



Preparation

- [Scenarios, on page 1](#)
- [System Requirements, on page 3](#)

Scenarios

Cisco Unified Contact Center Enterprise (Unified CCE) is supported only in a virtualized environment.



Note This Cisco Unified Contact Center Enterprise Installation and Upgrade Guide provides the Install and Upgrade details and procedures for both 12.5(1) release and 12.5(2) maintenance release.

Installation Scenario

The Unified CCE components are supported on the following platform in 12.5(1) release.

- Microsoft Windows Server 2016 and Microsoft SQL Server 2017

The CCE components are supported on the following platforms in 12.5(2) release.

- Microsoft Windows Server 2016 and Microsoft SQL Server 2017
- Microsoft Windows Server 2019 and Microsoft SQL Server 2019



Note The cross combination of platforms is not supported. For example, Windows Server 2016 with SQL Server 2019 or Windows Server 2019 with SQL Server 2017.

In a virtualized environment, you can run Unified CCE on a VMware ESXi platform. Run the virtual machines (VMs) on Cisco Unified Computing System (UCS) C-series servers, or equivalent third-party servers.

Install the Unified CCE components after you configure the VMs.

You can use the OVA template to deploy the VMs before beginning with the installation of Unified CCE components.



Note Deploying VM with Guest Operating System ‘Microsoft Windows Server 2019’ on ESXi 7.0 using CCE OVA template displays a warning message, “The configured guest OS (Microsoft Windows Server 2016 or later (64-bit)) for this virtual machine does not match the guest that is currently running (Microsoft Windows Server 2019 (64-bit)). You should specify the correct guest OS to allow for guest-specific optimization”. This warning message is informational only and has no detrimental effect on the system. This warning message is displayed only once and can be ignored.

The Unified CCE 12.5(2) installer is available as an add-on release to Unified CCE 12.5(1). Therefore, complete the installation of the base Unified CCE 12.5(1) before applying Unified CCE 12.5(2).



Note During Unified CCE installation on Windows Server 2019 and SQL Server 2019, SQL Server Security Hardening optional configuration should not be selected as part of the installation steps. Unified CCE services should be started only after installing Unified CCE 12.5(2) for Windows Server 2019 and SQL Server 2019 support. The SQL Security Hardening can be applied post installation using the Security Wizard tool.

Common Ground Upgrade is not supported if the platform upgrade from Windows Server 2016 and SQL Server 2017 to Windows Server 2019 and SQL Server 2019 is planned as part of upgrade process.

Technology Refresh Upgrade is the supported upgrade option for platform upgrade. Fresh Install on Windows Server 2019 and SQL Server 2019 is supported. Fresh Install, Common Ground Upgrade, and Technology Refresh Upgrade is supported for Microsoft Windows Server 2016 and Microsoft SQL Server 2017 platform, where platform upgrade is not planned.

Upgrade Scenarios

Upgrading to Unified CCE 12.5(2) from Unified CCE 12.5(1) is the same as upgrading or applying any other maintenance release.

You can upgrade from Unified CCE 12.0(1) to Unified CCE 12.5(1) or Unified CCE 12.5(2) by using one of the following two methods:

- **Common Ground Upgrades:** The Common Ground method is an in-place upgrade performed on your existing virtual machine which involves upgrading the Cisco Unified Contact Center Enterprise and all other associated software that is hosted on it. If your hardware meets the requirements for this release, you can perform a Common Ground upgrade without acquiring extra hardware.



Note Common Ground Upgrade is not supported if the platform upgrade from Windows Server 2016 and SQL Server 2017 to Windows Server 2019 and SQL Server 2019 is planned as part of upgrade process.

- **Technology Refresh Upgrades:** Use the Technology Refresh upgrade method to upgrade your hardware at the same time as the Cisco Unified Contact Center Enterprise system. When using the Technology Refresh method, you prepare a destination system on new hardware and then migrate data from your existing deployment to the new one.

Follow the documented procedures to build a parallel network using new hardware and pre-stage it with configuration data to support the existing production network. Use the Enhanced Database Migration Tool (EDMT) to transfer data and perform a schema upgrade during the upgrade process. Do not use backup and restore procedures to perform the pre-staged configuration on the parallel network.

Upgrade scenarios are considered at a component level; you can perform one type of upgrade on one component, and another type of upgrade on another component. However, the A and B side of any given component must be running on identical hardware.

Follow the task flow and tasks for the upgrade scenario that applies to each individual component involved in the overall upgrade.

The upgrade from Unified CCE 12.0(1) to Unified CCE 12.5(1) or Unified CCE 12.5(2) is specific to Unified CCE components (for example, Router, peripheral gateway, and so on).

Refer Fresh Install or Technology Refresh Upgrade section for details on prerequisites for installing Unified CCE components on Windows Server 2019 and SQL Server 2019 platform.



Note While upgrading from previous versions of Unified ICM / Unified CCE using the base installer for the current release, make sure that there are no other Windows sessions that are active. These sessions may have inadvertently left some Unified CCE tools like Configuration Manager open. This can prevent the tools from getting upgraded appropriately and this can cause the tool to malfunction or assert. The installer logs indicate that some files were locked, during the upgrade. To resolve the issue with these tools that were not upgraded, you need to re-run the base installer and ensure that no other windows sessions are open.

System Requirements

Before you start installation or upgrade activities, plan your Unified CCE contact center installation or upgrade. For system requirements, see the Compatibility Matrix at <https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-device-support-tables-list.html>.

By default, Windows Defender is enabled on Windows Server. For more information on Windows Defender antivirus compatibility, see <https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-antivirus/windows-defender-antivirus-compatibility>.

Before proceeding with Unified ICM application installation, ensure that you follow the antivirus guidelines specified in the Section, Antivirus Guidelines of the Security Guide for Cisco Unified ICM/Contact Center Enterprise at <https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-and-configuration-guides-list.html>.

Unified ICM installation can also take longer than expected due to scanning of files by Windows Defender. Based on your IT policy, either:

- Disable Windows Defender. For more information, see Disable Microsoft Defender Antivirus procedure in Microsoft documentation.

-OR-

- Add the Unified ICM product folder **<ICM install directory:>\icm** to the exclusion list of Windows Defender. For more information, see <https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-antivirus/configure-extension-file-exclusions-windows-defender-antivirus>.

On Logger, Rogger, AW, and HDS servers, the Unified CCE Installer adds BUILTIN\Administrators to SQL security logins and assigns **sysadmin** role to it. This is required for **Logger** and **Administration & Data Server** services to function appropriately.

Ensure that the system is ready, and meets all requirements for supported hardware and software.

This section provides a summary of the requirements for Unified CCE. If you have not confirmed all the information in this section, complete the planning phase before proceeding further.

For more information, see these documents:

- *Solution Design Guide for Cisco Unified Contact Center Enterprise* at http://www.cisco.com/en/US/products/sw/custcosw/ps1844/products_implementation_design_guides_list.html
- *Virtualization for Unified Contact Center Enterprise* at https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/cisco-collaboration-virtualization.html
- *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>

Platform Requirements

Server selection for Unified CCE in a virtualized environment involves several factors, including:

- The server and all related hardware must be supported for use in a virtualized Unified CCE system
- Minimum specifications for processing, memory, and storage
- Whether you want a packaged and tested Cisco configuration (Tested Reference Configuration or TRC) or a configuration that you base on Cisco-defined minimum requirements (Specs-based Configuration)
- Compatibility requirements for all hardware, and Cisco and third-party software including the VMware required to run and manage a virtual environment

Confirm that your hardware selection is supported for Unified CCE and meets all minimum specifications:

Server	VMware required	For detailed requirements information, see
UCS C-series (TRC):	<ul style="list-style-type: none"> • VMware vSphere ESXi • VMware vCenter (Optional) 	<i>Virtualization for Unified Contact Center Enterprise</i> at https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/cisco-collaboration-virtualization.html
UCS C-series (Specs-based):	<ul style="list-style-type: none"> • VMware vCenter • VMware vSphere ESXi 	
Third-party (Specs-based)	<ul style="list-style-type: none"> • VMware vCenter • VMware vSphere ESXi 	

In addition to confirming that your servers meet minimum specifications, confirm that your server choice is compatible with all Cisco and third-party software.

Related Topics

[Compatibility Requirements](#), on page 6

Network Requirements

Network requirements for virtualized Unified CCE systems vary widely, depending on the size and type of Unified CCE solution deployment. Confirm that you have clearly established all network requirements before you install or upgrade a Unified CCE contact center.

For more information, see *Virtualization for Unified Contact Center Enterprise* at https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/cisco-collaboration-virtualization.html.

Transport Layer Security Version 1.2 Required

Contact center enterprise solutions require the use of TLS 1.2 only connections in this release. Our services accept incoming TLS connections only over TLS 1.2. All outgoing TLS connection use only TLS 1.2.

All clients that connect to either our web interfaces or databases must support TLS 1.2.



Note The older versions of the TLS/SSL are disabled by installer.

For more information 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>.

Software License Requirements

Third-Party Products



Note For detailed information about the software editions and versions supported for this release, see the *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>.

Before you begin an installation or upgrade of any part of your contact center, confirm the following:

- That you have all the required software products.
- That all the software versions are compatible with each other.
- That all software versions are also compatible with all hardware and VMware.

Virtualization Requirements

You run the Unified Contact Center Enterprise solution on VMware ESXi platform.

The following requirements apply to VMware on virtual machines for Unified CCE:

- After you install the Unified CCE components on each VM, install the latest VMware Tools from your VMware host using the VMware Tool default settings.



Note Update the VMware Tools whenever you patch or upgrade ESXi.



Note Deploying VM with Guest Operating System ‘Microsoft Windows Server 2019’ on ESXi 7.0 using CCE OVA template displays a warning message, “The configured guest OS (Microsoft Windows Server 2016 or later (64-bit)) for this virtual machine does not match the guest that is currently running (Microsoft Windows Server 2019 (64-bit)). You should specify the correct guest OS to allow for guest-specific optimization”. This warning message is informational only and has no detrimental effect on the system. The warning message is displayed only once and can be dismissed.

For more information, see *Virtualization for Unified Contact Center Enterprise* at https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/cisco-collaboration-virtualization.html.

Related Topics

[Install VMware Tools for Windows](#)

ESXi Supportability

For information on supported versions of ESXi for this release 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>.

As part of the Common Ground upgrade process, if there are no available overlapping supported ESXi versions, upgrade the Unified CCE software first if a back-out of the upgrade is required.

If the upgrade is successful and working, you can then proceed to upgrade ESXi to a supported version for final testing and restoring production operation.

Compatibility Requirements

As part of the planning process, ensure that all hardware, Cisco software, third-party software, VMware, and firmware are compatible. Confirm that you meet all the following compatibility requirements:

For this compatibility information	See
VMware and Cisco software components	<i>Virtualization Software Requirements</i> at http://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-software-requirements.html

For this compatibility information	See
Required firmware	<p>See the following:</p> <p><i>VMware Compatibility Guide</i> at http://www.vmware.com/resources/compatibility/search.php.</p> <p>For more information, see <i>Virtualization for Unified Contact Center Enterprise</i> at http://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-unified-contact-center-enterprise.html.</p> <p>Cisco Installation and Upgrade Guides at http://www.cisco.com/c/en/us/support/servers-unified-computing/ucs-c-series-rack-servers/products-installation-guides-list.html</p>
Cisco software product intercompatibility	<p><i>Contact Center Enterprise Compatibility Matrix</i> at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-device-support-tables-list.html</p> <p>Note Review the compatibility between different versions of the Cisco components to plan upgrades that occur across multiple maintenance windows. Components that are upgraded in one maintenance window must continue to operate with other components that are still at the previous version until the full upgrade is completed.</p>
Windows OS and SNMP <ul style="list-style-type: none"> • SNMP Service • SNMP MI Provider 	<p>See the following:</p> <p><i>SNMP Guide for Cisco Unified ICM/Contact Center Enterprise</i> at http://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-and-configuration-guides-list.html</p> <p><i>Serviceability Guide for Cisco Unified ICM/Contact Center Enterprise</i> at http://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-and-configuration-guides-list.html</p>
Third party software products	<p><i>Contact Center Enterprise Compatibility Matrix</i> at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-device-support-tables-list.html</p>

Java Requirements

A new 12.5(1a) base installer is available for customers, which has OpenJDK JRE as the supporting Java run time for all the CCE applications. Its predecessor the 12.5(1) installer employs Oracle JRE. Any installation done using the 12.5(1) installer can continue to use Oracle JRE, and can receive Java security updates and fixes from the Oracle website.

However, if there is a need to apply an ES on 12.5(1) that mandates the installation of ES55 (mandatory OpenJDK ES), then the Java updates would have to be downloaded and installed from the OpenLogic website.

CCE VMs installed using the 12.5(1a) installer would need the OpenJDK patches applied. You can verify the base installer version to be 12.5(1a) from **Control Panel > Programs > Programs and Features > Cisco Unified ICM/CCE 12.5.1a**.

Certificate Management Requirements

During installation of 12.5(2), Unified CCE installs the Java version 8 update 332. If your system has a Java version that is lower than version 8 update 332, perform the following steps:

Procedure

Step 1

Before you install 12.5(2):

a) Run the command at the command prompt: `cd %CCE_JAVA_HOME%\bin.`

Important Use %JAVA_HOME% if you are employing Oracle JRE.

b) Export the certificates of all the components imported into the truststore.

c) The command to export the certificates is `keytool -export -keystore <JRE path>\lib\security\cacerts -alias <alias of the component> -file <filepath>.cer`

d) Enter the truststore password when prompted.

Step 2

After 12.5(2) installation is complete, perform the following steps:

a) Run the command at the command prompt: `cd %CCE_JAVA_HOME%\bin.`

b) Import the certificates for all the components that you previously exported from the truststore before you installed 12.5(2). The command to import certificates is `keytool -import -keystore <JRE path>\lib\security\cacerts -file <filepath>.cer -alias <alias>.`

c) Enter the truststore password when prompted.

d) Enter 'yes' when prompted to trust the certificate.
