Unified CCX System Management

Unified CCX administration provides options to configure, control, and monitor Unified CCX component activities and information across a cluster.

Note Support for High Availability and remote servers is available only in multiple-server deployments.

See the *Cisco Unified Contact Center Express Install and Upgrade Guide* for instructions about tasks that significantly change your Unified CCX deployment, such as:

- Changing from a single-server deployment to a multiple-server deployment.
- Removing a Unified CCX Software component from a server.
- Moving a Unified CCX Software component to another server.
- Changes to a Unified CCX cluster (adding, removing, or replacing a server).

The following sections describe the day-to-day management of Unified CCX components.

Basic Terminology

This section provides information about different Unified CCX terminology.

- **Cluster**. A Unified CCX cluster (often referred to as cluster in this manual) consists of one or more servers (nodes) that are running Unified CCX components in your Unified CCX deployment. If you deploy Unified CCX components on a single server, the Unified CCX cluster consists of that server. If you deploy Unified CCX on multiple servers, the cluster includes the Unified CCX server and standby server on which you installed Unified CCX. The Unified CCX cluster supports up to two Unified CCX

servers, one designated as the *active Unified CCX server* and the other designated as the *standby Unified CCX server* for high availability purposes.

Note Support for High Availability and remote servers is available only in multiple-server deployments.

- **Cluster profile**. The Unified CCX Administration web page (home page) displays information about the cluster profile. A cluster profile includes data relating to the Unified CCX servers, components, and licenses installed in a cluster.
- **Node (server)**. A server that is part of the Unified CCX cluster.
- **Active Server**. The active server provides all system services and resources. You can deploy one active server in each Unified CCX subsystem. If the active server fails, the Unified CCX subsystem automatically fails over to the standby server.
- **Standby Server**. You can deploy up to two servers in each Unified CCX system for high availability—one active server (master) and one standby (not active) server. With high availability, if an active server becomes unavailable, the standby server automatically becomes the active server.
- **Component**.The software units in the Unified CCX system. The main software components of the Unified CCX server are the Engine, datastores, monitoring, recording, and the Cluster View Daemon (CVD). See the *Cisco Unified Contact Center Express Install and Upgrade Guide* for more information on setup and installation procedures.
- **Service**. An executable unit. A service may have other services as its children. (For example, subsystems and managers are children of the engine service).
- **Feature**. A logical representation of the functional unit.
- **Master service**. A specially-elected service. Only one service from the Engine service, or database services set can be the master within the Unified CCX Engine component.
- **Standby service**. An active service that can take over the master functionality in case the master service becomes unavailable within the Unified CCX Engine component. You cannot configure the standby service. The Cluster View Daemon (CVD) dynamically elects the services on the active node to be the master.

High Availability and Automatic Failover

Note Support for High Availability (HA) and remote servers is available only in multiple-server deployments. Unified CCX does not support more than two nodes in a HA setup. Expansion servers where the Database, Monitoring, or Recording components are running on separate servers are not supported.

Unified CCX provides high availability and automatic failover capability through the use of two servers, the *active server* and the *standby server*.

The active server provides all system services and resources; no services or resources are available from the standby server. When you make administrative changes on the active server, both the servers are synchronized.

If the active server fails, there is automatic failover to the standby server. For detailed information on HA over WAN deployment, see *Cisco Unified Contact Center Express Design Guide* .

Note After a Unified CCX failover or failback the agent state changes to Not Ready state.

Network Partitions

Network malfunction or misconfiguration can create network partitions and split the network into separate *islands*. If a node enters this state, the node is referred to as being in the island mode. Nodes in the island mode are hard to detect. While these nodes can communicate within a partitioned island, they cannot communicate between partitioned islands. If the islands do not communicate, then each island will select its own active server.

Generally, you can connect to the Unified CCX administration on any node, and see a consistent cluster view. If a node is in the island mode, you will see different cluster views when you connect to nodes in each island.

Note Support for High Availability and remote servers is available only in multiple-server deployments.

If your node enters the island mode, it should recover from the island mode as soon as the underlying network issue is resolved. If the island mode persists, check the network connectivity/reachability between the two CCX servers and take action accordingly.

Unified CCX CDS Information Management

The Unified CCX system stores configuration information in the Cisco Configuration Datastore Server (CDS). The Unified CCX Administration configurations are stored in the CDS.

Note Support for High Availability and remote servers is available only in multiple-server deployments.

The Unified CCX server can receive directory information from one Cisco Unified Communications directory and application configuration and script logic from a repository on another server.

Manage System Parameters

The parameters in the System Parameters Configuration page are grouped logically into sections with headings. Each parameter has a corresponding suggested or default value on the right side of the page. Where applicable, radio buttons are used to toggle between the parameter options.

In this web page, you can configure the port settings, default session timeout, and codec.

Note Changing some system parameters like IP address, Network Time Protocol (NTP) and so on can result in a different License MAC. You need to get rehosted license files (with new License MAC) in such cases within 30-day grace period beyond which the system will stop working.

Procedure

Step 1 Choose **System** > **SystemParameters** from the Unified CCXAdministration menu bar.

The System Parameters Configuration web page appears.

Step 2 Click the **Update** icon that displays in the tool bar in the upper, left corner of the window or the **Update** button that displays at the bottom of the window.

The system notifies all nodes in the cluster about the changes.

Note If Cluster View Daemon is in Shutdown state during this operation, then the changes just made are synchronized on that node when Cluster View Daemon is started again.

Related Topics

System Parameters

Unified CCX IP Address/hostname Management

This section provides the steps you need to follow whenever there is a change in IP address/hostname for the following Unified CCX deployments:

- Unified CCX Cluster with Single-node
- Unified CCX Cluster with High Availability (HA)

You may want to change the IP address/hostname for a variety of reasons, including moving the server from one segment to another or resolving a duplicate IP address/hostname problem.

Note Hostname change is supported in Cisco Unified CCX.

The character limit for Hostname is 63 characters.

Prepare System for IP Address/hostname Change

Perform the following tasks to ensure that your system is prepared for a successful IP address/hostname change.

Note If you do not receive the results that you expect when you perform these tasks, do not continue with this procedure until after you resolve any problems that you find. DB replication across the entire cluster is essential for this process. Also, if the DNS check fails then the IP Address/hostname change will not happen.

Procedure

Step 1 List all servers in the cluster and note whether the nodes are defined by using IP addresses or hostnames.

- From **Cisco Unified CCX Administration** menu bar on the first node, navigate to **System** > **Server**. A list of all servers in the cluster displays.
- See whether the servers are defined using IP addresses or hostnames and capture this list of servers for later reference. Ensure that you have saved an inventory of both the hostname and IP address of each node in your cluster.

Step 2 Ensure that all servers in the cluster are up and available by checking for any active ServerDown alerts. You can check by using either the Real Time Monitoring Tool (RTMT) or the Command Line Interface (CLI) on the first node.

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

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

Step 3 Check the DB replication status on all the Cisco CRS nodes and Cisco Unified Communications nodes in the cluster to ensure that all servers are replicating database changes successfully using the following substeps:

a) **For Unified CCX**: In a High Availability deployment of Unified CCX, you can check the DB replication status for the datastores across all servers in the cluster using Unified CCX Serviceability Administration. Choose **Tools** > **Datastore Control Center** > **Replication Servers** from the Unified CCX Serviceability menu bar to view the replication status. The value in State field for both the servers in this web page should display ACTIVE/ CONNECTED.

b) **For Cisco Unified Communications Platform**: You can check the DB replication status on all the Cisco Unified Communications nodes in the cluster by using either RTMT or a CLI command.

- To check by using RTMT, access the Database Summary and inspect the replication status.
- To check by using the CLI, enter the command that is shown in the following example:

```
admin: show perf query class "Number of Replicates Created and
 State of Replication"
==>query class :

- Perf class (Number of Replicates Created and State of
Replication)
has instances and values:
ReplicateCount  -> Number of Replicates Created   = 344
ReplicateCount  -> Replicate_State                = 2
```

Be aware that the Replicate_State object shows a value of 2 in this case. The following list shows the possible values for Replicate_State:

- 0—Replication Not Started. Either no subscribers exist, or the Database Layer Monitor service is not running and 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.

Step 4 Run a manual DRS backup and ensure that all nodes and active services are backed up successfully.

Step 5 Run the CLI command **`utils diagnose module validate_network`** through Platform CLI on all nodes in the cluster to ensure network connectivity and DNS server configuration are intact.

IP Address Modification

This section describes how to change the IP address.

Caution Changing the IP address on any node in a Cisco CRS cluster can interrupt call processing and other system functions. Also, changing the IP address can cause the system to generate certain alarms and alerts such as ServerDown and automatic failover to a backup server may not operate. Because of this potential impact to the system, you must perform IP address changes during a planned maintenance window.

Note When there is a change in the Unified CCX server subnet, you must change the default gateway IP address. Ensure the following:

- The new default gateway IP address is configured on the Unified CCX server.
- The DNS is reachable and the DNS record exists for the Unified CCX server.

Change IP Address for Server in Single-Node Deployment

Use this procedure to change the IP address of the server in a single-node deployment.

Caution Ensure that the server on the same subnet or that is moved to the new subnet has access to the configured default gateway before proceeding to change the IP address of the server.

Procedure

Step 1 Change the DNS record of the server to point to the new IP address. Ensure that you correctly update both the forward (A) and reverse (PTR) records, and there are no duplicate PTR records.

Step 2 If you want to change the IP address of the server on the same subnet or a different subnet that requires a new default gateway address, use either of the following methods:

- CLI commands
- Cisco Unified Communications Operating System Administration interface

Using CLI commands:

a) To change the default gateway, enter the following CLI command:

set network gateway <*IP Address*>

The following sample output displays:

```
admin:set network gateway 10.3.90.2

WARNING: Changing this setting will invalidate software license
         on this server. The license will have to be re-hosted.
Continue(y/n):
Continue (y/n)?y
```

b) To change the IP address of the server, enter the following CLI command:

set network ip eth0 <ip_address> <netmask> <default gateway> where `ip_address` specifies the new server IP address and `netmask` specifies the new server network mask and `default gateway` specifies the default gateway of the new server.

The following sample output displays:

```
admin: set network ip eth0 10.3.90.21 255.255.254.0 10.3.90.1
** W A R N I N G ***
If there are IP addresses (not hostnames)
configured in UCCX Administration
under System -> Servers then you must change
the IP address there BEFORE changing it here
or call processing will fail. This will cause the
system to restart
=======================================================
Note: To recognize the new IP address all nodes within
the cluster will have to be manually rebooted.
=======================================================
Do you want to continue?
Enter "yes" to continue and restart or any other key
to abort
```

Enter **y** and press **Enter**. This will automatically reboot this server with the new IP address.

Using Cisco Unified Communications Operating System Administration interface:

Alternatively, you can change the IP address and default gateway of the server from **Cisco Unified Communications Operating System Administration** interface as follows:

- Choose **Settings** > **IP** > **Ethernet**.
- Change the IP address, default gateway, and netmask, and click **Save**. The server restarts automatically with the new IP address.

If you change the IP address, License MAC of the server will also change. Rehost the new license. Old license enters its grace period.

What to do next

When the Cloud Connect services are enabled, after the Unified CCX IP address has been changed, run the following CLI command to restart the services.

```
utils cloudconnect reinit services
```

Note In a high availability (HA) deployment, run this CLI command on other nodes of the cluster.

IP Address Modification in High-Availability (HA) Deployment

Note Ensure that the IP Address is sequentially changed first in the Publisher and then the Subscriber node of the Unified CCX servers.

Change IP Address for Publisher Server in HA Deployment

Use this procedure to change the IP address of the publisher server in a HA deployment.

Caution Before changing the IP address of the server, ensure that the server has access to the configured default gateway. This applies whether the server is on the same subnet or is moved to a new subnet.

Procedure

Step 1 Change the DNS record of the publisher server to point to the new IP address. Ensure that you correctly update both the forward (A) and reverse (PTR) records, and there are no duplicate PTR records.

Step 2 Verify that the DNS change propagates to other nodes. To verify, use the **utils network host** <*IP Address*> CLI command on all the cluster nodes.

Step 3 From the Cisco Unified Operating System Administration page of the subscriber server in the cluster, perform the following tasks:

a) Navigate to **Settings** > **IP** > **Publisher**.
b) Change the IP address of the publisher server.

Step 4 To update the new IP of the publisher server in the subscriber, enter the following CLI command on the subscriber server:

```
utils uccx modify remote_IPAddress <Old_IP_of_Publisher>
<New_IP_of_Publisher>
```

The following output appears:

```
admin:utils uccx modify remote_IPAddress 10.3.90.21  10.3.90.28

 Old Remote IP Address: 10.3.90.21
 New Remote IP Address: 10.3.90.28

This command should be executed only in case you are changing IP Address of remote server.
Are you sure you want to run this command?
Continue (y/n)?
```

Enter **y** and press **Enter**.

Step 5 To change the IP address of the server on the same subnet or a different subnet that requires a new default gateway address, use either of the following methods:

- CLI commands
- Cisco Unified Operating System Administration interface

Using CLI commands:

a) To change the default gateway, enter the following CLI command:

set network gateway <*IP Address*>

The following sample output appears:

```
admin:set network gateway 10.3.90.2

WARNING: Changing this setting will invalidate software license
         on this server. The license will have to be re-hosted.
Continue(y/n):
Continue (y/n)?y
```

Caution Ensure that the server is in the new subnet and has access to the default gateway before proceeding to the following sub-step.

b) To change the IP address of the publisher server, enter the following CLI command:

set network ip eth0 <ip_address> <netmask> <default gateway> where ip_address specifies the new server IP address, netmask specifies the new server network mask and default gateway specifies the default gateway of the new server.

The following sample output appears:

```
admin:set network ip eth0 10.78.92.55 255.255.255.0 10.78.92.1

WARNING: Changing this setting will invalidate software license
         on this server. The license will have to be re-hosted.
Continue (y/n)?y
           ***   W A R N I N G   ***
This command will cause the system to restart
======================================================
 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.
       To recognize the new ip address all nodes within
       the cluster will have to be manually rebooted.
======================================================
Continue (y/n)?y
```

Enter **y** and press **Enter**. The server is automatically rebooted with the new IP address.

Using Cisco Unified Operating System Administration interface:

Alternatively, you can change the IP address and default gateway of the server from the **Cisco Unified Operating System Administration** interface as follows:

- Choose **Settings** > **IP** > **Ethernet**.
- Change the IP address, default gateway, and netmask, and click **Save**. The server restarts automatically with the new IP address.

Step 6 Reboot the publisher server in the cluster by using the `utils system restart` CLI command. After 10 minutes, reboot the subscriber server with the same command.

Note If you do not reboot the subscriber after the IP address change, all the services on the publisher may not start properly.

If you change the IP address, the License MAC also changes. Rehost the new license for the new License MAC. Old license enters its grace period.

Change IP Address for Subscriber Server in HA Deployment

Use this procedure to change the IP address of a subscriber server in a HA deployment.

Caution Before changing the IP address of the server, ensure that the server has access to the configured default gateway. This applies whether the server is on the same subnet or is moved to a new subnet.

Procedure

Step 1 Change the DNS record of the subscriber server to point to the new IP address. Ensure that you correctly update both the forward (A) and reverse (PTR) records, and there are no duplicate PTR records.

Step 2 Verify that the DNS change propagates to the other nodes. To verify, use the `utils network host` <*IP Address*> CLI command on all the cluster nodes.

Caution Skip Step 3 if the server is defined by hostname and you are changing only the IP address.

Step 3 From **Cisco Unified CCX Administration** page, perform the following tasks:

a) Navigate to **System** > **Server**. From the List Servers web page, click the IP address of the subscriber server.

The Server Configuration page for the subscriber server opens.

b) Enter the new IP address in the **Host Name/IP Address** field and click **Save**.

Note You can use the CLI command `run sql select name,nodeid from ProcessNode` to check whether the new IP address has been replicated on all the servers.

Step 4 To update the new IP of the subscriber in the publisher, enter the following CLI command on the publisher server:

utils uccx modify remote_IPAddress <Old_IP_of_Subscriber> <New_IP_of_Subscriber>

The following output appears:

```
admin:utils uccx modify remote_IPAddress 10.3.90.21  10.3.90.28

 Old Remote IP Address: 10.3.90.21
 New Remote IP Address: 10.3.90.28

This command should be executed only in case you are changing IP
Address of remote server.
Are you sure you want to run this command?
Continue (y/n)?
```

Enter **y** and press **Enter**.

Step 5 If you want to change the IP address of the server on the same subnet or a different subnet that requires a new default gateway address, use either of the following methods:

- CLI commands
- Cisco Unified Communications Operating System Administration interface

Using CLI commands:

a) To change the default gateway, enter the following CLI command:

set network gateway <*IP Address*>

The following sample output appears:

```
admin:set network gateway 10.3.90.2

WARNING: Changing this setting will invalidate software license
         on this server. The license will have to be re-hosted.
Continue(y/n):
Continue (y/n)?y
```

Caution Ensure that the server is in the new subnet and has access to the default gateway before proceeding to the following sub-step.

b) To change the IP address of the server, enter the following CLI command:

set network ip eth0 <ip_address> <netmask> <default gateway> where ip_address specifies the new server IP address, netmask specifies the new server network mask and default gateway specifies the default gateway of the new server.

The following sample output appears:

```
admin:set network ip eth0 10.78.92.55 255.255.255.0 10.78.92.1

WARNING: Changing this setting will invalidate software license
         on this server. The license will have to be re-hosted.
Continue (y/n)?y
           ***   W A R N I N G   ***
This command will cause the system to restart
======================================================
 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.
       To recognize the new ip address all nodes within
       the cluster will have to be manually rebooted.
======================================================
Continue (y/n)?y
```

Enter **y** and press **Enter**. The server is now automatically rebooted with the new IP address.

Using Cisco Unified Communications Operating System Administration interface:

Alternatively, you can change the IP address and default gateway of the server from **Cisco Unified Communications Operating System Administration** interface as follows:

- Choose **Settings** > **IP** > **Ethernet**.
- Change the IP address, default gateway, and netmask, and click **Save**. The server restarts automatically with the new IP address.

Step 6 Reboot all the servers in the cluster including the publisher using the CLI command `utils system restart`.

Note If you do not reboot the subscriber after the IP address change, all the services on the publisher may not start properly.

HostName and Domain Name Modification

Changing the hostname or domain name on any node in the Unified CCX cluster can interrupt call processing and other system functions. It can cause the system to generate certain alarms and alerts such as ServerDown and automatic failover to a backup server may fail. To prevent these failures, ensure to change the hostname or domain name during a planned maintenance window.

As a prerequisite ensure that the DNS is reachable and the DNS record exists for the server with its current fully qualified domain name (FQDN) and the IP address.

Note
- Ensure Single Sign-On is disabled before modifying the hostname or domain name.

HostName Modification

This section describes how to change the hostname.

Change HostName for Server in a Single-Node Deployment

Use this procedure to change the hostname of the server in a single-node deployment.

Note The hostname can have a maximum of 63 characters.

Ensure Single Sign-On is disabled before modifying the hostname.

Procedure

Step 1 Change the DNS record of the server to point to the new hostname. Ensure that you correctly update both the forward (A) and reverse (PTR) records, and there are no duplicate PTR records.

Step 2 You can change the hostname of the server either using the CLI (command line interface) command or using **Cisco Unified OS Administration** interface. To change the hostname using CLI command, go to step 3 or to change the hostname using **Cisco Unified OS Administration** interface go to step 4.

Step 3 At the CLI prompt, perform the following tasks:

a) Enter the CLI command **`set network hostname`** and press **Enter**.

The following sample output displays:

```
admin:set network hostname

WARNING: Changing this setting will invalidate software license
         on this server. The license will have to be re-hosted.
Continue(y/n):
Continue (y/n)?y
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 UCCX Certificates including any third party
       signed Certificates that have been uploaded.

Continue (y/n)?y
Enter the hostname:
```

b) Enter **y** twice to continue and enter the hostname and press **Enter**.

Step 4 From **Cisco Unified OS Administration** interface, perform the following task:

a) Choose **Settings** > **IP** > **Ethernet**.
b) Change the hostname.
c) Click **Save**. The server automatically reboots with the new hostname.

Step 5 On changing the hostname/IP address, License MAC of the server changes. Rehost the new license. Old license enters its grace period.

Step 6 Verify the status of Customer Collaboration Platform:

Step 7 Regenerate the SAML certificate through the **Cisco Identity Service Administration**.

If Single Sign-On must be enabled, then perform the following steps:

a. Establish the trust between the Cisco Identity Service and Identity Provider.

b. Log in to the Cisco Unified CCX Administration and navigate to **System** -> **Single Sign-On**.

c. Click **Register** to onboard the SSO components even if you had onboarded the components earlier.

d. You can now enable Single Sign-On after you perform **SSO Test** again.

HostName Modification in High-Availability (HA) Deployment

The character limit for Host Name is 24 characters.

Related Topics

Single Sign-On (SSO)

Change HostName for Publisher Server in HA Deployment

Use this procedure to change the hostname of publisher server in a HA deployment.

Note Ensure Single Sign-On is disabled before performing the change in hostname.

Procedure

Step 1 Change the DNS record of the publisher server to point to the new hostname. Ensure that you correctly update both the forward (A) and reverse (PTR) records, and there are no duplicate PTR records.

Step 2 Verify that the DNS change propagates to other nodes by using the **`utils network host`** <*IP Address*> CLI command on all the cluster nodes.

Step 3 To change the hostname of the publisher on the subscriber node, use either of the following methods:

- CLI commands
- Cisco Cisco Unified OS Administration interface

Using CLI commands:

a) Run the following CLI command on the subscriber node:

`set network cluster publisher hostname` `<hostname>`

where `hostname` is the new publisher.

The following output displays:

```
admin:set network cluster publisher hostname hijk-lmn-n1

New Remote hostname: hijk-lmn-n1
```

Using Cisco Unified OS Administration interface:

From interface of the subscriber server, perform the following tasks:

a) Navigate to **Setting** > **IP** > **Publisher**.
b) The Server Configuration page for the publisher server opens. Change the hostname of Publisher server in the **Host Name** or **IP Address** field and then click **Save**.

Step 4 Run the following CLI command on the Subscriber node to update new hostname of the Publisher server :

```
utils uccx modify remote_hostname <Old_hostname_of_Publisher> <New_hostname_of_Publisher>
```

The following output displays:

```
admin:utils uccx modify remote_hostname abcd-efg-n1 hijk-lmn-n1

 Old Remote hostname: abcd-efg-n1
 New Remote hostname: hijk-lmn-n1

This command should be executed only in case you are changing Hostname of remote server.
Are you sure you want to run this command?
Continue (y/n)?
```

Enter **y** and press **Enter**.

Step 5 To change the hostname of publisher server, use either of the following methods:

- CLI commands
- Cisco Unified OS Administration interface

Using CLI commands:

a) Run the following CLI command on the publisher node:

```
set network hostname
```

The following output displays:

```
admin:set network hostname


***   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 UCCX Certificates including any third party
       signed Certificates that have been uploaded.

Continue (y/n)?
```

Enter **y** and press **Enter**.

b) Enter the hostname when prompted. The system services will automatically restart.

Using Cisco Unified OS Administration interface:

Change the hostname using Cisco Unified OS Administration interface of the publisher server:

a) Choose **Settings** > **IP** > **Ethernet**.
b) Change the hostname.
c) Click **Save**. The system services will automatically restart.

Step 6 Reboot all the servers in the cluster including the publisher using the CLI command **utils system restart**.

Note If you do not reboot the subscriber, all the services on the publisher may not start properly.

Step 7 From the publisher node, run CLI command **utils dbreplication reset all** to resetup Unified CM database replication across the entire cluster.

Step 8 From the publisher node, run CLI command **utils uccx dbreplication reset** to setup Unified CCX database replication across the cluster.

Step 9 On changing the hostname, License MAC changes. Rehost the new license for the new license MAC. Old license enters its grace period.

Step 10 Verify the status of Customer Collaboration Platform:

Step 11 Regenerate the SAML certificate through the **Cisco Identity Service Administration**.

If Single Sign-On must be enabled, then perform the following steps:

a. Establish the trust between the Cisco Identity Service and Identity Provider.

b. Log in to the Cisco Unified CCX Administration and navigate to **System** -> **Single Sign-On**.

c. Click **Register** to onboard the SSO components even if you had onboarded the components earlier.

d. You can now enable Single Sign-On after you perform **SSO Test** again.

Change HostName for Subscriber Server in HA Deployment

Use this procedure to change the hostname of a subscriber server in a HA deployment.

Note Ensure Single Sign-On is disabled before performing the change in hostname.

Procedure

Step 1 Change the DNS record of the subscriber server to point to the new hostname. Ensure that you correctly update both the forward (A) and reverse (PTR) records, and there are no duplicate PTR records.

Step 2 Verify that the DNS change propagates to other nodes by using the **utils network host** <*IP Address*> CLI command on all the cluster nodes.

Step 3 To update new hostname of the subscriber in publisher, enter the following CLI command on the publisher server:

utils uccx modify remote_hostname <Old_hostname_of_Subscriber> <New_hostname_of_Subscriber>

The following output displays:

```
admin:utils uccx modify remote_hostname abcd-efg-h1  ijkl-mno-p2

 Old Remote hostname: abcd-efg-h1
 New Remote hostname: ijkl-mno-p2

This command should be executed only in case you are changing Hostname
of remote server.
```

```
Are you sure you want to run this command?
Continue (y/n)?
```

Enter **y** and press **Enter**.

Step 4 To change the hostname of the subscriber server, perform either of the following methods:

- CLI commands
- Cisco Unified OS Administration interface

Using CLI commands:

a) Run the following CLI command on the subscriber server:

```
set network hostname
```

The following output displays:

```
admin:set network hostname

WARNING: Changing this setting will invalidate software license
         on this server. The license will have to be re-hosted.
Continue (y/n):
Continue (y/n)?y
***   W A R N I N G   ***
This command will cause the system to restart
======================================================
 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.
       To recognize the new ip address all nodes within
       the cluster will have to be manually rebooted.
======================================================
Continue (y/n)?y
```

Enter **y** and press **Enter**. The system services will automatically restart.

Using Cisco Unified OS Administration interface:

Change the hostname using Cisco Unified OS Administration interface of the subscriber server:

a) Choose **Settings** > **IP** > **Ethernet**.
b) Change the hostname.
c) Click **Save**. The system services will automatically restart.

Step 5 Restart all the servers in the cluster using the CLI command **utils system restart** .

Note If you do not reboot the subscriber, all the services on the publisher may not start properly.

Step 6 From the publisher node, run CLI command **utils dbreplication reset all** to resetup Unified CM database replication across the entire cluster.

Step 7 From the publisher node, run CLI command **utils uccx dbreplication reset** to setup Unified CCX database replication across the cluster.

Step 8 Verify the status of CCP.

a) Choose **Subsystems** > **Chat and Email** > **CCP Configuration**.
b) Click **Save** and verify that the **CCP Status** displays green for all the components.

Step 9 If Single Sign-On must be enabled, then reestablish the trust between the Cisco Identity Service and Identity Provider in the Publisher node.

Step 10 Log in to the Cisco Unified CCX Administration and navigate to **System** -> **Single Sign-On**.

Step 11 Click **Register** to onboard the SSO components even if you had onboarded the components earlier.

Step 12 You can now enable Single Sign-On after you perform **SSO Test** again.

Verify Proper Function of System after IP Address/hostname Change

After you change the IP addresses/hostnames of your cluster, complete the following tasks:

Procedure

Step 1 Ensure that all the servers in the cluster are up and available.

Step 2 Check the DB replication status as described in Step 3 of Prepare System for IP Address/hostname Change, on page 4 to ensure all the servers are replicating database changes successfully.

Step 3 Run a manual DRS Backup and ensure that all nodes and active services are successfully backed up.

Step 4 Run the CLI command `utils diagnose module validate_network` through platform CLI on all nodes in the cluster to ensure network connectivity and DNS server configuration are intact.

Step 5 If you have changed the IP address to move the Unified CCX server to a different network, then any firewall configuration on the other network must be changed to permit or deny traffic from the new IP address.

Step 6 If you have created any DSN using old IP address, change the DSN to point to the new IP. For example, the DSN created for Wallboard.

Step 7 Update the new IP address in the following web pages as well:

- **Work Flow Configuration** > **User Interface** > **Browser Setup** - URL and Home Page
- **Work Flow Configuration** > **HTTP Action** - Host
- **Work Flow Configuration** > **IPC Action** - IP Address
- Update the Recording configuration and the Cisco Customer Collaboration Platform configuration in the Unified CCX Administration page on the Publisher server.

Step 8 For Cisco Identity Service, Cisco Finesse and Unified Intelligence Centers users, delete the certificates entries for the old hostname/IP Address from the web browser before you log in to Cisco Identity Service, Cisco Finesse Agent Desktop or Unified Intelligence Center.

Step 9 Reregister the SSO components if the components were registered earlier.

Step 10 Perform the **SSO Test** to check if all the SSO components like CCX, CUIC and Finesse are registered and the test is successful for each component.

Domain Name Modification

This section describes how to change the domain name on single node and HA deployment.

Change the UCCX Domain Name

You can change the Unified CCX domain name based on the requirement. After changing the domain name, you must restart the server (in case of HA setup both publisher and subscriber nodes must be restarted). This regenerates all Unified CCX certificates including any third-party signed certificates. Unified CCX domain name change will not affect your existing license MAC unless the DNS server details are changed.

Before you begin

Before you change the Unified CCX domain name, ensure that you complete the following prerequisites:

- Change the Unified CCX fully qualified domain name (FQDN) in DNS server to reflect the new domain name.
- Ensure that both the forward and reverse lookups on the DNS server returns the fully qualified domain name (FQDN).
- Ensure that all the services are running. Run the following command in the Unified CCX OS platform CLI to verify that all the services are running:

  utils service list

Note If verification fails then identify the cause, resolve the issues to ensure that all the services are running.

- If you are using a HA setup, run the following command to check the database replication status:

  utils dbreplication runtimestate

Note Check if the database replication status is in sync on both the nodes.

Procedure

Step 1 Log in to Cisco Unified Communications OS Platform CLI using administrator username and password.

Step 2 Run the following command on the Unified CCX to set the new domain name:

set network domain <domain-name>

Step 3 Restart the node. Run the following command to restart the node:

utils system restart

Note If you are using a HA setup, first change the domain name of the publisher node, restart the publisher node and verify that all the services are running. Then change the domain name of the subscriber node, restart the subscriber node, and verify that all the services are running.

What to do next

After changing the Unified CCX domain name, perform the following:

- After restarting the node, run the following command to verify that all the services are running:

  utils service list

- Once the services are running, check if the new domain name is updated. Run the following command to check the domain name:

  show network eth0 detail

- If you are using a HA setup, run the following command to check the database replication status:

  utils dbreplication runtimestate

Note Check if the database replication status is in sync on both the nodes.

- Run the following command to check if all the system tests are passing:

  utils diagnose test

- Check the license MAC to find out the difference if the DNS server details and the domain name are changed. Run the following command to check the license MAC:

  show status

- Regenerate the SAML certificate through the **Cisco Identity Service Administration**.

If Single Sign-On must be enabled, then perform the following steps:

1. Establish the trust between the Cisco Identity Service and Identity Provider.
2. Log in to the Cisco Unified CCX Administration and navigate to **System** -> **Single Sign-On**.
3. Click **Register** to onboard the SSO components even if you had onboarded the components earlier.
4. You can now enable Single Sign-On after you perform **SSO Test** again.

Related Topics

Single Sign-On (SSO)

Set Up Certificates

Client Requirements

For more information on client requirements, see *Compatibility Information* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-device-support-tables-list.html.

Note Finesse Desktop client machines should be time synchronized with a reliable NTP server for the correct updates to the Duration fields within Live data reports.

Deploy Root Certificate for Internet Explorer

In environments where group policies are enforced via the Active Directory domain, the root certificate can be added automatically to each user's Internet Explorer. Adding the certificate automatically simplifies user requirements for configuration.

Note To avoid certificate warnings, each user must use the fully-qualified domain name (FQDN) of the Unified CCX server.

Set Up CA Certificate for Internet Explorer and Edge Browsers

After obtaining and uploading the CA certificates, the certificate must be automatically installed via group policy or all the users must accept the certificate.

In environments where users do not log in directly to a domain or where group policies are not utilized, every Internet Explorer user in the system must perform the following steps one time to accept the certificate:

Procedure

Step 1 In Windows Explorer, double-click the *ca_name*.cer file and then click **Open**.

Note Here the *ca_name* is the name of your certificate.

Step 2 In the **Certificate Import Wizard**, select **Current User**.

Step 3 Click **Install Certificate** > **Next** > **Place all certificates in the following store**.

Step 4 Click **Browse** and choose **Trusted Root Certification Authorities**.

Step 5 Click **OK** > **Next** > **Finish**.

Step 6 Click **Yes** on the install a certificate from a CA prompt.

Step 7 To verify that the certificate was installed, from the browser menu on IE, choose **Tools** > **Internet Options**.

Step 8 In the **Content** tab, click **Certificates**.

Step 9 In the **Trusted Root Certification Authorities** tab, ensure that the new certificate appears in the list.

Step 10 Restart the browser for the certificate installation to take effect.

Note If you are using Internet Explorer 11, you may receive a prompt to accept the certificate even if it is signed by a private CA.

Set Up CA Certificate for Firefox Browser

Every Firefox user in the system must perform the following steps once to accept the certificate:

Note To avoid certificate warnings, each user must use the FQDN of the Unified CCX server to access the desktop.

Procedure

Step 1 From the Firefox browser menu, choose **Options**.
Step 2 Go to **Privacy and Security** tab.
Step 3 Under Certificates section, click **View Certificates**.
Step 4 Select **Authorities**.
Step 5 Click **Import** and browse to the *ca_name*.cer file.

Note Here the *ca_name* is the name of your certificate.

Step 6 Check the **Validate Identical Certificates** check box.
Step 7 Restart the browser for the certificate to install.

Set Up CA Certificate for Chrome Browser

Procedure

Step 1 In the browser, go to **Settings**.
Step 2 In the Chrome browser, select **Advanced Settings** > **Privacy and Security**, click **Manage Certificates**.
Step 3 Click **Trusted Root Certification Authorities** tab.
Step 4 Click **Import** and browse to the *ca_name*.cer file.
In the **Trusted Root Certification Authorities** tab, ensure that the new certificate appears in the list.
Step 5 Restart the browser for the certificate to install.

Exit Unified CCX Administration

To exit Unified CCXAdministration without closing your web browser, you can do either of the following:

Note You can also exit Unified CCXAdministration by closing your web browser.

Procedure

Step 1 Click the **Logout** link displayed in the top right corner of any Cisco Unified CCX Administration web page
Step 2 Choose **System** > **Logout** from the Unified CCXAdministration menu bar.

The system logs you out of Unified CCX and displays the Unified CCX Authentication web page.