Installation Preparation

Cisco Finesse can be installed stand-alone in a deployment with Unified Contact Center Enterprise (Unified CCE) or coresident in a deployment with Unified Contact Center Express (Unified CCX).

This guide describes how to install a stand-alone Finesse for deployment with Unified CCE.

In a coresident deployment with Unified CCX, Finesse is installed when you run the installer for Unified CCX. For more information, see the Cisco Unified Contact Center Express Installation and Upgrade Guide.

Cisco Finesse is installed on a virtual machine as a primary or secondary node. The installation screens refer to the primary node as the first node.

Finesse is installed on the Linux-based Unified Communications Operating System. This system is an appliance model or "closed box" developed by Cisco, which does not support navigation into or manipulation of the file system.

☞

Important   This guide specifies all supported configurations for this release of Cisco Finesse. If a configuration is not stated, that configuration is not supported.

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). ESXi 5.5, 6.0 or 6.5 (VMFS 5 only) must be installed before you install Cisco Finesse.

For more information about supported VMs and VMware requirements, 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.

Operating System	Browser Version
Windows 7	Internet Explorer 11.0 (Native Mode) **Note** IE 11 requires Windows 7 SP1. Chrome (version 48 or higher) Firefox (version 38 and higher ESR)
Windows 10	Internet Explorer 11.0 (Native Mode) Chrome (version 48 or higher) Firefox (version 45 or higher)
Mac OS X	Firefox (version 45 or higher) Chrome (version 48 or higher)

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 bandwidth requirements for Cisco Finesse, see 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

The Cisco Finesse administration console and agent desktop support both HTTP and secure HTTP (HTTPS). Administrators can run a CLI command to enable or disable Cisco Finesse HTTPS Redirect for the administration console and the desktop. When Cisco Finesse HTTPS Redirect is enabled, agents and supervisors who attempt to access the desktop through HTTP are redirected to HTTPS.

Cisco Finesse HTTPS Redirect is enabled by default. After you install Finesse, if you want to use HTTP, you must run the CLI command to disable Cisco Finesse HTTPS Redirect.

When you upgrade Finesse, the setting for Cisco Finesse HTTPS Redirect is maintained. If Cisco Finesse HTTPS Redirect is disabled on your system before you upgrade, it remains disabled after you upgrade.

Note HTTPS is now supported for large deployments with more than 2000 users.

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 provided with Finesse.

This guide uses HTTP for all example URLs.

Related Topics

Cisco Finesse HTTPS Redirect

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.

Other Requirements and Considerations

- You must have access to a Network Time Protocol (NTP) server.

- You must have a valid hostname and domain.

- Choose the Finesse hostname, domain, and IP address carefully. After you install Finesse, you cannot change these values.

- You must have a preconfigured default router.

- You must have a preconfigured Domain Name Server (DNS) and have set up forward and reverse DNS.

- 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 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.

- Finesse requires a domain user that is configured with login and read permissions to access the AWDB.

- The 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 1: 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	_____	

Related Topics

System Account Privileges, on page 3

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 filenames for the OVA and associated ReadMe are as follows:

- Finesse_11.6.1_VOS11.6.1_vmv9_v1.2.ova

  This file is the VM template file that you deploy in your installation.

- Finesse_11.6.1_VOS11.6.1_vmv9_v1.2.ova.README.txt

  This file contains the instructions to import the OVA file and to edit the VM settings.

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.