Cisco Emergency Responder Installation

Cisco Emergency Responder Installation Overview

Cisco Emergency Responder (Emergency Responder) is distributed on an installation DVD that contains everything that is required to install Emergency Responder, including the Cisco Unified Communications Operating System software.

Hardware and Software Prerequisites

Cisco Emergency Responder requires specific hardware and software to run properly. Review the following sections before you proceed with an installation or upgrade:

- See the latest version of the Release Notes for Cisco Emergency Responder to verify that you have all the hardware and software, and in the supported versions, that you must install for Emergency Responder and to check that your CiscoUnifiedCommunicationsManager Appliance platform provides the Emergency Responder capabilities to meet your configuration needs. (You can also use equivalent Cisco-certified servers.)

- See the License Requirements section to make sure that you have all the required license keys available before you begin the installation process.

System Preparations

The Emergency Responder installation process installs both the platform software and the Emergency Responder software. During the installation, you are prompted to enter information needed by the system to complete the installation.

Note We recommend that you perform the installation or upgrade during off-peak hours. The installation or upgrade procedure completely reformats the hard disk, so Emergency Responder is unavailable for the duration of the installation or upgrade.

Review the following information before you install Cisco Emergency Responder or upgrade your system to the latest version:

- Upgrading Emergency Responder
  - Before you upgrade to the latest version of Emergency Responder, you must ensure that it is compatible with your existing version of Unified CM. You can use the Cisco Unified Communications Compatibility Tool to research this issue: http://tools.cisco.com/ITDIT/vtgsca/VTGServlet.
  - You must upgrade Emergency Responder before you upgrade Unified CM. Only after you have installed the new version of Emergency Responder can you then upgrade Unified CM.
  - After you have upgraded both Emergency Responder and Unified CM, you must then update the Unified CM Version on Emergency Responder.
  - See Table 1: Upgrading Tasks , on page 4 for the correct upgrade order and additional information about this subject.
  - If you have different security passwords in the active and inactive versions, and when you switch back to a lower version, ensure that you change the security password in the lower version to be same as the higher version. Follow these steps to change the security password:
    1. Switch the publisher node to a lower version.
    2. Change the security password of the publisher node to the new password which is same as the higher

       version.
    3. Switch the subscriber to a lower version.
    4. Change the security password of the subscriber node to the new password which is same as the higher version.

- Emergency Responder Versions
  - Different versions of Emergency Responder cannot be deployed in the same Emergency Responder group. The primary and the standby Emergency Responder servers must be running the same version of Emergency Responder. If you are upgrading to the most recent version of Emergency Responder, also make sure to upgrade both Emergency Responder servers.

Note Emergency Responder supports interoperability between two server groups in a cluster running different versions of Emergency Responder.

- Determine and list your Emergency Responder hostname and passwords.

  - The hostname for the Emergency Responder Publisher and Subscriber must not contain the underscore character (_). If you have an existing Emergency Responder server with an underscore in its hostname, change the hostname of the server before installing Emergency Responder.
  - The hostname for the Emergency Responder Publisher and Subscriber can begin with a numeric value.
  - Decide on a password for the Cisco Emergency Responder administrative user.

Note The Emergency Responder administrative users password must be at least six characters long and can contain alphanumeric characters, hyphens, and underscores. It must start with an alphanumeric character.

- Ethernet NIC speed and duplex mode:
  - Decide if you want to enable auto-negotiation of Ethernet NIC speed and duplex.
  - If yes, you do not need any additional information.
  - If no, determine what Ethernet NIC speed and duplex mode you will use.
- DHCP Configuration
  - Decide if you want to use the Dynamic Host Configuration Protocol (DHCP) to allocate IP addresses.
  - If yes, you do not need any additional information.
  - If no, you need the hostname, IP address, IP mask, and gateway address to enter for the Static Network Configuration.
- NTP Client information
  - The system prompts you to set up external Network Time Protocol (NTP) servers. We recommend that you use external NTP servers to ensure that the system time is accurate.
  - If you decide to use external NTP servers, you must enter the IP address or hostname of the servers.
  - If you do not choose to use external NTP servers, you must enter the system date and time clock information manually.

Note Use of NTP server is mandatory when installing Emergency Responder on UCS servers.

Note To avoid upgrade failures due to time sync issues with VM, disable the VM's NTP sync with the ESXi host using the workaround mentioned in the following link: http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1189.

- Database Access Security password

    - The system requires a database access security password to allow the nodes in a server group to communicate. The password is shared with all nodes in the server group.
    - The password must be at least six characters long and can contain alphanumeric characters, hyphens, and underscores. It must start with an alphanumeric character.
- SMTP host configuration (optional)
    - Decide if you want to use an SMTP host.
    - If yes, determine the hostname or IP address of the SMTP host.
- Caveats
    - Review the latest Release Notes for Emergency Responder before installation.

Perform the installation tasks in the order shown in this table.

Table 1: Upgrading Tasks

Installation Task	For More Information
Upgrade Emergency Responder	• Software Upgrades
Upgrade Unified CM	• http://www.cisco.com/en/US/products/sw/voicesw/ps556/tsd_products_support_series_home.html • http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_installation_guides_list.html • Change Cisco Unified Communications Manager Version
Update Unified CM Version	Update Cisco Unified Communications Manager Version

Install the components for Emergency Responder in the order shown in this table.

Table 2: Installation Tasks

Installation Task	For More Information
Install Cisco Unified Communications Manager	https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-guides-list.html
Install Emergency Responder as a new installation	Installation on a New System , on page 13

Installation and Migration on the Cisco UCS Server

The information in the following sections describe the changes for installation, upgrade, and migration of the Cisco Emergency Responder on the Cisco UCS Server.

System Requirements

To run Cisco Emergency Responder on the Cisco UCS Server, your system must meet the requirements listed in the following table.

Table 3: System Requirements

System Parameter	System Parameter options
Supported Virtual Machine Configuration	See the documentation at: https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-cisco-emergency-responder.html
IOPS per virtual machine (VM)	See the documentation at: https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-cisco-emergency-responder.html
VMware version	For Emergency Responder 15 compatible/supported ESXi releases, see https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-cisco-emergency-responder.html and https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/cisco-collaboration-infrastructure.html#VMwareCompatibility. **Note** Emergency Responder 15 VM is not supported to run on any older ESXi releases. For example, ESXi 6.7/older (including 6.5, 6.0, 5.x, 4.x). **Note** Ensure that you use ESXi, rather than ESX, to run Cisco Emergency Responder on the Cisco UCS Server. However, the server can be part of a VMware vCenter that includes ESX hosts.
VMware—vMotion	No **Note** We don't support vMotion on a VM that is running. However, we support powering-down a VM. This may be helpful if you want to put a rack server into maintenance mode.
VMware—Site Recovery Manager	Yes
VMware—High Availability	Yes
VMware—Data Recovery (VDR)	Yes
All other unlisted VMware features	Not supported

To operate Cisco Emergency Responder on the Cisco UCS Server successfully, you should have the experience and skills to manage a host server running VMware ESXi. If you do not have this experience and want to obtain the required information quickly, consider using VMware GO, a Web-based application that facilitates VMware.

Note Even if you use VMware GO, you still must use the supported VMware configuration on Cisco Emergency Responder on the Cisco UCS Server, which are documented at both http://www.cisco.com/go/swonly and https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-cisco-emergency-responder.html.

Installation on Cisco UCS Server

This following sections describe how to perform a fresh installation of a Cisco Emergency Responder on the Cisco UCS server:

- Configuration Checklist for Installing and Configuring the Server , on page 6
- Install Preparations , on page 7
- Set Up RAID , on page 8
- vSphere Client Installation , on page 9
- Aligning the Datastore Used for VMs , on page 9
- Create Virtual Machines, on page 9
- Download Virtual Machine Templates (OVA Templates) , on page 10
- Install Emergency Responder on VM, on page 11

Configuration Checklist for Installing and Configuring the Server

The following procedure provides the major steps required to install and configure Cisco Emergency Responder on the Cisco UCS Server.

Procedure

Step 1 Prepare to install the server.

For more information, see Install Preparations , on page 7.

Step 2 Physically install and connect the server.

Step 3 Power on the server and configure Cisco Integrated Management Controller (CIMC) for remote management.

Step 4 If you purchased the UCS server separately, configure the RAID settings to the following specification:

- The first two drives are configured as a RAID 1 (mirrored) drive. This drive is for ESXi installation.
- The next four drives are configured as a RAID 5 drive. This drive is for VMs.

Note Number of drives may be different in different versions of UCS servers.

For more information, see Set Up RAID , on page 8

Step 5 If you purchased the UCS server separately, configure the BIOS to the following specification:

- Disable Quiet Mode.
- Enable Enhanced SATA for CDROM access.
- Configure the following boot order:
  - SATA5:Optiarc DVD first
  - PCI Raid Adapter second

Step 6 Install and configure VMware EXSi on the smaller of the two available disks.

For more information, see the VMware ESXi documentation.

Step 7 Install vSphere Client.

For more information, see vSphere Client Installation , on page 9 and the vSphere Client documentation.

Step 8 Align the datastores for the VMs.

For more information, see Aligning the Datastore Used for VMs , on page 9.

Step 9 If you use 802.1q trunking, set the MTU size to 1472.

Step 10 Install and configure a virtual machine (VM).

For more information, see Create Virtual Machines, on page 9 and Download Virtual Machine Templates (OVA Templates) , on page 10.

Step 11 Install Cisco Emergency Responder on the VM.

For more information, see Install Emergency Responder on VM, on page 11.

Install Preparations

This section describes how to prepare to install a Cisco Emergency Responder on the Cisco UCS server in a standalone configuration, which indicates that it is not in a data center.

Allocate the following resources before installation:

- Space in a rack to receive a 2-RU UCS server
- Ethernet ports on a switch close to the UCS server:
  - One port for the CIMC
  - Two ports for the LAN on motherboard (LOM) NICs
- An IP address for the CIMC management port
- An IP address for the virtual host. The UCS server's IP address and is used by ESXi.
- A hostname, and optionally configured DNS for the virtual host's hostname
- IP addresses for the VMs

Set Up RAID

If you purchased the UCS server separately, configure the RAID settings to the following specifications:

- The first two drives are configured as a RAID 1 (mirrored) drive. This drive is for ESXi installation.
- The next four drives are configured as a RAID 5 drive. This drive is for VMs.

Note Number of drives may be different in different versions of UCS servers.

Procedure

Step 1 During server bootup, press **Ctrl+Y** to enter the preboot CLI.

Step 2 Enter the following commands to determine the current RAID configuration:

-ldinfo -l0 -a0

-ldinfo -l1 -a0

The required configuration is two drives in a RAID 1 array for logical drive 0, and four drives in a RAID 5 array for Logical drive 1. If the RAID configuration is wrong, continue with this procedure.

Note Do not continue with this procedure if RAID is configured correctly.

Step 3 Enter the command **-cfgclr -a0** to clear the RAID configuration.

Caution Clearing the RAID configuration deletes all data on the hard drives.

Step 4 Enter the following commands to configure RAID:

-cfgldadd -r1 [252:0, 252:1] -a0

-cfgldadd -r5 [252:2, 252:3, 252:4, 252:5] -a0

If the hard drives did not have a RAID configuration previously, you are done configuring RAID. If the hard drives had a RAID configuration before, continue with this procedure.

Step 5 Enter the following commands to initialize the logical volumes:

- ldinit -start -full -l0 -a0 (l0 is the letter l and the number 0, not the number 10)

- ldinit -start -full -l1 -a0 (l1 is the letter l and the number 1, not the number 11)

These commands clear data on the drives and initialize the new array.

Step 6 Allow these commands to finish running before exiting the Preboot CLI. Enter the following commands

to display the progress of the commands:

-ldinit -showprog -l0 -a0

-ldinit -showprog -l1 -a0

When both commands report that no initialization is running, it is safe to quit the Preboot CLI.

Step 7 After configuring the two logical volumes, you can exit the Preboot CLI by entering **q**.

vSphere Client Installation

When the virtual host is available on the network, you can browse to its IP address to bring up a web-based interface. The vSphere Client is Windows-based, so the download and install must be performed from a Windows PC.

After the vSphere Client is installed, you can run it and log into the virtual host using the virtual host's name or IP address, the root login ID, and the password you configured.

You can join the host to a vCenter if you want to manage it through vCenter.

Aligning the Datastore Used for VMs

When you install VMware ESXi, the second logical volume is automatically imported unaligned. VMs have better disk performance when all partitions (physical, ESXi, and VM) start on the same boundary and you will have fewer incidents of disk blocks being fragmented across the different boundaries.

To ensure that the ESXi partition used for VMs are aligned, delete the unaligned datastore (the larger disk partition, which is 407 GB), then recreate the datastore using vSphere client.

Create Virtual Machines

Cisco provides a VM template for you to download and transfer to your virtual host. Use this template to create the VM for Cisco Emergency Responder on the Cisco UCS Server installation.

Before you deploy the template and create the VM, you should have a hostname and IP address allocated for the new VM.

To create a VM and prepare to install Cisco Emergency Responder on the Cisco UCS Server, follow these steps.

Procedure

Step 1 Download the VM template for your application.

See Download Virtual Machine Templates (OVA Templates) , on page 10 for more information.

Note From Release 15 onwards, the OVA template is signed with sha512 using the Cisco authenticated certificates to ensure that there is no tampering of the OVA file.

Step 2 Upload the template to a datastore on the UCS server.

We recommend that you use the smaller datastore (with ESXi installed on it).

Step 3 Make this template available to the UCS server.

Step 4 Deploy the template file using vSphere Client. Enter the following information for the new VM:

- hostname
- datastore—Select a datastore that has enough resource.

Step 5 Complete creating the VM.

At this point a new VM is created with the correct amount of RAM, number of CPUs, size and number of disks for the intended application.

In case you are planning to upgrade any of your 12.5.x or 14 and SUs Emergency Responder to Release 15, note the following:

- Deployments with 12,000 or 20,000 users having 4GB vRAM should increase the vRAM size to 6GB before upgrading to Release 15.
- Deployments with 20000 users having 1 vCPU should increase the vCPU to 2 before upgrading to Release 15.

Table 4: Emergency Responder Release 15 VM Configuration Requirements

	Current Specifications			**Recommendation for Release 15**		
OVA Types	**vCPU**	**RAM**	**Disk**	**vCPU**	**RAM**	**Disk**
20, 000 users	1	4 GB	80 GB	2	6 GB	80 GB
30, 000 users	2	6 GB	110 GB	2	6 GB	110 GB
40, 000 users	4	6 GB	110 GB	4	6 GB	110 GB

Step 6 Install Cisco Emergency Responder on the Cisco UCS Server on the VM.

See Install Emergency Responder on VM, on page 11 for more information.

Download Virtual Machine Templates (OVA Templates)

The configuration of a Cisco Emergency Responder virtual machine must match a supported virtual machine template.

To obtain the virtual machine template for Cisco Emergency Responder on the Cisco UCS Server, follow these steps:

Procedure

Step 1 Select this URL in your browser:

http://www.cisco.com/cisco/software/navigator.html?mdfid=272877967

Step 2 If your browser prompts you to do so, type your Cisco.com User Name and Password in the text boxes, then click the **Log In** button.

Step 3 Select the desired version of Cisco Emergency Responder.

Step 4 Click the **Emergency Responder Virtual Machine Templates** link.

Step 5 Move your mouse over the filename and click the **Readme** link to view the virtual machine template's release information.

Step 6 Click the **Download Now** button. Follow the prompts and provide the required information to download the software.

Install Emergency Responder on VM

Procedure

Step 1 In vSphere Client, edit the VM to force entry into BIOS setup the next time the VM reboots.

Step 2 Make the Emergency Responder installation media available to the VM DVD-ROM drive.

Step 3 Power on the VM, then in BIOS setup, promote CD ROM to boot before the hard drive.

Step 4 Complete booting the VM.

The Cisco Emergency Responder installation program starts. For information about performing the installation, see the Installing Cisco Emergency Responder document.

Virtual Machine Configurations

With the virtual machine configuration for running Cisco Emergency Responder on the Cisco UCS Server, the VMware server must match the specifications described in the System Requirements, on page 5 to be supported by Cisco.

While Cisco Emergency Responder can be installed and licensed in other virtual machine configurations, Cisco does not support these configurations.

Migrate to Emergency Responder on Cisco UCS Server

Migrating from a Media Convergence Server (MCS server) to a Cisco Emergency Responder on the Cisco UCS Server follows a procedure that is very similar to replacing server hardware.

The following procedure outlines the migration process and references to other pertinent documentation.

Procedure

Step 1 Upgrade the MCS server to the most recent version of Cisco Emergency Responder.

Step 2 If the Emergency Responder VM uses a different IP address from the MCS server, change the IP address of the MCS server to the value used by the Emergency Responder VM.

Note The hostname on the Emergency Responder VM must remain the same as that on the MCS Server.

Step 3 Perform a DRS backup on the MCS server.

Step 4 Create the virtual machine (VM) on the Cisco UCS server used as the replacement for the MCS node.

For more information, see Installation on Cisco UCS Server , on page 6.

Step 5 Install the new version of Cisco Emergency Responder on the Cisco UCS server.

For more information, see Installation on Cisco UCS Server , on page 6.

Step 6 Perform a DRS restore to restore the data backed up from the MCS server to the Cisco UCS server.

Step 7 Upload the new licenses to the Cisco Emergency Responder on the Cisco UCS server.

VMWare Support

Consider the following, when using Cisco Emergency Responder on the Cisco UCS Server:

- Install, upgrade, and recovery procedures now use "soft media" such as ISO if the server does not have a DVD drive.
- USB tape backup is not supported.
- NIC teaming is configured at the VMware virtual switch.
- Hardware SNMP and syslog move to VMware and UCS Manager.
- Install logs are written only to the virtual serial port.
- Basic UPS Integration is not supported.
- Boot order is controlled by the BIOS of the VMware VM.
- Hardware BIOS, firmware, and drivers must be the required level and configured for compatibility with Cisco Emergency Responder supported VMware product and version.

For more information about the UCS C-series server, go to the following URL:

http://www.cisco.com/en/US/docs/unified_computing/ucs/c/sw/gui/config/guide/1.1.1/b_Cisco_UCS_C-Series_Servers_Integrated_Management_Controller_Configuration_Guide_1_1_1.html

To view the list of product installation and configuration guides for Cisco UCS C-Series Integrated Management Controller, go to the following URL:

http://www.cisco.com/en/US/products/ps10739/products_installation_and_configuration_guides_list.html

To view the list of product installation and configuration guides for Cisco UCS Manager, go to following URL:

http://www.cisco.com/en/US/products/ps10281/products_installation_and_configuration_guides_list.html

Emergency Responder Daily Operations on Cisco UCS Server

Daily operations for Cisco Emergency Responder on the Cisco UCS Server software applications are identical to when the application is installed on an MCS server.

There are some differences in hardware management and monitoring because Cisco Emergency Responder on the Cisco UCS Server operates in a virtual environment.

Hardware Monitoring From the VM

Applications running in a VM have no ability to monitor the physical hardware. Hardware monitoring must be done from the CIMC, ESXi plugins, vCenter, or by physical inspection (for example, for flashing LEDs.).

Hardware Monitoring From CIMC

The CIMC provides the following hardware monitoring:

- An overview of CPU, memory, and power supply health
- An overview of hardware inventory, including CPUs, memory, power supplies, and storage
- Monitoring of sensors for power supplies, fans, temperature, and voltage
- A system event log that contains BIOS and sensor entries

Hardware Monitoring From VSphere Client and VCenter

The vSphere Client provides the following monitoring features:

- When you are logged in to vCenter, the vSphere Client displays hardware and system alarms defined on the Alarms tab.
- VM resource usage is displayed on the Virtual Machines tab and on the Performance tab for each VM.
- Host performance and resource usage is displayed on the Performance tab for the Host.
- When ESXi is used standalone (without vCenter), hardware status and resource usage are available, but alarming is not possible.

Related Documentation

The *UCS RAID Controller SMI-S Reference Guide*, which describes Storage Management Initiative Specification (SMI-S) support in the Cisco UCS Servers, is available at the following URL:

http://www.cisco.com/en/US/partner/docs/unified_computing/ucs/sw/utilities/raid/reference/guide/ucs_raid_smis_reference.html

Installation on a New System

This procedure describes how to install Emergency Responder as a new installation.

You enter Emergency Responder group configuration through the Emergency Responder Administration web interface based on Publisher (primary) and Subscriber (secondary) server pairs as described in the following sections.

Note From Cisco Emergency Responder Release 14, all the certificate related operations are moved from Ipsec to Tomcat certificates. To create a trust between a publisher node and subscriber node, the Tomcat certificate should be exchanged between the publisher and subscriber for any cluster related operations to work.

Any Federal Information Processing Standards (FIPS) or hostname related changes require the same operation procedures.

Install Emergency Responder Publisher

To install Emergency Responder, you install the Publisher (primary) first, then you install the Subscriber (backup) on a separate server. You must install Emergency Responder on separate servers from CiscoUnifiedCommunicationsManager or any Cisco Unified Communications applications.

Allow approximately 1 hour to perform a new installation.

Procedure

- Insert the Emergency Responder Installation DVD.

  If the system finds the DVD, you are asked if you want to perform a media check before installation to determine if there are problems with the DVD. The system displays the checksum of the DVD and instructs you to verify this checksum on the Emergency Responder website.

  At the bottom of the screen you will see instructions for moving between elements and for selecting elements, as follows:

  - Use the **Tab** key to advance to the next element.
  - Use the **Alt-Tab** key combination to return to the previous element.
  - Use the **Space** bar to select a highlighted element.

  If you choose to perform the media check, the system performs the media check and displays the results.

  If the result of the media check is **PASS**, click **OK**. The system install begins the installation. Skip to Step 2.

  If the result of the media check is **FAIL**, obtain a new installation DVD from Cisco Systems.

- The Cisco Emergency Responder system installer starts. The Product Deployment Selection screen displays a message saying the Cisco Emergency Responder product suite is installing. Click **OK** to continue.
- The Proceed with Install page displays the current software version on the hard drive and the software version on the installation DVD.

  If you are performing a fresh installation, there will be no software on the hard drive and the system asks if you want to proceed with the installation. Click **Yes** to proceed.

  If you are performing an upgrade, the system displays the current software version and asks it you want to overwrite the hard drive. Click **Yes** to proceed.

  If you click **Yes**, the system continues with the installation and the Platform Configuration Wizard appears.

  If you click **No**, the installation is terminated.

- On the Platform Configuration Wizard page, click **Proceed** to continue with the platform installation.

  If you click **Skip**, the system installs both the platform and Emergency Responder software without prompting you to provide information during the installation. After the installation is completed and the system reboots, you are prompted to enter the required configuration details.

Note For version 8.6 and earlier, the Cisco Emergency Responder Subscriber may fail to install with unrecoverable internal error indicated in the logs. If this happens, do a Skip install by skipping the configurations step initially, proceed with the installation, and then key in the configuration details when prompted at the end of the procedure.

- Click **Continue** to proceed. The Timezone Configuration page appears.
- Choose the correct time zone to use from the list provided.

  Use the following keys to move between elements on the Timezone Configuration page:

  - **Arrow Up** or **Arrow Down** to select a time zone from the list
  - After selecting the correct time zone, click **OK**. The Auto Negotiation Configuration page appears.

- Click **Yes** to enable autonegotiation of the Ethernet NIC speed and duplex mode. The DHCP Configuration page appears. If you click **Yes**, skip to Step 10.

  If you click **No**, the NIC Speed and Duplex Configuration page appears.

- On the NIC Speed and Duplex Configuration page, do the following:

  a) Select the NIC Speed. The available options are 10 Megabit, 100 Megabit, or 1000 Megabit.
  b) Select the NIC Duplex setting. The available options are Full or Half.
  c) Click **OK**. The DHCP Configuration page appears.

- On the MTU Configuration page, you can set the maximum transmission unit (MTU) that can be sent in a network as follows:

  - Click **Yes** if you want to configure a a MTU value of less than 1500 bytes.
  - Click **No** to use the default MTU value of 1500 bytes.

- Click **Yes** if you want to use Dynamic Host Configuration Protocol (DHCP). The Administration Login Configuration page appears. Skip to Step 14.

  If you click **No**, the Static Network Configuration page appears.

- If you chose not to use DHCP, enter the following information about the Static Network Configuration page:

  - Host Name
  - IP Address
  - IP Mask
  - Gateway (GW) Address

  Click **OK**. The DNS Client Configuration page appears.

- On the DNS Client Configuration page, you are asked if you want to configure the Domain Name System (DNS) client.

Note Click the **Help** button for details about configuring DNS.

  If you select **Yes**, a second DNS Client Configuration page appears.

  If you select **No**, the Administration Login Configuration page appears. Skip to Step 14.

- On the second DNS Client Configuration page, you are prompted to enter the following information:

  - Primary
  - Secondary DNS (optional)
  - Domain

  Click **OK**. The Administration Login Configuration page appears.

- On the Administration Login Configuration page, enter an ID and password for the Administrator account. This password is used to access the CLI and the CiscoUnifiedOS Administration and Disaster Recovery System (DRS) websites. Click **Help** to display guidelines for creating this password.

  When you have finished, click **OK**. The Certificate Information page appears.

- Enter the following information about the Certificate Information page:
  - Organization
  - Unit
  - Location
  - State
  - Country (select from the scroll-down menu).

  Click **OK**. The Publisher Configuration page appears.

- Based on the type of installation you are performing, do one of the following:
  - If the server you are configuring is the Publisher in the server group, click **Yes**. The Network Time Protocol Client Configuration page appears. Proceed to Step 17.
  - If the server you are installing is not the Publisher in the server group, you must first configure this server on the Publisher before you can proceed. This server must also have network access to the Publisher, which must be in service for the installation to complete successfully. Click **No** only if you are configuring the Subscriber. See Install Emergency Responder Subscriber, on page 18 for information about installing the Subscriber.

- On the Network Time Protocol Client Configuration page, you are asked if you want to set up external Network Time Protocol (NTP) servers.

Note We strongly recommend that you use external NTP servers to ensure that the system time is kept accurate.

Caution For Emergency Responder install on UCS servers, it is mandatory to configure NTP server.

  If you click **Yes**, the system displays a second Network Time Protocol Client Configuration page. In the fields provided, enter the IP address or hostname of the external NTP servers, then click **OK**. The Database Access Security Configuration page appears. Skip to Step 18.

  If you click **No**, the Hardware Clock Configuration page appears. Enter the following information:
  - Year [yyyy]
  - Month [mm]
  - Day [dd]
  - Hour [hh]
  - Minute [mm]
  - Second [ss]

  When you finish entering this information, click **OK**. The Database Access Security Configuration page appears.

- On the Database Access Security Configuration page, enter the security password and then confirm the password in the fields provided.

Note The security password must be at least six characters long and can contain alphanumeric characters, hyphens, and underscores. It must start with an alphanumeric character. The security password is used for secure communications between Emergency Responder server groups when performing the installation or upgrade, DRS backup or restore, and "Point to a new Publisher" operations.

Click **Help** to display guidelines. When you finish, click **OK**. The SMTP Host Configuration page appears.

- You are asked if you want to configure a Simple Mail Transport Protocol (SMTP) host. This step is optional.
  - If you click **Yes**, a second SMTP Host Configuration page appears. Click **Help** for guidelines, then enter the SMTP hostname or IP address in the field provided. When you are finished, click **OK**. The Platform Configuration Confirmation page appears.
  - If you click **No**, the Platform Configuration Confirmation page appears.
- On the Platform Configuration Confirmation page, do one of the following:
  - Select **OK** to save the platform configuration information and continue with the installation. The Cisco Emergency Responder Configuration page appears.

Note After you select **OK**, you cannot modify the platform configuration information.

  - Select **Back** if you want to return to the previous page to make modifications. Continue to select **Back** to scroll through each platform configuration page.
  - Select **Cancel** to cancel the installation.
- On the Cisco Emergency Responder Configuration page, do the following:
  - Enter the emergency number (for example, **911**).
  - Select the Cisco Unified CommunicationsManager version. Use the **Up** or **Down** arrows to select the version number and then select **OK**.
- On the Security End User Language Selection page, choose a language for the Cisco Emergency Responder web pages. The system defaults to the English language.

  The Application User Password Configuration page appears.
- On the Application User Configuration page, enter the username and password. This username and password is associated with the default administrative account and is used to log in to the Emergency Responder Administration web page. Click **Help** for guidelines.

  When you are finished, click **OK**. The Cisco Emergency Responder Configuration Confirmation page appears.
- On the Cisco Emergency Responder Configuration Confirmation page, do one of the following:
  - Select **OK** to save the Cisco Emergency Responder configuration information and continue with the installation. The system continues the installation process and then reboots.

Caution After you select **OK**, you can not modify the Cisco Emergency Responder configuration information.

  - Select **Back** if you want to return to the previous page to make modifications. Continue to select **Back** to scroll through each Emergency Responder Application User Configuration page.
  - Select **Cancel** to cancel the installation.

- After the system reboots, it checks the status of various system components. If the system finds any problems, you are prompted to correct the problem.

  If the system does not find any problems, the installation process continues. The system ejects the installation DVD, reboot, and then finishes the installation. When the installation is complete, a CLI prompt appears.

Note During this process, the system displays the MAC address of the Publisher. Write down the MAC address when it displays; you use the MAC address later to acquire Emergency Responder licenses. If you are not able to capture the MAC address during installation, you can look it up later. See the Server Licenses section for information about looking up the server MAC address.

- To bring up the Emergency Responder websites, go to any Windows system on the network, start a supported web browser, and enter the following URL:

  ```
  http://your Emergency Responder hostname/
  ```

  or

  ```
  http://your Emergency Responder IP address/
  ```

Note Make sure that the Emergency Responder is configured with DNS so that hostname is resolved to the IP address.

Install Emergency Responder Subscriber

You must install Subscriber only after you have installed the Publisher. You must install the Subscriber on a separate server from the Emergency Responder Publisher.

Caution You must complete the installation of the Publisher, which includes a system reboot, before you start to install the Subscriber.

Procedure

Step 1 On the Publisher server, add the details about the Subscriber server by doing the following:

a) Log in the Publisher Emergency Responder Administration website.

b) Select **System** > **Add Subscriber**. The Add Server page appears.

c) Enter the hostname of the new Subscriber and click **Insert**. The Add Subscriber page appears again.

d) In the **Configured Servers** list, check that the hostname and IP address of the new Subscriber is listed.

Step 2 Follow Steps 1 through 15 in the Installation on a New System , on page 13 section. After you complete Step 15, the Publisher Configuration page appears.

Step 3 On the Publisher Configuration page, select **No** to indicate that you are installing a Subscriber, not a Publisher. The system displays a warning saying that if this is not the Publisher, you must first configure this server using the Publisher Administration web interface before you can proceed (see Step 1 of this procedure for more information). Also, this server being added must have network access to the Publisher, which must be in service for the installation to complete successfully.

Click **OK** to close the warning.

Step 4 The Network Connectivity Test Configuration page appears. The system attempts to verify system connectivity. Click **No** to continue the installation.

Step 5 The Publisher Access Configuration page appears. Enter the following:

- Publisher hostname
- Publisher IP address
- Publisher Database/Security password

Step 6 Verify that the Publisher information is correct and click **OK**.

Step 7 The SMTP Host Configuration page appears. Choose **Yes** if you want to configure the SMTP Host.

Step 8 The Platform Configuration Complete page appears. Select one of the following options:

- If the Publisher information is correct, click **OK**.
- If the information is not correct, click the **Back** button and make the needed corrections on the Publisher Access Configuration page, then click **OK**.

The installation of the Emergency Responder Subscriber begins and takes an additional 20 to 30 minutes to complete.

Step 9 When the installation completes, go to the Emergency Responder Administration website on the Subscriber to verify that the Subscriber was installed successfully. If the installation succeeded, a message saying “Primary Cisco Emergency Responder is active” appears. This message indicates that the Subscriber was installed successfully.

Note If the Subscriber installation cannot validate the Publisher, See Cannot Validate Publisher in the Troubleshooting chapter.

Emergency Responder Upgrade

To upgrade from version 10.0 or a later version of Cisco Emergency Responder to the most recent version of Emergency Responder, use the Cisco Unified OS Administration web interface or Command Line Interface (CLI). See Software Upgrades section for information about performing upgrades.

See "Performing Software Upgrades" section of the respective *Cisco Emergency Responder Administration Guide for Emergency Responder* for information about performing upgrades to Emergency Responder.

Touchless Installation

Previous releases of Cisco Emergency Responder (Emergency Responder) cluster environment required you to install the publisher node first before you proceed to install the subscriber nodes. You had to install the subscriber node after adding this node details to the **Cisco ER Administration** > **Add Subscriber** page of the publisher node first before you proceed to install the subscriber nodes.

Touchless installation makes the installation process seamless and promotes simplified installation of Emergency Responder. With the CER server Group touchless installation, the subscriber node is configured dynamically along with the publisher node during their installation. The touchless installation proceeds without the requirement to provide any subscriber details in the installation wizard as the subscriber is not dependent on the installation of the publisher.

Note After publisher installation is complete, and if the subscriber installation does not happen automatically, you must restart the Cisco Tomcat service using the CLI command **utils service restart Cisco Tomcat** from the publisher node.

This feature has the following benefits:

- No manual intervention and scheduling during the deployment of a new cluster.
- No manual entry of the subscriber node to an existing cluster.
- No requirement to wait until the publisher node is active.

Answer File Generator

Use the Answer File Generator (AFG) tool (http://www.cisco.com/web/cuc_afg/index.html) to generate the answer files or ISO images for configuration. These files include clusterConfig.xml and platformConfig.xml files.

Start the virtual machine on which you mounted the ISO image to start the Emergency Responder installation. No manual intervention is required during installation of a standalone node. In a cluster environment, you can install both the publisher node and the subscriber node simultaneously. Sometimes, the installation of the subscriber node can stop during the installation of the publisher node. In this case, after the publisher node installation is complete, it generates a signal for the subscriber node to continue the installation.

Predefined Cluster Configurations (AFG Process)

With the implementation of this feature, the Answer File Generator (AFG) tool generates the clusterConfig.xml file along with the existing the platformConfig.xml file. If you provide the details of the subscriber node to the AFG tool, the clusterConfig.xml file includes those details. After the Emergency Responder publisher is installed, it reads the clusterConfig.xml file and if the publisher finds any subscriber node, it adds them to its cerserver tables. Adding the subscriber to cerserver tables eliminates the need to wait for the Emergency Responder publisher to finish its installation, and then manually add the subscriber on the server page. The entire installation process occurs automatically.

Preinstall Tasks for Cisco Emergency Responder

Procedure

	Command or Action	Purpose
Step 1	Planning the Installation	Make sure to review the following: • Decide on your installation method. • Decide on your cluster topology.
Step 2	Required Installation Information, on page 22	Review the installation requirements and record the configurations settings for each server that you plan to install.
Step 3	Create virtual machines.	• Get base OVA. • Run Collab Sizing Tool to get the required virtual machine count and specs of each virtual machine. If you don't want to run Collab Sizing Tool, follow the guidance in the OVA readme and the OVA wizard to select a predefined starting point, which can be changed later if needed.
Step 4	Mount the installation ISO file.	Place the installation ISO file in a location where the virtual machine can access it and edit the virtual machine's DVD drive to map to the file. Select the option to mount the DVD drive when you power on the virtual machine. When you power on the virtual machine, it mounts the ISO file and start the installation process. Do not begin the installation process until you have completed all the steps in this procedure.
Step 5	Verify the NTP status on the publisher node.	If the publisher node fails to synchronize with an NTP server, subscriber node installation can fail. On the Emergency Responder publisher node, run the `utils ntp status` CLI command.
Step 6	Complete the following firewall updates: • If a firewall is in the routing path between nodes, disable the firewall. • Increase the firewall timeout settings until after you complete the installation.	Temporarily allowing network traffic in and out of the nodes (for example, setting the firewall rule for these nodes to IP any/any) does not always suffice. The firewall might still close necessary network sessions between nodes due to timeouts.
Step 7	If you use DNS, verify that all servers on which you plan to install Emergency Responder are properly registered in DNS.	

	Command or Action	Purpose
Step 8	Cisco Smart Software Licensing	Make sure that your system has adequate licensing.

Required Installation Information

When you install either Emergency Responder on a server, the installation process requires you to provide specific information. You can provide this information manually during the installation process or you can provide it using an answer file. For each server that you install in a cluster, you must gather this information before you begin the installation process.

The following table lists the information that you must gather before you begin the installation.

Note Because some of the fields are optional, they may not apply to your configuration. For example, if you decide not to set up an SMTP host during installation, the parameter still displays, but you do not need to enter a value.

You cannot change some of the fields after the installation without reinstalling the software, so be sure to enter the values that you want. The last column in the table shows whether you can change a parameter after installation, and if you can, it provides the appropriate menu path or Command Line Interface (CLI) command.

Table 5: Required Installation Information

Configuration Data	Description	Editable after Installation
Administrator Credentials		
Administrator Login	Specifies the name that you want to assign to the Administrator account.	No After installation, you can create additional administrator accounts, but you cannot change the original administrator account user ID.
Administrator Password	Specifies the password for the Administrator account.	Yes CLI: `set password user admin`
Application User Credentials		
Application User Username	Specifies the user ID for applications installed on the system.	Yes CLI: `utils reset_application_ui_administrator_name`
Application User Password	Specifies the password for applications on the system.	Yes CLI: `utils reset_application_ui_administrator_password`
Security Password		

Configuration Data	Description	Editable after Installation
Security password for Emergency Responder	Servers in the cluster use the security password to communicate with one another. Set this password on the Emergency Responder publisher node, and enter it when you install each additional node in the cluster.	Yes. You can change the security password on all nodes in the cluster using the following command: CLI: **`set password user security`**
Certificate Information		
Organization	Used to create the Certificate Signing Request.	Yes CLI: **`set web-security [orgunit] [orgname] [locality] [state] [country]`**
Unit	Used to create the Certificate Signing Request.	Yes CLI: **`set web-security [orgunit] [orgname] [locality] [state] [country]`**
Location	Used to create the Certificate Signing Request.	Yes CLI: **`set web-security [orgunit] [orgname] [locality] [state] [country]`**
State	Used to create the Certificate Signing Request.	Yes CLI: **`set web-security [orgunit] [orgname] [locality] [state] [country]`**
Country	Used to create the Certificate Signing Request.	Yes CLI: **`set web-security [orgunit] [orgname] [locality] [state]`**
(Optional) SMTP		
SMTP Location	Specifies the name of the SMTP host that is used for outbound email. You must fill in this field if you plan to use electronic notification. If not, you can leave it blank.	Yes • In Cisco Unified Operating System Administration Web Interface, select **Settings** > **SMTP** and enter the IP address or Hostname in the IP Address/Host Name field. • CLI: **`set smtp [host]`**
CER Emergency Number		

Configuration Data	Description	Editable after Installation
Emergency Number	Specifies the primary emergency number that is dial-able and is handled by Emergency Responder. All characters must either be numeric, a '*' or a '#'.	Yes
CER End User Language		
End User Language	Specifies the language the user wants to use for Emergency Responder.	Yes
CER CCM Version		
CCM Version	Indicates the version of Emergency Responder CCM.	Yes
Network Information		
DHCP (Dynamic Host Configuration Protocol)	Check the check box if you want to use DHCP to automatically configure the network settings on your server. Also, enter the hostname. If you uncheck the option, you must enter a hostname, IP Address, IP Mask, and Gateway Address.	Yes. • In Cisco Unified Operating System Administration Web Interface, select **Settings** > **IP** > **Ethernet**. • CLI: `set network dhcp eth0 [enable]` CLI: `set network dhcp eth0 disable [node_ip] [net_mask] [gateway_ip]`
Hostname	If DHCP is enabled, you must enter a hostname for this machine.	Yes; for Emergency Responder nodes, choose one of the following: • In Cisco Unified Operating System Administration Web Interface, select **Settings** > **IP** > **Ethernet**. • CLI: `set network hostname` You will be prompted to enter the parameters.

Configuration Data	Description	Editable after Installation
IP Address	If DHCP is disabled, you must enter the IP address of this machine.	Yes; for Emergency Responder nodes, choose one of the following: • In Cisco Unified Operating System Administration Web Interface, select **Settings** > **IP** > **Ethernet**. • CLI: `set network IP eth0 [ip-address] [ip-mask]`
IP Mask	If DHCP is disabled, you must enter the IP subnet mask of this machine. The subnet mask together with the IP address defines the network address and the host address. The subnet mask must use the following format: 255.255.255.0	Yes • In Cisco Unified Operating System Administration Web Interface, select **Settings** > **IP** > **Ethernet**. • CLI: `set network IP eth0 [ip-address] [ip-mask]`
Gateway Address	If DHCP is disabled, you must enter the gateway address.	Yes • In Cisco Unified Operating System Administration Web Interface, select **Settings** > **IP** > **Ethernet**. • CLI: `set network gateway [addr]`
(Optional) DNS		
Primary DNS	If you have a Domain Name Server (DNS), Emergency Responder contacts this DNS server first when attempting to resolve hostnames.	Yes CLI: `set network dns primary [address]`
Secondary DNS (optional)	When a primary DNS server fails, Emergency Responder will attempt to connect to the secondary DNS server.	Yes CLI: `set network dns secondary [address]`
Domain	Represents the name of the domain in which this machine is located	Yes CLI: `set network domain [name]`
Time Zone		

Configuration Data	Description	Editable after Installation
Region	Allows you to select a region for your time zone.	Yes
Time Zone	Reflects the local time zone and offset from Greenwich Mean Time (GMT). Select the time zone that most closely matches the location of your machine.	Yes CLI: `set timezone [zone`
Network Time Protocol		
NTP Server IP Address	During installation of the Emergency Responder publisher node, you must specify the IP address of an external Network Time Protocol (NTP) server. We recommend that you use the Emergency Responder publisher node as the NTP server.	Yes In Cisco Unified Operating System Administration Web Interface, select **Settings** > **NTP Servers**.
(Optional) List of Secondary Nodes	This list identifies the secondary nodes (subscribers) in the cluster by host name.	Yes

Touchless Installation Task Flow

Complete these tasks to install your Emergency Responder clusters in a single process using the touchless installation method.

Before you begin

Preinstall Tasks for Emergency Responder

Procedure

	Command or Action	Purpose
Step 1	Generate Answer Files for Touchless Install, on page 27	Use this procedure to generate the configuration files (clusterconfig.xml and platformconfig.xml) with your network settings. The touchless install process uses these files to install and configure the various cluster nodes.

	Command or Action	Purpose
Step 2	Generate ISO Images, on page 27	Use this procedure to create ISO images from the answer files. You will use the ISO image in your touchless installation.
Step 3	Upload ISO Image to Datastore, on page 28	Use this procedure to upload the ISO image to the datastore.
Step 4	Mount ISO Image to VM, on page 28	Use this procedure to mount the UC application ISO image on their corresponding VM.
Step 5	Run Touchless Install, on page 29	Begin the cluster installation. You can kick off all node installations simultaneously.

Generate Answer Files for Touchless Install

Use this procedure to generate answer files for your touchless installation of your cluster. The answer files (clusterconfig.xml and platformconfig.xml) contain the configuration information that the install process installs and configures on each cluster node.

Before you begin

You must have already planned your network topology, including addresses for your Emergency Responder cluster nodes.

Procedure

Step 1 Log in to the Cisco Emergency Responder Answer File Generator application at https://www.cisco.com/c/en/us/applicat/content/cuc-afg/index.html.

Step 2 In the **Hardware** section, choose **Virtual Machine**.

Step 3 From the **Product** section, select the product and version that you want to install.

Step 4 Complete the remaining fields under **Clusterwide Configuration** with your cluster configuration details.

Step 5 Complete the fields in the **Primary Node Configuration** with configuration details for the publisher node.

Step 6 Under **Secondary Node Configuration**, enter the node details for your subscriber node and click **Add Secondary Node**.

Step 7 Add your subscriber node.

Step 8 Click **Generate Answer Files**.

Step 9 Download the answer files to your computer.

Generate ISO Images

Use this procedure to create ISO images from the answer files. You will use the ISO images in your touchless installation.

Note This procedure describes how to use Winimage to create ISO images. You can download Winimage from http: www.winimage.com download.htm.

Procedure

Step 1 From Winimage, choose **File** > **New**.

Step 2 From the Standard format, choose **1.44 MB** and click **OK**.

Step 3 Navigate to the Menu Image, choose **Inject** and select the `platformConfig.xml` file.

Step 4 When prompted to inject the file into Winimage, click **Yes**.

Step 5 Choose **File** > **Save As**.

Step 6 Save the file as an ISO image (.iso file) using the following naming convention: `Emergency Responder—cer.iso`.

Step 7 Repeat these steps for the other Emergency Responder server groups in the cluster.

Upload ISO Image to Datastore

Use this procedure to upload the ISO images to the datastore.

Procedure

Step 1 Start the vSphere client.

Step 2 Select the **Configuration** tab.

Step 3 Select **Storage**.

Step 4 Right-click on a datastore and **Browse** the datastore.

Step 5 Navigate to the destination directory and click the **Upload files to this datastore** icon.

Step 6 Upload the ISO images to your local folder.

Step 7 At the **Upload/Download** warning, click **Yes**.

Step 8 Close the **Datastore Browser** window.

Mount ISO Image to VM

Use this procedure to mount the UC application ISO images on their corresponding virtual machine (VM).

Procedure

Step 1 In the vSphere client, choose the virtual machine.

Step 2 Open VMware Remote Console (VMRC), and click the **CD/DVD Drive 2**.

Step 3 **Browse** to the datastore and locate the ISO image.

Step 4 Select the file and click **OK**.

Step 5 Under **Device Status**, enable the **Connected and Connect at power on** option.

Step 6 Click the **Options** tab. Under **Boot Options**, check **Force entry to BIOS** and click **OK**.

Step 7 Repeat this procedure for each VM on which you want to install a node.

Run Touchless Install

After you have mounted your ISO image to your application VMs, run the touchless installation process. You can install all nodes simultaneously.

Procedure

Step 1 In vSphere client, right-click the **VM** and select **Open Console**. A console window opens.

Step 2 Click the **Power On** icon in the console toolbar to power on the virtual machine.

Step 3 When the BIOS screen appears, configure the following boot order:

a) CD-ROM
b) Hard Drive
c) Removable Devices
d) Network

Step 4 Save the settings and exit from the console. The installation commences immediately.

Step 5 Repeat these steps for each cluster node. All cluster nodes may install in parallel; you do not have to install them serially.

Step 6 After to emphasize the completion of an activity, remove the ISO configurations from the virtual machines.