CONTENTS

Preface 1

CHAPTER 1Overview of Cisco Prime Home 5.2 1-1
   TR-069 Overview 1-1
   How Does TR-069 Relate to Prime Home? 1-1
   User Roles 1-2

CHAPTER 2System Overview 2-1
   Supported Browsers 2-1
   Logging Into Prime Home 2-1
   Logging Out of Prime Home 2-2
   User Profile 2-2
      Automatically Refreshing Device Data 2-3
   Navigation Overview 2-3
   Dashboard Overview 2-4
   System Messages Overview 2-5
      Viewing System Messages 2-5
   Labels Overview 2-6
      Using Labels 2-6
   Domains Overview 2-6
   Scripts Overview 2-6
      What Can Scripts Do? 2-7
      How Do Scripts Run? 2-7

CHAPTER 3Customer Support Overview 3-1
   Finding and Selecting Subscribers and Devices 3-1
      How to Search 3-2
      Selecting Subscribers or Devices 3-3
   Applying or Removing Labels for Multiple Records 3-3
   About New Accounts 3-4
      Creating a Subscriber or Device Account 3-5
      Assigning a Device to a Subscriber 3-6
      Assigning a Subscriber to a Device 3-7
About Saving Changes 3-7

CHAPTER 4

Working with Accounts 4-1

Displaying an Account 4-1

What Happens When You Display an Account 4-2

Working with Subscribers 4-2

Managing Subscriber Information 4-2

Identification Information 4-3

Address and Phone Information 4-3

Managing Control Panel Access 4-3

Working with the Control Panel 4-4

Viewing Device Information 4-5

Enabling Local Interface Access 4-5

Managing Subscriber Labels 4-5

Deleting a Subscriber 4-6

Managing Devices 4-7

Working with Device Labels 4-7

Viewing Device Information 4-8

Rebooting a Device 4-8

Adding and Removing PPP Credentials 4-8

Enabling or Disabling Bulk Operations 4-8

Assigning a Device to a Domain 4-9

Removing the Association Between a Device and a Subscriber 4-9

Deleting a Device 4-9

Managing the Local Network 4-9

Viewing Local Network Status 4-9

Naming a LAN Device 4-10

Enabling Local Interface Access 4-10

Deleting a LAN Device 4-11

Viewing Device Status 4-11

Status 4-12

Line Information 4-12

DSL or Cable 4-12

Bonded Line Information/DSL Statistics 4-13

WAN Interface Statistics 4-13

CHAPTER 5

Working with Services 5-1

Monitoring Bandwidth Usage 5-1

Launching the Bandwidth Monitor 5-2
Analyzing the WAN Interface Chart 5-2
Analyzing the LAN Device Traffic Share Chart 5-3
LAN Device Table 5-3
Setting Chart Options 5-3
Managing Wireless Networking 5-3
   About Wireless Networking 5-5
      Wireless Networks 5-5
      Wireless Radios 5-6
Managing Port Forwarding 5-6
   Enabling Port Forwarding 5-7
   Disabling Port Forwarding 5-7
   Adding a Port Forward 5-7
   Deleting a Port Forward 5-9
Managing Content Filtering 5-9
   About Content Filtering Levels 5-10
   How Content Filtering Works 5-10
   Enabling the Content Filtering Service 5-12
   Disabling the Content Filtering Service 5-12
   Managing Default Content Filtering Settings 5-12
   Managing Content Filtering for Specific LAN Devices 5-13
Managing Time Blocking 5-13
   Enabling Time Blocking 5-14
   Disabling Time Blocking 5-14
   Managing Default Time Blocking Settings 5-14
   Managing Time Blocking for Specific Devices 5-14
   Adding Bonus Time 5-16

**Performing Advanced Tasks** 6-1

Working with Event Logs 6-1
   Refreshing the Event Logs List 6-2
   Viewing a Session Log 6-2
   Setting the Event Logging Level 6-3
Using the Parameter Browser 6-3
Working with Scripts 6-5
   Adding a Script 6-5
   Viewing Script Results 6-6
Updating Firmware 6-6
   Queuing a Firmware Update 6-7
Replacing a Device 6-7
Copying Device Settings to Another Device 6-8
Setting Up Local GUI Access 6-8

CHAPTER 7

Reports 7-1
Built-In Reports 7-1
  Running an Aggregate Report 7-2
  Custom Reports 7-2
Reports Tab 7-3
  Finding an Existing Report 7-3
  Running an Existing Report 7-4
Custom Reports 7-4
  Creating a Custom Report 7-5
  Working with Sort Order 7-6
  Working with Filters 7-6
    Applying Parameters 7-7
    Editing Parameters 7-7
    Using Boolean Logic 7-8
  Working with Advanced Syntax 7-8
Using Reports to Understand Your Network 7-8

CHAPTER 8

Administration Overview 8-1
Licensing 8-1
Managing Labels 8-2
  Labels Window 8-2
    Adding a New Label 8-2
    Editing a Label 8-3
    Deleting a Label 8-3
Managing Users 8-3
  Adding a New User 8-5
  Editing User Information 8-5
  Deleting a User 8-5
Managing Device Types 8-6
  Device Type Page 8-6
    Adding a Device Type 8-7
    Editing a Device Type 8-7
    Deleting a Device Type 8-8
Managing Firmware Versions 8-8
  Firmware List Window 8-8
Example 2: Enable Content Filtering on All CPEs 10-7
Best Practices for Working with Bulk Operations 10-9
Troubleshooting Failed Bulk Operations 10-9
Controlling Maximum Throughput/Throttling 10-9
Preparing to Run Firmware Update Operations 10-10
Understanding Bulk Operation Options 10-10
Action Options 10-10
Schedule Options 10-11
CPE Selection Options 10-11

CHAPTER 11
Troubleshooting Tools 11-1
Import Subscriptions Utility 11-1
Importing Multiple Subscriptions 11-2
RESTful Service Tool 11-2

CHAPTER 12
Control Panel for Subscribers 12-1
What’s on the Main Screen 12-1
Importing Multiple Subscriptions 12-2
RESTful Service Tool 12-2

APPENDIX A
Subscription Import Files A-1

APPENDIX B
Common Error Messages and Fault Codes B-3
Error Messages B-3
TR-069 Fault Codes B-5
CPE Fault Codes B-5
ACS Fault Codes B-7
Preface

This guide describes the structure and features of Cisco Prime Home 5.2 and how to use it. This preface contains the following sections:

- Audience, page I
- Related Documentation, page I
- Obtaining Documentation and Submitting a Service Request, page II

Audience

The primary audience for this guide is network operations personnel and system administrators. This guide assumes that you are familiar with the following products and topics:

- Basic internetworking terminology and concepts
- Network topology and protocols
- Telecommunication Management Network (TMN) architecture model

Related Documentation

See also the following Prime Home guides:

- *Cisco Prime Home 5.2 Installation Guide*
- *Cisco Prime Home 5.2 Release Notes*

Click [here](#) to access the entire Cisco Prime Home 5.2 documentation set.

**Note**

We sometimes update the documentation after original publication. Therefore, you should review the documentation on Cisco.com for any updates.
Obtaining Documentation and Submitting a Service Request

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:


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.
Overview of Cisco Prime Home 5.2

Cisco Prime Home 5.2 offers telecommunication service providers the ability to automatically activate and configure subscribers; manage customer premises equipment (CPE); and deliver advanced services via service packages over DSL, fiber, cable, T1/E1, wireless, and satellite networks. Advanced features include services such as time blocking, content filtering, managed Wi-Fi, remote port forwarding, and IPTV. Prime Home also lets you remotely manage TR-069-compliant CPEs from a variety of vendors.

TR-069 Overview

TR-069 is a technical report published by the Broadband Forum that defines the CPE WAN Management Protocol (CWMP). The CWMP defines the application layer for remote management of end-user devices and is used by Prime Home to provide a flexible, extensible, and scalable control panel for managing systems. TR-069 is the current standard for activation of CPEs in the broadband market.

TR-069 specifies communication between the CPE and automated configuration services (ACS) such as Prime Home. It provides safe auto configuration as well as control of other CPE management functions in an integrated framework. TR-069 uses HTTP as a transport protocol and Simple Object Access Protocol (SOAP) services as its message encapsulation protocol. It also uses models that standardize the data exchanged between devices and management servers.

How Does TR-069 Relate to Prime Home?

Prime Home is an enterprise application that manages and monitors TR-069-compliant subscriber devices. Prime Home provides the ability to investigate and control both individual CPEs and groups of CPEs defined by almost any characteristic. Management is driven by actions, which can select devices, communicate changes, and record status. In addition to included actions, customers can edit, create, and run actions based on CPE-related events. Prime Home fills a critical need for cutting-edge ISPs.
User Roles

Prime Home includes the following roles that you can apply to a user account:

- Admin—Allows access to all functions in Prime Home, except those limited by license settings.
- Customer Support Representative (CSR)—Manages individual device and subscriber records.

**Note**

Depending on your staffing model, you can create custom users with access to the features of your choice. When a custom user logs in, the Prime Home application runs with the features mapped to that user account. Contact Cisco Advanced Services to configure custom users with specific roles.

The following table shows which Prime Home tabs are visible to default users with specific roles.

<table>
<thead>
<tr>
<th>Tab</th>
<th>Admin Role</th>
<th>Customer Support Representative Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customer Support</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Dashboard</td>
<td>X</td>
<td>—</td>
</tr>
<tr>
<td>Administration</td>
<td>X</td>
<td>—</td>
</tr>
<tr>
<td>Audit</td>
<td>X</td>
<td>—</td>
</tr>
<tr>
<td>Bulk Operations</td>
<td>X</td>
<td>—</td>
</tr>
<tr>
<td>Reports</td>
<td>X</td>
<td>—</td>
</tr>
<tr>
<td>Utilities</td>
<td>X</td>
<td>—</td>
</tr>
</tbody>
</table>

**Note**

Prime Home is highly configurable. Prime Home administrators can assign access to tasks and parts of tasks to Admin or CSR roles. If a task is not available to you, contact your system administrator.
System Overview

Supported Browsers

To access Prime Home, use one of these browsers:

- Google Chrome 5 or later
- Internet Explorer 8 or later
- Firefox 3.6 or later
- Safari 5 or later

Logging Into Prime Home

To log into Prime Home:

**Step 1**
Go to the Prime Home URL. The login window (Figure 2-1) opens.

**Step 2**
Enter your username and password, which are case-sensitive. Note that the username can only contain the following characters: A-Z, a-z, 0-9, _ . \ -

**Step 3**
Click Log in.

The system processes your request and displays the Customer Support page.

If you forget your username or password or receive an error message, contact your system administrator.

**Note**
Your system might have a set limit of session logins per license. If you exceed the maximum number of simultaneous logins, you receive the message “The maximum number of users are already logged into the system. Another user must log out before you can log in.” You must wait until another user logs out, or request that a user log out.
Logging Out of Prime Home

In the top-right corner of the Prime Home GUI, click your username and choose **Logout**.

User Profile

Your user profile lets you automatically refresh device data, view system messages, and log out of Prime Home.

To view your user profile, click your username in the top-right corner of the Prime Home GUI.
Automatically Refreshing Device Data

If you check the Automatically Refresh Device Data check box (Figure 2-2), viewing an account immediately polls the device and refreshes the display with the latest data from the device.

If you uncheck the check box, you must explicitly refresh data by clicking the Refresh Device Data button.

Refreshing data takes time. If refreshing slows you down, you might want to uncheck the check box. Prime Home stores your selection in a browser cookie. You must reset your preference if you use a different computer.

Navigation Overview

The navigation tabs (Figure 2-3) allow access to all of the features in Prime Home. The tab bar appears at the top of every page. The tabs that you see depend on your user role.
Dashboard Overview

The Dashboard tab (Figure 2-4) displays a summary of recent activity.  

**Figure 2-4   Dashboard Tab**

The tab contains the following areas:

- **New Devices Connected by 24-Hour Period**—The number of new devices connected per 24-hour period for the last 7 days.
- **Cumulative Devices Connected**—The total number of devices connected per 24-hour period for the last 7 days.
- **Connected Devices by Manufacturer and Model**—The mix of devices you have based on their manufacturer and model type.
- **Subscribers by Label**—The top labels on the connected devices.
System Messages Overview

Prime Home displays the messages described in Table 2-1. Additionally, Prime Home constantly logs system messages that appear in the background, with no user action required.

### Table 2-1 Message Types

<table>
<thead>
<tr>
<th>Icon</th>
<th>Message Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="i" /></td>
<td>Informational</td>
<td>Displays user feedback. For example, if a script enters the queue successfully, the system displays a “Script successfully added” message.</td>
</tr>
<tr>
<td><img src="image" alt="?" /></td>
<td>Warning</td>
<td>Displays when important notifications and recoverable errors are triggered in the system. For example, if you want to delete a label, the system returns a warning message.</td>
</tr>
<tr>
<td><img src="image" alt="!!" /></td>
<td>Error</td>
<td>Displays when something fails. For example, if a script fails to run, the system returns an error message.</td>
</tr>
</tbody>
</table>

Viewing System Messages

System messages appear either as instant on-screen notifications or as a log file in a popup window. Instant messages appear in the right corner of the browser window. They display the most recent activity recorded by the system. Prime Home color codes the three types of messages so you can quickly distinguish them.

Figure 2-5 shows a sample instant message window.

**Figure 2-5 Sample Instant Messages**

Instant messages appear for only a few seconds, and then disappear. To access a record of all recent messages in the system, click the Messages link in your user profile (Figure 2-2).

To close the instant message window, click the close (X) link in the top-right corner, or press the Esc key.
Labels Overview

Labels give you a flexible, customized way of categorizing elements in your system. You can apply labels to devices, subscribers, firmware, users, scripts, events, and announcements.

Prime Home lets you create your own labels. You can think of a label as a digital bucket that holds related items. Labels keep devices, subscribers, and users grouped together for easy interaction. You can:

- Create new labels and apply them to any pre-existing device or subscriber.
- Assign multiple labels to devices or subscribers.

For example, you can create a label that groups together all devices located in the same region. Then, when you need to run a script on devices in that region, you can use the label to quickly select those devices for processing.

Using Labels

You can use labels to:

- Group together devices, subscribers, or users so you can find them easily.
- Restrict devices to a particular operation. Use labels in conjunction with bulk operations.
- Apply to scripts. You can have the script set or remove labels for a device or subscriber.
- Alter the behavior of a script when it applies to a labeled item.
- Search for information. If you enter the label name in the Search field, everything with that label appears.

You can apply labels to group devices that become faulty, or flag devices that have certain capabilities (such as voice). Using the Customer Support tab, you can apply labels to multiple subscribers or devices. Using the Device and Subscriber panes, you can apply a label to a single device or subscriber.

Domains Overview

You can assign devices, subscribers, and users to a specific domain. You can use domains to restrict CSR access to a specific set of accounts. For example, if your customer base is divided into regions, you can create a domain for each region.

CSR users who are assigned to domains can view and act on only those devices and subscribers assigned to the same domains. CSR users without a domain assignment can view and act on all accounts. Administrators can also view and act on all accounts.

Scripts Overview

Scripts are implemented using a customized JavaScript-based environment that runs on the ACS. This environment supports complete manipulation of the CPE via TR-069, as well as access to data models for subscribers and devices stored locally on the ACS.
Many scripts are bundled to run and use on your systems. However, system administrators can write customized scripts to perform specific tasks on your network. The primary script types are:

- Scheduled scripts, which run at specific times.
- Event-based scripts, which run when a specific event occurs, such as an inform or reboot.

**What Can Scripts Do?**

You can use scripts to:

- Read and write device configuration parameters.
- Read and write subscriber information, such as phone number, physical address, IP address, and billing information.
- Update firmware on a device.

Scripts can take parameters. For example, a script can set up a wireless configuration. You can create a parameter to tell the device which SSID to use.

**How Do Scripts Run?**

Scripts run:

- When a user tells the system to run them.
- During a scheduled time.
- During a device event.
- When enabling or disabling a subscription.

After entering the script queue, the script is run by the server. When a device checks in (either during its normal schedule or by an Apply Now request), the script is applied to that device.

**Figure 2-6  Script Workflow**
Scripts enter the queue in one of the following ways:

- Directly (via the Scripts window or by using the search results to apply to a batch of devices).
- Through bulk operations.
- On a defined event, such as a first connect or reboot.
Customer Support Overview

The Customer Support tab provides a central location for customer support representatives to manage subscribers and devices. You can perform the following customer service tasks:

- Search for subscribers or devices
  - Select specific records
  - Apply labels to selected subscribers or devices
- Create a new subscriber, device, or subscriber/device record
- Work with accounts (see Chapter 4, “Working with Accounts”)
- Work with services (see Chapter 5, “Working with Services”)
- Perform advanced functions (see Chapter 6, “Performing Advanced Tasks”)

Note

Some tasks are restricted to users with the Admin role. The tasks available to you depend on how your Prime Home installation is configured.

Finding and Selecting Subscribers and Devices

Before you can view or make changes to a subscriber or device, you must find the item in the Prime Home database. Prime Home provides robust search capabilities to help you locate information. You can search for different kinds of subscriber and device data. You must enter the property terms exactly as specified below.

You can use a free-text search for some items, such as person name or subscriber code; for other items, you must precede the item by the property name.
You can use a free-text search to find the following items:

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Firmware label</td>
<td>Firmware hardware version</td>
<td>Firmware manufacturer</td>
</tr>
<tr>
<td>Model</td>
<td>Product class</td>
<td>Software version</td>
</tr>
<tr>
<td>Report name</td>
<td>Script name</td>
<td>Script label</td>
</tr>
<tr>
<td>Subscriber primary e-mail address</td>
<td>Subscriber name</td>
<td>Person label</td>
</tr>
<tr>
<td>Subscriber phone number</td>
<td>Subscriber code</td>
<td>Subscriber domain</td>
</tr>
<tr>
<td>WAN POP connection username</td>
<td>Device domain</td>
<td>Device label</td>
</tr>
<tr>
<td>Device disposition</td>
<td>Device hardware version</td>
<td>Device manufacturer</td>
</tr>
<tr>
<td>Device model</td>
<td>Device OUI</td>
<td>Device product class</td>
</tr>
<tr>
<td>Device serial number</td>
<td>VOIP setting</td>
<td>VOIP username</td>
</tr>
<tr>
<td>WAN IP address</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**How to Search**

You perform a search by typing keywords into the search field. You can type one or more terms, or you can use Boolean expressions, wildcards, and property names to enhance your search. Search terms are not case-sensitive.

**Table 3-1 Search Terms and Results**

<table>
<thead>
<tr>
<th>This search term…</th>
<th>Finds this result…</th>
</tr>
</thead>
<tbody>
<tr>
<td>john</td>
<td>Records that contain the term <em>john</em>.</td>
</tr>
<tr>
<td>jack london</td>
<td>Records that contain both terms <em>jack</em> and <em>london</em>.</td>
</tr>
<tr>
<td>jack and london</td>
<td>Records that contain both terms <em>jack</em> and <em>london</em>.</td>
</tr>
<tr>
<td>jack or london</td>
<td>Records that contain the term <em>jack</em>, the term <em>london</em>, or both.</td>
</tr>
<tr>
<td>name: jack</td>
<td>Records that contain the term <em>jack</em> in the name property.</td>
</tr>
<tr>
<td>name: jack city:not london</td>
<td>Records that have <em>jack</em> in the name property and do not have <em>london</em> in the city property.</td>
</tr>
<tr>
<td>name:&quot;jack london&quot;</td>
<td>Records that contain the exact phrase <em>jack london</em> in the name property.</td>
</tr>
<tr>
<td>jack*</td>
<td>Records that contain terms that begin with <em>jack</em>.</td>
</tr>
<tr>
<td>*jack</td>
<td>Records that contain terms that end with <em>jack</em>.</td>
</tr>
<tr>
<td>192.168.1.*</td>
<td>Has any IP address in the range 192.168.1.0 to 192.168.1.255.</td>
</tr>
<tr>
<td>192.168.<em>,.</em></td>
<td>Has any IP address in the range 192.168.0.0 to 192.168.255.255.</td>
</tr>
</tbody>
</table>
Examples:

- `city: Portland`—Finds subscribers whose address includes Portland as the city.
- `city: *land`—Finds subscribers whose address includes a city name that ends with `land`.
- `model: AG10*`—Finds all devices with a model designation that starts with AG-10, such as AG10-NA1 and AG10W-NA2.
- `personLabel: Promo10`—Finds all subscribers who have the label Promo10.
- `wanip:192.168.*.* deviceLabel:Version3 softwareVersion:3.7`—Finds all devices with WAN IP addresses 192.168.0.0 through 192.168.255.255 that have a device label of Version3 and are running software version 3.7.

To perform a search:

**Step 1** On the Customer Support tab, type the search term in the **Find Subscriber or Device** field.

**Step 2** Press **Enter**.

Matching subscriber or device records appear on the Customer Support tab.

---

## Selecting Subscribers or Devices

After you locate one or more subscribers or devices, you can select them for further processing, such as applying labels. You can also display a single subscriber or device.

To select one or more subscribers or devices, check the check box to the left of the desired subscribers or devices.

**Note** Depending on how your Prime Home installation is configured, selecting multiple accounts might be restricted to Admin users.

To display a single subscriber or device, click the blue text in the search results for that record, such as the subscriber name or device model number.

---

## Applying or Removing Labels for Multiple Records

When you have multiple records selected, you can apply subscriber or device labels to all of them. You can also remove labels. For information about defining labels, see **Managing Labels, page 8-2**.

To apply a label to multiple records:

**Step 1** Search for the subscribers or devices you want to label.

**Step 2** Select the records you want to label.

**Step 3** Choose a label from the Add section of the Subscriber Labels or Device Labels menu.
To remove a label from multiple records:

**Step 1** Search for the subscribers or devices for which you want to remove a label.
**Step 2** Select the records for which you want to remove a label.
**Step 3** Choose a label from the Remove section of the Subscriber Labels or Device Labels menu.

---

### About New Accounts

An account usually consists of a subscriber and an associated device. Some accounts have only a subscriber or only a device.

**Note** Depending on how your Prime Home installation is configured, the ability to create accounts might be restricted to Admin users.

Creating new devices and subscribers is handled through the provisioning process. You use the Provisioning page to complete the following tasks:

- Create a new subscriber.
- Create a new device.
- Associate the subscriber with an existing device.
- Associate the device with an existing subscriber.

Creating a new subscriber establishes an account record for the subscriber and might associate the subscriber with a device. Provide the following information:

- **Subscriber code**—(Required) Unique code for the subscriber. You can use the subscriber’s phone number or any other unique identifier.

  **Note** Your system administrator might set this field to require a specific number of digits. If you have problems creating a record, contact your system administrator.

- **Name**—(Optional) The subscriber’s full name.
- **Email**—(Optional) The subscriber’s e-mail address, which must be unique.
- **Control panel login and password**—Credentials the subscriber uses to log into the control panel. You can specify a password, or click **Generate Password** to generate a secure one.
Creating a new device sets up device information for a specific device and might associate it with a subscriber. You can use the following types of information to identify the device. The identifier you use must be unique within your system so it is recognized when the device checks in.

- Serial number and OUI—The device’s serial number and the first six hexadecimal digits of the device’s MAC address.
- Provisioning code—A unique code that you specify.
- Control panel provisioning ID—A unique identifier used to associate the device with the subscriber when it is installed. An installer uses this code to bring up the control panel after installing the device at the customer location. The control panel associates the device with the subscriber and applies previously specified settings. You can use this method to configure settings prior to knowing the specific device the customer will use.

**Note**
You must specify a subscriber code when using the control panel provisioning ID. You cannot create a new device using this identifier unless you also create a subscriber or assign the device to an existing subscriber.

You must specify PPP credentials or allow the device to connect to your network with default credentials.

## Creating a Subscriber or Device Account

To create a new subscriber or device account:

**Step 1** On the Customer Support tab, click **Create New Subscriber/Device**.

**Step 2** In the Subscriber section of the Provisioning page, make sure the **Create New Subscriber** tab is selected.

**Step 3** Enter subscriber identification information: subscriber code, full name, and e-mail address.

**Note**
Your system might require a phone number or subscriber ID with a specific number of digits.

**Step 4** Do one of the following:

- Check the **Disable Control Panel** check box.
- Provide a username and password for the subscriber’s control panel. You can click **Generate Password** to create a password.

**Step 5** In the Assign Gateway section, make sure the **New Device** tab is selected.

**Step 6** In the New Device section, enter a unique device identifier for the device, using serial number or OUI, provisioning code, or control panel provisioning ID.

**Step 7** In the PPP Credentials section, do one of the following:

- Check the **Use Default** check box.
- Enter a username and password for PPP access.
Step 8 (Optional) Select a domain.

Step 9 Click **Provision Device**.

Prime Home displays the Customer Support page for the account. You can then enter additional information about the subscriber or device, enable services, or perform advanced tasks.

If you encounter errors, the errored fields are highlighted and more information about the error is displayed at the top of the page. Correct the errors and click **Provision Device**.

---

**Assigning a Device to a Subscriber**

To create a subscriber and assign an existing device or no device:

**Step 1** On the Customer Support tab, click **Create New Subscriber/Device**.

**Step 2** In the Subscriber section of the Provisioning page, make sure the **Create New Subscriber** tab is selected.

**Step 3** Enter subscriber identification information: subscriber code, full name, and e-mail address.

**Step 4** Do one of the following:

- Check the **Disable Control Panel** check box.
- Provide a username and password for the subscriber’s control panel. You can click **Generate Password** to create a password.

**Step 5** In the Assign Gateway section, do one of the following:

- Check the **No Device Information** check box.
- Click the **Existing Device** tab and do the following:
  a. In the Find Device field, type search criteria to locate the device.
  b. Click **Search**.
  c. Locate the device in the search results, and click the device information.
  d. Verify that the correct device is selected.

**Step 6** (Optional) Select a domain.

**Step 7** Click **Provision Device**.
Assigning a Subscriber to a Device

To create a device and assign an existing subscriber:

---

### Step 1
On the Customer Support tab, click **Create New Subscriber/Device**.

### Step 2
In the Subscriber section of the Provisioning page, do one of the following:

- Check the **No Subscriber Information** check box.
- Click the **Assign Existing Subscriber** tab and do the following:
  - a. In the Find Subscriber field, type search criteria to locate the subscriber.
  - b. Click **Search**.
  - c. Locate the subscriber in the search results, and click the subscriber information.
  - d. Verify that the correct subscriber is selected.

### Step 3
In the New Device section, enter a unique device identifier for the device, using serial number or OUI, provisioning code, or control panel provisioning ID.

### Step 4
In the PPP Credentials section, do one of the following:

- Check the **Use Default** check box.
- Enter a username and password for PPP access.

### Step 5
(Optional) Select a domain.

### Step 6
Click **Provision Device**.

---

### About Saving Changes

If you make changes to subscriber or device information, Prime Home displays a Save button (Figure 3-1). When you click Save, changes are saved to the server and sent immediately to the device. If the server cannot communicate with the device, changes are sent to the device the next time it checks in.

*Figure 3-1   Save Button*
Working with Accounts

Once you have created a Prime Home account, you can manage it. The tasks you can perform depend on the account and your user level. Some of the actions described in this section are available only to Admin users.

You can perform the following account management tasks:
- Manage subscriber information
- Manage devices
- Manage the local network
- View account status

Displaying an Account

To display an account:

Step 1: Click the Customer Support tab.
Step 2: Enter search criteria and click Search.
Step 3: In the list of search results, click the blue text within the desired account.

An account window (Figure 4-1) displays summary information about the account in the banner at the top. If no subscriber or device is associated with the account, the banner displays clickable links that let you quickly make an assignment.

The left side of the window contains a list of account management tasks. To select an item, click it. For example, to perform an account management task, click view next to the task.
What Happens When You Display an Account

When you display an account, the following happen:

1. Initial text and data are loaded from the server (unless you disabled automatic refresh in your user profile).

2. The system attempts to contact the devices associated with the account to obtain updated data, unless the device is configured as not contactable.
   - If the device is successfully contacted, a message is displayed and the data is updated as needed.
   - At the bottom of the Status section in the banner, the Refresh Device Data button appears.
   - If the device cannot be contacted, a message is displayed and the Status banner displays an alert.

Working with Subscribers

Use the Subscriber window to manage individual subscriber data. The Subscriber window contains several sections of subscriber data.

To display the Subscriber window, click view.

Managing Subscriber Information

You can view subscriber identification, address, and phone information. Whether you can edit these items depends on how your Prime Home installation is configured.
Identification Information

Basic subscriber information includes the following:

- Subscriber code—The unique code assigned to the subscriber when the account was created. Phone numbers are frequently used as subscriber codes.
- Name—The subscriber’s full name.
- Email—The subscriber’s e-mail address.

To edit subscriber information:

Step 1: Click the desired field and add or change information.
Step 2: Click Save.

Address and Phone Information

The Subscriber window displays addresses and phone numbers for the subscriber. Subscribers can have several addresses and phone numbers associated with their account.

To add an address or phone number:

Step 1: Click Add Address or Add Phone.
Step 2: Enter the desired information.
Step 3: Click Save.
Step 4: To delete an address or phone number, click the Remove button associated with the address or phone number.

Managing Control Panel Access

You can manage customers’ access to their CPE device control panel.

- To enable control panel login, uncheck the Disable Control Panel Login check box.
- To disable control panel login, check the Disable Control Panel Login check box.

To manage login credentials:

Step 1: In the Login field, enter the subscriber’s login name.
Step 2: To generate a password for the subscriber, click Generate Password.
If the subscriber has an existing password, click Change Password, then Generate Password to generate a new one.
Step 3: To enable the generated password to be sent to the subscriber, check the Notifications will be sent to subscriber@address.com check box.
Step 4: To access the subscriber’s control panel, click the Access Control Panel link as shown in (Figure 4-1).
Working with the Control Panel

In addition to subscribers accessing the Control Panel through a website on their own, there might be times when a CSR or a home technician finds it useful to access the Control Panel through the Prime Home GUI interface and make changes.

The following options are available:

- **Network Status**—Shows whether broadband is connected, and whether wireless networking is enabled.
- **Wireless Settings**—Here you can enable or disable wireless, or modify wireless settings, such as changing the WEP Key, changing the wireless broadcast channel, and enabling/disabling the broadcast of the subscriber’s SSID. Refer to Managing Wireless Networking for full configuration details.
- **Local Network**—This shows how many LAN devices are known to the local network, and how many are online. When you log in, the complete list of devices connected to the network is automatically displayed on the right-hand side of the screen.
- **Internet Time Blocking**—This allows the subscriber to set time limits on the Internet can be accessed. Refer to Managing Time Blocking for full configuration details.
- **Content Filtering**—Content filtering is used to prevent users from viewing inappropriate web sites or content. Refer to Requesting a Speed Test for full configuration details.
- **Port Forward** - You can manage port forwarding configuration from here. Refer to Managing Port Forwarding for full configuration details.
Viewing Device Information

Hovering over a device with your mouse will display a small window providing more information about applied services. Clicking on the device icon or name will load the Device Detail page for that device.

Figure 4-3  Device Detail

To change a name or icon for a particular device:

1. **Step 1**  Click on the required device.
2. **Step 2**  Click **Edit Name and Icon**.
3. **Step 3**  Type in the required name and if required, choose a different icon.
4. **Step 4**  Click **OK** and then click **Save**.

Enabling Local Interface Access

Some devices, such as webcams, may have a local management interface that you can access as a web page. This management interface might allow you to schedule events or view camera pictures. Refer to Enabling Local Interface Access for more information.

Managing Subscriber Labels

Labels can be used to tag subscribers. For example, you might tag subscribers who signed up for a specific promotional program. Labels can alert you to information about a subscriber, and you can search for subscribers with a specific label. Your system administrator sets up the available labels. For more
information about setting up labels, see Managing Labels, page 8-2.

To assign a label:

**Step 1**  From the Add section of the Labels menu, choose a label.
The label appears in the Label section of the Subscriber window.

**Step 2**  Click **Save**.

To remove a label:

**Step 1**  From the Remove section of the Labels menu, choose a label.
The label is removed from the Label section of the Subscriber window.

**Step 2**  Click **Save**.

## Deleting a Subscriber

Deleting a subscriber permanently removes all information about the subscriber from your system. Deleting the subscriber does not delete the associated device; the device and its settings remain in the system after a subscriber is deleted.

⚠️ **Caution**  Make sure you really want to delete a subscriber. Information about the subscriber cannot be retrieved after being deleted.

To delete a subscriber:

**Step 1**  In the Delete section of the Subscriber window, click **Delete Subscriber**.

**Step 2**  In the confirmation dialog box, click **OK**.
Managing Devices

You can use the Device window to review device information or manage the CPE device. Typical tasks include:

- Applying or removing device labels
- Reviewing device details
- Rebooting a device
- Adding PPP credentials to enable the CPE device to authenticate to the WAN
- Removing the association between a device and a subscriber
- Enabling or disabling bulk operations for the device
- Assigning a device to a domain
- Accessing a device control panel
- Deleting a device

Note: The specific tasks available to you depend on your user level (CSR or Admin) and how your Prime Home installation is configured. Sections within the Device window might appear in a different order.

To display the Device window (Figure 4-4), click **view**.

**Figure 4-4  Device Window**

Working with Device Labels

Device labels are defined by your system administrator. You can apply new labels or remove existing ones. There is no limit to the number of labels you can apply.

To apply a device label, click the **Labels** menu and select a label from the Add section of the menu.

To remove a device label, click the **Labels** menu and select a label from the Remove section of the menu.
Viewing Device Information

The Device window displays the manufacturer, model, serial number, firmware version, WAN type, IP address, and so on.

Rebooting a Device

To immediately reboot a device:

Step 1 In the Device Reboot section, check the Reboot device now check box.
Step 2 Click Save.

Adding and Removing PPP Credentials

Some ISPs require the CPE device to authenticate using PPP. You must resynchronize the information so that the PPP credentials are sent to the CPE device.

To add PPP credentials:

Step 1 In the PPP Credentials section, click Add PPP Credentials.
Step 2 Enter a username and password.
Step 3 Check the Resync PPP information check box.
Step 4 Click Save.

To remove PPP credentials:

Step 1 In the PPP Credentials section, click Remove.
Step 2 Check the Resync PPP information check box.
Step 3 Click Save.

Enabling or Disabling Bulk Operations

If you enable bulk operations for a device, it can participate in actions that affect many devices simultaneously. For example, you can update firmware, enable a service, or set a default configuration for a group of devices. For more information about bulk operations, see Chapter 10, “Managing Bulk Operations.”

- To enable bulk operations, check the Participates in Bulk Operations check box.
- To disable bulk operations, uncheck the Participates in Bulk Operations check box.
Assigning a Device to a Domain

You can assign a device to a specific domain. Domains can be used to restrict access to a group of CSRs or to group the devices.

To assign a device to a domain, choose a domain from the Domain menu.

Removing the Association Between a Device and a Subscriber

Removing an association breaks the link between a device and subscriber, but leaves the device and subscriber records available in the system.

To remove a subscriber/device association, click Remove Association.

Deleting a Device

Deleting a device removes its association with a subscriber (if one exists), and deletes all information about the device from the system.

To delete a device, click Delete Device.

Managing the Local Network

The Local Network window displays information about any LAN devices attached to the subscriber’s CPE device. The LAN devices might be physically attached, or if wireless networking is enabled, might be communicating wirelessly with the device.

You can view link throughput and the number of known LAN devices and actual devices online. You can also assign icons to devices and name them, and delete disconnected devices from the LAN.

Some local network devices (such as webcams) might have a local interface web service that lets you manage the device configuration. Prime Home can be used to set up a link to this interface that appears in the user’s control panel. It also sets up a port forward that allows the interface to be accessed from the internet.

If a device supports a local interface, its manual provides information on the port or path required to access the local interface. The device must be online to configure this link.

Viewing Local Network Status

The information displayed in the Local Network window can be useful for troubleshooting. For example, if a subscriber is running an unsecured wireless network, there might be unauthorized users who are impacting service. You can see device IP and MAC addresses, device status, connection type, and any applied services.

If the device is wireless, the Connections column shows the type of Wi-Fi (b, g, or n) and a graph indicating the signal strength.

If the device supports it, you can enable a local interface. You can also delete offline devices. For more information about working with services for specific devices, see Chapter 5, “Working with Services.”

To display the Local Network window (Figure 4-5), click view.
**Figure 4-5  Local Network Window**

### Naming a LAN Device

To name or rename a device:

**Step 1** In the Local Network window, click the icon in the Device column.

**Step 2** Type a name for the device.

**Step 3** If desired, select an icon for the device.

**Step 4** Click **OK**.

Some devices support a browser-based local interface for configuration. Review the documentation for the device to determine the port number or path needed to access the device.

### Enabling Local Interface Access

To enable local interface access:

**Step 1** In the Local Network window, click **Enable** in the Local Interface column.

**Step 2** If applicable, enter the port number or path (see **Figure 4-6**); then, click **OK**.

**Step 3** Save the changes to see the new link.

**Step 4** To disable local interface access, click **Disable** in the Local Interface column.
Deleting a LAN Device

To delete a LAN device:

**Step 1**  
In the Local Network window > Action column, click **Delete** for the device that you want to delete. 
The Delete option is available only for devices that are offline.

**Step 2**  
In the confirmation dialog box, click **Delete**.

Viewing Device Status

Device status provides information about the CPE gateway device for the account, including signal and statistical information you can use for troubleshooting a customer connection. The information available depends on the type of device.

To display the Status window (Figure 4-7), click **view**.
Status

The Status section of the Status window shows basic information about the device, including the time since the first inform (checkin), the time since the most recent inform, the current inform interval, and the amount of time the device has been on since installation or its most recent restart.

Line Information

The Line Information section of the Status window displays information about upstream and downstream line conditions, including throughput, signal/noise ratio, attenuation, and transmit power. This information is only available for devices that support it.

DSL or Cable

The DSL or Cable Statistics section of the Status window displays information about the amount of data (blocks) transmitted upstream and downstream. It also displays statistics about line errors. This information is available only for devices that support it.
**Bonded Line Information/DSL Statistics**

The Bonded WAN section of the Status window displays Line information such as Link Speed and Signal-to-noise ratio (SNR) on both Bonded lines - upstream and downstream. This section also displays DSL Statistics on various types of errors such as blocks and bit errors for both upstream and downstream bonded lines. This information is available only for devices that support it.

**WAN Interface Statistics**

The WAN Interface section of the Status window displays information about the subscriber’s WAN connection. Information includes the WAN ID, interface type, connection type, amount of data transmitted and received, and number of errors and dropped packets. This information is available only for devices that support it.
Working with Services

Each account can have multiple services enabled. Some services apply to the entire home network; others apply to specific devices. This chapter explains how to manage:

- Bandwidth monitoring
- Wireless networking
- Port forwarding
- Speed Test
- Content filtering
- Time blocking

Services appear on the left side of the Customer Support tab. To view services, click Services. To view a specific service, click view.

Note: You might see additional services, or services might appear in a different order, depending on how your system administrators configured Prime Home. For information on adding services or changing the order in which services are listed, see Managing Services, page 8-10.

Monitoring Bandwidth Usage

The Cisco Prime Home Bandwidth Monitor allows service providers to troubleshoot problems with degradation of Internet service caused by competition for bandwidth shared by multiple users. The Cisco Prime Home Bandwidth Monitor was developed to enable service providers to troubleshoot these issues and pinpoint their cause. Using intelligence in the CPE device (broadband modem or router), the Bandwidth Monitor routinely collects and reports bandwidth usage data for the whole home, as well as for each individual device behind the CPE device. With this data at their disposal, service providers can identify which devices are using the most bandwidth and resolve a customer’s Internet service issues more quickly.
Launching the Bandwidth Monitor

To launch the Bandwidth Monitor (Figure 5-1):

Step 1  From the Customer Support window, bring up a subscriber’s profile either by doing a search or by clicking the subscriber’s name in the Customer Support table.

Step 2  Expand the Services menu in the left sidebar.

Step 3  Select Bandwidth Monitor.

Figure 5-1  Bandwidth Monitor Window

Analyzing the WAN Interface Chart

The WAN Interface chart indicates the total amount of bandwidth that has been used by a particular CPE device. By viewing this chart, you can identify any usage patterns that exist and focus on times when bandwidth usage was higher. By default, results are shown for the past hour. To view results for a different period of time, click the appropriate link above the chart. When you place your cursor over any point on the chart, a tooltip displays the average downstream and upstream figures for that point in time. To view results for a specific portion of the current chart, move your cursor to the desired starting point, click, and then move the cursor to the desired end point while holding down the mouse.

Note  You can either hide or show downstream and upstream rate data by clicking the appropriate label below the chart.

To enable the collection and reporting of this data, select the Bandwidth Monitoring WAN Collection check box.
Analyzing the LAN Device Traffic Share Chart

The LAN Device Traffic Share chart takes things a step further and indicates the amount of bandwidth used by every device in a customer’s home network. By viewing this chart, you can quickly identify which LAN devices are using the most bandwidth and focus your troubleshooting efforts on them. By default, downstream rate data is shown here. To toggle between downstream and upstream data, click the appropriate link above the chart. When you place your cursor over any point on a device’s line chart, a tooltip displays the name of the LAN device and its average downstream or upstream figure for that point in time. To either hide or show the results for a particular device, click the appropriate label below the chart.

*Note*

This chart will display data for the same period of time covered in the WAN Interface chart.

To enable the collection and reporting of this data, select the **Bandwidth Monitoring Collection Per Device** check box.

LAN Device Table

The LAN Device table lists every device that the Bandwidth Monitor collects and reports information for. From here, you can view more specific information for those devices. Each entry in this table provides a representative icon, a short description of the device, the device’s IP and MAC addresses, and a graph that indicates the device’s bandwidth usage over the past hour.

Setting Chart Options

To set chart options:

1. From the bottom-left portion of the Bandwidth Monitor, click the Chart Options link.
2. Set the following options:
   - Hide LAN devices averaging below x kbps for the past hour: Devices that have used less bandwidth than the threshold you specify here are not displayed in the LAN Device Traffic Share chart. If you do not specify a threshold, Prime Home sets the default value of 0.1 kbps.
   - Zoom both charts together: When this option is selected and you zoom in on a particular period of time in one of the charts, the other chart automatically updates and displays information for the same period of time.
3. Click **Apply**, and then click **Close**.

Managing Wireless Networking

Wireless networking lets the subscriber connect LAN devices to the CPE device wirelessly. Any device capable of wireless networking—computers, video streaming devices, web cameras, or Wi-Fi-capable phones and tablets—can connect to the subscriber device.
You can configure Multi-band WiFi settings; i.e. WiFi devices that operate at either the 2.4GHz or 5GHz frequency band. Depending on the band, you can choose different modes - which vary in the speed that they transmit data. More than one network can be configured for each frequency band, provided the CPE device supports it.

You can set and modify primary and guest wireless networks for each radio on the device, depending on its capabilities. For both a primary and guest network, an SSID name and security level can be configured. Different Channels and Channel Widths can also be configured.
To display the Wireless Networking window (Figure 5-2), click **view**.

**Figure 5-2   Wireless Networking Window**

---

**About Wireless Networking**

To enable wireless service, specify the following parameters in the Wireless Networking window:

**Wireless Networks**

- **Enabled**—Turns the network on or off.
- **SSID**—Displays the CPE device ID; typically a word, code, or short phrase. Compatible devices can choose from available SSIDs to connect. Administrators can set the SSID, or subscribers can set it for their devices from their control panel.

  If the device supports multiple SSIDs/networks, each one has its own interface section where it can be enabled and disabled independently and the SSID and security type can be set.

- **Passphrase**—Password or phrase used to establish secure communications. You can specify a key, or Prime Home can generate a random one for you. Subscribers must know the key to connect LAN devices to the wireless access point.
Managing Port Forwarding

Port forwarding lets you specify ports that are open for communication. By default, the subscriber device blocks access to most ports. If an application requires other ports, you must specifically open them.

If a customer cannot use an application, you must determine which ports need to be open.

Port forwarding is specific to a device. To avoid conflicts, each port forward should be applied to only one device. Some CPE devices do not allow conflicting port forwards to be set; others do. Prime Home allows you to assign conflicting port forwards, but it flags them.

To display the Port Forward window (Figure 5-3), click view.
Enabling Port Forwarding

To enable port forwarding:

**Step 1**
In the Port Forward window, click **Enable**.

**Step 2**
Click **Save**.

Disabling Port Forwarding

To disable port forwarding:

**Step 1**
In the Port Forward window, click **Disable**.

**Step 2**
Click **Save**.

Adding a Port Forward

Before adding a port forward, you must know the following:

- The specific LAN device for which you are opening a port. If the LAN device is already known, you can choose it from a list of known devices. Otherwise, you must know the IP address of the LAN device.

- The specific port or range of ports to open and the protocol used (TCP or UDP). Alternatively, you can enter the name or partial name of an application; Prime Home locates the necessary port information.

To add a port forward:

**Step 1**
In the Port Forward window, click **Add Port Forward**.

**Step 2**
In the Add Port Forwards window, choose the LAN device for the port forward. Do one of the following:
Choose **Select Device**, and from the Select Device menu, choose a known LAN device. You can only add port forwards to devices that are currently online.

Choose **Enter IP Address** and enter the IP address of the LAN device.

**Step 3** Specify the port by doing one of the following:

- Choose **Enter Custom**. Enter the application name and protocol (TCP or UDP). Specify a range of port numbers by entering a starting port number and an ending port number. Specify the target port number.

- Choose **From List**. Enter the name or partial name of the application. Once you type three or more characters, a list of potential matches appears. If the application you want is in the list, select its name. The port numbers are displayed.

**Step 4** Click **OK**; then, click **Save**.
Deleting a Port Forward

To delete a port forward:

Step 1  In the Port Forward window, locate the port forward you want to delete.
Step 2  Click Delete.
Step 3  Click Save to save your changes.

Requesting a Speed Test

You can test the speed of both upstream and downstream traffic on your device. The result is displayed on the gauge after the device completes the speed test. Both the Download and Upload test results are displayed in a table with the following information:

- Start and end time
- Test bytes: actual size of the file downloaded during the speed test
- Total bytes: file size plus the headers and overhead associated with the request
- Throughput: rate of successful delivery measured in bps

You also have the ability to change the default settings by clicking on Configure URLs for Speed Test. For the Download speed test, you can change the FTP server from the default to a server of your choice. For the Upload speed test, you can determine both the FTP server and the upload file size.

Figure 5-4  Speed Test
Managing Content Filtering

Content filtering lets subscribers block inappropriate web content. You can set content filters at four levels, or specify no content filtering. Subscribers can create lists of specific sites to allow or block. You can apply filter settings to the entire network or to specific devices. Subscribers can change these settings in their control panel.

Note

Filter level names and categories are configured in a special configuration file. Configuration options can be set to disallow access if the content rating service is unavailable, if a site is unrated, or if the site is secure (https). For assistance with the content filtering configuration file, contact Cisco Advanced Services.

To display the Content Filtering window (Figure 5-5), click view.

Figure 5-5  Content Filtering Window
About Content Filtering Levels

Content filtering uses a third-party service that categorizes websites into specific categories:

- **Kids (6 and under)**—Allows access only to sites categorized as appropriate for children 6 and under. All other addresses are blocked. If a subscriber wants to allow access to additional sites, the site addresses can be added to the allow list.

- **Young Children (7-12)**—Blocks a wide range of content categorized as inappropriate for young children, as well as web-based communications, including access to webmail systems, chatting and chat sites, and forums and message boards. File sharing is not allowed. Sites that are not categorized as inappropriate are allowed. Subscribers can block additional content by adding specific addresses to the block list.

- **Young Teens (13-16)**—Blocks content categorized as inappropriate for young teens. It also blocks file sharing, chatting and chat sites, dating sites, and virtual communities. It does allow access to webmail and blogging. Sites that are not categorized as inappropriate are allowed. Subscribers can block additional content by adding specific addresses to the block list.

- **Mature Teens (17-18)**—Blocks sites categorized as pornography, alcohol, anonymizers, drugs, gambling, hate, tobacco, violence, and weapons. There are no restrictions on file sharing, webmail or chat, or virtual communities. Sites that are not categorized as inappropriate are allowed. Subscribers can block additional content by adding specific addresses to the block list, or allow blocked content by adding addresses to the allow list.

**Note**  
Content filtering is not infallible. New websites appear constantly online, and it takes time for them to be categorized.

How Content Filtering Works

When content filtering features are enabled, the system goes through a series of checks to determine whether to allow a request from a particular device on the subscriber’s network. The results vary depending on what type of filtering features are enabled, such as allow lists, block lists, content filtering, or time blocking. It is important to understand the interactions among these features to be able to troubleshoot specific site access issues.

**Note**  
If an allow list is active, but a category filter has not been applied, access is blocked to all addresses not on the allow list. The assumption is that if an allow list has been provided with no category filter specified, the desire is to limit access to only the addresses specified on the allow list.

If a category filter has been applied, access is allowed to items on the allow list that would normally be blocked by the category filter. In all cases, if a block list is active, access to items on the block list is blocked, regardless of any category filter applied.

When the in-home device receives a request for a web page, it does the following in this order:

1. Checks to see if a block list is active for the device. If a block list is active, it checks the address against the block list. If the address is on the block list, access is blocked.

2. Checks to see if Time Blocking is enabled. If access during the current time is not allowed, access is blocked. (For information about restricting access by time, see Managing Time Blocking, page 5-14.)
3. Checks to see if an allow list is active for the device. If the address is on the allow list, access is allowed.

4. Checks to see if a filter level (Kids, Young Children, and so on) has been applied.
   - If no filter level has been applied, but an allow list is active, access is not allowed unless the address is on the allow list.
   - If a category filter has been applied, the device sends the site address (URL) to the content rating service. The content rating service returns information about the category.
     - If the site is in a category banned by the filter, access is blocked.
     - If the site is not in a category banned by the filter or is unrated, access is allowed.
     - If the Kids filter category is applied, access is allowed only if the site is rated appropriate for children 6 and under.

Note: Prime Home can be configured to block access if the content rating service is unavailable, if the site has not been rated or categorized, or if the site is secure (https).

The following examples show how content filtering works.

Example 1: Allow list applied. Category filter set to Kids.
The user requests access to a site.
The device checks the allow list, which contains that site. Access is allowed. Because the site is on the allow list, it does not need to check with the content rating service.

Example 2: Allow list applied. Category filter is not applied.
The user requests access to a site.
The device checks the allow list, which does not contain that site. Because no category filter is applied, it does not send the URL to the content rating service. Because an allow list is active without a category filter, it does not allow access to other sites. Access is blocked.

Example 3: Block list applied. Category filter set to Young Teens.
The user requests access to a chat site.
The device checks the block list, which does not include that site. It then checks time blocking to see if access is allowed at this time. It sends the site address to the content rating service. The service returns a category of Chat, which is not allowed under the Young Teens category. Access is blocked.

Example 4: Allow list applied. Category filter set to Young Teens.
The user requests access to a site.
The device checks the block list, which does not include that site. It then checks time blocking to see if access is allowed at this time. The device checks the allow list, which contains that site. Access is allowed.

Example 5: Allow list applied. Category filter set to Young Teens. Time blocking applied.
The user requests access to a site.
The device checks the block list, which does not include that site. It then checks time blocking, which shows that the device is not available for use at the current time. Access is blocked.
Enabling the Content Filtering Service

To quickly enable content filtering for a subscriber:

Step 1  In the Content Filtering window, click Enable.
Step 2  Click Save.

Disabling the Content Filtering Service

To quickly disable content filtering for a subscriber:

Step 1  In the Content Filtering window, click Disable.
Step 2  Click Save.

Managing Default Content Filtering Settings

The default settings apply to LAN devices that join the network after the default is applied. They do not affect existing devices already connected unless they are set to use the default setting. You can set a filter level and enable or disable allow and block lists.

You also use the default settings to edit allow and block lists. These lists can then be applied to individual devices. An allow or block list is simply a list of website domains that the subscriber’s device allows or blocks access to. Allow and block lists override the filter-level setting. For example, if the filter allows access to a particular site, but you place it on a block list, that site is blocked.

To set default content filtering settings:

Step 1  In the Default Settings section of the Content Filtering window, choose a default filtering level from the Filter Level menu.
Step 2  From the Allow List menu, choose Enabled to enable the list or Disabled to disable the list.
Step 3  From the Block List menu, choose Enabled to enable the list or Disabled to disable the list.
Step 4  Click Save.
Step 5  Edit the default allow and block lists by doing the following:
   a.  Click Edit Default Lists.
   b.  In the allow/block list editor, enter the domain names for allowed and blocked websites. Enter only one domain name per row.
   c.  Click OK; then, click Save.
Managing Content Filtering for Specific LAN Devices

You can set content filtering for specific LAN devices. For example, a subscriber might want to filter content for computers used by children in the household, but not for computers used by adults. Each device can have its own filter level, and you can enable or disable the allow or block lists for each device. Individual devices use the allow and block lists set up in Default Settings. You cannot create separate lists for each device.

To set content filtering for specific devices:

- **Step 1**: In the Settings by Device section of the Content Filtering window, choose a filter level for each device.
- **Step 2**: Enable or disable the allow list for each device.
- **Step 3**: Enable or disable the block list for each device.
- **Step 4**: Click Save.
- **Step 5**: To reset content filtering for a specific device so it uses the network default, check the Use Default check box for that device.

Managing Time Blocking

Time blocking lets subscribers restrict local network access to certain hours. They can also add a bonus time, which is a period of additional time available during periods when access is restricted.

Time blocking settings can be applied to the entire home network or to specific devices on the network. Subscribers can view and change these settings in their control panel.

To display the Internet Time Blocking window (Figure 5-6), click view.

---

**Figure 5-6 Internet Time Blocking Window**
Enabling Time Blocking

To quickly enable time blocking:

**Step 1**  
In the Internet Time Blocking window, click **Enable**.

**Step 2**  
Click **Save**.

Disabling Time Blocking

To quickly disable time blocking:

**Step 1**  
In the Internet Time Blocking window, click **Disable**.

**Step 2**  
Click **Save**.

Managing Default Time Blocking Settings

Default settings specify the local time zone and apply to the entire home network.

**Note**  
Time blocking settings for specific devices override the default settings. Any devices that join the network after the default is set up use the default time blocking settings.

To set default time blocking settings:

**Step 1**  
In the Default Settings section of the Internet Time Blocking window, choose a time zone from the Time Zone menu.

**Step 2**  
Under Night Blocking, choose to block or unblock network access during specific hours for weekdays and weekends. If you choose Block, specify the hours during which access is blocked.

**Step 3**  
Click **Save**.

Managing Time Blocking for Specific Devices

You can apply time limits, night blocking, and bonus time to specific LAN devices. Once a LAN device has been recognized by the system, its blocking information continues in effect even if it leaves the network for a period. For example, if a laptop that is night blocked is removed from the network for a week, night blocking resumes when the laptop returns to the network.

**Note**  
Time blocking limits apply only when a device is connected to the local network. If the device connects to a different network, the limits do not apply.
To set time blocking for specific devices:

**Step 1** In the Settings by Device section of the Internet Time Blocking window, click a device name.

**Step 2** In the Edit Time Blocking window (Figure 5-7), uncheck the **User Default** check box.

**Step 3** Use the sliders to choose the number of hours per day the device can access the local network per weekday and per weekend day.

**Step 4** For night blocking, choose whether the device is blocked during the night for weekdays or weekends. Specify the time periods for weekday and weekend night blocking.

**Step 5** (Optional) Add bonus time.

**Step 6** Click **OK**; then, click **Save**.

---

**Figure 5-7  Edit Time Blocking Window**

![Edit Time Blocking Window](image)
Adding Bonus Time

Bonus time provides extra time to use the local network when access is blocked. The bonus time period begins immediately. You can add from 30 minutes to 23 hours and 30 minutes of time.

To add local network bonus time:

**Step 1**
In the Add Bonus Time section (Figure 5-8), choose the amount of time to add.

**Step 2**
Click Save.

---

**Figure 5-8 Add Bonus Time Section**

---
Performing Advanced Tasks

When working with accounts, you might need to investigate the customer network, send information to the customer’s device, or update device firmware. This chapter describes how to:

- View and manage event logs
- Browse parameters
- Run scripts
- Update firmware
- Replace devices
- Set up local GUI access

Advanced tasks appear on the left side of the Customer Support tab. To view advanced tasks, click Advanced. To view a specific task, click view.

Note: The available tasks and the order in which they appear depend on how your Prime Home installation is configured, and on your user level (CSR or Admin).

Working with Event Logs

Event logs record information about TR-069 communications between the device and the ACS, such as when data is sent to or received from a device, error messages, and the results of scripts or scheduled events. You can view event logs at different levels of detail, print event logs, and configure the amount and type of information collected. Logs are kept for a maximum of 10 days.

The Event Logs window (Figure 6-1) displays a list of recent sessions by date and time and a menu for configuring the logging level.

To view the Event Logs window, click view.
Figure 6-1  Event Logs Window

### Refreshing the Event Logs List

To refresh the Event Logs list, click ![Refresh](f01_24.png). The Recent Sessions list displays the most recent sessions.

### Viewing a Session Log

To view a session log:

**Step 1**  In the Event Logs window, click a log file.  
The logged information appears in the Session Log.

**Step 2**  Use the icons in the top-right corner of the session log to:

- ![Print](f01_25.png)  Print the log.
- ![Expand](f01_26.png)  Expand the log to fill the window.
- ![Collapse](f01_27.png)  Collapse the log display.
- ![Close](f01_28.png)  Close the log file.
**Step 3** Depending on the event logging level, check the following check boxes to view trace and SOAP details in the log:

- **Show Trace Detail**—Provides detailed information about events captured by the log. You can view the parameter and properties used, as well as detailed information about script execution.
- **Show SOAP Detail**—Displays the XML communications with the device for each event in the log.

---

**Setting the Event Logging Level**

Prime Home lets you set a level for capturing events to the log. The level applies to the device. If a device is functioning well, you might want to turn off logging to reduce traffic or to avoid using up disk space. Conversely, if a customer reports a problem, you might want to turn on a higher level of logging to troubleshoot the problem. The following logging levels are available:

- **No logging**—No log information is recorded.
- **Info**—Records when the device connects to the server and information about any events that occurred, such as inform or upgrade events.
- **Debug**—Records session and script information, including parameters used in scripts and the calls made by the scripts to the device.
- **Network**—Saves a complete record of all network traffic sent and received, in addition to session and debug information.

To set the event logging level:

**Step 1** Open the Event Logs window for an account.

**Step 2** In the Configure Logging Detail section, choose a logging level for the device.

The system displays a message that the logging level was changed.

---

**Using the Parameter Browser**

The Parameter Browser window displays device data in a tree hierarchy. The data model is based on the TR-098 specification but includes Prime Home extensions. You can browse the hierarchy and select a parameter to view its properties and parameter values.

To view the Parameter Browser window (Figure 6-2), click **view**.
The Parameter Browser uses color to categorize information:

- **Black text**—Shows TR-098-specified attributes for which data has been gathered.
- **Grey text**—Shows TR-098-specified attributes for which no data has been gathered.
- **Orange text**—Shows data not specified by the TR-098 specifications.

To view device parameters:

**Step 1**  Open the Parameter Browser window for an account.

**Step 2**  Use the plus and minus icons to display more of the parameter hierarchy until you see the parameter you want to investigate.

**Step 3**  Click the parameter.

**Step 4**  The parameter’s properties appear in the Properties section of the Parameter Browser window. Click the Expand icon to expand the Properties view.

**Step 5**  Use the icons on the Parameter Browser window to customize the display:

- Expand the parameter hierarchy.
- Collapse the parameter hierarchy.
- Expand the Properties section to fill the window.
- Collapse the Properties section.
- Close the Parameter Browser.
Working with Scripts

The Scripts window (Figure 6-3) lets you add predefined scripts to a queue. Scripts in a queue run against the device the next time it checks in. For more information about defining scripts, see Managing Scripts, page 8-15.

To view the Scripts window, click view.

Figure 6-3 Scripts Window

Adding a Script

Scripts define actions to be taken for a device. Prime Home supplies some scripts, and system administrators can write additional scripts. The scripts can address any parameters in the data model. For example, there is an included script to set the inform interval.

When you work with scripts in the context of an account, you select a script from a menu. You might need to specify parameters that the script requires to run. The script is placed in a queue, and it executes the next time the device checks in.

You can also view past script results from the Scripts window.

To add a script to the queue:

Step 1 In the Scripts window, choose a script from the Select Script menu.
Step 2 Click Add Script to Queue.
Step 3 If requested, specify script parameters.
Step 4 Click OK.
Step 5 If desired, add more scripts to the queue.
Step 6 Click Save to save your changes.

The Script Log displays the pending scripts.
Viewing Script Results

To view script results, click a script in the Scripts window > Activity column. Activities that are complete are shown in blue text. The status field is blank. The Script Log Detail window (Figure 6-4) shows the results of the action.

Figure 6-4  Script Log Detail Window

<table>
<thead>
<tr>
<th>Script Log Detail</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tue Apr 24th 2012 11:39:55</td>
</tr>
<tr>
<td>Tue Apr 24th 2012 11:39:55</td>
</tr>
<tr>
<td>Tue Apr 24th 2012 11:39:55</td>
</tr>
<tr>
<td>Tue Apr 24th 2012 11:39:57</td>
</tr>
<tr>
<td>Tue Apr 24th 2012 11:39:57</td>
</tr>
<tr>
<td>Tue Apr 24th 2012 11:40:05</td>
</tr>
<tr>
<td>Tue Apr 24th 2012 11:40:05</td>
</tr>
<tr>
<td>Tue Apr 24th 2012 11:40:05</td>
</tr>
<tr>
<td>Tue Apr 24th 2012 11:40:05</td>
</tr>
</tbody>
</table>

Updating Firmware

The Update Firmware window (Figure 6-5) lets you specify a new version of firmware to be applied to a device. The update is placed in a queue and the firmware is updated the next time the device checks in. The Update Firmware window lists any installed firmware updates that are available for the specified device model.

To view the Update Firmware window, click view.
Queuing a Firmware Update

To queue a firmware update:

**Step 1**  
In the Update Firmware window, select a firmware version.

**Step 2**  
Click **Add Firmware Update to Queue**.

**Step 3**  
Click **Save**.

Replacing a Device

If a device malfunctions, you might need to replace it. The Replace Device window (Figure 6-6) lets you copy settings from the currently displayed device to another device.

**Note**  
Make sure that the device from which you want to copy settings is selected and displayed on the Customer Support tab.

To display the Replace Device window, click **view**.
Copy Device Settings to Another Device

To copy device settings to another device:

**Step 1**  In the Replace Device window, click **Select Device**.

**Step 2**  Do one of the following to locate a device:

- Use the New Device tab to enter information about a new device that will check into your system in the future.
- Use the Existing Device tab to locate an existing CPE device not currently assigned to a subscriber. Click the device serial number to select it.
- Use the Activation Server Device tab to locate a CPE device.

**Note**  Depending on how your Prime Home installation is configured, you might not see the Activation Server Device tab.

**Step 3**  Click the device to which you want to copy settings.

**Step 4**  Verify that the selected device is the correct one.

**Step 5**  Click **Copy Settings**.

After you copy the settings, the page reloads the information about the device that received the settings. You can then make changes to the new device.

Setting Up Local GUI Access

The Local GUI Click Through window (Figure 6-7) lets you create a link to the user interface for a device. This link enables a CSR to access local statistics maintained by the CPE device, or configure device-specific settings that are not available through the Prime Home interface.

To view the Local GUI Click Through window, click **view**.

To set up local GUI access:

**Step 1**  In the Local GUI Click Through window, check the **Enable Local GUI Access** check box.

**Step 2**  Click **Save**.

**Step 3**  After the device has updated, return to the Local GUI Click Through window to use a link to the device user interface.

The link remains active for about 15 minutes. After that, access must be re-enabled before you use it again.
Figure 6-7  Local GUI Click Through Window

- ACCOUNT
- SERVICES
- ADVANCED
  - Event Logs  view
  - Parameter Browser  view
  - Replace Device  view
  - Scripts  view
  - Synchronization  view
  - Update Firmware  view
  - Local GUI Click Through

LOCAL GUI CLICK THROUGH

Device Click Through

Enable Local GUI Access

Steps:
1. Save changes
2. Wait for device update to complete
3. Check back here for Local GUI Access Link
Reports

Prime Home includes a customizable reporting tool with standard reports, exportability, and analysis. Reports can provide information about devices and subscribers across your entire installed base in a unified fashion. This information enables you to take preventive measures when support issues occur.

You can collect snapshot data and see just that moment in time, or you can continually export and aggregate data to study trends over time. Report results can be saved in comma-separated value (CSV) format and from there can be translated into graphs or spreadsheets, or opened with other tools such as Microsoft Excel or Crystal Reports.

Reporting is an optional, subscription-based product that is enabled with a license key.

Built-In Reports

Prime Home comes with five built-in reports:

- Device Count by Firmware Version
- Device Count by Manufacturer and Model
- Device Count by Label
- Subscriber Count by Label
- Device Count by WAN Interface

These reports, called aggregate reports, cannot be edited or deleted, but the results can be exported in CSV format to Excel or any other spreadsheet application. Aggregate reports give you insight into the total subscriber/device base (see Figure 7-1).
Running an Aggregate Report

To run an aggregate report:

**Step 1**
On the Reports tab, select **Aggregate Reports**.

**Step 2**
From the Available Reports drop-down list, choose a report.

**Step 3**
Do one of the following:

- View the results on your screen.
- To export the results, click **Save As CSV**.

Custom Reports

Custom reports are reports that you design. Custom reports can be saved, edited, and deleted. The results of custom reports can be exported in CSV format and used as the basis for bulk operations.
Reports Tab

You can easily locate and run reports from the Reports tab. The Reports tab displays a list of previously defined custom reports (Figure 7-2).

Figure 7-2 Previously Defined Custom Reports

You can use the following controls on this tab:

- Add a new custom report.
- Delete an existing report.
- Set the number of reports displayed on a page.
- Go to the beginning of the list of reports.
- Go backward one page in the list of reports.
- Go forward one page in the list of reports.
- Go to the end of the list of reports.
- Refresh the list of reports.

Finding an Existing Report

To find a report:

**Step 1**  On the Reports tab, type all or part of the report name in the search field.

**Step 2**  Click 


Running an Existing Report

To run an existing report, click the report name. Prime Home displays the report results (Figure 7-3).

**Figure 7-3 Wi-Fi Report Results**

You can do the following with the report results:

- Apply or remove labels to subscribers or devices found by the report—Choose a label from the Add or Remove section of the Labels menu.
- Save the report results as a CSV file—Click **Save as CSV**.
- Create a bulk operation for the subscribers or devices found by the report—Click New Bulk Operation. For more information about bulk operations, see Chapter 10, “Managing Bulk Operations.”
- Print the report—Click .
- Edit the report definition—Click .
- Close the report and return to the Find Report window—Click .

Custom Reports

Figure 7-4 indicates the tasks you need to complete when creating a custom report.

**Figure 7-4 Custom Report Creation Process**

As you build your report, Prime Home shows you the potential report results (Figure 7-5).
Creating a Custom Report

To create a custom report:

**Step 1** On the Reports tab, click .

**Step 2** In the Report Name field, enter a name for your report.

**Step 3** Choose your data fields. These fields are the headings for the columns in your report.

  a. From the Available Columns area, drag the field you want to see in the report and drop it into the Include these Columns area.

  b. Drag additional fields into the Available Columns area.

**Note** To search the available columns, enter a keyword and click . To expand the editing area, click .
**Step 4** (Optional) Define the sort order:

a. From the Available Columns area, drag the field you want to sort on and drop it in the Sorting area.

b. To sort on additional fields, drag each field to the Sorting area. Arrange the fields in the order in which you want to sort.

**Step 5** (Optional) Set up filtering:

a. From the Available Columns area, drag the field you want to use for filtering the report and drop it in the Filter Criteria area.

b. Select a parameter to apply to the filter. The available parameters depend on the field included.

c. To filter on additional fields, drag over the fields and arrange them in the order in which you want to filter.

**Step 6** Do one of the following:

- Click **Save** to save the report and stay in the Edit Report window.
- Click **Save and Return to View** to save the report and view the results on the Devices and Subscribers window.

After you save the report, it appears on the Find window.

---

**Working with Sort Order**

You can sort on one or more fields, you can order the fields to control the sort order, and you can choose an order for each field (ascending or descending.)

When you add a field to the Sorting area, the following options appear (Figure 7-6):

- **remove**—Click to remove the field from the sorting area.
- **A-Z**—Click to change the sort order from ascending to descending or vice versa.

**Figure 7-6 Sorting Options**

To change the sort order, drag the fields to represent the order in which you want the data sorted. The data is sorted on the top field first, then the next, and so on.

---

**Working with Filters**

Filtering enables you to limit the devices or subscribers found by a report. You filter the report results by adding criteria. Each available column has a set of parameters you can apply. You can create complex filters by grouping filter fields and using AND and OR.
Applying Parameters

You must apply a parameter to each filter criterion (Figure 7-7). The parameters can be a simple true or false, or you can specify a relationship (more than, less than, equal to) or set up a list of values.

For example, if you want to filter on devices that have Content Filtering and Port Forwards enabled, you can create a list of those two items.

After you select a parameter and supply additional information, do one of the following:

- Click **Apply** to apply the filter parameter.
- Click **Cancel** to cancel the parameter.

Editing Parameters

To change a parameter after applying it, click **edit** (Figure 7-8). Move the pointer over the filter criterion to display the edit link.
Using Boolean Logic

When you specify two or more filter criteria, the Boolean AND operator becomes available (Figure 7-9). To toggle between AND and OR, click the operator.

You can create complex, nested filters by grouping two or more criteria and applying AND or OR. To group two or more criteria, click Group. Drag additional criteria into the group.

![Filter Criteria: Boolean Logic](image)

Working with Advanced Syntax

You can view the query language statement for a report you create (Figure 7-10). You can edit this syntax or you can copy it and use it as a query for bulk operations.

![Advanced Syntax Window](image)

To view advanced syntax, click ☰.

Using Reports to Understand Your Network

Reports can be used to export data that is maintained in Prime Home. This data can be used to study a wide variety of conditions, including:

- Identifying potential problem access lines as indicated by SNR, attenuation, retrain, and data rate. This information can help reduce churn.
- Identifying CPEs with open Wi-Fi security and excessive Wi-Fi devices. This information reduces calls to your CSRs and saves costs.
• Studying device trends, which could include providing a snapshot of shipment trends during promotions or watching for information about which devices tend to churn more quickly than others. This data is useful when deciding on the value of higher- versus lower-end managed devices. It might also help indicate product longevity, based on a first-inform time analysis.

Examples of other trend reports include:
  - Number of managed devices by manufacturer, model, and firmware version
  - Distribution of wired versus wireless networks
  - Use of DSL versus Ethernet

• Studying device trends in the home, which is also helpful for understanding up-sell potential.

Examples of in-home, managed device trends include:
  - Number of LAN devices per subscriber
  - Number of Wi-Fi versus Ethernet devices per subscriber
  - Percentage of subscribers using Wi-Fi security (and at what level of security)
  - Wi-Fi channel use
  - Port forward use
  - Parental control use
  - Number of new customers who came online in the past week
  - Number of customers with multiple PCs in their home

• Examining speed breakdown of your installed base. This information can be correlated with network-side information and as a function of managed device manufacturer/model/version.

Examples of speed breakdown reports include:
  - Downstream/upstream link speed
  - Attenuation
  - Noise margin
  - Retrain frequency and uptime
  - Average broadband speed

• Investigating subscriber breakdown by device associated, advanced services enabled versus used, label, location, and first contact date.
Administration Overview

You use the Administration tab to control and manage the Prime Home software. System admins can:

- Create global system labels
- Add new user accounts to Prime Home and manage existing accounts
- Set roles for each new user to Prime Home
- Create and set up various actions
- Add device types
- Create new services that can be added to subscriber accounts
- Manage firmware
- Create automated action schedules
- Create and edit system announcements
- Synchronize devices

Licensing

The content in this guide is subject to your licensing agreement with Cisco. You might not have access to all features and sections of Prime Home. Features that must be explicitly licensed include:

- The number of users that can be logged into the system at the same time.
- The ability to run reports.
- The ability to write and run scripts.
Managing Labels

Use the Labels window (Figure 8-1) to review, edit, and create new labels to apply throughout Prime Home. You can apply labels to devices, subscribers, firmware, users, and scripts.

**Figure 8-1 Labels Window**

The Labels window comprises:

- **Existing Labels**—Shows all the current labels in the system. Click + to add a new label to the system with the Label Editor.
- **Label Editor**—Use the Label Editor to create new labels or edit existing labels. From here:
  - Click ✖️ to close the editor and discard your changes.
  - Click ✖️ to delete a label from the system.
  - Click ✶️ Save to save your changes.

**Labels Window**

To add a new label:

**Step 1** On the Administration tab, click Labels.

**Step 2** Click +.

The system displays the Label Editor.

**Step 3** Enter the label name in the Label Text field.

**Step 4** Click ✶️. A color palette window displays the colors you can use to distinguish your label.
Managing Users

The Users window (Figure 8-2) lets you manage users in Prime Home. This window includes a secondary search field that allows you to quickly search for user information. The field appears just under the User List heading.

Prime Home includes the following roles that you can apply to a user account:

- **Admin**—An Admin account allows access to all the functions in Prime Home.
- **Customer Support Representative**—A customer support representative (CSR) account can perform customer service tasks. The specific tasks that are available depends on how your Prime Home installation is configured.

---

**Step 5**
Select a color to apply from the color palette.

**Step 6**
Click ![Save](Save)

**Note**
Labels can include alphanumeric characters, underlines, and spaces only. Labels cannot exceed 32 characters in length.

---

**Editing a Label**

To edit a label:

**Step 1**
On the Administration tab, click **Labels**.

**Step 2**
Click a label to edit from the Existing Labels List.

**Step 3**
Make your changes to the fields. You can change a label’s name or color scheme.

**Step 4**
Click ![Save](Save)

---

**Deleting a Label**

To delete a label:

**Step 1**
Locate the label to delete from the Label list.

**Step 2**
Click ![Remove](Remove) next to the label’s name to remove it. The system refreshes the page, listing the remaining labels. If this label was applied to devices or subscribers, it is removed from those items.
The Users window comprises:

- **User list**—Displays a search result list of users in Prime Home. From here:
  - Click 🔄 to add a new user to Prime Home.
  - Click 🔄 to refresh the User list.
- **Search field and 🔍**—Use the search field to search for a username.
- **Search Results List**—This list displays all your search results. If your results are more than the page can handle, then use the page forward and page backward buttons to see more results. Use the Items per page drop-down menu to set the limit of results to 10, 25, or 50 per page.
- **Click 🗑 to delete a user from the system.**
- **User Editor**—The User Editor allows you to enter or edit user information. Enable the account by checking the **Enabled** check box. Disable the account by unchecking the **Enabled** check box.
- **User Actions**—Assign or remove labels from the user. From here:
  - Click 📲 to expand the User Editor to full size. When in full-size mode, click 📨 to restore the window to its original size.
  - Click 🗑 to close the editor and discard your changes.
  - Click 📦 Save to save your changes.
Adding a New User

To add a new user:

**Step 1** On the Administration tab, click **Users**.
**Step 2** Click **.**
**Step 3** Enter the user’s login name in the Login field.
**Step 4** Check the **Enabled** check box to activate the account and allow the user to log in. (To disable the account later, uncheck the **Enabled** check box.)
**Step 5** Enter the user’s full name in the Full Name field.
**Step 6** Enter the user’s e-mail address in the Email field.
**Step 7** Enter the user’s password in the Password field.
**Step 8** Enter the user’s password again in the Confirm field.
**Step 9** Select a role for your user from the Roles list.
**Step 10** (Optional) Select one or more domains that this user can view and work with. To select more than one domain, hold the Control (PC) or Command (Mac) key while selecting and deselecting.
**Step 11** Click **Save**.

Editing User Information

To edit user information:

**Step 1** Search for the user.
**Step 2** Click a username in the Users List to display the User Editor.
**Step 3** Edit any of the fields for that user.
**Step 4** Click **Save**.

Deleting a User

To delete a user:

**Step 1** Locate the user to delete from the User List.
**Step 2** Click ** in the user’s row to remove the user from the system.
The system refreshes the page, listing the remaining users.
Managing Device Types

Use the Device Type List page (Figure 8-3) to manage device type profiles in your system. A device type maps to a hardware model. Each model has its own unique signature. Prime Home uses device types to differentiate between different types of hardware.

When a device is created in the system, it gets associated to a device type. The system pulls in this information to create the association by locating the device's built-in hardware version or hardware class. The system tries to pull as much information from the device into the profile as it can.

When you connect a new device to Prime Home, the system automatically associates it to a device type. The system either uses an existing device type or creates a new one to match the device. When a new type is created, Model Name and Manufacturer are set to default values that can be modified by editing the device type.

Figure 8-3        Device Type List

The Device Type page consists of the following:

- Device Type List—This list displays all the available device types in the system. From here:
  - Click to refresh the list.
  - Click to add a new device type to the system.
  - Click to delete a device type from the system.

Device Type Page

The Device Type page consists of the following:

- Device Type List—This list displays all the available device types in the system. From here:
  - Click to refresh the list.
  - Click to add a new device type to the system.
  - Click to delete a device type from the system.
Device Type Editor—Click a device name from the Device Type list to open the Device Type Editor. Use the Device Type Editor to create or edit device types. From here:

- Click to clone and create a new device type based on the current settings. This option appears only when you are editing a pre-existing device type.
- Click to expand the Device Types Editor window to full size. To restore the window to its original size when in full-size mode, click again.
- Click to close the editor and discard your changes.
- Click to save changes to the device type.

### Adding a Device Type

To add a device type:

<table>
<thead>
<tr>
<th>Step 1</th>
<th>On the Administration tab, click Device Types.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Click .</td>
</tr>
<tr>
<td>Step 3</td>
<td>Enter the device name in the Hardware Version field.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Enter the device product class in the Product Class field.</td>
</tr>
<tr>
<td>Step 5</td>
<td>From the WAN Interface Type menu, select the WAN interface type.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Enter the model name in the Model Name field.</td>
</tr>
<tr>
<td>Step 7</td>
<td>Enter the manufacturer name in the Manufacturer field.</td>
</tr>
<tr>
<td>Step 8</td>
<td>Enter a URL to a product icon (if desired) in the Product Icon URL field. The icon can be no bigger than 64 x 64 pixels high and wide.</td>
</tr>
<tr>
<td>Step 9</td>
<td>Click .</td>
</tr>
</tbody>
</table>

### Editing a Device Type

To edit a device type:

<table>
<thead>
<tr>
<th>Step 1</th>
<th>On the Administration tab, click Device Types.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Select the device name from the Device Types list.</td>
</tr>
<tr>
<td></td>
<td>The system displays the Device Types Editor window.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Manually edit the fields.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Click .</td>
</tr>
</tbody>
</table>
Deleting a Device Type

To delete a device type:

**Step 1** Locate the device type to delete from the Device Types List.

**Step 2** Click to remove a device type from the system. The system refreshes the page, listing the remaining device types.

Managing Firmware Versions

Use the Firmware List window (Figure 8-4) to manage firmware versions for the CPE.

**Figure 8-4  Firmware List Window**

From this window, you can see various firmware for device types and track upgrade paths to verify that each upgrade is compatible with the previous firmware. If a subscriber’s current system has errors, you might want to update or downgrade the firmware running on the subscriber’s device.

Firmware List Window

The Firmware List window consists of the following:

- **Firmware List**—Displays a list of all available firmware versions for all CPE models available on the system.
  - Click to add a new firmware release to the list.
  - Click to refresh the list.
  - Click to delete a firmware release from the system.
Managing Firmware Versions

- Firmware Editor—Use the Firmware Editor to create new firmware releases or edit existing firmware releases.
  - Click to create a new firmware release based on the current settings.
  - Click to expand the Firmware Editor window to full size. To restore the window to its original size when in full-size mode, click again.
  - Click to close the editor and discard your changes.
  - Click to save the changes to the firmware.

Adding a Firmware Version

To add a firmware version:

1. On the Administration tab, click Firmware.
2. Click .
   The system displays the Firmware Editor window.
3. From the Device Type drop-down list, choose the model of a device to associate the firmware version to.
4. Enter the software version number in the Software Version field.
5. Enter a release date in the Release Date field. You can click to open up a calendar to select a release date as well.
6. Specify a web location for the firmware in the Binary URL field.
   - Note: You do not upload firmware directly to Prime Home. The URL must be accessible to the device.
7. Click .

Editing a Firmware Version

To edit a firmware version:

1. On the Administration tab, click Firmware.
2. Select the firmware version from the Firmware List.
   The system displays the Firmware Editor window with the firmware version info.
3. Manually edit the fields.
4. Click .
   You can clone a firmware version to quickly create new update releases that contain information similar to that of the previous firmware.
Cloning a Firmware Version

To clone a firmware version:

Step 1  Click \( \text{add} \) to create a new firmware version based on current settings.

Step 2  Edit and adjust the information in the Firmware Editor.

Step 3  Click \( \text{Save} \).

Managing Services

Use the Services window (Figure 8-5) to manage services offered by your company. You can create new services and edit them directly in this window.

When you are done setting up your services on this window, you can activate or deactivate the service on your customers' devices from the Customer Support tab.

Figure 8-5  Services Window

The Services window comprises the following:

- Services—A list of all services in the system.
  - Click \( \text{refresh} \) to force a refresh of all services and refresh the service list.
  - Click \( \text{add} \) to add a new service.
  - Click \( \text{delete} \) to delete a service. (This option is only available for custom services.)
  - Click \( \text{Save} \) to save the service.
• User Interface Groups—Lets you create groups of services, which control how services are grouped together onscreen.
  – Click to add a new user interface group.
  – Click to delete a user interface group. (Only available for custom groups.)
  – Click to save the user interface group.

Adding a New Service

To add a new service:

1. Add service information. For details, see Adding Service Information, page 8-11.
2. Configure When Enabled properties. For details, see Configuring When Enabled Properties, page 8-12.
3. Configure When Disabled properties—Add the settings, user interfaces, and actions as described in Step 2.
4. Click .

Adding Service Information

To add service information:

Step 1 On the Administration tab, click Services.
Step 2 Click to open the Service Editor window (Figure 8-6).
Step 3 In the Name field, enter the name of the service. (This name appears in the list of services on the Customer Support tab or on the subscriber’s control panel.)
Step 4 In the Code field, enter a unique identifier for this service.
Step 5 In the Color field, click the field to display the color picker. Use the sliders to select a color, or enter RGB, HSB, or hex color values. Click to set the color.
The color appears next to the service name on the Customer Support tab.
Step 6 From the Status menu, choose Active or Inactive. (Active services appear on the Customer Support tab; inactive ones do not.)
Step 7 Do one of the following:
  • Check the Is Always Enabled check box for services that are always enabled.
  • Uncheck the Is Always Enabled check box for services that can be enabled and disabled on the Customer Support tab.

Note If a service is always enabled, you can configure only the When Enabled User Interface properties.
Choose where and how to display this service:

- **Portal Display**—Determines where this service appears in the Services list on the Customer Support tab.
- **Control Panel Display**—Determines where this service appears in the subscriber’s control panel.
  - From the Group menu, select the user interface group under which this service will appear.
  - In the Order field, type a number indicating the order for this service within the group. Smaller numbers appear closer to the top.

### Configuring When Enabled Properties

To configure the properties for a service that has been enabled:

**Step 1** Configure the access level (to specify whether subscribers can modify settings for this service):

- In the Access Level section, click **Add Setting**.
- Enter the element of the data model that describes the setting (for example, `settings.enabled.timeblocking`).
- From the menu, choose **None** to deny access or **Modify** to allow access.
- Repeat steps a through c for each access level you want to add.
Step 2  Configure the user interface. This lets you control information and settings that are displayed for different user interface areas related to this service, both on the Customer Support tab and on the subscriber’s control panel.

a. In the User Interface section, click **Add User Interface**.

b. From the Slot menu, choose how much information to display:
   - **Detail**—Shows detailed information and settings for the selected user interface area. It appears in the window for the service on the Customer Support tab and the subscriber control panel.
   - **Summary**—Information is a brief read-only version of the settings for this user interface. It appears in the left navigation of the subscriber's control panel.
   - **Help**—Lets you display helpful information in the subscriber’s control panel.
   - **Status**—Reserved for future use.
   - **LAN Device Detail**—Appears within the control panel when the user is viewing a particular local device. It shows device-specific information and settings for the service.
   - **LAN Device Summary**—Appears on the subscriber’s control panel when they pause the mouse over a device.

c. From the menu, choose one of the available user interfaces.

d. Enter values for Portal Order and Control Panel Order to determine the order in which user interface information is displayed. Smaller numbers appear closer to the top.

e. Select the roles the user interface is visible to:
   - **Admin**—Appears to Admin users only.
   - **CSR**—Appears to CSR users only.
   - **Subscriber**—Appears on the subscriber’s control panel.

f. Repeat steps a through e to add additional user interfaces.

Step 3  Configure Actions.

a. In the Actions section, click **Add Action**.

b. From the Actions menu, choose an action:
   - **sync app**—Synchronizes an application. Choose the application from the Application menu.
   - **run script**—Runs a script. Choose a script from the menu.
   - **set attribute value**—Sets a value for a data model element. Enter the setting and value. Check the **Force** check box to change the value regardless of prior setting; uncheck the **Force** check box to leave an existing value unchanged.
   - **remove attribute**—Removes a setting from the data model. Enter the data model element.
Editing a Service

To edit a service:

**Step 1** On the Administration tab, click **Services**.

**Step 2** Locate the service from the Services List.

**Step 3** Edit any field.

**Step 4** Click ![Save](Save.png).

Managing User Interface Groups

User interface groups let you control how services are grouped together on the Prime Home Customer Support tab and on the subscriber’s control panel. Once you have created the groups that make sense for your users, you then assign new and existing services to those groups.

Adding a User Interface Group

To add a user interface group:

**Step 1** On the Administration tab, click **Services**.

The system displays the User Interface Groups window.

**Step 2** In the User Interface Groups window, click ![Add](Add.png).

**Step 3** In the Code field, enter a unique identifier for this group.

**Step 4** In the Name field, enter the name of the group.

**Step 5** In the Order field, type a number indicating where you want this group to appear in the list. Smaller numbers appear closer to the top.

**Step 6** From the Realm menu, choose where this group appears:

- Portal—Appears on the Prime Home Administrator tab in the Services list.
- Control Panel—Appears on the screen used by subscribers to manage their services.

**Step 7** Click ![Save](Save.png).
Editing a User Interface Group

To edit a user interface group:

**Step 1**
On the Administration tab, click Services.

**Step 2**
Locate the service in the User Interface Group window.

**Step 3**
Edit any field.

**Step 4**
Click Save.

Deleting a User Interface Group

**Note**
Only custom user interface groups can be deleted from the system.

To delete a user interface group:

**Step 1**
In the User Interface Groups window, locate the group you want to delete.

**Step 2**
Click to delete your custom group from the system. The system refreshes the page, listing the remaining groups.

Managing Scripts

**Note**
Your system might restrict script editing based on your license with Cisco. If your license restricts editing scripts, you cannot add new scripts or edit the source of existing scripts. You can change a script’s name field and the Usable With option field.

Scripts are implemented using a customized JavaScript-based environment that runs on the ACS. This environment supports complete manipulation of the CPE via TR-069, as well as access to data models stored locally on the ACS, such as the subscriber’s.

Use the Scripts window (Figure 8-7) on the Customer Support tab to manage scripts on your system. You can add new scripts, edit existing scripts, or delete custom scripts. When a device checks into the system, scripts are executed on the device in the order in which they were put into the queue.
Prime Home contains two types of scripts:

- Bundled scripts—Scripts that are bundled with Prime Home.
- Custom scripts—Scripts that you set up and apply to your own network.

All script names must be unique. When writing custom scripts, write them with the idea that the script will run against one device at a time. Scripts that run on a device that is associated with a subscriber have access to the subscriber’s information.

For more information on building scripts, contact Cisco Advanced Services.
**Scripts Window**

The Scripts window comprises the following:

- **Script List**—This list displays all existing scripts. The Name column displays the action name. The Labels column displays any labels applied to the script. From here, you can:
  - Click to refresh the Script List.
  - Click to add a new script.
  - Select a script from the list to edit it in the Script Editor.
  - Click to delete a script. (Only available for custom scripts.)

- **Script Editor**—The Script Editor allows you to write new scripts or edit existing ones. From here:
  - Click to expand the Script Editor to full size. When in full-size mode, click to restore the window to its original size.
  - Click to close the editor and discard your changes.

- **Script Labels**—Apply labels to the script currently selected. From here, click to save your changes.

**Adding a New Script**

To add a new script:

---

**Step 1**  
On the Administration tab, click **Scripts**.

**Step 2**  
Click .  
The system displays the Script Editor window.

**Step 3**  
In the Name field, enter the name of the script.

**Step 4**  
In the Code field, enter a unique identifier for this script.

**Step 5**  
Select where you want the script to execute. You can select more than one of the following locations:

- **Users**—Script executes on user accounts.
- **Events**—Script executes upon specific events.
- **Bulk Operations**—Script executes during bulk operations.
- **Services**—Script executes on services.

**Step 6**  
Click **Add New Parameter** and specify a type, name, and description. Click **Add Another Parameter** to add additional parameters.

**Step 7**  
In the JavaScript Source text box, enter the code for the script.

**Step 8**  
Select a script label, if appropriate to the action.

**Step 9**  
Click .

---
Managing Events

An event is a predefined occurrence on a CPE that triggers scripts at specified moments. Events represent various points within the device's lifecycle. You cannot add new events to the list, but you can add new scripts to be run at each event point. An event can have multiple scripts. However, each script needs to be added one at a time.

Prime Home defines the following types of events:

- **Initial Contact**—Occurs when the server sees the CPE appear on its network for the first time.
- **Subscriber Associated**—Occurs when a device is associated to a subscriber. This event also occurs when a future device informs for the first time.
- **Reboot**—Occurs when the CPE reboots due to a power outage or specific request. This event also typically occurs with Initial Contact.
- **Service Enable**—Occurs after a service is enabled on a device.
- **Service Disable**—Occurs after a service is disabled on a device.

Editing a Script

*Note* You can edit any script in the system.

To edit a script:

**Step 1**
On the Administration tab, click **Scripts**.

**Step 2**
In the Script List, select the name of the script to edit.

The system displays the Script Editor window.

**Step 3**
Make changes to any of the fields.

**Step 4**
Click ![Save](image).  

Deleting a Script

*Note* Only custom scripts can be deleted from the system.

To delete a script:

**Step 1**
In the Script List, locate the script you want to delete.

**Step 2**
Click ![Delete](image) to delete your custom script from the system. The system refreshes the page, listing the remaining scripts.
- Firmware Upgraded—Occurs when firmware is upgraded.
- Inform—Occurs every time the CPE contacts the server, after any previously scheduled actions have run. Because this happens so frequently, it is a good idea to avoid using this event as a script trigger and to find a different way to accomplish your goal. For example, Reboot is generally a better alternative for reporting purposes.

## Events Window

Use the Events window (Figure 8-8) on the Administration tab to manage events and their actions. You can add new actions to events and rearrange the order in which the actions execute.

![Figure 8-8 Events Window](image)

The Events window comprises:
- Event List—Shows a list of all available events for the CPE. Click the event name from the list to open the Event Editor.
- Event Editor—Use the Event Editor to add new event actions or edit existing event actions. From here, you can:
  - Click to expand the Event Editor window to full size.
  - When in full-size mode, click to restore the window to its original size.
  - Click to cancel the event and discard your changes.
  - Click to save your changes.

## Adding a New Event Action

To add a new event action:

**Step 1** On the Administration tab, click Events.

**Step 2** Select an event from the Events List.

The system opens the Event Editor window.

**Step 3** Select an action from the Action drop-down list.

**Step 4** Click to add the action to the event. Some actions require user input to complete and display the appropriate fields.

**Step 5** Click Save.
Managing Announcements

You can create custom announcements to communicate with your CSRs. For example, you can use announcements to alert CSRs to problems or to issue reminders about new services.

*Note* The location of the announcements depends on how your Prime Home installation is configured. Announcements can be configured as a standalone service, or an announcements panel can be added to another service.

Prime Home supports the following types of announcements:

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Information</td>
</tr>
<tr>
<td>!</td>
<td>Warning</td>
</tr>
<tr>
<td>✗</td>
<td>Alert</td>
</tr>
</tbody>
</table>

---

Editing an Event Action

To edit an event action:

**Step 1** On the Administration tab, click **Events**.

**Step 2** In the Event List, select the name of the event.

**Step 3** In the Event Editor, click the name of the action.

**Step 4** Edit the properties for the action, if any.

**Step 5** Use the ↑ and ↓ icons to rearrange the order in which the actions execute.

**Step 6** Click ![Save](save-icon.png).

Deleting an Event Action

To delete an event action:

**Step 1** On the Administration tab, click **Events**.

**Step 2** In the Event List, select the name of an event.

**Step 3** Click ![Delete](delete-icon.png) next to the action you want to delete from the event.

**Step 4** Click ![Save](save-icon.png).
Using the Announcements Editor

Use the Announcements editor (Figure 8-9) to create your announcements.

Figure 8-9 Announcements Editor

Adding a New Announcement

To add a new announcement:

Step 1 On the Administration tab, click Announcements.
Step 2 Click to add a new announcement.
Step 3 From the Announcement Type menu, choose an announcement type.
Step 4 Enter the announcement text.
Step 5 Click .

Editing an Announcement

To edit an announcement:

Step 1 On the Administration tab, click Announcements.
Step 2 Edit announcements as desired.
Step 3 Click .
Deleting an Announcement

To delete an announcement:

**Step 1**  On the Administration tab, click **Announcements**.

**Step 2**  Locate the announcement to delete and click **Delete**.

Managing Device Synchronization

The Synchronization window (Figure 8-10) lets you view parameters that can be synchronized between the device and server. You can see which applications need to be initialized or synchronized, and you can select items to synchronize. Use the Synchronization window to assess any synchronization failures that occur when you use the primary tools under the Account and Services menus (on the left sidebar).

**Caution**

Do not use the Synchronization window for routine synchronizing of applications. This function is exposed for deep level troubleshooting and requires training for use. Instead, use the primary tools under the Account and Services drop-down menus; doing so invokes multiple applications that synchronize the entire device, not just parts of the device.

![Figure 8-10 Synchronization Window](image)

Resolving Synchronization Failures

If you receive a “failed to sync” error while using the primary tools under the Account and Services menu, do the following:

**Step 1**  Expand the **Advanced** drop-menu on the left sidebar.

**Step 2**  To the right of the Synchronization option, click **view**.
The Synchronization window opens.

**Step 3**  
In the State column, locate the “Failed” notification and check the corresponding **Pending Sync** check box.

**Step 4**  
Click **Save** to force the selected application to resynchronize.

**Step 5**  
Verify that the “failed to sync” error clears.
Reviewing Audit Logs

Audit logs give you a view into exactly what is happening on your system. An audit log records every transaction and event.

You can view the audit log based on a date range.

Filters help you find information by showing only:

- Changes made by a particular portal user, a subscriber, or the system (root) user.
- Changes applied during bulk operations or to a particular device, portal user, or subscriber.

Here are definitions of a few key terms:

- Portal users—Admins or CSRs who can make changes to device or subscriber records and to other portal users’ accounts.
- Subscribers—Customers who can make changes to their devices through the control panel. The audit log shows changes to local network and wireless settings, parental controls, and port forwarding.
- System—Refers to the system, or root, user who can make changes to any device or user.
- Device—Refers to a CPE device or a customer device attached to the CPE device’s LAN.

Launching the Audit Log

To launch the audit log:

**Step 1**
Click the **Audit** tab.

**Step 2**
In the Audit window, specify a range of dates to display information for. The default is the past five days.

**Step 3**
(Optional) From the Changed By menu, choose one of the following:

- Portal User—Enter the username of a portal user.
- Subscriber—Enter a subscriber code.
- System—Leave this value blank.
Step 4  (Optional) From the Applied To menu, choose one of the following:
- Bulk Operation—Leave this value blank.
- Device—Enter a device serial number.
- Portal User—Enter a portal username.
- Subscriber—Enter a subscriber code.

Step 5  Click Query.
Prime Home displays the audit results (Figure 9-1). You can do the following:
- Under each transaction, click Changes+ to see details about the transaction.
- Click expand all to view details about all transactions. Click collapse all to hide transaction details.
- Set the number of results to display per page.
- Page through the results.
- Refresh the results.

Figure 9-1  Audit Window

Step 6  To view a CSV file of results:
  a. In the Results window, clickweiservice.
  b. Click webservice.
Managing Bulk Operations

Bulk operations are a flexible, convenient tool designed to help you automate and keep tight control over every part of many common activities. They allow you to use built-in or custom actions to automate a wide range of common activities, whether you use Cisco CPEs or third party CPEs.

Certain bulk operations are limited when using third-party CPEs. Contact Cisco Customer Support if you have questions.

Bulk operations allow you to run actions against some or all of your CPEs, either passively or actively. If the action runs passively, each CPE is affected by the bulk operation as the CPE calls into the ACS during its regular inform. If the action runs actively, then, based on processing availability, the server solicits CPEs to call in for the update.

With bulk operations, you can:

- Stage complicated WAN changes
- Silently accomplish firmware updates
- Enable and disable services
- Cause browser redirection for CPEs with Wi-Fi security issues, taking subscribers to a page with security configuration tech tips

The Bulk Operations interface uses simple drag-and-drop functionality, allowing you to quickly create customized search criteria. Search criteria can be based on CPE information, subscriber information, or a combination of both. When you run a bulk operation action, the search criteria allow the action to run on only the CPEs and subscribers that match your specific requirements.
Preparing for Bulk Operations

Prior to running a bulk operation, verify that there are no other bulk operations scheduled to run at a time that interferes with this bulk operation’s schedule.

You can prevent an individual CPE from being selected for any bulk operation by going to the Customer Support tab, locating the device, displaying the Device window, and unchecking the Participates In Bulk Operations check box.

Before doing a bulk upgrade:

- Always test your bulk firmware update process in a lab first, then run a limited test on a subset of the target population before deploying.
- Notify your subscribers that the update is coming. Tell subscribers to make sure they leave their modem on.
- Have a plan to ship spare CPEs in the rare event of a failure. Understand which users have what services when you schedule updates, as some actions reboot the CPE.
- Prepare for an update by planning ahead.
- Verify that the firmware version for your CPE type has been loaded in the Administration tab. Review network usage charts for an appropriate maintenance time window. Between 2:00 a.m. and 5:00 a.m. is a suggested time window.
- Consider time zones when scheduling.
- Inform intervals:
  - If the CPEs have an inform interval of 7 hours and a bulk firmware operation has a 5 hour window on all days of the week, all CPEs should be expected to go through the bulk update process in 2 days.
  - If the CPEs have an inform interval of 23 hours and a bulk firmware operation has a 2 hour window on all days of the week, all CPEs should be expected to go through the bulk update process in 23 days.

Creating Bulk Operations

Figure 10-1 indicates the tasks that you need to complete when creating a bulk operation.
Examples of Bulk Operations

Two common uses for bulk operations are updating firmware and enabling or disabling a service. This section describes each of these scenarios.

Example 1: Update Firmware on All SR100G CPEs

This example should familiarize you with the overall process; it is not intended to cover specifics.

For this example, say you want to update the firmware on SR100G CPEs on your activation server. You want the update to run once, starting on Monday, November 5, 2012, and you want it to run during your maintenance window, which is Monday through Friday from 12:01 a.m. to 5:59 a.m.

**Step 1**

In Prime Home, click the **Bulk Operations** tab.

The system displays a list of existing bulk operations (Figure 10-2).

**Figure 10-2  Bulk Operations List**

<table>
<thead>
<tr>
<th>Name</th>
<th>Beginning Date</th>
<th>Occurs</th>
<th>Status</th>
<th>Delete</th>
</tr>
</thead>
<tbody>
<tr>
<td>Update SR100G firmware to 2.3.1.8</td>
<td>11/10/2010</td>
<td>Once</td>
<td>Completed</td>
<td></td>
</tr>
<tr>
<td>John</td>
<td>02/16/2011</td>
<td>Now</td>
<td>Cancelled</td>
<td></td>
</tr>
<tr>
<td>Service through bulk op</td>
<td>06/01/2011</td>
<td>Now</td>
<td>Completed</td>
<td></td>
</tr>
<tr>
<td>test content filter enable</td>
<td>06/20/2011</td>
<td>Now</td>
<td>Completed</td>
<td></td>
</tr>
<tr>
<td>Resync STUN</td>
<td>09/10/2011</td>
<td>Now</td>
<td>Completed</td>
<td></td>
</tr>
</tbody>
</table>

**Step 2**

Click to add a new bulk operation.

The Create Bulk Operations window opens (Figure 10-3).

**Step 3**

In the Name field, enter a descriptive name for the operation.

**Step 4**

Do one of the following:

- To contact devices without waiting for an inform, check the Solicit Devices check box.
- To wait for an inform to run the operation, uncheck the Solicit Devices check box.

**Step 5**

(Optional) In the Max Sessions field, enter the number of maximum concurrent sessions. Click to create a new bulk operation.

**Step 6**

From the Action drop-down list, choose **Update firmware**.

After making your selection, if the Action requires a parameter, a list opens containing values for that parameter. The Update Firmware action requires you to choose a version.
Figure 10-3  Create Bulk Operation Window

Bulk Operation
Name: Upgrade SRS500E firmware to 2.4.3.5
Solicit Devices: (check the device instead of waiting for a periodic inform)
Max Sessions: (optional, limit the number of concurrent sessions for this bulk operation)
Action: Update firmware

Parameters:
<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>The name of the firmware image to upload</td>
<td>2.4.3.5 (2012-01-09)</td>
</tr>
</tbody>
</table>

Schedule
Run: Once
Beginning Date: 04/28/2012
Day of Week: Sun Mon Tue Wed Thu Fri Sat
Run from: 12:00 AM to 5:59 AM All Day

Schedule Preview

April 2012 | May 2012 | June 2012
---|---|---
| Sun Mon Tue Wed Thu Fri Sat | Sun Mon Tue Wed Thu Fri Sat | Sun Mon Tue Wed Thu Fri Sat |
| 1 2 3 4 5 6 7 | 8 9 10 11 12 13 14 | 15 16 17 18 19 20 21 |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 8 | 9 | 10 | 11 | 12 | 13 | 14 |
| 15 | 16 | 17 | 18 | 19 | 20 | 21 |
| 22 | 23 | 24 | 25 | 26 | 27 | 28 |
| 29 | 30 | 31 | 1 | 2 | 3 | 4 |

Legend
- Devices are selected on the first day of this occurrence
- Devices are selected on the first day of this occurrence
- Devices may be processed

Available Columns
- Captive Portal Application Message
- Captive Portal Application State
- Captive Portal URL
- Click Through Application Message
- Click Through Application State
- Content Filtering Dynamic In Use
- Content Filtering Enabled
- Content Filtering In Use
- Content Filtering Static In Use
- Central Panel Application Message

Filter Criteria
And
Drag a column from Available Columns here to refine results.

Advanced Syntax

13 matching devices with device type ClearAccess SRS500E

[Create] [Cancel]
Step 7  From the Parameters/Value menu, choose the appropriate firmware version for the desired CPE.

The Schedule Preview area at the bottom of the page reflects your choices. After making a selection, an expandable area shows exactly which devices are affected by this bulk operation, if the bulk operation runs at this time.

Note  If you schedule the bulk operation to start running at a future date, the list might be slightly different when the bulk operation actually runs. New devices that meet the selection criteria might be added to the system, or existing devices might leave or change.

Step 8  From the Run menu, select **Once**.

Step 9  Set the following scheduling parameters:
- Beginning date: 11/5/2012
- Day of week: Mon, Tues, Wed, Thu, Fri
- Run from: 12:01 AM
- Run to: 5:59 AM

Step 10  Click **Create**.

The bulk operation is listed in the Find window along with the operation’s scheduled beginning date, frequency, and status (Figure 10-4).

Figure 10-4  Updated Bulk Operations List

![Updated Bulk Operations List](image)

Viewing Bulk Operation Progress

Once the update starts, you can click the name to see a dashboard view of the operation’s progress (Figure 10-5).

The dashboard shows the following:
- A summary of the bulk operation you are viewing.
- The results of the operation. You can filter the results by checking the **Pending**, **Active**, **Success**, **Failure**, and **Cancelled** check boxes. If the results are longer than one page, you can scroll through the results using the page controls. You can set how many results display on a page.
- A pie chart showing the results, including the number of CPEs with each status.
- A pie chart showing the failure results along with error codes.
### Examples of Bulk Operations

**Figure 10-5** Bulk Operations Dashboard

#### Upgrade SR500NE to 2.4.3.5

<table>
<thead>
<tr>
<th>Action</th>
<th>Update firmware</th>
<th>Number of Devices:</th>
<th>13</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Running</td>
<td>Occurs:</td>
<td>Now</td>
</tr>
<tr>
<td>Selecting Devices:</td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Schedule Preview

<table>
<thead>
<tr>
<th>April 2012</th>
<th>May 2012</th>
<th>June 2012</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sun</td>
<td>Mon</td>
<td>Tue</td>
</tr>
<tr>
<td>8</td>
<td>9</td>
<td>10</td>
</tr>
</tbody>
</table>

#### Criteria

- Filter Criteria
  - Manufacturer & Model
    - matches: ClearAccess SR500NE
  - Exclude From Bulk Operations
    - is: false

#### Devices

<table>
<thead>
<tr>
<th>Manufacturer</th>
<th>Model</th>
<th>Serial Number</th>
<th>Status</th>
<th>Details</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>ClearAccess</td>
<td>SR500NE</td>
<td>00225FB1B68D</td>
<td>Pending</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ClearAccess</td>
<td>SR500NE</td>
<td>00225FB1D94A</td>
<td>Pending</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ClearAccess</td>
<td>SR500NE</td>
<td>00225FB193F9</td>
<td>Pending</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ClearAccess</td>
<td>SR500NE</td>
<td>00225FB3119</td>
<td>Pending</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ClearAccess</td>
<td>SR500NE</td>
<td>00225FB3F435</td>
<td>Pending</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ClearAccess</td>
<td>SR500NE</td>
<td>00225FB266A9</td>
<td>Pending</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ClearAccess</td>
<td>SR500NE</td>
<td>00225FB3B58</td>
<td>Pending</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ClearAccess</td>
<td>SR500NE</td>
<td>00225FB2A2E</td>
<td>Pending</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ClearAccess</td>
<td>SR500NE</td>
<td>00225FB2658</td>
<td>Pending</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Legend

- Devices are selected on the first day of this occurrence
- Devices are selected on the first day of this occurrence
- Devices may be processed

#### Cancel Bulk Operation
Example 2: Enable Content Filtering on All CPEs

When you deploy a new service, you might want to enable it on all CPEs as a promotional event. This example describes how to use CPE filtering to enable the Content Filtering service for all subscribers within a ZIP code range of 30300 through 30399. You also decide that you want the service to enable when devices check in rather than soliciting them.

**Step 1**
From the Bulk Operations menu, select Create.

**Step 2**
In the Bulk Operation section (Figure 10-6), do the following:

1. Enter a name for the operation.
2. From the Action menu, choose Enable Service.
3. From the Parameters menu, choose Content Filtering.

**Figure 10-6 Create Bulk Operation Window—Bulk Operation Section**

<table>
<thead>
<tr>
<th>Create Bulk Operation Window—Bulk Operation Section</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Bulk Operation</strong></td>
</tr>
<tr>
<td><strong>Name:</strong> Enable Content Filtering</td>
</tr>
<tr>
<td><strong>Solicit Devices:</strong> (contact the device instead of waiting for a periodic inform)</td>
</tr>
<tr>
<td><strong>Max Sessions:</strong> (optional: limit the number of concurrent sessions for this bulk operation)</td>
</tr>
<tr>
<td><strong>Action:</strong> Enable Service</td>
</tr>
<tr>
<td><strong>Parameters:</strong></td>
</tr>
<tr>
<td><strong>Name</strong></td>
</tr>
<tr>
<td><strong>Value</strong></td>
</tr>
</tbody>
</table>

**Step 3**
From the Run drop-down list, choose Once and set the following scheduling parameters (Figure 10-7):

- Beginning date: 4/30/2012
- Select all days of the week
- Click All Day
Step 4  Specify your zip code filter to limit the promotion to a subset of Atlanta zip codes (Figure 10-8).
   a. From the Available Columns section, drag Postal Code to the Filter Criteria section.
   b. From the menu, choose is between.
   c. In the parameter fields, enter 30300 and 30399.
   d. Click Apply.

Step 5  Click Create.

As each device checks in, the Content Filtering service is enabled.
Best Practices for Working with Bulk Operations

Caution

Bulk Operations is a powerful tool that you should understand before you use. It is possible to adversely affect your subscribers’ services if you do not understand the actions you schedule.

Troubleshooting Failed Bulk Operations

Bulk Operations rarely fail on all CPEs, if you have set up the operation correctly. However, there can be “failed actions” on a particular CPE. In this case, Prime Home does not attempt to rerun the action against that CPE.

If the operation is scheduled to run multiple times, the CPE might “enter the pool” of selected CPEs a second time. Otherwise, determine the reason the action failed and then run another bulk operation that includes that CPE.

Controlling Maximum Throughput/Throttling

There are three base parameters that control the maximum throughput of Bulk Operations:

- `bulkOp.maximumConcurrentRunningBulkOperations`
- `bulkOp.timeBetweenSolicitingSchedulerSecs`
- `bulkOp.minimumTimeBetweenSolicitsMS`

The first, `bulkOp.maximumConcurrentRunningBulkOperations`, is the maximum number of bulk operations that can run at a given time.

The second and third parameters control the behavior of the bulk operations engine when there are free bulk operation slots. The process is described below.

When a bulk operations starts, there are $N$ number of free slots for bulk operations. The engine retrieves $N$ CPEs from the result set (the list of CPEs that are part of the bulk operation) to solicit. It then solicits the CPEs, and the spacing between those solicits is `bulkOp.minimumTimeBetweenSolicitsMS`.

For every interval defined in `bulkOp.timeBetweenSolicitingSchedulerSecs`, the engine checks for free bulk operation slots. If there are free slots, it grabs that number of CPEs from the result set and solicits them.

For passive bulk operations, solicits don’t occur. Instead, when a CPE informs, if it’s in the result set and there are free bulk operation slots, the bulk operation runs.

The maximum number of bulk operations is modified internally by the system, depending on the number of CPE sessions that are active. For example, if `tr069.maxConcurrentSessions` is set to 100, `bulkOp.maximumConcurrentRunning-BulkOperations` is set to 50, and there are 50 CPEs checked in, the maximum number of bulk operations is reduced by 50%. Current sessions equal 50% of the maximum sessions, and the number of bulk operations is reduced by that percentage.
Preparing to Run Firmware Update Operations

Preparation is the key to a successful bulk firmware update process. There are several things to consider before updating to a newer firmware version:

- Make and model—You can only choose one CPE type per process, but you can schedule multiple bulk operations.
- Firmware version—Verify that the firmware version being updated from will go directly to the new version. If the CPEs to be updated are on a firmware release that is very far behind the current release, you might need to perform interim updates prior to updating them to the current version. Contact Cisco Customer Support if you have questions.
- Firmware definition—View the firmware definition on the Firmware window of the Administration tab. If any changes need to be made, edit the firmware definition.
- Field preparation—Verify that all CPEs in the selected group are informing.
- Always run a test update on a small group of CPEs before running an update on a large group of CPEs.
- Labels—If you have applied a time zone-related label to your devices, searching by labels is useful when updating CPEs in multiple time zones.

Understanding Bulk Operation Options

You have many choices to make when creating your bulk operations. For information on creating a custom solution, one tailored to your specific needs, contact Cisco Advanced Services.

The section below describes some of the built-in options you have for:

- Actions—The types of operations you can run.
- Scheduling—Allows you to set when you want the action to start running and how often you want Prime Home to select the pool of CPEs to be acted on.
- CPE Selection—The CPEs you want this operation to run on.

Action Options

Actions are designed to carry out a specific set of instructions. Each built-in action is named so it describes what the action does.

Prime Home has built-in actions, but you can also contact Cisco Advanced Services to create custom actions. If you are an advanced user, you can create actions by going to the Scripts window on the Administration tab to add a new script.
Some actions have parameters that refine the action. For example:

- **Inform Interval**—This action sets the inform interval for all affected CPEs. You need to enter the parameter for the number of seconds between informs.

- **Enable/Disable Service**—This action allows you to turn a subscriber service on or off. When you choose this option, the Parameters area requires you to select a value, which is the service you want to enable or disable. To create a custom service, contact Cisco Advanced Services.

## Schedule Options

Table 10-1 describes the schedule options that are available for bulk operations.

<table>
<thead>
<tr>
<th>If you choose…</th>
<th>The ACS creates a list of CPEs that meet your criteria…</th>
<th>And the action runs on the list of CPEs…</th>
</tr>
</thead>
<tbody>
<tr>
<td>Now</td>
<td>When you click Create.</td>
<td>When you click Create.</td>
</tr>
<tr>
<td>Once</td>
<td>On the beginning date.</td>
<td>On the first scheduled weekday after the beginning date.</td>
</tr>
<tr>
<td>Weekly</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• First time—On the beginning Date.</td>
<td>On the first scheduled weekday after the beginning date and every scheduled day thereafter.</td>
</tr>
<tr>
<td></td>
<td>• Each subsequent time—On the same weekday every week. For example, if the beginning date is Thursday, February 2nd, a new list of CPEs is chosen each Tuesday after that date.</td>
<td></td>
</tr>
<tr>
<td>Monthly</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• First time—On the beginning date.</td>
<td>On the first scheduled weekday after the beginning date and every scheduled day thereafter.</td>
</tr>
<tr>
<td></td>
<td>• Each subsequent time—On the same calendar day every month. For example, if the beginning date is February 2nd, a new list of CPEs is chosen March 2nd, April 2nd, and so on.</td>
<td></td>
</tr>
</tbody>
</table>

## CPE Selection Options

You have two options for selecting which CPEs are affected by a bulk operation:

- Use the options available from within Bulk Operations as shown in the examples.

- If you have Prime Home Reporting, you can design a report to select the desired CPEs and apply a label to all of the selected CPEs. You can then filter the CPEs by label for the bulk operation.

You can view the CPEs selected for a bulk operation by expanding the Matching Devices section at the bottom of the Create Bulk Operation window.
Troubleshooting Tools

Prime Home provides the following tools to help troubleshoot your system:

- Import Subscriptions utility—Allows you to batch upload your subscriber data.
- RESTful tool—A diagnostic tool that lets you run actions against URLs and call the integration API directly.

Import Subscriptions Utility

Use the Import Subscriptions utility to batch upload subscription information. A subscription includes many pieces of data including subscriber, services, device information, device settings, device labels, and subscriber login credentials for the control panel.

Your data must be in a CSV file and conform to the format described in Appendix A, “Subscription Import Files.”

The following options are available, as shown in Figure 11-1:

- Choose File button—Click to navigate to the CSV file you want to upload.
- File path—Indicates the file to be uploaded and its location.
- Upon completion check box—Select so Prime Home sends a summary e-mail when the import is completed.
- Upload button—Click to upload a CSV file that processes and loads subscriber information into the database.

Figure 11-1 Import Subscriptions Utility
Importing Multiple Subscriptions

To import multiple subscriptions:

---

**Step 1** On the Utilities tab, click **Import Subscriptions**.

**Step 2** Click **Choose File**.

**Step 3** In the system dialog box, choose a CSV file to upload.

**Step 4** Click **Upload**.

Prime Home imports your data, displays a progress bar, and informs you of success.

---

RESTful Service Tool

The RESTful service tool lets you run actions against URLs and call the integration API directly. The following options are available, as shown in Figure 11-2:

- **Operation**—Choose an HTTP verb from the drop-down list, and then enter a URL in the text box.
- **Execute**—Click to run the operation on the desired URL.

---

**Figure 11-2**  RESTful Service Tool

![RESTful Service Tool](image)
Control Panel for Subscribers

The Prime Home Control Panel for subscribers is a browser-based application that helps the end user to manage, protect and share their home network. It enables the subscriber to easily modify basic home network configuration such as wireless, firewall, and port forwarding, and provides a way to setup enhanced services such as time blocking and content filtering. The Control Panel provides remote access to the home network, providing a one-click process to access any IP-enabled device in the home.

What’s on the Main Screen

The following options are available:

- **Network Status**—Shows whether broadband is connected, and whether wireless networking is enabled.
- **My Network**—This shows how many LAN devices are known to the local network, and how many are online. When the subscriber logs in, the complete list of devices connected to the network is automatically displayed on the right-hand side of the screen.
- **My Wireless Network**—Here the subscriber can enable or disable their wireless, or modify wireless settings, such as changing their WEP Key, changing the wireless broadcast channel, and enabling/disabling the broadcast of their SSID.
- **Internet Time Blocking**—This allows the subscriber to set time limits on the Internet can be accessed. The subscriber can set individual blocks of time throughout the week to be blocked, limit the amount of time the Internet can be accessed each day, and limit the amount of time it can be accessed each week. There is also a Bonus Time feature which overrides the normal schedule and adds timed access starting immediately for a set amount of time.
- **Content Filtering**—Content filtering is used to prevent users from viewing inappropriate web sites or content. Filtering can be implemented on individual computers and devices or on the entire network. It is possible for different computers and devices on the network to have different levels of Internet access. There are two types of content filtering: Basic content filtering and Dynamic content filtering.
Importing Multiple Subscriptions

To import multiple subscriptions:

1. On the Utilities tab, click **Import Subscriptions**.
2. Click **Choose File**.
3. In the system dialog box, choose a CSV file to upload.
4. Click **Upload**.

Prime Home imports your data, displays a progress bar, and informs you of success.

RESTful Service Tool

The RESTful service tool lets you run actions against URLs and call the integration API directly. The following options are available, as shown in Figure 12-1:

- **Operation**—Choose an HTTP verb from the drop-down list, and then enter a URL in the text box.
- **Execute**—Click to run the operation on the desired URL.
Subscription Import Files

To import a subscription file (Figure A-1) into Prime Home, you must use an ISO-8859-1 encoded CSV file.

Figure A-1  Sample Subscription Import File

```
SerialNumber,ProvisioningCode,SubscriberCode,Subscriber.FullName,
Subscriber.EmailAddress,Subscriber.Address.1.Type,Subscriber.Address.1.City,Subscriber.Address.1.State,
Subscriber.Address.1.Street,Subscriber.Address.1.Zip,Subscriber.Phone.1.Type,Subscriber.Phone.1.Number,
Service.packageA,Service.packageB
00000000f4240,000000,,jada.clark,f4240,JadaGwena,jada.clark.1000000@test.com,mailing,Cleveland,Wa,5630
Oakway,,96206,home,311-188-2268,off,off
00000000f4241,000000,,alexander-10-f4241,AlexanderKo,alexander.10.1000001@test.com,mailing,Clayton,Id,5210 Silent
Blvd.,91464,home,909-809-3583,off,off
00000000f4242,000000,,waltz-williams-54262,Waltz
Williams,waltz,williams.1000002@test.com,mailing,Centerville,OH,5630 Battery
Hd.,92027,home,604-218-5782,can,off
00000000f4243,000000,,isahak-Com-f4243,IsaiahKow,Isaiah.Com.1000003@test.com,mailing,Bellevue,Id,5630 Martin Luther King
Ave.,20682,home,205-428-2107,off,off
```

The first line of the subscription file contains headers that are described in Table A-1.

<table>
<thead>
<tr>
<th>Column</th>
<th>Presence</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operation</td>
<td>Optional</td>
<td>+ or -, causing the record to be either updated or removed. Omitting this column causes the subscription file to be treated as if it were being updated.</td>
</tr>
<tr>
<td>SubscriberCode</td>
<td>Required</td>
<td>A unique identifier for the subscriber.</td>
</tr>
<tr>
<td>SerialNumber</td>
<td>Required, unless ProvisioningCode</td>
<td>The serial number of the device. If a value is specified in a row for this column, an OUI must also be specified in that row.</td>
</tr>
<tr>
<td>OUI</td>
<td>Required, unless ProvisioningCode</td>
<td>The OUI of the device. If a value is specified in a row for this column, a SerialNumber must also be specified in that row.</td>
</tr>
<tr>
<td>ProvisioningCode</td>
<td>Required, unless SerialNumber/OUI</td>
<td>An ISP-specific, unique provisioning code for the device. If this value is present, a serial number/OUI is not required. However, if both are present, the serial number/OUI gains precedence.</td>
</tr>
<tr>
<td>Subscriber.(PropertyName)</td>
<td>Optional, multiple</td>
<td>Specifies a subscriber property name.</td>
</tr>
</tbody>
</table>
### Table A-1 Subscription Import File Headers (continued)

<table>
<thead>
<tr>
<th>Column</th>
<th>Presence</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service.(ServiceName)</td>
<td>Optional, multiple</td>
<td>Specifies a service that is already defined in the system. Values for rows under this column can be On or Off.</td>
</tr>
<tr>
<td>Settings.(PropertyName)</td>
<td>Optional, multiple</td>
<td>Specifies a settings property name.</td>
</tr>
<tr>
<td>Label.(PropertyName)</td>
<td>Optional, multiple</td>
<td>Specifies a label that is already defined in the system. Values for rows under this column can be On or Off.</td>
</tr>
<tr>
<td>CP.UserName</td>
<td>Optional, but required if there is a CP.Password, CP.OverwriteLogin, or a CP.SendEmail field</td>
<td>The subscriber’s control panel username. If credentials already exist and CP.OverwriteLogin is not set to On, an error message is displayed and the credentials do not change.</td>
</tr>
<tr>
<td>CP.Password</td>
<td>Optional, but required if there is a CP.UserName, CP.OverwriteLogin, or a CP.SendEmail field</td>
<td>The subscriber’s control panel password. If credentials already exist and CP.OverwriteLogin is not set to On, an error message is displayed and the credentials do not change.</td>
</tr>
<tr>
<td>CP.OverwriteLogin</td>
<td>Optional, but required if there is a CP.Password, CP.UserName, or a CP.SendEmail field</td>
<td>Instructs the import process to overwrite the login credentials for this subscriber if they already exist. Values for rows under this column can be On or Off.</td>
</tr>
<tr>
<td>CP.SendEmail</td>
<td>Optional</td>
<td>This column header specifies whether or not to send an e-mail to the subscriber containing the subscriber’s control panel login credentials. The e-mail address is specified in Subscriber. EmailAddress. Values for rows under this column can be On or Off.</td>
</tr>
</tbody>
</table>
Common Error Messages and Fault Codes

This section covers the error messages and fault codes that you are most likely to see in Cisco Prime Home. Refer to the following topics for more information:

- Error Messages, page B-3
- TR-069 Fault Codes, page B-5

Error Messages

This topic describes the four most common error messages displayed by Cisco Prime Home and how to best deal with them.

Error Message  Synchronization failed.

Explanation  When either a device is informing or you are attempting to save changes to a device, a timeout occurs, resulting in one or more applications failing to complete their synchronization with the device.

Recommended Action  Use the Synchronization tool to resolve this state:
1. From the left sidebar, expand the Advanced drop-down list and look for "Synchronization."
2. Skim the State column for the "Failed" notification.
3. Check the adjacent check box under the Pending Sync column.
4. Click Save to force that specific application to attempt to synchronize again.

These steps may clear the error and put things back on track before you need to resort to a reboot or other potentially service affecting measures.
**Error Message** Device could not be contacted.

**Explanation** This error implies that the physical connection to the device has been severed in some fashion. This could be either a connection issue or another problem within the confines of the customer premise. This message could also indicate network congestion or a variety of possible problems with the outside plant/Telco infrastructure.

**Recommended Action** Do the following:
1. Confirm that the CPE device is plugged in and powered up, and that the LED indicators for WAN connectivity are lit.
2. Unplug and reseat the Ethernet cable from both the wall jack and the CPE WAN port end of the cable.
3. Consider rebooting the CPE device (note that Cisco Prime Home has the means to trigger a reboot remotely).
4. Consider replacing the Ethernet cable if it appears faulty.

**Error Message** Unknown error during refresh. Retry later.

**Explanation** One or more web calls that populate the page contents failed. This symptom may manifest with no message at all and the page simply does not populate completely.

**Recommended Action** Do the following:
1. Reload the page.
2. If the problem persists, try clearing the browser cache, history, cookies, and so on. Then, reload the page again.

**Error Message** Device Not Supported

**Explanation** Prime Home 5.1 has changed how device support is controlled. In previous versions of the product, the system would attempt to work with any device that informed. This caused several problems:
- Synchronizing applications that are not supported on the device; for example, trying to push PPP settings to an STB device.
- Incorrectly pushing other values to a device; for example, pushing "Mixed" as the wireless security type when the device does not support it.
- Displaying UI elements for a device that are not applicable for that device; for example, displaying Time Blocking when the device does not support it.
- Calls to Cisco's operational support team when rogue devices cause problems with system resources.

The Prime Home management platform now employs a white-list for devices. This means that Cisco must explicitly enable support for each device type before devices of that type can be used by the system. If you select a device from the "find device" page and you are taken to a message indicating that your device is not supported, this is expected behavior for devices that have not been configured for your particular instance of Cisco Prime Home.
Recommended Action  If you require support for a new device type, open a work request with the Prime Home Operational Support team. Please include the following information in your request:
  – Manufacturer
  – Product class
  – Software version
  – Hardware version

TR-069 Fault Codes

This topic describes the actions you should take when Prime Home displays either a TR-069 CPE or ACS fault code.

Error Message  Refer to Table B-1 and Table B-2 for a list of the fault codes that are generated by CPE and ACS and displayed via the Prime Home user interface.

Explanation  The device passing one of these codes has probably not been properly tested for interoperability with the Prime Home ACS.

Recommended Action  Check for the following:
  – A new device that was not previously being managed by Prime Home has been placed on the network and is attempting to interact with the ACS.
  – An existing device loaded with new firmware from its manufacturer that has not had the benefit of proper testing and driver development has been placed on the network.

In either case, open a work request with the Prime Home group for information on interoperability testing procedures and services.

CPE Fault Codes

Table B-1 provides a complete listing of the CPE fault codes that can be displayed in Prime Home.

<table>
<thead>
<tr>
<th>Fault Code</th>
<th>Description</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>9000</td>
<td>Method not supported</td>
<td>Server</td>
</tr>
<tr>
<td>9001</td>
<td>Request denied (no reason specified)</td>
<td>Server</td>
</tr>
<tr>
<td>9002</td>
<td>Internal error</td>
<td>Server</td>
</tr>
<tr>
<td>9003</td>
<td>Invalid arguments</td>
<td>Client</td>
</tr>
<tr>
<td>9004</td>
<td>Resources exceeded (when used in association with SetParameterValues, this must not be used to indicate parameters in error)</td>
<td>Server</td>
</tr>
</tbody>
</table>
### Table B-1  CPE Fault Codes (continued)

<table>
<thead>
<tr>
<th>Fault Code</th>
<th>Description</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>9005</td>
<td>Invalid parameter name (associated with Set/GetParameterValues,</td>
<td>Client</td>
</tr>
<tr>
<td></td>
<td>GetParameterNames, Set/GetParameterAttributes AddObject, and DeleteObject)</td>
<td></td>
</tr>
<tr>
<td>9006</td>
<td>Invalid parameter type (associated with SetParameterValues)</td>
<td>Client</td>
</tr>
<tr>
<td>9007</td>
<td>Invalid parameter value (associated with SetParameterValues)</td>
<td>Client</td>
</tr>
<tr>
<td>9008</td>
<td>Attempt to set a nonwritable parameter (associated with SetParameterValues)</td>
<td>Client</td>
</tr>
<tr>
<td>9009</td>
<td>Notification request rejected (associated with SetParameterAttributes method)</td>
<td>Server</td>
</tr>
<tr>
<td>9010</td>
<td>Download failure (associated with Download, TransferComplete, or</td>
<td>Server</td>
</tr>
<tr>
<td></td>
<td>AutonomousTransferComplete methods)</td>
<td></td>
</tr>
<tr>
<td>9011</td>
<td>Upload failure (associated with Upload, TransferComplete, or</td>
<td>Server</td>
</tr>
<tr>
<td></td>
<td>AutonomousTransferComplete methods)</td>
<td></td>
</tr>
<tr>
<td>9012</td>
<td>File transfer server authentication failure (associated with Upload,</td>
<td>Server</td>
</tr>
<tr>
<td></td>
<td>Download, TransferComplete, or AutonomousTransferComplete methods)</td>
<td></td>
</tr>
<tr>
<td>9013</td>
<td>Unsupported protocol for file transfer (associated with Upload and</td>
<td>Server</td>
</tr>
<tr>
<td></td>
<td>Download methods)</td>
<td></td>
</tr>
<tr>
<td>9014</td>
<td>Download failure: unable to join multicast group (associated with</td>
<td>Server</td>
</tr>
<tr>
<td></td>
<td>Download, TransferComplete, or AutonomousTransferComplete methods)</td>
<td></td>
</tr>
<tr>
<td>9015</td>
<td>Download failure: unable to contact file server (associated with</td>
<td>Server</td>
</tr>
<tr>
<td></td>
<td>Download, TransferComplete, or AutonomousTransferComplete methods)</td>
<td></td>
</tr>
<tr>
<td>9016</td>
<td>Download failure: unable to access file (associated with Download,</td>
<td>Server</td>
</tr>
<tr>
<td></td>
<td>TransferComplete, or AutonomousTransferComplete methods)</td>
<td></td>
</tr>
<tr>
<td>9017</td>
<td>Download failure: unable to complete download (associated with Download,</td>
<td>Server</td>
</tr>
<tr>
<td></td>
<td>TransferComplete, or AutonomousTransferComplete methods)</td>
<td></td>
</tr>
<tr>
<td>9018</td>
<td>Download failure: file corrupted (associated with Download,</td>
<td>Server</td>
</tr>
<tr>
<td></td>
<td>TransferComplete, or AutonomousTransferComplete methods)</td>
<td></td>
</tr>
<tr>
<td>9019</td>
<td>Download failure: file authentication failure (associated with Download,</td>
<td>Server</td>
</tr>
<tr>
<td></td>
<td>TransferComplete, or AutonomousTransferComplete methods)</td>
<td></td>
</tr>
<tr>
<td>9800-9899</td>
<td>Vendor-defined fault codes</td>
<td>—</td>
</tr>
</tbody>
</table>
ACS Fault Codes

Table B-2 provides a complete listing of the ACS fault codes that can be displayed in Prime Home.

<table>
<thead>
<tr>
<th>Fault Code</th>
<th>Description</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>8000</td>
<td>Method not supported</td>
<td>Server</td>
</tr>
<tr>
<td>8001</td>
<td>Request denied (no reason specified)</td>
<td>Server</td>
</tr>
<tr>
<td>8002</td>
<td>Internal error</td>
<td>Server</td>
</tr>
<tr>
<td>8003</td>
<td>Invalid arguments</td>
<td>Client</td>
</tr>
<tr>
<td>8004</td>
<td>Resources exceeded</td>
<td>Server</td>
</tr>
<tr>
<td>8005</td>
<td>Retry request</td>
<td>Server</td>
</tr>
<tr>
<td>8800 - 8899</td>
<td>Vendor-defined fault codes</td>
<td></td>
</tr>
</tbody>
</table>