Moderro
IEM Management Software

Administration Guide

Release 2.6

Moderro Technologies

www.moderro.com

Table of Contents

Introduction

Chapter Overview

The Moderro Interactive Experience Manager (IEM) is a console that allows for centralized management of Moderro IEC 4600 Series interactive digital signage controllers.

This guide assumes that the Moderro Interactive Experience Manager has already been installed. If not, refer to the *Moderro 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 Moderro Interactive Experience Platform including the Moderro Interactive Experience Manager.

Topics in this chapter include:

- About This Guide
  - Terminology
  - Audience
  - Scope
- Moderro Interactive Experience Platform
  - Moderro Interactive Experience Client 4600 Series
  - Moderro Interactive Experience Manager
  - Principles of Operation
- Getting Started
  - Logging In
  - Moderro IEM Interface

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 Moderro Interactive Experience Manager instance. Use accounts to segregate users, devices, and policies. Each organization will have at least one account.
- Administrators - People who have access to all accounts on the system. The *Moderro Interactive Experience Manager Installation Guide* provides administrators with all the information necessary to install and administer a Moderro Interactive Experience Manager instance.
- Devices - The client at the kiosk such as the Moderro Interactive Experience Client 4600 Series and the Panasonic Connected Solutions Agent.
- Policies - An easy and flexible way of applying settings to multiple devices or users.
- Profiles - The settings of a single device or user.

- Users - People who configure and manage the Moderro Interactive Experience Manager. Users are assigned to specific accounts.

Audience

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

Scope

This guide explains how to use the Moderro 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

Moderro Interactive Experience Platform

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

The Moderro Interactive Experience Platform is the collective name for a product family that consists of thin clients and server hardware and software that will power a host of solutions, including the Moderro Interactive Experience Client 4600 Series and the Moderro Interactive Experience Manager.

Moderro Interactive Experience Client 4600 Series

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

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

Moderro Interactive Experience Manager

The Moderro Interactive Experience Manager (IEM) is the management console that allows the administrator

to control and monitor devices such as the Moderro IEC4600 Series and the Panasonic Connected Solutions Agent. Devices are configured remotely through a combination of device, user, and policy settings from the Moderro IEM.

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

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

- Configuration - Moderro 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. Moderro 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 - Moderro IEM can be set up to log the traffic from the 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 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. **Devices need to exist on the IEM in order to be managed by it.** 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.

Note It is recommended that you do NOT use overlapping schedules on a runtime policy.

4. **IEC and IEM software versions are best-effort compatible.** A device that has a IEC software 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 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 devices 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 7
- Macintosh OS X 10.9.4

The following browser versions are supported by the IEM:

- Internet Explorer
- Firefox
- Chrome
- Safari

Step 1 Open a supported browser and enter the Moderro IEM URL. The Moderro IEM login window appears.

Step 2 Enter the account name in the **Account** field.

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

Step 4 Enter the password in the **Password** field.

Step 5 Click **Enter**.

The Moderro IEM opens.

Moderro IEM Interface

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

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

The top pane contains the following features:

- Hide/Show navigation pane button
- Hide/Show action pane button
- Refresh button
- Search button
- Directory structure
- Current account name
- Current user name
- Exit button

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**. 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.

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

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.

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.

Managing Licenses

Last Revised: October 27, 2016

Moderro Interactive Experience Client (IEC) version 2.4 cannot be upgraded from IEC version older than 2.3.4b (5.354.406) when upgrade is done via Moderro Interactive Experience Manager (IEM) or terminal. To upgrade IEC to version 2.4 from IEC version older than 2.3.4b, use the IEM or terminal and upgrade the IEC to version 2.3.4b first.

Chapter Overview

Every device using Moderro Interactive Experience Client (IEC) software requires a license in order for it be managed on a Moderro Interactive Experience Manager (IEM).

This chapter provides information about licensing IEC software on the IEM. Topics in this chapter include:

IEM License Options

A license is required for each IEC software device. A single license or license bundles can be purchased. License bundles support up to 10, 50, 100, 500, or 1,000 IEC devices. When ordering licenses, ensure that you have ordered enough licenses to cover all the IEC software that will be managed by the IEM.

Table 2-1 IEM License Options

Product Number	Description
L-IEP-MGR-FL-1	Single IEP Manager license
L-IEP-MGR-FL-10	10-pack IEP Manager license bundle
L-IEP-MGR-FL-50	50-pack IEP Manager license bundle
L-IEP-MGR-FL-100	100-pack IEP Manager license bundle
L-IEP-MGR-FL-500	500-pack IEP Manager license bundle
L-IEP-MGR-FL-1000	1000-pack IEP Manager license bundle

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 a 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 device 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.

Note The first two devices will function without a license thus allowing developers to configure and test the system before purchasing licenses.

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 device: “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 Moderro Licensing site.

Step 1 Purchase the license bundles.

Step 2 Go to the Moderro Licensing site at https://tools.cisco.com/SWIFT/LicensingUI/Home.

Step 3 When prompted, log in with your customer or partner credentials.

Step 4 On the Product License Registration home page, click the green **Continue to Product License Registration** button.

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

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**.

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 theIEM

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.

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

Step 6 In the Add License dialog box, click the **Upload license file button**.

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

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

Step 8 In the Add License dialog box, click **Add**.

The licenses appear in the center pane.

Managing Accounts and Users

Last Revised: October 27, 2016

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
  - The Root Account
  - Determining Number of Accounts Needed
  - Adding a New Account
  - Exporting Accounts
  - Importing Accounts
  - Delete Accounts
- Users
  - Adding a New User
  - Removing Administrator Access for a User
  - Adding a New Group
  - Exporting Users
  - Importing Users
  - Deleting Users

Tip

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 sub- accounts, 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 Moderro 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 ofAccounts Needed

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

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

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.

Within the Marketing account, the Administrator created several accounts for 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),

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.

Adding a New Account

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

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

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

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

Step 4 (Optional) Enter a description in the **Description** field.

Step 5 (Optional). Choose a Policy from the **Policies to Propagate** list.

Step 6 Click **Create**.

Exporting Accounts

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

Follow these steps to use the bulk export option:

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

Step 2 Choose an account.

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.

Step 5 Click **Export**.

Importing Accounts

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

Warning **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**.

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

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

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

Step 7 Click **Upload**.

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

Tip Check the **Overwrite existing entities** check box to overwrite a file.

Step 8 Click **Close**.

Delete Accounts

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.

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.

Step 4 Enter a password in the **Password** field.

Step 5 Re-enter the password in the **Re-type Password** field.

Step 6 (Optional) Enter the user's first name in the **First Name** field.

Step 7 (Optional) Enter the user's last name in the **Last Name** field.

Step 8 Enter the user's e-mail in the **Contact e-mail** field.

Step 9 (Optional) Enter a description of the user in the **Description** field.

Step 10 Click **Create**.

Removing Administrator Access for a User

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.

Note 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. 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.

Step 3 Uncheck the **Grant Administrator Access** check box to remove administrator access.

Step 4 Click **Apply**.

Adding a New Group

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.

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

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

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.

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.

Step 5 Click **Download**.

The file is an xml file.

Export Multiple Users

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.

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.

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**.

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

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

Step 6 Click **Upload**.

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

Tip If a file uploaded is not desired or there is an error message associated with it, delete that file. Choose that file and then click **remove**.

Step 7 Click **Close**.

Deleting Users

Administrators can delete a single user or multiple users.

Delete a Single User

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

Step 2 Click a user icon in the center pane.

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

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

Delete Multiple Users

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**.

Managing Devices

Last Revised: October 27, 2016

Chapter Overview

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

- Firmware Version
- Devices
  - Learning Device Status
  - Adding a New Device
  - Batch Registration
  - Sending Messages to Devices
  - Opening an URL
  - Rebooting Devices
  - Restarting Applications
  - Turning Display On or Off
  - Muting or Unmuting Devices
  - Applying Policies to Devices
  - Creating and Applying Custom Actions to Devices
  - Monitoring Events
  - Monitoring Performance
  - Exporting Logs
  - Deleting Devices
- Device Groups
  - Adding a New Group
  - Adding a Device to a Group
  - Adding Multiple Devices to a Group
  - Removing Devices from a Group
  - Setting a Group's Properties

Tip The new configuration will appear on the device after it is rebooted.

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

FirmwareVersion

Before you can add devices, verify the firmware version and update if necessary. Refer to the *Moderro Interactive Experience Manager Installation Guide* for instructions.

Devices

A device is the client at the kiosk such as the Moderro 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.

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.

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.

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.

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.

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).

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 Moderro 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.

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

Step 6 Click the **Policies** tab to learn which policies have been applied to that device.

Step 7 Click the **Status** tab and expand the menu to learn the following about the device:

- Hardware information
- Network interfaces' net masks, MAC addresses, and IP addresses; default gateway IP address;

and DNS servers IP addresses

- Display screen resolution
- Locale information including time zone, language, and country
- Connected USB and PCIe devices information
- Connected USB web cam information
- Volume information

Adding a New Device

You will need the following to register a new device:

1. Serial number of the device
2. License in the IEM

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**.

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

Note Only alphanumeric and underscores can be entered in the device name field. The dash/minus/hyphen sign is no longer allowed to be used within device names.

Step 4 Enter the serial number in the **Serial Number** field.

Step 5 (Optional) Enter a description of the device.

Step 6 Click **Register**.

Batch Registration

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

Step 1 Open Notepad or Microsoft Excel on your computer. **Step 2** Enter device names and serial numbers with one per row. **Step 3** Save as type CSV (Comma delimited).

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.

Step 6 In the Import dialog box, click the **add** button.

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

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

Step 9 Click **Upload**.

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

Step 10 Click **Close**.

The devices 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 devices. 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.

Step 3 Click **Message**.

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 devices. Follow the steps below to open an URL.

Tip 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.

Step 3 Click **Open URL**.

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 device must be rebooted for those changes to take effect.

Tip 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.

Step 3 Click **Reboot**.

Step 4 Click **Ok**.

Restarting Applications

The applications on the devices 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.

Step 3 Click **Restart Application**.

Step 4 Click **Ok**.

Turning Display On or Off

You can control a display connected to a 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.

Step 3 Click **Display On/Off**.

Step 4 Click **Display Off** or **Display On**.

Muting or Unmuting Devices

A 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.

Step 3 Click **Mute**.

Step 4 Click **Mute** or **Unmute**.

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**.

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

Step 3 Click the **Policies** tab.

Step 4 In the Available policies list, choose a policy.

Step 5 Click the **Green Arrow**.

The policy now appears in the Applied policies list.

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

Tip 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**.

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**.

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

The Create New Policy dialog box opens.

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.

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.

Note Custom actions are indicated by a blue arrow.

Step 8 Click **Devices**.

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

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.

Monitoring Events

You can monitor device 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.

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

You can monitor performance of a device'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.

Step 3 Click the **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**.

Exporting Logs

It may be necessary to export logs for compliance purposes. There are 3 methods for exporting the logs:

1. Save logs manually from the IEM UI: This is probably the least desirable option as it is labor intensive.
2. Use an IEM API: The logs can be stored on your archive server.
3. Use the Notification subscription to a third-party system where each log entry of interest will be also logged to your backend: This will require some development on the backend logic.

Deleting Devices

Users can delete a single device or multiple devices registered under same account.

Delete a Single Device

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

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

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**.

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

Step 4 Click **Create**.

Step 5 A folder labeled with the group's name appears in the left and center panes.

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.

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

Step 4 Check a group's check box.

Step 5 Click **Apply**.

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

Step 7 Click **Ok**.

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.

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

Three tabs appear in the center pane.

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

Step 5 Click **+**.

Step 6 In the Add to Group dialog box, check the devices' check boxes.

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

The devices appear in the group's member list.

Step 8 Click **Apply**.

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

Step 10 Click **Ok**.

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.

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

Three tabs appear in the center pane.

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

Step 5 Click a device.

Step 6 Click **X**.

Step 7 Click **Apply**.

Step 8 In the Predefined actions menu, click **Reboot**.

Step 9 Click **Ok**.

Setting a Group's Properties

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. The device icons within the group are displayed.

Step 3 In the Edit menu, click **Properties**. Three tabs appear in the center pane.

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

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.

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**.

Step 14 Click **Ok**.

Step 15 Click **Cancel** to exit.

Configuring Profiles

Last Revised: October 27, 2016

Chapter Overview

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
  - Accessing a Profile
- Properties
  - Persistent vs. Runtime vs. Persistent Runtime Properties
  - Configuring Application Data
  - Specifying Audio Sources
  - Configuring the Browser
  - Configuring the Startup URL
  - Setting the Clock and Synchronizing NTP Servers
  - Adjusting the Display
  - Creating Emergency Messages
  - Enabling Trusted Sites for the Flash Player
  - Enabling the System Settings Hotkeys
  - Specifying Keyboard Parameters
  - Adjusting the Mouse
  - Managing Power Modes
  - Adding and Configuring Network Printers
  - Enabling Profile Expiration
  - Enabling a Proxy Server
  - Managing Screen Shots
  - Managing IEC's System Settings Menu
  - Collecting System Health Status
  - Configuring Remote Logs
  - Enabling Services
  - Disabling the Watchdog Settings
  - Managing System Upgrades
  - Adjusting Volume
  - Enabling VNC for IECs

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

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.

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 aProfile

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**.

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

Step 3 Click the **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.

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 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**.

Step 4 Click on the icon within the Value column to open the 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**.

Step 7 Enter the name of the barcode scanner recognized by the IEC in the value field. See Appendix D of the *Moderro 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 Moderro IEC4600 Series can be configured from the Moderro 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 Moderro 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**.

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.

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

Step 10 Click **Cancel**.

Configuring theBrowser

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:

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

Step 2 Find the **browser** property.

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

Step 4 Click the values within the appearance settings to configure them:

- 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.
- 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.

Step 5 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.

Step 6 Click the values within the cache settings to configure them:

- To enable the caching of media:
  a. Choose c**ache** > **media** > **enabled**.
  b. Check or uncheck the **enabled** check box to enable or disable media caching.
- To choose the media cache size:
  a. Choose c**ache** > **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 c**ache** > **web** > **enabled**.
  b. Check or uncheck the **enabled** check box to enable or disable web caching.
- To choose the web cache size:
  a. Choose c**ache** > **web** > **size**.
  b. Click the **Up Arrow** to increase or the **Down Arrow** to decrease the size of the web cache.

Step 7 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.
- 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 c**ontent** > **java** > **enabled**.
  b. Check or uncheck the **enabled** check box to enable or disable java applets.
- To enable JavaScript:
  a. Choose c**ontent** > **javascript** > **enabled**.
  b. Check or uncheck the **enabled** check box to enable or disable JavaScripts.
- To enable browser plugins:
  a. Choose c**ontent** > **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 8 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.

Step 9 To enable or disable the virtual keyboard:

a. Choose **screen** > **keyboard** > **enabled**.

b. Check or uncheck the **enabled** check box to enable or disable the virtual keyboard.

Step 10 By default, JavaScript error logging is enabled.

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

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 11 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.

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 12 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.

Step 13 To configure the network:

a. Choose **browser > network** > **failover** > **enabled**.

b. Check or uncheck the **enabled** check box to enable or disable the network failover algorithm.

c. Choose **browser > 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 **browser > network** > **timeout**.

f. Click the **Up Arrow** to increase or the **Down Arrow** to decrease the network operations timeout.

g. Choose **browser > network** > **timeout** > **enabled**.

h. Check or uncheck the **enabled** check box to enable or disable timeout.

Step 14 To enable or disable printing of background colors and images:

a. Choose **browser > print** > **elementbackgrounds** > **enabled**.

b. Check or uncheck the **enabled** check box to enable or disable the printing of background colors and images.

Step 15 To configure security settings:

a. Choose **browser > security** > **certificates** > **selfsigned** > **enabled**.

b. Check or uncheck the **enabled** check box to enable or disable the accepting of self-signed certificates.

c. Choose **browser > 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 **browser > 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 **browser > security** > **newwindow** > **mode**.

h. From the mode drop-down list, choose the new windows opening mode.

i. Choose **browser > security** > **remotetolocal** > **enabled**.

j. Check or uncheck the **enabled** check box to specify whether remotely loaded documents are allowed to access local files.

Step 16 To configure the startup URLl:

a. Choose **browser > 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 **browser > startup** > **url**.

d. Enter the address of the startup url in the **url** field.

Step 17 To configure storage:

a. Choose **browser > storage** > **enabled**.

b. Check or uncheck the **enabled** check box to specify whether local storage is enabled.

c. Choose **browser > 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 **browser > 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 **browser > storage** > **html5** > **enabled**.

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

Step 18 To set a web page, enter an address in the **url** field.

Step 19 Click **Apply**. Or if you don't want to keep all the settings, click **Cancel**.

Step 20 In the Predefined actions menu, click **Reboot**.

Step 21 In the Reboot Devices Dialog Box, click **Ok**. **Step 22** Click **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.

Step 3 Enter the address of the startup url in the **url** field.

Step 4 Click **Apply**.

Step 5 In the Predefined actions menu, click **Reboot**.

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

Step 7 Click **Cancel**.

Setting the Clock and Synchronizing NTP Servers

The clock on a Moderro IEC4600 Series can be manually set or synchronized using NTP from the Moderro 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.

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** Click **Apply**. If you don't want to make those changes, click **Cancel**.

Step 12 In the Predefined actions menu, click **Reboot**.

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

Step 14 Click **Cancel**.

Adjusting theDisplay

The video displays connected to IECs can be managed remotely thru the Moderro 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.

Step 3 From the master drop-down list, choose the master display input.

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

Step 5 From the mode drop-down list, choose the screen resolution.

Note Starting with release 2.2, the custom resolution setting in the IEM was changed to force the IEC to output a custom resolution if a custom resolution is set in IEM. The IEC will display the custom resolution even if the connected display does not support that resolution. This new behavior prevents the IEC from changing its resolution to the lowest resolution if the IEC cannot get a supported resolution from the display or if it does but the custom resolution is not the monitor's supported resolution.

Step 6 From the rotation drop-down list, choose the display rotation.

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**.

Step 10 Click **Cancel**.

Creating Emergency Messages

Emergency messages can be displayed across the Moderro 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.

Step 3 Enter text in the **message** field.

Step 4 Click **Apply**.

Enabling Trusted Sites for the Flash Player

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:

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

Step 2 Click the **Right Arrow** to expand the Flash player settings.

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

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

Step 5 In the trustedsites value, click the button.

Step 6 In the List of web sites dialog box, click +.

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**.

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

Step 12 Click **Cancel**.

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.

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**.

Step 7 In the Predefined actions menu, click **Reboot**. **Step 8** In the Reboot Devices Dialog Box, click **Ok**.

Step 9 Click **Cancel**.

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.

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**.

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

Step 13 Click **Cancel**.

Adjusting the Mouse

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

Note The default value of the mouse.cursor.visible property is 'Hide mouse cursor'.

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.

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

Step 10 Click **Cancel**.

Managing Power Modes

The Moderro 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.

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**.

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

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.

Step 4 Click **+** to add a printer.

Step 5 In the Printers configuration editor, click on the printer you just added.

Step 6 Change the name of the printer if desired.

Step 7 Enter the IP address of the printer.

Step 8 Enter the correct CUPS protocol: **usb** for a USB connected printer or **lpd** for a network connected printer.

Step 9 Enter the printer's queue.

Step 10 Select printer model.

Step 11 Click **Ok**.

Step 12 In the Predefined actions menu, click **Reboot**.

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

Enabling Profile Expiration

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

Step 1 Go to the **Policy** tab of a policy:

Step 2 Go to the **profile** property.

Step 3 Click the **Right Arrow** to expand the property.

Step 4 To enable this property, check the check box in the Value column.

Step 5 Click the green checkmark.

Step 6 Click **Apply**.

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

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

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 Go to the **network** > **proxy** property.

Step 3 Click the **Right Arrow** to expand the proxy settings.

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 **mode** 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**.

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

Managing Screen Shots

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.

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**.

Managing IEC's System SettingsMenu

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.

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**.

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

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

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.

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**.

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.

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**.

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

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

Enabling Services

Bluetooth 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.

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 SSH menu.

Step 7 Check the **enabled** check box to enable SSH service.

Step 8 Click **Apply**. If you don't want to make those changes, click **Cancel**.

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

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

Step 11 Click **Cancel**.

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.

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**.

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

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.

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**.

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

Step 8 Click **Cancel**.

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.

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 **muted** check box to mute or unmute the master channel.

Step 6 In the microphone field, choose the microphone volume.

Step 7 Click the **Right Arrow** to expand the microphone settings.

Step 8 Check or uncheck the **muted** check box to mute or unmute the microphone.

Step 9 Click **Apply**. If you don't want to make those changes, click **Cancel**.

Step 10 In the Predefined actions menu, click **Reboot**.

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

Step 12 Click **Cancel**.

Enabling VNC for IECs

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".

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.

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.

Note 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".

Configuring Policies

Last Revised: October 27, 2016

Chapter Overview

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 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
  - Policy Hierarchy
  - Persistent Policies
  - Runtime Policies
  - Persistent vs. Runtime vs. Persistent Runtime Policies
  - Accessing Policies
  - Creating New Policies
  - Copying Policies
  - Exporting Policies
  - Importing Policies
  - Applying Policies
  - Deleting Policies
  - Policy Properties
- Policy Scheduling
  - Creating a Schedule
  - Applying a Schedule to a Policy
  - Sample Scenario 1
  - Sample Scenario 2
  - Effective Profile
  - Deleting Schedules

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

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.

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.

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

Runtime Policies

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.

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.

Note It is recommended that you do NOT set overlapping schedules for runtime properties on a device or on a group of devices.

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 Policies

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

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

Step 1 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**.

The Create New Policy dialog box opens.

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.

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

Step 7 Click **Create**.

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

Step 8 Click on the new policy to open it.

Step 9 Click on the **Policy** tab.

Step 10 Configure the properties. (See Chapter 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.

Note 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.

Step 3 In the Edit menu, click **Copy Policy**.

Figure 6-1 Copy Policy Button

The Copy Policy to Account dialog box opens.

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

Step 5 Click **Copy**.

Exporting Policies

Export a Single Policy

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

Step 1 Click **Policies**.

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

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

Step 4 In the Opening Policy dialog box, choose the **Save File** radio button.

Step 5 Click **OK**.

The file is downloaded to your computer.

Export Multiple Policies

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.

Step 4 Click **OK**.

The file is downloaded to your computer.

Importing Policies

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

Step 1 Click **Policies**.

Step 2 In the Edit menu, click **Import Policy**.

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

Step 4 Choose the file on your computer then click **Open**. The file name then appears in the Import dialog box.

Step 5 Click **Upload**.

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

Tip If a file uploaded is the wrong file or there is an error uploading it, delete that file. To delete the file, choose the file and then click **remove**.

Step 6 Click **Close**.

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.

Step 3 Click the **Policies** tab.

Step 4 In the Available policies list, choose a policy.

Step 5 Click the **Green Arrow**.

The policy now appears in the Applied policies list.

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

Tip 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**.

Deleting Policies

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**.

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.

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

PolicyScheduling

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.

Note If the new policy has display in standby, it should go in standby upon policy load however.

Tip Since the IEC will reboot to pick up the new policy, it is best not to schedule a policy change during business hours when customers could be standing in front of the kiosk. If you want to display different content, use runtime policies or build that change into the application so that the transition is seamless to the customer.

Q. How do IECs get notified of the schedule change?

A. IECs ping the IEM with a heartbeat and in response receive commands from the IEM if any. In the case where a schedule change is due, the IEM will instruct the IEC to reboot if the policy applied is non-runtime; upon reboot the IEC will receive the current profile as determined by the schedule.

Q. How can content on the screen change or an action be performed without the IECs rebooting each time the policy changes?

A. If you apply runtime policies rather than persistent policies, the IEC will not reboot when it applies a runtime policy.

Note The runtime policy must only contain runtime or persistent runtime properties in order for it not to reboot. If you create a runtime policy that contains persistent properties, for example debug panel, the IEC will reboot.

Tip Create a runtime policy to turn off the displays at night. This runtime policy will not reboot the IEC first before turning off the displays.

Q. How will the IEM compensate for the various time zones where the IECs might be located?

A. The IEC sends a timestamp with every heartbeat. The IEM will use the timestamp from the IEC to determine the scheduled policy change. This time value will already be adjusted for the time zone per IEC settings.

Creating a Schedule

To create a schedule, follow these steps:

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

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

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

Step 4 Click **+** to add an item.

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

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.

Step 9 Click **Ok**.

Step 10 Add more schedule items as needed.

Step 11 Click **Create**.

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.

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.

Note 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.

Step 5 Choose a schedule from the 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 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.

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

Step 7 Move a policy by highlighting it and then clicking the gray up or down button to the right side 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.

Step 8 Click **Apply.**

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.

Step 4 Choose a future time on the 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.

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

Deleting Schedules

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.

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

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

Configuring Notifications

Last Revised: October 27, 2016

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
- Creating a Notification and Associating It with a User
- Deleting Notifications

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 *Moderro 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.

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

The Create New Notification dialog box opens.

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.

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.

Step 10 Click the **+** button to add a rule.

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

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.

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**.

A Notification icon appears in the center pane. 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.

Step 25 Click the Green Arrow to move the notification to the Applied list.

Step 26 Click **Apply**.

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

Deleting Notifications

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 ServerSettings

Last Revised: October 27, 2016

Chapter Overview

This chapter explains how to modify server settings. The sections in this chapter are:

- Modifying Server Settings

Modifying ServerSettings

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

Note 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**.

Step 3 Check the **System log enabled** check box to collect logs from each of the IEC4600 Series devices.

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 Moderro 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.

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**.

Backing Up and Restoring the Server

Last Revised: October 27, 2016

Chapter Overview

This chapter explains how to perform maintenance activities. The sections in this chapter are:

- Backing up the Server
- Restoring the Server

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

Tip 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.

Note The Backup and Restore process only works with same version (e.g. 2.3) 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**.

Step 3 Click **Backup**.

Warning **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.

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**.

Warning **The Restore operation can be dangerous to the system.**

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.

Auditing

Last Revised: October 27, 2016

Chapter Overview

This chapter explains how to access and use the Audit feature. The sections in this chapter are:

- Audit
  - Sort Changes
  - Filter Changes

Audit

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.

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.

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. 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.

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

To clear the filter, click the X button.

Proxy Support

Appendix Overview

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

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, "*nfl*")) {
                return "PROXY 192.168.200.24:3128";
         }
    }
```

Step 3 Modify the script based on the number of proxy servers.

Note 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.

Step 4 Click **Create**.

Step 5 In the center pane, select the policy that you just created by double clicking the icon.

Step 6 Click the **Policy** tab.

Step 7 In the Policy tab, enter **proxy** in the Filter field.

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.

Step 4 Click **Create**.

Step 5 In the center pane, select the policy that you just created by double clicking the icon.

Step 6 Click the **Policy** tab.

Step 7 In the Policy tab, enter **proxy** in the Filter field.

Step 8 Go to the **network > proxy > autoconfig > script** property.

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.

Step 4 Click **Create**.

Step 5 In the center pane, select the policy that you just created by double clicking the icon.

Step 6 Click the **Policy** tab.

Step 7 In the Policy tab, enter **proxy** in the Filter field.

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**.

Step 13 Apply this proxy policy to an IEC device.

Step 14 Reboot the IEC device to activate the policy on the device.

Last Revised: October 27, 2016

9.11.17