Changing the IP Address and Hostname for Cisco Unified Communications Manager and IM and Presence Service, Release 12.5(1)

First Published: 2019-01-17

Last Modified: 2025-02-14

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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2019 Cisco Systems, Inc. All rights reserved.

CONTENTS

CHAPTER 1 **IP Address, Hostname, and Other Network Identifier Changes** 1

IP Address, Hostname, and Other Network Identifier Changes 1

IM and Presence Service Node Name and Default Domain Name Changes 1

Procedure workflows 2

Cisco Unified Communications Manager Workflow 2

IM and Presence Service Workflow 3

CHAPTER 2 **Pre-Change Tasks and System Health Checks** 5

Pre-Change Task List for Cisco Unified Communications Manager Nodes 5

Pre-Change Task List for IM and Presence Service Nodes 6

System Health Checks 7

Check System Health 7

Pre-Change Setup 10

Perform Pre-Change Setup Tasks for Cisco Unified Communications Manager Nodes 10

Perform Pre-Change Setup Tasks for IM and Presence Service Nodes 11

CHAPTER 3 **IP Address and Hostname Changes** 15

Change IP Address and Hostname Task List 15

Change IP Address or Hostname Through OS Admin GUI 16

Change IP Address or Hostname Through Unified CM Administration GUI 17

Change IP Address or Hostname Through CLI 18

Example CLI Output for Set Network Hostname 19

Change IP Address Only 21

Example Output for Set Network IP Address 22

Change DNS IP Address Using CLI 22

CHAPTER 4 **Domain Name and Node Name Changes** 25

Domain Name Change 25

IM and Presence Service Default Domain Name Change Tasks 26

Update DNS Records 27

Update Node Name in FQDN Value 28

Update DNS Domain 29

Cluster Nodes Considerations 31

Regenerate Security Certificates 32

Node Name Change 33

IM and Presence Service Node Name Change Task List 34

Update Node Name 34

Verify Node Name Changes Using CLI 35

Verify Node Name Changes Using Cisco Unified CM IM and Presence Administration 36

Update Domain Name for Cisco Unified Communications Manager 36

CHAPTER 5 **Post-Change Tasks and Verification** 39

Post-Change Task List for Cisco Unified Communications Manager Nodes 39

Post-Change Task List for IM and Presence Service Nodes 41

Perform Post-Change Tasks for Cisco Unified Communications Manager Nodes 43

Security enabled cluster tasks for Cisco Unified Communications Manager nodes 45

Initial Trust List and Certificate Regeneration 45

Regenerate certificates and ITL for single-server cluster phones 45

Certificate and ITL Regeneration for Multi-Server Cluster Phones 46

Perform Post-Change Tasks for IM and Presence Service Nodes 46

CHAPTER 6 **Troubleshooting Address Change Issues** 49

Troubleshoot Cluster Authentication 49

Troubleshoot Database Replication 49

Verify Database Replication 50

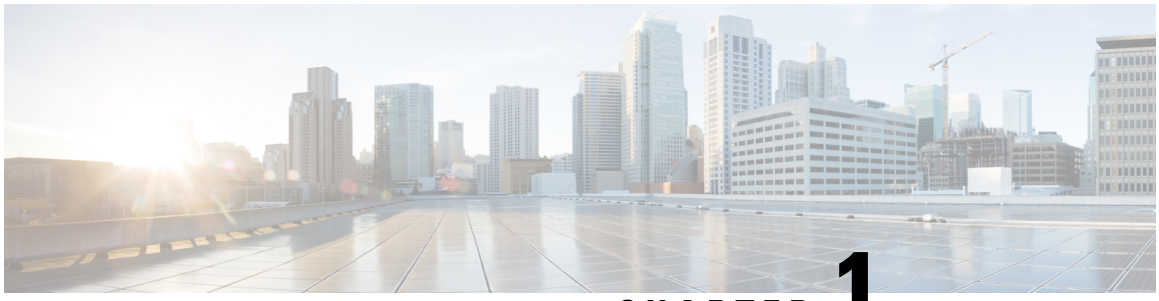
Example Database Replication CLI Output 51

Repair Database Replication 52

Reset Database Replication 55

Troubleshoot Network 55

Network Time Protocol troubleshooting 56
Troubleshoot NTP on Subscriber Nodes 56
Troubleshoot NTP on Publisher Nodes 56



CHAPTER 1

IP Address, Hostname, and Other Network Identifier Changes

- IP Address, Hostname, and Other Network Identifier Changes, on page 1
- Procedure workflows, on page 2

IP Address, Hostname, and Other Network Identifier Changes

You can change the network-level IP address and hostname name of nodes in your deployment for a variety of reasons, including moving the node from one cluster to another or resolving a duplicate IP address problem. The IP address is the network-level Internet Protocol (IP) associated with the node, and the Hostname is the network-level hostname of the node.

Note All Unified Communications products such as Cisco Unified Communications Manager, Cisco Unity Connections, and Cisco IM and Presence, and so on, have only one interface. Thus, you can assign only one IP address for each of these products.

For changes to other network identifiers, such as the node name and domain name, see the following resources:

- *Cisco Unified Communications Manager Administration Guide*
- System Configuration Guide for Cisco Unified Communications Manager
- *Deployment Guide for IM and Presence Service on Cisco Unified Communications Manager*
- *Installing Cisco Unified Communications Manager*

For IM and Presence Service, instructions to change the node name and the network-level DNS default domain name for the node are also included in this document.

IM and Presence Service Node Name and Default Domain Name Changes

The node name is configured using Cisco Unified CM Administration GUI and must be resolvable from all other IM and Presence Service nodes and from all client machines. Therefore, the recommended node name value is the network FQDN of the node. However, both IP address and hostname are also supported as values for the node name in certain deployments. See the *Deployment Guide for IM and Presence Service on Cisco*

Unified Communications Manager for more information about node name recommendations and the supported deployment types.

The network-level DNS default domain name of the node is combined with the hostname to form the Fully Qualified Domain Name (FQDN) for the node. For example, a node with hostname “imp-server” and domain “example.com” has an FQDN of “imp-server.example.com”.

Do not confuse the network-level DNS default domain of the node with the enterprise-wide domain of the IM and Presence Service application.

- The network-level DNS default domain is used only as a network identifier for the node.
- The enterprise-wide IM and Presence Service domain is the application-level domain that is used in the end-user IM address.

You can configure the enterprise-wide domain using either Cisco Unified CM IM and Presence Administration GUI or Cisco Unified Communications Manager Administration. See the *Deployment Guide for IM and Presence Service on Cisco Unified Communications Manager* for more information about enterprise-wide domains and the supported deployment types.

Note From Cisco Unified Presence Release 8.6(5), the default domain and the enterprise domain settings are no longer required to match.

Procedure workflows

Cisco Unified Communications Manager Workflow

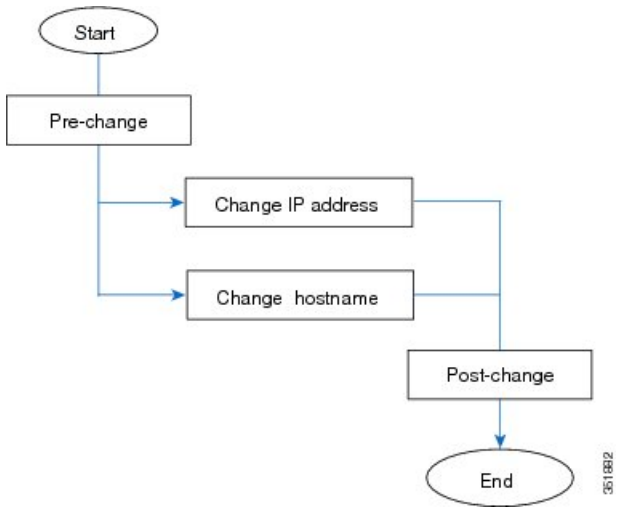
This document provides detailed procedures for the following tasks for Cisco Unified Communications Manager nodes:

- Change the IP address of a node
- Change the hostname of a node

Task lists are provided for each of these procedures that summarize the steps to perform.

Note You must complete all pre-change tasks and system health checks before you make these changes, and you must complete the post-change tasks after you make any of these changes.

Figure 1: Cisco Unified Communications Manager Workflow



IM and Presence Service Workflow

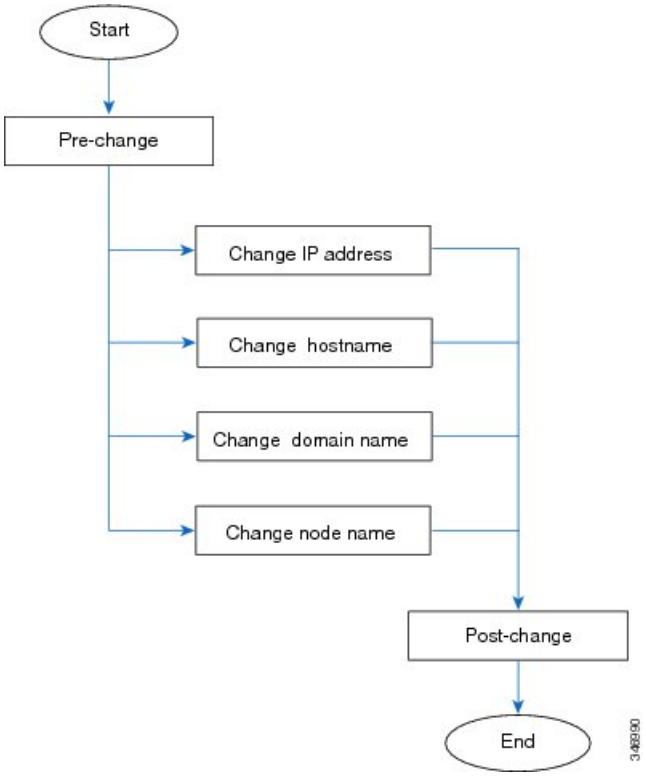
This document provides detailed procedures for the following tasks for IM and Presence Service nodes:

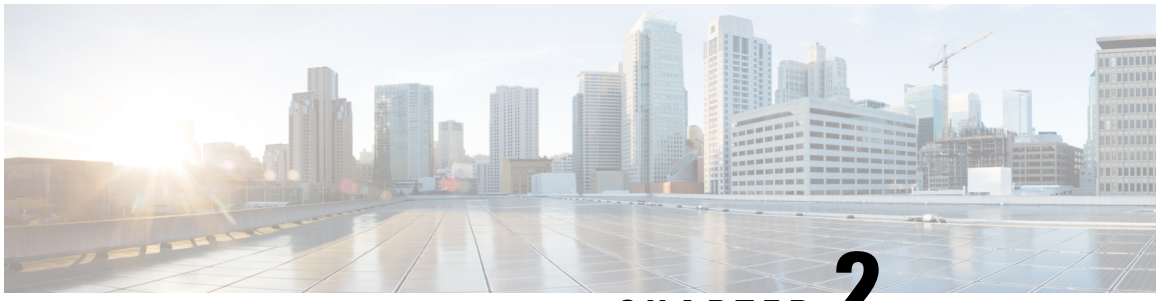
- Change the IP address of a node
- Change the hostname of a node
- Change the DNS default domain name
- Change the node name of a node

Task lists are provided for each of these procedures that summarize the steps to perform.

Note You must complete all pre-change tasks and system health checks before you make these changes, and you must complete the post-change tasks after you make any of these changes.

Figure 2: IM and Presence Service Workflow





CHAPTER 2

Pre-Change Tasks and System Health Checks

- Pre-Change Task List for Cisco Unified Communications Manager Nodes, on page 5
- Pre-Change Task List for IM and Presence Service Nodes , on page 6
- System Health Checks, on page 7
- Pre-Change Setup, on page 10

Pre-Change Task List for Cisco Unified Communications Manager Nodes

The following table lists the tasks to perform before you proceed to change the IP address and hostname for Cisco Unified Communications Manager nodes. You must perform these procedures during a scheduled maintenance window. Perform all system health checks before you perform the pre-change setup tasks.

For details about any of the tasks that are listed, see topics related to performing system health checks on nodes and pre-change setup.

Caution If you do not receive the results that you expect when you perform these tasks, do not continue until you have resolved the issue.

Table 1: Pre-Change Task List for Cisco Unified Communications Manager Nodes

Item	Task
System health checks	
1	If you have DNS configured anywhere on the Cisco Unified Communications Manager servers, ensure that forward and reverse records (for example, A record and PTR record) are configured and that the DNS is reachable and working.
2	Ensure that all servers in the cluster are up and available, and check for any active ServerDown alerts.
3	Check the database replication status of all Cisco Unified Communications Manager nodes in the cluster to ensure that all servers are replicating database changes successfully.

Item	Task
4	Check network connectivity and DNS server configuration.
Pre-change setup tasks	
5	Use Cisco Unified Communications Manager Administration to compile a list of all nodes in the cluster. Retain this information for use later.
6	Run a manual Disaster Recovery System backup and ensure that all nodes and active services are backed up successfully. For more information, see the *Administration Guide for Cisco Unified Communications Manager* .
7	For security-enabled clusters (Cluster Security Mode 1 - Mixed), update the Certificate Trust List (CTL) file. For detailed instructions on updating and managing the CTL file, including adding a new TFTP server to an existing CTL file, see the *Cisco Unified Communications Manager Security Guide*. All IP phones that support security always download the CTL file, which includes the IP address of the TFTP servers with which the phones are allowed to communicate. If you change the IP address of one or more TFTP servers, you must first add the new IP addresses to the CTL file so that the phones can communicate with their TFTP server. **Caution** To avoid unnecessary delays, you must update the CTL file with the new IP address of your TFTP servers before you change the IP address of the TFTP servers. If you do not perform this step, you will have to update all secure IP phones manually. **Note** Note: This is not applicable when the CallManager certificate is a Multi-SAN certificate.

Pre-Change Task List for IM and Presence Service Nodes

The following table lists the tasks to perform before you proceed to change the IP address, hostname, domain name, or the node name for IM and Presence Service nodes. You must perform these procedures during a scheduled maintenance window. Perform all system health checks before you perform the pre-change setup tasks.

For details about any of the tasks that are listed, see topics related to performing system health checks on nodes and pre-change setup.

Caution If you do not receive the results that you expect when you perform these tasks, do not continue until you have resolved the issue.

Table 2: Pre-Change Task List for IM and Presence Service Nodes

Item	Task
System health checks	
1	Check the database replication status to ensure that all nodes are replicating database changes successfully if you have more than one IM and Presence Service node in your deployment.
2	Check network connectivity and DNS server configuration.
Pre-change setup tasks	
3	Run a manual Disaster Recovery System backup and ensure that all nodes are backed up successfully. For more information, see the *Administration Guide for Cisco Unified Communications Manager* .
4	Disable High Availability (HA) on all presence redundancy groups. For more information about how to disable HA, see the *Deployment Guide for IM and Presence Service on Cisco Unified Communications Manager*.
5	If you are changing the hostname, disable single sign-on (SSO). For more information about SSO, see the *Deployment Guide for IM and Presence Service on Cisco Unified Communications Manager*.
6	Compile a list of all services that are currently activated on the node.
7	Stop all feature services for the node.
8	Stop IM and Presence Service network services for the node in the specified order. For a detailed list of the network services to stop and the order in which to stop them, see the procedure to perform pre-change setup tasks for IM and Presence Service nodes.
9	For IM and Presence Service node name and domain name changes, verify that the Cisco AXL Web Service is started on the Cisco Unified Communications Manager publisher node.
10	For IM and Presence Service node name and domain name changes, verify on the IM and Presence database publisher node that the Cisco Sync Agent service has started and that synchronization is complete using either the Cisco Unified Serviceability GUI or the System Dashboard on Cisco Unified CM IM and Presence Administration.

System Health Checks

Check System Health

Perform the applicable system health checks on the nodes in your deployment as part of the pre-change setup and as part of the post-change tasks that you must perform after you have changed any network identifiers.

Caution If you do not receive the results that you expect when you perform these tasks, do not continue until you have resolved the issue.

Some of the checks in this procedure are required only for post-change verification. See the post-change task list for a complete list of the system health checks to perform.

Note If you are performing system health checks as part of the pre-change setup, you can skip the following steps which are only required when you are performing the post-change tasks:

- Verification that the new hostname or IP address appears on the Cisco Unified Communications Manager server list.
- Verification that changes to the IP address, hostname, or both are fully implemented in the network.
- Verification that changes to the hostname are fully implemented in the network.

Procedure

Step 1 If you have DNS configured anywhere on the Cisco Unified Communications Manager servers, ensure that a forward and reverse lookup zone has been configured and that the DNS is reachable and working.

Step 2 Check for any active ServerDown alerts to ensure that all servers in the cluster are up and available. Use either the Cisco Unified Real-Time Monitoring Tool (RTMT) or the command line interface (CLI) on the first node.

a) To check using Unified RTMT, access Alert Central and check for ServerDown alerts.
b) To check using the CLI on the first node, enter the following CLI command and inspect the application event log:

```
file search activelog syslog/CiscoSyslog ServerDown
```

Step 3 Check the database replication status on all nodes in the cluster to ensure that all servers are replicating database changes successfully.

For IM and Presence Service, check the database replication status on the database publisher node using the CLI if you have more than one node in your deployment.

Use either Unified RTMT or the CLI. All nodes should show a status of **2**.

a) To check by using RTMT, access the Database Summary and inspect the replication status.
b) To check by using the CLI, enter **`utils dbreplication runtimestate`**.

For example output, see topics related to example database replication output. For detailed procedures and troubleshooting, see topics related to verifying database replication and troubleshooting database replication.

Step 4 Enter the CLI command **`utils diagnose`** as shown in the following example to check network connectivity and DNS server configuration.

Example:

```
admin: utils diagnose module validate_network
Log file: /var/log/active/platform/log/diag1.log

Starting diagnostic test(s)
===========================
test - validate_network    : Passed

Diagnostics Completed
admin:
```

If you are performing the pre-change system health checks, you are done; otherwise, continue to perform the post-change verification steps.

Step 5 (Post-change step) Verify that the new hostname or IP address appears on the Cisco Unified Communications Manager server list. In Cisco Unified Communications Manager Administration, select **System** > **Server**.

Note
Perform this step only as part of the post-change tasks.

Step 6 (Post-change step) Verify that changes to the IP address, hostname, or both are fully implemented in the network. Enter the CLI command **`show network cluster`** on each node in the cluster.

Note
Perform this step only as part of the post-change tasks.

The output should contain the new IP address or hostname of the node.

Example:

```
admin:show network cluster
10.63.70.125 hippo2.burren.pst hippo2 Subscriber cups DBPub authenticated
10.63.70.48 aligator.burren.pst aligator Publisher callmanager DBPub
authenticated using TCP since Wed May 29 17:44:48 2013
```

Step 7 (Post-change step) Verify that changes to the hostname are fully implemented in the network. Enter the CLI command **`utils network host`** <***new_hostname***> on each node in the cluster.

Note
Perform this step only as part of the post-change tasks.

The output should confirm that the new hostname resolves locally and externally to the IP address.

Example:

```
admin:utils network host hippo2
Local Resolution:
hippo2.burren.pst resolves locally to 10.63.70.125

External Resolution:
hippo2.burren.pst has address 10.63.70.125
```

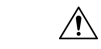
Pre-Change Setup

Perform all pre-change setup tasks to ensure that your system is prepared for a successful IP address, hostname, domain, or node name change. You must perform these tasks during a scheduled maintenance window.

You should perform the system health checks on your deployment before performing the pre-change setup.

Perform Pre-Change Setup Tasks for Cisco Unified Communications Manager Nodes

Perform the following pre-change setup tasks before you change the IP address or hostname. You must perform these tasks during a scheduled maintenance window. See the pre-change task list for more information.



Caution If you do not receive the results that you expect when you perform these tasks, do not continue until you have resolved the issue.

Before you begin

Perform the system health checks on your deployment.

Procedure

Step 1 From Cisco Unified Communications Manager Administration on the first node, select **System** > **Server** and click **Find**. A list of all servers in the cluster displays. Retain this list of servers for future reference.

Ensure that you save an inventory of both the hostname and IP address of each node in your cluster.

Step 2 Run a manual Disaster Recovery System backup and ensure that all nodes and active services are backed up successfully.

For more information, see the *Administration Guide for Cisco Unified Communications Manager* .

Step 3 For security-enabled clusters (Cluster Security Mode 1 - Mixed), update the Certificate Trust List (CTL) file.

For detailed instructions on updating and managing the CTL file, including adding a new TFTP server to an existing CTL file, see the *Cisco Unified Communications Manager Security Guide*.

Note
All IP phones that support security always download the CTL file, which includes the IP address of the TFTP servers with which the phones are allowed to communicate. If you change the IP address of one or more TFTP servers, you must first add the new IP addresses to the CTL file so that the phones can communicate with their TFTP server.

Caution

To avoid unnecessary delays, you must update the CTL file with the new IP address of your TFTP servers before you change the IP address of the TFTP servers. If you do not perform this step, you will have to update all secure IP phones manually.

Perform Pre-Change Setup Tasks for IM and Presence Service Nodes

Perform the applicable pre-change setup tasks to ensure that your system is prepared for a successful IP address, hostname, domain, or node name change. You must perform these tasks during a scheduled maintenance window. See the pre-change task list for more information.

Caution If you do not receive the results that you expect when you perform these tasks, do not continue until you have resolved the issue.

Note You do not need to perform the steps to verify that the Cisco AXL Web service and the IM and Presence Cisco Sync Agent services are started unless you are changing the domain name or the node name. See the pre-change task list for a complete list of the tasks to perform.

Before you begin

Perform the system health checks on your deployment.

Procedure

Step 1 Run a manual Disaster Recovery System backup and ensure that all nodes and active services are backed up successfully.

For more information, see the *Administration Guide for Cisco Unified Communications Manager* .

Step 2 Disable High Availability (HA) on all presence redundancy groups. For information on Presence Redundancy Groups configuration, see the "Configure Presence Redundancy Groups" chapter in the *System Configuration Guide for Cisco Unified Communications Manager*.

Note

- Before you disable HA, take a record of the number of users in each node and subcluster. You can find this information in the **System** > **Presence Topology** window of Cisco Unified CM IM and Presence Administration.
- After you disable HA, wait at least 2 minutes for the settings to sync across the cluster before completing any further changes.

Step 3 If you are changing the hostname, disable OpenAM single sign-on (SSO). For more information about OpenAM SSO, see the *Deployment Guide for IM and Presence Service on Cisco Unified Communications Manager*.

Step 4 Compile a list of all services that are currently activated. Retain these lists for future reference.

a) To view the list of activated network services using Cisco Unified Serviceability, select **Tools** > **Control Center - Network Services**.
b) To view the list of activated feature services using Cisco Unified Serviceability, select **Tools** > **Control Center - Feature Services**.

Step 5 Stop all feature services using Cisco Unified Serviceability, select **Tools** > **Control Center - Feature Services**. The order in which you stop feature services is not important.

Tip
You do not need to complete this step if you are changing the IP address, hostname, or both the IP address and hostname. Feature services are automatically stopped for these name changes.

Step 6 Stop the following network services that are listed under the IM and Presence Service services group using Cisco Unified Serviceability when you select **Tools** > **Control Center - Network Services**.

You must stop these IM and Presence Service network services in the following order:

a. Cisco Config Agent
b. Cisco Intercluster Sync Agent
c. Cisco Client Profile Agent
d. Cisco OAM Agent
e. Cisco XCP Config Manager
f. Cisco XCP Router
g. Cisco Presence Datastore
h. Cisco SIP Registration Datastore
i. Cisco Login Datastore
j. Cisco Route Datastore
k. Cisco Server Recovery Manager
l. Cisco IM and Presence Data Monitor

Step 7 Verify that the Cisco AXL Web Service is started on the Cisco Unified Communications Manager publisher node using Cisco Unified Serviceability, **Tools** > **Control Center - Feature Services**.

Note
Perform this step only if you are changing the domain name or node name.

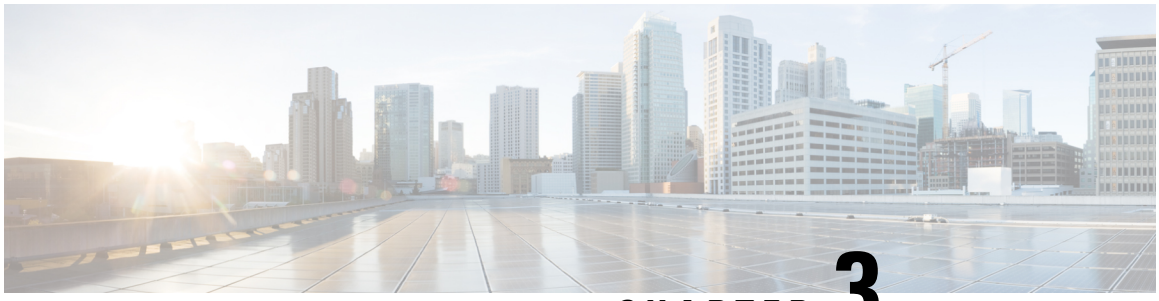
Step 8 Verify that the IM and Presence Cisco Sync Agent service has started and that synchronization is complete.

Note
Perform this step only if you are changing the domain name or node name.

a) To verify using Cisco Unified Serviceability, perform the following steps:

1. Select **Tools** > **Control Center - Network Services**.
2. Select the IM and Presence database publisher node.
3. Select **IM and Presence Service Services**.
4. Verify that the Cisco Sync Agent service has started.
5. From the Cisco Unified CM IM and Presence Administration GUI, select **Diagnostics** > **System Dashboard** > **Sync Status**.
6. Verify that synchronization is complete and that no errors display in the synchronization status area.

b) To verify using the Cisco Unified CM IM and Presence Administration GUI on the IM and Presence database publisher node, select **Diagnostics** > **System Dashboard**.



CHAPTER 3

IP Address and Hostname Changes

- Change IP Address and Hostname Task List, on page 15
- Change IP Address or Hostname Through OS Admin GUI, on page 16
- Change IP Address or Hostname Through Unified CM Administration GUI, on page 17
- Change IP Address or Hostname Through CLI, on page 18
- Change IP Address Only, on page 21
- Change DNS IP Address Using CLI, on page 22

Change IP Address and Hostname Task List

The following table lists the tasks to perform to change the IP address and hostname for Unified Communications Manager and IM and Presence Service nodes.

Note

- Cisco recommends changing the IP address of node(s) only during the maintenance window.
- From Release 12.5(1)SU7 and 14SU3 and onwards, changing the IP address/hostname on a single node will trigger the restart of Service Manager and all services on all nodes.

Table 3: Change IP Address and Hostname Task List

Item	Task
1	Perform the pre-change tasks and system health checks.

Item	Task
2	Change the IP address or hostname for the node using either the Command Line Interface (CLI) or the Unified Operating System GUI. For IM and Presence Service nodes, observe the following conditions: • Change the IP address and hostname for the database publisher node before you change any subscriber nodes. • You can change the IP address and hostname for all subscriber nodes simultaneously or one at a time. **Note** After you change the IP address or hostname of an IM and Presence Service node, you must change the Destination Address value for the SIP publish trunk on Unified Communications Manager. See the post-change task list.
3	Perform the post-change tasks.

Change IP Address or Hostname Through OS Admin GUI

You can use Cisco Unified Operating System Administration to change the IP address or hostname for publisher and subscriber nodes that are defined by a hostname in your deployment. Unless otherwise stated, each step in this procedure applies to both publisher and subscriber nodes on Unified Communications Manager and IM and Presence Service clusters.

Changing the hostname through **set network hostname** command triggers an automatically self-signed certificate regeneration. This causes all devices in the cluster to reset so that they can download an updated ITL file. If your cluster is using CA-signed certificates, you need to have them re-signed.

Changing only the IP address using the **set network hostname** command causes all devices in the cluster to reset so that they can download an updated ITL file. Certificates are not updated.

Note Changing the hostname does not trigger the ITL recovery certificates regeneration.

Caution

- Through Cisco Unified Operating System Administration, we recommend that you change only one of these settings at a time. To change both the IP address and hostname at the same time, use the CLI command **set network hostname**.
- If the Unified Communications Manager cluster security is operating in mixed mode, secure connections to this node will fail after changing the hostname, or IP address until you run the CTL client and update the CTL file or run **utils ctl update CTLFile** if you used the tokenless CTL feature.

Before you begin

Perform the pre-change tasks and system health checks on your deployment.

Note In case you must change the vNIC from vcenter, use the CLI command **set network hostname**.

Procedure

Step 1 From Cisco Unified Operating System Administration, select **Settings** > **IP** > **Ethernet**

Step 2 Change the hostname, IP address, and if necessary, the default gateway.

Step 3 Click **Save**.

Node services automatically restart with the new changes. Restarting services ensures the proper update and service-restart sequence for the changes to take effect.

Changing the hostname triggers an automatically self-signed certificate regeneration and causes all devices in the cluster to reset so they can download an updated ITL file. Changing the hostname does not trigger the ITL recovery certificates regeneration.

What to do next

Perform all applicable post-change tasks to ensure that your changes are properly implemented in your deployment.

Note Do not proceed if the new hostname does not resolve to the correct IP address.

If your cluster is using CA-signed certificates, you need to have them re-signed.

Run the CTL Client to update the CTL file if you used that process to put your cluster into mixed mode. If you used the tokenless CTL feature, then run the CLI command **utils ctl update CTLFile**

Change IP Address or Hostname Through Unified CM Administration GUI

You can use Cisco Unified CM Administration to change the IP address or hostname, which is defined in the database, for the publisher and subscriber nodes. Doing this ensures that the hostname entries are uniform with the system-defined hostname or IP values.

Changing the IP address or hostname triggers an automatically self-signed certificate regeneration. This causes all devices in the cluster to reset so that they can download an updated ITL file. If your cluster is using CA-signed certificates, you must have them re-signed.

Caution

- A change of the hostname or IP address requires the system services to be restarted. Hence, refrain from making this change during normal operating hours.
- Through Cisco Unified CM Administration, we recommend that you change only one of these settings at a time. To change both the IP address and hostname at the same time, use the CLI command **set network hostname**.
- If the Unified Communications Manager cluster security is operating in mixed mode, secure connections to this node will fail after changing the hostname, or IP address until you run the CTL client and update the CTL file or run **utils ctl update CTLFile** if you used the tokenless CTL feature.
- If the hostname or IP address that is defined on the Cisco Unified OS Administration and Cisco Unified CM Administration pages do not match, the applications are unable to fetch the correct phone status. Also, due to certificate mismatch, TLS handshake fails. Hence, ensure that the IP address and hostname entries in both the Cisco Unified OS Administration and the Cisco Unified CM Administration pages are alike.

Before you begin

Perform the prechange tasks and system health checks on your deployment.

Procedure

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

The **Find and List Servers** window appears.

Step 2 To get a list of all servers, click **Find**.

Step 3 From the list, click the server for which you want to modify the hostname.

Step 4 In the **Host Name/IP Address*** field, enter the new host name or the IP address and click **Save**.

Step 5 Using the Admin CLI GUI, reboot the node using the **utils system restart** CLI command.

Change IP Address or Hostname Through CLI

You can use the CLI to change the IP address or hostname for publisher and subscriber nodes that are defined by a hostname in your deployment. Unless otherwise stated, each step in this procedure applies to both publisher and subscriber nodes on Cisco Unified Communication Manager and IM and Presence Service clusters.

Changing the hostname triggers an automatically self-signed certificate regeneration. This causes all devices in the cluster to reset so that they can download an updated ITL file. If your cluster is using CA-signed certificates, you must have them re-signed. Changing the hostname does not trigger the ITL recovery certificates regeneration.

Caution If the Cisco Unified Communications Manager cluster security is operating in mixed mode, secure connections to this node will fail after changing the hostname, or IP address until you run the CTL client and update the CTL file or run **utils ctl update CTLFile** if you used the tokenless CTL feature.

Before you begin

Perform the pre-change tasks and system health checks on your deployment.

Procedure

Step 1 Log in to the CLI of the node that you want to change.

Step 2 Enter **set network hostname**.

Step 3 Follow the prompts to change the hostname, IP address, or default gateway.

a) Enter the new hostname and press **Enter**.
b) Enter **yes** if you also want to change the IP address; otherwise, go to Step 4.
c) Enter the new IP address.
d) Enter the subnet mask.
e) Enter the address of the gateway.

Step 4 Verify that all your input is correct and enter **yes** to start the process.

What to do next

Perform all applicable post-change tasks to ensure that your changes are properly implemented in your deployment.

Note Do not proceed if the new hostname does not resolve to the correct IP address.

If your cluster is using CA-signed certificates, you must have them re-signed.

Run the CTL Client to update the CTL file if you used that process to put your cluster into mixed mode. If you used the tokenless CTL feature, then run the CLI command **utils ctl update CTLFile**

Example CLI Output for Set Network Hostname

Note In case you need to change the vNIC from vcenter, update the vNIC after the step `calling 4 of 5 component notification script: regenerate_all_certs.sh` as displayed in the following output.

```
admin:set network hostname
```

```
ctrl-c: To quit the input.

         ***   W A R N I N G   ***
Do not close this window without first canceling the command.

This command will automatically restart system services.
The command should not be issued during normal operating
hours.

=====================================================
 Note: Please verify that the new hostname is a unique
       name across the cluster and, if DNS services are
       utilized, any DNS configuration is completed
       before proceeding.
=====================================================

Security Warning : This operation will regenerate
       all CUCM Certificates including any third party
       signed Certificates that have been uploaded.

Enter the hostname:: newHostname

Would you like to change the network ip address at this time [yes]::


Warning: Do not close this window until command finishes.



ctrl-c: To quit the input.



           ***   W A R N I N G   ***
=====================================================
 Note: Please verify that the new ip address is unique
       across the cluster.
=====================================================

Enter the ip address:: 10.10.10.28
Enter the ip subnet mask:: 255.255.255.0
Enter the ip address of the gateway:: 10.10.10.1
Hostname:       newHostname
IP Address:     10.10.10.28
IP Subnet Mask: 255.255.255.0
Gateway:        10.10.10.1

Do you want to continue [yes/no]? yes



calling 1 of 5 component notification script: ahostname_callback.sh
Info(0): Processnode query returned =
name
==========
bldr-vcm18
updating server table from:'oldHostname', to: 'newHostname'
Rows: 1
updating database, please wait 90 seconds
updating database, please wait 60 seconds
updating database, please wait 30 seconds
Going to trigger /usr/local/cm/bin/dbl updatefiles --remote=newHostname,oldHostname

calling 2 of 5 component notification script: clm_notify_hostname.sh  notification
```

```
Verifying update across cluster nodes...
platformConfig.xml is up-to-date: bldr-vcm21

cluster update successfull
calling 3 of 5 component notification script: drf_notify_hostname_change.py
calling 4 of 5 component notification script: regenerate_all_certs.sh
calling 5 of 5 component notification script: update_idsenv.sh
calling 1 of 2 component notification script: ahostname_callback.sh
Info(0): Processnode query returned =
name
====
Going to trigger /usr/local/cm/bin/dbl updatefiles
--remote=10.10.10.28,10.67.142.24
calling 2 of 2 component notification script: clm_notify_hostname.sh
Verifying update across cluster nodes...
Shutting down interface eth0:
```

Change IP Address Only

You can change the IP address of a node by using the CLI.

If the node is defined by hostname or FQDN, you must update only the DNS before you make the change (if DNS is used).

Note For IM and Presence Service:

- Change and verify the IM and Presence database publisher node first.
- You can change the IM and Presence Service subscriber nodes simultaneously or one at a time.

Before you begin

Perform the pre-change tasks and system health checks on your deployment.

Procedure

Step 1 Log in to the CLI of the node that you want to change.

Step 2 Enter **set network ip eth0** ***new-ip_address new_netmask new_gateway*** to change the IP address of the node.

Note
Changing IP address only with the **set network ip eth0** command does not trigger Certificate Regeneration.

where *new_ip_address* specifies the new server IP address, *new_netmask* specifies the new server network mask and *new_gateway* specifies the gateway address.

The following output displays:

```
admin:set network ip eth0 10.53.57.101 255.255.255.224 10.53.56.1
```

```
WARNING: Changing this setting will invalidate software license
on this server. The license will have to be re-hosted.

Continue (y/n)?
```

Step 3 Verify the output of the CLI command. Enter **yes**, and then press **Enter** to start the process.

What to do next

Perform all applicable post-change tasks to ensure that your changes are properly implemented in your deployment.

Example Output for Set Network IP Address

Note In case you need to change the vNIC from vcenter, update the vNIC after the step `calling 3 of 6 component notification script: aetc_hosts_verify.sh` as displayed in the following output.

```
admin:set network ip eth0 10.77.30.34 255.255.255.0 10.77.30.1

           ***   W A R N I N G   ***

This command will restart system services
======================================================
 Note: Please verify that the new ip address is unique
       across the cluster and, if DNS services are
       utilized, any DNS configuration is completed
       before proceeding.
======================================================


Continue (y/n)?y
calling 1 of 6 component notification script: acluster_healthcheck.sh
calling 2 of 6 component notification script: adns_verify.sh
No Primary DNS server defined
No Secondary DNS server defined
calling 3 of 6 component notification script: aetc_hosts_verify.sh
calling 4 of 6 component notification script: afupdateip.sh
calling 5 of 6 component notification script: ahostname_callback.sh
Info(0): Processnode query returned using 10.77.30.33:
name
====
calling 6 of 6 component notification script: clm_notify_hostname.sh
```

Change DNS IP Address Using CLI

You can use CLI to change the DNS IP Address for publisher and subscriber nodes in your deployment. This procedure applies to both publisher and subscriber nodes on Unified Communications Manager and IM and Presence Service clusters.

Before you begin

Perform the pre-change tasks and system health checks on your deployment.

Procedure

Step 1 Log in to the CLI of the node that you want to change.

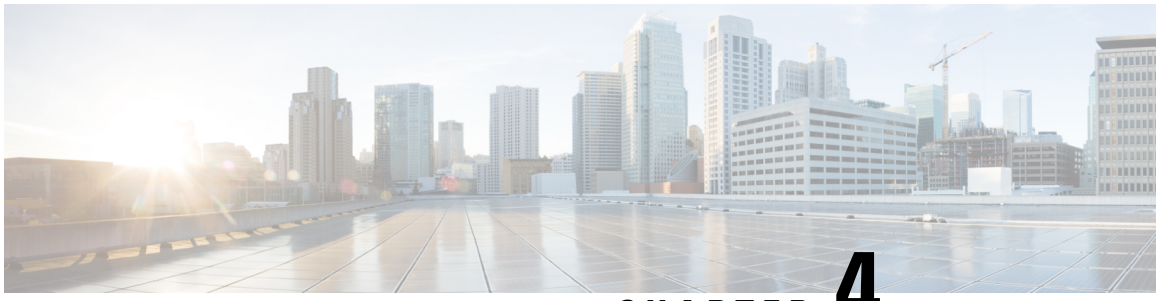
Step 2 Enter `set network dns primary/secondary <new IP address of the DNS>`

Note
If you change the IP address for the DNS servers, you must reboot the server through the **utils system restart** CLI command.

The following ouput displays:

```
admin:set network dns primary/secondary <new IP address of DNS>
*** W A R N I N G ***
This will cause the system to temporarily lose network connectivity
```

Step 3 Verify the output of the CLI command. Enter **Yes** and then press **Enter** to start the process.



CHAPTER 4

Domain Name and Node Name Changes

- Domain Name Change, on page 25
- Node Name Change, on page 33
- Update Domain Name for Cisco Unified Communications Manager , on page 36

Domain Name Change

Administrators can modify the network-level DNS default domain that is associated with an IM and Presence Service node or group of nodes.

The enterprise-wide IM and Presence Service domain does not need to align with the DNS default domain of any IM and Presence Service node. To modify the enterprise-wide domain for your deployment, see the *Deployment Guide for IM and Presence Service on Cisco Unified Communications Manager Configuration and Administration Guide for the IM and Presence Service*.

Caution Changing the default domain on any node in an IM and Presence Service cluster will result in node restarts and interruptions to presence services and other system functions. Because of this impact to the system, you must perform this domain change procedure during a scheduled maintenance window.

When you change the default domain name for a node, all third-party signed security certificates are automatically overwritten with new self-signed certificates. If you want to have those certificates re-signed by your third-party Certificate Authority, you must manually request and upload the new certificates. Service restarts may be required to pick up these new certificates. Depending on the time that is required to request new certificates, a separate maintenance window may be required to schedule the service restarts.

Note New certificates cannot be requested in advance of changing the default domain name for the node. Certificate Signing Requests (CSRs) can only be generated after the domain has been changed on the node and the node has been rebooted.

IM and Presence Service Default Domain Name Change Tasks

The following table contains the step-by-step instructions for modifying the network-level DNS default domain name associated with an IM and Presence Service node or group of nodes. The detailed instructions for this procedure specify the exact order of steps for performing the change on multiple nodes within the cluster.

If you are performing this procedure across multiple clusters, you must complete the changes sequentially on one cluster at a time.

Note You must complete each task in this procedure in the exact order presented in this workflow.

Procedure

Step 1 Complete the pre-change tasks on all applicable nodes within the cluster. Some of the pre-change tasks may apply only to the IM and Presence database publisher node and can be skipped if you are modifying a subscriber node.

Step 2 Update the DNS records for the IM and Presence Service node on all applicable nodes within the cluster. Also update SRV, Forward (A), and Reverse (PTR) records as appropriate to incorporate the new node domain.

Step 3 Update the IM and Presence Service node name on all applicable nodes within the cluster using Cisco Unified Communications Manager Administration.

Note
This step is mandatory for the FQDN node name format. It is not applicable if the node name is an IP address or a Hostname.

- If the node name is an FQDN, then it references the old node domain name. Therefore, you must update the node name such that the FQDN value reflects the new domain name.
- If the node name is an IP address or hostname, then the domain is not referenced and therefore no changes are required.

Step 4 Update the DNS domain on all applicable nodes using the Command Line Interface (CLI). The CLI command makes the required domain change on the node operating system and triggers an automatic reboot of each node.

Step 5 Restart the 'A Cisco DB' service of all the nodes in the cluster after the domain name update to ensure that operating system configuration files on all nodes pick up the DNS domain name change that is associated with the modified nodes.

Note
Verify that the system is working properly. If you observe any replication issues, ensure that you restart all the nodes in the cluster.

Step 6 Verify database replication using the CLI. See topics related to performing system health checks and troubleshooting database replication for details. After all system files are synchronized within the cluster, you must verify database replication.

Step 7 Regenerate security certificates on the node.

- The Subject Common Name on all IM and Presence Service security certificates is set to the node FQDN. Therefore, to incorporate the new node domain, all certificates are automatically regenerated after a DNS domain change.
- Any certificates that were previously signed by a certificate.

Step 8 Complete the post-change tasks for all applicable nodes within the cluster to ensure that the cluster is fully operational.

Update DNS Records

Because you are changing the DNS domain for the node, you must also update any existing DNS records associated with that node. This includes the following types of records:

- A records
- PTR records
- SRV records

If multiple nodes within a cluster are being modified, you must complete the following procedure for each of these nodes.

If you are modifying the IM and Presence database publisher node, you must complete this procedure on the IM and Presence database publisher node first before repeating on any applicable IM and Presence Service subscriber nodes.

Note

- These DNS records must be updated during the same maintenance window as the DNS domain change itself on the node.
- Updating the DNS records before the scheduled maintenance window may adversely affect IM and Presence Service functionality.

Before you begin

Perform all pre-change tasks and the applicable system health checks on your deployment.

Procedure

Step 1 Remove the old DNS forward (A) record for the node from the old domain.

Step 2 Create a new DNS forward (A) record for the node within the new domain.

Step 3 Update the DNS reverse (PTR) record for the node to point to the updated Fully Qualified Domain Name (FQDN) of the node.

Step 4 Update any DNS SRV records that point to the node.

Step 5 Update any other DNS records that point to the node.

Step 6 Verify that all the above DNS changes have propagated to all other nodes within the cluster by running the following Command Line Interface (CLI) command on each node:

a) To validate the new A record, enter **utils network host new-fqdn**, where `new-fqdn` is the updated FQDN of the node.

Example:

```
admin: utils network host server1.new-domain.com
Local Resolution:
server1.new-domain.com resolves locally to 10.53.50.219

External Resolution:
server1.new-domain.com has address 10.53.50.219
```

b) To validate the updated PTR record, enter **utils network host ip-addr**, where `ip-addr` is the IP address of the node.

```
admin: utils network host 10.53.50.219
Local Resolution:
10.53.50.219 resolves locally to server1.new-domain.com

External Resolution:
server1.new-domain.com has address 10.53.50.219
219.50.53.10.in-addr.arpa domain name pointer server1.new-domain.com.
```

Note
At this point in the procedure, the **Local Resolution** result for the IP address will continue to point to the old FQDN value until the DNS domain is changed on the node.

c) To validate any updated SRV records, enter **utils network host srv-name srv**, where `srv-name` is the SRV record.

Example:

_xmpp-server SRV record lookup example.

```
admin: utils network host _xmpp-server._tcp.galway-imp.com srv
Local Resolution:
Nothing found

External Resolution:
_xmpp-server._tcp.sample.com has SRV record 0 0 5269 server1.new-domain.com.
```

What to do next

Update the IM and Presence Service node name.

Update Node Name in FQDN Value

If the node name defined for the node in the Presence Topology window on the Cisco Unified CM IM and Presence Administration GUI is set to the Fully Qualified Domain Name (FQDN) of the node, then it references the old domain name. Therefore you must update the node name to reference the new domain name.

Note This procedure is only required if the node name value for this node is set to FQDN. If the node name matches the IP address or the hostname of the node, then this procedure is not required.

If multiple nodes within a cluster are being modified, you must complete the following procedure sequentially for each of these nodes.

If the IM and Presence database publisher node is being modified, you must complete this procedure for the IM and Presence Service subscriber nodes first, before completing the procedure on the publisher node.

Before you begin

Update the DNS records for the node.

Procedure

Step 1 Modify the node name for the IM and Presence Service node.

a) Sign in to Cisco Unified Communications Manager Administration.
b) Select **System** > **Server**.
c) Search for and select the node.
d) Update the **Fully Qualified Domain Name/IP Address** field so that the FQDN references the new domain value. For example, update the **Fully Qualified Domain Name/IP Address** value from `server1.old-domain.com` to `server1.new-domain.com`.
e) Select **Save**.

Step 2 Verify that the Application Server entry for this node has been updated to reflect the new node name on the **Presence Topology** window of the Cisco Unified CM IM and Presence Administration GUI.

a) Sign in to Cisco Unified Communications Manager Administration and select **System** > **Application Server**.
b) Click **Find**, if required, on the **Find and List Application Servers** window.
c) Ensure that an entry exists for the updated node name in the list of Application Servers.

Note
Do not continue if there is no entry for this node or if there is an entry but it reflects the old node name for the node.

What to do next

Update the DNS domain on all applicable nodes.

Update DNS Domain

You can change the DNS domain of the IM and Presence Service node using the Command Line Interface (CLI).

The enterprise-wide IM and Presence Service domain does not need to align with the network-level DNS default domain of any IM and Presence Service node. To modify the enterprise-wide domain for your deployment, see the *Deployment Guide for IM and Presence Service on Cisco Unified Communications Manager*.

If you are modifying multiple nodes within a cluster, then you must complete the following procedure sequentially for each node.

If you are modifying the IM and Presence database publisher node, then you must first complete this procedure on the database publisher node before you modify any subscriber nodes.

Before you begin

Update the IM and Presence Service node name.

Procedure

Step 1 Sign in to the CLI on the node and enter **`set network domain new-domain`**, where `new-domain` is the new domain value to be set.

Example:

```
admin: set network domain new-domain.com

*** W A R N I N G ***
Adding/deleting or changing domain name on this server will break
database replication. Once you have completed domain modification
on all systems that you intend to modify, please reboot all the
servers in the cluster. This will ensure that replication keeps
working correctly. After the service is rebooted, please
confirm that there are no issues reported on the Cisco Unified
Reporting report for Database Replication.

The server will now be rebooted. Do you wish to continue.

Security Warning : This operation will regenerate
all CUP Certificates including any third party
signed Certificates that have been uploaded.

Continue (y/n)?
```

Step 2 Enter **`y`** and press **Return** to confirm the domain change and restart of the node or enter **`n`** to cancel.

Tip
When the node name change is complete, all certificates are regenerated on the node. If any of those certificates were signed by a third-party Certificate Authority, then you must re-request those signed certificates later in the procedure.

Step 3 After the node restarts, enter `show network eth0` to confirm the domain name change has taken effect.

Example:

The new domain in the following example is new-domain.com.

```
admin: show network eth0
Ethernet 0
```

```
DHCP         : disabled       Status      : up
IP Address   : 10.53.50.219   IP Mask     : 255.255.255.000
Link Detected: yes            Mode        : Auto disabled, Full, 1000 Mbits/s
Duplicate IP : no

DNS
Primary  : 10.53.51.234       Secondary   : Not Configured
Options  : timeout:5 attempts:2
Domain   : new-domain.com
Gateway  : 10.53.50.1 on Ethernet 0
```

Step 4 Repeat the previous steps on all applicable nodes in the cluster.

What to do next

Reboot all nodes in the cluster.

Cluster Nodes Considerations

You can use the Command Line Interface (CLI) to restart the "A Cisco DB" service in the nodes in your cluster.

After you change the domain name and the node reboots, you need to restart the 'A Cisco DB' service of all the nodes in the cluster, including those nodes that have automatically rebooted, starting with the Unified CM publisher and then for all the subscribers as the published database comes up. This ensures that the Operating System configuration files on all nodes are aligned with the new domain values.

Verify that the system is working properly. If you observe any replication issues, ensure that you restart all the nodes in the cluster.

Initiate the reboot process on the IM and Presence database publisher node first. When the database publisher node has restarted, proceed to reboot the remaining IM and Presence Service subscriber nodes in any order.

Before you begin

Ensure that the DNS domain name of the node was changed.

Procedure

Step 1 Reboot the IM and Presence database publisher node using the CLI. Enter **`utils system restart`**.

Example:

```
admin: utils system restart
Do you really want to restart ?
Enter (yes/no)?
```

Step 2 Enter **`yes`** and press **Return** to restart.

Step 3 Wait until you see the following message that indicates the IM and Presence database publisher node has restarted.

Example:

```
Broadcast message from root (Wed Oct 24 16:14:55 2012):

The system is going down for reboot NOW!
Waiting .

Operation succeeded

restart now.
```

Step 4 Sign in to the CLI on each IM and Presence Service subscriber node and enter **utils system restart** to reboot each subscriber node.

Note
After several minutes of trying to stop services, the CLI may ask you to force a restart. If this occurs, enter **yes**.

What to do next

Verify database replication. See topics related to system health checks for more information.

Regenerate Security Certificates

The Fully Qualified Domain Name (FQDN) of the node is used as Subject Common Name in all IM and Presence Service security certificates. Therefore, when the DNS domain is updated on a node, all security certificates are automatically regenerated.

If any certificates were signed by a third-party Certificate Authority, then you must manually generate new Certificate Authority signed certificates.

If you are modifying multiple nodes within a cluster, you must complete the following procedure for each node.

Note New certificates cannot be requested in advance of changing the default domain name for the node. Certificate Signing Requests (CSRs) can only be generated after the domain has been changed on the node and the node has been rebooted.

Before you begin

Verify database replication to ensure that database replication is successfully established on all nodes.

Procedure

Step 1 If a certificate must be signed by a third-party Certificate Authority, sign in to the Cisco Unified Operating System Administration GUI and perform the required steps for each relevant certificate.

Step 2 After you upload the signed certificate, you may need to restart services on the IM and Presence Service node.

The required service restarts are as follows:

- Tomcat certificate: Restart the tomcat service by running the following Command Line Interface (CLI) command:

```
utils service restart Cisco Tomcat
```

- Cup-xmpp certificate: Restart the Cisco XCP Router service from the Cisco Unified Serviceability GUI.
- Cup-xmpp-s2s certificate: Restart the Cisco XCP Router service from the Cisco Unified Serviceability GUI.

Note

- These actions restart the affect service. Therefore, depending on the time lag in acquiring the signed certificates, you may need to schedule the restarts for a later maintenance window. In the meantime, the self-signed certificates will continue to be presented on the relevant interfaces until the services are restarted.
- If a certificate is not specified in the preceding list, no service restarts are required for that certificate.

What to do next

Perform the post-change task list on all applicable nodes within the cluster.

Node Name Change

You can modify the node name that is associated with an IM and Presence Service node or group of nodes. The updates are displayed on the **Server Configuration** window of Cisco Unified Communications Manager Administration.

Use these procedures for the following node name change scenarios:

- IP address to hostname
- IP address to Fully Qualified Domain Name (FQDN)
- hostname to IP address
- hostname to FQDN
- FQDN to hostname
- FQDN to IP address

For more information about node name recommendations, see the *Deployment Guide for IM and Presence Service on Cisco Unified Communications Manager*.

Caution Use this procedure to change the node name only for an IM and Presence Service node where there are no network-level changes needed. Perform the procedures that are specific to changing the network IP address, hostname, or the domain name in that case. You must perform this node name change procedure during a scheduled maintenance window. Changing the node name on any node in an IM and Presence Service cluster will result in node restarts and interruptions to presence services and other system functions.

IM and Presence Service Node Name Change Task List

The following table contains the step-by-step instructions to change the node name that is associated with an IM and Presence Service node or group of nodes. The detailed instructions for this procedure specify the exact order of steps for performing the change.

If you are performing this procedure across multiple clusters, complete all the sequential steps to change the node name on one cluster at a time.

Table 4: Change IM and Presence Service Node Name Task List

Item	Task
1	Complete the pre-change tasks on all applicable nodes within the cluster. Some of the pre-change tasks may apply only to the IM and Presence database publisher node and can be skipped if you are modifying a subscriber node.
2	Update the IM and Presence Service node name using Cisco Unified Communications Manager Administration.
3	Verify the node name updates and ensure that the node name change is synchronized with IM and Presence Service.
4	Verify database replication using the Command Line Interface (CLI) after the node name updates are complete. Ensure that the new node names have replicated across the cluster and that database replication is operational on all nodes.
5	Complete the post-change tasks list on the updated nodes and verify that the node is fully functional.

Update Node Name

If multiple nodes within a cluster are being modified, you must complete the following procedure sequentially for each node.

If the IM and Presence database publisher node is being modified, you must complete this procedure for the IM and Presence Service subscriber nodes first, before completing the procedure on the publisher node.

Note For IM and Presence nodes, it's recommended to use a fully qualified domain name. However, IP addresses and hostnames are also supported.

Before you begin

Perform all pre-change tasks and the applicable system health checks for your deployment.

Procedure

Step 1 Sign in to Cisco Unified CMAdministration.

Step 2 Select **System** > **Server**.

Step 3 Select the node that you want to modify.

Step 4 Update the **Host Name/IP Address** field with the new node name.

Note
Ensure you upload the newly generated SP metadata to the IDP server.

Step 5 If multiple nodes within a cluster are being modified, repeat this procedure for each node.

Note
If you update the IM and Presence Service node name and you also have third-party compliance configured, you must update the compliance server to use the new realm which is based on the node name. This configuration update is made on the third-party compliance server. The new realm will be displayed on the **Cisco Unified CM IM and Presence Administration** > **Messaging** > **Compliance** > **Compliance Settings** window.

What to do next

Verify the node name change.

Verify Node Name Changes Using CLI

You can verify that the new node name has replicated across the cluster using the Command Line Interface (CLI).

Procedure

Step 1 Enter **`run sql name select from processnode`** to validate that the new node name has replicated correctly on each node in the cluster.

Example:

```
admin:run sql select name from processnode
name
====================
EnterpriseWideData
server1.example.com
server2.example.com
server3.example.com
server4.example.com
```

Step 2 Verify that there is an entry for each node in the cluster that specifies the new node name. No old node name should appear in the output.

a) If the output is as expected, then validation has passed and you do not need to validate database replication for the nodes.

b) If any new node names are missing or if there are peferences to old node names, then continue to Step 3.

Step 3 To troubleshoot missing node names or old node names that appear for the node, perform the following actions:

a) For an IM and Presence database publisher node, check if the sync agent is running ok and verify that there are no errors in the sync agent status using the dashboard on the Cisco Unified CM IM and Presence Administration GUI.
b) For subscriber nodes, perform the validate database replication procedure.

Verify Node Name Changes Using Cisco Unified CM IM and Presence Administration

For IM and Presence Service nodes only, verify that the application server entry for this node has been updated to reflect the new node name on Cisco Unified CM IM and Presence Administration GUI.

Before you begin

Update the IM and Presence Service node name.

Procedure

Step 1 Sign in to the Cisco Unified CM IM and Presence Administration GUI.
Step 2 Select **System** > **Presence Topology**.
Step 3 Verify that the new node name appears in the **Presence Topology** pane.

What to do next

Verify database replication.

Update Domain Name for Cisco Unified Communications Manager

You can use the Command Line Interface (CLI) to change the domain name for Cisco Unified Communications Manager. Update the DNS domain name on all applicable nodes using the CLI. The CLI command makes the required domain name change on the node and triggers an automatic reboot for each node.

If the Unified CM cluster security mode is non-secure and you are updating or changing the domain, then as a part of domain changes all certificates will be regenerated. To make sure that the ITLs are updated on the phones, perform the following steps needed prior to updating the domain name:

1. Ensure that all phones are online and registered so that they can process the updated ITLs. For phones that are not online when this procedure is performed, the ITL must be deleted manually.
2. Set the **Prepare Cluster for Rollback to pre-8.0 enterprise** parameter to **True**. All phones automatically reset and download an ITL file that contains empty Trust Verification Services (TVS) and TFTP certificate sections.

3. On the phone, select **Settings** > **Security** > **Trust List** > **ITL File** to verify that the TVS and TFTP certificate sections of the ITL file are empty.
4. Change the domain of the server and let the phones configured for rollback register to the cluster.
5. After all the phones have successfully registered to the cluster, set the enterprise parameter **Prepare Cluster for Rollback to pre-8.0** to **False**.

Before you begin

- Ensure to enable the DNS before changing the domain name.
- Sign in to Cisco Unified Communications Manager Administration and navigate to the **System** > **Server Fields** page. If this server configuration settings page has an existing hostname entry, you should first change the hostname entry of the domain name.
- Perform all pre-change tasks and the applicable system health checks. See the Related Topic section for more information.

Procedure

Step 1 Log in to Command Line Interface.

Step 2 Enter **run set network domain <new_domain_name>**.
The command prompts for a system reboot.

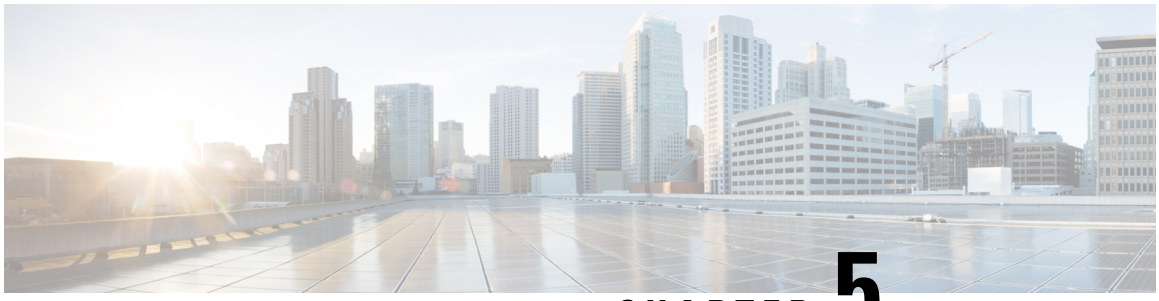
Step 3 Click **Yes** to reboot the system.
The new domain name gets updated after the system is rebooted.

Step 4 Enter the command **show network eth0** to check if the new domain name is updated after the reboot.

Step 5 Repeat this procedure for all cluster nodes.

What to do next

Perform all applicable post-change tasks to ensure that your changes are properly implemented in your deployment.



CHAPTER 5

Post-Change Tasks and Verification

- Post-Change Task List for Cisco Unified Communications Manager Nodes, on page 39
- Post-Change Task List for IM and Presence Service Nodes , on page 41
- Perform Post-Change Tasks for Cisco Unified Communications Manager Nodes, on page 43
- Security enabled cluster tasks for Cisco Unified Communications Manager nodes, on page 45
- Perform Post-Change Tasks for IM and Presence Service Nodes, on page 46

Post-Change Task List for Cisco Unified Communications Manager Nodes

The following table lists the tasks to perform after you have changed the IP address or hostname of the Unified Communications Manager nodes in your cluster.

Perform the tasks that apply to your deployment in the order in which they are presented in the task list. For details about system health checks or generating ITL certificates, see the related topics.

Caution If you do not receive the results that you expect when you perform these tasks, do not continue until you have resolved the issue.

Table 5: Post-Change Task List for Unified Communications Manager Nodes

Item	Task
System health checks	
1	Ensure that all servers in the cluster are up and available, and check for any active ServerDown alerts. **Note** ServerDown alerts in the Syslog are normal during the change process, but should not appear in the log after the change is done.

Item	Task
2	Check the database replication status of all Unified Communications Manager nodes in the cluster to ensure that all servers are replicating database changes successfully. **Note** Verify the hostname changes of the publisher and subscriber nodes in the cluster. If the hostname changes are not replicated, you need to restart the 'A Cisco DB' service of all the other nodes in the cluster.
3	Check network connectivity and DNS server configuration on the node that was changed using the CLI command `utils diagnose module validate_network`.
4	In Cisco Unified Reporting, generate the Unified CM Database Status report. Look for any errors or warnings in this report.
5	In Cisco Unified Reporting, generate the Unified CM Cluster Overview report. Look for any errors or warnings in this report.
Security enabled cluster tasks	
6	For security-enabled clusters (Cluster Security Mode 1 - Mixed), update the CTL file and then restart all nodes in the cluster before you perform the system health checks and other post-change tasks. For detailed instructions on updating and managing the CTL file, including adding a new TFTP server to an existing CTL file, see the Security Guide for Cisco Unified Communications Manager.
7	If you enabled cluster security using Certificate Trust List (CTL) files and USB eTokens, you must regenerate the Initial Trust List (ITL) file and the certificates in the ITL if you changed the IP address or hostname for Release 8.0 or later nodes. Skip this step if you have not enabled cluster security using Certificate Trust List (CTL) files and USB eTokens.
Post-change tasks	
8	Run a manual DRS backup and ensure that all nodes and active services back up successfully. For more information, see the Administration Guide for Cisco Unified Communications Manager. **Note** You must run a manual DRS backup after you change the IP address of a node, because you cannot restore a node with a DRS file that contains a different IP address or hostname. The post-change DRS file will include the new IP address or hostname.
9	Update all relevant IP phone URL parameters.
10	Update all relevant IP phone services using Cisco Unified Communications Manager Administration.
11	Update Unified RTMT custom alerts and saved profiles.
12	If you are using the integrated DHCP server that runs on Unified Communications Manager, update the DHCP server.

Item	Task
13	Check and make any required configuration changes to other associated Cisco Unified Communications components, such as Cisco Unity Connection and Cisco Unified MeetingPlace Express. **Note** Consult the documentation for your product to determine how to make any required configuration changes.
14	Reset the phone after you change the DNS IP address for the phone to reflect the updated information. Resetting the phone clears the phone cache.
15	When you change the hostname or remove the node from the cluster, you need to remove the node from the intercluster, wait until syncing of the nodes and configure the node again in the cluster.

Note You need to update hostname on other clusters if we have multi-cluster deployment. Cluster hostname is defined on other cluster sip trunk, h323 trunk, ILS/cluster view.

Post-Change Task List for IM and Presence Service Nodes

The following table lists the tasks to perform after you have changed the IP address, hostname, domain name, or the node name of the IM and Presence Service nodes in your cluster.

Perform the tasks in the order in which they are presented in the task list.

Caution If you do not receive the results that you expect when you perform these tasks, do not continue until you have resolved the issue.

Table 6: Post-Change Task List for IM and Presence Service Nodes

Item	Task
System health checks	
1	Verify that changes to the hostname or IP address are updated on the Cisco Unified Communications Manager server.
2	Check network connectivity and DNS server configuration on the node that was changed. **Note** If you changed the IP address to a different subnet, ensure that your network adapter is now connected to the correct VLAN. Also, if the IM and Presence Service nodes belong to different subnets after the IP address change, ensure that the Routing Communication Type field of the Cisco XCP Router service parameter is set to **Router to Router**. Otherwise, the Routing Communication Type field should be set to **Multicast DNS**.

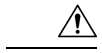
Item	Task
3	Verify that the changes to the IP address, hostname, or both are fully implemented in the network.
4	If you changed the hostname, verify that the hostname change has been fully implemented in the network. **Note** Verify the hostname changes of the publisher and subscriber nodes in the cluster. If the hostname changes are not replicated, you need to restart the 'A Cisco DB' service of all the other nodes in the cluster.
5	Verify that database replication has been successfully established. All nodes should show a status of **2** and be **Connected**. If replication is not set up, see topics related to troubleshooting database replication.
Post-change tasks	
6	If you disabled OpenAM SSO prior to performing a procedure, you can enable it now. For information about how to enable OpenAM SSO, see the *Deployment Guide for IM and Presence Service on Cisco Unified Communications Manager*.
7	Ensure that the cup, cup-xmpp and Tomcat certificates contain the new hostname.
8	If the IP address for a node has changed, update Unified RTMT custom alerts and saved profiles.
9	Check and make any required configuration changes to other associated Cisco Unified Communications components, for example, SIP trunks on Cisco Unified Communications Manager.
10	Start all network services that are listed under the CUP Services group. You must start the CUP Services network services in the prescribed order. **Note** You do not need to complete this step if you are changing the IP address, hostname, or both the IP address and hostname. Network services are automatically started for these name changes. However, if some services do not automatically start after the change, complete this step to ensure that all network services are started.
11	Start all feature services. The order in which you start feature services is not important. **Note** You do not need to complete this step if you are changing the IP address, hostname, or both the IP address and hostname. Feature services are automatically started for these name changes. However, if some services do not automatically start after the change, complete this step to ensure that all feature services are started.

Item	Task
12	If you disabled HA during the pre-change setup, confirm that your Cisco Jabber sessions have been recreated before you re-enable High Availability. Otherwise, Jabber clients whose sessions are created will be unable to connect. Run the `show perf query counter "Cisco Presence Engine" ActiveJsmSessions` CLI command on all cluster nodes. The number of active sessions should match the number of users that you recorded when you disabled high availability. If it takes more than 30 minutes for your sessions to start, you may have a larger system issue. Once you are sure that your Jabber sessions are created, re-enable High Availability in all presence redundancy groups.
13	Verify that IM and Presence Service is functioning properly after the changes.
14	Run a manual Disaster Recovery System backup after you change the IP address or hostname of a node.

Perform Post-Change Tasks for Cisco Unified Communications Manager Nodes

Perform all post-change tasks to ensure that your changes are properly implemented in your deployment.

Perform the tasks in the order in which they are presented in the task list.



Caution If you do not receive the results that you expect when you perform these tasks, do not continue until you have resolved the issue.

Before you begin

- Perform all applicable system health checks to verify the changes that were made to your deployment.
- Perform the security enabled cluster tasks if cluster security is enabled for your deployment.

Procedure

Step 1 Run a manual DRS backup and ensure that all nodes and active services back up successfully.

For more information, see the *Administration Guide for Cisco Unified Communications Manager* .

Note
You must run a manual DRS backup after you change the IP address of a node, because you cannot restore a node with a DRS file that contains a different IP address or hostname. The post-change DRS file will include the new IP address or hostname.

Step 2 Update all relevant IP phone URL parameters.

Step 3 Update all relevant IP phone services using Cisco Unified Communications Manager Administration. Choose **System** > **Enterprise Parameters**.

Step 4 Update Unified RTMT custom alerts and saved profiles.

- Unified RTMT custom alerts that are derived from performance counters include the hard-coded server IP address. You must delete and reconfigure these custom alerts.
- Unified RTMT saved profiles that have performance counters include the hard-coded server IP address. You must delete and re-add these counters and then save the profile to update it to the new IP address.

Step 5 If you are using the integrated DHCP server that runs on Cisco Unified Communications Manager, update the DHCP server.

Step 6 Check and make any required configuration changes to other associated Cisco Unified Communications components.

The following is a partial list of some of the components to check:

- Cisco Unity
- Cisco Unity Connection
- CiscoUnity Express
- SIP/H.323 trunks
- IOS Gatekeepers
- Cisco Unified MeetingPlace
- Cisco Unified MeetingPlace Express
- Cisco Unified Contact Center Enterprise
- Cisco Unified Contact Center Express
- DHCP Scopes for IP phones
- SFTP servers that are used for Cisco Unified Communications Manager trace collection for CDR export, or as a DRS backup destination
- IOS hardware resources (conference bridge, media termination point, transcoder, RSVP agent) that register with Cisco Unified Communications Manager
- IPVC video MCUs that register or integrate with Cisco Unified Communications Manager
- Cisco Emergency Responder
- Cisco Unified Application Environment
- Cisco Unified Presence
- Cisco Unified Personal Communicator
- Associated routers and gateways

Note
Consult the documentation for your product to determine how to make any required configuration changes.

Security enabled cluster tasks for Cisco Unified Communications Manager nodes

Initial Trust List and Certificate Regeneration

If you change the IP address or the hostname of a server in a Cisco Unified Communications Manager Release 8.0 or later cluster, the Initial Trust List (ITL) file and the certificates in the ITL are regenerated. The regenerated files do not match the files stored on the phones.

Note If you enable cluster security using Certificate Trust List (CTL) files and USB eTokens, it is not necessary to perform the steps in the following procedure because trust is maintained by the eTokens and the eTokens are not changed.

If cluster security is not enabled, perform the steps in the Single-server cluster or Multi-server cluster procedures to reset the phones.

Regenerate certificates and ITL for single-server cluster phones

If you change the IP address or the hostname of the server in a Cisco Unified Communications Manager Release 8.0 or later single-server cluster and you are using ITL files, perform the following steps to reset the phones.

Enable rollback prior to changing the IP address or hostname of the server.

Procedure

Step 1 Ensure that all phones are online and registered so that they can process the updated ITLs. For phones that are not online when this procedure is performed, the ITL must be deleted manually.

Step 2 Set the Prepare Cluster for Rollback to pre-8.0 enterprise parameter to True. All phones automatically reset and download an ITL file that contains empty Trust Verification Services (TVS) and TFTP certificate sections.

Step 3 On the phone, select **Settings** > **Security** > **Trust List** > **ITL File** to verify that the TVS and TFTP certificate sections of the ITL file are empty.

Step 4 Change the IP address or hostname of the server and let the phones configured for rollback register to the cluster.

Step 5 After all the phones have successfully registered to the cluster, set the enterprise parameter Prepare Cluster for Rollback to pre-8.0 to **False**.

What to do next

If you use CTL files or tokens, re-run the CTL client after you change the IP address or hostname of the server, or after you change the DNS domain name.

Certificate and ITL Regeneration for Multi-Server Cluster Phones

In a multi-server cluster, the phones should have primary and secondary TVS servers to validate the regenerated ITL file and certificates. If a phone can not contact the primary TVS server (due to recent configuration changes), it will fall back to the secondary server. The TVS servers are identified by the CM Group assigned to the phone.

In a multi-server cluster, ensure that you change the IP address or hostname on only one server at a time. If you use CTL files or tokens, re-run the CTL client or the CLI command set **utils ctl** after you change the IP address or hostname of the server, or after you change the DNS domain name.

Perform Post-Change Tasks for IM and Presence Service Nodes

Perform all post-change tasks to ensure that your changes are properly implemented in your deployment.

Caution If you do not receive the results that you expect when you perform these tasks, do not continue until you have resolved the issue.

Before you begin

Perform all the applicable verification system health checks to verify the changes that were made to your deployment.

Procedure

Step 1 If you disabled OpenAM single sign-on (SSO), you can enable it now. For more information about OpenAM SSO, see the *Deployment Guide for IM and Presence Service on Cisco Unified Communications Manager*.

Step 2 If you changed the hostname, you must ensure that the cup, cup-xmpp and Tomcat certificates contain the new hostname.

a) From the Cisco Unified OS Administration GUI, select **Security** > **Certificate Management**.
b) Verify that the names of the trust certificates contain the new hostname.
c) If the certificates do not contain the new hostname, regenerate the certificates.

For more information, see the *Administration Guide for Cisco Unified Communications Manager* .

Step 3 If the IP address for a node has changed, update Cisco Unified Real-Time Monitoring Tool (RTMT) custom alerts and saved profiles:

- RTMT custom alerts that are derived from performance counters include the hard-coded server address. You must delete and reconfigure these custom alerts.
- RTMT saved profiles that have performance counters include the hard-coded server address. You must delete and re-add these counters and then save the profile to update it to the new address.

Step 4 Check and make any required configuration changes to other associated Cisco Unified Communications components, for example, SIP trunks on Cisco Unified Communications Manager.

Step 5 Start all network services that are listed under the CUP Services group using Cisco Unified Serviceability, select **Tools** > **Control Center - Network Services**.

Tip
You do not need to complete this step if you are changing the IP address, hostname, or both the IP address and hostname. Network services are automatically started for these name changes. However, if some services do not automatically start after the change, complete this step to ensure that all network services are started.

You must start the CUP Services network services in the following order:

a. Cisco IM and Presence Data Monitor
b. Cisco Server Recovery Manager
c. Cisco Route Datastore
d. Cisco Login Datastore
e. Cisco SIP Registration Datastore
f. Cisco Presence Datastore
g. Cisco XCP Config Manager
h. Cisco XCP Router
i. Cisco OAM Agent
j. Cisco Client Profile Agent
k. Cisco Intercluster Sync Agent
l. Cisco Config Agent

Step 6 Start all feature services using Cisco Unified Serviceability, select **Tools** > **Control Center - Feature Services**. The order in which you start feature services is not important.

Tip
You do not need to complete this step if you are changing the IP address, hostname, or both the IP address and hostname. Feature services are automatically started for these name changes. However, if some services do not automatically start after the change, complete this step to ensure that all feature services are started.

Step 7 Confirm that your Cisco Jabber sessions have been recreated before you re-enable High Availability. Otherwise, Jabber clients whose sessions are created will be unable to connect.

Run the `show perf query counter "Cisco Presence Engine" ActiveJsmSessions` CLI command on all cluster nodes. The number of active sessions should match the number of users that you recorded when you disabled high availability. If it takes more than 30 minutes for your sessions to start, you may have a larger system issue.

Step 8 Enable High Availability (HA) on all presence redundancy groups if you disabled HA during the pre-change setup.

Step 9 Verify that IM and Presence Service is functioning properly after the changes.

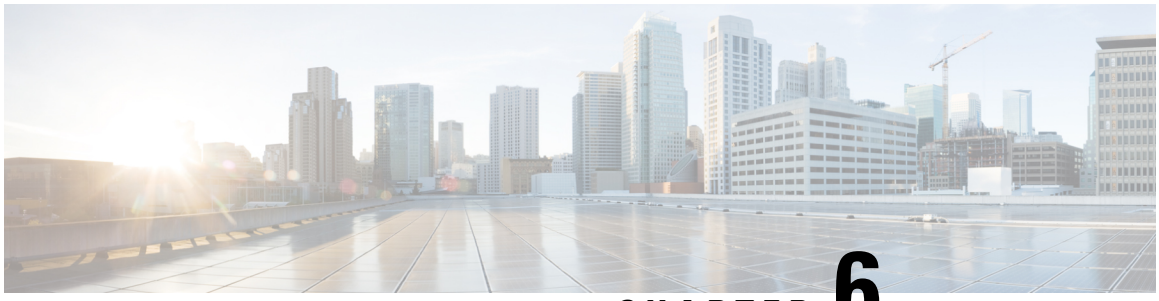
a) From the Cisco Unified Serviceability GUI, select **System** > **Presence Topology**.

- If HA is enabled, verify that all HA nodes are in the Normal state.
- Verify that all services are started.

b) Run the System Troubleshooter from the Cisco Unified CM IM and Presence Administration GUI and ensure that there are no failed tests. Select **Diagnostics** > **System Troubleshooter**.

Step 10 You must run a manual Disaster Recovery System backup after you change the IP address or hostname of a node, because you cannot restore a node with a DRS file that contains a different IP address or hostname. The post-change DRS file will include the new IP address or hostname.

For more information, see the *Administration Guide for Cisco Unified Communications Manager* .



CHAPTER 6

Troubleshooting Address Change Issues

- Troubleshoot Cluster Authentication, on page 49
- Troubleshoot Database Replication, on page 49
- Troubleshoot Network, on page 55
- Network Time Protocol troubleshooting, on page 56

Troubleshoot Cluster Authentication

You can troubleshoot cluster authentication issues on subscriber nodes using the Command Line Interface (CLI).

Procedure

Step 1 Enter **`show network eth0 [detail]`** to verify network configuration.

Step 2 Enter **`show network cluster`** to verify the network cluster information.

- If the output displays incorrect publisher information, enter the **`set network cluster publisher [hostname/IP address]`** CLI command on the subscriber node to correct the information.
- If you are on a publisher node, and the `show network cluster` CLI command displays incorrect subscriber information, login to Cisco Unified Communications Manager Administration and choose **System** > **Server** to check the output.
- If you are on a subscriber node and the `show network cluster` output displays incorrect publisher information, use the `set network cluster publisher [hostname | IP_address]` CLI command to change the publisher hostname or IP address.

Troubleshoot Database Replication

You can use the Command Line Interface (CLI) to troubleshoot database replication on the nodes in your cluster.

- Verify that database replication is in a correct state in the cluster.

- Repair and reestablish database replication for the nodes.
- Reset database replication.

For more information about these commands or using the CLI, see the *Command Line Interface Guide for Cisco Unified Communications Solutions*.

Verify Database Replication

Use the Command Line Interface (CLI) to check the database replication status for all nodes in the cluster. Verify that the Replication Setup (RTMT) & Details shows a value of `2`. Anything other than 2 means that there is a problem with database replication and that you need to reset replication for the node. See topics related to database replication examples for example output.

Procedure

Step 1 Enter **`utils dbreplication runtimestate`** on the first node to check database replication on all nodes in the cluster.

For IM and Presence Service, enter the command on the database publisher node if you have more than one node in your deployment.

Tip
If replication is not set up for the nodes in your cluster, you can reset database replication for the nodes using the CLI. For more information, see topics related to resetting database replication using the CLI.

Example:

```
admin: utils dbreplication runtimestate

DDB and Replication Services: ALL RUNNING

DB CLI Status: No other dbreplication CLI is running...

Cluster Replication State: BROADCAST SYNC Completed on 1 servers at:
2013-09-26-15-18
     Last Sync Result: SYNC COMPLETED 257 tables sync'ed out of 257
     Sync Errors: NO ERRORS

DB Version: ccm9_0_1_10000_9000
Number of replicated tables: 257
Repltimeout set to: 300s

Cluster Detailed View from PUB (2 Servers):

                          PING        REPLICATION REPL. DBver& REPL. REPLICATION
SETUP
SERVER-NAME IP ADDRESS    (msec) RPC? STATUS      QUEUE TABLES LOOP? (RTMT) &
details
----------- ------------ ------ ---- ----------- ----- ------ -----
-----------------
server1     100.10.10.17 0.052  Yes  Connected   0     match  Yes   (2) PUB Setup
 Completed
server2     100.10.10.14 0.166  Yes  Connected   0     match  Yes   (2) Setup
Completed
```

Step 2 Verify the output.

The output should show a replication status of **Connected** and a replication setup value of **(2) Setup Complete** for each node. This means that the replication network within the cluster is functioning properly. If the output results are different, proceed to troubleshoot and repair database replication.

Example Database Replication CLI Output

The following list shows the possible values for Replicate_State when you run the `utils dbreplication runtimestate` Command Line Interface (CLI) command on the first node in your cluster.

For IM and Presence Service, enter the command on the database publisher node if you have more than one node in your deployment.

- 0 - Replication Not Started. Either no subscribers exist, or the Database Layer Monitor service has not been running since the subscriber was installed.
- 1 - Replicates have been created, but their count is incorrect.
- 2 - Replication is good.
- 3 - Replication is bad in the cluster.
- 4 - Replication setup did not succeed.

Note It is important to verify that the Replication Setup (RTMT) & Details shows a value of `2`. Anything other than 2 means that there is a problem with database replication and that you need to reset replication. For information about resolving database replication issues, see topics related to troubleshooting database replication.

Example CLI Output for Cisco Unified Communications Manager Node

In this example, the Replication Setup (RTMT) & Details shows a value of `2`. Replication is good.

```
admin: utils dbreplication runtimestate
Server Time: Mon Jun 1 12:00:00 EDT 2013

Cluster Replication State: BROADCAST SYNC Completed on 1 servers at:
2013-06-01-12-00
   Last Sync Result: SYNC COMPLETED on 672 tables out of 672
   Sync Status: NO ERRORS
   Use CLI to see detail: 'file view activelog
cm/trace/dbl/2013_06_01_12_00_00_dbl_repl_output_Broadcast.log'

DB Version: ccm10_0_1_10000_1
Repltimeout set to: 300s
PROCESS option set to: 1

Cluster Detailed View from uc10-pub (2 Servers):

                      PING       Replication  REPLICATION SETUP
SERVER-NAME IP ADDRESS (msec) RPC? Group ID     (RTMT) & Details
----------- ---------- ------ ---- ----------- -------------------
uc10-pub    192.0.2.95 0.040  Yes    (g_2)     (2) Setup Completed
uc10-sub1   192.0.2.96 0.282  Yes    (g_3)     (2) Setup Completed
```

Example CLI Output for IM and Presence Service Node

In this example, the Replication Setup (RTMT) & Details shows a value of 2. Replication is good.

```
admin: utils dbreplication runtimestate
Server Time: Mon Jun 1 12:00:00 EDT 2013

DB and Replication Services: ALL RUNNING

Cluster Replication State: Replication status command started at: 2012-02-26-09-40

   Replication status command COMPLETED 269 tables checked out of 269
   No Errors or Mismatches found.
   Use 'file view activelog
cm/trace/dbl/sdi/ReplicationStatus.2012_02_26_09_40_34.out' to see the details

DB Version: ccm8_6_3_10000_23
Number of replicated tables: 269

Cluster Detailed View from PUB (2 Servers):

                        PING       REPLICATION   REPL. DBver&  REPL.  REPLICATION
 SETUP
SERVER-NAME IP ADDRESS (msec) RPC? STATUS        QUEUE TABLES  LOOP? (RTMT) &
details
----------- ------------ ------ ---- ----------- ----- ------- -----
-----------------
gwydla020218 10.53.46.130 0.038 Yes Connected    0     match   Yes   (2) PUB Setup
 Completed
gwydla020220 10.53.46.133 0.248 Yes Connected    128   match   Yes   (2) Setup
Completed
```

Repair Database Replication

Use the Command Line Interface (CLI) to repair database replication.

Procedure

Step 1 Enter **utils dbreplication repair all** on the first node to attempt to repair database replication.

For IM and Presence Service, repair the database replication status from the database publisher node if you have more than one node in your deployment.

Depending on the size of the database, it may take several minutes to repair database replication. Proceed to the next step to monitor the progress of database replication repair.

Example:

```
admin:utils dbreplication repair all
-------------------- utils dbreplication repair --------------------

Replication Repair is now running in the background.
Use command 'utils dbreplication runtimestate' to check its progress

Output will be in file cm/trace/dbl/sdi/ReplicationRepair.2013_05_11_12_33_57.out
```

```
Please use "file view activelog
cm/trace/dbl/sdi/ReplicationRepair.2013_05_11_12_33_57.out " command to see the
output
```

Step 2 Enter **utils dbreplication runtimestate** on the first node to check the progress of replication repair.

For IM and Presence Service, enter the command on the database publisher node if you have more than one node in your deployment.

The bolded text in the example replication output highlights the final status of the replication repair.

Example:

```
admin:utils dbreplication runtimestate

DB and Replication Services: ALL RUNNING

Cluster Replication State: Replication repair command started at: 2013-05-11-12-33

     Replication repair command COMPLETED 269 tables processed out of 269
     No Errors or Mismatches found.

     Use 'file view activelog
cm/trace/dbl/sdi/ReplicationRepair.2013_05_11_12_33_57.out' to see the details

DB Version: ccm8_6_4_98000_192
Number of replicated tables: 269

Cluster Detailed View from PUB (2 Servers):

                          PING        REPLICATION REPL. DBver& REPL. REPLICATION
SETUP
SERVER-NAME IP ADDRESS    (msec) RPC? STATUS      QUEUE TABLES LOOP? (RTMT) &
details
----------- ------------ ------ ---- ----------- ----- ------ -----
-----------------
server1     100.10.10.17 0.052  Yes  Connected   0     match  Yes   (2) PUB Setup
 Completed
server2     100.10.10.14 0.166  Yes  Connected   0     match  Yes   (2) Setup
Completed
```

a) If replication repair runs to completion without any errors or mismatches, run the procedure to verify the node name change again to validate that the new node name is now correctly replicated.
b) If errors or mismatches are found, there may be a transient mismatch between nodes. Run the procedure to repair database replication again.

Note
If, after several attempts to repair replication, mismatches or errors are being reported, contact your Cisco Support Representative to resolve this issue.

Step 3 Enter **utils dbreplication reset all** on the first node to attempt to reestablish replication.

For IM and Presence Service, enter the command on the database publisher node if you have more than one node in the deployment.

Depending on the size of the database, it may take several minutes to over an hour for replication to be fully reestablished. Proceed to the next step to monitor the progress of database replication reestablishment.

Example:

```
admin:utils dbreplication reset all
This command will try to start Replication reset and will return in 1-2 minutes.
Background repair of replication will continue after that for 1 hour.
Please watch RTMT replication state. It should go from 0 to 2. When all subs
have an RTMT Replicate State of 2, replication is complete.
If Sub replication state becomes 4 or 1, there is an error in replication setup.
Monitor the RTMT counters on all subs to determine when replication is complete.
Error details if found will be listed below
OK [10.53.56.14]
```

Step 4 Enter **utils dbreplication runtimestate** on the first node to monitor the progress of the attempt to reestablish database replication.

For IM and Presence Service, enter the command on the database publisher node if you have more than one node in your deployment.

Replication is considered to be reestablished when all nodes show a replication status of **Connected** and a replication setup value of **(2) Setup Complete**.

Example:

```
admin: utils dbreplication runtimestate

DDB and Replication Services: ALL RUNNING

DB CLI Status: No other dbreplication CLI is running...

Cluster Replication State: BROADCAST SYNC Completed on 1 servers at:
2013-09-26-15-18
     Last Sync Result: SYNC COMPLETED 257 tables sync'ed out of 257
     Sync Errors: NO ERRORS

DB Version: ccm9_0_1_10000_9000
Number of replicated tables: 257
Repltimeout set to: 300s

Cluster Detailed View from newserver100 (2 Servers):
                          PING       REPLICATION REPL. DBver& REPL. REPLICATION
 SETUP
SERVER-NAME IP ADDRESS     (msec) RPC? STATUS      QUEUE TABLES LOOP? (RTMT)  &
details
----------- -------------- ------ ---- ----------- ----- ------ -----
-----------------
server1     100.10.10.201  0.038  Yes  Connected   0     match  Yes   (2) PUB
Setup Completed
server2     100.10.10.202  0.248  Yes  Connected   0     match  Yes   (2) Setup
Completed
server3     100.10.10.203  0.248  Yes  Connected   0     match  Yes   (2) Setup
Completed
server4     100.10.10.204  0.248  Yes  Connected   0
```

a) If replication is reestablished, run the procedure to verify the node name change again to validate that the new node name is now correctly replicated.

b) If replication does not recover, contact your Cisco Support Representative to resolve this issue.

Caution

Do not proceed beyond this point if database replication is broken.

Reset Database Replication

Reset database replication if replication is not set up for the nodes in your cluster. You can reset database replication using the command line interface (CLI).

Before you begin

Check database replication status for all nodes in the cluster. Verify that the Replication Setup (RTMT) & Details shows a value of `2`. Anything other than 2 means that there is a problem with database replication and that you need to reset replication for the node.

Procedure

Step 1 Reset replication on nodes in your cluster. Do one of the following:

a) For Unified Communications Manager, enter **`utils db replication reset all`**.

Before you run this CLI command on any Cisco Unified Communications Manager nodes, first run the command **`utils dbreplication stop`** on all subscriber nodes that are reset, and then on the publisher server. For more information, see the *Command Line Interface Guide for Cisco Unified Communications Solutions*.

b) For IM and Presence Service, enter **`utils db replication reset all`** on the database publisher node to reset all IM and Presence Service nodes in the cluster.

Tip
You can enter a specific hostname instead of **all** to reset database replication on only that node. For more information, see the *Command Line Interface Guide for Cisco Unified Communications Solutions*.

Step 2 Enter **`utils dbreplication runtimestate`** to check the database replication status.

For IM and Presence Service, run the CLI command on the IM and Presence database publisher node

Troubleshoot Network

You can troubleshoot network issues on nodes using the Command Line Interface (CLI).

Procedure

Step 1 Enter **`show network eth0 [detail]`** to verify network configuration.

Step 2 If any of the fields are missing, then reset the network interface.

a) Enter **`set network status eth0 down`**.

b) Enter **`set network status eth0 up`**.

Step 3 Verify the IP address, mask, and gateway.

Ensure that these values are unique across the network.

Network Time Protocol troubleshooting

Troubleshoot NTP on Subscriber Nodes

You can troubleshoot Network Time Protocol (NTP) issues on subscriber nodes using the Command Line Interface (CLI).

Procedure

Step 1 Enter **`show network eth0 [detail]`** to verify network configuration.

Step 2 Enter **`utils ntp status`** to verify NTP status.

Step 3 Enter **`utils ntp restart`** to Restart NTP.

Step 4 Enter **`show network cluster`** to verify the network cluster.

If the output displays incorrect publisher information, use the **`set network cluster publisher [hostname/IP_address]`** CLI command to reset the publisher.

Troubleshoot NTP on Publisher Nodes

You can troubleshoot Network Time Protocol (NTP) issues on publisher nodes using the Command Line Interface (CLI).

Procedure

	Command or Action	Purpose
Step 1	Enter **`show network eth0 [detail]`** to verify network configuration.	
Step 2	Enter **`utils ntp status`** to verify NTP status.	
Step 3	Enter **`utils ntp restart`** to Restart NTP.	
Step 4	Enter **`utils ntp server list`** to verify NTP servers.	To add or delete an NTP server, use the **`utils ntp server [add/delete]`** CLI command.