Cisco Extended Care Installation and Configuration Guide

Release 1.2.1
April 2017

Cisco Systems, Inc.
www.cisco.com

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.
Preface 1
Audience 1
Organization 2
Not Intended for Use in Emergency or for Patient Monitoring 2

Platform Overview and System Requirements 1-1
Overview of the Cisco Extended Care Platform 1-1
Cisco Extended Care Architecture 1-1
Proxy Server 1-3
Cisco Extended Care Application Server 1-3
Cisco Remote Expert Mobile (REM) 1-3
Cisco Extended Care Data Center Components 1-4
Data Center Software Requirements 1-4
Data Center Hardware Requirements 1-4
Video Conferencing Data Center Components 1-5
Video Endpoints 1-5
Soft Client Browser Requirements 1-5
Before You Begin Installation 1-6

Installing Software for the Cisco Extended Care Application Server 2-1
Creating a Virtual Machine 2-1
Installing Cisco Extended Care on a Virtual Machine 2-4
Upgrading the Extended Care Server 2-8
Verifying the Installation 2-8
Changing the Password 2-9
Setting Up the Network Time Protocol (NTP) 2-9
Synchronizing the JVM Time Zone 2-10
Generating the SSL Certificate for the Data Center Server 2-11

Configuring the Cisco Extended Care Application Server 3-1
Prerequisites 3-1
CUCM 3-1
Contents

REM 3-1
Logging into the Cisco Extended Care Administration Server 3-2
Uploading the Cisco Extended Care License Files 3-3
Configuring the System Parameters 3-4
  Resetting Endpoint Sessions 3-4
Configuring the Regions 3-5
Configuring the UC Servers 3-6
Configuring the UC Server Groups 3-9
Configuring the Endpoints 3-11
Configuring the Security Policy 3-14

Appendix A

Assorted Tasks A-1
  Values to be Gathered Before Installation A-1
  Troubleshooting A-2
    Incorrect Number of Licenses Displayed A-2
  Additional Resources A-2

Glossary
Preface

This Cisco Extended Care 1.2 Application Server Installation and Configuration Guide outlines the steps and best practices to install and configure the Cisco Extended Care Application Server and the associated components.

This Preface includes the following major topics:

- Audience, page 1
- Organization, page 2
- Not Intended for Use in Emergency or for Patient Monitoring, page 2

Audience

This guide is intended for an experienced Information Technology (IT) professional familiar with Linux who will be installing the Cisco Extended Care Application Server. Specifically, the installation person should have at least one to two years of Linux administration experience covering the following:

- Ability to administer the Unix/Linux system
- Ability to execute basic file and directory operations
- Experience installing, uninstalling, and upgrading software
- Experience with network client configuration (IP address, NTP, and DNS)
- Starting and stopping application services
- User management
Organization

<table>
<thead>
<tr>
<th>Title</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Platform Overview and System Requirements</td>
<td>Describes the Cisco Extended Care platform, the architecture, and the system requirements.</td>
</tr>
<tr>
<td>Installing Software for the Cisco Extended Care Application Server</td>
<td>Describes the installation procedure for the Cisco Extended Care application server.</td>
</tr>
<tr>
<td>Configuring the Cisco Extended Care Application Server</td>
<td>Describes the configuration of the Cisco Extended Care application server after it is installed.</td>
</tr>
</tbody>
</table>

Not Intended for Use in Emergency or for Patient Monitoring

Cisco Extended Care is intended to allow healthcare providers to drive and promote health and wellness. Cisco Extended Care is not intended for use in emergency situations. In the event of an emergency, call 911 or your local emergency response system. Cisco Extended Care is not for use in situations involving real-time patient monitoring or alarming.
This chapter includes the following major topics:

- Overview of the Cisco Extended Care Platform, page 1-1
- Cisco Extended Care Architecture, page 1-1
- Cisco Extended Care Data Center Components, page 1-4
- Video Endpoints, page 1-5
- Before You Begin Installation, page 1-6

**Overview of the Cisco Extended Care Platform**

Cisco Extended Care is much more than a telehealth solution; it is a healthcare collaboration platform that transforms the clinician experience. It helps unify the communication infrastructure components and devices, helps simplify workflows, and helps enable high-quality interactive visual communications and collaboration. Healthcare organizations can use their existing Cisco video devices or use telehealth capabilities built in to their provider portals and applications for a unified visual experience.

As opposed to being merely a video endpoint, Cisco Extended Care is a solution that helps eliminate disjointed platforms and cobbling together of code with questionable levels of reliability, security, and scalability. It is agnostic to electronic medical records (EMR), video endpoint, and applications. This solution helps increase clinician efficiency and productivity by unifying communication infrastructure components.

**Cisco Extended Care Architecture**

The Cisco Extended Care architecture is built using a layered approach to help enable the patient-provider interaction.

- **Figure 1-1** illustrates the layered architecture of Cisco Extended Care.
- **Figure 1-2** illustrates an overview of the components in Cisco Extended Care with VCS Expressway Integration.
- **Figure 1-3** illustrates an overview of the components in Cisco Extended Care with REM Integration and UC setup.
- **Figure 1-3** illustrates an overview of the components in Cisco Extended Care with REM Integration.
Figure 1-1  Cisco Extended Care Layered Architecture and Supported Cisco Video and Infrastructure Equipment

Figure 1-2  Cisco Extended Care Architecture
Proxy Server

The proxy server (see Figure 1-2) is the software that helps enable the provider and the patient to connect to the Cisco Extended Care application from outside the enterprise network.

Cisco Extended Care Application Server

The Cisco Extended Care application server (see Figure 1-2) is the data center software that manages all of the connectivity and provides services to the end users. This server ties together all the components of Cisco Extended Care.

Cisco Remote Expert Mobile (REM)

Cisco Remote Expert Mobile (see Figure 1-3) is a Cisco software product that helps enable patients and care team members to connect with Extended Care in order to participate in live video appointments and also perform other collaboration activities by using an internet viewer from their computer, tablet, mobile phone or other internet-connected device. Cisco REM provides secure, two-way calling capabilities via an Internet web page address (URL) that is provided by the care team contact.

Cisco REM is a software solution that helps enable consumer communication devices to use their browser-based or mobile applications to make IP-based calls to traditional enterprise devices - without using plugins or clients.

Users can conduct their business through their smart phones, tablets, laptops, and PCs. They can make and receive voice and video calls, send and receive instant messages, communicate presence status, and share application events in real-time.

Cisco REM can also provide a WebRTC-to-SIP gateway that helps enable access through the enterprise firewall from the outside. Cisco REM works with Cisco Collaboration infrastructure to integrate with enterprise customer relations management and other line-of-business applications.

For details about Cisco Remote Expert Mobile, refer to the following URL:

Cisco Extended Care Data Center Components

Cisco Extended Care requires software and data center hardware in an enterprise data center. The required components can vary, depending on the features and video components selected. This section briefly describes the required components.

Data Center Software Requirements

Cisco Extended Care software is the core of the solution that leverages Cisco unified communications technologies to help achieve the telehealth use case. Cisco Extended Care offers the following to the core of the server:

- **Application Server**—Provides the user interface for the administrator for provision video endpoints and integrates Cisco unified communication servers.
- **Web Services**—Used by the software to interface with the partner applications.

Data Center Hardware Requirements

**Cisco UCS Server**

The Cisco UCS server is best suited to install the Cisco Extended Care application software. The UCS server supports installation of the Cisco Extended Care application as a VM installation. The following is the recommended configuration for the VM installation:

- Virtual Machine:
  - Virtual Machine Version 7 or 8
  - Guest OS: RHEL 6 64 Bit
  - Virtual Processor
  - Number of Virtual Sockets: 2
  - Number of cores per virtual Socket: 2
  - Memory: 16 GB
  - Hard Disk: 100 GB
  - Virtual Network Interface Cards: 1 Adapter: E1000

- Additional components required if implementing the high availability design option:
  - An additional physical server that is identical to the first one.
  - VMware vSphere Hypervisor (ESXi) 5.0 or higher.
  - Vsphere Client 5.0 or higher. This runs on a Windows platform.
  - Network File System1.
  - Center Server 5.1. This runs on a 64 bit Windows platform.

**Reverse Proxy Server**

A separate server is required to act as the Reverse Proxy server, similarly configured as the enterprise server, if accessing Cisco Extended Care from outside the enterprise network.

For the recommended TRC of UCS Server, refer to the Business Edition 6000M and Business Edition 6000H server configuration at the following URL:
Video Conferencing Data Center Components

Cisco Extended Care supports a variety of servers and multi-point bridges that typically reside in a data center.

Servers
Cisco Extended Care supports the following servers:

- Cisco Unified Communication Manager (CUCM), Version 10.5.2
- Cisco Remote Expert Application Mobile Server, Version 11.5 - SU1 (ES3)

With Cisco Extended Care, the application can support interoperability between diverse video endpoints in a point-to-point configuration, greatly reducing the cost of deployment.

Video Endpoints

The video endpoint facilitates video conferencing for two or more locations. Supporting a variety of video endpoints gives enterprises a choice in video quality, size/form factors, required bandwidth, and cost.

Cisco Extended Care is compatible with an SIP standards-based video conferencing system, and the compatibility falls into one of three categories:

- **Fully Integrated**—One click Join and Leave on the Cisco Extended Care window.
- **Partially Integrated**—One click Join on the Cisco Extended Care window, but ending the teleconference is handled outside of Cisco Extended Care.
- **Compatible but not Integrated**—Manual dial is required.

Cisco Extended Care helps facilitate video conferencing with the following video endpoints:

Hard Endpoints

- Cisco DX Series (DX80 - 10.2, DX70)
- Cisco TelePresence System EX Series (EX90 - 7.3.4)
- TelePresence SX Quick Set (SX20 - 7.1.4, SX10)
- Cisco Telepresence Integrator C Series, Version 5.1.0

Soft Endpoints

- Cisco Remote Expert Mobile 11.5 - SU1 (ES3)
- Jabber Client 11.5 (Windows 7, 8.1, 10; Mac 10.8.1, 10.9, 10.10)

Soft Client Browser Requirements

- On platforms that support WebRTC [Remote Expert Mobile 11.5 - SU1 (ES3)]
- Windows 7 (32/64-bit), Windows 8.1 (32/64-bit), or Mac OS-X 10.8, or later
Before You Begin Installation

For proper operation of the Cisco Extended Care application server, perform the following steps before performing the Cisco Extended Care application server software installation and configuration procedures.

### Step 1
Acquire the following values needed for installation:
- The Fully Qualified Domain Name (FQDN) (for example, hostname.subdomain.domain.tld) of every server and endpoint in the installation
- IP Address of the Cisco Extended Care Application Server
- Server Subnet Mask
- Server Gateway Address
- Domain Name System (DNS) Server 1 Address
- DNS Server 2 Address
- Domain Suffix
- Network Time Protocol (NTP) Server 1 and Server 2 addresses local to the network

### Step 2
Acquire the appropriate licenses for your installation.

### Step 3
Install and configure the applicable call management software. Configure the video endpoints. For information on how to install and configure these components, see “Appendix A, “Assorted Tasks.”“

- Plugin-Less Video (WebRTC)
- Chrome: Version > 47
- Firefox (Windows): Version > 44
- Firefox (Macintosh): Version > 44
- Chrome (Macintosh): Version > 23
Installing Software for the Cisco Extended Care Application Server

The Cisco Extended Care application server installation process consists of the following tasks that are described in this chapter:

1. Creating a Virtual Machine, page 2-1
2. Installing Cisco Extended Care on a Virtual Machine, page 2-4
   a. Verifying the Installation, page 2-8
   b. Changing the Password, page 2-9
3. Setting Up the Network Time Protocol (NTP), page 2-9
4. Synchronizing the JVM Time Zone, page 2-10
5. Generating the SSL Certificate for the Data Center Server, page 2-11

Note: Refer to your server vendor’s documentation for remote management configuration.

Creating a Virtual Machine

- If this is a multi-tenancy environment, create one VM for every tenant, up to a maximum of five.
- If this is a single-tenant environment, you still need to create one VM to take advantage of the high availability feature.

In both cases, after you create the VM, install the appropriate Cisco Extended Care Server software in the VM, and then set up NTP.

Note: If you do not have vSphere Client installed on your system, download the vSphere Client from the EXSi server, and run the installer.

Screen images are for reference purpose only and may change if you are using other clients like the vSphere web client.

To create a VM in a host, perform the following steps:
Creating a Virtual Machine

Step 1 Right-click the host’s IP address on the left. One of the two drop-down menus shown in Figure 2-1 appears.

Figure 2-1 Create New Virtual Machine

Step 2 Click New Virtual Machine from the drop-down menu. The Create New Virtual Machine window appears.

Step 3 Select the Custom check box. Then, click Next. The Name and Location window appears.

Step 4 Enter the name for the new virtual machine. Then click Next. The Datastore window appears.

Step 5 Select the data store you want to use for this virtual machine. (For high availability, it should be the NFS server you installed.) Click Next. The Virtual Machine Version window appears.


Step 7 Select Linux and choose Red Hat Enterprise Linux 6 (64-bit) from the drop-down menu. Click Next. The CPUs window appears.

Step 8 Choose 2 as the number of core processors from the drop-down menu. Click Next. The Memory window appears.

Step 9 Enter the memory size (16 GB). Click Next. The Network window appears.

Step 10 From the following drop-down menus:
1. How many NICs do you want to connect? Choose 1.
2. NIC 1: Choose VM Network.
3. Adapter: Choose E1000.
Select the Connect at Power On check box. Click Next. The SCSI Controller window appears.

Step 11 Select the LSI Logic Parallel check box. Click Next. The Select a Disk window appears.

Step 12 Select the Create a new virtual disk check box.

Step 13 Click Next. The Create a Disk window appears.
1. Specify the Disk Size as 100 GB. The large disk size is required to store log files. Older log files are purged, but only after a limit is reached.
2. Select the Allocate and commit space on demand (Thin Provisioning) check box.
3. Select the Store with the virtual machine check box.
4. Click Next. The Advanced Options window appears.

   **Step 14** Select the **SCSI (0:0)** check box. (Do not select the **Independent** check box.) Click Next. The summary appears.

   **Step 15** Select the **Edit the virtual machine settings before completion** check box. Click Continue. The Virtual Machine Properties window appears.

   **Step 16** Select the **New CD/DVD (adding)** check box to indicate that you want to boot this virtual machine from a CD.

   **Step 17** Click **Datastore ISO File** and choose the ISO file.

   **Step 18** Select the **Connect at power on** check box as shown in **Figure 2-2**.

   ![Figure 2-2 Booting from CD/DVD](image)

   **Warning** If you do not select the Connect at power on check box, the CD drive does not connect to the VM and the system fails to boot.

   **Step 19** Select **Options > Boot Options**. Increase the value in the **Power On Boot Delay** field.
Installing Cisco Extended Care on a Virtual Machine

This section describes the installation process of the Cisco Extended Care application server software on a VM.

To install the application server, perform the following steps:

**Step 1** Click the VM you configured in the left pane of the main window, and power the VM on.

**Figure 2-4  Power On the VM**

**Step 2** Click the **Console** tab, then click into the window, and press the **Esc** key to bring up the boot menu.
Step 3 Use the up and down arrow keys to navigate to the CD-ROM Drive option, and then press Enter.

Step 4 Enter the following command: #install.

Step 5 Press Enter. The installation process starts and takes several minutes to complete.

Step 6 After the installation process is completed, log in to the server with the following credentials:
   - Login: root
   - Password: changeit
Step 7 After you are logged in, enter the following command: `setup` to set up the network configuration. Then, press Enter. The Choose a Tool window appears.

Step 8 Use the tab key to select Run Tool, and press Enter. The Select Action window appears.
Step 9 Use the tab key to select Device Configuration, and press Enter. The Select a Device window appears.

Step 10 The default device is already selected. Press Enter. The Network Configuration window appears.

Step 11 Enter the appropriate network configuration details. Use the tab key to select OK, and then press Enter. The Select a Device window appears.

Step 12 Use the tab key to select Save, and then press Enter. The device configuration details are saved. The Select Action window appears.
Step 13 Use the tab key to select **DNS Configuration**, and then press **Enter**. The DNS configuration window appears.

![Figure 2-12 DNS Configuration Window](image)

Step 14 Enter the appropriate DNS configuration details. Use the tab key to select **OK**, and then press **Enter**. The DNS configuration details are saved. The **Select Action** window appears.

Step 15 Use the tab key to select **Save&Quit**, and then press **Enter**. The Choose a Tool window appears.

Step 16 Use the tab key to choose **Quit**, and then press **Enter**.

Step 17 Reboot the server/VM by entering the following command: `#reboot`.

---

### Upgrading the Extended Care Server

The following steps are used to upgrade extended care server:

- **Step 1** Download the upgrade files from cisco.com and copy it to the `/opt` folder on the Extended Care server.
- **Step 2** Extract the zip file.
- **Step 3** Add execute permissions to `upgrade-extcare-XXX.sh` - `chmod 777 upgrade-extcare-XXX.sh`.
- **Step 4** Run the upgrade script - `./upgrade-extcare-XXX.sh`.
- **Step 5** Check the `upgrade-extcare.log` for any errors.
- **Step 6** Log in to the **Admin** page and then check the **About** page.
- **Step 7** Verify the new version in the Web UI.

---

### Verifying the Installation

To verify the server installation, perform the following steps:

- **Step 1** After the server boots up, verify that you can log into the server as a root user via ssh.
- **Step 2** Verify that the services are running using the following command: `# service cec status`.

The command output for the Cisco Extended Care application server should be:
Changing the Password

To change the password, perform the following steps:

**Step 1** After the server boots up, verify that you can log into the server as a root user via SSH.

**Step 2** Enter the following command: `# passwd`.

**Step 3** Enter the new password in the **New Password** field, and then press **Enter**.

**Step 4** Re-enter the new password in the **Retype New Password** field, and then press **Enter**. The password is updated.

Setting Up the Network Time Protocol (NTP)

**Note**

All UC-related servers and the EC application server must be NTP synchronized. For example, if you are using VCS and MCU with the EC application server, they both should be NTP synchronized. The reset session timer will execute at the proper time only when the server time is in sync with the NTP timing.

To set up NTP, perform the following steps:

**Step 1** Open the file `/etc/ntp.conf` for editing.

**Step 2** Add the following line to the top of the `ntp.conf` file: `tinker panic 0`

**Step 3** Locate the following lines in the file:

```
server 0.rhel.pool.ntp.org iburst
server 1.rhel.pool.ntp.org iburst
server 2.rhel.pool.ntp.org iburst
```

These represent the Red Hat NTP servers. Ideally, you should use NTP servers within close proximity to your data center. While these work, they are not the best choice.

**Step 4** Add the `#` character at the beginning of each of these the lines to make them comments. They should now appear as follows:

```
# server 0.rhel.pool.ntp.org iburst
# server 1.rhel.pool.ntp.org iburst
# server 2.rhel.pool.ntp.org iburst
```

**Step 5** Add an entry for the NTP server with which this server will sync time. (These should be listed in the NIP.) The entry should look similar to these:

```
server [ip_addr_ntp_server1]
```
Synchronizing the JVM Time Zone

In the ISO build, the JVM time zone should be in sync with the VM time zone. Whenever the user changes the VM time zone, the user has to manually run the following script to keep JVM time zone in sync with the updated VM/OS time zone.

vi /etc/sysconfig/clock

Update the following settings:

ZONE="(server timezone)"
UTC=false
ARC=false
Write and Exit (:wq)

service cec restart
To synchronize time, use the following command:

```
hwclock --systohc --localtime
```

Use the "hwclock" command to check status of hardware clock:

---

## Generating the SSL Certificate for the Data Center Server

This section describes how to generate the Secure Socket Layer (SSL) certificates for the Data Center servers.

---

**Note**

Before performing this procedure, determine if your installation uses the Domain Name Server (DNS) or IP addresses at the endpoints to identify the Data Center servers.

---

To install OpenSSL signed certificate, perform the following steps:

---

**Step 1**

SSH/console into the server and run the following commands, with the desired server address:

```
export SERVER_IP=<Server Address>
sudo openssl genrsa -out /etc/pki/tls/private/localhost.key 4096
```

**Note**

For netscaler use encryption key - 2048 instead of 4096.

```
sudo openssl req -new -key /etc/pki/tls/private/localhost.key -subj "/CN=${SERVER_IP}" -out /etc/pki/tls/certs/localhost.csr
```

---

**Step 2**

Submit the contents of `/etc/pki/tls/certs/localhost.csr` to the certificate signer.

**Note**

Request the certificate in BASE64 fFormat.

---

**Step 3**

After you receive the signed certificate from the certificate signer, place it in `/etc/pki/tls/certs/localhost.crt`.

**Step 4**

Restart Apache HTTPD via `sudo service httpd restart`. 
Configuring the Cisco Extended Care Application Server

This chapter describes how to configure the Cisco Extended Care application server, including configuring system parameters and adding new endpoint information.

Prerequisites

Before configuring the Cisco Extended Care Administration Server, the following configurations must be in place in the Cisco Unified Communications Manager (CUCM) and Remote Expert Mobile (REM) servers.

CUCM

You will perform the following major steps:

1. Create partitions for Managers, All users, and CTI route point.
2. Create CTI route point: Cisco Unified Communications Manager requires creation of CTI Route Point to intercept and route calls from managers.
3. Configure endpoints.
4. Add end users.
5. Associate end users to controlled devices.

REM

You will perform the following major steps:

1. Configure the outbound server to be the CUCM IP or Hostname.
2. Add a web application ID

The Cisco Extended Care application server configuration process consists of the following tasks:

Note

After you log in, you can perform the subsequent tasks in any order.

- Logging into the Cisco Extended Care Administration Server, page 3-2
Logging into the Cisco Extended Care Administration Server

To log in to the Cisco Extended Care administration server, perform the following steps:

**Step 1**  Access the following URL in a web browser: https://[IP_address_application_server]/admin/. The Cisco Extended Care Server Administration login page appears.

*Figure 3-1  Cisco Extended Care Server Administration Login Page*

**Step 2**  Log in using the default login values.

- Username = `sysadmin`
- Password = `cisco123`

The Cisco Extended Care Server Administration home page appears. The drop-down menu under **Configuration** lists the configuration possibilities for this server. (You can optionally change the password at any time. If you change the password, record the new password in the Network Implementation Plan.)
Uploading the Cisco Extended Care License Files

The Cisco Extended Care system can include the license files listed here. Every license file that applies to this installation should have already been copied to the computer you are working from.

- **Server**—Locks the application to a specific hardware machine (MAC address).
- **Resource**—Controls the maximum number of endpoints.

To upload a license file into Cisco Extended Care application server, for each file, perform the following steps:

**Step 1** Choose **Upload License File** from the **Configuration** drop-down menu. The **Upload License File** pane appears.
Step 2  Browse to the location where you copied the license file you want to upload the file. Click **Upload**.

- Repeat steps 1 and 2 for every license file.

Step 3  To view license files that have already been uploaded, click on the license file name.

Step 4  To view license details, click **License Information** from the **Configuration** drop-down menu. The **License Information** pane appears.

**Figure 3-4  License Information**

---

### Configuring the System Parameters

#### Activation

These parameters should be left with their default values. Do not configure the system parameters unless the Cisco personnel direct you to do so.

#### Resetting Endpoint Sessions

Extended Care provides the ability to reset orphaned endpoint sessions on a regular basis (configurable).

**Note**

This is one parameter under System Parameters that you can configure based on your requirements.

By default, endpoint sessions, appointment sessions, conference sessions, and dependent databases that are active for more than four hours are removed from the Extended Care database.

**Note**

The reset session timer will execute at the proper time only when the server time is in sync with the NTP timing.

To configure the system clean-up timer, perform the following steps:
Step 1  To view the system parameters defined for this Cisco Extended Care application server, choose System Parameters from the Configuration drop-down menu. The System Parameters pane appears.

Figure 3-5  System Parameters Pane

Step 2  To modify the endpoint reset timer, enter the appropriate time in the System Cleanup Timer field. The default value in the system is 4 hours.

Step 3  Change the collaboration API Password to match your call control key on EMR URL.

Step 4  Click Save.

Configuring the Regions

By default, all endpoints managed by a single instance of Cisco Extended Care belong to the default region. If you have multiple call control regions (separate UC resources), you can add regions. This helps enable you to add endpoint computers, later, to the appropriate region corresponding to the desired UC resource, as described in Configuring the Endpoints, page 3-11.

To configure the regions for this Cisco Extended Care application server, perform the following steps:

Step 1  To view the list of configured regions for this Cisco Extended Care application server, choose Regions from the Configuration drop-down menu. The Regions pane appears.

Figure 3-6  Regions

Step 2  To update any listed region, click the region ID that you want to update. The Update Region pane appears.
**Step 3** Update the Region Name and then click **Save**.

**Step 4** To add a region, click **Add**. The **Add Region** pane appears.

![Add Region Pane](image)

**Step 5** Enter a Region ID that is unique for this instance of Cisco Extended Care. The region ID can contain only letters, numbers, underscores (_) and dashes (-).

**Step 6** Enter a region name. The name can use any characters.

**Step 7** Click **Save**.

**Note** If you need to delete a region, select the check box to the left of the designated Region ID in the Regions pane and then click **Delete**.

---

**Configuring the UC Servers**

Cisco Extended Care supports two types of unified communications (UC) servers:

- Cisco Unified Communications Manager (CUCM)
- Remote Expert Mobile (REM)

Unified communications servers are required for video conferencing.

To configure the UC servers, perform the following steps:
**Step 1**
To view the list of the configured UC servers for this Cisco Extended Care application server, choose **UC Servers** from the **Configuration** drop-down menu. The **UC Server** pane appears.

**Figure 3-8  UC Server Pane**

**Step 2**
To modify the configuration for a UC server, click the UC Server ID of the UC server you want to update. The **Update UC Server** pane appears.

**Figure 3-9  CUCM - Sample Configuration**

**Figure 3-10  REM - Sample Configuration**
Step 3  You can modify all the fields except UC Server ID. Click **Save**.

Step 4  To add a UC server, click **Add**. The **Add UC Server** pane appears.

*Figure 3-11  Add UC Server*

![Add UC Server](image)

Step 5  Choose the UC server model from the **UC Server Type** drop-down list, and enter the appropriate values for all the other fields. Note that the fields may vary depending on which server model you choose.

*Table 3-1  UC Server Type - CUCM or VCS Expressway or VCS Control*

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>UC Server Id</td>
<td>Enter a meaningful name for the UC server you are adding in Extended Care.</td>
</tr>
<tr>
<td>UC Server Type</td>
<td>Choose the UC server model from the <strong>UC Server Type</strong> drop-down list.</td>
</tr>
<tr>
<td>UC Server HostName</td>
<td>Enter the IP address of the UC server as configured in CUCM.</td>
</tr>
<tr>
<td>UC Server Description</td>
<td>Enter an appropriate description for the UC server.</td>
</tr>
<tr>
<td>UC Server URL</td>
<td>Enter the UC Server URL as configured in CUCM. For example,</td>
</tr>
<tr>
<td></td>
<td><code>https://&lt;UC Server Hostname&gt;</code></td>
</tr>
<tr>
<td>UC Server Access Id</td>
<td>Enter the user ID created for the end user in CUCM.</td>
</tr>
<tr>
<td>UC Server Access Password</td>
<td>Enter the password corresponding to the UC Server Access ID as created in CUCM.</td>
</tr>
<tr>
<td>Device Pool Enabled</td>
<td>This field is visible if the selected UC server type is CUCM. Select the check box.</td>
</tr>
<tr>
<td></td>
<td>The Cisco Extended Care server is configured with a pool of numbers it uses</td>
</tr>
<tr>
<td></td>
<td>for API endpoints and a starting phone number. When the add endpoint API</td>
</tr>
<tr>
<td></td>
<td>is called, the Cisco Extended Care server assigns it the next available number</td>
</tr>
<tr>
<td></td>
<td>in its pool.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Device Pool Size</strong>—Enter the number of devices configured for an</td>
</tr>
<tr>
<td></td>
<td>application that is integrating with Cisco Extended Care.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Starting Phone Number</strong>—Enter the starting phone number for the</td>
</tr>
<tr>
<td></td>
<td>Device pool as configured in CUCM.</td>
</tr>
<tr>
<td>API Mode</td>
<td>This field is visible if the selected UC server type is VCS Expressway or</td>
</tr>
<tr>
<td></td>
<td>VCS Control.</td>
</tr>
<tr>
<td></td>
<td>Choose the supported API XML type for the VCS devices from the <strong>API Mode</strong></td>
</tr>
<tr>
<td></td>
<td>drop-down menu. VCS 8 and above supports formputxml, whereas</td>
</tr>
<tr>
<td></td>
<td>versions below 8 support putxml.</td>
</tr>
</tbody>
</table>
Configuring the UC Server Groups

Cisco Extended Care helps enable you to configure the UC server groups. These groups enable you to specify a group of UC servers that can be used by an endpoint to establish the telepresence conferences. To make a telepresence call on behalf of an endpoint, the Cisco Extended Care application server attempts to reach any of the servers in the group.

When creating the UC server groups:

- Configure all the UC servers before you configure the UC server groups. You can add the UC servers to a UC server group, but you cannot specify a UC server group when configuring a UC server.

### Configuring the UC Server Groups

Cisco Extended Care helps enable you to configure the UC server groups. These groups enable you to specify a group of UC servers that can be used by an endpoint to establish the telepresence conferences. To make a telepresence call on behalf of an endpoint, the Cisco Extended Care application server attempts to reach any of the servers in the group.

When creating the UC server groups:

- Configure all the UC servers before you configure the UC server groups. You can add the UC servers to a UC server group, but you cannot specify a UC server group when configuring a UC server.

#### Configuring the UC Server Groups

Cisco Extended Care helps enable you to configure the UC server groups. These groups enable you to specify a group of UC servers that can be used by an endpoint to establish the telepresence conferences. To make a telepresence call on behalf of an endpoint, the Cisco Extended Care application server attempts to reach any of the servers in the group.

When creating the UC server groups:

- Configure all the UC servers before you configure the UC server groups. You can add the UC servers to a UC server group, but you cannot specify a UC server group when configuring a UC server.

#### Configuring the UC Server Groups

Cisco Extended Care helps enable you to configure the UC server groups. These groups enable you to specify a group of UC servers that can be used by an endpoint to establish the telepresence conferences. To make a telepresence call on behalf of an endpoint, the Cisco Extended Care application server attempts to reach any of the servers in the group.

When creating the UC server groups:

- Configure all the UC servers before you configure the UC server groups. You can add the UC servers to a UC server group, but you cannot specify a UC server group when configuring a UC server.

<table>
<thead>
<tr>
<th>Table 3-2</th>
<th>UC Server Type - REM</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>UC Server Id</td>
<td>Enter a meaningful name for the UC server you are adding in Extended Care.</td>
</tr>
<tr>
<td>UC Server Type</td>
<td>Choose the UC server model from the UC Server Type drop-down list.</td>
</tr>
<tr>
<td>UC Server HostName</td>
<td>Enter the IP address of the UC server as configured in REM.</td>
</tr>
<tr>
<td>UC Server Description</td>
<td>Enter an appropriate description for the UC server.</td>
</tr>
<tr>
<td>UC Server URL</td>
<td>Enter the UC Server URL as configured in REM. For example, <code>https://&lt;REAS-External-Cluster-Address&gt;:443/gateway/</code></td>
</tr>
<tr>
<td>Application ID</td>
<td>Enter the application name as configured in REM server.</td>
</tr>
<tr>
<td>UC Server Domain</td>
<td>Internal FQDN of REAS Server</td>
</tr>
<tr>
<td>Interop Enabled</td>
<td>Select the Interop Enabled check box to enable calls between REM and CUCM servers.</td>
</tr>
<tr>
<td>Interop UC Server Host Name</td>
<td>Enter the IP address of the CUCM server with which the REM server will communicate.</td>
</tr>
<tr>
<td>Device Pool Enabled</td>
<td>This field is visible if the selected UC server type is REM. Select the check box. The Cisco Extended Care server is configured with a pool of numbers it uses for API endpoints, and a starting phone number. When the add endpoint API is called, the Cisco Extended Care server assigns it the next available number in its pool.</td>
</tr>
<tr>
<td>Device Pool Size</td>
<td>— Enter the number of devices configured for an application that is integrating with Cisco Extended Care.</td>
</tr>
<tr>
<td>Starting Phone Number</td>
<td>— Enter the starting phone number for the Device pool as configured in REM.</td>
</tr>
</tbody>
</table>

| Step 6 | Click **Save**. |

| Note | If you need to delete a UC server, select the check box to the left of the designated UC Server ID in the UC Server pane and then click **Delete**. |
- The default UC server group is empty until you add servers to it. Therefore, during installation, you must click Default in the list of UC server groups, and then select servers to add to the default group.
- When the endpoints are configured, they are associated with a UC server group. If no UC server group is specified, the endpoint will use the default UC server group.

To configure a UC server group, perform the following steps:

**Step 1**
To view the list of the configured UC server groups for this Cisco Extended Care application server, choose UC Server Groups from the Configuration drop-down menu. The UC Server Group pane appears.

**Figure 3-12 UC Server Group Pane**

**Step 2**
To modify the configuration for a UC server, click the UC Server Group ID of the UC server group you want to update. The Update UC Server Group pane appears.

**Step 3**
You can modify all the fields except UC Server Group ID. Click Save.

**Step 4**
To add a UC server group, click Add. The Add UC Server Group pane appears.

**Figure 3-13 Add UC Server Group**

**Step 5**
Specify the UC Server Group ID, UC Server Group Description, and select the UC Servers check box that you want to include for this group. Then click Save.
Configuring the Endpoints

For the application server to manage video calls, you must configure the telepresence attributes of the video endpoint.

To configure the endpoints, perform the following steps:

**Step 1**  To view the list of endpoints configured for this Cisco Extended Care application server, choose **Endpoints** from the **Configuration** drop-down menu. The Endpoints pane appears.

**Figure 3-14  Cisco Extended Care Endpoints Pane**

**Step 2**  To modify the configuration of an existing endpoint, click the Endpoint ID of the endpoint you want to update. The **Update Endpoint** pane appears.

**Step 3**  Modify the applicable editable fields. Click **Save**.

**Step 4**  To add an endpoint, click **Add**. The **Add Endpoint** pane appears.
Step 5  Enter applicable information in the fields.

Table 3-3  Basic Configurations

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Endpoint Id</td>
<td>The Endpoint Id must be unique among all endpoints communicating within a tenant. It can include any alphanumeric characters, underscores, or dashes. The ID you enter should be meaningful and must be able to indicate the endpoint being used.</td>
</tr>
<tr>
<td>Endpoint Name (Location)</td>
<td>The Endpoint Name (Location) will appear on the provider’s Ready Appointments pane, so the location name should be something meaningful and unique (such as Molina clinic or Mayo Cardiac Telemedicine Room.) The characters of the endpoint location have no restrictions.</td>
</tr>
<tr>
<td>Endpoint Type</td>
<td>Only one endpoint type, the API Endpoint, is available. It is auto populated</td>
</tr>
<tr>
<td>API Endpoint Password</td>
<td>Enter any password in the API Endpoint Password field. This is user defined.</td>
</tr>
<tr>
<td>Region</td>
<td>Specify the Region. The default region includes all the meeting resources configured to this Cisco Extended Care application server.</td>
</tr>
<tr>
<td>OS Type</td>
<td>Select the OS Type. Choose from Windows, Mac, or iPhone/iPad as needed.</td>
</tr>
</tbody>
</table>

Step 6  Click **Unified Communications**. The **Unified Communications** pane appears.
Step 7 Enter the applicable information in the fields as specified in the Network Implementation Plan, Endpoints tab.

Table 3-4 Unified Communications

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Video Endpoint Type</td>
<td>Choose the Video Endpoint Type from the list. The drop-down menu lists the compatible video endpoints that have been configured in CUCM or REM. If you specify Others, then the support defaults to Manual Dial. Not all the fields are enabled for all the endpoints. Based on the endpoint selected, the relevant fields get enabled for user updates.</td>
</tr>
<tr>
<td>Manual Dial</td>
<td>Manual Dial is for support only. Do not select this check box unless you are supporting a problem or instructed to do so by a Cisco representative. It can be modified during support and then set back to its original setting.</td>
</tr>
<tr>
<td>Outside the Enterprise</td>
<td>Select the Outside the Enterprise check box if this is a Provider endpoint outside of the enterprise network and the Providers at this endpoint need the ability to receive video calls from an endpoint inside the enterprise network.</td>
</tr>
<tr>
<td>Enable Dynamic IP</td>
<td>Select the Enable Dynamic IP check box if you want your endpoint to be IP address independent. If you have selected this check box, enter the FQDN instead of the IP address in the Video Endpoint IP Address field.</td>
</tr>
<tr>
<td>Phone Number</td>
<td>Enter the Phone Number associated with the device pool for this video endpoint in CUCM.</td>
</tr>
<tr>
<td>Video Endpoint Host Name</td>
<td>Enter the Video Endpoint Host Name, which is derived from the MAC address (if hard endpoint) and Device Name (if soft endpoint) as configured in CUCM.</td>
</tr>
<tr>
<td>Video Endpoint IP Address</td>
<td>Enter the Video Endpoint IP Address, which is configured in CUCM for this video endpoint. The corresponding field in CUCM is IPv4 Address.</td>
</tr>
<tr>
<td>Video Endpoint Access Id</td>
<td>Enter the Video Endpoint Access ID, which is configured in CUCM for this video endpoint.</td>
</tr>
<tr>
<td>Video Endpoint Password</td>
<td>Enter the Video Endpoint Password, which is configured in CUCM for this video endpoint.</td>
</tr>
<tr>
<td>UC Server Group</td>
<td>Specify the UC Server Group, CUCM or REM. Except for REM-based endpoints, for all other endpoints, the selection would be CUCM.</td>
</tr>
</tbody>
</table>
Step 8. Click **Save**. The system message *Successfully added Endpoint <Endpoint Id>* appears.

Step 9. Repeat Steps 2-5 for all the applicable endpoints.

**Note**: If you need to delete an endpoint, select the check box to the left of the designated Endpoint ID in the Endpoints pane and then click **Delete**.

---

### Configuring the Security Policy

To configure the security policy to be used by this enterprise, perform the following steps:

**Step 1**. Choose **Security Policy** from the **Configuration** drop-down menu. The **Security Policy** pane appears.

**Figure 3-17 Security Policy Pane**

Configure the policy as described below:

1. Select **Enabled** if you want to lockout (that is, automatically log out) a user for PC inactivity during a session.
   - If enabled, specify the inactivity warning time and logout time.

2. The **Inactivity Warning Time** is a warning message that appears on an EC PC after a specified number of minutes of no activity (pressing enter, clicking a mouse key, etc.) during a session. The time between activity and when the inactivity warning message appears can be set from 1 to 999 minutes.
3. The **Logout Time** is the amount of time AFTER the Inactivity Warning before the end user is logged off. It can be between 1 and 60 minutes.

**Step 3** When complete, click **Save**.
# Assorted Tasks

This appendix includes the following major topics:

- Values to be Gathered Before Installation, page A-1
- Troubleshooting, page A-2
- Additional Resources, page A-2

## Values to be Gathered Before Installation

Table A-1 describes the information that must be gathered to complete the installation.

<table>
<thead>
<tr>
<th>Information</th>
<th>Value(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fully Qualified Domain Names (FQDNs) for Cisco Extended Care Application Server</td>
<td>--</td>
</tr>
<tr>
<td>Domain Name System (DNS) Server 1 Address</td>
<td>--</td>
</tr>
<tr>
<td>DNS Server 2 Address</td>
<td>--</td>
</tr>
<tr>
<td>Domain Suffix</td>
<td>--</td>
</tr>
<tr>
<td>IP Addresses of Application Server</td>
<td>--</td>
</tr>
<tr>
<td>Server Subnet Mask</td>
<td>--</td>
</tr>
<tr>
<td>Server Gateway Address</td>
<td>--</td>
</tr>
<tr>
<td>Network Time Protocol (NTP) Server 1 and Server 2 Addresses</td>
<td>--</td>
</tr>
<tr>
<td>Prescription header and footer, if applicable (for E-Pen)</td>
<td>--</td>
</tr>
<tr>
<td>Applicable licenses for this installation</td>
<td>--</td>
</tr>
</tbody>
</table>
Troubleshooting

Incorrect Number of Licenses Displayed

During very heavy loads, the Cisco Extended Care Admin Home page may indicate a greater number of end user licenses in use than is actually the case. To resolve this issue, you must restart the service connecting the endpoints as follows:

1. Open a command shell on the Application Server and log on as root.
2. Type the command service cec restart and then press Enter.

Additional Resources

The *Cisco Extended Care Application Server Installation and Administration Guide* does not include details on configuring unified communication and video components. Use the following tables, which include links to supporting documentation, as guidelines for the configuration process.

Installing and Configuring CUCM, VCS, and TMS

The following resources and associated reference URLs will help you to install and configure CUCM, VCS, or TMS.

- Installing Cisco Unified Communications Manager.

- Installing Cisco Remote Expert Mobile.

Configuring Telepresence Endpoint in CUCM

The following steps and associated reference URLs will help you to configure a Video endpoint.

**Step 1** Create a Session Initiation Protocol (SIP) trunk to integrate a Telepresence endpoint and CUCM.


**Step 2** Create an application user in CUCM.


**Tip** Refer to this document to configure CUCM for all Telepresence endpoints in the Cisco Extended Care software.

**Step 3** Configure REP.

B

Business Entity  In Cisco Extended Care, refers to the resources (patient and provider endpoints and users) managed by a single Cisco Application Server.

C

Cisco Extended Care Administration  The application used by the installation team to configure, administer and manage the Extended Care Application Server.

Cisco Extended Care Application Server  The Cisco Extended Care component that maintains the master information of resources and manages conferences, sessions and appointments. The Application Server interfaces with Admin, Portal, and the Unified Communications (UC) servers.

Cisco Extended Care Package  The orderable software that includes the Cisco Extended Care Application Server and Cisco Administration.

Cisco Extended Care Software  Cisco Extended Care is a software-defined platform that facilitates patients connecting with healthcare professionals in a telehealth environment.

Cisco TelePresence Video Communication Server  A video server that provides Session Initiation Protocol (SIP) proxy and call control as well as H.323 gatekeeper services for video endpoints. The Cisco VCS Control application connects all infrastructure, management, and endpoints and is critical to interoperability with unified communications and IP telephony networks and voice-over-IP (VoIP) endpoints.

Cisco Unified Communications Manager  The application that extends enterprise telephony features and capabilities to packet telephony network endpoints, such as IP phones and multimedia applications. Open telephony application interfaces make possible services, such as multimedia conferencing and interactive multimedia response systems.

CTMS  See Cisco TelePresence Multipoint Switch

CUCM  See Cisco Unified Communications Manager

CUVC  Cisco Unified Video Communications

H

Hosted  In Cisco Extended Care, refers to a software delivery model in which the Cisco Extended Care software and associated client data reside in a central location managed by a hosting service and accessed by clients using a web browser.
P

**Partner Server**

The partner server can be any of the systems available with the partner/customer that is connected with Cisco Extended Care, such as:

- A HL7-based EMR—for patient information and appointment scheduling.
- A wellness readings Store server—to save and/or retrieve wellness readings.
- An iFrame-based integration with an existing partner/customer portal—for providing an integrated user experience across portals with single sign-on (SSO).
- A custom authentication system being used by the partner/customer—to authenticate Providers.
- A custom scheduling system being used by the partner/customer—for appointment scheduling.

**Provider**

A medical professional who provides medical consultation in a Cisco Extended Care environment.

**Provider Endpoint**

A computer from which the end user logged in as a provider and that acts as that provider’s associated video endpoint.

T

**TeleHealth**

The delivery of health-related services and information via telecommunications technologies. Telehealth is an expansion of telemedicine, and, unlike telemedicine (which more narrowly focuses on the curative aspect), it encompasses preventive, promotive and curative aspects.

U

**UC**

Unified Communications

**User Profile**

Your User Profile determines which pages you see, and which functions you can perform. User IDs are configured so that users with a particular role (or roles) see only the pages and options appropriate to that job description. Any given user can have from one to five roles, or User Profiles, within one User ID. The Site Administrator configures the User IDs.

V

**VCS**

Video Communication Server