Preinstallation

Preinstallation Task Flow

Before you can install Unified CCE and the associated components, set up the network, create virtual machines, and install and configure third-party software.

Important The length of the hostname of any Unified CCE server must not exceed 24 characters.

Task	See
If you are integrating Unified CCE into an existing corporate network, verify Domain Controller health. If you are installing into a new Active Directory domain, install and configure Active Directory and DNS server.	Set up Active Directory, on page 1
Download Open Virtualization Format (OVA) templates and create virtual machines.	Set Up Virtual Machines, on page 2
Install and configure third-party software.	Set Up Third-Party Software, on page 6

Preinstallation Tasks

Set up Active Directory

Ensure that you have a completed plan for your domain structure and Active Directory implementation before you set up your network.

Warning The Unified CCE servers should be in the same domain, and multiple domains are not supported.

For more information, see the *Staging Guide for Cisco Unified ICM/Contact Center Enterprise* at http://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.html.

Set Up Virtual Machines

Verify Datastores

Before you install the VMs, verify that the datastore is in place. The type of datastore depends on the type of server on which you deploy the VMs. For example, UCS-B servers use a SAN datastore and UCS-C servers use DAS datastores.

For more information, see the VMware documentation at https://www.vmware.com/support/pubs/.

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/virtualization-unified-contact-center-enterprise.html.

Configure HyperFlex M5 Series and M6 Series

Cisco HyperFlex HX-Series System provides a unified view of the storage across all nodes of the HyperFlex HX cluster via the HX Data Controller Platform. For optimal performance, it is recommended that all VMs are mapped to the single unified datastore. This mapping enables the HX Data Platform to optimize storage access based on the workload and other operating parameters.

For more information, see the documentation on Cisco HyperFlex HX Data Platform at https://www.cisco.com/c/en/us/support/hyperconverged-systems/hyperflex-hx-data-platform-software/products-installation-guides-list.html.

For information on installing collaboration software, see the *Cisco Collaboration on Virtual Servers* at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-guides-list.html.

Configure RAID for Cisco UCS C240 M5SX and Cisco UCS C240 M6SX

The disk array configuration for the Cisco UCS C240 M5SX and Cisco UCS C240 M6SX is already set up to match the requirements. Verify the settings as follows:

Procedure

Using Cisco Integrated Management Controller, check that the following settings are configured correctly:

- Virtual Drive Info: RAID 5 with 6 (Physical Disks) * 4 (Virtual Drives or Datastores)
- Stripe Size: 128KB
- Write Policy: Write Back with BBU
- Read Policy: Read Ahead Always

For more information regarding RAID configuration for Cisco UCS C240 M5SX or Cisco UCS C240 M6SX, see the *Installation and Configuration* section of the Cisco Collaboration on Virtual Servers Guide.

Download Unified CCE OVA Files

The Unified CCE Open Virtualization Format (OVA) files define the basic structure of the corresponding VMs that are created. The structure definition includes the CPU, RAM, disk space, reservation for CPU, and reservation for memory.

Before you begin

You must have a valid service contract associated with your Cisco.com profile.

Procedure

Step 1 Go to the Unified CCE Download Software page on Cisco.com.

Step 2 Click **Download** to download and save the appropriate OVA file to your local hard drive. When you create VMs, you select the OVA required for the application.

Create a Virtual Machine from the OVA

To create virtual machines (VMs) from the OVA files, complete the following procedure.

Note ECE requires a second virtual hard drive on its VM. The OVA creates one virtual hard drive. Create a second hard drive of an appropriate size for your solution requirements.

Procedure

Step 1 Select the host in the vSphere client and click **Deploy OVF Template**.

Step 2 On the **Select an OVF template** page, browse to the location on your local drive where you stored the OVA. Click **Open** to select the file. Click **Next.**

Step 3 On the **Select a name and folder** page, enter a name for the virtual machine and then choose the location for the virtual machine.

Important The virtual machine name cannot contain spaces or special characters. Enter a maximum of 32 characters. After the VM is created, you cannot rename it.

Step 4 Click **Next**.

Step 5 On the **Select a compute resource** page, select the destination compute resource. Click **Next.**

Step 6 On the **Review details** page, verify the OVF template details.

Step 7 On the **Configuration** page, select the applicable configuration from the available list. Click **Next**.

Step 8 On the **Select storage** page, ensure that the virtual disk format is **Thick provision Lazy Zeroed** and then choose a datastore on which you want to deploy the new virtual machine. Click **Next.**

Note **Thick provision Eager Zeroed** is also supported, but **Thin provisioned** is not supported.

For each datastore, the following tables describe the RAID group, the ESXi Host, and the virtual machines for the Cisco UCS C240 M4SX, Cisco UCS C240 M5SX, and Cisco UCS C240 M6SX servers.

RAID configuration for the Cisco UCS C240 M4SX, Cisco UCS C240 M5SX, and Cisco UCS C240 M6SX

RAID Group	VM Datastore	ESXi Host	Virtual Machines
VD0	datastore 1	A	ESXi operating system Unified CCE Rogger, Side A Unified Communications Manager Publisher Cisco Finesse Primary
VD1	datastore 2	A	Unified CCE AW-HDS-DDS, Side A
VD2	datastore 3	A	Unified Communications Manager Subscriber 1 Unified CVP OAMP Server Unified CVP Server, Side A
VD3	datastore 4	A	Unified Intelligence Center Server Publisher Unified CCE PG, Side A
VD0	datastore 1	B	ESXi operating system Unified CCE Rogger, Side B Unified Communications Manager Subscriber 2 Cisco Finesse Secondary
VD1	datastore 2	B	Unified CCE AW-HDS-DDS, Side B
VD2	datastore 3	B	Unified Customer Voice Portal Reporting Server (optional) Unified CVP Server, Side B
VD3	datastore 4	B	Unified Intelligence Center Server Subscriber Unified CCE PG, Side B Enterprise Chat and Email Server (optional)

Step 9 On the **Select networks** page, select the destination network:

a) Public network adapter to Public network

b) Private network adapter to Private network

Note Certain VMs do not require a private network connection. The OVAs for those VMs do not create a second network adapter.

Step 10 On the **Ready to complete** page, click **Finish** to create the VM.

Note For more information, see *Virtualization for Unified Contact Center Enterprise* at http://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-unified-contact-center-enterprise.html.

Allocate a Second Virtual Hard Drive

After deploying the OVA files, the second hard drive is no longer automatically created. To create a second hard drive:

Procedure

Step 1 Right-click the virtual machine and click **Edit Settings**.

Step 2 In the **Virtual Hardware** tab, click on **Add New Device**.

Step 3 You can select the type of device you wish to add. Select **Hard Disk**. The new hard disk appears. Assign the desired disk space to the hard disk.

Note Virtual machine templates for Logger, Rogger, AW, and HDS servers do not have a SQL database drive preprovisioned. The following reference table can be used to assign disk space to the virtual machine based on the type:

Virtual Machine Template	Default Second Disk Size
Logger	500 GB
Rogger	150 GB
AW-HDS-DDS	500 GB
AW-HDS	500 GB
HDS-DDS	500 GB

You can custom size the SQL database disk space to meet data retention requirements, as calculated by the Database Estimator tool.

Step 4 On the **Disk Provisioning** section, choose **Thick provision Lazy Zeroed**.

Step 5 In the **VM Options** > **Advanced Options** section, retain the default options.

Step 6 Click **OK** to confirm the changes.

The Recent Tasks window at the bottom of the screen displays the progress.

Mount ISO Files

Upload ISO image to data store:

1. Select the host in the vSphere client and click **Configuration**. Then click **Storage** in the left panel.
2. Select the datastore that will hold the ISO file.
3. Right click and select **Browse datastore**.
4. Click the **Upload** icon and select **Upload file**.
5. Browse to the location on your local drive where you saved the ISO file, and upload the ISO to the datastore.

Mount the ISO image:

1. Right-click the VM in the vSphere client and select **Edit virtual machine settings**.
2. Click **Hardware** and select **CD|DVD Drive 1**.
3. Check **Connect at power on** (Device status panel upper right).
4. Click the **Datastore ISO File** radio button and then click **Browse**.
5. Navigate to the data store where you uploaded the file.
6. Select the ISO file and click **OK**.

Unmount ISO File

Procedure

Step 1 Right-click the virtual machine in the vSphere client and select **Edit virtual machine settings**.
Step 2 Click **Hardware** and select **CD/DVD Drive 1**.
Step 3 Select **Client Device** and click **OK**.

Set Up Third-Party Software

Install Microsoft Windows Server

Complete the following procedure to install Microsoft Windows Server on the virtual machines deployed.

Note For information about supported editions, 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

Procedure

Step 1 Mount the Microsoft Windows Server ISO image to the virtual machine.

Check the **Connect at power on** check box when mounting the ISO.

For more information, see *Mount and Unmount ISO File*.

Step 2 Power on the VM.

Step 3 Enter the Language, Time and Currency Format, and Keyboard settings. Click **Next**.

Step 4 Click **Install Now**.

Step 5 If prompted, enter the product key for Windows Server and click **Next**.

Step 6 Select the Desktop Experience option for the Windows Server and click **Next**.

Step 7 Accept the license terms and click **Next**.

Step 8 Select **Custom: Install Windows only (advanced)**, select **Drive 0** to install Microsoft Windows Server, and then click **Next**.

The installation begins. After the installation is complete, the system restarts without prompting.

Step 9 Enter and confirm the password for the administrator account, and then click **Finish**.

Step 10 Enable Remote Desktop connections as follows:

a) Navigate to **Control Panel** > **System and Security** > **System**.
b) Click **Remote Settings**.
c) Click the **Remote** tab.
d) Select the **Allow remote connections to this computer** radio button. The Remote Desktop Connection dialog displays a notification that the Remote Desktop Firewall exception is enabled. Click **OK**.

Step 11 Install VMWare tools. See Install Vmware Tools, on page 8.

Step 12 Open the **Network and Sharing Center**, and in the View your active networks section, click **Ethernet**.

Step 13 In the Ethernet Status window, click **Properties**.

Step 14 In the **Ethernet Properties** dialog box, configure the network settings and the Domain Name System (DNS) data:

a) Uncheck **Internet Protocol Version 6 (TCP/IPv6)**.
b) Select Internet Protocol Version 4 (TCP/IPv4) and click **Properties**.
c) Select **Use the following IP Address**.
d) Enter the IP address, subnet mask, and default gateway.
e) Select **Use the following DNS Server Address**.
f) Enter the preferred DNS server address, and click **OK**.

Step 15 Navigate to **Control Panel** > **System and Security** > **System**. Follow the instructions:

a) Click**Change Settings**.
b) In Computer name tab, click **Change**.

c) Change the name of the computer from the name randomly generated during Microsoft Windows Server installation. The name does not contain underscores or spaces.
d) Select **Domain** radio button to change the member from Workgroup to Domain.
e) Enter qualified domain name and click **OK**.
f) In the Windows security dialog, validate the domain credentials and click **OK**.
g) On successful authentication, click **OK**.
h) Reboot the server and sign in with domain credentials.

Restart your system for the change to take effect.

Step 16 Go to **Settings** > **Update & Security** and run Microsoft Windows Update.

Microsoft Windows Server is installed. In addition, Internet Explorer 11 is installed automatically.

Note If you want to install Unified CCE on a multilingual version of Windows Server, refer to Microsoft documentation for details in installing Microsoft Windows Server Multilingual language packs.

If Unified CCE language pack is applied on Chinese Windows OS machine, set the screen resolution to 1600 x 1200.

Set Windows Locale

If the Windows system locale differs from the display language (and therefore also the SQL collation setting), some characters appear incorrectly in the user interface and are saved incorrectly to the database. For example, if the system locale is English and an agent works in Spanish, characters such as the acute *a* do not appear correctly.

If you use a multilingual version of Microsoft Windows Server, complete this procedure to set the Windows locale.

Procedure

Step 1 Open **Control Panel** > **Clock, Region and Language**.
Step 2 In the Region section, click **Change date, time, or number formats**.
Step 3 Click the **Administrative** tab.
Step 4 In the Language for non-Unicode programs section, click **Change system locale**.
Step 5 In the **Region Settings** window, select the language that matches the display language.
Step 6 Restart the virtual machine.

Install Vmware Tools

VMware Tools is a suite of utilities that enhance the performance of the virtual machine guest operating system. It also aids virtual machine management.

Note The AppInfo feature provided by the VMware tools has to be disabled. For instructions to disable the AppInfo feature, see the VMware documentation.

Install VMware Tools for Windows

Procedure

Step 1 From the vSphere Client, right-click the virtual machine, select **Power**, and click **Power On**.

Step 2 Click the **Summary** tab.

In the General section, the VMware Tools field indicates whether VMware Tools are:

- installed and current
- installed and not current
- not installed

Step 3 Click the **Console** tab to make sure that the guest operating system starts successfully. Log in if prompted.

Step 4 Right-click the virtual machine, select **Guest OS**, and then click **Install/Upgrade VMware Tools**. The **Install/Upgrade VMware Tools** window appears with the option - Interactive Tools Upgrade and Automatic Tools Upgrade.

a) To install/upgrade the VMware tools manually, select the **Interactive Tools Upgrade** option, and click **OK**. Follow the on-screen instructions to install/upgrade the VMware tools, and restart the virtual machine when prompted.

b) To install/upgrade the VMware tools automatically, select the **Automatic Tools Upgrade** option, and click **OK**. This process takes a few minutes to complete, and restart the virtual machine when prompted.

Initialize and Format Secondary Disk

After the second hard disk is created, allocate memory to the hard disk.

Procedure

Step 1 Open the command prompt, and type **`diskmgmt.msc`**.

Step 2 Right-click **Disk 1**, and click **Online**.

Step 3 After the disk goes online, right-click the disk, and then click **Initialize Disk**.

Step 4 Select **Master Boot Record (MBR)** radio button.

Step 5 After the disk is initialized, right-click the disk, and then click **Convert to Dynamic Disk**.

Step 6 In the **Convert to Dynamic Disk** window, check the **Disk 1** check box to select it, and then click **OK**.

Step 7 Right click on the unallocated disk space, and click **New Simple Volume**. The **New Simple Volume** Wizard window appears.

Step 8 Click **Next** and follow the on-screen instructions to create a simple volume on the disk.

Step 9 Click **Finish** to complete the process of allocating memory to the hard drive.

Install Microsoft SQL Server

Install Microsoft SQL Server and store the SQL Server log and temporary files on the same vDisk as the operating system when using **default** (two) vDisk design. If you choose to use more than two virtual disks, then the tempDB cannot be on the same vDisk as the solution database.

For further information about the database placement and performance tuning the SQL installation, see the Microsoft documentation.

Note For information about supported editions, 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

Note Microsoft SQL Server does not contain SQL Server Management Studio in the default toolkit. To rerun the SQL Server setup to install Management Studio, navigate to: **SQL Selection Center** > **Installation** > **Install SQL Server Management Tools**. If your computer has no internet connection, download and install SQL Server Management Studio manually.

VC++ 2017 `build# 14.12.25810` is not compatible with the Cisco Contact Center Enterprise, ensure that it is not installed.

Procedure

Step 1 Mount the Microsoft SQL Server ISO image to the virtual machine. For more information, see Mount ISO Files, on page 6.

Step 2 Select **Installation** in the left pane and then click **New SQL Server stand-alone installation or add features to an existing installation**. Click **OK**.

Step 3 On the **Product Key** page, enter the product key and then click **Next**.

Step 4 Accept the **License Terms** and then click **Next**.

Step 5 Optional: On the **Microsoft Update** page, check the **Use Microsoft Update to check for updates** check box, and then click **Next**.

Note If you do not check the **Use Microsoft Update to check for updates** option, click **Next** on the **Product Updates** page.

Step 6 On the **Install Rules** page, click **Next**.

In this step, the installation program checks to see that your system meets the hardware and software requirements. If there are any issues, warnings or errors appear in the **Status** column. Click the links for more information about the issues.

Step 7 On the **Feature Selection** page, select only the following, and click **Next**:

- **Database Engine Services**
- **Client Tools Connectivity**
- **Client Tools SDK**
- **SQL Client Connectivity SDK**

Step 8 On the **Instance Configuration** page, select **Default Instance** and click **Next.**

Step 9 On the **Server Configuration** page, click the **Services Account** tab.

a) Associate the SQL services with the virtual account.

- For the SQL Server Database Engine, in the Account Name field, select **NT Service\MSSQLSERVER**.

Note While you can use the Network or Local Services account instead of the Virtual account, using the Virtual account provides security.

b) For the remaining services, accept the default values.

c) In the **Start Up Type** column, for the **SQL Server Agent service** account, select **Automatic** from the list.

d) Enable **Grant Perform Volume Maintenance Task privilege to SQL Server Database Engine Service**.

Note Unified ICM Installer automatically enables the **Grant Perform Volume Maintenance Task** for the NT service account.If it is not enabled automatically then you must enable **Grant Perform Volume Maintenance Task privilege to SQL Server Database Engine Service** manually on the SQL server.

Step 10 On the **Server Configuration** page, click the **Collation** tab.

a) In the Database Engine section, click **Customize**.

b) Select the **Windows Collation designator and sort order** radio button.

c) Select the appropriate collation. Typically, you choose the SQL Server collation that supports the Windows system locale most commonly used by your organization; for example, "Latin1_General" for English.

The database entry is related to the collation that you select. For example, if you set the collation for Latin1_General, but you select Chinese language at sign-in. When you enter field values in Chinese, the application displays the `unsupported character` error, because the database does not support the characters.

Important It is critical to select the correct collation setting for the language display on your system. If you do not select the correct collation during installation, you must uninstall and reinstall Microsoft SQL Server.

d) Check the **Binary** check box.

e) Click **OK**, and then click **Next**.

Step 11 On the **Database Engine Configuration** page:

a) On the Server Configuration tab, click the **Mixed Mode** radio button.

b) Enter the password for the SQL Server system administrator account, and confirm by reentering it.

c) Click **Add Current User** to add the user who is installing the SQL Server as an administrator.

d) On the **TempDB** tab, set the **Initial size** and **Autogrowth** for Rogger, Logger, AW-HDS-DDS, AW-HDS, and HDS-DDS. For information about values for respective components Increase Database and Log File Size for TempDB, on page 14.

For more information about the SQL Server TempDB Database and its use, see the Microsoft SQL Server documentation.

e) On the **MaxDOP** tab, choose the value of MaxDOP as half the value of logical CPU cores detected on the computer which is displayed just above the MaxDOP configuration. For example, if the logical CPU cores are detected as 4, then MaxDOP should be configured as 2.

Note SQL Server installation automatically recommends the MaxDOP server configuration based on the number of processors available. This feature is introduced in SQL Server 2019 and later. In SQL Server 2017, you can configure MaxDOP post installation. To configure MaxDOP, do the following:

1. In **Object Explorer**, right-click the database instance and select **Properties**.
2. Select **Advanced**.
3. In the **Max Degree of Parallelism** box, configure the number of processors as recommended above.

f) Click **Next**.

Step 12 On the **Ready to Install** page, click **Install**.

Step 13 On the **Complete** page, click **Close**.

Step 14 Enable Named Pipes and set the sort order as follows:

a) Open the SQL Server Configuration Manager.
b) In the left pane, navigate to **SQL Native Client 11.0 Configuration (32bit)** > **Client Protocols**.
c) In the right pane, confirm that **Named Pipes** is **Enabled**.
d) Right-click **Client Protocols** and select **Properties**.
e) In the **Enabled Protocols** section of the **Client Protocols Properties** window, use the arrow buttons to arrange the protocols in the following order:

1. Named Pipes
2. TCP/IP

f) Check the **Enable Shared Memory Protocol** and then click **OK**.
g) In the left pane, navigate to **SQL Server Network Configuration** > **Protocols for MSSQLSERVER**.
h) In the right pane, right-click **Named Pipes** and select **Enable**.

Note By default, Microsoft SQL Server dynamically resizes its memory. The SQL Server reserves the memory based on process demand. The SQL Server frees its memory when other processes request it, and it raises alerts about the memory monitoring tool.

Cisco supports the Microsoft validation to dynamically manage the SQL Server memory. If your solution raises too many memory alerts, you can manually limit SQL Server's memory usage. Set the maximum and minimum limit of the SQL memory using the **maximum memory usage** settings in the **SQL Server Properties** menu.as shown below:

Component	SQL Server Minimum Memory	SQL Server Maximum Memory
Logger	2GB	4GB
Rogger	2GB	3GB
AWS-HDS	4GB	8GB
AWS-HDS=DDS	4GB	8GB
HDS-DDS	4GB	8GB

For more information about the SQL Server memory settings and its use, see the Microsoft SQL Server documentation.

Step 15 Set the SQL Server's default language to English as follows:

a) Launch SQL Server Management Studio.
b) In the left pane, right-click the server and select **Properties**.
c) Click **Advanced**.
d) In the **Miscellaneous** section, set the **Default Language** to **English**.
e) Click **OK**.

Important Set the SQL Server default language to English because Cisco Unified Contact Center Enterprise requires a US date format (MDY). Many European languages use the European date format (DMY) instead. This mismatch causes queries such as `select * from table where date = '2012-04-08 00:00:00'` to return data for the wrong date. Handle localization in the client application, such as Cisco Unified Intelligence Center.

Step 16 Restart the SQL Server service as follows:

a) Navigate to the **Windows Services** tool.
b) Right-click **SQL Server (MSSQLSERVER)** and click **Stop**.
c) Right-click **SQL Server (MSSQLSERVER)** and click **Start**.

Step 17 Ensure that the SQL Server Browser is started, as follows:

a) Navigate to the **Windows Services** tool.
b) Navigate to the SQL Server Browser.
c) Right-click to open the **Properties** window.
d) Enable the service, change the startup type to **Automatic**, and click **Apply**.
e) To start the service, click **Start**, and then click **OK**.

What to do next

Caution Do not change the SQL port number. Retain the default port numbers as 1433 for TCP and 1434 for UDP connections. In case you change the port numbers, the applications like CCEAdmin will not work.

Increase Database and Log File Size for TempDB

To get the benefits of TempDB multiple data files support in CCE components, configure the following values as suggested for respective components.

CCE Component	vCPU	TempDB Data Files			TempDB Transaction Log File	
		Number of Files	Initial Size	Autogrowth	Initial Size	Autogrowth
Rogger	4	4	800MB	100MB	600MB	10MB
Logger	4	4	800MB	100MB	600MB	10MB
AW-HDS-DDS	4	4	800MB	100MB	600MB	10MB
AW-HDS	8	8	400MB	100MB	600MB	10MB
HDS-DDS	8	8	400MB	100MB	600MB	10MB

Install Antivirus Software

For details about supported anitvirus softwares, see *Contact Center Enterprise Compatibility Matrix*, see https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-device-support-tables-list.html

Use your antivirus vendor's product documentation for installation instructions, and adhere to the following:

- Update antivirus software manually. Do not enable automatic updates.
- To allow required access to installation program files or folders, perform file-blocking exclusions in the antivirus product file-and-folder protection rules. For example, to create the exclusions in McAfee VirusScan:
  1. Open the VirusScan console.
  2. Right-click **Access Protection** and select **Properties**.
  3. In the Anti-virus Standard Protection category, make sure that the rule **Prevent IRC communication** is unchecked in the **Block** column.
- Be aware that in the firewall component of Symantec Endpoint Protection 14.2, the Network Threat Protection feature must be disabled. The feature is enabled by default. When the feature is enabled, both sides of a redundant router come up in stand-alone mode which blocks communication between each side of the router pair. This blocking affects all deployment types.

  If you retain the default (enabled) and start serviceson side A and B of the router, the following Symantec message appears in the system tray: “The client will block traffic from IP address [side A router address] for the next 600 seconds.” The same message is also written to the security login client management. The Symantec Network Threat Protection traffic log indicates that a default firewall rule called “Block_all”

was dynamically enabled. The router logs show that both sides of the router came up in stand-alone mode.

To resolve the issue, disable the Symantec firewall on all Unifed CCE boxes and restart the services.

If you are using a managed client, perform the following steps:

1. Launch Symantec Endpoint Protection Manager.
2. Click **Policies**.
3. To disable a firewall policy, right-click on it and select **Edit**.
4. Uncheck **Policy**.
5. Click **OK**.

If you are using an unmanaged client, perform the following steps:

1. Double-click on the **Symantec** icon, in the system tray.
2. Select **Change Settings**.
3. Configure the required settings for Network Threat Protection and uncheck **Enable Firewall**.

- The firewall component of Trend Micro Deep Security blocks the communication between each side of the Router/PG. If you retain the default (enabled) setting and start the services on side A and side B, then the system logs a new deny event in the location: **Trend Micro Manager** > **Events** > **Firewall Events**.

  To resolve the issue, disable the Trend Micro firewall policy or add a new firewall exception for that particular policy.

Set Up Virtual Machines for Installation

Validate Network Adapter Settings and Power On

Procedure

Step 1 Select the virtual machine (VM) in the vSphere client. Right-click the VM and choose **Edit settings**.

Step 2 On the Hardware tab, select each network adapter. Make sure that **Connect at power on** in the Device Status group is checked.

Step 3 Under Network Connection, select the applicable network connection from the **Network label** drop-down list:

- Network adapter 1 = **Public** (visible)
- Network adapter 2 = **Private**

Note Certain VMs do not require a private network connection. The OVAs for those VMs do not create a second network adapter.

Step 4 Close the dialog box.

Step 5 If you are powering up the VM for the first time, power on the VM and wait for the VM to restart and to apply customization. The restart can take 5–10 minutes.

Important Do not press Ctrl-Alt-Delete. If you press Ctrl-Alt-Delete after powering on, the customization does not take effect, which requires completing the customization manually.

Configure Network Cards

Procedure

Step 1 In the virtual machine, open Network and Sharing Center.

Step 2 Click **Change adapter settings**.

Step 3 Rename Ethernet 0 to **public** for the Public network card.

Step 4 Rename Ethernet 1 to **private** for the Private network card.

Step 5 Assign an interface metric value for the network adapter:

a) Select the network adapter and right-click **Properties**.

b) In the **Networking** tab, select the appropriate Internet Protocol version and click **Properties**.

c) In the **Internet Protocol Version Properties** dialog box, click **Advanced**.

d) In the **IP Settings** tab, uncheck the **Automatic metric** checkbox and type a low value in the **Interface metric** text box.

Note A low value indicates a higher priority. Make sure that the Public Network card should have a lower value compared to the Private Network card.

By default, the value of the Interface Metric property for a network adapter is automatically assigned and is based on the link speed.

e) Click **OK** to save the settings.

Repeat the steps to assign an interface metric value for the internal/private cluster communication network adapter.

Set Persistent Static Routes

For geographically distributed Central Controller sites, redundant CallRouter, Logger, and Peripheral Gateway components typically have a Private IP WAN connection between Side A and Side B. Windows only allows one default gateway for each VM (which sends the Private Network traffic to the Public Network). So, you add a Static Route to all the VMs running the CallRouter, Logger, and PG applications.

To create a persistent static route with the **route add** command, you need the destination subnet, the subnet mask, the local gateway IP, and the interface number of the local Private Network interface:

```
route add <destination subnet> mask <subnet mask> <gateway IP> IF <interface number> -p
```

You must launch the DOS prompt as an administrator to run the commands in this procedure.

Procedure

Step 1 On each CallRouter, Logger, or PG VM, run `ipconfig /all`.
Record the `IPv4 Address`, `Subnet Mask`, and `Physical Address` (MAC address) for the Private Network interface.

Step 2 On each of these VMs, run `route print -4`.
Record the `Interface` for the Private Network. You can identify the correct interface by looking for its `Physical Address` (MAC address).

Step 3 On each of these VMs, run `route add <destination subnet> mask <subnet mask> <gateway IP> IF <interface number> -p` to add a persistent static route for the remote Private Network.

Configure Private Ethernet Card

Procedure

Step 1 Right-click **private** and select **Properties**.

Step 2 Uncheck **Client for Microsoft Networks**.

Step 3 Uncheck **File and Printer Sharing for Microsoft Networks**.

Step 4 Uncheck **Internet Protocol Version 6 (TCP/IPV6)**.

Step 5 Check **Internet Protocol Version 4 (TCP/IPV4)** and click **Properties**.

a) Remove the IP Address for the Default Gateway.
b) Remove the IP Address for the Preferred DNS server.
c) Remove the IP Address for the Alternate DNS server.

Step 6 Click the **Advanced** button. Open the DNS tab. Uncheck **Register this connection's addresses in DNS**.

Step 7 Add an entry for the private IP address.

Note This IP address should have an entry in the DNS server. This would be required while adding the Router or a Peripheral Gateway through Websetup and PeripheralGatewaySetup respectively.

A host (A) resource record must be created in the **DNS' Forward Lookup Zones**, and can be of the form hostname followed by a suffix "p" to easily identify it as the private interface.

For example: If the host name is **RoggerA**, make an entry in the DNS as "RoggerAp" for the private IP address.

Step 8 Optional: Add another entry for the private high IP address.

Note This IP address should have an entry in the DNS server. This would be required while adding the Router or a Peripheral Gateway through Websetup and PeripheralGatewaySetup respectively.

A host (A) resource record must be created in the **DNS' Forward Lookup Zones**, and can be of the form hostname followed by a suffix "ph" to easily identify it as the private interface.

For example: If the host name is **RoggerA**, make an entry in the DNS as "RoggerAph" for the private high IP address.

Step 9 Click **OK** twice. Then, click **Close**.

Configure Public Ethernet Card

Procedure

Step 1 Right-click **Visible** and select **Properties**.

Step 2 Check **Client for Microsoft Networks**.

Step 3 Check **File and Printer Sharing for Microsoft Networks**.

Step 4 Uncheck **Internet Protocol Version 6 (TCP/IPV6)**.

Step 5 Check **Internet Protocol Version 4 (TCP/IPV4)** and click **Properties**.

Step 6 Confirm the **Public IP address**, **Subnet mask**, **Default gateway** and **Preferred DNs server**, and click **Advanced**.

Step 7 On the **Advanced** tab, enter the public IP addresses.

Step 8 On the DNS tab, in the DNS suffix for this connection field, enter the name of the local DNS zone for the server and check **Register this connection's addresses in DNS**.

Step 9 Optional: Add another entry for the public IP address.

Note This IP address should have an entry in the DNS server. This would be required while adding the Router or a Peripheral Gateway through Websetup and PeripheralGatewaySetup respectively.

A host (A) resource record must be created in the **DNS' Forward Lookup Zones**, and can be of the form hostname followed by a suffix "PuH" to easily identify it as the public interface.

For example: If the host name is **RoggerA**, make an entry in the DNS as "RoggerAPuH" for the public IP address.

Step 10 If the server requires access to resources in a different trusting or trusted domain or DNS zone, select **Append these DNS suffixes (in order)** and enter the local DNS zone for the server first, and then add the other secondary zones that represent the trusting or trusted domain.

Step 11 Click **OK** twice. Then, click **Close**.

Verification of the Downloaded ISO or Minor Release Installer

Perform the following procedure to validate the downloaded ISO or Minor Release Installer signed by Cisco, to ensure that it is authorized.

Procedure

Step 1 Install **OpenSSL** on Microsoft Windows.

Step 2 Add the OpenSSL installation path to **System variables** in the **Environment Variables** of the system.

Step 3 Add the downloaded ISO Image or Minor Release Installer, ISO Image signature file or Minor Release Installer signature file and the Public key.der file in the same folder for the specific product component.

Step 4 Launch **Command Prompt** on the system.

Step 5 Run the following CLI (Command Line Interface) command to verify the files:

```
openssl dgst -sha512 -keyform der -verify <PUBLIC key.der> -signature
<ISO Image.iso.signature or Minor Release Installer.exe.signature> <ISO
Image or Minor Release Installer exe>
```

The system displays `Verified OK` on successful verification and `Verification failed` on verification failure.

Note If the verification fails do not proceed with the installation, contact Cisco Support for a valid ISO or Minor Release Installer.