Cisco Finesse Installation and Upgrade Guide, Release 12.6(1)

First Published: 2021-05-14

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

CONTENTS

Preface

Change History

This table lists the changes that are made to this guide. Most recent changes appear at the top.

Change	See	Date
Added information related to 12.5(1) SU	Upgrade>Supported Upgrade Paths	July 2022
Initial Release of Document for Release 12.6(1)		May 2021
Added client OS details and updated supported browsers	Client Requirements	
Added Edge Chromium details	Browser Settings for Agent and Supervisor Desktop	

About This Guide

The *Cisco Finesse Installation and Upgrade Guide* describes how to install Finesse, upgrade Finesse, and perform initial configuration.

Audience

This guide is prepared for system engineers and administrators who are responsible for the installation and initial configuration of Cisco Finesse.

Related Documents

Document or resource	Link
Cisco Finesse Documentation Guide	https://www.cisco.com/en/US/partner/products/ps11324/products_documentation_roadmaps_list.html
Configure SNMP Trap in Cisco Finesse	https://www.cisco.com/c/en/us/support/docs/contact-center/finesse/214387-configure-snmp-trap-in-cisco-finesse.html
Cisco.com site for Finesse documentation	https://www.cisco.com/en/US/partner/products/ps11324/tsd_products_support_series_home.html

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.

Field Notice

Cisco publishes Field Notices to notify customers and partners about significant issues in Cisco products that typically require an upgrade, workaround, or other user action. For more information, see *Product Field Notice Summary* at https://www.cisco.com/c/en/us/support/web/tsd-products-field-notice-summary.html.

You can create custom subscriptions for Cisco products, series, or software to receive email alerts or consume RSS feeds when new announcements are released for the following notices:

- Cisco Security Advisories
- Field Notices
- End-of-Sale or Support Announcements
- Software Updates
- Updates to Known Bugs

For more information on creating custom subscriptions, see *My Notifications* at https://cway.cisco.com/mynotifications.

Documentation Feedback

To provide comments about this document, send an email message to the following address: contactcenterproducts_docfeedback@cisco.com

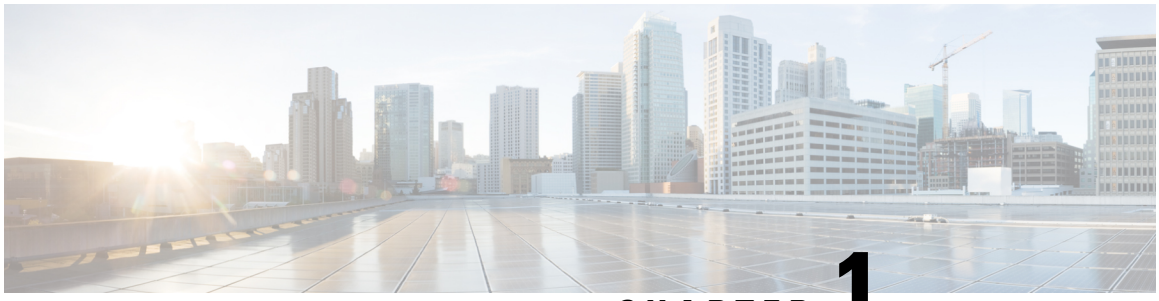
We appreciate your comments.

Conventions

This document uses the following conventions:

Convention	Description
boldface font	Boldface font is used to indicate commands, such as user entries, keys, buttons, folder names, and submenu names. For example: • Choose **Edit** > **Find**. • Click **Finish**.
italic font	Italic font is used to indicate the following: • To introduce a new term. Example: A *skill group* is a collection of agents who share similar skills. • A syntax value that the user must replace. Example: IF (*condition*, *true-value*, *false-value*) • A book title. Example: See the *Cisco Unified Contact Center Enterprise Installation and Upgrade Guide*.
`window font`	Window font, such as Courier, is used for the following: • Text as it appears in code or that the window displays. Example: `<html><title>Cisco Systems, Inc. </title></html>`

Convention	Description
< >	Angle brackets are used to indicate the following: • For arguments where the context does not allow italic, such as ASCII output. • A character string that the user enters but that does not appear on the window such as a password.



CHAPTER 1

Installation Preparation

System Requirements

This section provides a summary of the requirements for Cisco Finesse.

Platform Requirements

All Cisco Finesse servers run on virtual machines (VM) using the Unified Communications Operating System (Unified OS). The supported versions must be installed before you install Cisco Finesse.

For more information about supported VMs and VMware requirements, refer to Virtualization for Cisco Finesse.

Client Requirements

No Cisco Finesse software is installed on the clients. Agents and Supervisors use a web browser to access the Finesse desktop. Administrators use a web browser to access the Finesse administration console. The following table lists the supported operating systems and browsers for Cisco Finesse clients.

Note When a new VM is deployed using Cisco provided OVA using thin-client vCenter 6.5, the **Check and upgrade Tools during power cycling** setting is not enabled.

Manually enable this setting to ensure that the performance levels are not affected.

Cisco Finesse does not support the use of Compatibility View with Internet Explorer. If the user is on Compatibility View the following banner message is displayed on the Finesse Desktop login screen:

The Cisco Finesse Desktop is not supported in compatibility mode. Contact your administrator to change the browser settings to non-compatibility mode and sign in again.

If the user tries to change the compatibility mode after logging in to the Finesse Desktop, an error page is displayed and the user must sign in to the Finesse Desktop again.

Table 1: Client Operating System

Components	Clients OS
Cisco Finesse	Microsoft Windows 10 and Windows 11
	Mac OS X 10.15.x or later
	Chrome OS 88.0.4324 or later

Table 2: Supported Browsers

Operating System	Browser Version
Microsoft Windows 10	• Google Chrome 88.0.4324 or later. • Edge Chromium (Microsoft Edge v79 and later). • Firefox Extended Supported Release (ESR) 68.4 and later ESRs.
Microsoft Windows Server 2016 (Standard and Datacenter editions)	• Google Chrome 88.0.4324 or later. • Edge Chromium (Microsoft Edge v79 and later). • Firefox ESR 68.4 and later ESRs.
Mac OS X	• Firefox ESR 68.4 and later ESRs. • Google Chrome v88.0.4324 and later. • Edge Chromium (Microsoft Edge v79 and later)
Chromebook with Chrome OS v70	• Chromium v73 and later. • Google Chrome v60 and later.

For more information, see *Contact Center Enterprise Solution Compatibility Matrix* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-device-support-tables-list.html.

For more information, see *Unified CCX Software Compatibility Matrix* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-device-support-tables-list.html.

Important Requirements, such as processor speed and RAM, for clients that access the Cisco Finesse desktop can vary. Desktops that receive events for more than one agent (such as a supervisor desktop running Team Performance and Queue Statistics gadgets or an agent desktop running Live Data reports that contain information about other agents or skill groups) require more processing power than desktops that receive events for a single agent.

Factors that determine how much power is required for the client include, but are not limited to, the following:

- Contact center traffic.
- Additional integrated gadgets in the desktop (such as Live Data reports or third-party gadgets).
- Other applications that run on the client and share resources with the Cisco Finesse desktop.

Network Requirements

For optimal Finesse performance, network characteristics should not exceed the following threshold:

- Latency: 80 ms (round-trip) between Finesse servers and 400 ms (round-trip) from Finesse client to Finesse server

For information about port usage, refer to the *Port Utilization Guide for Cisco Unified Contact Center Solutions* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-and-configuration-guides-list.html.

For information about bandwidth requirements for Cisco Finesse, refer to the Cisco Finesse Bandwidth Calculator.

System Account Privileges

During the installation of Cisco Finesse, you must specify credentials for the following:

- **Administrator User account:** This account is used to access the CLI.
- **Application User account:** This account is used to access the Finesse administration console.
- **Database access security password:** This password is required if you replace or add a server in the future or if you want to replace the security password with a new one. Keep a record of this password.

The database security password and the passwords for the Administrator and Application User accounts must be at least six characters long. They can contain alphanumeric characters, hyphens, and underscores.

Security Considerations

Administrators can configure allowed origins for Cross-Origin Resource Sharing (CORS) requests and the allowed sources for gadget URI's through CLI.

HTTPS Support

Cisco Finesse does not support plain HTTP but supports only secure HTTP (HTTPS). In response to clients accessing Finesse using plain HTTP, the 301 HTTP redirect is issued to the secured port 8445.

Note Cisco Finesse supports HTTP/2 protocol by default.

To access the administration console using HTTPS, enter the following URL in your browser:

`https://FQDN:8445/cfadmin`

Where FQDN is the name of your primary Finesse server and 8445 is the port number.

Similarly, agents and supervisors can access their desktops using HTTPS as follows:

`https://FQDN:8445/desktop`

To eliminate browser security warnings each time you access the administration console or agent desktop through HTTPS, you can obtain and upload a CA certificate or you can use the self-signed certificate that is provided with Finesse.

If you add custom gadgets that perform HTTPS requests to Finesse, you must add a certificate to the Finesse server for that gadget.

Security Enhancements

The security enhancements in Cisco Finesse are as follows:

- By default, Cisco Finesse Notification Service unsecure XMPP port 5222 and BOSH/WebSocket (HTTP) port 7071 are disabled.

  Use the CLI command **utils finesse set_property webservices enableInsecureOpenfirePort true** to enable these ports.

- Validation of the X.509 certificate is enforced. It is mandatory to have the following valid non-expired X.509 CA or self-signed certificates, which must be imported into the Cisco Finesse trust store.
  - Cisco Finesse node certificates are available by default. The administrator must verify the validity of the certificates, as non-expired certificates are invalid.
    - Valid non-expired Cisco Finesse primary certificate must be present on the secondary Cisco Finesse.
    - Valid non-expired Cisco Finesse secondary certificate must be present on the primary Cisco Finesse.
  - Import the CUCM certificate to both the primary and secondary Finesse nodes.
  - Import the IdS certificate to both the primary and secondary Finesse nodes.
  - Import the Customer Collaboration Platform server certificates to both the primary and secondary Finesse nodes in the Unified CCE.
  - Import the LiveData server certificates to both the primary and secondary Finesse nodes in the Unified CCE.

- Import the Cloud Connect server certificates to both the primary and secondary Finesse nodes in the Unified CCE.

You can override the trust certificate enforcement by using the CLI command **utils finesse set_property webservices trustAllCertificates true**.

For more information on CLI commands, see *Cisco Finesse Administration Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-maintenance-guides-list.html.

For more information about ports, see *Port Utilization Guide for Cisco Unified Contact Center Solutions* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-and-configuration-guides-list.html.

Installation Spanning Multiple Domains

You can install the Finesse nodes on separate domains as long as the following requirements are met:

- Each Finesse server can perform a DNS lookup of the other using the fully-qualified domain name (FQDN).
- All Finesse clients can perform DNS lookups of the Finesse servers using the FQDN.

Failover Considerations

For faster failover, use optimal browser and gadget configurations.

For more information on deployment practices and guidelines to ensure optimal failover performance, see *Guidelines for Optimal Desktop Failover* and *Failover Planning* sections in *Cisco Finesse Administration Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-maintenance-guides-list.html.

For more information on ensuring how the custom gadgets improve failover performance, see *Best Practices for Gadget Development* section in *Cisco Finesse Web Services Developer Guide* at https://developer.cisco.com/docs/finesse/#!rest-api-dev-guide.

For more information on bandwidth measurements, see *Finesse Bandwidth Calculator for Unified Contact Center Enterprise* and *Cisco Unified Contact Center Express Bandwidth Calculator* at https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-technical-reference-list.html.

Other Requirements and Considerations

- To use the Desktop Chat feature, Cisco Unified Communications Manager version 12.5 or higher is required.
- You must have access to a Network Time Protocol (NTP) server.

Note The default desktop notification connection type is WebSocket.

- You must have a valid hostname and domain.

- It is recommended that you choose the Cisco Finesse hostname, domain and IP address carefully because changing these configurations after installation requires other steps to be followed, such as: manual verification of certificate validity, cluster restart, invalidation of the existing backups, and running commands through the Command Line Interface (CLI).

Note For more information on the steps to be followed to change the Cisco Finesse hostname, domain or IP address, see the *Manage IP Address and Hostname* chapter in the *Cisco Finesse Administration Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-maintenance-guides-list.html.

Changing the Cisco Finesse hostname, domain or IP address after installation is supported.

- You must have a preconfigured default router.
- You must have a preconfigured Domain Name Server (DNS) and have set up forward and reverse DNS.
- Cisco Finesse is supported on a Call Manager Peripheral Gateway (PG) and a Generic PG. Finesse does not support a System PG. On a System PG, assuming that a Voice Response Unit (VRU) is also set up for queuing, Finesse would receive queuing events meant for the VRU.
- The Cisco Finesse server uses Windows authentication to access the Administration & Data server database (AWDB). You can set the MS SQL server authentication mode to either Windows Authentication or Mixed.
- Cisco Finesse requires a domain user that is configured with login and read permissions to access the AWDB.
- The Cisco Finesse JDBC driver is configured to use NTLMv2. Therefore, Finesse can connect to the AWDB even if the AWDB is configured to use only NTLMv2.
- The port for the primary and backup Administration & Data Servers must be the same.
- To ensure secure communication between Finesse and CTI Server, enable the secure mode in the PG. Also, in the Cisco Finesse Administration Console, enable the option in the CTI Server Settings.
- If you plan to use Cisco Unified Customer Voice Portal (Unified CVP) for queuing, configure Unified CVP to support warm transfer and conference, as described in the section Using the Warm Transfer feature with SIP Calls in the Configuration and Administration Guide for Cisco Unified Customer Voice Portal and the section Network Transfer in the Cisco Unified Customer Voice Portal Solutions Reference Network Design.
- In Cisco Unified Communications Manager Administration, under Device > Phone, ensure that the Maximum Number of Calls is set to no more than 2 and Busy Trigger is set to 1.

Preinstallation Tasks

Before you can install Cisco Finesse, complete the following preinstallation tasks:

- Record your network and password information on the configuration worksheet.

- Obtain the installation files.

Configuration Worksheet

Use this configuration worksheet to record network and password information that is required to install and configure Finesse. Store this worksheet information for future reference.

Note Many of the values that you enter on the installation configuration screens (such as hostnames, user IDs, and passwords) are case-sensitive.

Table 3: Configuration Worksheet

Configuration Data	Your Entry	Notes
Hostname	_____	The hostname cannot be "local host". The hostname must be the hostname of the server as registered in the DNS.
IP Address and Mask	_____	
Gateway (GW) Address	_____	
Primary DNS IP Address	_____	
Secondary DNS IP Address (optional)	_____	
Domain	_____	
Administrator User credentials	Administrator User ID: _____ Administrator User password: _____	This account is used to access the Finesse CLI.
Timezone	_____	
Certificate Information	Organization:_____ Unit:_____ Location:_____ State:_____ Country:_____	
NTP Server Host Name or IP Address	NTP Server 1: _____ NTP Server 2: _____	

Configuration Data	Your Entry	Notes
Database Access Security Password	_____	
Application User credentials	Application User ID: _____ Application User Password: _____	This account is used to sign in to the Finesse administration console.
A Side CTI Server Hostname/IP Address	_____	The hostname or IP address of the A Side CTI server.
A Side CTI Server Port	_____	The port of the A Side CTI server.
B Side CTI Server Hostname/IP Address	_____	The hostname or IP address of the B Side CTI server.
B Side CTI Server Port	_____	The port of the B Side CTI server.
Peripheral ID	_____	The ID of the CallManager Peripheral Gateway (PG).
Primary Administration & Data Server Hostname/IP Address	_____	The hostname or IP address of the primary Unified CCE Administration & Data server.
Backup Administration & Data Server Hostname/IP Address	_____	The hostname or IP address of the backup Unified CCE Administration & Data server.
Database Port	_____	The port of the Unified CCE Administration & Database server. The port must be the same for the primary and backup Administration & Data servers.
AW Database Name	_____	The name of the AW Database (AWDB). For example, *ucceinstance*_awdb.
Domain	_____	The domain of the AWDB.

Configuration Data	Your Entry	Notes
Username to access the AWDB	_____	This user refers to the Administrator Domain user that the AWDB uses to synchronize with the Logger. The AWDB server must use Windows authentication and the configured username must be a domain user.
Password to access the AWDB	_____	
Hostname/IP address of the secondary Finesse server	_____	

Installation Files

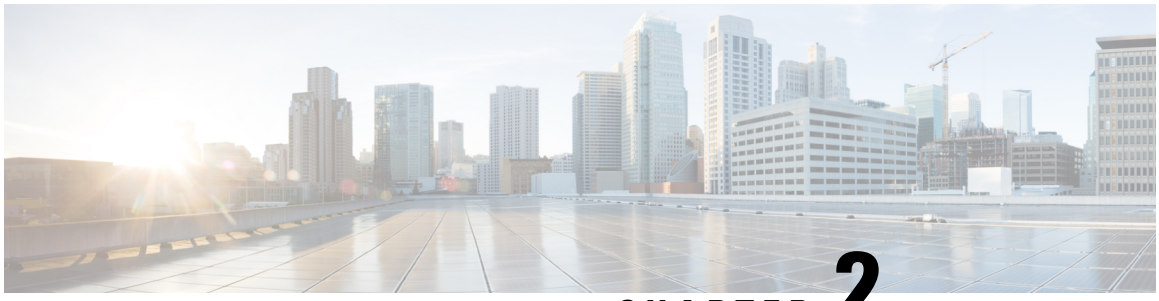
Before you install Cisco Finesse, you must obtain the OVA file. Cisco Finesse supports a single OVA template with two deployment configurations. Choose the configuration you need based on the size of your deployment. The file names for the OVA and associated Readme are as follows:

For Release 12.6.1:

- **OVA:** Finesse_12.6.1_VOS12.6.1_vmv13_v1.3.ova
- **Readme:** Finesse_12.6.1_VOS12.6.1_vmv13_v1.3.ova.README.txt

You must purchase the Cisco Finesse media kit to obtain the installer. For more information, see the *Ordering Guide for Cisco Customer Contact Solutions* (http://www.cisco.com/web/partners/downloads/partner/WWChannels/technology/ipc/downloads/CCBU_ordering_guide.pdf).

You can obtain the Cisco Virtual Server (OVA) files needed to create a virtual machine from Cisco.com at the following URL: http://software.cisco.com/download/type.html?mdfid=283613135&i=rml.



CHAPTER 2

Cisco Finesse Server Installation

Installation Task Flow

The following table provides an overview of the tasks you perform to install Cisco Finesse. Tasks must be performed in the order they are listed.

1	Install Finesse on the primary node.
2	Configure the database settings.
3	Configure the CTI server settings.
4	Configure the cluster settings for the secondary node.
5	Restart Cisco Finesse Tomcat on the primary node.
6	Install Finesse on the secondary node.
7	Ensure replication is functioning between the two nodes.
8	Install language packs (optional).

Install Finesse on Primary Node

Procedure

Step 1 Follow the instructions in the OVA README.txt file to import and deploy the OVA, to edit VM settings, and to power on the VM and edit the BIOS settings in the console. For more information, see the section on *Installation Files*.

Note Do not use Thin Provisioning or a VM snapshot when creating a VM to host Cisco Finesse. The use of Thin Provisioning or snapshots can negatively impact the performance of Cisco Finesse operation.

Messages appear while the preinstallation script runs. When the preinstallation script ends, the DVD Found screen opens.

Step 2 Select **OK** on the Disk Found screen to begin the verification of the media integrity and a brief hardware check.

If the media check passes, select **OK** to open the Product Deployment Selection screen. Continue to Step 3.

If the media check fails, the installation terminates.

Step 3 The Product Deployment Selection screen states that the Cisco Finesse product suite will be installed. This screen has only one choice: **OK**.

Select **OK** to open the Proceed with Install screen.

Step 4 The Proceed with Install screen shows the version of the product that is currently installed (if any) and the version of the product for this ISO. For the initial installation, the version currently installed shows NONE.

Select **Yes** on the Proceed with Install screen to open the Platform Installation Wizard screen.

Step 5 On the Platform Installation Wizard screen, select **Proceed** to open the Basic Install screen.

Step 6 Select **Continue** on the Basic Install screen to open the Basic Install wizard.

The Basic Install wizard presents a series of screens that present questions and options pertinent to the platform and the setup configuration. Help is available for each wizard screen.

The first Basic Install wizard screen is Timezone Configuration.

Step 7 On the Timezone Configuration screen:

a) Use the up and down arrows to locate the local time zone that most closely matches your server location. You can also type the initial character of the time zone to move to that item in the list. The Timezone field is based on country and city and is mandatory. Setting it incorrectly can affect system operation.
b) Select **OK** to open the Auto Negotiation Configuration screen.

Step 8 On the Auto Negotiation Configuration screen, select **Continue** to use automatic negotiation for the settings of the Ethernet network interface card (NIC).

The MTU Configuration screen appears.

Step 9 In the MTU Configuration screen, select **No** to keep the default setting for Maximum Transmission Units (1500).

Note Finesse supports the default setting of 1500 for MTU only. No other value is supported.

Your selection of No opens the Static Network Configuration screen.

Step 10 On the Static Network Configuration screen, enter static network configuration values as follows, referring to the Configuration Worksheet if necessary:

a) Enter the **Host Name**.
b) Enter the **IP Address**.
c) Enter the **IP Mask**.
d) Enter the **GW Address**.

e) Select **OK** to open the Domain Name System (DNS) Client Configuration screen.

Step 11 On the DNS Client Configuration screen, select **Yes** to specify the DNS client information.

Important DNS client configuration is *mandatory* for Cisco Finesse. Select Yes on this screen. If you select No, after the installation is complete, agents *cannot* sign in to the desktop and you have to reinstall Finesse.

Step 12 Specify your DNS client information as follows, referring to the Configuration Worksheet if necessary:

a) Enter the **Primary DNS** (mandatory).
b) Enter the **Secondary DNS** (optional).
c) Enter the **Domain** (mandatory).
d) Select **OK** to open the Administrator Login Configuration screen.

Step 13 On the Administrator Login Configuration screen:

a) Enter the credentials for the administrator.
b) Select **OK** to open the Certificate Information screen.

Step 14 On the Certificate Information screen:

a) Enter the following data to create your Certificate Signing Request: Organization, Unit, Location, State, and Country.
b) Select **OK** to open the First Node Configuration screen.

Step 15 On the First Node Configuration screen, select **Yes** to indicate that you are configuring the first node.

Your selection of Yes opens the Network Time Protocol Client Configuration screen.

Step 16 On the Network Time Protocol Client Configuration screen, enter the IP address, NTP server name, or NTP Server Pool name for at least one external NTP server.

Step 17 After you complete the NTP configuration, select **OK**. This action opens the Security Configuration screen.

Step 18 On the Security Configuration screen, enter the Database Access Security password, and then select **OK**.

Step 19 On the Application User Configuration screen, enter the credentials for the application user.

Select **OK** to open the Platform Configuration Confirmation screen. This screen states that the platform configuration is complete.

Step 20 On the Platform Configuration Confirmation screen, select **OK**.

The installation begins.

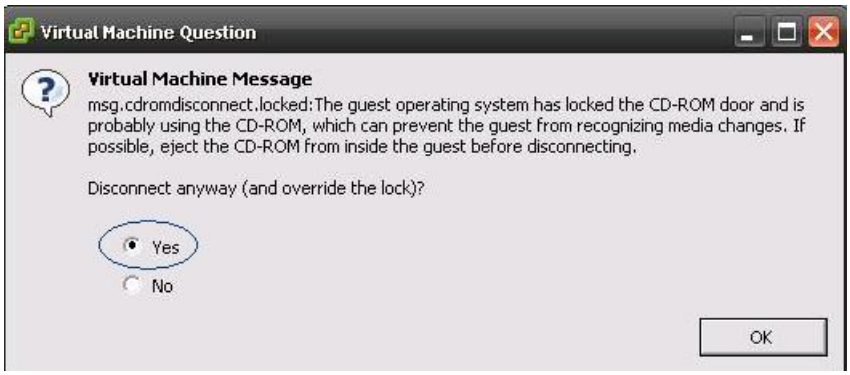
The installation can take up to an hour to complete and can run unattended for most of that time.

During the installation, the monitor shows a series of processes, as follows:

- Formatting progress bars
- Copying File progress bar
- Package Installation progress bars
- Post Install progress bar
- Populate RPM Archive progress bar
- Application Installation progress bars (multiple Component Install screens, security checks)
- An informational screen saying the system will reboot momentarily to continue the installation

If you see the following virtual machine question, select **Yes**, and then click **OK**:

Figure 1: Virtual Machine Message



- A system reboot

  Messages stream down your monitor during the reboot. Some of them prompt you to press a key. *Do not* respond to these prompts to press a key.

- Application Pre Install progress bars
- Configure and Setup Network progress bars

  Note If a Network Connectivity Failure screen appears during the Configure and Setup Network process, click **Review**, and then click **OK** at the Errors screen. Follow the prompts to reenter the information that caused the failure. The installation continues when the connection information is complete.

- Security configuration

A message appears that states the installation of Cisco Finesse has completed successfully.

```
The installation of Cisco Finesse has completed successfully.

Cisco Finesse <version number>
<hostname> login: _
```

What to do next

Sign in to the Finesse administration console on the primary Finesse server (https://*FQDN of Finesse server:8445*/cfadmin) to configure CTI server, Administration & Database server, and cluster settings.

After you configure these settings, install Finesse on the secondary node.

Install Finesse on Secondary Node

Install the same version of Finesse on both the primary and secondary Finesse nodes.

Note Configure a Datastore ISO file on the virtual CD/DVD drive of the target VM to install Finesse.

Note Finesse administration tasks can only be performed on the primary Finesse server. After you install the secondary server, sign in to the administration console on the primary server to perform administration tasks (such as configuring reason codes or call variable layout).

Before you begin

- Install Finesse on the primary server. See *Install Finesse on Primary Node*.
- Use the Finesse administration console on the primary Finesse server to configure CTI server, Administration & Database server, and cluster settings.
- Ensure that the DNS server has forward and reverse DNS set up for both the primary and secondary node.

Procedure

Step 1 Follow the instructions in the OVA README.txt file to import and deploy the OVA, to edit VM settings, and to power on the VM and edit the BIOS settings in the Console.

Messages appear while the preinstallation script runs. When the preinstallation script ends, the DVD Found screen opens.

Step 2 Select **Yes** on the DVD Found screen to begin the verification of the media integrity and a brief hardware check.

If the media check passes, select **OK** to open the Product Deployment Selection screen. Continue to Step 3.

If the media check fails, the installation terminates.

Step 3 The Product Deployment Selection screen states that the Cisco Finesse product suite will be installed. This screen has only one option: **OK**.

Select **OK** to open the Proceed with Install screen.

Step 4 The Proceed with Install screen shows the version of the product that is currently installed (if any) and the version of the product for this ISO. For the initial installation, the version currently installed shows NONE.

Select **Yes** on the Proceed with Install screen to open the Platform Installation Wizard screen.

Step 5 On the Platform Installation Wizard screen, select **Proceed** to open the Basic Install screen.

Step 6 Select **Continue** on the Basic Install screen to open the Basic Install wizard.

The Basic Install wizard presents a series of screens that present questions and options pertinent to the platform and the setup configuration. Help is available for each wizard screen.

The first Basic Install wizard screen is Timezone Configuration.

Step 7 In the Timezone Configuration screen:

a) Use the up and down arrows to locate the local time zone that most closely matches your server location. You can also type the initial character of the time zone to move to that item in the list. The Timezone field is based on country and city and is mandatory. Setting it incorrectly can affect system operation.
b) Select **OK** to open the Auto Negotiation Configuration screen.

Step 8 On the Auto Negotiation Configuration screen, select **Continue** to use automatic negotiation for the settings of the Ethernet network interface card (NIC).

The MTU Configuration screen appears.

Step 9 On the MTU Configuration screen, select **No** to keep the default setting for Maximum Transmission Units (1500).

Note Finesse supports the default setting of 1500 for MTU only. No other value is supported.

Your selection of No opens the Static Network Configuration screen.

Step 10 On the Static Network Configuration screen, enter the static network configuration values as follows, referring to the Configuration Worksheet if necessary:

a) Enter the **Host Name**.
b) Enter the **IP Address**.
c) Enter the **IP Mask**.
d) Enter the **GW Address**.
e) Select **OK** to open the Domain Name System (DNS) Client Configuration screen.

Step 11 On the **DNS Client Configuration** screen, select **Yes** to specify the DNS client information.

IMPORTANT: DNS client configuration is *mandatory* for Cisco Finesse. Select Yes on this screen. If you select No, after the installation is complete, agents **can't** sign in to the desktop and you have to reinstall Finesse.

Step 12 Specify your DNS client information as follows, referring to the Configuration Worksheet if necessary:

a) Enter the **Primary DNS** (mandatory).
b) Enter the **Secondary DNS** (optional).
c) Enter the **Domain** (mandatory).
d) Select **OK** to open the Administrator Login Configuration screen.

Step 13 On the Administrator Login Configuration screen:

a) Enter the credentials for the administrator.
b) Select **OK** to open the Certificate Information screen.

Step 14 On the Certificate Information screen:

a) Enter the following data to create your Certificate Signing Request: Organization, Unit, Location, State, and Country.
b) Select **OK** to open the First Node Configuration screen.

Step 15 On the First Node Configuration screen, select **No** to indicate that you're configuring the second node.

A warning message appears that indicates you must first configure the server on the first node before you can proceed. If you already configured the first node, select **OK**.

Step 16 On the Network Connectivity Test Configuration screen, select **No** to proceed with the installation after connectivity is verified.

Step 17 On the First Node Configuration screen, specify the information about the first node as follows:

a) Enter the **Host Name** of the primary Finesse server.
b) Enter the **IP Address** of the primary Finesse server.
c) Enter the **Security Password** of the primary Finesse server.
d) Confirm the **Security Password**.

Step 18 Select **OK** to open the Platform Configuration Confirmation screen.

Step 19 On the Platform Configuration Confirmation screen, select **OK**.

The installation begins.

The installation can take up to an hour to complete and can run unattended for most of that time.

A message appears that states the installation of Cisco Finesse has completed successfully.

```
The installation of Cisco Finesse has completed successfully.

Cisco Finesse <version number>
<hostname> login: _
```

What to do next

Check the replication status. If all nodes in the cluster show a **replication status of 2**, replication is functioning correctly.

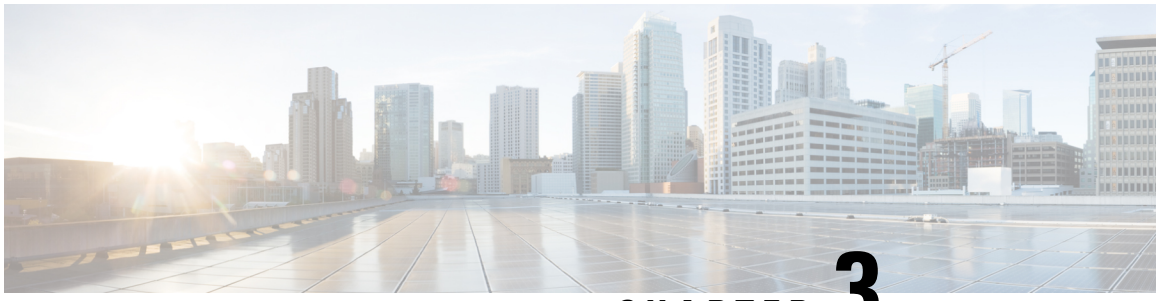
After installation, by default the configuration that controls the reverse-proxy authentication is enabled. When the reverse-proxy authentication is enabled and multiple client-side certificates are configured on the system, it impacts the certificate acceptance pop-ups from clients that are connected directly to the Finesse server without using a reverse-proxy. To prevent these pop-ups from appearing, use the **utils systems reverse-proxy client-auth** command on both the Finesse nodes to disable the reverse-proxy authentication that don't need VPN-less access to Finesse.

Note It can take 10–20 minutes to establish replication fully between the two nodes.

To access platform-specific applications like Disaster Recovery System, Cisco Unified Serviceability, and Cisco Unified Operating System Administration, use the following URL, https://*FQDN of Finesse server*:8443.

Installation Troubleshooting

If	Then
The installation fails.	If the installation fails, a screen appears that asks if you want to copy diagnostic information to a device. In this situation, you must reinstall from the beginning, but first you must attach a serial port to the VM. Then, you dump the install logs into the serial port of the VM.



CHAPTER 3

Upgrade

Supported Upgrade Paths

The following table lists the supported upgrade paths to Cisco Finesse Release 12.6(1):

Current Version	Upgrade Path
Release 12.0(x) or 12.5(x) **Note** If you upgrade from Cisco Finesse 12.5(1) SU to Cisco Finesse 12.6(1), you must immediately upgrade to Cisco Finesse 12.6(1) ES05 or above.	Upgrade to Release 12.6(1)

Note

- To upgrade from releases prior to Cisco Finesse 12.0(1) to Cisco Finesse 12.6(1), you must first upgrade to 12.0(1) and then upgrade to 12.6(1).
- Before upgrading to Cisco Finesse 12.6(1), you must download and install `ucos.keymanagement.cop.sgn` file from https://software.cisco.com/download/home/268439622/type/286325642/release/12.6(1).

Aligned Partitions Support

Cisco Finesse supports aligned partitions with a fresh installation.

If you perform an upgrade from a previous release, the platform detects the unaligned partitions and displays the following error:

```
ERROR-UNSUPPORTED: Partitions unaligned
```

You can run Cisco Finesse with the unaligned partitions, as there's no functional impact to Finesse. However, you can't experience the benefits of aligned partitions unless you perform a fresh installation.

To support aligned partitions, do the following:

1. Upgrade Cisco Finesse.
2. Perform a backup on the primary Finesse server using the Disaster Recovery System (DRS) application. To access the DRS application, direct your browser to https://*FQDN of Finesse server*:8443/drf.
3. Perform a fresh installation of Cisco Finesse.
4. Access the DRS application and perform a restore from your backup.

For more information about DRS backup and restore, see the *Cisco Finesse Administration Guide* and the detailed online help provided with the DRS application.

Perform Upgrade

You must upgrade the primary Finesse node first and then the secondary Finesse node. Both the primary and secondary Finesse nodes must be running the same version before the upgrade.

Before you begin

- Upgrade Finesse during off-peak hours or during a maintenance window to avoid service interruptions.
- Perform a DRS backup on the primary Finesse server. To access the DRS application, direct your browser to https://*FQDN of Finesse server*:8443/drf. For more information, see the online help that is provided with the DRS application.
- For large deployments, allocate extra vRAM and other resources to avoid impacting the performance of the upgraded version. For more information on the virtualization details, see the Virtualization for Cisco Finesse wiki.
- Place the Cisco Finesse ISO file on an FTP or SFTP server that you can access from your Finesse system or burn the ISO file to DVD.
- The Finesse desktop has a new look due to the Multi-Tab gadget-based layout. To save the existing layout, sign in to the cfadmin (https://*FQDN of Finesse server:8445*/cfadmin) and copy the custom layout from **Desktop Layout** > **Manage Desktop Layout**. Save the custom layout as a text file in your local file system.
- Icons (both custom and in-built) that appear on the Finesse desktop and the left navigation bar are now customizable. Finesse specific tabs with no change in labels automatically display their respective in-built icons. Tabs that are created or modified have a default icon. You can customize these icons in the desktop layout through the administration portal of Finesse. You can upload custom icons into the Finesse third-party gadget. For more information see, *Default Layout XML* section in the *Cisco Finesse Administration Guide*.
- For upgraded layouts, the "hidden=false" attribute is introduced for non-voice state control gadgets. For example, the existing non-voice control gadget URLs are migrated to the new URL. **<gadget hidden="true">https://localhost/uccx-nvcontrol/gadgets/NonVoiceControl.xml</gadget>**

- For upgraded layouts, TeamMessage, Desktop Chat, and sample configurations for customizing desktop properties don't appear by default. The administrator must copy the XML from the **View Default Layout** and add to the respective custom layouts. For more information, see the *Cisco Finesse Administration Guide*.
- After you upgrade to Cisco Finesse 12.0(1), the name, format, and folder references of the Cisco-provided gadgets are changed automatically. Automatically modified gadget details are as follows:
  - From `/desktop/gadgets/QueueStatistics.jsp` to `/desktop/scripts/js/queueStatistics.js`
  - From `desktop/gadgets/TeamPerformance.jsp` to `desktop/scripts/js/teamPerformance.js`
  - From `/desktop/gadgets/CallControl.jsp` to `/desktop/scripts/js/callcontrol.js`

Note Gadgets within commented sections aren't modified automatically. After the upgrade, if you want to use the gadgets that are in the commented sections, you must manually modify the name, format, and path of the gadgets.

- The **maxRow** is changed from being a query parameter to an attribute. During an upgrade, it is removed from the URL of the Team Performance gadget and is added as an attribute. After the upgrade, the height of the rows in the Team Performance gadget remains the same.
- In upgrade scenarios, by default, the first two call variables are displayed in the agent call pop over and in the supervisor active call details. You can modify the configuration of the pop over variables to improve the agent and supervisor experience.
- After upgrades, manually remove the Context Service gadgets from the Desktop Layout and Team Desktop Layout.

Note After the successful upgrade, the CAs that are unapproved by Cisco are removed from the platform trust store. However, you can add them back, if necessary.

- For information about the list of CAs that we support, see the *Cisco Trusted External Root Bundle*.
- For information about adding a certificate, see *Insert a New Tomcat-trust Certificate* section in the *CUCM Certificate Management and Change Notification*.

Procedure

Step 1 SSH to your Finesse system and sign-in with the platform administration account.

Step 2 Access the CLI and run the **utils system upgrade initiate** command.

Step 3 Follow the instructions that are provided by the **utils system upgrade initiate** command.

If you choose to install from a remote source (FTP or SFTP server), provide the location and credentials for the remote file system.

If you choose to install from the local CD/DVD drive, ensure that the drive is connected to the Finesse virtual machine (VM) as follows:

a) Right-click the VM and choose **Edit Settings**.
b) Click the **Hardware** tab.
c) In the left pane, select **CD/DVD Drive**.
d) In the right pane, under Device Status, check the **Connected** and **Connect at power on** check boxes.
e) Under Device Type, select **Datastore ISO File**.
f) Click **Browse** and navigate to the Finesse ISO file.
g) Click **OK**.

Finesse also prompts you for SMTP Server information, but it's not mandatory. If you don't have an SMTP Server, you can skip the SMTP prompt.

Step 4 At the **Automatically switch versions if the upgrade is successful** prompt, type **yes**. The upgrade isn't active until a switch version is performed.

Note Once the switch version is complete, the system reboots.

Step 5 At the Start installation (yes/no) prompt, type **yes** to start the upgrade.

Step 6 If you're installing from the local CD/DVD drive, when the upgrade enters the BIOS screen, on the Boot tab, move CD-ROM Drive to the top. Save your settings and exit.

Step 7 After the upgrade is complete, disconnect the CD/DVD drive.

a) Right-click the VM and choose **Edit Settings**.
b) Click the **Hardware** tab.
c) Select **CD/DVD Drive 1**.
d) Clear the **Connected** and **Connect at power on** check boxes.
e) Click **OK**.

Step 8 Perform the preceding steps on the secondary Finesse server.

Step 9 Sign in to the Finesse desktop to verify that the upgrade was successful (https://*FQDN of Finesse server:8445*/desktop).

Note After Finesse restarts, wait approximately 20 minutes before you attempt to sign in to the desktop. Finesse services may take a few minutes to reach the STARTED state.

What to do next

- After the system upgrade, ensure that all agents, supervisors, and administrators clear their browser cache.
- If you had a modified desktop layout before the upgrade, perform the following steps to ensure you obtain the latest changes:
  1. Sign in to the Finesse administration console and click the **Desktop Layout** tab.
  2. On the Manage Desktop Layout gadget, click **Restore Default Layout**.
  3. Click **Save**.

4. Using the text file of the desktop layout that you saved before the upgrade as a reference, modify the layout to include the changes that you made to the previous layout.
5. Click **Save** to save your changes.

- In the Manage Reasons (Not Ready) gadget, check for Not Ready reason codes with code values that are not unique. Edit any that you find to give them unique values.
- In the Manage Reasons (Sign Out) gadget, check for Sign Out reason codes with code values that aren't unique. Edit any that you find to give them unique values.
- Reset the third-party account password as it is a Unix user account. Use the **utils reset_3rdpartygadget_password** command to reset the third-party account password. You may reset to the previously configured password or change to a new password.

Perform Rollback

If a problem occurs with the upgrade, you can roll back to the earlier release.

Procedure

Step 1 Perform a switch-version on the primary node.

a) Access the CLI and enter the command **utils system switch-version**.
b) Enter **yes** to confirm.

The system attempts to switch back to the original version and reboots if the switch is successful.

Step 2 Repeat Step 1 on the secondary node.

Step 3 1 hour after the switch version is complete, use the following command on both nodes to confirm that the replication is successful: **utils dbreplication runtimestate**.

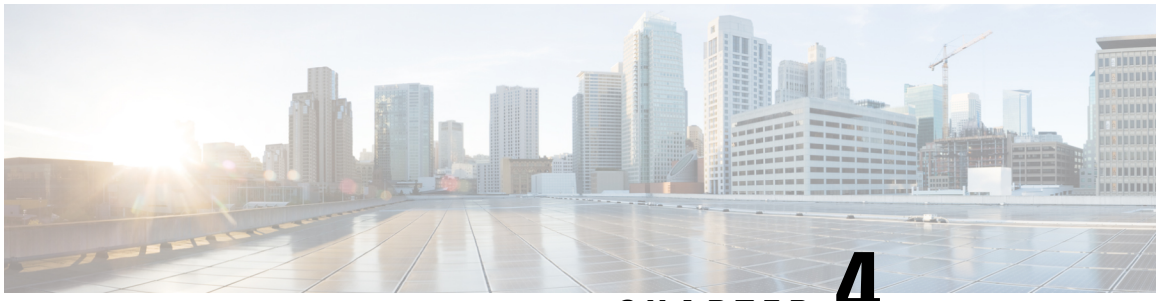
The replication is successful if the output shows a replication status of 2.

Note If the replication is unsuccessful, run the following database replication commands on the primary node:

utils dbreplication stop all

utils dbreplication reset all

After you enter these commands, wait again for 1 hour (or more depending on the volume of data) before again using the **utils dbreplication runtimestate** command to confirm the replication is successful.



CHAPTER 4

Initial Configuration

Configure Contact Center Enterprise Administration and Data Server Settings

Configure the Contact Center Enterprise Administration & Data Server settings to enable authentication for Cisco Finesse agents and supervisors.

Note If you are using HTTPS, the first time you access the administration console, you see a browser security warning. To eliminate browser security warnings each time you sign in, you can trust the self-signed certificate provided with Finesse or obtain and upload a CA certificate.

Procedure

Step 1 Sign in to the administration console.

Step 2 In the Contact Center Enterprise Administration & Data Server Settings area, enter the Administration & Data Server settings as described in the following table. Refer to your configuration worksheet if necessary.

Field	Description
Primary Host/IP Address	The hostname or IP address of the Unified CCE Administration & Data Server. For example, **abcd12-5-aw-a**.
Backup Host/IP Address	The hostname or IP address of the backup Unified CCE Administration & Data Server. For example, **abcd12-5-aw-b**.
Database Port	The port of the Unified CCE Administration & Data Server. The default value is 1433. **Note** Cisco Finesse expects the primary and backup Administration & Data Server ports to be the same, hence the Finesse administration console exposes one port field. You must ensure that the port is the same for the primary and backup Administration & Data Servers.
AW Database Name	The name of the AW Database (AWDB). For example, **ucceinstance_awdb**.
Domain	The domain name of the AWDB. For example, **cisco.com**.
Username	The username required to sign in to the AWDB. **Note** If you specify a domain, this user refers to the Administrator Domain user that the AWDB uses to synchronize with the logger. In which case, the AWDB server must use Windows authentication and the configured username must be a domain user. If you do not specify a domain, this user must be an SQL user.
Password	The password required to sign in to the AWDB.

Step 3 Click **Save**.

Configure Contact Center Enterprise CTI Server Settings

Configure the A Side and B Side CTI servers on the primary Finesse server.

Procedure

Step 1 If you are not already signed in, sign in to the administration console on the primary Finesse server:

https://FQDN of Finesse server/cfadmin

Step 2 Sign in with the Application User credentials defined during installation.

Step 3 In the Contact Center Enterprise CTI Server Settings area, enter the CTI server settings as described in the following table. Refer to your configuration worksheet if necessary.

Field	Description
A Side Host/IP Address	Enter the hostname or IP address of the A Side CTI server. This value is typically the IP address of the Peripheral Gateway (PG). The CTI server runs on the PG.
A Side Port	Enter the port number of the A Side CTI server. The value of this field must match the port configured during the setup of the A Side CTI server.
Peripheral ID	Enter the ID of the Agent PG Routing Client (PIM). The Agent PG Peripheral ID should be configured to the same value for the A Side and B Side CTI servers.
B Side Host/IP Address	Enter the hostname or IP address of the B Side CTI server.
B Side Port	Enter the port of the B Side CTI server. The value of this field must match the port configured during the setup of the B Side CTI server.
Enable SSL encryption	Check this box to enable secure encryption.

Step 4 Click **Save**.

Configure Cluster Settings

Configure the cluster settings for the secondary Finesse node. The secondary Finesse node handles agent requests if the primary server goes down.

Procedure

Step 1 If you are not already signed in the primary node, sign in to the administration console of the primary node with the Application User credentials.

Step 2 In the Cluster Settings area, in the Hostname field, enter the hostname of the secondary Finesse server.

Step 3 Click **Save**.

Restart Cisco Finesse Tomcat

After you make changes to the Contact Center Enterprise CTI Server, Contact Center Enterprise Administration & Data Server, or cluster settings, restart Cisco Finesse Tomcat for the changes to take effect.

Note After you restart Finesse, it can take approximately 6 minutes for all server-related services to restart. Therefore, you wait 6 minutes before you attempt to access the Finesse administration console.

Procedure

Step 1 Access the CLI and run the following command:

utils service restart Cisco Finesse Tomcat

Step 2 You can enter the command **utils service list** to monitor the Cisco Finesse Tomcat Service. After Cisco Finesse Tomcat changes to STARTED, the configured agents can sign in to the desktop.

Check Replication Status

Procedure

Step 1 Access the CLI on the primary Finesse server.

Step 2 Sign in with the Administrator User credentials that are defined during installation.

Step 3 Run the following command:

utils dbreplication runtimestate

This command returns the replication status on both the primary and secondary Finesse servers.

Install Language Pack

Download and install a language pack only if you want to use the Finesse desktop interface in a language other than English.

The language pack for Finesse is delivered as a single Cisco Option Package (COP) file. The file is available to download from Cisco.com and contains a single installer for all language variants.

You can download the language pack for Finesse at the following link:

https://software.cisco.com/download/release.html?mdfid=283613135&softwareid=284259728&relind=AVAILABLE&rellifecycle=&reltype=latest

COP files can generally be installed on an active, running system. However, language COP files cannot be removed or rolled back.

Note If the ReadMe file for a specific COP file contradicts these general guidelines, follow the instructions provided with the file.

For more information about supported languages, see the *Cisco Finesse Administration Guide* (https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-user-guide-list.html).

Procedure

Step 1 Download the Finesse COP file from the Cisco Software site https://software.cisco.com/download/type.html?mdfid=283613135&i=rm to a local source or an SFTP server that can be accessed by the Finesse server.

Step 2 Use SSH to log in to your Finesse system with the platform administration account.

Step 3 Use the CLI to run the command **utils system upgrade initiate**.

Step 4 Follow the instructions provided by the utils system upgrade initiate command.

Step 5 Reboot the server.

Step 6 Repeat step 2 through step 5 on the secondary Finesse server.

Step 7 When the installation is complete on both Finesse servers, agents and supervisors must clear their browser cache and cookies.

Configure IPv6 Settings

Cisco Finesse supports IPv6 using dual stack (IPv4 and IPv6). By default, only IPv4 is enabled at installation. You can enable IPv6 after installation using either Cisco Unified Communications Operating System Administration or the CLI.

With IPv6 enabled, the Finesse Administration Console, Finesse Desktop Interface, and Finesse REST APIs can connect to the Finesse server using IPv4 or IPv6. However, the Finesse server can connect to Unified CCE and the CTI server using IPv4 only.

When you set up IPv6 on Finesse, restart the system for the updates to take effect.

Set Up IPv6 Using Cisco Unified Communications Operating System Administration

To set up IPv6 using Cisco Unified Operating System Administration, perform the following procedure on both the primary and secondary Finesse servers.

Procedure

Step 1 Sign in to Cisco Unified Operating System Administration on the Finesse server (https://*FQDN*:8443/cmplatform, where *FQDN* is the fully qualified domain name of the Finesse server).

Step 2 Navigate to **Settings** > **IP** > **Ethernet IPv6**.

Step 3 To enable IPv6, check the **Enable IPv6** check box (or uncheck the box to disable IPv6).

Step 4 Enter values for **IPv6 Address**, **Prefix Length**, and **Default Gateway**.

Step 5 To restart after you save the changes, check the **Update with Reboot** check box.

Step 6 Click **Save**.

Set Up IPv6 Using the CLI

To set up IPv6 using the CLI, perform the following procedure on both the primary and secondary Finesse servers.

Procedure

Step 1 Access the CLI on the Finesse server.

Step 2 To enable or disable IPv6, enter:
set network ipv6 service {enable | disable}

Step 3 Set the IPv6 address and prefix length:
set network ipv6 static_address *addr mask*

Example:

```
set network ipv6 static_address 2001:db8:2::a 64
```

Step 4 Set the default gateway:
set network ipv6 gateway *addr*

Step 5 Restart the system for the changes to take effect.
utils system restart

Step 6 To display the IPv6 settings, enter:
show network ipv6 settings

Ensure Agents Have Passwords

Agents who do not have a password defined in Unified CCE Configuration Manager cannot sign in to Finesse.

Agent password is an optional field in Unified CCE, but it is mandatory for Cisco Finesse.

For agents who do not have passwords, you must perform the following steps:

Procedure

Step 1 Launch Unified CCE Configuration Manager.

Step 2 Locate the record for the agent (Agent Explorer > Agent tab).

Step 3 Enter a password, and save the record.

Ensure Logout Non-Activity Time for Agents is Configured

The Logout non-activity time specifies how long an agent can remain inactive in the Not Ready state before that agent is signed out of Finesse.

For agents who use the Task Routing interface on Finesse for non-voice tasks, set the Logout non-activity time to blank.

Perform the following steps to configure Logout non-activity time for an agent.

Procedure

Step 1 Launch the Unified CCE Configuration Manager.

Step 2 Launch Agent Desk Settings List (**Tools** > **List Tools**).

Step 3 Select **Agent Desk Settings List**.

Step 4 In the Logout non-activity time field, enter the number of seconds of agent inactivity while in the Not Ready state before the system software signs the agent out. You can enter a value between 10 seconds and 7200 seconds.

Step 5 Click **Save**.

The modified settings are applied to all of the agents who use these agent desktop settings.

Configure Agent Phones

Before agents can sign in to the Finesse desktop, you must ensure that the agent phones are configured in Unified Communications Manager. For more information about configuring agent phones, see the "Agent Phones" section of the *Solution Design Guide for Cisco Unified Contact Center Enterprise* (https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-implementation-design-guides-list.html).

Configure Finesse IP Phone Agent

With Finesse IP Phone Agent (IPPA), agents and supervisors can access Finesse features on their Cisco IP Phones as an alternative to accessing Finesse through the browser. Finesse IPPA supports fewer features than the Finesse desktop in the browser, but it does allow agents and supervisors to receive and manage Finesse calls if they lose or do not have access to a computer.

To set up Finesse IPPA, see the *Cisco Finesse Administration Guide* (https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-user-guide-list.html).

Note The Finesse IPPA setup requires a Cisco Finesse Tomcat restart.

Browser Settings for Agent and Supervisor Desktop

To ensure that all features of the Cisco Finesse agent and supervisor desktop work properly, you must disable popup blockers from the supported browsers. For the list of supported browsers, see the Unified CCE Compatibility Matrix.

Ensure Agents Can Sign in to Desktop

After the system administrator defines configuration settings and restarts services, agents who have passwords and operational handsets can sign in to the Finesse Agent Desktop.

Note Finesse agents can enter either their `AgentID` or `Login name` (in the **Username** field of the desktop login screen) to sign in. Ensure that each agent's `AgentID` and `Login name` are unique across both sets of data. If one agent's `AgentID` matches another agent's `Login name`, neither agent can sign in.

Note After you restart Finesse, it takes approximately 6 minutes for all server-related services to restart. Therefore, you should wait 6 minutes before you attempt to sign in to the desktop.

Note If you are using HTTPS, the first time you access the agent desktop, you see a browser security warning. To eliminate browser security warnings each time you sign in, you can trust the self-signed certificate provided with Finesse or obtain and upload a CA certificate.

Procedure

Step 1 Enter the following URL in the address bar of your browser:

https://FQDN of Finesse server/desktop

Step 2 If you installed the language pack COP file, on first login, select the language you want to appear on the desktop from the drop-down menu in the language selector screen and click **Next**. If you did not install the language pack COP file, the language selector drop-down list does not appear in the user interface.

Note If you installed the language pack COP file, you can also select a language by passing the locale as part of the URL (for example, https://FQDN of Finesse server/desktop?locale=fr_FR) or by changing your browser preferred language. The default language is English (en_US).

Step 3 Enter your username, password, and extension, and then click **Sign In**.

Note The Sign In button is enabled once the username, password and extension fields are entered. If any field is incomplete, the Sign In button will remain disabled.

Step 4 If you wish to change the language that appears on your desktop, use the **Change the Language** link to return to the language selector screen and choose the language.

If your agent is signed into the Agent Desktop in Single Sign-On Mode or Hybrid Mode, refer to the sections *Sign In to Finesse Desktop Single Sign-On Mode* or *Sign In to Finesse Desktop Hybrid Mode* in the *Cisco Finesse Desktop User Guide for Unified Contact Center Enterprise.*

Ensure Failover Functions Correctly

Finesse provides a diagnostic tool that you can run on the Finesse desktop to ensure that failover is functioning correctly.

Note For this tool to make an accurate diagnosis, the alternate Finesse server must be accessible and in service

Procedure

Step 1 Sign in to the Finesse desktop.

Step 2 Enter the following URL in the address bar of the browser:

https://*FQDN of Finesse server*/desktop/failover

The tool performs a simulated failover test and displays the results. If the test passes, the following message appears:

Test sequence passed for failover to <Finesse alternate server name>. Click OK to test failback by running the test sequence from <Finesse alternate server name>.

Step 3 Click **OK** to test failback.

Note If the failover test fails, the server may not be accessible (for example, certificate exceptions may be blocking browser access). To ensure that this is not the case, try to access the alternate Finesse server directly using the FQDN and manually sign in to the desktop. If sign-in succeeds, certain browser settings or policies may be preventing failover from working properly. For example, accessing Finesse with its hostname or IP address instead of the FQDN may cause browsers to place client-side security restrictions on access between the two servers because they are considered to be third-party to each other. If the two servers are on the same domain and accessed with the FQDN, these restrictions are not as strict.

Configure DNS on Clients

Note This procedure is required for uncommon environments where non-hierarchical DNS configuration exists. If your environment has hierarchical DNS configuration, you do not need to perform this procedure. This procedure applies to clients that use a Windows operating system. For information about configuring DNS on Mac clients, see your Apple documentation (www.apple.com/mac).

Configuring DNS on client computers allows the clients to resolve the fully-qualified domain name (FQDN) of the active Finesse server during a failover.

Procedure

Step 1 Go to **Control Panel** > **Network and Internet** > **Network and Sharing Center**. (Open the Control Panel, enter Network Connections in the search bar, and then click **View network connections**.)

Step 2 Click the appropriate network connection.
A dialog box showing the status of the connection appears.

Step 3 Click **Properties**.

Step 4 On the Networking tab, select Internet protocol version 4 (TCP/IPv4) or Internet protocol version 6 (TCP/IPv6) if the client is IPV6, and then click **Properties**.

Step 5 Click **Advanced**.

Step 6 On the DNS tab, under DNS server addresses, in order of use, click **Add**.

Step 7 Enter the IP address of the DNS server that was entered during installation and click **Add**.

Step 8 If a secondary DNS was entered during installation, repeat Step 5 and Step 6 to add its IP address.

Cloud Connect Certificates

Import Cloud Connect certificates to the trust store of Finesse to communicate with the Cloud Connect server using HTTPS. You must import a valid non-expired X.509 CA or self-signed certificate into the Cisco Finesse trust store.

- For a CA-signed certificate, see CA-Signed Certificate, on page 35.
- For a self-signed certificate, see Self-Signed Certificate, on page 35.

CA-Signed Certificate

Procedure

Step 1 Obtain the CA-signed certificate from the certification authority for Cloud Connect server.

a) Sign in to Cisco Unified OS Administration on the Cloud Connect server using the following URL: *https://FQDN of Cloud Connect server:8443/cmplatform*.

b) Generate the CSR and sign it from the certification authority. For more information on generating the CSR, see the *Certificate Management* section in the *Getting Started* chapter of *Cisco Finesse Administration Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-maintenance-guides-list.html.

Step 2 Import the CA-signed certificate of Cloud Connect server to the Cisco Finesse server trust store as **tomcat-trust**. For more information, see Import Cloud Connect Certificate, on page 36.

Self-Signed Certificate

Procedure

Step 1 Export the self-signed Cloud Connect certificate from the Cisco Unified Operating System Administration. For more information, see Export Cloud Connect Certificate, on page 35.

Step 2 Import the downloaded self-signed Cloud Connect certificate to the Cisco Finesse trust store as **tomcat-trust**. For more information, see Import Cloud Connect Certificate, on page 36.

Export Cloud Connect Certificate

Procedure

Step 1 Sign in to Cisco Unified OS Administration on the Cloud Connect server using the following URL: `https://FQDN of Cloud Connect server:8443/cmplatform`.

Step 2 Select **Security** > **Certificate Management**.

Step 3 Enter the search criteria as **tomcat** and then click **Find** to filter the certificate.

The tomcat certificates list is displayed. If you do not find the tomcat certificate for your server in the **Certificate List**, then click **Generate Self-signed**. When the certificate generation is complete, reboot your server. Then restart this procedure. For more information on generating the self-signed certificate, see *Cisco Unified Operating System Administration Online Help*.

Step 4 Click **Download .PEM File**.

Step 5 Save the .PEM file in your local machine.

What to do next

Follow the same steps for both publisher and subscriber nodes.

Import Cloud Connect Certificate

Before you begin

Export tomcat certificate for all Cloud Connect nodes and save in your local machine. For more information, see *Export Cloud Connect Certificate*.

Procedure

Step 1 Sign in to Cisco Unified OS Administration on the primary Finesse server using the following URL: `https://FQDN of Finesse server:8443/cmplatform`

Step 2 Select **Security** > **Certificate Management** > **Upload Certificate/Certificate chain**.

Step 3 Upload the Cloud Connect certificate.

a) From the **Certificate Purpose** drop-down list, select **tomcat-trust**.

b) In the **Upload File** field, click **Browse** and browse to the Cloud Connect certificate file.

c) Click **Upload**.

Step 4 Reboot the Cisco Finesse server.

Customer Collaboration Platform Certificates

You can develop applications using Customer Collaboration Platform and Cisco Finesse APIs in order to use Task Routing. The Customer Collaboration Platform Task API enables applications to submit non-voice task requests to Unified CCE. Cisco Finesse uses Customer Collaboration Platform APIs for task management.

Validation of the X.509 certificate is enforced. It is mandatory to have a valid non-expired Customer Collaboration Platform X.509 CA or self-signed certificate to be imported into the Cisco Finesse trust store.

The administrator must set the **utils finesse set_property webservices trustAllCertificates** to *false* to enable the validation of the X.509 CA or the self-signed certificate.

For more information on CLI commands, see *Service Properties* section in *Cisco Finesse Administration Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-maintenance-guides-list.html.

Export Customer Collaboration Platform

Before you begin

Add the Customer Collaboration Platform IP address to the allowed list addresses.

Procedure

Step 1 Sign in to Cisco Unified OS Administration on the CUCM server using the following URL: `https://FQDN of Customer Collaboration Platform server/cmplatform`.

Step 2 Select **Security** > **Certificate Management**.

Step 3 Enter the search criteria as **`tomcat`** and then click **Find** to filter the certificate.

The tomcat certificates list is displayed. If you do not find the tomcat certificate for your server in the **Certificate List**, then click **Generate Self-signed**. When the certificate generation is complete, reboot your server. Then restart this procedure. For more information on generating the self-signed certificate, see *Cisco Unified Operating System Administration Online Help*.

Step 4 Click **Download .PEM File**.

Step 5 Save the .PEM file in your local machine.

What to do next

Follow the same steps to export the certificate for all the CUCM nodes.

Import Customer Collaboration Platform Certificate

Procedure

Step 1 Sign in to Cisco Unified OS Administration on the Finesse server using the following URL: `https://FQDN of Finesse server: 8443/cmplatform`

Step 2 Select **Security** > **Certificate Management** > **Upload Certificate/Certificate chain**.

Step 3 Upload the Customer Collaboration Platform certificate.

a) From the **Certificate Purpose** drop-down list, select **tomcat-trust**.
b) In the **Upload File** field, click **Browse** and browse to the Customer Collaboration Platform certificate file.
c) Click **Upload** .

Note Configure Customer Collaboration Platform in Unified CCE and Unified CCX using the fully-qualified domain name (FQDN).

Step 4 After the upload is complete, sign out from the platform administration page of Cisco Finesse.

Step 5 Reboot the Cisco Finesse server.

Note Follow the same steps to upload the Customer Collaboration Platform certificate on both the primary and secondary Finesse nodes.

Load Balancing for Finesse

After agents sign in to the Finesse desktop, Finesse desktop client manages the failover. For example, if a Finesse server goes out of service, the Finesse client automatically redirects and signs the agent into the other Finesse server. The client can manage various network and server failure use cases. Given this client-side logic, the use of a load balancer after sign-in is not required nor supported.

However, the following are two scenarios in which you can use a load balancer with Finesse. These scenarios apply only to the Finesse desktop and not to Finesse IP Phone Agents.

Note Starting from the Finesse 12.6.1 ES05 release, the allowed hosts must not contain the hostname or IP address of the load balancer. It should contain only the internal and external hostname and IP address of the reverse-proxy.

When Agents Navigate to the Finesse Sign-In Page

If agents attempt to navigate to a Finesse server that is down or not reachable, agents cannot access the sign-in page. Agents receive an error and must manually sign in to the other Finesse server. To avoid this manual step, you can use a load balancer using URL redirect mode to direct the agents to a Finesse server that is operational. One option is to use the Finesse `SystemInfo` REST API, which provides the status of the Finesse server. For details about this API, see the *Cisco Finesse Web Services Developer Guide*.

When you configure a load balancer to determine the status of the Finesse servers, the call flow is as follows:

1. When agents sign in to Finesse, they point their browsers to the load balancer.
2. The load balancer redirects the agent browser to an appropriate Finesse server.
3. The agent signs in to the Finesse server directly. At this stage, the load balancer is no longer part of the call flow.

When Customers Use the Finesse API Directly

If you use the Finesse REST API directly, the Finesse client-side failover logic is not in the call flow. In this case, you can opt to use a load balancer to manage high availability. This load balancer is considered part of a custom application which, like all custom applications, Cisco does not support. You must provide the required support for the load balancer.

Before you configure the load balancer, remember that there are two connections between Finesse clients and the Finesse server:

- A REST channel for request and response.
- An XMPP channel that the server uses to send notifications to the client.

Both channels for a given client must connect to the same Finesse server.

You cannot connect the load balancer to the REST connection for one Finesse server and to the XMPP channel connection for the other Finesse server. This setup provides unpredictable results and is not supported.

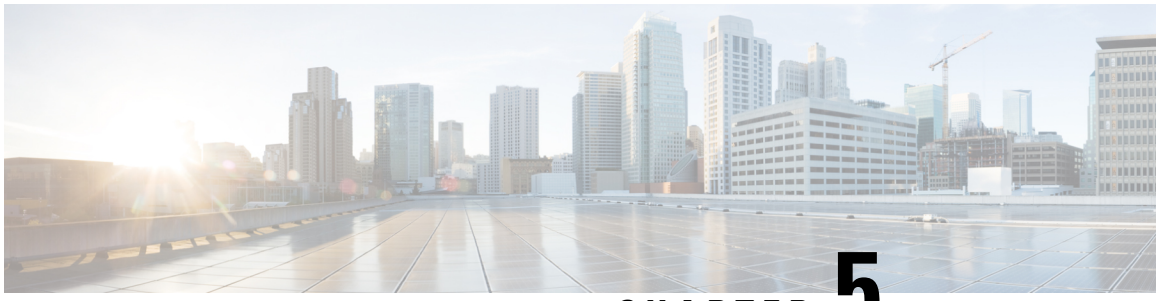
Initial Configuration Troubleshooting

If	Then
The administration console does not load after a fresh installation.	**1.** Clear your browser cache (delete browsing history and cookies). **2.** If the problem persists, restart the Cisco Finesse Tomcat service or restart the Finesse server.

If	Then
Agents cannot sign in to the desktop after a fresh installation.	

If	Then
	1. Verify that the agent ID and password are correct. **Note** Finesse agents can use either their `loginID` or `loginName` to sign in. Ensure that each agent's `loginID` and `loginName` are unique across both sets of data. If one agent's `loginID` matches another agent's `loginName`, neither agent can sign in. **2.** Verify that a valid domain was configured during installation and that forward and reverse DNS are set up correctly. To check whether DNS was configured during installation, check the install.log for the following: InstallWizard|USER_ACTION_BTN_PUSH: Screen = DNS Client Configuration, button pushed = No|<LVL::Info The preceding message indicates that DNS was not configured during the installation. Reinstall Finesse and configure the DNS with a valid domain. **3.** Verify that the agent is configured in Unified CCE. **4.** Verify that the AWDB is configured correctly. **a.** Check the realm.log for the following line: "ERROR com.cisco.ccbu.finesse.realms.ccerealm.CCERealmConfig - Cannot connect to any AWDB! Ensure that at least one AWDB is configured properly and running!" This line indicates that Finesse cannot connect to the AWDB. **b.** Check that the values entered in the Contact Center Enterprise Administration & Data Server Settings gadget are correct. • Verify that the username entered is a Windows domain user. • Verify that the username is not prepended with the domain (for example, domain\username). • Verify that the port configured is open to the Finesse server. **c.** Check that the AWDB is set up correctly and running. • The AWDB SQL server must use Windows authentication. • Verify that the AWDB server is up and that the Distributor service is running. **5.** Restart Cisco Finesse Tomcat on the primary and secondary Finesse servers. **6.** Verify that the agent's device is properly configured in Unified

If	Then
	Communications Manager and is active.



CHAPTER 5

Cisco Finesse Virtualization

Virtualization Hardware

Before you install the Finesse software on any server, you must address the following requirement:

- If you are performing a fresh install of Finesse in any deployment, be sure to verify that the virtual machine is also fresh (no previously-installed OS is present in the VM).
- If you use SATA 7200 RPM disks in your server, you must configure the datastore as RAID 10.

Virtualization Software

All Finesse servers run on VMs using the Unified Communications Operating System (Unified OS or UCOS). See https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-software-requirements.html.

- Finesse ISO or DVD

Note You must install Finesse by configuring a DataStore ISO file on the virtual CD or DVD drive of the target VM.

- ESXi must be installed prior to the installation of Cisco Finesse.

Deploying Virtual Machines for Cisco Finesse

Perform the following steps in vSphere client to deploy the Virtual machines:

Before you begin

See Unified Communications VMWare Requirements.

The following software requirements apply specifically to Finesse:

- For other third-party software requirements and for a list of approved UCS servers, see the server requirements and version compatibility with Unified CM sections in the C*isco Unified Contact Center Enterprise Design Guide* available at http://www.cisco.com/en/US/products/sw/custcosw/ps1844/products_implementation_design_guides_list.html.

Procedure

Step 1 Highlight the host or cluster to which you wish the VM to be deployed.

Step 2 Select **File** > **Deploy OVF Template**.

Step 3 Click the **Deploy from File** radio button and specify the name and location of the file you downloaded in the previous section OR click the **Deploy from URL** radio button and specify the complete URL in the field, then click **Next**.

Step 4 Enter the name of the VM machine that you are creating and the location where it will be created.

Step 5 Choose the type of deployment (Production or Lab).

Step 6 Choose the datastore on which you would like the VM to reside (ensure there is sufficient free space to accommodate the new VM), then click **Next**.

Step 7 Verify the deployment settings, then click **Finish**.

Step 8 Update boot order as per instructions as specified in the topic *Changing the Boot Order of the Virtual Machine*.

Step 9 Insert the Finesse disk and follow the instructions specified in the topic *Cisco Finesse Server Installation*.

Changing the Boot Order of the Virtual Machine

You must change the boot order of the Virtual Machine so that the system boots off the CD/DVD drive for the install. Perform the following steps to change the boot order of the Virtual Machine:

Procedure

Step 1 In VMware vSphere Client, power off the virtual machine onto which you deployed the OVA .

Step 2 In the left pane of vSphere Client, right-click the name of the virtual machine, and select **Edit Settings**.

Step 3 In the **Virtual Machine Properties** dialog box, select the **Options** tab.

Step 4 In the Settings column, under Advanced, select **Boot Options**.

Step 5 Under Force BIOS Setup, check **The Next Time the Virtual Machine Boots, Force Entry into the BIOS Setup Screen** check box.

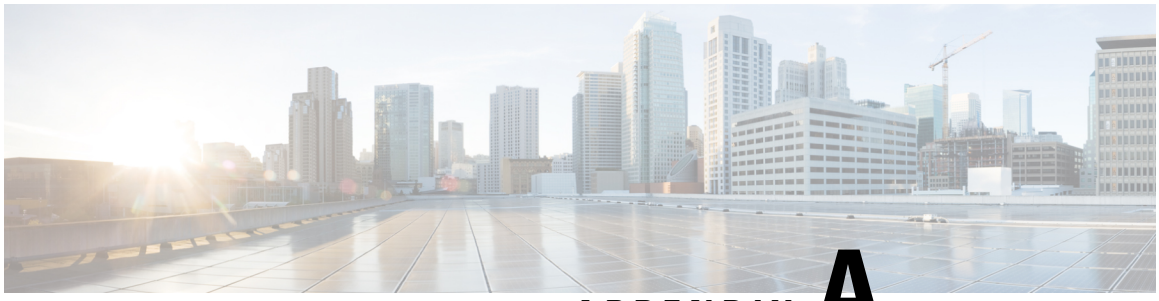
Step 6 Click **OK** to close the Virtual Machine Properties dialog box.

Step 7 Power on the virtual machine (the virtual machine boots into the BIOS menu).

Step 8 Navigate to the Boot menu and change the boot device order so the CD-ROM device is listed first and the Hard Drive device is listed second.

Step 9 Save the change and exit BIOS setup.

Note After finishing the installation, consider changing the boot order back so that the Hard Drive device is again listed before the CD-ROM device.



APPENDIX A

Network and System Services Used for Cisco Finesse

To view the platform TCP/IP services, UDP services, and Unix domain sockets that are used by Cisco Finesse, access the CLI using the Administrator User credentials and enter the following command:

show network all detail

To view the system services that are used by Cisco Finesse, access the CLI using the Administrator User credentials and enter the following command:

utils service list

The following services are enabled by default when Cisco Finesse starts. These services are essential for product operation and must not be disabled.

- A Cisco DB[STARTED]
- A Cisco DB Replicator[STARTED]
- Cisco AMC Service[STARTED]
- Cisco Audit Event Service[STARTED]
- Cisco CDP[STARTED]
- Cisco CDP Agent[STARTED]
- Cisco Certificate Change Notification[STARTED]
- Cisco Certificate Expiry Monitor[STARTED]
- Cisco DRF Local[STARTED]
- Cisco DRF Primary[STARTED]

Note Cisco DRF Primary should be started only on the Finesse primary (A Side) server.

Status on the Finesse primary (A Side) server should be “STARTED”. Status on the Finesse secondary (B Side) server should be “STOPPED” Command Out of Service.

- Cisco Database Layer Monitor[STARTED]

- Cisco Finesse Notification Service[STARTED]
- Cisco Finesse Tomcat[STARTED]
- Cisco Log Partition Monitoring Tool[STARTED]
- Cisco RIS Data Collector[STARTED]
- Cisco RTMT Reporter Servlet[STARTED]
- Cisco Syslog Agent[STARTED]
- Cisco Tomcat[STARTED]
- Cisco Tomcat Stats Servlet[STARTED]
- Cisco Trace Collection Service[STARTED]
- Cisco Trace Collection Servlet[STARTED]
- Cisco Web Proxy Service[STARTED]
- Host Resources Agent[STARTED]
- MIB2 Agent[STARTED]
- Platform Administrative Web Service[STARTED]
- SNMP Primary Agent[STARTED]
- SOAP -Log Collection APIs[STARTED]
- SOAP -Performance Monitoring APIs[STARTED]
- SOAP -Real-Time Service APIs[STARTED]
- System Application Agent[STARTED]