



Cisco Interactive Experience Manager Administrator Guide

Release 2.1.1

January 26, 2014

Americas Headquarters

Cisco Systems, Inc. 170 West Tasman Drive San Jose, CA 95134-1706 USA http://www.cisco.com Tel: 408 526-4000 800 553-NETS (6387) Fax: 408 527-0883

Text Part Number: OL-26458-05

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

Modifications to this product not authorized by Cisco could void the FCC approval and negate your authority to operate the product.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0910R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco Interactive Experience Manager Administrator Guide © 2013 Cisco Systems, Inc. All rights reserved.



CONTENTS

CHAPTER 1	Introduction
CHAPTER 2	Managing Licenses
CHAPTER 3	Managing Accounts and Users
CHAPTER 4	Managing Devices
CHAPTER 5	Configuring Profiles
CHAPTER 6	Configuring Policies
CHAPTER 7	Configuring Notifications
CHAPTER 8	Modifying Server Settings
CHAPTER 9	Backing Up and Restoring the Server
CHAPTER 10	Auditing
APPENDIX A	Proxy Support

Γ

Contents

1



CHAPTER

Introduction

Revised: January 26, 2014, OL-26458-05

Chapter Overview

I

The Cisco Interactive Experience Manager is a console that allows for centralized management of Cisco Interactive Experience Client 4600 Series devices.

This guide assumes that the Cisco Interactive Experience Manager has already been installed. If not, refer to the *Cisco Interactive Experience Manager Installation Guide* for instructions on how to install the software first.

This chapter explains the audience and scope of this guide and provides an overview of the Cisco Interactive Services Solution including the Cisco Interactive Experience Manager.

Topics in this chapter include:

- What's New About the IEM in This Release, page 1-2
 - VNC Managed by the IEM, page 1-2
 - Audio Mode Falls Back to 'Analog', page 1-2
 - Hide Mouse Cursor, page 1-2
- About This Guide, page 1-2
 - Terminology, page 1-2
 - Audience, page 1-3
 - Scope, page 1-3
- Cisco Interactive Services Solution, page 1-3
 - Cisco Interactive Experience Client 4600 Series, page 1-4
 - Cisco Interactive Experience Manager, page 1-4
 - Principles of Operation, page 1-5
- Getting Started, page 1-6
 - Logging In, page 1-6
 - Cisco IEM Interface, page 1-7

I

What's New About the IEM in This Release

Release 2.1.1 includes the following new and enhanced features for the Cisco Interactive Manager (IEM):

- VNC managed by the IEM
- Audio mode falls back to 'Analog' when USB devices are configured but not connected
- Default value of the mouse.cursor.visible property has changed to 'Hide mouse cursor'

VNC Managed by the IEM

The vncstart and vncstop debugging commands have been removed from the custom shell in the IEC so that VNC can be managed by the IEM. To enable VNC in the IECs, the remoteview.enabled property in a policy is set to 'true'. Since remoteview.enabled is a runtime property, you will need to create a custom action for it. Then when you want to use a VNC viewer, you will push the custom action to an IEC.

See the Profiles chapter for instructions on how to enable VNC for an IEC.

Audio Mode Falls Back to 'Analog'

The audio mode falls back to 'Analog' when the audio output is configured as 'USB headset' or 'USB speaker' but a USB headset or speaker is not connected to the IEC.

Hide Mouse Cursor

The default value of the mouse.cursor.visible property has changed to 'Hide mouse cursor' from "Show mouse cursor".

About This Guide

This section describes the audience and scope of this guide.

Terminology

The following terms are used in this guide.

- Accounts Allow multiple organizations to configure and manage devices and policies in a single Cisco 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. The *Cisco Interactive Experience Manager Installation Guide* provides administrators with all the information necessary to install and administer a Cisco Interactive Experience Manager instance.
- Devices The Cisco 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 Cisco Interactive Experience Manager. Users are assigned to specific accounts.

Audience

Administrators are the intended audience for this guide. Administrators will configure and manage the Cisco Interactive Experience Manager. At some sites, more than one person may have this responsibility.

Scope

This guide explains how to use the Cisco Interactive Experience Manager console.

This guide provides instructions so that an administrator can:

- Register accounts
- Create users
- Manage users
- Add new devices
- Manage devices
- Monitor devices
- Configure profiles
- Configure policies
- Apply policies

Cisco Interactive Services Solution

Cisco Interactive Services Solutions leverages the network as the platform to transform customer experience with interactive digital media. Leveraging Cisco's video, collaboration, and cloud architectures, the solution allows large and small enterprises and public agencies to seamlessly provide 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 Cisco Interactive Services Solution is the collective name for a product family that consists of thin clients and server hardware and software that will power a host of solutions, including the Cisco Interactive Experience Client 4600 Series and the Cisco Interactive Experience Manager.





Cisco Interactive Experience Client 4600 Series

The Cisco Interactive Experience Client 4600 Series (IEC4600 Series) is a robust, configurable, and manageable web computer designed for public venues and web-centric computing. The devices can be controlled remotely using a manager console, the Cisco Interactive Experience Manager.

It is highly recommended that all the Cisco IEC4600 Series devices are managed and monitored using the Cisco Interactive Experience Manager as it ensures consistency as well as remote management, although it is possible configure the devices locally as well.

Cisco Interactive Experience Manager

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

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

- Configuration Cisco IEM allows the administrator to manage the system behavior, such as desktop elements, window mode (kiosk vs. single-window vs. multiple-window), network settings, printing preferences, peripheral support, etc.
- Session Management An administrator can apply a session time limit, providing libraries, Internet cafés and other public venues with mechanism to control the terminal usage. Session management includes after-session clean-up and session time counter.
- Remote Assistance Users are given a way to ask for and receive help, and administrator to provide help, without interrupting their surroundings. The user simply presses a help button on their desktop, which initiates a desktop sharing and chat session with any of the administrators or support personnel.
- Remote Control Administrators have a need to control the behavior of the terminal on real-time basis. This means muting a station, locking out the user, sending user a message, etc. Cisco IEM supports remote control by which an administrator can issue a command to the terminal without being in the same network. Remote control traverses the NAT firewalls making it possible to support the user from a different network.
- Kiosk Configuration Kiosk mode refers to a full-screen mode of operation. Under this model, the kiosk will start with a predetermined internet resource (a special web page, flash, or movie), and let the user navigate within a "walled garden" environment.
- Logging and Reporting Cisco IEM can be set up to log the traffic from the Cisco IEC4600 Series devices, making it easy for the administrators to analyze the data and make access restriction decisions. This traffic data collection and be performed in private mode with the administrator seeing the aggregate data only.
- Policy Management- Policies provide an easy and flexible way of applying settings to a group of users or devices. For example, an administrator can apply a policy to use certain printer for certain section of the building, or restrict internet access on some, but not other terminals.

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 server will still be supported although some things may not work. The fact that device version is out of sync is indicated by the red FW flag. Communication between client and a server is defined by the communication protocol and specification that defines capabilities of each FW build: older communication protocols are supported in the newer server builds, but older specifications that reflect properties of the firmware are often not fully compatible with the later ones.

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 **Is action** checkbox 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. Runtime policies can only work for runtime properties, which are marked by an orange arrow in the policy or profile.

- 6. Notifications work on a subscription basis. Once a notification has been created, it has to be assigned to a user. A notification submit to a third party application collecting the data the URL has to be provisioned through the User profile.
- 7. In order to optimize kiosk 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.

Getting Started

Logging In

To log in IEM, you will need the account credentials (account name, user name, and password).

Use a supported platform and browser version to access the IEM.

The following platforms are supported by the IEM:

- Windows XP (32bit or 64bit)
- Windows 7 (32bit or 64bit)
- Macintosh OS 10.6.8

The following browser versions are supported by the IEM:

- Internet Explorer 8 and 9 (32bit and 64bit)
- Firefox 12 and higher
- Chrome
- Safari
- **Step 1** Open a supported browser and enter the Cisco IEM URL. The Cisco IEM login window appears.
- **Step 2** Enter the account name in the **Account** field.

iguio i L		
		Cisco IEP Manager
	Account	Root
	User Name	Administrator
	Password	*******
		Enter
		Register New Account
		cisco

Figure 1-2 IEM Login Screen

Step 3 Enter the user name in the **User Name** field.

IEM Start Screen

- **Step 4** Enter the password in the **Password** field.
- Step 5 Click Enter.

Figure 1-3

The Cisco IEM opens.

-iliilii cisco		
🗂 🗂 🕞 🔍 > Accounts		Cal Account Root 1 Administrator Distant
Devices Users Podcis Podcis Podcis Accounts Acco	Cisco TEM Cisco Interactive Experience Manager	

Cisco IEM Interface

ſ

The following section contains instructions on how to navigate the Cisco IEM interface. The Cisco IEM interface is comprised of four panes:

- Top Features and Notifications Pane
- Left Navigation Pane
- Center Information and Settings Pane
- Right Actions Pane

Figure 1-4 Cisco IEM Interface



The top pane contains the following features:

- Hide/Show navigation pane button
- Hide/Show action pane button
- Refresh button
- Search button
- Directory structure

Figure 1-5 Navigation Pane Button, Action Pane Button, Refresh Button, Search Button, and Directory Structure in the Top Pane



- Current account name
- Current user name
- Exit button

Figure 1-6 Account and User Identity and Exit Button in the Top Pane

Account: VEP User: vep9	EXIT
Account: VEP User: vep9	EXIT

The left pane contains buttons for the following categories: Devices, Users, Policies, Notifications, Schedules, Accounts, and Maintenance (for root administrators).

Click a category to access its icons and buttons.

To expand a category, click the Right Arrow.

ſ

N. U	sers
D D	evices
	BLRGBC0
	SJC30124
.	SN656015030118
-	MyDevice

Figure 1-7 Expanding a Category

To collapse a category, click the Down Arrow.

In the center pane, individual devices, users, accounts, policies, and default profiles are configured. Click an icon to access its Edit menu. Double-click an icon to access its settings tabs.

Figure 1-8 Icons in Center Pane



Click a tab to view information or settings for that device, user, account, or policy.

Deside Name + SPFVeresosic Setal Namer 6404 500 666 Mantenance Cole Down Podut EC Family 4060 Version 1.0.8 Ball 4.140.500 User fitada 623 User Description	Device laws + SPOensonic Senter hummer + essent 5004666 Harmmanne Cloke	General	Member Of	ProNe	Policies	Status	Events	Fedomatice	4
Sensi Number 64694503646 Marinesance Coles **** Product EC Family 4660 Varian 1.8 Baid 4.546.360 User thatis 623 User Colescription	Bead furnes: 65601502656 Marininance Close Product: EC Product: 4600 Version 1.1.8 Build: 4.55300 Uber Status: CD Uber Build: 200 Uber Build: 200 Build: 200		Device Name	* SIPViews	onic		-		
Mantasaca Octo www international Control of	Martenance Cross		Senal Number	65601503	1656				
Product KC Family 400 Version 11.0 Dus 4445.00 User Costoption Desorption	Photest BEC Family 4600 Version 11.0 Build 4.146.300 User Data 500 200 Logitime 506 2000 Cescription		Maintenance Code		STON .				
Famby 4860 Version 1.0. Balad 4.444.500 User Balad 623 Uptime 94200 205 Locatoo	Family 4600 Variano 1.1.8 Build 4.546-300 User Builds 623 Uptime 99.2002 200 Cesorgition		Product	IEC					
Varsion 1.1.0 Build 4.546.300 User Batu CC Uptime 90.2016 Location Description	Verson 1.1.8 Build 1.45300 User Status 201 Uspires 99.20m 20s Location Description		Family	4600					
Build 4.546.360 User User datase 623 Uptime 90.28m 20s Location Image: Comparison of Com	Buidt 4.546.360 User Hotunis CCI Uptims 99.20m 20s Location Description		Version	1.1.0					
User datus 6926s2bs Locaton Description	User totalis CCC Uptime de 20m 20s Location Description		Build	4.145.360					
tatus 20 Ustra 99-26s Locator Description	touton EEE . Uptime 99 20th 20th Location Description		User						
Uptime 98-26m 26m Location Description	Uptime 99.28m 20e Location Description		Status	CFF					
Cesoption	Loaton Description		Uptime	90 20m 20					
Descripton	Description		Location				1		
			Description	8			1		

Figure 1-9 Tabs in Center Pane

If you modify any information, click **Apply** at the bottom of the pane. To exit the tabs, click **Cancel**. You can view the devices as icons, in a table, or as kiosk screen shots. To change your view, click a view button (Show as icons, Show as table, or Show Screenshots) at the upper right corner of the center pane.

Figure 1-10 Show Screenshots View



The right pane contains menus with buttons that perform actions.



Click an edit button to open a dialog box for that action.

The Devices category has additional menus: Predefined Actions and Custom Actions. To access these menus, click either **Predefined Actions** or **Custom Actions** at the bottom of the right pane.

Γ

-	Edit
Pr	edefined actions
ø	Message
	Open URL
21.2 27.5	Reboot
U	Display On/Off
*	Mute
9	Upgrade
Q	Restart Application

Figure 1-12 **Predefined Actions Menu**

Figure 1-13



1



снартек **2**

Managing Licenses

Revised: January 26, 2014, OL-26458-05

Chapter Overview

Each Cisco Interactive Experience Client Series 4600 (IEC 4600) device requires a license in order for it to be managed on a Cisco Interactive Experience Manager (IEM).

This chapter provides information about licensing IEC 4600 devices on the IEM.

Topics in this chapter include:

- IEM License Bundles, page 2-1
- Licensing Guidelines, page 2-2
 - No Licenses in the System, page 2-2
 - Registrations Limit has been Reached, page 2-2
- Generating a License File, page 2-2
- Adding Licenses to the IEM, page 2-4

IEM License Bundles

I

The IEM license bundles support up to 10, 50, 100, 500, or 1,000 IEC 4600 devices. When ordering a license bundle, ensure that you have ordered enough licenses to cover all the IEC 4600 devices that will be managed by the IEM.

Product Number	Description
IEP-MGR-FL-10	10-pack IEP Manager license bundle
IEP-MGR-FL-50	50-pack IEP Manager license bundle
IEP-MGR-FL-100	100-pack IEP Manager license bundle
IEP-MGR-FL-500	500-pack IEP Manager license bundle
IEP-MGR-FL-1000	1000-pack IEP Manager license bundle

Table 2-1 IEM License Bundles

Licensing Guidelines

- If multiple licenses exist in the IEM, the number of simultaneously connected devices is calculated by adding up all licenses.
- If the number of registered devices is exceeded, no additional devices can be registered in the IEM until additional licenses are added to the IEM.

No Licenses in the System

When trying to register an IEC 4600 device to an IEM without active licenses, a message will be seen on the device side (i.e. the monitor or touch screen connected to the IEC 4600 that you are trying to register) that indicates that the device cannot be registered.

When the administrator logs into the IEM, a message will be displayed that no active licenses are present.

Registrations Limit has been Reached

If the number of registrations has reached the limit of licenses available in the IEM and an administrator or user tries to register another device, the following error message appears on the IEM or the screen connected to the IEC: "Number of registered devices exceeds the number permitted by the licenses".

Note

All previously registered devices that are still present on the IEM will work without interruption.

Generating a License File

You must first generate a license file from the Cisco Licensing site.

tep 1	Purchase the license bundles.
tep 2	Go to the Cisco Licensing site at https://tools.cisco.com/SWIFT/LicensingUI/Home.
tep 3	When prompted, log in with your customer or partner credentials.
tep 4	On the Product License Registration home page, click the green Continue to Product License Registration button.

Figure 2-1 Product License Registration Home Page

Tools & Resources Product License Registration

Did you know? You can now complete many types of license transactions yourself? To learn more about the new self-service features on this site, check out these resources in the Help section or select a video here:

Overview of the new Self Service Capabilities

- Quick Reference Guide
- Frequently Asked Questions
 Select a video demo below.

Continue to Product License Registration

Do not show this page next time.

Step 5 Enter a single PAK or multiple PAKs in the Quickstart page.

Figure 2-2 Quickstart Page

					View in French	Contact Us	Feedback	He
Quickstart	Get New 🔻	Get Existing 👻 G	Set Demo	Transfer 🔹	My Information	▼ F	Related Tools	•
Get New License	s From PAKs							
iter a Single PAK to fulf	ill:		Fulfill Single PAK	How do I				
		A CONTRACTOR OF						
	Load	More PAKS						
Get New License	Load	electing Multiple PAKs						
Get New License	Load s by Loading and Se	electing Multiple PAKs						
Get New License	Load S by Loading and Se load into the PAKs list to F	electing Multiple PAKs						
Get New License becify Multiple PAKs to I Fulfill Selected PAKs	Load S by Loading and Se load into the PAKs list to F	Nore PAKS						
Get New License becify Multiple PAKs to I Fulfill Selected PAKs Group by PAK +	Load s by Loading and Se load into the PAKs list to F	electing Multiple PAKs						
Get New License becify Multiple PAKs to I Fulfill Selected PAKs Group by PAK	Load S by Loading and Se load into the PAKs list to F	Nore PAKS	mily		SKI I Name	Otv	Search	
Get New License pecify Multiple PAKs to I Fulfill Selected PAKs Group by PAK • PAK	Load S by Loading and Se load into the PAKs list to F PAK Status	Nore PAKS electing Multiple PAKs ulfill: Load More PAKs Product Fa	mily	search sku	SKU Name	Qty	Search	
Get New License pecify Multiple PAKs to I Fulfill Selected PAKs Group by PAK • PAK Search pak	Load s by Loading and Se load into the PAKs list to F PAK Status search pak status	electing Multiple PAKs utfill: Load More PAKs Product Fa	mily	search sku	SKU Name	Qty	Search	

View the licenses that you have fulfilled for your products.

- **Step 6** Click either the **Fulfill Single PAK** button if you entered a single PAK or the **Fulfill Selected PAKs** if you entered multiple PAKs.
- **Step 7** Specify the quantity to assign.
- **Step 8** Enter the MAC addresses of the IEM.
- Step 9 Click the Assign button.
- **Step 10** The assignments will be displayed in the Device, PAK and SKU assignment table.
- Step 11 Click Next.

ſ

- Step 12 Enter your email address. This email address will receive the license file.
- Step 13 Check the I agree with the Terms of the License check box.
- Step 14 Click the Get License button.

A green checkmark indicates that the request was successful. You will then receive an email with the license file. The license file is required to add licenses to the IEM.

Proceed to "Adding Licenses to the IEM" section.

Adding Licenses to the IEM

To add licenses to the IEM, follow these steps:

- **Step 1** Download the license file that you received in the email to your desktop.
- **Step 2** Log in to the IEM as an administrator in the Root account.
- **Step 3** Click the **Maintenance** menu option in the left pane.
- **Step 4** Click **Licenses** either in the left or center pane.

Figure 2-3 Licenses Option in Left Pane Menu



Figure 2-4 Licenses Option in Center Pane



Step 5 In the Licenses window, click the + button in the lower left corner of the center pane to add licenses.

Figure 2-5 Licenses Window

Status	Company	Issuer	Devices	Connections	Expiration	Hosts
+ * @						



Figure 2-6Add License Dialog Box



Step 7 Find the license file on your local system and click Open to upload the file.

<u>Note</u>

I

Alternatively, you can open the license file and copy and paste the string into the License string field.

Step 8In the Add License dialog box, click Add.The licenses appear in the center pane.

Figure 2-7	List of Licenses
------------	------------------

MAC:005056BA4F7C						
Status	Company	Issuer	Devices	Connections	Expiration	Hosts
active	Cisco Systems, Inc.	Cisco Inc.	100	100	never expired	005056BA4F7C





Managing Accounts and Users

Revised: January 26, 2014, OL-26458-05

Chapter Overview

Accounts and users are not the same. Accounts represent companies, departments, projects, or events. Users represent people including administrators. Each user is associated with a particular account.

This chapter explains how to manage and configure accounts and users.

Topics in this chapter include:

- Accounts, page 3-2
 - The Root Account, page 3-2
 - Determining Number of Accounts Needed, page 3-2
 - Adding a New Account, page 3-6
 - Exporting Accounts, page 3-8
 - Importing Accounts, page 3-11
 - Delete Accounts, page 3-13
- Users, page 3-14
 - Adding a New User, page 3-14
 - Removing Administrator Access for a User, page 3-16
 - Adding a New Group, page 3-18
 - Exporting Users, page 3-19
 - Importing Users, page 3-20
 - Deleting Users, page 3-22



I

After you make a change to accounts or users, press the Refresh button at the upper left corner of the screen to view those changes.

Accounts

Accounts are used to segregate users, devices, and policies. They are a way of limiting visibility to subaccounts, and that they will not share policies/schedules/users between them. Accounts are the method to maintain domains within the system particularly for service providers and large enterprises.

As mentioned above, accounts represent companies, departments, projects, or event. Accounts do not represent people. A user within an account represent an individual person.

The Root Account

The Root Account is an account that has already been configured by Cisco so that it is available after the IEM has been installed. The Root Account is the overarching account; its name cannot be changed.

By default, the Root Account already has one user configured - the Administrator. The Administrator is a user that has complete access and control of the IEM. The Administrator sees everything (users, devices, policies, etc.).

If you want more than one person to have administrative privileges, you can create additional administrators in the Root Account. Follow the "Adding a New User" steps later in this chapter. Make sure to add the administrators to the Root Account and to the Users category; do not add them to other accounts. Once they are added to the Root Account, they will have the same permission levels as the default Administrator.

The Administrator's password should be changed as soon after the IEM is installed to prevent an unauthorized person from gaining access to the IEM by using the default password.

Determining Number of Accounts Needed

Accounts allow you to manage multi-tenants. For example if you are a technology services company that is managing Cisco IEM for multiple retail customers, each retail customer would be assigned an account on the Cisco IEM. If you are the retail company, you would only have one account configured on the Cisco IEM.

Each organization should have a separate account. If you have an installed an IEM that will serve only one organization, only one account is required. If you have installed an IEM that will serve multiple organizations, create one account for each organization. Users associated with an organization's account can then only configure and manage devices and policies for that organization and not others on the IEM. You can also tier accounts.

Scenario: Single Tenant/Single Account

If the instance of the IEM is dedicated for a single company or public sector organization, one account is sufficient to manage all the users, devices, and policies.



Figure 3-1 Single Account for Blue Company

All the Users within the Blue Company would be created under the BlueCompany account. All Users can view and modify all users, devices, and policies on the IEM instance.

Scenario: Single Tenant/Multiple Accounts

I

Alternatively, multiple accounts can be created to segregate users and devices in different departments (i.e. marketing, sales, human resources, customer service, etc.) or for projects or events (i.e. new product launch, corporate training, etc.).

For example, the Blue Company purchased a single instance of the IEM. The Blue Company's IEM Administrator created three accounts - one for each department that will deploy IECs.

Figure 3-2 Accounts for Blue Company's Departments



Within the Marketing account, the Administrator created several accounts for events.



Figure 3-3 Accounts for Marketing Events

Under each account, the Administrator created Users. Those Users can only view and configure the devices and policies within the account under which they were created; they cannot view or configure devices and policies in other accounts.

Sally Jones is a User created under the Marketing account. Sally Jones can view and configure all devices, users, and policies within the Marketing account and all its sub-accounts (i.e. Demos, Product_Launch, and Tradeshows),

ſ



Figure 3-4 User Sally Jones

Johnny Smith is a User created for the Tradeshows account under the Marketing account. Johnny Smith can only view devices, users, and policies within the Tradeshow account; he cannot view devices, users and policies within the Demos, Product_Launch, Sales, or Human Resources accounts.



Figure 3-5 User Johnny Smith

Adding a New Account

To add an account to the Cisco IEM, follow these steps:

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

Γ

Figure 3-6

	Devices
► 🤱	Users
⊩∎	Policies
► ∰	Notifications
▶ 📰	Schedules
► <u>1</u>	Accounts
▶%	Maintenance

Accounts Button

Step 2 In the Edit menu, click **New Account**.

Figure 3-7 New Account Button in the Edit Menu



Step 3 In the Create New Account dialog box, enter an account name in the Account Name field.

		Alphabetica	al characters	only	
C	escription				
Profi	les to Propag	ate			
Polic	ies to Propag	jate			
Polic	cies to Propag	jate DS			
Polic	cies to Propag ANGRYBIRE BART	jate DS			
Polic X X X	cies to Propag ANGRYBIRD BART BGL-GBC-S	jate)S howcase			
Polic X X X	cies to Propag ANGRYBIRE BART BGL-GBC-S BofA	jate)S howcase	_		
Polic X X X X X X X X	ANGRYBIRE BART BGL-GBC-S BofA BRI-ONLINE	jate DS howcase BANK			
Polic X X X X X	ANGRYBIRE BART BGL-GBC-S BofA BRI-ONLINE Carrefour	jate)S howcase E-BANK			

Figure 3-8 Create New Account Window

Step 4	(Optional) Enter a description in the Description field.
Step 5	(Optional) Choose a Profile from the Profile to Propagate list.
Step 6	(Optional). Choose a Policy from the Policies to Propagate list.
Step 7	Click Create.

Exporting Accounts

If the account will be moved or replicated on another Cisco IEM, you can export the account file so that it does not have to be reconfigured on the other instance of Cisco IEM.

How is Backup and Restore different from Export and Import? The Backup and Restore functionalities deal with the entire data set from the system, whereas the Export and Import functionalities deal with subsets of data such as accounts, devices, policies, schedules, etc. Backup and Restore are most appropriate for periodic system backups; Export and Import are most appropriate for data migrations either for upgrades or between systems.

There are two types of export buttons:

- 1. Export Account This type exports the entire account and keeps the association between elements (e.g. policy/schedule on device, notification on user, etc.).
- **2.** Bulk Export This type allows you to select which elements to export. Note that the association between elements will be lost.

Follow these steps to export an account that keeps the association between elements:

- **Step 1** In the left pane, click **Accounts**.
- **Step 2** Choose an account.
- Step 3 In the Edit menu, click Export Account.

Figure 3-9 Export Account Button



Follow these steps to use the bulk export option:

- **Step 1** In the left pane, click **Accounts**.
- Step 2 Choose an account.

I

Step 3 In the Edit menu, click Bulk Export.



The Bulk Export dialog box opens.

Step 4 From the drop-down list, choose the elements to export from the account or check the check boxes next to the elements desired.

	Select	Nothing
		Nothing
ID)	All
1 👗 1	30	All devices
1 🧘 1:	33	All users
1 🧘 1:	36	All policies
1	29	iservices
1:	32	iservices1
1	35	iservices2
3	87	Citi_Video

Figure 3-11 Bulk Export Dialog Box

Importing Accounts

Step

If an account is on another Cisco IEM, that data can be imported so the account does not have to be configured again.

Δ Warning

I

Modifying any data within the exported file can prevent the accounts from being imported correctly and account creation failure. It is best to import the file "as is" and then modify the accounts' information in the IEM.

Follow these steps to import an account:

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

- **Step 2** Choose an account.
- **Step 3** In the Edit menu, click **Import Account**.

Figure 3-12	Import Account Button
-------------	-----------------------



Step 4 In the Import Account dialog box, click **add**.

Figure 3-13 Import Account Dialog Box



Step 5 Find the file on your computer. Choose the file and then click **Open**.

Look in:	Desktop		🛨 🧿 🖉 🖡	ຯ▼
Nar	ne	Size	Item type	Date modified
S	Adobe FrameMaker	2 KB	Shortcut	11/30/2011 8:15
TI Flaces	Mozilla Firefox	2 KB	Shortcut	5/30/2011 11:51
a	SnagIt 8	2 KB	Shortcut	2/1/2010 11:04
ktop 🛣	EXCEL - Shortcut	2 KB	Shortcut	9/4/2011 5:57 P
- D	iSkysoft DVD Ripper	2 KB	Shortcut	4/14/2010 9:22
2	POWERPNT - Shortc	2 KB	Shortcut	9/4/2011 5:57 P
aries 📷	WinSCP	1 KB	Shortcut	11/25/2011 11:4
1	WINWORD - Shortcut	2 KB	Shortcut	9/4/2011 5:57 P
s 🗋	CombinedFile	1 KB	Text Document	12/9/2011 10:57
puter	test	1 KB	Text Document	12/8/2011 2:21
👌 🗋	user_sam	3 KB	Text Document	12/8/2011 2:56
rk 🔮	user_10	3 KB	XML Document	12/8/2011 2:34
٠.		ш		
File r	ame:		- 0	- Open
∢ _ File r Files	ame: All Files (*	.)	1	- <u>(</u>

Figure 3-14 Select Files Dialog Box on Computer

Step 6 The file name then appears in the Import dialog box.

Figure 3-15 File in Import Account Dialog Box

Import Account	
account_ABC.xml	2.0 Kb
loaded(0 files - 0 Bytes) / total(1 fi	les - 2.0 Kb) 0%
Overwrite existing entitie	upload
Cancel	

Step 7 Click Upload.

A green check mark appears next to the file after it has been uploaded.

<u>)</u> Tip	Check the Overwrite existing entities check box to overwrite a file.
Click (Close.

Delete Accounts

I

Step 8

To delete an account, follow these steps:

Step 1 Choose an account and then click the **Delete** button in the Edit menu.



Step 2 In the Confirm Delete dialog box, choose **Delete**.

Users

Users are individuals who have access to the IEM to configure and manage devices and policies.

Adding a New User

New users can be given access to the IEM. Follow these steps:

Step 1 Click Users in the left pane.
Γ

Figure 3-17 Users Button



Step 2 In the Edit menu, click New User.





Step 3 In the Create New User dialog box, enter a login name in the Login Name field.

Login Name 🔹	
	Alphanumeric, -, _, 3 characters minimum, must start with letter
Password *	
Re-type Password *	
First Name	
	Use alphanumeric characters only
Last Name	
	Use alphanumeric characters only
Contact e-mail 🔹	
Description	
L	
	Create Cancel
nter a password in the P	assword field.
e-enter the password in	the Re-type Password field.
Optional) Enter the user'	s first name in the First Name field.
Optional) Enter the user?	's last name in the Last Name field.

Figure 3-19 Create New User Dialog Box

Removing Administrator Access for a User

Click Create.

Users by default are granted administrator-level access and permissions. With administrator-level access, they can add, delete, and modify devices, policies, profiles, and other users that are within their account.

Step Step Step Step Step Step

Step 10



Users with administrator-level access do not have full rights and permissions as administrators created in the Root account. Users cannot access or modify any of the features within the Maintenance menu such as adding supported products or modifying server settings. Users also cannot view all accounts on the IEM; they can only view the account to which they are assigned and the sub-accounts of that account.

Administrator-level access can be removed for users that only need to view and monitor devices. These users are known as "non-administrator users". This provides administrators with more access control.

Non-administrator users have access to the following tabs within the Device screen:

- General
- Status
- Events
- Performance
- Effective Profile

Non-administrator users can also use the predefined action buttons for devices including Reboot and Message. If any custom action buttons have been created, they too can be accessed by the non-administrator users. Both predefined and custom action buttons are found in the right pane.

Figure 3-20 Predefined Action Buttons for Devices



To remove administrator access for a particular user, follow these steps:

- Step 1 Choose the user by clicking on the user's name in the left or center pane.
- **Step 2** Click the **Security** tab in the User screen.

General	Contact Info	Member Of	Profile	Security	Policies	Notifications
		Gran	nt Administrator	Access vancel		
Step 3	Step 3 Uncheck the Grant Administrator Access check box to remove administrator access.					
Step 4	Click Apply.					

Security Tab in the Users Screen

Adding a New Group

Figure 3-21

Groups are an efficient way of managing users. To add a group for users, follow the steps below.

Step 1 Click Users in the left pane.		ft pane.
Step 2	In the Edit menu, cli	ck New Group
	Figure 3-22 Edi	t Menu
	Edit	
	Rew Use	r
	New Grou	ip.

48

Step 3 In the Create New Group dialog box, enter a group name in the Group Name field.

Figure 3-23 Create New Group Dialog Box

	Create New Group	
Group Name 🔺	Alphabetical characters only	
	Create	

Step 4 Click Create.

Exporting Users

A user's configuration can be exported to another instance of IEM.

Export a Single User

Follow these steps to export a user.

- **Step 1** Click **Users** in the left pane.
- **Step 2** Click a user icon in the center pane.

Figure 3-24 User Icons in Center Pane



Step 3 In the Edit menu, click **Export**.

Your computer's download dialog box opens.

Step 4 In the Save to field, enter the destination to download the file.

Figure 3-25 Create New Download Dialog Box



Step 5 Click Download.

The file is an xml file.

Export Multiple Users

I

Follow the steps below to export multiple users.

- Step 1 Use the Shift key or CTRL key and arrows or the mouse to select two or more users.
- **Step 2** Click the **Export** button in the Edit menu.

The Export dialog box opens.

Step 3 In the Save to field, enter the destination to download the file.

URL:	http:/	//kioskstage.veptc.com/in	dex.php/get/?file=	user_10;	xml	
Save to:	C:\D	ownloads\		•	Browse]-#
Save as:	user	_10(1).xml	Tag:			
Size: 2.04	КВ	Disk Free Space:	90.58GB			

Figure 3-26 Create New Download Dialog Box

Step 4 Click Download.

The file is an xml file.

Importing Users

If a person is a user on another instance of IEM, that user configuration can be imported into the new instance of IEM.

A Warning

Modifying any data within the exported file can prevent users from being imported correctly and failure of user creation. It is best to import the file "as is" and then modify the users' information in the IEM.

After you have the user file on your desktop, follow the steps below to import the user.

- **Step 1** Click **Users** in the left pane.
- Step 2 In the Edit menu, click Import User.





Step 3 In the Import dialog box, click **add**.

Figure 3-28	Import Dialog Box
	Import
loaded(0 f	iles - 0 Bytes) / total(0 files - 0 Bytes) 0%
	💿 add 🛛 upload
	Cancel

Step 4 Find the file on your computer. Choose the file and then click **Open**.

Figure 3-29 Select Files Dialog Box on Computer

Look in:	Desktop		🗾 🔇 🗊 🖡	୬ 🛄 🔻
œ.	Name	Size	Item type	Date modified
	Adobe FrameMaker	2 KB	Shortcut	11/30/2011 8:15
ecent Flaces	🛃 Mozilla Firefox	2 KB	Shortcut	5/30/2011 11:51
	naglt 8	2 KB	Shortcut	2/1/2010 11:04 A.
Desktop	KEXCEL - Shortcut	2 KB	Shortcut	9/4/2011 5:57 PM
	🔊 iSkysoft DVD Ripper	2 KB	Shortcut	4/14/2010 9:22 A.
6755B	POWERPNT - Shortc	2 KB	Shortcut	9/4/2011 5:57 PM
Libraries	B WinSCP	1 KB	Shortcut	11/25/2011 11:4
	😿 WINWORD - Shortcut	2 KB	Shortcut	9/4/2011 5:57 PM
	CombinedFile	1 KB	Text Document	12/9/2011 10:57
Computer	test	1 KB	Text Document	12/8/2011 2:21 P.
	user_sam	3 KB	Text Document	12/8/2011 2:56 P.
Network	iuser_10	3 KB	XML Document	12/8/2011 2:34 P.
	•			•
	File name:			Open
	Files of type: All Files (*	-)		- Cancel

Step 5 The file name then appears in the Import dialog box.

Figure 3-30 File Chosen in Import Dialog Box

Import	_
o user_9.xml	2.0 Kb
loaded(0 files - 0 Bytes) /	total(1 files - 2.0 Kb) 0%

Step 6 Click Upload.

ſ

A green check mark appears next to the file after it has been uploaded.

	Import	_			
~	user_9.xml	2.0 Kb			
	loaded(1 files - 2.0 Kb) / 1	total(1 files - 2.0 Kb) 100%			
		upload			
	Close	_			
$\mathbf{\rho}$					
Тір	If a file upload Choose that file	ed is not desired or ther e and then click remove	is an error messa	ge associated with it, dele	ete that f

Deleting Users

Administrators can delete a single user or multiple users.

Delete a Single User





Step 4 In the Confirm Delete dialog box, click **Delete**.

Figure 3-34	Confirm Delete Dialog Box
	Confirm Delete
Do you rea	Ily want to remove user "vep9"?
De	lete Cancel

Delete Multiple Users

Γ

Step 1	To delete multiple users, use the Shift key or CTRL key and arrows or the mouse to select two or more users.
Step 2	Click the Delete button in the Edit menu.
Step 3	In the Confirm Delete dialog box, choose Delete .

Users

1



снартек 4

Managing Devices

Revised: January 26, 2014, OL-26458-05

Chapter Overview

I

This chapter explains how to configure devices in the Cisco IEM. Topics in this chapter include:

- Firmware Version, page 4-2
- Devices, page 4-9
 - Learning Device Status, page 4-9
 - Adding a New Device, page 4-15
 - Batch Registration, page 4-16
 - Sending Messages to Devices, page 4-20
 - Opening an URL, page 4-21
 - Rebooting Devices, page 4-22
 - Restarting Applications, page 4-23
 - Turning Display On or Off, page 4-24
 - Muting or Unmuting Devices, page 4-25
 - Upgrading Devices, page 4-26
 - Applying Policies to Devices, page 4-27
 - Creating and Applying Custom Actions to Devices, page 4-29
 - Monitoring Events, page 4-32
 - Monitoring Performance, page 4-33
 - Deleting Devices, page 4-34
- Device Groups, page 4-35
 - Adding a New Group, page 4-35
 - Adding a Device to a Group, page 4-36
 - Adding Multiple Devices to a Group, page 4-37
 - Removing Devices from a Group, page 4-39



Firmware Version

Before you can add devices, verify the firmware version and update if necessary.

Step 1 Open a web browser.

Step 2 Enter the IEM's IP address in the browser.

The IEM login window opens.

Figure 4-1 IEM Login Window

Cisco Inte	eractive Experience Manager
Account 🔹	
User Name 🔹	
Password	
	Enter

- **Step 3** In the Account field, enter **Root**.
- Step 4 In the User Name field, enter Administrator.
- Step 5 In the Password field, enter cisco!123.You are now logged in the IEM as the administrator.
- **Step 6** In the left pane, click **Maintenance**.

	Devices
► 🤱	Users
⊾	Policies
►₩	Notifications
	Schedules
► <u>Å</u>	Accounts
▶%	Maintenance

Figure 4-2 Maintenance Button

Step 7 Click Supported Products





Step 8 Click IEC.

Figure 4-4 Product Name in the Left Pane



Step 9 Click 4600.

ſ

Figure 4-5 Model Name in the Left Pane





	Edit
+	New Family
-	Delete
\$	Versions

Figure 4-6 Versions Button in the Edit Menu

A list of versions is displayed in the center pane.

Figure 4-7 List of Versions

Version	Build	System Image	Applications Image	Specification	Active
2.1.0	5.40.55	Wed Aug 14 2013	Wed Aug 14 2013	Wed Aug 14 2013	Yes

If the version (build) listed is the desired version, proceed to the "Administrators" section of this chapter. If a different or newer version should be loaded or no versions are listed, continue this step set.

You will need the following files:

- System file
- Application file
- Specification file
- Step 11 Click New Firmware in the Edit menu.

The Add firmware dialog box opens.

Figure 4-8 Add Firmware Dialog Box

		Add f	irmw	are			
New firmware build	0	÷	*	0		0	¢
	Ok		1	Can	cel		

- Step 12 In the New firmware version fields, enter the latest version number.
- Step 13 Click Ok.
- **Step 14** Make sure that you have the following files available on your desktop:
 - System file
 - Application file
 - Specification file

<u>Note</u>

If specification file is incorrectly saved to your desktop, it will report 'Specification is not found' when uploading to the IEM. See "Saving XML Files" in this chapter to learn how to save this XML file to your desktop correctly.

Step 15 In the System Image column, click +.

Figure 4-9

Version	System Ima	ige
4.96.180	Wed Jul 27 2011	≠ ×
4.97.187	Tue Aug 2 2011	≠ ×
4.97.188	Tue Aug 2 2011	\Rightarrow ×
4.98.191	H	
	+	

Add Image Button

The Upload Image dialog box opens.

Step 16 Click +add.

ſ

Figure 4-10 Upload Image Dialog Box



Step 17 Find the file on your desktop and click Open.

9	Name			
<u></u>	Name	Size	Item type	Date modified
Parent Disease	Adobe FrameMaker	2 KB	Shortcut	11/30/2011 8:15
cent Flaces	🗒 Mozilla Firefox	2 KB	Shortcut	5/30/2011 11:51
	🔊 SnagIt 8	2 KB	Shortcut	2/1/2010 11:04 A.
Desktop	KEXCEL - Shortcut	2 KB	Shortcut	9/4/2011 5:57 PM
	🔊 iSkysoft DVD Ripper	2 KB	Shortcut	4/14/2010 9:22 A.
(internal)	POWERPNT - Shortc	2 KB	Shortcut	9/4/2011 5:57 PM
Libraries	WinSCP	1 KB	Shortcut	11/25/2011 11:4
1	😿 WINWORD - Shortcut	2 KB	Shortcut	9/4/2011 5:57 PM
100 C	CombinedFile	1 KB	Text Document	12/9/2011 10:57
Computer	test	1 KB	Text Document	12/8/2011 2:21 P.
	user_sam	3 KB	Text Document	12/8/2011 2:56 P.
Network	iuser_10	3 KB	XML Document	12/8/2011 2:34 P.
	•	111		•
	File name:			- Open

Figure 4-11 Select Files Dialog Box

The file appears in the Upload Image dialog box.

Figure 4-12 System File in Upload Image Dialog Box

Upload Image
kae-sys-4.98.fwimg
loaded(0 files - 0 Bytes) / total(0 files - 0 Bytes) 0%
Cancel

Step 18 Click upload.

The file will appear in the System Image list.

Step 19 In the Application column, click +.

Figure 4-13	Add Image Button
-------------	------------------

Wed Jul 27 2011	≓ ×
Tue Aug 2 2011	≓ ×
+	

The Upload Image dialog box opens.

Step 20 Click +add.

loaded(0 files - 0 Bytes) / total(0 files - 0 Bytes) 0%

Figure 4-14 Upload Image Dialog Box



Figure 4-15 Select Files Dialog Box

Name Size Item type Date modified Desktop	Look in:	Desktop		🛨 🔇 🗊 🖡	🎐 🛄 -
Adobe FrameMaker 2 KB Shortcut 11/30/2011 8:15 . Mozilla Firefox 2 KB Shortcut 5/30/2011 11:51 . Desktop Snaglt 8 2 KB Shortcut 2/1/2010 11:04 A Desktop Skysoft DVD Ripper 2 KB Shortcut 9/4/2011 5:57 PM Dibranes Skysoft DVD Ripper 2 KB Shortcut 9/4/2011 5:57 PM WinSCP 1 KB Shortcut 9/4/2011 5:57 PM WiNWORD - Shortcut 2 KB Shortcut 9/4/2011 5:57 PM Computer CombinedFile 1 KB Shortcut 9/4/2011 5:57 PM WiNWORD - Shortcut 2 KB Shortcut 9/4/2011 5:57 PM Weiser_sam 3 KB Text Document 12/8/2011 10:57. Weiser_sam 3 KB Text Document 12/8/2011 2:56 P. Weiser_sam 3 KB Text Document 12/8/2011 2:56 P. Weiser_sam 3 KB Text Document 12/8/2011 2:34 P. K 11 11/3/2011 2:34 P. 11/3/2011 2:34 P. K 11/3/2011 2:34 P. 11/3/2011 2:34 P. 11/3/2011 2:34 P. K 11/3/201	C.	Name	Size	Item type	Date modified
electri triades	And Disease	Adobe FrameMaker	2 KB	Shortcut	11/30/2011 8:15
Image: Snagit 8 2 KB Shortcut 2/1/2010 11:04 A Desktop Image: Skysoft DVD Ripper 2 KB Shortcut 9/4/2011 5:57 PM Image: Skysoft DVD Ripper 2 KB Shortcut 9/4/2011 5:57 PM Image: Downer POWERPNT - Shortcut 2 KB Shortcut 9/4/2011 5:57 PM Image: Downer POWERPNT - Shortcut 2 KB Shortcut 9/4/2011 5:57 PM Image: Downer POWERPNT - Shortcut 2 KB Shortcut 9/4/2011 5:57 PM Image: Downer POWERPNT - Shortcut 2 KB Shortcut 9/4/2011 5:57 PM Image: Downer POWERPNT - Shortcut 2 KB Shortcut 9/4/2011 5:57 PM Image: Downer Downer POWERPNT - Shortcut 2 KB Shortcut 9/4/2011 5:57 PM Image: Downer Downer Downer Downer Downer POWERPNT - Shortcut 2 KB Shortcut 9/4/2011 2:57 PM Image: Downer Downe	ecent Flaces	🛞 Mozilla Firefox	2 KB	Shortcut	5/30/2011 11:51
Desktop Image: Computer interview interv		naglt 8	2 KB	Shortcut	2/1/2010 11:04 A.
Image: Skysoft DVD Ripper 2 KB Shortcut 4/14/2010 9:22 A Image: Skysoft DVD Ripper 2 KB Shortcut 9/4/2011 9:57 PM Image: Skysoft DVD Ripper 2 KB Shortcut 9/4/2011 5:57 PM Image: Skysoft DVD Ripper 1 KB Shortcut 1/25/2011 11:4. Image: Skysoft DVD Ripper 1 KB Shortcut 9/4/2011 5:57 PM Image: Skysoft DVD Ripper 2 KB Shortcut 9/4/2011 5:57 PM Image: Skysoft DVD Ripper 1 KB Text Document 12/9/2011 10:57 PM Image: Skysoft DVD Ripper 1 KB Text Document 12/8/2011 2:31 PM Image: Skysoft DVD Ripper 3 KB XML Document 12/8/2011 2:35 PM Image: Skysoft DVD Ripper 3 KB XML Document 12/8/2011 2:35 PM Image: Skysoft DVD Ripper 3 KB XML Document 12/8/2011 2:35 PM Image: Skysoft DVD Ripper 3 KB XML Document 12/8/2011 2:35 PM	Desktop	武 EXCEL - Shortcut	2 KB	Shortcut	9/4/2011 5:57 PM
Image: Second state of the state o	(Second	🔊 iSkysoft DVD Ripper	2 KB	Shortcut	4/14/2010 9:22 A.
Libranes WinSCP 1 KB Shortcut 11/25/2011 11:4 WWINWORD - Shortcut 2 KB Shortcut 9/4/2011 5:57 PM Computer test 1 KB Text Document 12/9/2011 10:57 . User_sam 3 KB Text Document 12/8/2011 2:31 P. User_10 3 KB XML Document 12/8/2011 2:34 P. File name: Open	1000 B	POWERPNT - Shortc	2 KB	Shortcut	9/4/2011 5:57 PM
WINWORD - Shortcut 2 KB Shortcut 9/4/2011 5:57 PM Computer CombinedFile 1 KB Text Document 12/9/2011 10:57 Itest 1 KB Text Document 12/8/2011 2:21 P. Itest 1 KB Text Document 12/8/2011 2:56 P. Itest 3 KB Text Document 12/8/2011 2:34 P. Itest 3 KB XML Document 12/8/2011 2:34 P. Itert Itert Itert Itert	Libraries	B WinSCP	1 KB	Shortcut	11/25/2011 11:4
Computer CombinedFile 1 KB Text Document 12/9/2011 10:57 . Computer 1 kB Text Document 12/8/2011 2:21 P. User_sam 3 KB Text Document 12/8/2011 2:32 P. User_10 3 KB XML Document 12/8/2011 2:34 P. Image: Image: Image: Image: Image:		😿 WINWORD - Shortcut	2 KB	Shortcut	9/4/2011 5:57 PM
Computer itest ites	187 C	CombinedFile	1 KB	Text Document	12/9/2011 10:57
Network 	Computer	test	1 KB	Text Document	12/8/2011 2:21 P.
Network Image: second sec		user_sam	3 KB	Text Document	12/8/2011 2:56 P.
< III ► File name: Open	Network	📄 user_10	3 KB	XML Document	12/8/2011 2:34 P.
File name: Open		•	111		•
		File name:		1	✓ Open

The file appears in the Upload Image dialog box.

Figure 4-16 Application File in Upload Image Dialog Box

Upload Image
kae-apps-4.206.fwimg
loaded(0 files - 0 Bytes) / total(0 files - 0 Bytes) 0%
● add upload
Cancel

Step 22 Click upload.

ſ

The file will appear in the Applications Image list.

Step 23 In the Specification column, click +.

Specification	n
Wed Jul 27 2011	≓ ×
Tue Aug 2 2011	⇒ ×
+	

Figure 4-17 Add Image Button

The Upload Image dialog box opens.

Step 24 Click +add.

Figure 4-18 Up	load Image	Dialog	Box
----------------	------------	--------	-----

Upload Image
loaded(0 files - 0 Bytes) / total(0 files - 0 Bytes) 0%
● add upload
Cancel

Step 25 Find the file on your desktop and click **Open**.

Figure 4-19 Select Files Dialog Box

Look in:	Desktop		🛨 🔇 🗊 🖡	୬▼
C:	Name	Size	Item type	Date modified
2 2	Adobe FrameMaker	2 KB	Shortcut	11/30/2011 8:15
ecent Flaces	🛃 Mozilla Firefox	2 KB	Shortcut	5/30/2011 11:51
	naglt 8	2 KB	Shortcut	2/1/2010 11:04 A.
Desktop	KEXCEL - Shortcut	2 KB	Shortcut	9/4/2011 5:57 PM
(Second	🔊 iSkysoft DVD Ripper	2 KB	Shortcut	4/14/2010 9:22 A.
1000 B	POWERPNT - Shortc	2 KB	Shortcut	9/4/2011 5:57 PM
Libraries	B WinSCP	1 KB	Shortcut	11/25/2011 11:4
	😿 WINWORD - Shortcut	2 KB	Shortcut	9/4/2011 5:57 PM
- 1	CombinedFile	1 KB	Text Document	12/9/2011 10:57
Computer	test	1 KB	Text Document	12/8/2011 2:21 P.
	user_sam	3 KB	Text Document	12/8/2011 2:56 P.
Network	🔮 user_10	3 KB	XML Document	12/8/2011 2:34 P.
	•		-	•
	File name:			Open
	Files of type: All Files (*	•		Cancel

The file appears in the Upload Image dialog box.



Figure 4-20 Specification File in Upload Image Dialog Box

Step 26 Click upload.

The file will appear in the Specification list.

All three files should now be uploaded.

Step 27 In the right pane, click **enable**.

The version is now active. In the Active column, the word "Yes" appears.

Figure 4-21	Active Column

The images will become available for pushing to the IECs that are registered and active in the IEM. Deactivate the previous version if one was already activated. You do not need to delete older versions.

Devices

I

A device is a Cisco IEC4600 Series.

Learning Device Status

You can view information about a particular device. The following steps will show you how to get all the information about a device.

Step 1 Click **Devices** in the left pane.

4-22 Devices Button
Devices
Users
Policies
Alerts
Schedules
Accounts
Maintenance

In the left pane, a list of all the devices and groups are displayed.

In the center pane, the icons for those devices and groups are displayed.

Figure 4-23 Device Icons in Center Pane



To view detailed information about the state of the devices, click the **Show as table** button at the upper left corner of the center pane.

Figure 4-24 Show as table Button



I

This screen provides the administrator with visual device monitoring so that they can assess the state of the devices quickly and react accordingly. The snapshot, serial number, name, IP address, version of the firmware, CPU and memory utilization, the uptime, and the last ping period are indicated for each device in a grid view. The columns can be dropped and dragged in different orders to best suit the needs of the administrator.



Figure 4-25 Grid View of Devices

To view what the devices are displaying on their attached touchscreens/monitors, click the **Show** screenshots button at the upper left corner of the center pane.

Figure 4-26 Device Screenshots



Step 2 To identify whether the device is turned on or off, find the device in the center pane. Look at the box to the upper right of the icon. If the box is green and contains the word ON, the device is plugged into a working electrical outlet. If the box is red and contains the word OFF, the device is unplugged or the power to the electrical outlet has been turned off. Below the ON/OFF indication, there is an indication of the number of days or hours that the device has been on or off (d=days, h=hours).



Figure 4-27 Device that has been on for 5 days

Figure 4-28 Device that bas been off for 10 days and 19 hours



<u>P</u> Tip

If the device has been recently turned on or off, refresh the page by clicking the Refresh button in the top pane. You may need to refresh the page a few times to allow the change in status to be registered by the Cisco IEM.

- **Step 3** If there is a firmware update available for a device, a red box containing the letters FW appears between the icon and the device's name.
- Step 4 Double-click on the device icon to display the tabs containing information about that particular device. The first tab is the General tab, which contains the device name, serial number, model, version number, location, and description. It also indicates its status (ON or OFF) and contains a button to get the maintenance code for the device.

Γ

Figure 4-29

General Tab

General Me	ember Of Profile	Policies	Status	Events	Performance	Effect.Prof.	
	Device Name	* Single_Core					
		Alphanumeric,	_, -, 3 characters min	nimum, must start w	/ith letter.		
	Serial Number	656015330005					
	Maintenance Code		how				
	Product	IEC					
	Family	4600					
	Version	4000					
	version	5 420 450					
	Build	5.130.150					
	Status	ON					
	Uptime	48m 7s					
	Location						
	Description						
		STREE -	Cancel				

Step 5 Click the **Member Of** tab to learn whether the device is a member of a group.

I

Genera	I Member Of	Profile	Policies	Status	Events	Performance	Effect.Prof.
	Test_from_103						
▶ 	GroupB						
	GrpupC2						
►	🗖 Multi						
► 	New2						
			ABDY	Cancel			

Figure 4-30 Member Of Tab

Step 6 Click the **Profile** tab to view the device settings.

Γ

	General	Member Of	Profile	Policies	Status	Events	Performance	Effect.Prof.	1	4
Filter	8	🗖 run time pr	operties only							E III
Property		Comp	atibility		Va	alue			Description	
►		-								
▶ 💼 audio										
▶ 💼 browser										
▶ 💼 clock										
▶ 💼 cohttpd										
▶ 💼 display										
emergency										
▶ 💼 flashplayer										
▶ 💼 hotkeys										
▶ 💼 keyboard										
▶ 💼 management										
▶ 💼 mouse										
network										
▶ 💼 power										
▶										
▶ 💼 profile										
P -				AllalV	Cancel					A

Figure 4-31 Profile Tab

Step 7 Click the **Policies** tab to learn which policies have been applied to that device.



Step 8

Click the Status tab and expand the menu to learn the following about the device:

- Network interfaces' net masks, MAC addresses, and IP addresses; default gateway IP address; and ٠ DNS servers IP addresses
- Locale information including time zone, language, and country ٠
- Display screen resolution •
- Connected USB devices information ٠

	General	Member Of	Profile	Policies	Status	Events	Performance	Effect.Prof.	
	Na	ame					Value		
🕶 💼 Hardware					1				
1 CPU					1x1.2GHz				
🕕 Memory					2GB				
🕕 Storage					60GB				
Network									
🔻 🚞 Interface 10'									
MAC address					00:00:00:00:00:00)			
🔻 🚞 Interface 'eth0'									
MAC address					00:21:11:00:21:C	1			
🕕 IP address					171.69.73.167				
🕕 Net mask					255.255.254.0				
🔻 🚞 Interface 'ra0'									
MAC address					74:2F:68:0A:F2:D	5			
🔻 🚞 Interface 'pan0'									
MAC address					96:E4:F9:70:4A:11	-			
DNS servers									
1					171.70.168.183				
1 2					173.36.131.10				
3					64.102.6.247				
🕕 Default gateway					171.69.72.1				

Figure 4-33 Status Tab

Adding a New Device

You will need the following to register a new device:

- 1. Serial number of the IEC4600 Series device
- 2. License in the IEM



ſ

For information about licensing, refer to the Cisco Interactive Services Solution Licensing Guide.

Follow the steps below to add a new device.

- **Step 1** Click **Devices** in the left pane.
- Step 2 In the Edit pane, click New Device.

	Edit
+	New Device
Ŧ	New Group
**	Import Device

Figure 4-34

Step 3 In the Register New Device dialog box, enter a device name in the Device Name field.

	Register New Device
Device Name 🔹	<u></u>
	Alphabetical characters only
Serial Number 🌸	
	Use Numbers only
Description	[
	Register Cancel

Figure 4-35 Register New Device Dialog Box

New Device Button

dash/minus/hyphen sign is no longer allowed to be used within device names

Only alphanumeric and underscores can be entered in the device name field. The

Step 4	Enter the IEC's serial n	umber in the Serial N	umber field.
--------	--------------------------	-----------------------	--------------

Step 5	(Optional)	Enter a description	on of the device
--------	------------	---------------------	------------------

Step 6 Click Register.

Note

Batch Registration

You can also register multiple IEC devices to the IEM at one time.

- Step 1 Open Notepad or Microsoft Excel on your computer.
- **Step 2** Enter the serial numbers with one per row.

Γ

4	А	B
1	840359954843	
2	876045922769	
3	947030763333	
4	654876800986	
5	996689007654	
6	889977224670	
7	799876546790	
8	398743009866	
9	458758900764	
10	875423007533	
11		

Figure 4-36 Serial Numbers in Excel Spreadsheet

Step 3 Save as type CSV (Comma delimited).

eneral Secu	urity Details Previous Versions
Xa,	batch
Type of file:	Microsoft Excel Comma Separated Values File (.csv)
Opens with:	Microsoft Excel Change
Location:	C:\Users\budgie\Desktop
Size:	40 bytes (40 bytes)
Size on disk:	4.00 KB (4,096 bytes)
Created:	Today, June 04, 2012, 16 minutes ago
Modified:	Today, June 04, 2012, 16 minutes ago
Accessed:	Today, June 04, 2012, 16 minutes ago
Attributes:	Read-only Hidden Advanced

Figure 4-37 CSV File Properties

- **Step 4** In the IEM, click **Devices** in the left menu.
- **Step 5** Click **Import Device** in the Edit menu to the right side of the screen.

3 Import Device Button

Edit		
+	New Device	
+	New Group	
**	Import Device	



Γ

Figure 4-39



Import Dialog Box

Step 7 Find the file on your computer. Choose the file and then click **Open**.

(Ba)				
	Name	Size	Item type	Date modified
Passet Plassa	Adobe FrameMaker	2 KB	Shortcut	11/30/2011 8:15
Necenii Flaces	🛞 Mozilla Firefox	2 KB	Shortcut	5/30/2011 11:51
	naglt 8	2 KB	Shortcut	2/1/2010 11:04 A.
Desktop	EXCEL - Shortcut	2 KB	Shortcut	9/4/2011 5:57 PM
	🔊 iSkysoft DVD Ripper	2 KB	Shortcut	4/14/2010 9:22 A.
COMPANY.	POWERPNT - Shortc	2 KB	Shortcut	9/4/2011 5:57 PM
Libraries	B WinSCP	1 KB	Shortcut	11/25/2011 11:4
1 .	😿 WINWORD - Shortcut	2 KB	Shortcut	9/4/2011 5:57 PM
100 C	CombinedFile	1 KB	Text Document	12/9/2011 10:57
Computer	test	1 KB	Text Document	12/8/2011 2:21 P.
	user_sam	3 KB	Text Document	12/8/2011 2:56 P.
Network	🔮 user_10	3 KB	XML Document	12/8/2011 2:34 P.
	€ [111		•
	File name:			Open

Figure 4-40 Select Files Dialog Box on Computer

Step 8 The file name then appears in the Import dialog box.

	Impor	t
0	batch.csv	40 Bytes
	loaded(0 files - 0 Bytes)	/ total(1 files - 40 Bytes) 0%
		upload
	Close	

Figure 4-41 File in Import Dialog Box

Step 9 Click Upload.

A green check mark appears next to the file after it has been uploaded.

atch.csv	40 Bytes
ded(1 files - 40 Bytes) / tota	al(1 files - 40 Bytes) 100%
	atch.csv ded(1 files - 40 Bytes) / tota

Figure 4-42 File Uploaded

Step 10 Click Close.

The IECs will appear in the Devices list in the left menu and as icons in the center pane.

Sending Messages to Devices

Messages can be sent to the IEC4600 Series. For example, if the IEM will be offline for a period of time, you can send a message that the devices may experience issues during that time so as to prepare the users of the kiosks. If you want to send a message to all devices, follow the steps below.

Step 1 Click **Devices** in the left pane.

Step 2 In the right pane, click **Predefined actions** to open the list of actions that have been predefined.

Figure 4-43 Predefined Actions Menu



Step 3 Click Message.

ſ

Figure 4-44 Send Message Dialog Box

Send Message	
 Show message Hide message Timeout (sec) 	
Send action to device Single_Core	
Ok Cancel	

Step 4 In the **Send Message** dialog box, enter a message in the field.

Step 5 Click Ok.

Opening an URL

An URL can be opened on the video display connected to the IEC4600 Series. Follow the steps below to open an URL.



If you want to select multiple devices to perform predefined actions such as Message or Open URL, use the Shift key or CTRL key and arrows or the mouse to select two or more devices in either the icon or grid view.

- **Step 1** Click **Devices** in the left pane.
- **Step 2** In the right pane, click **Predefined actions** to open the list of actions that have been predefined.

Figure 4-45 Predefined Actions Menu



Step 3 Click Open URL.

Figure 4-46 Open URL Remotely Dialog Box

	Open URL remotely	
URL to open	Will be applied to all devices from VEP account	
	Ok Cancel	

Step 4 Enter a URL in the **URL to open** field.

Step 5 Click Ok.

Rebooting Devices

After changes are made to a device's settings, the IEC4600 Series must be rebooted for those changes to take effect.

If an application has frozen, you can restart the application rather than rebooting the device. Restarting an application will not cause the entire screen to go black and show the rebooting process.

Follow the steps below to reboot a device.

- **Step 1** Click **Devices** in the left pane.
- **Step 2** In the Edit pane, click **Predefined actions** to open the list of actions that have been predefined.



Figure 4-47 Predefined Actions Menu

Step 3 Click Reboot.

I



Restarting Applications

The applications on the IEC4600 Series can be restarted remotely. Restart an application if it is non-responsive. Follow the steps below to restart applications.

- **Step 1** Click **Devices** in the left pane.
- Step 2 In the right pane, click Predefined actions to open the list of actions that have been predefined.

Edit	
Predefined actions	
Ø	Message
URL the	Open URL
**	Reboot
U	Display On/Off
*	Mute
0	Upgrade
Q	Restart Application

Figure 4-49 Predefined Actions Menu

Step 3 Click Restart Application.





Turning Display On or Off

You can control a display connected to an IEC4600 Series device. To turn the display on or off, follow the steps below.

Step 1 Click **Devices** in the left pane.

Step 2 In the right pane, click **Predefined actions** to open the list of actions that have been predefined.
	Edit
Pr	edefined actions
ø	Message
URL	Open URL
*	Reboot
U	Display On/Off
*	Mute
Ø	Upgrade
Q	Restart Application

Figure 4-51 Predefined Actions Menu

Step 3 Click Display On/Off.

Figure 4-52 Device Display On/Off Dialog Box



Muting or Unmuting Devices

ſ

The IEC4600 Series device can be muted or unmuted remotely. To mute or unmute the devices, follow the steps below.

- **Step 1** Click **Devices** in the left pane.
- Step 2 In the right pane, click **Predefined actions** to open the list of actions that have been predefined.



Figure 4-53 Predefined Actions Menu

Step 3 Click Mute.



Step 4 Click Mute or Unmute.

Upgrading Devices

The software of the IEC4600 Series can be upgraded remotely. Follow the steps below to upgrade their software.

- **Step 1** Click **Devices** in the left pane.
- **Step 2** In the right pane, click **Predefined actions** to open the list of actions that have been predefined.

Edit						
Pre	defined actions					
ø	Message					
URL	Open URL					
*	Reboot					
U	Display On/Off					
*	Mute					
Ø	Upgrade					
Q	Restart Application					

Figure 4-55 Predefined Actions Menu

Step 3 Click Upgrade.

Figure 4-56 Upgrade Devices Dialog Box



Applying Policies to Devices

A policy provides an easy and flexible way of applying settings to multiple devices. Policies can be persistent (long-term) or runtime (short-term). Runtime policies can be used for troubleshooting, demos, or special events.

Use the steps below to apply a policy to a device.

Step 1 Click Devices.

I

Step 2 In the center pane, double-click a device's icon.

Figure 4-57 Device	lcons in Center Pane
--------------------	----------------------

BLRGBC0	53030124	EN656015030118	MyDexice	GAPvep2	5malkiosx	DSiTestUnit	BLRGBC3	
BGL142singlecor.	SJC30051	MOBILEDEMO	5N656015030016	BLRGBC2	WMT	GAPvep3	EM030072	BIN-RI-TC
GAPvep1	Sing1	dgus 💭	BLADCTEST1	groupG				

- Step 3 Click the Policies tab.
- **Step 4** In the Available policies list, choose a policy.

Figure 4-58 Availa	ble Pol	icies l	List
--------------------	---------	---------	------

	General	Member Of	Profile	Paton	Clatus -	Eventa Performance		62
-	Available policies				Appl	led policies	Schedule	
Rotate90CCW				1				
Actate30				1044				1040
& Rotate 180								
Rogbol-HDM								-

Step 5 Click the Green Arrow.

The policy now appears in the Applied policies list.

Figure 4-59 Applied Policies List

	General	Mamber Of	Profile	Pitters	Otaus	Everta	Performance		6
1	Available policies				Ao	plied policies		Schedule	
YTYLLYS				•	& Rotate90		always		
L DUALSCREEN									12417
A THOMSON				1000					1000
1 DotA				1000					121

Step 6 (Optional) Add more policies to the Applied policies list.



To remove a policy from the Applied policies list, choose the policy and click the **Red Arrow**.

- Step 7 Click Apply.
- Step 8 Click Close.
- **Step 9** In the Reboot Devices Dialog Box, click **Ok**.

Figure 4-60 Reboot Devices Dialog Box

_	Reboot Device	
	Will be applied to device SJC30124 Reboot device?	
	Ok Cancel	

ſ

Creating and Applying Custom Actions to Devices

A custom action can be created and applied to all devices within an account.

Step 1 Click Policies.

Figure 4-61 Policies Button

	Devices
▶ 🤱	Users
▶ 🆺	Policies
►#	Notifications
	Schedules
► <u>Å</u>	Accounts
▶%	Maintenance

Step 2 In the Edit menu, click New Policy.

Figure 4-62 Edit Menu



The Create New Policy dialog box opens.

-	Create New Policy
°olicy Name 🔹	
Is action	Alphanumeric, _, -, 3 characters minimum, must start with letter.
Description	

Figure 4-63 Create New Policy Dialog Box

- **Step 3** Enter a policy name in the **Policy Name** field.
- **Step 4** Check the **Is action** check box. After you check the Is action checkbox, you will see the Add to custom actions checkbox.
- Step 5 Check the Add to custom actions checkbox.

Policy Name * Policy_A Alphanumeric, _, -, 3 characters minimum, must start with letter Is action I Id to cust I Description Add to custom actions		
Alphanumeric, _, -, 3 characters minimum, must start with letter Is action Image: A start with letter dd to cust Image: Comparison of the start with letter Description Add to custom actions	olicy Name 🜸	Policy_A
Is action Is action Is action Is action Is action Is actions		Alphanumeric, _, -, 3 characters minimum, must start with letter.
Add to cust Image: Add to custom actions	Is action	~
Description Add to custom actions	Add to cust	₽
	Description A	dd to custom actions
	_	

Figure 4-64 Add to Custom Actions Checkbox

Step 6 (Optional) Enter a description of the policy in the **Description** field.

Step 7 Click Create.

A new custom action is created and its icon appears in the center pane along with policies and other custom actions.



Custom actions are indicated by a blue arrow.



Step 8 Click Devices.

Figure 4-66 Devices Button

	Devices	
12	Users	
▶∎	Policies	
► 🗱	Alerts	
•	Schedules	
► Å	Accounts	
**	Maintenance	

Step 9 In the right pane, click **Custom actions** to open the list of actions.



Γ

Figure 4-67 Custom Actions Menu

Step 10 In the Custom actions menu, click on a custom action.

Step 11 Click **Call** in the Call Action dialog box to apply that custom action, which is a policy, to all devices in that account.

Figure 4-68	Call Action Dialog Box
-	Call action
Apply policy 'EE	3C' to all devices from VEP account?
	all Cancel

Monitoring Events

You can monitor IEC4600 Series events remotely or view a log of events, such as errors and warnings. There is a filter that lets you view a subset of events to help pinpoint a problem.

The logging of events can be controlled within the profile of a device or a policy applied to that device. To configure which browser events are logged, see the "Configuring the Browser" section of Chapter 5.

- **Step 1** Click **Devices** in the left pane.
- **Step 2** In the center pane, double-click a device's icon.



Step 3 Click the Events tab.

	General	Namber Of	Profile	Policies	Stakus	Events	Performance	
			Event trees				Harran	
	Sat Day 10.11	10.53 GMT-0700 2	011			Densis of raminants	Title Constant weeks constructed CODD Exclude analysis in	
Severities 2	Sat Dec 10 11	30 39 CMT-0700 2	011			Rowser requests	The increased vestor comic collection ORRAN Styles alone Subm	
	Sat Dec 10 11	29 58 Call-0700 2	011		-	Drowner reduests	Title (contant) varie comicontant/COBR44.03/(a aAeo/EG h	
Eutor	Sat Dec 10 11	29-56 GMT-0700 2	011			Rowser requests	Title (content vests com/content/CDERA) (5//s aacodedin	
U Warning	Sat Dec 10 11:	29.56 GMT-0700 2	011		1	Drowser requests	Tits (content yests com/content/COBRAUS/Is accoReto)	
The last second second	Sat Dec 10 11	29-56 GMT-0700 2	011			Browser requests	Titls ilcontent vestc.com/content/COBRAUSVisaApp/Rese	
[] anounteeu	Sat Dec 10 11	29.56 GMT-0700 2	011			Browser requests	http://content.veptc.com/content/COERA/UTIVisiaApp/weico	
Debug	Sat Dec 10 11.	29-56 GMT-0700 2	011		1	Browser requests	http://content.veptc.com/content/COER4/USVIsaApp/	
Facilities	Sat Dec 10 11:	29 56 GMT-0700 2	011		1	Browser requests	Title Roontent veptc.com/content/COBRA/US/VisiaApp/seal s	
Turners 2	Sat Dec 10 11:	29.56 GMT-0700 2	011		1	Browser requests	http://content.veptc.com/content/COBRAUSVisaApp/butto	
S prowner	Sat Dec 10 11:	29.58 GMT-0700 2	011		1	Browser requests	http://content.veptc.com/content/COER4/USV/saApp/Subm	
😨 co	Sat Dec 10 11:	29.56 GMT-0700 2	011		1	Browser requests 1/to incontent veptc com/content/COBRAUSVIsaApp/hardcog		
	Sat Dec 10 11:	29.56 GMT-0700 2	011		1	Browser requests 'http://content.veptc.com/content/COBRA/USV/isaApp/Snapsh-		
Ø deplay	Sat Dec 10 11:	29.55 GMT-0700 2	011		1	Browser requests http://content.veptc.com/content/COBRAUSV/saAppicitck2sn		
2 keyboard	Sat Dec 10 11	29.56 GMT-0700 2	011		1	Browser requests http://content.veptc.com/content/COBRAUGVIsaAppicameyer		
	Sat Dec 10 11:	29.55 GMT-0700 2	011		. (Browser requests http://content.veptc.com/content/COBRA/USV/saApp7.		
😨 mouse	Sat Dec 10 111	29.43 GMT-0700 2	011		1	Browser requests 'http://content.veptc.com/content/COBR4/startpage/index.htm		
2 melicator	Sat Dec 10 11:	29.35 GMT-0700 2	011		1	Browser requests 1/8p./content.veptc.com/content/COBRA/webclip/.		
	Sat Dec 10 11	29.35 GMT-0700 2	011		1	Browser requests http://content.veptc.com/content/COBRA/webclip/bg.jpg		
2 screenmonitor	Sat Dec 10 11;	29 15 GMT-0700 2	011		1	Management failure 'Field 'message' on events must contains maximum 255		
🛛 austern	Sat Dec 10 111	29 08 GMT-0700 2	011		1.8	Browser requests "http://ds-log.channelinfelligence.com/?vid=11303&eid=13P		
	Sat Dec 10 11:	29.08 GMT-0700 2	011		1	Browser requests 'http://switch.atdmi.com/laction/bestbuy_page//3/catNam		
😨 volume	Sat Dec 10 11:	29:08 GMT-0700 2	011			Browser requests	Titlp itspe atom comimages/pixel.gif.	
Max number of events	Sat Dec 10 11:	29.08 GMT-0700 2	011		1	Management tailu	re Field "message" on events must contains maximum 25	
200	Sat Dec 10 11:	29.08 GMT-0700 2	011			Browser requests	http://mages.bestbuy.com/BestBuy_US/js/fsrscripts/fores	
100	Sat Dec 10 11:	Sat Dec 10 11 29 07 GMT-0700 2011			1	Browser requests Tritp://mages.bestbuy.com/BestBuy_U5/js/tracking/atas-		
Time range	Sat Dec 10 11:	Sat Dec 10 11 29 07 GMT-0700 2011			1	Browser requests http://mages.bestbuy.com/BestBuy_US(s/tracking/onel-mi		
😨 AL	Sat Dec 10 11;	29.07 GMT-0700 2	011		1	Browser requests	http://mages.bestbuy.com/BestBuy_US/js/tracking/s_cod	
1000	Sat Dec 10 11:	29-07 GMT-0700 2	011		1	Browser requests	http://mages.bestouy.com/80/BestBuy_US/en_US/mage	
pen in	Sat Dec 10 11:	29:07 GMT-0700 2	011		1	Drowser requests	http://mages.bestbuy.com/BestBuy_Utilien_Util/mages/a	
THE LEAD	Sat Dec 10 11	29.97 GMT-0700 2	011		1	Browser requests	http://mages.bes/buy.com.80/Bes/Buy_US(js/bby/inno-m	
	Sat Dec 10 11;	29 07 GAIT-0700 2	011		1	Drowser requests	Tits ilmages bestbuy com 80/BestBuy_US(s/bbylabl-min	
	the second second second	AT A 20 AT ALL AND ALL						

Figure 4-70 Events Tab

- **Step 4** (Optional) To filter events by severity, check one or more Severities check boxes.
- **Step 5** (Optional) To filter events by facilities, check the one or more Facilities check box.
- **Step 6** In the Max number of events field, choose a value.
- Step 7 To specify a time range, uncheck the All check box and enter dates in the From and Till fields.
- Step 8 Click Apply.

Monitoring Performance

ſ

You can monitor performance of an IEC's memory and CPU usage as well as the temperature of the CPU.

- **Step 1** Click **Devices** in the left pane.
- **Step 2** In the center pane, double-click a device's icon.



BLRGBC0	5JC30124	EN656015030118	MyDevice	GAPvep2	5malKiesk	DOITestUnit.	BLRGBC3	
BGL142singlecor	SJC30061	MOBILEDEMO	SN656015030015	BLRGBC2	WMT	GAPvep3	DK030072	BBRTC
				-				
				amen				





Figure 4-72 Performance Tab

- Step 4 (Optional) To filter performance by memory values, uncheck one or more Memory check boxes.
- Step 5 (Optional) To filter events by CPU values, uncheck the one or more CPU check box.
- Step 6 Click Apply.

Deleting Devices

Administrators can delete a single device or multiple devices.

Delete a Single Device

Step 1 Choose a device and then click the **Delete** button in the Edit menu.

Figure 4-73 Edit Menu



Step 2 In the Confirm Delete dialog box, choose **Delete**.

Delete Multiple Devices

- **Step 1** To delete multiple devices, use the Shift key or CTRL key and arrows or the mouse to select two or more devices in either the icon or grid view.
- **Step 2** Click the **Delete** button in the Edit menu.
- **Step 3** In the Confirm Delete dialog box, choose **Delete**.

Figure 4-74 Select Multiple Devices and Delete Them



Device Groups

Devices can be grouped together. A device group can then be configured and managed rather than configuring and managing devices individually.

Adding a New Group

I

To add a new group, follow the steps below.

- **Step 1** Click **Devices** in the left pane.
- Step 2 In the Edit menu, click New Group.

Figure 4-75	New Group	Button in	the Edit Menu
-------------	-----------	-----------	---------------

-	Edit
+	New Device
+	New Group
**	Import Device

Step 3 In the Create New Group dialog box, enter a group name in the Group Name field.

Figure 4-76

76 Create New Group Dialog Box

Group Name 🤉	Alphanumeric, _, -, 3 characters minimum, must start with letter
	Create

Adding a Device to a Group

To add a device to a group, follow these steps:

- **Step 1** Click **Devices** in the left pane.
- **Step 2** In the center pane, double-click the device's icon.

	-		-					
BLRGBC0	53C30124	EN656015030118	III MyDevice	GAPvep2	5mal9Gost	DSITestUnit	BLRGBC3	
EGI 147sintinger	SJC3001		594646015030035	BI BGBC2	WAIT	CAP-en3	DK030077	BARIC
				_				
				groupG				

Figure 4-77 Device and Group Icons in the Center Pane

Step 3 Click the **Member Of** tab.



N	General MumberOF Profile Policies Status Events Performan	
14	P ∰ □ groopG	

- **Step 4** Check a group's check box.
- Step 5 Click Apply.
- **Step 6** In the Predefined actions menu, click **Reboot**.

Figure 4-79	Reboot Devices Dialog Box
5	Reboot Devices
Will	be applied to group groupG Reboot device?
-	Ok Cancel

Step 7 Click Ok.

ſ

Adding Multiple Devices to a Group

Follow these steps to add multiple devices to a group:

- **Step 1** Click **Devices** in the left pane.
- **Step 2** In the center pane, double-click the group's icon.

Figure 4-80

4-80 Device and Group lcons in the Center Pane

				**				
BLRGBC0	5JC30124	EN656015030118	IllyDevice	GAPvep2	5malkiosk	DSITestUnit	BLRGBC3	UKDEMOTC
BGL142singlecor	5JC30051	MOBILEDEMO	SN656015030015	ELRGBC2	WMT	GAPvep3	CK030072	BRR-TC
				-				
GAPvep1	Sing1	dgus	BLADCTEST1	prospG				

Step 3 n the Edit menu, click **Properties**.

Figure 4-81 Properties Button in Edit Menu



Three tabs appear in the center pane.

Step 4 Click the **Members** tab to view a list of devices in the group.

General Hambers Follows	
McDevice	

Figure 4-82 Members Tab

- Step 5 Click +.
- **Step 6** In the Add to Group dialog box, check the devices' check boxes.

Figure 4-83 Add to Group Dialog Box

Add To Group	
BLRGBC0	J
GAPvep2	
SJC30124	
SN656015030118	
SmallKiosk	<u></u>
·) + *

Step 7 Scroll to the bottom of the Add to Group dialog box and click Add.



Add To Group	
GAPvep1 Sing1 dgus	Â
Add Cancel	,

The devices appear in the group's member list.

Step 8 Click Apply.

ſ

Step 9 In the Predefined actions menu, click **Reboot**.



Removing Devices from a Group

To remove a device from a group, follow these steps:

- **Step 1** Click **Devices** in the left pane.
- **Step 2** In the center pane, double-click the group's icon.

Figure 4-86

4-86 Device and Group Icons in the Center Pane



Step 3 In the Edit menu, click **Properties**.

Figure 4-87 Properties Button in Edit Menu



Three tabs appear in the center pane.

Step 4 Click the **Members** tab to view a list of devices in the group.

Figure 4-88	Members Tab	
	Central Members Follows	
	MCewor	
	+ ×	

- Step 5 Click a device.
- Step 6 Click X.
- Step 7 Click Apply.

Step 8 In the Predefined actions menu, click Reboot.

Figure 4-89	Reboot Devices Dialog Box
	Reboot Devices
Will I	be applied to group groupG Reboot device?
-	Ok Cancel
Click Ok .	

Setting a Group's Properties

Step 9

Γ

To modify a group's properties, follow these steps:

- Step 1 Click **Devices** in the left pane.
- Step 2 In the center pane, double-click the group's icon.

Figure 4-90		Device and Group Icons in Center Pane						е
ELRGBC0	53C30124	EN656015030118	M/Device	GAPvep2	5malkiesk	DSiTestUnit	BLRGBC3	
BGL 142singlecor	SJC30061	MOBILEDEMO	SN656015030016	BLRGBC2	WMT	GAPvep3	DK030072	BIN-RI-TC
				-				
GAPvep1	Eing1	dgus	BLADCTEST1	proupG				

The device icons within the group are displayed.

Step 3 In the Edit menu, click **Properties**.

Figure 4-91 Properties Button in Edit Menu

	Edit
+	New Group
	Delete
Ø	Properties
ts	Export Account
¥8	Import Account

Three tabs appear in the center pane.

Step 4 Click the **General** tab to modify the group's name and description.

Figure 4-92 General Tab

General Members Policies	
Group Name + groupG	
Adhibition starticture start	
Chirol Chirol	

Step 5 (Optional) Enter a new group name in the **Group Name** field. No spaces or special characters can be used.

- **Step 6** (Optional) Enter a new description in the **Description** field.
- Step 7 Click Apply.
- **Step 8** Click the **Policies** tab to change the group's policy.

52002-00-00-00-00-00-00-00-00-00-00-00-00		and an entry of the	12101011
Available policies		Applied policies	Schedule
Y THLYS	100		
A DUALSCREEN			
THOMSON	100		
E DofA			
ART BART			
CNNandsSNDC			
2 Ošbank-India			
CIS-Try-openURL			
NYCT			
😰 wur			
🗜 HomeDepot			
2 Carrefour			
2 Rotate90			
Retaty90CCW			
RE-DUALSCREEN			
😰 srs			
BGL-GBC-Showcase			
🖢 try-share-desktop			
Restart-COBRA			
RATP			
Rogbet-Audio-Player	1		
SJ-EBC-Demo			
PD176Test			
Rootef			
2 IndonesiaDemo			
IndonesiaGBC			
BRI-CHLINE-BANK			
NoRotation			
t dava			
SIXHSX			
S coltent	U I		

Figure 4-93 Policies Tab

- **Step 9** Click a policy in the Available policies list.
- Step 10 Click the Green Arrow to move the policy from the Available policies list to the Applied policies list.
- Step 11 (Optional) To remove a policy in the Applied policies list, click the Red Arrow.
- Step 12 Click Apply.
- **Step 13** In the Predefined actions menu, click **Reboot**.

Figure 4-94 Reboot Devices Dialog Box



Step 14 Click Ok.

I

Step 15 Click **Cancel** to exit.

1





Configuring Profiles

Revised: January 26, 2014, OL-26458-05

Chapter Overview

I

This chapter explains how to configure profiles.

Profiles apply settings to a single device and the users of that device.

Topics in this chapter include:

- Profiles, page 5-2
 - Accessing a Profile, page 5-2
- Properties, page 5-5
 - Persistent vs. Runtime vs. Persistent Runtime Properties, page 5-5
 - Configuring Application Data, page 5-6
 - Specifying Audio Sources, page 5-8
 - Configuring the Browser, page 5-10
 - Configuring the Startup URL, page 5-19
 - Setting the Clock and Synchronizing NTP Servers, page 5-20
 - Enabling Access to a Cobalt Control Server, page 5-21
 - Adjusting the Display, page 5-22
 - Creating Emergency Messages, page 5-24
 - Enabling Trusted Sites for the Flash Player, page 5-25
 - Enabling the System Settings Hotkeys, page 5-27
 - Specifying Keyboard Parameters, page 5-28
 - Enabling Management Failover, page 5-29
 - Adjusting the Mouse, page 5-31
 - Managing Power Modes, page 5-32
 - Adding and Configuring Network Printers, page 5-33
 - Enabling Profile Expiration, page 5-35
 - Enabling a Proxy Server, page 5-36

- Managing Screen Shots, page 5-37
- Managing User Sessions, page 5-39
- Managing IEC's System Settings Menu, page 5-40
- Collecting System Health Status, page 5-42
- Configuring Remote Logs, page 5-43
- Enabling Services, page 5-44
- Disabling the Watchdog Settings, page 5-46
- Managing System Upgrades, page 5-47
- Adjusting Volume, page 5-48
- Enabling VNC for IECs, page 5-49

<u>P</u> Tip

You must reboot the Cisco IEC4600 Series after adding or modifying any configuration in Cisco IEM for the configuration changes to reflect on the device.

 \mathcal{P} Tip

After you make a change to profiles, click the **Refresh** button at the upper left corner of the screen to view those changes.

Profiles

You could configure a device's profile if you are configuring only one device.

<u>P</u> Tip

If you are configuring multiple devices that have a number of settings in common, it is more efficient to configure a policy and apply it to those devices.

Accessing a Profile

To configure or modify a configuration of a profile, you will first need to access that profile. Follow the steps below to access a device's profile.

Step 1 Click Devices.

	Devices	
F	Users	
►	Policies	
►.	Alerts	
	Schedules	
-1	Accounts	
▶%	Maintenance	

Figure 5-1 Devices Button

Step 2 In the center pane, double-click a device's icon.

Figure 5-2 Device Icons in Center Pane

E			•	C##				C011
BLRGBC0	5JC30124	SN656015030118	MyDevice	GAPvep2	SmalkGosk	DS/TestUnit	BLRGBC3	UKDEMOTC
C11							CTT	
BGL142singlecor	SJC30051	MOBILEDEMO	SN656015030016	BLRGBC2	WMT	GAPvep3	DK030072	BIN-R-TC
677	673	CT1						
G/Pven1	Singt	daus	RLADCTEST1	proupG				

Step 3 Click the **Profile** tab.

Γ

1

	General	Member Of	Profile			
Filter			3			
Property		Compatibility				
application						
audio 🗎						
browser						
Clock						
► 💼 cohttpd						
🕨 🧰 display	•					
emergency						
flashplayer 💼						
hotkeys						
► 💼 keyboard						
▶ 💼 management						
▶ 💼 mouse						
▶						
▶ 💼 printers						
▶ 💼 profile						
▶ 💼 proxy						
► 💼 screenmonitor						
ession						
▶ 💼 settings						
▶ 💼 system						
▶ 💼 upgrade						
▶ 💼 volume						

Figure 5-3 Profile Tab

Properties

A device's profile contains properties that can be configured such as audio, browser, proxy server, session, and VPN.

Enter a keyword in the filter at the top of the screen to find a specific property.

Figure 5-4	Filter	
Filter		0

The properties legend shows the icons that are used to distinguish properties. Click the ? icon at the bottom left of the property screen to view the legend in the Profile tab.





The legend shows the icons used to indicate whether a property has been modified:

- blue dot: This is a value that has been changed from the default setting and saved.
- orange dot: This is a value that has been changed but not saved.
- orange dot with blue circle: This is a child value that has been changed but not saved.

The legend also shows the icons used to indicate whether a property is persistent, runtime, or persistent runtime.

Persistent vs. Runtime vs. Persistent Runtime Properties

There are three different types of properties:

- 1. Persistent: This type of property is permanent when set. Once you modify these properties, you must reboot the IECs. To undo a modification, change the property and reboot, Examples of persistent properties include the application data property, the browser startup url property, and the management failover enabled property.
- 2. Runtime: This type of property is temporary. Use these properties for changes on the fly. The changes will not be saved locally so they will be lost if the IEC is rebooted. You do not need to reboot IECs to apply runtime properties but you may need to restart applications. To undo a runtime property, reboot the IECs. Examples of runtime properties include the browser application restart property, the emergency message property, and the power reboot property.
- **3.** Persistent runtime: This type of property is both permanent and temporary meaning that it can be act like a runtime property by being applied temporarily but then once it has been applied, it is permanent. This type of property is saved locally in the registry. Although you do not need to reboot the IECs to see the persistent runtime properties applied to the IECs, you may not see the changes immediately on the IECs. For example, changes to the display rotation property does not require rebooting. To undo a persistent runtime property, reset properties to default settings and reboot the

I

IECs or create a policy that sets all property settings to their defaults and apply the new policy to the IECs and reboot them. If you created a policy and configured persistent runtime properties in that policy, create another persistent runtime policy that counteracts the property settings and apply the new policy to the IECs and reboot them. Examples of persistent runtime properties include the clock date property, system health frequency property, and volume master muted property.

To view only runtime properties, check the run time properties only checkbox at the top of the page.





Configuring Application Data

The application property is used to configure peripherals that are connected to the IEC such as a magnetic card reader and barcode scanner or configure the SIP client.

- **Step 1** Go to the **Profile** tab of a device.
- **Step 2** Find the **application** property.
- **Step 3** Expand the application property by clicking the **Right Arrow**.

Figure 5-7 Application Property Expanded

Property	Compatibility	Value	Description
application			
🧰 data			Application data

Step 4 Click on the icon within the Value column to open the Application Data Editor dialog box.

ſ



Figure 5-8 Application Data Editor Dialog Box

Step 5 Click the **+** button in the lower left corner of the dialog box.

The values entered in the Application Data Editor dialog box are dependent on what you are trying to configure. The following instructions are for configuring a barcode scanner that is connected to the IEC.

Step 6 In the key field, enter **barcode.scanner**.

	Application data editor	_
barcode.scanner	Honeywell USB Fixed Position Bar Co	de Scanner
+ ×		
	Ok Cancel	(A)

Figure 5-9 Barcode Scanner Entered in the Application Data Editor

Step 7 Enter the name of the barcode scanner recognized by the IEC in the value field. See Appendix D of the *Cisco Interactive Experience Client 4600 Series User Guide* for instructions on how to obtain the name.

Step 8 Click Ok.

Step 9 Click Apply.

Specifying Audio Sources

The audio input and output sources for the Cisco IEC4600 Series can be configured from the Cisco IEM.

Note

The audio mode falls back to 'Analog' when the audio output is configured as 'USB headset' or 'USB speaker' but a USB headset or speaker is not connected to the IEC.

Follow the steps below to specify which sources that the Cisco IEC4600 Series should use.

- **Step 1** Go to the **Profile** tab of a device.
- **Step 2** Find the **audio** property.
- Step 3 To expand the Audio menu, click the Right Arrow.

Figure 5-10 Audio Menu Expanded

🖲 🎕 audio	
► 健 source	

Step 4 Click the **Right Arrow** to expand the Source menu.

You will see the input and output sources. Both of these properties are persistent runtime and can be set on-the-fly.

Step 5 From the audio input drop-down list, choose an input source.

Figure 5-11 Audio Input Drop-Down List



- **Step 6** From the audio output drop-down list, choose an output source. By default, audio output is analog.
- Step 7 Click Apply. If you don't want to make those changes, click Cancel.
- **Step 8** In the Predefined actions menu, click **Reboot**.

Figure 5-12 Reboot Dialog Box



Step 9 In the Reboot Devices Dialog Box, click **Ok**.

I



Configuring the Browser

There are a number of properties that an administrator can configure for the browser. For example, the administrator can manage the logging of browser network activity or set the startup URL.

To configure the browser and startup URL, follow these steps:

Browser Menu

- **Step 1** Go to the **Profile** tab of a device.
- **Step 2** Find the **browser** property.

Figure 5-14

Step 3 Click the **Right Arrow** to expand the browser menu or click **Unfold all** in the upper right corner to expand all menus.

			1 Secondarios
Property	Compatibility	Value	Description
▶ Q about			
► 🔆 audio			
The browser			
➤ Q appearance			
► Capplication			
▶ Q cache			
► @ content			
► 🕃 debug			
► Q input			
► 🛈 navigation			
► @ network.			
► Q print			
► C security			
► Q startup			
► 🛈 storage			
Kille und			URL

Figure 5-15 Unfold All Button



- **Step 4** Click the values within the appearance settings to configure them:
 - To enable the fade in effect:
 - **a.** Choose **appearance** > **effect** > **fadein** > **enabled**.
 - **b.** Check the check box.

I

Figure 5-16 Browser Settings Menu

Property	Compatibility	Value	Description
C trowser			
* Q appearance			1
* Gened			
▼ illtadein			
Chenabled	true		Enable Tade in' effect

The value changes to "true".

- To enable the fade in effect:
 - a. Choose appearance > effect > fadein > enabled.
 - **b.** Check the check box to change the value to "true".
- To modify the frame settings:
 - a. Choose appearance > frame > bottom > width.
 - b. Click the Up Arrow to increase or the Down Arrow to decrease the size of the frame.
 - c. Repeat steps a and b for the top, left, and right frames.

Figure 5-17 Frame Width Settings

Y Gtame		
* GLootom		
General	1 🖉 🖉 🖬	Frame bottom side width
▼ QLieft		
Gwich	0	Frame left side width
▼ GLinght		
Gewidth	0	Frame right side width
▼ QLtop		
i width	0	Frame top side width

- To modify the new window settings:
 - a. Choose appearance > new window > height.
 - b. Click the Up Arrow to increase or the Down Arrow to decrease the size of the new window.
 - c. Repeat steps a and b for the width setting.

Figure 5-18 New Window Settings

Property	Compatibility	Value	Description
* Q newwindow			
Se height		768 🔛 🖂 🥹 🖬	Tener window height in plats
Gewish		1024	New window width in pixels

- To modify the panel settings:
 - a. Choose appearance > panel > navigation > button > back.
 - **b.** Check the check box to enable the back button in the navigational panel of the kiosk.
 - **c.** Repeat steps a and b for the other panel settings: forward, help, home, keyboard, print, reload, stop, enabled, and title.

Property	Compatibility	Value	Description
Y Q panel			
Y Q navigation			
▼ Gt button			
T GL back			
Genetics		🤊 💌 🥥 🗊	
Torward 💭 🐨		R	
Genabled		true	Enable Forward button in the navigation par
▼ Qheb			
Genabled		true	Enable Help' button in the navigation panel
* Q home			
Genabled		true	Enable Home' button in the navigation panel
* Q keyboard			
Genatied		true	Enable Keyboard button in the navigation pa
* G print			
Canabled .		true	Enable Print button in the navigation panel
T Q reload			
Genabled		true	Enable Reload button in the navigation pan
* GL stop			
Genabled		true	Enable 'Stop' button in the navigation panel
dia enabled		faise	Enable navigation panel
* Quite			
Character.		tuine	Emphia title manual

- **Step 5** To modify the spinner, which is the onscreen indicator that shows the browser's progress of loading content:
 - **a**. Check the enabled checkbox to enable the spinner.
 - **b.** Click the green checkmark. The enabled value will appear as "true".
 - c. Enter a number in the timeout field.

Figure 5-20 Spinner Property

V 🙆 spinner		
k enabled	true	Specifies if the browser progress indicator is enabled
ki timeout	-1	Progress indicator timeout in seconds

- **Step 6** To enable or disable restarting the browser:
 - **a**. Choose **application** > **restart**.
 - **b.** Check or uncheck the **restart** check box to enable or disable restarting the browser.

Figure 5-21 Restart Browser Setting

Restant Restant Restant torreser

Step 7 Click the values within the cache settings to configure them:

Figure 5-22 Cache Settings

Property	Compatibility	Value	Description
Gade			
▼ SI maximum			
Capages		3	Maximum number of pages in cach
Y Q meda			
Genabled		true	Enable media cache
Gepath		/data/cache/media	Path to media cache directory
Gastre		2048	Media cache size in megabytes
T Q web			
Genabled		fatee	Enable web cache
Geforce		false	Force browser to use web cache
Gepath		/data/cache/web	Path to web cache directory
Gastre		1024	Web cache aize in megabites

- To set the maximum number of pages to hold in the memory page cache:
 - a. Choose cache > maximum > pages.
 - b. Click the Up Arrow to increase or the Down Arrow to decrease the number of pages.

- To enable the caching of media:
 - a. Choose cache > media > enabled.
 - b. Check or uncheck the enabled check box to enable or disable media caching.
- To enter the path to the media cache directory:
 - **a.** Choose cache > media > path.
 - **b.** Enter the path in the **path** field.
- To choose the media cache size:
 - **a**. Choose cache > media > size.
 - b. Click the Up Arrow to increase or the Down Arrow to decrease the size of the media cache.
- To enable web caching:
 - a. Choose cache > web > enabled.
 - b. Check or uncheck the enabled check box to enable or disable web caching.
- To force the browser to use web caching:
 - **a**. Choose cache > web > force.
 - **b.** Check or uncheck the **force** check box to force or not force the browser to use web caching.
- To enter the path to the web cache directory:
 - a. Choose cache > web > path.
 - **b.** Enter the path in the **path** field.
- To choose the web cache size:
 - a. Choose cache > web > size.
 - b. Click the Up Arrow to increase or the Down Arrow to decrease the size of the web cache.
- **Step 8** click the values within the content settings to configure them:
 - To set the font families used by the browser:
 - a. Choose content > font > family > cursive.
 - **b.** Enter a font in the **cursive** field.
 - c. Repeat steps a and b to set the font families for fantasy, fixed, sansserif, serif, and standard.

Figure 5-23 Font Settings

I

Property	Compatibility	Value	Description
* 🕰 content			
▼ Q fort			
▼ 42 family			
Kill cursive		tahoma	Cursive font family for the browser.
Kantasy		tahoma	Fantacy font family for the browser.
Kinted		monospace	Fixed fort family for the browser,
Ka sansaerf		Arial	Sansserf font family for the browser.
Kaser.		verdana	Serif font family for the browser.
Kastandard		tahoma	Standard fort family for the browser.
* 62, stas			
T Kin default		14	Default font size for the browser.
Kafted		14	Minimum fixed font size for the browser
T Ria minimum		11	Minimum font size for the browser.
Colonical.			Minimum Invited forthing for the hermitia

- To set the font sizes used by the browser:
 - a. Choose content > font > size > default.
 - b. Click the Up Arrow to increase or the Down Arrow to decrease the font size.

- c. Repeat steps a and b to set the minimum font size.
- To enable java applets:
 - a. Choose content > java > enabled.
 - b. Check or uncheck the enabled check box to enable or disable java applets.

Figure 5-24 Java Applet, JavaScript, Plugins, Widgets, and Zoom Settings

Contraction of the second seco	Company.	vare -	Parat strates
▼ @ content			
► GL fort			
* QLjava			
Genabled		true	Enable Java appleta
▼ Q javascript			
Genabled		true	Enable JavaScript
* 🛈 plugins			
Genabled		true	Enable browser plugins
¥ Q widgets			
Genabled		true	Enable browser widgets
* Q zzem			
Gatactor		4	Zoom factor for web pages
▼ Qimages			
* Q antaliasing			
Genabled		True	Zoom web pages with antialiasing

- To enable JavaScript:
 - a. Choose content > javascript > enabled.
 - **b.** Check or uncheck the **enabled** check box to enable or disable JavaScripts.
- To enable browser plugins:
 - a. Choose content > plugins > enabled.
 - b. Check or uncheck the enabled check box to enable or disable browser plugins.
- To enable browser widgets:
 - a. Choose content > widgets > enabled.
 - b. Check or uncheck the enabled check box to enable or disable browser widgets.
- To set the zoom for web pages:
 - a. Choose content > zoom > factor.
 - b. Click the Up Arrow to increase or the Down Arrow to decrease the factor size.
 - c. Choose images > antialiasing > enabled.
 - **d.** Check or uncheck the **enabled** check box to enable or disable antialiasing when zooming web pages.
- **Step 9** To enable or disable the debug panel:
 - a. Choose debug > panel > enabled.
 - **b.** Check or uncheck the **enabled** check box to enable or disable the debug panel.
 - **c.** From the position drop-down list, click **Top** or **Bottom** to choose the position of the debug panel.

Figure 5-25 Debug Settings

Property		Compatibility .		Value		Description
¥ €a debug						
* Q panel						
Genabled			false			Enable debug panel
A position			Dottern		<u>a</u>	Debug panel position
* Q iroit	•		Top	N		
• Q navgation			Bottom	. All		

Step 10 To enable or disable the virtual keyboard and its button:

- a. Choose input > keyboard > button > enabled.
- **b.** Check or uncheck the **enabled** check box to enable or disable the virtual keyboard button.
- c. Choose popup > keyboard > enabled.
- d. Check or uncheck the enabled check box to enable or disable the popup keyboard.

Figure 5-26 Input Settings

Property	Compatibility	Value	Description
▼ @ input			A CONTRACTOR OF
* 🕰 keyboard			
V Six button			
Genatied		true	Enable virtual keyboard button
T C popup			
T 🙀 keyboard			
Cenabled		true	Enable popup keyboard

Step 11 By default, JavaScript error logging is enabled.

a. To disable JavaScript error logging, choose log > javascript> enabled and change the value to false.

Figure 5-27 Browser JavaScript Activity Logging

▼ 💼 log		
▼ 💼 javascript		
i enabled	true	Log browser JavaScript activity
nilter 🔂		👩 🛐 Browser JavaScript activity log filter

- **b.** To filter the JavaScript log files, enter a wildcard in the filter property. Only the log records that match the wildcard will be logged to the IEM.
- **Step 12** By default, browser network activity logging is disabled to reduce the amount of network traffic between the IEC and IEM.
 - **a.** The network mode property can be changed to log all network activity or just network errors to only capture HTTP errors. Choose **log > network > mode** and then the desired logging mode.

Figure 5-28 Browser Network Activity Logging

🔻 💼 network	
filter	Browser network activity log filter
🕅 mode	Network activity log disable Browser network activity logging mode
▶	Network activity log disabled
▶	Log network errors only
▶ ■ network	Log all network activity

- **b.** To filter the browser network log files, enter a wildcard in the **browser log network filter** property. Only the log records that match the wildcard will be logged to the IEM.
- **Step 13** To configure navigation:
 - a. Choose **navigation** > **history** > **enabled**.
 - b. Check or uncheck the enabled check box to enable or disable the browser navigation history.
 - c. Choose **navigation** > **history** > **maximum** > **size**.
 - d. Click the Up Arrow to increase or the Down Arrow to decrease the maximum number of items in the browser navigation history.

- e. Choose **navigation** > scrolling > mode.
- f. From the mode drop-down list, choose the scrolling mode.
- g. Choose **navigation** > scrolling > orientation.
- **h.** From the orientation drop-down list, choose the scrolling orientation.

Figure 5-29 Navigation Settings

Property	Compatibility	Value	Description
▼ C navigation			
* Statistory			
Genabled		faise	Enable history
▼ @ maximum			
dia size		5	Maximum history size
* Cascroling			
samode .		Flicking	Scrolling mode
The and and the set		0.0	Provide a constant of

Step 14 To configure the network:

- a. Choose network > failover > enabled.
- b. Check or uncheck the enabled check box to enable or disable the network failover algorithm.
- c. Choose network > failover > recovery > interval.
- **d.** Click the **Up Arrow** to increase or the **Down Arrow** to decrease the period of time in failover mode when the browser tries to open an initial URL.
- e. Choose **network** > **failover** > **recovery** > **url**.
- f. Enter an address in the url field that will be used if the browser cannot open some URL.
- g. Choose **network** > **timeout**.
- **h.** Click the **Up Arrow** to increase or the **Down Arrow** to decrease the network operations timeout.
- i. Choose network > timeout > enabled.
- j. Check or uncheck the enabled check box to enable or disable timeout.

Figure 5-30 Network Settings

Property	Compatibility	Value	Description
* C network			
* GLtatover			
Cenabled		talse	Enable network failover
▼ GL recovery			
Ginterval		15	Network failover recovery interval in seconds
Gut			Network failover URL
* Gatmeout		60	Network timeout
Genabled		tue	Enable network \$meout

Step 15 To enable or disable printing of background colors and images:

- a. Choose print > elementbackgrounds > enabled.
- **b.** Check or uncheck the **enabled** check box to enable or disable the printing of background colors and images.

Figure 5-31 Print Background Colors and Images Setting

Property	Compatibility	Value	Description
▼ Sk print	5 C		
 Q elementbackgrounds 			
Genabled	true		Print element backgrounds

- **Step 16** To configure security settings:
 - a. Choose security > certificates > selfsigned > enabled.
- **b.** Check or uncheck the **enabled** check box to enable or disable the accepting of self-signed certificates.
- c. Choose security > localtoremote > enabled.
- **d.** Check or uncheck the **enabled** check box to specify whether locally loaded documents are allowed to access remote URLs.
- e. Choose security > newwindow > modal > max.
- f. Click the Up Arrow to increase or the Down Arrow to decrease the maximum number of modal windows.
- g. Choose security > newwindow > mode.
- h. From the mode drop-down list, choose the new windows opening mode.
- i. Choose security > remotetolocal > enabled.
- j. Check or uncheck the **enabled** check box to specify whether remotely loaded documents are allowed to access local files.

Figure 5-32 Security Settings

Property	Compatibility	Value	Description
* Sit security			
* Q certificates			
V ilk selfsigned			
Genabled		tue	Accept selfsigned certificates
▼ QLiocaltoremote			
Genabled		true	Allow local content to access remote URLs
▼ si newwindow			
V Q modal			
G max		1	Maximum number of modal windows
Grode		in the same 💦 😒 🥝 🚹	New windows opening mode
▼ @ remotetolocal		Disabled	
Genabled		e in the same	Allow remote content to access local files.
► Castanup		Modal	

Step 17 To configure the startup URLI:

- a. Choose startup > about > timeout.
- **b.** Click the **Up Arrow** to increase or the **Down Arrow** to decrease the length of page timeout in seconds.
- **c.** Choose **startup** > **url**.
- d. Enter the address of the startup url in the **url** field.

Figure 5-33 Startup URL Settings

Property		Compatibility	Value	Description
▼ 🕃 startup				
Tuode 💭 🔻				
Getmeout			10	About page timeout in seconds
Church	1.0		http://contant.work_com/contant/CODDA/startpapa/aday.html	Status LIDI

Step 18 To configure storage:

- a. Choose storage > enabled.
- **b.** Check or uncheck the **enabled** check box to specify whether local storage is enabled.
- c. Choose storage > html5 > appcache > enabled.
- **d.** Check or uncheck the **enabled** check box to specify whether support for the HTM5 web application cache feature is enabled
- e. Choose storage > html5 > database > enabled.
- f. Check or uncheck the **enabled** check box to specify whether support for the HTM5 offline storage feature is enabled

- g. Choose storage > html5 > enabled.
- **h.** Check or uncheck the **enabled** check box to specify whether support for the HTM5 local storage feature is enabled

Figure 5-34 Storage Settings

Property	Compatibility	Value	Description
¥ 🕰 storage			
Genatied		tue	Enable local storage
* GLIMMES			
▼ iQ appcache			
Genabled		false	Enable HTML 5 web applications cache
* 🕰 database			
anabled .		taise	Enable HTML 5 offline storage
Genabled		fatow	Enable HTML 5 local storage

Step 19 To set a web page, enter an address in the **url** field.

Figure 5-35	URL	URL Setting			
Property		Compatibility	Value	Description	
Kaut		www	cisco.com	UBL	

- Step 20 Click Apply. Or if you don't want to keep all the settings, click Cancel.
- **Step 21** In the Predefined actions menu, click **Reboot**.

Figure 5-36 Reboot Dialog Box



Step 22 In the Reboot Devices Dialog Box, click **Ok**.



Reboot Device	
Will be applied to device SJC30124 Reboot device?	
Ok Cancel	

Configuring the Startup URL

The startup URL is the website content that displays on the kiosk. To modify the startup URL, follow these steps:

Step 1 Go to the **startup** property within the **browser** property.

Step 2 Click the **Right Arrow** to expand the startup property.

Figure 5-38 Startup URL Settings

🕼 startup			
🕨 🎕 about			
🚰 url	•	http://content.veptc.com/content/development/NYCT-SIP/SIP/index.ht	Startup URL
Step 3	Enter the addre	ss of the startup url in the url field.	
Step 4	Click Apply.		
Step 4 Step 5	Click Apply . In the Predefine	ed actions menu, click Reboot .	



ſ

Step 6 In the Reboot Devices Dialog Box, click **Ok**.



Setting the Clock and Synchronizing NTP Servers

The clock on a Cisco IEC4600 Series can be manually set or synchronized using NTP from the Cisco IEM. Follow the steps below to modify the clock's settings.

- **Step 1** Go to the **Profile** tab of a device.
- **Step 2** Click the **Right Arrow** to expand the clock menu.

Figure 5-41 Clock Menu

Property	Compatibility	Value	Description
7 € dock			
Ka date		Mon Dec 12 2011	Date
* Kilentp		true	Enable NTP
Ka sever1		0 pool.ntp. org	First NTP server
Kasever2		1 pool ntp.org	Second NTP server
Kin server3		2 pool ntp.org	Third NTP server
Kätme		0.0.0	Time
- Bankatore		Americañiew_York 🔻 🖌 🖌	Time zone
Ca automatic	4	tr AmericaNassau	Use automatic time zone
a control		America/New,York	
G display		AmericaNipigon	
0.dmm		AmericaNome	
Canada and a second and a secon		AmericaNoronha	

- **Step 3** In the date value, click a date in the calendar.
- **Step 4** Check or uncheck the **enabled** check box to enable or disable the synchronization of date and time using NTP.
- **Step 5** Click the **Right Arrow** to expand the NTP menu.
- **Step 6** Enter the address of the first NTP server to be synchronized in the server1 field.
- **Step 7** (Optional) Enter the address of the second NTP server to be synchronized in the server2 field.
- **Step 8** (Optional) Enter the address of third NTP server to be synchronized in the server3 field.
- **Step 9** Enter values for the hour, minute, and second using a 24 hour clock.
- **Step 10** From the timezone drop-down list, choose a city in your time zone.
- **Step 11** Check or uncheck the **enabled** check box to enable or disable the automatic determination of the time zone.
- Step 12 Click Apply. If you don't want to make those changes, click Cancel.
- Step 13 In the Predefined actions menu, click Reboot.

	Edit		
Predefined actions			
ø	Message		
	Open URL		
*	Reboot		
٢	Display On/Off		
K	Mute		
Ø	Upgrade		
Q	Restart Application		

Reboot Dialog Box

Figure 5-42

Step 14 In the Reboot Devices Dialog Box, click **Ok**.



Enabling Access to a Cobalt Control Server

External access to a Cobalt Control Server can be managed with Cisco IEM. Follow the steps below to manage such access.

Step 1 Go to the **Profile** tab of a device.

I

- **Step 2** Click the **Right Arrow** to expand the cohttpd menu.
- **Step 3** Click the **Right Arrow** to expand the access menu.
- **Step 4** Click the **Right Arrow** to expand the external menu.
- **Step 5** Check or uncheck the **enabled** check box to enable or disable external access to the Cobalt Control Server. If the value is false, the server can only be accessed from within the device.
- **Step 6** From the mode drop-down list, choose an operational mode.



- Step 7 Click Apply. If you don't want to make those changes, click Cancel.
- **Step 8** In the Predefined actions menu, click **Reboot**.



Step 9 In the Reboot Devices Dialog Box, click **Ok**.



Adjusting the Display

The video displays connected to IECs can be managed remotely thru the Cisco IEM. Follow the steps below to manage their video displays.

Step 1 Go to the **Profile** tab of a device.

Step 2 Click the **Right Arrow** to expand the display settings.

ſ

Property	Compatibility	Value	Description
🛍 display			
* Cabrightness		0	Display brightness
Kie enabled		faise	Enable brightness adjustment
* Kacontrast		0	Display contrast
Renabled		false	Enable contrast adjustment
Camaster		HDMI master	Master display, VGA or HDMI
Y @ resolution			
Camode .		Preferred screen resolution	Maximum or preferred screen resolution
Reretation		None	Display rotation

- **Step 3** Click the **Up Arrow** or the **Down Arrow** to set the level of brightness on the display.
- **Step 4** Click the **Right Arrow** to expand the brightness menu.
- **Step 5** Check or uncheck the **enabled** check box to enable or disable brightness adjustment.
- Step 6 Click the Up Arrow or the Down Arrow to set the level of contrast on the display.
- **Step 7** Click the **Right Arrow** to expand the contrast menu.
- Step 8 Check or uncheck the enabled check box to enable or disable contrast adjustment.
- Step 9 From the master drop-down list, choose the master display input.
- **Step 10** Click the **Right Arrow** to expand the resolution menu.
- **Step 11** From the mode drop-down list, choose the screen resolution.
- **Step 12** From the rotation drop-down list, choose the display rotation.

Figure 5-48 Rotation Drop-Down List

Property		Compatibility	Value	Description
Y 🕰 deplay	•			
V Ka brightness			0	Display brightness
Kin enabled			false	Enable brightness adjustment
V Ka contrast			0	Display contrast
Renabled			false	Enable contrast adjustment
Si master			HCMI master	Master display, VGA or HOM
V Q resolution				
Carnode	•		Preferred screen resolution	Maximum or preferred screen resolution
Service on the service of the servic			None 💌 🐼 🙆 🖬	Display rotation
▶ 🕃 dmm			Note	
➤ QL fashplayer			90 deg clockwise	
► @ hotieys			90 deg. counter clockwis	
P 17 hashand			180 deg.	

- Step 13 Click Apply. If you don't want to make those changes, click Cancel.
- **Step 14** In the Predefined actions menu, click **Reboot**.

Figure	e 5-49	Rebo	oot Dia	log Box
	Edit			
Pr	edefined actio	ns		
ø				
URL	Open URL			
*				
U	Display On/Off			
*	Mute			
Ø	Upgrade			
Q	Restart Applica			

Step 15 In the Reboot Devices Dialog Box, click **Ok**.



Creating Emergency Messages

Emergency messages can be displayed across the Cisco IEC4600 Series video displays.

Step 1	Go to the Profile tab of a device.						
Step 2	Click the Right Arrow to expand the emergency message settings.						
	Figure 5-51 Emergency Message Settings						
	🔻 🎕 emergency						
	🛍 message				Emergency message		
Step 3	Enter text in t	he message field	l.				
Step 4	Click Apply.						
Step 5	In the Predefined actions menu, click Reboot .						

Figure	5-52	Reboot Dialog Box
	Edit	
Pre	defined action	5
ø	Message	
URL	Open URL	
*	Reboot	
U	Display On/Off	
K	Mute	
Ø	Upgrade	
Q	Restart Applicati	on

Figure 5-52

Step 6 In the Reboot Devices Dialog Box, click Ok.



Enabling Trusted Sites for the Flash Player

I

A list of trusted websites can be added so as to allow full access to web cameras, URLs, or IP addresses. To populate this list, follow these steps:

ep 1	Go to the Profile tab of a device.					
ep 2	Click the Righ	Click the Right Arrow to expand the Flash player settings.				
	Figure 5-54	Flash Player	Settings			
	Property	Compatibility	Value	Description		
	▼ Q Rashplayer					
	* Q security					
	* Q hardware		1.000			
	 O holizys 			Lot of who sees to invade for access to web Ephinis, UNLS of P 203(#534%		
3 4	Click the Righ Click the Righ	t Arrow to expa t Arrow to expa	and the sec and the ha	curity menu. rdware menu.		
ep 5	In the trusteds	tes value, click	the button			

- **Step 6** In the List of web sites dialog box, click +.
 - Figure 5-55 List of Web Sites Dialog Box



- **Step 7** Enter an address in the **new string** field.
- **Step 8** After all the addresses have been added, click **Ok**.
- Step 9 Click Apply. If you don't want to make those changes, click Cancel.
- **Step 10** In the Predefined actions menu, click **Reboot**.

Figure 5-56 Reboot Dialog Box

Edit			
Pr	edefined actions		
ø			
URL	Open URL		
*	Reboot		
U	Display On/Off		
	Mute		
Ø	Upgrade		
Q	Restart Application		

Step 11 In the Reboot Devices Dialog Box, click **Ok**.



Enabling the System Settings Hotkeys

To access the System Settings panel on the IEC, its hotkeys must be enabled. The hotkeys are enabled by default. If you want to disable the hotkeys or change the keys, follow these steps:

- **Step 1** Go to the **Policy** tab of a policy:
- **Step 2** Go to the **hotkeys** property.
- **Step 3** Click the **Right Arrow** to expand the property.

Figure 5-58 Hotkeys Property Expanded

▼ 🗎 hotkeys		
🔻 🦚 settings	Ctrl + Alt + S	Open system settings
ka enabled	true	Enable hotkey to open system settings

- **Step 4** To change the hotkeys, enter the new key combination in the settings field.
- **Step 5** To disable the hotkeys, change the enabled field to **false**.
- Step 6 Click Apply.

I

Step 7 In the Predefined actions menu, click **Reboot**.

Figure	5-59	Rebo	oot Di	alog	Вох
	Edit				
Pre	defined action	ıs			
ø					
URL	Open URL				
*					
U	Display On/Off				
*	Mute				
Ø	Upgrade				
Q	Restart Applicat				

Step 8 In the Reboot Devices Dialog Box, click **Ok**.



Specifying Keyboard Parameters

Keyboards used with the IECs can be managed remotely. To adjust keyboard parameters, follow the steps below.

- **Step 1** Go to the **Profile** tab of a device.
- **Step 2** Click the **Right Arrow** to expand the keyboard settings.

Figure 5-61	Keyboard Settings
-------------	-------------------

Property	Compatibility	Value		Description
▼ 🤹 teyboard				
V Chardware				
V Stautorepeat				
Kile delay		400	Autorepeat delay	
Kikenabled		true	Enable keyboard autorepeat	
Karate		35	Autorepeat rate	
* Q Layouts				
(Caralanie		C	Keyboard layouts	
▼ Q vitual		W.		
Exenabled		faise	Enable virtual keyboard	

Step 3 Click the **Right Arrow** to expand the hardware menu.

- **Step 4** Click the **Right Arrow** to expand the autorepeat menu.
- **Step 5** In the delay setting field, choose the keyboard autorepeat delay value in milliseconds.
- **Step 6** Check or uncheck the **enabled** check box to enable or disable keyboard autorepeat.
- **Step 7** In the rate field, choose the keyboard autorepeat rate value in symbols per second.
- **Step 8** Click the **Right Arrow** to expand the virtual menu.
- **Step 9** Check or uncheck the **enabled** check box to enable or disable the virtual keyboard.
- Step 10 Click Apply. If you don't want to make those changes, click Cancel.
- **Step 11** In the Predefined actions menu, click **Reboot**.

Figure 5-62 Reboot Dialog Box



Step 12 In the Reboot Devices Dialog Box, click **Ok**.



Enabling Management Failover

I

Management failover is enabled by default. To change the setting, follow these steps:

Step 1 Go to the **Profile** tab of a device.

- **Step 2** Choose the **management** property.
- **Step 3** Click the **Right Arrow** to expand the property settings.

Figure 5-64 Management Property

Compatibility	Value	Description
	true	Enable management failover
	Compatibility	Compatibility Value

Step 4 To enable or disable management failover, change the enabled setting.

Reboot Dialog Box

Step 5 Click Apply.

Figure 5-65

Step 6 In the Predefined actions menu, click **Reboot**.

Edit			
Pre	defined actions		
ø	Message		
URL	Open URL		
**	Reboot		
U	Display On/Off		
	Mute		
Ø	Upgrade		
Q	Restart Application		

Step 7 In the Reboot Devices Dialog Box, click **Ok**.

	Figure 5-66	Reboot Devices Dialog Box
		Reboot Device
	Will be	applied to device SJC30124 Reboot device?
	-	Ok Cancel
Step 8	Click Cancel.	

Adjusting the Mouse

The settings for a mouse connected to a Cisco IEC4600 Series can be managed remotely.



The default value of the mouse.cursor.visible property has changed to 'Hide mouse cursor' from "Show mouse cursor" starting with release 2.1.1.

To adjust the settings, follow these steps:

- **Step 1** Go to the **Profile** tab of a device.
- **Step 2** Click the **Right Arrow** to expand the mouse settings.

Figure 5	5-67	Mouse	Settings
----------	------	-------	----------

Property	Compatibility	Value	Description
* Qimouse			
Reacceleration		2	Nouse acceleration
T Cacursor			
Gevisible		Show mouse carsor only when mouse is contected	Show mouse cursor
Kahand		Right	Mouse hand
Treshold		4	Nouse threshold to start drapping

- **Step 3** In the acceleration field, choose the mouse acceleration speed value.
- Step 4 From the visible drop-down list, choose whether the mouse cursor should be visible on the kiosk display.
- **Step 5** From the hand drop-down list, choose whether the mouse should be configured to accommodate right-handed or left-handed users.
- **Step 6** In the threshold field, choose the mouse threshold to start dragging value.
- **Step 7** Click **Apply**. If you don't want to make those changes, click **Cancel**.
- **Step 8** In the Predefined actions menu, click **Reboot**.

Figure 5-68	Reboot Dialog Box

Edit		
Pr	edefined actions	
ø	Message	
URL	Open URL	
*	Reboot	
U	Display On/Off	
*	Mute	
Ø	Upgrade	
Q	Restart Application	

ſ

Step 9 In the Reboot Devices Dialog Box, click **Ok**.



Managing Power Modes

The Cisco IEC4600 Series can be powered off or rebooted remotely. The video display can also be placed in standby mode. To enable these power modes, follow the steps below.

- **Step 1** Go to the **Profile** tab of a device.
- **Step 2** Click the **Right Arrow** to expand the power settings.

Figure 5-	-70	Power	Settings
-----------	-----	-------	----------

Property	Competibility	Value	Description
* Q power			
* Q daptay			
Kastanday		tute	Put connected display to standby mode
* Guing			
Kamode		Stand by	Topple the special 'Power off' bullon mude
Geowent		failse .	Turn of the device
Garabect		tative	Rebot the device

- **Step 3** Check or uncheck the **standby** check box to put the connected display to standby mode.
- Step 4 From the mode drop-down list, choose whether the power button will toggle to stand by or power off.
- **Step 5** Check or uncheck the **poweroff** check box to turn off the device.
- Step 6 Check or uncheck the reboot check box to put the connected display to standby mode.
- Step 7 Click Apply.
- **Step 8** In the Predefined actions menu, click **Reboot**.

-	Edit
Pr	edefined actions
ø	Message
URL alba	Open URL
21/2 27/2	Reboot
٢	Display On/Off
	Mute
9	Upgrade
Q	Restart Application

Figure 5-71 Reboot Dialog Box

Step 9 In the Reboot Devices Dialog Box, click **Ok**.

Figure 5-72 Reboot Devices Dialog Box



Adding and Configuring Network Printers

To configure network printers, follow these steps:

- **Step 1** Go to the **Policy** tab of a policy:
- **Step 2** Go to the **printers** property.
- **Step 3** Click the **Right Arrow** to expand the property.

₹ É	🗃 printers		
	Configurations		Printers configurations

Step 4 Click + to add a printer.

I

- **Step 5** In the Printers configuration editor, click on the printer you just added.
- **Step 6** Enter the IP address of the printer.

Printers co	onfigurations editor
Printer0 IP Address Printer Name Queue t	 Printer0 print Network Enabled or Linux Printer Windows Shared Printer
ОК	Cancel

Figure 5-74 Printer Configuration Editor

- **Step 7** Change the name of the printer if desired.
- **Step 8** Enter the printer's queue.
- Step 9 Choose either the Network Enabled or Linux Printer or Windows Shared Printer radio button.
- Step 10 Click Ok.
- **Step 11** In the Predefined actions menu, click **Reboot**.

Figure 5-75 Reboot Dialog Box



Step 12 In the Reboot Devices Dialog Box, click **Ok**.

Figure 5-76	Reboot Devices Dialog Box			
	Reboot Device			
Will be	applied to device SJC30124 Reboot device?			
-	Ok Cancel			
Click Cancel.				

Enabling Profile Expiration

Step 13

By default, the profile expiration is set to false. To change this setting, follow these steps:

Step 1	Go to th	e Policy	tab of	a policy:
--------	----------	----------	--------	-----------

- **Step 2** Go to the **profile** property.
- **Step 3** Click the **Right Arrow** to expand the property.

Figure 5-77 Profile Property

Property	Compatibility	Value	Description
🕶 🧰 profile			
🔻 💼 expiration			
i enabled	fals	e	Enable profile expiration support

- **Step 4** To enable this property, check the check box in the Value column.
- **Step 5** Click the green checkmark.
- Step 6 Click Apply.

I

Step 7 In the Predefined actions menu, click **Reboot**.

Figure	9 5-78	Reboot Dialog Box
	Edit	
Pr	edefined actio	ns
ø		
URL	Open URL	
*		
U	Display On/Off	
	Mute	
Ø	Upgrade	
Q	Restart Applica	ition

Step 8 In the Reboot Devices Dialog Box, click **Ok**.

Figure 5-79 Reboot Devices Dialog Box



Enabling a Proxy Server

A proxy server can be enabled, Follow the steps below to enable a proxy server.

- **Step 1** Go to the **Profile** tab of a device.
- **Step 2** Click the **Right Arrow** to expand the proxy settings.

Figure 5-80 Proxy Settings

Property	Compatibility	Value		Description
St provy				
Genabled		faise	Enable proxy	
Chost			Proxy host name	
apssword			Proxy password	
Capot		0	Proxy port	
Catype		Disabled	Prosy type	
Gunn			Provi user name	

- **Step 3** Check or uncheck the **enabled** check box to enable or disable the network proxy.
- **Step 4** If the proxy is enabled, enter the proxy host name in the **host** field.
- **Step 5** Enter the password in the **password** field.
- **Step 6** In the port field, choose the port number of the proxy server.

- **Step 7** From the type drop-down list, choose the network proxy server type.
- Step 8 Click Apply. If you don't want to make those changes, click Cancel.
- **Step 9** In the Predefined actions menu, click **Reboot**.

Figure 5-81	Reboot Dialog Box
-------------	-------------------

	Edit	
Predefined actions		
ø	Message	
URL allin	Open URL	
21/2 7/2	Reboot	
٢	Display On/Off	
*	Mute	
Q	Upgrade	
Q	Restart Application	

Step 10 In the Reboot Devices Dialog Box, click **Ok**.

Figure 5-82	Reboot Devices Dialog Box
	Reboot Device
Will be	applied to device SJC30124 Reboot device?
-	Ok Cancel

Managing Screen Shots

ſ

Screen shots of the kiosk's video display can be managed remotely. Follow the steps below to adjust the screen shot settings.

- **Step 1** Go to the **Profile** tab of a device.
- **Step 2** Click the **Right Arrow** to expand the screen monitor settings.

Figure 5-83	Screen	Monitor	Settings
-------------	--------	---------	----------

Property	Compatibility	Value	Descripti
• Q screenmonitor			
Genabled		true	Enable screenshots
Chinterval		10 minutes	Interval
▼ @screenshot			
Cheight		640	Screenshot height
Gwidth		640	Screenshot width
V Sathumonail			
Caheight.		128	Thumbnail height
Cawlotts		128	Thumbrail width
Kaupdate		faise	Lindale screenshot

- **Step 3** Check or uncheck the **enabled** check box to enable or disable screenshots.
- **Step 4** From the interval drop-down list, choose the time interval between two screenshots.
- **Step 5** In the screenshot height field, choose the height of the screenshot in pixels.
- **Step 6** In the screenshot width field, choose the width of the screenshot in pixels.
- **Step 7** In the thumbnail height field, choose the height of the thumbnail in pixels.
- **Step 8** In the thumbnail width field, choose the width of the thumbnail in pixels.
- Step 9 Check or uncheck the update check box to trigger immediate updates of screenshots.
- Step 10 Click Apply. If you don't want to make those changes, click Cancel.
- **Step 11** In the Predefined actions menu, click **Reboot**.





Step 12 In the Reboot Devices Dialog Box, click **Ok**.

Figure 5-85 Reboot Devices Dialog Box

ACU be see list day	4	
will be applied to	device SJC30124	
Reboot	t device?	
OK	Cancal	
UK	Cancer	

I

Managing User Sessions

User sessions can be managed remotely. User sessions can be limited to a number of seconds or locked altogether. Users can be forced to log out after their session. To manage user sessions, follow the steps below.

Step 1 Go to the **Profile** tab of a device.

Figure 5-86

Step 2 Click the **Right Arrow** to expand the session settings.

Session Settings

Property	Compatibility	Value		Description
a screenmonitor				
Quession .				
Ala locked		fatse	Session locked	
V Calocking				
Kaenabled		tue	Enable session lock	
* Ala logout		false	Force user to log out	
Ka enabled		true	Enable logout	
TATImeout		0	Session Smeout in seconds	
Ka enabled		taise	Enable session timeout	
T 🕰 unlocking				
Ka enabled		tue	Enable pession unlock	

- **Step 3** Check or uncheck the **locked** check box to lock or unlock current user session.
- **Step 4** Click the **Right Arrow** to expand the locking menu.
- **Step 5** Check or uncheck the **enabled** check box to enable or disable session locking ability.
- **Step 6** Click the **Right Arrow** to expand the logout menu.
- **Step 7** Check or uncheck the **logout** check box to specify whether user should be forced to log out.
- Step 8 Check or uncheck the enabled check box to enable or disable logging out ability for the user.
- **Step 9** In the timeout field, choose the session timeout in seconds.
- **Step 10** Click the **Right Arrow** to expand the timeout menu.
- **Step 11** Check or uncheck the **enabled** check box to enable or disable auto logout after the number of seconds set in the timeout field above.
- **Step 12** Click the **Right Arrow** to expand the unlocking menu.
- **Step 13** Check or uncheck the **enabled** check box to enable or disable session unlocking ability.
- Step 14 Click Apply. If you don't want to make those changes, click Cancel.
- **Step 15** In the Predefined actions menu, click **Reboot**.

Figure	9 5-87	Rebo	oot Di	alog Bo	ЭX
	Edit				
Pro	edefined actio	ons			
ø					
	Open URL				
*					
U	Display On/Off				
*	Mute				
۲	Upgrade				
Q	Restart Applic	ation			

Step 16 In the Reboot Devices Dialog Box, click Ok.



Managing IEC's System Settings Menu

You can control which icons are displayed in the IEC's System Settings menu. By default, all the icons are enabled so that they show in the menu. To disable any of the icons, follow these steps:

- **Step 1** Go to the **Policy** tab of a policy:
- **Step 2** Go to the **settings** property.
- **Step 3** Click the **Right Arrow** to expand the property.

Property	Compatibility	Value	Description
🕶 💼 settings			
🔻 🧰 audio			
i enabled		true	Enable audio settings
🔻 🛅 calibrator			
i enabled		true	Enable calibrator settings
🕈 💼 clock			
🕋 enabled		true	Enable clock settings
🔻 🧰 display			
i 🖓 enabled		true	Enable display settings
🔻 💼 keyboard			
i 🕋 enabled		true	Enable keyboard settings
🔻 🧰 kiosk			
i 🖓 enabled		true	Enable kiosk settings
🔻 💼 mouse			
i 🕋 enabled		true	Enable mouse settings
🔻 🧰 network			
i enabled		true	Enable network settings
🔻 💼 proxy			
i 🕋 enabled		true	Enable proxy settings
▼ 💼 reboot			
i enabled		true	Enable reboot
🔻 🛅 syslog			
i enabled		true	Enable event viewer

Figure 5-89 Settings Property

- **Step 4** Choose the System Setting's icon that you want to disable.
- **Step 5** Change the value from 'true' to 'false'.
- Step 6 Click Apply.

Γ

Step 7 In the Predefined actions menu, click **Reboot**.

Figure 5-90 Reboot Dialog Box

	Edit		
Pr	edefined actions		
ø	Message		
	Open URL		
	Reboot		
٢	Display On/Off		
*	Mute		
Ø	Upgrade		
Q	Restart Application		

Step 8 In the Reboot Devices Dialog Box, click **Ok**.

Reboot Devices Dialog Box
eboot Device
ied to device SJC30124 eboot device?
Cancel

Collecting System Health Status

The system's health status can be collected. Follow the steps below to set the frequency and period of their collection.

- **Step 1** Go to the **Profile** tab of a device.
- **Step 2** Click the **Right Arrow** to expand the system settings.

Figure	5-92	System	Settinas
Iguie	J-32	Jystem	Settings

* 🕰 system		
▼ Q heath		
Kate quency	15	Number of times to collect system health status during period
Caperiod .	300	Period to collect system health status
T Q service		
Y Ka bluetooth		
Ka enabled	true	Enable bluetooth service
* GL10		
Kienabled	true	Enable FTP service
* Qash		
Ris enabled	tue	Enable SSH service

- **Step 3** In the frequency field, choose the number of times that system health status will be collected during the period set next.
- **Step 4** In the period field, choose the period in seconds to collect system health status.
- Step 5 Click Apply.
- **Step 6** In the Predefined actions menu, click **Reboot**.

Figure 5-93	Reboot Dialog Box
Edit	
Predefined act	ions
🙍 Message	
URL Open URL	
Reboot	
Display On/O	ff
Mute	
👩 Upgrade	
Restart Appli	cation

Step 7 In the Reboot Devices Dialog Box, click **Ok**.



Configuring Remote Logs

If you want to have the logging information sent to a remote server, follow these steps.

- **Step 1** Go to the system property.
- **Step 2** Expand the system property and the logging property.

Figure 5-95	Logging Properties			
🔻 ն system				
► 🙆 health				
V 🗟 logging				
🔻 🙉 remote				
kîn (p		Remote IP address to send logs to using RELP protoc		
Kin port	0	Remote port to send logs to using RELP protocol		

- Step 3 Enter the IP address of the remote server where the logs should be sent in the ip field.
- **Step 4** Enter the port number for the remote server in the port field.
- Step 5 Click Apply.

ſ

Step 6 In the Predefined actions menu, click **Reboot**.



Step 7 In the Reboot Devices Dialog Box, click **Ok**.



Enabling Services

Bluetooth, FTP, and SSH services can be enabled when you follow the steps below.

	Step 1	Go to	the	Profile	tab	of a	device.
--	--------	-------	-----	---------	-----	------	---------

Step 2 Click the **Right Arrow** to expand the system settings.

▼ @ system		
▼ Q heath		
Katequency	15	Number of times to collect system health status during period
Caperiod .	300	Period to collect system health status
* Q service		
▼ Ka bluetooth		
Ra enabled	true	Enable bluelooth service
T GLTD		
Kie enabled	true	Enable FTP service
▼ Q sah		
Ra enabled	true	Enable SSH service

ſ

- **Step 3** Click the **Right Arrow** to expand the service menu.
- **Step 4** Click the **Right Arrow** to expand the bluetooth menu.
- **Step 5** Check the **enabled** check box to enable bluetooth service.
- **Step 6** Click the **Right Arrow** to expand the FTP menu.
- **Step 7** Check the **enabled** check box to enable FTP service.
- **Step 8** Click the **Right Arrow** to expand the SSH menu.
- **Step 9** Check the **enabled** check box to enable SSH service.
- Step 10 Click Apply. If you don't want to make those changes, click Cancel.
- **Step 11** In the Predefined actions menu, click **Reboot**.

Figure 5-99 Reboot Dialog Box



Step 12 In the Reboot Devices Dialog Box, click **Ok**.



Disabling the Watchdog Settings

Watchdogs are enabled by default. There are three types of watchdog properties in the IEM:

- **1.** System: This watchdog watches the system for responsiveness. If a process stops, the watchdog considers the system to be hung and reboots it.
- 2. XWindows: This watchdog watches whether the Windows system is alive and running. This watchdog's settings can be disabled.
- **3.** Browser: This watchdog watches the browser for responsiveness. The watchdog tries to detect whether the browser is frozen.

Watchdogs can be added to applications when designing them to monitor their performance.

If you want to disable them, follow these steps.

- **Step 1** Go to the system property.
- **Step 2** Expand the system property and the watchdog property.

Figure 5-101 Logging Properties

🔻 🎕 watchdog		
▼ @xwindows	true	Watch for window system is alive
down	true	Watch for window system is running

- **Step 3** Uncheck the xwindows value checkbox to disable watching whether the Windows system is alive. The value will change to "false".
- **Step 4** Uncheck the down value checkbox to disable watching whether the window system is running. The value will change to "false".
- Step 5 Click Apply.
- **Step 6** In the Predefined actions menu, click **Reboot**.

Figure 5-102 Reboot Dialog Box

Edit			
Pr	edefined actions		
ø	Message		
	Open URL		
214	Reboot		
0	Display On/Off		
ĸ	Mute		
0	Upgrade		
	Restart Application		
Q	Restan Application		

Step 7 In the Reboot Devices Dialog Box, click **Ok**.

Figure 5-103	Reboot Devices Dialog Box
	Reboot Device
Will be	applied to device SJC30124
	Reboot device?
	Cancel

Managing System Upgrades

A system upgrade can be managed remotely. Follow the steps below to manage a system upgrade.

- **Step 1** Go to the **Profile** tab of a device.
- **Step 2** Click the **Right Arrow** to expand the upgrade settings.

Figure 5-104	Upgrade Settings		
¥ Q upgrade			
Command	Stop system upgrade if possible	Start upgrade	
Ka enabled	true	Enable upgrade for user	
- Expush	5	Start upgrade to a specifie diversion	
V Ca volume	4		

- Step 3 To start or stop the system upgrade, choose an action form the command drop-down list.
- **Step 4** Check or uncheck the **enabled** check box to enable or disable device firmware upgrade for the user.
- Step 5 Click Apply. If you don't want to make those changes, click Cancel.
- **Step 6** In the Predefined actions menu, click **Reboot**.



I

Figure 5-105 Reboot Dialog Box

Step 7 In the Reboot Devices Dialog Box, click **Ok**.



Adjusting Volume

The volume of the kiosks can be controlled remotely. Follow the steps below to set the volume of the kiosks.

- **Step 1** Go to the **Profile** tab of a device.
- **Step 2** Click the **Right Arrow** to expand the volume settings.

Figure 5-107 Volume Settings

 sa volume 	•		
* imaster •		75	Master channel volume
Ka enabled		faise	Enable master channel settings
i muted		Talse	Master channel muted
* All microphone		75	Microphone volume
Kalenabled false		fatse	Enable microphone settings
Kamuted		false	Microphone muted

- **Step 3** In the master field, choose the master channel volume.
- **Step 4** Click the **Right Arrow** to expand the master settings.
- Step 5 Check or uncheck the enabled check box to enable or disable master channel settings.
- **Step 6** Check or uncheck the **muted** check box to mute or unmute the master channel.
- **Step 7** In the microphone field, choose the microphone volume.
- **Step 8** Click the **Right Arrow** to expand the microphone settings.
- **Step 9** Check or uncheck the **enabled** check box to enable or disable microphone settings.
- Step 10 Check or uncheck the muted check box to mute or unmute the microphone.
- **Step 11** Click **Apply**. If you don't want to make those changes, click **Cancel**.
- Step 12 In the Predefined actions menu, click Reboot.

Edit						
Predefined actions						
ø	Message					
List.	Open URL					
2 ¹ /2 2 ¹ /2	Reboot					
U	Display On/Off					
	Mute					
Ø	Upgrade					
Q	Restart Application					

Figure 5-108 Reboot Dialog Box

Step 13 In the Reboot Devices Dialog Box, click **Ok**.

Figure 5-109 Reboot Devices Dialog Box Reboot Device Will be applied to device SJC30124 Reboot device? Ok Cancel Step 14

Enabling VNC for IECs

In releases 2.0 and 2.1, VNC was managed from the IEC by using the debugging commands vncstart and vncstop. Starting in 2.1.1, the ability to use VNC to access the IEC remotely is managed by the IEM. To enable VNC in the IECs, the remoteview.enabled property in a policy is set to 'true'.

Note

remoteview.enabled is a runtime property so you will need to create a custom action for it. Then when you want to use a VNC viewer, you will push the custom action to an IEC.

To create a custom policy that can push VNC to an IEC, follow these steps:

- **Step 1** Log into the IEM.
- Step 2 Click Policies in the left pane.
- **Step 3** In the Edit menu, click **New Policy**.
- **Step 4** Enter a policy name in the **Policy Name** field that indicates the purpose of this policy such as "VNC_Start".

I

- **Step 5** Check the **Is action** check box to make this policy runtime.
- **Step 6** Check the **Add to custom actions** checkbox to create a custom action.
- Step 7 Click Create.
- **Step 8** After the policy is created, open the policy and click the **Policy** tab.
- **Step 9** Find the **remoteview > enabled** property.

Figure 5-110 remoteview.enabled Property

Property		Compatibility	Value	
▼	•			
kan enabled	•		true	Start or stop a remove view for this system

Step 10 Change the value to **true**.

Step 11 Click Apply.

Note

You will need the IEC's Maintenance Code to access an IEC using a VNC viewer.

When you are ready to use a VNC viewer to access an IEC, follow these steps:

- **Step 1** In the IEM, go to the IEC that you want to access using a VNC viewer.
- Step 2 From the Custom actions menu, click the custom action that you created for VNC such as "VNC_Start".
- Step 3 When the VNC viewer opens, enter the IEC's Maintenance Code for the password.



When entering the Maintenance Code as the password, enter the letters of the Maintenance Code as upper case. If for example the Maintenance Code is 6A54F3, enter "6A54F3". The password will not work if you enter "6a54f3".



CHAPTER **6**

Configuring Policies

Revised: January 26, 2014, OL-26458-05

Chapter Overview

ſ

This chapter explains how to configure policies.

Policies represent dynamic and transportable setup rules. Policies provide an easy and flexible way of applying settings to a group of users or devices. For example, an administrator can apply a policy to use certain printer for certain section of the building, or restrict Internet access on some, but not other terminals.

Topics in this chapter include:

- Policies, page 6-2
 - Policy Hierarchy, page 6-2
 - Persistent Policies, page 6-3
 - Runtime Policies, page 6-3
 - Persistent vs. Runtime vs. Persistent Runtime Properties, page 6-5
 - Accessing Policies, page 6-5
 - Creating New Policies, page 6-6
 - Copying Policies, page 6-8
 - Exporting Policies, page 6-10
 - Importing Policies, page 6-12
 - Applying Policies, page 6-14
 - Deleting Policies, page 6-15
 - Policy Properties, page 6-16
- Policy Scheduling, page 6-17
 - Creating a Schedule, page 6-18
 - Applying a Schedule to a Policy, page 6-24
 - Sample Scenario 1, page 6-27
 - Sample Scenario 2, page 6-27
 - Effective Profile, page 6-28

- Deleting Schedules, page 6-29

You must reboot the Cisco IEC4600 Series after adding or modifying any configuration in Cisco IEM for the configuration changes to reflect on the device.



<u>}</u> Tip

After you make a change to policies, press the Refresh button at the upper left corner of the screen to view those changes.

Policies

A policy is a template for configuring IEC behavior. If you are configuring multiple devices and want them all to have the same settings (also called properties), configure a policy and then apply that policy to those devices.

Policy Hierarchy

The figure below illustrates the hierarchy for settings. If a policy is applied to a device, it takes precedence over the device's profile. A policy applied to a device takes precedence over a policy applied to a group.





<u>}</u> Tip

Group the devices according to the common settings and apply group policies. Then deal with exceptions by configuring a policy and applying it to the individual devices.
Persistent Policies

Policies can be persistent (long-term or permanent) or runtime (short-term or runtime).

Persistent policies are applied when the IEC4600 Series device is booted or rebooted. Persistent policies are permanent until they are unapplied.

To create a persistent policy, do NOT check the Is action check box when the policy is created.

Figure 6-2 Is action Check Box in the Create New Policy Dialog Box

_	Create New Policy
Policy Name	*
Is action	Alphabetical characters only
Description	
	Create

Once the persistent policy is created, its icon appears in the center pane without a white arrow within a blue circle.

Figure 6-3 Persistent Policy Icon



Runtime Policies

I

Runtime policies, on the other hand, are temporary and will only apply until the properties are changed, the device is rebooted, or a counter action policy is applied. Runtime policies are generally used for troubleshooting, demos, or special events.

Runtime policies are created by checking the **Is action** check box when creating the policy or in the General tab of the policy.

If an administrator wants the runtime policy to also be a Custom Action and appear in the Custom actions menu, check the **Add to custom actions** checkbox.

olicy Name 🔞	Policy_A
	Alphanumeric, $_{\omega}$ -, 3 characters minimum, must start with letter.
Is action	~
dd to cust	~
Description	Add to custom actions
	Create

Figure 6-4 Creating a Runtime Property that is also a Custom Action





Runtime policies can only work for runtime properties. A runtime property is marked in the policy or profile by an orange arrow. Examples of runtime properties include browser url, session locked, and session timeout enabled. When a runtime policy is applied by scheduling or by custom action, any runtime properties within it will get applied immediately; no reboot is necessary.

In the center pane of the Policies menu, a runtime policy icon appears with a white arrow within a blue circle.



Persistent vs. Runtime vs. Persistent Runtime Properties

Persistent policies are different than persistent properties. Similarly, runtime properties are different than runtime properties.

Just like with the Profiles tab, the properties in the Policy tab are divided into three categories:

- 1. Persistent
- 2. Runtime
- 3. Persistent runtime

Refer to the Profiles chapter for an explanation of each type of property.

Accessing Policies

Step 1

ſ

Use the steps below to access a policy to view its settings, configure it, or modify its configuration.



Click **Policies** in the left pane.

Step 2 In the center pane, double-click a policy's icon.



Step 3 Click the Policy tab.





Creating New Policies

If a policy does not already exist, you can create a new policy, copy an existing policy, or import a policy.

You can create a single policy and configure each of the settings. Alternatively you can create a policy for each setting (screen orientation, mouse, startup URL). Follow the steps below to create a new policy.

Step 1 Click Policies.

Step 2 In the Edit menu, click New Policy.

Figure 6	6-10	Edit Menu
	Edit	
1	ew Policy	
💘 🖿 In	nport Policy	
et E	ort Account	
In each	nport Account	

The Create New Policy dialog box opens.

Figure 6-11 Create New Policy Dialog Box

Policy Name 🌸	<u>j</u>
	Alphabetical characters only
Is action	
Description	

- **Step 3** Enter a policy name in the **Policy Name** field.
- **Step 4** (Optional) Check the **Is action** check box if this policy should be runtime.
- **Step 5** (Optional) If the runtime policy should also become a custom action, check the **Add to custom actions** checkbox.

Figure 6-12 Creating a Runtime Property that is also a Custom Action

_	Create New Policy
Policy Name 🔹	Policy_A Alphanumeric, _, -, 3 characters minimum, must start with letter.
Is action Add to cust	⊽ ⊽
Description	Add to custom actions
	Create Cancel

- **Step 6** (Optional) Enter a description of the policy in the **Description** field.
- Step 7 Click Create.

ſ

A new policy is created and its icon appears in the center pane.

	Figure	6-13	Nev	v Polic	y Icon					
		BART	BGL-GBC-Showe	Bot.	BRI-ONLINE-BANK	Carrefoor	CiscoCampus	CB-Singapor-TE.	C6-Singapore-T.	CIB-Try-spenURL
	Citbani-India	CHINAMENIEC	COBRA	COBRAT	dgus	DISCHART	DUALSCREEN	ERC	Emiralita	GO-Transit
	GOEMERGENCY	HD176Test	HomeDepot	IndonesiaDemo	IndonesiaGBC	JCD-Womens-Fo.	NoRotation	NICT	RATP	RE-DUALSCREEN
	Restart-COBRA	Rogbot	Rogbot-Audio-Pt	Regbet-HDM	Rotate 100	Retain 90	RotatePOCCW	SJ-EBC-Demo	SLXH5X	1 878
	THOMSON	ty-share-desidop	TILITS	WMT						
Step 8	Click o	n the n	ew pol	icy to o	open it.					
Step 9	Click o	n the I	Policy t	ab.						
Step 10	Config	ure the	proper	ties. (S	See Cha	pter 5.)			

Copying Policies

Users of the Root account can copy policies. Copying a policy saves time if the majority of the configuration will be re-used for the new policy. For example, a retailer may want to display three different startup URLs within their stores but all other configurations would be the same. In that case, the retailer would configure a policy with one of the startup URLs and then copy that policy twice. In each of the copies, a different startup URL would be configured. The benefit of copying policies is that all settings would be the same saving configuration time as well as time troubleshooting issues. Use the steps below to copy a policy.



Users of accounts other than "Root" will not have access to the Copy button.

Step 1 Click Policies.

Step 2 In the center pane, click an icon.







The Copy Policy to Account dialog box opens.

Step 4 From the Copy to Account drop-down list, choose an account.

Figure 6-16	Copy Policy to Account Dialog Box
	Copy Policy to Account
Copy To Account 🔹	bluefox
	Copy Cancel

Step 5 Click Copy.

Γ

Exporting Policies

Export a Single Policy

If you want to use a policy on another Cisco IEM instance, follow the steps below to download the file to your desktop.

Step 1 Click Policies.

Figure 6-17

Step 2 In the center pane, click a policy's icon.

Policy Icons

1		L				1		1	
ANGRYBIRDS	BART	BGL-GBC-Showc	Both	BRI-ONLINE-BANK	Carrefour	CI6-Singapor-TE	OB-Singapore-T	Citi-Try-openURL	Citibank-India
						8			
CNNandMSNBC	COBRA	COBRA1	dgus	DMGNYCT	DUALSCREEN	EBC	Errorates	GO-Transit	GOEMERGENCY
		L	1		1				
HD176Test	HomeDepot	IndonesiaDemo	IndonesiaGBC	JCD-Womens-Fo_	NoRotation	NYCT	RATP	RE-DUALSCREEN	Restart-COBRA
		1		2			8	1	5
Rogbot	Rogoot-Audio-P1	Rogbol HDMI	Rotate 100	Rotate90	Rotate90CCW	SJ-EBC-Demo	SLX-HSX	STS	THOMSON
		L							
by-share-desidop	TYLLYS	WMT							

Step 3 In the Edit menu, click **Export**.



Edit				
-	Delete			
\$	Properties			
et	Export			
~	Copy Policy			
et:	Export Account			
4 8	Import Account			





Figure 6-19 **Opening Policy Dialog Box**

Step 5 Click OK.

The file is downloaded to your computer.

Export Multiple Policies

ſ

Follow the steps below to export multiple policies.

- Step 1 Use the Shift key or CTRL key and arrows or the mouse to select two or more policies.
- Step 2 In the Edit menu, click Export.





Step 3 In the Opening Policy dialog box, choose the Save File radio button.

I



Figure 6-21 **Opening Policy Dialog Box**



The file is downloaded to your computer.

Importing Policies

If a policy exists on another Cisco IEM instance that you want to use, you can import it into your instance of Cisco IEM. Follow these steps to import a policy:

Click Policies. Step 1

Figure 6-22

Step 2 In the Edit menu, click Import Policy.



Import Policy Button

In the Import dialog box, click add. Step 3

Figure 6-2	3 Import Dialog Box
	Import
load	ed(0 files - 0 Rytes) / total(0 files - 0 Rytes) 0%
1000	Sadd upload
	Cancel

Step 4 Choose the file on your computer then click **Open**.

Figure 6-24 Select Files Dialog Box on Computer

Look in:	Desktop		🛨 🧿 🗊 🖡	🤊 🛄 🔻
C.	Name	Size	Item type	Date modified
	Adobe FrameMaker	2 KB	Shortcut	11/30/2011 8:15 .
lecent Flaces	🛃 Mozilla Firefox	2 KB	Shortcut	5/30/2011 11:51 .
	naglt 8	2 KB	Shortcut	2/1/2010 11:04 A
Desktop	KEXCEL - Shortcut	2 KB	Shortcut	9/4/2011 5:57 PM
(Here)	🔊 iSkysoft DVD Ripper	2 KB	Shortcut	4/14/2010 9:22 A
6	POWERPNT - Shortc	2 KB	Shortcut	9/4/2011 5:57 PM
Libraries	WinSCP	1 KB	Shortcut	11/25/2011 11:4
1	😿 WINWORD - Shortcut	2 KB	Shortcut	9/4/2011 5:57 PM
- 1	CombinedFile	1 KB	Text Document	12/9/2011 10:57 .
Computer	test	1 KB	Text Document	12/8/2011 2:21 P.
	user_sam	3 KB	Text Document	12/8/2011 2:56 P.
Network	🔮 user_10	3 KB	XML Document	12/8/2011 2:34 P.
	•	111		Þ
	File name:			• Open
	Files of type: All Files (*	-)		Cancel

The file name then appears in the Import dialog box.

Figure 6-25 File Chosen in Import Dialog Box

Import	_
policy_EasternUS.xml	2.0 Kb
loaded(0 files - 0 Bytes) / total(1	files - 2.0 Kb) 0%
	upload
Cancel	

Step 5 Click Upload.

ſ

A green check mark appears next to the file after it has been uploaded.

	Import		
~	policy_EasternUS.xml	2.0 Kb	
	loaded(1 files - 2.0 Kb) / total(1	es - 2.0 Kb) 100%	
		upload	
	Close		
\sim			
<u>}</u> Tip	If a file uploaded is file, choose the file	he wrong file or there is an error uploading it, delete that file.	To delete

Applying Policies

Use the steps below to apply a policy to a device.

Step 1	Click Devices.

Step 2 In the center pane, double-click a device's icon.



BLRGBC0	5JC30124	EN656015030118	IllyDevice	GAPvep2	Smalkiosk	DSITestUnit	BLRGBC3	UKDEMOTC
BGL 142singlectr	SJC30051	MOBILEDEMO	SN656015030016	BLRGBC2	WMT	GAPvep3	DK030072	BB-R-TC
				-				
GAPvep1	Sing1	dgus	BLADCTEST1	groupG				

- Step 3 Click the Policies tab.
- **Step 4** In the Available policies list, choose a policy.

Figure 6-28 Available Policies List

	General Member Of	Profile Police	Datus Events Perform	arce 🛃
1	Available policies	4	Applied policies	Schedule
2	Rotate90CCW	1	No. Street	
2	Rictate 90			(4)
2	Rotate 180			
2	Rogbol-HDMI			100

Step 5 Click the Green Arrow.

The policy now appears in the Applied policies list.



Deleting Policies

I

If you want to delete a policy, follow these steps:

- Step 1 Click Policies.
- **Step 2** In the center pane, click a policy's icon. If you want to delete multiple policies, use the Shift key or CTRL key and arrows or the mouse to select two or more policies.





Step 3 In the Edit menu, click **Delete**.



Step 4 In the Confirm Delete dialog box, click **Delete**.

Figure 6-33 Confirm Delete Dialog Box



Policy Properties

If you make a change to a property in a policy, those changes will affect all devices that use that policy. On the other hand, if you change a property in the profile of a device, those changes will only impact that particular device.

The same properties that can be configured in a profile can be configured in a policy.

			General	Policy	
Filter S Inter					
Property		Compatibility			Valu
application					
▶ 💼 audio					
▶ 💼 browser					
▶ 💼 clock					
▶ 💼 cohttpd					
▶ 💼 display					
▶ 💼 emergency					
▶ 💼 flashplayer					
▶ 💼 hotkeys					
▶ 💼 keyboard					
▶ imanagement					
▶					
▶					
▶					
▶					
▶					
▶ 🛅 screenmonitor					
▶ 💼 session					
▶ 💼 settings					
▶ 💼 system					
▶ 💼 upgrade					
▶ 💼 volume					

Figure 6-34 Policy Properties

Refer to the "Configuring Profiles" chapter for the list of properties and instructions on how to configure them.

Policy Scheduling

The Schedules feature allows users to control when policies are applied to devices.

- **Q.** How do schedules get calculated?
- **A.** The IEM looks at the policy stack and determines what the current policy is by examining both the order of the stack and the time values. Since the IEM is looking at the order of the stack, you must put the "always" policies at the bottom of the stack.
- **Q.** How does the type of policies scheduled determine whether the IEC is rebooted when the schedule changes from the current policy to a new policy?
- **A.** If the schedule indicates to change the current runtime policy to a different runtime policy, the IEC will not reboot. If you use persistent policies, the IEC will be rebooted when the schedule indicates to change the current policy to a new policy in order for the IEC to pick up the new policy.



Creating a Schedule

To create a schedule, follow these steps:

Step 1 Click the **Schedules** menu in the left pane.

Γ

Figure	6-35 Schedules
	Devices
-1	Users
►	Policies
► 🗱	Alerts
	Schedules
×1	Accounts
**	Maintenance

Step 2 Click **New Schedule** in the Edit menu to the right of the screen.

Figure 6-36	New Schedule Button
	Edit
+ Ne	w Schedule

Step 3 In the Create New Schedule dialog box, enter a name in the Schedule Name field.

I

ocredule Name * Schedule				
Start	Duration	Recurrent		

Figure 6-37 Create New Schedule Dialog Box

Step 4 Click + to add an item.



Step 5 Check the Recurrent checkbox if you want the item to be recurring.

Γ

Schedule Item
Recurent Start Start date 05/17/2012 Start time 9:52
Ouration Until unapplied Una
Ok Cancel

Figure 6-39 Schedule Item Dialog Box

- **Step 6** Enter the start date in the Start date field.
- **Step 7** Enter the start time in the Start time field.
- **Step 8** Choose either the Until applied or days radio button. If you choose the days radio button, enter the time-frame of how long you want the schedule to run which can range from minutes to days by entering them in their corresponding fields.

Schedule Item	
Recurent Start Start date 07/01/2012 Start time 12:00	
Duration O Until unapplied I I I hours 0	minutes
Ok Cancel	

Figure 6-40 Schedule Item Dialog Box

Step 9 Click Ok.

Step 10 Add more schedule items as needed.

Start	Duration	Recurrent
Thu May 17 2012 at 10:00	3h	every Mon, Wed, Fri at 10:00
Wed May 23 2012 at 12:00	1d 1h	No

Figure 6-41 Schedule with Two Items

Step 11 Click Create.

ſ

If you click on the schedule that you created, you will see the start date and time, the duration, and whether or not it is recurring.

Once you have created one or more schedules, you can view them either as icons or a list.

Figure 6-42 Schedule Icons



Figure 6-43	Schedule List			
E Filter	8	: = 6		
Name	*	Info		
Chedule_A				
Schedule_B				
Schedule_C				
No. No.				

Applying a Schedule to a Policy

After a schedule is created, it is applied to a policy.

- **Step 1** Go to the device that you want to schedule.
- **Step 2** Go to the **Policies** tab for that device.
- **Step 3** If the policy that you want scheduled has not already been applied to the device, choose the policy and click the Green Arrow.

	General	Member Of	Profile	Policies	Status	Events	Perfomance	
		Changing acti	ve policies or p	olicy schedules may	lead to reboot of	f the device.		
Available policies	<u> </u>		A	pplied policies				Schedule
COBRA		L SIPStart	Up			always		
DSE		📕 SIP				always		
EBC								
ecturecapturevyopta		2						
Maersk								
/larketingWall								
NRF-Array								
NYCT								
sip2		ä						
Test								
FestPolicy								
VSCT								
vamcclou								
wamcclou-SIP								
		U						
					<u></u>			
			Deliaire	inharitad from		1.1		Pahadula
			Policles	innented nom group	5			ochequie
		-						
		-	Second Street		-	N.		

Figure 6-44 Policies Tab with Applied Policies

Note

ſ

e By default, all policies are marked as "always" in the Schedule column. That means that they are operating 24x7 on that device.

Step 4 Click the Schedule field within the applied policy to display a list of schedules that have been created.

Figure 6-45 Schedule Field



Step 5 Choose a schedule from the drop-down menu.

I

Figure 6-46 Schedule Drop-Down Menu



Step 6 Schedule additional policies if desired.

Next you will organize the applied policies. The system will start at the top of the list to figure out which policy it should apply and when. The policy or policies that you configure as "always" must be at the bottom of the list. If an always policy is at the top, the system will ignore all other non-always policies below it.

Note

Figure 6-47 Always Policy Placed on the Bottom

	Applied policies	Schedule
L	dual_screen_2	suspend
•	DisplayPortrait	dualscreen2
•	Training	dualscreen1
L	sip_phone	always

<u>P</u> Tip

If you want a policy to start before another finishes, put it on the top of the list.

Note If the device belongs to a group and group policies have been applied to the group, those policies will be listed in the Policies inherited from groups area below the Applied policies. These group policies may have an effect on when an applied policy will begin or end.

Move a policy by highlighting it and then clicking the gray up or down button to the right side of the list.

Figure 6-48 Inherited Group Policies

Policies inherited from groups	Schedule
▼	always
📕 portrait	always
L clockwise	always

If policy schedules overlap, the policy at the top of the list takes precedence. That policy will be in effect until it reaches the end of its scheduled duration.

Step 7

Sample Scenario 1

An administrator scheduled the following policies in this order:

- 1. Runtime Policy "Morning": scheduled to start at 06:00 for a duration of 6 hours
- 2. Runtime Policy "Evening": scheduled to start at 12:00 for a duration of 8 hours
- 3. Runtime Policy "Display_OFF": scheduled to start at 20:00 for a duration of 8 hours
- 4. Persistent Policy "Unexpected": always
- **Q.** What will appear on the kiosks during the day?
- **A.** The policies will appear at the following times:

00:00 - 06:00 "Display_OFF"

06:00 - 12:00 "Morning"

12:00 - 20:00 "Evening"

20:00 - 00:00 "Display_OFF"

- **Q.** When will the IEC reboot?
- **A.** The IEC will not reboot since there is no rebooting between runtime policies. In case something happens and the IEC reboots, it will pick up and play the persistent policy "Unexpected" until the next scheduled event.

Sample Scenario 2

An administrator scheduled the following policies in this order:

- 1. Persistent Policy "Before Hours": scheduled to start at 7:00 am for 1 hour (for branch employees)
- **2.** Runtime Policy "After Hours": scheduled to start at 5:00 pm for a duration of 1 hour (for branch employees)
- **3.** Persistent Policy "Maintenance": scheduled to start at 10:00 pm for a duration of 8 hours (for maintenance workers)
- 4. Persistent Policy "Customers": always (for customers)
- **Q.** What will appear on the kiosks during the day?
- **A.** The policies will appear at the following times:

0:00-06:00 Policy "Maintenance"

06:00-07:00 Policy "Customers"

07:00-08:00 Policy "Before Hours"

08:00-17:00 Policy "Customers"

17:00-18:00 Policy "After Hours"

18:00-22:00 Policy "Customers"

22:00-24:00 Policy "Maintenance"

- **Q.** When will the IEC reboot?
- **A.** The IEC will reboot at 06:00, 07:00, 08:00, and 22:00 to pick up the persistent policies.

Effective Profile

The Effective Profile tab on the Devices screen provides a time line of configuration changes to the IEC based on the scheduling of policies. With this feature, the administrator can see a cumulative view of the configuration changes applied to a device and understand where the configuration is originating. The cumulative changes on that device can come from the device profile, policies applied to the device, and the group to which the device belongs.

To view the Effective Profile of a device, follow these steps:

- **Step 1** Click **Devices** in the left pane.
- **Step 2** Choose a device either in the left or central pane.
- **Step 3** Click the **Effective Profile** tab.

Gene	aral Member Of Profile Polic	ies Status Events Performanc	e Effect.Prof.
	Now 14:20 02:26 15:20 02:26	14:20 03.05 15:20 03.05 15:20 03.12	Now
Filter	0		三 三
Property	Inheritance	Value	Description
Rapplication			
audio			
🕮 browser			
Clock			
💼 cohttpd			
🕮 display			
emergency			
💼 flashplayer			
hotkeys			
📾 keyboard			
🖿 management			
mouse			
network			
apower 💼 power			
printers			
En profile			
screenmonitor			
E session			
n settings			

Figure 6-50 Effective Profile Tab

Step 4 Choose a future time on the time line.

Figure 6-51 Effective Profile Time Line



The times on the time line indicate when the configurations will change in the future. In the figure above, the administrator chose the configuration change that would occur at 3:20 p.m. on March 5, 2013.

Step 5 Look for a blue dot or dots next to the properties under the chosen time. A blue dot indicates a configuration change to that property at that time.

Figure 6-52 Blue Dot Indicating Configuration Change

	General	Member Of	Profile	Policies	Status	Events	Performance	Effect.Prof.	6
	Now	14:20 02.26	15:20 02.26	14:20 03.05	15:20 03.0	5 15:20 03	3.12) 14:2	20 02.26.2013	
Filter		43	0						「三」 ゴ
Property		Inheri	tance		V	alue		C	escription
application				-					
► 💼 audio									
▶ 💼 browser									

Step 6 Expand the property to view details of the configuration change.

Figure 6-53 Details of Configuration Change

▶ 📾 shortcuts			
🔻 🚞 startup			
🕨 💼 about			
🚰 url	₿ Moderro_Demos	moderro.com/DEMOS	Startup URL
► 🛅 storage			

Deleting Schedules

I

If you want to delete a single schedule or multiple schedules, follow these steps:

- Step 1 Choose Schedules.
- **Step 2** Click a schedule icon or use the Shift key or CTRL key and arrows or the mouse to select two or more schedules.

🔒 🗶 Filter	8		 ß
Schedule_A	Schedule_B	Schedule_C	

Schedule Icons

Step 3 In the Edit menu, click **Delete**.

Figure 6-54

Step 4 In the Confirm Delete dialog box, click **Delete**.

Cisco Interactive Experience Manager Administrator Guide



CHAPTER 7

Configuring Notifications

Revised: January 26, 2014, OL-26458-05

Chapter Overview

This chapter explains how to create notifications if there are events or issues with the IECs. Topics in this chapter include:

- Notifications Overview, page 7-1
- Creating a Notification and Associating It with a User, page 7-1
- Deleting Notifications, page 7-9

Notifications Overview

The Notifications feature sends automatic e-mails to users about devices' status, errors, performance, or events at scheduled intervals.

What is required:

- 1. SMTP relay hostname or IP address of the SMTP provider has been added to the IEM. See the *Cisco Interactive Experience Manager Installation Guide* for instructions on how to add the SMTP relay host or IP address of the SMTP provider in the IEM.
- 2. IEM user credentials with a valid email address.

Creating a Notification and Associating It with a User

Notifications are mapped to users. Notifications will be sent for all devices associated with the user chosen to receive those notifications. If you want to only receive notifications about one or a couple of devices, set up a separate account for that user and those devices.

Notifications can be sent to the user's e-mail address in addition to an URL.

Once a notification is created, you can associate other users in your account so they too can receive the notifications. Or they can subscribe to that notification since it will be visible in the Notifications menu.

Step 1 Go to the user who will receive the notifications and ensure that the email address is correct.

Step 2 Click **Notifications** in the left pane.

Figure 7-1	Notifications	Button
------------	---------------	--------

	Devices
► 🤱	Users
▶ 🖺	Policies
►∰	Notifications
▶ 🛄	Schedules
► <u>Å</u>	Accounts
▶%	Maintenance

Step 3 Click **New Notification** in the Edit menu in the right pane.

Figure 7-2 New Notification Button



The Create New Notification dialog box opens.

Create New Notification
Notification Name * Notification Alphanumeric, _, -, 3 characters minimum, must start with letter. Notification frequency 10 sec • Device Status Information & Errors Performance Events Device ON _ Device OFF _
Create Cancel

Figure 7-3 Create New Notification dialog box

- **Step 4** Enter a name for the notification in the Notification Name field.
- Step 5 From the Notification Frequency drop-down list, choose how often you want to receive notifications.
- **Step 6** Check either or both the Device ON and Device OFF check boxes to be notified when devices are turned on or off.
- **Step 7** Click the **Information & Errors** radio button.

ſ

	Create New Notification
Notification Name 🔹	Notification Alphanumeric, _, -, 3 characters minimum, must start with letter.
Notification frequency	10 sec
🔿 Device Status 🧉) Information & Errors 🔿 Performance 🔿 Events
Т	Severities Error Warning Information Debug
	Create Cancel

Figure 7-4 Information & Errors

Step 8 If you want to be notified when a severe event takes place, check one or more Severities check boxes.Step 9 If you want to be notified about performance, click the Performance radio button.

Create New Notification					
Notification Name Notification Alphanumeric, _, -, 3 characters minimum, must start with letter. Notification frequency 10 sec O Device Status Information & Errors Performance Events					
Data O OR O AND					
Data	Operator	Value			
		_			
		_			
Create Cancel					

Figure 7-5 Performance

Step 10 Click the + button to add a rule.

Γ

Step 11 Choose the type of rule from the Name drop-down list.

Name	Memory usage, average
Operator	
Value	

Figure 7-6 Add Notification Rule

- **Step 12** Choose the type of operator from the Operator drop-down list.
- **Step 13** Enter a value.
- Step 14 Click the Add button.
- **Step 15** Add more rules if desired.
- **Step 16** If you have more than one rule, click the **OR** radio button to choose that the notification should be triggered if any of the rules are met or click the **AND** radio button if all the rules must be met to trigger the notification.
- Step 17 If you want to be notified about events, choose the Events radio button.

Create New Notification
Notification Name * Notification Alphanumeric, _, -, 3 characters minimum, must start with letter.
Notification frequency 10 sec
🔿 Device Status 🔿 Information & Errors 🔿 Performance 💿 Events
USB Device name USB Device ON USB Device OFF
Create Cancel

Figure	7-7	Events
--------	-----	--------

- **Step 18** Enter the USB device name in the USB Device name field.
- **Step 19** Check either or both the USB Device ON and USB Device OFF check boxes to be notified when USB devices are turned on or off.
- Step 20 Click Create.

ſ

A Notification icon appears in the center pane.

Figure 7.8	Notification Icon
Figure 7-0	Νυτητατισή τουπ



Now you will assign Notifications to users.

- **Step 21** Click **Users** in the left pane.
- **Step 22** Click the user that should receive the notifications.
- **Step 23** Click the **Notifications** tab.
- Step 24 Choose one or more Notifications from the Available list.

Figure 7-9 Available Notifications

	General	Contact Info	Member Of	Profile	Security	Policies	Notifications	4
	Available notifi	cations					Applied notifications	
🔅 Alert23								
Notification-234								
🗰 Alert1								
🔑 DEV_on								
🔅 CPU_memory_usage								
🔅 Notification								
🔑 Debug								
🤑 fsdgsdfg								
🗜 Dev_off								
🔑 Info_error								
Action_url								
🔅 Info_warning								
🖟 Notification1								
🔅 test2_from_6331								
🔅 Information								
Notification2								
All_Errors_and_Warnings								
🔑 Alert								
🔅 Notification123								
			100		ancel			

Step 25 Click the Green Arrow to move the notification to the Applied list.
	Figure 7-10	Applied Notifications
		Applied notifications
	🌻 AlertA	
Step 26	Click Apply.	

The User receive notifications for all devices that are associated with the user.

Deleting Notifications

ſ

If you want to delete a single notification or multiple notifications, follow these steps:

Step 1	Click Notifications in the left pane.
Step 2	Choose a Notification icon or use the Shift key or CTRL key and arrows or the mouse to select two or more Notifications.
Step 3	In the Edit menu, click Delete .
Step 4	In the Confirm Delete dialog box, click Delete .





Modifying Server Settings

Revised: January 26, 2014, OL-26458-05

Chapter Overview

This chapter explains how to modify server settings.

The sections in this chapter are:

• Modifying Server Settings, page 8-1

Modifying Server Settings

You can modify some of the server's settings, such as number of logs to store and enabling the gateway.



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.

- **Step 1** Click **Maintenance** in left pane to expand menu.
- Step 2 Double-click System Settings.

*X M	aintenance
► 100	Supported Products
	Backup/Restore
1	Server Settings
B	Licenses
1	Audit

Figure 8-1 Server Settings Button in Left Pane



Figure 8-2	Server Settings
------------	-----------------

System log enabled	
Device gateway enabled	2
Sender name	IEM-1914(on30)
Administrator email	jsmith@abc.com
Maximum events number in log	1000
Event logs purged after, hours	12
Session lifetime, minutes	200
Device online timeout, sec	65
License inactive warning, days before	5
Failed attempts to user login, quantity	6
User lock timeout, sec.	30
Apply	Cancel

- **Step 4** Check the **Device gateway enabled** check box after you have registered IEC4600 Series devices that have been configured with the server's URL.
- **Step 5** In the **Sender name** field, enter the name that should appear when notifications are sent to users.
- **Step 6** Enter the administrator's email. This email account will be used as the sender's address when the system sends out notifications to users. The account will also receive system notifications.
- **Step 7** Enter the maximum number of events that you want collected in the **Maximum events number in log** field.
- **Step 8** In the **Events logs purged after** field, enter the number of hours that the event logs should remain accessible to the user after they are collected.
- **Step 9** In the **Session lifetime** field, enter the number of minutes that an IEM session will remain active before the user will be automatically logged out. This security feature can help prevent unauthorized persons from gaining access to the IEM if authorized users have walked away from their workstations for a period of time.

Step 10 In the **Device online timeout** field, enter the number of seconds that an IEC will have to reply to an IEM's request before it is considered offline.



Note You do not need to configure the License inactive warning field because the Cisco licenses do not expire.

Step 11 In the Failed attempts to user login field, enter the number of attempts that a user has to log in to the IEM before being locked out by the system. IF the user reaches the maximum number of attempts, the user is locked out and a message will be displayed (see figure below). This security feature can help prevent unauthorized persons from trying to guess credentials in order to access the system.

Cisco Interactive Experience Manager
Account
User Name
Password

Enter
User is locked now. Try again later.

Figure 8-3 User Lockout Message

- **Step 12** In the **User lock timeout** field, enter the number of seconds that a user will be locked out of the system after the number of failed attempts has been reached in the previous field.
- Step 13 Click Apply.

I



1





Backing Up and Restoring the Server

Revised: January 26, 2014, OL-26458-05

Chapter Overview

This chapter explains how to perform maintenance activities.

The sections in this chapter are:

- Backing up the Server, page 9-1
- Restoring the Server, page 9-3



The default username for the Post-Install Configuration site is **admin** and the default password is **cisco**!123.



The default username for the IEM Configuration Menu is **installer**. Use the password that was chosen when the IEM was installed.

Backing up the Server

You can back up the server's data to create backup files in case the system crashes. The backup file captures all configuration data such as those for devices and policies but does not capture the events.



The Backup and Restore process only works with same version (e.g. 2.1) and same install type (virtual machine). You can only restore backup files to either the system that crashed (and has not been upgraded since the backup files were generated) or a system that has the same version and same install type of the original system.

Q. How is the Backup and Restore process different from the Export and Import process?

A. Backup and Restore captures the entire data set from the system, whereas the Export and Import captures subsets of data such as accounts, devices, policies, schedules, etc. The Backup and Restore process is most appropriate for periodic system backups and upgrading the system. The Export and Import process is most appropriate for data migrations or data duplications such as when you want to replicate data on another server.

Follow these steps to create a backup file:

- **Step 1** Click **Maintenance** in left pane to expand menu.
- Step 2 Double-click Backup/Restore.

Figure 9-1 Backup/Restore Button in Left Pane



Step 3 Click Backup.

Figure 9-2	Backup Button
------------	---------------

	Attention! Restore operation can be dangerous to the system.
	Backup Restore
Δ	
/arning	Be careful not to click the Restore button instead of the Backup button. The Restore feature is discussed next.

Step 4 Choose the **Save File** radio button.

ou have chosen to	open
all_01_31_20	12_01_31_10_506.xml
which is a: X	ML Document (53.1 KB)
from: http://	kiosk.veptc.com
What should Firefo	ox do with this file?
Open with	XML Editor (default)
Save File	
🔲 Do this <u>a</u> uto	omatically for files like this from now on.
	OK Cancel

Figure 9-3 Save File Radio Button

Step 5 Click OK.

The backup file will save to your computer.

Restoring the Server

If the system crashes, use a backup file that you saved earlier to restore the server to that previous state. You can also restore the file to a different server for redundancy.

- **Step 1** Click **Maintenance** in left pane to expand menu.
- Step 2 Double-click Backup/Restore.

Figure 9-4

VX M	laintenance
► 10	Supported Products
	Backup/Restore
8	Server Settings
	Licenses
10	Audit



ſ

The Restore operation can be dangerous to the system.

Backup/Restore Button in Left Pane

Step 3 Click Restore.
Step 4 Click Add to choose the backup file from your computer.
Step 5 Click Upload to upload the backup file.



CHAPTER **10**

Auditing

Revised: January 26, 2014, OL-26458-05

Chapter Overview

This chapter explains how to access and use the Audit feature.

The sections in this chapter are:

- Audit, page 10-1
 - Sort Changes, page 10-2
 - Filter Changes, page 10-2

Audit

I

The Audit feature provides a trail of changes that have been applied to the system. The administrator uses the audit trail for troubleshooting and administrative purposes.

To access the Audit feature, expand the Maintenance menu and then double-click the Audit button.



Figure 10-1 Audit Button

Sort Changes

Changes to the system are presented in chronological order representing the order in which they were applied to the system and by whom they were applied. Administrators can sort the lists in alphabetical order by clicking on the column headings. The figure below shows the Action column sorted alphabetically in ascending order.

Action
A new account "GSX" (#2) was created
A new device "USI163600DJ" (#1) was created
A new firmware "5.40.55" (#1) was created
A new license was added in system
A new policy "CustomerListeningCtr1" (#1) was created
A new user "admin" (#2) was created
Device "USI163600DJ" (#1) was updated
Device "USI163600DJ" (#1) was updated
Firmware "5.40.55" (#1) was enabled
Firmware "5.40.55" (#1) was updated
Policy "CustomerListeningCtr1" (#1) was updated
Policy "GSX1" (#1) was updated
Policy list from device "USI163600DJ" (#1) was changed
Send action "upgrade.push" to device USI163600DJ
User login in

Figure 10-2 Sort Action Column in Ascending Order

Filter Changes

By default, all changes are displayed. Use the filter drop-down menu to search by devices, users, accounts, profiles, policies, user groups, device groups, firmware, models, products, schedules, and notifications.

ſ

Figure 10-3 Filter by Device

Filter device				25 💌 😣		
Action	Object	Account	Modified by	Modification time		
Policy list from device "USI163600DJ" (#1) was changed	Ciscio a forma in the second and the	🔒 GSX	admin	Thu Aug 15 17:43:46 2013 UTC		
Device "USI163600DJ" (#1) was updated	USI163600DJ			Thu Aug 15 17:40:38 2013 UTC		
Device "USI163600DJ" (#1) was updated	- US(153500DJ)	🛦 GSX	admin	Thu Aug 15 17:05:07 2013 UTC		
A new device "USI163600DJ" (#1) was created	USI163600DJ	🛦 GSX	admin	Thu Aug 15 17:05:06 2013 UTC		

Figure 10-4

	Filter policy			25 💌 😣
Action	Object	Account	Modified by	Modification time
Policy "GSX1" (#1) was updated	E 690	🛦 GSX	admin	Thu Aug 15 17:42:46 2013 UTC
Policy "CustomerListeningCtr1" (#1) was updated	L CustomerListeningCir1	& GSX	admin	Thu Aug 15 17:41:30 2013 UTC
A new policy "CustomerListeningCtr1" (#1) was created	L ContomentistaningClin	A GSX	admin	Thu Aug 15 17:41:30 2013 UTC

Figure 10-5

Filter by Firmware

Filter by Policy

	Filter firmwar	e 🔽		25 💌 😣
Action	Object	Account	Modified by	Modification time
Firmware "5.40.55" (#1) was enabled		A Root	Administrator	Wed Aug 14 21:46:06 2013 UTC
Firmware "5.40.55" (#1) was updated	FW 5.40.55	🗼 Root	Administrator	Wed Aug 14 21:45:54 2013 UTC
A new firmware "5.40.55" (#1) was created	EW 6 40 55	A Root	Administrator	Wed Aug 14 20:31:21 2013 UTC

Alternatively, enter a value in the blank field at the top of the screen to customize your search. In the figure below, the administrator entered the word "license" to filter all changes related to licensing.

Figure 10-6 Custom Filter

	Filter	all	▼	license)		25	V	8
Action	Object		Ac	count	Modified by	Modificatio	n time		
A new license was added in system			A	Root	Administrator	Wed Aug 1	4 21:54	:34 20	13 UTC

The administrator can control the number of actions displayed on the screen. Choose 25, 50, 100, 500, or 1000 from the drop-down menu.

	50	• 😣
Modification	25	
Thu Aug 15	50	I3 UTC
Thu Aug 15	100 500	I3 UTC
Thu Aug 15	1000	I3 UTC

Figure 10-7 Number of Actions to be Displayed

To clear the filter, click the X button.









Proxy Support

Revised: January 26, 2014, OL-26458-05

Appendix Overview

ſ

This appendix explains how to configure proxy support using the PAC file script format. You will perform the following tasks:

- 1. Set up the URL and create the script
- 2. Configure a proxy policy

Topics in this appendix include:

- URL Setup and Script Creation, page A-1
- IEM Proxy Support, page A-2
 - Static (Single Host), page A-2
 - Script (PAC File), page A-5
 - URL (Remote PAC File), page A-7

URL Setup and Script Creation

The first task is to set up the URL and create the script

Step 1 On the web/http server, create a file with an html extension.

Step 2 Copy and paste the following script into the file.

```
function FindProxyForURL(url, host) {
```

```
if (shExpMatch(url, "*espn*") ||
    shExpMatch(url, "*cnn*")) {
        return "PROXY 192.168.200.2:3128";
}
if (shExpMatch(url, "*google*") ||
        shExpMatch(url, "*yahoo*")) {
        return "PROXY 192.168.200.21:3128";
}
```

```
if (shExpMatch(url, "*abc*") ||
shExpMatch(url, "*nbc*")) {
    return "PROXY 192.168.200.22:3128";
}
if (shExpMatch(url, "*cbs*") ||
shExpMatch(url, "*fox*")) {
    return "PROXY 192.168.200.23:3128";
}
if (shExpMatch(url, "*nba*") ||
shExpMatch(url, "*nf1*")) {
    return "PROXY 192.168.200.24:3128";
}
```

Step 3 Modify the script based on the number of proxy servers.

<u>Note</u>

}

The above script was written for five proxy servers. Adjust according to the number of proxy servers that you are using.

- **Step 4** Replace the IP addresses in the script with your proxy servers' IP addresses.
- **Step 5** Replace the example URLs in the script (e.g. www.espn.com) with actual URLs.
- Step 6 Open a browser and enter the URL of the file to confirm it is reachable via network.

IEM Proxy Support

Three are three methods for configuring proxy support in the IEM:

- 1. Static: Configure the proxy server's IP address
- 2. Script: Enter the PAC file script
- 3. URL: Configure the PAC file script's URL

Static (Single Host)

This method points the IEM to the proxy server.

Step 1 From the IEM menu in the left pane, click	Policies.
---	-----------

- **Step 2** In the right pane, click the **New Policy** button.
- Step 3 In the Create New Policy dialog box, enter a name and description.

Create New Policy

Policy Name
Policy

Alphanumeric, _3 characters minimum, must start with letter.
Is action
Description
For Document Purpose

Create
Caract

Policy Icons

Figure A-1 Create New Policy Dialog Box

Step 4 Click Create.

Figure A-2

Step 5 In the center pane, select the policy that you just created by double clicking the icon.

Apple	dafault	Display_90	Dual_Display	Dual_Display_iS	
Dual_Display_Mo	Dual_Display_R	Dual_Display_W	ESPN	Google	
NYCTSIP	NYCTSIPpart1	proxy	Proxy_5_Script_G	Proxy_5_URL_ES_	
Proxy_CM_NBA	Proxy_Content_E	Proxy_Manager	Proxy_Multiple_S	Proxy_Multiple_U	

Step 6 Click the **Policy** tab.

Γ

Figure A-3 Tabs in a Policy

		General	Policy	
Name 🕯	proxy			
Description	For Docume	nt Purpose.		1

Step 7 In the Policy tab, enter **proxy** in the Filter field.

		Ge	neral Folloy	<u>L</u>
Filter proxy	۲	only runtime		E II
Property		Compatibility	Value	Description
network	۲			
▼ mproxy	۲			
🔻 🚞 autoconfig				
▼ 📄 cache				
enabled			true	Cache HTTP proxy autocor
G size			5000	HTTP proxy autoconfigurat
▼ 📄 check				
G interval			60	HTTP proxy autoconfigurat
Script				HTTP proxy autoconfigurat
(in the second s				HTTP proxy autoconfigurat
G host	٠		192.168.200.2	HTTP proxy host
🚰 mode	٠		Static	HTTP proxy mode
password				HTTP proxy password
i port			3128	HTTP proxy port
Guser				HTTP proxy user name
n settings				
T proxy				
in enabled			true	Enable proxy settings
	Y	ou have to apply or can	cel your changes in order to leave this	form.

Figure A-4 Proxy-Related Properties

- **Step 8** Go to the **network > proxy > autoconfig > host** property.
- **Step 9** Enter the proxy server IP address in the value field.
- **Step 10** Go to the **network > proxy > autoconfig > mode** property.
- Step 11 Choose Static.
- Step 12 Click Apply.
- **Step 13** Apply this proxy policy to an IEC device.
- **Step 14** Reboot the IEC device to activate the policy on the device.

Script (PAC File)

This method enters the PAC file script directly into a policy on the IEM.

- **Step 1** From the IEM menu in the left pane, click **Policies**.
- **Step 2** In the right pane, click the **New Policy** button.
- **Step 3** In the Create New Policy dialog box, enter a name and description.

Figure A-5	Create New Policy Dialog Box
1 ⁻¹	Create New Policy

olicy Name 🔹	proxy
	Alphanumeric, _, 3 characters minimum, must start with letter
Is action	
Description	For Document Purpose.

Step 4 Click Create.

Step 5 In the center pane, select the policy that you just created by double clicking the icon.





I

Figure A-7

	General	Policy	
Name 🌸	proxy		_
Is action			
Description	For Document Purpo	ose.	

Tabs in a Policy

Step 7 In the Policy tab, enter **proxy** in the Filter field.

		Ge	eneral Policy	Ŀ
Filter proxy	8	only runtime		T III
Property		Compatibility	Value	Description
🖊 🚞 network	۲			
🔻 🚞 proxy	۲			
🔻 🚞 autoconfig	۲			
🔻 🚞 cache				
🍙 enabled			true	Cache HTTP proxy autocor
iz e			5000	HTTP proxy autoconfigurat
🔻 📄 check				
interval 🎧			60	HTTP proxy autoconfigurat
🚰 script			function FindProxyForURL(url, host) {	HTTP proxy autoconfigurat
Giuri				HTTP proxy autoconfigurat
G host				HTTP proxy host
mode	•		Auto Configuration Script	HTTP proxy mode
assword				HTTP proxy password
(port			3128	HTTP proxy port
Guser				HTTP proxy user name
🖉 🚞 settings				
🔻 🚞 proxy				
nabled 🙀			true	Enable proxy settings
	Yo	u have to apply or can	cel your changes in order to leave this form.	

Figure A-8 Proxy-Related Properties



Step 9 Enter the PAC file script in the value field.

- **Step 10** Go to the **network > proxy > autoconfig > mode** property.
- Step 11 Choose Auto Configuration Script URL.
- Step 12 Click Apply.
- **Step 13** Apply this proxy policy to an IEC device.
- **Step 14** Reboot the IEC device to activate the policy on the device.

URL (Remote PAC File)

This method points the IEM to the PAC file on a remote server.

- Step 1 From the IEM menu in the left pane, click Policies.
- **Step 2** In the right pane, click the **New Policy** button.
- **Step 3** In the Create New Policy dialog box, enter a name and description.

Figure A-9 Create New Policy Dialog Box

Policy Name 🌸	proxy
	Alphanumeric, _ 3 characters minimum, must start with letter
Is action	
Description	For Document Purpose.

Step 4 Click Create.

ſ

Step 5 In the center pane, select the policy that you just created by double clicking the icon.

Figure A-	10 Po	licy lcons			
L					
Apple	dafault	Display_90	Dual_Display	Dual_Display_iS	
Dual_Display_Mo	Dual_Display_R	Dual_Display_W	ESPN	Google	
NYCTSIP	NYCTSIPpart1	proxy	Proxy_5_Script_G	Proxy_5_URL_ES_	
L					
Proxy_CM_NBA	Proxy_Content_E	Proxy_Manager	Proxy_Multiple_S	Proxy_Multiple_U	

Step 6 Click the **Policy** tab.



Policies > proxy		ON
	General Policy	
Name a Is action Description	For Document Purpose.	

Step 7 In the Policy tab, enter **proxy** in the Filter field.

General Policy						
Filter proxy	8 🗖 only runtime			E II		
Property		Compatibility	Value	Description		
🔻 🚞 network	۲					
🔻 🚞 proxy	۲					
🔻 🚞 autoconfig	۲					
🔻 🚞 cache						
🚱 enabled			true	Cache HTTP proxy autocor		
Ga size			5000	HTTP proxy autoconfigurati		
🔻 🚞 check						
🙆 interval			60	HTTP proxy autoconfigurati		
Script				HTTP proxy autoconfigurati		
Gii uri			http://392.368.200.2/pac_multiple.html	HTTP proxy autoconfigurati		
G host				HTTP proxy host		
mode			Auto Configuration Script URL	HTTP proxy mode		
password				HTTP proxy password		
Ge port			3128	HTTP proxy port		
Guser				HTTP proxy user name		
▼ 🗎 settings						
▼ 📄 proxy						
i enabled			true	Enable proxy settings		
	_					
	Yo	u have to apply or can	cel your changes in order to leave this form.			

Figure A-12 Proxy-Related Properties

Step 8 Go to the **network > proxy > autoconfig > url** property.

Step 9 Enter the URL of the PAC file script in the value field.

- **Step 10** Go to the **network > proxy > autoconfig > mode** property.
- Step 11 Choose Auto Configuration Script URL.
- Step 12 Click Apply.

ſ

- **Step 13** Apply this proxy policy to an IEC device.
- **Step 14** Reboot the IEC device to activate the policy on the device.

1