Cisco EnergyWise Orchestrator Administrator Guide

Cisco EnergyWise Phase 2
June 2010

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

Text Part Number: OL-19816-01

Cisco EnergyWise Orchestrator Administrator Guide

CONTENTS

Preface ix

Document Conventions ix

Related Publications x

Obtaining Documentation and Support on the Cisco Developer Network xi

Obtaining Documentation, Obtaining Support, and Security Guidelines i-xii

CHAPTER 1 **Introduction to Cisco EnergyWise Orchestrator** 1-1

Overview 1-1

Cisco EnergyWise Orchestrator 1-1

Orchestrator Features 1-1

Configuring Power Management in Orchestrator 1-2

Orchestrator System Components 1-3

Cisco EnergyWise 1-5

PC Power States and Sleep 1-5

Getting Started with Power Management 1-6

Open the Administrator console 1-7

CHAPTER 2 **Managing Administrative Groups** 2-1

Overview of Administrative Groups 2-1

Strategies for Creating Groups 2-1

Configuring Administrative Groups 2-2

Creating Administrative Groups 2-2

Assigning Devices to Groups 2-2

Configuring Group Assignment Rules 2-3

CHAPTER 3 **Security and Permissions in the Orchestrator System** 3-1

Configuring Permissions for Delegated Administration 3-1

Overview of the Orchestrator Security Model 3-1

Using Roles for Delegated Administration 3-1

Permissions Categories 3-2

Granting Root Administrator Permissions 3-2

Creating Additional Security Roles and Grant Permissions 3-3

Administrative Permissions and Descriptions 3-4

Permission Types 3-4
Global Permissions 3-4
Group-Level Permissions 3-5
Effective Permissions 3-5
Configuring Windows Firewall To Allow Server Access to Web Components 3-6

CHAPTER 4 **Managing and Viewing Devices** 4-1
Understanding Device Management 4-1
Configuring Devices for Cisco EnergyWise 4-2
Devices, Policies, and Power Level Settings 4-2
Device Connections and Check-Ins 4-2
Devices Checking In 4-3
Devices and Groups 4-5
Viewing Device Information 4-5
Device Properties and EnergyWise Attributes 4-6
Power States and Activity 4-6
Device Charts 4-7
Device Attributes and Properties 4-7
Displaying Device Information 4-14
Viewing Devices and Attributes 4-14
Excluding Interfaces from the Device List 4-15
Excluding Unlicensed Devices from the Device List 4-15
Managing Devices 4-16
Assigning Devices to Groups 4-16
Assigning Policies to Devices 4-17
Controlling Devices Directly 4-17
Setting Device Properties and Attributes 4-18
Removing a Device from the System 4-19

CHAPTER 5 **Managing Policies** 5-1
Policies 5-1
Baseline Mode and Operational Mode 5-2
Setting Up New Policies 5-2
Policy Inheritance 5-4
Strategies for Creating Policies 5-4
Recurrence Settings 5-6
Power State Changes 5-7
Configuring Policies 5-7

Setting New Policies 5-7
Creating and Editing Policies 5-8
Configuring Policy Assignment Rules 5-10
Disabling a Policy 5-11
Enforcing Policies 5-11
Using Power Schemes 5-12
Power Schemes 5-12
Default Power Schemes in Orchestrator 5-13
Creating and Editing Power Schemes 5-14
Creating and Editing Power State Change Rules 5-14

CHAPTER 6 **Waking Computers** 6-1
Waking Clients Through the Server 6-1
How End Users Wake Their Computers 6-2
Determining Whether a Computer Can Wake from Standby 6-2
Configuring the Mouse or Keyboard to Wake the Computer 6-2
Configuring the Mouse or Keyboard to Wake the Computer Using the Administrator Console 6-3
Changing Wake Settings 6-4
Using Wake on WAN to Wake Clients Across the Network 6-5
Wake on WAN Overview 6-5
Configuring Client Computers for Wake on LAN 6-6
Enabling Policy Wake on WAN Settings 6-7
Setting a Device As a Preferred Wake on WAN Proxy 6-8
Setting the Wake on WAN Proxies Per Broadcast Domain 6-8
How Orchestrator Selects Wake on WAN Proxies 6-10
Waking Selected Devices 6-11
Waking Clients on a Regular Schedule 6-11
Wake from Sleep or Wake from Off 6-12
Wake Settings 6-13
Basic Settings 6-13
Advanced Settings 6-13
Wake on WAN Settings 6-14

CHAPTER 7 **Viewing Reports** 7-1
Overview 7-1
Data Summarization Process Overview 7-1
Global Settings and Summarization 7-2
Scheduling the Process 7-2

Running the Summarization Process 7-3
Running the Data Summarization Process Manually 7-3
Running the Data Summarization Process as a Scheduled Task 7-3
Resetting Summarization Data 7-4
Viewing the Operational State Report 7-5
Viewing the Events Summary Report 7-6

CHAPTER 8 **Getting Diagnostic Information from Event Logs** 8-1
Data Tention in Device Logs 8-1
Event Categories and Types 8-1
Data Retention 8-3
Log File Locations 8-3
Server File Locations 8-3
Specifying Server Logging Levels and File Sizes 8-4
Displaying Event Data in the Administrator Console 8-6

CHAPTER 9 **Sustainability Dashboard** 9-1
About the Sustainability Dashboard 9-1
General Steps for Installing, Configuring, and Deploying the Dashboard 9-2
System Components 9-4
Tasks, Roles, and Required Skills 9-6
Configuring and Deploying the Dashboard 9-7
Considerations 9-7
Viewing the Sustainability Dashboard 9-8
Troubleshooting 9-10
Global Settings for Dashboard Reports 9-11
Metadata and Summary Tables Used by the Dashboard 9-15
Deploying the DashboardApp.swf File 9-17
Chart Types and Filters 9-21
Charts in the Default Configuration 9-21
Viewing Energy Savings for PCs 9-24
Two Time Period Configuration 9-26
Change Filter Settings 9-27
Date Filter Settings 9-27
Date Grouping Options 9-29
Data Group Settings 9-29
Display Members of Data Groups 9-29
Sustainability Dashboard Reports 9-30

Data Availability Report 9-30
Baseline Report 9-31

CHAPTER 10 **Troubleshooting** 10-1
Power Management Processor Is Not Running 10-1
Pressing Power Button Does Not Wake Computer 10-2
Detecting the Hardware Issue 10-2
Updating the Hardware Does Not Resolve the Issue 10-2

APPENDIX 11 **Important Notice** 11-1
Disclaimer 11-1
Statement 361—VoIP and Emergency Calling Services do not Function if Power Fails 11-1
Statement 1071—Warning Definition 11-3

Preface

Document Conventions

Command-line interface (CLI) syntax descriptions use these conventions:

- Commands and keywords are in **boldface** text.
- Arguments for which you supply values are in *italic*.
- Square brackets ([ ]) mean optional elements.
- Braces ({ }) group required choices, and vertical bars (|) separate the alternative elements.
- Braces and vertical bars within square brackets ([{ | }]) mean a required choice within an optional element.

Interactive examples use these conventions:

- Terminal sessions and system displays are in `screen` font.
- Information that you enter is in **`boldface screen`** font.
- Nonprinting characters, such as passwords or tabs, are in angle brackets (< >).

Interactive examples use these conventions:

Note Means *reader take note*. Notes contain helpful suggestions or references to materials not contained in this manual.

Tip Means *the following information will help you solve a problem*.

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Warning

IMPORTANT SAFETY INSTRUCTIONS

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device. Statement 1071

SAVE THESE INSTRUCTIONS

Related Publications

- *Cisco EnergyWise Configuration Guide, EnergyWise Phase 2* on Cisco.com
- *Cisco IOS Release Notes for Cisco EnergyWise, EnergyWise Phase 2* on Cisco.com
- Documentation for the software release running on your device: http://www.cisco.com/cisco/web/support/index.html.

For Cisco EnergyWise partner documentation: http://developer.cisco.com/web/esdk/home.

- *Cisco EnergyWise Documentation Roadmap*
- *Cisco EnergyWise Partner Development Guide*
- *Cisco EnergyWise Programmer Reference Guide for the End Point SDK*
- *Cisco EnergyWise Programmer Reference Guide for the Management API*
- *Cisco IOS Release Notes for the Cisco EnergyWise Configuration Guide, EnergyWise Phase 2*

Obtaining Documentation and Support on the Cisco Developer Network

Cisco partners can access the EnergyWise documents, API and SDK software code, and Cisco IOS software by joining the Cisco Developer Network at http://developer.cisco.com/web/esdk/home.

You must have a support contract and license to access EnergyWise resources on the Cisco Developer Network and on TAC. The business development manager who registered your license must set your Cisco.com account with the appropriate access privileges.

The forum, wiki, and resources on the Cisco Developer Network provide a self-help knowledge base and community for EnergyWise application developers and programmers. You can get additional support by opening a case in the TAC Service Request Tool at http://tools.cisco.com/ServiceRequestTool/create/launch.do.

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

CHAPTER 1

Introduction to Cisco EnergyWise Orchestrator

- Overview, page 1-1
- Getting Started with Power Management, page 1-6
- Open the Administrator console, page 1-7

Overview

- Cisco EnergyWise Orchestrator, page 1-1
- Orchestrator Features, page 1-1
- Configuring Power Management in Orchestrator, page 1-2
- Orchestrator System Components, page 1-3
- Cisco EnergyWise, page 1-5
- PC Power States and Sleep, page 1-5

Cisco EnergyWise Orchestrator

- Measure—Orchestrator identifies the time that a device is in each power state and the usage data for PCs and EnergyWise-enabled devices (for example, IP phones, switches, routers, and wireless access points).
- Monitor and report—Data collected by Orchestrator is reported in charts and graphs that show device and user activity.
- Regulate—Orchestrator manages the power states of network-connected devices by direct commands and scheduled policies that you define.

Orchestrator Features

- Administration of device power states from a web-based administrator console.
- Device management in real time or by using automatic, policy-based control.
- Agent-based, nonintrusive PC power management that ensures zero impact to end users, business applications, or IT maintenance activity.
- Collection of usage information for PCs so that you can create power management policies.

- Remote access to PCs and Wake on LAN support for PCs. End users can wake Orchestrator client PCs from a remote location over the web and schedule wake requests to work around scheduled maintenance windows.
- Group-oriented administration with role-based security privileges.
- Event reporting for analysis and optimization. Events on devices are recorded and reported to a central server.
- Dashboard views for high-level reporting of environmental impact.
- Unified control of EnergyWise-enabled devices through network-based measurement of power draw and network-based control of device power levels. (Requires EnergyWise-enabled network hardware and Power over Ethernet [PoE] devices.)

Configuring Power Management in Orchestrator

Power management is the ability to move devices into appropriate power states as demand requires by putting devices into the right power state for your needs. For example, **on** is often the right power state for a device. Successfully waking a computer at the correct time is just as important as putting it to sleep at the right time.

The first step is to determine how you want to enforce power management in your network by determining how energy is being used.

A *device* can be a PC, or EnergyWise-enabled router, switch, IP phone, or wireless access point (WAP).

Orchestrator runs in two modes: Operational and Baseline. Operational mode enforces policies. Baseline mode only measures energy use.

- In Operational server mode, Orchestrator uses *policies* to manage network-connected PCs. A policy can be assigned to one or more devices in any group.
- In Baseline mode, Orchestrator collects data for all devices as each device connects to the system. The data updates each time a device checks in. You can see this data in different reports and device views.

Policies settings:

- Scheduled PC power schemes that specify the length of time that a user is inactive before a device transitions to a lower power state. Each scheme can have a unique schedule.
- An unscheduled PC power scheme that runs in the background when no other power schemes are scheduled.
- Scheduled power level changes (such as wake, shut down, sleep, or restart), each with a unique schedule. Power-level changes apply to PCs or PoE devices.
- PC wake-up settings.
- Logging and monitoring settings for PC clients.

Orchestrator assigns policies manually, or you can create assignment rules. Each device can have only one assigned policy, but each policy can have multiple schemes and power level changes, each with its own schedule.

Note All power settings in policies apply to PCs. For other types of devices, only scheduled power state changes apply. Orchestrator collects data for all device types for reporting purposes.

Devices can be assigned to administrative groups, either manually or through assignment rules that you create. You can use groups to organize devices logically and to apply role-based permissions for delegated administration.

Orchestrator System Components

Figure 1-1 shows the Orchestrator components before integration with Cisco Energywise.

Figure 1-1 Orchestrator System Components

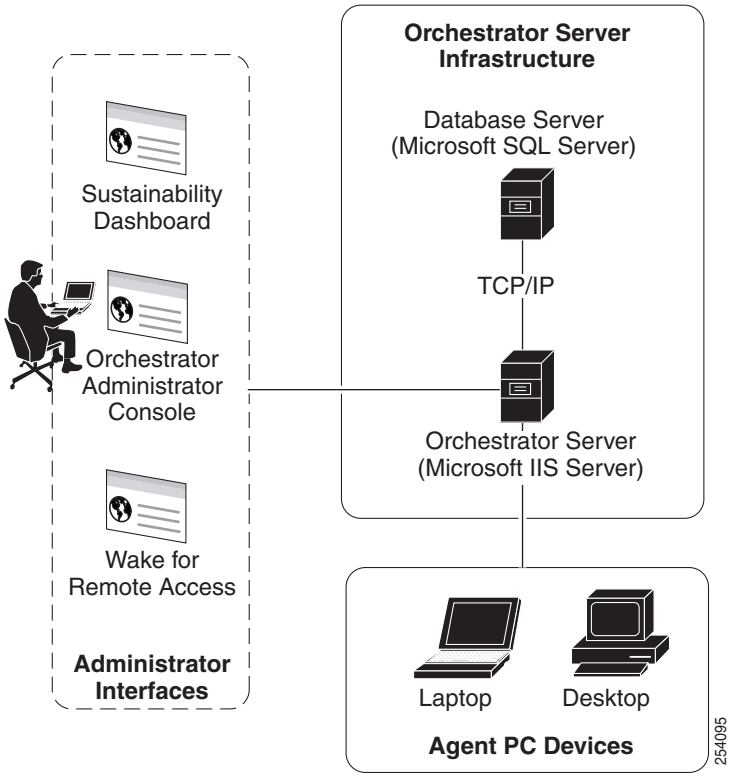


Figure 1-2 show the same Orchestrator components after integration with Cisco EnergyWise devices:

Figure 1-2 Orchestrator System Components for EnergyWise Devices

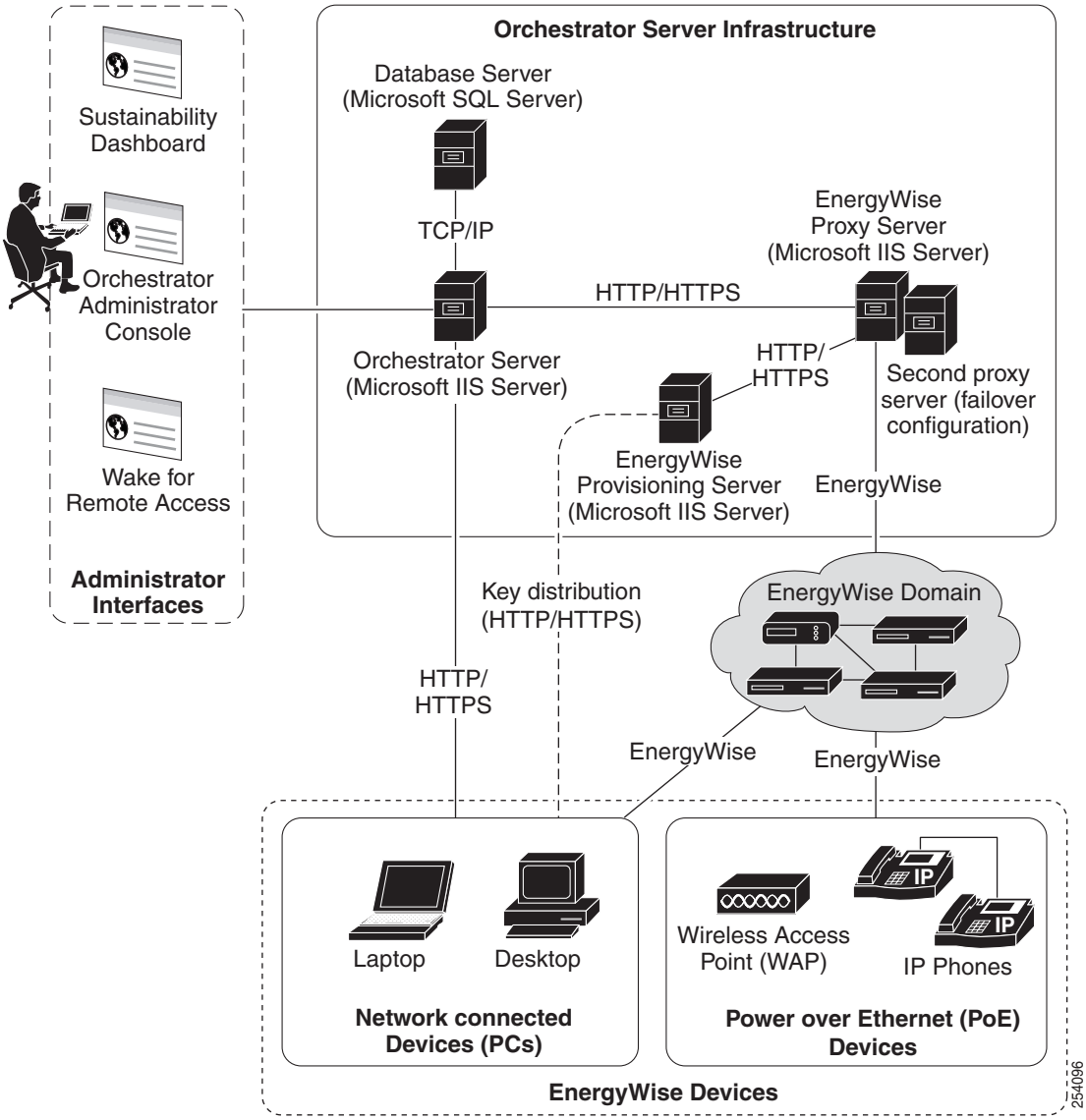


Table 1-1 Orchestrator System Components for EnergyWise Devices

Component	Description
Orchestrator server	Manages policy distribution, sends power-state change instructions to devices, and captures data to send to the Orchestrator database. The Orchestrator server communicates directly with PCs and indirectly with EnergyWise-enabled devices through the EnergyWise proxy server.
Enterprise power management database	An Microsoft SQL server database that stores power state and other device data sent to the server.

Table 1-1 Orchestrator System Components for EnergyWise Devices (continued)

Component	Description
Administrator web server	A computer running Microsoft IIS 6.0. The administrator console is a Web application hosted on an IIS server. You use the administrator console to • Configure and schedule power state changes. • Add, arrange, remove, and monitor devices. • Manage and delegate permissions. • Perform other management tasks.
EnergyWise proxy server	A bridge between the Orchestrator server and the EnergyWise protocol. The proxy service acts as a proxy for EnergyWise devices to the Orchestrator server. It polls EnergyWise attributes (such as device and power usage information), sending EnergyWise commands, and sending EnergyWise status to the Orchestrator server.
EnergyWise provisioning server	Manages the assignment of EnergyWise domains to instances of the EnergyWise Proxy Service.
Agent PC devices	Desktop and laptop PCs (sometimes referred to as clients) that receive and enforce power management instructions from the Orchestrator server.
PoE devices	Network connected devices that support the Cisco EnergyWise protocol, such as Catalyst Power over Ethernet (PoE) switches, all Cisco PoE IP phones and wireless access points. Each device in an EnergyWise domain is called an end point.

Note In a basic installation, the Proxy Service and Provisioning Service can run on the same system as the Orchestrator Power Management Server. In large installations, multiple power management servers and proxy servers can provide load balancing.

Cisco EnergyWise

Orchestrator supports EnergyWise Phase 2. You can configure Orchestrator to recognize IP phones and wireless access points) that are connected to Cisco network devices.

For Cisco-specific information, see the EnergyWise configuration and deployment guides on Cisco.com.

For a list of supported devices, see the *Release Notes for Cisco EnergyWise, EnergyWise Phase 2* on Cisco.com.

PC Power States and Sleep

Orchestrator monitors these PCs power states: *on*, *idle*, *sleep*, *hibernate*, and *off*.

When a PC is on and being used, it consumes 60 to 250 W. You can put it into low-power states:

- Sleep (also called standby)—Uses the least amount of power while the computer is on. Open programs or documents stay open when the computer is in sleep mode.

- Hibernate—Saves open documents to the disk, closes programs, and turns the computer off.
- Off—All programs are closed, the operating system is shut down, and the computer is powered off.

Getting Started with Power Management

You can use the Orchestrator Administrator console to determine the energy use of network devices and to set policies with scheduled power schemes to enforce power management.

You can set up administrative groups and power-management policies in any order. You can define security groups first to control administrative permissions and access to network devices and power management settings.

	Task	Description
Step 1	In your web browser, enter the URL for the local web site on the computer where you installed the Orchestrator server, such as http://hostname/Admin/ where hostname = Orchestrator power management server name. For details, see the "Open the Administrator console" section on page 1-7.	Open the Administrator console to see and manage devices, groups, policies, and server settings.
Step 2	In the Devices menu, choose **Filtered Search**, and click the Groups, Policies, or PC Subnets tab to filter the view. Or, in the Search tab, choose different options in the drop-down filter lists to show sets of devices.	Display devices to get an overall picture of connected devices. Use different filtering and sorting options to see different sets of devices.
Step 3	In the Devices menu, choose **Manage Groups**.	Create groups organize to control access to devices.
Step 4	In the Devices menu • To manually assign devices to specific groups, choose **Filtered Search**. • To automatically assign devices to specific groups, choose **Configure Group Assignment Rules**.	Assign devices to administrative groups manually or through assignment rules.
Step 5	(Optional) To configure security settings, in the Permissions menu, choose **Edit Roles**.	(Optional) Configure security settings to control administrator access to devices and policies.
Step 6	Determine initial policy settings from user and system activity. For details, see the "Gathering Data for and Creating Initial Power Management Policies" chapter in the *Cisco EnergyWise Orchestrator Installation Guide* and the "Data Availability Report" section on page 9-30.	Run Orchestrator in Baseline mode for 2 weeks to monitor energy usage and determine policy assignment. **Note** To display data for the Operational State report, you must first run the summarization process. For details, see the "Data Summarization Process Overview" section on page 7-1.

	Task	Description
Step 7	In the Policies menu, choose **Edit Policies**. Use the tabs and buttons to control the policy settings and schedule including schemes, power level changes, and power state transition rules.	Determine the policies for enforcing power management. Change or create policies.
Step 8	In the Devices menu, choose **Filtered Search** for manual assignment. Choose **Configure Policy Assignment Rules** to automatically assign policies to devices.	Assign policies to devices manually or through assignment rules.
Step 9	In the Server menu, choose **Configure Server Settings**. For Server mode, choose **Operational**.	Begin policy enforcement by setting Orchestrator to Operational mode.
Step 10	In the Reports menu, choose a report type or event view.	Review reports on user and device activity.

Open the Administrator console

You use the Orchestrator Administrator console to configure and schedule power state changes; add, arrange, remove, and monitor devices; manage and delegate permissions; and perform other management tasks.

In your web browser, enter the URL for the local web site on the computer where you installed the Orchestrator server, such as **http://*hostname*/Admin/default.aspx** where *hostname* = Orchestrator power management server name.

For example, **http://localhost/admin/default.aspx** or **http://myPCname.myDomain.local/admin/default.aspx**.

Note If Windows Firewall is enabled on the Orchestrator server, you will need to make sure v TCP port 80 is added to the exceptions list. For details see the "Configuring Windows Firewall To Allow Server Access to Web Components" section on page 3-6.

CHAPTER 2

Managing Administrative Groups

- Overview of Administrative Groups, page 2-1
- Strategies for Creating Groups, page 2-1
- Configuring Administrative Groups, page 2-2
- Assigning Devices to Groups, page 2-2
- Configuring Group Assignment Rules, page 2-3

Overview of Administrative Groups

Groups in Orchestrator provide:

- A mechanism for role-based system security for assigning group-level permissions and control administrator access to devices. For details on role-based security and group-level permissions, see the "Configuring Permissions for Delegated Administration" section on page 4-1.
- A logical way for you to organize the devices in the system to access and manage sets of devices.

Devices can be assigned to groups, either manually or by your assignment rules (**Devices > Configure Group Assignment Rules**). Policies and groups have no direct relationship. You can assign policies to devices but not to groups.

You create groups on the Manage Groups page (**Devices > Manage Groups**). When you create a group, you can specify a parent group to create nested groups.

Orchestrator provides a root device Power management group and a Default group. New devices connected to the server and that do not meet your group assignment rules appear in the Default group.

Strategies for Creating Groups

When you create groups for devices, you should consider how you plan to apply security and role-based permissions for the groups.

You might create groups based on geographic location or on a particular business function, such as distributed administration. For example, you could create a Help Desk group that can wake or restart PCs as needed.

You can identify your security needs and groups during the 2-week period when Orchestrator is running in baseline mode.

After you set up your initial security groups, you can then set assignment rules so that PCs and other devices are placed into groups as you add them to the system. For details, see the "Configuring Group Assignment Rules" section on page 2-3.

Configuring Administrative Groups

- Creating Administrative Groups, page 2-2
- Assigning Devices to Groups, page 2-2
- Configuring Group Assignment Rules, page 2-3

Creating Administrative Groups

Step 1 From the Device menu, choose **Manage Groups**.

Step 2 Click **New Group**.

Step 3 Enter a name for the group, a description, and select a parent for the group.

Step 4 Click **Save**.

Assigning Devices to Groups

You can assign devices to groups manually from the device list or automatically by using group assignment rules.

For details on group assignment rules, see the "Configuring Group Assignment Rules" section on page 2-3.

For details on creating groups, see the "Configuring Administrative Groups" section on page 2-2.

Follow these steps to assign groups:

Step 1 On the Devices menu, choose **Filtered Search**.

Step 2 Click the tab Groups, Policies, or Subnets and select a filter option to see the results in the device list.

You can also click the Search tab, select different options in the device filters to display a set of devices, and enter a search string.

Step 3 Click the Search button to see the device list.

Step 4 Select the device or devices in the list.

Step 5 On the Move to Group menu, click **Manually Assign Group** or **Use Group Assignment Rules**.

Note When you manually assign a policy to a device, it is flagged as a manual assignment. To clear the flag, select the device from the device list. On the Move To Group menu, click **Use Group Assignment Rules**.

If you choose Use Group Assignment Rules and one or more of the selected devices had been manually assigned, select **Include N manually assigned devices** and click **OK** to confirm the change from a manually assigned group to rule-based assignment.

Step 6 For manual assignment, click the group name, and click **OK**.

Step 7 For rule-based assignment, click **OK**.

Configuring Group Assignment Rules

After you create groups, you can configure Orchestrator to place new devices into the appropriate groups when the devices connect to the server.

When you configure group assignment rules, devices are automatically assigned to specific groups based on a set of criteria. Because the rules that you set for automatically assigning devices to a group are saved as a set, their order is important and you will need to consider the best order to get the results you want.

You can choose the rule-set automatically only when new devices connect or for all connections. Rules run when a device wakes or when the device moves from one network card to another, such as a PC moving from a network line to a wireless connection.

Each rulehas a set of criteria that a device must meet to be placed into the group. When you connect new devices to the server, only the devices complying with the criteria of a group are placed in that group.

For example, you can create a rule for a Training Lab group that accepts clients only from a particular IP segment and with the string *train* in the DNS names.

Note If a device does meet the criteria in a specific rule, the device is placed into the specific group having that rule. If a device does not meet any of the criteria in the rule, the device is placed into the Default group.

Step 1 From the Devices menu, choose **Configure Group Assignment Rules**.

Step 2 Click **New Rule**. Enter a name and a description for the rule, and select the name of the group to be assigned when the rule runs.

Step 3 As you add other criteria, you can click the **Test Conditions** tab to see the results.

Step 4 Specify when to enforce the rule:

- When all criteria are met.
- When any criteria is met.

Step 5 Click **Done**.

Step 6 Specify when the rule runs automatically.

- When new devices connect to the server.
- When all devices connect to the server.

Note If you select *All connections*, the rules run when a computer wakes up or when it moves from one network card to another (such as from a network line to a wireless connection).

Step 7 Click **Save Rule Set** to save all changes.

Step 8 Order rules by selecting a rule in the set and clicking **Move Up** or **Move Down**.

CHAPTER 3

Security and Permissions in the Orchestrator System

- Configuring Permissions for Delegated Administration, page 3-1
- Granting Root Administrator Permissions, page 3-2
- Creating Additional Security Roles and Grant Permissions, page 3-3
- Administrative Permissions and Descriptions, page 3-4
- Configuring Windows Firewall To Allow Server Access to Web Components, page 3-6

Configuring Permissions for Delegated Administration

You can configure different levels of access to the Orchestrator network. This section describes its role-based security and permissions model.

Overview of the Orchestrator Security Model

Orchestrator uses a role-based approach to security:

- Roles are created for sets of permissions required to access particular administration tasks.
- To grant users access, add them to the roles that have the required permissions.
- The Windows user or group has no direct relationship with the Orchestrator task or component. Instead, roles represent business functions, such as Help Desk or Policy Administrator.

Using Roles for Delegated Administration

A built-in *Root Administrator* role gives members of that role access to the Orchestrator network. Anyone who has local administrator permissions on the Orchestrator server has root administrator access level.

When setting up delegated administration, a member in the root administrator role uses the Administrator console to:

- Add users and groups to the built-in administrator role.
- Create security roles for specific permissions sets.

- Configure system-wide or group-level permissions in the roles.
- Add users (or groups) to the roles and apply role permission sets to those users.

Permissions Categories

Security role categories:

- Global (server-wide)—Permission to manage a particular area of functionality across the entire Orchestrator network.
- Group level—Permission to perform specified management tasks on selected groups.

Security roles can have global, group, or both types of permissions. For example, the built-in Policy Administrator role has Manage policies (global) permission by default. You can also give this role Apply policies permission for specific groups.

For information about each setting and creating effective permissions, see the "Administrative Permissions and Descriptions" section on page 3-4.

Granting Root Administrator Permissions

A user or group that has root administrator permissions is granted access to all tasks and groups in the system.

Follow these search guidelines:

- Search results return users and groups that contain the search string that you enter. Wildcard characters * and ? are treated as text characters.
- Search operations are case insensitive for domain users and case sensitive for local users. For example:

  Searching for *admin* returns:

  - DOMAIN\Admin2 (domain user)
  - DOMAIN\Administrator (domain user)

  Searching for *admin* returns:

  - DOMAIN\Admin2 (domain user)
  - DOMAIN\Administrator (domain user)
  - BUILTIN\Administrators (local group)
  - Administrator (local user)

You must have local administrator permissions on the Orchestrator server computer to grant permissions.

Step 1 In the Administrator console, from the Permissions menu, choose **Edit Roles**.

Step 2 In the list of roles on the Configure Permission page, choose **Root Administrator**.

Step 3 On the Users tab, for each Windows user or group that you want toadd to the role, click **Add** to find and select the user.

Note Search operations are limited to the current domain, even if your user account has access to multiple domains. If you specify a different domain, the search returns a *user not found* message.

Step 4 When you are done adding users to the root administrator role, click **Save**.

Creating Additional Security Roles and Grant Permissions

To grant access to perform administrative tasks, create security roles, configure permissions sets for each role, and add users to the appropriate roles.

Before you complete this procedure, see the "Overview of the Orchestrator Security Model" section on page 3-1.

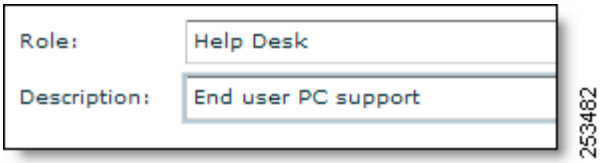
This procedure must be completed by a local administrator of the Orchestrator server who is also a member of the root administrator role in the Orchestrator Administrator console.

Step 1 In the Administrator console, from the Permissions menu, choose **Edit Roles**.

Step 2 On the Edit Roles page, click **New Role**, or select an existing role to customize or copy.

If you create, customize, or copy a role, give the new role a name and description (Figure 3-1).

Figure 3-1 Adding the Role Name and Description



Step 3 On the Users tab, for each Windows user or group that you want to include in the role, click **Add** to find and select the user.

Note Search operations are limited to the current domain, even if your user account has access to multiple domains. If you specify a different domain, the search returns a *user not found* message.

Step 4 Configure permissions for this role. For details about permission levels, see the "Administrative Permissions and Descriptions" section on page 3-4.

a. On the Device Groups tab, expand the tree to display the groups that you want this role to have access to, and select the appropriate permissions.

Note When you enable permissions on a group, they are also enabled on its subgroups.

b. If you want this role to have access to policies or group assignment rules across the entire system (independent from group-level permissions), on the Global Permissions tab, check the appropriate check box.

Omit this step when granting only group-level permissions.

Step 5 When you complete assigning permissions, click **Save**.

Administrative Permissions and Descriptions

This section describes the permission types that you can enable across the system or on specific device groups to set up an administration environment.

- Permission Types, page 3-4
- Global Permissions, page 3-4
- Group-Level Permissions, page 3-5
- Effective Permissions, page 3-5

Permission Types

You can assign permission types to roles that you create in the Administrator console:

- Global (server-wide)—Permission to manage a particular area of functionality across the Orchestrator system.
- Group level—Permission to perform specified management tasks on selected groups.

For example, a Policy Administrator role can have permission to create and edit policies across the system but not to apply policies to devices. A Help Desk role might only have permission to change the power state of devices in specific groups.

Global Permissions

In the Administrator console, you can give administrative permissions across the Orchestrator system.

- Manage policies—Create a new power management policy; modify any component of an existing policy, including scheduling schemes, power state transitions and policy assignment rules; and give permission to delete policies.
- Manage group assignment rules—Create, modify, or delete group assignment rules and criteria that move devices from one organizational tree location to another.

Global permissions expand the access of a role to some group-level tasks. See the "Effective Permissions" section on page 3-5.

Caution Global permissions grant access to the selected area over the entire Orchestrator system. If you use these permissions, consider your changes carefully. Evaluate how the changes would affect existing policies and devices.

Group-Level Permissions

Note Permissions that you enable on a group are inherited by all of its subgroups.

Table 3-1 Group-Level Permissions

Permission	Allowed Access Level
Manage group	Adds, deletes, and edits settings on groups or subgroups and removes devices from groups (for example, renaming a group or changing its parent). Does not give access to policies. You can move devices from one group to another when you have Manage groups permission for both groups. However, if you have Manage groups permission on the source group but not the destination group (as defined in the rule criteria), you can manually run group assignment rules for a set of devices.
Assign policy	Assigns policies to new devices and different policies to existing devices. Does not give access to create, modify, or delete policies.
Change device state	Changes the power state of a device. For example, wake the device, and change it to standby mode.
Edit devices	Changes device properties, such as whether a device can receive a license, its description, and EnergyWise properties. Does not give access to policies.

Effective Permissions

If a user is a member of multiple roles, the effective permissions that the user has on a group is the set that provides the highest level of access. This is true whether or not the role is given permissions directly on the group or indirectly through inheritance from an ancestor group.

Sometimes global permissions for an area can effectively expand group-level permissions:

- *Assign policies* permission is granted at the group level. However, members of a role with global *Manage policies* permissions can change settings on existing policies or delete policies that are assigned to devices. Either is a form of policy assignment.
- Enabling the global permissions set *Manage group assignment rules* gives access to create rules that move any device to any location in the organizational tree. Moving devices among groups is a management task that can be done through this global permissions set even if the *Manage group* permission is not enabled at the group level.

Configuring Windows Firewall To Allow Server Access to Web Components

If you use Orchestrator components that access the server through HTTP and Windows Firewall is enabled on the server, make sure that TCP port 80 is added to the exceptions list.

You need to access the server through HTTP to:

- Use the Sustainability Dashboard when the dashboard is not installed on the server computer.
- Enable Wake for Remote Access so that end users can wake their computers from off-site.

Tip Wake for Remote Access is an add-on component that comes with Orchestrator. See the *Cisco EnergyWise Orchestrator Wake for Remote Access Administrator Guide*.

- Administer the server from a remote computer, for example, as you would if you set up delegated administration.

Step 1 On the server computer, go to **Windows Start** menu > **Control Panel** > **Windows Firewall**.

Step 2 On the Exceptions tab, click **Add Port**.

Step 3 In the Add a Port dialog box:

a. Enter a name that shows that the exception is for power management components. This name appears in the exceptions list.

b. Specify port 80.

c. Select TCP.

Step 4 Click **OK**, and click **OK** in the Windows Firewall dialog box.

For additional information, see the *Add a Port to the Firewall Rules List* Microsoft TechNet topic.

CHAPTER 4

Managing and Viewing Devices

- Understanding Device Management, page 4-1
  - Configuring Devices for Cisco EnergyWise, page 4-2
  - Devices, Policies, and Power Level Settings, page 4-2
  - Device Connections and Check-Ins, page 4-2
  - Devices Checking In, page 4-3
  - Devices and Groups, page 4-5
  - Viewing Device Information, page 4-5
  - Device Properties and EnergyWise Attributes, page 4-6
  - Power States and Activity, page 4-6
  - Device Charts, page 4-7
  - Device Attributes and Properties, page 4-7
- Displaying Device Information, page 4-14
- Managing Devices, page 4-16

Understanding Device Management

A device in Orchestrator can be a PC or an EnergyWise-enabled router, switch, IP phone, or wireless access point (WAP).

Orchestrator collects data on all connected devices for reporting purposes. You can see how much energy is used by each device, why, and at what times of day users are most active.

Orchestrator begins collecting data for all devices as each device connects to the system. The data updates each time a device checks in.

Note The frequency for device check-in and how Orchestrator staggers check-ins is set in Server Configuration under Device check-in internal (Server menu).

On the Manage Devices page in the Administrator Console, you can:

- Display devices according to broad or specific search and filtering criteria.
- Control device power states and levels directly outside of a policy.

- Assign policies to devices.
- Assign devices to groups.
- Edit PC properties and EnergyWise device attributes.
- Manage Wake on WAN proxies.
- Run policy or group assignment rules.
- See reports on device activity and type, policy assignment, and group membership.

Configuring Devices for Cisco EnergyWise

Orchestrator recognizes EnergyWise devices based on the domains that you specify in the EnergyWise provisioning server configuration file.

For details on enabling EnergyWise devices in Orchestrator, see the "Configuring Orchestrator for EnergyWise devices" chapter in the *Cisco EnergyWise Orchestrator Installation Guide*.

Devices, Policies, and Power Level Settings

Each device can have only one assigned policy, but each policy can contain multiple schemes and power state changes, each with its own schedule.

Note Scheduled power schemes cannot overlap.

You can assign a policy to a device, either manually from the Assign Policies menu on the Manage Devices page or through assignment rules that you create (**Devices > Configure Policy Assignment Rules**).

Note All power settings in policies apply to PCs. For other types of devices, only scheduled power level changes apply. Orchestrator collects data for all device types for reporting purposes.

Outside of a policy, you can apply power state changes to any device and change EnergyWise device attributes or PC device properties either individually or as a set.

Device Connections and Check-Ins

When a device connects to the Orchestrator server for the first time, or whenever a device reestablishes contact with the server after being out of contact for a specified period of time, the server and client PC exchange a series of queries and responses referred to as a *handshake*. During a handshake, the server:

- Sends a query for the device GUID, netBIOS, MAC address, and policy version.
- Evaluates PCs as Wake on WAN proxies.
- Evaluates group and policy assignment rules.
- Compares its policy version with the policy version reported by the device.

PCs and EnergyWise devices (via the proxy server) send a message to the server the first time they connect to the Orchestrator server, or any time they attempt to reestablish contact with the server after being out of contact with the server for a period of time.

A PC will send this message when it: starts up, reboots, transitions out of sleep or a low power state to on, reestablishes network connectivity after being disconnected from the network (i.e., when the PC is out of contact with the server for any reason, for a period of time, and then reestablishes network connectivity).

Devices Checking In

PC devices check in with the Orchestrator server based on the *Device check-in interval* setting on the Configure Server Settings page. Each time the client checks in, the server records the time.

If a device misses two consecutive check-in times, the Orchestrator server marks the device as *Not checking in*. When the device checks in again, the Orchestrator server sets the device status to *Checking in*.

Note Whether a device is checking in or not is not related to its power state or whether the device is on or off. It is an indication that the device is communicating with the server.

In the case of EnergyWise devices, a device can be checking in even when it is at power level 0 (Off) because the device is still present in the EnergyWise domain.

When the EnergyWise proxy server is managing devices, a device is considered *Not checking in* if the proxy server is stopped, or if the proxy server polls a domain and the device is no longer present in the domain.

Table 4-1 describes the communication that takes place between Orchestrator and PC clients and EnergyWise devices when devices connect to, and check in, with Orchestrator.

Table 4-1 Check-In Actions

Action	Description
Connections (New and Reestablished)	• Device asks Orchestrator server what pieces of information it should send. • Orchestrator server asks the device to send the device GUID, netBIOS, MAC address, and policy version. Server receives the device GUID, NetBIOS, and MAC address values from the device and registers the device. For PCs, the server uses these values to determine if a PC is new, existing, or an imaged machine that has been replicated. • Server tells the device the check-in interval based on the interval setting in the Configure Server Settings page. **Note** There are three check-in interval settings: device check in, Wake on WAN proxy check-in, and EnergyWise proxy server check-in. Only the device check-in interval can be set on the Configure Server Settings page. The other settings are set in an Orchestrator configuration file. • Server assigns a new PC to a broadcast domain based on its new IP address. • Server evaluates a PC as a candidate for Wake on WAN proxy. • Server evaluates group and policy assignment rules. If the rule is set for *New connections only*, the server evaluates the rule only on first connection. If the rule is set for *All connections*, the server evaluates the rule every time the device reestablishes a connection with the server. • Server compares its policy version with the policy version reported by the device. If the device policy is out of date, the server sends an updated policy to the device.

Table 4-1 Check-In Actions (continued)

Action	Description
Check-ins (subsequent)	• Server tells the device its check-in interval. • Server records the check-in time and flags the device status as *Checking in* if it was previously *Not checking in*. • Devices with updated information, such as attribute changes, or power usage data, send this data to the server. • Server evaluates group and policy assignment rules if the rule is set for *All connections.* • Server evaluates PC clients as a candidates for Wake on WAN proxy. **Note** When a PC client that is a Wake on WAN proxy is flagged by the server as *Not checking in*, Orchestrator deselects that PC client from being a proxy and searches for a new Wake on WAN proxy. • Server compares its policy version with the policy version reported by the device. If the versions do not match and the device is checking in regularly, the server will send the latest policy information to the device. If a PC agent or device is not actively checking in, the server sends the latest policy information the next time the PC or device restarts or changes from a low power state and reconnects to the server.
Policy changes	Whenever a policy is modified, the server finds all devices that are assigned with that policy that are actively checking in. It then puts a policy change message into the server message queue for these devices the next time they check in or reconnect with the server (restarting or changing from a low power state).

Devices and Groups

You can assign devices to groups, either manually or through assignment rules that you create (**Devices > Configure Group Assignment Rules**). A device can only be assigned to one group at a time.

Viewing Device Information

All device attributes and information can be accessed on the Manage Devices page in the Administrator Console. You can display and search for any device, by group, by policy, by device family, or by PC subnet. All devices that meet the filter or search criteria appear in the device list.

Note By default, the device list displays the first 2000 devices that meet the search and filter criteria. If you need to see a larger set of devices, in the Server menu, click **Configure Server Settings**, and increase the *Max items per search result* value. The maximum value allowed is 20,000. Setting this value to a higher number can result in longer display times for search results.

- Click the **Customize View** button on the Manage Devices page to add columns or remove columns from the view.
- Change the order of columns by dragging a column to a new position in the list.

- Click the Charts tab to see a high-level picture of device activity and membership.

The chart data is based on the current result set of devices being viewed in the device list (2000 by default). For a representative sample of devices in the charts, you might need to increase the *Max items per search result* value on the Configure Server Settings page.

Click the **Reports** menu to display details on operational state, user activity, and event log information for devices.

Device Properties and EnergyWise Attributes

The Orchestrator server stores device properties and EnergyWise attributes for each device that connects to the server. (Some fields might not be populated for devices in some device families.) Some device attributes are created by the server, and some are reported by the device.

- The Orchestrator agent software reports attributes for PCs.
- The Orchestrator Proxy Server reports attributes for EnergyWise-enabled devices (switches, routers, IP phones, and wireless access points).

For a complete list of device properties and attributes, see the "Device Properties and EnergyWise Attributes" section on page 4-6.

For information on customizing the device list to show certain attributes and properties, see the "Viewing Devices and Attributes" section on page 4-14.

For details on changing device attributes or properties in Orchestrator, see the "Setting Device Properties and Attributes" section on page 4-18.

Power States and Activity

Orchestrator tracks different power states for PCs compared to other devices.

PCs:

- On
- Idle
- Sleep
- Hibernate
- Off

Monitors:

- Low power
- On
- Off

Orchestrator tracks user activity, including mouse clicks, keyboard touches, and any hard disk or processor activity.

Orchestrator tracks and enforces power state changes on PCs:

- Wake
- Sleep
- Hibernate

- Shut down
- Restart
- EnergyWise power levels that map to wake, sleep, hibernate, and shut down (if configured for EnergyWise support).

Note PC clients always respond to EnergyWise power levels set through the Administrator console.

Orchestrator tracks and manages power levels for EnergyWise-enabled devices (including PCs):

- Levels 3 to 10—Wake or On
- Level 2—Sleep
- Level 1—Hibernate
- Level 0—Shut down or Off

Note The default power level is 10. A Cisco switch does not support level 0. You cannot turn off the power to a switch.

Device Charts

The Charts tab on the Manage Devices page provides charts with high-level pictures of device activity and membership based on the current result set of devices.

Note The chart data is based on the devices being viewed in the device list (2000 by default). For a representative sample of devices in the charts, you might need to increase the *Max items per search result* value on the Configure Server Settings page.

See the "Displaying Device Information" section on page 4-14.

Device Attributes and Properties

The Orchestrator server stores device properties and EnergyWise attributes for each device that connects to the server. (Some fields might not be populated for devices in some device families.) You can see device properties and attributes in the Orchestrator Administrator console on the Manage Devices page (**Devices** menu > **Filtered Search**). Some device attributes are created by the server, and some are reported by the device. The Orchestrator agent software reports attributes for PCs. The Orchestrator Proxy Server reports attributes for non-PC devices (switches, routers, IP phones, and wireless access points).

For a complete list of device properties and attributes, see the "Device Properties and EnergyWise Attributes" section on page 4-6.

For information on customizing the device list to show certain attributes and properties, see the "Viewing Devices and Attributes" section on page 4-14.

For details on changing device attributes or properties in Orchestrator, see the "Setting Device Properties and Attributes" section on page 4-18.

Attribute and Property Descriptions

- Table 4-2: Default Attributes and Properties
- Table 4-3: EnergyWise Attributes and Properties
- Table 4-4: Advanced Attributes and Properties
- Table 4-5: Troubleshooting Attributes and Properties

Table 4-2 Default Attributes and Properties

Name	Description
Assigned group	Name of the Orchestrator group assigned to the device.
Assigned policy	Name of the Orchestrator policy assigned to the device.
Device family	Used for reporting. Possible values: PC, IP Phone, wireless access point (WAP), Switch, Router, Unknown, Interface, and Service (EnergyWise proxy service). Unknown means that the device family is not supported.
Device name	For PC devices, this is the NetBIOS name. For EnergyWise devices, the name varies based on the device family. • Phone—Host name of the phone. For example, SEP*, where * is the MAC address of the phone. • Switch—Hostname of the switch. Default hostname is Switch. • Router—Hostname of the switch. Default hostname is Switch. • WAP—Hostname of the access point. Default hostname is ap. • Empty interface—Short name of the interface. For example, Gix.y.z.
Device status	Shows whether the device is checking in regularly. Devices check in with the Orchestrator server based on the *Device check-in* interval setting on the Configure Server Settings page. Each time the client checks in, the server records the check-in time. If a device misses two consecutive check-in times, the Orchestrator server marks the device as *Not checking in*. When the device begins checking in again, the Orchestrator server will set the device status to *Checking in again*. **Note** Whether a device is checking in or not checking in is not related to its power state, or whether the device is on or off. It simply is an indication of whether the device is communicating with the server.
Group assignment	*Rule* means that the group is assigned automatically through assignment rules. *Manual* means that the group was manually assigned. **Note** When you manually assign a group to a device, it is flagged as a manually assignment. To clear the manually assigned flag, select the device from the device list on the Manage Devices page. On the Move To Groups menu, click **Use Policy Assignment Rules**.

Table 4-2 Default Attributes and Properties (continued)

Name	Description
IP address	For a PC client, switch, or service (EnergyWise proxy server), this is the IP address most recently used for communication with the Orchestrator server. This address is the only port that Orchestrator uses to attempt Wake on LAN. Assignment rules are applied to the collection of all network adapters.
Licensed	Shows whether the device has a valid Orchestrator license. • Green check mark means yes. • Red X means no.
NetBIOS name	NetBIOS name of the PC device.
OS version	Name and version of the operating system, for example, Windows XP Professional SP 3.
Policy assignment	*Rule* means that the policy is automatically assigned through assignment rules. Manual means that the policy is manually assigned. When you manually assign a policy to a device, it is automatically flagged as manually assigned. To clear the manually assigned flag, select the device from the device list on the Manage Devices page. On the Assign Policies menu, click **Use Policy Assignment Rules**.
Policy status	Specifies whether a named policy has been retrieved from the Orchestrator server and the proxy server or device has acknowledged receipt of the most current policy. Values are *Delivered* or *Pending*. • *Delivered* means the PC agent or EnergyWise proxy server has retrieved the current policy from the Orchestrator server. • *Pending* means the PC agent or EnergyWise proxy server has not yet retrieved the current policy. **Note** Delivered does not necessarily mean the policy has been completely applied. For EnergyWise devices with policies that are updated through the EW proxy server, there can be a delay between policy deliveries and policy updates on the switches.
Wake on WAN proxy	A green check mark means that the computer is operating as a Wake On WAN proxy. Devices not running the Orchestrator agent software cannot be elected as proxies.

Table 4-3 table describes EnergyWise attributes and properties.

Table 4-3 EnergyWise Attributes and Properties

Name	Description
Caliber	The value received during the most recent scan that describes how the usage was measured: • Max—Means that the actual power drawn cannot be determined. A presumed value that is the maximum that the Cisco EnergyWise entity could draw appears. • Presumed—Means that the actual power drawn cannot be determined but can be presumed from the model, for example, PC model X draws 200 W, and PC model Y draws 210 W. • Unknown—Means that the usage reported is unknown. In some cases, entities report aggregate power as does a lighting controller or aggregate controller. In such cases, it is not known whether the usage reported is actual or presumed. • Actual—Means that the usage data reported is the real power drawn. For example, a PoE phone drawing *x* watts of power can be determined by reading from the port, and then report the actual usage as *x* W. • Trusted—Means that the usage data reported was reported from another source.
Delta vector	The difference between the actual power usage and the maximum power usage for each power level. A range from 0 to 10 represent the difference between the *Usage in Watts* and the *Usage Vector* for each level.
Domain name	Name of the EnergyWise domain that the device belongs to.
Energy units	Shows the units of power for a Cisco EnergyWise entity. The value represents an exponent of 10. For example, if current usage of an entity is 3, it could be 3 W, 3 mW, 3 KW, or 3 MW, depending on the value of Cisco EnergyWise power unit, that is, 0, –3, 3, or 6, respectively.
Importance	The relative priority of one device compared another. The range is from 1 (least important) to 100 (most important). The default is 1. Importance is used to differentiate among devices in the domain and to determine the relative importance of different switches in the network. For example, an office phone has a lower importance compared to an emergency phone. An emergency phone would be set to 100, and an office phone would be set to 50. This attribute is editable.
Keywords	A tag for the EnergyWise entity. Separate multiple keywords with commas (no spaces between keywords).
Physical description	The physical description of the device.

Table 4-3 EnergyWise Attributes and Properties (continued)

Name	Description
Power level	An EnergyWise power level, from 0 to 10. **Note** The default power level is 10. A Cisco switch does not support level 0. You cannot turn off the power to a switch. Orchestrator maps EnergyWise power levels to PC power states as: • Levels 3 - 10—Wake or On • Level 2—Sleep • Level 1—Hibernate • Level 0—Shut down or Off
Provisioned	The maximum power in watts that a Cisco EnergyWise entity can draw at the current level.
Role	The role of an EnergyWise entity in the EnergyWise domain, for example, *lobby.b20*. For a switch, the default is the model number. This attribute is editable.
Usage vector	A vector from 0 to 10 representing the maximum power in watts that an EnergyWise entity can draw at each power level.
Usage in watts	The power draw of an entity in watts. Orchestrator reads this value from a device or PC client. If the Caliber is *Actual*, this value varies with the actual watt usage of the device. For example, a phone uses more power when its speaker is on than when off. Usage sampled while the phone is on will be higher than when it is off.

Table 4-4 table describes the advanced attributes and properties.

Table 4-4 Advanced Attributes and Properties

Name	Description
Baseboard manufacturer	The name of the organization responsible for producing the physical element of the baseboard, for example, Dell Computer Corporation.
Baseboard product	The baseboard part number defined by the manufacturer, for example, OOT606.
CPU	The processor on the PC, for example, Intel Pentium 4 CPU 2.40 GHz.
Chassis type	The physical container housing the components of a computer, for example, desktop or laptop.
DNS name	Fully qualified domain name of the computer.
Description	A text string that describes a Windows PC client. This property is editable.
Device GUID	Unique identifier of the device. Also the EnergyWise identifier for EnergyWise-capable devices.

Table 4-4 Advanced Attributes and Properties (continued)

Name	Description
LDAP distinguished name	Distinguished name from LDAP server.
Licensing disabled	*Yes* means that licensing is disabled for the device. *No* means that a license will be allocated when available. The option selected in Device Licensing page (**Edit Devices > Device Licensing**) controls the setting.
Manufacturer	Name of the company that manufactures the computer or device.
Power platform role	Shows an OEM's preferred power management profile for a computer. These values are read from the Preferred_PM_Profile field of the Fixed ACPI Description Table (FADT). For example, PlatformRoleDesktop or PlatformRoleMobile.
System BIOS	BIOS string text, for example, DELL - 8, 02/26/03

Table 4-5 table describes the troubleshooting attributes and properties.

Table 4-5 Troubleshooting Attributes and Properties

Name	Description
Client version	Build number of the Orchestrator agent software installed on a device.
Computer model	Model name of the computer, for example, OptiPlex GX260.
Last connected	Date and time of the last complete connection. The last connected time is the last time the EnergyWise proxy server checked in with Orchestrator for a device. For EnergyWise devices, this occurs even when the device is at power level 0 (Off) because the device is still in the EnergyWise domain.
MAC address	MAC address of the interface most recently used for communication with the server.
Memory (KB)	Available memory in KB.
Network address	Unique identifier of the device on the network at Layer 3.
Portable	*Yes* if a Windows notebook. *No* if otherwise. This is a derived (computed) field, based on the values of Chassis Type and Platform Power Role.

Table 4-5 Troubleshooting Attributes and Properties (continued)

Name	Description
Proxy Wake on WAN preference	Shows the ranking for the computer as a Wake on WAN proxy. Preferred—The computer is ranked higher in proxy-selection criteria. Never—The computer is never selected as a proxy. Default—Other computer attributes are only used as selection criteria if no preferred proxies are available. The setting is controlled by an option selected in Edit Device Properties (click **Edit Devices > Edit Device Properties**.)
Subnet mask	Subnet mask (network mask and an address of a host in the network) of the broadcast domain.

Displaying Device Information

- Viewing Devices and Attributes, page 4-14
- Excluding Interfaces from the Device List, page 4-15
- Excluding Unlicensed Devices from the Device List, page 4-15

Viewing Devices and Attributes

Use the Manage Devices page to access device information. You can search for and display devices based on a variety of attributes, including by group, by policy, by device family, or by PC subnet. All devices meeting the filter or search criteria appear in the device list.

For a list of device attributes and properties, see the "Device Properties and EnergyWise Attributes" section on page 4-6.

Orchestrator provides many options to see devices. You can go to tab views that filter devices based on group, policy, or subnet (displays only PCs on the selected subnet). You can also use the search function to filter by group, policy, subnet (PCs only), and device family.

Note By default, the device list displays the first 2000 devices that meet the search and filter criteria. If you need to see a larger set of devices, in the Server menu click **Configure Server Settings**, and increase the *Max items per search result* value. The maximum value allowed is 20,000. Setting this value to a higher number can result in longer display times for search results.

- Click **Customize View** on the Manage Devices page to add columns to or remove columns from the view.
- Change the order of columns by dragging a column to a new position in the list.
- Click the **Charts** tab to see a high-level picture of device activity and membership.

Note
- The chart data is based on the current result set of devices being viewed in the device list (2000 by default). For a representative sample of devices in the charts, you might need to increase the *Max items per search result* value on the Configure Server Settings page.
- Click the **Reports** menu to display details on operational state, user activity, and event log information for devices.
- To display only devices that are currently licensed, select **Exclude devices with licensing disabled in the device lists** on the Configure Server Settings page (on the Server menu, click **Configure Server Settings**).
- Devices that appear as *Interface* in the device list are ports with no IP phones, wireless access points, or other PoE devices plugged into them. To hide interfaces from the device list, select **Do not display Interface devices in the device lists** on the Configure Server Settings page (on the Server menu, click **Configure Server Settings**).

To see device information:

Step 1 On the Devices menu, click **Filtered Search**.

Step 2 Click the tab (Groups, Policies, or Subnets) that you want to use to filter the display, and select a filter on that tab to see the results in the device list.

You can also click the **Search** tab, select options in the device filters to display the set of devices that you want, and enter a search string.

Step 3 Click **Search** to see the results set in the device list.

Note To see only licensed devices, select **Exclude devices with licensing disabled in the device lists** on the Configure Server Settings page. On the Server menu, click **Configure Server Settings**.

Devices that appear as *Interface* in the device list are empty ports (ports with no end points).

To hide interfaces from the device list, select **Do not display Interface devices in the device lists** on the Configure Server Settings page. On the Server menu, click **Configure Server Settings**.

Excluding Interfaces from the Device List

Devices that appear as *Interface* in the device list are ports with no IP phones, wireless access points, or other PoE devices plugged into them.

To hide empty ports in the device list, select **Do not display Interface devices in the device lists** on the Configure Server Settings page.

Step 1 On the Server menu in the Administrator console, click **Configure Server Settings**.

Step 2 Check the **Do not display Interface devices in the device lists** check box.

Step 3 Click **Save**.

For information on viewing devices, see the "Viewing Devices and Attributes" section on page 4-14.

Excluding Unlicensed Devices from the Device List

To see only the licensed devices in the device list, you can select **Exclude devices with licensing disabled in the device lists** on the Configure Server Settings page.

For information on removing a device or disabling its licensing, see the "Removing a Device from the System" section on page 4-19.

Step 1 On the Server menu, click **Configure Server Settings**.

Step 2 Check the **Exclude devices with licensing disabled in the device lists** check box.

Step 3 Click **Save**.

For information on viewing devices, see the "Viewing Devices and Attributes" section on page 4-14.

Managing Devices

- Assigning Devices to Groups, page 4-16
- Assigning Policies to Devices, page 4-17
- Controlling Devices Directly, page 4-17
- Setting Device Properties and Attributes, page 4-18
- Removing a Device from the System, page 4-19

Assigning Devices to Groups

You can assign devices to groups from the device list or automatically by using group assignment rules.

For details on configuring group assignment rules, see the "Configuring Group Assignment Rules" section on page 2-3.

For details on creating groups, see the "Creating Administrative Groups" section on page 3-2.

Follow these steps to manually assign a device to a group:

Step 1 On the Devices menu, click **Filtered Search**.

Step 2 Click the tab (Groups, Policies, or Subnets) that you want to use to filter the display, and select a filter option for seeing the results in the device list.

(Optional) Click the Search tab, select different options in the device filters to display the set of devices that you want, and enter a search string.

Step 3 Click the Search button to see the results in the device list.

Step 4 Select the device or devices in the list.

Step 5 On the Move to Group menu, click Manually Assign Group, or click Use Group Assignment Rules.

Note When you manually assign a policy to a device, it is flagged as a manual assignment. To clear the flag, select the device from the device list. On the Move to Group menu, click **Use Group Assignment Rules**.

If you choose Use Group Assignment Rules and one or more selected devices was manually assigned, select **Include N manually assigned devices** and click **OK** to confirm that you want to change from a manually assigned group to rule-based assignment.

Step 6 For manual assignment, click the group name, and click **OK**.

Step 7 For rule-based assignment, click **OK**.

Assigning Policies to Devices

You can assign policies to devices in device list or automatically by using policy assignment rules.

Note All power settings in policies apply to PCs. For other types of devices, only scheduled power level changes apply. For non-PC devices, a scheduled power level change might be the only setting that you apply by using a policy.

For details on policy assignment rules, see the "Configuring Group Assignment Rules" section on page 2-3.

For details on creating policies, see the "Creating and Editing Policies" section on page 5-8.

To manually assign policies:

Step 1 On the Devices menu, click **Filtered Search**.

Step 2 Click the tab (Groups, Policies, or Subnets) that you want to use to filter the display, and select a filter option to see the results in the device list.

(Optional) Click the Search tab, select different options in the device filters to display the set of devices you want, and enter a search string.

Step 3 Click the Search button to see the results set in the device list.

Step 4 Select the device or multiple devices in the resulting list.

Step 5 On the Assign Policies menu, click **Manually Assign Policy** or **Use Policy Assignment Rules**.

Note When you manually assign a policy to a device, it is flagged as being manually assigned. To clear the flag, select the device from the device list, and then on the Assign Policies menu, click **Use Policy Assignment Rules**.

If you choose **Use Policy Assignment Rules** and one or more of the selected devices had been manually assigned, select **Include N manually assigned devices** and click **OK** to confirm that you want to change from a manually assigned policy to a rule-based assignment.

Step 6 For manual assignment, click the policy name, and click **OK**.

Step 7 For rule-based assignment, click **OK**.

Controlling Devices Directly

You can change the power levels of devices directly from the device list.

For details on enforcing power state changes within policies, see the "Creating and Editing Policies" section on page 5-8.

Step 1 On the Devices menu, click **Filtered Search**.

Step 2 Click the tab (Groups, Policies, or Subnets) that you want to use to filter the display, and select a filter option on that tab to see the results in the device list.

You can also click the Search tab, select different options in the device filters to display the set of devices that you want, and enter an optional search string.

Step 3 Click the **Search** button to see the results set in the device list.

Step 4 Select the device or devices in the list.

Step 5 On the Set Power Level menu, click a power level.

Note

- You can also right-click a device to select a power level from a context menu.
- Set EnergyWise Power Level automatically maps to PC power states. This works for PCs and non-PC devices.
- For PCs only: If you select *Sleep*, *Shut Down*, *Restart*, or *EnergyWise Power Level*, you can force a change of the power state by selecting **Force transition**. You can also choose whether to force a state change for Wake on WAN proxies.
- Use **Force transition** only when necessary. Some applications could block normal Windows shut down requests. For example, Word or Notepad might display a dialog box asking a PC user to save document changes. When you select **Force transition**, applications cannot block shut down and unsaved changes in the application are lost.

Step 6 (PCs only) Enter and select the options that you want to use for the transition (message, force transition), and click OK.

Note The options for forcing a transition or displaying a message are ignored for non-PC devices.

Step 7 Enter and select the options that you want to use for the transition, and click **OK**.

Setting Device Properties and Attributes

You can change device properties for PCs (description Wake on WAN), or edit EnergyWise attributes (Role, Keyword, or Importance) from the device list on the Manage Devices page (**Devices** menu > **Filtered Search**).

For PC properties, you can specify the ranking for the device as a Wake on WAN proxy. In the Edit Device Properties dialog box, check the **Preferred Wake on WAN proxy** check box, and select:

- **Preferred** increases the ranking of the selected computers in the proxy selection criteria.
- **Never** prevents the selected computers from being selected as proxies.
- **Default** or **Don't change** means that other computer attributes are used as selection criteria and only if there are no preferred proxies available.

For other details, see the "Setting a Device As a Preferred Wake on WAN Proxy" section on page 6-8.

For EnergyWise devices, you can edit the Role, Keyword, and Importance attributes for parents (switches) or children (interfaces). You can use the attributes to identify a specific device or a group of devices.

- Use the Role attribute to show the general business context.

- Importance ranges from 1 (least important) to 100 (most important). Use the Importance attribute to differentiate between devices in a domain.

  For example, an office phone has a lower importance compared to an emergency phone. Because it is critical that the emergency phone never enter sleep mode, you should set the Importance to 100.

Step 1 On the Devices menu, click **Filtered Search**.

Step 2 Click the tab (Groups, Policies, or PC Subnets) that you want to use to filter the display, and select a filter on that tab to see the results in the device list.

You can also click the Search tab, select options in the device filters to display the set of devices you want, and enter a search string.

Step 3 Click **Search** to see the results set in the device list.

Step 4 Select the device or devices in the list.

Step 5 On the Edit Devices menu, select **Edit device properties** or **Edit EnergyWise attributes**.

Step 6 Enter and select the options that you want to use, and click **OK**.

Removing a Device from the System

To remove a device from the Orchestrator system or to unlicense a device, you can disable the device license on the Manage Devices page (**Edit Devices > Device Licensing > Do not allocate a license to the device**). Orchestrator does not collect or report data for any devices with disabled licensing. However, historical data collected while the device was licensed is retained.

Reinstall a device by choosing **Allocate a license when one is available** in the License devices dialog box.

To see only the licensed devices in the device list, select **Exclude devices with licensing disabled in the device lists** on the Configure Server Settings page. On the Server menu, click **Configure Server Settings**.

Step 1 On the Devices menu, click **Filtered Search**.

Step 2 Click the tab (Groups, Policies, or Subnets) that you want to use to filter the display, and select a filter on that tab to see the results in the device list.

You can click the Search tab, select different options in the device filters to display the set of devices that you want, and then enter a search string.

Step 3 Click the **Search** button to display the results set in the device list.

Step 4 Select the device or devices in the list.

Step 5 On the Edit Devices menu, click **Device Licensing**.

Note You can also right-click a device, and click **Device Licensing**.

Step 6 Click **Do not allocate a license to the device**, and click OK.

Note You can re-enable a device by choosing the **Allocate a license when one is available** option in the License Devices dialog box.

CHAPTER 5

Managing Policies

- Policies, page 5-1
- Baseline Mode and Operational Mode, page 5-2
- Setting Up New Policies, page 5-2
- Policy Inheritance, page 5-4
- Strategies for Creating Policies, page 5-4
- Recurrence Settings, page 5-6
- Power State Changes, page 5-7
- Configuring Policies, page 5-7
- Enforcing Policies, page 5-11
- Using Power Schemes, page 5-12
- Creating and Editing Power State Change Rules, page 5-14

Policies

A policy is a collection of the settings that Orchestrator uses to enforce power management in your network. You can assign the same policy to multiple PCs or devices in a network.

Note All power settings in policies apply to PCs. For other types of devices, only scheduled power level changes apply. Orchestrator collects data for all device types for reporting purposes.

Policies can have these settings:

- A background scheme, which is a power scheme that runs 24 hours a day, 7 days a week, when no other schemes are explicitly scheduled.

  You can create a policy with just the background power scheme to serve as a default for simple PC power management.
- One or more power schemes, each with a unique schedule. Each scheme can also include one or more power-state change rules for different applications. Power state transition rules can prevent a PC from transitioning to standby or shut down while a specified application is running.
- One or more power level changes (such as wake, sleep, or restart), each with a unique schedule.

- Power-state change rules, which tell Orchestrator what action to take when a particular application (such as iexplore.exe or firefox.exe) is running on a PC, and when Orchestrator attempts to change the PC to standby or shut down. Rules can run unscheduled as part of the background settings or as part of a scheduled scheme. The rules take effect whenever their associated scheme takes effect, including the background scheme.
- Device wake-up settings.
- Logging and monitoring settings for PC clients.

Each device is assigned the default *No Enforcement* policy until you explicitly assign a different policy. Orchestrator captures data and events for devices using the *No Enforcement* policy, but does not enforce any power schemes.

Baseline Mode and Operational Mode

Orchestrator can run in two server modes: *Operational* and *Baseline.* These are set in the Configure Server Settings page (Server menu). Policies are enforced in *Operational* mode. *Baseline* mode is used for measuring energy use only.

- In Baseline server mode, Orchestrator begins collecting data for all devices as each device connects to the system. The data updates each time a device checks in. You can then display this data in different reports and device views.
- In Operational server mode, in addition to data collection, Orchestrator enforces policies either manually or through assignment rules that you create. Each device can have only one policy assigned to it, but each policy can contain multiple schemes and power state changes, each with its own schedule.

New devices that do not match the criteria defined in the policy assignment rules are assigned the default policy when they first connect to Orchestrator. Typically, the default policy is not enforced and no schemes are associated with the default policy.

Setting Up New Policies

When you create a new policy, it uses the policy default settings for wake settings and data collection. You can then select:

- The background scheme and power state transition rules that are in effect when the background scheme is in effect.
- Power schemes, power state changes, and power state transition rules that run according to schedule and override background settings.

New polices that you create inherit policy default settings. To change these settings, you must deselect the option **Use policy default settings** on the Wake and Data Collection tabs.

Table 5-1 General Steps for Setting Up a Policy

Step	Tasks	Procedure
1	Create a policy.	On the Policies menu, select **Edit Policies**, and then click **New Policy**.
2	Set the power scheme that should run when no other schemes are scheduled. Set any transition rules that should run when no other schemes are scheduled.	Click the **Background** tab.
3	Create a comprehensive schedule for the policy. The schedule can include one or more schemes that run during specific days and times and one or more power state changes that run on specific days and times. **Note** Scheduled power schemes cannot overlap. If you need to create or edit a power scheme, click **Power Schemes** on the top right button bar.	While editing a policy: Click the **Schedule** tab, and click **Insert Scheme** or **Insert <*Wake / Sleep / Hibernate / Shut Down / Restart / EnergyWise Power Level*>**. **Note** **Insert EnergyWise Power Level** automatically maps to PC power states and works for PCs as well as non-PC devices. The options for omitting, delaying, or forcing a change, or displaying a message are ignored for non-PC devices.
4	Add one or more transition rules if necessary.	While editing a policy: Click the **Schedule** tab, click **Insert Scheme**, and click the **Power State Transition Rules** tab.
5	Review the wake settings. If you need wake settings that are different from the policy default settings, clear the *Use policy default settings* option.	While editing a policy: Click the **Wake Settings** tab.
6	Review settings for logging and data collection. If you need settings that are different from the policy default settings, clear the *Use policy default settings* option.	While editing a policy, Click the **Data Collection** tab.
7 (optional)	Create, edit, or reorder policy assignment rules.	Click **Assignment Rules** in the top right corner of the Edit Policies page.
8 (optional)	Create or edit power state transition rules.	Click **Power State Transition Rules** in the top right corner of the Edit Policies page.

Policy Inheritance

All policies initially inherit wake and data collection settings from the policy default settings: these are the wake settings, logging, and data collection settings without a scheduled component. The settings apply to all policies that use the *Use policy default settings* option.

You can apply the same wake and data collection settings for all policies and customize wake and data collection settings for specific policies as needed by deselecting the *Use policy default settings* option on Wake and Data Collection tabs for that policy.

Each policy that you create must include a background scheme, which can include a scheme and power-state change rules automatically applied 24 hours a day, 7 days a week, unless you schedule other schemes and rules.

The background scheme and scheduled power schemes can also have associated power state transition rules that are active when the particular schemes are active.

Any scheduled power settings that you specify (schemes, power state changes, or power state change rules) and unique wake and data collection settings take precedence over default policy settings and background settings.

Strategies for Creating Policies

The policies that you create should be based on your knowledge of the energy that PCs and devices in use, why, the times of day that users are most active, and patch management needs.

Analyzing the Operational State report and Event Summary report during the baseline period can help you gain understanding of when devices are On but are not actively being used.

For details on implementing power management through policies, see Chapter 2, "Gathering Data for Initial Power Management Policies."

Figure 5-1 shows a new policy that was created to address most power management needs.

Figure 5-1 New Policy Example

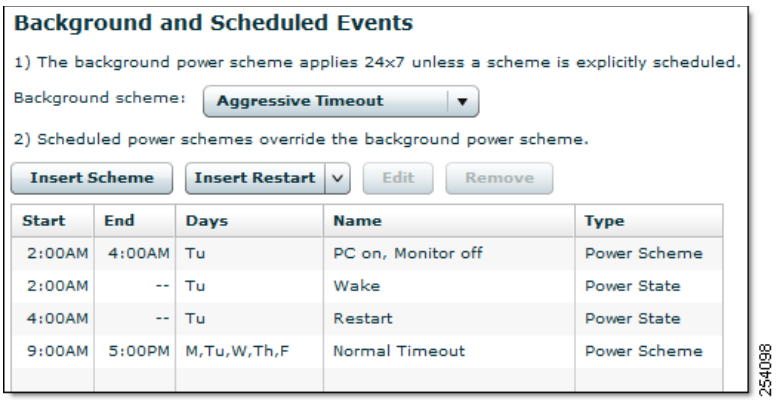
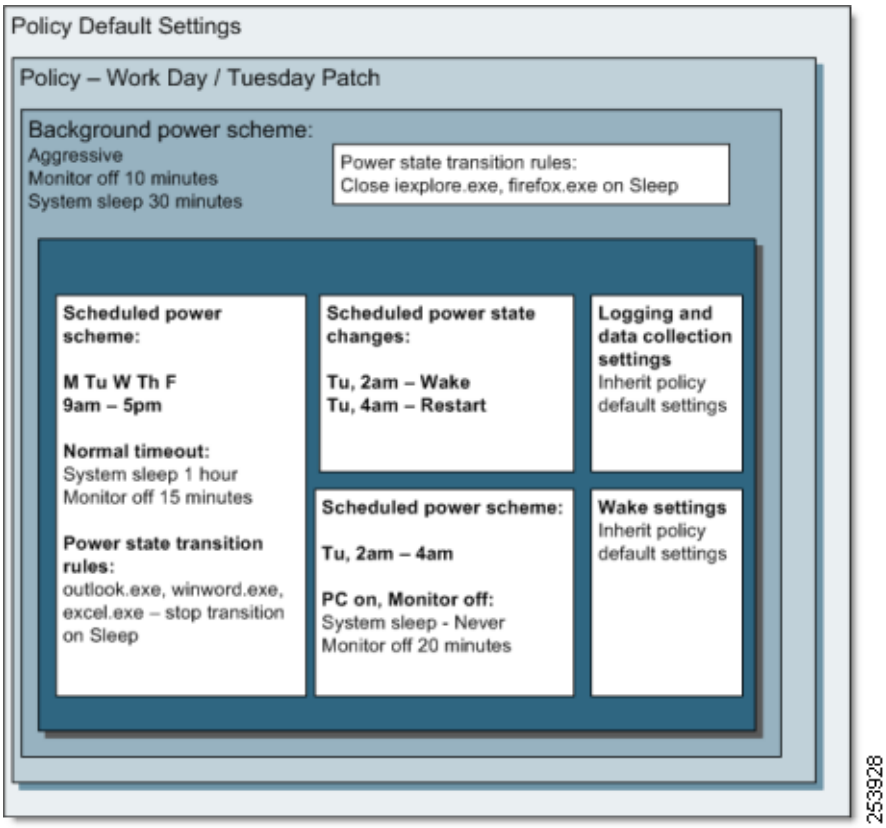


Figure 5-2 Example of Policy Inheritance

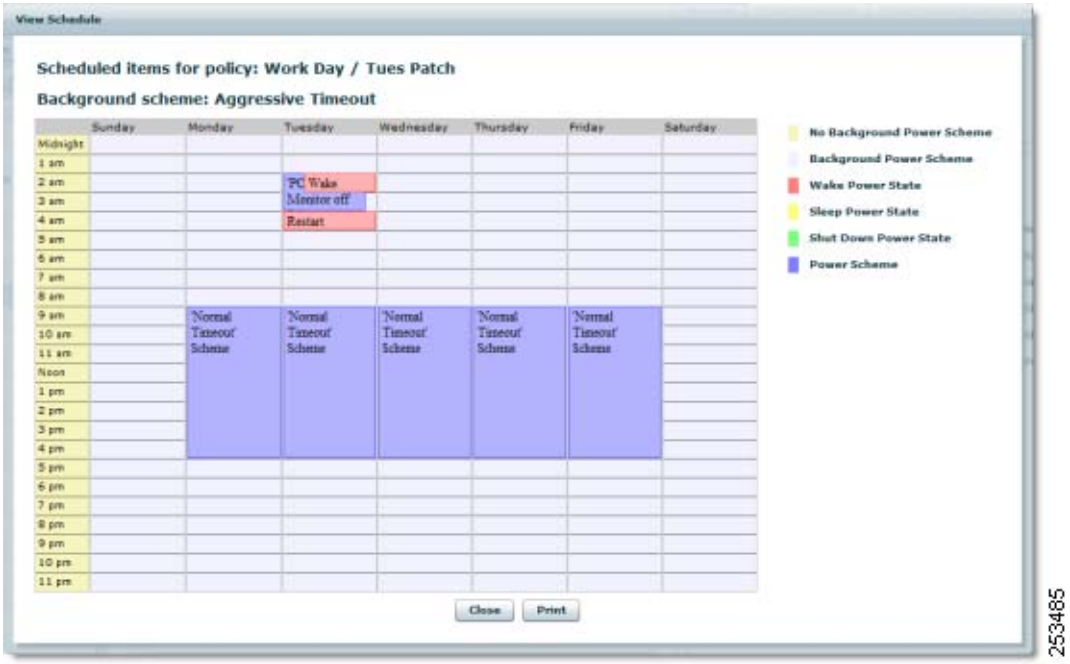


Settings for policy called *Work Day/Tuesday Patch*:

- Inherit policy default settings for wake and data collection settings.
- Enforce an aggressive scheme for any day and time that another scheme is not in effect (background).
- Enforce a normal scheme for work hours 0900 to 1800 during the week.
- Enforce a *PC on, Monitor off* scheme during a Tuesday early morning patch maintenance window.

On Tuesday, two power state changes are scheduled to wake machines for patching and to restart computers when patching should be complete (Figure 5-3).

Figure 5-3 Power State Changes in a Policy Example



After you create the policy, you can manually assign it to one or more devices in the device list or automatically through policy assignment rules.

Recurrence Settings

EnergyWise recurrence strings that you set for devices on the switch through the CLI or another management application are overwritten when the Orchestrator server updates the policy that is assigned to the device:

- Orchestrator changes from baseline to operational server mode, and Orchestrator begins policy enforcement.
- An administrator clears the *Do not enforce this policy* option for an assigned policy for a device while Orchestrator is in Operational mode.
- A policy is modified and saved in operational mode, and Orchestrator sends the updated policy information to a device.

Note If previously set recurrences exist on any ports when EnergyWise proxy service is started for the first time, the recurrences still exist on the ports. If the **No Enforcement** policy is assigned to these ports and you need to clear the preexisting recurrences, follow these steps:

Step 1 In Orchestrator Administrator console, on the Policies menu, select **Edit Policies**.

Step 2 Select the **No Enforcement** policy.

Step 3 Clear the **Do not enforce this policy** option.

Step 4 Click **Save**. Wait until the recurrences have cleared. You can check this by using show EnergyWise recurrences command on the switch CLI.

Step 5 Select the **Do not enforce this policy** option again.

Step 6 Click **Save**.

Power State Changes

A power state change is part of a policy that can be scheduled and instructs a device to wake, sleep, hibernate, shut down, restart, or change its EnergyWise power level.

You can also change the power levels of devices directly, outside of policy settings, from the device list.

Options for power state changes are available on the Edit Policies page on the Schedule tab (**Policies > Edit Policies > Insert <Wake / Sleep / Hibernate / Shutdown / Restart / EnergyWise Power Level>** and in the Manage Devices page on the Devices tab (**Devices > Set Power Level <Wake / Shutdown / Sleep / Restart / EnergyWise Power Level>**).

Note Insert EnergyWise Power Level and Set EnergyWise Power Level automatically map to PC power states and work for PCs as well as non-PC devices.

When you specify a power state change to a PC to sleep, hibernate, shut down, or restart, you can also specify options to force a change (directly or in a policy) to allow a user to delay or omit a change for a specified period of time (policies only).

Note

- The options for skipping, delaying, or forcing a transition, or displaying a message are ignored for non-PC devices.
- Use Force transition only when necessary. Some applications might block normal Windows shut down requests. For example, Word or Notepad display a dialog box asking the PC user to save document changes. When you select Force transition, applications are prevented from blocking shut down and any unsaved changes in the user's application are lost.

Configuring Policies

- Setting New Policies, page 5-7
- Creating and Editing Policies, page 5-8
- Configuring Policy Assignment Rules, page 5-10
- Disabling a Policy, page 5-11

Setting New Policies

When you create a policy, Orchestrator uses the policy default settings for wake settings and data collection. You can select:

- The background scheme and power state transition rules that are in effect 24 hours a day, 7 days a week, when no other schemes or rules are explicitly scheduled.

- Power schemes, power state changes, and power state change rules that run according to schedule and that override background settings.

Note Policies that you create inherit policy default settings. To change settings, you deselect **Use policy default settings** on the Wake and Data Collection tabs.

	Task	Description
Step 1	From the Policies menu, choose **Edit Policies**, and click **New Policy**.	Create a policy.
Step 2	Click the **Background** tab.	Set the power scheme to run when no other schemes are scheduled. Set any change rules to run when no other schemes are scheduled.
Step 3	While editing a policy, click the **Schedule** tab, and click **Insert Scheme** or **Insert <Wake / Sleep / Hibernate / Shut Down / Restart / EnergyWise Power Level>**.	Create a schedule for the policy. The schedule can include one or more schemes that run during specific days and times and one or more power state changes that run on specific days and times. **Note** If you need to create or edit a power scheme, click **Power Schemes** in the top right button bar.
Step 4	While editing a policy, click the **Schedule** tab, click **Insert Scheme**, and click the **Power State Transition Rules** tab.	Add one or more change rules if necessary.
Step 5	While editing a policy, click the **Wake Settings** tab.	Review the wake settings. If you need different wake settings, clear the *Use policy default settings* option.
Step 6	While editing a policy, click the **Data Collection** tab.	Review settings for logging and data collection. If you need different settings, clear the *Use policy default settings* option.
Step 7	(Optional) Click **Assignment Rules** in the top right corner of the Edit Policies page.	Create, edit, or reorder policy assignment rules.
Step 8	(Optional) Click **Power State Transition Rules** in the top right corner of the Edit Policies page.	Create or edit power state change rules.

Creating and Editing Policies

A policy is a collection of settings that Orchestrator uses to enforce power management in your network. You can assign the same policy to multiple PCs or devices in a network.

Note All power settings in policies apply to PCs. For other types of devices, only scheduled power level changes apply. For non-PC devices, it is likely a scheduled power level change would be the only setting that you apply by using a policy.

Step 1 From the Policies menu, choose **Edit Policies**.

Step 2 Click **New Policy**, or select a policy in the list. You can also click **Copy** to start with an existing policy as your template.

Step 3 For a new policy, enter the policy name and a description.

Step 4 On the Schedule tab, select the background power scheme to use whenever no other scheme is scheduled.

You can also click the Background tab to select a background power scheme and specify power state change rules that run when no other power state change rules are scheduled.

Step 5 Click the **Insert Scheme** to add a scheduled power scheme to the policy.

Step 6 Select the scheme, days, and time range, and click **Insert**.

Continue to add schemes as needed for the policy. Scheduled power schemes cannot overlap.

If you want to include power state change rules that accompany the scheduled scheme, click the **Power State Transition Rule** tab.

a. Click the Power State Transition Rule tab.

b. Click **Insert**, select the rule that you want to add, and then click **Add**.

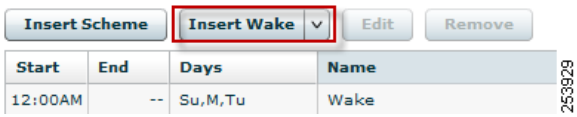
Click **New Rule** to add a rule to the list.

Power state transition rules can apply to applications running locally, on the network, or both. The application name that you provide should be the executable name as it appears in the Windows Task Manager under Processes, for example: firefox.exe.

c. Click the Schedule tab when you are done.

d. Repeat these steps to configure another power state transition rule.

Step 7 On the Insert Power State menu, click a power state change to add it to the policy.



Note Insert EnergyWise Power Level automatically maps to PC power states and works for PCs as well as non-PC devices.

(PCs only) If you select **Insert Sleep**, **Insert Hibernate**, **Insert Shutdown**, **Insert Restart**, or **Insert EnergyWise Power**, you can choose whether you want to force the change of power state by selecting **Force transition**.You also can choose to force a transition for Wake on WAN proxies.

Note Use Force transition only when necessary. Some applications might block normal Windows shut down requests. For example, Word or Notepad might display a dialog box asking a PC user to save document changes. When you select Force transition, applications are prevented from blocking shut down, and any unsaved changes in the user's application are lost.

(PCs only) You can specify whether users can omit or delay a change and change the message displayed for a Sleep, Hibernate, Shut Down, or Restart change.

Note The options for skipping, delaying, or forcing a transition, or displaying a message are ignored for non-PC devices.

Step 8 Select the days and time, and click **Insert**.

Continue to add power state changes as needed for the policy.

Step 9 Adjust the Wake and Data Collection tab settings, if needed. These settings affect PCs only. You need to clear the *Use policy default settings* option to edit the settings.

If you clear the *Collect power state data* option, PC power state change data is not available in reports.

Step 10 Click **Save**.

You can also configure power schemes and power state transition results for the policy. See the "Using Power Schemes" section on page 5-12 and the "Creating and Editing Power State Change Rules" section on page 5-14.

Configuring Policy Assignment Rules

After you create policies, you can configure Orchestrator to automatically assign the appropriate policies to new devices when the devices connect to the server.

When you configure policy assignment rules, policies are automatically assigned to specific devices based on a set of criteria. Because rules that you set up for automatically assigning policies to devices are saved as a set, the order is important, and you need to consider the best order to get the results that you want.

You can only run the rule set automatically when new devices connect, or for all connections. This means that rules run whenever a device wakes or whenever the device moves from one network card to another (such as a PC moving from a network line to a wireless connection).

Each rule can contain a set of criteria that a policy must meet to be assigned to the device. When you connect new devices to the server, they must comply with the policy criteria for the policy to be automatically assigned to a set of devices.

Note If a device does not meet any of the criteria in the rule, the device is assigned to the default policy.

Step 1 In the Administrator console, from the Devices menu, choose **Configure Policy Assignment Rules**.

Step 2 Click **New Rule**. Enter a name and a description for the rule, and select the name of the policy to be assigned when the rule runs.

Step 3 Click **Add condition** to add as many criteria as necessary.

As you add criteria, you can see what the result would be by clicking the **Test Conditions** tab.

Step 4 Specify whether the rule should be enforced when all criteria are satisfied or when any criteria is satisfied.

Step 5 Click **Done**.

Step 6 For Enforcement, specify whether the rule runs automatically when new devices connect to the server or when all devices connect to the server.

Note With *All connections*, the rules run whenever a computer wakes up or whenever a computer moves from one network card to another, such as from a network line to a wireless connection or back.

Step 7 Reorder rules by selecting a rule and clicking **Move Up** or **Move Down**.

Step 8 Click **Save Rule Set** to save all changes.

Disabling a Policy

To disable a policy for all PCs and devices that use that policy, select the **Do not enforce this policy** option on the Edit Policies page.

You can also create a new policy for a specific set of devices to which you can apply the *Do not enforce this policy* option as needed.

Notify your Orchestrator administrator when you make this change to ensure that the PCs or devices receive the correct enforcement instructions for your organization.

Note The *No enforcement* policy in Orchestrator is the default policy that is applied to new devices that do not meet the criteria of a policy assignment rule. The default settings use *Do not enforce this policy* option.You can apply the No enforcement policy to devices to disable policy enforcement if it is still using the default settings.

Step 1 In the Policies menu, click **Edit Policies**.

Step 2 In the policy list, select the policy that you want to disable.

Step 3 Select **Do not enforce this policy**.

Step 4 Click **Save**.

Enforcing Policies

After you determine initial policies and assign them to devices, you can take the server out of Baseline mode and start measuring and managing power use on the devices.

This topic assumes either of these situations:

- You have created initial power management policies after completing the baseline data collection phase, and you have assigned the policies to devices.
- You have set the server to Baseline mode for another reason, such as at the suggestion of a Technical Support representative for troubleshooting purposes.

If you have not obtained baseline numbers or created initial policies, see an overview of the process at Establishing the baseline level of energy use.

Step 1 Make sure that the policies you are using are not disabled:

a. On the **Policies** menu, click **Edit Policies**, and select a policy name in the list.

b. Confirm that the **Do not enforce this policy** box is not selected.

Figure 5-4 Box for Do Not Enforce This Policy

Step 2 On the **Server** menu in the Administrator console, click **Configure Server Settings**.

Step 3 For *Server mode*, select **Operational**.

When the server is in Operational mode, devices follow policy instructions, and device data is reported to the Orchestrator database.

Using Power Schemes

- Power Schemes, page 5-12
- Default Power Schemes in Orchestrator, page 5-13
- Creating and Editing Power Schemes, page 5-14

Power Schemes

A power scheme is part of a policy scheduled for PCs, and provides instructions about when a PC should change power levels, such as transitioning the system to sleep after 1 hour of no activity, or turning the monitor off after 15 minutes.

Schemes include these settings:

- Basic settings for system standby, monitor (on or off), and narcolepsy timeout.

Note Narcolepsy timeout refers the period of time in which the Windows operating system is prevented from putting a PC back to sleep during a period of no activity (such as during maintenance windows).You can also disable narcolepsy behavior completely.

- Idle timer settings for Windows and Orchestrator.

Note PC insomnia is a condition in which a computer initiates a low power state, but something on the system erroneously keeps the computer awake. PC insomnia is generally caused by various applications and processes that can reset the Windows idle timer. Using the Orchestrator idle timer helps to ensure accurate and predictable sleep transitions. The Orchestrator idle timer is enabled by default in schemes. The Orchestrator idle timer must be enabled to use power state transition rules in a scheme.

- Advanced settings that apply to specific versions of Windows (XP, Vista, or Windows 7).

Default Power Schemes in Orchestrator

Orchestrator includes several predefined schemes to use in policies or to modify You can edit or create your own schemes as needed. Click **Power Schemes** in the top right corner of the Edit Policies page.

You apply schemes to policies by using the Schedule tab in the Edit Policies page. Table 5-2 lists the default power schemes.

Table 5-2 Default Power Schemes

Scheme	Description
Very aggressive timeout	• System sleep after 15 minutes. • Turn off monitor after 5 minutes. • Narcolepsy timeout after 4 hours. • Orchestrator idle timer on by default (Windows idle timer disabled).
Aggressive timeout	• System sleep after 30 minutes. • Turn off monitor after 10 minutes. • Narcolepsy timeout after 4 hours. • Orchestrator idle timer on by default (Windows idle timer disabled).
Normal timeout	• System sleep after 1 hour. • Turn off monitor after 15 minutes. • Narcolepsy timeout after 4 hours. • Orchestrator idle timer on by default (Windows idle timer disabled).
Conservative timeout	• System sleep after 2 hours. • Turn off monitor after 20 minutes. • Narcolepsy timeout after 4 hours. • Orchestrator idle timer on by default (Windows idle timer disabled).
PC on, monitor off	• System sleep is never. • Turn off monitor after 20 minutes. • Narcolepsy timeout after 4 hours. • Orchestrator idle timer on by default (Windows idle timer disabled).
PC on, monitor on	• System sleep is never. • Turn off monitor is never. • Narcolepsy timeout after 4 hours. • Orchestrator idle timer on by default (Windows idle timer disabled).

Creating and Editing Power Schemes

A power scheme is a part of a policy that can be scheduled and provides instructions about when a device should change power levels, such as changing the system to sleep after 1 hour of no activity or turning the monitor off after 15 minutes.

The process of creating or editing a power scheme is separate from assigning the scheme to a policy. You must first create a power scheme to be able to add it to a policy.

Step 1 On the Policies menu, click **Edit Policies**.

Step 2 Click **Power Schemes** in the top right corner of the page.

Step 3 Click **New Scheme**, or select an existing scheme to edit it. You can also click **Copy** to start with an existing policy as your template.

Step 4 For a new scheme, enter the scheme name and a description.

Step 5 On the Basic Settings tab, select the main settings for the scheme.

You can optionally click the Advanced Settings tab to specify settings that affect specific versions of Windows.

Step 6 On the Idle Timer Settings tab, select whether the scheme should use the Windows idle timer or the Orchestrator idle timer.

Select options for refining how the Orchestrator idle timer behaves.

The Orchestrator idle timer must be enabled to use power state transition rules in a scheme. The Orchestrator idle timer is enabled by default in schemes.

For background information on PC insomnia, the Windows idle timer, and the Orchestrator idle timer, see Addressing PC insomnia through the Orchestrator idle timer.

Step 7 Click **Save**.

Creating and Editing Power State Change Rules

Power state change rules tell Orchestrator the action to take when a particular application (such as iexplore.exe or firefox.exe) is running on a PC and Orchestrator tries to change the PC to standby or shut down. Unscheduled rules can run as part of the background settings or as part of a scheduled power scheme. The rules take effect whenever their associated scheme takes effect, including the background scheme.

Power state transition rules can prevent a PC from transitioning to standby or shut down while a specified application is running.

Power state change rules can prevent data loss, such as when a user forgets to save changes in an open document. They can be useful for ending applications (such as some media applications) that are known to cause problems when you restart a machine to install a patch.

Note The Orchestrator idle timer must be enabled to use power state change rules in a scheme. (The Orchestrator idle timer is enabled by default in schemes.)

This procedure creates or edits rules that become available for assignment to a background or a scheduled power scheme. You can assign a rule to a policy or background. For details, see the "Creating and Editing Policies" section on page 5-8.

Step 1 On the Policies menu, click **Edit Policies**.

Step 2 Click **Power State Transition Rules** in the top right corner of the page.

Step 3 Click **New Rule** or select an existing scheme, and click **Edit**.

Step 4 For a new rule, enter the name for the transition rule and the name of the executable file for the application, for example, firefox.exe.

Power state transition rules can apply to applications running locally, or on the network, or both. The application name that you provide should be the executable name as it appears in the Windows Task Manager under Processes.

Step 5 Select the executable location.

- Local
- Network
- Local and network

Step 6 Select the affected changes.

- Shutdown
- Sleep

Step 7 Select the action that should be taken.

- Report only
- Terminate application

Note Use **Terminate application** only when necessary. Some applications might block normal Windows shut down requests. For example, Word or Notepad might display a dialog box asking the PC user to save document changes. When you select **Terminate application**, applications are prevented from blocking shut down, and any unsaved changes in the user's application are lost.

- Ignore transition

Step 8 Click **Save**.

CHAPTER 6

Waking Computers

The method used to wake computers depends on the circumstances. For example, if you want to set a patch management schedule, you might want to wake computers once per week at a specific time of day and for a specific length of time. If you want to wake computers on demand, you can use a Orchestrator Wake on LAN magic packet.

- Waking Clients Through the Server, page 6-1
- How End Users Wake Their Computers, page 6-2
- Determining Whether a Computer Can Wake from Standby, page 6-2
- Using Wake on WAN to Wake Clients Across the Network, page 6-5
- Waking Selected Devices, page 6-11
- Waking Clients on a Regular Schedule, page 6-11
- Wake Settings, page 6-13

Waking Clients Through the Server

You can set the server to wake clients as part of power management policies, to prepare them to receive patch updates, or to troubleshoot issues.

- Schedule a wake event in a policy.

  For example, wake PC clients at 0600 every morning before users come in.

- Schedule a Wake on WAN event in a policy to send a Wake on LAN magic packet to proxy computers, after which proxies wake the clients on their subnets.

  A standard scheduled wake event can wake computers from the sleep state but cannot wake computers that have been turned off. To reach as many clients as possible for a system update, set a Wake on WAN event to run shortly after a standard wake operation.

Note Most computers manufactured within the past couple of years are enabled for Wake on LAN by default. However, if you have older computers or network cards, you might need to enable Wake on LAN on those computers. For information see the Configuring Client Computers for Wake on LAN, page 6-6.

- Select a set of clients in the Administrator console, and choose the Wake command.

You do this if you need to apply an urgent patch update before the next scheduled maintenance window.

How End Users Wake Their Computers

End users can wake their computers to use them during a time when the computers are normally in the sleep state.

- End users who are at their computers can use the keyboard, mouse, or tap the power button.
- If users need to access their client computer from a remote location, you can use Orchestrator Wake for Remote Access so that they can wake the computer through a web browser.

Note To reduce the impact of centralized power management on end users, make sure that device drivers on client computers are current and support waking computers.

Determining Whether a Computer Can Wake from Standby

Step 1 If the computer is on, change it to standby through the Windows Start menu.

Step 2 Test wake capability:

- Press a key on the keyboard.
- Move or click the mouse.
- Press the power button for 1 second. (Holding the button down longer might shut down the computer.)

Step 3 Repeat the first two steps, so that you can try each method.

If the computer wakes when you press the power button but not through the keyboard or mouse, you can enable the keyboard and mouse. See the "Configuring the Mouse or Keyboard to Wake the Computer" section on page 6-2.

If the computer does not wake when you press the power button, see the "Pressing Power Button Does Not Wake Computer" section on page 10-2.

Configuring the Mouse or Keyboard to Wake the Computer

If mouse or keyboard actions do not wake a computer from standby, you enable them to do so.

Step 1 Open the Windows Control panel, and open either the Mouse or Keyboard.

Step 2 On the Hardware tab in the Properties dialog box, click **Properties**.

Step 3 On the Power Management tab (Figure 6-1), select **Allow this device to wake the computer**.

Figure 6-1 Power Management Tab

Note If a Power Management tab does not appear in the Mouse or Keyboard Properties dialog box, the device might not support waking from standby. You might need to upgrade the driver or the device itself.

Configuring the Mouse or Keyboard to Wake the Computer Using the Administrator Console

If you cannot configure a mouse or keyboard through the Windows Control Panel to wake the connected computer you can enable them both, as well as the network interface card (NIC), through the Administrator console.

You might need to configure support for users waking their computers through the mouse or keyboard. You can simultaneously enable multiple devices through the Administrator console.

Step 1 On the Policies menu, click **Edit Policies**, and select a policy name in the list.

You can also change the policy default settings.

Step 2 Click the **Wake Settings** tab, and if necessary, clear the **Use policy default settings**.

Step 3 Set these values under Basic Settings:

Table 6-1 Settings

Property	Value
Wake on mouse movement	Enable
Wake on keyboard press	Enable
Require password on wake	As appropriate for your organization

Step 4 Under Advanced Settings, enable all settings.

Note If you change these settings in an individual policy, that policy does not inherit future changes that you make to the policy defaults.

For information about the Wake on WAN Settings section, see the "Using Wake on WAN to Wake Clients Across the Network" section on page 6-5.

Changing Wake Settings

These settings affect how you can wake PCs from the Administrator console, as well as how end users can wake their own PCs.

You can change wake settings for a specific policy, or you can set new policy default wake settings.

To access the Wake Settings tab:

Step 1 On the Policies menu, click **Edit Policies**.

Step 2 To change the settings that all new policies created inherit, click **Edit Policy Default Settings**, and click the Wake Settings tab.

To change the settings for a specific policy, select that policy in the left navigation pane, click the Wake Settings tab in the main content section, and clear the **Use policy default settings** check box.

Note The setting **Don't change** means to use whatever is set in the operating system or hardware for this action.

Using Wake on WAN to Wake Clients Across the Network

- Wake on WAN Overview, page 6-5
- Configuring Client Computers for Wake on LAN, page 6-6
- Enabling Policy Wake on WAN Settings, page 6-7
- Setting a Device As a Preferred Wake on WAN Proxy, page 6-8
- Setting the Wake on WAN Proxies Per Broadcast Domain, page 6-8
- How Orchestrator Selects Wake on WAN Proxies, page 6-10

Wake on WAN Overview

Wake on WAN technology provides a reliable method for waking computers from any low-power state (including off) across the enterprise network. It extends the Wake on LAN functionality present in most modern computers for sending magic packet data.

Orchestrator combines Wake on LAN with IT best practices to prevent packets from routing across subnet boundaries. It elects two proxy computers on each subnet, a primary and a secondary. Wake on WAN proxies are always awake. The one that receives a Wake on LAN magic packet from the server forwards the packet to clients within its subnet.

If the primary proxy has a problem interfering with communication with the server, the server can promote the other proxy to primary. It also selects another computer on the subnet, and wakes it if necessary to be the new secondary proxy.

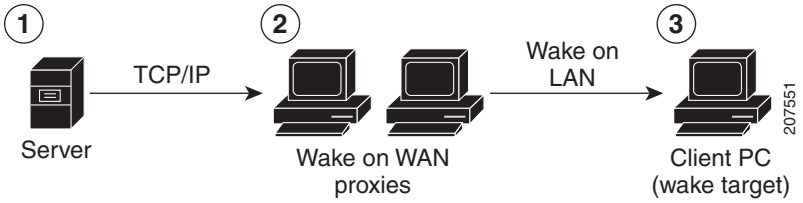
You can assign as many proxies as you want per subnet. The best practice is to designate at least two.

- Determining Subnet Boundaries, page 6-5
- Setting the System for Wake on WAN, page 6-6

Determining Subnet Boundaries

Orchestrator uses IP network number clustering. Computers within the same IP network number can broadcast Wake on LAN packets to each other.

Figure 6-2 Orchestrator Wake on WAN



1. The server sends a message to the Wake on WAN proxies on each subnet. The message has a request to wake the target computer.
2. The primary proxy receives the wake message and sends a Wake on LAN packet that contains the target node address over its subnet.
3. The target computer receives the Wake on LAN packet and wakes.

The primary Wake on WAN proxy that receives the magic packet broadcasts it to the remaining clients on the subnet using port 7 and the subnet broadcast address.This address is formed by using the subnet's prefix, followed by all 1s. For example for 10.35.0.0/255.255.255.0 the broadcast address would be 10.35.0.255.

Setting the System for Wake on WAN

The Orchestrator server is enabled for Wake on WAN by default. Complete the following tasks:

- Enable policy wake settings.
- Confirm that Wake on LAN is enabled on client computers. For information, see the "Configuring Client Computers for Wake on LAN" section on page 6-6.

If power management policies include scheduled wake requests, waking a computer from standby does not require Wake on LAN. Enable it to wake clients for operations that are not on a regular schedule or to wake them from an off state. For information, see the "Waking Clients on a Regular Schedule" section on page 6-11.

Configuring Client Computers for Wake on LAN

To use Wake on WAN, computers must be enabled for Wake on LAN.

Issues that can mean that computers are not enabled for Wake on LAN:

- They can change to standby, but they immediately wake.
- You have followed the steps for enabling Wake on WAN, and some clients do not respond to wake requests sent by Wake on WAN proxies.

Wake on LAN is enabled in the computer BIOS and the network card. Settings vary slightly among hardware manufacturers. If you have specific questions about Wake on LAN support on your systems, refer to the documentation provided by the hardware vendor.

Note Devices that are not enabled for Wake on LAN still receive wake requests that you schedule in the Administrator console.You can continue to measure power use on those devices.

Step 1 In the Windows Control Panel, open **Network Connections**, right-click the connection that the computer uses, and choose **Properties**.

Step 2 On the General tab, click **Configure**.

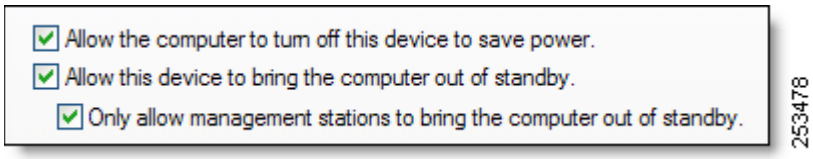
Step 3 On the Power Management tab (or Advanced tab, depending on the driver) of the network card dialog box, look for Wake on LAN settings such as the following

Table 6-2 NIC Settings

Property	Value
Wake From Shutdown (or power off state)	Enable
Wake-Up Capabilities (or Wake on LAN)	Set to Magic Packet or enable, depending on the choice

Step 4 Also look for and enable settings such as those in Figure 6-3 that allow management systems to initiate power state changes.

Figure 6-3 Power Management Tab



Tip When clients do not stay in standby because network traffic wakes them, select **Only allow management stations to bring the computer out of standby** to resolve the problem.

Note If you update the NIC driver, the settings you change in this procedure might revert to the defaults, which can prevent the client from following Orchestrator power management policies. Be sure to check these settings any time you update the NIC driver.

Step 5 To configure the BIOS, restart the computer. During the startup process, press the keyboard key shown to enter the BIOS settings.

This option appears before Windows starts, and the key shown can vary among computer types.

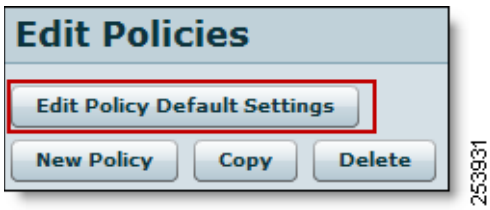
When you have access to the BIOS settings, look for the settings related to devices waking the computer, and enable those. For specific settings, refer to the hardware documentation.

Enabling Policy Wake on WAN Settings

The first step to using Wake on WAN is to create policies in which it is enabled.

Step 1 On the Policies menu, click **Edit Policies**, and select a policy name in the list.

You can also change the policy default settings.



Step 2 Click the Wake Settings tab, and, if necessary, clear the **Use policy default settings**.

Step 3 Under Wake on WAN Settings, select **Enable all settings**.

If you want to edit these settings individually, click **Customize settings.** (The setting **Don't change** means to keep the default operating system setting.)

The settings correspond to the network card settings that you configure through the Windows Control Panel.

Test a wake operation through Wake on LAN. If some clients do not respond, you might need to configure the network card and BIOS separately on those clients.

Setting a Device As a Preferred Wake on WAN Proxy

If you enable Wake on WAN, you might also want to designate devices that Orchestrator checks first when it needs to select a new Wake on WAN proxy.

Step 1 On the Devices menu, click **Filtered Search**.

Step 2 Configure the search filters to match the attributes of the computers to be set as preferred proxies or that you want to set to never be selected as a proxy.

For tips and more information, see the How Orchestrator Selects Wake on WAN Proxies, page 6-10.

Step 3 Select one or more computers in the device list, and from the properties and attributes menu, click **Edit Device Properties**.

Figure 6-4 Edit Device Properties Tab

Step 4 In the Edit Device Properties dialog box, check the **Preferred Wake on WAN proxy** check box, and select the setting for the computers.

- **Preferred** increases the ranking of the computers in the proxy-selection criteria.
- **Never** prevents the computers from being selected as proxies.
- **Default** means that other computer attributes are used as selection criteria and that these computers are selected only if there are no available preferred proxies.

Setting the Wake on WAN Proxies Per Broadcast Domain

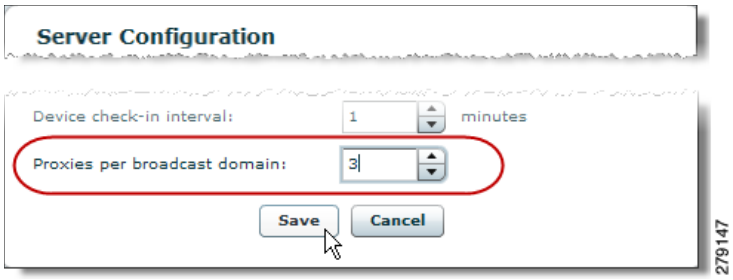
By default, Orchestrator designates two Wake on WAN proxies per broadcast domain, a primary and secondary. You can use the server settings page to change the number assigned within each broadcast domain.

For more information, see Using Wake on WAN to wake clients across the network.

Step 1 In the Orchestrator Administrator console, on the Server menu, click **Configure Server Settings**.

Step 2 Under Server Configuration, use the arrows, or enter a value for *Proxies per broadcast domain*.

Figure 6-5 Proxies Per Broadcast Domain



Note We recommend at least two proxies per broadcast domain. One proxy is always up to forward Wake on LAN packets from the server. If your network includes broadcast domains with fewer than six devices, work with a professional service consultant to determine the proxy settings.

Step 3 If you increase the number of proxies per broadcast domain, save the new settings. You do not need to complete the remaining steps. Orchestrator selects the additional proxies based on its built-in selection criteria, as well as Preferred Proxy settings that you can set on individual clients.

If you reduce the number of proxies, complete the remaining steps to change the settings on the clients that you want to clear of proxy status.

Step 4 On the Devices menu, click **Filtered Search**.

Figure 6-6 Filtered Search

Step 5 On the Search tab, use the **By subnets** filter and specify the subnets to display.

Step 6 In the device display, make sure the Wake on WAN Proxy column appears.

If it is not, click **Customize View**, and select it on the Default tab. After you display the column, you can drag it to the left.

Step 7 Click the **Wake on WAN Proxy** column heading once or twice to sort the display with the proxies listed at the top.

Step 8 Determine which of the proxies you want to run as standard devices (that is, change to low power states according to policies assigned to them). Select them, and on the Edit Devices drop-down menu, click **Edit Device Properties**.

Step 9 For *Preferred Wake on WAN proxy*, select **Never**.

After you change the setting, a polling interval set on proxies can take up to 15 minutes to receive the change from the server.

Step 10 When all of the devices you selected are cleared of proxy status, you set the **Preferred Wake on WAN proxy** setting on any of them to Preferred or Default so that they can be returned to the pool of devices that are available for proxy selection.

For information about preferred Wake on WAN proxy settings, see the "Setting a Device As a Preferred Wake on WAN Proxy" section on page 6-8.

How Orchestrator Selects Wake on WAN Proxies

Orchestrator uses a built-in selection criteria for selecting new proxies. This helps you determine which devices to set as preferred proxies or to never be proxies.

Device Ranking For Proxy Selection

In the Administrator console, you can specify Wake on WAN proxy preference for devices in the device properties. Right-click selected devices and choose **Device Properties**.

When the Orchestrator server needs to select a new Wake on WAN proxy for a broadcast domain, the proxy is selected based on one of these factors and in the order listed:

1. Devices with the *Preferred Wake on WAN proxy* setting of Preferred.
2. Devices with a *Preferred Wake on WAN proxy* setting of Default if the device is not a laptop.
3. Laptops with a *Preferred Wake on WAN proxy* setting of Default.

The server runs other checks to determine whether the computer meets requirements for relaying data packets. For example, it confirms that the device IP address, and subnet mask are set properly for Wake on LAN within its broadcast domain.

Note If a new device joins a broadcast domain, and it has a higher preference ranking than an existing proxy, Orchestrator removes the existing proxy and assigns the new device in its place.

Determining Devices To Set As Preferred Proxies

Wake on WAN proxies remain on at all times. Therefore, some devices are more appropriate than others to serve as proxies. For example, devices that need to be on 24 hours a day, 7 days a week, to serve critical functions are good candidates for preferred proxies.

Laptops tend to be moved around frequently. Set as many laptops as you can to *never* be preferred proxies, and leave the remaining laptops in the default setting.

The best practice is to leave most devices with the *Preferred Wake on WAN proxy* setting of Default and to allow Orchestrator to select new proxies as needed.

Waking Selected Devices

You can wake clients by selecting them in the Administrator console and running the Wake command.

You might need to wake clients for a specific reason, such as to apply a security patch. To do this, you can select devices in the Administrator console and manually run a wake request.

If you want to wake devices from the off as well as from the sleep states, you can do so through Wake on WAN. For information about enabling Wake on WAN, see the "Using Wake on WAN to Wake Clients Across the Network" section on page 6-5.

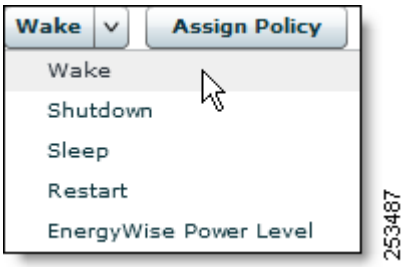
Step 1 In the Administrator console, on the Devices menu, click **Filtered Search**.

Step 2 In the navigation panel, use the search filters to show the devices that you want to wake up (or use filters on one of the other tabs), and click **Search**.

For example, use the Policy filter to wake only clients with a particular assigned policy.

Step 3 On the Devices tab, select the devices that you want to wake up, and on the power-state menu, click **Wake**.

Figure 6-7 Wake Power States



Note The menu button for setting power states shows the last-selected state. You might need to display the menu to see the state that you want.

Waking Clients on a Regular Schedule

You can set clients to wake at a regular specified time through a policy schedule.

For example, if end users start working on their computers at 0700, set a wake request to run at 0650, or set computers to wake in preparation for the scheduled maintenance window.

Wake from Sleep or Wake from Off

You can set a scheduled task to wake computers from sleep (standby) without using Wake on LAN. This option works well for waking computers at the beginning of the work day.

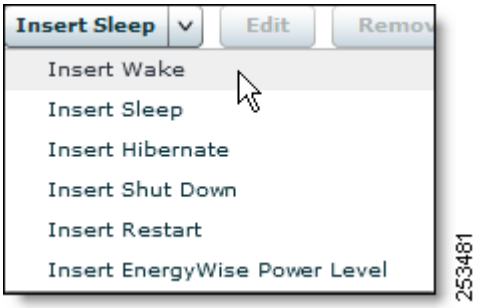
However, if you want to wake computers for maintenance, you might also want to reach the computers that have been turned off. To wake these computers, you need to enable Orchestrator Wake on WAN. After that, include a second wake task in the policy that you set to go through Wake on WAN.

Step 1 In the Administrator console, from the Policies menu, choose **Edit Policies**.

Step 2 Create a new policy or select an existing one, and then click the **Schedule** tab.

Step 3 From the power-state menu, choose **Insert Wake** (Figure 6-8).

Figure 6-8 Insert Sleep Power States



Note The menu button for setting power states shows the last-selected state, so you might need to display the menu to see the state that you want.

Step 4 In the Insert Power State Change dialog box:

- Select the days of the week on which you want to wake computers.
- Enter the time of day that you want the change to start.
- If you want this wake event to reach computers in the off state, select the **Wake using Wake on WAN** check box.

Step 5 Configure any additional policy settings, and save the changes.

For example, if you wake computers at the beginning of the day, you might want to set a work-hours power scheme. For information about creating policies, see the "Overview of Policies and Power Management Settings" section on page 6-1.

Wake Settings

These settings affect how you can wake PCs from the Administrator console, as well as how end users can wake their own PCs.

You can change wake settings for a specific policy, or you can set new policy default wake settings.

To access the Wake Settings tab:

Step 1 On the Policies menu, click **Edit Policies**.

Step 2 To change the settings that all new policies created will inherit, click **Edit Policy Default Settings**, and click the Wake Settings tab.

To change the settings for a specific policy, select that policy in the left navigation pane, click the **Wake Settings** tab in the main content section, and clear the **Use policy default settings** check box.

Note The setting *Don't change* means to use whatever is set in the operating system or hardware for this action.

- Basic Settings, page 6-13
- Advanced Settings, page 6-13
- Wake on WAN Settings, page 6-14

Basic Settings

- *Wake on mouse movement* and *Wake on keyboard press*—Enabled by default so that users can move the mouse or press a key to wake the computers.
- *Require password on wake*—Enable this setting to add a layer of security to waking on mouse movement or key press.

Advanced Settings

Table 6-3 Advanced Wake Settings

Setting	Action
Turn on display on wake.	Turns on the monitor when a wake request is sent through Wake on LAN or a policy schedule change.

Table 6-3 Advanced Wake Settings (continued)

Setting	Action
Wake enable USB.	Enable for USB mouse or other pointing devices.
Allow suspend with remote user.	Enable if you implement the Wake for Remote Access component, through which end users can wake their computers and log in from a remote location. If enabled, the computer can change to low power according to the scheduled scheme set while the user is logged in from another location. If not enabled, the computer stays on while the user is logged in, regardless of activity.

Wake on WAN Settings

The settings in this section correspond to network card settings that you configure through the Windows control panel. All the settings are enabled by default. You can use the Orchestrator Wake on WAN feature, which extends the Wake on LAN technology within your network.

For information, see the "Using Wake on WAN to Wake Clients Across the Network" section on page 6-5.

When you use Wake on WAN, enable all these settings to ensure that the maximum number of client agents can receive wake requests through Wake on LAN.

CHAPTER 7

Viewing Reports

Overview

Orchestrator includes reports and views of information about power states for all devices, PC user activity, and events. It provides summarized views of device data in the Operational State report and the Events Summary report.

For a summarized display of savings and energy use data shown in a dashboard, see the "About the Sustainability Dashboard" section on page 9-1 and the "Chart Types and Filters" section on page 9-21.

The device data in each report is determined by the filters that you set for the display and also by the *Max items per search result* value set on the Configure Server Settings page. The maximum value allowed is 20,000. Setting this value to a higher number can result in longer display times for search results.

Note By default, the device list displays the first 2000 devices that meet the search and filter criteria. If you need to see a larger set of devices, on the Server menu, click **Configure Server Settings**, and increase the *Max items per search* result value.

Note Move the cursor over different areas of the chart to see various data points.

For details on how to use event data for troubleshooting and optimization, see Chapter 8, "Getting Diagnostic Information from Event Logs."

Data Summarization Process Overview

The data displayed in the Operational State report and the Sustainability Dashboard is aggregated, summarized data.

The summary process reads Orchestrator data from the *DeviceComponentStatePeriod* and *DeviceSample* tables, and writes the data into the *ComponentStateDaySum* and *ComponentStateHourSum* tables.

The first time that the process runs, it reads all the data from the DeviceComponentStatePeriod and DeviceSample tables. Because of the potential amount of data being processed, running the summary process for the first time can use significant system resources on the computer. If you are running the summarization process on the Orchestrator server computer (recommended), be sure to run the process when the Orchestrator server is not required to be active.

Note When Orchestrator is installed, data must first be generated before it can be summarized. When the Orchestrator server sends data to the database, the summarization process waits until the data is fully committed before processing begins.

Factors affecting the time for the summarization process the first time it runs:

- Database I/O—The summarization process can request large amounts of data from the database. The speed of database I/O affects processing time.
- Defragmentation—Table indexes are defragmented during summarization. The amount of defragmentation required can affect how quickly the summarization process completes.
- Groups—Number of locations, business units, policies, and administrative groups.
- Memory—Available memory for SQL and the summarization can also affect the time required.

Each time that the process runs after the initial summarization, data is summarized on an incremental basis and takes less time to complete. Only data that has been added since the last summarization is processed.

Global Settings and Summarization

The default values defined in the Global Settings tab of the Sustainability Dashboard determine the default values for the data summarization process and the energy calculations. We recommend that you set these values before you run the summarization process for the first time get the most accurate and uniform report results over time.

If you change a setting, you need to run the summarization process again to show the updated values in your dashboard reports. However, because data is summarized on an incremental basis after the first time that you run the process, only data that is collected and reported on from the time of the change shows the new values. Historical data is still based on the old values.

If devices in Orchestrator are assigned to new groups or policies, the historical (already summarized) data reflects the old grouping and policy structure.

When you want to run the summarization process from the beginning to reset summarization data, see the "Resetting Summarization Data" section on page 7-4.

To restate summarized data by using new policies and groupings, rerun summarization completely from the beginning. Be aware that the new Global Setting values in the Sustainability Dashboard are also applied to all historical data.

For example, if old data reflected a $0.10 per kilowatt hours (kWh) cost, and the cost has been updated to $0.11 kWh, all the data is summarized by using the $0.11 cost.

Scheduling the Process

We recommend that you use the Windows Task Scheduler to run the data summarization and that you run this process when the Orchestrator server does not need to be active.

When deciding how often you want to run the summarization process or what schedule to follow, consider how timely you want the data to be.

Consider scheduling or manually running the process on a daily, monthly, or quarterly schedule. Allow up to a day for summarization to complete if it runs only monthly. Run summarization on a daily basis to keep the dashboard up to date without increasing the load on the Orchestrator server.

For details, see the "Running the Data Summarization Process Manually" section on page 7-3 and the "Running the Data Summarization Process as a Scheduled Task" section on page 7-3.

Running the Summarization Process

Before running the summarization process, make sure that the summarization.exe.config has the correct database connection string.

To start the process, run DataSummarization.exe from the same folder as the summarization.exe.config file (typically C:\Program Files\Cisco Systems\Cisco EnergyWise Orchestrator\BackgroundProcessor\DataSummarization.exe).

The process begins to read data from the DeviceComponentStatePeriod and DeviceSample tables, and writes the summarized data into the ComponentStateDaySum and ComponentStateHourSum tables.

Note You can run only one summarization process at one time.

To determine the status of the summarization process:

- Review the processes running in Windows Task Manager.
- Run Perfmon.exe.

To see the summarization process results, open the log file GeneralReport.log in C:\Program Files\Cisco Systems\Cisco EnergyWise Orchestrator\Logs.

Running the Data Summarization Process Manually

To start the summarization process manually, run DataSummarization.exe from the same folder as the DataSummarization.exe.config (typically C:\Program Files\Cisco Systems\Cisco EnergyWise Orchestrator\BackgroundProcessor\).

Running the Data Summarization Process as a Scheduled Task

Step 1 To open Windows Task Scheduler, click **Start**, click **All Programs**, point to Accessories, point to System Tools, and click **Scheduled Tasks**.

Step 2 Double-click **Add Scheduled Task** to start the Scheduled Task Wizard, and click **Next** in the first dialog box.

Step 3 In the next dialog box, click **Browse**, browse to C:\Program Files\Cisco Systems\Cisco EnergyWise Orchestrator\BackgroundProcessor\ (default installed location), select DataSummarization.exe, and click **Open**.

Step 4 Enter a name for the task, and choose an option:

- Daily
- Monthly
- Weekly
- One time only

- When my computer starts (before a user logs on)
- When I log on (only after the current user logs on)

Step 5 Click **Next**, specify the date and time and click **Next**.

Note The information about the date and time to run the task varies depending on the selection that you made in the previous wizard dialog box. For example, if you chose Weekly, you must enter the day of the week, the time, and if the task should run every week, every 2 weeks, every 3 weeks, and so on.

Step 6 Enter the name and password of the user who is associated with this task. Make sure that you choose a user with sufficient permissions to run the program. By default, the wizard selects the name of the user who is currently logged on.

Step 7 Click **Next**, and click **Finish** after you verify the choices that you have made.

Note Right-click the name of the task that you created in Windows Explorer, and click **Run** to run the summarization process at any time.

Resetting Summarization Data

If you change an important value in Global Settings (such as energy cost, wattage consumption, or emission equivalents) or change how you group clients, you might want to completely resummarize data.

Note Changes to Global Settings values that affect summarized data:

Energy Cost per kWh and Currency
CO2 Kilogram Emissions per kWh
CO2 Kilogram Equivalent of One Car Saved
CO2 Kilogram Equivalent of One Tree Saved
CO2 Kilogram Equivalent of 1 Litre of Gas Saved
Watt Consumption values: CPU On, CPU Sleep, CPU Off, Display On, Display Not On

To completely (not just incrementally) resummarize all Orchestrator data with the current Global Settings values, run this script in SQL Server Management Studio for EnterprisePowerManagementDB.

```
update SumTableLastLoad
set lastupdatedate = '2000'
go
truncate table ComponentStateDaySum
go
truncate table ComponentStateHourSum
go
```

Note Do not run this script unless you are certain that you want to reset the dashboard summary data. Running this script starts the full summarization process, which reads all of the data from the DeviceComponentStatePeriod and DeviceSample tables.

Any new Global Setting values are applied to all historical data. For example, if old data reflected a $0.10 per kWh cost, and the cost has been updated to $0.11 kWh, all the data is summarized using the $0.11 cost.

Because of the potential amount of data being processed, running the complete summary process can use significant system resources on the computer running the summarization process and might take some time to complete. If you are running the summarization process on the Orchestrator server computer (recommended), be sure to run the process when Orchestrator server is not required to be active.

Step 1 Connect to the Orchestrator database server.

Step 2 Click **New Query**.

Step 3 In the SQL Editor toolbar, select **EnterprisePowerManagementDB** from the drop-down list of available databases.

Step 4 Enter the following SQL statement in the query window:

```
update SumTableLastLoad
set lastupdatedate = '2000'
go
truncate table ComponentStateDaySum
go
truncate table ComponentStateHourSum
go
```

Step 5 Click **Execute**.

Viewing the Operational State Report

The data displayed in the Operational State report is aggregated, summarized data. For details, see the "Data Summarization Process Overview" section on page 7-1.

The Operational State report is most useful for looking at trends in PC states and user activity, such as viewing data for the past week. It is not a real-time display of system status. Because the Operational State data is summarized, data for some devices can be incomplete in the most recent reporting period (days/hours) until summarization runs again.

Note The device count that shows on the Manage Devices page does not always match the device count on the Operational State report at a given time. The device list is a real-time display of the devices currently connected to Orchestrator. The Operational State report shows the device count and data based on the last time the summarization process ran.

If a subset of devices in the Manage Devices page is not v checking in and reporting data to the Orchestrator server, data for these devices is not included in summarization. The devices are not represented in the Operational State report for that time.

The Operational State report calculates the device count as the total number of hours. For hourly reporting, as an example: If ten devices report in to Orchestrator for half an hour, this information is reported as five devices for that hour. If, in the following hour, all ten devices report in to Orchestrator

for the entire hour, this information is reported as ten device hours, and the report shows ten devices. The same concept applies to daily reporting, where the device count equals the total number of device hours/24.

The device data in each report is determined by the filters that you set for the view and also by the *Max items per search* result value set on the Configure Server Settings page.

Note By default, the device list displays the first 2000 devices that meet the search and filter criteria. If you need to see a larger set of devices, on the Server menu, click **Configure Server Settings**, and increase the *Max items per search* result value. The maximum value allowed is 20,000. Setting this value to a higher number can result in longer display times for search results.

You can print the list or save it as a PDF file.

Move the cursor over different areas of the chart to see various data points.

Step 1 On the Reports menu, click **Operational State Report** (PC or EnergyWise).

Step 2 Select a date range and the view (day or hour).

Step 3 Specify the filter parameters to define the set of devices that you want to see in the report, and click the **Search** button.

Step 4 In the report, select different viewing options as needed (include users, include PCs, include monitors, show all states, show On states only).

Note Move the cursor over different areas of the chart to see details.

Step 5 Click **Print** to print the view, or click **Save** to save it as a PDF file.

Viewing the Events Summary Report

Move the cursor over different areas of the chart to see details on various data points.

For details on how to use event data for troubleshooting and optimization, see Chapter 8, "Getting Diagnostic Information from Event Logs."

The device data in each report is determined by the filters that you set for the view and also by the Max items per search result value set on the Configure Server Settings page.

Note By default, the device list displays the first 2000 devices that meet the search and filter criteria. If you need to see a larger set of devices, on the Server menu, click Configure Server Settings, and increase the *Max items per search* result value. The maximum value allowed is 20,000. Setting this value to a higher number can result in longer display times for search results.

Step 1 On the Reports menu, click **Events Summary Report**.

Step 2 Select a date range and the view (day or hour).

Step 3 Select an Event Category.

Step 4 Specify the filter parameters to define the set of devices that you want to see in the report results, and click the **Search** button.

Step 5 In the report, double-click an area of the pie chart to see details on that category.

Note Move the cursor over areas of the chart to see details. Click the Devices tab to see results by device. Click the Events tab to see results by event.

Step 6 Click **Print** to print the current display. You cannot save the display.

CHAPTER 8

Getting Diagnostic Information from Event Logs

Clients report end-user and power-state actions in log files, which you can display from the Administrator console. Each logged action is referred to as an event. You can use event logs to determine whether policies are effective and to detect and resolve errors.

- Data Tention in Device Logs, page 8-1
- Specifying Server Logging Levels and File Sizes, page 8-4
- Displaying Event Data in the Administrator Console, page 8-6

Data Tention in Device Logs

- Event Categories and Types, page 8-1
- Data Retention, page 8-3
- Log File Locations, page 8-3
- Server File Locations, page 8-3

Event Categories and Types

When you see data logged from system or user activity, you can filter it to select a specific *event category*. The view is broken down by *event types* for the selected category. Event types represent the specific actions or errors that occurred, such as power-state changes to sleep or wake, a user action that delayed a power-state change, and so on.

The following table lists the event categories and describes the event types logged under each.

Table 8-1 Event Categories and Types

Category	Description
Admin Actions	Includes all manual transitions to low-power states that an administrator sets on devices. For example, selecting a set of devices in the Administrator console, right-clicking, and selecting Sleep, Shutdown, or Restart.
Idle Timer Actions	Changes to low power states that occur specifically when the client is inactive (idle) for the length of time set in the assigned policy.

Table 8-1 Event Categories and Types (continued)

Category	Description
Policy Actions	Includes actions that occur through power state transition manager (PSTM) rules. For example, a PSTM rule can terminate a running application before it changes the client to low power, or it can veto the power-state change. event logs record both of those actions. Other events recorded in this category include initial power scheme value when the client service is started, when a power scheme is set according to the policy schedule, when a scheme is set by the user (because the scheme is created to allow the user to override it), and so on.
Scheduled Actions	Any power-state change that occurs according to the schedule set in the policy assigned to the client.
Service Events	Events logged by the client service, such as start, stop, or device check in. Events also include new database creation, and if data collection stops or starts for power state changes and user activity.
State Changes	Detailed power state change data and the request source (Orchestrator server, a third party, or an unknown trigger). Also includes display-only logs for power-state changes.
User Actions	Actions that users take on power schemes or power-state change notifications. For example, omitting or delaying a power-state change or changing the power scheme in the Windows Control Panel. **Note** End users have access to these policy options only if your administrator enables them when configuring the policy in the Administrator console.
User Activity	Events that show whether a user is active or not, whether a transition to a low power state based on idle time is pending, and if user activity is unknown (in which case data and activity collection might have stopped, which generates an event in the Service Events category).
Configuration Errors	Error setting, querying, or deleting a power scheme; changing wake settings on mouse, keyboard (including whether it is a USB device); or loading, parsing, or saving configuration files.
Policy Errors	Errors that prevent a PSTM rule from running. For example, PSTM does not veto a power state change, end an application, or report that an application has ended.
Service Errors	Errors that cause the client service to stop running properly. For example, the client computer loses power; the service does not parse or run a request from the power management service; performance counter for the idle timer is missing or failed; errors that occur during the user or display state queries.
Transition Errors	Problems that occur when the API for a power state transition is called but returns a failure code; errors occurring while processing a power state transition; failure to dispatch a Wake on LAN magic packet; unexpected errors while trying to prevent narcolepsy (computer transition to sleep while in use).
EnergyWise Power Level	Events that occur in the setting or operation of any of the EnergyWise power levels.

If you want to make the event report display more detail, you can combine the event category filter with any of the other standard filters for searching. For example, see successful transitions for a particular policy or user actions in a particular device group or subnet.

Data Retention

The historical period for which you can report on events depends upon a variety of system factors: the number of devices being managed, the reporting interval, the database server hardware, and so on. They determine the rate at which events are generated and the speed at which the database processes large numbers of events.

Under reasonable circumstances, you should be able to see events for 2 to 7 months in the past. However, you might need to trim the data sooner to achieve acceptable performance.

The Orchestrator database contains a table for all events and a separate table for PC power state and user activity events. The latter events are kept for a longer time than error events. Error events are generally used for troubleshooting and resolved relatively shortly after a problem occurs.

Log File Locations

The PC client agent logs event data to a file called PwrMgrService.log in the Orchestrator program directory on the client computer C:\Program Files\Cisco Systems\EnergyWise Orchestrator Agent\Logs.

On 64-bit versions of Windows, Orchestrator Agent folders and files are under Program Files (x86).

Server File Locations

Table 8-2 lists the locations in which you can find log files that contain status and diagnostic information for the Orchestrator server components.

When a new log file is created, the date is appended to the existing log file name, for example, PMPWebService.yyyy.mm.dd.log. The most current log takes the base file name.

Table 8-2 File Locations

Server Component	Path to Log Files
PMP web service	C:\Program Files\Cisco Systems\Cisco EnergyWise Orchestrator\Logs\PMPWebService.log
Enterprise power management service	C:\Program Files\Cisco Systems\Cisco EnergyWise Orchestrator\Logs\PowerManagementProcessor.log
Administrator web service	C:\Program Files\Cisco Systems\Cisco EnergyWise Orchestrator\Logs\AdminWebService.log
ActiveMQ	C:\Program Files\Cisco Systems\Cisco EnergyWise Orchestrator\activemq-5.3.0\bin
EnergyWise proxy service	C:\Program Files\Cisco Systems\EnergywiseProxyServer
The summarization process for reporting (DataSummarization.exe)	C:\Program Files\Cisco Systems\Cisco EnergyWise Orchestrator\Logs\GeneralRepo.log

Note The Sustainability Dashboard does not create log files.

Specifying Server Logging Levels and File Sizes

This procedure contains steps for settings for server logging level and log file size, to set policy default settings or override the defaults in individual policies.

Step 1 In the Administrator console, click the **Policies** menu button bar.

Step 2 On the Manage Policies page, click **Edit Policy Default Settings**.

Step 3 On the Data Collection tab, select the default logging level that you want for all policies that you create.

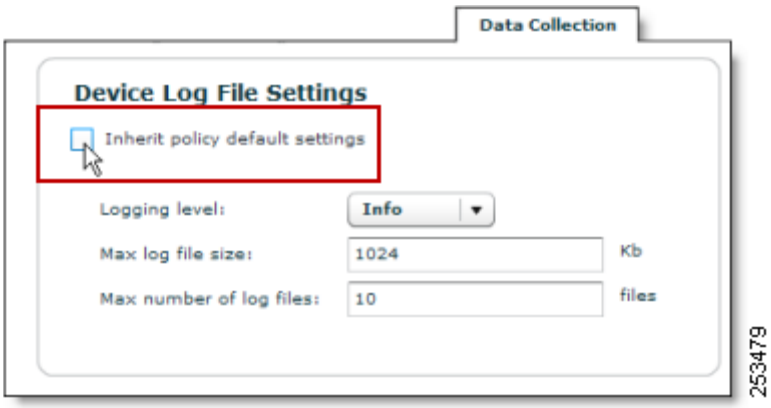
- Info—Informational messages, warning messages, and error messages
- Warning—Warning and error messages
- Error—Only error messages
- Trace—The most verbose and frequent logging
- Debug—A level of logging to use to troubleshoot a particular issue. Only use this on a small set of clients at a time and only under the direction of a Technical Support representative.

Step 4 Select the remaining device log file and data settings.

Setting	Value
Max log file size	Sets the maximum size of log file that you want to maintain. When the current log file reaches that size, Orchestrator creates a new file for subsequent messages, until that file reaches the maximum size, and so on.
Max number of log files	Sets the maximum number of log files to store on client machines.When the maximum is reached, the oldest file is deleted to make room for a new file.
Collect power state data	Select to record power state change events, including successful changes and change errors.
Collect user activity data	Select to record user activity events. Includes actions such as delaying or omitting a power state change or using the Windows Control Panel to change the power scheme from that set by Orchestrator.

To access these settings in an individual policy, on the Policies menu, choose **Manage Policies**, and click the **Data Collection** tab (Figure 8-1). Clear the **Inherit policy default settings** check box, and specify the log settings.

Figure 8-1 Data Collection Tab



When you change policy default settings, all policies that you create after the change inherit those settings by default. If you want a policy to have its own wake or data collection settings, you can change those settings within the policy itself.

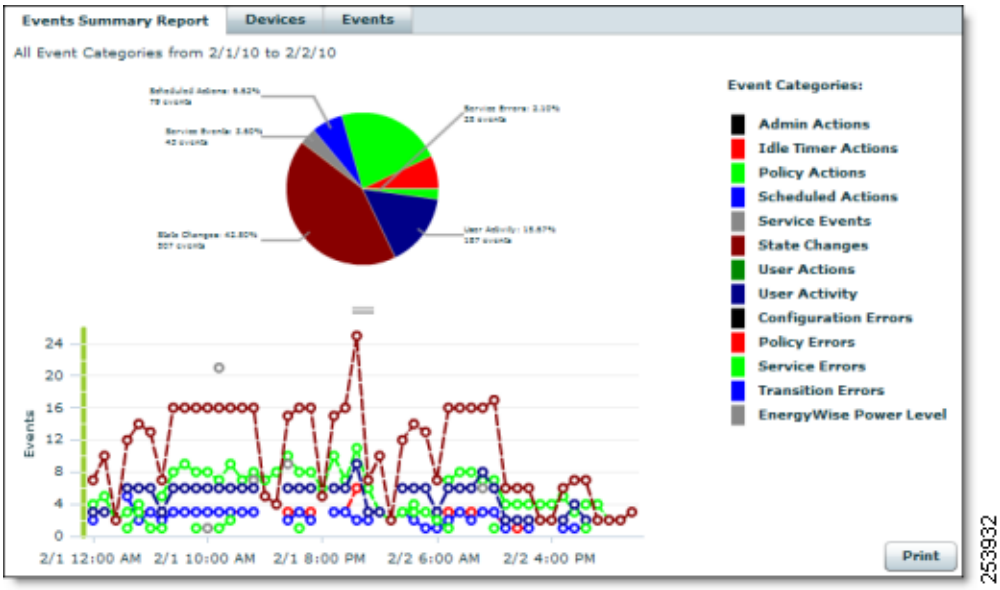
Note If you change these settings in an individual policy, it does not inherit future changes that you make to the policy defaults.

Displaying Event Data in the Administrator Console

You can see client agent activity in a summary report, see a list of devices by event, or see events by event type. You can use search filters to fine-tune the data, for example, to see events only in a particular administration group, events to which a particular policy is assigned, and so on.

1. In the Administrator console, on the Reports menu, click **Events Summary Report**.

   A chart appears, showing events from all event categories, by hour, over the past day. Charts represent the event categories, graphs represent the number of events, and lines represent event categories.



2. To fine-tune the data shown or see the same data differently, choose any process or a combination:

Table 8-3 Displaying Event Data

To Display	Do This
More detail about a part of the chart in the report	Hover the cursor over the section of a pie chart or on a bar chart data point.
All of the event types that occurred within an event category	Double-click the event category in a pie chart. A new chart appears, showing event types within that category.
Information from devices based on particular device attributes	Use the device filters on the left to refine the results by administration group, policy, device family, or subnet. Enter a search string to filter by device name or description.
Events reported by a particular device	In the Event Summary report, click the Devices tab. Click Customize View to add or remove columns.

Table 8-3 Displaying Event Data (continued)

To Display	Do This
All events that occurred on each device or on a specific device, how many times a particular event was logged, and when it occurred	In the Event Summary view, click the Events tab.
A different chart	Select a specific category in the Event category drop-down list.

Variations and Tips

To analyze power-state transitions for one specific device, enter the device name in the Search box, and enter the start and end dates.

See changes by day for a larger set of devices or for longer date ranges. Click column headings to sort by other parameters.

Search Phrase Tips

Search phrases that you enter are not case sensitive.

Orchestrator returns results that contain the search string. Wildcard characters * and ? are processed as text characters, not as wildcards.

For information about seeing devices in the Administrator console, see the "Viewing Devices and Attributes" section on page 4-14.

CHAPTER 9

Sustainability Dashboard

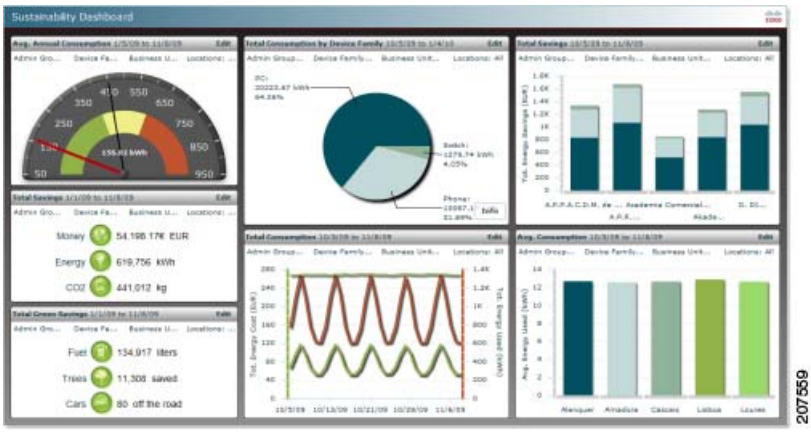
- About the Sustainability Dashboard, page 9-1
- General Steps for Installing, Configuring, and Deploying the Dashboard, page 9-2
- System Components, page 9-4
- Tasks, Roles, and Required Skills, page 9-6
- Configuring and Deploying the Dashboard, page 9-7
- Chart Types and Filters, page 9-21
- Sustainability Dashboard Reports, page 9-30

About the Sustainability Dashboard

The Sustainability Dashboard, an integrated component of Orchestrator, is an interactive reporting tool that shows how much energy and carbon emissions is saved as a result of enforcing PC power management policies.

The dashboard can be customized around your Green-IT strategy, only reporting specific energy or green metrics that matter.

Figure 9-1 Sustainability Dashboard



The dashboard displays charts and summary reports based on data collected in the Orchestrator database. Users seeing the dashboard can change chart views by selecting different filters for date ranges or grouping structures.

Sustainability Dashboard key features:

- Interactive flash and browser-based interface for accessing energy reports so that customers can easily see how much money and energy Orchestrator saves.
- Customizable chart objects to fit specific customer needs, with full control over the layout, chart presentation, and content displayed by the Dashboard.
- Green Savings presents the positive environmental impact of savings by reporting in carbon equivalent units, such as CO_2, fuel, or cars off the road.
- Embeddable chart objects for sharing the positive impact of Green IT initiatives with key stakeholders and colleagues.
- Energy-savings reports based on geographical location, business unit, or both.
- Increased data accuracy from entering specific regional energy rates and per-PC wattage information.
- The data displayed in the Sustainability Dashboard is aggregated, summarized data. You run a summarization process to make data available to the dashboard. For details, see the "Data Summarization Process Overview" section on page 7-1.

General Steps for Installing, Configuring, and Deploying the Dashboard

Step 1 Run the Sustainability Dashboard setup program (OrchestratorDashboardSetup.exe) on a computer with IIS 6.0 or later.

For details, see "Installing the Sustainability Dashboard" in the *Cisco EnergyWise Orchestrator Installation Guide*.

Step 2 Set account permissions in the SQL Server to allow IIS communication with the Server.

You need to create a new login and a new user for the IIS user account in the SQL Server and give the account permission to access Orchestrator database.

The IIS computer and SQL Server computer must be in the same domain. To support delegation (for remote IIS access), the server must run as a domain administrator, local system, or network service account (not as a local account). The network service account must have read and write access to the Orchestrator database.

See the "Configuring and Deploying the Dashboard" section on page 9-7 for details.

Step 3 (Optional) Determine the metadata that you want to import for grouping, configuring the database tables, and importing the data. By default, the dashboard groups data by Orchestrator administrative groups. Contact Cisco technical support for information on implementing metadata with the dashboard.

See the "Metadata and Summary Tables Used by the Dashboard" section on page 9-15 for details.

Step 4 Open the dashboard in your local browser, and click the **Global Settings** tab to set the values for the settings used to calculate report data for the dashboard.

The global settings determine the default values for the data summarization process and energy calculations. We recommend that you set these values before you run the summarization process for the first time to get the most accurate and uniform report results over time.

See the "Viewing the Sustainability Dashboard" section on page 9-8 for details.

Step 5 Run the summarization process (summarization.exe) to create the aggregated data that the dashboard uses for reports.

Step 6 Open the IIS web site dashboard in your web browser, and verify that the data is appearing in the dashboard.

See the "Viewing the Sustainability Dashboard" section on page 9-8 for details.

Step 7 Determine the security and location for dashboard access on your intranet.

- Copy the DashboardApp.swf file that displays the dashboard to the appropriate computer (if necessary).
- Determine the method that you want to use to pass tokens between the SWF file and the dashboard API.
- Create or modify a wrapper page for the dashboard with the appropriate server-side and client-side code to communicate with the dashboard API.

Step 8 Deploy DashboardApp.swf in a page on your intranet, and share the URL with users.

See the "Deploying the DashboardApp.swf File" section on page 9-17 and the "Code Sample" section on page 9-19 for details.

System Components

The Sustainability Dashboard installation program installs these components:

- All files required for displaying the Sustainability Dashboard, including the dashboard SWF file.
- The dashboard API (ASP.NET, hosted in IIS). Any client in your organization that needs access to the dashboard must be able to access the API Server on the IIS computer.

The following Orchestrator and Sustainability Dashboard components are required to deploy the dashboard on an intranet:

Table 9-1 Descriptions and Roles of the Dashboard Architecture Components

Component	Description and Role
Summary tables and data, Orchestrator database, metadata	The dashboard uses summarized data from summary tables in the Orchestrator database. By default, the dashboard creates groups for data based on Orchestrator administrative groups and device family. You can also to group data by other meaningful categories, such as business units, location, utility, and utility cost. You can filter data by hardware type and wattage. You can set up and import metadata in the summary tables to create the data groupings. Contact technical support for assistance with determining and importing metadata.
Summarization Process (DataSummarization.exe) and Scheduler	The report data displayed by the dashboard is summarized data that is generated when you run DataSummariziation.exe for Orchestrator. Data is summarized to the daily power management group level for the fastest possible display of report data in the dashboard. **Note** When Orchestrator is first installed, data must be generated before it can be summarized. When the Orchestrator server sends data to the database, the summarization process must wait until the data is fully committed before processing can begin. When the summarization process runs, it retrieves raw data from the Orchestrator database table, aggregates the data, and then writes the summarized data back into the appropriate tables. You will need to run the summarization process on a regular basis (daily or weekly) to keep the dashboard report data current. Use the Windows Task Scheduler to run the summarization process regularly.

Table 9-1 Descriptions and Roles of the Dashboard Architecture Components (continued)

Component	Description and Role
Sustainability Dashboard Web Site Services	The Sustainability Dashboard Web Site service must be installed and on a server running IIS 6.0. **Note** The computer with the dashboard web site and its related API files must be network-accessible to any user in the network who needs to display the dashboard. The installation creates a web site in IIS and the references to the required files, such as the SWF file (Adobe Flash) that displays the dashboard. You might need to copy the SWF file to another computer later, depending on how you implement the dashboard in your intranet. By default, the dashboard web site is installed in the root context of port 80 in IIS. You can change this to another port if necessary. You might want to create an alias for the computer. The charts and configuration of the dashboard are defined in XML elements in the default files provided with the dashboard. Contact Cisco technical support for assistance with customizing these files for custom dashboard views.
Dashboard SWF file	When the Flash-based dashboard application loads, it requests an XML-based configuration from the dashboard web site API. The configuration file name matches a config_id parameter that is passed to the Flash application by the page in which the dashboard is embedded. This configuration information determines the report types displayed in the dashboard, how they are laid out, and the initial filter settings.
Intranet with wrapper page for dashboard	To deploy the dashboard in your intranet, you need to create a wrapper page for the dashboard with the appropriate server-side and client-side code to communicate with the dashboard web site API. Flash 9.0.xx or higher must be installed on each client computer to display the dashboard.

Tasks, Roles, and Required Skills

Depending on your organization size and structure, different roles can be required for the installation, configuration, and deployment of the dashboard.

Table 9-2 Tasks, Roles, and Skills

Task	Role	Skills Required
Install dashboard components and set database connections.	The system administrator performs the installation and might communicate with a database, IT, or IIS administrator to set up IIS and database access.	• Orchestrator administrator with knowledge of Orchestrator Server, Database, and Client setup. • Knowledge of intranet network topology (particularly as it relates to Orchestrator Server/Database). • Knowledge of SQL Server and IIS.
Configure settings in the Sustainability Dashboard.	The system administrator configures Global Settings values to be used for dashboard reporting.	• Knowledge of SQL Server and IIS to ensure that the local version of the dashboard Administrator Console can be accessed in an Internet browser. • Knowledge of the organization energy use baseline (PC power consumption before Orchestrator was implemented). • Knowledge of the energy cost per kWh (averaged weighted value) for your organization. • (Optional) Knowledge of device-specific wattage for computers and monitors in different states.
Run the summarization process.	The system administrator runs the summarization process to create the data set for dashboard reports.	• Knowledge of Orchestrator server and database setup.
Deploy the dashboard on an intranet.	The web developer writes code for a wrapper page that displays the dashboard. The system administrator works with the web developer to develop a plan for presenting the dashboard: home page or portal, existing reporting page or dashboard, and so on.	• Knowledge of intranet presentation technology that your organization uses (such as SharePoint, static HTML, PHP, ASP.NET). • Knowledge of intranet authentication and identity management technology.

Table 9-2 Tasks, Roles, and Skills (continued)

Task	Role	Skills Required
(Optional) Determine and import metadata.	A system administrator, IT administrator, or database administrator might have to work with a professional service consultant to determine what data can be imported into the Orchestrator database for inclusion in dashboard reports.	• Knowledge of IT systems to determine organizational structures for reporting (such as IP address tracking, LDAP directory tree, computer names and users).
(Optional) Determine custom dashboard configurations.	A system administrator might have to work with a professional service consultant to determine customized dashboard views.	• Knowledge of organizational structures and reporting needs.

Configuring and Deploying the Dashboard

- Considerations, page 9-7
- Viewing the Sustainability Dashboard, page 9-8
- Troubleshooting, page 9-10
- Global Settings for Dashboard Reports, page 9-11
- Metadata and Summary Tables Used by the Dashboard, page 9-15
- Deploying the DashboardApp.swf File, page 9-17

Considerations

- Setting global values to use during the summarization process and also when displaying the dashboard.
- Optionally, adding organization metadata to the Orchestrator database to include in the summarization process.
- Creating a web page for the dashboard and deploying the dashboard on your intranet.
- Original and updated weighted average baseline energy use. The CPU and Display baselines that you use for the dashboard global settings determine how energy and cost savings are calculated.

Note For details, see the "Establishing the Baseline Level of Energy Usage" and "Generating the Baseline Numbers for Future Energy-Savings Reports" chapters in the *Cisco EnergyWise Orchestrator Installation Guide*. Contact Cisco EnergyWise Orchestrator Technical Support if you need assistance with determining your baseline energy use values.

- Orchestrator server and database setup diagram and descriptions (computers, network topology).
- Intranet network topology (particularly relating to Orchestrator).
- Intranet presentation technology that your organization uses (such as SharePoint, static HTML, PHP, ASP.NET).

- Intranet authentication/identity management technology (such as public/none, custom, Windows).
- Implementation plan for the dashboard on your intranet (such as home page, portal, existing reporting page, or dashboard).

Viewing the Sustainability Dashboard

When you first open the Sustainability Dashboard, you see a preview based on the settings on the Dashboard Preview tab.

Tabs available to administrators:

- Dashboard Preview displays the dashboard based on current Global Settings and the dashboard XML configuration file that is selected.

  The Dashboard Preview includes options for selecting the configuration file that is displayed for the dashboard and for selecting the parts of the interface to be shown or hidden in the dashboard preview.

  When you select options to hide various parts of the console interface, you can share the URL for the dashboard so that others can see these selected parameters. For example:

  ```
  http://sustain.yourCompany.local/dashboard-preview.aspx?config_id=Default&
  hide_panel=on&hide_tabs=on&hide_header_title=on
  ```

  Two default configurations are provided: Default and Two Time Period.

  - For details on the Default configuration, see the "Charts in the Default Configuration" section on page 9-21.
  - For details on the Two Time Period configuration, see the "Two Time Period Configuration" section on page 9-26.
- Dashboard Configuration provides options for creating, editing, deleting, and previewing the result of XML configuration files. For details on using the configuration editor and customizing the dashboard, contact Cisco Orchestrator Technical Support.
- Filter Builder provides a way to generate XML code to specify administrative groups, business units, locations, device families, and date ranges set for a custom dashboard filter. For details on using the Filter Builder, contact Cisco EnergyWise Orchestrator Technical Support.
- Global Settings determine the default values for data summarization, baseline calculations, and energy calculations. For more details, see the "Global Setting Options" section on page 9-12.
- Baseline Report provides tools for generating Data Availability and Baseline reports.

  The Data Availability report shows the number of clients reporting to the server each day during the specified period of time.

  For more details, see the "Gathering Data for and Creating Initial Power Management Policies" chapter in the *Cisco EnergyWise Orchestrator Installation Guide* and the "Data Availability Report" section on page 9-30.

  The Baseline report generates the baseline number for the average rate of energy use for the PC CPU and display during the specified 2-week period. Baseline numbers are used in future system-health and energy-savings reports.

For details, see the "Gathering Data for and Creating Initial Power Management Policies" chapter in the *Cisco EnergyWise Orchestrator Installation Guide* and "Baseline Report" section on page 9-31.

Open the Sustainability Dashboard

In your web browser, enter the URL for the web site on the computer where you installed the dashboard, such as http://*hostname*/*website*/API/default.aspx:

hostname = computer hosting the dashboard.

website = name of the web site specified during installation.

For example:

```
http://localhost/dashboard/api or http://myPCname.myDomain.local/dashboard/api
```

If the dashboard does not appear, follow the steps in the "Troubleshooting" section on page 9-10.

If Windows Firewall is enabled on the Orchestrator server, make sure that TCP port 80 is added to the exceptions list. For details, see the "Configuring Windows Firewall To Allow Server Access to Web Components" section on page 3-6.

Preview the Dashboard Configuration

Step 1 In your web browser, enter the URL for the web site on the computer where you installed the dashboard, such as *http://localhost/dashboard/api*.

If the dashboard does not appear, follow the steps in the "Troubleshooting" section on page 9-10.

Step 2 Click the **Dashboard Preview** tab in the Sustainability Dashboard.

Note Use the links in the dashboard interface to go to chart views, settings, and the main dashboard. Browser application buttons do not function within the dashboard application.

Change the Configuration Settings for Report Data

The default values defined in the Global Settings tab of the Sustainability Dashboard determine the default values for the data summarization process and the energy calculations. We recommend that you set these values before you run the summarization process for the first time so that you get the most accurate and uniform report results over time.

For details, see the "Global Setting Options" section on page 9-12.

For details on customizing the dashboard charts and layout, contact Cisco EnergyWise Orchestrator Technical Support.

Step 1 In your web browser, enter the URL for the web site on the computer where you installed the dashboard, such as h*ttp://localhost/dashboard/api.*

If the Administrator Console does not appear, follow the steps in the "Troubleshooting" section on page 9-10.

Step 2 Click the **Global Settings** tab in the Sustainability Dashboard.

Troubleshooting

Sustainability Dashboard: ASP.NET is Not Registered in IIS

If the Sustainability Dashboard does not open, make sure that the correct version of ASP.NET on the computer is properly registered with IIS.

This issue can occur when

- IIS was installed after the NET framework on the computer and multiple versions of ASP.NET are on the computer. Aspnet_regiis.exe must be run to create the correct IIS script mapping for the Sustainability Dashboard application.
- The 32-bit version of the .NET framework was installed on a computer running a 64-bit operating system.

You can run the ASP NET IIS Registration Tool (Aspnet_regiis.exe) to

- Display the status of all installed versions of ASP NET.
- Register the ASP.NET version that is coupled with an application.
- Create client-script directories and perform other configuration operations.

This tool is available on MSDN at ASP.NET IIS Registration.

This command line installs the ASP.NET version that is associated with the ASP.NET IIS Registration tool and updates the script maps of all ASP.NET applications. Note that only the applications that are currently mapped to an earlier version of ASP.NET are affected. Be sure to run this command line from the correct location:

```
<.NET installDir>\aspnet_regiis.exe -i
```

For example:

```
C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727>aspnet_regiis.exe -i
```

Sustainability Dashboard: Virtual Directory Not Configured as an Application

If you are running IIS 7.0 and ASP.NET is enabled, but the Sustainability Dashboard does not open, you might need to configure the virtual directory for the dashboard web site as an application in IIS.

Step 1 In IIS Manager under Web Sites or Sites (depending on your version of IIS), expand the Dashboard web site, right-click the API directory, and click **Convert to Application**.

Step 2 Click the **Dashboard** web site icon, and under Actions, click **Enable**.

Administrator Console: Correct Version of ASP.NET Not Enabled in IIS

If the Sustainability Dashboard does not open when you try to see it and multiple versions of ASP.NET are installed on your computer where you installed the dashboard API, you might need to select the correct version of ASP.NET in IIS manager.

To see the Administrator Console from the IIS web site, ASP.NET version 2.0.50727 must be enabled in IIS.

Step 1 In IIS Manager under Web Sites or Sites (depending on your version of IIS), right-click the Dashboard web site, and then click **Properties**.

Step 2 In the Default Web Site Properties dialog box, click the **ASP.NET** tab, and for the ASP.NET version, select **2.0.50727**.

Step 3 Click **OK**.

Global Settings for Dashboard Reports

The default values in the Global Settings tab of the Sustainability Dashboard determine the default values for the data summarization process and energy calculations.

For accurate and uniform report results over time, set these values before you run the summarization process in Orchestrator for the first time.

If you change a setting, the updated values do not appear in your dashboard reports until you run the summarization process again.

Because data is summarized on an incremental basis after the first time you run the process, only data that is collected and reported on from the time of the change reflects the new values. Historical data is still based on the old values. To reset summarization data and then resummarize the data based on the new settings, see Reset summarization data.

Changes to Global Settings values affect summarized data:

- Energy cost per kWh and currency
- CO_2 kilogram emissions per kWh
- CO_2 kilogram equivalent of one car saved
- CO_2 kilogram equivalent of one tree saved
- CO_2 kilogram equivalent of 1 liter of gas saved
- Watt consumption values: CPU On, CPU Off, CPU Suspend, CPU Hibernate, Display On, Display Suspend, Display Off

Note Accurate data reporting depends on accurate baseline energy use values. Accuracy also depends on when the summarization process was last run and the number of clients reporting to Orchestrator at that time.

Global Setting Options

Table 9-3 Global Settings in the Sustainability Dashboard Administrator Console

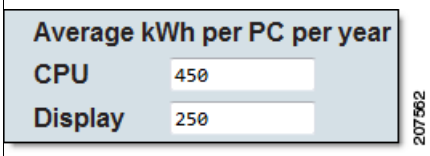
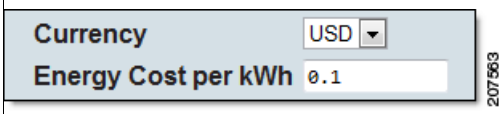
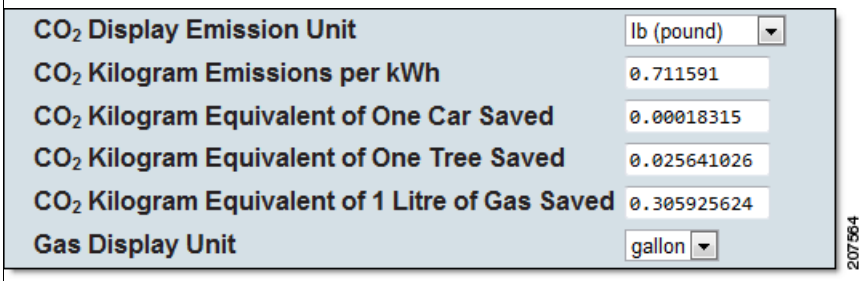
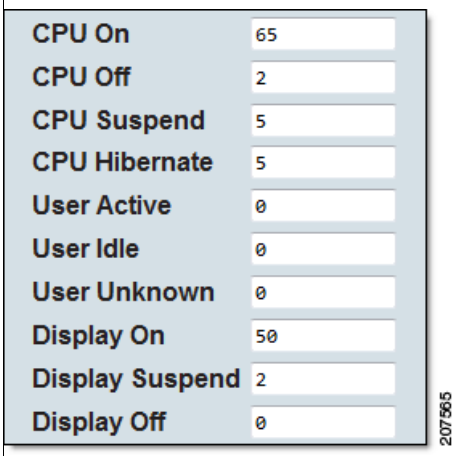
Option	Description
Baseline Energy	A baseline value represents the base energy usage of PCs and monitors before using Orchestrator power management policies. The baseline value is the most important default global setting, as it is used in calculations to determine energy and cost savings. Enter the energy usage value from the baseline data collection phase. If you do not have separate values for CPU and Display, enter the sum of the CPU and Display values in the CPU field, and enter 0 in the Display field.  Use only the actual baseline number. Setting this number to another value that is not based on real data results in inaccurate report information. **Note** The baseline is a weighted average determined by monitoring a representative set of workstations for a 2-week period before using power management policies. For details on determining the baseline number, see the "Gathering Data for and Creating Initial Power Management Policies" chapter in the *Cisco EnergyWise Orchestrator Installation Guide*.
Energy Costs	Specify the cost per kWh based on the utilities used. These values determine the cost of energy consumed and the amount of money saved. The cost/kWh should be the weighted value averaged across all utilities.  If you do not change this value on the global settings page before running the summarization process for the first time, the summarization uses an energy rate default value of 0.1 kWh/USD.

Table 9-3 Global Settings in the Sustainability Dashboard Administrator Console (continued)

Option	Description
CO_2 Emissions	Enter the appropriate conversion factor values to show the environmental impact of power management. The default display units are provided. Authoritative carbon equivalent values are available from the Environmental Protection (Calculations).  Links to reference information and calculators: • Green Power Partnership Tools • Clean Energy Calculations • Greenhouse Gas Equivalencies
CPU and Monitor Watt Consumption	These default values can be used for CPUs and monitors that do not have device-specific wattage assignments.  The default values are weighted averages for different CPU and monitor states. The values are based on client data collected over time and represent a typical, modern (4 years old or less) PC used for business. If you have device-specific wattage assignments based on specific watt measurements of different devices (using a watt meter such as the WattsUp Pro, Brultech EML-2020, or Kill-A-Watt meter), you can enter those values.

Default Data Values

Default values used for Global Settings in the Sustainability Dashboard:

Table 9-4 Default Values for Global Settings in the Sustainability Dashboard

Global Setting	Default Value
Ave Kwh per PC	700
kWhEnergyCost	$0.10
kWhEmission	1.712992 CO_2 pounds/kWh
lastUpdateDate	1/1/2000
currencyId	USD
emissionUnitId	lb (pound), kg (kilogram), ton (2000 lb), metric tonne
Gallons	(US only) $8.81*10^{-3}$ metric tons CO_2/gallon (gallons is used by default)
Liters	UK $8.81*10^{-3}$ metric tons CO_2/3.78541178 liters
One Urban Tree	.039 metric ton CO_2 per urban tree planted
Cars	5.46 metric tons CO_2E /vehicle/year
Currency	AUD, CAD, CHF, EUR, GBP, JPY, SEK, USD

How Dashboard Data is Calculated

Links to www.epa.gov

- Green Power Partnership Tools and Calculators
- Clean Energy Calculations and References
- Greenhouse Gas Equivalencies Calculator

Passenger Vehicles Per Year

To determine annual greenhouse gas (GHG) emissions per passenger vehicle:

- Vehicle miles traveled (VMT) is divided by average gas mileage to determine gallons of gasoline consumed per vehicle per year.
- Gallons of gasoline consumed is multiplied by carbon dioxide per gallon of gasoline to determine carbon dioxide emitted per vehicle per year.
- Carbon dioxide emissions are divided by the ratio of carbon dioxide emissions to total vehicle greenhouse gas emissions to account for vehicle methane and nitrous oxide emissions.

For more information, visit the EPA website:
http://www.epa.gov/cleanenergy/energy-resources/refs.html

Sample Calculation

Note Due to rounding, the calculations return approximate values.

8.81(10^{-3} metric tons CO_2/gallon gasoline)
* 11,856 VMT car/truck average
* 1/19.7 miles per gallon car/truck average
* 1 CO_2, CH_4, and N_2O / 0.971 CO_2
= 5.46 metric tons CO_2E /vehicle/year

Gallons of Gasoline Consumed

Average heat content of conventional motor gasoline is 5.22 million btu per barrel (EPA 2007).

Average carbon coefficient of motor gasoline is 19.33 kg carbon per million btu (EPA 2007).

Fraction oxidized to CO_2 is 100 percent (IPCC 2006).

Carbon dioxide emissions per barrel of gasoline are determined by multiplying heat content times the carbon coefficient times the fraction oxidized times the ratio of the molecular weight ratio of carbon dioxide to carbon (44/12). A barrel equals 42 gallons.

Sample Calculation

Note Due to rounding, the calculations return approximate values.

22 mmbtu/barrel
* 19.33 kg C/mmbtu
* 1 barrel/42 gallons
* 44 g CO_2/12 g C
* 1 metric ton/1000 kg
= $8.81*10^{-3}$ metric tons CO_2/gallon

Number of Tree Seedlings Grown For 10 Years

A medium growth coniferous tree, planted in an urban setting and allowed to grow for 10 years, sequesters 23.2 lbs of carbon.

Sample Calculation

Note Due to rounding, the calculations return approximate values.

2 lbs C/tree
* (44 units CO_2 / 12 units C)
* 1 metric ton / 2204.6 lbs
= 0.039 metric ton CO_2 per urban tree planted

Metadata and Summary Tables Used by the Dashboard

By default, the Sustainability Dashboard reports energy savings and consumption based on administrative groups created in Orchestrator.

The dashboard can show this information based on other dimensions, such as business unit (organizational structure, department) and location (geography,location-specific utility rate).

To use these optional reporting views, you need to import this information (metadata), preferably before running the summarization process for the first time. The approach you take for importing metadata into Sustainability Dashboard summary tables depends on how your desktop infrastructure is organized.

- Number of business units and physical locations
- Number and name of utilities that provide electricity
- Descriptions of standard hardware profiles (from CECA or implementation process)
- Description of any available metadata sources (IP addresses, Active Directory structures, LDAP directory trees, other management system, spreadsheets)

Note For assistance setting up and importing metadata in the database, contact Cisco EnergyWise Orchestrator Technical Support.

Database Tables Used by the Sustainability Dashboard

The tables used by the dashboard are in the Orchestrator database. Some of the tables are used internally. You can populate other tables to customize your dashboard configuration.

The summary tables used by the Sustainability Dashboard correlate data between administrative groups, business units, and locations.

Note For assistance setting up and importing metadata in the Orchestrator database, contact Cisco EnergyWise Orchestrator Technical Support.

Table 9-5 Tables Required for Imported Data

Table Purpose	Table Names
Main tables	ComponentStateDaySum, ComponentStateHourSum
Collection tables	Collection, CollectionType, DeviceCollection, UtilityRate The Collection table is used to specify a custom organization for data. The data organization can be by business unit (sales, marketing), location (Seattle, New York), for example. Location can link to a specific utility and utility rate. UtilityRate is tied only to Location. You must define this value for collections before the summarization process runs, and every time a new client is added. Otherwise, the Global Settings tab values are used. **Note** PeakStartTime and PeakEndTime for utility rates must be in UTC (Coordinated Universal Time).
Device state, type, and wattage	Component, ComponentState, ComponentType, DeviceComponentStateDraw, ComponentTypeStateDraw, AdminGroup, DeviceFamily, Device

Table 9-5 Tables Required for Imported Data (continued)

Table Purpose	Table Names
Global settings	Global Attribute, GasUnit, Currency, EmissionUnit
Summary process	SumTableLastLoad
API-related tables	Application, Config

Collection Tables

The Sustainability Dashboard uses the Collection table to identify grouping structures for report data from clients. The Collection table is a way to structure data to fit your needs.

A collection has an ID, a name, and a type (such as business unit or location).

Strategies for Determining Your Collections

In determining the collections you might need and the metadata you will need to import:

- Top-down—The existing organizational structures do you use and the data collection process for those structures
- Bottom-up—The available data that can be leveraged for reports

Large organizations can use the IP address, LDAP, or computer name to assign clients to a business unit or a location.

- IP address— IP addresses often have some relationship to a physical location. If you create a collection based on IP address, you need to determine how the IP addresses map to a physical location (such as building numbers or cubical numbers). Use the system that you have in place to map IP address to location.
- LDAP directory tree—The LDAP often reflects various geographic or organizational boundaries or an internal IT structure.
- Computer—If your organization keeps track of each computer and who it belongs to, you can use this to determine the grouping for different sets of clients.

Deploying the DashboardApp.swf File

There are several different options for how you deploy the dashboard, depending on how accessible or public you want the dashboard to be.

- Intranet URL with IP address
- Intranet with permissions
- Embedded in a SharePoint site as a web part - use a web part for embedding Flash or use JavaScript in SharePoint Designer Source view (not Design View).

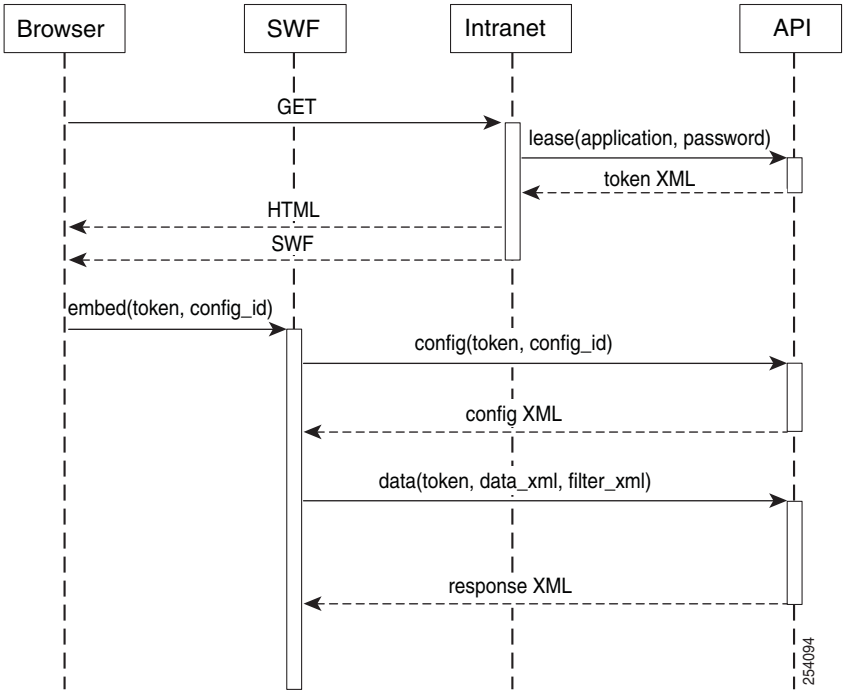
If you need ID management for dashboard access, use the same system that you use for your intranet to make the dashboard secure and to authorize users to access the dashboard.

Note For assistance with deploying the dashboard on your intranet, please contact Cisco EnergyWise Orchestrator Technical Support.

API Tokens and Security

The dashboard uses a token-based security model. If you are deploying the dashboard in your intranet, you need to copy the DashboardApp.swf file from the IIS computer to the computer that hosts your intranet and create a wrapper page for the SWF file. You also need to provide code to use the API tokens for authentication.

Figure 9-2 Service-Level Sequence Diagram



When the dashboard is installed, there are no default security restrictions. The SWF file must reference the computer that hosts the API.

Note All client computers needing to display the dashboard must have network connectivity to the computer hosting the API.

When the dashboard loads on a client computer, it makes an API call using the Lease method to get the named XML configuration. The Lease method generates security tokens. If you are displaying the dashboard on your intranet, your intranet needs to acquire and pass the tokens to the dashboard on each client.

The DashboardApp.swf file needs this information:

- The location of the API (computer name or domain name)
- Code that dynamically generates the token or a static Lease method call.
- The specific name of the XML configuration file that serves as the template for the dashboard, for example, config-id: “Default”.

The SWF file references swfobject (http://code.google.com/p/swfobject and also needs to reference the computer that hosts the API.

A web developer needs to edit a PHP, HTML, SharePoint, or ASP.NET page to dynamically generate a token using the Lease method or to manually generate the token and paste it in the code.

Note For assistance with deploying the dashboard on your intranet, contact Cisco EnergyWise Orchestrator Technical Support.

By default, tokens expire after 1 hour. If you use static HTML to display the dashboard, you need to change the expiration time to never expire. You can change the expiration time in the timeout_mri element in the Application table in the Orchestrator database.

A token that you paste into a static HTML page never expires after you set this property in Orchestrator database. Therefore, this practice is less secure.

Code Sample

This topic is a simple example of ASP.NET code that could be used in a wrapper page that facilitates server-side and client-side communication between the SWF file and the API.

Note For assistance with deploying the dashboard on your intranet, please contact Cisco EnergyWise Orchestrator Technical Support.

ASP.NET example code that could be used in a wrapper page that facilitates server-side and client-side communication between the SWF file and the API.

This example code dynamically requests a token through Sustainability Dashboard web service:

```
<%@ Page Language="C#" %>
<%
    string application = "dashboard";
// must match a row in the Application table of your Orchestrator database
    string password = "green";
    string config_id = Request["config_id"];
    if (String.IsNullOrEmpty(config_id)) config_id = "default";
    string api_prefix = "http://sustain.mycompany.local/api.asmx/";
    string token;

    System.Net.WebRequest request = System.Net.WebRequest.Create(api_prefix +
"lease" + "?" + "application=" + HttpUtility.UrlEncode(application) + "&" + "password=" +
HttpUtility.UrlEncode(password));
    System.Net.WebResponse response = request.GetResponse();
    // TODO: check for and handle error
    System.Xml.XmlReader xmlReader =
 System.Xml.XmlReader.Create(response.GetResponseStream());
    xmlReader.ReadStartElement();
    token = xmlReader.ReadContentAsString();
    response.Close();
%>
```

This example code creates an HTML layout in which the dashboard appears on the page:

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN"
"http://www.w3.org/TR/html4/strict.dtd">
<html>
<head>
<title>Green Portal</title>
<script type="text/javascript"
src="http://ajax.googleapis.com/ajax/libs/swfobject/2/swfobject.js">
</script>
```

```
<script type="text/javascript" src="resizeswf.js"></script>
<style type="text/css">
html, body, #resizeContainer, #dashboard { height: 100%; overflow-y: hidden; }
</style>
</head>
<body>
<img style="float: right;" src="http://www.mycompany.com/greenportal/logo.gif">
<h2>Green Portal</h2>
<div id="resizeContainer">
    <div id="dashboard">
    <a href="http://www.adobe.com/go/getflashplayer">
   <img src="http://www.adobe.com/images/shared/download_buttons/get_flash_player.gif"
alt="Get Adobe Flash player" /></a>
    </div>
</div>
<script type="text/javascript" defer="defer">
// <![CDATA[
// NOTE: Typically you would copy the DashboardApp.swf to the current
// directory and not need an absolute URL
```

The example code embeds the SWF file in the wrapper page:

```
swfobject.embedSWF(
    "http://sustain.mycompany.local/dashboard/DashboardApp.swf","dashboard",
"100%", "100%","9","http://sustain.mycompany.local/dashboard/expressInstall.swf",
    // URL provided is the location of Dashboard SWF
    // “dashboard” is the id of div that will be replaced by the dashboard
    // “100%”,“100%” is the width and height of the dashboard
    // “9” is the minimum Flash Player version
        {
            api_prefix: "<%= api_prefix %>",
            api_token: "<%= token %>",
            config_id: "<%= config_id %>",
            locale: navigator.browserLanguage
        },
        { menu: "false" },
        { id: "DashboardApp", name: "DashboardApp"}
    );
window.onresize = resizeswf;
resizeswf();
<script>
</body>
</html>
```

Chart Types and Filters

- Charts in the Default Configuration, page 9-21
- Viewing Energy Savings for PCs, page 9-24
- Two Time Period Configuration, page 9-26
- Change Filter Settings, page 9-27
- Date Filter Settings, page 9-27
- Date Grouping Options, page 9-29
- Data Group Settings, page 9-29
- Display Members of Data Groups, page 9-29

Charts in the Default Configuration

The Default configuration of the dashboard provides charts with different views on energy usage and savings. For details on customizing the charts and layout of the dashboard, contact Cisco EnergyWise Orchestrator Technical Support.

The Sustainability Dashboard reports on energy savings and cost based on the baseline values and displays charts and summary reports based on summarized data from your Orchestrator database.

The data that users see in the dashboard is determined by the data in the Orchestrator database, when the summarization process was last executed, the number of clients reporting to date, the energy use baseline value (determined during Orchestrator implementation), and how you are currently enforcing power management.

Report types available by default in the Sustainability Dashboard:

- Gauge—Gauge display that shows power consumption levels during power management enforcement compared to baseline power consumption levels measured before enforcement
- Pie—Pie chart that shows power consumption levels by device family
- Summary—Text report with summary figures and text
- Time Series—Time-series line chart with dates on the horizontal axis
- Category Series—Column or bar chart that can include stacked data

Table 9-6 Dashboard Components

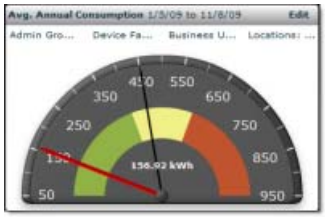
Dashboard Component	Description
Average Annual Consumption Gauge  207567	The gauge shows the annualized weighted average for PC energy consumption (by default). The black line represents the baseline value (power consumption before power management settings. The red line represents current power consumption levels. **Note** The baseline value in the gauge does not necessarily match the CPU and Display baseline values in Global Settings. It reflects an annualized weighted average of the clients that reported into Orchestrator during the specified date range. If there are gaps in reporting for some clients or an entire year of data is not available, the baseline value displayed in the gauge is adjusted to account for gaps in data. The default date range filter is set to Latest 4 Weeks to show the cumulative savings since Orchestrator was implemented. By default, the Device Families filter displays data only for PCs. If someone viewing the dashboard selects another type of device under Device Families (Service, Access Point, Interface, Phone, Router, Switch), the gauge returns the values for those device types. The gauge needle will be close to zero. You can create a custom gauge for a given device type and customize the ranges in the gauge to reflect the power consumption of that device type.
Total Savings Summary Report  207568	This summary report shows savings in units of dollars (or another currency set on the Global Settings tab), energy in kWh, and CO_2 in lbs or another emission unit as set in Global Settings. The default date range filter is set to All to show the cumulative savings since Orchestrator was implemented. The default Device Families filter is set to All.
Total Green Savings Summary Report  207569	This summary report shows savings in units of gallons of gasoline (or liters, as set in Global Settings), number of trees saved, or number automobiles kept off the road. The default date range filter is set to All to show the cumulative savings since Orchestrator was implemented. The default Device Families filter is set to All.

Table 9-6 Dashboard Components (continued)

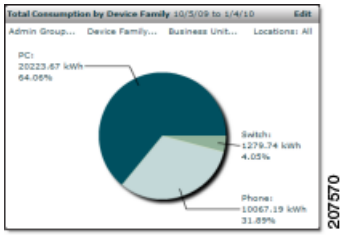
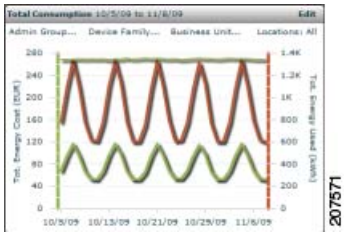
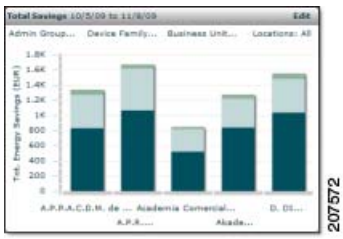
Dashboard Component	Description
Total Consumption by Device Family Pie Chart  	Shows total kWh of energy used by each device family. The default date range filter is set to Latest 13 Weeks. The default Device Families filter is set to All.
Total Consumption / Total Energy Used Time Series Line Chart  	Shows total energy cost (money) and energy used (kWh) across groups. Place your cursor on any point on the Total Energy Cost line to see total energy costs (based on the selected currency) on a particular point in time. Place your cursor on any point on the Total Energy Used line to see total energy used (based on the selected currency) on a particular point in time. Select **Show Right Axis** to include data on Total Energy Used. Select **Show Baseline** to display the baseline as a comparison. **Note** The baseline value displayed in the chart does not necessarily match the CPU and Display baseline values in Global Settings. It reflects a weighted average of the clients that reported into Orchestrator during the specified date range. If there are gaps in reporting for some clients or an entire year of data is not available, the baseline value displayed in the Gauge is adjusted to account for gaps in data. Select a Grouping option (Day, Week, Month, Quarter) to change the display of the time periods. The default date range filter is set to Latest 13 Weeks, and grouping is set to Daily. The default Device Families filter is set to All.
Total Savings Category Series Stacked Bar Chart  	Shows groups sorted in descending order by amount of money saved. Shows savings by device family, stacked in each bar. Place your cursor over a bar to see details on money saved and the percentage of energy reduction. By default, all groups are included. The top five groups appear, sorted in descending order by amount of money saved in the date range. When you select specific groups, only those groups are sorted in descending order, and the top five are shown. The default date range filter is set to Latest 13 Weeks. The default Device Families filter is set to All.

Table 9-6 Dashboard Components (continued)

Dashboard Component	Description
Average Consumption Category Series Bar Chart 	Shows groups sorted in ascending order by average amount of kWh consumed in the date range. Place your cursor over a bar to see the group name, energy used, and reduction percentage (calculated using the baseline). By default, all groups are included. The top five groups appear, sorted in ascending order (from lowest to highest) by the average amount of kWh consumed in the date range. When you select specific groups, only those groups are sorted in ascending order, and the top five are shown. The default date range filter is set to Latest 13 Weeks. The default Device Families filter is set to All.

Viewing Energy Savings for PCs

The Default configuration for the dashboard shows data for PCs only in the Average Annual Consumption gauge and all device families with data available in the following charts: Total Savings summary chart, Total Energy Savings summary chart, Total Consumption pie chart, Total Consumption line chart, Total Savings stacked bar chart, and Average Consumption stacked bar chart.

To display savings only for PCs in all charts, select the **PC** option under Devices Families in Filter Settings. To display only PC data by default, edit the Default configuration file. For details, see the "Editing the Default Configuration File To Show Data For PCs Only" section on page 9-25.

Step 1 In the Sustainability Dashboard administrator console, click the Dashboard Preview tab.

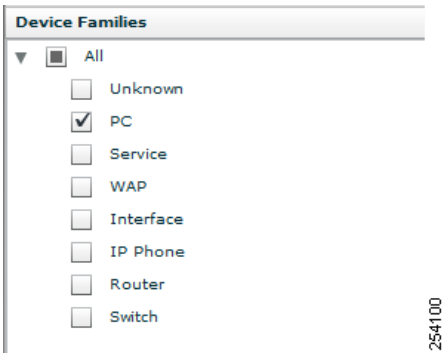
If it is not already selected, select **Default** as the configuration, and then click **Load**.

Step 2 For each chart in which you want to display PC data only, click **Edit** in the chart.

Step 3 In Filter Settings, click **Device Families**.

Step 4 Clear all of the device types except for PC.

Figure 9-3 Clear Device Types

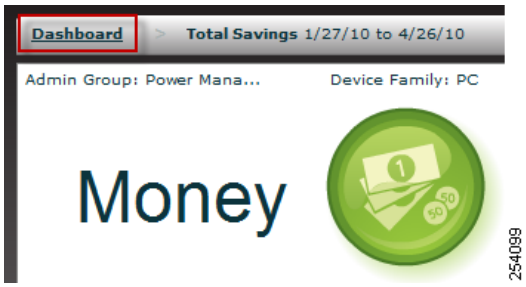


Tip A fast way to do this is to clear **All** and select **PC**.

Step 5 Click **Update**.

Step 6 Click the **Dashboard** link in the top left corner of the chart to display the dashboard with the updated data.

Figure 9-4 Dashboard



Editing the Default Configuration File To Show Data For PCs Only

To only display PC data, add the <collections> element to the configuration file within the <filter> element in the XML code of the default configuration file.

Step 7 In the Sustainability Dashboard administrator console, click the Dashboard Configuration tab.

Step 8 Under Available Configurations, for Default, click **Edit**.

Step 9 Scroll to each filter section in the XML code and paste the following code just before the `</filter>` element end:

```
<collections>
  <collection_type name="device_family">
    <collection collection_id="1">
      <name>PC</name>
    </collection>
  </collection_type>
</collections>
```

For example, where you see:

```
<filter>
  <date_range range_id="latest_4_weeks" />
</filter>
```

You would paste the *collections* element just before the `</filter>` element end with the following result:

```
<filter>
  <date_range range_id="latest_4_weeks" />
  <collections>
    <collection_type name="device_family">
      <collection collection_id="1">
        <name>PC</name>
      </collection>
```

```
      </collection_type>
    </collections>
  </filter>
```

Step 10 Click **Save** in the XML window (or **Save & Preview**).

Step 11 Click the Dashboard Preview tab to display the updated Default configuration.

You might need to select **Default** as the configuration and then click **Load**.

Two Time Period Configuration

The Two Time Period report configuration shows average annualized consumption, average annualized savings, and total consumption for PCs during the latest 4 weeks compared to the baseline period.

Configure the Baseline Date Range for the Two Time Period Report

To show the Two Time Period data, update the baseline row in the NamedDateRange table of the EnterprisePowerManagmentDB database.

Note By default, the Device Families filter is set to display data only for PCs. If someone viewing the dashboard selects another type of device under Device Families (Service, Access Point, Interface, Phone, Router, Switch), the gauge returns the values for those device types. The gauge needle will be close to zero (because many EnergyWise devices consume a fraction of power that a PC consumes).

Step 1 Connect to the Orchestrator database server.

Step 2 Click **New Query**.

Step 3 In the SQL Editor toolbar, select **EnterprisePowerManagementDB** from the drop-down list of available databases.

Step 4 Enter this SQL statement in the query window:

```
update NamedDateRange
set StartDate = '<YYYY-MM-DD>',
    EndDate = '<YYYY-MM-DD>'
where Name = 'baseline'
```

where *YYYY-MM-DD* is a valid date.

Step 5 Replace the given date values with the values you determined to be the baseline period (from the Data Availability report). For details, see the "Gathering Data for and Creating Initial Power Management Policies" chapter in the *Cisco EnergyWise Orchestrator Installation Guide*.

Step 6 Click **Execute**.

Note To see the current date range settings for the baseline row, enter this SQL statement:

```
select * from NamedDateRange
```

and click **Execute**.

By default, the Device Families filter displays data only for PCs. If someone viewing the dashboard selects another type of device under Device Families (Service, Access Point, Interface, Phone, Router, Switch), the gauge returns the values for those device types. The gauge needle will be close to zero. (Most EnergyWise devices consume a fraction of power that a PC consumes.)

For results that are more informative, you need to create a custom gauge for a given device type and customize the ranges in the gauge to reflect the power consumption of that device type.

Change Filter Settings

Step 1 Click Edit on a chart.

Step 2 Click **Fixed** and select a date setting in the dropdown list. Or, click **Custom** and select a *From* date and a *to* date.

Step 3 Click **Update**. Changes you make to the dashboard exist for the current browser session.

Step 4 To return to the main dashboard, click the **Dashboard** link near the top left of the chart or the **Close** link near the top right of the chart.

Note When you are viewing the Sustainability Dashboard, use the links in the dashboard interface to navigate between chart views, settings, and the main dashboard view. Internet browser navigation buttons do not function within the dashboard application.

Date Filter Settings

Table 9-7 Date Range Settings for Dashboard Reports

Table Purpose	Table Names
All	Reports on data collected since Orchestrator has been installed and running.
Current Month	Reports on data collected between the first day of the current month through today.
Current Quarter	Reports on data collected between the first day of the current quarter through today.
Current Year	Reports on data collected between January 1 of the current year through today.
Previous Month	Reports on data collected between the first day though the last day of the previous month.
Previous Quarter	Reports on data collected between the first day data of the previous quarter though the last day of the third month in the previous quarter.
Previous Year	January 1 of the previous year though December 31 of the previous year.
Latest 4 Weeks	Includes the week that ended on the nearest previous Saturday and the 3 weeks preceding that.
Latest 13 Weeks	Includes the week that ended on the nearest previous Saturday and the 12 weeks preceding that.

Table 9-7 Date Range Settings for Dashboard Reports (continued)

Table Purpose	Table Names
Latest 52 Weeks	Includes the week that ended on the nearest previous Saturday and the 51 weeks preceding that.
Rolling 365 Days	Includes the previous 365 days, ending yesterday.
Baseline	This setting is a custom date range defined for the baseline row in the NamedDateRange table of the Orchestrator database. For details on using and configuring the baseline date setting, see Configure the the "Configuring the Baseline Date Setting" section on page 9-28.

The *latest* date filter options report on week-based cycles to show usage patterns.

To change the default date settings for charts, you must edit the configuration file. For details on customizing Sustainability Dashboard charts and layout, contact Cisco EnergyWise Orchestrator Technical Support.

Configuring the Baseline Date Setting

The **baseline** date setting is a custom date range defined for the baseline row in the NamedDateRange table of the Orchestrator database.

The baseline date range is used by default in the Two Time Period configuration. To show the correct data in the Two Time Period configuration, you will need to update the baseline row.

Step 1 Connect to the Orchestrator database server.

Step 2 Click **New Query**.

Step 3 In the SQL Editor toolbar, select **EnterprisePowerManagementDB** (the Orchestrator database) from the drop-down list of available databases.

Step 4 Enter this SQL statement in the query window:

```
update NamedDateRange
set StartDate = '<YYYY-MM-DD>',
    EndDate = '<YYYY-MM-DD>'
where Name = 'baseline'
```

where *YYYY-MM-DD* is a valid date.

Step 5 Replace the given date values with the values you determined as the baseline period (from the Data Availability report). For details, see "Selecting the 2-Week Baseline Period" in the *Cisco EnergyWise Orchestrator Installation Guide*.

Step 6 Click **Execute**.

Step 7 To see the current date range settings for the baseline row, enter this SQL statement:

select * from NamedDateRange

and click **Execute**,

Date Grouping Options

The grouping options for the Total Savings and Total Consumption time series line charts provide different views of trends, based on day, week, month, or quarter.

Table 9-8 Grouping Options for Total Savings and Total Consumption Charts

Table Purpose	Table Names
Day	Total energy savings and consumption for each day in the date range.
Week	Total energy savings and consumption for each week in the selected date range.
Month	Total energy savings and consumption for each month in the selected date range.
Quarter	Total energy savings and consumption for each quarter in the selected date range.

Data Group Settings

Click **Edit** in a chart and select or deselect specific members of the groups. Then select or clear the checkboxes next to the member names.

- Administrative Groups
- Device Families (PC, Service, Interface, Access Point, Phone, Switch, Router, or Unknown)
- Business Units (if implemented by metadata)
- Locations (if implemented by metadata)

If you import metadata and create other collections in the database, other groups might be available.

To change the default data group settings for charts, edit the configuration file. For details on customizing Sustainability Dashboard charts and layout, contact Cisco EnergyWise Orchestrator Technical Support.

Display Members of Data Groups

Step 1 Click **Info** on a chart to display the members of groups being used for chart, table, or gauge data.

Step 2 Click **Done** to return to chart view.

Note When you are viewing the Sustainability Dashboard (or users in your organization are viewing the deployed dashboard), use the links provided in the dashboard interface to navigate between chart views, settings, and the main dashboard. Internet browser navigation buttons do not function within the dashboard application.

Sustainability Dashboard Reports

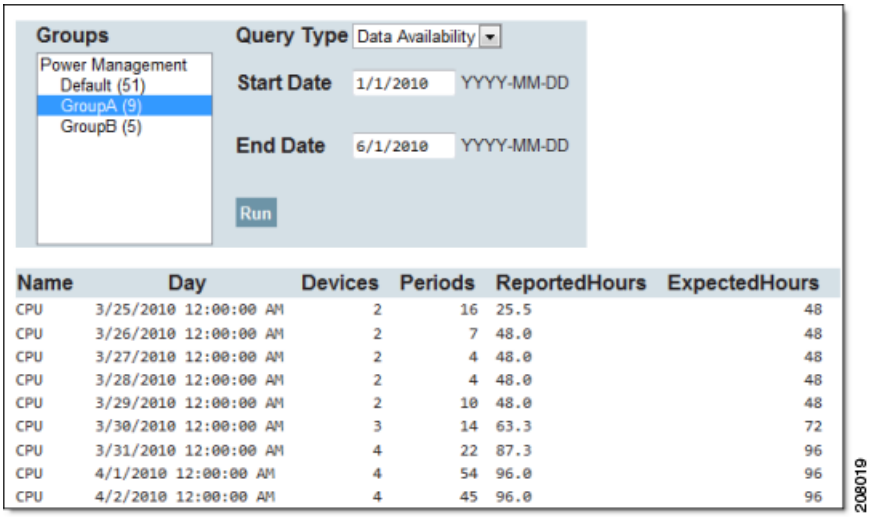
- Data Availability Report, page 9-30
- Baseline Report, page 9-31

Data Availability Report

The Data Availability report provides information on when PC data is available for PC clients so that you can determine a baseline start and end date and generate a Baseline report.

The Data Availability report displays a table showing data for every day for which data has been reported in the specified date range and administrative group.

Figure 9-5 Data Availability Report



Name	Day	Devices	Periods	ReportedHours	ExpectedHours
CPU	3/25/2010 12:00:00 AM	2	16	25.5	48
CPU	3/26/2010 12:00:00 AM	2	7	48.0	48
CPU	3/27/2010 12:00:00 AM	2	4	48.0	48
CPU	3/28/2010 12:00:00 AM	2	4	48.0	48
CPU	3/29/2010 12:00:00 AM	2	10	48.0	48
CPU	3/30/2010 12:00:00 AM	3	14	63.3	72
CPU	3/31/2010 12:00:00 AM	4	22	87.3	96
CPU	4/1/2010 12:00:00 AM	4	54	96.0	96
CPU	4/2/2010 12:00:00 AM	4	45	96.0	96

- Name—Specifies whether the data is from a CPU or display.
- Day—The date for which data was reported.
- Devices—Specifies the number of devices reporting any data for a specific day (not necessarily for the entire day).
- Periods—The number of periods (any continuous period) in which a CPU or display was in a particular state.
- Reported Hours—Specifies the number of hours actually reported in the DeviceComponentStatePeriod table. The number might be less than the expected hours, depending on when PCs came online.
- Expected Hours—The number of devices multiplied by 24 hours.

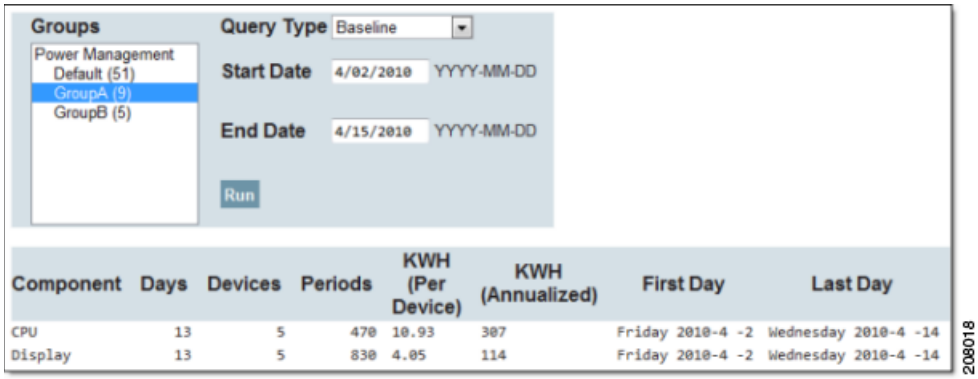
For details on determining which 2-week period is the best for calculating the baseline, see the "Selecting the 2-Week Baseline Period" chapter in the *Cisco EnergyWise Orchestrator Installation Guide*.

Baseline Report

The Baseline report calculates the baseline numbers for PC devices (CPU and Display) based on a specified date range. Use the date range for the values of the Average kWh per PC per year setting in the Global Settings tab.

The Baseline report presents the energy consumed by CPUs and Displays (per device and annualized) for the specified administrative group and date range, which represents the baseline period of reporting.

Figure 9-6 Baseline Report



- Component—The type of device (CPU or Display).
- Days—The number of days in the baseline reporting period.
- Devices—The number of devices in the reporting period.
- Periods—The number of periods in which a CPU or Display was in a particular state (any continuous period where a device was in a particular state).
- kWh (Per Device)—The calculated kWh (based on given wattages on the Global Settings page) for the component.
- kWh (Annualized)—The kWh calculated and annualized (based on given wattages on the Global Settings page) for the component.
- First Day—The date of the first day of the reporting period.
- Last Day—The date of the last day of the reporting period.

For details about the baseline report, see the “Generating the Baseline Numbers for Future Energy-Savings Reports” chapter in the *Cisco EnergyWise Orchestrator Installation Guide*.

CHAPTER 10

Troubleshooting

- Power Management Processor Is Not Running, page 10-1
- Pressing Power Button Does Not Wake Computer, page 10-2

Power Management Processor Is Not Running

The power management processor serves many critical functions. This topic lists symptoms that can mean that it has stopped running.

The power management processor runs as a Windows service, and it should be configured to start automatically. If it does not, or if it is running and something stops the processor, any of these symptoms can occur:

- Device check-ins are not processed.

  The Device Status column in the Administrator console is not correctly updated. For example, you might see inactive devices marked as active or the reverse. If the Last Connected column appears, it is not updated for active devices.
- Wake jobs are not processed.

  In the WakeJob table in the database, you would see your wake job with a *LastWakeJobServiceUpdateTimeUtc* value showing the time you submitted the job. When the background processor is running, this field is updated roughly every minute.
- Policy changes are not delivered to all affected clients.
- New Wake on WAN proxies are not elected if an existing one shuts down.
- Wake on LAN power state changes that are scheduled in policies do not run as scheduled.
- New devices that connect are not allocated a license.
- Operational Hours report data is missing or truncated after a particular time.

If you see any of these symptoms, open the Windows Services console to check that the service is running: Windows Start menu / Run / services.msc.

In the Services console, look for the Enterprise Power Management Processor. If it has stopped, you can restart it manually.

If you experience any of these issues, and the power management processor is running properly, further troubleshooting depends on the specific issue. For assistance, contact Cisco Technical Support.

Pressing Power Button Does Not Wake Computer

If a computer does not wake when you press the power button, an outdated driver or other hardware conflict might be preventing the power-state change.

- Detecting the Hardware Issue, page 10-2
- Updating the Hardware Does Not Resolve the Issue, page 10-2

Detecting the Hardware Issue

When you press the power button on a computer in standby, the power button light can show the issue that is preventing the computer from waking.

Table 10-1 shows the hardware signals, indications, and the resolutions.

Table 10-1 Hardware Issues and Resolutions

Signal	Meaning	Resolution
Power light changes from blinking blue or green to blinking red or orange	A piece of hardware is preventing the system from waking, for example, the video card.	Update the hardware or video card, or try a different video driver.
Power light changes to blue or green, and the CPU engages, but the monitor does not.	Conflict with the video card or driver.	Contact the video card manufacturer to get the most recent version.
Multiple monitors do not wake properly or consistently, screens display incorrect resolution on wake, and so on.	Conflict with the video card.	Contact the video card manufacturer to get the most recent version.

Video driver issues are more common in computers that were built in 2006 and earlier, but they could also be present in new systems. Obtaining the latest driver version usually resolves the wake issue.

Tip To ensure that you get the latest version of the video driver, contact the video card manufacturer rather than the computer manufacturer.

Updating the Hardware Does Not Resolve the Issue

If updating to the latest video driver does not resolve the wake issue, apply a policy to the computer that turns the computer off at night instead of changing it to standby and that does not change the computer to standby after idle time.

Tip If you use Wake on WAN, set this computer as a preferred proxy. Proxy computers are always on. For information, see the "Setting a Device As a Preferred Wake on WAN Proxy" section on page 6-8.

APPENDIX 11

Important Notice

- Disclaimer, page 11-1
- Statement 361—VoIP and Emergency Calling Services do not Function if Power Fails, page 11-1
- Statement 1071—Warning Definition, page 11-3

Disclaimer

Cisco EnergyWise enables you to reduce energy consumption in your network by turning off the power to devices when they are not in use. If IP phones are part of your network, they can also be turned off through EnergyWise, in which case calls cannot be made or received, and the phones cannot be turned on except by the network administrator or according to rules established in EnergyWise by the network administrator. Laws in the location of your network might require phones to remain available for emergencies. It is your responsibility to identify the laws which apply and to comply with them. Even in the absence of a law, we strongly recommend that you designate certain phones which will always be on and available to make and receive emergency calls. These phones should be clearly identified, and all employees or others who might require emergency access to make or receive calls should be informed of the availability of these phones.

Statement 361—VoIP and Emergency Calling Services do not Function if Power Fails

Warning **Voice over IP (VoIP) service and the emergency calling service do not function if power fails or is disrupted. After power is restored, you might have to reset or reconfigure equipment to regain access to VoIP and the emergency calling service. In the USA, this emergency number is 911. You need to be aware of the emergency number in your country.**

Waarschuwing **Voice over IP (VoIP)-service en de service voor noodoproepen werken niet indien er een stroomstoring is. Nadat de stroomtoevoer is hersteld, dient u wellicht de configuratie van uw apparatuur opnieuw in te stellen om opnieuw toegang te krijgen tot VoIP en de noodoproepen. In de VS is het nummer voor noodoproepen 911. U dient u zelf op de hoogte te stellen van het nummer voor noodoproepen in uw land.**

Varoitus Voice over IP (VoIP) -palvelu ja hätäpuhelupalvelu eivät toimi, jos virta katkeaa tai sen syötössä esiintyy häiriöitä. Kun virransyöttö on taas normaali, sinun täytyy mahdollisesti asettaa tai määrittää laitteisto uudelleen, jotta voisit jälleen käyttää VoIP-palvelua ja hätäpuhelupalvelua. Yhdysvalloissa hätänumero on 911. Selvitä, mikä on omassa kotimaassasi käytössä oleva hätänumero.

Attention Le service Voice over IP (VoIP) et le service d'appels d'urgence ne fonctionnent pas en cas de panne de courant. Une fois que le courant est rétabli, vous devrez peut-être réinitialiser ou reconfigurer le système pour accéder de nouveau au service VoIP et à celui des appels d'urgence. Aux États-Unis, le numéro des services d'urgence est le 911. Vous devez connaître le numéro d'appel d'urgence en vigueur dans votre pays.

Warnung Bei einem Stromausfall oder eingeschränkter Stromversorgung funktionieren VoIP-Dienst und Notruf nicht. Sobald die Stromversorgung wieder hergestellt ist, müssen Sie möglicherweise die Geräte zurücksetzen oder neu konfigurieren, um den Zugang zu VoIP und Notruf wieder herzustellen. Die Notrufnummer in den USA lautet 911. Wählen Sie im Notfall die für Ihr Land vorgesehene Notrufnummer.

Avvertenza Il servizio Voice over IP (VoIP) e il servizio per le chiamate di emergenza non funzionano in caso di interruzione dell'alimentazione. Ristabilita l'alimentazione, potrebbe essere necessario reimpostare o riconfigurare l'attrezzatura per ottenere nuovamente l'accesso al servizio VoIP e al servizio per le chiamate di emergenza. Negli Stati Uniti, il numero di emergenza è 911. Si consiglia di individuare il numero di emergenza del proprio Paese.

Advarsel Tjenesten Voice over IP (VoIP) og nødanropstjenesten fungerer ikke ved strømbrudd. Etter at strømmen har kommet tilbake, må du kanskje nullstille eller konfigurere utstyret på nytt for å få tilgang til VoIP og nødanropstjenesten. I USA er dette nødnummeret 911. Du må vite hva nødnummeret er i ditt land.

Aviso O serviço Voice over IP (VoIP) e o serviço de chamadas de emergência não funcionam se houver um corte de energia. Depois do fornecimento de energia ser restabelecido, poderá ser necessário reiniciar ou reconfigurar o equipamento para voltar a utilizar os serviços VoIP ou chamadas de emergência. Nos EUA, o número de emergência é o 911. É importante que saiba qual o número de emergência no seu país.

¡Advertencia! El servicio de voz sobre IP (VoIP) y el de llamadas de emergencia no funcionan si se interrumpe el suministro de energía. Tras recuperar el suministro es posible que deba que restablecer o volver a configurar el equipo para tener acceso a los servicios de VoIP y de llamadas de emergencia. En Estados Unidos el número de emergencia es el 911. Asegúrese de obtener el número de emergencia en su país.

Varning! Tjänsten Voice over IP (VoIP) och larmnummertjänsten fungerar inte vid strömavbrott. Efter att strömmen kommit tillbaka måste du kanske återställa eller konfigurera om utrustningen för att få tillgång till VoIP och larmnummertjänsten. I USA är det här larmnumret 911. Du bör ta reda på det larmnummer som gäller i ditt land.

Figyelem Az IP csatornán történő hangátvitel (VoIP) és a segélyhívó szolgáltatás nem működik, ha az áramellátás megszűnik vagy megszakad. Az áramellátás helyreállítását követően előfordulhat, hogy alaphelyzetbe kell állítani vagy újra kell konfigurálni a berendezést, hogy újra hozzáférhessen a VoIP és a segélyhívó szolgáltatáshoz. Az Egyesült Államokban a segélyhívó szám 911. Tisztában kell lennie a saját országának segélyhívó számával.

Предупреждение **Служба передачи голоса по IP (VoIP) и служба экстренных вызовов не будут работать, если произошел сбой питания. После восстановления питания, возможно, потребуется перенастроить оборудование, чтобы возобновить доступ к службе VoIP и службе экстренных вызовов. В США телефон службы экстренных вызовов 911. Вам необходимо знать телефон этой службы в своей стране.**

警告 如果电源出现故障或中断，您将无法使用 Voice over IP (VoIP) 服务与紧急呼叫服务。电源恢复之后，您可能需要重新设置或重新配置设备，以便重新获得进入 VoIP 与紧急呼叫服务的权限。在美国，此紧急呼叫号码是 911。您必须知道本国的紧急呼叫号码。

警告 電源障害や停電の場合、ボイス オーバー アイピー (VoIP) サービスと緊急呼出しサービスは機能しません。電源の回復後、VoIP と緊急呼出しサービスにアクセスするには機器をリセットまたは再設定する必要があります。米国内の緊急呼出し番号は 911 です。お住まいの地域の緊急呼出し番号をあらかじめ調べておいてください。

Statement 1071—Warning Definition

Warning **IMPORTANT SAFETY INSTRUCTIONS**

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device. Statement 1071

SAVE THESE INSTRUCTIONS

Waarschuwing **BELANGRIJKE VEILIGHEIDSINSTRUCTIES**

Dit waarschuwingssymbool betekent gevaar. U verkeert in een situatie die lichamelijk letsel kan veroorzaken. Voordat u aan enige apparatuur gaat werken, dient u zich bewust te zijn van de bij elektrische schakelingen betrokken risico's en dient u op de hoogte te zijn van de standaard praktijken om ongelukken te voorkomen. Gebruik het nummer van de verklaring onderaan de waarschuwing als u een vertaling van de waarschuwing die bij het apparaat wordt geleverd, wilt raadplegen.

BEWAAR DEZE INSTRUCTIES

Varoitus **TÄRKEITÄ TURVALLISUUSOHJEITA**

Tämä varoitusmerkki merkitsee vaaraa. Tilanne voi aiheuttaa ruumiillisia vammoja. Ennen kuin käsittelet laitteistoa, huomioi sähköpiirien käsittelemiseen liittyvät riskit ja tutustu onnettomuuksien yleisiin ehkäisytapoihin. Turvallisuusvaroitusten käännökset löytyvät laitteen mukana toimitettujen käännettyjen turvallisuusvaroitusten joukosta varoitusten lopussa näkyvien lausuntonumeroiden avulla.

SÄILYTÄ NÄMÄ OHJEET

Attention **IMPORTANTES INFORMATIONS DE SÉCURITÉ**

Ce symbole d'avertissement indique un danger. Vous vous trouvez dans une situation pouvant entraîner des blessures ou des dommages corporels. Avant de travailler sur un équipement, soyez conscient des dangers liés aux circuits électriques et familiarisez-vous avec les procédures couramment utilisées pour éviter les accidents. Pour prendre connaissance des traductions des avertissements figurant dans les consignes de sécurité traduites qui accompagnent cet appareil, référez-vous au numéro de l'instruction situé à la fin de chaque avertissement.

CONSERVEZ CES INFORMATIONS

Warnung **WICHTIGE SICHERHEITSHINWEISE**

Dieses Warnsymbol bedeutet Gefahr. Sie befinden sich in einer Situation, die zu Verletzungen führen kann. Machen Sie sich vor der Arbeit mit Geräten mit den Gefahren elektrischer Schaltungen und den üblichen Verfahren zur Vorbeugung vor Unfällen vertraut. Suchen Sie mit der am Ende jeder Warnung angegebenen Anweisungsnummer nach der jeweiligen Übersetzung in den übersetzten Sicherheitshinweisen, die zusammen mit diesem Gerät ausgeliefert wurden.

BEWAHREN SIE DIESE HINWEISE GUT AUF.

Avvertenza **IMPORTANTI ISTRUZIONI SULLA SICUREZZA**

Questo simbolo di avvertenza indica un pericolo. La situazione potrebbe causare infortuni alle persone. Prima di intervenire su qualsiasi apparecchiatura, occorre essere al corrente dei pericoli relativi ai circuiti elettrici e conoscere le procedure standard per la prevenzione di incidenti. Utilizzare il numero di istruzione presente alla fine di ciascuna avvertenza per individuare le traduzioni delle avvertenze riportate in questo documento.

CONSERVARE QUESTE ISTRUZIONI

Advarsel **VIKTIGE SIKKERHETSINSTRUKSJONER**

Dette advarselssymbolet betyr fare. Du er i en situasjon som kan føre til skade på person. Før du begynner å arbeide med noe av utstyret, må du være oppmerksom på farene forbundet med elektriske kretser, og kjenne til standardprosedyrer for å forhindre ulykker. Bruk nummeret i slutten av hver advarsel for å finne oversettelsen i de oversatte sikkerhetsadvarslene som fulgte med denne enheten.

TA VARE PÅ DISSE INSTRUKSJONENE

Aviso **INSTRUÇÕES IMPORTANTES DE SEGURANÇA**

Este símbolo de aviso significa perigo. Você está em uma situação que poderá ser causadora de lesões corporais. Antes de iniciar a utilização de qualquer equipamento, tenha conhecimento dos perigos envolvidos no manuseio de circuitos elétricos e familiarize-se com as práticas habituais de prevenção de acidentes. Utilize o número da instrução fornecido ao final de cada aviso para localizar sua tradução nos avisos de segurança traduzidos que acompanham este dispositivo.

GUARDE ESTAS INSTRUÇÕES

¡Advertencia! **INSTRUCCIONES IMPORTANTES DE SEGURIDAD**

Este símbolo de aviso indica peligro. Existe riesgo para su integridad física. Antes de manipular cualquier equipo, considere los riesgos de la corriente eléctrica y familiarícese con los procedimientos estándar de prevención de accidentes. Al final de cada advertencia encontrará el número que le ayudará a encontrar el texto traducido en el apartado de traducciones que acompaña a este dispositivo.

GUARDE ESTAS INSTRUCCIONES

Varning! **VIKTIGA SÄKERHETSANVISNINGAR**

Denna varningssignal signalerar fara. Du befinner dig i en situation som kan leda till personskada. Innan du utför arbete på någon utrustning måste du vara medveten om farorna med elkretsar och känna till vanliga förfaranden för att förebygga olyckor. Använd det nummer som finns i slutet av varje varning för att hitta dess översättning i de översatta säkerhetsvarningar som medföljer denna anordning.

SPARA DESSA ANVISNINGAR

Figyelem **FONTOS BIZTONSÁGI ELOÍRÁSOK**

Ez a figyelmezeto jel veszélyre utal. Sérülésveszélyt rejto helyzetben van. Mielott bármely berendezésen munkát végezte, legyen figyelemmel az elektromos áramkörök okozta kockázatokra, és ismerkedjen meg a szokásos balesetvédelmi eljárásokkal. A kiadványban szereplo figyelmeztetések fordítása a készülékhez mellékelt biztonsági figyelmeztetések között található; a fordítás az egyes figyelmeztetések végén látható szám alapján keresheto meg.

ORIZZE MEG EZEKET AZ UTASÍTÁSOKAT!

Предупреждение **ВАЖНЫЕ ИНСТРУКЦИИ ПО СОБЛЮДЕНИЮ ТЕХНИКИ БЕЗОПАСНОСТИ**

Этот символ предупреждения обозначает опасность. То есть имеет место ситуация, в которой следует опасаться телесных повреждений. Перед эксплуатацией оборудования выясните, каким опасностям может подвергаться пользователь при использовании электрических цепей, и ознакомьтесь с правилами техники безопасности для предотвращения возможных несчастных случаев. Воспользуйтесь номером заявления, приведенным в конце каждого предупреждения, чтобы найти его переведенный вариант в переводе предупреждений по безопасности, прилагаемом к данному устройству.

СОХРАНИТЕ ЭТИ ИНСТРУКЦИИ

警告 重要的安全性说明

此警告符号代表危险。您正处于可能受到严重伤害的工作环境中。在您使用设备开始工作之前，必须充分意识到触电的危险，并熟练掌握防止事故发生的标准工作程序。请根据每项警告结尾提供的声明号码来找到此设备的安全性警告说明的翻译文本。

请保存这些安全性说明

警告 安全上の重要な注意事項

「危険」の意味です。人身事故を予防するための注意事項が記述されています。装置の取り扱い作業を行うときは、電気回路の危険性に注意し、一般的な事故防止策に留意してください。警告の各国語版は、各注意事項の番号を基に、装置に付属の「Translated Safety Warnings」を参照してください。

これらの注意事項を保管しておいてください。

주의 중요 안전 지침

이 경고 기호는 위험을 나타냅니다. 작업자가 신체 부상을 일으킬 수 있는 위험한 환경에 있습니다. 장비에 작업을 수행하기 전에 전기 회로와 관련된 위험을 숙지하고 표준 작업 관례를 숙지하여 사고를 방지하십시오. 각 경고의 마지막 부분에 있는 경고문 번호를 참조하여 이 장치와 함께 제공되는 번역된 안전 경고문에서 해당 번역문을 찾으십시오.

이 지시 사항을 보관하십시오.

Aviso INSTRUÇÕES IMPORTANTES DE SEGURANÇA

Este símbolo de aviso significa perigo. Você se encontra em uma situação em que há risco de lesões corporais. Antes de trabalhar com qualquer equipamento, esteja ciente dos riscos que envolvem os circuitos elétricos e familiarize-se com as práticas padrão de prevenção de acidentes. Use o número da declaração fornecido ao final de cada aviso para localizar sua tradução nos avisos de segurança traduzidos que acompanham o dispositivo.

GUARDE ESTAS INSTRUÇÕES

Advarsel VIGTIGE SIKKERHEDSANVISNINGER

Dette advarselssymbol betyder fare. Du befinder dig i en situation med risiko for legemesbeskadigelse. Før du begynder arbejde på udstyr, skal du være opmærksom på de involverede risici, der er ved elektriske kredsløb, og du skal sætte dig ind i standardprocedurer til undgåelse af ulykker. Brug erklæringsnummeret efter hver advarsel for at finde oversættelsen i de oversatte advarsler, der fulgte med denne enhed.

GEM DISSE ANVISNINGER

تحذير

إرشادات الأمان الهامة

يوضح رمز التحذير هذا وجود خطر. وهذا يعني أنك متواجد في مكان قد ينتج عنه التعرض لإصابات. قبل بدء العمل، احذر مخاطر التعرض للصدمات الكهربائية وكن على علم بالإجراءات القياسية للحيلولة دون وقوع أي حوادث. استخدم رقم البيان الموجود في أخر كل تحذير لتحديد مكان ترجمته داخل تحذيرات الأمان المترجمة التي تأتي مع الجهاز.

قم بحفظ هذه الإرشادات

Upozorenje

VAŽNE SIGURNOSNE NAPOMENE

Ovaj simbol upozorenja predstavlja opasnost. Nalazite se u situaciji koja može prouzročiti tjelesne ozljede. Prije rada s bilo kojim uređajem, morate razumjeti opasnosti vezane uz električne sklopove, te biti upoznati sa standardnim načinima izbjegavanja nesreća. U prevedenim sigurnosnim upozorenjima, priloženima uz uređaj, možete prema broju koji se nalazi uz pojedino upozorenje pronaći i njegov prijevod.

SAČUVAJTE OVE UPUTE

Upozornění

DŮLEŽITÉ BEZPEČNOSTNÍ POKYNY

Tento upozorňující symbol označuje nebezpečí. Jste v situaci, která by mohla způsobit nebezpečí úrazu. Před prací na jakémkoliv vybavení si uvědomte nebezpečí související s elektrickými obvody a seznamte se se standardními opatřeními pro předcházení úrazům. Podle čísla na konci každého upozornění vyhledejte jeho překlad v přeložených bezpečnostních upozorněních, která jsou přiložena k zařízení.

USCHOVEJTE TYTO POKYNY

Προειδοποίηση

ΣΗΜΑΝΤΙΚΕΣ ΟΔΗΓΙΕΣ ΑΣΦΑΛΕΙΑΣ

Αυτό το προειδοποιητικό σύμβολο σημαίνει κίνδυνο. Βρίσκεστε σε κατάσταση που μπορεί να προκαλέσει τραυματισμό. Πριν εργαστείτε σε οποιοδήποτε εξοπλισμό, να έχετε υπόψη σας τους κινδύνους που σχετίζονται με τα ηλεκτρικά κυκλώματα και να έχετε εξοικειωθεί με τις συνήθεις πρακτικές για την αποφυγή ατυχημάτων. Χρησιμοποιήστε τον αριθμό δήλωσης που παρέχεται στο τέλος κάθε προειδοποίησης, για να εντοπίσετε τη μετάφρασή της στις μεταφρασμένες προειδοποιήσεις ασφαλείας που συνοδεύουν τη συσκευή.

ΦΥΛΑΞΤΕ ΑΥΤΕΣ ΤΙΣ ΟΔΗΓΙΕΣ

אזהרה

הוראות בטיחות חשובות

סימן אזהרה זה מסמל סכנה. אתה נמצא במצב העלול לגרום לפציעה. לפני שתעבוד עם ציוד כלשהו, עליך להיות מודע לסכנות הכרוכות במעגלים חשמליים ולהכיר את הנהלים המקובלים למניעת תאונות. השתמש במספר ההוראה המסופק בסופה של כל אזהרה כד לאתר את התרגום באזהרות הבטיחות המתורגמות שמצורפות להתקן.

שמור הוראות אלה

Opomena

ВАЖНИ БЕЗБЕДНОСНИ НАПАТСТВИЈА
Симболот за предупредување значи опасност. Се наоѓате во ситуација што може да предизвика телесни повреди. Пред да работите со опремата, бидете свесни за ризикот што постои кај електричните кола и треба да ги познавате стандардните постапки за спречување на несреќни случаи. Искористете го бројот на изјавата што се наоѓа на крајот на секое предупредување за да го најдете неговиот период во преведените безбедносни предупредувања што се испорачани со уредот.
ЧУВАЈТЕ ГИ ОВИЕ НАПАТСТВИЈА

Ostrzeżenie

WAŻNE INSTRUKCJE DOTYCZĄCE BEZPIECZEŃSTWA

Ten symbol ostrzeżenia oznacza niebezpieczeństwo. Zachodzi sytuacja, która może powodować obrażenia ciała. Przed przystąpieniem do prac przy urządzeniach należy zapoznać się z zagrożeniami związanymi z układami elektrycznymi oraz ze standardowymi środkami zapobiegania wypadkom. Na końcu każdego ostrzeżenia podano numer, na podstawie którego można odszukać tłumaczenie tego ostrzeżenia w dołączonym do urządzenia dokumencie z tłumaczeniami ostrzeżeń.

NINIEJSZE INSTRUKCJE NALEŻY ZACHOWAĆ

Upozornenie

DÔLEŽITÉ BEZPEČNOSTNÉ POKYNY

Tento varovný symbol označuje nebezpečenstvo. Nachádzate sa v situácii s nebezpečenstvom úrazu. Pred prácou na akomkoľvek vybavení si uvedomte nebezpečenstvo súvisiace s elektrickými obvodmi a oboznámte sa so štandardnými opatreniami na predchádzanie úrazom. Podľa čísla na konci každého upozornenia vyhľadajte jeho preklad v preložených bezpečnostných upozorneniach, ktoré sú priložené k zariadeniu.

USCHOVAJTE SI TENTO NÁVOD

Opozorilo

POMEMBNI VARNOSTNI NAPOTKI

Ta opozorilni simbol pomeni nevarnost. Nahajate se v situaciji, kjer lahko pride do telesnih poškodb. Preden pričnete z delom na napravi, se morate zavedati nevarnosti udara električnega toka, ter tudi poznati preventivne ukrepe za preprečevanje takšnih nevarnosti. Uporabite obrazložitveno številko na koncu posameznega opozorila, da najdete opis nevarnosti v priloženem varnostnem priročniku.

SHRANITE TE NAPOTKE!

警告

重要安全性指示
此警告符號代表危險，表示可能造成人身傷害。使用任何設備前，請留心電路相關危險，並熟悉避免意外的標準作法。您可以使用每項警告後的聲明編號，查詢本裝置隨附之安全性警告譯文中的翻譯。
請妥善保留此指示