Moderro
IEM Management Software

Installation Guide

Release 2.6

Moderro Technologies

www.moderro.com

Table of Contents

Preface

This preface describes the purpose, audience, content organization, and conventions in this guide, and provides information on the related documents.

- Purpose
- Audience
- Organization
- Document Conventions
- Related Documentation

Purpose

This guide provides information about the Moderro Interactive Experience platform system. This user guide explains how to use the Moderro Interactive Experience Client 4650. This user guide provides instructions so that an administrator or user can:

- Connect the equipment
- Configure the system
- Configure the network
- Connect to the Moderro Interactive Experience Manager
- Register an account
- Configure local settings for demos

Audience

The intended audience for this guide are administrators who will install, manage, and upgrade the Moderro Interactive Experience hardware and software.

Organization

Title	Purpose
Introduction	This chapter explains the audience and scope of this user guide and provides an overview of the Moderro Interactive Experience Manager.
Installing the IEM Software	This chapter explains how to install the IEM software on a virtual machine.
Configuring the IEM Software	This chapter explains how to configure the IEM software after it has been installed on a virtual machine.
Using the IEM Configuration Menu	This chapter explains how to use the IEM Configuration Menu that is accessed by using a SSH client.
Upgrading the IEM	This chapter explains how to upgrade from an earlier VM.
Adding or Upgrading the IEC Firmware	This chapter explains how to add or upgrade the IEC firmware.
Starting the Web Service	This chapter explains how and when to enable the device gateway so that the IEM can communicate with the IECs.
Management Server (IEM) IP Provisioning with DHCP	This chapter explains how to auto connect the IEC to the IEM by provisioning the Management Server (IEM) IP with DHCP.

Document Conventions

Convention	Indication
bold font	Commands, keywords, and user-entered text appear in the **bold** font.
italic font	Document titles, new or emphasized terms, and arguments for which you assign values are in the *italic* font.
[ ]	Elements in the square brackets are optional.
{x | y | z}	Required alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A non-quoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
courier font	Terminal sessions and information that the system displays appear in the courier font.
courier bold font	Command names and samples appear in the **courier bold** font.
< >	Non-printing characters, such as passwords, are in the angle brackets.
[ ]	Default responses to the system prompts are in the square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.
Option > Option	Used to describe a series of menu options.

Note Means *reader take note*. Notes contain suggestions or references to materials that are not covered in the guide.

Related Documentation

Moderro Interactive Experience Platform Installation Guide

Introduction

Last Revised: October 27, 2016

Chapter Overview

The Moderro Interactive Experience Manager is software that allows for centralized management of Moderro Interactive Experience Client 4600 Series devices.
This chapter explains the audience and scope of this installation guide and provides an overview of the Moderro Interactive Experience Manager.
The sections in this chapter are:

- About This Installation Guide
  - Terminology
  - Audience
  - Scope
- Moderro Interactive Experience Platform
  - Moderro Interactive Experience Client 4600 Series
  - Moderro Interactive Experience Manager
  - Principles of Operation

About This Installation Guide

This section describes the audience and scope of this installation guide.

Terminology

The following terms are used in this user guide.

- Accounts - Allow multiple organizations to configure and manage devices and policies in a single Moderro Interactive Experience Manager instance. Use accounts to segregate users, devices, and policies. Each organization will have at least one account.
- Administrators - People who have access to all accounts on the system. This *Moderro Interactive Experience Manager Installation Guide* provides administrators with all the information necessary to install and administer a Moderro Interactive Experience Manager.
- Device - Moderro Interactive Experience Client 4600 Series
- Policies- An easy and flexible way of applying settings to multiple devices or users.
- Profiles - The settings of a single device or user.
- Users - People who configure and manage the Moderro Interactive Experience Manager. Users are associated with specific accounts on the Moderro Interactive Experience Manager. The *Moderro Interactive Experience Manager User Guide* was developed for users.

Audience

The intended audience for this guide is administrators. They will install, manage, and upgrade the Moderro Interactive Experience hardware and software.

Scope

This installation guide explains how to install the Moderro Interactive Experience Manager software. There is also a troubleshooting chapter so that the administrator can handle simple installation issues.

This user guide provides instructions so that an administrator can:

- Set up the Interactive Experience Manager
- Enable supported products
- Create and delete administrators
- Upgrade product version
- Add new products and models

After the Moderro Interactive Experience Manager has been installed, refer to the *Moderro Interactive Experience Manager User Guide* for instructions on how to use it to configure and manage Moderro Interactive Experience Client 4600 Series.

Moderro Interactive Experience Platform

The Moderro Interactive Experience Platform leverages the network as the platform to transform customer experience with interactive digital media. Leveraging Moderro's video, collaboration, and cloud architectures, the solution allows large and small enterprises and public agencies to seamlessly provide the most updated product or service information including educational content in real-time, improving customer experience and increasing customer retention. With built-in remote management capabilities, the solution enables organizations to get feedback instantaneously from end users to measure marketing
effectiveness and impact as well as dynamically provision and disperse relevant content. Effective reuse of web content and applications along with remote delivery of content and advertisements helps increase advertising revenues, improve business and customer processes, through effective management of digital displays and open online spaces.

The Moderro Interactive Experience Platform is the collective name for a product family that consists of thin clients hardware and software known as the Moderro Interactive Experience Client 4600 Series and remote management software which is called the Moderro Interactive Experience Manager.

Moderro Interactive Experience Client 4600 Series

The Moderro Interactive Experience Client 4600 Series (IEC4600 Series) is a robust, configurable, and manageable web device designed for public venues and web-centric delivery. The devices can be controlled remotely using management software, the Moderro Interactive Experience Manager (IEM).

It is highly recommended that all the Moderro IEC4600 Series devices are managed and monitored using the Moderro Interactive Experience Manager as it ensures consistent remote management, with the option to configure the devices locally.

Moderro Interactive Experience Manager

The Moderro Interactive Experience Manager (IEM) is the management software that allows the administrator to control and monitor Moderro IEC4600 Series devices. The Moderro IEC4600 Series devices are configured remotely through a combination of device, user, profile, and policy settings from the Moderro IEM.

Configuration settings are distributed between user and device settings; however profiles contain all the settings available to both device and users. Policies represent dynamic and transportable setup rules.

Moderro IEM is a solution allowing configuration, control, and support of Moderro Interactive Experience Client 4600 Series devices. With Moderro IEM, an administrator can perform the following functions:

- Configuration - Moderro IEM allows the administrator to configure the Moderro IEC4600 Series devices. IEC4600 Series devices can be configured to start with a predetermined Internet resource, such as a web page, flash, or movie, and then let the user navigate within a "walled garden" environment.
- Policy Management- Policies provide an easy and flexible way for administrators to apply settings to a group of users or devices.
- Session Management - An administrator can apply a session time limit to IEC4600 Series devices.
- Remote Control - Administrators can control the behavior of the IEC4600 Series devices in real-time including muting a station, locking out the user, or sending the user a message.
- Remote Assistance - To ask for help, users can simply press a help button on the screen to initiate a chat session with a virtual attendant or remote agent.
- Logs - Moderro IEM can be set up to log the traffic from the Moderro IEC4600 Series devices, making it easy for the administrators to analyze the data.

Principles of Operation

The following are principles of operation for this solution:

1. **IEC4600 Series devices need to exist on the IEM in order to be managed by it.** IEC4600 Series devices can either be provisioned ahead of time or from the device interactively. If registered from the device interactively, the installer has to use their account info to authorize the registration.
2. **Policy applied to a device overrides its profile.** Policies are templates for property settings.
3. **Multiple policies can be attached to the same device (group).** If policies contain conflicting settings, the policy that is higher in the stack order takes precedence. Device policies take precedence over group policies.
4. **IEC4600 Series and IEM versions are best-effort compatible.** A device that has a version that is not actively supported by the IEM will still be supported although some things may not have full functionality. A device version which is out of sync is indicated by the red FW flag. Communication between client and the IEM is defined by the communication protocol and specification that defines capabilities of each FW build. Older communication protocols are supported in the newer builds, but older specifications that reflect properties of the firmware are often not fully compatible with the later versions.

5. **Policies can be persistent or runtime (applied for short periods of time).** Persistent policies are long-term or permanent. Persistent policies are applied when the IEC4600 Series device is booted or rebooted. Persistent policies are permanent until they are unapplied.

   Runtime policies are created by checking the IsAction check box when creating the policy or in the General tab of the policy. Runtime policies are marked by a blue circle with a white arrow and are made available in form of a button under “Custom Actions”. These policies change the settings on the IEC4600 Series temporarily and will be reset by changing the settings within the policy, by applying counter action policy, or on the next reboot. IsAction policies can only work for runtime properties, which are marked by an orange arrow in the policy or profile.

6. **Alerts work on a subscription basis.** Once an alert has been created, it has to be assigned to a user. An alert can submit to a third party application collecting the data – the URL has to be provisioned through the User profile.

7. **In order to optimize screen behavior, the application has to implement native components.** Native components are available in form of a Browser API (refer to the documentation) and essentially move resource-intensive or asynchronously used components outside of the browser process-space.

Installing IEM Software

Chapter Overview

This chapter explains how to install the IEM software on a virtual machine. The sections in this chapter are:

What You Will Need

To install and configure the Moderro IEM, you will need the following:

- IEM software files downloaded from www.cisco.com:
  1. IEM-VM ISO file
  2. IEM OVA.zip file

Note The OVA.zip file includes five OVA files with different vCPU configurations. You should use the appropriate OVA file based on the number of IECs that you are deploying.

- IEM license
- IP address of host server
- Network credentials
- Server requirements:
  - A server (Cisco or third-party) running VMware ESXi 5.0 or above
- If High Availability is required:
  - Minimum of two ESX/ESXi hosts
  - Cluster setup with external shared storage
  - vSphere HA configured and enabled on the server

IEM Server Requirements

Table 2-1 Physical Server

Model	UCSC-C220-M35
CPU Cores	16 CPUs x 2.40 GHz
Processor Type	Intel Xeon CPU E5-2665 @ 2.40GHz
Processor Sockets	2
Cores per Socket	8
Logical Processors	32
Hyperthreading	Active

The table below lists recommended number of vCPUs for the number of IECs deployed for each IEM.

Note The numbers of recommended vCPUs in the table below are based on a high volume of event requests (e.g. 45 event requests per minute) from IECs. The required number of vCPU may vary depending on the number of event requests and other factors.

Table 2-2 vCPU Recommendations

Number of IECs	Recommended Number of vCPUs (Average CPU Usage)
100	2 (47%)
300	6 (51%)
500	8 (67%)
700	12 (75%)
1000	16 (78%)

Gather the IEM Software Files

The IEM-VM ISO and IEM OVA files are available for download. Follow the steps below to download them.

Step 1 Enter the following URL in your web browser: http://www.cisco.com/c/en/us/support/video/interactive-experience-manager/tsd-products-support-gen eral-information.html

Step 2 Log in using your partner or customer credentials.

Step 3 Within the Support area, click **Download Software**.

Step 4 Choose the correct Release and then select the IEM OVA file.

Step 5 Click the **Download** button.

Step 6 Select the IEM ISO file.

Step 7 Click the **Download** button.

Install IEM Software on a Virtual Machine

Follow the instructions below to install the IEM software on a virtual machine (VM).

Configure High Availability in vSphere (Optional)

The IEM supports High Availability (HA) configured on vSphere.

If you wish to have HA on the IEM VM, make sure that you have configured HA on vSphere before installing the IEM software. vSphere HA provides the infrastructure to protect all workloads with the infrastructure. You do not need to install special software within the application or virtual machine. All workloads are protected by vSphere HA. After vSphere HA is configured, no actions are required to protect new virtual machines; they are automatically protected.

vSphere HA provides high availability for virtual machines by pooling the virtual machines and the hosts they reside on into a cluster. Hosts in the cluster are monitored and in the event of a failure, the virtual machines on a failed host are restarted on alternate hosts. vSphere HA leverages multiple ESXi hosts configured as a cluster to provide rapid recovery from outages and cost-effective high availability for applications running in virtual machines. vSphere HA protects application availability in two ways.
First, it protects against a server failure by restarting the virtual machines on other hosts within the cluster. Second, it protects against application failure by continuously monitoring a virtual machine and resetting it in the event that a failure is detected.

Refer to the vSphere Availability documentation for how to set up, configure, and enable vSphere HA. The documentation for your vSphere version and edition can be found at:
http://www.vmware.com/support/pubs/vsphere-esxi-vcenter-server-pubs.html

Launch VMware vSphere Client

Step 1 Launch your VMware vSphere client.

Step 2 In the IP address / Name field, enter the IP address of the ESX host server that will be hosting the IEM virtual machine.

Step 3 In the User name field, enter the username of the ESX host server.

Step 4 In the Password field, enter the password of the ESX host server.

Step 5 Click **Login**.

Step 6 When prompted with a security warning pop-up about Certificate Warnings, click **Ignore**.

Step 7 A Warning window appears. Click **OK**.

Step 8 Click on the IP address of the ESX host server in the left window pane and then click on the **Summary** tab in the right window pane.

Create a Virtual Machine and Deploy the OVA File

The IEM OVA file contains all the VM settings that you need so you do not need to configure or modify any VM settings when you are creating the VM for the IEM.

Note If you have configured vSphere HA, you will create a VM for IEM in the vSphere Client in the vCenter.
If you have not configured vSphere HA, you will create a VM for IEM in the ESX/ESXi host.

Step 1 Ensure that the OVA file that you need is available locally such as on your desktop.

Note The OVA.zip file includes five OVA files with different vCPU configurations. You should use the appropriate OVA file based on the number of IECs that you are deploying.

Step 2 In vSphere, choose **Deploy OVF Template** option under File.

The Deploy OVF Template dialog box opens.

Step 3 Click **Browse**.

Step 4 In the Open dialog box, go to the location where the IEM OVA file is located and choose it.

Step 5 Click **Open**.

Step 6 The path to the OVA file appears in the Source screen.

Step 7 Click **Next**.

Step 8 The Details screen displays the details of the OVA file including the product, release number, download size, and size on disk. Click **Next**.

Step 9 The Name and Location screen appears. By default, the template name appears as “Interactive Experience Manager”. It is recommended that you keep the default template name so it is easy to identify later. Click **Next**.

Step 10 (Optional) Choose a resource pool if you have set up a hierarchy of resources and then click **Next**.

Step 11 In the Storage screen, choose a datastore and then click **Next**.

Note In a non-HA environment, you will have only one datastore available.

Step 12 In the Disk Format screen, do not modify any of the settings. Click **Next**.

Step 13 In the Network Mapping screen, choose the destination network that your VM will run on and then click **Next**.

Step 14 In the Ready to Complete screen, click **Finish**.

Note Be sure to leave the “Power on after deployment” checkbox unchecked.

The Deploy OVF Template dialog box will close and the Deploying Interactive Experience Manager dialog box will appear.

Step 15 When the deployment is complete and the new VM is created, you will see the message “Completed Successfully” in the Deployment Completed Successfully pop up dialog box. Click **Close**.

Step 16 Click the Virtual Machine tab to view the newly

created VM. **Step 17** In the left pane, choose **Interactive**

Experience Manager. **Step 18** Click the **Summary** tab to view

details about the IEM’s VM.

Note Your details may be different from those shown in the graphic above.

Upload and Deploy ISO File

Now you upload and deploy the ISO file.

Step 1 In the Summary tab of the IEM’s VM, right-click **datastore** in the Resources area.

Step 2 Choose **Browse Datastore**.

Step 3 In the Datastore Browser dialog box, click the **Upload files to this datastore** button, which is the fourth button from the left.

Step 4 Choose **Upload File**.

Step 5 In the Upload Items dialog box, find the IEM-VM ISO file and select it.

Step 6 Click **Open**.

The IEM-VM ISO file is uploaded from your disk to the virtual disk.

Step 7 When the upload is complete, the ISO file appears in the Datastore Browser dialog box.

Step 8 Close the Datastore Browser dialog box by clicking the X in the upper right corner of the box.

Step 9 In the Summary tab, go to the Commands section and click **Edit Settings**.

Step 10 In the Virtual Machine Properties dialog box, choose **CD/DVD drive 1**.

Step 11 Click the **Datastore ISO File** radio button within the Device Type area.

Step 12 Click the **Browse** button next to it.

Step 13 In the Browse Datastores dialog box, select the datastore and then the ISO file that you just uploaded.

Step 14 Click **OK**.

Step 15 Check the **Connect at power on** check box within the Device Status area.

Step 16 Click **OK**.

Install ISO and Boot Up

Step 1 In the menu bar, click **Launch Virtual Machine Console** icon to open the Console window. Alternatively, you can click the **Console** tab.

Step 2 Click the green play button in the menu bar to power on the VM. Alternatively, click **Power On** in the Commands area of the Summary tab.

When the VM power on process is complete, you will see the Cisco logo and the boot prompt.

Step 3 Move your pointer within the Cisco logo and click your mouse button to enter commands within the console.

Tip If you want to access features in vSphere, press Ctrl-Alt.

Step 4 Type **install** at the boot prompt and press the Enter key.

The ISO installs and auto boots up.

If the IEC does not obtain the IP address during the installation process, a network configuration menu appears during the installation.

To configure the network, perform the following steps:

a. In the Select Action dialog box, choose **Edit Devices** by highlighting it and pressing the Enter key.

Note Press the tab key or the arrow keys to navigate between the selections. Press the space bar to confirm your selection.

b. In the Select A Device dialog box, choose the Ethernet card.

c. In the Devernet Configuration dialog box, press the space bar to uncheck the **Use DHCP** check box.

d. Enter the IP address in the Static IP field.

e. Enter the netmask in the Netmask field.

f. In the Default gateway IP field, enter the default gateway IP address.

g. Choose **OK**.

h. Press the Enter key.

i. In the Select A Device dialog box, choose **Save**.

j. Press the Enter key.

k. In the Select Action dialog box, choose **Edit DNS configuration**.

l. Press the Enter key.

m. Enter the host name of the IEM server in the DNS Configuration dialog box.

a. Enter the primary DNS address in the Primary DNS field.

b. (Optional) Enter additional DNS addresses in the Secondary and Tertiary DNS fields.

c. (Optional) Enter a search value.

d. Choose **OK**.

e. Press the Enter key.

f. In the Select Action dialog box, choose **Save & Quit**.

g. Press the Enter key.

The installation is complete when you see the IEM login prompt.

Verify High Availability of the IEM's VM

If vSphere HA has already been configured, then it is automatically enabled for every VM including the IEM's VM.

To verify that vSphere HA is turned on for your cluster, follow these steps:

Step 1 Choose the cluster and then choose **Edit settings**.

Step 2 Verify that the Turn On vSphere HA checkbox has a checkmark under the Features section.

You can also verify whether an individual VM such as the IEM's VM is protected by HA by performing the following steps:

Step 1 Choose the VM.

Step 2 Go to the Summary tab.

Step 3 Look at the last entry in the General section listed as "vSphere HA Protection".

Step 4 If there is a green checkmark and word "Protected" next to it, HA is protecting the VM.

If you are experiencing issues with vSphere HA or have questions, please refer to VMware's documentation for your particular version and edition at: http://www.vmware.com/support/pubs/vsphere-esxi-vcenter-server-pubs.html

Configuring IEM Software

Chapter Overview

This chapter explains how to configure the IEM software after it has been installed on a virtual machine. The sections in this chapter are:

Log In as Installer and Change Installer Password

Before you log in as the installer, choose a password now as the window of opportunity to enter the password is limited.

Warning **Forgetting the installer password may result in reinstalling the IEM since there is no method for resetting or retrieving the installer password without logging into the TUI.**

The installer password or passphrase must meet the following criteria:

- Password: A combination of upper case letters, lower case letters, numbers, and other characters. If you choose a twelve character long password, then choose characters from at least three out of the four categories. If you choose an eight character password, you must use characters from all four categories. But if you start your password with an upper case letter or end it with a number, additional characters from those categories must also be included in the password in order for the password to be valid.
- Passphrase: Should be of at least three words and sixteen to forty characters that are a combination of upper and lower case letters, numbers, and other characters.

Step 1 Choose a password or passphrase.

Step 2 At the iem login prompt, type **installer**.

Step 3 Press the Enter key.

Step 4 At the Password prompt, type **cisco!123**, which is the default password.

Step 5 Press the Enter key.

Step 6 Re-enter the default password.

You will now be prompted to change the password.

Step 7 Enter a new password following the password criteria outlined on the screen.

Note If you do not choose a password that meets the criteria, you will be logged out and must repeat the steps in this section.

Step 8 Re-enter the new password.

Install VMware Tools

Installing VMware Tools is optional. VMware Tools provide a better user experience and improved management of the VM. To install VMware Tools, follow these steps:

Step 1 In the vSphere Client inventory, right-click the VM and choose **Guest** >**Install/Upgrade VMware Tools**.

Step 2 Go to the VM Console in the vSphere Client (or SSH into the VM) to access the TUI.

Step 3 In the Main Menu, choose **System Settings**.

Step 4 In the System Settings menu, choose **Install VMware Tools**.

Step 5 Follow the on-screen instructions to install the tools.

Configure Server Settings

Configure Network Settings

It is recommended that you use static addressing instead of DHCP.

Note The IEM does not support two network interfaces.

Tip The default username for the IEM Configuration Menu is **installer**. Use the new password not the default password.

The instructions below will configure a static address for the IEM.

Step 1 In the Main menu of the IEM Configuration Menu, type **a** to access the System Settings menu.

Step 2 In the System Settings menu, type **a** to access the Network Settings.

Step 3 In the Network Settings menu, type **a** to access the Setup Network Information.

Step 4 Press any key to begin network configuration.

You should verify the network settings next.

Step 5 In the Select Action dialog box, choose **Edit Devices** by highlighting it and pressing the **Enter** key.

Note Press the **Tab** or **Arrow** keys to navigate between choices. Press the **Space** key to confirm your selection.

Step 6 In the Select A Device dialog box, choose the Ethernet card.

Step 7 Press **F12**.

Step 8 In the Devernet Configuration dialog box, uncheck the **Use DHCP** field by pressing the **Space** key.

Step 9 In the Static IP field, enter the IP address.

Step 10 In the Netmask field, enter the netmask.

Step 11 In the Default gateway IP field, enter the default gateway IP address.

Step 12 Choose **Ok**.

Step 13 Press **Enter**.

Step 14 In the Select Action dialog box, choose **Edit DNS configuration**.

Step 15 Press **Enter**.

Step 16 In the DNS configuration dialog box, enter the hostname for the IEM server.

Step 17 In the Primary DNS field, enter the primary DNS address.

Step 18 (Optional) In the Secondary and Tertiary DNS fields, enter additional DNS addresses.

Step 19 (Optional) Enter a search value.

Step 20 Click **Ok**.

Step 21 Press **Enter**.

Step 22 In the Select Action dialog box, choose **Save & Quit**.

Step 23 Press **Enter**.

Step 24 When it quits, you see an empty blue box on the screen. Press any key to continue to the IEM Configuration menu.

You are returned to the Network Settings menu.

Step 25 Press the **R**, **<**, or **,** key to return to the System Settings menu.

Step 26 Press the **R**, **<**, or **,** key to return to the Main menu.

Restart Networking

Step 1 In the Main Menu, type **c** to access the Services Control menu.

Step 2 In the Services Control menu, type **a** to access Networking.

Step 3 In the Networking menu, type **a** to Restart networking. This restarts the network and

updates the configuration.

When it is complete, you will see the “Command completed successfully.” message.

Step 4 Press any key.

Get MAC Address of Active Network Interface

You will need the MAC address of the active network interface for licensing.

Step 1 Use a Secure Shell (SSH) client to log into the VM.

Step 2 In the Main menu, type **a** to access the System Settings menu.

Step 3 In the System Settings menu, type **d** to access System Information.

Step 4 Copy the MAC address, which follows the term “HWaddr” in the first line of the eth0 details of the IEM Configuration Menu screen.

Step 5 Press any key to return to the System Settings menu.

Step 6 Press the **R**, **<**, or **,** key to return to the Main menu.

Configure Time Zone

Step 1 In the Main menu, type **a** to access the System Settings menu.

Step 2 In the System Settings menu, type **b** to access the Date and Time Settings.

Step 3 In the Date and Time Settings menu, type **b** to change the time zone.

Step 4 Select the time zone.

Step 5 Select **OK** and press the Enter key.

Step 6 Press any key to return to the menu.

Configure NTP

Using Console

Step 1 In the Main menu, type **a** to access the System Settings menu.

Step 2 In the System Settings menu, type **b** to access the Date and Time Settings.

Step 3 In the Date and Time Settings menu, type **a** to access the NTP setup.

Step 4 In the Configure NTP screen, press any key to begin set up.

Step 5 Enter the NTP configuration information.

Step 6 When you are finished, type **:wq** and press the Enter key to save and quit.

Set Up SMTP Outbound Relay Server

The SMTP Provider in the IEM sends notifications including the IECs' status. The SMTP Provider is configured with an outbound URL in order to send the notifications.

The SMTP feature only works with non-authenticated mail servers. Free email service providers such as Gmail and Hotmail are not supported because they require authentication.

Note Cisco Advanced Services offers customized services such as the configuration of authenticated mail servers. Customers who are in need of this service should contact Cisco Advanced Services.

Once you have set up the SMTP provider, follow the instructions in the "Notifications" chapter of the *Moderro Interactive Experience Manager Administrator Guide* to create a notification and associate it with users.

The following are instructions on how to configure the SMTP provider.

Step 1 Use a Secure Shell (SSH) client to log into the VM.

Step 2 In the Main menu, type **d** to access the IEM Server Administration menu.

Step 3 In the IEM Server Administration menu, type **b) SMTP Email Alerts Setup** to access the SMTP Outbound Relay Setup.

Step 4 Enter the IP or FQDN of the outbound SMTP Relay Server.

Step 5 Press the Enter key.

Step 6 Press any key to return to the menu.

Step 7 When finished, press the **R**, **<**, or **,** key to return to the previous menu.

Log Into the IEM as the Administrator

Use a supported platform and browser version to

access the IEM. The following platforms are supported

by the IEM:

- Windows 7
- Macintosh OS X 10.9.4

The following browser versions are supported by the IEM:

- Internet Explorer
- Firefox
- Chrome
- Safari

Step 1 Open a supported browser and enter the IEM's IP address in the browser.

The IEM login window opens.

Step 2 In the Account field, enter **Root**.

Step 3 In the User Name field, enter **Administrator**.

Step 4 In the Password field, enter **cisco!123**.

You are now logged in the IEM.

Using the IEM Configuration Menu

Chapter Overview

This chapter explains how to use the IEM Configuration Menu that is accessed by using a SSH client. The topics in this chapter are:

Tip When logging into the IEM using a SSH client, use the password that was chosen when the IEM was installed.

Note If you are configuring the server settings for the IEM in the console screen and have changed the password for the Administrator within the Root account, the message "IEM Installation has FAILED!". This message is due to the fact that the IEM ISO in this build is using the default password to check whether the IEM is up and running. No action is required; you can ignore the failure message.

View System Settings

The administrator can view system settings using the Console tab in the VM or a Secure Shell (SSH) client.

Step 1 Log into the VM.
Step 2 In the Main menu, type **a** to access the System Settings menu.
Step 3 In the System Settings menu, type **d** to access System Information.
Step 4 Review the system information.
Step 5 Press any key to return to the System Settings menu.
Step 6 Press the **R**, **<**, or **,** key to return to the Main menu.

Ping a Host

Use the Ping utility to verify that the IEM can reach an IEC or that the NTP and SMTP servers

are up.

Step 1 Use a Secure Shell (SSH) client to log into the VM.

Step 2 In the Main menu, type **e** to access the Troubleshooting menu.

Step 3 In the Troubleshooting menu, type **a** to ping a host.

Step 4 When finished, press any key to return to the Troubleshooting menu.

Step 5 Press the **R**, **<**, or **,** key to return to the Main menu.

View Logs

Step 1 Use a Secure Shell (SSH) client to log into the VM.

Step 2 In the Main menu, type **e** to access the Troubleshooting menu.

Step 3 In the Troubleshooting menu, type **b** to access logs.

Step 4 Choose the type of logs desired, such as the Web Server logs.

Step 5 Choose one of the menus, such as the Web Server SSL Engine Log menu.

Step 6 Type **b** to view the log.

Step 7 Press a key to begin watching the log.

Step 8 Press **ESC :q!** to stop watching the log.

Step 9 When finished, press the **R**, **<**, or **,** key to return to the previous menu.

Enable XML API Gateway

Note XML API Gateway must be enabled in order to use IEM service API.

Step 1 Use a Secure Shell (SSH) client to log into the VM.

Step 2 In the Main menu, type **d** to access the IEM Server Administration menu.

Step 3 In the IEM Server Administration menu, type **d** to access the XML API Gateway.

Step 4 In the XML API Gateway menu, type **a** to enable API access.

Step 5 Press any key to return to the menu.

Step 6 When finished, press the **R**, **<**, or **,** key to return to the previous menu.

Reboot the Server

Step 1 Use a Secure Shell (SSH) client to log into the VM.

Step 2 In the Main menu, type **d** to access the IEM Server Administration menu.

Step 3 In the IEM Server Administration menu, type **f** to reboot the server.

Power Off the Server

Step 1 Use a Secure Shell (SSH) client to log into the VM.

Step 2 In the Main menu, type **d** to access the IEM Server Administration menu.

Step 3 In the IEM Server Administration menu, type **g** to power off the server.

Enable Cisco TAC User

Customers who have purchased SMARTnet can give SSH access to Cisco TAC engineers to troubleshoot and fix IEM issues remotely.

For a TAC engineer to SSH into the IEM, you must first create a TAC user account.

Note A validation string is required to create a TAC user account. The validation string must be generated by the TAC Token Generator using the UUID of the system. UUID can be found in the main menu.

Follow the steps below to create a TAC user account.

Step 1 Use a Secure Shell (SSH) client to log into the VM.
Step 2 In the Main menu, type **b** to access the System Accounts menu.
Step 3 In the System Accounts menu, type **a** to access the TAC Accounts menu.
Step 4 In the TAC Accounts menu, type **a** to create a TAC user account.
Step 5 Enter the validation string and press the Enter key.

Upgrading IEM

Chapter Overview

This chapter explains how to upgrade from an

earlier VM. The sections in this chapter are:

- Upgrade Overview, page 5-1
- What You Will Need For an Upgrade, page 5-1
- ISO Upgrade from 2.x VM, page 5-2

Upgrade Overview

If you have already installed an earlier version on a VM, only the ISO needs to be upgraded.

If 2.0 was installed on bare metal, you will need to perform a fresh install to upgrade (see Chapter 2).

Table 5-1 Upgrade Matrix

	Method Required
Virtual Machine	ISO upgrade
Bare Metal	Fresh install

What You Will Need For an Upgrade

To upgrade from an earlier version that is on a VM, you will need the IEM ISO file downloaded from www.cisco.com.

Follow the steps below to download the file.

Step 1 Enter the following URL in your web browser: http://www.cisco.com/c/en/us/support/video/interactive-experience-manager/tsd-products-support-gen eral-information.html

Step 2 Log in using your partner or customer credentials.

Step 3 Select the IEM ISO file.

Step 4 Click the **Download** button.

ISO Upgrade from 2.x VM

As explained above, this option is only possible if you already have 2.x installed on a VM.

Tip Perform the backup before the upgrade to prevent data loss from upgrade failure.

Step 1 You will need to change the primary boot device to **CD/DVD drive** in order to see the boot prompt; this is due to the CD/DVD drive's priority being lower than HDD in VMware. You can change the boot device by pressing the Escape (**Esc**) key at the VMware boot screen and then selecting **CD-ROM Drive.**

Step 2 Launch VMware vSphere Client and click the IEM VM 2.x.

Step 3 Follow the instructions in section "Upload and Deploy ISO File" of Chapter 2 to upload and deploy the ISO File. The upgrade uses the same ISO as for the fresh install.

Step 4 In the Summary tab, go to the Commands section and click **Edit Settings**.

Step 5 In the Virtual Machine Properties dialog box, choose **CD/DVD drive 1**

Step 6 Click the **Datastore ISO File** radio button within the Device Type area. **Step 7** Click the **Browse** button next to it.

Step 8 In the Browse Datastores dialog box, select the datastore and then the ISO file that you just uploaded.

Step 9 Click **Open**.

Step 10 Check the **Connect at power on** check box within the Device Status area.

Step 11 Check the **Connected** check box within the Device Status area.

Step 12 Click **OK**.

Step 13 In the menu bar, click the **Launch Virtual Machine Console** icon to open the Console window. Alternatively, can click the **Console** tab.

Step 14 In the Main menu, type **d** to access the IEM Server Administration menu.

Step 15 In the IEM Server Administration menu, type **d** to reboot the server.

Step 16 Press **Y** to continue.

Note The IEM must be restarted from the IEM TUI option as described above in order to successfully complete the upgrade procedure. If the IEM is restarted from the VMware option (e.g. **VM > Power > Reset**) and start upgrade, the upgrade may not complete and instead will roll back to the previous version.

When the VM restarts, the Cisco logo and the "boot" prompt appear.

Step 17 Type **upgrade** at the boot prompt and press the Enter key. The upgrade process will begin.

Caution During upgrade, the Setup Agent menu appears. **DO NOT change any settings in the Setup Agent menu**; **otherwise, the IEM may not function correctly**. When prompted,choose only **Exit** or **Ignore** and then press the Enter key. Wait until the Setup Agent menu is skipped.

During the upgrade process, the IEM reboots automatically.

The Cisco logo and boot prompt appears. DO NOT type anything and leave it for 25 seconds. It will boot the IEM from the disk to continue the upgrade process.

The installation is complete when you see the login prompt.

Note The build version may still show the old version. The version will be updated when you log in.

Step 18 Log in as installer and make sure that the software version is updated.

Adding or Upgrading the IEC Firmware

Note There are three ways to upgrade the IEC to version 2.6: 1) Using the IEM, 2) Using the Terminal Utility of IEC, and 3) Using a USB Stick

You can directly upgrade to IEC version 2.6 from either IEC version 2.3.4b, 2.4, or 2.5.

For the older IEC versions, such as 2.3.1 or older, refer to the table below for the procedure to upgrade to 2.6.

Table 6-1 IEC Upgrade Compatibility Chart

Version	Upgrade Feasibility
From version 2.3.4b (5.354.406), 2.4, or 2.5 to 2.6	Yes
From version 2.3.1 (5.288.320) or older to version 2.6	No
Using a two-step upgrade process: 1. From version 2.3.1 (5.288.320) or older to version 2.3.4b (5.354.406) 2. From version 2.3.4b to version 2.6	Yes

Note You can downgrade to any version of the IEC from version 2.6.

Chapter Overview

This chapter explains how to add or upgrade the IEC

firmware. Topics in this chapter include:

Warning **Before upgrading an IEC to the latest version, ensure that the software version of the IEM has been upgraded to the latest version too.**

Add or Upgrade IEC Firmware Using the IEM

Note IEC version 2.6 is only supported in IEM version 2.5 and 2.6. Therefore, it is mandatory to upgrade the IEM to version 2.5 or 2.6 before upgrading the IEC firmware to version 2.6 when using the IEM.

You will need the IEC firmware file that can be downloaded from www.cisco.com.

Note Starting with IEM version 2.5, you will only need a single IEC image.

Note In IEM version 2.6, you can still upload and use IEC images from older versions.

Tip It is recommended that only one version of the IEC firmware is active in the IEM at any one time.

Step 1 In the left pane, click **Maintenance**.

Step 2 Click **Supported Products**

Step 3 Click **Upload Spec** in the Edit menu.

Step 4 Click **+add**.

Step 5 Find the file on your desktop and click **Open.**

The file appears in the Upload Image dialog box.

Step 6 Click **upload**.

Step 7 Click **Close**. **Step 8** Click **IEC**. **Step 9** Click **4600**.

A list of versions is displayed in the center pane.

Step 10 In the System Image column, click **+**. The Upload Image dialog box opens.

Step 11 Click **+add**.

Step 12 Find the file on your desktop and click **Open**.

The file appears in the Upload Image dialog box.

Step 13 Click **upload**.

Step 14 Click **Close**.

Today's date will appear in both the System Image and Specification columns to identify

when you uploaded the image.

Note The Application Image column will not be used starting with version 2.5.

Step 15 Select and highlight the image you want to activate in the center pane.

Step 16 In the right pane, click **enable**.

In the Active column, the word "Yes" appears, which indicates that the image for this version is now available for pushing to the IECs that are registered and active in the IEM.

Step 17 If a previous version was active, deactivate it.

Note You do not need to delete older versions.

Upgrade IEC Firmware Using the Terminal Utility

In this method you will use the debugging console of the Moderro IEC to upgrade the firmware.

Note You can directly upgrade to IEC 2.6 from either IEC 2.3.4b, 2.4, or 2.5. If upgrading from an older version (i.e. 2.3.1 or older), upgrade first to 2.3.4b and then upgrade from 2.3.4b to 2.6.

You will need the IEC firmware file that can be downloaded from www.cisco.com. You will also need the URL of where you placed this file.

Note It is not mandatory to upgrade to the IEM to version 2.6 if using the terminal utility to upgrade the IECs.

To upgrade the firmware, follow these steps:

Step 1 Press **Ctrl-Alt-S** to open the System Settings menu.

Step 2 Click the **Terminal** icon.

The console window opens with the password prompt.

Step 3 Type the DMC for the password and press the **Enter** key.

Step 4 (Optional) To view a list of commands, type **help** and press the Enter key.

Step 5 Enter the **usys <url_to_the_image>** command where the URL is the location of the image file.

Note The uapps command is not needed after the usys command.

Step 6 Enter the **uloaders** command. The uloaders command switches from the old partition to the new partition. The old partition then become available for future upgrades.

Upgrade the IEC Firmware Using a USB Stick

Tip The best practice is to upgrade the IEC firmware using the IEM. Alternatively, you can upgrade the IEC firmware using a USB stick.

The IEC's firmware can be upgraded using a USB stick if you have physical access to the IEC. First you will burn the IEC OS onto a USB stick and then use the stick to upgrade the firmware. The steps below will show how to burn the IEC operating system onto a USB flash drive.

There are two parts to this process:

1. Extracting the IEC OS using Win32DiskImger
2. Burning the IEC OS

Step 1 Extract the OS file from emergency-stick-iec-X.XYZ.XYZ.gz using 7-Zip or any other compression tool that supports the .gz file format. An example of the file name is "emergency-stick-iec-5.387.453". Once extracted, the OS file will be called "emergency-stick-iec-5.387.453" with the file type shown as "453 File".

Step 2 Insert the USB flash drive that will be used to store the OS.

Note The USB flash drive must have a capacity of at least 1 GB of storage space and be formatted in FAT32.

Step 3 Launch the Win32DiskImager.exe application.

Step 4 In the Win32 Disk Imager dialog box, click the folder icon to the right of the Image File field to view the directories.

Step 5 In the lower right corner of the Select a desk window above the Open button, choose ***.*** as the file type.

Step 6 Locate the directory where the "emergency-stick-iec-5.387.453" file is kept. Select the file and click the Open button or drag and drop the file into the Image File field of the Win32Disk Imager dialog box.

The complete path will be listed in the Image File field.

Step 7 Click **Write** to burn the image to the USB flash drive.

The program will begin burning the software on to the USB flash drive. The Progress bar will indicate the progress of the burn.

When the burning utility states "Done," the burning is complete and the OS is now on the USB drive.

Step 8 Click **Exit**.

Step 9 Remove the USB stick.

Now you will use the USB stick to upgrade the firmware on the IEC.

Step 10 Unplug the IEC's power adapter.

Step 11 Connect the following to the IEC:

- USB stick with the IEC OS to a USB port
- Keyboard to a USB port
- Monitor to the HDMI port (on 4610/4632/4650 models), Mini DisplayPort (on 4650 models only), or VGA port (on 4610 and 4632 models only)
- Power adapter to the DC 12V in connector

Step 12 Hold down (or keep pressing) the **Ctrl** key on the lower left corner of the keyboard until Step 5.

Step 13 Plug the power adapter into an electrical outlet. The IEC will power up as indicated by the power LED.

Note Make sure that you are still holding down or pressing the **Ctrl** key during this step.

Step 14 When a number appears in the lower right corner of the screen, release the **Ctrl** key.

The monitor displays the booting sequence in command-line mode.

Step 15 You will be prompted four times. Press the **Enter** key at every prompt to choose the default value (i.e. "Y" for the first three prompts and "N" for the last prompt).

After the booting process is over, you will see the message "Full system upgrade has FINISHED. Everything looks fine. Remove USB stick and reboot."

Step 16 Remove the USB stick.

Step 17 Reboot the IEC by unplugging it and then plugging it in again.

Starting the Web Service

Chapter Overview

This chapter explains how and when to enable the device gateway so that the IEM can communicate with the IECs.

Enable the Device Gateway

Note The IEM's device gateway must be turned **ON** in order to communicate with the IECs.

Although the device gateway must be turned ON in order to communicate with IECs, the device gateway checkbox by default is turned OFF to prevent the following scenario: *If IEC4600 Series devices are first configured to point to a server but have not been registered by it, they will continue to ping the server until the server is brought online. Once the server has been brought online, the server will reply to those devices that they are not registered. That will cause the devices to revert to stand-alone mode. Once the administrator registers those devices on the server, they will need to physically configure each and every IEC4600 Series to point to the server again.* Therefore, you should first register all the devices in the IEM before checking the **device gateway enabled** checkbox to turn it ON.

Step 1 Click **Maintenance** in left pane to expand menu and then double-click **System Settings**. Alternatively, click the ON or OFF button for the State of Device Gateway.

Step 2 Check the **Device gateway enabled** check box after you have registered IEC4600 Series devices that have been configured with the server's URL.

Step 3 Click **Apply**.

Management Server (IEM) IP Provisioning with DHCP

Appendix Overview

This appendix explains how to auto connect the IEC to the IEM by provisioning the Management Server (IEM) IP with DHCP. The IEC automatically is connected to the IEM only if the serial number of the IEC is pre-registered with the IEM and the DHCP server is configured correctly.

Topics in this appendix include:

Management Server (IEM) IP Provisioning with DHCP

The following provisioning of the management server IP assumes the use of DHCP that is running on IPCop Firewall Linux.

The DHCP server config file must include the following lines (syntax may vary in different DHCP server config files):

- option mms-server code 202 = string;
- option mms-server "192.168.1.202";

For Cisco IOS, this is done by using the “option” definition in the IP DHCP pool declaration. Instructions for this can be found in the “Configuring DHCP Address Pools” section of the “Configuring the Cisco IOS DHCP Server” chapter of the *IP Addressing: DHCP Configuration Guide, Cisco IOS Release 12.4T*, which can be found at the following link:
http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_dhcp/configuration/12-4t/dhcp-12-4t-book/c onfig-dhcp-server.html#GUID-6B6DD9A0-623E-4D1B-B92E-608C32C84BA1

For Cisco Network Registrar, this is done by using the “option” directive defined under the option-set dhcp-config option within the CNR CLI. Instructions for this can be found in the “Using Standard Option Definition Sets” section of the “Configuring Policies and Options” chapter of the *User Guide for Cisco Network Registrar 7.2*, which can be found at the following link:
http://www.cisco.com/c/en/us/td/docs/net_mgmt/network_registrar/7-2/user/guide/cnr72book/UG22_P ol.html#wp1242215

Provisioning steps:

Step 1 The IEC broadcasts ‘DHCP Discover’. It contains option 55 (Parameter Requet List). This is the option that includes a numeric list of DHCP options that it intends to receive from the DHCP server. Option 202 is one of the requested parameters.

Step 2 The DHCP Server sends ‘DHCP OFFER’ to the IEC. This packet contains the value for option 202 (IEM IP) along with the IP address, lease time, subnet mask, domain name, DNS, etc.

Step 3 The IEC broadcasts ‘DHCP Request’.

Step 4 The DHCP Server sends ‘DHCP ACK’. This packet contains the value for option 202 along with other options.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).
This product includes software written by Tim Hudson (tjh@cryptsoft.com).
This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/).

9.11.17