Configure System and Enterprise Parameters

Initial System and Enterprise Parameters Overview

Consider the following system-wide parameters when you set up a Unified Communications Manager node for the first time. You can modify system-wide parameters for your deployment if needed; however, the recommended default settings should work in most cases.

- Set the fall-back connection monitor duration for IP phones.
- Allow searches of the corporate directory for all users.
- Set the Fully Qualified Directory Number (FQDN) for the cluster and the top-level domain for the organization.
- Set the Cisco Jabber start condition for video.
- (Optional) Enable Multi-Level Precedence and Preemption (MLPP) if your cluster uses MLPP.
- (Optional) Enable IPv6 if your network uses IPv6.
- (Optional) Enter a remote syslog server name.
- (Optional) Set up call trace log to troubleshoot your deployment.
- (Optional) Enable dependency records.

Initial System and Enterprise Configuration Task Flow

Before you begin

Set up your Unified Communications Manager node and port settings.

Procedure

	Command or Action	Purpose
Step 1	Configure Initial System and Enterprise Parameters, on page 2	Configure the system-wide parameters that are required for an initial setup of your Unified Communications Manager node. For a list of the recommended system settings, see Common Enterprise Parameters, on page 4.
Step 2	Configure SSO Login Behavior for Cisco Jabber on iOS, on page 8	Configure the enterprise parameter that is required to allow Cisco Jabber to perform certificate-based authentication with the IdP in a controlled mobile device management (MDM) deployment.
Step 3	Configure SSO for RTMT, on page 9	Configure the enterprise parameter through Unified Communications Manager to enable SAML SSO for Real-Time Monitoring Tool (RTMT).

What to do next

Configure some core settings for device pools to lay a foundation of common settings to apply across all devices that are configured in the Unified Communications Manager cluster, see Core Settings for Device Pools Configuration Task Flow .

Configure Initial System and Enterprise Parameters

You can use Cisco Unified Communications Manager Administration to configure system and enterprise parameters for your particular deployment. Although we've listed parameters that are important for an initial system setup, the recommended default settings work for most deployments.

Parameters that are useful for troubleshooting, such as enabling call trace logs, should be disabled after you are finished troubleshooting so that network performance is not impacted.

Most parameters require that you reset all devices for the changes to take effect. Consider completing all configuration steps before you perform a reset of all devices. We recommend that you reset all devices during off-peak hours.

Note From Release 10.0(1), the same enterprise parameters are used on Unified Communications Manager and IM and Presence Service. If you change the value of an enterprise parameter on IM and Presence Service, the changed value is automatically updated to Unified Communications Manager.

Procedure

Step 1 In Cisco Unified Communications Manager Administration, choose **System** > **Enterprise Parameters**.

Step 2 In the **Enterprise Parameters Configuration** section, enter the number of seconds in the **Connection Monitor Duration** field before a IP phone in the cluster falls back to the primary node when the TCP connection becomes available, then click **Save**. The default value is 120 seconds.

Tip To apply the changes to all affected devices in the cluster without resetting all devices, click **Apply Config**, and then click **OK**.

Step 3 In the **User Data Service Parameters** section, select **True** in the **Enable All User Search** field to allow users to search the corporate directory for all users when no last name, first name, or directory number is specified.

Step 4 In the **Clusterwide Domain Configuration** section, set up the clusterwide domain.

a) Enter the top-level domain for the organization in the **Organization Top Level Domain** field. The maximum length is 255 characters.

b) Enter the Fully Qualified Domain Name (FQDN) for the cluster in the **Cluster Fully Qualified Domain Name** field. The maximum length is 255 characters.

Multiple FQDNs must be separated by a space. Wildcards can be specified within an FQDN using an asterisk (*). Example: cluster-1.cisco.com *.cisco.com.

Step 5 In the Cisco Jabber section, select **False** in the **Never Start Call with Video** field.

Step 6 (Optional) In the **MLPP and Confidential Access Level Parameters** section, enter the Multi-Level Precedence and Preemption (MLPP) domain and enable devices to use MLPP.

a) Enter the domain for the MLPP service in the **MLPP Domain Identifier** field. This parameter accepts hexadecimal values starting with 0x.

b) Select **MLPP indication turned on** in the **MLPP Indication Status** field.

Step 7 (Optional) In the **IPv6** section, set the **Enable IPv6** field to **True**.

Step 8 (Optional) In the **Cisco Syslog Agent** section, enter the name or IP address of the remote Syslog server in the **Remote Syslog Server Name 1** field. If a server name is not specified, Cisco Unified Serviceability does not send the Syslog messages.

Step 9 (Optional) In the **Call Trace Log Configuration for Session Trace** section, set up the call trace log to allow the collection of SIP call information for session traces.

The Session Trace feature in the Real-Time Monitoring Tool (RTMT) uses this information to generate call flow diagrams that are useful for troubleshooting.

a) Set the **Enable Call Trace Log** field to **True**.

b) Enter the maximum number of SIP call trace log files that Unified Communications Manager can generate in the **Max Number of Call Trace Log Files** field.

The default value is 2000. Valid range is from 5 to 4000.

c) Enter the maximum file size, in megabytes, of the SIP call trace log files in the **Call Trace Log** field.

The default value is 2. Valid range is from 1 to 10.

Note Some performance degradation can occur during periods of high SIP call traffic. To reduce the impact on system performance, set the Cisco CallManager service parameter called **Log Call-Related REFER/NOTIFY/SUBSCRIBE SIP Messages for Session Trace** to False. This will omit the REFER, NOTIFY, and SUBSCRIBE messages from the SIP call tracing.

Step 10 In the in the **CCMAdmin Parameters** section, select **True** in the **Enable Dependency Records** field.

Step 11 Click **Save**.

Step 12 Click **Reset**, and then click **OK** to reset all devices.

We recommend that you reset all devices during off-peak hours.

Tip To reset all devices, you can reset every device pool in the system.

Common Enterprise Parameters

The following table lists common enterprise parameters that are used to set enterprise settings such as Organization Top-Level Domain or Cluster Fully Qualified Domain Name. For a detailed list, use the **System** > **Enterprise Parameters** menu in Cisco Unified CM Administration.

Table 1: Common Enterprise Parameters for an Initial Unified Communications Manager Setup

Parameter Name	Description
Enterprise Parameters	
Connection Monitor Duration	If an IP phone in the cluster registers on a secondary node, use this parameter to set the amount of time that the IP phone waits before it falls back and re-registers with the primary node after the primary node becomes available. This parameter affects all secure devices for a specific Secure Survivable Remote Site Telephony (SRST) router. For more information, see *Security Guide for Cisco Unified Communications Manager*. Default: 120 seconds Restart all services for the changes to take effect.
CCMAdmin Parameters	
Enable Dependency Records	This parameter is used to display dependency records that are required for troubleshooting. Displaying the dependency records may be beneficial during an initial system setup. Displaying the dependency records could lead to high CPU usage spikes and could impact call processing. To avoid possible performance issues, disable this parameter after the system setup is complete. We recommend displaying dependency records only during off-peak hours or during a maintenance window. When enabled, you can select **Dependency Records** from the **Related Links** drop-down list, which is accessible from most configuration windows using Unified Communications Manager. Default: False
User Data Service Parameters	

Parameter Name	Description
Enable All User Search	This parameter allows you to search the corporate directory for all users when no last name, first name, or directory number is specified. This parameter also applies to directory searches on the **Cisco CallManager Self Care** (CCMUser) window. Default: True
Clusterwide Domain Configuration	
Organization Top Level Domain	This parameter defines the top-level domain for the organization. For example, cisco.com. Maximum length: 255 characters Allowed values: A valid domain using upper and lowercase letters, numbers (0-9), hyphens, and dots (as a domain label separator). Domain labels must not start with a hyphen. The last label must not start with a number. For example, this domain is invalid -cisco.1om.
Cluster Fully Qualified Domain Name	This parameter defines one or more Fully Qualified Domain Names (FQDN) for the cluster. Multiple FQDNs must be separated by a space. Specify wildcards within an FQDN using an asterisk (*). Example: `cluster-1.cisco.com *.cisco.com`. Requests containing URLs, such as SIP calls, that have a host portion that matches any of the FQDNs in this parameter are routed to that cluster and the attached devices. Maximum length: 255 characters Allowed values: An FQDN or a partial FQDN using the * wildcard. Upper and lowercase letters, numbers (0-9), hyphens, and dots (as a domain label separator). Domain labels must not start with a hyphen. The last label must not start with a number. For example, this domain is invalid -cisco.1om.
IPv6	

Parameter Name	Description
Enable IPv6	This parameter determines whether Unified Communications Manager can negotiate Internet Protocol Version 6 (IPv6) and whether phones are allowed to advertise IPv6 capability. IPv6 must be enabled on all other network components including on the platform of all nodes before you enable this parameter. Otherwise, the system continues to run in IPv4-only mode. This is a required field. Default: False (IPv6 is disabled) You must restart the following services for the IPv6 parameter change to take effect, and the affected services in the IM and Presence Service cluster. • Cisco CallManager • Cisco IP Voice Media Streaming App • Cisco CTIManager • Cisco Certificate Authority Proxy Function
Cisco Syslog Agent	
Remote Syslog Server Name 1	Enter the name or IP address of the remote Syslog server. Cisco Unified Serviceability do not send the Syslog messages if a server name is not specified. This parameter is required only if you are using the Syslog server for logs. Maximum length: 255 characters Allowed values: A valid remote Sylog server name using upper and lowercase letters, numbers (0-9), hyphens, and dots. Do not specify another Unified Communications Manager node as the destination.
Cisco Jabber	
Never Start Call with Video	This parameter determines if video is sent when a video call starts. Select **True** to start video calls without immediately sending video. Anytime during the video call, you can choose to start sending your video. This parameter overrides any IM and Presence Service preferences. When set to False, video calls start according to the preferences set in IM and Presence Service. Default: False.
SSO and OAuth Configuration	

Parameter Name	Description
SSO Login Behavior for iOS	This parameter is required to allow Cisco Jabber to perform the certificate-based authentication with the IdP in a controlled mobile device management (MDM) deployment. The **SSO Login Behavior for iOS** parameter includes the following options: • **Use Embedded Browser**—If you enable this option, Cisco Jabber uses the embedded browser for the SSO authentication. Use this option to allow iOS devices prior to version 9 to use SSO without cross-launching into the native Apple Safari browser. • **Use Native Browser**—If you enable this option, Cisco Jabber uses the Apple Safari framework on an iOS device to perform the certificate-based authentication with an Identity Provider (IdP) in the MDM deployment. **Note** We do not recommend configuring this option, except in a controlled MDM deployment, because using a native browser is not as secure as the using the embedded browser. This is a required field. Default: Use the embedded browser (WebView).
OAuth with Refresh Login Flow	This parameter controls the login flow used by clients such as Cisco Jabber when connecting to Unified Communications Managers. • Enabled—If you enable this option, clients can use an oAuth-based Fast Login flow to provide a quicker and streamlined login experience, without requiring the user input to re-log in. For example, due to a network change. The option requires support from the other components of the Unified Communications solution, such as Expressway and Unity Connection (compatible versions with the refresh login flow enabled). • Disabled—If you enable this option, the existing behavior is preserved and is compatible with older versions of other system components. **Note** For Mobile and Remote Access deployment with Cisco Jabber, we recommend enabling this parameter only with a compatible version of Expressway that supports oAuth with Refresh login flow. Incompatible version may impact the Cisco Jabber functionality. Please refer the specific product documents for supported version and configuration requirements. This is a required field. Default: Disabled.

Parameter Name	Description
Use SSO for RTMT	This parameter is configured to enable SAML SSO for Real-Time Monitoring Tool (RTMT). The **Use SSO for RTMT** parameter includes the following options: • **True**—If you choose this option, RTMT displays the SAML SSO-based IdP sign-in window. **Note** When you perform a fresh install, the default value of the **Use SSO for RTMT** parameter appears as **True**. • **False**—If you choose this option, RTMT displays the basic authentication sign-in window. **Note** When you perform an upgrade from a Cisco Unified Communications Manager version where **Use SSO for RTMT** parameter does not exist, the default value of this parameter in the newer version appears as **False**. This is a required field. Default: True.

Configure SSO Login Behavior for Cisco Jabber on iOS

Procedure

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

Step 2 To configure the opt-in control, in the SSO Configuration section, choose the **Use Native Browser** option for the **SSO Login Behavior for iOS** parameter:

Note The **SSO Login Behavior for iOS** parameter includes the following options:

- **Use Embedded Browser**—If you enable this option, Cisco Jabber uses the embedded browser for SSO authentication. Use this option to allow iOS devices prior to version 9 to use SSO without cross-launching into the native Apple Safari browser. This option is enabled by default.
- **Use Native Browser**—If you enable this option, Cisco Jabber uses the Apple Safari framework on an iOS device to perform certificate-based authentication with an Identity Provider (IdP) in the MDM deployment.

  Note We don't recommend to configure this option, except in a controlled MDM deployment, because using a native browser is not as secure as the using the embedded browser.

Step 3 Click **Save**.

Configure SSO for RTMT

Procedure

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

Step 2 To configure SSO for RTMT, in the SSO Configuration section, choose **True** for the **Use SSO for RTMT** parameter:

Note The **Use SSO for RTMT** parameter includes the following options:

- **True**—If you choose this option, RTMT displays the SAML SSO-based IdP sign-in window.

  Note When you perform a fresh install, the default value of the **Use SSO for RTMT** parameter appears as **True**.

- **False**—If you choose this option, RTMT displays the basic authentication sign-in window.

  Note When you perform an upgrade from a Cisco Unified Communications Manager version where **Use SSO for RTMT** parameter does not exist, the default value of this parameter in the newer version appears as **False**.

Step 3 Click **Save**.