Push Notifications Deployment for Cisco Jabber on iPhone and iPad with Cisco Unified Communications Manager

First Published: 2018-07-05
Last Modified: 2019-10-03

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883
CONTENTS

CHAPTER 1
Preface 1
  Purpose of this Document 1
  Important Notice 1
  Upgrade Requirements for Push Notifications 2

CHAPTER 2
Push Notifications (On-Premises Deployments) 3
  Push Notifications Overview 3
  Push Notifications High Availability for IM and Presence 5
  Proxy Support for Cloud Connection 6
  Push Notifications Prerequisites 8
  Push Notifications Configuration Task Flow 10
    Synchronize Licenses 12
    Open Ports for Push Notifications 12
    Enable Push Notifications 13
    Enable Push Notifications High Availability 15
    Configure OAuth Regresh Logins 16
      Configure OAuth Refresh Logins in Unified Communications Manager 16
      Confirm OAuth Configuration in Expressway 17
    Enable OAuth on Unity Connection 18
    Refresh Settings from Expressway 19
    Configure Troubleshooting Options 19
  Push Notifications Troubleshooting 20
    Upgrades from 11.5(1)SU2 with Push Notifications Enabled 21
    Update Refresh Token Manually 22
    Push Notifications Interactions and Restrictions 23

Push Notifications Deployment for Cisco Jabber on iPhone and iPad with Cisco Unified Communications Manager
CHAPTER 3
Push Notifications (Cloud Deployment) 25
  Cloud Deployments with WebEx Messenger 25

CHAPTER 4
Certificates and Performance Monitoring 27
  Certificates for Cloud Connection 27
  Push Notifications Alarms 29
  Performance Counters for Push Notifications 31
  Open Caveats - Release 11.5(1)SU3 35

APPENDIX A
Push Notifications Support in Release 11.5(1)SU2 37
  Push Notifications Support in Release 11.5(1)SU2 37
  Terminated Push Notifications for Service Shutdowns 38
  Push Notifications Configuration Task Flow - Release 11.5(1)SU2 38
  Synchronize Licenses 39
  Open Ports for Push Notifications in Release 11.5(1)SU2 39
  Enable Push Notifications (Release 11.5(1)SU2) 40
  Push Notifications Counters in 11.5(1)SU2 42
  Open Caveats - Release 11.5(1)SU2 43
Preface

• Purpose of this Document, on page 1
• Important Notice, on page 1
• Upgrade Requirements for Push Notifications, on page 2

Purpose of this Document

This document describes how to configure Push Notifications for Cisco Unified Communications Manager and the IM and Presence Service. With Push Notifications, your deployment uses Apple's cloud-based Push Notification service to push voice calls, video calls, and instant message notifications to Cisco Jabber for iPhone and iPad clients that are running in the background. You must enable Push Notifications to maintain persistent communication with Cisco Jabber for iPhone and iPad.

This document describes how to enable Push Notifications for the following deployment types:

• Push Notifications (On-Premises Deployments)—For on-premises deployments of Cisco Unified Communications Manager and IM and Presence Service, refer to Chapter 2 for instructions on how to enable Push Notifications. This includes deployments where Cisco Jabber for iPhone and iPad clients register to an on-premises Cisco Unified Communications Manager and IM and Presence Service via Expressway's Mobile and Remote Access (MRA) feature.

• Push Notifications (Cloud Deployment)—For cloud deployments with WebEx Messenger, refer to Chapter 3 for deployment requirements.

Important Notice

In alignment with Apple's changes to the iOS notification architecture, Cisco Jabber is in the process of implementing Apple Push Notification support for notifications. We highly recommend that customers upgrade Cisco Unified Communications Manager, IM and Presence Service, Cisco Expressway, and Cisco Jabber before June 2018 or as soon as possible thereafter. Failure to upgrade in a timely manner will result in loss of voice, video, and IM notifications for Jabber iOS users.
**Upgrade Requirements for Push Notifications**

Use the following table to determine whether you need to upgrade your system in order to deploy Push Notifications. Cisco Unified Communications Manager Release 11.5(1)SU3 includes full Push Notifications support for voice and video calls as well as instant messaging with High Availability.

*Table 1: Upgrade Requirements to Support Push Notifications*

<table>
<thead>
<tr>
<th>If your Apple mobile deployment includes...</th>
<th>Upgrade to these releases...</th>
</tr>
</thead>
<tbody>
<tr>
<td>No Jabber clients on iOS</td>
<td>No upgrade required</td>
</tr>
</tbody>
</table>
| Unified Communications (calling and instant messaging) | • Cisco Jabber 11.9  
• Cisco Unified Communications Manager and IM and Presence Service 11.5(1)SU3*  
• Cisco Expressway X8.10.1 (if MRA is deployed) |
| Unified Communications (calling and WebEx Messenger) | • Cisco Jabber 11.9  
• Cisco Unified Communications Manager 11.5(1)SU3*  
• Cisco Expressway X8.10.1 (if MRA is deployed) |

* If you need to use an HTTPS Proxy server, you must be running a minimum release of 11.5(1)SU4. This feature is not supported by 12.0(1) or 12.0(1)SU1.
Push Notifications Overview

When your cluster is enabled for Push Notifications, Cisco Unified Communications Manager and the IM and Presence Service use Apple's cloud-based Push Notification service to push notifications for voice and video calls, instant messages, and Cisco WebEx invitations to Cisco Jabber for iPhone and iPad clients that are running in suspended mode. Push Notifications allows your system to maintain a persistent communication with Cisco Jabber. Push Notifications is required both for Cisco Jabber for iPhone and iPad clients that connect from within the enterprise network, and for clients that register to an on-premise deployment via Expressway's Mobile and Remote Access (MRA) feature.

Note

Push Notifications is required only for Cisco Jabber for iPhone and iPad clients. The feature is not supported for Android and is not applicable for Windows and Mac users.

How Push Notifications Works

At startup, Cisco Jabber clients that are installed on iPhone and iPad devices register to Cisco Unified Communications Manager, the IM and Presence Service and to the Apple cloud. With MRA deployments, the Cisco Jabber for iPhone or iPad client registers to the on-premises servers via Expressway. So long as the Jabber client remains in foreground mode, Cisco Unified Communications Manager and the IM and Presence Service can send calls and instant messages to the Jabber client directly.

However, once the Cisco Jabber client moves to suspended mode (for example, to maintain battery life), the standard communication channel is unavailable, preventing Cisco Unified Communications Manager and IM and Presence Service from communicating directly with the client. Push Notifications provides another channel to reach the Jabber client via the Cisco and Apple clouds.
Cisco Jabber is considered to be running in suspended mode if any of the following conditions are true:

- the Cisco Jabber application is running off-screen (i.e., in the background)
- the iPhone or iPad is locked
- the iPhone or iPad screen is turned off

The above diagram displays what happens when Cisco Jabber for iPhone and iPad clients run in the background or are stopped. The figure illustrates: (1) an MRA deployment where the Cisco Jabber client that connects with an on-premises Cisco Unified Communications Manager and IM and Presence Service deployment via Expressway, and (2) a Cisco Jabber for iPhone or iPad client that connects directly to the on-premises deployment from within the enterprise network.

For a detailed description of what happens with each use case, see the following table:

**Table 2: Message Flow for Cisco Jabber for iPhone and iPad when Push Notifications is Enabled**

<table>
<thead>
<tr>
<th>Jabber client is running...</th>
<th>Cisco Unified Communications Manager and IM and Presence Service send push notification to...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Foreground Mode</td>
<td>Standard communication channels are used for voice, video, IM and Presence:</td>
</tr>
<tr>
<td></td>
<td>• For on-premises mobile clients, Cisco Unified Communications Manager and IM and Presence Service send the call or instant message to the Jabber client directly.</td>
</tr>
<tr>
<td></td>
<td>• For MRA clients, the call or IM notification is sent to the Jabber client via Expressway.</td>
</tr>
</tbody>
</table>

**Note** For voice and video calls, the Push Notification is still sent via the Push Notification channel, but the Cisco Jabber client uses the standard channel.
### Push Notifications High Availability for IM and Presence

Push Notifications High Availability provides failover and redundancy for Push Notifications-enabled IM and Presence sessions for Cisco Jabber on iPhone and iPad clients. With this feature, the IM and Presence Service saves the IM session in the local in-memory database (IMDB), which gets replicated automatically to the in-memory database on the subcluster backup node. This ensures that the backup node has the session information and can take over the session without user action from the Jabber user.

**IM History**

When Push Notifications High Availability is configured, the Jabber user does not lose the chat history when failover occurs.

**Unread Message Queue when Jabber is in Suspended Mode**

For Push Notifications-enabled IM sessions, when a Cisco Jabber for iPhone or iPad client moves into suspended mode, the IM and Presence Service sends Push Notifications to the Jabber client, but stops sending unread instant messages, Presence updates, and other XMPP stanzas (for example, chat room invites). Instead, these messages are queued on the local server until the Jabber client clicks on a Push Notification, or reenters foreground mode.

There is a limitation involving the unread message queue for Push Notifications-enabled IM sessions where Cisco Jabber is in suspended mode. In some failover use cases, the unread message queue is lost. See "Redundancy and Failover Use Cases" for a description of when this occurs.

---

<table>
<thead>
<tr>
<th>Jabber client is running...</th>
<th>Cisco Unified Communications Manager and IM and Presence Service send push notification to...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Suspended Mode</td>
<td><strong>Voice or Video Calls</strong></td>
</tr>
<tr>
<td></td>
<td>Standard communication channels are unavailable. Cisco Unified Communications Manager uses the Push Notifications channel.</td>
</tr>
<tr>
<td></td>
<td>Upon receiving the notification, the Jabber client re-enters foreground mode automatically, and the client rings.</td>
</tr>
<tr>
<td></td>
<td><strong>Instant Messaging</strong></td>
</tr>
<tr>
<td></td>
<td>Standard communication channels are unavailable. IM and Presence Service uses the Push Notifications channel to send IM notifications as follows:</td>
</tr>
<tr>
<td></td>
<td>1. IM and Presence Service sends the IM notification to the Push REST service in the Cisco cloud, which forwards the notification to the Apple cloud.</td>
</tr>
<tr>
<td></td>
<td>2. The Apple cloud pushes the IM notification to the Jabber client and a notification appears on the Jabber client.</td>
</tr>
<tr>
<td></td>
<td>3. When the user clicks the notification, the Jabber client moves back the foreground. The Jabber client resumes the session with the IM and Presence Service and downloads the instant message.</td>
</tr>
</tbody>
</table>

**Note** While the Cisco Jabber client is in suspended mode, the user's Presence status displays as **Away**.
Redundancy and Failover Use Cases

The following use cases are covered by this feature:

- **Node failure (automatic failover)**—If a node fails suddenly, the backup node takes over the IM session and Push Notifications continue to be sent to the Jabber user, this time from the backup node. Jabber users can continue working without any user action or loss of IM history. However, the unread messages that were queued on the failed server while Jabber was in suspended mode, and which had not yet been sent to the Jabber client, are lost.

- **Node shutdown (manual failover)**—If a node is shut down gracefully, the backup node takes over the IM session and Push Notifications continue to be sent, this time from the backup node. Jabber users can continue working without any user action or loss of IM history. The unread messages that were queued on the original node, and which were waiting to be sent to the Jabber client, are lost temporarily when the backup node takes over. However, after the original node comes back up, and the user falls back to the original node, that message queue is retrieved, and is sent to the user.

- **Cisco XCP Router crash**—If the Cisco XCP Router crashes suddenly, once the router comes back up, the node resumes the session and continues to send Push Notifications. The IM history is maintained, and Jabber users can continue working without any user action. However, the unread messages that were queued on the server prior to the router crash, and which had not yet been sent to the Jabber client, are lost.

- **Cisco XCP Router restarts**—If an administrator restarts the Cisco XCP Router, such as may happen after a configuration update, both the IM history and the unread message queue are maintained. Once the router restarts, the IM and Presence Service resumes sending Push Notifications. The unread message queue is sent once the Jabber client logs in again.

---

**Note**

For voice and video calls, redundancy and failover is handled by Cisco Unified Communications Manager Groups.

---

Proxy Support for Cloud Connection

For some deployments, you may need to use a proxy server to connect to the Cisco cloud. This is particularly true if your on-premise deployment is behind a company firewall that does not allow direct access to the cloud. Cisco Unified Communications Manager supports the Cisco Web Security Appliance as an HTTPS proxy server. However, you can use any HTTP or HTTPS proxy server that supports one of the below call flows. Note that if you decide to use an HTTP proxy with authentication enabled, Cisco recommends that you configure digest authentication for the proxy server for credential security.
Supported Call Flow for HTTPS Proxy

1. CUCM
2. HTTPS Proxy
3. Cisco Cloud

TCP Connection (SYN-SYN, ACK-ACK)

Client Hello

Server Hello, Cert

Client key exchange

HTTP CONNECT (over established TLS)

TCP CONNECT (SYN-SYN, ACK-ACK)

Client Hello (over established TLS)

Server Hello, cert, key exchange (over established TLS)

Client key exchange (over established TCP)

Traffic between client and Cloud over Tunneled TCP

Supported Call Flow for HTTP Proxy

1. CUCM
2. HTTP Proxy
3. Cisco Cloud

TCP Connection (SYN-SYN, ACK-ACK)

HTTP CONNECT (Destination in Cloud)

Client Hello (over established TCP)

Server Hello, cert, key exchange (over established TCP)

Client key exchange (over established TCP)

Traffic between client and Cloud over Tunneled TCP
DNS Requirements for Proxy Servers

- For the Cisco Unified Communications Manager to proxy server connection, if you use a FQDN address for the proxy server, DNS is used to connect to the proxy server. If the proxy server FQDN resolves to multiple IP addresses, Unified Communications Manager tries the first IP address and waits two seconds before moving on to the second address.

- After sending a push notification, Cisco Unified Communications Manager waits five seconds for a confirmation before trying the second address.

- For the proxy server to Cisco cloud connection, Cisco recommends that you configure the proxy server with a low failover rate in order to speed up the failover process for connection failures.

- If you are deploying the Cisco Web Security Appliance, the FQDN must map to the WSA’s virtual IP address.

Note
The default Time To Live (TTL) for proxy IP addresses is one hour. As a result, if an IP address is changed, it may take up to one hour for that change to be available for DNS requests.

Push Notifications Prerequisites

The following prerequisites are required to onboard Push Notifications for on-premises deployments:

- DNS must be configured in both Cisco Unified Communications Manager and IM and Presence Service and must be able to resolve externally routable addresses.

- Connectivity must be enabled from Cisco Unified Communications Manager and IM and Presence Service over port 443 for the following connections to the Cisco cloud:
  - Fusion Onboarding Service at fos-a.wbx2.com—Cisco Unified Communications Manager connects to this service for Push Notification subscription requests. Cisco Unified Communications Manager communicates with the Fusion Onboarding Service (FOS) in order to provision a Common Identity (CI) machine account.
  - Push REST service at push.webexconnect.com—Cisco Unified Communications Manager and IM and Presence Service connect to this service to send Push Notifications.
  - Common Identity service at idbroker.webex.com—Cisco Unified Communications Manager and IM and Presence Service authenticates to this service prior to sending a Push Notification.

- Make sure that your underlying iOS network allows traffic from the Apple Push Notifications Service coming in from the 17.0.0.0/8 range. This is necessary so that access control lists don’t block Push Notifications that are sent from the Apple cloud to Cisco Jabber clients.


- The Stream Management feature must be configured on the IM and Presence Service. For details, see the Release Notes for Cisco Unified Communications Manager Release 10.5(2) and IM and Presence

- Push Notifications is dependent on the following network services, which were introduced with Release 11.5(1)SU3. You can confirm that these services are running in the **Control Center - Network Services** window of Cisco Unified Serviceability. Both services are enabled by default.
  
  - **Cisco Push Notification Service**—handles the Push Notification for voice and video calls.
  - **Cisco Management Agent Service**—handles the sending of troubleshooting information related to Push Notifications.

- The iOS device must be configured to allow notifications from the Cisco Jabber application.

- If you require a proxy server for the cloud connection, refer to Proxy Support for Cloud Connection, on page 6 for HTTP(S) proxy support.

**Licensing Prerequisites**

- For 11.5(x) releases, Cisco Unified Communications Manager uses Cisco Prime License Manager for licensing. As part of the Push Notifications onboarding process, you will be required to synchronize licenses in Prime License Manager.

- For 12.x and later releases, Cisco Unified Communications Manager uses Smart Licensing for licensing. Smart Licensing must be configured before you onboard the cluster for Push Notifications. For details on how to setup Cisco Unified Communications Manager for Smart Licensing, see the "Smart Software Licensing" chapter of the *System Configuration Guide for Cisco Unified Communications Manager*.

- From Release 12.5(x) and onward, Push Notifications is not supported when Smart Licensing is configured with Specific License Reservation. The Specific License Reservation feature must be disabled for Push Notifications to work.

**Certificate Prerequisites**

- If MRA is configured, you must exchange certificates between Cisco Unified Communications Manager, the IM and Presence Service, and Cisco Expressway-C. Cisco recommends that you use CA-signed certificates with the same CA for each system. In this case:
  
  - Install the CA root certificate chain on each system (for Cisco Unified Communications Manager and the IM and Presence Service install the certificate chain to the tomcat-trust store).
  
  - For Cisco Unified Communications Manager, issue a CSR to request CA-signed tomcat and Cisco CallManager certificates.
  
  - For the IM and Presence Service, issue a CSR to request CA-signed tomcat certificates.

---

**Note**

If you use different CAs, you must install each CA's root certificate chain on Cisco Unified Communications Manager, IM and Presence Service, and Expressway-C.
You can also use self-signed certificates for both Cisco Unified Communications Manager and the IM and Presence Service. In this case, you must upload onto Expressway-C the tomcat and Cisco CallManager certificates for Cisco Unified Communications Manager and a tomcat certificate for the IM and Presence Service.

Minimum Release Requirements for Push Notifications Solution

Make sure that your deployment meets the minimum release requirements for Push Notifications as per the below table:

Table 3: Minimum Release Requirements for Push Notifications Solution

<table>
<thead>
<tr>
<th>Push Notifications Support</th>
<th>Minimum Releases</th>
</tr>
</thead>
</table>
| Calling with IM and Presence | • Cisco Unified Communications Manager 11.5(1)SU3  
  • IM and Presence Service 11.5(1)SU3  
  • Cisco Jabber 11.9  
  • Cisco Expressway X8.10.1 (if MRA is deployed) |

| Push Notifications Configuration Task Flow |

Complete the following tasks to configure Cisco Unified Communications Manager and IM and Presence Service clusters for Push Notifications. This configuration is required for Cisco Jabber clients that are installed on iPhone and iPad devices.

Before you begin

Push Notifications Prerequisites, on page 8

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 Synchronize Licenses, on page 12</td>
<td>Release 11.5(1)SUx only. Synchronize your system licensing in Cisco Prime License Manager. This is a mandatory task regardless of whether you have added new licenses.</td>
</tr>
</tbody>
</table>
## Command or Action | Purpose
--- | ---
**Note** | You can skip this task for Cisco Unified Communications Manager Release 12.0(1) and higher as Prime License Manager is replaced by Smart Licensing.

**Step 2** | Open Ports for Push Notifications, on page 12
--- | ---
Open the ports that are required for Push Notifications.

**Step 3** | Enable Push Notifications, on page 13
--- | ---
Onboard the Cisco Unified Communications Manager and IM and Presence Service clusters for Push Notifications.

**Step 4** | Enable Push Notifications High Availability, on page 15
--- | ---
For IM and Presence deployments, enable Push Notifications High Availability.

**Step 5** | Configure OAuth Regfresh Logins, on page 16
--- | ---
Complete this set of tasks to deploy OAuth Refresh Logins for faster Cisco Jabber logins.

**Note** | OAuth Refresh Logins are enabled by default in Cisco Expressway, but are disabled by default in Cisco Unified Communications Manager. If you use the default settings for both systems, a configuration mismatch occurs.

**Step 6** | Refresh Settings from Expressway, on page 19
--- | ---
On the Expressway-C, refresh your Unified Communications Manager servers to allow for a resync of the Authz certificate. After you are done, restart the Expressway-C.

**Step 7** | Configure Troubleshooting Options, on page 19
--- | ---
Configure troubleshooting parameters that determine how often Cisco Unified Communications Manager sends Push Notifications alarms to the Cisco Cloud, and for which alarm severities.

---

**Note**
For Mobile and Remote Access (MRA) deployments with Cisco Expressway, see the *Mobile and Remote Access via Cisco Expressway Deployment Guide* at the below URL for information about Push Notifications with Expressway.

Synchronize Licenses

For 11.5(1)SU systems, use this procedure in Cisco Prime License Manager to synchronize your system licensing. This is a mandatory task to enable Push Notifications for on-premises deployments, regardless of whether you have updated your licensing.

Note

This task is required for Cisco Unified Communications Manager 11.5(1)SU releases only. You can skip this task for Release 12.0(1) and higher as Smart Licensing replaces Prime License Manager.

Before you begin

For details on licensing, including procedures for adding licenses or product instances, refer to the Cisco Prime License Manager User Guide:


Procedure

Step 1
In Cisco Prime License Manager, select the Product Instance tab.

Step 2
Click Synchronize Licenses.

What to do next

Open Ports for Push Notifications, on page 12

Open Ports for Push Notifications

Make sure that the following outbound ports are open in Cisco Unified Communications Manager, IM and Presence Service, and in your Cisco Jabber for iPhone or iPad client.
### Table 4: Port Requirements for Push Notifications

<table>
<thead>
<tr>
<th>From</th>
<th>To</th>
<th>Port</th>
<th>Port Description</th>
</tr>
</thead>
</table>
| Cisco Unified Communications Manager / IM and Presence Service | Cisco cloud | 443/TCP | HTTPS-based communications:  
• Subscription requests from Cisco Unified Communications Manager to Fusion Onboarding Service at fos-a.wbx2.com from publisher node  
• Authentication requests to Common Identity Service at idbroker.webex.com  
• Push notifications to the Push REST service at push.webexconnect.com  
This port should be open for all cluster nodes. |
| Cisco Jabber client (when operating behind a firewall) | Apple cloud (17.0.0.0/8)* | 5223/TCP | Communications with Apple Push Notification service. |
| Cisco Jabber client | Apple cloud (17.0.0.0/8)* | 443/TCP | Fallback port for 5223 if wi-fi is used. |

* Apple Push Notifications Service uses the 17.0.0.0/8 range. Make sure that your network doesn't have an access control list that blocks this range.

---

**Note**  
In addition, port 9966 is used internally by the Cisco Push Notification Service to communicate with the Cisco CallManager Service on all Cisco Unified Communications Manager cluster nodes. This port needs to be open in the firewall if communication between nodes in your cluster traverse through a firewall (for example the nodes are located in a different subnet if as an example they are clustered over the WAN). In this case, this port needs to be open in the firewall so that these services can communicate.

---

**What to do next**

Enable Push Notifications, on page 13

---

**Enable Push Notifications**

Use this procedure to set up the Push Notifications feature for Cisco Jabber for iPhone and iPad clients. This release provides Push Notifications support for voice calls and instant messaging with High Availability.

**Before you begin**

Make sure of the following:
• Port 443 must be open from the Cisco Unified Communications Manager publisher node for outbound HTTPS requests.

• Both the Cisco Push Notification Service and the Cisco Management Agent Service network services must be running in Cisco Unified Serviceability. Both services are enabled by default.

Procedure

Step 1
Log in to the Cisco Unified Communications Manager publisher node.

Step 2
From Cisco Unified Communications Manager Administration, choose Advanced Features > Cisco Cloud Onboarding.

The page may take a minute to load while Cisco Unified Communications Manager checks whether the Cisco cloud is reachable, and whether certificates are present.

Step 3
Click the Generate Voucher button to synchronize system licensing.

For more information, refer to Chapter 2 for Licensing Prerequisites under the Push Notifications Prerequisites.

Step 4
Check the Enable Push Notifications check box.

Step 5
Check the I want Cisco to manage the Cisco Cloud Service CA Certificates required for this trust check box to have the system update certificates automatically.

Note: If you check this check box, Cisco installs your cloud certificate requirements automatically. However, if a new certificate requirement is added that was not included in the file that you used to install your system, you may need to obtain cloud certificates manually. For information on uploading certificates manually, see Certificates for Cloud Connection, on page 27.

Step 6
If you require an HTTP(S) Proxy to reach the Cisco cloud, check the Enable HTTP(S) Proxy check box and enter the server details.

Note: Cisco supports Basic and Digest authentication for the proxy server. The recommended authentication method is digest authentication.

Step 7
Click Save.

Step 8
On the publisher node only, restart the Cisco Tomcat service to install Cisco-managed certificates.

a) Log in to the Command Line Interface.

b) Run the utils service restart Cisco Tomcat command.

After the Cisco Tomcat service restarts, the Status in the Cisco Cloud Onboarding Configuration window displays the message "Cisco Cloud Onboarding Pending".

Step 9
In the Cisco Cloud Onboarding Configuration window, make sure that the Enable Push Notifications and the I want Cisco to manage the Cisco Cloud Service CA Certificates required for this trust check boxes are still checked. You may need to recheck them.

Step 10
Optional. Configure troubleshooting settings to ensure that system issues can be resolved quickly. See the online help for field descriptions.

a) Check the Send Troubleshooting Information to the Cisco Cloud check box.

b) Check the Send encrypted PII to the Cisco Cloud for troubleshooting check box.

Step 11
Click Save.

The cluster initiates a Push Notifications subscription request. When the request completes, and Push Notifications is enabled, the Status displays the message "Cloud Onboarding Completed".
Step 12: If your deployment includes the IM and Presence Service, restart the Cisco XCP Config Manager and Cisco XCP Router service for all IM and Presence Service cluster nodes:

a) Click the Control Center - Network Services link that appears in the Status area of the Cisco Cloud Onboarding window. If no link appears, log in to the Cisco Unified Serviceability interface and select Tools > Control Center - Network Services.

b) From the Server drop-down list box, choose the IM and Presence database publisher node, and click Go.

c) Select the Cisco XCP Config Manager service and click Restart.

d) Select the Cisco XCP Router service and click Restart.

e) Repeat this step for all IM and Presence cluster nodes.

Note: Restarting the Cisco XCP Router does not update the Status message in the Cisco Cloud Onboarding Configuration window. If you complete the above procedure for all nodes and then return to the Cisco Cloud Onboarding Configuration window, the Status message will still say that you need to restart the Cisco XCP router. However, you need restart it only once on each IM and Presence cluster node.

Note: To disable Push Notifications, uncheck the Enable Push Notifications check box and click Save. After saving, restart the Cisco XCP Router on all IM and Presence Service cluster nodes.

What to do next

Enable Push Notifications High Availability, on page 15

Enable Push Notifications High Availability

Use this procedure to confirm that Push Notifications High Availability is enabled. This feature is required to provide redundancy and failover for Cisco Jabber on iPhone and iPad clients that are in suspended mode.

Procedure

Step 1: From Cisco Unified CM IM and Presence Administration, choose System > Service Parameters.

Step 2: From the Server drop-down, choose an IM and Presence node.

Step 3: From the Service drop-down, choose Cisco XCP Router (Active).

Step 4: Under Push Notifications (Clusterwide), set the Push Notifications High Availability service parameter to Enabled.

Step 5: Click Save.

Step 6: If you edited the setting of this service parameter, restart the Cisco XCP Router on all IM and Presence nodes. Otherwise, you can go to the next task:

a) From Cisco Unified Serviceability, choose Tools > Control Center - Network Services.

b) From the Server drop-down, choose an IM and Presence cluster node and click Go.

c) Select Cisco XCP Router and click Restart.
d) Repeat this procedure on all IM and Presence cluster nodes.

What to do next
Configure OAuth Refresh Logins in Unified Communications Manager, on page 16

Configure OAuth Refresh Logins

Complete these tasks to set up OAuth Refresh Logins for your Cisco Jabber deployment. OAuth Refresh Logins are an optional deployment that provides a faster login for Cisco Jabber.

Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Configure OAuth Refresh Logins in Unified Communications Manager, on page 16</td>
<td>Configure Refresh Logins with OAuth access tokens and refresh tokens in Cisco Unified Communications Manager.</td>
</tr>
<tr>
<td>Note</td>
<td>OAuth Refresh Logins are an optional deployment in Cisco Unified Communications Manager.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Confirm OAuth Configuration in Expressway, on page 17</td>
<td>If you have Cisco Expressway deployed, make sure that the OAuth Refresh Login configuration on Expressway matches your Cisco Unified Communications Manager configuration.</td>
</tr>
<tr>
<td>Note</td>
<td>OAuth Refresh Logins are enabled by default in Cisco Expressway, but are disabled by default in Cisco Unified Communications Manager. If you use the default settings for both systems, a configuration mismatch occurs.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 3</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Enable OAuth on Unity Connection, on page 18</td>
<td>In Cisco Unity Connection, enable OAuth Refresh Logins and assign the Cisco Unified Communications Manager publisher node as an Authz server.</td>
</tr>
</tbody>
</table>

Configure OAuth Refresh Logins in Unified Communications Manager

Use this procedure in Cisco Unified Communications Manager to configure Refresh Logins with OAuth access tokens and refresh tokens for Cisco Jabber clients. OAuth Refresh Logins provide a streamlined login flow that doesn't require Jabber users to re-login after network changes.
To ensure compatibility, make sure that the various Unified Communications components of your deployment, such as Cisco Jabber, Cisco Expressway and Cisco Unity Connection, support refresh logins. Once OAuth Refresh Logins are enabled, disabling the feature requires you to reset all Cisco Jabber clients.

Cisco recommends that you enable OAuth Refresh Logins, which are disabled by default in Cisco Unified Communications Manager, but are enabled by default in Cisco Expressway. If you are have both systems deployed, and you are using the default settings, you must either enable Refresh Logins in Cisco Unified Communications Manager or disable them in Cisco Expressway. Otherwise, a configuration mismatch results.

Procedure

Step 1  From Cisco Unified CM Administration, choose System > Enterprise Parameters.

Step 2  Under SSO Configuration, do either of the following:

- To enable OAuth Refresh Logins, set the OAuth with Refresh Login Flow enterprise parameter to Enabled.
- To disable OAuth Refresh Logins, set the OAuth with Refresh Login Flow enterprise parameter to Disabled. This is the default setting.

Step 3  If you enabled OAuth Refresh Logins, configure expiry timers for access tokens and refresh tokens by configuring the following enterprise parameters:

- OAuth Access Token Expiry Timer (minutes) — This parameter specifies the expiry timer, in minutes, for individual OAuth access tokens. The OAuth access token is invalid after the timer expires, but the Jabber client can request and obtain new access tokens without the user having to re-authenticate so long as the refresh token is valid. The valid range is from 1 - 1440 minutes with a default of 60 minutes.
- OAuth Refresh Token Expiry Timer (days) — This parameter specifies the expiry timer, in days, for OAuth refresh tokens. After the timer expires, the refresh token becomes invalid and the Jabber client must re-authenticate to get a new refresh token. The valid range is from 1 - 365 days with a default of 60 days.

Step 4  Click Save.

Note  Once you've saved the configuration, reset all Cisco Jabber clients.

What to do next

Make sure that the OAuth Refresh Login configuration in Cisco Expressway matches your Cisco Unified Communications Manager setting. For details, Confirm OAuth Configuration in Expressway, on page 17.

Confirm OAuth Configuration in Expressway

If you have Cisco Expressway deployed, make sure that the OAuth Refresh Login configuration on Expressway matches your Cisco Unified Communications Manager configuration.
OAuth Refresh Logins are enabled by default in Cisco Expressway, but are disabled by default in Cisco Unified Communications Manager. If you use the default settings for both systems, a configuration mismatch occurs. In Cisco Unified Communications Manager, OAuth Refresh Logins are configured via the **OAuth with Refresh Login Flow** enterprise parameter.

**Procedure**

**Step 1**
Sign in to Cisco Expressway-C.

**Step 2**
Choose **Configuration > Unified Communications > MRA Access Control**.

- If OAuth Refresh Logins are enabled in Cisco Unified Communications Manager, set the **Authorize by OAuth token with refresh** setting to **On**. This is the default setting.
- If OAuth Refresh Logins are disabled in Cisco Unified Communications Manager, set the **Authorize by OAuth token with refresh** setting to **Off**.

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

---

**Enable OAuth on Unity Connection**

If you have Cisco Unity Connection deployed and you are deploying OAuth Refresh Logins for Jabber, use this procedure to enable this feature in Unity Connection. As part of your OAuth configuration for Cisco Unity Connection, you must also assign the Cisco Unified Communications Manager publisher node as an Authz server.

**Procedure**

**Step 1**
Enable OAuth Refresh Logins on Cisco Unity Connection:

a) From Cisco Unity Connection Administration, choose **System Settings > Enterprise Parameters**.
b) Configure the settings under **SSO and OAuth Configuration**.
c) Set the **OAuth with Refresh Login** enterprise parameter to **Enabled**.
d) Click **Save**.

**Step 2**
Add the Cisco Unified Communications Manager publisher node as the Authz server for Cisco Unity Connection:

a) From Cisco Unity Connection Administration, choose **System Setting > Authz Server**.
b) Do one of the following:
   - To edit an existing Authz server configuration, select the server.
   - To add a new Authz server, click **Add New**.

c) Configure the fields on the page.
d) Click **Save**.
Refresh Settings from Expressway

Use this procedure to refresh settings on Cisco Expressway for Push Notifications. This will allow Expressway to sync configurations and certificates with Cisco Unified Communications Manager.

For detailed information on Cisco Expressway configurations, see the Cisco Expressway Administrator Guide for your release at the Expressway Maintain and Operate Guides page.

Procedure

Step 1 Log in to Expressway-C.
Step 2 Refresh the Cisco Unified Communications Manager servers:
   a) On the Expressway-C, go to Configuration > Unified Communications > Unified CM servers.
   b) Click Refresh Servers.
      Expressway synchronizes the Authz certificate with Cisco Unified Communications Manager.
Step 3 After the servers refresh, restart the Expressway-C. Until the restart, Expressway-C doesn’t recognize the push capability on the IM and Presence Service, and does not send PUSH messages to the Jabber clients:
   a) Select Maintenance > Restart options.
   b) Click Restart.

Configure Troubleshooting Options

Use this procedure on the Cisco Unified Communications Manager publisher node to configure parameters that determine how often you send Push Notifications alarms to the Cisco cloud, and for which alarm severities.

Before you begin

The Cisco Management Agent Service network service must be running for Cisco Unified Communications Manager to send Push Notifications alarms to the Cisco Cloud. You can confirm that the service is running in the Control Center - Network Services window of Cisco Unified Serviceability. The service is enabled by default.

Procedure

Step 1 Log in to the Command Line Interface.
Step 2 To configure how often Push Notifications alarms are sent to the cloud, run the `utils managementAgent alarms pushfrequency <minutes>` command where `<minutes>` represents an integer between 5 and 90 minutes. The default value is 30 minutes.
Step 3 To configure the minimum alarm severity for sending Push Notifications alarms to the Cisco Cloud, run the `utils managementAgent alarms minpushlevel <alarm_level>` command where `<alarm_level>` represents the minimum severity. Push Notifications alarms below this severity will not be sent to the Cisco Cloud.

For Push Notifications, the `<alarm_level>` options from most-to-least severe are as follows:
• Critical
• Error (Default value)
• Warning
• Notice
• Information

Step 4 If you want to send Push Notifications alarms to the Cisco Cloud immediately, and can't wait for the scheduled upload, run the `utils managementAgent alarms pushnow` command.

---

**Push Notifications Troubleshooting**

Push Notifications impacts many different components, some of which are hosted locally and some of which are in the cloud. It's important to configure Push Notifications troubleshooting so that Cisco TAC has the required information to troubleshoot system issues proactively.

**Send Troubleshooting information to Cisco Cloud**

By default, Cisco Unified Communications Manager sends Push Notifications troubleshooting information to the Cisco Cloud at regular intervals. Cisco may use this information for proactive debugging of Push Notifications and system components. This speeds up system troubleshooting by ensuring that Push Notifications alarms can be accessed quickly by Cisco TAC.

This option is enabled by default after Push Notifications is enabled, but administrators can disable it in the Cisco Cloud Onboarding Configuration window. When this option is enabled, Cisco Unified Communications Manager also generates a Customer Cluster ID and saves the ID in the customer's home Cisco Unified Communications Manager cluster. Customers who call Cisco TAC for Push Notifications issues must provide the ID so that TAC personnel can locate the customer's Push Notifications alarms.

**Personally-Identifiable Information (PII) Encryption**

You can also configure Cisco Unified Communications Manager to encrypt personally-identifiable information (PII) that is saved with the Push Notifications alarms. PII data includes any data that allows you to identify a specific person, such as a username, hostname, or device name. Select the Send encrypted PII to the Cisco Cloud for Troubleshooting option to enable this feature.

To provide greater security, the Cisco Support Token that decrypts the PII data is provided only in the Cisco Cloud Onboarding Configuration window of the customer's Cisco Unified Communications Manager server. Cisco cannot decrypt this data unless you provide the token. Customers who call Cisco TAC for Push Notifications issues must provide the token (assuming that PII encryption is configured) so that TAC can read the encrypted information with the Push Notifications alarms.

If you don't select this option, no personally-identifiable information is sent to the Cisco Cloud.

**CLI Commands for Troubleshooting Push Notifications**

Push Notifications provides the following CLI commands, which can be run on the Cisco Unified Communications Manager publisher node for troubleshooting:
• **utils managementAgent alarms pushfrequency**—Run this command to configure the interval following which Cisco Unified Communications Manager sends Push Notifications alarms to the Cisco Cloud. The default value is 30 minutes.

• **utils managementAgent alarms pushlevel**—Run this command to configure the minimum severity level for which Cisco Unified Communications Manager sends Push Notifications alarms to the Cisco Cloud. The default severity is **Error**.

• **utils managementAgent alarms pushnow**—Run this command to upload Push Notifications alarms to the Cisco Cloud immediately, without waiting for the interval to expire.

**Traces**

You can also run traces on the Cisco Management Agent Service and the Cisco Push Notification Service. By default, traces are set to the Info level and get saved to the following location:

- Cisco Management Agent Service—/var/log/active/cm/trace/cmas/log4j/
- Cisco Push Notification Service—/var/log/active/cm/trace/ccmpns/log4j/


**Upgrades from 11.5(1)SU2 with Push Notifications Enabled**

If you are upgrading from the 11.5(1)SU2 release and you had Push Notifications enabled in the old release, you must disable Push Notifications in the current release and then follow the onboarding process to enable Push Notifications once again. This is required due to API changes in this release that were not a part of the 11.5(1)SU2 release. Your upgraded system will not be able to send troubleshooting logs to the Cisco Cloud unless you disable Push Notifications and then follow the onboarding process for this release.

After you upgrade your system to the new release, do the following:

**Procedure**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
|        | Disable Push Notifications | Follow these steps:  
1. From Cisco Unified CM Administration, choose **Advanced Features > Cisco Cloud Onboarding**  
2. Uncheck the following check boxes:  
   - **Enable Push Notifications**  
   - **Send Troubleshooting information to the Cisco Cloud**  
   - **Send encrypted PII to the Cisco Cloud for troubleshooting**  
3. Click **Save**. |
### Update Refresh Token Manually

If you receive a 400 Bad Request message then your machine access token to the Push Notifications service has expired and you need to update the access token manually. Follow this process to update your access token manually.

<table>
<thead>
<tr>
<th>Step</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Install a new Cisco Unified Communications Manager server using the same version as the affected machine. For installation instructions, see the Installation Guide for Cisco Unified Communications Manager and the IM and Presence Service.</td>
</tr>
<tr>
<td>Step 2</td>
<td>License your new node</td>
</tr>
<tr>
<td></td>
<td>See the &quot;Smart Software Manager&quot; chapter of the System Configuration Guide for Cisco Unified Communications Manager.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Upload the necessary certificate chains to tomcat-trust and onboard your new node for Push Notifications</td>
</tr>
<tr>
<td></td>
<td>Follow the onboarding instructions in this document.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Verify that onboarding was successful</td>
</tr>
</tbody>
</table>
|         | Restart the Cisco Push Notification Service by running the `utils service restart Cisco Push Notification service` command. 
|         | View logs and ensure that a token was retrieved successfully.                                                                                                                                   |
| Step 5  | Get the refresh token from your new machine                                                                                                                                                     |
|         | On the original node with the expired token obtain machine details by running the `run sql select * from machine account details` CLI command.                                                       |
| Step 6  | Get the machine details from your original node                                                                                                                                                 |
|         | Run the `run sql * from machineaccountdetails` CLI command.                                                                                                                                      |
| Step 7  | Update the customer's refresh token                                                                                                                                                              |
|         | Run the `run sql update machineaccountdetails set refreshToken=<actual_token_text>` CLI command.                                                                                                  |
| Step 8  | Update the refresh token across your cluster                                                                                                                                                     |
|         | Run the following CLI command on all nodes across the Cisco Unified Communications Manager and IM and Presence Service clusters: `run sql select refreshToken from machineaccountdetails` |
Push Notifications Interactions and Restrictions

The following feature interactions and restrictions have been observed with Push Notifications.

Table 5: Feature Interactions and Restrictions for Push Notifications

<table>
<thead>
<tr>
<th>Feature</th>
<th>Interactions and Restrictions</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAT and Firewall Connections</td>
<td>Cisco recommends that you configure NAT and Firewall devices to keep idle TCP connections to the Push REST service open for at least 30 minutes. Push notifications do not get retried on new TCP connections when an error occurs on an existing connection. Keeping existing connections open ensures that errors are not introduced due to premature termination by NAT and Firewall devices.</td>
</tr>
<tr>
<td>Voice calls</td>
<td>For voice and video calls, where Cisco Jabber is in suspended mode, there may be a delay in connecting a call while the Push Notifications channel is established. After 5 seconds, if Unified CM hasn't received a ring back from the iOS device, Unified CM provides a ring on the calling device. If there is a delay in the Push Notifications process that prevents Unified CM from offering the call to the IOS device, Unified CM drops the call after 13 seconds.</td>
</tr>
</tbody>
</table>
## Interactions and Restrictions

<table>
<thead>
<tr>
<th>Feature</th>
<th>Interactions and Restrictions</th>
</tr>
</thead>
</table>
| Push Notifications High Availability | High Availability is supported for Push Notifications deployments as of 11.5(1)SU3. If Push Notifications is enabled, and a node fails over, the following occurs for Cisco Jabber on iPhone and iPad clients:  
  • For Cisco Jabber clients in foreground mode, the Jabber client logs in automatically to the backup node, which takes over until the main node recovers. There is no interruption in services, either when the backup node takes over, or when the main node recovers.  
  • For Cisco Jabber clients in background mode, the backup node takes over, but there is a delay before any Push Notifications are sent. Because the Jabber client is in background mode, it does not have an active connection to the network so it doesn’t log in automatically to the backup node. The backup node must recreate JSM sessions for all failed over users who were in background mode before any Push Notifications can be sent.  
  The length of the delay depends on the system load. Testing has shown that for a 15,000 user OVA with users evenly distributed in an HA pair, it takes 10-20 minutes for Push Notifications to be sent following a failover. This delay is observed when the backup node takes over, and again after the main node recovers.  
  **Note** In the event of a node failure or unexpected crash of the Cisco XCP Router, the user's IM session, including the IM history, is maintained without the need for any user action. However, if the Cisco Jabber on iPhone or iPad client was in suspended mode, it will be unable to retrieve unread messages that were queued on the server when it crashed.  
| Stopping the application without logging out | Stopping the application without logging out can cause inconsistent behavior with Push Notifications. This refers to these situations:  
  • On an iPhone, double-tapping the home button and swiping up.  
  • If the IOS stops the application randomly while Jabber is in the background.  
  To ensure that behavior remains consistent, log out of Cisco Jabber to stop the application.  |
CHAPTER 3

Push Notifications (Cloud Deployment)

- Cloud Deployments with WebEx Messenger, on page 25

Cloud Deployments with WebEx Messenger

At startup, Cisco Jabber for iPhone and iPad clients register both to Cisco WebEx Messenger and to the Apple cloud. If a Cisco Jabber for iPhone or iPad client moves into the background, the standard communication channel from WebEx Messenger to Cisco Jabber becomes unavailable. Push Notifications provides an alternative channel to reach the Jabber client.

For instant messages, an IM notification gets sent to the Jabber client via the Apple cloud. When the user clicks the IM notification, the Jabber client moves back into the foreground, resumes the session with WebEx Messenger, and downloads the instant message.

For voice and video calls, the call gets sent to the Jabber client via the Apple cloud. When the Cisco Jabber client receives the push notification, the client moves back to the foreground and the client rings.

Push Notifications Configuration

For IM-only cloud deployments, no configuration is required to enable Push Notifications—WebEx Messenger supports Push Notifications for Cisco Jabber on iPhone and iPad by default.

To add voice and video call support, you must onboard an on-premise Cisco Unified Communications Manager for Push Notifications. For details, refer to the prerequisites and configuration tasks in the chapter Push Notifications (On-Premises Deployments), on page 3.


Terminated Push Notifications for Cloud Deployments

If WebEx Messenger shuts down gracefully, a terminated push notification gets sent to the Cisco Jabber for iPhone or iPad client. The terminated push notification notifies the user of the server shutdown and notifies the user that all queued instant messages, Presence updates, and other XMPP stanzas (for example, chat room invites) are lost. The user must move Cisco Jabber back to the foreground to start a new session with Push Notifications enabled for the new session.

If the WebEx Messenger server fails, no terminated push notification is sent. All queued instant messages, Presence updates, and XMPP stanzas that are queued on the server and waiting to be delivered to the client,
are lost. The user must move Cisco Jabber back to the foreground to begin a new session with Push Notifications enabled in the new session.
CHAPTER 4

Certificates and Performance Monitoring

- Certificates for Cloud Connection, on page 27
- Push Notifications Alarms, on page 29
- Performance Counters for Push Notifications, on page 31
- Open Caveats - Release 11.5(1)SU3, on page 35

Certificates for Cloud Connection

For on-premises deployments, you must obtain and upload certificates manually if you choose not to have Cisco manage cloud certificates automatically, or if a new certificate requirement is added that was not included in your system installation file. In these instances, you will have to download certificates manually from the CA site and upload them to Cisco Unified Communications Manager and IM and Presence Service. To choose this option, uncheck the I want Cisco to manage the Cisco Cloud Service CA Certificates required for this trust check box in the Cloud Onboarding Configuration window in Cisco Unified Communications Manager.

Root Certificates for Cloud Connection

Refer to the below table for the root certificates that you must obtain if you are uploading certificates manually. For details on how to upload certificates to Cisco Unified Communications Manager and IM and Presence Service, see the "Manage Certificates" chapter of the Administration Guide for Cisco Unified Communications Manager. Make sure to select tomcat-trust as the Certificate Purpose.
Table 6: Root Certificates for Cloud Connection

<table>
<thead>
<tr>
<th>Cloud hosts signed by this CA</th>
<th>Must be trusted by</th>
<th>For this purpose</th>
<th>Issuing CA</th>
<th>Fingerprint (Thumbprint)</th>
</tr>
</thead>
</table>
| Common Identity (CI) service | Cisco Unified Communications Manager and IM and Presence Service | 1. Cisco Unified Communications Manager requests a CI machine token to authenticate with Cisco Push REST service.  
2. Secure https communication between Cisco Unified Communications Manager, IM and Presence Service, and the Cisco Push REST service. | O=QuoVadis Limited                                     | ca3afbcf1240364b44b216208880483919937cf7 | |
| Cisco Spark                  | Cisco Unified Communications Manager and IM and Presence Service | Cisco Unified Communications Manager communicates with Fusion Onboarding Service (FOS) to provision CI machine account. | O = The Go Daddy Group, Inc.  
OU = Go Daddy Class 2 Certification Authority | 27 96 ba e6 3f 18 01 e2  
77 26 1b a0 d7 77 70 02  
8f 20 ee e4 | |

Scenarios Where Cloud Certificates can be Uploaded Automatically

The following table shows whether onboarding will be successful with the I want Cisco to manage the Cisco Cloud Service CA certificates required for this trust check box selected in the Cisco Cloud Onboarding Configuration window, or whether certificates need to be uploaded manually for onboarding to be successful.

Table 7: Scenarios Where Cloud Certificates can be Uploaded Automatically

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Installation iso file included the required certificates?</th>
<th>You have chosen to have Cisco manage certificate requirements</th>
<th>Onboarding is Successful?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Onboarding for first time</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Onboarding for first time</td>
<td>No. The certificate requirements changed sometime after the installation iso was created</td>
<td>Yes</td>
<td>No. You must obtain and upload the new certificates manually. See the preceding table &quot;Root Certificates for Cloud Connection&quot;.</td>
</tr>
</tbody>
</table>
Onboarding is Successful?

You have chosen to have Cisco manage certificate requirements?

Installation iso file included the required certificates?

You have chosen to have Cisco manage certificate requirements?

Onboarding is Successful?

Scenario

You are already onboarded, but now a new certificate requirement has arisen

Your installation will not include the required certificates

Yes

Yes. The system can fetch and install new certificates automatically.

Push Notifications Alarms

The following table highlights alarms that were added to support Push Notifications call support in Cisco Unified Communications Manager and IM and Presence Service Release 11.5(1)SU3.

Table 8: Alarms for Push Notifications

<table>
<thead>
<tr>
<th>Alarm</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cisco CallManager Alarms</strong></td>
<td></td>
</tr>
</tbody>
</table>
| PushNotificationServiceUnavailable | **Description:** Unable to connect with Cisco Push Notification Service. The CallManager service requires a connection in order to send Push Notifications to the Cisco Cloud.  
**Severity:** ALERT_ALARM  
**Action:** In Cisco Unified Serviceability, check that the Cisco Push Notification Service status is running. If the service is stopped, start it. If the service is running, restart it. |
| PushNotificationInvalidDeviceTokenResponse | **Description:** Cloud returned Error code 410 for Push Notification sent from CallManager Service due to invalid device token. Push Notification for this IOS Jabber device will be stopped until valid device token is set by IOS Jabber device.  
**Severity:** ERROR_ALARM  
**Action:** User should log out and log back in to Jabber client on that IOS device. |
| PushNotificationServiceAccessTokenUnavailable | **Description:** Cisco Push Notification Service (CPNS) does not have a valid Access Token. Cisco Unified Communications Manager requires valid Access Token to send Push Notifications to Cloud. This Access Token is not available from Cloud due to authentication or network error.  
**Severity:** ALERT_ALARM  
**Action:** Check the Cisco Cloud Onboarding Configuration window to confirm that the onboarding process has completed successfully. If the issue persists contact Cisco TAC for further assistance. |

**Cisco Push Notification Service Alarms**
<table>
<thead>
<tr>
<th>Alarm</th>
<th>Description</th>
</tr>
</thead>
</table>
| StartFailed                                | **Description:** This alarm indicates that an internal failure prevented the Cisco Push Notification Service from starting  
|                                            | **Severity:** CRITICAL_ALARM  
|                                            | **Action:** Try restarting the Cisco Push Notification Service. If the issue persists check the Cisco Push Notification Service application logs and contact Cisco TAC for further assistance. |
| AccessTokenInvalid                         | **Description:** This alarm indicates that current access token is expired and become invalid and new access token is unavailable.  
|                                            | **Severity:** ALERT_ALARM  
|                                            | **Action:** Check the Cisco Cloud Onboarding Configuration window to confirm that the onboarding process has completed successfully. If the issue persists, contact Cisco TAC for further assistance. |
| HttpClientPoolCreationError               | **Description:** Indicates an error in creating the Http Client connection pool  
|                                            | **Severity:** ALERT_ALARM  
|                                            | **Action:** Check the Cisco Cloud Onboarding Configuration window and verify that the HTTP proxy settings are correct. In addition, verify that the on-boarding process has completed. |
| Cisco XCP Config Manager                   |                                                                 |
| PushNotificationFailed                     | **Description:** Cisco XCP Config Manager was not able to send Push Notification.  
|                                            | **Severity:** CRITICAL_ALARM  
|                                            | **Action:** Check the Error Code and follow the Error action that is directed. |
| PushNotificationFailedInvalidDeviceToken  | **Description:** An attempt to send a Push Notification to the Cisco Cloud failed due to an invalid device token.  
|                                            | **Severity:** CRITICAL_ALARM  
|                                            | **Action:** User should re-login to Jabber. |
| PushNotificationFailedInvalidAccessToken  | **Description:** An attempt to send a Push Notification to the Cisco Cloud failed due to an invalid access token.  
|                                            | **Severity:** CRITICAL_ALARM  
|                                            | **Action:** Look at the IM and Presence Service Cisco XCP Config Manager service logs to verify whether the AccessToken was fetched and refreshed on a timely basis. If the AccessToken was fetched and refreshed it on timely basis then do check the Cisco Cloud for further debugging. |
| AccessTokenFetchFailed                     | **Description:** Cisco XCP Config Manager was unable to fetch the Access Token.  
|                                            | **Severity:** CRITICAL_ALARM  
|                                            | **Action:** Check the Error Code and follow the Error action that is directed |
Cisco XCP Config Manager was unable to fetch the access token.

**Severity:**

**Action:** IM and Presence Service nodes must connect to the Cisco cloud to obtain the Access Token. Verify the following:

- Verify that the access token URL and refresh token are valid.
- Verify that the proxy details are correct on the **Cisco Cloud Onboarding** window.
- Check connectivity to the Cisco cloud.

An iOS Jabber client was unable to process a Push Notification.

**Severity:** ALERT_ALARM

**Action:** Contact Cisco TAC for further assistance.

Unread Messages alert

**Description:** An iOS Jabber client gets the following message: Unread messages might be deleted from server due to timeout. Please sign in Jabber to check unread messages.

**Severity:** ALERT_ALARM

**Conditions:** Cisco Jabber for iPhone running in the background. The user did not sign out of Cisco Jabber prior to closing the application.

---

### Performance Counters for Push Notifications

The following table shows the counters that have been added to the Cisco Unified Real Time Monitoring Tool to support Push Notifications for on-premises deployments of Cisco Unified Communications Manager and IM and Presence Service Release 11.5(1)SU3. Note that the counters increment only for specific APNS subscriber services (for example, APNS, APNS:beta, APNS:dev, APNS:test, APNS:load). For example, if the subscriber service is 'APNS:beta' only the APNS:beta counters increment, and none of the APNS:dev counters increment. The Cisco Jabber service type determines which subscriber service is used.

<table>
<thead>
<tr>
<th>RTMT Counter</th>
<th>Counter Description</th>
<th>Counter increments if the Subscriber service is set to...</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cisco CallManager Counters</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NumberOfPushReqSent</td>
<td>The total number of Push Notification Requests sent by the Cisco CallManager Service.</td>
<td>Any APNS Subscriber Services.</td>
</tr>
<tr>
<td>NumberOfPushResReceived</td>
<td>The total number of Push Notification Responses received by the Cisco CallManager Service.</td>
<td></td>
</tr>
<tr>
<td>NumberOfPushErrorResReceived</td>
<td>The total number of Push Notification Responses received by Cisco CallManager Service with response code other than 200 OK.</td>
<td></td>
</tr>
</tbody>
</table>
### RTMT Counter

<table>
<thead>
<tr>
<th>Counter Description</th>
<th>Counter increments if the Subscriber service is set to...</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cisco Mobility Manager Counters</strong></td>
<td></td>
</tr>
<tr>
<td>MobilityPushNotificationCallsExtendedToMIDueToTimeout</td>
<td>This represents the total number of calls sent to the Mobility Identity destination where Jabber did not register after receiving push notification before the &quot;Jabber Dual Mode (iPhone) Incoming Call Push Notification Wait Timer&quot; expired.</td>
</tr>
<tr>
<td>MobilityPushNotificationCallsExtendedToJabber</td>
<td>This represents the total number of calls sent to Jabber where Jabber registers successfully after receiving push notification before the &quot;Jabber Dual Mode (iPhone) Incoming Call Push Notification Wait Timer&quot; expired.</td>
</tr>
<tr>
<td><strong>Cisco XCP Config Manager Counters</strong></td>
<td></td>
</tr>
<tr>
<td>NumberOfPushSuccess</td>
<td>Number of successful Push Notifications sent.</td>
</tr>
<tr>
<td>NumberOfPushFailure</td>
<td>Number of failed attempts to send Push Notifications.</td>
</tr>
<tr>
<td>TargetInvalid</td>
<td>Total number of Push Notification failures due to an invalid target.</td>
</tr>
<tr>
<td>TargetExpired</td>
<td>Total number of Push Notification failures due to an expired target.</td>
</tr>
<tr>
<td><strong>Cisco XCP Push Counters</strong></td>
<td></td>
</tr>
<tr>
<td>PushEnabledSessionsApns</td>
<td>Number of push enabled sessions for APNS clients with APNS as the subscriber service. The counter gets incremented when push notifications is enabled and decrements when push notifications is disabled or a session terminates.</td>
</tr>
<tr>
<td>PushEnableReqRcvdApns</td>
<td>Number of push enable requests received for clients with APNS as the subscriber service, during the 60 second interval. This counter resets to 0 every 60 seconds.</td>
</tr>
<tr>
<td>PushErrorsApns</td>
<td>Number of push errors received during the 60 second interval. This counter resets to 0 every 60 seconds.</td>
</tr>
<tr>
<td>PushSentSilentApns</td>
<td>Number of messages sent to sessions in silent mode during the 60 second interval. This counter resets to 0 every 60 seconds.</td>
</tr>
<tr>
<td>PushSentDisconnApns</td>
<td>Number of messages sent to sessions in suspended state during the 60 second interval. This counter resets to 0 every 60 seconds.</td>
</tr>
<tr>
<td>RTMT Counter</td>
<td>Counter Description</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>--------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>PushEnabledSessionsApnsBeta</td>
<td>Number of push enabled sessions for clients with APNS:beta as the subscriber service. The counter gets incremented when push notifications is enabled and decrements when push notifications is disabled or a session terminates.</td>
</tr>
<tr>
<td>PushEnableReqRcvdApnsBeta</td>
<td>Number of push enable requests received for clients with APNS:beta as the subscriber service, during the 60 second interval. This counter resets to 0 every 60 seconds.</td>
</tr>
<tr>
<td>PushErrorsApnsBeta</td>
<td>Number of push errors received during the 60 second interval where the subscriber service is APNS:beta. This counter resets to 0 every 60 seconds.</td>
</tr>
<tr>
<td>PushSentSilentApnsBeta</td>
<td>Number of messages sent to sessions in silent mode during the 60 second interval where the subscriber service is APNS:beta. This counter resets to 0 every 60 seconds.</td>
</tr>
<tr>
<td>PushSentDisconnApnsBeta</td>
<td>Number of messages sent to sessions in suspended state during the 60 second interval where the subscriber service is APNS:beta. This counter resets to 0 every 60 seconds.</td>
</tr>
<tr>
<td>PushEnabledSessionsApnsDev</td>
<td>Number of push enabled sessions for clients with APNS:dev as the subscriber service. The counter gets incremented when push notifications is enabled and decrements when push notifications is disabled or a session terminates.</td>
</tr>
<tr>
<td>PushEnableReqRcvdApnsDev</td>
<td>Number of push enable requests received for clients with APNS:dev as the subscriber service, during the 60 second interval. This counter resets to 0 every 60 seconds.</td>
</tr>
<tr>
<td>PushErrorsApnsDev</td>
<td>Number of push errors received during the 60 second interval where the subscriber service is APNS:dev. This counter resets to 0 every 60 seconds.</td>
</tr>
<tr>
<td>PushSentSilentApnsDev</td>
<td>Number of messages sent to sessions in silent mode during the 60 second interval where the subscriber service is APNS:dev. This counter resets to 0 every 60 seconds.</td>
</tr>
<tr>
<td>PushSentDisconnApnsDev</td>
<td>Number of messages sent to sessions in suspended state during the 60 second interval where the subscriber service is APNS:dev. This counter resets to 0 every 60 seconds.</td>
</tr>
<tr>
<td>RTMT Counter</td>
<td>Counter Description</td>
</tr>
<tr>
<td>--------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>PushEnabledSessionsApnsLoad</td>
<td>Number of push enabled sessions for clients with APNS:load as the subscriber service. The counter gets incremented when push notifications is enabled and decrements when push notifications is disabled or a session terminates;</td>
</tr>
<tr>
<td>PushEnableReqRcvdApnsLoad</td>
<td>Number of push enable requests received for clients with APNS:load as the subscriber service, during the 60 second interval. This counter resets to 0 every 60 seconds.</td>
</tr>
<tr>
<td>PushErrorsApnsLoad</td>
<td>Number of push errors received during the 60 second interval where the subscriber service is APNS:load. This counter resets to 0 every 60 seconds.</td>
</tr>
<tr>
<td>PushSentSilentApnsLoad</td>
<td>Number of messages sent to sessions in silent mode during the 60 second interval where the subscriber service is APNS:load. This counter resets to 0 every 60 seconds.</td>
</tr>
<tr>
<td>PushSentDisconnApnsLoad</td>
<td>Number of messages sent to sessions in suspended state during the 60 second interval where the subscriber service is APNS:load. This counter resets to 0 every 60 seconds.</td>
</tr>
<tr>
<td>PushEnabledSessionsApnsTest</td>
<td>Number of push enabled sessions for clients with APNS:test as the subscriber service. The counter gets incremented when push notifications is enabled and decrements when push notifications is disabled or a session terminates.</td>
</tr>
<tr>
<td>PushEnableReqRcvdApnsTest</td>
<td>Number of push enable requests received for clients with APNS:test as the subscriber service, during the 60 second interval. This counter resets to 0 every 60 seconds.</td>
</tr>
<tr>
<td>PushErrorsApnsTest</td>
<td>Number of push errors received during the 60 second interval where the subscriber service is APNS:test. This counter resets to 0 every 60 seconds.</td>
</tr>
<tr>
<td>PushSentSilentApnsTest</td>
<td>Number of messages sent to sessions in silent mode during the 60 second interval where the subscriber service is APNS:test. This counter resets to 0 every 60 seconds.</td>
</tr>
<tr>
<td>PushSentDisconnApnsTest</td>
<td>Number of messages sent to sessions in suspended state during the 60 second interval where the subscriber service is APNS:test. This counter resets to 0 every 60 seconds.</td>
</tr>
</tbody>
</table>
Open Caveats - Release 11.5(1)SU3

The following table lists open caveats for deploying the Push Notifications solution with Release 11.5(1)SU3 of Cisco Unified Communications Manager and IM and Presence Service. These issues may cause unexpected behavior. Bugs are listed in alphabetical order by component and then in numerical order by severity.

**Table 9: Open Caveats - Release 11.5(1)SU3**

<table>
<thead>
<tr>
<th>Defect</th>
<th>Severity</th>
<th>Component</th>
<th>Headline</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCve85731</td>
<td>3</td>
<td>cpi-platform-api</td>
<td>Cluster manager does not recover after network error causing switch version to fail.</td>
</tr>
<tr>
<td>CSCf42769</td>
<td>3</td>
<td>ccm-serviceability</td>
<td>Cisco Support Token &quot;null&quot; after Cloud Onboarding</td>
</tr>
<tr>
<td>CSCf57440</td>
<td>3</td>
<td>voice-cpns</td>
<td>No push is sent to devices during rapid link OOS and link ISV between nodes.</td>
</tr>
<tr>
<td>CSCf66551</td>
<td>3</td>
<td>sync-agent</td>
<td>ReplWatcher allows dependent services to start after reading old sync status</td>
</tr>
<tr>
<td>CSCf78576</td>
<td>4</td>
<td>any</td>
<td>MRA - allow more auth methods when checking internally and token refresh in use</td>
</tr>
<tr>
<td>CSCf80854</td>
<td>4</td>
<td>ucm-signaling</td>
<td>Voice push, JCC connected too long(APNS-142): edge configure error with VCSe/c/CUCM not matched</td>
</tr>
<tr>
<td>CSCf81528</td>
<td>4</td>
<td>general</td>
<td>Long time to stop/start spService</td>
</tr>
<tr>
<td>CSCf81540</td>
<td>3</td>
<td>general</td>
<td>Jabber cannot connect phone service - voice push - SIP task blocked by receive UDP message</td>
</tr>
</tbody>
</table>
Push Notifications Support in Release 11.5(1)SU2

If your deployment includes Cisco Jabber on iPhone and iPad clients, Cisco highly recommends that you upgrade to a minimum release of Cisco Unified Communications Manager 11.5(1)SU3 to receive full support for the Push Notifications solution with voice and video calling as well as high availability for instant messaging.

Note

If you are currently running Release 11.5(1)SU2 with Push Notifications and don't want to upgrade, Release 11.5(1)SU2 provides limited Push Notifications support for IM and Presence. Refer to the contents of this appendix for Push Notifications information that is relevant to your release.

Release 11.5(1)SU2 provides Push Notification support for IM and Presence (without High Availability)

The following restrictions apply to the Push Notifications feature with Release 11.5(1)SU2:

• High Availability for IM and Presence is not supported for Jabber on Cisco iPhone and iPad.
• Voice call support—Cisco Jabber on iPhone and iPad clients cannot receive incoming voice calls when the Jabber client is in suspended mode. If you want to use Jabber on iPhone or iPad for calling, configure Single Number Reach.

Minimum Releases

IM and Presence support is provided for Push Notifications in Cisco Unified Communications Manager and IM and Presence Service Release 11.5(1)SU2 with the following minimum compatible releases:

• Cisco Prime License Manager 11.5(1)SU2 in a co-resident deployment or 11.5.1SU1 (Build11.5.1.10000-4) in a standalone deployment.
• Cisco Jabber 11.8.1
• Cisco Expressway x8.9 (if MRA is deployed)
Terminated Push Notifications for Service Shutdowns

Terminated Push Notifications are included with Release 11.5(1)SU2 only. The Push Notifications High Availability feature introduced with 11.5(1)SU3 replaces Terminated Push Notifications.

When a Cisco Jabber for iPhone and iPad client begins running in the background, the IM and Presence Service queues all instant messages, Presence updates, and other XMPP stanzas (for example, chat room invites) on the local server. Only when the Jabber user clicks on an IM notification, or moves the client back to the foreground, does the IM and Presence Service send all queued messages to the Jabber client.

If the Cisco XCP router stops or is restarted (for example, an administrator restarts the service for a configuration change or upgrade), the IM and Presence Service flushes out the message queue resulting in all queued messages being lost.

However, before the service shuts down, the IM and Presence Service sends a terminated push notification to Cisco Jabber for iPhone and iPad clients notifying them that the service is shutting down and that all queued messages are lost. The Jabber user must move the client back to the foreground to create a new session so that Push Notifications are enabled in this new session.

Failover Situations

If a node fails suddenly, no terminated push notification gets sent and all instant messages, Presence updates, and XMPP stanzas that were queued on the failed node are lost. If High Availability is configured for IM and Presence, the backup node in the Presence Redundancy Group takes over, but the queue on the failed node is still lost. When the backup node takes over, it sends an iOS system notification to the user and the user must click the notification to bring Jabber back to the foreground and create a new session. Push Notifications is not enabled until the new session is created.

Push Notifications Configuration Task Flow - Release 11.5(1)SU2

Complete the following tasks to configure Push Notifications in Release 11.5(1)SU2.

Before you begin

Push Notifications Prerequisites, on page 8

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Synchronize Licenses, on page 39</td>
</tr>
</tbody>
</table>
Purpose

Command or Action | Purpose
--- | ---
Step 2 | Open Ports for Push Notifications in Release 11.5(1)SU2, on page 39
Step 3 | Enable Push Notifications (Release 11.5(1)SU2), on page 40
Step 4 | Restart Expressway-E

Note

For Mobile and Remote Access (MRA) deployments with Cisco Expressway, see the Mobile and Remote Access via Cisco Expressway Deployment Guide at the below URL for information about Push Notifications with Expressway.


Synchronize Licenses

Procedure

Step 1 | In Cisco Prime License Manager, select the Product Instance tab.
Step 2 | Click Synchronize Licenses.

Open Ports for Push Notifications in Release 11.5(1)SU2

Make sure that the following outbound ports are open in Cisco Unified Communications Manager, IM and Presence Service, and in your Cisco Jabber for iPhone or iPad client.

Table 10: Port Requirements for Push Notifications in Release 11.5(1)SU2

<table>
<thead>
<tr>
<th>From</th>
<th>To</th>
<th>Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Unified Communications Manager</td>
<td>Cisco cloud</td>
<td>443/TCP</td>
<td>HTTPS-based Subscription requests to Fusion Onboarding Service at fos-a.wbx2.com from publisher node</td>
</tr>
<tr>
<td>From</td>
<td>To</td>
<td>Port</td>
<td>Port Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>------------------------</td>
<td>------</td>
<td>----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>IM and Presence Service</td>
<td>Cisco cloud</td>
<td>443/TCP</td>
<td>HTTPS-based communications:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Authentication requests to Common Identity Service at idbroker.webex.com</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Push notifications to the Push REST service at push.webexconnect.com</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>This port should be open for all cluster nodes.</td>
</tr>
<tr>
<td>Cisco Jabber client</td>
<td>Apple cloud</td>
<td>5223/TCP</td>
<td>Communications with Apple Push Notification service.</td>
</tr>
<tr>
<td>(when operating behind a firewall)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cisco Jabber client</td>
<td>Apple cloud</td>
<td>443/TCP</td>
<td>Fallback port for 5223 if wi-fi is used.</td>
</tr>
</tbody>
</table>

**Note**

In addition, port 9966 is used internally by the Cisco Push Notification Service to communicate with the Cisco CallManager Service on all Cisco Unified Communications Managers cluster nodes. This port needs to be open in the firewall if communication between nodes in your cluster traverse through a firewall (for example the nodes are located in a different subnet if as an example they are clustered over the WAN). In this case, this port needs to be open in the firewall so that these services can communicate.

---

**Enable Push Notifications (Release 11.5(1)SU2)**

Use this procedure in Release 11.5(1)SU2 to set up the Push Notifications feature for Cisco Jabber for iPhone and iPad clients in your Cisco Unified Communications Manager and IM and Presence Service cluster.

**Note**

With this release, Push Notifications provides instant messaging support. For Push Notifications call support, upgrade to at least release 11.5(1)SU3.

**Before you begin**

Make sure that port 443 is open from the Cisco Unified Communications Manager publisher node for outbound HTTPS requests.

**Procedure**

**Step 1**

Log in to the Cisco Unified Communications Manager publisher node.

**Step 2**

From Cisco Unified CM Administration, choose **Advanced Features > Cisco Cloud Onboarding**.
Step 3  Check the **Enable Push Notifications and Send Troubleshooting and Analytics Information to Cisco Cloud** check box.

Step 4  Check the **I want Cisco to manage the Cisco Cloud Service CA Certificates required for this trust** check box to have the system update certificates automatically.

**Note**  If you leave the check box unchecked, you will have to obtain CA certificates manually and copy them to Cisco Unified Communications Manager and IM and Presence Service. For details, see *Certificates for Cloud Connection*, on page 27.

Step 5  If you want to use an HTTP Proxy, check the **Enable HTTP Proxy** check box and enter the server details.

Step 6  Click **Save**.

Step 7  On the publisher node only, restart the Cisco Tomcat service to install Cisco-managed certificates.
   a)  Log in to the Command Line Interface.
   b)  Run the `utils service restart Cisco Tomcat` command.

Step 8  After the Cisco Tomcat service restarts, return to the **Cisco Cloud Onboarding Configuration** window. The **Status** indicates that "Cisco Cloud Onboarding Pending".

Step 9  Make sure the following check boxes are checked. You may need to recheck them:

   - Enable Push Notifications and Send Troubleshooting and Analytics Information to Cisco Cloud
   - I want Cisco to manage the Cisco Cloud Service CA Certificates required for this trust

Step 10  Click **Save**

   The cluster initiates a Push Notifications subscription request. When the request completes, and Push Notifications is enabled, the **Status** field displays the message "Cloud Onboarding Completed".

Step 11  Restart the **Cisco XCP Router** service for all IM and Presence Service cluster nodes:
   a)  Click the **Control Center - Network Services** link that appears in the **Status** area of the Cisco Cloud Onboarding window. If no link appears, log in to the Cisco Unified Serviceability interface and select **Tools > Control Center - Network Services**.
   b)  From the **Server** drop-down list box, choose the IM and Presence database publisher node, and click **Go**.
   c)  Under **IM and Presence Services**, select the **Cisco XCP Router** service.
   d)  Click **Restart**.
   e)  Repeat this step for all IM and Presence cluster nodes.

**Note**  Restarting the Cisco XCP Router does not update the **Status** message in the **Cisco Cloud Onboarding Configuration** window of Cisco Unified Communications Manager. If you complete the above procedure for all nodes and then return to the **Cisco Cloud Onboarding Configuration** window, the **Status** message will still say that you need to restart the Cisco XCP Router. However, you need restart it only once on each IM and Presence cluster node.

**Note**  If you want to disable Push Notifications, uncheck the **Enable Push Notifications and Send Troubleshooting and Analytics Information to Cisco Cloud** check box and click **Save**. After saving, restart the Cisco XCP Router on all IM and Presence Service cluster nodes.

---

### What to do next

If your deployment includes Cisco Expressway, restart the Expressway-E. Otherwise Expressway-E doesn't recognize the push capability on the IM and Presence Service, and does not send PUSH messages to Jabber.
clients. For details, see the *Cisco Expressway Administrator Guide* at the [Expressway Maintain and Operate Guides](#) page.

## Push Notifications Counters in 11.5(1)SU2

Release 11.5(1)SU2 contains a subset of the counters that are available with Release 11.5(1)SU3. With Release 11.5(1)SU2 the following *Cisco XCP Config Manager* counters provide Push Notifications information:

- NumberOfPushSuccess
- NumberOfPushFailure
- TargetInvalid
- TargetExpired

The following *Cisco XCP Push* performance counters provide Push Notifications information for 11.5(1)SU2:

- PushEnabledSessionsApns
- PushEnableReqRcvdApns
- PushErrorApns
- PushSentSilentApns
- PushSentDisconnApns
- PushEnabledSessionsApnsBeta
- PushEnableReqRcvdApnsBeta
- PushErrorApnsBeta
- PushSentSilentApnsBeta
- PushSentDisconnApnsBeta
- PushEnabledSessionsApnsDev
- PushEnableReqRcvdApnsDev
- PushErrorApnsDev
- PushSentSilentApnsDev
- PushSentDisconnApnsDev
- PushEnabledSessionsApnsLoad
- PushEnableReqRcvdApnsLoad
- PushErrorApnsLoad
- PushSentSilentApnsLoad
- PushSentDisconnApnsLoad
- PushEnabledSessionsApnsTest
• PushEnableReqRcvdApnsTest
• PushErrorApnsTest
• PushSentSilentApnsTest
• PushSentDisconnApnsTest

For descriptions of these counters, see Performance Counters for Push Notifications, on page 31.

### Open Caveats - Release 11.5(1)SU2

The following table lists open caveats for deploying the Push Notifications solution with Release 11.5(1)SU2 of Cisco Unified Communications Manager and IM and Presence Service. These issues may cause unexpected behavior. Bugs are listed in alphabetical order by component and then in numerical order by severity.

**Table 11: Open Caveats - Release 11.5(1)SU2**

<table>
<thead>
<tr>
<th>Defect</th>
<th>Severity</th>
<th>Component</th>
<th>Headline</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCvc71472</td>
<td>3</td>
<td>xcp</td>
<td>MRA jabber user disconnect</td>
</tr>
<tr>
<td>CSCvc86151</td>
<td>3</td>
<td>xcp-router</td>
<td>XCP Router stuck during the shutdown phase</td>
</tr>
<tr>
<td>CSCvc86422</td>
<td>3</td>
<td>xcp-router</td>
<td>XCP Router which wrongly increments JSM received stanzas counter.</td>
</tr>
<tr>
<td>CSCvd09710</td>
<td>3</td>
<td>xcp-router</td>
<td>Jabber client receives duplicate push notifications for the same message</td>
</tr>
</tbody>
</table>

---

**Push Notifications Deployment for Cisco Jabber on iPhone and iPad with Cisco Unified Communications Manager**

---

**Open Caveats - Release 11.5(1)SU2**

The following table lists open caveats for deploying the Push Notifications solution with Release 11.5(1)SU2 of Cisco Unified Communications Manager and IM and Presence Service. These issues may cause unexpected behavior. Bugs are listed in alphabetical order by component and then in numerical order by severity.

**Table 11: Open Caveats - Release 11.5(1)SU2**

<table>
<thead>
<tr>
<th>Defect</th>
<th>Severity</th>
<th>Component</th>
<th>Headline</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCvc71472</td>
<td>3</td>
<td>xcp</td>
<td>MRA jabber user disconnect</td>
</tr>
<tr>
<td>CSCvc86151</td>
<td>3</td>
<td>xcp-router</td>
<td>XCP Router stuck during the shutdown phase</td>
</tr>
<tr>
<td>CSCvc86422</td>
<td>3</td>
<td>xcp-router</td>
<td>XCP Router which wrongly increments JSM received stanzas counter.</td>
</tr>
<tr>
<td>CSCvd09710</td>
<td>3</td>
<td>xcp-router</td>
<td>Jabber client receives duplicate push notifications for the same message</td>
</tr>
</tbody>
</table>

---

**Push Notifications Deployment for Cisco Jabber on iPhone and iPad with Cisco Unified Communications Manager**

---