Manage IP Address and Hostname

IP Address or Hostname or Domain Name Change

Note Before you change the IP address or hostname or domain name, update the DNS server with a new host entry.

You can change the IP address or hostname or domain name of the Cisco Finesse cluster nodes in your deployment. These changes can be done for a variety of reasons such as:

- to resolve a duplicate IP address or hostname.
- to move the server from one segment to another.

Note Hostname supports 24 alphanumeric characters.

Change IP Address or Hostname Task List

The following table lists the tasks to perform before you change the IP address or hostname for Cisco Finesse cluster nodes.

Procedure

	Command or Action	Purpose
Step 1	System health checks before the IP address or hostname change	Perform system health checks before the IP address or hostname change.

	Command or Action	Purpose
Step 2	Change IP Address or Hostname using Unified Operating System GUI or Change IP Address or Hostname Using CLI.	Change IP address or hostname for the Cisco Finesse cluster node using either the Unified OS GUI or Command Line Interface (CLI).
Step 3	Post-Change Tasks and Verification.	Verify system health checks after the IP address or hostname change.

Pre-Change Tasks

Perform the following system health checks for the Cisco Finesse cluster nodes before you change the IP address or hostname or domain name.

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

Procedure

Step 1 Check the active ServerDown alerts to ensure that all servers are active and available on the Cisco Finesse cluster nodes.

- Check by using RTMT—Select **Alert Central** from the tree hierarchy or choose **System** > **Tools** > **Alert** > **Alert Central** and verify the alerts.
- Check by using CLI—Enter **file search activelog syslog/CiscoSyslog ServerDown** command and verify the application event log.

  Sample Output:

```
admin:file search activelog syslog/CiscoSyslog ServerDown
Searching path: /var/log/active/syslog/CiscoSyslog
Searching file: /var/log/active/syslog/CiscoSyslog
Search completed
```

Step 2 Check the DB replication status on all the Cisco Finesse cluster nodes to ensure that all servers are replicating database changes successfully.

- Check by using RTMT—Choose **CallManager** > **Service** > **Database Summary** and verify the replication status.
- Check by using CLI—Enter **show perf query class "Number of Replicates Created and State of Replication"** command and verify the application event log.

  Sample Output:

```
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
```

Note All nodes must show the Replicate_State as 2. The value 2 refers that the replication state is good.

Step 3 Check network connectivity and DNS server configuration by running the **utils diagnose module validate_network** command on all Cisco Finesse cluster nodes.

Sample Output:

```
admin:utils diagnose module validate_network
Log file: platform/log/diag1.log
Starting diagnostic test(s)
===========================
test - validate_network    : Passed
Diagnostics Completed
The final output will be in Log file: platform/log/diag1.log
Please use 'file view activelog platform/log/diag1.log' command to see the output
```

Step 4 Run a manual Disaster Recovery System (DRS) backup to ensure that all Cisco Finesse cluster nodes and active services are backed up successfully. For more information, see *Disaster Recovery* chapter in the *Administration Guide for Cisco Unified Communications Manager* at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

Disaster Recovery

Important If you have DRS backup, then you can restore your system from the backup files in case of any failure.

Note The DRS backup files are invalid after successful change of hostname, IP address, or domain name.

Change IP Address or Hostname using Unified Operating System GUI

You can use Cisco Unified Operating System Administration to change the IP address or hostname of the Cisco Finesse cluster nodes in your deployment.

Before you begin

- Perform the system health checks on your deployment. For more information, see
- Ensure that Single Sign-On is disabled.

Procedure

Step 1 In Cisco Unified OS Administration, choose **Settings** > **IP** > **Ethernet**.

Step 2 Change the **Hostname** and **IP Address**. If required, change 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 automatic self-signed certificate regeneration.

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

Step 4 Restart the Cisco Finesse cluster nodes using CLI **utils system restart**.

a) Enter **y** and press **Enter** to restart the system.

Sample Output:

```
admin:utils system restart
     ***   W A R N I N G   ***
Please make sure database replication setup is complete. Use the command 'utils dbreplication
 runtimestate' to get the current status.
If database replication setup is in progress, restarting the server may leave database
replication unable to complete.
Do you really want to restart ?
Enter (yes/no)? yes
Appliance is being Restarted ...
Warning: Restart could take up to 5 minutes.
Stopping Service Manager...
-  Service Manager shutting down services... Please Wait
```

What to do next

Post-Change Tasks and Verification, on page 9.

Change IP Address or Hostname Using CLI

You can use the CLI to change the IP address or hostname of the Cisco Finesse cluster nodes in your deployment.

Note If the certificates are invalid or have expired, you must renew the certificates before using the CLI set network hostname.

Before you begin

- Perform the system checks on your deployment. For more information, see
- Ensure that Single Sign-On is disabled.

Procedure

Step 1 Sign in to the CLI of the Cisco Finesse cluster node that you want to change.

Step 2 Enter **set network hostname**.

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

a) Enter the new hostname and press **Enter**.
b) Enter **yes**, if you also want to change the IP address. Otherwise, press **Enter** and move 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.

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

Sample Output:

```
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 CUCM Certificates including any third party
       signed Certificates that have been uploaded.
Enter the hostname:: samplehostname
Would you like to change the network ip address at this time [yes]:: 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:: 10.10.10.9
Enter the ip subnet mask:: 255.255.255.224
Enter the ip address of the gateway:: 10.10.10.1
Hostname:       samplehostname
IP Address:     10.10.10.9
IP Subnet Mask: 255.255.255.224
Gateway:        10.10.10.1

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

calling 1 of 6 component notification script: ahostname_callback.sh
Info(0): Processnode query returned using finesse25:
name
=========
finesse25
updating server table from:'finesse25', to: 'samplehostname'
Rows: 1
updating database, please wait 90 seconds
updating database, please wait 60 seconds
updating database, please wait 30 seconds
calling 2 of 6 component notification script: clm_notify_hostname.sh
calling 3 of 6 component notification script: drf_notify_hostname_change.py
calling 4 of 6 component notification script: idsLocalPrefsUpdateFile.sh
Going to trigger /usr/bin/python /usr/local/cm/lib/dblupdatefiles-plugin.py
-f=samplehostname,finesse25
calling 5 of 6 component notification script: regenerate_all_certs.sh
calling 6 of 6 component notification script: update_idsenv.sh
calling 1 of 3 component notification script: afupdateip.sh
calling 2 of 3 component notification script: ahostname_callback.sh
Info(0): Processnode query returned using 192.168.1.25:
name
====
calling 3 of 3 component notification script: clm_notify_hostname.sh
```

Step 5 Restart the Cisco Finesse cluster node using CLI **utils system restart**.

a) Enter **y** and press **Enter** to restart the system.

Sample Output:

```
admin:utils system restart
     ***   W A R N I N G   ***
Please make sure database replication setup is complete. Use the command 'utils dbreplication
 runtimestate' to get the current status.
If database replication setup is in progress, restarting the server may leave database
replication unable to complete.
Do you really want to restart ?
Enter (yes/no)? yes
Appliance is being Restarted ...
Warning: Restart could take up to 5 minutes.
Stopping Service Manager...
-  Service Manager shutting down services... Please Wait
```

What to do next

Post-Change Tasks and Verification, on page 9.

Change IP Address Only

You can use the CLI to change the IP address of the Cisco Finesse cluster nodes in your deployment.

Before you begin

- Perform the system health checks on your deployment. For more information, see
- Ensure that Single Sign-On is disabled.

Procedure

Step 1 Sign in to the CLI of the Cisco Finesse cluster node that you want to change.

Step 2 Enter **set network ip eth0** *addr mask gw*.

Table 1: Syntax Description

Parameters	Description
eth0	Specifies Ethernet interface 0.
addr	Specifies the server IP address that you want to assign.
mask	Specifies the server network mask that you want to assign.
gw	Specifies the default gateway of the server that you want to assign.

a) Enter **y** and press **Enter** to start the process.

Sample Output:

```
admin:set network ip eth0 10.53.57.101 255.255.255.224 10.53.56.1
          ***   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)?
```

Step 3 Restart the Cisco Finesse cluster nodes using CLI **utils system restart**.

a) Enter **y** and press **Enter** to restart the system.

Sample Output:

```
admin:utils system restart
     ***   W A R N I N G   ***
Please make sure database replication setup is complete. Use the command 'utils dbreplication
 runtimestate' to get the current status.
If database replication setup is in progress, restarting the server may leave database
replication unable to complete.
Do you really want to restart ?
Enter (yes/no)? yes
Appliance is being Restarted ...
Warning: Restart could take up to 5 minutes.
Stopping Service Manager...
-  Service Manager shutting down services... Please Wait
```

What to do next

Post-Change Tasks and Verification, on page 9.

Change Domain Name

You can use the CLI to change the domain name of the Cisco Finesse cluster nodes in your deployment.

Before you begin

- Perform the system health checks on your deployment. For more information, see
- Ensure that Single Sign-On is disabled.

Procedure

Step 1 Sign in to the CLI of the Cisco Finesse cluster node that you want to change.

Step 2 Enter **set network domain** *name*.

Table 2: Syntax Description

Parameters	Description
name	Specifies the system domain name that you want to assign..

a) Enter **y** and press **Enter** to start the process.

Sample Output:

```
admin:set network domain sampledomainname
          ***   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 servers have 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 host certificates.

Continue (y/n)? y
```

Step 3 Restart the Cisco Finesse cluster nodes using CLI **utils system restart**.

a) Enter **y** and press **Enter** to restart the system.

Sample Output:

```
admin:utils system restart
     ***   W A R N I N G   ***
Please make sure database replication setup is complete. Use the command 'utils dbreplication
 runtimestate' to get the current status.
If database replication setup is in progress, restarting the server may leave database
replication unable to complete.
Do you really want to restart ?
Enter (yes/no)? yes
Appliance is being Restarted ...
Warning: Restart could take up to 5 minutes.
Stopping Service Manager...
-  Service Manager shutting down services... Please Wait
```

What to do next

- Enter **utils service list** to verify list of all services and their states.
- Enter **show network eth0** *detail* to verify the new domain name.
- Post-Change Tasks and Verification, on page 9.

Post-Change Tasks and Verification

Verify if the IP address, hostname, or domain name changes that were made to your deployment are implemented successfully.

Note If you do not receive the results that you expect when you perform these tasks, do not continue with this procedure. Resolve any problems that you find, and then continue.

Procedure

Step 1 Check the active ServerDown alerts to ensure that all servers in the Cisco Finesse cluster nodes are active and available.

Step 2 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.

Step 3 Restart the Cisco Finesse cluster nodes using CLI `utils system restart`.Make sure that the cluster output displays the correct publisher before proceeding.

Step 4 Check the db replication status on all the Cisco Finesse cluster nodes to ensure that all servers are replicating database changes successfully.

Step 5 Check network connectivity and DNS server configuration by running the **utils diagnose module validate_network** command on all the Cisco Finesse cluster nodes.

Step 6 Start a manual DRS backup to ensure that all the Cisco Finesse cluster nodes and active services are backed up successfully.

Step 7 Enable SSO and perform the following tasks.

a) Regenerate the SAML certificate.
b) Reestablish trust relationship between Identity Provider (IdP) and Cisco Identity Service (IdS).
c) If the components are registered earlier, then

- Reregister all the SSO components.
- Perform the SSO Test to check if all the SSO components are registered. Verify that the test is successful for each component.

For more information, see the *Single Sign-On* chapter in *Cisco Unified Contact Center Enterprise Features Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-feature-guides-list.html.

Step 8 Regenerate and upload the following certificates that contain new hostname or domain name.

- CA-signed certificate to Cisco Finesse.
- Cisco Finesse tomcat certificate to aCTI server and third-party server (if necessary).
- Cisco Finesse tomcat-trust certificate to Cisco Unified Intelligence Center and Live Data.
- Cisco Finesse tomcat certificate to Customer Collaboration Platform as tomcat-trust.

Step 9 Update Cross-Origin Resource Sharing (CORS) requests for Cisco Finesse, Cisco Unified intelligence center, and Live Data.

Step 10 Enable Shindig allowed list to add Cisco Finesse new FQDN for Cisco Finesse, Unified Intelligence Center, and Live Data.

Step 11 Verify and update Finesse desktop layout with new FQDN for the resource loading.

Step 12 Update Unified CCE inventory with the Cisco Finesse IP address.

From Step 6 to Step 10, after you complete each step, you must restart the services to reflect new changes.