# Frequently Asked Questions About Installation



# Frequently Asked Questions

**Can I install on a virtual machine?**

Starting with Release 8.0(3), you can install Unified Intelligence Center on a virtual machine.

**Can my Cisco Support Provider log in to assist me?**

Yes. There is a utility that allows Cisco technicians to troubleshoot your system, its configurations, and databases.

Set up and enable a time-limited access account to your system using the CLI commands under the `utils remote_account` command or run the utility from the Cisco Unified Operating System Administration Console (select **Services** > **Remote Support**).

The procedure to do this is documented in the online help for the Cisco Unified Operating System Administration Console.

**How do I handle "No Such File or Directory" error?**

During installation on some servers, you might see an error similar to this:

```
rmmod: ohci_hcd: no such file or directory
```

This is a message related to USB driver modules and can be safely ignored.

The installation attempts to delete all modules on the server before loading new ones. If a module does not exist on the server where the installation is running, a message indicates that there is no such file to be deleted. Messages differ slightly for different driver names.

**How do I access log files?**

If you encounter problems with the installation, you can obtain and examine the install log files by entering the following commands in Command Line Interface.

- Enter the CLI command `file list install *` to obtain a list of all install log files from the command line.
- Enter the CLI command `file view install <log_file>` to view the log file from the command line where log_file is the log file name.

Other ways to access log files are as follows:

- Use the CLI file dump commands.
- Use the Syslog Viewer in the Real-Time Monitoring Tool (RTMT). Download RTMT from the Administration console (**Tools** > **RTMT Plugin Download**).

**How do I add or replace devices in the cluster?**

To add a device (for example, to add an additional Member to the cluster):

1. Verify that the virtual machine meets the hardware requirements.
2. Make sure that the other devices in the cluster are up and running.
3. Run a fresh (DVD) installation on the new or replacement device. It must be the same version of Unified Intelligence Center that is currently installed on all other nodes.
4. Test that the new device can connect to the other devices in the cluster. See *How do I test server connectivity?*.

**How do I sign in to the Administration Console?**

1. Direct a browser to the URL for the administration console.

   The URL is `https://<HOST ADDRESS:8443/oamp/` where HOST ADDRESS is the IP address or host name of your controller node with the default port.
2. Enter the System Application user ID and password that you defined during installation.

   This person is the initial, default Super User.

Any Super Users who were added after the installation can also log in.

**How do I sign in to Unified Intelligence Center Reporting?**

There are two ways to do this:

- From the browser:
  1. Direct a browser to the URL for the reporting application.

     The URL is `https://<<host>:8444/cuicui/Main.jsp` where HOST ADDRESS is the IP address or host name of your member node.
  2. Enter your login credentials.
- From the Administration Console:
  1. Open the Control Center page.
  2. Locate the Member you want to access.
  3. Click the Member name to open the sign in page for that Member.
  4. Enter your login credentials.

The System Application user ID and password defined during installation can log in to the Reporting application. Any additional Login Users who have been created and authenticated can also log in.

### How do I switch between Administration Console and Unified Intelligence Center Reporting?

If you are signed in to the Administration Console and wish to redirect your browser to the Unified Intelligence Center Reporting web page:

1. Open **Control Center** > **Device Control**.
2. Locate the Member node you want to access.
3. Click the name for that Member node.

   The name is a link that opens the sign in page for the node.
4. Enter your login credentials.

### How do I access the Command-Line Interface?

You can access the CLI directly from any node, using the monitor and keyboard at the server console.

1. Enter the ID for the System Administrator account created during install.

   See *What accounts and passwords are defined during the installation?*.
2. When prompted, enter the password for the System Administrator account.

The CLI is documented in the *Administration Console User Guide for Cisco Unified Intelligence Center* available at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-intelligence-center/products-maintenance-guides-list.html.

### How do I test server connectivity?

There is a step to test network connectivity during the installation of the Controller and Member servers. You can also run a basic check that one server can connect to another using this CLI command: `utils network ping`. See *Complete Configuration for Member Node*.

### How do I use the Recovery Disk?

The installation package includes a Recovery Disk on CD media to help you to recover from a catastrophic failure, such as an unbootable system.

To use the Recovery Disk, insert it into the tray and boot up into it.

For more information on Server Recovery, see https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/cucm/recovery_cd/Server_Recovery-README.pdf.

**Note** The recovery disk menu option [A] [a] is not supported.

### How do I uninstall?

There is no way to uninstall other than reinserting the installation DVD, which will reformat the hard disk.

### How is data handled during an upgrade?

Data migration occurs during an upgrade installation. This includes the database, configuration properties, and licensing files. See *Where is an upgrade installation installed?*.

**Warning** Do not make configuration changes from the start of the upgrade process until you have activated the inactive partition and re-booted the system.

If you decide to downgrade or switch the system to the inactive partition that contains the older version of the software, any configuration changes that you made since upgrading will be lost.

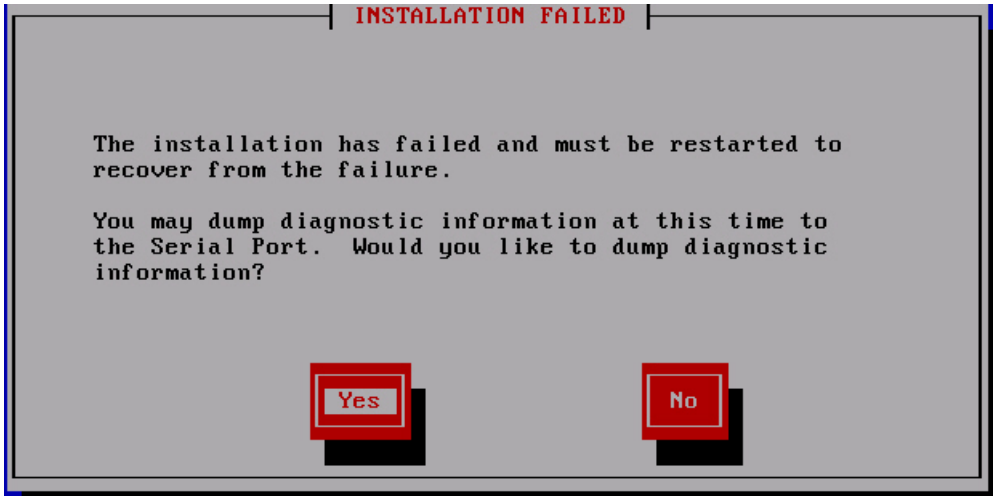
**Is Unified Intelligence Center supported in a hosted deployment?**

Yes, deployment in a hosted environment is qualified and tested. The deployments tested are Unified Intelligence Center with Live Data, Live Data, IdS and Unified Intelligence Center only.

**What if the installation fails?**

If the installation fails, you see a screen asking if you want to copy diagnostic information to a device.

***Figure 1: Installation Failed Screen***




1. Insert a USB key.
2. Select **Yes**.
3. Select **Continue** at the next two screens.

**Note** The CLI command to view the install logs is file view install.

The CLI is documented in the *Administration Console User Guide for Cisco Unified Intelligence Center* available at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-intelligence-center/products-maintenance-guides-list.html.

If the installation fails over a virtual machine, you see a screen asking if you want to copy diagnostic information to a device.

**Which accounts and passwords are defined during the installation?**

During the installation, you specify three passwords: the System Administrator user, the System Application user, and the database access security password. All three must start with an alphabetic

character, must be at least six characters long, and can contain alphanumeric characters, hyphens, and underscores. Only the application user and password are passed to the online Administration console.

- **System Administrator account:** The System Administrator account User ID and password are configured at installation for each node. Enter the same user name and password for all nodes. The System Administrator for the Controller can access:
  - The CLI for the Controller.
  - The Cisco Systems tools on the Navigation dropdown in the Administration console: Disaster Recovery System, Cisco Unified Serviceability, and Cisco Unified OS Administration interfaces.

  The System Administrator has no access to functions in the Unified Intelligence Center reporting application.

  **Note** If you configure unique System Administrator credentials for Member nodes, you must use those credentials to access the CLI for those Member servers only.

- **System Application User account:** The System Application account User ID and password are configured at installation for each node. Enter the same user name and password for all nodes.

  The System Application user name and password that are configured for the Controller allow an initial login to the Administration console. This user becomes that initial Super User and, once the license is applied, can log in to the Unified Intelligence Center Reporting application on all Member nodes.

  As the initial Super User, the System Application User can create additional Super Users in the User Management screen or by using the CLI command set account. This user can also sign in to the Unified Intelligence Center Reporting interface with full access to all functions.

  The initial Super User (the System Application user) created in the installation does not need to be set up in Active Directory. Any additional Super Users created through the Administration console are considered to be IMS users. They can sign into Unified Intelligence Center Reporting and will be limited to the Login User role until they are given additional privileges.

  **Note** If you configure unique System Application credentials for Member nodes, those users have no login rights.

- **Security Password:** The security password defined in the installation wizard is used by the system for the database security password to authorize communications between devices. This password is identical on all servers in the cluster. The security password is also used by the Disaster Recovery System (DRS) for encryption of the backup file.

  You can change the security password using the CLI command set password security.

### How do I dump install logs to the serial port of the virtual machine?

1. Configure a serial port on the virtual machine.

   While the virtual machine is powered OFF, edit settings and add a serial port to the virtual machine. You cannot add a serial port while the virtual machine is running. Attach the serial port to a .tmp file, and then power on the virtual machine and start the install.

2. When you are ready to dump the log files, attach a new, empty file to the serial port.

   If the system halts due to an install failure and asks if you want to dump the logs, before you answer yes, you must edit settings on the virtual machine and attach the actual file name where you want to dump the logs. The reason for originally attaching the .tmp file to the serial port is that during the boot-up of Linux, a few garbage characters (terminal escape sequences) get output to that port. If you dump the logs into that file, these characters will corrupt the .tar format of the file. In order to create a valid .tar file, you must connect the serial port to a new and empty file just before you dump the logs to it.

3. Return to the virtual machine console and proceed to dump the logs to the serial port.

   After the file is complete, open it with 7-zip, which you can download from http://www.7-zip.org/download.html.

4. After a successful install, power off the virtual machine, edit settings, and remove the serial port from the virtual machine.

**Important** Leaving the serial port (or any other virtual hardware) can negatively impact performance of the virtual machine. The serial port has no other use other than dumping the install logs and you will not need it again, unless you perform a fresh install.

### What do I do if the upgrade stalls?

During the installation of upgrade software, the upgrade may appear to stall. The upgrade log stops displaying new log messages. When the upgrade stalls, you must cancel the upgrade, disable I/O throttling, and restart the upgrade procedure. When you successfully complete the upgrade, you do not need to reenable I/O throttling.

- To disable I/O throttling, enter the CLI command `utils iothrottle disable`.
- To display the status of I/O throttling, enter the CLI command `utils iothrottle status`.
- To enable I/O throttling, enter the CLI command `utils iothrottle enable`. By default, iothrottle is enabled.

If the system does not respond to the cancellation, you must reboot the server, disable I/O throttling, and restart the upgrade process procedure.

### Where is a fresh installation installed?

All Controller servers have an active bootable partition, an inactive bootable partition, and a common partition. The installation creates these partitions, and a fresh (first-time) installation places the new software and operating system on the active partition. The system boots up and operates on the active partition.

### Where is an upgrade installation installed?

All Controller servers have an active bootable partition, an inactive bootable partition, and a common partition. Upgrade versions are installed on the inactive partition.

To complete the upgrade, you switch partitions using the CLI command `utils system switch-version`.

You can also do this from the Cisco Unified Communications Operating System Administration screen. Navigate to **Settings** > **Version**. This opens the **Version Settings** screen, which shows the software version on both the active and inactive partitions. To switch versions and restart, click **Switch Versions**.

When the system restarts, it boots to the now-active (formerly inactive) partition with your migrated data in place. For more information, see *Upgrades*.

**What is the supported screen resolution?**

Supported screen resolution for Cisco Unified Intelligence Center: 1366 x 768 or higher.

**Related Topics**

Before You Upgrade