a backup LDAP server.</td>
</tr>
<tr>
<td>LDAP Server 3</td>
<td>(Optional) Choose a backup LDAP server.</td>
</tr>
</tbody>
</table>
Related Topic
Configure LDAP Server Names and Addresses for XMPP Clients, page 9-13

What To Do Next
Turn on the Cisco UP XCP Directory Service, page 9-16

Turn on the Cisco UP XCP Directory Service

You must turn on the Cisco UP XCP Directory Service to allow users of a third-party XMPP client to search and add contacts from the LDAP directory. Turn on the Cisco UP XCP Directory Service on all nodes in the cluster.

Note
Do not turn on the Cisco UP XCP Directory Service until you configure the LDAP server, and LDAP search settings for third-party XMPP clients. If you turn on the Cisco UP XCP Directory Service, but you do not configure the LDAP server, and LDAP search settings for third-party XMPP clients, the service will start, and then stop again.

Before You Begin
Configure the LDAP server, and LDAP search settings for third-party XMPP clients.

Procedure

Step 1 Choose Cisco Unified Serviceability > Tools > Service Activation.
Step 2 Choose the Cisco Unified Presence server from the Server menu.
Step 3 Choose Cisco UP XCP Directory Service.
Step 4 Click Save.

Related Topics
- Configure LDAP Server Names and Addresses for XMPP Clients, page 9-13
- Configure the LDAP Search Settings for XMPP Clients, page 9-14
Verify Domain Name for XMPP Clients

The domain name on the XMPP client, specifically the XMPP connection attempt domain name, must match the domain on Cisco Unified Presence. Verify the domain value on Cisco Unified Presence by performing the following procedure.

Procedure

Step 1 Choose Cisco Unified Presence Administration > System > Cluster Topology.
Step 2 Click Settings in the right pane, and verify the Domain Name value.

What To Do Next
Configure a Secure Connection between Cisco Unified Presence and XMPP Clients, page 10-1

Configure a Secure Connection between Cisco Unified Presence and XMPP Clients

Procedure

Step 1 Cisco Unified Presence Administration > System > Security > Settings
Step 2 Perform these configuration steps:
Chapter 10      Third-party XMPP Client Application Configuration on Cisco Unified Presence

If You Want To...

Establish a secure TLS connection between Cisco Unified Presence and XMPP client applications in a cluster.

Do This

Check Enable XMPP Client To CUP Service Secure Mode.

Note
Cisco recommends that you do not turn off this secure mode unless the XMPP client application can protect the client login credentials in non-secure mode. If you do turn off the secure mode, verify that you can secure the XMPP client-to-server communication in some other way.

Establish a secure TLS connection between Cisco Unified Presence and XMPP-based API client applications in a cluster.

Check Enable Web Client To CUP Service Secure Mode.

Note
If you turn on this setting, upload the certificates or signing certificates for the web client in the cup-xmpp-trust repository on Cisco Unified Presence.

Step 3  Click Save.

Step 4  If you checked Enable XMPP Client To CUP Service Secure Mode, choose Cisco Unified Serviceability > Tools > Control Center - Feature Services to restart the Cisco UP XCP Connection Manager service.
If you checked Enable Web Client To CUP Service Secure Mode, choose Cisco Unified Serviceability > Tools > Control Center - Feature Services to restart the Cisco UP XCP Web Connection Manager service

What To Do Next

Turn on Cisco Unified Presence Services to Support XMPP Clients, page 10-2

Related Topic

Verify Domain Name for XMPP Clients, page 10-1

Turn on Cisco Unified Presence Services to Support XMPP Clients

Note
Perform this procedure on each node in your Cisco Unified Presence cluster.
**Procedure**

**Step 1** Choose **Cisco Unified Serviceability > Tools > Service Activation**.

**Step 2** Choose the Cisco Unified Presence server from the Server menu.

**Step 3** Turn on the following services:

- Cisco UP XCP Connection Manager - Turn on this service if you are integrating XMPP clients (such as Cisco Unified Personal Communicator), or XMPP-based API clients, on Cisco Unified Presence.

- Cisco UP XCP Authentication Service - Turn on this service if you are integrating XMPP clients (such as Cisco Unified Personal Communicator), or XMPP-based API clients, or XMPP-based API clients, on Cisco Unified Presence.

- Cisco UP XCP Web Connection Manager - Optionally, turn on this service if you are integrating XMPP clients (such as Cisco Unified Personal Communicator), or XMPP-based API clients, on Cisco Unified Presence.

- Cisco UP XCP Router - Turn on this service to ensure XMPP clients function correctly.

**Step 4** Click **Save**.

**Related Topics**

*Verify Domain Name for XMPP Clients, page 10-1*
Turn on Cisco Unified Presence Services to Support XMPP Clients
Security Configuration on Cisco Unified Presence

June 16, 2014

• Create Login Banner, page 11-1
• Cisco Unified Presence Certificate Types, page 11-2
• Certificate Exchange Configuration between Cisco Unified Presence and Cisco Unified Communications Manager, page 11-3
• SIP Security Settings Configuration on Cisco Unified Presence, page 11-6
• XMPP Security Settings configuration on Cisco Unified Presence, page 11-8
• FIPS 140-2 Mode Configuration, page 11-10

Create Login Banner

From Cisco Unified Presence Release 8.6(4), administrators can create a banner that users acknowledge as part of their login to any Cisco Unified Presence interfaces. The administrator creates a .txt file using any text editor, includes important notifications that users should be made aware of, and uploads it to the Cisco Unified Presence OS Administration page. This banner will then appear on all Cisco Unified Presence interfaces notifying users of important information before they log in, including legal warnings and obligations. The following interfaces will display this banner before and after a user logs in: Cisco Unified Presence Administration, Cisco Unified OS Administration, Serviceability, Reporting, Disaster Recovery System, User Options, and the Cisco Unified Presence CLI prompt.

Procedure

Step 1 Create a .txt file with the contents you want to display in the banner.
Step 2 Sign in to Cisco Unified Operating System Administration.
Step 3 Choose Software Upgrades > Customized Logon Message.
Step 4 Click Browse and locate the .txt file.
Step 5 Click Upload File.
The banner will appear before and after login on most Cisco Unified Presence interfaces.
Cisco Unified Presence Certificate Types

This section describes the different certificates required for the clients and services on Cisco Unified Presence.

<table>
<thead>
<tr>
<th>Client Certificate</th>
<th>Certificate Types for Client Applications on Cisco Unified Presence</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP client (Cisco Unified Personal Communicator Release 7.x, IPPM, Cisco Unified Communications Manager)</td>
<td>tomcat</td>
</tr>
<tr>
<td>XMPP client (Cisco Unified Personal Communicator Release 8.0, third-party client)</td>
<td>cup-xmpp</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Service</th>
<th>Certificate</th>
<th>Certificate Trust Store</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP Proxy</td>
<td>cup</td>
<td>cup-trust</td>
<td></td>
</tr>
<tr>
<td>Presence Engine</td>
<td>cup</td>
<td>cup-trust</td>
<td></td>
</tr>
<tr>
<td>SOAP</td>
<td>tomcat</td>
<td>directory-trust</td>
<td></td>
</tr>
<tr>
<td>AXL</td>
<td>tomcat</td>
<td>directory-trust</td>
<td></td>
</tr>
<tr>
<td>LDAP</td>
<td>tomcat</td>
<td>directory-trust</td>
<td>LDAP uses the tomcat certificate because directory/directory-trust is now tomcat/ttrust.</td>
</tr>
<tr>
<td>Microsoft Exchange</td>
<td></td>
<td>cup-trust</td>
<td></td>
</tr>
<tr>
<td>Microsoft OCS/LCS Call Control</td>
<td>cup</td>
<td>cup-trust</td>
<td></td>
</tr>
<tr>
<td>SIP Federation</td>
<td>cup</td>
<td>cup-trust</td>
<td></td>
</tr>
<tr>
<td>XMPP Federation</td>
<td>cup-xmpp-s2s</td>
<td>cup-xmpp-trust</td>
<td>The trust certificates for cup-xmpp-s2s are stored in cup-xmpp-trust along with the general XMPP trust certificates.</td>
</tr>
</tbody>
</table>
Certificate Exchange Configuration between Cisco Unified Presence and Cisco Unified Communications Manager

This module describes the exchange of *self-signed* certificates between the Cisco Unified Communications Manager server and the Cisco Unified Presence server. You can use the Certificate Import Tool on Cisco Unified Presence to automatically import the Cisco Unified Communications Manager certificate to Cisco Unified Presence. However, you must manually upload the Cisco Unified Presence certificate to Cisco Unified Communications Manager.

Only perform these procedures if you require a secure connection between Cisco Unified Presence and Cisco Unified Communications Manager.

- **Prerequisites for Configuring Security**, page 11-3
- **Import the Cisco Unified Communications Manager Certificate to Cisco Unified Presence**, page 11-4
- **Restart the SIP Proxy Service**, page 11-4
- **Download the Certificate from Cisco Unified Presence**, page 11-4
- **Upload the Cisco Unified Presence Certificate to Cisco Unified Communications Manager**, page 11-5
- **Restart the Cisco Unified Communications Manager Service**, page 11-5

### Prerequisites for Configuring Security

Configure the following items on Cisco Unified Communications Manager:

- Configure a SIP security profile for Cisco Unified Presence.
- Configure a SIP trunk for Cisco Unified Presence:
  - Associate the security profile with the SIP trunk.
  - Configure the SIP trunk with the subject Common Name (CN) of Cisco Unified Presence certificate.

⚠️ **Note**

In Cisco Unified Presence Release 8.6(5), Subject Common Name has been renamed to Subject Alternative Name.

**Related Topic**

SIP Trunk Configuration on Cisco Unified Communications Manager, page 6-4
Import the Cisco Unified Communications Manager Certificate to Cisco Unified Presence

After the Certificate Import Tool completes the import operation, it reports whether or not it successfully connected to Cisco Unified Communications Manager, and whether or not it successfully downloaded the certificate from Cisco Unified Communications Manager. If the Certificate Import Tool reports a failure, see the Online Help for a recommended action. You can also manually import the certificate by choosing Cisco Unified OS Administration > Security > Certificate Management.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Choose Cisco Unified Presence Administration &gt; System &gt; Security &gt; Certificate Import Tool.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Choose CUP Service Trust from the Certificate Trust Store menu.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Enter the IP address, hostname or FQDN of the Cisco Unified Communications Manager server.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Enter a port number to communicate with the Cisco Unified Communications Manager server.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Click Submit.</td>
</tr>
</tbody>
</table>

What To Do Next

Restart the SIP Proxy Service, page 11-4

Restart the SIP Proxy Service

Before You Begin

Import the Cisco Unified Communications Manager certificate to Cisco Unified Presence.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Choose Cisco Unified Serviceability &gt; Tools &gt; Control Center - Feature Services on Cisco Unified Presence.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Choose Cisco UP SIP Proxy.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click Restart.</td>
</tr>
</tbody>
</table>

What To Do Next

Download the Certificate from Cisco Unified Presence, page 11-4

Download the Certificate from Cisco Unified Presence

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Choose Cisco Unified OS Administration &gt; Security &gt; Certificate Management on Cisco Unified Presence.</td>
</tr>
</tbody>
</table>
Step 2  Click **Find**.

Step 3  Choose the **cup.pem** file.

Step 4  Click **Download** and save the file to your local computer.

---

**Note**
Ignore any errors that Cisco Unified Presence displays regarding access to the cup.csr file; The CA (Certificate Authority) does not need to sign the certificate that you exchange with Cisco Unified Communications Manager.

---

**What To Do Next**
Upload the Cisco Unified Presence Certificate to Cisco Unified Communications Manager, page 11-5

### Upload the Cisco Unified Presence Certificate to Cisco Unified Communications Manager

**Before You Begin**
Download the certificate from Cisco Unified Presence.

**Procedure**

---

**Step 1**  Choose Cisco Unified OS Administration > Security > Certificate Management on Cisco Unified Communications Manager.

**Step 2**  Click **Upload Certificate**.

**Step 3**  Choose **Callmanager-trust** from the Certificate Name menu.

**Step 4**  Browse and choose the certificate (.pem file) previously downloaded from Cisco Unified Presence.

**Step 5**  Click **Upload File**.

---

**Related Topic**
Download the Certificate from Cisco Unified Presence, page 11-4

**What To Do Next**
Restart the Cisco Unified Communications Manager Service, page 11-5

### Restart the Cisco Unified Communications Manager Service

**Before You Begin**
Upload the Cisco Unified Presence certificate to Cisco Unified Communications Manager.
SIP Security Settings Configuration on Cisco Unified Presence

Configuring a TLS Peer Subject

When you import a Cisco Unified Presence certificate, Cisco Unified Presence automatically attempts to add the TLS peer subject to the TLS peer subject list, and to the TLS context list. Verify the TLS peer subject and TLS context configuration is set up to your requirements.

Before You Begin
You must configure the TLS Peer Subject before you configure the TLS Context.

Procedure

Step 1 Choose Cisco Unified Presence Administration > System > Security > TLS Peer Subjects.
Step 2 Click Add New.
Step 3 Perform one of the following actions for the Peer Subject Name:
   • Enter the subject CN of the certificate that the server presents.
   • Open the certificate, look for the CN and paste it here.
Step 4 Enter the name of the server in the Description field.
Step 5 Click Save.

What To Do Next
Configuring a TLS Context, page 11-7
Configuring a TLS Context

When you import a Cisco Unified Presence certificate, Cisco Unified Presence automatically attempts to add the TLS peer subject to the TLS peer subject list, and to the TLS context list. Verify the TLS peer subject and TLS context configuration is set up to your requirements.

Before You Begin
Configure a TLS peer subject on Cisco Unified Presence.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Choose Cisco Unified Presence Administration &gt; System &gt; Security &gt; TLS Context Configuration.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Click Find.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Choose Default_Cisco_UPS_SIP_Proxy_Peer_Auth_TLS_Context.</td>
</tr>
<tr>
<td>Step 4</td>
<td>From the list of available TLS peer subjects, choose the TLS peer subject that you configured.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Move this TLS peer subject to Selected TLS Peer Subjects.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Click Save.</td>
</tr>
<tr>
<td>Step 7</td>
<td>Choose Cisco Unified Presence Serviceability &gt; Tools &gt; Service Activation.</td>
</tr>
<tr>
<td>Step 8</td>
<td>Restart the Cisco Unified Presence SIP Proxy service for changes to the TLS context to take effect.</td>
</tr>
</tbody>
</table>

Related Topics
- Configuring a TLS Peer Subject, page 11-6
- Restart the SIP Proxy Service, page 11-4

Configuring the SIP Proxy-to-Proxy Intracluster Protocol Type

Choose the protocol that Cisco Unified Presence uses to route SIP messages securely in an intracluster deployment. The default value is the TLS protocol. Use TLS if a cluster node sends traffic over a unsecured network and you want a secure (encrypted) connection channel.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Choose System &gt; Security &gt; General Settings.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Choose a protocol type from the SIP Intra-cluster Proxy-to-Proxy Transport Protocol menu.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click Save.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Restart the Cisco Unified Presence SIP Proxy service for changes to the SIP proxy protocol to take effect.</td>
</tr>
</tbody>
</table>

Related Topic
- Restart the SIP Proxy Service, page 11-4
XMPP Security Settings configuration on Cisco Unified Presence

- XMPP Security Modes, page 11-8
- Configure the XMPP Certificate Settings, page 11-9

XMPP Security Modes

Cisco Unified Presence provides increased security for XMPP-based configuration. Table 11-3 describes these XMPP secure modes. To configure the XMPP secure modes on Cisco Unified Presence, choose Cisco Unified Presence Administration > System > Security > Settings.

<table>
<thead>
<tr>
<th>Secure Mode</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable XMPP Client To CUP Service Secure Mode</td>
<td>Restart the Cisco UP XCP Connection Manager if you edit Enable XMPP Client To CUP Service Secure Mode. Choose Cisco Unified Serviceability &gt; Tools &gt; Control Center - Feature Services to restart this service.</td>
<td>If you turn on this setting, Cisco Unified Presence establishes a secure TLS connection between the Cisco Unified Presence servers and XMPP client applications in a cluster. Cisco Unified Presence turns on this secure mode by default. Cisco recommends that you do not turn off this secure mode unless the XMPP client application can protect the client login credentials in non-secure mode. If you do turn off the secure mode, verify that you can secure the XMPP client-to-server communication in some other way.</td>
</tr>
</tbody>
</table>
### Configure the XMPP Certificate Settings

**Procedure**

<table>
<thead>
<tr>
<th>Secure Mode</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable XMPP Router-to-Router Secure Mode</td>
<td>Restart the Cisco UP XCP Router if you edit the Enable XMPP Router-to-Router Secure Mode. Choose Cisco Unified Serviceability &gt; Tools &gt; Control Center - Network Services to restart this service.</td>
<td>If you turn on this setting, Cisco Unified Presence establishes a secure TLS connection between XMPP routers in the same cluster, or in different clusters. Cisco Unified Presence automatically replicates the XMPP certificate within the cluster, and across clusters, as an XMPP trust certificate. An XMPP router will attempt to establish a TLS connection with any other XMPP router that is in the same cluster, or a different cluster, and is available to establish a TLS connection.</td>
</tr>
<tr>
<td>Enable Web Client to CUP Service Secure Mode</td>
<td>Restart the Cisco UP XCP Web Connection Manager if you edit Enable Web Client To CUP Service Secure Mode. Choose Cisco Unified Serviceability &gt; Tools &gt; Control Center - Feature Services to restart this service.</td>
<td>If you turn on this setting, Cisco Unified Presence establishes a secure TLS connection between the Cisco Unified Presence servers and XMPP-based API client applications. If you turn on this setting, upload the certificates or signing certificates for the web client in the cup-xmpp-trust repository on Cisco Unified Presence.</td>
</tr>
</tbody>
</table>

**Related Topics**

- Third-party XMPP Client Application Configuration on Cisco Unified Presence, page 10-1
- Configure the XMPP Certificate Settings, page 11-9
FIPS 140-2 Mode Configuration

The Federal Information Processing Standard (FIPS) is a U.S. and Canadian government certification standard that defines requirements that cryptographic modules must follow.

When you enable FIPS 140-2 mode, Cisco Unified Presence reboots, runs certification self-tests at startup, performs the cryptographic modules integrity check, and then regenerates the keying materials. At this point, Cisco Unified Presence operates in FIPS 140-2 mode.

Cisco Unified Presence FIPS mode uses FIPS 140-2 level 1 validated OpenSSL FIPS Module version 1.2. The relevant OpenSSL documentation can be found at: http://www.openssl.org/docs/fips/

In Cisco Unified Presence, you can perform the following FIPS-related tasks:
- Enable FIPS 140-2 mode
- Disable FIPS 140-2 mode
- Check the status of FIPS 140-2 mode

By default, Cisco Unified Presence is in non-FIPS mode. The administrator must enable FIPS mode. See the Command Line Reference Guide for Cisco Unified Presence for more information.

Node Reboot in FIPS 140-2 Mode

When you enable or disable FIPS, the Cisco Unified Presence server is automatically rebooted. When a Cisco Unified Presence server reboots in FIPS 140-2 mode, it will trigger FIPS startup self-tests in each of the FIPS 140-2 modules after rebooting.

If any of these self-tests fail, Cisco Unified Presence halts. If the startup self-test fails because of a transient error, restarting the Cisco Unified Presence server fixes the issue. However, if the start self-test error persists, it indicates a critical problem in the FIPS module and the only option is to use a recovery CD.

Forced Manual Sync of Certificates

When FIPS is enabled, all certificates are regenerated. However certificates may not be exchanged between intercluster peers. If this situation arises, follow the procedure below to manually sync the certificates between intercluster peers.
Certificates will not be exchanged between intercluster peers where one peer has FIPS enabled and the other peer does not have non-FIPS enabled. You can only sync certificates between intercluster peers when all peers are in FIPS mode.

**Procedure**

**Step 1** Choose [Cisco Unified Presence Administration > Presence > Inter-Clustering](#).

**Step 2** Choose the intercluster peer whose certificate is not present and choose the **Force Manual Sync** option.

**Step 3** Note the configuration details and click **Delete**.

**Step 4** Enable SSO from the CLI using this command:

```bash
utils fips enable
```

The node reboots.

**Step 5** Choose [Cisco Unified Presence Administration > Presence > Inter-Clustering](#) and re-add the intercluster peer.

**Step 6** Verify that all certificates are synced.

**Note** This may take several minutes.

**Step 7** If the certificates do not sync after 20 minutes, choose the intercluster peer whose certificate is not present and choose the **Force Manual Sync** option.

**Note** Cisco recommends that you allow ten minutes after importing intermediate or root Certificate Authority certificates before importing signed certificates.
Intercluster Peer Configuration

Prerequisites for Intercluster Deployment

You configure an intercluster peer between the publisher nodes in standalone Cisco Unified Presence clusters. No configuration is required on the subscriber nodes in a cluster for intercluster peer connections. Before you configure Cisco Unified Presence intercluster peers in your network, note the following:

- The intercluster peers must each integrate with a different Cisco Unified Communications Manager cluster.
- You must complete the required multi-node configuration in both the home Cisco Unified Presence cluster, and in the remote Cisco Unified Presence cluster:
  - Configure the system topology and assign your users as required.
  - Activate the services on each Cisco Unified Presence node in the cluster.
- You must turn on the AXL interface on the local Cisco Unified Presence publisher node, and on the remote Cisco Unified Presence publisher node. Cisco Unified Presence creates, by default, an intercluster application user with AXL permissions. To configure an intercluster peer, you will require the username and password for the intercluster application user on the remote Cisco Unified Presence server.
- You must turn on the Sync Agent on the local Cisco Unified Presence publisher node, and on the remote Cisco Unified Presence publisher node. Allow the Sync Agent to complete the user synchronization from Cisco Unified Communications Manager before you configure the intercluster peers.

For sizing and performance recommendations for intercluster deployments, including information on determining presence user profile, see the Cisco Unified Presence SRND.

Related Topics

- Expand the Cluster, page 17-8
- Cisco Unified Communication SRND: http://www.cisco.com/go/designzone
Intercluster Peer Configuration

- Configure an Intercluster Peer, page 12-2
- Turn on the Intercluster Sync Agent, page 12-3
- Verify the Intercluster Peer Status, page 12-4
- Update Intercluster Sync Agent Tomcat Trust Certificates, page 12-4

Configure an Intercluster Peer

Perform this procedure on the publisher node of the local Cisco Unified Presence cluster, and on the publisher node of the remote Cisco Unified Presence cluster (with which you want your local cluster to form a peer relationship).

Before You Begin

- Activate the AXL interface on the local Cisco Unified Presence node, and confirm that the AXL interface is activated on the remote Cisco Unified Presence publisher node.
- Confirm that the Sync Agent has completed the user synchronization from Cisco Unified Communications Manager on the local and remote cluster. If you configure the intercluster peer connection before the Sync Agent completes the user synchronization from Cisco Unified Communications Manager (on either the local or remote cluster), the status of the intercluster peer connection will display as failed.
- Acquire the AXL username and password for the intercluster application user on the remote Cisco Unified Presence server.
- If you do not use DNS in your network, read the Domain topic and the Node Name topic in this module.

Restriction

Cisco recommends that you use TCP as the intercluster trunk transport for all Cisco Unified Presence clusters.

Procedure

Step 1  Choose Cisco Unified Presence Administration > Presence > Inter-Clustering.
Step 2  Enter the IP address of the publisher node of a remote Cisco Unified Presence cluster.
Step 3  Enter the username of the application user on the remote Cisco Unified Presence server that has AXL permissions.
Step 4  Enter the associated password of the application user on the remote Cisco Unified Presence server that has AXL permissions.
Step 5  Enter the preferred protocol for SIP communication.
Intercluster Peer Configuration

Chapter 12

Note
If you enter TLS as the intercluster transport protocol, Cisco Unified Presence attempts to automatically exchange certificates between intercluster peers to establish a secure TLS connection. Cisco Unified Presence indicates whether or not the certificate exchange is successful in the intercluster peer status section.

Step 6
(Optional) Enter the External Phone Number Mask value. This is the E164 mask to apply to Directory Numbers retrieved from the remote cluster.

Step 7
Click Save.

Step 8
Restart the Cisco UP XCP Router service on all nodes in the local cluster.

Step 9
Repeat this procedure to create the remote intercluster peer, and then restart the Cisco UP XCP Router service on all nodes in the remote cluster.

What To Do Next

Turn on the Intercluster Sync Agent, page 12-3

Related Topics
- Restart the Cisco UP XCP Router Service, page 7-2
- Prerequisites for Intercluster Deployment, page 12-1
- How to Perform Intercluster Upgrades. For more information, see the Upgrade Guide for Cisco Unified Presence Release 8.6.
- Verify the Intercluster Peer Status, page 12-4

Turn on the Intercluster Sync Agent

By default, Cisco Unified Presence turns on the Intercluster Sync Agent parameter. Use this procedure to either verify that the Intercluster Sync Agent parameter is on, or to manually turn on this service.

The Intercluster Sync Agent uses the AXL/SOAP interface for the following:

- to retrieve user information for Cisco Unified Presence to determine if a user is a local user (on the local cluster), or a user on a remote Cisco Unified Presence cluster within the same domain.
- to notify remote Cisco Unified Presence clusters of changes to users local to the cluster.

Note
You must turn on the Intercluster Sync Agent on all nodes in the Cisco Unified Presence cluster because in addition to synchronizing user information from the local publisher node to the remote publisher node, the Intercluster Sync Agent also handles security between all nodes in the clusters.

Procedure

Step 1
Choose Cisco Unified Serviceability > Tools > Control Center - Network Services.

Step 2
Choose the Cisco Unified Presence server from the Server menu.

Step 3
Choose Cisco UP Intercluster Sync Agent.
Step 4 Click Start.

Related Topics
- Configure an Intercluster Peer, page 12-2
- Multi-node Scalability Feature, page 2-1

What To Do Next
Verify the Intercluster Peer Status, page 12-4

Verify the Intercluster Peer Status

Procedure

Step 1 Choose Cisco Unified Presence Administration > Presence > Inter-Clustering.
Step 2 Choose the peer address from the search criteria menu.
Step 3 Click Find.
Step 4 Choose the peer address entry that you wish to view.
Step 5 In the Intercluster Peer Status window:
  - Verify that there are check marks beside each of the result entries for the intercluster peer.
  - Make sure that the Associated Users value equals the number of users on the remote cluster.
  - If you choose TLS as the intercluster transport protocol, the Certificate Status item displays the status of the TLS connection, and indicates if Cisco Unified Presence successfully exchanged security certificates between the clusters. If the certificate is out-of-sync, you need to manually update the tomcat trust certificate (as described in this module). For any other certificate exchange errors, check the Online Help for a recommended action.
Step 6 Choose Cisco Unified Presence Administration > Diagnostics > System Troubleshooter.
Step 7 Verify that there are check marks beside the status of each of the intercluster peer connection entries in the InterClustering Troubleshooter section.

Related Topic
Update Intercluster Sync Agent Tomcat Trust Certificates, page 12-4

Update Intercluster Sync Agent Tomcat Trust Certificates

If the tomcat certificate status for an intercluster peer is out-of-sync, you need to update the Tomcat trust certificate. In an intercluster deployment this error can occur if you reuse the existing Intercluster Peer Configuration to point to a new remote cluster. Specifically, in the existing Intercluster Peer Configuration window, you change the Peer Address value to point to a new remote cluster. This error can also occur in a fresh Cisco Unified Presence install, or if you change the Cisco Unified Presence host or domain name, or if you regenerate the Tomcat certificate.
This procedure describes how to update the Tomcat trust certificate when the connection error occurs on the local cluster, and the ‘bad’ Tomcat trust certificates are associated with the remote cluster.

**Procedure**

**Step 1** Choose **Cisco Unified Presence Administration > Presence > Inter-Clustering**.

**Step 2** Click **Force Sync** to synchronize certificates with the remote cluster.

**Step 3** In the confirmation window that displays, click **Also resync peer’s Tomcat certificates**.

**Step 4** Click **OK**.

**Related Topics**

- Verify the Intercluster Peer Status, page 12-4
- For information about how to perform intercluster upgrades, see the *Upgrade Guide for Cisco Unified Presence*. 
PART 3

Feature Configuration

- Availability and Instant Messaging Configuration
- Cisco IP PhoneMessenger Service Configuration, page 14-1
- End User Setup and Handling
- Single Sign-On Configuration
Availability and Instant Messaging Configuration

Availability Setup

Turn On or Off Availability Sharing

This procedure describes how to turn on or off availability sharing for all client applications in a Cisco Unified Presence cluster.

Note

Availability sharing is turned on by default on Cisco Unified Presence.

Procedure

Step 1
Choose Cisco Unified Presence Administration > Presence > Settings.

Step 2
Configure the availability setting as follows:
Chapter 13  Availability and Instant Messaging Configuration

### Availability Setup

**Step 3**  Click **Save**.

**Step 4**  Restart the following services:

- Cisco UP XCP Router
- Cisco UP Presence Engine

---

### Configure Ad-hoc Presence Subscription Settings

**Note**  This section only applies if you deploy Cisco Unified Personal Communicator Release 8.5 or higher with Cisco Unified Presence.

These settings allow Cisco Unified Personal Communicator users to initiate temporary availability subscriptions to users that are not on their contact list.

**Procedure**

**Step 1**  Choose **Cisco Unified Presence Administration > Presence > Settings**.

**Step 2**  Check **Enable ad-hoc presence subscriptions** to turn on temporary availability subscriptions for Cisco Unified Personal Communicator Release users.

**Step 3**  Configure the maximum number of active temporary subscriptions that Cisco Unified Presence permits at one time. If you configure a value of zero, Cisco Unified Presence permits an unlimited number of active temporary subscriptions.

**Step 4**  Configure the time-to-live value (in seconds) for the temporary availability subscriptions.
When this time-to-live value expires, Cisco Unified Presence drops any temporary availability subscriptions and no longer temporarily monitors the availability status for that user.

**Note**
If the time-to-live value expires while the user is still viewing an instant message from a temporary availability subscription, the availability status that displays may not be current.

**Step 5**
Click Save.

**Step 6**
Cisco Unified Personal Communicator users need to sign out and sign back in to retrieve the latest temporary availability subscriptions settings on Cisco Unified Presence.

## Configure Maximum Contact List Size Per User

You can configure the maximum contact list size for a user; this is the number of contacts the user can add to their contact list. This setting applies to the contact list on Cisco Unified Personal Communicator client applications and on third-party client applications.

**Note**
Users who reach the maximum number of contacts are unable to add new contacts to their contact list, nor can other users add them as a contact. If a user is close to the maximum contact list size, and the user adds a group of contacts that pushes the contact list over the maximum number, Cisco Unified Presence does not add the surplus contacts. For example, if the maximum contact list size on Cisco Unified Presence is 200. A user has 195 contacts and attempts to add 6 new contacts to the list, Cisco Unified Presence adds five contacts and does not add the sixth contact.

If you are migrating users to Cisco Unified Presence, Cisco recommends that you set the Maximum Contact List Size and Maximum Watchers settings to Unlimited while importing user contact lists. This ensures that each migrated user contact list is fully imported. After all users have migrated, you can reset the Maximum Contact List Size and Maximum Watchers settings to the preferred values.

### Procedure

**Step 1**
Choose Cisco Unified Presence Administration > Presence > Settings.

**Step 2**
Edit the value of the Maximum Contact List Size (per user) setting.
The default value is 200.

**Step 3**
Click Save.

**Step 4**
Restart the Cisco UP XCP Router service.

### Related Topics
- Configure Maximum Number of Watchers Per User, page 13-4
- Restart the Cisco UP XCP Router Service, page 7-2
- Performing intercluster upgrades. For more information, see the Upgrade Guide for Cisco Unified Presence Release 8.6.
Configure Maximum Number of Watchers Per User

You can configure the number of watchers for a user, specifically the maximum number of people that can subscribe to see the availability status for a user. This setting applies to the contact list on Cisco Unified Personal Communicator clients and on third-party clients.

If you are migrating users to Cisco Unified Presence, Cisco recommends that you set the Maximum Contact List Size and Maximum Watchers settings to Unlimited while importing user contact lists. This ensures that each migrated user contact list is fully imported. After all users have migrated, you can reset the Maximum Contact List Size and Maximum Watchers settings to the preferred values.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Choose Cisco Unified Presence Administration &gt; Presence &gt; Settings.</td>
</tr>
<tr>
<td>2</td>
<td>Edit the value of the Maximum Watchers (per user) setting. The default value is 200.</td>
</tr>
<tr>
<td>3</td>
<td>Click Save.</td>
</tr>
<tr>
<td>4</td>
<td>Restart the Cisco UP XCP Router service.</td>
</tr>
</tbody>
</table>

IM Setup

Turn On or Off Instant Messaging for a Cisco Unified Presence Cluster

This procedure describes how to turn on or off instant message capabilities for all client applications in a Cisco Unified Presence cluster. Instant message capabilities is turned on by default on Cisco Unified Presence.

⚠️ Caution

When you turn off instant message capabilities on Cisco Unified Presence, all group chat functionality (adhoc and persistent chat) will not work on Cisco Unified Presence. Cisco recommends that you do not turn on the Cisco UP XCP Text Conference service or configure an external database for persistent chat on Cisco Unified Presence.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Choose Cisco Unified Presence Administration &gt; Messaging &gt; Settings.</td>
</tr>
<tr>
<td>2</td>
<td>Configure the instant messaging setting as follows:</td>
</tr>
</tbody>
</table>
Chapter 13  Availability and Instant Messaging Configuration

IM Setup

Step 3  Click Save.

Step 4  Restart the Cisco UP XCP Router service.

Turn On or Off Offline Instant Messaging

By default Cisco Unified Presence stores (locally) any instant messages that are sent to a user when they are offline, and Cisco Unified Presence delivers these instant messages to the user the next time they sign in to the client application. You can turn off (suppress) this feature so Cisco Unified Presence does not store offline instant messages. For example, in large deployments, this feature could require significant message storage, so you may want to suppress offline instant messages to increase performance.

Procedure

Step 1  Choose Cisco Unified Presence Administration > Messaging > Settings.

Step 2  Configure the offline instant messaging setting as follows:

<table>
<thead>
<tr>
<th>If You Want To...</th>
<th>Do This</th>
</tr>
</thead>
<tbody>
<tr>
<td>Turn off the storage of offline instant messages on Cisco Unified Presence. If you uncheck this setting, any instant messages that are sent to a user when they are offline, Cisco Unified Presence delivers these instant messages to the user the next time they sign in to the client application.</td>
<td>Uncheck Suppress Offline Instant Messaging.</td>
</tr>
<tr>
<td>Turn on the storage of offline instant messages on Cisco Unified Presence. If you check this setting, any instant messages that are sent to a user when they are offline, Cisco Unified Presence does not deliver these instant messages to the user the next time they sign in to the client application.</td>
<td>Check Suppress Offline Instant Messaging.</td>
</tr>
</tbody>
</table>
Step 3  Click Save.

Allow Clients to Log Instant Message History

You can prevent or allow users to log instant message history locally on their computer. On the client side, the application must support this functionality; it must enforce the prevention of instant message logging.

Procedure

Step 1  Choose Cisco Unified Presence Administration > Messaging > Settings.

Step 2  Configure the log instant message history setting as follows:

<table>
<thead>
<tr>
<th>If You Want To...</th>
<th>Do This</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow users of client applications to log instant</td>
<td>Check Allow clients to log instant message history (on supported clients only).</td>
</tr>
<tr>
<td>message history on Cisco Unified Presence.</td>
<td></td>
</tr>
<tr>
<td>Prevent users of client applications from logging</td>
<td>Uncheck Allow clients to log instant message history (on supported clients only).</td>
</tr>
<tr>
<td>instant message history on Cisco Unified Presence.</td>
<td></td>
</tr>
</tbody>
</table>

Step 3  Click Save.

Configure Do Not Disturb Settings

You can configure global administrator-level Do Not Disturb (DND) availability states as an alternative to the Busy state for phone calls and meetings. Cisco Unified Presence then sets global administrator-level Do Not Disturb (DND) availability states on all instant message client applications.

Note the following behavior for the DND feature:

- Cisco Unified Presence does not pass the administrator-level DND status to associated devices for the user.
- The administrator-level DND settings impact future calls and meetings, not those calls and meetings in progress at the time that you configure the DND setting.

If you turn off availability sharing on Cisco Unified Presence, the DND settings only impact users when they view their own availability.

Procedure

Step 1  Choose Cisco Unified Presence Administration > Presence > Settings.

Step 2  Configure the administrator-level DND setting as follows:
**Step 3**
Click **Save**.

---

**Related Topic**
Section “Do Not Disturb Behavior of Cisco Unified Personal Communicator” in the *Cisco Unified Personal Communicator Administration Guide for Cisco Unified Presence Release 8.6*
Cisco IP PhoneMessenger Service Configuration

June 16, 2014

- Prerequisites for Integrating Cisco IP PhoneMessenger, page 14-1
- Cisco IP PhoneMessenger Configuration on Cisco Unified Communications Manager, page 14-1
- Cisco IP PhoneMessenger Configuration on Cisco Unified Presence, page 14-3

Prerequisites for Integrating Cisco IP PhoneMessenger

Before you configure Cisco IP PhoneMessenger, make sure that you have configured the following:

- Configured the Cisco Unified Communications Manager server for integration with Cisco Unified Presence
- Configured the Cisco Unified Presence server for deployment in the network.

Related Topics

- Cisco Unified Communications Manager Configuration for Integration with Cisco Unified Presence, page 6-1.
- Cisco Unified Presence Network Setup, page 7-1

Cisco IP PhoneMessenger Configuration on Cisco Unified Communications Manager

- Configure Cisco IP PhoneMessenger as an Application User, page 14-2
- Configure a Phone Service for the Cisco IP PhoneMessenger, page 14-2
- Subscribe Phones to the Cisco IP PhoneMessenger Service, page 14-3
Configure Cisco IP PhoneMessenger as an Application User

**Procedure**

**Step 1**  
Choose Cisco Unified Communications Manager Administration > User Management > Application User.

**Step 2**  
Click Add New.

**Step 3**  
Enter an application username in the User ID field, for example, PhoneMessenger.

**Step 4**  
Enter a password for this application user, and confirm the password.

**Step 5**  
Choose the devices that you want the application user to control.

**Step 6**  
Click Save.

**Related Topic**

Subscribe Phones to the Cisco IP PhoneMessenger Service, page 14-3

**What To Do Next**

Configure a Phone Service for the Cisco IP PhoneMessenger, page 14-2

Configure a Phone Service for the Cisco IP PhoneMessenger

**Before You Begin**

Configure Cisco IP PhoneMessenger as an application user on Cisco Unified Communications Manager.

**Procedure**

**Step 1**  
Choose Cisco Unified Communications Manager Administration > Device > Device Settings > Phone Services.

**Step 2**  
Click Add New.

**Step 3**  
Enter PhoneMessenger in the Service Name field.

**Step 4**  
Enter IP Phone Messenger in the Service Description field.

**Step 5**  
Enter this URL in the Service URL field:

\[http://my-cups:8081/ippm/default?name=#DEVICENAME#\]

where my-cups specifies the IP address of the Cisco Unified Presence unless DNS is enabled on the phone.

**Step 6**  
Choose XML Service from the Service Category menu.

**Step 7**  
Choose Standard IP Phone Service from the Service Type menu.

**Step 8**  
Check Enable.

**Step 9**  
Click Save.
Subscribe Phones to the Cisco IP PhoneMessenger Service

Before You Begin
Configure a Phone Service for Cisco IP PhoneMessenger on Cisco Unified Communications Manager.

Procedure

Step 1  Choose Cisco Unified Communications Manager Administration > Device > Phone.
Step 2  Click Find.
Step 3  Choose a phone device link to access the Phone Configuration window.
Step 4  Choose Subscribe/Unsubscribe Services from the menu in the Related Links navigation box at the top right of the window.
Step 5  Click Go.
Step 6  Choose PhoneMessenger from the Select a Service menu in the Subscribed Cisco IP Phone Services window.
Step 7  Click Next.
Step 8  Click Subscribe when the window displays again.
Step 9  Click Save when the window displays again.
Step 10 Reset the phones individually or as a group.

Related Topic
Configure Cisco IP PhoneMessenger as an Application User, page 14-2

What To Do Next
Subscribe Phones to the Cisco IP PhoneMessenger Service, page 14-3

Cisco IP PhoneMessenger Configuration on Cisco Unified Presence

- Configure the Cisco IP PhoneMessenger Settings, page 14-4
- Use Cisco IP PhoneMessenger Across Clusters, page 14-4
- Configure Meeting Notification Settings, page 14-5
- Meeting Notification Feature Information, page 14-5
- Configure Cisco IP Phone Messenger Response Messages, page 14-6
Configure the Cisco IP PhoneMessenger Settings

**Before You Begin**
Obtain the application username and password that you configured for the Cisco IP PhoneMessenger on Cisco Unified Communications Manager.

**Restriction**
The Cisco IP PhoneMessenger application username and password must match the configured application username and password on Cisco Unified Communications Manager for the Cisco IP PhoneMessenger service to work properly.

**Procedure**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Choose Cisco Unified Presence Administration &gt; Application &gt; IP Phone Messenger &gt; Settings.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Choose On from the Application Status menu.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Enter the application username that you configured on Cisco Unified Communications Manager for the Cisco IP PhoneMessenger service.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Enter the password that you configured on Cisco Unified Communications Manager for the Cisco IP PhoneMessenger service.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Click Save.</td>
</tr>
</tbody>
</table>

**Troubleshooting Tip**
You can also use the System Dashboard to view enabled Cisco IP PhoneMessenger users in Cisco Unified Presence Administration. Choose Diagnostics > System Dashboard.

**Related Topics**
- Configure Cisco IP PhoneMessenger as an Application User, page 14-2
- Section “Configuring Firewalls to Pass Cisco Unified Personal Communicator Traffic” in the Cisco Unified Personal Communicator Administration Guide for Cisco Unified Presence Release 8.6

**Use Cisco IP PhoneMessenger Across Clusters**
Users can add contacts using valid extension numbers. Extension numbers are considered valid when both the user and contact reside within the same cluster. If the contact resides in a different cluster, the user will receive an error message after entering the extension number and the contact will be not added to the user’s contact list. In this case, contacts can be added by user ID. The geographic limitation does not exist for this method of adding contacts.
Configure Meeting Notification Settings

The Meeting Notification feature allows users to receive incoming meeting notifications from a Microsoft Outlook calendar on their Cisco IP PhoneMessenger enabled phone. To configure the Meeting Notification feature, you must integrate Cisco Unified Presence with a Cisco Unified MeetingPlace server.

Note
Cisco Unified Presence does not support Cisco Unified MeetingPlace Express.

Before You Begin
Obtain the hostname or IP address for the Cisco Unified MeetingPlace server.

Procedure

Step 1 Choose Application > IP Phone Messenger > Meeting Notification > Settings.

Step 2 Enter the host name or IP address for the Cisco Unified MeetingPlace server.

Step 3 Enter the port number for the Cisco Unified MeetingPlace server.
The default port numbers are 80 (SSL disabled) or 443 (SSL enabled).

Step 4 Check Use SSL if you want to use Secure Socket Layer (SSL) to communicate with the Cisco Unified MeetingPlace server.

Step 5 (If SSL enabled) Enter the subject common name for the Cisco Unified MeetingPlace server.

Note
If you choose to configure a secure connection between Cisco Unified Presence and Cisco Unified MeetingPlace, you must configure certificate exchange between the two servers. You must upload the Cisco Unified MeetingPlace server certificate to Cisco Unified Presence as a cup-trust certificate. Once you have uploaded the certificate to Cisco Unified Presence, you must restart the SIP proxy service.

Related Topics
- Configure the Cisco IP PhoneMessenger Settings, page 14-4
- Upload the Cisco Unified Presence Certificate to Cisco Unified Communications Manager, page 11-5

Meeting Notification Feature Information

Provide the following information to your users about setting up the Meeting Notification feature in Microsoft Outlook.

The Meeting Notification feature allows you to receive Microsoft Outlook meeting notifications on your Cisco IP PhoneMessenger phone. To use the Meeting Notification feature, you must set up your meeting invitations in Microsoft Outlook as follows:

- If you schedule a Cisco Unified MeetingPlace meeting, set the Location field on the Microsoft Outlook meeting invite window to:
MeetingPlace: XXXXXXX ID: XXXX
For example, MeetingPlace: 4761000 ID: 1020 where 4761000 is the meeting bridge number and 1020 is the meeting ID.

- If you schedule a meeting on another supported conferencing server, set the Location field on the Microsoft Outlook meeting invite window to:
  
  **Dial: XXXXXXX ID: XXXX**
  
  For example, Dial: 4762000 ID: 2000 where 4762000 is the meeting bridge number and 2000 is the meeting ID.

When the meeting alert message displays on your Cisco Unified IP Phone, you can join the scheduled meeting by pressing **Join**.

If you schedule a Cisco Unified MeetingPlace meeting, you can set Cisco Unified MeetingPlace to call your Cisco Unified IP Phone when the scheduled meeting is about to begin. On your Cisco Unified IP Phone, press **Today’s meetings**, choose the meeting entry, and press **Callback**.

**Note**
You can turn off the Meeting Notification feature on your Cisco Unified IP Phone. Choose **Settings > Meeting Notifications**, and turn off **Enable Meeting Notifications**.

**Related Topic**
*User Guide for Cisco Unified Presence*

## Configure Cisco IP Phone Messenger Response Messages

You can configure a predefined set of response messages to display in Cisco IP PhoneMessenger, for example:

- On the phone, hold on
- On the phone, call later
- Not available
- Yes

These response messages allow the phone user to respond to incoming phone messages quickly. In addition, you can predefine a custom message, and control and change the order in which messages are displayed on the phone.

You can configure up to a maximum of 10 predefined response messages.

**Procedure**

**Step 1** Choose **Cisco Unified Presence Administration > Application > IP Phone Messenger > Response Messages**.

**Step 2** Click **Add New**.

**Step 3** Enter or modify the message text.

**Step 4** Click the up or down arrow adjacent to the message to change the order in which the messages display.

**Step 5** Click **Save**.
Send a Broadcast Message

You can send a broadcast message to one or more Cisco IP PhoneMessenger users. Note the following changes to the broadcast feature behavior for Cisco Unified Presence Release 8.0(x):

- The Cisco IP PhoneMessenger user receives broadcast messages in the Messages menu on their phone. The sender of the message is ‘cupsystemadmin’.
- If a user signs in to Cisco IP PhoneMessenger and Cisco Unified Personal Communicator at the same time, the user does not receive the broadcast message.
- If a user signs in to Cisco IP PhoneMessenger and an XMPP client at the same time, but not Cisco Unified Personal Communicator, the user receives the broadcast message.

Procedure

**Step 1** Choose Cisco Unified Presence Administration > Application > IP Phone Messenger > Status.

**Step 2** Locate the Cisco IP PhoneMessenger user(s).

**Step 3** Perform one of the following actions:

**Step 4** Choose the end users to whom you want to send a broadcast message.

- Click Select All.
- Enter the broadcast message text in the Message box.

**Step 5** Click Broadcast.

**Step 6** Perform one of the following actions when you are prompted to confirm that you want to send a broadcast message:

- Click OK to send the message.
- Click Cancel to exit without sending the message.

**Step 7** Turn on the Cisco UP XCP SIP Federation Connection Manager service. In Cisco Unified Serviceability, choose Tools > Service Activation.

Sign Out a Cisco IP Phone Messenger User

You can force one or more users to sign out from the Cisco IP Phone Messenger service.

Procedure

**Step 1** Choose Cisco Unified Presence Administration > Application > IP Phone Messenger > Status.

**Step 2** Locate the Cisco IP Phone Messenger user.

**Step 3** Perform one of the following actions:

- Choose the end users that you want to sign out.
- Click Select All.

**Step 4** Click Logout.
Step 5  Perform one of the following actions when you are prompted to confirm that you want to sign out the users:

- Click OK to sign out the users.
- Click Cancel to exit without signing out the users.
End User Setup and Handling on Cisco Unified Presence

You can set up the authorization policy for Cisco Unified Presence end users and perform bulk user contact list imports and exports.

Configure User Assignment in System Topology

Note
This topic is only applicable if you have chosen to manually assign your users.

In system topology management GUI, you can manually unassign, assign or reassign users. You can assign users to a single node, and you can also distribute groups of users across the node, or nodes, in a cluster, or a given subcluster.

Before You Begin
- Read the user assignment recommendations topic.
- You may want to export users in bulk. Use the Bulk Administration Tool (BAT) to perform this procedure.

Restriction
- You can only assign licensed users.
- If you turn on High Availability in a subcluster, note that you can only assign or move users to nodes in that subcluster that are not in a failover state. Valid node states are Normal and Running in Backup Mode.
**Configuration and Administration of Cisco Unified Presence Release 8.6**

**Chapter 15  End User Setup and Handling**

**Authorization Policy Configuration**

**Automatic Authorization**

Cisco Unified Presence authorizes all availability subscription requests that it receives from SIP-based clients in the local enterprise. A local user running a SIP-based client automatically receives the availability status for contacts in the local enterprise, without being prompted to authorize these subscriptions on the client. Cisco Unified Presence only prompts the user to authorize the subscription of a contact in the local enterprise if the contact is on the blocked list for the user. This is the default authorization behavior for SIP-based clients on Cisco Unified Presence, and you cannot configure this behavior.
In the XMPP network, it is standard behavior for the server to send all availability subscriptions to the client, and the client prompts the user to authorize or reject the subscription. To allow enterprises to deploy Cisco Unified Presence with a mix of SIP-based and XMPP-based clients (to align the authorization policy for both client types), Cisco provides the following automatic authorization setting on Cisco Unified Presence:

- When you turn on automatic authorization, Cisco Unified Presence automatically authorizes all availability subscription requests it receives from both XMPP-based clients and SIP-based in the local enterprise. This is the default setting on Cisco Unified Presence.

- When you turn off automatic authorization, Cisco Unified Presence only supports XMPP-based clients. For XMPP-based clients, Cisco Unified Presence sends all availability subscriptions to the client, and the client prompts the user to authorize or reject the availability subscription. SIP-based clients will not operate correctly on Cisco Unified Presence when you turn off automatic authorization.

**Caution**

If you turn off automatic authorization, SIP-based clients such as Cisco Unified Personal Communicator Release 7.x are not supported. Only XMPP-based clients (Cisco Unified Personal Communicator Release 8.0 and third-party XMPP clients) are supported when you turn off automatic authorization.

**Related Topics**

- User Policy and Automatic Authorization, page 15-3
- Configure the Authorization Policy, page 15-4
- Integration Guide for Configuring Cisco Unified Presence for Interdomain Federation

### User Policy and Automatic Authorization

In addition to reading the automatic authorization policy, Cisco Unified Presence reads the policy settings for the user to determine how to handle availability subscription requests. Users configure the policy settings from either the Cisco Unified Personal Communicator client and the Cisco Unified Presence User Options interface. A user policy contains the following configuration options:

- **Blocked list** - a list of local and external (federated) users that will always see the availability status of the user as unavailable regardless of the true status of the user. The user can also block a whole federated domain.

- **Allowed list** - a list of local and external users that the user has approved to see their availability. The user can also allow a whole external (federated) domain.

- **Default policy** - the default policy settings for the user. The user can set the policy to block all users, or allow all users.

On the Cisco Unified Presence User Options interface, the user can also choose an ‘ask me’ setting so that the user is prompted to set their own Allow/Block policy for external contacts (except those external contacts that a user explicitly adds to their Allowed/Blocked list).

Note that if you turn off automatic authorization, Cisco Unified Presence automatically authorizes subscription requests a user that is on the contact list of another user. This applies to users in the same domain, and users in different domains (federated users). For example:

- UserA wishes to subscribe the view the availability status of UserB. Automatic authorization is off on Cisco Unified Presence, and UserB is not in the Allowed or Blocked list for the UserA.

- Cisco Unified Presence sends the availability subscription request to the client application of UserB, and the client application prompts userB to accept or reject the subscription.
• UserB accepts the availability subscription request, and UserB is added to the contact list of UserA.
• UserA is then automatically added to the contact list for UserB without being prompted to authorize the availability subscription.

Cisco Unified Presence will automatically add UserA to the contact list of UserB even if the policy for UserB (i) blocks the external domain, or (ii) the default policy for the user is block all, or (ii) ‘ask me’ is chosen.

If you deploy interdomain federation between a local Cisco Unified Presence enterprise and a supported external enterprise, Cisco Unified Presence does not apply the automatic authorization setting to availability subscription requests received from external contacts, unless the user has applied a policy on that external contact or domain. On receipt of a availability subscription request from an external contact, Cisco Unified Presence will only send the subscription request to the client application if the user chooses ‘ask me’ to be prompted to set their own Allow/Block policy for external contacts, and if the external contact or domain is not in either the Allowed or Blocked list for the user. The client application prompts the user to authorize or reject the subscription.

---

**Note**

Cisco Unified Presence uses common user policies for both availability and instant messages.

**Related Topics**

- Configure the Authorization Policy, page 15-4

---

**Configure the Authorization Policy**

See the Online Help topic in the Cisco Unified Presence Administration interface for a definition of all the parameters on this window.

**Procedure**

**Step 1** Choose Cisco Unified Presence Administration > Presence > Settings.
**Step 2** Configure the authorization setting as follows:
Bulk Rename of Contact IDs

The Cisco Unified Presence Bulk Assignment Tool (BAT) allows you to rename the contact ID (JID) in user contact lists from one format to another. For example, you can rename a user’s contact ID from firstname.lastname@domain.com to userid@domain.com and BAT will update each user’s contact list with the new contact ID.

Before you can run this job, you must upload a file containing a list of contact IDs and the corresponding new format of each of those contact IDs. The file must be a CSV file with the following format:

```
<Contact ID>, <New Contact ID>
```

where `<Contact ID>` is the existing contact ID and `<New Contact ID>` is the new format of the contact ID.

The following is a sample CSV file entry:

```
bob.jones@example.com, bjones@example.com
```
Complete the following procedure to upload the CSV file and rename the contact IDs for a list of users.

**Note**

You must complete this procedure on each Cisco Unified Presence cluster.

### Procedure

**Step 1** Upload the CSV file with the list of contact IDs that you want to rename in all contact lists.

- **a.** On the publisher node, choose Cisco Unified Presence Administration > Bulk Administration > Upload/Download Files.
- **b.** Click Add New.
- **c.** Click Browse to locate and choose the CSV file.
- **d.** Choose Contact as the Target.
- **e.** Choose Rename Contacts – Custom File as the Transaction Type.
- **f.** Click Save to upload the file.

**Step 2** On the publisher node, choose Cisco Unified Presence Administration > Bulk Administration > Contact List > Rename Contacts.

**Step 3** In the **File Name** field, choose the file that you uploaded.

**Step 4** Choose one of the following:

- Click Run Immediately to execute the Bulk Administration job immediately.
- Click Run Later to schedule a time to execute the Bulk Administration job. For more information about scheduling jobs in BAT, see the Online Help in CiscoUnified Presence Administration.

**Step 5** Click Submit. If you chose to run the job immediately, the job runs after you click Submit.

### Bulk Export of User Contact Lists

The Cisco Unified Presence Bulk Assignment Tool (BAT) allows you to export the contact lists of users who belong to a particular node or subcluster to a CSV data file. You can then use BAT to import the user contact lists to another node or subcluster in a different cluster. The BAT user contact list export and import features facilitate the moving of users between clusters. For more information about importing user contact lists, see Bulk Import of User Contact Lists, page 15-8.

BAT allows you to find and choose the users whose contact lists you want to export. The user contact lists are exported to a CSV file with the following format:

```
<User ID>,<User Domain>,<Contact ID>,<Contact Domain>,<Nickname>,<Group Name>
```

Table 15-1 describes the parameters in the export file.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User ID</td>
<td>The user ID of the Cisco Unified Presence user.</td>
</tr>
<tr>
<td>User Domain</td>
<td>The Presence domain of the Cisco Unified Presence user.</td>
</tr>
</tbody>
</table>
The following is a sample CSV file entry:

userA,example.com,userB,example.com,buddyB,General

Complete the following procedure to export user contact lists with BAT and download the export file.

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Choose Cisco Unified Presence Administration &gt; Bulk Administration &gt; Contact List &gt; Export</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Use the selection criteria to find the users whose contact lists you want to export. See the Online Help topic in the Cisco Unified Presence Administration interface for more information about finding and choosing users.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Click Next.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>In the File Name field, enter a name for the CSV file.</td>
</tr>
</tbody>
</table>
| **Step 5** | Choose one of the following:  
  - Click Run Immediately to execute the Bulk Administration job immediately.  
  - Click Run Later to schedule a time to execute the Bulk Administration job. For more information about scheduling jobs in BAT, see the Online Help in Cisco Unified Presence Administration. |
| **Step 6** | Click Submit. If you chose to run the job immediately, the job runs after you click Submit. |
| **Step 7** | To download the export file after the job has run, choose Cisco Unified Presence Administration > Bulk Administration > Upload/Download Files. |
| **Step 8** | Find and choose the export file that you want to download. |
| **Step 9** | Click Download Selected. |

**Related Topic**

Bulk Import of User Contact Lists, page 15-8
Bulk Import of User Contact Lists

You can use the Cisco Unified Presence Bulk Assignment Tool (BAT) to import user contact lists into Cisco Unified Presence. With this tool, you can prepopulate contact lists for new Cisco Unified Presence client users or add to existing contact lists. To import user contact lists, you must provide BAT with an input file that contains the user contact lists.

The input file must be a CSV file in the following format:

<User ID>,<User Domain>,<Contact ID>,<Contact Domain>,<Nickname>,<Group Name>

The following is a sample CSV file entry:

userA,example.com,userB,example.com,buddyB,General

Table 15-2 describes the parameters in the input file.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User ID</td>
<td>The user ID of the Cisco Unified Presence user. It can have a maximum of 132 characters.</td>
</tr>
<tr>
<td>User Domain</td>
<td>The Presence domain of the Cisco Unified Presence user. It can have a maximum of 128 characters.</td>
</tr>
<tr>
<td>Note</td>
<td>This is a mandatory parameter.</td>
</tr>
<tr>
<td>Contact ID</td>
<td>The user ID of the contact list entry. It can have a maximum of 132 characters.</td>
</tr>
<tr>
<td>Contact Domain</td>
<td>The Presence domain of the contact list entry. The following restrictions apply to the format of the domain name:</td>
</tr>
<tr>
<td></td>
<td>• Length must be less than or equal to 128 characters</td>
</tr>
<tr>
<td></td>
<td>• Contains only numbers, upper- and lowercase letters, and hyphens (-)</td>
</tr>
<tr>
<td></td>
<td>• Must not start or end with hyphen (-)</td>
</tr>
<tr>
<td></td>
<td>• Length of label must be less than or equal to 63 characters</td>
</tr>
<tr>
<td></td>
<td>• Top-level domain must be characters only and have at least two characters</td>
</tr>
<tr>
<td>Note</td>
<td>This is a mandatory parameter.</td>
</tr>
<tr>
<td>Nickname</td>
<td>The nickname of the contact list entry. It can have a maximum of 255 characters.</td>
</tr>
<tr>
<td>Group Name</td>
<td>The name of the group to which the contact list entry is to be added. It can have a maximum of 255 characters.</td>
</tr>
<tr>
<td>Note</td>
<td>This is a mandatory parameter.</td>
</tr>
</tbody>
</table>

Note: If you are moving users to another node or subcluster in a different cluster, you can use BAT to generate the CSV file for chosen users. See Bulk Export of User Contact Lists, page 15-6 for more information.
Complete the following steps to import user contact lists into Cisco Unified Presence:

- **Check Maximum Contact List Size**, page 15-9
- **Upload the Input File using BAT**, page 15-10
- **Create a New Bulk Administration Job**, page 15-10
- **Check Results of Bulk Administration Job**, page 15-10

### Before You Begin

Before you import the user contact lists, you must complete the following:

1. Provision the users on Cisco Unified Communications Manager.
2. Ensure that the users are licensed and assigned to Cisco Unified Presence.

**Note**

The default contact list import rate is based on the server hardware type. You can change the contact list import rate by choosing **Cisco Unified Presence Administrator > System > Service Parameters > Cisco Bulk Provisioning Service**. However, if you increase the default import rate, this will result in higher CPU and memory usage on Cisco Unified Presence.

### Check Maximum Contact List Size

Before you import contact lists, Cisco recommends that you check the Maximum Contact List Size and Maximum Watchers settings in Cisco Unified Presence.

Cisco recommends that you set the Maximum Contact List Size and Maximum Watchers settings to Unlimited while importing user contact lists to Cisco Unified Presence. This ensures that each migrated user contact list is fully imported. After all users have migrated, you can reset the Maximum Contact List Size and Maximum Watchers settings to the preferred values.

**Note**

It is possible to exceed the maximum contact list size without losing data when importing contact lists using BAT; however, Cisco recommends temporarily increasing the Maximum Contact List Size setting or setting the value to Unlimited for the import. You can reset the maximum value after the import is complete.

**Configure Maximum Contact List Size Per User**, page 13-3 describes how to configure the Maximum Contact List Size. **Configure Maximum Number of Watchers Per User**, page 13-4 describes how to configure the Maximum Watchers settings. The system default value is 200 for Maximum Contact List Size and 200 for Maximum Watchers.

**Note**

You only need to check the maximum contact list size on those clusters that contain users for whom you wish to import contacts. When you change Presence settings, the changes are applied to all nodes in the cluster; therefore you only need to change these settings on the Cisco Unified Presence Publisher node within the cluster.

### What To Do Next

**Upload the Input File using BAT**, page 15-10
Upload the Input File using BAT

The following procedure describes how to upload the CSV file using BAT.

**Procedure**

Step 1  Choose Cisco Unified Presence Administration > Bulk Administration > Upload/Download Files.

Step 2  Click Add New.

Step 3  Click Browse to locate and choose the CSV file.

Step 4  Choose Contact Lists as the Target.

Step 5  Choose Import Users’ Contacts – Custom File as the Transaction Type.

Step 6  Click Save to upload the file.

What To Do Next

Create a New Bulk Administration Job, page 15-10

Create a New Bulk Administration Job

The following procedure describes how to create a new bulk administration job in Cisco Unified Presence Administration.

**Procedure**

Step 1  Choose Cisco Unified Presence Administration > Bulk Administration > Contact List > Update.

Step 2  From the File Name drop-down list, choose the file to import.

Step 3  In the Job Description field, enter a description for this Bulk Administration job.

Step 4  Choose one of the following:

- Click Run Immediately to execute the Bulk Administration job immediately.
- Click Run Later to schedule a time to execute the Bulk Administration job. For more information about scheduling jobs in BAT, see the Online Help in Cisco Unified Presence Administration.

Step 5  Click Submit. If you chose to run the job immediately, the job runs after you click Submit.

What To Do Next

Check Results of Bulk Administration Job, page 15-10

Check Results of Bulk Administration Job

When the Bulk Administration job is complete, the Cisco Unified Presence BAT tool writes the results of the contact list import job to a log file. The log file contains the following information:

- The number of contacts that were successfully imported.
- The number of internal server errors that were encountered while trying to import the contacts.
- The number of contacts that were not imported (ignored). The log file lists a reason for each ignored contact at the end of the log file. The following are the reasons for not importing a contact:
  - Invalid format—invalid row format, for example, a required field is missing or empty
  - Invalid contact domain—the contact domain is in an invalid format; see Table 15-2 for the valid format of the contact domain
  - Cannot add self as a contact—you cannot import a contact for a user if the contact is the user
  - User’s contact list is over limit—the user has reached the maximum contact list size and no more contacts can be imported for that user
  - User is not assigned to local node—the user is not assigned to the local node
- The number of contacts in the CSV file that were unprocessed due to an error that caused the BAT job to finish early. This error rarely occurs.

Complete the following procedure to access this log file.

**Procedure**

**Step 1**  Choose **Cisco Unified Presence Administration > Bulk Administration > Job Scheduler.**

**Step 2**  Click **Find** and choose the job ID of the contact list import job.

**Step 3**  Click the **Log File Name** link to open the log.
CHAPTER 16

Single Sign-On Configuration

June 16, 2014

• Introduction, page 16-1
• Single Sign-On Configuration, page 16-4
• Disable Single Sign-On, page 16-29
• Uninstall OpenAM, page 16-31
• Set the Debug Level, page 16-32

Introduction

Cisco Unified Presence Release 8.6(4) and later supports Single Sign-On (SSO). SSO allows system administrators to log in to a Windows client machine on a Windows domain and use the following Cisco Unified Presence applications without being required to sign in again:

- Cisco Unified Presence User Options
- Cisco Unified Presence Administration
- Cisco Unified Serviceability
- Cisco Unified Reporting
- Disaster Recovery System
- Real-Time Monitoring Tool (RTMT) Administration
- Cisco Unified Operating System Administration
- Cisco UP Client Profile Agent - This option is only available in Cisco Unified Presence Release 8.6(5) and later and is only applicable to customers using Common Access Card (CAC) sign-on.

Task Flow for Single Sign-On Configuration

The following figure provides the sequence of tasks that are required to successfully configure SSO. Cisco recommends that you complete each task outlined in this flow in the order indicated, unless otherwise indicated. The following tasks are optional and do not fall within this task flow:

• Disable Single Sign-On, page 16-29
• Uninstall OpenAM, page 16-31
• Set the Debug Level, page 16-32
System Requirements

The Single Sign-On (SSO) feature makes use of a third-party application from ForgeRock called OpenAM. Support for the OpenAM application is available only from ForgeRock. This section of the document outlines the software requirements and configuration guidelines to enable the SSO feature to work with OpenAM. This document describes the installation of OpenAM on a Windows Server environments.

Advanced OpenAM configurations such as deploying OpenAM behind load balancers or the use of session replication between OpenAM servers has not been validated. For information about these advanced features, see http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/miscellany/oam90-cucm8586-cuc86-sso.pdf.

The SSO feature requires the following third-party applications:
Microsoft Windows Server 2008 R2
Microsoft Active Directory
ForgeRock Open Access Manager (OpenAM) Version 9.0

The SSO feature uses Active Directory and OpenAM in combination to provide SSO access to web-based client applications.

These third-party products must meet the following configuration requirements:

- Active Directory must be deployed in a Windows domain-based network configuration, not just as an LDAP server.
- The OpenAM server must be accessible on the network to all client systems and the Active Directory server.
- The Active Directory (Domain Controller) server, Windows clients, Cisco Unified Presence, and OpenAM must be in the same domain.
- DNS must be enabled in the domain.
- The clocks of all the entities that are participating in SSO must be synchronized.

See the third-party product documentation for more information about those products.

The following table provides a list of the software applications and versions that were used and tested in the procedures that appear in this chapter. In order for you to receive Cisco support, Cisco recommends that you adhere to these suggested requirements during your configuration.

<table>
<thead>
<tr>
<th>Component</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Directory</td>
<td>Windows Server 2008 R2 Enterprise</td>
</tr>
<tr>
<td>Desktop Operating System for end user clients</td>
<td>Windows 7 Professional (SP1)</td>
</tr>
<tr>
<td>Open Access Manager (OpenAM)</td>
<td>OpenAM Release 9.0:</td>
</tr>
<tr>
<td></td>
<td><a href="http://www.forgerock.org/downloads/openam_release9_20100207.zip">http://www.forgerock.org/downloads/openam_release9_20100207.zip</a></td>
</tr>
<tr>
<td></td>
<td>For more information:</td>
</tr>
<tr>
<td></td>
<td><a href="https://wikis.forgerock.org/confluence/display/openam/OpenAM+Snapshot+9+Release+Notes">https://wikis.forgerock.org/confluence/display/openam/OpenAM+Snapshot+9+Release+Notes</a></td>
</tr>
<tr>
<td>OpenAM underlying Operating System</td>
<td>Windows Server 2008 R2 Enterprise</td>
</tr>
<tr>
<td>Apache Tomcat on which OpenAM is loaded</td>
<td>Tomcat 6.0.2.0, Tomcat 7.0.29</td>
</tr>
<tr>
<td></td>
<td><a href="http://archive.apache.org/dist/tomcat/tomcat-7/v7_0.29/bin">http://archive.apache.org/dist/tomcat/tomcat-7/v7_0.29/bin</a></td>
</tr>
<tr>
<td>Java Development Kit (JDK) of OpenAM</td>
<td>JDK 7 Update 3</td>
</tr>
<tr>
<td>underlying Operating System</td>
<td>Web browser</td>
</tr>
<tr>
<td></td>
<td>Internet Explorer 8, 9 and Mozilla Firefox 10, 11</td>
</tr>
</tbody>
</table>
Before You Begin

To help ensure that the configuration of SSO runs as smoothly as possible, Cisco recommends that you gather the following information before you configure SSO:

- Ensure that the installed base operating system (such as Windows server) for the OpenAM system is running.
- Make a note of the Fully Qualified Domain Name (FQDN) of the Windows Active Directory (AD) server to which the OpenAM will be integrating.
- Make a note of the FQDN of the Windows server on which OpenAM is to be installed.
- Ensure that the Cisco Unified Presence Web Application timeout is set consistently across all Cisco Unified Presence nodes in the cluster and make note of that timeout value. You can use the Cisco Unified Presence Administration CLI to verify the timeout value by entering the following command: show webapp session timeout. For more information, see the Command Line Interface Reference Guide for Cisco Unified Presence Release 8.0, 8.5, and 8.6.
- Ensure that Cisco Unified Communications Manager has been configured to sync users from Active Directory (AD) using “sAMAccountName” as the LDAP Attribute for User ID. For more information, see the “DirSync Service” section in the Cisco Unified Communications Manager System Guide.

Single Sign-On Configuration

Provision Active Directory for Single Sign-On

Prerequisite

Ensure that you have Windows Server 2008 support tools installed. Support tools are installed on Windows Server 2008 by default.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Log in to the Active Directory (AD) server.</td>
</tr>
<tr>
<td>Step 2</td>
<td>From the Start menu, choose All Programs &gt; Administration Tools &gt; Active Directory Users and Computers.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Right-click Users and choose New &gt; User.</td>
</tr>
<tr>
<td>Step 4</td>
<td>In the User logon name field, enter the OpenAM server hostname.</td>
</tr>
<tr>
<td>Note</td>
<td>The OpenAM server hostname should not include the domain name.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Click Next.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Enter and confirm a password. This password is required in Step 10.</td>
</tr>
<tr>
<td>Step 7</td>
<td>Uncheck the User must change password at next login check box.</td>
</tr>
<tr>
<td>Step 8</td>
<td>Click Next.</td>
</tr>
</tbody>
</table>
Step 9  Click **Finish** to finish creating the new user account.

Step 10  Create a keytab file on the AD server using the following command from the command prompt.

```
ktpass -princ HTTP/<hostname>.<domainname>@<DCDOMAIN> -pass <password> -mapuser <userName> -out <hostname>.HTTP.keytab -ptype KRBS_NT_PRINCIPAL -target <DCDOMAIN>
```

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>hostname</td>
<td>The hostname (not the FQDN) of your OpenAM server</td>
<td>server1</td>
</tr>
<tr>
<td>domainname</td>
<td>The AD domain name</td>
<td>cisco.com</td>
</tr>
<tr>
<td>DCDOMAIN</td>
<td>The AD domain name, entered in block capitals</td>
<td>CISCO.COM</td>
</tr>
<tr>
<td>password</td>
<td>The password value that was specified when you created the user account for the OpenAM server earlier in this procedure.</td>
<td></td>
</tr>
<tr>
<td>userName</td>
<td>The AD account name entered in Step 4; this value should be the OpenAM server hostname.</td>
<td>server1</td>
</tr>
</tbody>
</table>

**Example:**

```
ktpass -princ HTTP/server1.cisco.com@CISCO.COM -pass cisco!123 -mapuser server1 -out server1.HTTP.keytab -ptype KRBS_NT_PRINCIPAL -target CISCO.COM
```

**Note**  Make a note of the `-princ` value for later procedures.

Step 11  After successful creation of the keytab file, copy the keytab file to a location on the OpenAM server; this path will later be specified in OpenAM configuration. Create a directory under C:\> and copy the above keytab file. For example, “C:/keytab/server1.HTTP.keytab”.

---

**Client Browser Configuration for Single Sign-On**

To use SSO for a browser-based client application, you must configure the web browser. The following sections describe how to configure client browsers to use SSO:

- Configure Internet Explorer for Single Sign-On, page 16-5
- Configure Firefox for Single Sign-On, page 16-7

**Configure Internet Explorer for Single Sign-On**

The SSO feature supports Windows clients running Internet Explorer. Perform the following procedure to configure Internet Explorer to use SSO.

**Note**  For a list of web browsers and supported versions, see Table 16-1.
Single Sign-On Configuration

Chapter 16  Single Sign-On Configuration

Procedure

Step 1  Choose Tools > Internet Options > Advanced tab.
Step 2  Check Enable Integration Windows Authentication.
Step 3  Click OK to save the changes.
Step 4  Restart Internet Explorer.
Step 5  Choose Tools > Internet Options > Security > Local Intranet and click Custom Level.
Step 6  Under User Authentication, check Automatic Logon Only in Intranet Zone.
Step 7  Click OK.
Step 8  Click Sites.
Step 9  Check Automatically detect intranet network.
Step 10  Click Advanced.
Step 11  Fill in the Add this website to the zone field with the FQDN of the OpenAM server using the following format: https://OpenAM_FQDN.
Step 12  Click Add.
Step 13  Click Close.
Step 14  Click OK.
Step 15  Uncheck Enable Protected Mode.
Step 16  Click Apply.
Step 17  Click OK.
Step 18  Restart Internet Explorer.
Step 19  Open the Windows Registry Editor:
   • For Windows XP or Windows 2008 - Choose Start > Run and type regedit.
   • For Windows Vista and Windows 7.0 - Choose Start and type regedit. For Windows Vista, you must click Continue.
Step 20  Under registry key HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA, right-click and choose New > DWORD (32-bit) value and rename it to be SuppressExtendedProtection.
Step 21  Right-click on the newly created DWORD, choose Modify.

Note  Only an administrator can set the DWORD.

Step 22  Set the following values:
   • Base: hexadecimal
   • Value data: 002
Chapter 16      Single Sign-On Configuration

Single Sign-On Configuration

Note
The newly created DWORD will appear in the LSA directory list as follows:
Name: SuppressExtendedProtection
Type: REG_DWORD
Value: 0x00000002 (2)

Configure Firefox for Single Sign-On

The SSO feature supports Windows clients that are running Firefox.

Note
For a list of web browsers and supported versions, see Table 16-1.

Procedure

Step 1
Open Firefox and enter the following URL page: about:config.

Step 2
Scroll down to network.negotiate-auth.trusted-uris.

Step 3
Right-click the Preference Name network.negotiate-auth.trusted-uris, and choose Modify.

Step 4
Set the string value to your domain (for example, cisco.com).

Step 5
Click OK.

Windows Registry Configuration for Real-Time Monitoring Tool

Configuring SSO for the Real-Time Monitoring Tool (RTMT) is optional. To achieve this configuration, you must create the following new registry key on your Desktop client (Windows XP or Windows 7).

Note
An administrator must set the allowtgtsessionkey registry key entry for the Desktop client.

Procedure

Step 1
Go to either of the following locations, depending on your operating system:
   - Windows XP: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\Kerberos
   - Windows Vista/Windows 7:
     HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\Kerberos\Parameters

Step 2
Right-click the folder, choose New > DWORD (32-bit) Value, and rename it to be allowtgtsessionkey.

Step 3
Right-click the newly created registry key and choose Modify.

Step 4
In the Value data: field, enter 1.
Install Java

OpenAM requires a Java Runtime Environment (JRE) to operate. The following procedure provides details for installing the JRE on your Windows server, forming the OpenAM base system.

Procedure

**Step 1** Go to [http://www.oracle.com/technetwork/java/archive-139210.html](http://www.oracle.com/technetwork/java/archive-139210.html).

**Step 2** Download the recommended version of the JDK installation file by choosing the executable file that corresponds to your server architecture (Windows x86 or Windows x64).

**Note** See Table 16-1 for a list of the recommended versions of software.

**Step 3** Double-click the downloaded file to begin the installation of the JDK and accept the default values provided in the Installation wizard.

**Note** Make a note of the installation directory. This value indicates the location of the Java JRE and can be used to infer the JDK directory path. Example values may be as follows, depending on the JDK values that are used:

- jre-path=C:\Program Files\Java\jre7
- jdk-path=C:\Program Files\Java\jdk1.7.0_03

**Step 4** A Java keystore and the associated security certificates are required to facilitate secure connections to the OpenAM server, which runs on Apache Tomcat. Choose one of the following options:

- If you use a self-signed security certificate for OpenAM/Tomcat, proceed to Step 5.
- If you use a Certificate Authority (CA) signed security certificate for OpenAM/Tomcat, proceed to Step 11.

**Step 5** Create the Java keystore by opening a Windows command prompt on the Windows Server, and executing the following command:

```
C:\> "C:\Program Files\Java\jdk1.7.0_03\bin\keytool.exe" -genkey -alias tomcat -keyalg RSA -validity 1825 -keystore C:\keystore -ext BC:c=ca:true
```

This command creates the Java keystore file at the following location: C:\keystore.

The keytool command is located in the <jdk-path>/bin directory, the exact path to the keytool command in the preceding command may vary depending on the JDK version used. For information about the keytool command, see [http://docs.oracle.com/javase/7/docs/technotes/tools/windows/keytool.html](http://docs.oracle.com/javase/7/docs/technotes/tools/windows/keytool.html).

**Note** The keytool command with -ext option requires JDK 7. Using the -ext option with the above value results in an OpenAM/Tomcat certificate with the CA flag set to True. The CA flag must be set to True or the Cisco Unified Presence Operating System Administration interface may fail to upload the certificate into the tomcat-trust trust store. For more information, see Import the OpenAM Certificate into Cisco Unified Presence, page 16-25.

**Step 6** When you are prompted for a keystore password, enter a valid keystore password. For example, “cisco!123”. Make a note of the keystore password as it is required to access the keystore.
Step 7 When you are prompted to enter the first name and last name, enter the FQDN (hostname.domainname) of the OpenAM server. You also are prompted to enter your organization unit name, organization name, city or locality, state or province, and two-letter country code.

Step 8 When you are prompted for a Tomcat password, press RETURN to use the same keystore password value for the Tomcat private key. The Java keystore is created at the location specified in the keytool command. For example, C:\keystore.

Step 9 You can view the Tomcat certificate in the keystore using the following command:

Example:
```
C:\>"C:\Program Files\Java\jdk1.7.0_03\bin\keytool.exe" -list -v -alias tomcat -keystore C:\keystore
```

Step 10 If you chose to use a self-signed security certificate for Tomcat, proceed to the end of this procedure and consider this task complete.

Step 11 Create a Java keystore to store Certificate Authority (CA)-signed security certificates for OpenAM/Tomcat. Open a command prompt on the Windows Server and execute the following command:

Example:
```
C:\>"C:\Program Files\Java\jdk1.7.0_03\bin\keytool.exe" -genkey -alias tomcat -keyalg RSA -validity 1825 -keystore C:\keystore
```

This command creates the Java keystore file at the following location: C:\keystore. The keytool command is located in the <jdk-path>/bin directory, the exact path to the keytool command in the example provided above may vary depending on the JDK version used. For information about the keytool command, see http://docs.oracle.com/javase/7/docs/technotes/tools/windows/keytool.html.

Step 12 When you are prompted for a keystore password, enter a valid keystore password. For example, “cisco!123”. Make a note of the keystore password as it is required to access the keystore.

Note Do not use example values on the production server; Use a unique password value for the keystore. This password will be visible in plain text in the Apache Tomcat configuration files and utilities.

Step 13 When you are prompted to enter first name and last name, enter the FQDN (hostname.domainname) of your OpenAM server. You also are prompted to enter your organization unit name, organization name, city or locality, state or province, and two-letter country code.

Step 14 When you are prompted for a Tomcat password, press RETURN to use the same keystore password value for the Tomcat private key. The Java keystore is created at the location specified in the keytool command. For example, C:\keystore.

Step 15 You can view the Tomcat certificate in the keystore using the following command:

Example:
C:\>"C:\Program Files\Java\jdk1.7.0_03\bin\keytool.exe" -list -v
-alias tomcat -keystore C:\keystore

Step 16 Generate a certificate signing request (CSR) for this OpenAM/Tomcat instance. Open a command
prompt on the Windows Server and execute the following command:

Example:
C:\>"C:\Program Files\Java\jdk1.7.0_03\bin\keytool.exe" -certreq
-keyalg RSA -alias tomcat -file certreq.csr -keystore C:\keystore

Note This command creates the CSR and writes it to a file called certreq.csr.

Step 17 Submit the CSR to your CA, request the CA to sign the CSR and create a certificate. Obtain and copy
the following certificates to the Windows Server that is going to be the OpenAM server:
- CA signing or root certificate
- Intermediate signing certificates (if applicable)
- Newly signed OpenAM/Tomcat certificate

Note Refer to the CA documentation for instructions about completing these tasks.

Step 18 Import the CA signing or root certificate into the Java keystore that was created in Step 11. Open a
command prompt on the Windows Server and execute the following command, answering “yes” to the
prompt, “Trust this certificate?”:

Example:
C:\>"C:\Program Files\Java\jdk1.7.0_03\bin\keytool.exe" -import -alias
root -trustcacerts -file <filename_of_the_CA_root_certificate>
-keystore C:\keystore

Step 19 You can view the CA signing certificate in the keystore using the following command:

Example:
C:\>"C:\Program Files\Java\jdk1.7.0_03\bin\keytool.exe" -list -v
-alias root -keystore C:\keystore

Step 20 Import any other intermediate signing certificates (if applicable) into the Java keystore that was created
in Step 11. Open a command prompt on the Windows Server and execute the following command,
answering “yes” to the prompt, “Trust this certificate?”:

Example:
C:\>"C:\Program Files\Java\jdk1.7.0_03\bin\keytool.exe" -import -alias
inter01 -trustcacerts -file <filepath_of_the_intermediate_signing_certificate>
-keystore C:\keystore

Note The -alias option must be updated with a value unique to the Java keystore, otherwise the import
operation will result in an error similar to the following: “Certificate not imported,
alias<inter01> already exists.”

Step 21 You can view any of the intermediate signing certificates in the keystore using the following command:

Example:
C:\>"C:\Program Files\Java\jdk1.7.0_03\bin\keytool.exe" -list -v
-alias inter01 C:\keystore

**Note** The -alias option must be updated with the corresponding alias value for the intermediate
certificates you wish to view. The above example uses a sample alias value of “inter01”.

**Step 22** Import the newly signed certificate OpenAM/Tomcat certificate into the Java keystore that was created
in Step 11. Open a command prompt on the Windows Server and execute the following command:

**Example:**

C:\>"C:\Program Files\Java\jdk1.7.0_03\bin\keytool.exe" -import -alias
tomcat -file <new_certificate_filepath> -keystore C:\keystore

**Step 23** You can view the new OpenAM/Tomcat certificate in the keystore using the following command:

**Example:**

C:\>"C:\Program Files\Java\jdk1.7.0_03\bin\keytool.exe" -list -v
-alias tomcat -keystore C:\keystore

**Note** The issuer of this new Tomcat certificate is the CA or one of the intermediate CAs (if applicable).

---

**Import Cisco Unified Presence Certificates into OpenAM**

OpenAM must communicate with a J2EE Agent component that exists on each Cisco Unified Presence
node for which SSO is enabled. This communication is over an encrypted channel and therefore the
necessary security certificates must be imported onto OpenAM.

The OpenAM server must trust the security certificate presented by each Cisco Unified Presence node
for the encrypted communication channel to be established. OpenAM trusts a security certificate by
importing the required security certificates into the OpenAM keystore. A given Cisco Unified Presence
node can present one of two types of security certificate:

- Self-signed certificate
- CA-signed certificate

**Note** The Cisco Unified Presence tomcat certificate and tomcat-trust trust store contain the security
certificates of interest for secure communication with OpenAM. The other Cisco Unified Presence
certificates and associated trust stores are not relevant for SSO (for example, cup, cup-xmpp,
cup-xmpp-s2s or ipsec).

If your SSO-enabled Cisco Unified Presence deployment is configured to use self-signed certificates,
each of the self-signed certificates must be imported into OpenAM.

If your SSO-enabled Cisco Unified Presence deployment is configured to use CA-signed certificates, the
CA root certificate and any associated intermediate certificates must be imported into OpenAM. If you
are also using a CA-signed certificate for your OpenAM/Tomcat instance, the required CA root and
intermediate certificates may already be imported into the OpenAM keystore.
This procedure provides the details on how to identify the type of security certificate being used by the Cisco Unified Presence node and how to import the certificates into the OpenAM keystore that was created in Install Java, page 16-8.

**Procedure**

**Step 1** Sign in to Cisco Unified Presence Operating System Administration for a given Cisco Unified Presence node for which SSO is to be enabled.

**Step 2** Choose **Security > Certificate Management**.

**Step 3** Click **Find**.

**Step 4** Locate the entry with **Certificate Name** of tomcat.

**Step 5** Examine the **Description** column of the tomcat certificate.

**Step 6** If the description states that the tomcat certificate is **Self-signed certificate generated by system**, this indicates that the Cisco Unified Presence node is using a self-signed certificate. If this description is not present, a CA-signed certificate can be assumed.

- If the certificate is self-signed, proceed to Step 7.
- If the certificate is CA-signed, proceed to Step 13.

**Step 7** Choose the **tomcat.pem** link.

**Step 8** Click **Download** to download the tomcat.pem file.

**Step 9** Copy the **tomcat.pem** file to the OpenAM server.

**Step 10** Import the **tomcat.pem** file into the keystore (created in Install Java, page 16-8) on the OpenAM server as a trusted certificate. Open a command prompt on the Windows server (OpenAM) and execute the following command, updating the command with the values for your keytool command path and keystore location as applicable for your environment, and answer “yes” to the prompt “Trust this certificate?”:

```
C:\>"C:\Program Files\Java\jdk1.7.0_03\bin\keytool.exe" -import
-alias cup01 -trustcacerts -file <full_filepath_of_the_tomcat.pem>
-keystore C:\keystore
```

**Note** The -alias option must be updated with a value unique to the Java keystore, otherwise the import operation will result in an error similar to the following: “Certificate not imported, alias <cup01> already exists.”

**Step 11** You can view the **tomcat.pem** in the keystore using the following command, updating the command with the values for your keytool command path and keystore location as applicable for your environment:

```
C:\>"C:\Program Files\Java\jdk1.7.0_03\bin\keytool.exe" -list -v
-alias cup01 -keystore C:\keystore
```

**Note** The -alias option must match the value used in Step 10, otherwise the keystore entry may not be found.

**Step 12** Skip to Step 16.

**Step 13** Identify the CA root certificates and any intermediate certificates that were used to sign your Cisco Unified Presence Tomcat certificate. Download the required certificates (CA root certificates and any intermediate certificates) from your CA to your OpenAM server.
Step 14  Import these certificates into the keystore on the OpenAM server as trusted certificates. Open a command prompt on the Windows server (OpenAM) and execute the following command for each downloaded certificate, updating the command with the values for your keytool command path and keystore location as applicable for your environment, and answer “yes” to the prompt “Trust this certificate?”.

C:\>"C:\Program Files\Java\jdk1.7.0_03\bin\keytool.exe" -import -alias root_ca -trustcacerts -file <full_filepath_of_the_certificate> -keystore C:\keystore

**Note**  The -alias option must be updated with a value unique to the Java keystore, otherwise the import operation will result in an error similar to the following: “Certificate not imported, alias <root_ca> already exists.”

Step 15  You can view the certificate in the keystore using the following command, updating the command with the values for your keytool command path and keystore location as applicable for your environment:

C:\>"C:\Program Files\Java\jdk1.7.0_03\bin\keytool.exe" -list -v -alias root_ca -keystore C:\keystore

**Note**  The -alias option must match the value used in Step 14, otherwise the keystore entry may not be found.

Step 16  Repeat this procedure for each Cisco Unified Presence node for which SSO is to be enabled.

**Note**  In the case of CA-signed certificates used on the Cisco Unified Presence node, it is not necessary to import the same CA and/or intermediate certificate into the OpenAM keystore more than once. If you find that a Cisco Unified Presence node has been signed by the same CA and/or intermediate certificate, there is no need to import those certificates into the OpenAM keystore again.

### Install Tomcat

OpenAM requires that the Apache Tomcat Web Container be installed on the OpenAM Windows server base system. This procedure provides details on how to install Apache Tomcat on the OpenAM Windows server base system. See the following table for descriptions of the variables referred to in this procedure.
Table 16-2 Variable Descriptions

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;certstore-path&gt;</td>
<td>The file path to the Java keystore used by Java applications and Apache Tomcat. Trusted server public certificates are stored in this keystore. See Steps 5 or 11 of Install Java, page 16-8 to determine the file path for the Java keystore.</td>
</tr>
<tr>
<td>&lt;certstore-password&gt;</td>
<td>The password used to access the Java keystore located at &lt;certstore-path&gt;. See Step 6 or 12 of Install Java, page 16-8 to determine the value used for the Java keystore password.</td>
</tr>
</tbody>
</table>

Procedure

**Step 1** Download the recommended version of Apache Tomcat to your Windows server that forms the OpenAM base system.

**Note** See Table 16-1 for a list of the recommended versions of software.

**Note** Download the 32bit/64bit Windows Service Installer executable file.

**Step 2** Double-click the downloaded file to begin the installation of Apache Tomcat.

**Step 3** From the Apache Tomcat Setup wizard, click Next.

**Step 4** In the License Agreement dialog box, click I Agree.

**Step 5** In the Choose Components dialog box, Click Minimum as the type of install and click Next.

**Step 6** In the Configuration dialog box, accept the default settings and click Next.

**Step 7** In the Java Virtual Machine dialog box, ensure the installed JRE path is set to the value of jre-path. See Step 3 of Install Java, page 16-8.

**Note** If you are using the recommended version of Java, the path will display by default. If you are not using the recommended version of Java, ensure that the path chosen reflects the path chosen in Step 3 of Install Java, page 16-8.

**Step 8** Click Next.

**Step 9** In the Choose Install Location dialog box, accept the default settings and click Install. Note the Tomcat install location, because it is required later.

**Note** The installation location is referred to as tomcat-dir later in this procedure.

**Step 10** Click Finish.

**Step 11** Configure Apache Tomcat to start automatically:

a. Choose Start > All Programs > Apache Tomcat 7.0 Tomcat7 > Configure Tomcat.
b. From the General tab, set the Startup type as Automatic.
c. Click Apply.
d. Click OK.

Step 12 Configure the Apache Tomcat runtime parameters:

a. Choose Start > All Programs > Apache Tomcat 7.0 Tomcat7 > Configure Tomcat.
b. From the Java tab, add the following Java options:
   -Djavax.net.ssl.trustStore=<certstore-path>
   -Djavax.net.ssl.trustStorePassword=<certstore-password>
   -XX:MaxPermSize=256m

Note See Table 16-2 for descriptions of the above variables.

Example:
   -Djavax.net.ssl.trustStore=C:\keystore
   -Djavax.net.ssl.trustStorePassword=cisco!123
   -XX:MaxPermSize=256m

 c. Set the Initial memory pool to 512.
d. Set the Maximum memory pool to 1024.
e. Click Apply.
f. Click OK.

Step 13 Using a Text Editor, open the server.xml file under <tomcat-dir>\conf folder. See Step 9 to determine the value for <tomcat-dir>. An example value is "C:\Program Files\Apache Software Foundation\Tomcat 7.0\conf".

Step 14 Comment out the 8080 connector port. Enter the code as follows:

Example:
   <!-- <Connector port="8080" protocol="HTTP/1.1"
   connectionTimeout="20000"
   redirectPort="8443" /> -->

Step 15 Uncomment the 8443 connector port; Remove <!-- code at the beginning and --> at the end of the 8443 connector. You must add three more attributes to the connector configuration:

- keyStoreFile (location of the keystore file that was created in section Install Java, page 16-8. In this example, it was created under C:\keystore)
- keyStorePass
- keyStoreType

Enter the code as follows:

Example:
   <Connector port="8443" protocol="HTTP/1.1" SSLEnabled="true"
   maxThreads="150" scheme="https" secure="true"
   clientAuth="false" sslProtocol="TLS"
   keyStoreFile="<certstore-path>"
   keyStorePass="<certstore-password>"
   keyStoreType="JKS"/>
Step 16  Save the server.xml file.

Step 17  Start the Tomcat service:
   a. Choose Start > All Programs > Apache Tomcat 7.0 Tomcat7 > Configure Tomcat.
   b. From the General tab, click Start. If the Tomcat service was already running, click Stop, then Start.

Step 18  To test the configuration, launch a web browser on the Windows Server that contains the Tomcat instance and go to https://localhost:8443/tomcat.gif. The web browser may present warning dialogs about insecure connections because the web browser does not trust the security certificates that are presented by the Tomcat instance. Either examine the certificates and add them to your local certificate store so that the browser trusts them or proceed to the web application (less secure option) using the available browser controls. If the configuration is correct, the Tomcat logo appears in the web browser window.

Step 19  Configure Windows firewall to allow incoming connections to Apache Tomcat:
   c. Right-click Inbound Rules.
   d. Click New Rule.
   e. From the What type of rule would you like to create list of options, choose Port.
   f. Click Next.
   g. From the Does this rule apply to TCP or UDP? list of options, choose TCP.
   h. From the Does this rule apply to all local ports or specific local ports? list of options, choose Specific local ports.
   i. Enter 8443 and click Next.
   j. From the What action should be taken when a connection matches the specified conditions? list of options, choose Allow the connection.
   k. Click Next.
   l. From the When does the rule apply? list of options, choose Domain only.
   m. Click Next.
   n. Enter a name and description of your choosing and click Finish.

Step 20  To test the configuration, log in to another host on the network, launch a web browser on the Windows server that contains the Tomcat instance and go to https://<openam-fqdn>:8443/tomcat.gif, where <openam-fqdn> is the Fully Qualified Domain Name of the Windows Server that contains the Tomcat instance. The web browser may present warning dialogs about insecure connections because the web browser does not trust the security certificates that are presented by the Tomcat instance. Either examine the certificates and add them to your local certificate store so that the browser trusts them or proceed to the web application anyway (this is less secure) using the available browser controls. If the configuration is correct, the Tomcat logo appears loaded into the web browser window.
Deploy OpenAM War on Apache Tomcat

Procedure

Step 1
Download the recommended OpenAM release from the ForgeRock website, as indicated in Table 16-1Software Versions, page 16-3.

Step 2
Extract the .zip file and locate the opensso.war file that is contained within it.

Step 3
Copy the WAR file to the Windows server that is to be your OpenAM server. This Windows server should be running the previously configured Tomcat service.

Step 4
Stop the Apache Tomcat service if it is running:

  a. Choose Start > All Programs > Apache Tomcat 7.0 Tomcat7 > Configure Tomcat.
  b. From the General tab, click Stop.

Step 5
Deploy the WAR file on the Windows server that contains the Tomcat instance by copying the WAR file to the following location: <tomcat-dir>\webapps. See Install Tomcat, page 16-13 for a description of the <tomcat-dir> variable.

Example:
C:\Program Files\Apache Software Foundation\Tomcat 7.0\webapps

Step 6
Start the Apache Tomcat service:

  a. Choose Start > All Programs > Apache Tomcat 7.0 Tomcat7 > Configure Tomcat.
  b. From the General tab, click Start.

Note
The WAR file will fully deploy within a couple minutes. Under the webapps folder, a new folder is created with the same name as the WAR file but with the .war extension removed.

Step 7
Verify your configuration by launching a web browser and entering https://<openam-fqdn>:8443/<war-file-name>, where <openam-fqdn> is the FQDN of the Windows server that contains the OpenAM/Tomcat instance and <war-file-name> is the name of the OpenAM WAR file with the .war extension removed. If the configuration is correct, the OpenAM administration interface should load in the web browser window.

Set up OpenAM using the GUI Configurator

The following procedure specifies a method of configuring OpenAM. If you have an existing OpenAM server or a solid understanding of OpenAM, you can configure the server differently.

OpenAM server and J2EE Policy Agents require FQDNs for the hostname of the machines on which you will perform your installations. To avoid problems with installation, configuration, and usage, Cisco highly recommends that you avoid using hostnames like “localhost” or numeric IP addresses like “192.168.1.2”.

OpenAM provides a web-based administration interface that must be accessed using a web browser, for example Mozilla Firefox. When accessing OpenAM for the first time, you must use the FQDN of the OpenAM server in the URL, for example, https://server1.cisco.com:8443/opensso, where the sample URL value assumes that the OpenAM WAR file is deployed as “opensso”.

OpenAM configuration and logging information is typically stored in two directories that can be found in the home directory of the user running the OpenAM/Tomcat instance, for example:

- C:\opensso (where the folder name matches the deployed URI for the OpenAM WAR file. For example, opensso.)
- C:\.openssocfg

If a problem occurs during the configuration, the Configurator displays an error message. If possible, correct the error and retry the configuration. The following log file directories may provide useful information:

- Tomcat Web Container logs: tomcat-dir\logs
- OpenAM Install log: C:\opensso (where the folder name matches the deployed URI for the OpenAM WAR file. For example, opensso.)

By default, OpenAM is deployed under C:\opensso on Windows platforms.

**Procedure**

**Step 1**
Open the web browser and navigate to the OpenAM server using the following URL: https://<fqdn of openam server>:8443/<WAR filename>.

*Example:*
https://server1.cisco.com:8443/opensso

*Note*  
When you access OpenAM for the first time, you are directed to the Configurator to perform the initial configuration of the OpenAM. The Configuration Options window appears when you access the OpenAM for the first time.

**Step 2**
Choose **Create Default Configuration**.

*Note*  
If you encounter an error, repeating steps 1 and 2 on your local machine. Windows 2008, for example, may not trust this site, even if it is listed as a trusted sites.

**Step 3**
In the OpenSSO Configurator window, specify and confirm passwords for the OpenAM administrator (amAdmin) and the default policy agent user (UrlAccessAgent). The default policy agent user is not used later in this example configuration; amAdmin is used each time you log in to OpenAM to change the configuration.

**Step 4**
Click **Create Configuration**.

You are notified when the configuration is complete.

**Step 5**
Click **Proceed to Login**.

**Step 6**
Log in to your deployed OpenAM web application using the previously configured username and password for “amAdmin”.

**Step 7**
From the Access Control tab, click //(Top Level Realm).

**Step 8**
From the Authentication tab, click Core.

**Step 9**
Click All Core Settings.

**Step 10**
Set the User Profile to Ignored.

**Step 11**
Click Save to update the profile.
Step 12  Log out of the OpenAM GUI.

Set up Policies on OpenAM Server

Set up policies on the OpenAM server using the policy rules detailed in the following table.

<table>
<thead>
<tr>
<th>Service Type</th>
<th>Name</th>
<th>Resource Name</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>URL Policy Agent (with resource name)</td>
<td>&lt;hostname&gt;-01</td>
<td>https://&lt;CUP FQDN&gt;/*</td>
<td>Enable GET, Value = Allow</td>
</tr>
<tr>
<td></td>
<td>&lt;hostname&gt;-02</td>
<td>https://&lt;CUP FQDN&gt;/**?*</td>
<td>Enable POST, Value = Allow</td>
</tr>
<tr>
<td></td>
<td>&lt;hostname&gt;-03</td>
<td>https://&lt;CUP FQDN&gt;/**?*?</td>
<td>Allow</td>
</tr>
<tr>
<td></td>
<td>&lt;hostname&gt;-04</td>
<td>https://&lt;CUP FQDN&gt;:8443/#</td>
<td>Enable POST, Value = Allow</td>
</tr>
<tr>
<td></td>
<td>&lt;hostname&gt;-05</td>
<td>https://&lt;CUP FQDN&gt;:8443/#? *</td>
<td>Allow</td>
</tr>
<tr>
<td></td>
<td>&lt;hostname&gt;-06</td>
<td>https://&lt;CUP FQDN&gt;:8443/#?*?</td>
<td>Allow</td>
</tr>
</tbody>
</table>

When you apply the policy rules as defined in this procedure, the Cisco Unified Presence Administration/User interfaces can only be accessed with the web browser using the following URL formats:

- https://<CUP FQDN> - For example, https://CUP-Node-01.cisco.com

It is not possible to access the Cisco Unified Presence Administration/User interface using a URL that only specifies a hostname such as https://<CUP HOSTNAME> (for example, https://CUP-Node-01/).

Procedure

Step 1  Log in to the OpenAM Administration interface using the credentials you specified in section Set up OpenAM using the GUI Configurator, page 16-17.

Step 2  From the Access Control tab, click / (Top Level Realm).

Step 3  From the Policies tab, click New Policy.

Step 4  In the Name field, enter the PolicyName (for example, CUPPolicy) and click OK.

CUPPolicy is only a suggested value. You can use any valid name value. This value is not required later in this configuration.

Step 5  Choose the new policy, CUPPolicy, for editing.

Step 6  Click Rules.

Step 7  Add the rules in the following order:

a. Under the Rules section, click New.
b. Choose Service Type as URL Policy Agent (with resource name).

c. Click Next.

d. In the Name field, enter the suggested rule Name from Table 16-3Policy Rules, page 16-19, replacing <hostname> with the actual hostname of the Cisco Unified Presence node.

e. In the ResourceName field provided, enter the corresponding Resource Name for this rule, replacing <CUP FQDN> with the actual Fully Qualified Domain Name of the Cisco Unified Presence node.

f. Check the GET action with a value of Allow.

g. Check the POST action with a value of Allow.

h. Click Finish to complete the rule update.
i. Click Save to save the policy update.

j. Repeat this entire step for each rule in Table 16-3Policy Rules, page 16-19 then click Finish. You must add this set of six rules for each Cisco Unified Presence node that is enabled for SSO.

Step 8

You must add a single Subject to the policy. Add the Subject as follows:

a. Under the Subjects section, click New.

b. Choose Authenticated Users as Subject Type.

c. Click Next.

d. Enter CUPSubject as the Name value.

   CUPSubject is only a suggested value. You can use any valid value. This value is not required later in this configuration.

e. Click Finish to complete the Subject update.

f. Click Save to save the policy update.

Only a single Subject is required for this policy even if multiple Cisco Unified Presence nodes are enabled for SSO.

Step 9

You must add a single Condition to the policy. Add the Condition as follows:

a. Under the Conditions section, click New.

b. Choose Active Session Time as Condition Type.

c. Click Next.

d. Enter CUPTimeOutCondition as the Name value.

   CUPTimeOutCondition is only a suggested value. You can use any valid name value. This value required later in this configuration.

e. Enter 120 as the Maximum Session Time (minutes).

f. Ensure the Terminate Session field is set to No.

g. Click Finish to complete the Subject update.

h. Click Save to save the policy update.

Note that only a single Condition is required for this policy, even if multiple Cisco Unified Presence nodes are enabled for SSO.
Configure Single Sign-On Module Instance

This single module instance can be shared by multiple Cisco Unified Presence nodes that are configured for SSO as long as the same Active Directory domain is used throughout the deployment. Deployment scenarios involving more than one Active Directory domain are not covered in this documentation.

Procedure

**Step 1** Log in to the OpenAM administration interface using the credentials you specified in Set up OpenAM using the GUI Configurator, page 16-17.

**Step 2** From the Access Control tab, click Top Level Realm.

**Step 3** From the Authentication tab, click Module Instances.

**Step 4** In the Module Instances window, click New.

**Step 5** Enter a name for the new login module instance (for example, CUPKRB) and choose Windows Desktop SSO from the Type list.

**Step 6** Click OK.

---

**Note** This module instance name will be used later when enabling SSO on the Cisco Unified Presence server.

**Step 7** Click Save.

**Step 8** In the Module Instances window, choose the name of the new login module (for example, CUPKRB) and provide the following information:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Sample Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Principal</td>
<td>This value should exactly match the value specified in Provision Active Directory for Single Sign-On, page 16-4. For example, -princ value.</td>
<td>HTTP/server1.cisco.com@CISCO.COM (using openAM server name and domain)</td>
</tr>
<tr>
<td>Keytab File Name</td>
<td>This value should be the location of the keytab file that was created in Provision Active Directory for Single Sign-On, page 16-4 copied to the OpenAM server in Step 11.</td>
<td>C:\keytab\server1.HTTP.keytab (on Windows platform)</td>
</tr>
<tr>
<td>Kerberos Realm</td>
<td>Domain for OpenAM server</td>
<td>CISCO.COM</td>
</tr>
<tr>
<td>Kerberos Server Name (Active Directory)</td>
<td>Provide the FQDN of the AD server. The AD server is normally the Kerberos Domain Controller. If multiple Kerberos Domain Controllers exist for failover purposes, all Kerberos Domain Controllers can be set using a colon (:) as the separator.</td>
<td>ad.cisco.com</td>
</tr>
</tbody>
</table>
Chapter 16      Single Sign-On Configuration

Single Sign-On Configuration

Step 9  Click **Save**.

The module instance is created and called CUPKRB.

Step 10 Validate that the SSO Module is working correctly by logging in to a Windows Desktop session as a valid Windows user (a valid end user that exists in the AD; do not use the Administrator account). Access the following URL:

**Note**  The browser must be configured for SSO.

https://<openam-FQDN>:8443/<war-file-name>/UI/Login?module=<SSO_Module>

Where:
- `<openam-FQDN>` is the FQDN of the OpenAM server
- `<war-file-name>` is the name of the deployed OpenAM WAR file, for example “opensso”
- `<SSO_Module>` is the name of the WindowsDesktopSSO module.

A screen notifies you that login was successful.

Configure J2EE Agent Profile on OpenAM

The J2EE Agent is an internal component that is instantiated on each Cisco Unified Presence node with SSO enabled. You must configure an associated J2EE Agent Profile on the OpenAM server for each J2EE Agent. As such, a J2EE Agent Profile is required for every Cisco Unified Presence node with SSO enabled. If multiple nodes are to be configured for SSO, a J2EE Agent Profile must be created for each additional node.

Procedure

**Step 1**  Log in to the OpenAM Administration interface using the credentials you specified in section Set up OpenAM using the GUI Configurator, page 16-17.

**Step 2**  From the Access Control tab, click `/Top Level Realm`.

**Step 3**  From the Agents tab, choose the J2EE tab.

**Step 4**  In the Agents section, click **New**.

**Step 5**  Enter values for the following fields:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Sample Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Return Principal with Domain Name</td>
<td>Uncheck the <strong>Enabled</strong> check box.</td>
<td></td>
</tr>
<tr>
<td>Authentication Level</td>
<td></td>
<td>22</td>
</tr>
</tbody>
</table>
Step 6
Click **Create**.
A J2EE Agent with the name of `<hostname-j2ee-agent>` is created.

Step 7
Choose the J2EE agent that you created.

Step 8
From the **Application** tab, under the **Login Processing** section, add the Login Form URIs for each web GUI application on Cisco Unified Presence as follows:

<table>
<thead>
<tr>
<th>Application</th>
<th>Sample Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Unified Presence</td>
<td><code>/cupadmin/WEB-INF/pages/logon.jsp</code></td>
</tr>
<tr>
<td>Administration</td>
<td></td>
</tr>
<tr>
<td>Cisco Unified Serviceability</td>
<td><code>/ccmservice/WEB-INF/pages/logon.jsp</code></td>
</tr>
<tr>
<td>Cisco Unified Reporting</td>
<td><code>/cureports/WEB-INF/pages/logon.jsp</code></td>
</tr>
</tbody>
</table>
Step 9 Click **Save**.

Step 10 From the **OpenSSO Services** tab, under Login URL, add OpenSSO Login URL as `https://<OpenAM FQDN>:8443/<war-file-name>/UI/Login?module=<SSO_Module>`.

**Note** Replace the place holders OpenAM FQDN, war-file-name and SSO_Module with the correct values where SSO_Module should be the same value as the one you created in Configure Single Sign-On Module Instance, page 16-21. For example, `https://server1.cisco.com:8443/opensso/UI/Login?module=CUPKRB`.

Step 11 In the text area, remove all URLs other than the Login URL. Only the Login URL specified in the previous step should be listed in the text area.

Step 12 Click **Save**.

Step 13 Click **Back to Main Page**.

Step 14 Repeat Steps 4 through 13 to create a J2EE Profile Agent for every other Cisco Unified Presence node to be enabled for SSO.

---

### Set the OpenAM Session Timeout

The OpenAM session timeout must be set to a value that is higher than the session timeout parameter that is set on the Cisco Unified Presence server. To determine the session timeout value on the Cisco Unified Presence server, enter the following command using the CLI:

```
show webapp session timeout
```

**Procedure**

Step 1 Log in to the OpenAM Administration interface using the credentials you specified in section **Set up OpenAM using the GUI Configurator**, page 16-17.

Step 2 From the **Configuration** tab, choose **Global**.

Step 3 Click **Session**.
import the OpenAM Certificate into Cisco Unified Presence

Cisco Unified Presence nodes with SSO communicate with the OpenAM server over an encrypted channel. Establishing an encrypted communication channel requires each Cisco Unified Presence node with SSO to trust the security certificate presented by the OpenAM server. A Cisco Unified Presence node trusts a security certificate by importing the required security certificates into the tomcat-trust trust store.

The required procedure is dependent on the security configuration used when creating the Java keystore for the OpenAM Server in section Before You Begin, page 16-4:

• Use a self-signed security certificate for OpenAM/Tomcat instance
• Use a CA-signed security certificate for OpenAM/Tomcat instance

Caution

Importing OpenAM certificates affects service; Cisco highly recommends that you import the OpenAM certificates during a maintenance window.

Note

For information about importing certificates, see Cisco Unified System Maintenance Guide for Cisco Unified Presence.

Procedure

Step 1 Sign in to the Cisco Unified Presence Administration for a given Cisco Unified Presence publisher node that is to be enabled with SSO.
Step 2 Choose System > Security > Certificate Import Tool.
Step 3 Choose Tomcat Trust as the Certificate Trust Store.
Step 4 Enter the Fully Qualified Domain Name of the OpenAM server as the Peer Server.
Step 5 Enter 8443 as the Peer Server Port.
Step 6 Click Submit.

The Certificate Import Tool executes two tests:

• Verify reachability of the specified certificate server (pingable) - checks that the OpenAM server is reachable by this Cisco Unified Presence node. If this test fails, it may be due to the firewall on the OpenAM base Windows system blocking the ping operation. See the following link for further information about how to allow a ping through a Windows firewall: http://technet.microsoft.com/en-us/library/cc749323(WS.10).aspx
• Verify SSL connectivity to the specified certificate server - checks if this Cisco Unified Presence node can securely connect to the OpenAM server. If this test fails due to “Missing certificates”, the required certificates are missing and a secure connection cannot be established. If this test fails, proceed to the next step. If this test passes, proceed to Step 15.
**Single Sign-On Configuration**

Step 7  Click **Configure** to open the Certificate Viewer. The Certificate Viewer provides a visual representation of the certificate chain presented by OpenAM during a TLS connection handshake. This indicates which certificates must be imported into this Cisco Unified Presence node.

Step 8  Inspect the certificates in the chain and ensure that you trust the issuers.

Step 9  Check **Accept Certificate Chain** and click **Save**.  
The required certificates from the chain are now imported into the tomcat-trust trust store of this Cisco Unified Presence node.

Step 10  Click **Close**.

The Certificate Import Tool reports that the “Certificates verified successfully”.

Step 11  Restart the Cisco UP Intercluster Sync Agent service on this node using the following CLI command:  
```
utils service restart Cisco UP Intercluster Sync Agent.
```

Step 12  Restart the Tomcat service on this node using the following CLI command:  
```
utils service restart Cisco Tomcat.
```

Step 13  Repeat Steps 11 and 12 for each subscriber node in this cluster.

Step 14  Verify the secure connection by using the Certificate Import Tool on each subscriber node in this cluster.

   a.  Sign in to Cisco Unified Presence Administration for a given Cisco Unified Presence subscriber node that is being configured with SSO.

   b.  Choose **System > Security > Certificate Import Tool**.

   c.  Choose **Tomcat Trust** as the **Certificate Trust Store**.

   d.  Enter the FQDN of the OpenAM server as the **Peer Server**.

   e.  Enter **8443** as the **Peer Server Port**.

Step 15  Repeat this procedure for all Cisco Unified Presence clusters for which you will be enabling SSO.

**Activate Single Sign-On**

When enabling SSO, you must perform the following tasks in the order indicated.

-  Enable Single Sign-On, page 16-28

**Caution**

Enabling SSO affects service; Cisco highly recommends that you enable SSO during a maintenance window.
Configure Access Permissions Before Enabling Single Sign-On

It is important to understand the user access permissions that should be in place before and after SSO is enabled. Understanding the permissions can help avoid situations in which users have incorrect permissions when accessing the Cisco Unified Presence applications.

<table>
<thead>
<tr>
<th>Application</th>
<th>Notes</th>
</tr>
</thead>
</table>
| Cisco Unified Presence Administration (Cisco Unified Presence Administration, Cisco Unified Presence Serviceability, Cisco Unified Presence Reporting) | Before enabling SSO, ensure that an end user who is a member of the necessary User Groups exists in order to facilitate administration access. The default administrator application user that was created at the time of installation has the following: Groups:  
  - Standard Audit Users  
  - Standard Cisco Unified Presence Super Users  
  - Standard RealtimeAndTraceCollection  
Roles:  
  - Standard AXL API Access  
  - Standard Audit Log Administration  
  - Standard CCM Admin Users  
  - Standard CCMADMIN Administration  
  - Standard CUReporting  
  - Standard RealtimeAndTraceCollection*  
  - Standard SERVICEABILITY Administration  
Any end user that is a member of the above User Groups with those Roles will have full access rights to Cisco Unified Presence, similar to that of the default administrator. To view the default application user on Cisco Unified Presence, choose Cisco Unified Presence Administration > User Management > Application User > Find. Choose the default application user (that was created during installation) to view their details. To assign an end user to these groups on Cisco Unified Presence, choose Cisco Unified Presence Administration > User Management > User Groups > Find. Choose a group and click Add End Users. Search for the desired end user, choose the user, and click Add Selected. |
| Cisco Unified Presence User Options | Ensure that the end users are members of the Standard CCM End User group on the corresponding Cisco Unified Communications Manager node. |
Enable Single Sign-On

This application is split into three components:

- Status
- Server Settings
- Select Applications

Status
A warning message displays indicating that the change in SSO settings causes Tomcat to restart.

The following error messages may display when you enable the SSO application:

- Invalid Open Access Manager (OpenAM) server URL - This error message displays when you enter an invalid OpenAM server URL.
- Invalid profile credentials - This error message displays when you enter a wrong profile name or wrong profile password or both.
- Security trust error - This error message displays when this Cisco Unified Presence node does not trust the certificate chain presented by the OpenAM server.

Note
If you see any of the above error messages while enabling SSO, then the status changes to that error.

Server Settings
You can edit the server settings only when SSO is disabled for all applications.

Select Applications
You can enable or disable SSO on any of the following applications:

- Cisco Unified Presence Administration - Enables SSO for Cisco Unified Presence Administration, Cisco Unified Serviceability, and Cisco Unified Reporting
- Cisco Unified Presence User Options - Enables SSO for End User Options
- Cisco Unified Operating System Administration - Enables SSO for Cisco Unified Operating System Administration and Disaster Recovery System

### Application | Notes
---|---
Cisco Unified Presence Operating System Administration (Cisco Unified Presence Operating System Administration, Cisco Unified Presence Disaster Recovery System) | Normally, the default administrator application user does not have access to these web applications. These web applications are only accessible by the Cisco Unified Presence Operating System administrator. This administrator has access to the Administration CLI in addition to these web applications. After SSO is enabled for these applications, the applications are accessible by any end user that has the same permissions as the default administrator application user.
Real-Time Monitoring Tool | Before enabling SSO, ensure that an end user exists that is a member of the necessary user groups to allow administrative access to the Real-Time Monitoring Tool. Refer to the note for Cisco Unified Presence Administration above.
Configuration and Administration of Cisco Unified Presence Release 8.6

Chapter 16      Single Sign-On Configuration

Disable Single Sign-On

If you choose to disable SSO, you must perform the following tasks in the order indicated.

- Disable Single Sign-On, page 16-30

Configure Access Permissions Before Disabling Single Sign-On

If SSO is disabled for any Cisco Unified Presence web application that supports SSO, all users accessing that application need to provide a username and password. Cisco recommends that if you are a Cisco Unified Presence administrator intending to disable SSO for any Cisco Unified Presence web applications, ensure that users can access the application after SSO is disabled. This action is important to avoid inadvertently locking out the active Cisco Unified Presence administration account.
### Disable Single Sign-On

You can disable SSO using either the GUI, as described in this procedure, or the CLI. For information

<table>
<thead>
<tr>
<th>Application</th>
<th>Notes</th>
</tr>
</thead>
</table>
| Cisco Unified Presence Administration (Cisco Unified Presence Administration, Cisco Unified Presence Serviceability, Cisco Unified Presence Reporting) | Before disabling SSO, ensure that an application users exists with a known username/password and that this user is a member of the necessary User Groups. The default administrator application user that was created at the time of installation has the following: Groups:  
  - Standard Audit Users  
  - Standard Cisco Unified Presence Super Users  
  - Standard RealtimeAndTraceCollection  
Roles:  
  - Standard AXL API Access  
  - Standard Audit Log Administration  
  - Standard CCM Admin Users  
  - Standard CCMADMIN Administration  
  - Standard CUReporting  
  - Standard RealtimeAndTraceCollection*  
  - Standard SERVICEABILITY Administration  
Any application user that is a member of the above User Groups with those Roles will have full access rights to Cisco Unified Presence if SSO is disabled. To view the application users on Cisco Unified Presence, choose **Cisco Unified Presence Administration > User Management > Application User > Find.** Choose a user to view their details.  

<table>
<thead>
<tr>
<th>Cisco Unified Presence User Options</th>
<th>Ensure that passwords exist for the end users and that they are aware of their password values. This information is required by each end user to access the application.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Unified Presence Operating System Administration (Cisco Unified Presence Operating System Administration, Cisco Unified Presence DRS)</td>
<td>Before disabling SSO, ensure that an OS Administration user exists with a known username/password and that this user has access to Cisco Unified Presence Operating System Administration CLI. After SSO is disabled, this user has access rights to the Cisco Unified Presence Operating System Administration GUIs.</td>
</tr>
<tr>
<td>Real-Time Monitoring Tool</td>
<td>Before disabling SSO, ensure that an application user with a known username/password exists and that this user has the same access rights as the user specified for Cisco Unified Presence Administration (Cisco Unified Presence Administration, Cisco Unified Presence Serviceability, and Cisco Unified Presence Reporting).</td>
</tr>
</tbody>
</table>
about how to disable SSO using the CLI, see the `utils sso disable` command in the *Command Line Interface Guide for Cisco Unified Presence Release 8.0, 8.5, and 8.6.*

**Procedure**

**Step 1** Navigate to the Cisco Unified Presence Operating System Administration page and choose **Security > Single Sign On.**

**Step 2** Uncheck all applications that were previously enabled for SSO.

**Step 3** Click **Save.**

**Step 4** In the **Confirmation** dialog box, click **OK** to restart Tomcat.

---

**Uninstall OpenAM**

**Prerequisites**

Ensure that you have completed the following tasks before you uninstall OpenAM:

- Disable Single Sign-On, page 16-29

**Procedure**

**Step 1** Access the OpenAM server Windows desktop and choose **Start > All Programs > Apache Tomcat 7.0 Tomcat 7 > Configure Tomcat.**

---

**Note**

This menu path assumes you are using Tomcat 7.

**Step 2** From the **General** tab, click Stop to stop the Tomcat service if it is running on the OpenAM server.

**Step 3** Delete the OpenAM configuration data. This data is typically stored in two directories that can be found in the home directory of the user running the Tomcat instance. For example, C:\opensso (where the folder name matches the deployed URI for the OpenAM WAR file such as opensso) and C:\openssocfg.

**Step 4** Delete the deployed OpenAM WAR file and the WAR file itself from the following location on the OpenAM/Tomcat instance: `tomcat-dir\webapps`. See Install Tomcat, page 16-13 for a description of the `tomcat-dir` variable.

**Example:**

C:\Program Files\Apache Software Foundation\Tomcat 7\webapps

**Step 5** Access the Windows desktop of the OpenAM server and choose **Start > All Programs > Apache Tomcat 7.0 Tomcat 7 > Configure Tomcat.**

**Step 6** From the **General** tab, click **Start** to start the Tomcat service.
Set the Debug Level

You can gather additional debug information the Cisco Unified Presence node by setting the log level for the J2EE Policy Agent accordingly. The log level for this component is configured on the OpenAM server itself. The default log level is Error. You can change the log level to Message to provide additional debug information. Cisco recommends that you use the Message log level only for short periods of time, because the associated log files can grow quite large.

Procedure

Step 1  Sign in to OpenAM (https://<OpenAM FQDN>:8443/opensso) from your web browser (for example, Mozilla Firefox).

Step 2  From the Access Control menu, choose Top Level Realm > Agents > J2EE.

Step 3  Under the General heading, choose Agent Debug Level.
PART 4

Administration

- Multi-node Deployment Administration
- Chat Setup and Management
- User Migration between Cisco Unified Presence Clusters
- Multilingual Support Configuration
Multi-node Deployment Administration

June 16, 2014

- Multi-node Deployment Models, page 17-1
- Cluster Topology Management, page 17-5
- High Availability Deployments, page 17-12
- High Availability Configuration, page 17-16
- Cluster-wide Routing Information on Cisco Unified Presence, page 17-24
- Static Route Configuration, page 17-24
- Presence Gateway Configuration on Cisco Unified Presence, page 17-29

Multi-node Deployment Models

You need to consider how you are going to deploy the multi-node feature in your network. You configure your desired multi-node deployment model in system topology management GUI in Cisco Unified Presence Administration. Choose **System > Cluster Topology** in Cisco Unified Presence Administration to access system topology management GUI.

This module provides an overview of the deployment model options for the multi-node feature, and provides examples of these deployments on system topology management GUI.

You only use system topology management GUI to configure your **local** Cisco Unified Presence cluster. See the intercluster peer module for information about configuring intercluster peer relationships with remote Cisco Unified Presence clusters.

**Note**
The High Availability deployment models described in this module are only applicable to Cisco Unified Presence Release 8.5.x or later releases.

Balanced User Assignment Redundant High Availability Deployment

You can achieve a balanced mode High Availability deployment by evenly balancing users across all nodes in the subcluster, but only using up to 35% of the CPU of each Cisco Unified Presence server.
The balanced mode High Availability deployment option in a redundant mode supports up to fifteen thousand users per cluster. For example, if you have six Cisco Unified Presence nodes in your deployment, and fifteen thousand users, you assign 2.5 thousand users to each Cisco Unified Presence node.

When you use the balanced mode High Availability deployment option in a redundant mode, as compared to a non-redundant mode, only half the number of users are assigned to each node. However, if one node fails, the other node will handle the full load of the additional 50% of users in the subcluster, even at peak traffic. In order to support this failover protection, you must turn on High Availability in each of the subclusters in your deployment.

See Figure 17-1 for an example of this deployment model on system topology management GUI. In this example, there are 15,000 users in total, so 2500 users are evenly balanced across the six nodes.

Related Topics
- Configure Routing Communication, page 7-12
- Create Subclusters in System Topology, page 17-9
- High Availability Deployments, page 17-12
- For the hardware user assignment guidelines for the multi-node feature, see the Cisco Unified Presence compatibility matrices at this URL:

Active/Standby User Assignment Redundant High Availability Deployment

For this deployment model, assign all your users to the primary Cisco Unified Presence node, and none to the backup node. When you turn on High Availability in the subcluster, the backup node can handle all traffic from the primary node if the primary node fails.
See Figure 17-2 for an example configuration for this deployment model on system topology management GUI. In this example, there are 15,000 users in total, so 5000 users are assigned to the first node of each subcluster.

**Figure 17-2 Active/Standby User Assignment High Availability Deployment**

### Related Topics
- [Configure Routing Communication](#), page 7-12
- [User Redistribution](#), page 1-8
- [Create Subclusters in System Topology](#), page 17-9
- [Cluster Topology Management](#), page 17-5
- [High Availability Deployments](#), page 17-12
- For the hardware user assignment guidelines for the multi-node feature, see the Cisco Unified Presence compatibility matrices at this URL:
  

### High Availability for Cisco Unified Personal Communicator 7.x and 8.x Clients

Cisco Unified Presence provides server-side failback, which uses the same throttle mechanism as server failover. This feature detects when a failed Cisco Unified Presence server in a High Availability deployment comes back in service. It then sends terminating notify messages to Cisco Unified Personal Communicator clients that are failed over to initiate failback to their home node. Also, if a user is moved between nodes in the subcluster, the Cisco Unified Presence server sends terminating notify messages, and the client will sign out and sign in to the new node. To balance the load between two nodes in the subcluster, you can assign the users equally in each node.
Cisco Unified Personal Communicator Sign-in and Redirect

Cisco Unified Presence supports the ability to redirect a Cisco Unified Personal Communicator client application to the Cisco Unified Presence node to which the user is assigned (home node). The redirect feature is supported in intracluster and intercluster deployments. In both types of deployments, redirect occurs automatically when the client application signs in. After the user successfully signs in to the home node, Cisco Unified Personal Communicator caches the server name. As a result, redirect happens only once, unless a user is reassigned.

Using Figure 17-3 as a reference, see the following examples to gain a better understanding of the various redirect scenarios. In Figure 17-3, Cluster1 is assumed to be a Cisco Unified Presence Release 8.6 cluster and Cluster2 is a 7.x or 8.x cluster.

Figure 17-3 Intercluster and Intracluster Redirect Diagram

In the preceding figure, Cluster1 has three nodes, a publisher (C1Node1) and two subscribers (C1Node2 and C1Node3) and has an intercluster peer relationship with Cluster2, which contains a publisher (C2Node1) and subscriber (C2Node2). Several different redirect scenarios are possible:

1. A Cisco Unified Personal Communicator user is assigned C1Node1 as a home node and attempts to sign in to C1Node2. C1Node2 automatically redirects the Cisco Unified Personal Communicator client to C1Node1. In this scenario, High Availability is disabled in Subcluster1. If High Availability is enabled in Subcluster1, C1Node2 will process the login request. There is no redirect.
2. A Cisco Unified Personal Communicator user is assigned C1Node3 as a home node and attempts to sign in to C1Node1 or C1Node2. Regardless of whether High Availability is enabled in Subcluster1, C1Node1 or C1Node2 redirects the Cisco Unified Personal Communicator client to C1Node3. High Availability rules do not apply here because C1Node3 is part of Subcluster2.

3. A Cisco Unified Personal Communicator user is assigned C2Node1 or C2Node2 as a home node and attempts to sign in to C1Node1, C1Node2, or C1Node3. C1Node1, C1Node2, or C1Node3 automatically redirects the Cisco Unified Personal Communicator client its home node.

**Note**
For more information about establishing intercluster peer relationships and syncing users, see *Intercluster Peer Configuration, page 12-1.*

---

**Cluster Topology Management**

This module is only applicable if you are deploying the multi-node feature. When you configure the multi-node feature, note the following:

- Perform the system topology configuration on the Cisco Unified Presence *publisher* node.
- Before configuring the system topology, read the multi-node planning and deployment information for best practice information about configuring this type of deployment.

**Caution**
Only use the system topology interface to configure your *local* Cisco Unified Presence cluster. See the intercluster peer module for information about configuring intercluster peer relationships with remote Cisco Unified Presence clusters.

- **Subcluster, Node and User Management Recommendations, page 17-5**
- **Add a New Node, page 17-7**
- **Create, Assign and Move Nodes in System Topology, page 17-10**
- **High Availability Deployments, page 17-12**

**Subcluster, Node and User Management Recommendations**

- **Node Creation and Movement Recommendations, page 17-5**
- **Node Name Recommendations, page 17-6**
- **Add a New Node, page 17-7**
- **Manual User Assignment Recommendations, page 1-7**
- **User Redistribution, page 1-8**

**Node Creation and Movement Recommendations**

When you create nodes in system topology management GUI you can:

- Assign the nodes to a subcluster in Cisco Unified Presence, or allow the nodes to remain unassigned. These states are interchangeable.
Cluster Topology Management

Chapter 17  Multi-node Deployment Administration

- Assign Cisco Unified Presence users to the nodes, or allow the nodes to remain without any user assignments.
- Turn on or off High Availability on a subcluster. See the section about configuring High Availability deployments later in this chapter.
- Move a node from one subcluster to another if the node is assigned, has no users and high-availability is turned off in the subcluster.
- Move a node from one subcluster to another if the node is assigned and has no users.
- Configure real pingable nodes, or logical nodes which can be installed later and which remain inaccessible until that time.

To move nodes with users assigned, perform one of the following actions:
- Unassign the users, move the node, and then reassign the users to the node. Note that when you unassign the users, they will lose service.
- Create a logical node and move the users to the logical node. Move the node, reassign the users to the node, and remove the logical node.

**Note**
- Remove all users from a node before you unassign or move it.
- Turn off High Availability in the subcluster before you unassign or move a node in that subcluster.
- We strongly recommend that you perform any node movements that involve unassigning or moving a large numbers of users at off peak times. Such large operations can adversely impact performance.

**Related Topics**
- Node Name Recommendations, page 17-6
- Add a New Node, page 17-7
- Create, Assign and Move Nodes in System Topology, page 17-10

### Node Name Recommendations

**Cisco Unified Presence Release 8.6(4) and Earlier**

By default, the name for a node is the hostname that you configure during the Cisco Unified Presence installation. For example, if the hostname of your Cisco Unified Presence node is called “cup1”, the node name is “cup1”. You can change the node name to the dotted IP address or the FQDN, for example, “192.168.0.1” or "cup1.acme.com". If you change the default name for the node, note the following:

- You must be able to resolve the hostname or the FQDN from the Cisco Unified Presence server, and Cisco Unified Personal Communicator client computers.
- If either Cisco Unified Presence server or the Cisco Unified Personal Communicator client computer cannot resolve the hostname or the FQDN, configure the IP address for the node name value.
- To test the name resolution from the Cisco Unified Presence server, use the command

  ```bash
  utils network ping <node_name>
  ```

- To test the name resolution from the Cisco Unified Personal Communicator client computer, use the command

  ```bash
  ping <node_name>
  ```
If your network uses DNS that can map to IPv4 addresses, you can enter the Cisco Unified Presence hostname. Otherwise, you must enter the full IPv4 address of the Cisco Unified Presence server.

**Cisco Unified Presence Release 8.6(5) and Later**

If you are using DNS in your deployment, then the name of the publisher node is set to its FQDN by default. This is the Cisco recommended node name value for all subscriber nodes as it ensures that the node is fully resolvable from all clients and servers. The FQDN of a node is a concatenation of the hostname and domain that you configure during the Cisco Unified Presence installation. For example, if the hostname of your Cisco Unified Presence node is called “node1” and the DNS domain is “acme.com”, the node name is “node1.acme.com”. You can change the node name to the dotted IP address or just simply the hostname, for example, “192.168.0.1” or “node1.com”. If you are using the hostname or FQDN as the node name, note the following:

- You must be able to resolve the hostname or the FQDN from all Cisco Unified Presence servers, across all clusters.
- You must be able to resolve the hostname or the FQDN from all Cisco Jabber client computers.
- If either the Cisco Unified Presence server or the Cisco Jabber client computer cannot resolve the hostname or the FQDN, consider the following options:
  - Configure the IP address for the node name value.
  - Make the required DNS configuration to ensure that the hostname or FQDN is resolvable from all client machines and all Cisco Unified Presence servers.
- To test resolution of the node name use the following commands:
  - From the Cisco Unified Presence server, use the command `utils network ping <node_name>`
  - From the Cisco Jabber client computer, use the command `ping <node_name>`

**Note**

- Cisco Unified Personal Communicator 7 does not support FQDN based node names. If you are planning to deploy this client, you must change the node name to either the IP address or the hostname.
- When using the Cisco Jabber client, certificate warning messages can be encountered if the IP address is configured as the IM and Presence Service node name. To prevent Cisco Jabber from generating certificate warning messages, the FQDN should be used as the node name.

**Related Topics**

- Node Creation and Movement Recommendations, page 17-5
- Create, Assign and Move Nodes in System Topology, page 17-10
- Changing the IP Address, Hostname and Domain Name for Cisco Unified Presence on cisco.com

**Add a New Node**

Follow this procedure if you need to add new nodes after a multi-node deployment is running.

You must create the new node in your topology before you install the node, specifically before you install the Cisco Unified Presence software on the new node. However, you cannot assign the new node to a subcluster before you install Cisco Unified Presence software on the new node.
Note
You no longer have to manually add Cisco Unified Presence as an Application Server on Cisco Unified Communications Manager. When you add or remove a node on the system topology management GUI, the node is automatically added to or removed from the Application Server list on Cisco Unified Communications Manager.

Before You Begin
Check the following:

- From System troubleshooter page, verify that the Cisco UP Replication Watcher service is running on all nodes.
- On the Network services screen in Cisco Unified Serviceability (on the subscriber node), verify that all Cisco Unified Presence services are running.
- High Availability is turned off in a subcluster before you move or unassign a node in that subcluster.

Restrictions
Your hardware must comply with the multi-node hardware recommendations.

Procedure

- Step 1 Create a new subcluster in system topology management GUI (if required).
- Step 2 Create a new node in system topology management GUI.
- Step 3 Install the Cisco Unified Presence software on the new node.
  See the Installation Guide for Cisco Unified Presence for the installation procedure.
- Step 4 Assign the node to the subcluster (if required).
  Cisco Unified Presence assigns the node to the cluster, but the node will not receive traffic until you assign users to it.
- Step 5 Turn on High Availability in the subclusters as required.
- Step 6 Assign users from other nodes to the new node as required.

Related Topics
- Clustering over WAN for Intracluster and Intercluster Deployments, page 2-4
- Create Subclusters in System Topology, page 17-9
- Create, Assign and Move Nodes in System Topology, page 17-10
- Configure User Assignment in System Topology, page 15-1
- High Availability Deployments, page 17-12

Expand the Cluster

Before You Begin
Check the following:
• From System troubleshooter page, verify that the Cisco UP Replication Watcher service is running on all nodes.

• On the Network services screen in Cisco Unified Serviceability (on the subscriber node), verify that all Cisco Unified Presence services are running.

• High Availability is turned off in a subcluster before you move or unassign a node in that subcluster.

Restrictions

• Your hardware must comply with the multi-node hardware recommendations.

• We strongly recommend that you perform any node movements that involve you unassigning or moving a large numbers of users at off peak times. Such large operations can adversely impact performance.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Create the new subcluster(s) in system topology management GUI (if required).</td>
</tr>
<tr>
<td>Step 2</td>
<td>Create the new nodes in system topology management GUI.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Install each new node.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Assign the nodes to the (new) subclusters.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Turn on High Availability in the subclusters as required.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Once all the nodes are online, assign users to the new nodes using the following user assignment options:</td>
</tr>
</tbody>
</table>

• Using the Find User Assignment feature, unassign chosen users from each node, and use the User Assignment Mode parameter to reassign new users to new subcluster(s) and nodes.

• Using the Find User Assignment feature, manually move users to new nodes.

• Unassign all users, and then reassign the users to the cluster using the appropriate User Assignment Mode parameter setting for the whole cluster.

Related Topics

• Clustering over WAN for Intracluster and Intercluster Deployments, page 2-4
• Create Subclusters in System Topology, page 17-9
• Create, Assign and Move Nodes in System Topology, page 17-10
• Configure User Assignment in System Topology, page 15-1
• High Availability Configuration, page 17-16

Create Subclusters in System Topology

The system automatically assigns the first Cisco Unified Presence node that you install as the publisher node. After you install the publisher node, create the required subclusters and subsequent nodes in your Cisco Unified Presence cluster in system topology management GUI. After a subcluster has been created, you can update or view the status of the subcluster by clicking Edit.

Repeat this procedure for each subcluster that you require for your deployment.
Note Perform this procedure on the publisher Cisco Unified Presence node.

Before You Begin
Plan your multi-node deployment model.

Procedure

Step 1 Choose Cisco Unified Presence Administration > System > Cluster Topology.
Step 2 Click Add New Subcluster.
Step 3 Define a unique name for the subcluster.
Step 4 Click Save.

Related Topics
- Cisco Unified Presence Planning Requirements, page 3-1
- High Availability Deployments, page 17-12

Create, Assign and Move Nodes in System Topology

Create the required subsequent nodes for your deployment. By creating the subsequent nodes in the topology view of the publisher node, Cisco Unified Presence associates the subsequent nodes with the publisher node.

Note
- Perform this procedure on the publisher Cisco Unified Presence node.
- Perform this procedure before you install any of the subsequent Cisco Unified Presence nodes. If you assign a subsequent Cisco Unified Presence node to a subcluster prior to installing it, users in remote clusters will not receive availability information. An availability outage will occur until the node is installed.

Before You Begin
- Create the required subclusters for your deployment.
- Depending on how you plan to configure your node name, obtain the required value for your nodes (for example hostname, dotted IP address, FQDN or DNS-SRV).

Restrictions
- If you wish to change the default node name, there are certain node name restrictions. Read the node name recommendations topic.
- You can only move a node from one subcluster to another if the node is assigned and has no users.
- You must turn off High Availability in a subcluster before you move or unassign a node in that subcluster.
Procedure

**Step 1** Choose Cisco Unified Presence Administration > System > Cluster Topology.

**Step 2** Create the required subsequent nodes for your deployment:

a. Click **Add New Node**.

b. Define a unique name for the node.

c. Click **Save**.

**Step 3** Perform one of these actions:

<table>
<thead>
<tr>
<th>If you want to:</th>
<th>Action</th>
<th>Notes</th>
</tr>
</thead>
</table>
| Assign a node to a subcluster      | Drag the node into the empty slot in the subcluster | • Do not assign the subsequent node to a subcluster until after you install it, and you have checked the status of the node.
|                                    |                                                | • Before you assign a node to a subcluster, check the following                        |
|                                    |                                                |   – From System troubleshooter page, verify that the Cisco UP Replication Watcher service is running on all nodes. |
|                                    |                                                |   – On the Network services screen in Cisco Unified Serviceability (on the subscriber node), verify that all Cisco Unified Presence services are running on the assigned node. |
| To move a previously assigned node.| Drag the node from the subcluster and drop it into the empty slot of the peer subcluster. | • Turn off high-availability in the subcluster before you move the node. |
|                                    |                                                | • Unassign all users from the node before you move it.                                  |
| To update or view the status of a node. | Click the **edit** link on the node to view the **Node Detail** screen. | • View the total users assigned to the node.  
• Verify the status of the node.  
• If you turn on High Availability in the subcluster, the critical services that Cisco Unified Presence monitors on the node for failover are marked in the ‘Monitored’ column.  
• If you turn on High Availability, you can also view the High Availability state of the node, and the reason for this state. |

**Related Topics**

- DNS Domain Configuration, page 7-3
- Add a New Node, page 17-7
- Node Name Recommendations, page 17-6
High Availability Deployments

Requirements for High Availability

The requirements for High Availability are:

- You must be running CiscoUnified Presence release 8.5 (x), or a later 8.x release. Any earlier Cisco Unified Presence 8.0(x) releases do not support High Availability.
- Cisco Unified Presence supports High Availability at a subcluster level. Both nodes in the subcluster must be running the same version of Cisco Unified Presence 8.x software for High Availability to work.

High Availability in a Subcluster

Cisco Unified Presence supports High Availability in a subcluster meaning if a node in the subcluster fails, the Instant Message and Availability services from that node can failover to the second node in the subcluster.

You must manually turn on High Availability in a subcluster on the Cluster Topology interface on Cisco Unified Presence Administration interface. On the main Cluster Topology interface, the subcluster icon indicates that you have turned on High Availability on the subcluster.

A green tick beside the High Availability icon indicates that High Availability in the subcluster is running normally. A red ‘x’ beside the High Availability icon indicates that the subcluster is in a failed state.

Cisco Unified Presence automatically detects failover in a subcluster by monitoring the heartbeat and monitoring the critical services on the peer node. When Cisco Unified Presence detects failover, it automatically moves all users to the backup node. From the Cisco Unified Presence Administration interface, you can initiate a manual fallback to the primary node. Cisco Unified Presence Release 8.6(4) and later supports automatic fallback to the primary node after failover.

Caution

Cisco Unified Presence Release 8.6(3) and earlier does not perform an automatic fallback to the primary node after failover. You must manually perform the fallback from the Cluster Topology interface, otherwise the users that were moved will remain on the backup node.

Note

Cisco Unified Presence performs an automatic fallback when the backup activated node fails due to a critical service failure and the peer node is in the “Failed Over” state and supports the automatic recovery fallback.
To monitor and troubleshoot the status of the High Availability functionality on a subcluster, view the High Availability states that Cisco Unified Presence assigns to each node. See Node State Definitions, page 17-21 and Node States, Causes and Recommended Actions, page 21-1 for descriptions of these states and recommended actions if the subcluster is in a failed state. If a failover occurs, on the node detail screen, Cisco Unified Presence marks the users that have failed over to the backup node.

Related Topics
- Automatic Failover Detection, page 17-13
- Automatic Fallback, page 17-15
- Manual Failover and Fallback, page 17-16
- High Availability Configuration, page 17-16

Impact of Failover to Cisco Unified Presence Clients and Services

Cisco Unified Presence supports High Availability for Cisco Unified Personal Communicator Release 7.x and Cisco Unified Personal Communicator Release 8.5(x) and later.

During failover to the backup node, availability and instant messaging services are temporarily unavailable on client applications. After failover is complete, the availability and instant messaging services become available on the client again when the client signs back in. Similarly, if fallback occurs, availability and instant messaging services are temporarily unavailable on client applications until fallback completes and the client signs back in. Cisco Unified Personal Communicator signs users back in automatically.

The impact of failover on temporary adhoc chat messages depends on the particular client application. On Cisco Unified Personal Communicator, any adhoc chat windows that were open before failover should display again after the failover is complete. However, if all of the users in a chat room automatically exit the chat room as part of a failover or fallback process, or if the adhoc chat room is hosted on a failed node, the adhoc chat windows will not display again after failover and a message is displayed explaining that the chat room was deleted. On all clients, any persistent chat rooms that users create on the failed node cannot be accessed again until recovery.

If Cisco Unified Personal Communicator is operating in softphone mode (the user is on a voice call) during failover, the voice call is not disconnected.

Automatic Failover Detection

Cisco Unified Presence uses these methods to automatically detect if a node fails:
- **Peer Heartbeat** - In a subcluster, each node sends heartbeat intervals to the other node to check if the node is up and running. If a node detects a loss of heartbeat in the peer node, the node initiates a failover. You can configure the heartbeat interval and the heartbeat timeout from the Service Parameters page on Cisco Unified Presence Administration interface.
- **Monitor Critical Services** - Each node monitors a list of critical services. If the node detects that any critical service is not running for a configurable outage period (ninety seconds is the default value), it instructs the peer node to initiate a failover. You can configure this critical service delay from the Service Parameters page on Cisco Unified Presence Administration interface. These are the list of critical services that the node monitors:
  - Cisco DB (internal IDB database)
  - Cisco UP Presence Engine (if you activate this service)
- Cisco UP XCP Router
- Cisco UP Message Archiver (if you integrate Cisco Unified Presence with a third-party off-board database, and you activate this service)
- Cisco UP SIP Proxy (if you configure SIP federation, enable Partitioned Intradomain Federation, or you have an intercluster connection with a Cisco Unified Presence Release 7.x cluster, and you activate this service)
- Cisco UP XCP SIP Federation Connection Manager (if you configure SIP federation, enable Partitioned Intradomain Federation, or you have an intercluster connection with a Cisco Unified Presence Release 7.x cluster, and you activate this service)
- Cisco UP Presence Datastore—Cisco Unified Presence Release 8.6(4) or later only
- Cisco UP Route Datastore (if you configure SIP federation, enable Partitioned Intradomain Federation, or you have an intercluster connection with a Cisco Unified Presence Release 7.x cluster, and you activate this service)—Cisco Unified Presence Release 8.6(4) or later only

You can view the critical services that Cisco Unified Presence monitors for failover on the node details screen on the Cluster Topology interface. The critical services that Cisco Unified Presence monitors are marked in the ‘Monitored’ column in the services list.

**Note**

- Cisco Unified Presence only detects a failover if a critical service is not running for the duration of the outage period. It does not detect a failover in the case where one or more critical services are not running during the outage period, but not for the duration of the outage period, for example, a rolling outage. In this case, Cisco Unified Presence generates alarms indicating that services are starting and stopping, and you can perform a manual failover on Cisco Unified Presence.
- If you manually stop a critical service, and the service is stopped for longer than the permitted outage period, failover will occur.

Prior to Cisco Unified Presence Release 8.6, if Cisco Unified Presence detects the situation where both nodes in the subcluster think they own the same user, both nodes go into a failed state, and you need to perform a manual recovery from the Cluster Topology interface. In Cisco Unified Presence Release 8.6, manual recovery is not required. When the network issue is resolved, auto-recovery occurs without administrator intervention.

If manual recovery is required for another reason, you may experience IDS replication delays. To check the status of the IDS replication on a node either:

- Use this CLI command:

  `utils dbreplication runtimestate`

- Use the Cisco Unified Reporting Tool (CURT). The ‘Unified CUP Database Status’ report displays a detailed status of the cluster.

**Related Topics**

- Perform a Manual Failover to Backup Node, page 17-21
- Configure the Advanced Service Parameters for the Server Recovery Manager, page 17-18
- Cisco UP Replication Watcher Service, page 22-3
Automatic Fallback

Cisco Unified Presence Release 8.6(4) and later supports automatic fallback to the primary node after a failover. Automatic fallback is the process of moving users back to the primary node after a failover without manual intervention. You can enable automatic fallback with the Enable Automatic Fallback service parameter on the Cisco Unified Presence Administration interface.

Automatic fallback occurs in the following scenarios:

- A critical service on Node A fails—A critical service (for example, the Presence Engine) fails on Node A. Automatic failover occurs and all users are moved to Node B. Node A is in a state called "Failed Over with Critical Services Not Running". When the critical service recovers, the node state changes to "Failed Over." When this occurs Node B tracks the health of Node A for 30 minutes. If no heartbeat is missed in this time frame and the state of each node remains unchanged, automatic fallback occurs.
- Node A is rebooted—Automatic failover occurs and all users are moved to Node B. When Node A returns to a healthy state and remains in that state for 30 minutes automatic fallback occurs.
- Node A loses communications with Node B—Automatic failover occurs and all users are moved to Node B. When communications are re-established and remain unchanged for 30 minutes automatic fallback occurs.

If failover occurs for a reason other than one of the three scenarios listed here, you must recover the node manually. If you do not want to wait 30 minutes before the automatic fallback, you can perform a manual fallback to the primary node.

Related Topics

- High Availability Deployments, page 17-12
- Configure the Advanced Service Parameters for the Server Recovery Manager, page 17-18
- Perform a Manual Fallback to Primary Node, page 17-22

Cisco UP Server Recovery Manager (SRM)

The Cisco UP Server Recovery Manager (SRM) on Cisco Unified Presence manages the failover between nodes in a subcluster. The Cisco UP Server Recovery Manager manages all state changes in a node; state changes are either automatic or initiated by the administrator (manual).

After you turn on High Availability in a subcluster, the Cisco UP Server Recovery Manager on each node establishes heartbeat connections with the peer node, and begins to monitor the critical processes.

The SRM is responsible for the user move operations after it detects that failover has occurred. It is the SRM on the peer node, not on the failed node, that performs the user move operation. For example, if node A fails, the SRM on node B performs the user move operation. The SRM throttles the number of users moved to the peer node, it moves the users in batches or iterations. You can configure the number of users that the SRM moves per iteration (the default value is 25). On failover, the SRM will move users that are signed in first, and then move users that are not signed in. Note that if you initiate a fallback, or for Cisco Unified Presence Release 8.6(4) or later automatic fallback occurs, users that are not signed in are moved first, and then users that are signed in.

If the SRM is not turned on, it does not monitor any critical processes, nor does it monitor the heartbeat connections with the peer node.
Before you turn on High Availability in a subcluster, you must configure the SRM service parameters to properly reflect your deployment, see High Availability Client Login Profiles, page I-1.

Related Topics
- High Availability Deployments, page 17-12
- Configure the Advanced Service Parameters for the Server Recovery Manager, page 17-18

Manual Failover and Fallback

From the Cluster Topology interface, you can perform the following procedures:

- Initiate a manual failover for a subcluster. When you initiate a manual failover, the Cisco UP Server Recovery Manager stops the critical services on the failed node, and moves all users to the backup node.
- Initiate a manual fallback from the Cluster Topology interface, where the Cisco UP Server Recovery Manager restarts critical services on the primary node and moves users back to the primary node.
- Perform a manual recovery for a subcluster (when both nodes in the subcluster are in a failed state). When you perform a manual recovery, Cisco Unified Presence restarts the Cisco UP Server Recovery Manager service on both nodes in the subcluster.

Related Topics
- Perform a Manual Failover to Backup Node, page 17-21
- Perform a Manual Fallback to Primary Node, page 17-22
- Perform a Manual Recovery of a Subcluster, page 17-23

Important Note about High Availability and Intercluster Deployments

When failover occurs, the Intercluster Sync Agent is responsible for communicating the user move information to other clusters. The Intercluster Sync Agent runs on both the publisher and subscriber nodes in a cluster. In an Active-Standby configuration, if the publisher node fails or the Intercluster Sync Agent on the publisher node fails, the Intercluster Sync Agent on the subscriber node becomes Active and resumes synchronization, meaning the other clusters will continue to receive the information that users have moved to a different node. Intercluster availability and IM continue to work. Users that have failed over will receive availability information for remote users. Remote users continue to receive availability information and IMs from users that have failed over, and all IMs they send to a failed over user are delivered. When the publisher node recovers, the publisher falls back to Active mode and the subscriber returns to Standby mode.

High Availability Configuration

- Turn On or Off High Availability for a Subcluster, page 17-17
- Configure the Advanced Service Parameters for the Server Recovery Manager, page 17-18
- Configuration Verification, page 17-20
- Perform a Manual Failover to Backup Node, page 17-21
Turn On or Off High Availability for a Subcluster

You have to manually turn on High Availability in a subcluster; Cisco Unified Presence does not turn on High Availability in a subcluster by default. You can turn on High Availability in a subcluster when:

- there are two nodes in the subcluster, and
- both nodes have IP addresses that are resolvable addresses, and
- both nodes are running Cisco Unified Presence Release 8.5 or higher.

You can either assign users to the nodes in the subcluster before or after you turn on High Availability for the subcluster.

Before You Begin

- Configure the subclusters and nodes in your network, and assign nodes to the subclusters.
- Make sure critical services are running on both nodes in the subcluster before you turn on high-availability in a subcluster. If one or more critical services are not running on a node, when you turn on High Availability, that node will failover to the backup node. When one or more critical services are not running on one node in a subcluster, but all critical services are running on the second node, the subcluster will go into a failed state after you turn on High Availability.

Restriction

- You can only turn on High Availability in a subcluster when there are two nodes assigned to that subcluster. The High Availability checkbox does not display when there are no nodes, or one node, assigned to the subcluster.
- You can only turn off High Availability when the nodes in the subcluster are not in a transition state (Failing Over, Falling Back). If you turn off High Availability in a subcluster when either node is in a failed over scenario (Failed Over, Failed), users that Cisco Unified Presence fails over to the backup node are homed to the backup node. Cisco Unified Presence will not move these users back to the primary node, they remain on the secondary node.

Procedure

Step 1 Cisco Unified Presence Administration > System > Cluster Topology.
Step 2 Click the edit link on the appropriate subcluster.
Step 3 Check Enable High Availability.

Note If the nodes in the subcluster are not in a transition state (Failing Over, Falling Back), you can turn off High Availability for the subcluster by unchecking Enable High Availability.
Step 4  Click Save.

Cisco Unified Presence displays the following information about High Availability for the subcluster

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitored Node</td>
<td>The node in the subcluster that Cisco Unified Presence is monitoring for failover detection.</td>
</tr>
<tr>
<td>Node State</td>
<td>The state of the node. See High Availability Deployments, page 17-12 for definitions of the states.</td>
</tr>
<tr>
<td>Node Reason</td>
<td>The reason for the node state.</td>
</tr>
<tr>
<td>Node Action</td>
<td>The action you can take to change the state of the node:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Fallback</strong> - This option is displayed for nodes that are in Idle or Failed Over states. Choose to manually initiate a fallback to this node.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Failover</strong> - This option is displayed for nodes that are in Normal state. Choose to manually initiate a failover to this node.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Recovery</strong> - This option is displayed if both nodes in the subcluster are in a failed state. Choose to manually initiate a recovery of the subcluster where Cisco Unified Presence restarts the SRM service on both nodes.</td>
</tr>
</tbody>
</table>

Configure the Advanced Service Parameters for the Server Recovery Manager

**Procedure**

**Step 1**  Choose Cisco Unified Presence Administration > System > Service Parameters.

**Step 2**  Choose a Cisco Unified Presence server from the Server menu.

**Step 3**  Choose Cisco UP Server Recovery Manager from the Service menu.

**Step 4**  Configure these service parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Additional Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Port</td>
<td>This parameter specifies the port that Cisco UP Server Recovery Manager uses to communicate with its peer.</td>
<td>If you modify this parameter, Cisco Unified Presence restarts the Cisco UP Server Recovery Manager on all nodes in the cluster.</td>
</tr>
<tr>
<td>Admin RPC Port</td>
<td>This parameter specifies the port that Cisco UP Server Recovery Manager uses to provide admin RPC requests.</td>
<td>If you modify this parameter, Cisco Unified Presence restarts the Cisco UP Server Recovery Manager on all nodes in the cluster.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
<td>Additional Information</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Critical Service Down Delay</td>
<td>This parameter determines the duration a critical service can be down before Cisco Unified Presence initiates an automatic failover.</td>
<td>If you change this value, this affects how long a critical service can be down before Cisco Unified Presence initiates an automatic failover.</td>
</tr>
</tbody>
</table>
| Enable Automatic Failover         | This parameter turns automatic failover on or off on Cisco Unified Presence. | This parameter is on by default. Turn this parameter off only if you do not want automatic failover on Cisco Unified Presence and you only want to perform manual failover.  
**Note:** This parameter applies to Cisco Unified Presence Release 8.6(3) and earlier only. |
| Enable Automatic Fallback         | This parameter turns automatic fallback on or off on Cisco Unified Presence. | This parameter is off by default. Turn this parameter on only if you want to enable automatic fallback on Cisco Unified Presence.  
**Note:** This parameter applies to Cisco Unified Presence Release 8.6(4) and later only. |
| Initialization Keep Alive (Heartbeat) Timeout | This parameter specifies the duration that the heartbeat is lost with the peer node (SRM) when the peer SRM restarts and is in the initialization state. | Cisco recommends that you configure this value to at least twice the value of the Keep Alive (Heartbeat) Timeout in order to avoid unnecessary failovers. |
| Keep Alive (Heartbeat) Timeout    | This parameter specifies the duration that the heartbeat is lost with the peer node (SRM) before Cisco Unified Presence initiates an automatic failover. | Cisco recommends that you configure this value to at least twice the value of KeepAliveInterval value. If this value is too close to the KeepAliveInterval value, this can cause a failover to occur. |
| Keep Alive (Heart Beat) Interval  | This parameter specifies the interval between keep alive (heartbeat) messages sent to the peer node. | N/A                                                                                                                                                                                                                     |
| Users Moved Per Iteration         | This parameter specifies the number of users that Cisco Unified Presence moves for each iteration when it performs a failover or a fallback. There is a delay of one second between each iteration. | Increasing this value will shorten the failover time at the expense of CPU. Lowering the value will lengthen failover time, but have less impact on the CPU.  
**Caution:** Before you configure the Users Moved Per Iteration parameter value, refer to the High Availability Client Login Profiles, page I-1. |
Step 5 Click Save.

Related Topic
High Availability Client Login Profiles, page I-1

Configuration Verification

After you have configured High Availability, you can check the status of nodes.

Verify the Cisco UP Service Recovery Manager Service is Running

When you turn on High Availability in a subcluster, Cisco Unified Presence restarts the Cisco UP Service Recovery Manager service and it begins to monitor for failover detection. To verify this service is running, choose Cisco Unified Serviceability > Tools > Control Center - Network Services.
Node State Definitions

Table 17-1 describes the different node states and associated reasons. You can view the state of an existing node by either viewing the node details or the subcluster details on the Cluster Topology interface.

<table>
<thead>
<tr>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initializing</td>
<td>This is the initial (transition) state when the Cisco UP Server Recovery Manager service starts; it is a temporary state.</td>
</tr>
<tr>
<td>Idle</td>
<td>Cisco Unified Presence is in Idle state when failover occurs and services are stopped. In Idle state, the Cisco Unified Presence node does not provide any availability or Instant Messaging services. In Idle state, you can manually initiate a fallback to this node from the Cluster Topology interface.</td>
</tr>
<tr>
<td>Normal</td>
<td>This is a stable state. The Cisco Unified Presence node is operating normally. In this state, you can manually initiate a failover to this node from the Cluster Topology interface.</td>
</tr>
<tr>
<td>Running in Backup Mode</td>
<td>This is a stable state. The Cisco Unified Presence node is acting as the backup for its peer node. Users have moved to this (backup) node.</td>
</tr>
<tr>
<td>Taking Over</td>
<td>This is a transition state. The Cisco Unified Presence node is taking over for its peer node.</td>
</tr>
<tr>
<td>Failing Over</td>
<td>This is a transition state. The Cisco Unified Presence node is being taken over by its peer node.</td>
</tr>
<tr>
<td>Failed Over</td>
<td>This is a stable state. The Cisco Unified Presence node has failed over, but no critical services are down. In this state, you can manually initiate a fallback to this node from the Cluster Topology interface.</td>
</tr>
<tr>
<td>Failed Over with Critical Services Not Running</td>
<td>This is a stable state. Some of the critical services on the Cisco Unified Presence node have either stopped or failed.</td>
</tr>
<tr>
<td>Falling Back</td>
<td>This is a transition state. The system is falling back to this Cisco Unified Presence node from the node running in Backup Mode.</td>
</tr>
<tr>
<td>Taking Back</td>
<td>This is a transition state. The failed Cisco Unified Presence node is taking back over from its peer.</td>
</tr>
<tr>
<td>Running in Failed Mode</td>
<td>An error occurs during the transition states or Running in Backup Mode state.</td>
</tr>
<tr>
<td>Unknown</td>
<td>State unknown.</td>
</tr>
</tbody>
</table>

Perform a Manual Failover to Backup Node

You can perform a manual failover to the backup node in the subcluster using the Cluster Topology interface. When you initiate a manual failover, the Cisco UP Server Recovery Manager stops the critical services on that node, and moves all users to the backup node.

The Cisco UP Server Recovery Manager stops the following critical services on the node:

- Cisco UP SIP Proxy
- Cisco UP Presence Engine
High Availability Configuration

Chapter 17  Multi-node Deployment Administration

- Cisco UP XCP Router (this causes all XCP processes to stop)
- Cisco UP Client Profile Agent

The Cisco UP Server Recovery Manager then moves all users to the backup node

Restriction

You can only initiate a failover for a node that is in ‘Normal’ state.

Before You Begin

Make sure that these services are running on the Failing Over node:
- Cisco UP XCP Connection Manager service
- Cisco UP XCP Router
- Cisco UP Presence Engine

Procedure

Step 1  Cisco Unified Presence Administration > System > Cluster Topology.
Step 2  Click the edit link on the appropriate subcluster.
Step 3  Choose Failover in the Node Action column.
Step 4  Click Ok to confirm the failover operation.
Step 5  To verify the failover operation is complete and successful:
  - When the failover operation is in progress, the primary node should be in the “Failing Over” state, and the backup node should be in the “Taking Over” state. When the failover operation is complete, check that the backup node is in the state ‘Running in Backup Mode’, and the primary node is in “Idle” state. If the failover is unsuccessful, and the nodes are in a failed state, see Node States, Causes and Recommended Actions, page 21-1 for a recommended action.
  - Check that the users have failed over to the backup node:
    - On the subcluster details screen, check that all users are now assigned to the backup node, and no users are assigned to the primary node.
    - On the node details screen, the ‘Failed Over’ column indicates the users that have failed over to the backup node.

Related Topic

High Availability Deployments, page 17-12

Perform a Manual Fallback to Primary Node

You can perform a manual fallback to the primary node in the Cluster Topology interface. When you initiate a manual fallback, the Cisco UP Server Recovery Manager restarts any critical services that are not already running on the primary node, and moves the failed over users back to the primary node.

When you manually initiate a fallback, the Cisco UP Server Recovery Manager restarts the following services on the primary node (if they are not already running):
- Cisco UP SIP Proxy
High Availability Configuration

The Cisco UP Server Recovery Manager then moves all failed over users back to the primary node.

Restriction
You can only initiate fallback for a node that is in ‘Idle’ or ‘Failed Over’ state.

Procedure

Step 1: Cisco Unified Presence Administration > System > Cluster Topology.
Step 2: Click the edit link on the appropriate subcluster.
Step 3: Choose Fallback in the Node Action column.
Step 4: Click Ok to confirm the fallback operation.
Step 5: To verify the fallback operation is complete and successful:
   - When fallback operation is in progress, the primary node should be in the “Taking Back” state, and
     the backup node should be in the “Falling Back” state. When the fallback operation is complete, check that both nodes are in ‘Normal’ state. If the fallback is unsuccessful, and the nodes are in a failed state, see Node States, Causes and Recommended Actions, page 21-1 for a recommended action.
   - Check that the users have fallen back to the primary node.
     - On the subcluster details screen, check that all users are now assigned to the primary node, and no users are assigned to the backup node.
     - On the node details screen, the ‘Failed Over’ column should be empty.

Related Topic
High Availability Deployments, page 17-12

Perform a Manual Recovery of a Subcluster

When you perform a manual recovery of a subcluster, Cisco Unified Presence restarts the Cisco UP Server Recovery Manager service on both nodes in the subcluster. You may experience IDS replication delays. You can check the status of the IDS replication on a node using this CLI command:

```
utils dbreplication rundownstate
```

Restriction
You can only initiate a recovery for a subcluster if both nodes are in a failed state.

Procedure

Step 1: Choose Cisco Unified Presence Administration > System > Cluster Topology.
Step 2  Click the edit link on the appropriate subcluster.

Step 3  Choose Recovery in the Node Action column.

Step 4  See Node States, Causes and Recommended Actions, page 21-1 to verify the status of the subcluster after you perform the manual recovery.

Related Topic
High Availability Deployments, page 17-12

Cluster-wide Routing Information on Cisco Unified Presence

Configure a Cluster-wide Cisco Unified Presence Address

This procedure is only applicable if you are configuring a multi-node deployment. Configure the cluster-wide Cisco Unified Presence address on the publisher node, and Cisco Unified Presence will replicate the address on all nodes in the cluster.

Note
When you configure a cluster-wide Cisco Unified Presence address, set the port of SRV to 5060.

Before You Begin
Read the cluster-wide DNS SRV topic.

Procedure

Step 1  Choose Cisco Unified Presence Administration > System > Service Parameters.
Step 2  Choose the Cisco Unified Presence server from the Server menu.
Step 3  Choose Cisco UP Sip Proxy from the Service menu.
Step 4  Edit the SRV Cluster Name field in the General Proxy Parameters (Clusterwide) section.
By default this parameter is empty.
Step 5  Click Save.

What To Do Next
Upload the licenses on Cisco Unified Presence. For more information, see the Upgrade Guide for Cisco Unified Presence Release 8.6.

Static Route Configuration

If you configure a static route for SIP proxy server traffic, consider the following:
A dynamic route represents a path through the network that is automatically calculated according to routing protocols and routing update messages.

A static route represents a fixed path that you explicitly configure through the network.

Static routes take precedence over dynamic routes.

This section contains the following subsections:

- Route Embed Templates, page 17-25
- Configure Route Embed Templates, page 17-26
- Configure Static Routes, page 17-26

## Route Embed Templates

You must define a route embed template for any static route pattern that contains embedded wildcards. The route embed template contains information about the leading digits, the digit length, and location of the embedded wildcards. Before you define a route embed template, consider the sample templates we provide below.

When you define a route embed template, the characters that follow the '.' must match actual telephony digits in the static route. In the sample route embed templates below, we represent these characters with 'x'.

### Sample Route Embed Template A

Route embed template: **74..78xxxxx***

With this template, Cisco Unified Presence will enable this set of static routes with embedded wildcards:

<table>
<thead>
<tr>
<th>Destination Pattern</th>
<th>Next Hop Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>74..7812345*</td>
<td>1.2.3.4:5060</td>
</tr>
<tr>
<td>74..7867890*</td>
<td>5.6.7.8.9:5060</td>
</tr>
<tr>
<td>74..7811993*</td>
<td>10.10.11.37:5060</td>
</tr>
</tbody>
</table>

With this template, Cisco Unified Presence will NOT enable these static route entries:

- 73..7812345* (The initial string is not ‘74’ as the template defines)
- 74..781* (The destination pattern digit length does not match the template)
- 74...7812345* (The number of wildcards does not match the template)

### Sample Route Embed Template B

Route embed template: **471….xx**

With this template, Cisco Unified Presence will enable this set of static routes with embedded wildcards:
Static Route Configuration

Chapter 17      Multi-node Deployment Administration

Configuration and Administration of Cisco Unified Presence Release 8.6

Static Route Configuration

With this template, Cisco Unified Presence will NOT enable these static route entries:

- 47…344* (The initial string is not '471' as the template defines)
- 471…4* (The string length does not match template)
- 471.450* (The number of wildcards does not match template)

Configure Route Embed Templates

You can define up to five route embed templates. However, there is no limit to the number of static routes that you can define for any route embed template.

A static route that contains an embedded wildcard must match at least one of the route embed templates.

Procedure

Step 1
Choose Cisco Unified Presence Administration > System > Service Parameters.

Step 2
Choose a Cisco Unified Presence server.

Step 3
Choose the Cisco UP SIP Proxy service.

Step 4
Define a route embed templates in the RouteEmbedTemplate field in the Routing Parameters (Clusterwide) section. You can define up to five route embed templates.

Step 5
Click Save.

What To Do Next
Configure Static Routes, page 17-26

Configure Static Routes

Procedure

Step 1
Choose Cisco Unified Presence Administration > Routing > Static Routes.

Step 2
Click Add New.

Step 3
Configure these static route settings:

<table>
<thead>
<tr>
<th>Destination Pattern</th>
<th>Next Hop Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>471....34*</td>
<td>20.20.21.22</td>
</tr>
<tr>
<td>471....55*</td>
<td>21.21.55.79</td>
</tr>
</tbody>
</table>
## Static Route Configuration

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination Pattern</td>
<td>This field specifies the pattern of the incoming number, up to a maximum of 255 characters. The SIP proxy allows only 100 static routes to have an identical route pattern. If you exceed this limit, Cisco Unified Presence logs an error.</td>
</tr>
<tr>
<td><strong>Wildcard Usage</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>You can use &quot;.&quot; as a wildcard for a single character and &quot;*&quot; as a wildcard for multiple characters. Cisco Unified Presence supports embedded &quot;.&quot; wildcard characters in static routes. However, you must define route embed templates for static routes that contain embedded wildcards. Any static route that contains an embedded wildcard must match at least one route embed template. See the route embed template topic (referenced in the Related Topics section below) for information about defining route embed templates. For phones:</td>
</tr>
<tr>
<td></td>
<td>• A dot can exist at the end of the pattern, or embedded in a pattern. If you embed the dot in a pattern, you must create a route embed template to match the pattern.</td>
</tr>
<tr>
<td></td>
<td>• An asterisk can only exist at the end of the pattern. For IP addresses and host names:</td>
</tr>
<tr>
<td></td>
<td>• You can use an asterisk as part of the a host name.</td>
</tr>
<tr>
<td></td>
<td>• The dot acts as a literal value in a host name. An escaped asterisk sequence, \*, matches a literal * and can exist anywhere.</td>
</tr>
<tr>
<td>Description</td>
<td>Specifies the description of a particular static route, up to a maximum of 255 characters.</td>
</tr>
<tr>
<td>Next Hop</td>
<td>Specifies the domain name or IP address of the destination (next hop) and can be either a Fully Qualified Domain Name (FQDN) or dotted IP address. Cisco Unified Presence supports DNS SRV-based call routing. To specify DNS SRV as the next hop for a static route, set this parameter to the DNS SRV name.</td>
</tr>
<tr>
<td>Next Hop Port</td>
<td>Specifies the port number of the destination (next hop). The default port is 5060. Cisco Unified Presence supports DNS SRV-based call routing. To specify DNS SRV as the next hop for a static route, set the next hop port parameter to 0.</td>
</tr>
</tbody>
</table>
### Static Route Configuration

#### Field | Description
--- | ---
**Route Type** | Specifies the route type: User or Domain. The default value is user. For example, in the SIP URI "sip:19194762030@myhost.com" request, the user part is '19194762030', and the host part is 'myhost.com'. If you choose User as the route type, Cisco Unified Presence uses the user-part value '19194762030' for routing SIP traffic. If you choose the Domain as the route type, Cisco Unified Presence uses 'myhost.com' for routing SIP traffic.  
**Protocol Type** | Specifies the protocol type for this route, TCP, UDP, or TLS. The default value is TCP.  
**Priority** | Specifies the route priority level. Lower values indicate higher priority. The default value is 1.  
**Weight** | Specifies the route weight. Use this parameter only if two or more routes have the same priority. Higher values indicate which route has the higher priority.  
**Allow Less-Specific Route** | Specifies that the route can be less specific. The default setting is On.  
**In Service** | Specifies whether this route has been taken out of service. This parameter allows the administrator to effectively take a route out of service (versus removing it completely and re-adding it).  
**Block Route Check Box** | Check to block the static route. The default setting is Unblocked.

#### Example:
Consider these three routes with associated priorities and weights:
- 1, 20
- 1, 10
- 2, 50

In this example, the static routes are listed in the correct order. The priority route is based on the lowest value priority, that is 1. Given that two routes share the same priority, the weight parameter with the highest value decides the priority route. In this example, Cisco Unified Presence directs SIP traffic to both routes configured with a priority value of 1, and distributes the traffic according to weight; The route with a weight of 20 receives twice as much traffic as the route with a weight of 10. Note that in this example, Cisco Unified Presence will only attempt to use the route with priority 2, if it has tried both priority 1 routes and both failed.

#### Step 4
Click **Save**.
Presence Gateway Configuration on Cisco Unified Presence

- Presence Gateway Configuration Option, page 17-29
- Configuring the Presence Gateway, page 17-29

Presence Gateway Configuration Option

You must configure Cisco Unified Communications Manager as a Presence Gateway on Cisco Unified Presence to enable the SIP connection that handles the availability information exchange between Cisco Unified Communications Manager and Cisco Unified Presence.

When configuring the Presence Gateway, specify the FQDN (Fully Qualified Domain Name) or the IP address of the associated Cisco Unified Communications Manager server. Depending on your network this value can be one of the following:

- the FQDN address of the Cisco Unified Communications Manager publisher
- a DNS SRV FQDN that resolves to the Cisco Unified Communications Manager subscriber nodes
- the IP address of the Cisco Unified Communications Manager publisher

If DNS SRV is an option in your network, configure the following:

1. Configure the Presence Gateway on the Cisco Unified Presence server with a DNS SRV FQDN of the Cisco Unified Communications Manager subscriber nodes (equally weighted). This will enable Cisco Unified Presence to share availability messages equally among all the servers used for availability information exchange.

2. On Cisco Unified Communications Manager, configure the SIP trunk for the Cisco Unified Presence server with a DNS SRV FQDN of the Cisco Unified Presence publisher and subscriber.

If DNS SRV is not an option in your network, and you are using the IP address of the associated Cisco Unified Communications Manager server, you cannot share availability messaging traffic equally across multiple subscriber nodes because the IP address points to a single subscriber node.

Related Topic
SIP Trunk Configuration on Cisco Unified Communications Manager, page 6-4

Configuring the Presence Gateway

Before You Begin

- Read the Presence Gateway configuration options topic.
- Depending on your configuration requirements, obtain the FQDN, DNS SRV FQDN, or the IP address of the associated Cisco Unified Communications Manager server.

Procedure

Step 1 Choose Cisco Unified Presence Administration > Presence > Gateways.
Step 2 Click Add New.
Step 3 Choose CUCM for the Presence Gateway Type.
Step 4 Enter a description of the presence gateway in the Description field.
Specify the FQDN, DNS SRV FQDN, or the IP address of the associated Cisco Unified Communications Manager server in the Presence Gateway field.

Click Save.

Related Topic
Presence Gateway Configuration Option, page 17-29
Chat Setup and Management

June 16, 2014

- Chat Deployments, page 18-1
- Chat Settings Administration, page 18-4
- Chat Node Alias Management, page 18-8

Chat Deployments

The tables below contain a sample range of deployment scenarios that administrators may want to configure.

For more information about the Chat feature, see Chat, page 1-9.

Scenario 1

Deployment Scenario: You do not want to include the Cluster ID in the chat node alias. Instead of the system-generated alias `conference-1-mycup.cisco.com`, you want to use the alias `primary-conf-server.cisco.com`.

Configuration Steps:
1. Choose Messaging > Group Chat and Persistent Chat to turn off the system-generated alias. (This is on by default).
2. Edit the alias and change it to `primary-conf-server.cisco.com`.

Notes: When you turn off the old system-generated alias, `conference-1-mycup.cisco.com` reverts to a standard, editable alias listed under Group Chat Server Aliases. This maintains the old alias and the chat room addresses associated with that alias.
Scenario 2

Deployment Scenario:
You want to:

- maintain the address of existing persistent chat rooms in the database so that users can still find old chat rooms of type xxx@conference-1-mycup.cisco.com.

Configuration Steps:
2. See Appendix 7, “Configure Routing Communication”, for steps on how to Edit the Domain and change it to linksys.com.

Notes:
When you change the domain, the fully qualified cluster name (FQCN) automatically changes from conference-1-mycup.cisco.com to conference-1-mycup.linksys.com. The old system-generated alias conference-1-mycup.cisco.com reverts to a standard, editable alias listed under Group Chat Server Aliases. This maintains the old alias and the chat room addresses associated with that alias.

Scenario 3

Deployment Scenario:
You:

- want to change the Cluster ID from mycup to ireland to use conference-1-ireland.cisco.com instead of conference-1-mycup.cisco.com.
- do not need to maintain the address of existing persistent chat rooms in the database.

Configuration Steps:
2. Edit the Cluster ID and change it to ireland.

Notes:
When you change the Cluster ID, the fully qualified cluster name (FQCN) automatically changes from conference-1-mycup.cisco.com to conference-1-ireland.cisco.com. The old system-generated alias conference-1-mycup.cisco.com reverts to a standard, editable alias listed under Group Chat Server Aliases. This maintains the old alias and the chat room addresses associated with that alias. Because (in this example) the Administrator has no need to maintain the old alias address, it is appropriate to delete it.
Scenario 4

Deployment Scenario: You want to:

- change the Cluster ID from mycup to ireland to use conference-1-ireland.cisco.com instead of conference-1-mycup.cisco.com.
- only maintain chat room addressing via the old alias (does not need to associate nodes with the new system-generated alias).

Configuration Steps:

2. Edit the Cluster ID and changes it to ireland.
3. Choose Messaging > Group Chat and Persistent Chat and turn off the new system-generated alias, conference-1-ireland.cisco.com. (This is on by default).

Notes: When you change the Cluster ID, the fully qualified cluster name (FQCN) automatically changes from conference-1-mycup.cisco.com to conference-1-ireland.cisco.com. When you turn off the new system-generated alias, conference-1-ireland.cisco.com reverts to a standard, editable alias listed under Group Chat Server Aliases. Because (in this example) the Administrator has no need to maintain the new alias address, it is appropriate to delete it. The old system-generated alias conference-1-mycup.cisco.com reverts to a standard, editable alias listed under Group Chat Server Aliases. This maintains the old alias and the chat room addresses associated with that alias.
Scenario 5

Deployment Scenario: You want to:
- delete a node associated with an existing alias from the System Topology, for example, conference-3-mycup.cisco.com.
- add a new node with a new node ID (node id: 7) to the System Topology, for example, conference-7-mycup.cisco.com.
- maintain the address of chat rooms that were created using the old alias.

Configuration Steps:

**Option 1**
2. Click **Add New** to add the additional alias, conference-3-mycup.cisco.com.

**Option 2**
1. Choose **Messaging > Group Chat and Persistent Chat** and turn off the default system-generated alias, conference-7-mycup.cisco.com. (This is on by default).
2. Edit the alias and change it to conference-3-mycup.cisco.com.

Notes: When you add the new node to the System Topology, the system automatically assigns this alias to the node: conference-7-mycup.cisco.com.

**Option 1**
- If you add an additional alias, the node is addressable via both aliases, conference-7-mycup.cisco.com and conference-3-mycup.cisco.com.

**Option 2**
- If you turn off the old system-generated alias, conference-7-mycup.cisco.com reverts to a standard, editable alias listed under Group Chat Server Aliases.

Chat Settings Administration

- Change IM Gateway Settings, page 18-5
- Enable File Transfer, page 18-5
- Limit the Number of Sign-in Sessions, page 18-6
- Enable Persistent Chat, page 18-6
Change IM Gateway Settings

You can configure IM Gateway settings for Cisco Unified Presence.

The SIP-to-XMPP connection on the Cisco Unified Presence IM Gateway is enabled by default. This allows IM interoperability between SIP and XMPP clients so that users of SIP IM clients can exchange bidirectional IMs with users of XMPP IM clients. Cisco recommends that you leave the IM Gateway Status parameter on; however, you can turn off the IM Gateway Status parameter to prevent XMPP and SIP clients from communicating with each other.

You can also change the default inactive timeout interval of IM conversations, as well as choose the error message that gets displayed if the IM fails to get delivered.

Restriction

SIP clients cannot participate in chat rooms because this is an XMPP-specific feature.

Procedure

Step 1 Choose Cisco Unified Presence Administration > System > Service Parameters.
Step 2 Choose a Cisco Unified Presence server from the Server menu.
Step 3 Choose Cisco UP SIP Proxy as the service on the Service Parameter Configuration window.
Step 4 Set IM Gateway Status to On in the SIP XMPP IM Gateway (Clusterwide) section.
Step 5 Set the Inactive Timeout interval (in seconds) of IM conversations maintained by the gateway. The default setting is 600 seconds, which is appropriate to most environments.
Step 6 Specify the error message that you want users to see if the IM fails to deliver. Default error message: Your IM could not be delivered.
Step 7 Click Save.

What To Do Next

Enable Persistent Chat, page 18-6

Enable File Transfer

Administrators can enable or disable Cisco Unified Presence server support for file transfer capability (XEP-0096). Enabling file transfer support allows XMPP clients to extend file transfer capabilities to end users.

Note

File transfer between a local user and an intercluster peer contact is only possible if both clusters have the feature enabled.

Procedure

Step 1 Choose Cisco Unified Presence Administration > System > Service Parameters.
Step 2 Choose a Cisco Unified Presence server from the Server menu.
Step 3 Choose Cisco UP XCP Router as the service on the Service Parameter Configuration window.
Step 4  Choose On or Off from the Enable file transfer drop-down list.
Step 5  Click Save.
Step 6  Restart the Cisco UP XCP Router Service on every node in the cluster. For more information, see DNS Domain Configuration, page 7-3.

Limit the Number of Sign-in Sessions

Administrators can limit the number of logon sessions per user on the Cisco UP XCP Router. If the limit is reached, existing XMPP login sessions remain active; however, new XMPP login sessions are prevented.

Note
This parameter is applicable to XMPP clients only.

Procedure

Step 1  Choose Cisco Unified Presence Administration > System > Service Parameters.
Step 2  From the Server drop-down list, choose a Cisco Unified Presence server.
Step 3  From the Service drop-down list, choose Cisco UP XCP Router.
Step 4  Enter a parameter value in the Maximum number of logon sessions per user in the XCP Session Manager Configuration Parameters (Clusterwide) section.
Step 5  Click Save.
Step 6  Restart the Cisco UP XCP Router Service on every node in the cluster. For more information, see DNS Domain Configuration, page 7-3.

Enable Persistent Chat

You need to configure persistent chat settings only if you use persistent chat rooms as opposed to temporary (ad-hoc) chat rooms. This configuration is specific to persistent chat and has no impact on IM archiving for regulatory compliance.

Restriction
SIP clients cannot participate in chat rooms because this is an XMPP-specific feature.

Before You Begin
- To use persistent chat rooms, you must configure a unique external database instance per node.
- If you use an external database for persistent chat logging, consider the size of your database. Archiving all the messages in a chat room is optional, and will increase traffic on the node and consume space on the external database disk. In large deployments, disk space could be quickly consumed. Ensure that your database is large enough to handle the volume of information.
Before you configure the number of connections to the external database, consider the number of IMs you are writing offline and the overall volume of traffic that results. The number of connections that you configure will allow the system to scale. While the default settings on the UI suit most installations, you may want to adapt the parameters for your specific deployment.

The heartbeat interval is typically used to keep connections open through firewalls. Do not set the Database Connection Heartbeat Interval value to zero without contacting Cisco support.

**Procedure**

**Step 1** Choose Cisco Unified Presence Administration > Messaging > Group Chat and Persistent Chat.

**Step 2** Check Enable Persistent Chat.

**Step 3** (Optional) Specify how to store chat room messages, if required:

- a. Check Archive all room messages if you want to archive all the messages that are sent in the room. This is a cluster-wide setting that applies to all persistent chat rooms. Cisco recommends that you monitor the performance of each external database used for persistent chat. You should anticipate an increased load on the database server(s).

  **Note** If you turn on the Archive all room messages option for persistent chat, Cisco Unified Personal Communicator actively queries Cisco Unified Presence for all instant message history regardless of the value you configure for the Number of messages in chat history displayed for new chat participants setting.

- b. Enter the number of connections to the database that you want to use for processing requests. This is a cluster-wide setting that applies to all connections between chat nodes and associated databases.

- c. Enter the number of seconds after which the database connection should refresh. This is a cluster-wide setting that applies to all connections between chat nodes and associated databases.

**Step 4** Choose from the list of preconfigured external databases and assign the appropriate database to the chat node.

  **Note** If you do not establish the correct connection with the external database, the chat node will fail. Under these circumstances, you will lose the functionality of all chat rooms - both temporary and persistent. If a chat node establishes a connection (even if other chat nodes fail), it will still start.

**Step 5** Click Save.

**Step 6** Restart the Cisco UP XCP Text Conference Manager for a chance in Persistent Chat settings to take effect. Choose Cisco Unified Serviceability > Tools > Control Center - Feature Services to restart this service.

**Related Topics**

- Change IM Gateway Settings, page 18-5
- Chat Node Alias Management, page 18-8
- To configure an external database instance for offline message logging and retrieval, see the Database Setup Guide for Cisco Unified Presence.
Chat Node Alias Management

- Chat Node Aliases, page 18-8
- Key Considerations, page 18-9
- Turn On System-generated Chat Node Aliases, page 18-9
- Manage Chat Node Aliases Manually, page 18-10
- Turn On the Cisco UP XCP Text Conference Service, page 18-12

Chat Node Aliases

Aliases create a unique address for each chat node so that users (in any domain) can search for specific chat rooms on specific nodes, and join chat in those rooms. Each chat node in a system must have a unique alias.

Note

This chat node alias, conference-3-mycup.cisco.com, for example, will form part of the unique ID for each chat room created on that node, roomjid@conference-3-mycup.cisco.com

You can assign your aliases cluster-wide, in these ways:

- System-generated - allows the system to automatically assign a unique alias to each chat node. You do not have to do anything further to address your chat node if you enable the system-generated aliases. The system will auto-generate one alias per chat node by default using the following naming convention: conference-x-clusterid.domain, where:
  - conference - is a hardcoded keyword
  - x - is the unique integer value that denotes the node ID
  - Example: conference-3-mycup.cisco.com

Note

Even if you configure a system-generated alias for a chat node, you can associate more than one alias with the node if required.

- Manually - You may choose to override the default system-generated alias if the conference-x-clusterid.domain naming convention does not suit your customer deployment, for example, if you do not want to include the Cluster ID in your chat node alias. With manually-managed aliases, you have complete flexibility to name chat nodes using aliases that suit your specific requirements.

- Additional Aliases - You can associate more than one alias with each chat node on a per-node basis. Multiple aliases per node allows users to create additional chat rooms using these aliases. This applies whether you assign a system-generated alias or manage your aliases manually.
Key Considerations

Changing chat node aliases can make the chat rooms in the database unaddressable and prevent your users from finding existing chat rooms.

Note these results before you change the constituent parts of aliases or other node dependencies:

- **Cluster ID** - This value is part of the fully qualified cluster name (FQCN). Changing the Cluster ID (choose System > Cluster Topology: Settings) causes the FQCN to incorporate the new value and the system-managed alias to automatically change across the cluster. For manually-managed aliases, it is the responsibility of the Administrator to manually update the alias list if the Cluster ID changes.

- **Domain** - This value is part of the FQCN. Changing the Domain (choose System > Service Parameters > Cisco UP Proxy) causes the FQCN to incorporate the new value and the system-managed alias to automatically change across the cluster. For manually-managed aliases, it is the responsibility of the Administrator to manually update the alias list if the Domain changes.

- **Connection between the chat node and external database** - The chat node will not start if persistent chat is enabled and you do not maintain the correct connection with the external database. If you are federating with external domains, you may want to inform federated parties that the aliases have changed and new aliases are available. To advertise all aliases externally, configure DNS and publish the aliases as DNS records.

- **Deletion of a chat node** - If you delete a node associated with an existing alias from the Cluster Topology, chat rooms created using the old alias may not be addressable unless you take further action.

Cisco recommends that you do not change existing aliases without considering the wider implications of your changes, namely:

- Make sure that you maintain the address of old chat nodes in the database so that users can locate existing chat rooms via the old alias, if required

- If there is federation with external domains, you may need to publish the aliases in DNS to inform the users in those domains that the aliases have changed and new addresses are available. This depends on whether or not you want to advertise all aliases externally.

**Related Topic**
For best practice guidelines, see Scenario 1, page 18-1

Turn On System-generated Chat Node Aliases

**Before You Begin**

- Review the topics about chat node aliases and key considerations.

- You cannot edit or delete a system-generated alias, for example, conference-3-mycup.cisco.com.

**Procedure**

**Step 1** Choose Cisco Unified Presence Administration > Messaging > Group Chat and Persistent Chat.

**Step 2** Check System Automatically Manages Primary Group Chat Server Aliases to enable the system to automatically assign chat room aliases to nodes, using this alias naming convention: conference-x-clusterid.domain.
Step 3  The **Number of messages in chat history displayed for new conference participants** setting controls the number of instant messages from the recent message history that Cisco Unified Presence pushes to the client application of a user when that user joins a chat room. Increase this number if you want to display more text message history to users. If users of client applications create a chat room, they may potentially override the default number of messages that display in a chat room.

---

**Note**  If you turn on the **Archive all room messages** option for persistent chat, Cisco Unified Personal Communicator actively queries Cisco Unified Presence for all instant message history regardless of the value you configure for the **Number of messages in chat history displayed for new chat participants** setting.

---

Step 4  Choose **Messaging > Group Chat Server Alias Mapping** to verify that the system-generated alias is listed under Primary Group Chat Server Aliases.

Step 5  If you updated any of the system-generated alias configuration, except the **Number of messages in chat history displayed for new chat participants** setting, restart the Cisco UP XCP Text Conference Manager. Choose **Cisco Unified Serviceability > Tools > Control Center - Feature Services** to restart this service.

---

**Note**  The **Number of messages in chat history displayed for new chat participants** setting updates dynamically; You do not need to restart the Cisco UP XCP Text Conference Manager.

---

**Related Topics**
- Chat Node Aliases, page 18-8
- Key Considerations, page 18-9
- Enable Persistent Chat, page 18-6
- Manage Chat Node Aliases Manually, page 18-10

---

**Manage Chat Node Aliases Manually**

You can manually add, edit, or delete chat node aliases. To manually manage chat node aliases, you must turn off the default setting which uses system-generated aliases. If you turn off a system-generated alias, the existing alias (conference-x-clisterid.domain) reverts to a standard, editable alias listed under Conference Server Aliases. This maintains the old alias and the chat room addresses associated with that alias.

You can manually assign multiple aliases to chat nodes. Even if a system-generated alias already exists for a chat node, you can associate additional aliases to the node manually.

For manually-managed aliases, it is the responsibility of the Administrator to manually update the alias list if the Cluster ID or Domain changes. System-generated aliases will incorporate the changed values automatically.

---

**Note**  Although it is not mandatory, Cisco recommends that you always include the Domain when you assign a new chat node alias to a node. Use this convention for additional aliases, newalias.domain. Choose **System > Cluster Topology: Settings** in Cisco Unified Presence Administration to see the Domain.
Before You Begin

- Review the topics about chat node aliases and key considerations.

Procedure

**Step 1** Choose **Cisco Unified Presence Administration > Messaging > Group Chat and Persistent Chat**.

**Step 2** Uncheck **System Automatically Manages Primary Group Chat Server Aliases** to turn off the default system-generated alias.

**Step 3** All the existing chat node aliases (including the disabled system-generated alias) are listed together under Group Chat Server Aliases. To view the alias list, perform these actions:

a. Choose **Messaging > Group Chat Server Alias Mapping**.

b. Click **Find**.

**Step 4** Complete one or more of the following actions as required:

<table>
<thead>
<tr>
<th>If you want to:</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| Edit an existing alias | a. Click the hyperlink for any existing alias that you want to edit.  
b. Edit the alias for the node in the Group Chat Server Alias field. Make sure the alias is unique for the node.  
c. Choose the appropriate node to which you want to assign this changed alias. | If you are federating with external domains, you may want to inform federated parties that the aliases have changed and new aliases are available. To advertise all aliases externally, configure DNS and publish the aliases as DNS records.  
A chat node alias name *cannot* match the Cisco Unified Presence domain name. |
| Add a new chat node alias | a. Click **Add New**.  
b. Enter a unique alias for the node in the Group Chat Server Alias field.  
c. Choose the appropriate node to which you want to assign the new alias. | Every chat node alias must be unique. The system will prevent you from creating duplicate chat node aliases across the cluster.  
A chat node alias name *cannot* match the Cisco Unified Presence domain name. |
| Delete an existing alias | a. Check the check box for the alias that you want to delete.  
b. Click **Delete Selected**. | You can delete old aliases only if you no longer need to maintain the address of chat rooms via the old alias. |

**Step 5** If you updated any of the chat node alias configuration, restart the Cisco UP XCP Text Conference Manager. Choose **Cisco Unified Serviceability > Tools > Control Center - Feature Services** to restart this service.

Related Topics

- Chat Node Aliases, page 18-8
- Key Considerations, page 18-9
Chat Node Alias Management

- Turn On System-generated Chat Node Aliases, page 18-9
- For best practice guidelines, see Chat Deployments, page 18-1
- Domain Value Configuration, page 7-7

What To Do Next
- Turn On the Cisco UP XCP Text Conference Service, page 18-12

Turn On the Cisco UP XCP Text Conference Service

This procedure applies if you configure the persistent chat room settings, or manually add one or more aliases to a chat node. You must also turn on this service if you want to enable temporary (ad-hoc) chat on a node.

Before You Begin

If persistent chat is enabled, an external database must be associated with the Text Conference Manager service, and the database must be active and reachable or the Text Conference Manager will not start. If the connection with the external database fails after the Text Conference Manager service has started, the Text Conference Manager service will remain active and functional, however, messages will no longer be persisted to database and new persistent rooms cannot be created until the connection recovers.

Procedure

Step 1  Choose Cisco Unified Serviceability > Tools > Service Activation.
Step 2  Choose the chat node from the Server menu.
Step 3  Choose the Cisco UP XCP Text Conference Manager service to turn it on.
Step 4  Click Save.

Related Topics
- Enable Persistent Chat, page 18-6
- Manage Chat Node Aliases Manually, page 18-10
- DNS Domain Configuration, page 7-3
User Migration between Cisco Unified Presence Clusters

June 16, 2014

- Unassign Users from the Current Cluster, page 19-2
- Export User Contact Lists, page 19-3
- Unlicense Users, page 19-4
- Move Users to the New Cluster, page 19-4
- License the Users on the New Cluster, page 19-5
- Import Contact Lists on the New Home Cluster, page 19-6

This section describes how to migrate users between Cisco Unified Presence clusters.

Note

This procedure only migrates user contacts that are provisioned with an IM Address. User contacts with only phone numbers are not migrated and must be manually re-added by the end user after the migration completes.

You must complete the following procedures in the order in which they are presented:

- Unassign the migrating users from their current cluster
- Export the contact lists of the migrating users from their current home cluster
- Unlicense the migrating users for Cisco Unified Presence and Cisco Jabber on their current home cluster from Cisco Unified Communications Manager
- If LDAP Sync is enabled on Cisco Unified Communications Manager:
  - move the users to the new Organization Unit, from which their new cluster synchronizes its information
  - synchronize the users to the new home Cisco Unified Communications Manager, see
- If LDAP Sync is not enabled on Cisco Unified Communications Manager, manually provision the migrating users on Cisco Unified Communications Manager
- License users for Cisco Unified Presence and Cisco Jabber
- Import contact lists to the new home cluster to restore contact list data for migrated users
Before You Begin

- Perform a full DRS of the current cluster and the new home cluster.
  See the Disaster Recovery System Administration Guide for Cisco Unified Presence for more information.
- Ensure that the following services are running:
  - Cisco UP Intercluster Sync Agent
  - Cisco AXL Web Service
  - Cisco UP Sync Agent
- Run the Troubleshooter and ensure that there are no Intercluster Sync Agent issues reported. All Intercluster Sync Agent issues reported on the Troubleshooter must be resolved before proceeding with this procedure.
- Cisco recommends that the Allow users to view the availability of other users without being prompted for approval setting is enabled. To enable this setting, choose Cisco Unified Presence Administration > Presence > Settings. Any change to this setting requires a restart of the Cisco XCP Router.
- Cisco recommends that the following settings are set to No Limit:
  - Maximum Contact List Size (per user)
  - Maximum Watchers (per user)
  To configure these settings, choose Cisco Unified Presence Administration > Presence > Settings.
- Ensure that the users to be migrated are licensed for Cisco Unified Presence or Cisco Jabber on their current (pre-migration) home cluster only. If these users are licensed on any other cluster, they need to be fully unlicensed before proceeding with the following procedures.

Unassign Users from the Current Cluster

Complete this procedure to unassign the migrating users from their current cluster.

Procedure

Step 1  Choose Cisco Unified Presence Administration > System > Cluster Topology.
Step 2  Choose the users that you want to migrate to a remote Cisco Unified Presence cluster.
Step 3  Click Assign Selected Users and in the next dialog box, choose Unassigned.
Step 4  Click Save.

What To Do Next
Export User Contact Lists, page 19-3
Export User Contact Lists

Complete this procedure to export the contact lists of the migrating from their current cluster.

**Procedure**

**Step 1**
Export the contact lists of the migrating users from the current home cluster.

a. Choose Cisco Unified Presence Administration > Bulk Administration > Contact List > Export.

b. Choose All unassigned users in the cluster and click Find.

c. Review the results and use the AND/OR filter to filter the search results as required.

d. When the list is complete, click Next.

e. Choose a filename for the exported contact list data.

f. Optionally update the Job Description.

g. Click Run Immediately or schedule the job to run later.

**Step 2**
Monitor the status of the contact list export job.

a. Choose Cisco Unified Presence Administration > Bulk Administration > Job Scheduler.

b. Click Find to list all BAT jobs.

c. Find your contact list export job and when it is reported as completed, choose the job.

d. Choose the CSV File Name link to view the contents of the contact list export file. Note that a timestamp is appended to the filename.

e. From the Job Results section, choose the log file to see the summary of what was exported. The job begin and end time is listed and a result summary for the job is presented.

**Step 3**
Download the contact list export file and store it for use later when the user migration is complete.


b. Click Find.

c. Choose the contact list export file and click Download Selected.

d. Save the CSV file locally for upload later in the procedure.

**What To Do Next**
Unlicense Users, page 19-4

**Unlicense Users**

The following procedure describes how to unlicense the migrating users for Cisco Unified Presence and Cisco Jabber on their current home cluster from Cisco Unified Communications Manager.
Move Users to the New Cluster

The procedure to move the users to the new cluster differs depending on whether LDAP Sync is enabled on Cisco Unified Communications Manager.

LDAP Sync Enabled on Cisco Unified Communications Manager

If LDAP Sync is enabled on Cisco Unified Communications Manager, you must move users to the new Organizational Unit and synchronize the users to the new home cluster.

Move Users to the New Organizational Unit

If LDAP Sync is enabled on Cisco Unified Communications Manager, you must move the users to the new Organizational Unit (OU) from which their new cluster synchronizes if the deployment uses a separate LDAP structure (OU divided) for each cluster, where users are only synchronized from LDAP to their home cluster.

Note

You do not need to move the users if the deployment uses a flat LDAP structure, that is, all users are synchronized to all Unified Communications Manager and Cisco Unified Presence clusters where users are licensed to only one cluster.

For more information about how to move the migrating users to the relevant OU of the new home cluster, see the LDAP Administration documentation.

After you move the users, you must delete the LDAP entries from the old LDAP cluster.

What To Do Next

Synchronize the Users to the New Home Cluster, page 19-5
Chapter 19      User Migration between Cisco Unified Presence Clusters

License the Users on the New Cluster

Synchronize the Users to the New Home Cluster

If LDAP is enabled on Cisco Unified Communications Manager, you must synchronize the users to the new home Cisco Unified Communications Manager cluster. You can do this manually on Cisco Unified Communications Manager or you can wait for a scheduled synchronization on Unified CM.

To manually force the synchronization on Cisco Unified Communications Manager, complete the following procedure.

**Procedure**

**Step 1**
From Cisco Unified Communications Manager, choose **System > LDAP > LDAP Directory**.

**Step 2**
Click **Perform Full Sync Now**.

**What To Do Next**
License the Users on the New Cluster, page 19-5

LDAP Sync not Enabled on Cisco Unified Communications Manager

If LDAP Sync is not enabled on Cisco Unified Communications Manager, you must manually provision the users on the new Unified Communications Manager cluster. See the *Cisco Unified Communications Manager Administration Guide* for more information.

**What To Do Next**
License the Users on the New Cluster, page 19-5

License the Users on the New Cluster

When the users have been synchronized, or manually provisioned, on the new home cluster, you must license the users for Cisco Unified Presence and Cisco Jabber.

**Procedure**

**Step 1**
From Cisco Unified Communications Manager Administration, choose **System > Licensing > Capabilities Assignment**.

**Step 2**
Choose the users that were migrated to the cluster and click **Bulk Assignment**.

**Step 3**
Use the Bulk Assignment Tool to license the users on their new home cluster.

**Step 4**
Provision the users on Cisco Unified Communications Manager for Phone and CSF. See the *Cisco Unified Communications Manager Administration Guide* for more information.
After you have licensed the users on the new cluster, Cisco recommends that you rebalance users on Cisco Unified Presence.

What To Do Next
Import Contact Lists on the New Home Cluster, page 19-6

Import Contact Lists on the New Home Cluster

You must import the contact lists to restore contact data for the migrated users.

Procedure

Step 1 Upload the previously exported contact list CSV file.
   b. Click Add New.
   c. Click Browse to locate and choose the contact list CSV file.
   d. Choose Contact Lists as the Target.
   e. Choose Import Users’ Contacts - Custom File as the Transaction Type,
   f. Optionally check Overwrite File if it exists.
   g. Click Save to upload the file.

Step 2 Run the import contact list job.
   a. Choose Cisco Unified Presence Administration > Bulk Administration > Contact List > Update.
   b. Choose the CSV file you uploaded in Step 1.
   c. Optionally update the Job Description.
   d. To run the job now, click Run Immediately. Choose Run Later to schedule the update for a later time.
   e. Click Submit.

Step 3 Monitor the contact list import status.
   a. Choose Cisco Unified Presence Administration > Bulk Administration > Job Scheduler.
   b. Click Find to list all BAT jobs.
   c. Choose the job ID of the contact list import job when its status is reported as complete.
   d. To view the contents of the contact list file, choose the file listed at CSV File Name.
   e. Click the Log File Name link to open the log.
      The begin and end time of the job is listed and a result summary is also displayed.
Multilingual Support Configuration

June 16, 2014

If you want to expand your Cisco Unified Presence deployment to support multiple languages, you must configure Cisco Unified Communications Manager and Cisco Unified Presence to support the user locales that you require. There is no limit to the number of supported languages.

- Install the Locale Installer on Cisco Unified Communications Manager, page 20-1
- Install the Locale Installer on Cisco Unified Presence, page 20-3
- Localized Applications, page 20-5

Install the Locale Installer on Cisco Unified Communications Manager

User locale files provide translated text for user applications and user web pages in the locale that the user chooses. User locales are country-specific.

Before You Begin

- Install Cisco Unified Communications Manager (Release 6.x or a higher release) on every server in the cluster before you install the Cisco Unified Communications Manager Locale Installer.

- If you want to use a locale other than English, you must install the appropriate language installers on both Cisco Unified Communications Manager and on Cisco Unified Presence. Ensure the locale installer is installed on every server in the cluster (install on the Publisher server before the Subscriber servers).

- User locales should not be set until all appropriate locale installers are loaded on both systems. Users may experience problems if they inadvertently set their user locale after the locale installer is loaded on Cisco Unified Communications Manager but before the locale installer is loaded on Cisco Unified Presence. If issues are reported, Cisco recommends that you notify each user to sign into Cisco Unified Communications Manager user options pages and change their locale from the current setting to English and then back again to the appropriate language. You can also use the BAT tool to synchronize user locales to the appropriate language.

- You must restart the servers for the changes to take effect. After you complete all locale installation procedures, restart each server in the cluster. Updates do not occur in the system until you restart all servers in the cluster; services restart after the server reboots.
### Chapter 20      Multilingual Support Configuration

#### Install the Locale Installer on Cisco Unified Communications Manager

**Procedure**

**Step 1** Perform one of the following actions to download the locale installer:

**Step 2**

<table>
<thead>
<tr>
<th>To download the locale installer from</th>
<th>Do this:</th>
</tr>
</thead>
</table>
| Plugin window in Cisco Unified Communications Manager Administration | a. Sign in to Cisco Unified Communications Manager Administration using the administrator account and password  
   b. Choose **Application > Install Plugins**.  
   c. Click the icon that represents the Cisco Unified Communications Manager Locale Installer.  
   d. Go to Step 2. |

**Step 3** Click the version of the Cisco Unified Communications Manager Locale Installer.

**Step 4** To download the installer file to the server, click **Download**.

**Step 5** After downloading the file, save the file to the hard drive and note the location of the saved file.

**Step 6** Double-click the file to begin the installation.

**Step 7** Perform these actions to complete the installation:

<table>
<thead>
<tr>
<th>Window</th>
<th>Configuration Steps</th>
</tr>
</thead>
</table>
| License Agreement Window      | a. Read and accept the license agreement.  
   b. Click **Next** to display the Readme Notes dialog. |
| Page 1 of 4                   | **Note** The readme notes contain build-time information such as components and devices that are supported in the released build. The readme may be printed for reference. Examine and accept the readme notes then click **Next** to proceed to the Setup Type dialog. |
| Setup Type Window             | a. Choose a custom setup type to allow you to select or deselect user locales as required.  
   b. Click **Next**. |
| Page 2 of 4                   |                     |
Step 8 When the installation is complete, a new dialog requests confirmation of a restart. Should you wish to apply another locale installer, repeat this procedure before restarting the server in order to reduce downtime.

Step 9 Click Finish. The Setup dialog box displays. Do not click any buttons or press any keys.

Step 10 When the dialog box automatically closes, you have completed the installation on the server. Install the Cisco Unified Communications Manager Locale Installer on every server in the cluster.

Note Make sure that you install the same components on every server in the cluster.

Step 11 After you complete all locale installation procedures, complete these actions:
   a. Run the following command on the CLI: run sql update enduser set cucm_cdrtime=0
   b. Restart the Sync Agent service in Cisco Unified Serviceability (choose Tools > Service Activation).
   c. Restart each server in the cluster.

Step 12 Verify that your users can choose the locale(s) for supported products.

What To Do Next
Install the Locale Installer on Cisco Unified Presence, page 20-3

Install the Locale Installer on Cisco Unified Presence

Before You Begin
- Install the Locale Installer on Cisco Unified Communications Manager. If you want to use a locale other than English, you must install the appropriate language installers on both Cisco Unified Communications Manager and on Cisco Unified Presence.
- If your Cisco Unified Presence cluster has more than one node, make sure that the locale installer is installed on every server in the cluster (install on the Publisher server before the Subscriber servers).
- User locales should not be set until all appropriate locale installers are loaded on both systems. Users may experience problems if they inadvertently set their user locale after the locale installer is loaded on Cisco Unified Communications Manager but before the locale installer is loaded on Cisco Unified Presence. If issues are reported, Cisco recommends that you notify each user to sign into Cisco Unified Communications Manager user options pages and change their locale from the current setting to English and then back again to the appropriate language. You can also use the BAT tool to synchronize user locales to the appropriate language.
Install the Locale Installer on Cisco Unified Presence

You must restart the server for the changes to take effect. After you complete all locale installation procedures, restart each server in the cluster. Updates do not occur in the system until you restart all servers in the cluster; services restart after the server reboots.

Procedure

Step 1 Browse to this location on cisco.com to locate the Cisco Unified Presence locale installer:

Step 2 Click the version of the Cisco Unified Presence Locale Installer that is appropriate for your working environment.

Step 3 After downloading the file, save the file to the hard drive and note the location of the saved file.

Step 4 Copy this file to a server that supports SFTP.

Step 5 Sign into Cisco Unified OS Administration using the administrator account and password.

Step 6 Choose **Software Upgrades > Install/Upgrade**.

Step 7 Choose Remote File System as the software location source.

Step 8 Enter the file location, for example /tmp, in the Directory field.

Step 9 Enter the Cisco Unified Presence server name in the Server field.

Step 10 Enter your username and password credentials in the User Name and User Password fields.

Step 11 Choose SFTP for the Transfer Protocol.

Step 12 Click **Next**.

Step 13 Choose the Cisco Unified Presence locale installer from the list of search results.

Step 14 Click **Next** to load the installer file and validate it.

Step 15 After you complete the locale installation, restart each server in the cluster.

Note Make sure that you install the same components on every server in the cluster.

Step 16 The default setting for installed locales is “English, United States”. While your Cisco Unified Presence server is restarting, change the language of your browser, if necessary, to match the locale of the installer that you have downloaded.
Chapter 20  Multilingual Support Configuration

Localized Applications

Cisco Unified Presence does not currently support Safari browser.

Step 17 Verify that your users can choose the locale(s) for supported products.

Related Topics
Localized Applications, page 20-5

Localized Applications

Cisco Unified Presence applications support a variety of different languages. See Table 20-1 for a list of localized applications and the available languages.
### List of Localized Applications and Supported Languages

<table>
<thead>
<tr>
<th>Interface</th>
<th>Supported Languages</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>End User Applications</strong></td>
<td></td>
</tr>
<tr>
<td>IP Phone Messenger</td>
<td>Arabic (Algeria, Bahrain, Egypt, Iraq, Jordan, Kuwait, Lebanon, Morocco, Oman, Qatar, Saudi Arabia, Tunisia, United Arab Emirates, Yemen)</td>
</tr>
<tr>
<td>User Options</td>
<td>Bulgarian, Catalan (Spain), Chinese (China, Hong Kong, Taiwan), Croatian, Czech (Czech Republic), Danish (Denmark), Dutch (Netherlands), English, Estonian (Estonia), Finnish (Finland), French (France), German (Germany), Greek (Greece), Hebrew (Israel), Hungarian (Hungary), Italian (Italy), Japanese (Japan), Korean (Korean Republic), Latvian (Latvia), Lithuanian (Lithuania), Norwegian (Norway), Polish (Poland), Portuguese (Brazil, Portugal), Romanian (Romania), Russian (Russian Federation), Serbian (Republics of Montenegro and Serbia), Slovak (Slovakia), Slovenian (Slovenia), Spanish (Columbia and Spain), Swedish (Sweden), Thai (Thailand), Turkish (Turkey)</td>
</tr>
</tbody>
</table>

| **Administrative Applications** |                                                                                      |
| Administration                | Chinese (China), English, Japanese (Japan), Korean (Korean Republic)                  |
| OS                             | Chinese (China), English, Japanese (Japan), Korean (Korean Republic)                  |
P A R T  5

Troubleshooting

- Troubleshooting High Availability
- Troubleshooting a Cisco Unified Presence Multi-node Deployment
- Troubleshooting Single Sign-On
- General Troubleshooting Tasks
Troubleshooting High Availability

June 16, 2014

- Node States, Causes and Recommended Actions, page 21-1

Node States, Causes and Recommended Actions

Table 21-1 describes the node states, reasons, causes, and recommended actions for failed states.

<table>
<thead>
<tr>
<th>Node 1 State</th>
<th>Node 1 Reason</th>
<th>Node 2 State</th>
<th>Node 2 Reason</th>
<th>Cause/Recommended Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Normal</td>
<td>Normal</td>
<td>Normal</td>
<td>Normal</td>
<td>High Availability is running on both nodes in the subcluster. Subcluster is running normally (it is in non failover mode). The critical services on both nodes in the subcluster are running.</td>
</tr>
<tr>
<td>Failing Over</td>
<td>On Admin Request</td>
<td>Taking Over</td>
<td>On Admin Request</td>
<td>The administrator initiates a manual failover from node 1 to node 2. The manual failover is in progress.</td>
</tr>
<tr>
<td>Idle</td>
<td>On Admin Request</td>
<td>Running in</td>
<td>On Admin Request</td>
<td>The manual failover from node 1 to node 2 (initiated by the administrator) is complete.</td>
</tr>
<tr>
<td>Taking Back</td>
<td>On Admin Request</td>
<td>Falling Back</td>
<td>On Admin Request</td>
<td>The administrator initiates a manual fallback from node 2 to node 1. The manual fallback is in progress.</td>
</tr>
<tr>
<td>Idle</td>
<td>Initialization</td>
<td>Running in</td>
<td>On Admin Request</td>
<td>The administrator restarts the SRM service on node 1 while node 1 is in Idle state.</td>
</tr>
<tr>
<td>Idle</td>
<td>Initialization</td>
<td>Running in</td>
<td>Initialization</td>
<td>The administrator restarts both nodes in the subcluster, or restarts the SRM service on both nodes in the subcluster, while the subcluster was in manual failover mode (failover initiated by the administrator).</td>
</tr>
<tr>
<td>Idle</td>
<td>On Admin Request</td>
<td>Running in</td>
<td>Initialization</td>
<td>The administrator restarts the SRM service on node 2 while node 2 is running in backup mode, but before the heartbeat on node 1 times out.</td>
</tr>
</tbody>
</table>
Table 21-1  Node High Availability states, causes and recommended actions (continued)

<table>
<thead>
<tr>
<th>Node 1 State</th>
<th>Reason</th>
<th>Node 2 State</th>
<th>Reason</th>
<th>Cause/Recommended Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failing Over</td>
<td>On Admin Request</td>
<td>Taking Over</td>
<td>Initialization</td>
<td>The administrator restarts the SRM service on node 2 while node 2 is taking over, but before the heartbeat on node 1 times out.</td>
</tr>
<tr>
<td>Taking Back</td>
<td>Initialization</td>
<td>Falling Back</td>
<td>On Admin Request</td>
<td>The administrator restarts the SRM service on node 1 while taking back, but before the heartbeat on node 2 times out. After the taking back process is complete, both nodes are in Normal state.</td>
</tr>
<tr>
<td>Taking Back</td>
<td>Automatic Fallback</td>
<td>Falling Back</td>
<td>Automatic Fallback</td>
<td>Automatic Fallback has been initiated from node 2 to node 1 and is currently in progress.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td><strong>Note:</strong> This state applies to Cisco Unified Presence Release 8.6(4) and later only.</td>
</tr>
<tr>
<td>Failed Over</td>
<td>Initialization or Critical</td>
<td>Running in Backup Mode</td>
<td>Critical Service Down</td>
<td>Node 1 transitions to Failed Over state when:</td>
</tr>
<tr>
<td></td>
<td>Services Down</td>
<td></td>
<td></td>
<td>– Critical service(s) come back up due to reboot of node 1, or</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>– The administrator starts critical service(s) on node1 while node1 is in &quot;Failed Over with Critical Services Not Running&quot; state</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>When node1 transitions to Failed Over state the node is ready for the administrator to perform a manual fallback to restore the nodes in the subcluster to Normal state.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td><strong>Recommended Actions:</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1. Check what critical services are down on node 1, and try to start these services manually.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>2. If the critical services on node 1 do not start, reboot node 1.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>3. After the reboot and when all the critical services are running, perform a manual fallback to restore the nodes in the subcluster to Normal state.</td>
</tr>
<tr>
<td>Failed Over</td>
<td>Database Failure</td>
<td>Running in Backup Mode</td>
<td>Database Failure</td>
<td>A database service is down on node 1. Cisco Unified Presence performs an automatic failover to node 2.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td><strong>Recommended Actions:</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1. Reboot Node 1.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>2. After the reboot and when all the critical services are running, perform a manual fallback to restore the nodes in the subcluster to Normal state.</td>
</tr>
</tbody>
</table>
### Table 21-1  Node High Availability states, causes and recommended actions (continued)

<table>
<thead>
<tr>
<th>Node 1</th>
<th>Reason</th>
<th>Node 2</th>
<th>Reason</th>
<th>Cause/Recommended Actions</th>
</tr>
</thead>
</table>
| Running in Failed Mode | Start of Critical Services Failed | Running in Failed Mode | Start of Critical Services Failed | Critical services fail to start while a node in subcluster is taking back from the other node. **Recommended Actions:** (on the node that is taking back)  
1. Check what critical services are down on the node. To start these services manually, choose **Recovery** on the subcluster details screen.  
2. If the critical services do not start, reboot the node.  
3. After the reboot and when all the critical services are running, perform a manual fallback to restore the nodes in the subcluster to Normal state. |
| Running in Failed Mode | Critical Service Down | Running in Failed Mode | Critical Service Down | Critical services go down while a node in subcluster is running in backup mode for the other node. **Recommended Actions:**  
1. Check what critical services are down on backup node. To start these services manually, choose **Recovery** on the subcluster details screen.  
2. If the critical services do not start, reboot the subcluster. |
| **Node1 is down due to loss of network connectivity or the SRM service is not running.** | Running in Backup Mode | Peer Down | Node2 has lost its heartbeat with node 1. Cisco Unified Presence performs an automatic failover to node 2. **Recommended Action:**  
(If node 1 is up)  
1. Check and repair the network connectivity between nodes in the subcluster. When you reestablish the network connection between the nodes, the node may go into a failed state. Choose **Recovery** on the subcluster details screen to restore the nodes in the subcluster to Normal state.  
2. Start the SRM service, and perform manual fallback to restore the nodes in the subcluster to Normal state. (If the node is down)  
1. Repair/Power up node1.  
2. When node is up and all critical services are running, perform manual fallback to restore the nodes in the subcluster to Normal state. |
### Configuration and Administration of Cisco Unified Presence Release 8.6

#### Chapter 21  Troubleshooting High Availability

### Node States, Causes and Recommended Actions (continued)

<table>
<thead>
<tr>
<th>Node 1</th>
<th>Node 2</th>
<th>Cause/Recommended Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Node 1 is down (due to possible power down, hardware failure, shutdown, reboot)</strong></td>
<td>Running in Backup Mode</td>
<td>Cisco Unified Presence performs an automatic failover to node 2 due to possible hardware failure/power down/restart/shutdown of Node 1.</td>
</tr>
<tr>
<td><strong>Running in Failed Mode</strong></td>
<td>Running in Failed Mode</td>
<td>Recommended Action:</td>
</tr>
<tr>
<td><strong>Failed Over with Critical Services not Running OR Failed Over</strong></td>
<td>Peer Down During Initialization</td>
<td>1. Repair/Power up node 1.</td>
</tr>
<tr>
<td><strong>Running in Failed Mode</strong></td>
<td>Peer Down During Initialization</td>
<td>2. When node is up and all critical services are running, perform manual fallback to restore the nodes in the subcluster to Normal state.</td>
</tr>
<tr>
<td><strong>Running in Failed Mode</strong></td>
<td>Peer Down During Initialization</td>
<td>User move fails during taking over process.</td>
</tr>
<tr>
<td><strong>Backup Activated</strong></td>
<td>Peer Down During Initialization</td>
<td><strong>Recommended Action:</strong></td>
</tr>
<tr>
<td><strong>Auto Recover Database Failure</strong></td>
<td>Peer Down During Initialization</td>
<td>Possible database error. Choose Recovery on the subcluster details screen. If that doesn't resolve the issue, reboot the subcluster.</td>
</tr>
<tr>
<td><strong>Backup Activated</strong></td>
<td>Peer Down During Initialization</td>
<td>Possible database error. Choose Recovery on the subcluster details screen. If that doesn't resolve the issue, reboot the subcluster.</td>
</tr>
<tr>
<td><strong>Backup Activated</strong></td>
<td>Peer Down During Initialization</td>
<td>A critical service goes down on the backup node. The peer node is in failover mode and can take over for all users in the subcluster. Auto-recovery operation automatically occurs and all users are moved over to the primary node.</td>
</tr>
</tbody>
</table>

---

### Table 21-1  Node High Availability states, causes and recommended actions (continued)

<table>
<thead>
<tr>
<th>State</th>
<th>Reason</th>
<th>State</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>Node 1</td>
<td>Running in Backup Mode</td>
<td>Node 2</td>
<td>Peer Reboot</td>
</tr>
<tr>
<td><strong>Failed Over with Critical Services not Running OR Failed Over</strong></td>
<td>Peer Down During Initialization</td>
<td><strong>Backup Activated</strong></td>
<td>Peer Down During Initialization</td>
</tr>
<tr>
<td><strong>Running in Failed Mode</strong></td>
<td>Peer Down During Initialization</td>
<td><strong>Backup Activated</strong></td>
<td>Peer Down During Initialization</td>
</tr>
<tr>
<td><strong>Backup Activated</strong></td>
<td>Peer Down During Initialization</td>
<td><strong>Backup Activated</strong></td>
<td>Peer Down During Initialization</td>
</tr>
<tr>
<td><strong>Backup Activated</strong></td>
<td>Peer Down During Initialization</td>
<td><strong>Backup Activated</strong></td>
<td>Peer Down During Initialization</td>
</tr>
</tbody>
</table>
Troubleshooting a Cisco Unified Presence Multi-node Deployment

June 16, 2014

- Monitor a Multi-node System, page 22-1
- Resolve a Hardware Problem, page 22-2
- Cisco UP Replication Watcher Service, page 22-3

Monitor a Multi-node System

Restriction
If you need to add hardware to your multi-node deployment, the hardware must comply with the multi-node hardware recommendations.

Procedure

Step 1 Use the Cisco Unified Presence Real-Time Monitoring Tool (RTMT) tool to monitor the CPU and memory usage of each Cisco Unified Presence node in the cluster.

Step 2 Use these guidelines to determine if you need additional hardware:
Resolve a Hardware Problem

Follow this procedure if there is a problematic server, or some general hardware failure.

Restrictions

If you need to add hardware to your multi-node deployment, the hardware must comply with the multi-node hardware recommendations.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Create a new node in system topology management GUI.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Perform a fresh installation on this node.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Unassign the users from the problematic node.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Stop all services on the problematic node.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Unassign the problematic node.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Assign the new node to the subcluster, replacing the problematic node.</td>
</tr>
<tr>
<td>Step 7</td>
<td>Reassign the unassigned users to the new node.</td>
</tr>
<tr>
<td>Step 8</td>
<td>Delete the problematic node.</td>
</tr>
</tbody>
</table>
**Step 9** Activate all services on the new node.

**Troubleshooting Tip**
You must turn off High Availability in a subcluster before you move or unassign a node in that subcluster.

**Related Topics**
- Clustering over WAN for Intracluster and Intercluster Deployments, page 2-4
- Create, Assign and Move Nodes in System Topology, page 17-10
- Configure User Assignment in System Topology, page 15-1

---

**Cisco UP Replication Watcher Service**

**Note** This section is only applicable to Cisco Unified Presence Release 8.5.x or higher.

The Cisco UP Replication Watcher monitors user database replication state on Cisco Unified Presence. Other Cisco Unified Presence services are dependent on the Cisco UP Replication Watcher service. These dependent services use the Cisco UP Replication Watcher service to delay startup until such time as user database replication is in a stable state.

On the subscriber nodes, the Cisco UP Replication Watcher service delays the startup of feature services until user database replication is successfully established. The Cisco UP Replication Watcher service only delays the startup of feature services on the problem subscriber node in a cluster, it will not delay the startup of feature services on all subscriber nodes due to one problem node. For example, if user database replication is successfully established on node1 and node2, but not on node3, the Cisco UP Replication Watcher service allows feature services to start on node1 and node2, but delays feature service startup on node3.

The Cisco UP Replication Watcher service behaves differently on the publisher node. It only delays the startup of feature services until a timeout expires. When the timeout expires, it allows all feature services to start on the publisher node even if user database replication is not successfully established.

The Cisco UP Replication Watcher service generates an alarm when it delays feature service startup on a node. It then generates a notification when user database replication is successfully established on that node.

The Cisco UP Replication Watcher service impacts both a fresh multi-node installation, and a software upgrade procedure. Both will only complete when the publisher and subscriber nodes are running the same Cisco Unified Presence release, and user database replication is successfully established on the subscriber nodes.

To check the status of the IDS replication on a node either:

- **Use this CLI command:**
  
  ```shell
  utils dbreplication runtimestate
  ```

- **Use the Cisco Unified Reporting Tool (CURT).** The ‘Unified CUP Database Status’ report displays a detailed status of the cluster.

**Related Topics**
- Add a New Node, page 17-7
• Upgrade from Cisco Unified Presence Release 7.0(x) to Release 8.5(x). For more information, see the *Upgrade Guide for Cisco Unified Presence Release 8.6*. 
Troubleshooting Single Sign-On

June 16, 2014

- "Invalid Profile Credentials" Message, page 23-1
- "Module Name Is Invalid" Message, page 23-2
- Web Browser Indicates a 401 Error, page 23-2
- Web Browser Indicates a 403 Error or Displays a Blank Screen, page 23-2
- "User Is Not Authorized to Perform This Function" Error, page 23-3
- Web Browser Indicates an HTTP 404 Error, page 23-3
- Web Browser Indicates an HTTP 500 Error or Displays a Blank Screen, page 23-3
- "Authentication Failed" Message, page 23-4
- Web Browser Displays an OpenAM Login Screen, page 23-4
- Web Browser Displays Cisco Unified Presence Login Screen, page 23-4
- Internet Explorer Prompts for Username and Password, page 23-5
- "User has no Profile on this Organization" Message, page 23-5
- Certificate Failure, page 23-6

"Invalid Profile Credentials" Message

Problem
When enabling SSO, an “Invalid Profile Credentials” message displays.

Possible Cause
You may be specifying the incorrect name and password for the Cisco Unified Presence node J2EE Agent.

Solution
Refer to Configure J2EE Agent Profile on OpenAM, page 16-22 and note the name and password values that were entered. These values must be specified when enabling SSO.
"Module Name Is Invalid" Message

**Problem**
When enabling SSO, a “Module Name is Invalid” message displays.

**Possible Cause**
You may be specifying the incorrect name for the SSO Module Instance.

**Solution**
Refer to Configure Single Sign-On Module Instance, page 16-21 and review the instructions.

"Invalid OpenAM Access Manager (OpenAM) Server URL" Message

**Problem**
When enabling SSO, an “Invalid OpenAM Access Manager (Openam) Server URL” message displays.

**Possible Cause**
The OpenAM URL that is specified on the GUI or CLI when you enable SSO may not be correct.

**Solution**
Ensure that the correct OpenAM URL is being specified on the GUI or CLI when you enable SSO. The OpenAM URL must be the Fully Qualified Domain Name with the port number. For example, https://server1.cisco.com:8443/opensso. You must also ensure that the OpenAM server is up and running and that the OpenAM administration GUI is accessible.

Web Browser Indicates a 401 Error

**Problem**
When accessing an SSO-enabled web application for a Cisco Unified Presence node, the web browser indicates an HTTP 401 error code.

**Possible Cause**
There may be a problem with the user’s browser settings.

**Solution**
Refer to Client Browser Configuration for Single Sign-On, page 16-5 and review instructions.

Web Browser Indicates a 403 Error or Displays a Blank Screen

**Problem**
When accessing an SSO-enabled web application for a Cisco Unified Presence node, the web browser indicates an HTTP 403 error code or I get a blank screen.

**Possible Cause**
There may be a problem with OpenAM policy configuration for this Cisco Unified Presence node.
Solution
Ensure that you have added all six policy rules for this Cisco Unified Presence node and that all policy rules have been enabled with GET/POST actions and are set to Allow. You must also ensure that the Subject has been added to the policy. For more information, see Set up Policies on OpenAM Server, page 16-19.

"User Is Not Authorized to Perform This Function" Error

Problem
After accessing the web application and trying to access a page, the following message displays: “User is not authorized to perform this function.”

Possible Cause
There may be a problem with the user’s assigned permissions for Cisco Unified Presence.

Solution
If accessing the User Options web application is failing, ensure that the user is a member of the Standard CCM End User group on the corresponding Cisco Unified Communications Manager node. If access to any other Cisco Unified Presence web applications is failing, ensure that the user is a member of the Standard CUP Super Users group or a group with the equivalent roles on this Cisco Unified Presence node.

Web Browser Indicates an HTTP 404 Error

Problem
When accessing an SSO-enabled web application for a Cisco Unified Presence node, the web browser indicates an HTTP 404 error code.

Possible Cause
There may be a problem with one of the following configurations for this Cisco Unified Presence node: OpenAM policy configuration or OpenAM J2EE Agent configuration.

Solution
Ensure you are not attempting to access this Cisco Unified Presence node using a URL that contains the hostname only, because this method is not supported when SSO is enabled for a web application. Refer to section Set up Policies on OpenAM Server, page 16-19 and review the policy rules for this Cisco Unified Presence node. See Configure J2EE Agent Profile on OpenAM, page 16-22 and review the steps related to Login Processing. You must also ensure that you have added the Login Processing URIs to the Cisco Unified Presence J2EE Agent configuration on the OpenAM server.

Web Browser Indicates an HTTP 500 Error or Displays a Blank Screen

Problem
When accessing an SSO-enabled web application for a Cisco Unified Presence node, the web browser indicates an HTTP 500 error code or a blank screen displays.
Possible Cause
There may be a problem with OpenAM J2EE Agent configuration for this Cisco Unified Presence node.

Solution
Refer to Configure J2EE Agent Profile on OpenAM, page 16-22 and complete the following tasks: You must ensure that you have added the Login Processing URLs for the J2EE Agent for this node and that you have added the Login URL on the OpenSSO Service tab and removed all other Login URLs.

"Authentication Failed" Message

Problem
When accessing an SSO-enabled web application for a Cisco Unified Presence node, the web browser displays an OpenAM login screen with an “Authentication failed” message.

Possible Cause
There may be a problem with the WindowsDesktopSSO login module.

Solution
Refer to Configure Single Sign-On Module Instance, page 16-21 and review the instructions to ensure that all the Module Instance settings are correct, the keytab file exists at the specified directory, and the clocks are synchronized on the user’s Windows PC, the Active Directory, the OpenAM Server and Cisco Unified Presence node.

Web Browser Displays an OpenAM Login Screen

Problem
When accessing an SSO-enabled web application for a Cisco Unified Presence node, the web browser displays an OpenAM login screen.

Possible Cause
There may be a problem with OpenAM J2EE Agent configuration for this Cisco Unified Presence node.

Solution
Refer to Configure J2EE Agent Profile on OpenAM, page 16-22 and ensure that you have added the Login URL on the OpenSSO Service tab and removed all other Login URLs.

Web Browser Displays Cisco Unified Presence Login Screen

Problem
When accessing an SSO-enabled web application for a Cisco Unified Presence node, the web browser displays the web application login screen.

Possible Cause
There may be a problem with OpenAM J2EE Agent configuration for this Cisco Unified Presence node.
Solution
Refer to Configure J2EE Agent Profile on OpenAM, page 16-22 and ensure that you have added the Login Processing URLs for this Cisco Unified Presence nodes J2EE Agent.

Internet Explorer Prompts for Username and Password

Problem
When accessing an SSO-enabled web application for a Cisco Unified Presence node, the Internet Explorer web browser prompts you for a username and password.

Possible Cause
There may be a problem with the user's browser settings.

Solution
Refer to Client Browser Configuration for Single Sign-On, page 16-5 and review the instructions.

"User has no Profile on this Organization" Message

Problem
When accessing an SSO-enabled web application for a Cisco Unified Presence node, the web browser displays an OpenAM screen with a "User has no profile on this organization" message.

Possible Cause
The OpenAM User Profile may not be set to ignored.

Solution
Refer to the section for Set up OpenAM using the GUI Configurator, page 16-17.

Problems Enabling Single Sign-On

Problem
You are unable to enable the SSO feature.

Possible Cause
If the Tomcat instance on which the OpenAM server is deployed becomes unresponsive or shuts down unexpectedly, you may not be able to enable the SSO feature on Cisco Unified Presence. In order to enable SSO successfully on Cisco Unified Presence, OpenAM must be operational. Cisco Unified Presence does not monitor the OpenAM Tomcat instance. As a result, no Cisco Unified Presence alarm or notification is generated for this occurrence.

Solution
If you experience difficulty when enabling SSO from either the Cisco Unified Presence Operating System Administration GUI or the Cisco Unified Presence Administration CLI, verify that Tomcat is running on the OpenAM server. If you continue to experience difficulty after verifying that Tomcat is running on the OpenAM server, restart Tomcat on the OpenAM server and try enabling SSO again.
When Tomcat crashes on the OpenAM server, OpenAM becomes unresponsive. Cisco Unified Presence may not be notified.

Certificate Failure

**Problem**
When using the Certificate Import Tool to validate the communication between OpenAM and Cisco Unified Presence, you may encounter an error with the “Verify SSL connectivity to the specified certificate server” test. This test may fail with the following error: “The Troubleshooter has encountered an internal error”.

**Possible Cause**
This error may be the result of the way the OpenAM/Tomcat instance has configured its HTTP Connector.

**Solution**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Locate the server.xml configuration file on the OpenAM/Tomcat server. This file is typically located here:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>C:\Program Files\Apache Software Foundation\Tomcat 7.0\conf\server.xml.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Check the value set for the <code>clientAuth</code> attribute of the <code>Connector</code> with a port value of 8443. If this attribute is set to true, this can cause the Certificate Import Tool to fail.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Change the <code>clientAuth</code> attribute to <code>want</code> or <code>false</code>.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Restart the Tomcat service on the OpenAM server.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Re-run the Certificate Import Tool and return to Step 7 of Import the OpenAM Certificate into Cisco Unified Presence, page 16-25.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Change the <code>clientAuth</code> attribute back to its original value.</td>
</tr>
<tr>
<td>Step 7</td>
<td>Restart the Tomcat service on the OpenAM server.</td>
</tr>
</tbody>
</table>
Chapter 24

General Troubleshooting Tasks

June 16, 2014

- When to Restart Services, page 24-1
- System Troubleshooter, page 24-1
- CUPC Server Health, page 24-1
- Certificate Import Tool, page 24-2
- Intercluster Peer Connection Failed, page 24-2

When to Restart Services

If you modify the DNS entry of the Publish SIP Trunk SRV record by changing the port number or IP address, you must restart all devices that previously published to that address and ensure each device points to the correct Cisco Unified Presence contact.

System Troubleshooter

Choose Cisco Unified Presence Administration > Diagnostics > System Troubleshooter to verify the status of your topology configuration.

The System Troubleshooter indicates if there are any two node subclusters without High Availability turned on. Choose Cisco Unified Presence Administration > Diagnostics > System Troubleshooter. The System Troubleshooter in Cisco Unified Presence Administration indicates if there are users who have reached the maximum contact list size.

CUPC Server Health

You can see the LDAP server information and attribute mappings in the Server Health window in Cisco Unified Personal Communicator (Help > Show Server Health on Windows and Help > Show System Diagnostics on Mac OS).
Certificate Import Tool

You can use the certificate import tool to check the communication with the LDAP server hostname/port after you upload the certificate for the LDAP server. Choose Cisco Unified Presence Administration > System > Security > Certificate Import Tool.

Intercluster Peer Connection Failed

If you configured the intercluster peer connection before the Sync Agent completes the user synchronization from Cisco Unified Communications Manager (on either the local or remote cluster), the status of the intercluster peer connection will display as failed.
PART 6

Appendix

- High Availability Client Login Profiles
- XMPP Standards Compliance
- Glossary of Terms
High Availability Client Login Profiles

June 16, 2014

- How to use High Availability Login Profiles, page I-1
- 2 GB Active/Active Profile, page I-3
- 2 GB Active/Standby Profile, page I-4
- 4 GB Active/Active Profile, page I-4
- 4 GB Active/Standby Profile, page I-5
- 6 GB Active/Active Profile, page I-5
- 6 GB Active/Standby Profile, page I-8

How to use High Availability Login Profiles

- Important Notes about High Availability Login Profiles, page I-1
- Using the High Availability Login Profile Tables, page I-2
- Example High Availability Login Configurations, page I-3

Important Notes about High Availability Login Profiles

- The High Availability login profiles only apply to Cisco Unified Presence Release 8.5 or higher 8.x releases, and Cisco Unified Personal Communicator Release 8.5 or higher 8.x releases.
- You can use the High Availability login profile tables in this section to configure the upper and lower client re-login values for your subcluster. You configure the upper and lower client login values by choosing Cisco Unified Presence Administration > System > Service Parameters, and choosing Cisco UP Server Recovery Manager from the Service menu.
- By configuring the upper and lower client re-login limits on your subcluster based on the tables we provide here, you can avoid performance issues and high CPU spikes in your deployment.
- We provide a High Availability login profile for each Cisco Unified Presence server memory size (2, 4 or 6 GB), and for each High Availability deployment type, active/active or active/standby.
- The High Availability login profile tables are calculated based on the following inputs:
How to use High Availability Login Profiles

Configuration and Administration of Cisco Unified Presence Release 8.6

Appendix I       High Availability Client Login Profiles

How to use High Availability Login Profiles

– The Users Moved Per Iteration service parameter. This parameter determines the number of users moved per iteration during a failover or a fallback operation. We provide a recommended value for the Users Moved Per Iteration service parameter for each High Availability login profile table.

– The total number of users in the subcluster for Active/Standby deployments, or the node with highest number of users for Active/Active deployments.

• You must configure the upper and lower client re-login limit values, and the Users Moved Per Iteration service parameter on both nodes in a subcluster. You must manually configure all these values on both nodes in the subcluster.

• The upper and lower client re-login limit values must be the same on each node in the subcluster.

• If you rebalance your users, you must reconfigure the upper and lower client re-login limit values based on the High Availability login profile tables.

Related Topic
Configure the Advanced Service Parameters for the Server Recovery Manager, page 17-18

Using the High Availability Login Profile Tables

Use the High Availability login profile tables to retrieve the following values:

• Client Re-Login Lower Limit service parameter value

• Client Re-Login Upper Limit service parameter value.

• Users Moved Per Iteration service parameter value.

Procedure

Step 1 Choose a profile table based on your memory size, and your High Availability deployment type.

Step 2 In the profile table, choose the number of users in your deployment (round up to the nearest value). If you have an active/standby deployment, use the node with the highest number of users.

Step 3 Based on the Number of Users value for your subcluster, retrieve the corresponding lower and upper retry limits in the profile table.

Step 4 Configure the lower and upper retry limits on Cisco Unified Presence by choosing Cisco Unified Presence Administration > System > Service Parameters, and choosing Cisco UP Server Recovery Manager from the Service menu.

Step 5 Retrieve the corresponding Users Moved Per Iteration service parameter value for your High Availability login profile table.

Step 6 Configure the Users Moved Per Iteration value on Cisco Unified Presence by choosing Cisco Unified Presence Administration > System > Service Parameters, and choosing Cisco UP Server Recovery Manager from the Service menu.

Related Topic
Example High Availability Login Configurations, page I-3
Example High Availability Login Configurations

Example 1: 6GB active/standby standard deployment
You have 3,000 users in your subcluster, with 2000 users on one node, and 1000 users on the second node. For active/standby deployments, Cisco recommends you use the node with the highest number of users, in this case the node with 2000 users. Using Table I-12, you retrieve these lower and upper retry values:

<table>
<thead>
<tr>
<th>Number of Users</th>
<th>Lower Retry Limit</th>
<th>Upper Retry Limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>2000</td>
<td>40</td>
<td>107</td>
</tr>
</tbody>
</table>

Note
The upper retry limit is the approximate time (seconds) it takes for all clients to login to their backup node after a failover occurs.

You also configure the corresponding Users Moved per Iteration service parameter value for Table I-12 which is 50.

Example 2: 4GB active/active IM-only deployment
You have 6800 users on the first node in your subcluster in an IM-only deployment. Cisco recommends that you round up to the nearest value, so using Table I-4 you retrieve the lower and upper retry value based on a number of users value of 7000:

<table>
<thead>
<tr>
<th>Number of Users</th>
<th>Lower Retry Limit</th>
<th>Upper Retry Limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>7000</td>
<td>280</td>
<td>1447</td>
</tr>
</tbody>
</table>

You also configure the corresponding Users Moved per Iteration service parameter value for Table I-4 which is 25.

2 GB Active/Active Profile
Corresponding Users Moved per Iteration service parameter value: 6

<table>
<thead>
<tr>
<th>Number of Users</th>
<th>Lower Retry Limit</th>
<th>Upper Retry Limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>100</td>
<td>17</td>
<td>83</td>
</tr>
<tr>
<td>250 (Default)</td>
<td>42 (Default)</td>
<td>208 (Default)</td>
</tr>
<tr>
<td>500</td>
<td>83</td>
<td>417</td>
</tr>
</tbody>
</table>
2 GB Active/Standby Profile

Corresponding Users Moved per Iteration service parameter value: 6

<table>
<thead>
<tr>
<th>Number of Users</th>
<th>Lower Retry Limit</th>
<th>Upper Retry Limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>100</td>
<td>17</td>
<td>57</td>
</tr>
<tr>
<td>250</td>
<td>42</td>
<td>142</td>
</tr>
<tr>
<td>500</td>
<td>83</td>
<td>283</td>
</tr>
<tr>
<td>750</td>
<td>125</td>
<td>425</td>
</tr>
<tr>
<td>1000</td>
<td>167</td>
<td>567</td>
</tr>
</tbody>
</table>

4 GB Active/Active Profile

Corresponding Users Moved per Iteration service parameter value: 25

<table>
<thead>
<tr>
<th>Number of Users</th>
<th>Lower Retry Limit</th>
<th>Upper Retry Limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>100</td>
<td>4</td>
<td>21</td>
</tr>
<tr>
<td>500 (Default)</td>
<td>20 (Default)</td>
<td>103 (Default)</td>
</tr>
<tr>
<td>1000</td>
<td>40</td>
<td>207</td>
</tr>
<tr>
<td>1500</td>
<td>60</td>
<td>310</td>
</tr>
<tr>
<td>2000</td>
<td>80</td>
<td>413</td>
</tr>
<tr>
<td>2500</td>
<td>100</td>
<td>517</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Number of Users</th>
<th>Lower Retry Limit</th>
<th>Upper Retry Limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>3000</td>
<td>120</td>
<td>620</td>
</tr>
<tr>
<td>3500</td>
<td>140</td>
<td>723</td>
</tr>
<tr>
<td>4000</td>
<td>160</td>
<td>827</td>
</tr>
<tr>
<td>4500</td>
<td>180</td>
<td>930</td>
</tr>
<tr>
<td>5000</td>
<td>200</td>
<td>1033</td>
</tr>
<tr>
<td>6000</td>
<td>240</td>
<td>1240</td>
</tr>
<tr>
<td>7000</td>
<td>280</td>
<td>1447</td>
</tr>
<tr>
<td>7500</td>
<td>300</td>
<td>1550</td>
</tr>
</tbody>
</table>
4 GB Active/Standby Profile

Corresponding Users Moved per Iteration service parameter value: 25

<table>
<thead>
<tr>
<th>Table I-5, Part 1</th>
<th>User login retry limits for standard deployment (4GB active/standby)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of Users</td>
<td>Lower Retry Limit</td>
</tr>
<tr>
<td>100</td>
<td>4</td>
</tr>
<tr>
<td>500</td>
<td>20</td>
</tr>
<tr>
<td>1000</td>
<td>40</td>
</tr>
<tr>
<td>1500</td>
<td>60</td>
</tr>
<tr>
<td>2000</td>
<td>80</td>
</tr>
<tr>
<td>2500</td>
<td>100</td>
</tr>
<tr>
<td>3000</td>
<td>120</td>
</tr>
<tr>
<td>3500</td>
<td>140</td>
</tr>
<tr>
<td>4000</td>
<td>160</td>
</tr>
<tr>
<td>4500</td>
<td>180</td>
</tr>
<tr>
<td>5000</td>
<td>200</td>
</tr>
</tbody>
</table>

Corresponding Users Moved per Iteration service parameter value: 25

<table>
<thead>
<tr>
<th>Table I-6</th>
<th>User login retry limits for IM-only deployment (4GB active/standby)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of Users</td>
<td>Lower Retry Limit</td>
</tr>
<tr>
<td>6000</td>
<td>240</td>
</tr>
<tr>
<td>7000</td>
<td>280</td>
</tr>
<tr>
<td>8000</td>
<td>320</td>
</tr>
<tr>
<td>9000</td>
<td>360</td>
</tr>
<tr>
<td>10000</td>
<td>400</td>
</tr>
<tr>
<td>11000</td>
<td>440</td>
</tr>
<tr>
<td>12000</td>
<td>480</td>
</tr>
<tr>
<td>13000</td>
<td>520</td>
</tr>
<tr>
<td>14000</td>
<td>560</td>
</tr>
<tr>
<td>15000</td>
<td>600</td>
</tr>
</tbody>
</table>

6 GB Active/Active Profile

This section includes the upper and lower user login retry limits for both standard and IM-only deployments.

- User Login Retry Limits for Standard Deployments, page I-6
- User Retry Limits for IM-only Deployments, page I-7
User Login Retry Limits for Standard Deployments

Corresponding Users Moved per Iteration service parameter value: 50

**Table I-7**  
User login retry limits for standard deployment (6 GB active/active)—Cisco Unified Presence release 8.6(1)

<table>
<thead>
<tr>
<th>Number of Users</th>
<th>Lower Retry Limit</th>
<th>Upper Retry Limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>100</td>
<td>2</td>
<td>8</td>
</tr>
<tr>
<td>500 (Default)</td>
<td>10 (Default)</td>
<td>38 (Default)</td>
</tr>
<tr>
<td>1000</td>
<td>20</td>
<td>76</td>
</tr>
<tr>
<td>1500</td>
<td>30</td>
<td>113</td>
</tr>
<tr>
<td>2000</td>
<td>40</td>
<td>151</td>
</tr>
<tr>
<td>2500</td>
<td>50</td>
<td>189</td>
</tr>
</tbody>
</table>

**Table I-8**  
User login retry limits for standard deployment (6 GB active/active)—Cisco Unified Presence release 8.6(2) and 8.6(3)

<table>
<thead>
<tr>
<th>Number of Users</th>
<th>Lower Retry Limit</th>
<th>Upper Retry Limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>100</td>
<td>2</td>
<td>8</td>
</tr>
<tr>
<td>500 (Default)</td>
<td>10 (Default)</td>
<td>38 (Default)</td>
</tr>
<tr>
<td>1000</td>
<td>20</td>
<td>76</td>
</tr>
<tr>
<td>1500</td>
<td>30</td>
<td>113</td>
</tr>
<tr>
<td>2000</td>
<td>40</td>
<td>151</td>
</tr>
<tr>
<td>2500</td>
<td>50</td>
<td>189</td>
</tr>
<tr>
<td>3000</td>
<td>60</td>
<td>310</td>
</tr>
<tr>
<td>3500</td>
<td>70</td>
<td>362</td>
</tr>
<tr>
<td>4000</td>
<td>80</td>
<td>413</td>
</tr>
<tr>
<td>4500</td>
<td>90</td>
<td>465</td>
</tr>
<tr>
<td>5000</td>
<td>100</td>
<td>517</td>
</tr>
<tr>
<td>6000</td>
<td>120</td>
<td>620</td>
</tr>
<tr>
<td>7000</td>
<td>140</td>
<td>723</td>
</tr>
<tr>
<td>7500</td>
<td>150</td>
<td>775</td>
</tr>
</tbody>
</table>

**Table I-9**  
User login retry limits for standard deployment (6 GB active/active)—Cisco Unified Presence release 8.6(4) and later

<table>
<thead>
<tr>
<th>Number of Users</th>
<th>Lower Retry Limit</th>
<th>Upper Retry Limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>100</td>
<td>2</td>
<td>10</td>
</tr>
<tr>
<td>500 (Default)</td>
<td>10 (Default)</td>
<td>52 (Default)</td>
</tr>
<tr>
<td>1000</td>
<td>20</td>
<td>103</td>
</tr>
<tr>
<td>1500</td>
<td>30</td>
<td>155</td>
</tr>
</tbody>
</table>
Appendix I      High Availability Client Login Profiles

6 GB Active/Active Profile

Table I-9  User login retry limits for standard deployment (6 GB active/active)—Cisco Unified Presence release 8.6(4) and later (continued)

<table>
<thead>
<tr>
<th>Number of Users</th>
<th>Lower Retry Limit</th>
<th>Upper Retry Limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>2000</td>
<td>40</td>
<td>207</td>
</tr>
<tr>
<td>2500</td>
<td>50</td>
<td>258</td>
</tr>
<tr>
<td>3000</td>
<td>60</td>
<td>310</td>
</tr>
<tr>
<td>3500</td>
<td>70</td>
<td>362</td>
</tr>
<tr>
<td>4000</td>
<td>80</td>
<td>413</td>
</tr>
<tr>
<td>4500</td>
<td>90</td>
<td>465</td>
</tr>
<tr>
<td>5000</td>
<td>100</td>
<td>517</td>
</tr>
<tr>
<td>6000</td>
<td>120</td>
<td>620</td>
</tr>
<tr>
<td>7000</td>
<td>140</td>
<td>723</td>
</tr>
<tr>
<td>7500</td>
<td>150</td>
<td>775</td>
</tr>
</tbody>
</table>

User Retry Limits for IM-only Deployments

Corresponding Users Moved per Iteration service parameter value: 50

Table I-10  User login retry limits for IM-only deployment (6 GB active/active)—Cisco Unified Presence release 8.6(1)

<table>
<thead>
<tr>
<th>Number of Users</th>
<th>Lower Retry Limit</th>
<th>Upper Retry Limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>3000</td>
<td>60</td>
<td>227</td>
</tr>
<tr>
<td>3500</td>
<td>70</td>
<td>264</td>
</tr>
<tr>
<td>4000</td>
<td>80</td>
<td>302</td>
</tr>
<tr>
<td>4500</td>
<td>90</td>
<td>340</td>
</tr>
<tr>
<td>5000</td>
<td>100</td>
<td>378</td>
</tr>
<tr>
<td>6000</td>
<td>120</td>
<td>453</td>
</tr>
<tr>
<td>7000</td>
<td>140</td>
<td>529</td>
</tr>
<tr>
<td>7500</td>
<td>150</td>
<td>569</td>
</tr>
</tbody>
</table>

Table I-11  User login retry limits for IM-only deployment (6 GB active/active)—Cisco Unified Presence release 8.6(2) and later

<table>
<thead>
<tr>
<th>Number of Users</th>
<th>Lower Retry Limit</th>
<th>Upper Retry Limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>3000</td>
<td>60</td>
<td>227</td>
</tr>
<tr>
<td>3500</td>
<td>70</td>
<td>264</td>
</tr>
<tr>
<td>4000</td>
<td>80</td>
<td>302</td>
</tr>
<tr>
<td>4500</td>
<td>90</td>
<td>340</td>
</tr>
<tr>
<td>5000</td>
<td>100</td>
<td>378</td>
</tr>
<tr>
<td>6000</td>
<td>120</td>
<td>453</td>
</tr>
</tbody>
</table>

Configuration and Administration of Cisco Unified Presence Release 8.6
6 GB Active/Standby Profile

This section includes the upper and lower user login retry limits for both standard and IM-only deployments.

- User Login Retry Limits for Standard Deployments, page I-8
- User Login Retry Limits for IM-only Deployments, page I-10

User Login Retry Limits for Standard Deployments

Corresponding Users Moved per Iteration service parameter value: 50

<table>
<thead>
<tr>
<th>Number of Users</th>
<th>Lower Retry Limit</th>
<th>Upper Retry Limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>100</td>
<td>2</td>
<td>5</td>
</tr>
<tr>
<td>500 (Default)</td>
<td>10 (Default)</td>
<td>27 (Default)</td>
</tr>
<tr>
<td>1000</td>
<td>20</td>
<td>53</td>
</tr>
<tr>
<td>1500</td>
<td>30</td>
<td>80</td>
</tr>
<tr>
<td>2000</td>
<td>40</td>
<td>107</td>
</tr>
<tr>
<td>2500</td>
<td>50</td>
<td>133</td>
</tr>
<tr>
<td>3000</td>
<td>60</td>
<td>160</td>
</tr>
<tr>
<td>3500</td>
<td>70</td>
<td>187</td>
</tr>
<tr>
<td>4000</td>
<td>80</td>
<td>213</td>
</tr>
<tr>
<td>4500</td>
<td>90</td>
<td>240</td>
</tr>
<tr>
<td>5000</td>
<td>100</td>
<td>267</td>
</tr>
</tbody>
</table>

Table I-11: User login retry limits for IM-only deployment (6 GB active/active)—Cisco Unified Presence release 8.6(2) and later (continued)

<table>
<thead>
<tr>
<th>Number of Users</th>
<th>Lower Retry Limit</th>
<th>Upper Retry Limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>7000</td>
<td>140</td>
<td>529</td>
</tr>
<tr>
<td>7500</td>
<td>150</td>
<td>569</td>
</tr>
<tr>
<td>8000</td>
<td>160</td>
<td>827</td>
</tr>
<tr>
<td>9000</td>
<td>180</td>
<td>930</td>
</tr>
<tr>
<td>10000</td>
<td>200</td>
<td>1033</td>
</tr>
<tr>
<td>11000</td>
<td>220</td>
<td>1137</td>
</tr>
<tr>
<td>12000</td>
<td>240</td>
<td>1240</td>
</tr>
<tr>
<td>12500</td>
<td>250</td>
<td>1292</td>
</tr>
</tbody>
</table>
Table I-13  User login retry limits for standard deployment (6 GB active/standby)—Cisco Unified Presence release 8.6(2) and 8.6(3)

<table>
<thead>
<tr>
<th>Number of Users</th>
<th>Lower Retry Limit</th>
<th>Upper Retry Limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>100</td>
<td>2</td>
<td>5</td>
</tr>
<tr>
<td>500 (Default)</td>
<td>10 (Default)</td>
<td>27 (Default)</td>
</tr>
<tr>
<td>1000</td>
<td>20</td>
<td>53</td>
</tr>
<tr>
<td>1500</td>
<td>30</td>
<td>80</td>
</tr>
<tr>
<td>2000</td>
<td>40</td>
<td>107</td>
</tr>
<tr>
<td>2500</td>
<td>50</td>
<td>133</td>
</tr>
<tr>
<td>3000</td>
<td>60</td>
<td>160</td>
</tr>
<tr>
<td>3500</td>
<td>70</td>
<td>187</td>
</tr>
<tr>
<td>4000</td>
<td>80</td>
<td>213</td>
</tr>
<tr>
<td>4500</td>
<td>90</td>
<td>240</td>
</tr>
<tr>
<td>5000</td>
<td>100</td>
<td>267</td>
</tr>
<tr>
<td>6000</td>
<td>120</td>
<td>393</td>
</tr>
<tr>
<td>7000</td>
<td>140</td>
<td>458</td>
</tr>
<tr>
<td>8000</td>
<td>160</td>
<td>524</td>
</tr>
<tr>
<td>9000</td>
<td>180</td>
<td>589</td>
</tr>
<tr>
<td>10000</td>
<td>200</td>
<td>655</td>
</tr>
<tr>
<td>11000</td>
<td>220</td>
<td>720</td>
</tr>
<tr>
<td>12000</td>
<td>240</td>
<td>785</td>
</tr>
<tr>
<td>13000</td>
<td>260</td>
<td>851</td>
</tr>
<tr>
<td>14000</td>
<td>280</td>
<td>916</td>
</tr>
<tr>
<td>15000</td>
<td>300</td>
<td>982</td>
</tr>
</tbody>
</table>

Table I-14  User login retry limits for standard deployment (6 GB active/standby)—Cisco Unified Presence release 8.6(4) and later

<table>
<thead>
<tr>
<th>Number of Users</th>
<th>Lower Retry Limit</th>
<th>Upper Retry Limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>100</td>
<td>2</td>
<td>7</td>
</tr>
<tr>
<td>500 (Default)</td>
<td>10 (Default)</td>
<td>33 (Default)</td>
</tr>
<tr>
<td>1000</td>
<td>20</td>
<td>65</td>
</tr>
<tr>
<td>1500</td>
<td>30</td>
<td>98</td>
</tr>
<tr>
<td>2000</td>
<td>40</td>
<td>131</td>
</tr>
<tr>
<td>2500</td>
<td>50</td>
<td>164</td>
</tr>
<tr>
<td>3000</td>
<td>60</td>
<td>196</td>
</tr>
<tr>
<td>3500</td>
<td>70</td>
<td>229</td>
</tr>
<tr>
<td>4000</td>
<td>80</td>
<td>262</td>
</tr>
</tbody>
</table>
Table I-14  
User login retry limits for standard deployment (6 GB active/standby)—Cisco Unified Presence release 8.6(4) and later (continued)

<table>
<thead>
<tr>
<th>Number of Users</th>
<th>Lower Retry Limit</th>
<th>Upper Retry Limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>4500</td>
<td>90</td>
<td>295</td>
</tr>
<tr>
<td>5000</td>
<td>100</td>
<td>327</td>
</tr>
<tr>
<td>6000</td>
<td>120</td>
<td>393</td>
</tr>
<tr>
<td>7000</td>
<td>140</td>
<td>458</td>
</tr>
<tr>
<td>8000</td>
<td>160</td>
<td>524</td>
</tr>
<tr>
<td>9000</td>
<td>180</td>
<td>589</td>
</tr>
<tr>
<td>10000</td>
<td>200</td>
<td>655</td>
</tr>
<tr>
<td>11000</td>
<td>220</td>
<td>720</td>
</tr>
<tr>
<td>12000</td>
<td>240</td>
<td>785</td>
</tr>
<tr>
<td>13000</td>
<td>260</td>
<td>851</td>
</tr>
<tr>
<td>14000</td>
<td>280</td>
<td>916</td>
</tr>
<tr>
<td>15000</td>
<td>300</td>
<td>982</td>
</tr>
</tbody>
</table>

User Login Retry Limits for IM-only Deployments

Corresponding Users Moved per Iteration service parameter value: 50

Table I-15  
User login retry limits for IM-only deployment (6 GB active/standby)—Cisco Unified Presence release 8.6(1)

<table>
<thead>
<tr>
<th>Number of Users</th>
<th>Lower Retry Limit</th>
<th>Upper Retry Limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>6000</td>
<td>120</td>
<td>320</td>
</tr>
<tr>
<td>7000</td>
<td>140</td>
<td>373</td>
</tr>
<tr>
<td>8000</td>
<td>160</td>
<td>427</td>
</tr>
<tr>
<td>9000</td>
<td>180</td>
<td>480</td>
</tr>
<tr>
<td>10000</td>
<td>200</td>
<td>533</td>
</tr>
<tr>
<td>11000</td>
<td>220</td>
<td>587</td>
</tr>
<tr>
<td>12000</td>
<td>240</td>
<td>640</td>
</tr>
<tr>
<td>13000</td>
<td>260</td>
<td>693</td>
</tr>
<tr>
<td>14000</td>
<td>280</td>
<td>747</td>
</tr>
<tr>
<td>15000</td>
<td>300</td>
<td>800</td>
</tr>
</tbody>
</table>

Table I-16  
User login retry limits for IM-only deployment (6 GB active/standby)—Cisco Unified Presence release 8.6(2) and later

<table>
<thead>
<tr>
<th>Number of Users</th>
<th>Lower Retry Limit</th>
<th>Upper Retry Limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>6000</td>
<td>120</td>
<td>320</td>
</tr>
<tr>
<td>7000</td>
<td>140</td>
<td>373</td>
</tr>
</tbody>
</table>
### Table I-16  
User login retry limits for IM-only deployment (6 GB active/standby)—Cisco Unified Presence release 8.6(2) and later (continued)

<table>
<thead>
<tr>
<th>Number of Users</th>
<th>Lower Retry Limit</th>
<th>Upper Retry Limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>8000</td>
<td>160</td>
<td>427</td>
</tr>
<tr>
<td>9000</td>
<td>180</td>
<td>480</td>
</tr>
<tr>
<td>10000</td>
<td>200</td>
<td>533</td>
</tr>
<tr>
<td>11000</td>
<td>220</td>
<td>587</td>
</tr>
<tr>
<td>12000</td>
<td>240</td>
<td>640</td>
</tr>
<tr>
<td>13000</td>
<td>260</td>
<td>693</td>
</tr>
<tr>
<td>14000</td>
<td>280</td>
<td>747</td>
</tr>
<tr>
<td>15000</td>
<td>300</td>
<td>800</td>
</tr>
<tr>
<td>16000</td>
<td>320</td>
<td>1047</td>
</tr>
<tr>
<td>17000</td>
<td>340</td>
<td>1113</td>
</tr>
<tr>
<td>18000</td>
<td>360</td>
<td>1178</td>
</tr>
<tr>
<td>19000</td>
<td>380</td>
<td>1244</td>
</tr>
<tr>
<td>20000</td>
<td>400</td>
<td>1309</td>
</tr>
<tr>
<td>21000</td>
<td>420</td>
<td>1375</td>
</tr>
<tr>
<td>22000</td>
<td>440</td>
<td>1440</td>
</tr>
<tr>
<td>23000</td>
<td>460</td>
<td>1505</td>
</tr>
<tr>
<td>24000</td>
<td>480</td>
<td>1571</td>
</tr>
<tr>
<td>25000</td>
<td>500</td>
<td>1636</td>
</tr>
</tbody>
</table>
Appendix I  High Availability Client Login Profiles

6 GB Active/Standby Profile
XMPP Standards Compliance

June 16, 2014

- XMPP Standards, page II-1

XMPP Standards

Cisco Unified Presence is compliant with the following XMPP standards:

- RFC 3920 Extensible Messaging and Presence Protocol (XMPP): Core
  - XEP-0004 Data Forms
  - XEP-0012 Last Activity
  - XEP-0013 Flexible Offline Message Retrieval
  - XEP-0016 Privacy Lists
  - XEP-0030 Service Discovery
  - XEP-0045 Multi-User Chat
  - XEP-0054 Vcard-temp
  - XEP-0055 Jabber Search
  - XEP-0060 Publish-Subscribe
  - XEP-0065 SOCKS5 Bystreams
  - XEP-0066 Out of Band Data Archive OOB requests
  - XEP-0068 Field Standardization for Data Forms
  - XEP-0071 XHTML-IM
  - XEP-0082 XMPP Date and Time Profiles
  - XEP-0092 Software Version
  - XEP-0106 JID Escaping
  - XEP-0114 Jabber Component Protocol
  - XEP-0115 Entity Capabilities
  - XEP-0124 Bidirectional Streams over Synchronous HTTP (BOSH)
  - XEP-0126 Invisibility
- XEP-0128 Service Discovery Extensions
- XEP-0160 Best Practices for Handling Offline Messages
- XEP-0163 Personal Eventing Via PubSub
- XEP-0170 Recommended Order of Stream Feature Negotiation
- XEP-0178 Best Practices for Use of SASL EXTERNAL
- XEP-0220 Server Dialback
- XEP-0273 SIFT (Stanza Interception and Filtering Technology)
# Glossary of Terms

## June 16, 2014

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cluster</td>
<td>One or multiple subclusters providing service to a single Cisco Unified Communications Manager cluster. Each Cisco Unified Communications Manager cluster requires one Cisco Unified Presence cluster.</td>
</tr>
<tr>
<td>High Availability Deployment</td>
<td>The deployment model that provides redundant services for users in case of the failure of services or hardware. Cisco Unified Presence supports a non High Availability deployment, a best effort High Availability deployment, and redundant High Availability deployment.</td>
</tr>
<tr>
<td>Intercluster</td>
<td>A collection of Cisco Unified Presence clusters interconnected to provide uniform availability and IM services to all Cisco Unified Presence clusters.</td>
</tr>
<tr>
<td>Lightweight Directory Access Protocol (LDAP)</td>
<td>The Lightweight Directory Access Protocol (LDAP) provides applications with a standard method for accessing and potentially modifying the user information stored in the corporate directory. This capability enables enterprises to centralize all user information in a single repository available to several applications.</td>
</tr>
<tr>
<td>Line Appearance</td>
<td>A line appearance is the association of a particular line with a particular device. A single line can be associated with multiple devices, and a single device can be associated with multiple lines. You can associate one user, or many users, with a line appearance, rather than with a line or to a device.</td>
</tr>
<tr>
<td>Multi-Node Feature</td>
<td>The Cisco Unified Presence multi-node feature enables the customer to increase the scalability of a Cisco Unified Presence cluster by a factor of three. The Cisco Unified Presence multi-node feature allows the customer to create Cisco Unified Presence groups, also known as subclusters, with up to 45,000 users within a Cisco Unified Presence cluster.</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>-----------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Subcluster</td>
<td>A single Cisco Unified Presence server, or a pair of Cisco Unified Presence servers operating with a shared availability database that is able to support common users. In a single-node deployment within the subcluster, there is no High Availability failover protection for the users assigned to that node. In a dual-node deployment within a subcluster, users have High Availability failover protection as each node acts as a backup for the other node allowing clients to fail over in case of outages of components or nodes. In this high-availability mode, all users in the subcluster have failover capabilities.</td>
</tr>
<tr>
<td>User</td>
<td>A user for whom Cisco Unified Presence will maintain availability state. A Cisco Unified Presence user is assigned to a node in a subcluster.</td>
</tr>
<tr>
<td>Node</td>
<td>A single Cisco Unified Presence server instance supporting up to 15,000 users. A Cisco Unified Presence node can be assigned to a subcluster.</td>
</tr>
</tbody>
</table>