# Installation — All Nodes



## Installation Media

The installation for Unified Intelligence Center is delivered on DVD media. Run the DVD installation on each node, and use the same DVD for all nodes.

**Note** All nodes must be running the same version of Cisco Unified Intelligence Center.

## Before You Begin

Every installation begins with an optional pre-install media check, which includes a hardware check. You then make your product deployment selection before continuing to the basic install configuration.

### Procedure

**Step 1** Mount ISO to the virtual DVD drive. Then restart or power on the server so that it boots from the DVD.

You see messages as the pre-install script runs. When the pre-install script ends, the **DVD Found** screen opens.

**Step 2** In the **DVD Found** screen, you have the option to perform a media check to verify the integrity of the DVD. If you want to check the media:

**a.** Select **Yes** to begin the verification of the media integrity.

**Note** The media check can take up to an hour. If the media check for the Controller passes, you can safely skip the media check when you install the Members.

**b.** If the media check passes, select **OK**. The **Product Deployment Selection** screen appears, and you can continue to Step 3.

If the media check fails, the DVD is ejected and the installation terminates. Contact your support provider for assistance.

If you want to skip the media check:

**a.** Select **No**. The **Product Deployment Selection** appears.

**b.** Proceed to Step 3.

**Step 3** Choose one of the following options:

- **Cisco Unified Intelligence Center**
- **Live Data**
- **Cisco Identity Service (IdS)**
- **Cisco Unified Intelligence Center with Live Data and IdS**

**Note**
- For the 2000 agent reference design, choose the co-resident deployment option **Cisco Unified Intelligence Center** with **Live Data** and **IdS**; and then select **OK**. The **Cisco Unified Intelligence Center**, **Live Data**, and **IdS** option installs **Cisco Unified Intelligence Center**, **Live Data** and **Cisco Identity Service (IdS)** on the same server.
- For all other deployments, select one of the standalone install options. For example, select **Cisco Unified Intelligence Center, Live Data**, or **Cisco Identity Service (IdS)**. Then select **OK**.

**Step 4** Click **OK** to initiate a hard drive check, during which the installation checks for a supported hardware platform with the correct number of disks.

A successful hardware check opens the **Proceed with Install** screen. The **Proceed with Install** screen shows the version of the product that is currently on the hard drive (if any) and the version of the product that is on the DVD. For the initial installation, the version on the hard drive shows NONE.

**Note** If the server hardware is unsupported, a message appears indicating that the installation cannot proceed, and the installation halts. If you require assistance understanding the message, write it down to facilitate your conversation with your support provider. See *Contact Center Enterprise Compatibility Matrix* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-device-support-tables-list.html for details on supported hardware.

**Step 5** Select **Yes** on the **Proceed with Install** screen.
The **Platform Installation Wizard** screen appears.

**Step 6** In the **Platform Installation Wizard** screen, select **Proceed** to open the **Apply Patch** screen.

**Step 7** Select **No** at the **Apply Patch** screen. Do not apply patches from the Installation wizard. See *About Upgrades* for instructions on upgrading Unified Intelligence Center software with Engineering Specials, Minor Releases, and Maintenance Releases.

Your selection of **No** opens the **Basic Install** screen.

If you select **Yes** by mistake and open the **Apply Patch** screen, select **Back**. Then choose one of the following options:

- To enter your configuration information manually and have the installation program install the configured software on the server, choose **Proceed** and continue with this procedure.
- To do any of the following tasks, choose **Skip**; then continue with the *Entering Preexisting Configuration Information* procedure:
  - Manually configure the software that is preinstalled on your server — In this case you do not need to install the software, but you must configure the preinstalled software.
  - Perform an unattended installation — In this case, you provide preexisting configuration information on a USB key or floppy disk.
  - Install the software before manually configuring it — In this case the installation program installs the software, then prompts you to configure it manually. You can choose **Skip** if you want to preinstall the application on all your servers first and then enter information at a later time. This method might cause you to spend more time performing the installation than the other methods.

**Step 8** Select **Continue** at the **Basic Install** screen to enter the configuration screens.

**Related Topics**

Before You Upgrade

Enter Pre-Existing Configuration Information, on page 3

# Enter Pre-Existing Configuration Information

Start here if you have a server that has the product pre-installed or if you chose **Skip** in the Platform Installation Wizard window.

**Procedure**

**Step 1** After the system restarts, the Pre-existing Installation Configuration window displays.

**Step 2** If you have pre existing configuration information (Created by Answer File Generator) in a floppy disc or a USB key, insert the disc or the USB key now and choose **Continue**. The installation wizard will read the configuration information during the installation process.

**Note** If a popup window states that the system detected new hardware, press any key and then choose Install from the next window.

The Platform Installation Wizard window displays.

**Step 3** To continue with the Platform Installation Wizard, choose **Proceed**.

**Step 4** In the Basic Install window, choose **Continue**. Continue with the "Configure basic install" section.

# Configure Basic Install

The basic install launches a series of screens that present questions and options pertinent to the platform and the setup configuration. There is online help for each wizard screen.

**Note** You can change many of the basic installation configuration settings after the installation using the Set commands in the Command Line Interface (CLI). The CLI is documented in the *Administration Console User Guide for Cisco Unified Intelligence Center*.

The first Basic Install wizard screen is Timezone Configuration.

### Procedure

**Step 1** In the **Timezone Configuration** screen:

a) Use the down arrow to select the local timezone that most closely matches where your server is located. You can also type the initial character of the timezone to move to that item in the list. The timezone field is based on country/city and is mandatory. Setting it incorrectly can affect system operation.

**Note** Use the same timezone for all nodes.

b) Select **OK** to open the Auto Negotiation Configuration screen.

**Step 2** In the **Auto Negotiation Configuration** screen, select whether or not you want to use automatic negotiation for the settings of the Ethernet network interface card (NIC).

| If | Then |
|---|---|
| You want to disable auto-negotiation and specify NIC speed and duplex settings. | Select **No** to open the NIC Speed and Duplex Configuration screen, where you can manually configure the settings.<br>Proceed to Step 3. |
| The ethernet network interface card (NIC) attached to your hub or Ethernet switch supports automatic negotiation. | Select **Yes** to open the MTU Configuration screen.<br>Proceed to Step 4. |

**Step 3** In the **NIC Speed and Duplex Configuration** screen, configure settings as follows:

a) Specify the speed of the Network Interface (NIC) card in megabits per second. Speed options are **10** or **100**.

b) Specify the duplex setting of the server NIC. Options are **Full** or **Half**.

c) Select **OK** to open the MTU Configuration screen.

**Step 4** In the **MTU Configuration** screen, select **No** to keep the default setting for Maximum Transmission Units (1500). If you do not accept the default and configure the MTU size incorrectly, your network performance can be affected.

Your selection of No opens the DHCP Configuration screen.

**Step 5** In the **DHCP Configuration** screen, select **No** to open the Static Network Configuration screen.

**Step 6** At 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 7** Select **Yes** to enable the Domain Name System (DNS) Client.

**Step 8** Enter your DNS client information as follows:

a) *Configuration Worksheet* 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 9** In the **Administrator Login Configuration** screen:

a) Enter the ID for the System Administrator.
b) Enter and then confirm the password for the administrator.
c) Select **OK** to open the Certificate Information screen.

**Step 10** In the **Certificate Information** screen:

a) Enter data to create your Certificate Signing Request—Organization, Unit, Location, State, and Country.
b) Select **OK** to open the First Node Configuration screen. ("Is this server the First Node in the cluster?")

**Step 11** In the **First Node Configuration** screen, specify whether you are configuring the first node (the Controller).

| If | Then |
|---|---|
| You are installing and configuring the primary node (the Controller). | Select **Yes** to open the Network Time Protocol Client Configuration screen.<br>Continue to *Controller Configuration.* |
| You are installing and configuring a secondary node (a Unified Intelligence Center Member). | Select **No** to open the First Node Configuration Warning screen.<br>Continue to *Complete Configuration for Member Node* . |

# Post-Install Configuration

If Live data is supported and installed in the customer deployment, you must also perform some Live Data configuration tasks. Refer chapter 4 on *Live Data Installation* in the Cisco Unified Contact Center Enterprise Installation and Upgrade Guide https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.html.

### Cross-Origin Resource Sharing (CORS)

For Unified Intelligence Centre gadgets (Live Data and Historical) to load in Cisco Finesse, ensure to run the following commands in the Unified Intelligence Center server:

- Enable CORS using the `utils cuic cors enable` command.
- Set the Finesse host URL in the `utils cuic cors allowed_origin add URLs` command.

  **Examples:**

  - https://<finesse-FQDN>
  - https://<finesse-FQDN>:port

For Live Data gadgets, in addition to the above settings, ensure to enable CORS using the `utils live-data cors enable` command and set the Finesse host URL in the `utils live-data cors allowed_origin add` URLs command. If Live Data is coresident to Unified Intelligence Center, then run these Live Data commands on the same Unified Intelligence Center system; Otherwise, run on the standalone Live Data system.

For more information, see *Administration Console User Guide for Cisco Unified Intelligence Center* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-intelligence-center/products-maintenance-guides-list.html.

### Self-Signed Certificates

**Note** Follow the below steps, if you are using self-signed certificates.

Prerequisite—Download the Unified Intelligence Center tomcat certificate from Cisco Unified OS Administration page of Unified Intelligence Center.

Perform the following tasks to upload the Unified Intelligence Center server certificate to Cisco Finesse.

1. Sign in to Cisco Unified OS Administration on Cisco Finesse using the following URL: `https://FQDN of Finesse server:8443/cmplatform`.
2. Select **Security** > **Certificate Management** > **Upload Certificate/Certificate chain**.
3. From the **Certificate Purpose** drop-down list, select **tomcat-trust**.
4. In the **Upload File** field, click **Choose File** and browse to the tomcat.pem file that you saved on your system.
5. Click **Upload**.
6. Restart the Cisco Finesse Tomcat on the Cisco Finesse server.

**Note**

- Follow the same steps for both the Cisco Finesse publisher and subscriber nodes.
- If there is a standalone Live Data system in this deployment, then upload Live Data tomcat certificate in addition to Cisco Finesse, using the above-stated procedure.

For more information, see the *Certificates for Live Data* chapter in *Cisco Finesse Administration Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-maintenance-guides-list.html.

### Hazelcast Cluster Configuration

**Note** Follow the below steps, if your network does not support multicasting, and when the Unified Intelligence Center administrator sign-in page displays a banner message about the application cluster issues.

Perform the following tasks change the discovery mechanism to `tcp-ip` mode.

1. Log in to the Cisco Unified Intelligence Center CLI. Specify the System Administrator username and password.

**Note** Run the following CLIs on all nodes in the given sequence, starting from the publisher node.

2. Enter the command **utils service stop** *Intelligence Center Reporting Service*.
3. Enter the command **utils cuic cluster mode**.
4. Select cluster mode **2) Enable tcp-ip**.
5. Enter the command **utils cuic cluster show**.

**Note** Ensure that all nodes have an identical configuration.

6. Enter the command **utils service start** Intelligence Center Reporting Service.

**Note** If there happens to be a disconnect and reconnect, check that the database replication is successfully set up across all nodes in the cluster. Perform "Synchronize Cluster" from Cisco Unified Intelligence Center to ensure that cache is in sync across the cluster.

For more information, see the *Cluster Configuration for JVM Using Hazelcast* section in *Administration Console User Guide for Cisco Unified Intelligence Center* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-intelligence-center/products-maintenance-guides-list.html.

# Cisco Unified Intelligence Center Answer File Generator

Unified Intelligence Center Answer File Generator, a web application, generates answer files for unattended Unified Intelligence Center installations. Individual answer files get copied to the root directory of a USB key or a floppy diskette and are used in addition to the Unified Intelligence Center DVD during the installation process.

The web application supports the following features:

- Allows simultaneous generation and saving of answer files for unattended installs on the publisher server and all subscriber servers.
- Provides syntactical validation of data entries.
- Provides online help and documentation.

The following usage requirements apply:

- The web application supports only fresh installs and does not support upgrades.
- If DHCP client is being used on the publisher server, and subscriber server answer files are also being generated, you must specify the publisher server IP address.

You can access the Cisco Unified Communications Answer File Generator at the following URL:

https://www.cisco.com/c/en/us/applicat/content/cuc-afg/index.html

The Cisco Unified Communications Answer File Generator supports Internet Explorer version 10 and 11 (Compatibility View Mode), and Mozilla Firefox 38.0 ESR and above.

**Note** Cisco requires that you use USB keys that are compatible with Linux 2.6.32 You should use USB keys that are preformatted to be compatible with Linux 2.6.32 for the configuration file. These keys will have a W95 FAT32 format.