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 6.7 and 7.0, 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 and higher
	Chrome OS 106.0.5249 and higher

Table 2: Supported Browsers

Operating Systems	Browser Versions
Microsoft Windows 10 and Windows 11 (64 bit)	• Google Chrome version 106.0.5249 and higher • Edge Chromium version 106.0.5249 and higher • Firefox Extended Supported Release (ESR) 78.11 and later ESRs
Microsoft Windows Server 2016 (Standard and Datacenter editions) Microsoft Windows Server 2019 (Standard and Datacenter editions)	
Mac OS X	
Chromebook with Chrome OS	• Google Chrome version 60 and higher • Edge Chromium version 73 and higher

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:

- After the fresh install, by default the **utils system reverse-proxy client-auth** is enabled. If this is enabled and there are multiple certificates in the client system, when agents login to Finesse through LAN, it forces the agents to select one of the certificates to communicate with the Finesse server. If the deployments aren't configured for VPN-less access to Finesse, disable it by running the **utils system reverse-proxy client-auth disable** command on both the Finesse nodes.
- 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: _____	
Database Access Security Password	_____	

Configuration Data	Your Entry	Notes
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 12.6.2:

- **OVA:** Finesse_12.6.2_vmv13_v1.3.ova
- **Readme:** Finesse_12.6.2_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.