



# Installation

---

- [Installation Duration, on page 1](#)
- [Installation Processes, on page 1](#)
- [Installation Failure, on page 2](#)
- [Post Installation, on page 2](#)

## Installation Duration

The installation can take from 60 to 75 minutes to complete and can run unattended for most of that time.

## Installation Processes

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

- Formatting Progress Bars
- Copying File Progress Bar
- Platform Installation Progress Bars (as multiple packages are installed)
- Post Install Progress Bar
- Application Installation Progress Bars (multiple packages are backed up to the archive directory)
- An informational screen saying that the system reboots.



---

**Note** At the start of the reboot, the CD tray holding the DVD ejects. This is usual behavior. You can remove the DVD.

---

- A System Reboot, which includes a second hardware check.

Messages appear during the reboot, some of which 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 opens during the Configure and Setup Network process, click **Review**. Then click **OK** at the Errors screen. Follow the prompts to reenter your hostname, IP Address, and so forth. The installation continues when the connection information is complete.

---

- Member Nodes only - Connection Validation message.
- Security Configuration
- Member Nodes only - A screen stating that there is a successful connection to the first node (select **Continue**).
- The SMTP Host Configuration screen(s). Select **Yes** or **No**, according to your preference.
- Platform Configuration Complete screen. Select **OK**.
- Display of Cryptographic Information screen.
- Application Post-Install Progress Bars

The installation ends at a login prompt, at which you can enter CLI commands.

To access the web interface, you need to open a browser and enter the URL *https://Controller hostname or IP/oamp* and User ID/Password of the System Application user.

#### Related Topics

[Frequently Asked Questions](#)

## Installation Failure

Mount ISO to the virtual DVD drive and perform all steps in Chapter 2, and proceed to *Configure Basic Install*.

If a critical error occurs during installation, you are prompted to collect log files. To do this, insert a USB memory key in any available USB port and follow the instructions on the screen.

If the installation fails over a Virtual Machine. For more information, see *Frequently asked Questions*.

#### Related Topics

[Configure Basic Install](#)

[Frequently Asked Questions](#)

## Post Installation

The action to take after the installation, depends on the type of node you installed.



**Note** After installing the Unified Intelligence Center, you can download the Unified CCE templates from the Download Software page at <https://software.cisco.com/download/release.html?mdfid=282163829&softwareid=282377062&release=8.5.4>. You can then import these templates to Unified Intelligence Center.

If	Then
If you have installed a Controller, and your cluster consists of a Controller node only	The installation is complete.  <ol style="list-style-type: none"> <li>1. Open a browser and enter the URL for your Controller (<i>https://Controller hostname or IP/oamp</i>). This opens the Administration Console. Sign in using the System Application credentials.</li> </ol> <p><b>Note</b> This is not applicable for Live Data and Ids installation.</p>
If you have installed a Controller, and you intend to install a Member	<ol style="list-style-type: none"> <li>1. Open a browser and enter the URL for your Controller (<i>https://Controller hostname or IP/oamp</i>). This opens the Administration Console.</li> <li>2. Sign in using the System Application credentials.</li> <li>3. <i>Define the Member node in the Administration console.</i></li> </ol> <p><b>Note</b> This is not applicable for Live Data and Ids installation.</p>
If you have installed a Member node	Open a browser and enter the URL for your Member <i>https://IP/cuicui/Main.jsp</i> . This opens the Unified Intelligence Center Reporting web page.  Sign in using the System Application credentials.  Until other users are added or integrated, the System Application user has full access to the Unified Intelligence Center Member nodes.  <p><b>Note</b> This is not applicable for Live Data and Ids installation.</p>

If	Then
<p>If you are using self-signed certificates</p>	<p>Prerequisite—Download the Unified Intelligence Center tomcat certificate from Cisco Unified OS Administration page of Unified Intelligence Center.</p> <p>Perform the following tasks to upload the Unified Intelligence Center server certificate to Cisco Finesse.</p> <ol style="list-style-type: none"> <li>1. Sign in to Cisco Unified OS Administration on Cisco Finesse using the following URL:  <a href="https://FQDN of Finesse server:8443/cmplatform">https://FQDN of Finesse server:8443/cmplatform</a>.</li> <li>2. Select <b>Security &gt; Certificate Management &gt; Upload Certificate/Certificate chain</b>.</li> <li>3. From the <b>Certificate Purpose</b> drop-down list, select <b>tomcat-trust</b>.</li> <li>4. In the <b>Upload File</b> field, click <b>Choose File</b> and browse to the tomcat.pem file that you saved on your system.</li> <li>5. Click <b>Upload</b>.</li> <li>6. Restart the Cisco Finesse Tomcat on the Cisco Finesse server.</li> </ol> <p><b>Note</b></p> <ul style="list-style-type: none"> <li>• Follow the same steps for both the Cisco Finesse publisher and subscriber nodes.</li> <li>• 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.</li> </ul> <p>For more information, see the <i>Certificates for Live Data</i> chapter in <i>Cisco Finesse Administration Guide</i> at <a href="https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-maintenance-guides-list.html">https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-maintenance-guides-list.html</a>.</p>

If	Then
<p>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.</p>	<p>Perform the following tasks change the discovery mechanism to <code>tcp-ip</code> mode.</p> <ol style="list-style-type: none"> <li>1. Log in to the Cisco Unified Intelligence Center CLI. Specify the System Administrator username and password.           <p><b>Note</b> Run the following CLIs on all nodes in the given sequence, starting from the publisher node.</p> </li> <li>2. Enter the command <b>utils service stop</b> <i>Intelligence Center Reporting Service</i>.</li> <li>3. Enter the command <b>utils cuic cluster mode</b>.</li> <li>4. Select cluster mode 2) <b>Enable tcp-ip</b>.</li> <li>5. Enter the command <b>utils cuic cluster show</b>.           <p><b>Note</b> Ensure that all nodes have an identical configuration.</p> </li> <li>6. Enter the command <b>utils service start</b> <i>Intelligence Center Reporting Service</i>.           <p><b>Note</b> 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.</p> </li> </ol> <p>For more information, see the <i>Cluster Configuration for JVM Using Hazelcast</i> section in <i>Administration Console User Guide for Cisco Unified Intelligence Center</i> at <a href="https://www.cisco.com/c/en/us/support/customer-collaboration/unified-intelligence-center/products-maintenance-guides-list.html">https://www.cisco.com/c/en/us/support/customer-collaboration/unified-intelligence-center/products-maintenance-guides-list.html</a>.</p>

#### Related Topics

[Define Member Node in Administration Console](#)

